



# NETAŞ Server

## BMC User Guide (BMC V4)

---

Version: R1.1

NETAŞ TELEKOMÜNIKASYON A.Ş  
Yenişehir Mahallesi Osmanlı Bulvarı Aeropark Sitesi  
B Blok No:11B İç Kapı No:40  
Postcode: 34912  
Tel: +90 (216) 522 20 00  
URL: <https://destek.netas.com.tr>  
E-mail: [info@netas.com.tr](mailto:info@netas.com.tr)

## LEGAL INFORMATION

---

Copyright 2024 NETAŞ CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of NETAŞ CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of NETAŞ CORPORATION or of their respective owners.

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. NETAŞ CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

NETAŞ CORPORATION 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 NETAŞ CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

NETAŞ CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the NETAŞ technical support website <http://support.NETAŞ.com.cn> to inquire for related information.

The ultimate right to interpret this product resides in NETAŞ CORPORATION.

### 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 NETAŞ, 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. NETAŞ will provide technical support for the embedded software of this product.

## Revision History

---

Revision No.	Revision Date	Revision Reason
R1.1	2024-04-24	Fully updated.
R1.0	2023-09-07	First edition.

Serial Number: SJ-20230907115354-004

Publishing Date: 2024-04-24 (R1.1)

# Contents

---

<b>1 BMC Overview.....</b>	<b>1</b>
1.1    Operating Principle.....	1
1.2    Functions.....	3
1.3    Software Security.....	4
1.4    1.4 Operation Interfaces.....	7
<b>2 Performing Client Commissioning.....</b>	<b>9</b>
<b>3 Logging In to the Web Portal of the BMC.....</b>	<b>14</b>
<b>4 Common Operations.....</b>	<b>20</b>
4.1    Logging In to the BMC Through SSH.....	20
4.2    Logging In to the BMC Through a Serial Port.....	22
4.3    Modifying the BMC Address.....	25
4.4    Checking Server Information.....	26
4.5    Managing Storage Devices.....	27
4.6    Installing an OS Remotely.....	30
4.7    Resetting the BMC When the Web Portal Is Unavailable.....	36
4.8    Querying and Configuring Services.....	37
4.9    Configuring an NTP Server.....	40
4.10    Configuring an SMTP Server.....	41
4.11    Configuring Trap Notification Parameters.....	42
4.12    BMC Log Export.....	44
4.12.1    Exporting Logs in One Click Through the Web Portal.....	45
4.12.2    Exporting Logs by Category Through the Web Portal.....	46
4.12.3    Exporting Logs Through the CLI (SSH).....	47
4.12.4    Exporting Logs Through the CLI (Serial Port).....	47
4.13    Upgrading the BMC Firmware.....	48
4.14    Restoring Factory Defaults.....	49
4.15    Backing Up BMC Configurations.....	50
4.16    Creating an SNMP User.....	51
<b>5 System Management.....</b>	<b>55</b>
5.1    Querying System Information.....	55
5.2    Querying Performance Data.....	56
5.3    Querying Fan Information.....	58

---

5.4	Configuring the Heat Dissipation Policy.....	59
5.5	Querying Temperature KPIs.....	60
5.6	Managing Storage Devices.....	62
5.7	Powering On/Off the Server.....	64
5.8	Configuring the Server Startup Policy.....	65
5.9	Configuring Power-On Delay Parameters.....	66
5.10	Querying Power Supply Information.....	67
5.11	Configuring the Power Mode.....	68
5.12	Querying Power Statistics.....	69
5.13	Configuring Power Control Parameters.....	70
5.14	Querying Power KPIs.....	72
5.15	Configuring Boot Options.....	73
5.16	Configuring the Serial Port Output Mode.....	74
<b>6</b>	<b>Diagnosis and Maintenance.....</b>	<b>76</b>
6.1	Querying Alarms.....	76
6.2	Alarm Reporting Parameter Configuration.....	77
	6.2.1 Configuring Trap Notification Parameters.....	78
	6.2.2 Configuring Syslog Notification Parameters.....	80
	6.2.3 Configuring Email Notification Parameters.....	81
6.3	Configuring Screen Recording Parameters.....	83
6.4	Viewing Recorded Videos.....	85
6.5	Taking a Screenshot.....	86
6.6	Viewing POST Codes.....	87
6.7	Downloading Server Logs.....	88
6.8	Querying BMC Logs.....	89
6.9	Querying SEL Logs.....	90
<b>7</b>	<b>Service Management.....</b>	<b>92</b>
7.1	Configuring Port Service Parameters.....	92
7.2	Configuring Web Service Parameters.....	94
7.3	Configuring KVM Service Parameters.....	97
7.4	Starting the KVM.....	99
7.5	Configuring Virtual Media Parameters.....	108
7.6	Mounting a Virtual Media Device.....	111
7.7	Configuring VNC Parameters.....	112

7.8	Configuring SNMP Parameters.....	114
<b>8</b>	<b>BMC Management.....</b>	<b>117</b>
8.1	Network Parameter Configuration.....	117
8.1.1	Configuring the Host Name.....	117
8.1.2	Configuring the Network Port Mode.....	119
8.1.3	Configuring IP Addresses of Network Ports.....	121
8.1.4	Configuring the DNS.....	123
8.1.5	Configuring a VLAN.....	125
8.2	Setting the Time of the BMC.....	127
8.3	Resetting the BMC on the Web Portal of the BMC.....	130
8.4	Upgrading Firmware.....	131
8.5	Updating BMC Configurations.....	133
8.6	Restoring Factory Defaults.....	135
<b>9</b>	<b>User and Security.....</b>	<b>136</b>
9.1	Adding a Local User.....	136
9.2	Configuring Authentication Parameters for Domain Users.....	138
9.3	Querying Online Users.....	142
9.4	Configuring Permissions for a Customized Role.....	143
9.5	Configuring Security Enhancement Parameters.....	144
9.6	Configuring Firewall Parameters.....	145
9.7	Configuring Two-Factor Authentication.....	147
<b>10</b>	<b>Reference: Default Passwords.....</b>	<b>149</b>
<b>11</b>	<b>Reference: Accessing Documents.....</b>	<b>150</b>
	<b>Glossary.....</b>	<b>154</b>

# About This Manual

---

## Purpose

This manual describes the **BMC** management software of **NETAŞ** 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, Logging In to the Web Portal of the BMC	Describes how to log in to the Web portal of the BMC.
Chapter 4, Common Operations	Describes common operations in the BMC.
Chapter 5, System Management	Describes how to perform system management operations.
Chapter 6, Diagnosis and Maintenance	Describes how to perform diagnosis and maintenance operations.
Chapter 7, Service Management	Describes how to perform service management operations.
Chapter 8, BMC Management	Describes how to perform BMC management operations.
Chapter 9, User and Security	Describes how to perform user and security management operations.
Chapter 10, Reference: Default Passwords	Describes the default passwords that are used to log in to the BMCs in <b>NETAŞ</b> servers of different models.

Chapter 11, 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.

V

VI



# Chapter 1

# BMC Overview

---

## Table of Contents

Operating Principle.....	1
Functions.....	3
Software Security.....	4
Operation Interfaces.....	7

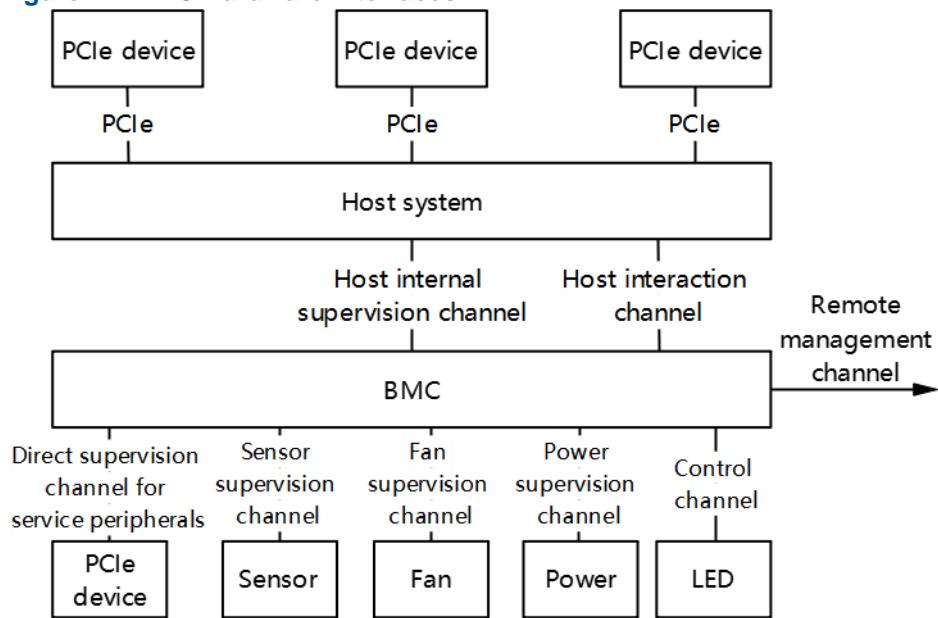
The **BMC** is the management system of a NETAŞ server, which monitors and manages server hardware, and provides a Web portal for operation and maintenance, achieving the purposes of software and hardware configuration, fault diagnosis, operating system installation, and operations on the server.

## 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**

For a description of the BMC channels, refer to [Table 1-1](#).

**Table 1-1 BMC Hardware Channel Descriptions**

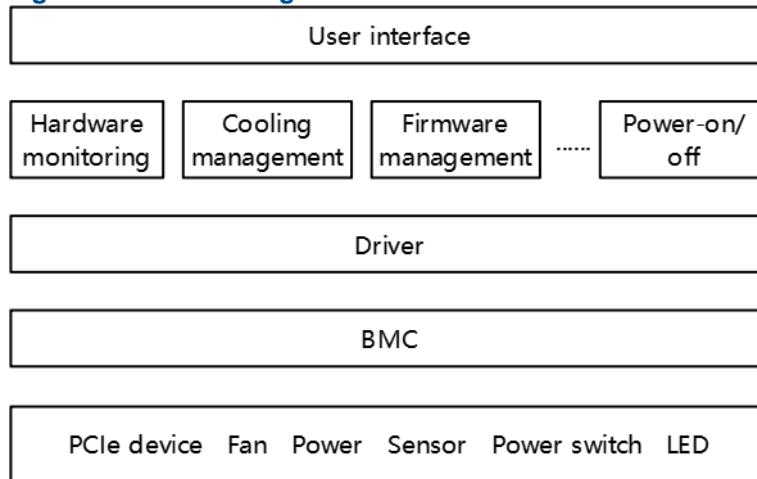
Channel	Typical Physical Link	Typical Management Object or Function
Service peripheral supervision channel	PCIe and SMBUS	PCIe devices of a server
Host internal supervision channel	SMBUS and PECI	Internal functional units of the CPU or bridge chip
Host interaction channel	PCIe, USB, LPC, KCS, and SMBUS	Supports KVM, virtual media function, and host serial port functions, and the IP-MI 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 <b>SGPIO</b>	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 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 the syslog, [SNMP](#) trap, email 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 [BIOS](#)s 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 → 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, and [HTTP](#).

### 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 time period, 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.
- Retrieval of lost user identity authentication information: If a user password is lost, it can be retrieved by email.
- Certificate service: The BMC supports certificate encryption and import services, which can only be operated by the administrator. The system supports the secure certificate signature algorithm, supports certificate validity period configuration, and prompts on certificate expiration, or about to expire.

## 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, maintenance logs, and security 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.
- Log backup: If the local storage space is insufficient, logs can be transferred to other storage space through [FTP](#).
- 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.
- Vulnerability-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 thirdparty 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, you can log in to the Web portal of the [BMC](#) on a client through the [iSAC](#) management network port of a server. Before logging in to the Web portal of the BMC for the first time, you need to commission the client to ensure that it is interconnected with the [iSAC](#) management network port.

## Prerequisite

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

---

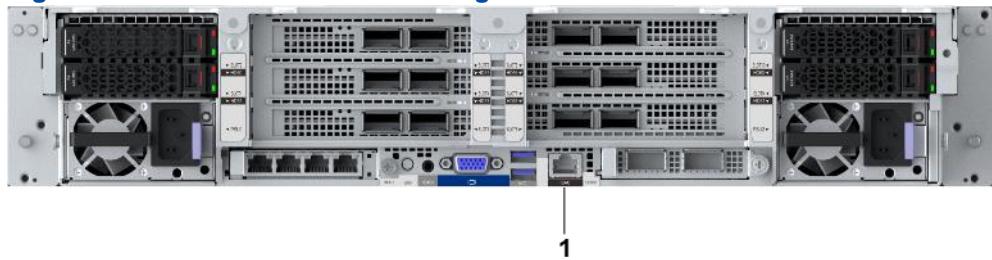


Google Chrome 59 and later versions are recommended.

---

## Context

The default [IP](#) address of the [iSAC](#) management network port of a server is 192.168.5.7. [Figure 2-1](#) shows the position of the [iSAC](#) management network port on the rear panel of the server.

**Figure 2-1 Position of the iSAC Management Network Port**

1. iSAC management network port



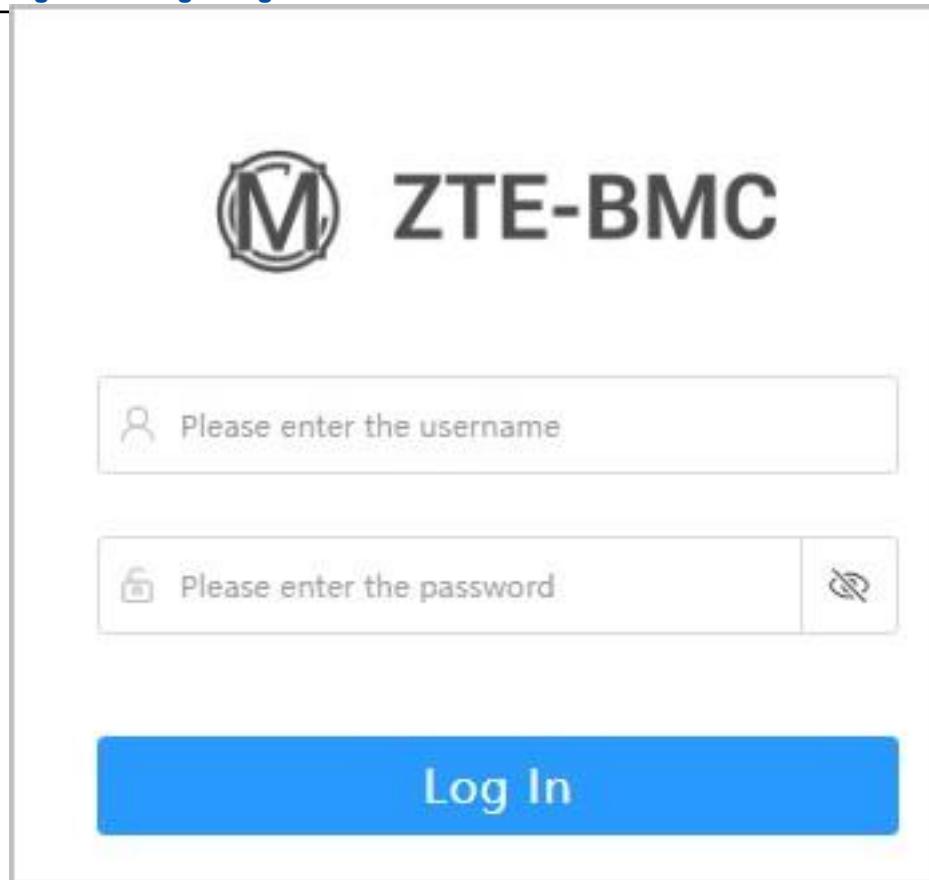
The network port with the **iSAC** silk screen on the rear panel of a server identifies the iSAC management network port. The locations of the iSAC management network interfaces on different servers are slightly different. This procedure uses an R5300 G5 server as an example to describe the position of the iSAC management network port. For other servers, refer to the corresponding [Hardware Description](#).

### Steps

1. Connect the PC to the iSAC management network port on the rear panel of the server through a network cable.
2. On the PC, change the IP address of the PC to an IP address (for example, 192.168.5.8) in the same network segment as 192.168.5.7.
3. On the PC, launch the specified browser.
4. In the address bar of the browser, enter <https://192.168.5.7> and press **Enter**. The page for login is displayed, see [Figure 2-2](#).

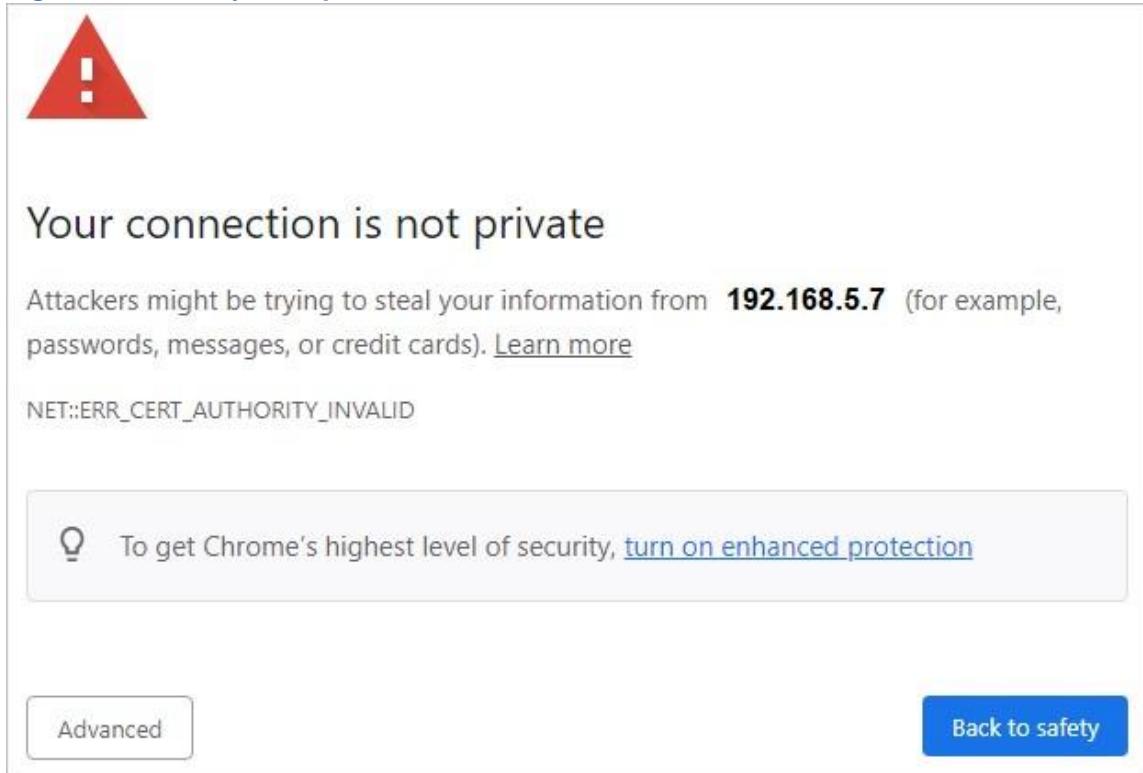
[2 Performing Client Commissioning](#)

Figure 2-2 Login Page



If the prompt information as shown in Figure 2-3 is displayed before login, click **Advanced** and select **Proceed to** to enter the login page.

**Figure 2-3 Security Prompt**



5. Enter your username and password.



**Note**

The default username and password are as follows:

- Username: Administrator
- Password: Superuser9!

To unhide the password, you can click the  button on the right.



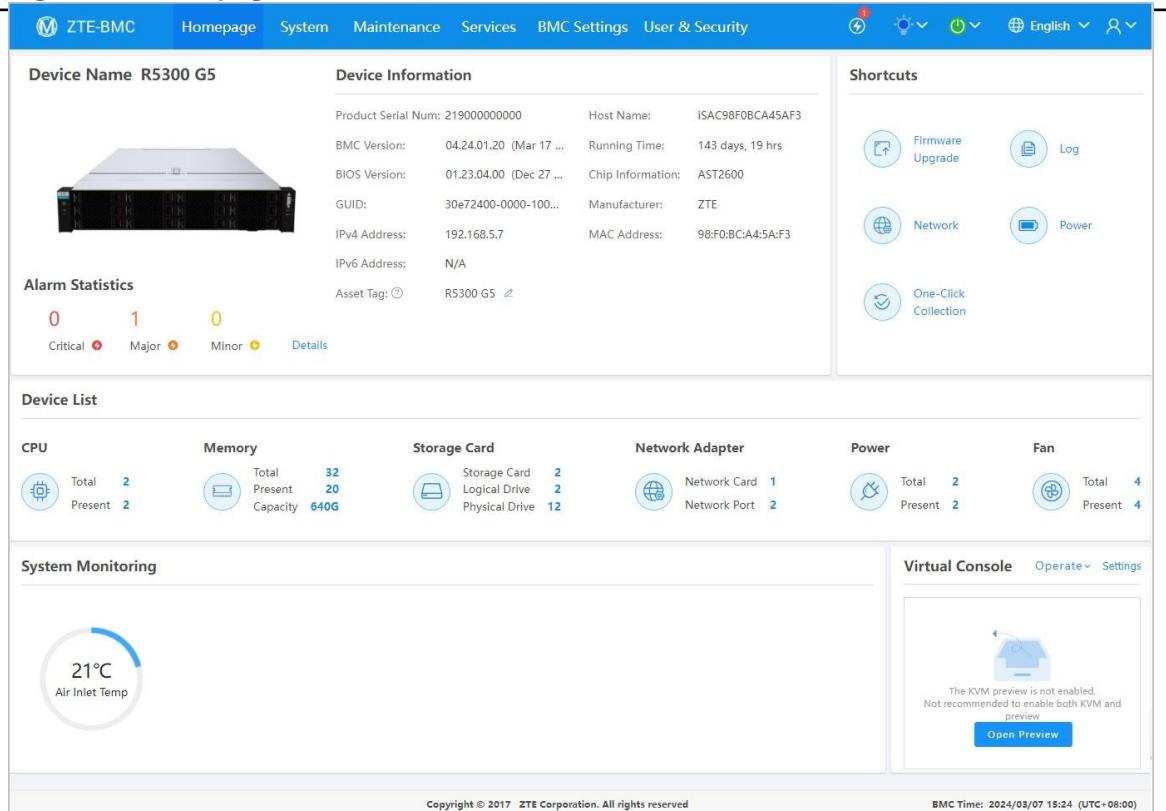
**Note**

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. Click **Log In**, The **Homepage** of the Web portal of the BMC is displayed, see [Figure 2-4](#).

2 Performing Client Commissioning

Figure 2-4 Homepage



- Set the IP address of the iSAC management network port as planned, for example, 10.235.51.202.



#### Note

For how to set the IP address of the iSAC management network port, refer to [8.1.3 Configuring IP Addresses of Network Ports](#).

- Record the IP address of the iSAC management network port.
- Connect the iSAC management network port to the corresponding switch through a network cable.
- On the PC, change the IP address of the PC to an IP address (for example, 10.235.51.203) in the same network segment that the iSAC management network port belongs to.
- Connect the PC to the corresponding switch through a network cable, so that the PC and the iSAC management network port are in the same [LAN](#).
- Run the `ping` command on the [CLI](#) of the PC to make sure that the PC can communicate with the iSAC management network port properly.

# Chapter 3

# Logging In to the Web Portal of the BMC

---

## Abstract

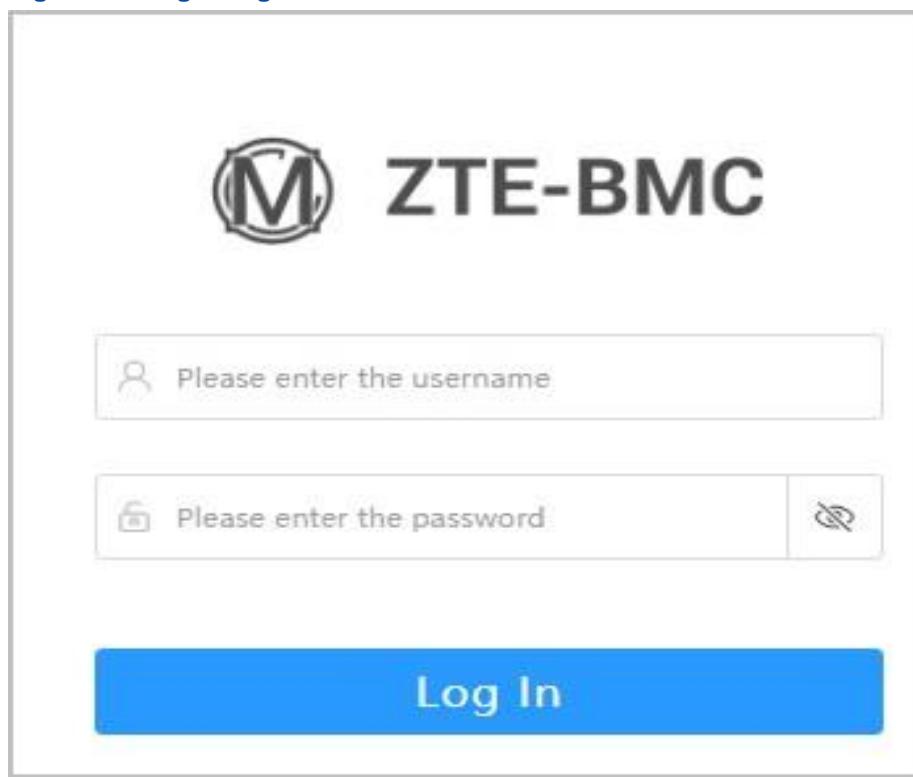
This procedure describes how to log in to the Web portal of the **BMC** of a server through the specified browser on your **PC**. You can monitor and manage the server on the portal.

## Prerequisite

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

## Steps

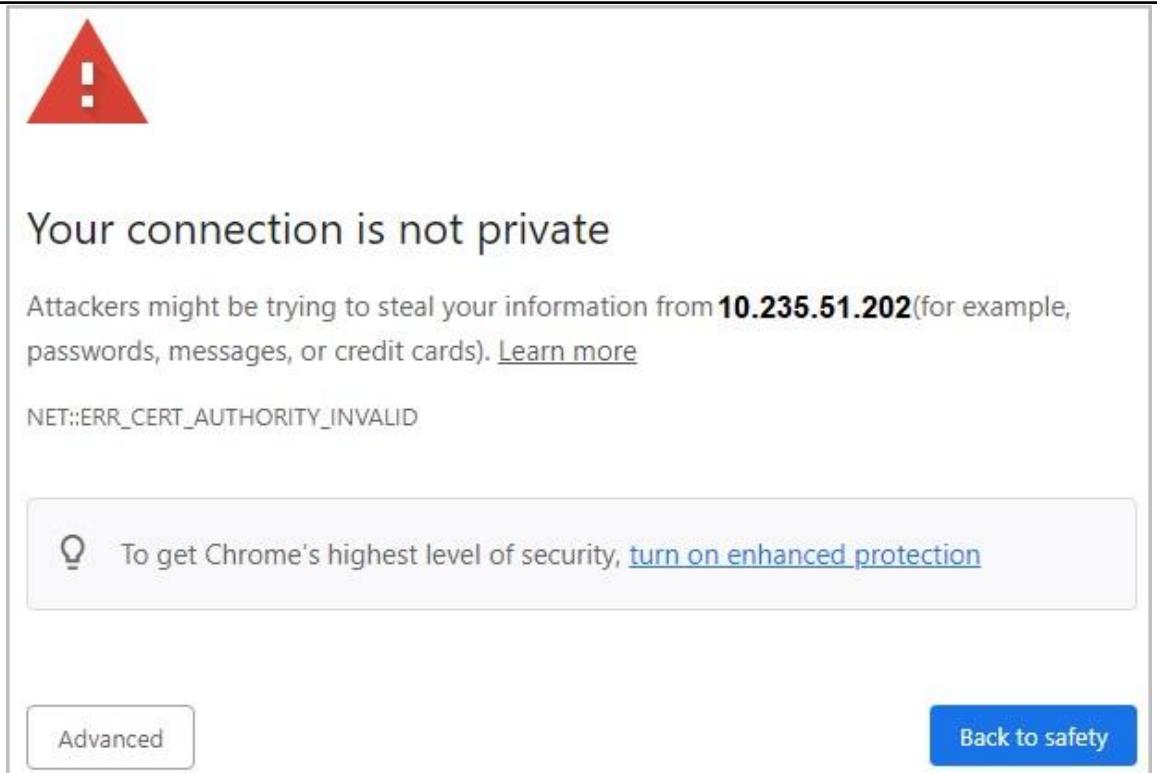
1. In the address bar of the browser, enter the address of the Web portal of the BMC, and press **Enter**. The page for login is displayed, see [Figure 3-1](#).

**Figure 3-1 Login Page****Note**

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

If the prompt information as shown in [Figure 3-2](#) is displayed before login, click **Advanced** and select **Proceed to** to enter the login page.

Figure 3-2 Security Prompt



2. Enter your username and password.



**Note**

The default username and password are as follows:

- Username: Administrator
- Password: Superuser9!

To unhide the password, you can click the  button on the right.

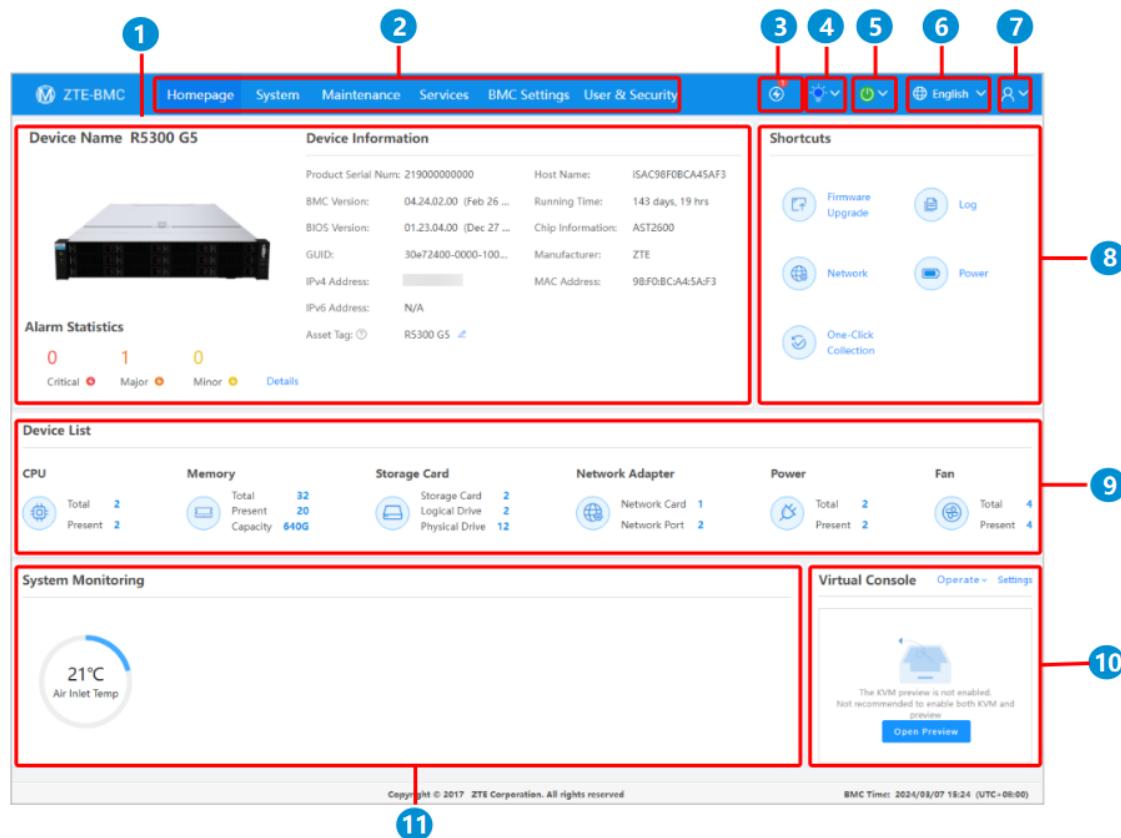


**Note**

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. Click **Log In**, The **Homepage** of the Web portal of the BMC is displayed, see [Figure 3-3](#).

Figure 3-3 Homepage



For a description of the **Homepage**, refer to [Table 3-1](#).

Table 3-1 Homepage Descriptions

No.	Name	Description
1	<b>Device Information</b>	<p>Displays the detailed information and active alarm statistics of the server.</p> <ul style="list-style-type: none"> <li>To modify the asset flag of the server, click .</li> <li>To view alarm details, click <b>Details</b>.</li> </ul>
2	Menu bar	Displays all the function menus in the format of a navigation tree in the left pane after you click any main menu on the menu bar.
3	Alarm button	<p>Displays the total number of active alarms.</p> <ul style="list-style-type: none"> <li>To view the number of alarms at each level, hover the mouse pointer over this button.</li> <li>To view alarm details, click this button.</li> </ul>

4	UID button	<p>Displays the UID indicator status of the server.</p> <p>To change the status of the UID indicator, click this button and select the corresponding shortcut menu.</p> <p>The shortcut menus include:</p> <ul style="list-style-type: none"> <li>● <b>Steady on:</b> The UID indicator is lit, helping you to identify the current server among the servers in the equipment room.</li> </ul>
---	------------	--

No.	Name	Description
		<ul style="list-style-type: none"> <li>● <b>Blink:</b> The UID indicator flashes, indicating that the BMC is being operated. The UID indicator flashes automatically when the BMC, Web portal, KVM, or virtual media is being used.</li> <li>● <b>Off:</b> The UID indicator is off.</li> </ul> <p>The grayed shortcut menu indicates the current status of the UID indicator. For example, if the <b>Blink</b> shortcut menu is grayed, the UID indicator of the server is flashing.</p>
5	Power button	<p>Displays the power status of the server.</p> <p>To change the power status, click this button and select the corresponding shortcut menu.</p> <p>The shortcut menus include:</p> <ul style="list-style-type: none"> <li>● <b>Power On:</b> Power on the server.</li> <li>● <b>Normal Power Off:</b> Power off the server.</li> <li>● <b>Forced Power Off:</b> Forcibly power off the server.</li> <li>● <b>Power Reset:</b> Perform a warm reboot.</li> </ul> <p>Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.</p> <ul style="list-style-type: none"> <li>● <b>Power Cycle:</b> Perform a cold reboot.</li> </ul> <p>Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.</p> <p>The grayed shortcut menu indicates the current power status of the server. For example, if the <b>Power On</b> shortcut menu is grayed, the server is in power-on status.</p>
6	Language button	<p>Displays the current language of the Web portal of the BMC.</p> <p>To change the language, click this button.</p>
7	Current user	<p>Displays the currently logged-in user.</p> <ul style="list-style-type: none"> <li>● To view the details of the currently logged-in user, including the IP address and login time, click this button.</li> <li>● To log out the currently logged-in user, click this button and then click <b>Log Out</b> in the detailed information box displayed.</li> </ul>

8	<b>Shortcuts</b>	Displays the shortcut operation buttons on the Web portal of the BMC, including: <ul style="list-style-type: none"> <li>● <b>Firmware Upgrade</b>: upgrades firmware. For details, refer to <a href="#">8.4 Upgrading Firmware</a>.</li> <li>● <b>Log</b>: queries BMC logs. For details, refer to <a href="#">6.8 Querying BMC Logs</a>.</li> <li>● <b>Network</b>: configures network parameters. For details, refer to <a href="#">8.1 Network Parameter Configuration</a>.</li> <li>● <b>Power</b>: queries server power-on/off information, and power supply and power consumption information. For details, refer to <a href="#">5.7 Powering On/Off the Server</a> and <a href="#">5.13 Configuring Power Control Parameters</a>.</li> </ul>
---	------------------	---

No.	Name	Description
		<ul style="list-style-type: none"> <li>● <b>One-Click Collection</b>: collects all configuration files, databases, and logs for fault location, packages them, and downloads them to the PC. It takes a long time to collect the required information, and no other operations can be performed during the collection period.</li> </ul>
9	<b>Device List</b>	Displays the components in the server by category. To view the details of components of a category, click the category.
10	<b>Virtual Console</b>	Displays the operations related to the virtual console, including: <ul style="list-style-type: none"> <li>● To enable <b>KVM</b> preview in the <b>Virtual Console</b> area, click <b>Open Preview</b>.</li> <li>● To disable KVM preview in the <b>Virtual Console</b> area, click <b>Close Preview</b>.</li> <li>● To start the virtual console in <b>HTML</b> mode, click <b>Operate</b> and then select <b>Start HTML Virtual Console</b> from the shortcut menu.</li> <li>● To start the virtual console in Java mode, click <b>Operate</b> and then select <b>Start Java Virtual Console</b> from the shortcut menu.</li> <li>● To reset the virtual console, click <b>Operate</b> and then select <b>Reset Virtual Console</b> from the shortcut menu.</li> <li>● Click <b>Settings</b>.</li> </ul>
11	<b>System Monitoring</b>	Displays system monitoring information.

# Chapter 4

# Common Operations

---

## Table of Contents

Logging In to the BMC Through SSH.....	20
Logging In to the BMC Through a Serial Port.....	22
Modifying the BMC Address.....	25
Checking Server Information.....	26
Managing Storage Devices.....	27
Installing an OS Remotely.....	30
Resetting the BMC When the Web Portal Is Unavailable.....	36
Querying and Configuring Services.....	37
Configuring an NTP Server.....	40
Configuring an SMTP Server.....	41
Configuring Trap Notification Parameters.....	42
BMC Log Export.....	44
Upgrading the BMC Firmware.....	48
Restoring Factory Defaults.....	49
Backing Up BMC Configurations.....	50
Creating an SNMP User.....	51

## 4.1 Logging In to the BMC Through SSH

### Abstract

This procedure describes how to log in to the **BMC** through **SSH** to configure the BMC.

### Prerequisite

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



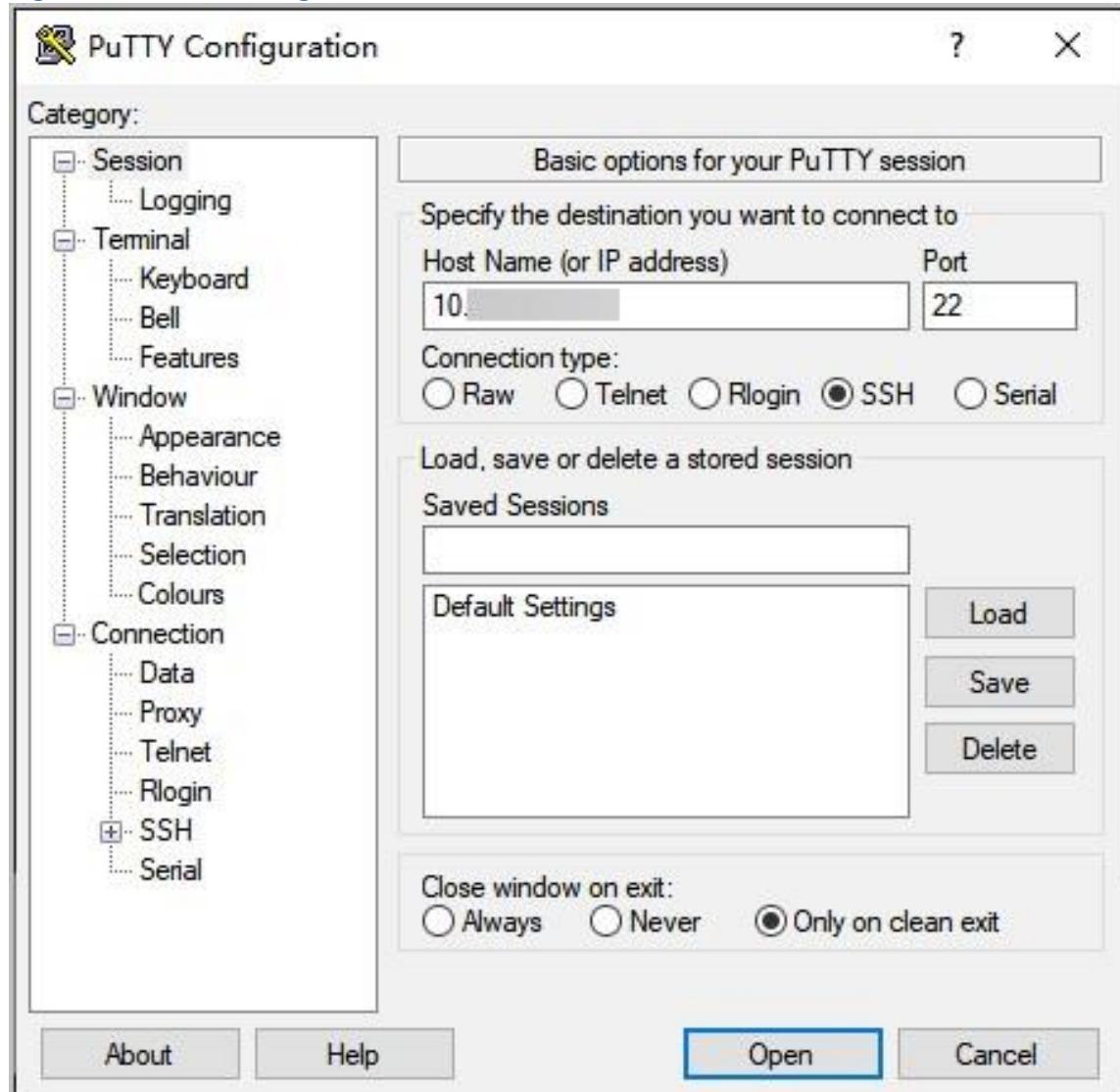
**Note**

The operations for different SSH software are similar. This procedure uses the *PuTTY* software as an example.

## Steps

1. On the PC, start the *PuTTY* software. The **PuTTY Configuration** window is displayed, see Figure 4-1.

**Figure 4-1 PuTTY Configuration Window**



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

**Table 4-1 PuTTY Configuration Parameter Descriptions**

Parameter	Setting
Category	Select <b>Session</b> .
Host Name (or IP address)	Enter the IP address of the <b>iSAC</b> management network port or shared network port.

Port	Enter 22.
<b>Parameter</b>	<b>Setting</b>
Connection type	Select <b>SSH</b> .

3. Click **Open**. The CLI is displayed.
4. Enter the username 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 [10 Reference: Default Passwords](#).

5. Press **Enter** to log in to the BMC.

## 4.2 Logging In to the BMC Through a Serial Port

### Abstract

When neither the [iSAC](#) management network port nor the shared network port is available for accessing the [BMC](#), you can log in to the BMC through a serial port to configure the BMC.

### Prerequisite

- The [PC](#) is already installed with [SSH](#) software, for example, *PuTTY*.



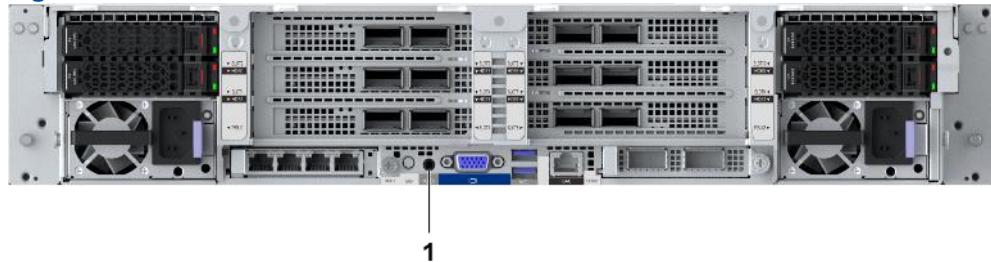
#### Note

The operations for different SSH software are similar. This procedure uses the *PuTTY* software as an example.

- If the PC needs to convert a [USB](#) port into a serial port, the corresponding driver must be installed.
- A serial cable is available.

### Steps

1. Connect the 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 Serial Port Position**

1. Serial port



The port with the **UID** silk screen on the rear panel of a server identifies the serial port. This procedure uses an R5300 G5 server as an example to describe the position of the serial port.

2. Press and hold the **UID** button on the front panel of the server for six seconds. The serial port is switched to the BMC serial port commissioning mode.

For the position of the **UID** button on the front panel, refer to [Figure 4-3](#).

**Figure 4-3 Position of the UID Button**

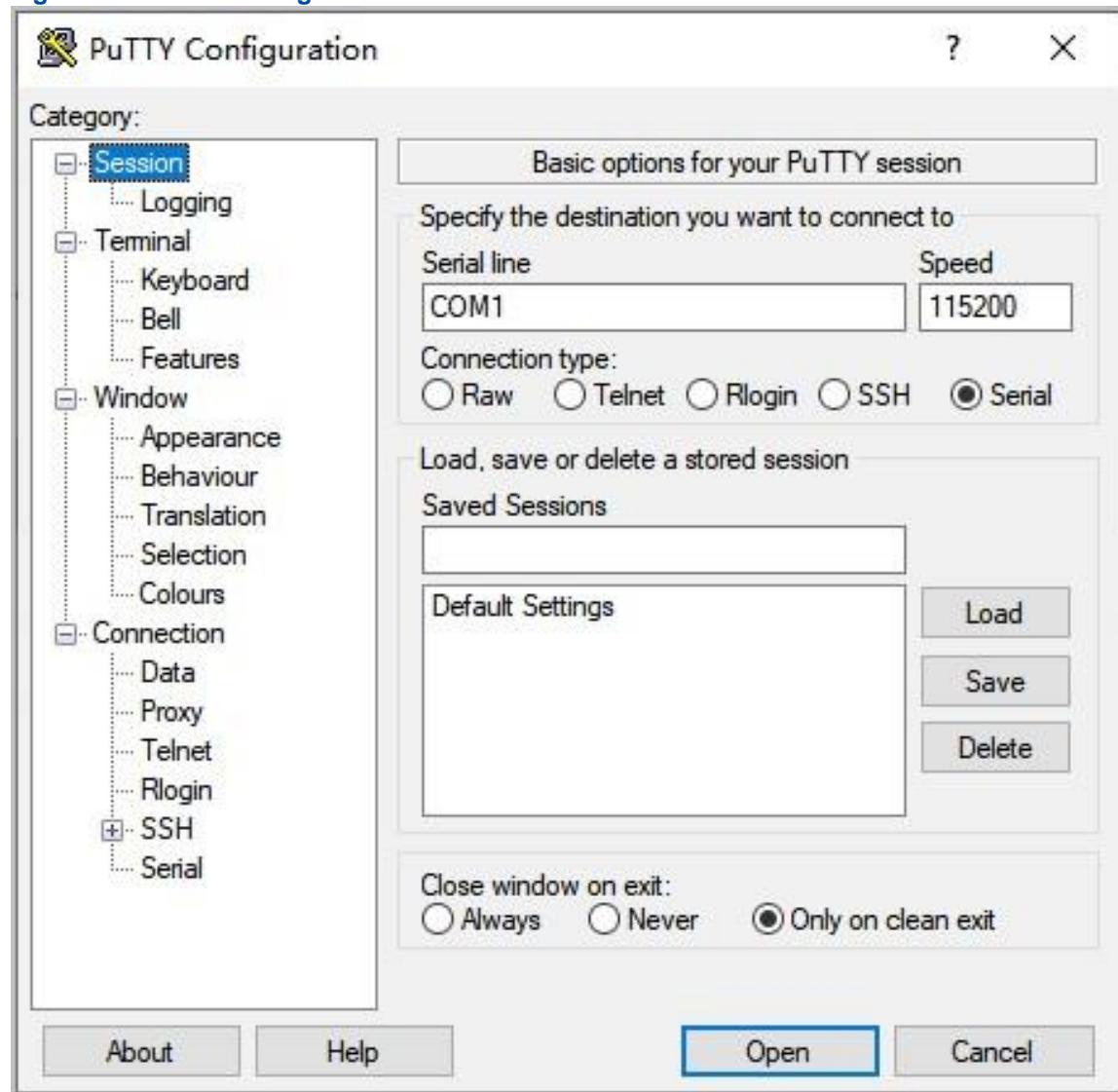
1. UID button



The button with the **UID** silk screen on the front panel of a server is the **UID** button. This procedure uses an R5300 G5 server as an example to describe the position of the **UID** button.

3. In the **Device Manager** window on the PC, check the serial port connected with the serial cable.
4. On the PC, start the *PuTTY* software. The **PuTTY Configuration** window is displayed, see [Figure 4-4](#).

Figure 4-4 PuTTY Configuration Window



5. Set the parameters. For a description of the parameters, refer to [Table 4-2](#).

Table 4-2 PuTTY Configuration Parameter Descriptions

Parameter	Setting
Category	Select <b>Session</b> .
Serial line	Enter the serial port obtained in <a href="#">Step 3</a> .
Speed	Enter <i>115200</i> .
Connection type	Select <b>Serial</b> .

6. Click **Open**. The CLI is displayed.
7. Enter the username 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 [10 Reference: Default Passwords](#).

8. Press **Enter** to log in to the BMC.

## 4.3 Modifying the BMC Address

### Abstract

To replan the **IP** address of the **iSAC** management network port or shared network port of the server, you need to modify the address of the **BMC**.

### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 4-5](#).

**Figure 4-5 Network Settings Page**

**Network Settings**

**Host Name**

**Network Port**

**Network Protocols**

Select Network Port:  Dedicated Port  Shared Port

Network Protocols:  IPv4  IPv6

**IPv4**

Acquisition method:  Manually set IP address  Automatically obtain IP address

Address: 10.

Mask: 255.255.255.0

Default Gateway: 10.

MAC Address: E2:24:A2:82:E0:35

**IPv6**

Acquisition method:  Manually set IP address  Automatically obtain IP address

Address: -

Prefix Length: 0

Default Gateway: -

Link Local Address: fe80::e024:a2ff:fe82:e035

**DNS**

**NCI VLAN Configuration**

3. Set the parameters in the **Network Protocols** area. For a description of the parameters, refer to [Table 4-3](#).

**Table 4-3 Network Protocol Parameter Descriptions**

Parameter	Setting
Select Network Port	<p>This parameter can be set only if <b>Select Mode</b> is set to <b>Alone</b> in the <b>Network Port</b> area.</p> <p>Select the network port for which you want to configure an IP address.</p> <ul style="list-style-type: none"> <li>● <b>Dedicated Port</b>: configures the IP address of the iSAC management network port.</li> <li>● <b>Shared Port</b>: configures the IP address of the shared network port.</li> </ul>
Network Protocols	<p>Select the network protocol(s) for the network port.</p> <ul style="list-style-type: none"> <li>● The IPv4 settings need to be configured if you select <b>IPv4</b> only.</li> <li>● The IPv6 settings need to be configured if you select <b>IPv6</b> only.</li> <li>● Both IPv4 settings and IPv6 settings need to be configured if you select <b>IPv4 and IPv6</b>.</li> </ul>
Acquisition method	<p>Select the method of obtaining the IP address.</p> <p>The parameters below do not need to be configured if <b>Acquisition method</b> is set to <b>Automatically obtain IP address</b>.</p>
Address	Enter the address of the BMC as planned.
Mask	Enter the mask.
Default Gateway	Enter the IP address of the default gateway.

4. Click **Save**.

## 4.4 Checking Server Information

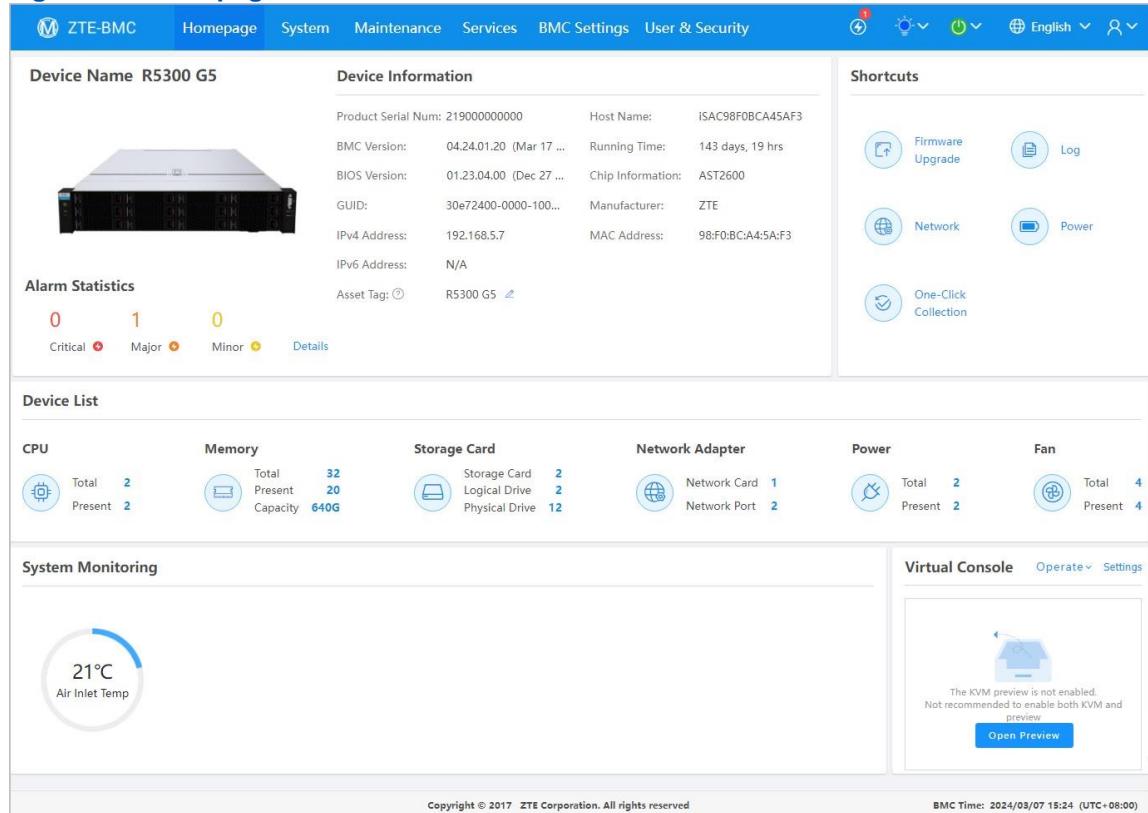
### Abstract

Before reporting a fault or replacing hardware, you must check the server information, including:

- Serial number
- [CPU](#)
- Memory
- [NIC](#)

### Steps

1. On the [Homepage](#), check the serial number of the server, see [Figure 4-6](#).

**Figure 4-6 Homepage**

2. Select **System**. The **System** page is displayed.
3. From the navigation tree in the left pane, select **System Information**. The **System Information** page is displayed, see [Figure 4-7](#).

**Figure 4-7 System Information Page**

System Information														
CPU Information		Memory Information		Disk Information		Network Adapter		FRU Information		Sensor		Other		
Details	No.	Name	Present Status	Health Status	Manufacturer	Model	TDP(Watt)	Frequency(MHz)	Maximum Frequency(MHz)	Core	Threads	Architecture		
▼	1	CPU 0	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86		
▼	2	CPU 1	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86		

- To check CPU information, switch to the **CPU Information** tab.
- To check memory information, switch to the **Memory Information** tab.
- To check NIC information, switch to the **Network Adapter** tab.

## 4.5 Managing Storage Devices

### Abstract

The storage devices of a server refer to **RAID** controllers and hard disks.

The physical disks managed by a RAID controller can be created as logical disks.

On the **Storage Management** page, the **Storage Card** tab displays **SAS/SATA** disks, and the **NVMe** tab displays NVMe disks.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Storage Management**. The **Storage Management** page is displayed, see [Figure 4-8](#).

**Figure 4-8 Storage Management Page**

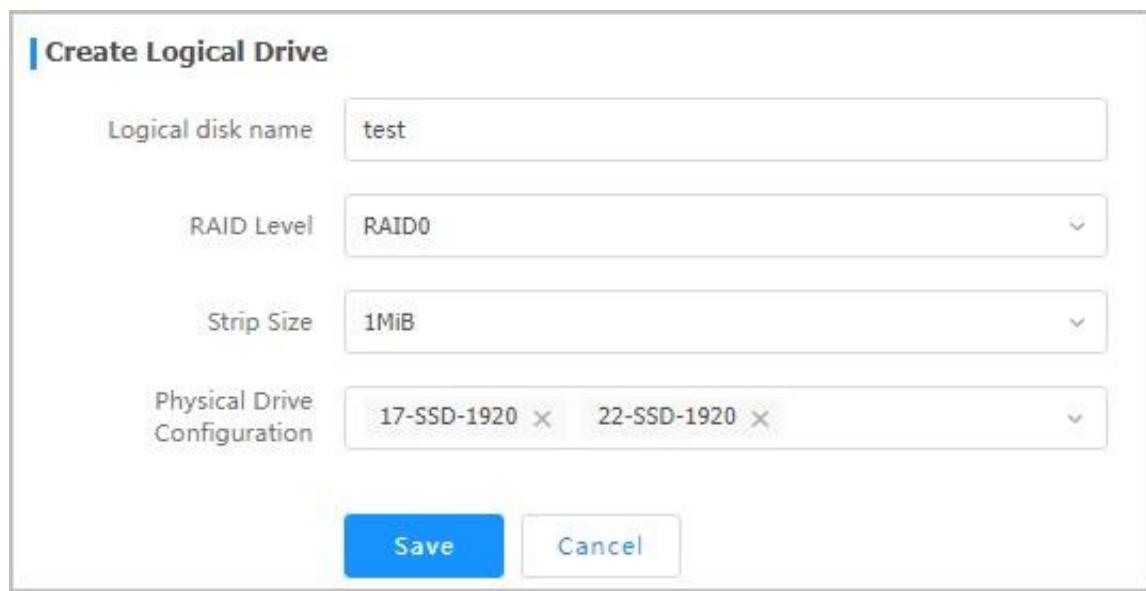
1. RAID controller
2. Logical disk
3. Physical disk

3. Perform the following operations as required.

To...	Do...
Check RAID controller and <a href="#">BBU</a> information	On the <b>Storage Card</b> tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the <b>Storage Card</b> tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, <b>Status</b> includes: <ul style="list-style-type: none"> <li>● <b>Optimal</b></li> <li>● <b>Degraded</b></li> <li>● <b>Part Degraded</b></li> <li>● <b>Offline</b></li> </ul>

Set the <b>UID</b> indicator of a logical disk	<ol style="list-style-type: none"> <li>a. On the <b>Storage Card</b> tab, click the desired logical disk.</li> <li>b. Click <b>Settings</b> on the right. The <b>Logical Drive Setting</b> dialog box is displayed.</li> </ol>
--	--

To...	Do...
	<ol style="list-style-type: none"> <li>c. Select <b>Open</b> or <b>Close</b>.           <ul style="list-style-type: none"> <li>● <b>Open</b>: turns on the UID indicators of all member disks of the logical disk.</li> <li>● <b>Off</b>: turns off the UID indicators of all member disks of the logical disk.</li> </ul> </li> <li>d. Click <b>Submit</b>.</li> </ol>
Check physical disk information	On the <b>Storage Card</b> tab, click the desired physical disk. The detailed physical disk information is displayed on the right.
Create a logical disk	<ol style="list-style-type: none"> <li>a. On the <b>Storage Card</b> tab, click <b>+</b> next to a RAID controller. The <b>Create Logical Drive</b> area is displayed on the right, see <a href="#">Figure 4-9</a>.</li> <li>b. Configure the following parameters:           <ul style="list-style-type: none"> <li>● <b>Logical disk name</b>: Enter the name of the logical disk.</li> <li>● <b>RAID Level</b>: Select the corresponding RAID level.</li> <li>● <b>Stripe Size</b>: Select a stripe size.</li> <li>● <b>Physical Drive Configuration</b>: Select the member disks that form the logical disk.</li> </ul> </li> <li>c. Click <b>Save</b>.</li> </ol>
Query <b>NVMe</b> hard disk information	On the <b>Storage Management</b> page, click <b>NVMe</b> to switch to the <b>NVMe</b> tab. The detailed NVMe disk information is displayed.

**Figure 4-9 Create Logical Drive Area**


The dialog box is titled 'Create Logical Drive'. It contains the following fields:

- Logical disk name: test
- RAID Level: RAID0
- Strip Size: 1MiB
- Physical Drive Configuration: 17-SSD-1920 X 22-SSD-1920 X

At the bottom are 'Save' and 'Cancel' buttons.



Different types of RAID controllers have different pages for creating logical disks.

## 4.6 Installing an OS Remotely

### Abstract

When you are not on the customer site, you can install the [OS](#) for a server remotely through a PC.

The operations for remote OS installation include:

1. Disabling media redirection configurations
2. Configuring a boot mode
3. Installing an OS

### Prerequisite

- The *iso* file of the OS is already obtained.
- The [RAID](#) configuration for the system disk of the server is already completed.
- If the [KVM](#) needs to be started in Java mode, [JRE](#) (for example, *jre-8u191*) is already installed on the PC.

### Steps

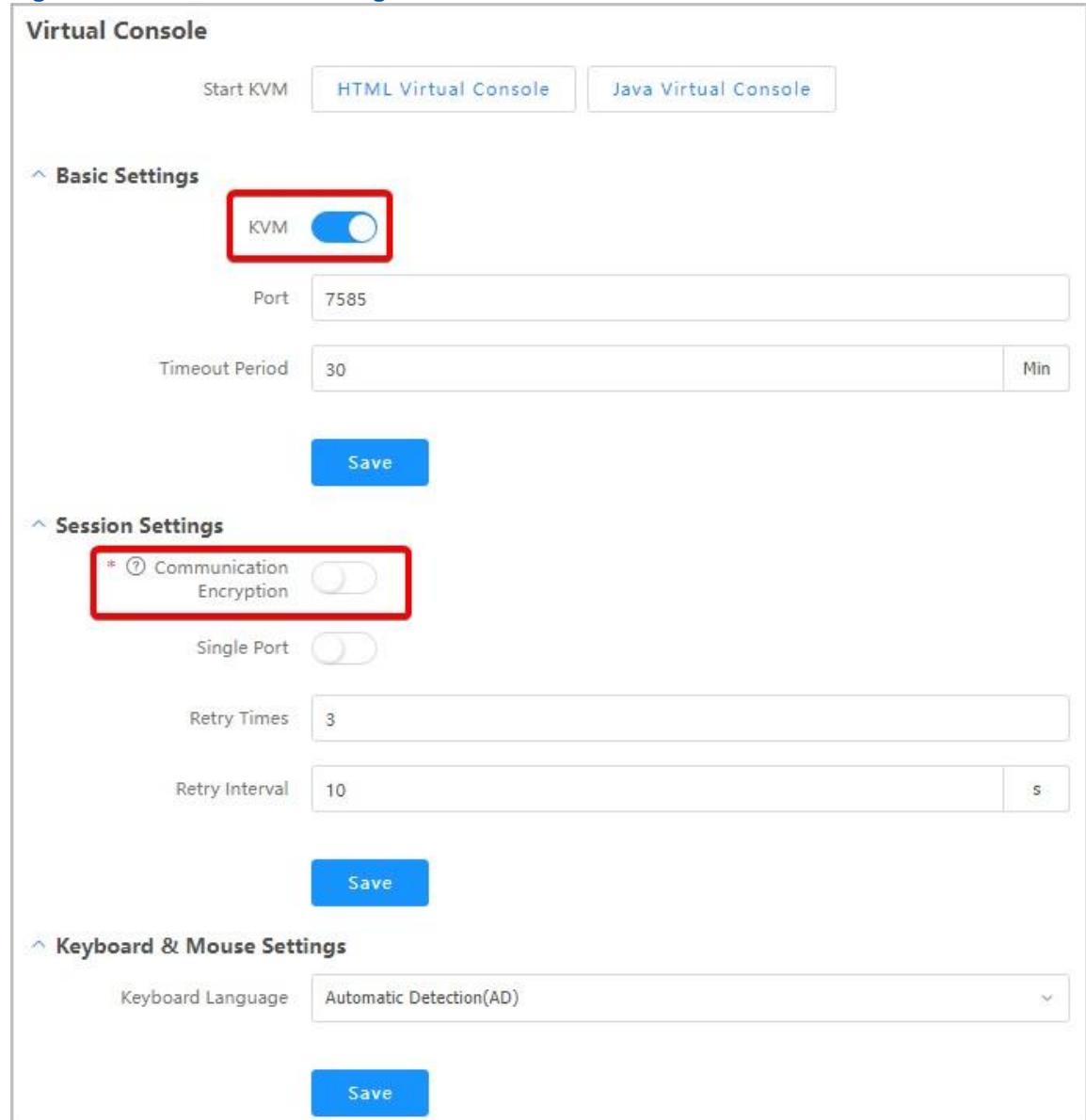
#### Disabling Media Redirection Configurations

1. Select **Services**. The **Services** page is displayed.

- From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed, see [Figure 4-10](#).

**Figure 4-10 Virtual Media Page**

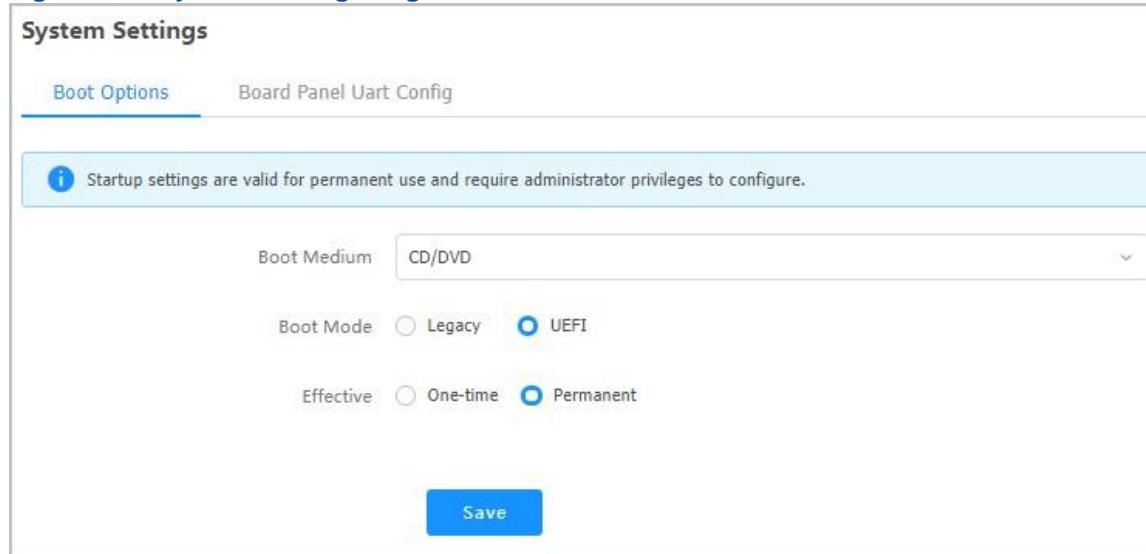
- In the **VMedia Entity Settings** area, turn off **Media Redirection Encryption**, and click **Save**.
- In the **Media Service Settings** area, turn on **CD Media**, and click **Save**.
- From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see [Figure 4-11](#).

**Figure 4-11 Virtual Console Page**

6. In the **Basic Settings** area, turn on **KVM**, and click **Save**.
7. In the **Session Settings** area, turn off **Communication Encryption**, and click **Save**.

#### Configuring a Boot Mode

8. Select **System**. The **System** page is displayed.
9. From the navigation tree in the left pane, select **System Settings**. The **System Settings** page is displayed, see [Figure 4-12](#).

**Figure 4-12 System Settings Page**

10. Set the parameters. For a description of the parameters, refer to [Table 4-4](#).

**Table 4-4 Boot Option Parameter Descriptions**

Parameter	Setting
Boot Medium	Select <b>CD/DVD</b> .
Boot Mode	Select <b>UEFI</b> .
Effective	Select <b>Permanent</b> .

11. Click **Save**.

### Installing an OS

12. Select **Services**. The **Services** page is displayed.

13. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed.

14. Perform the following operations as required.

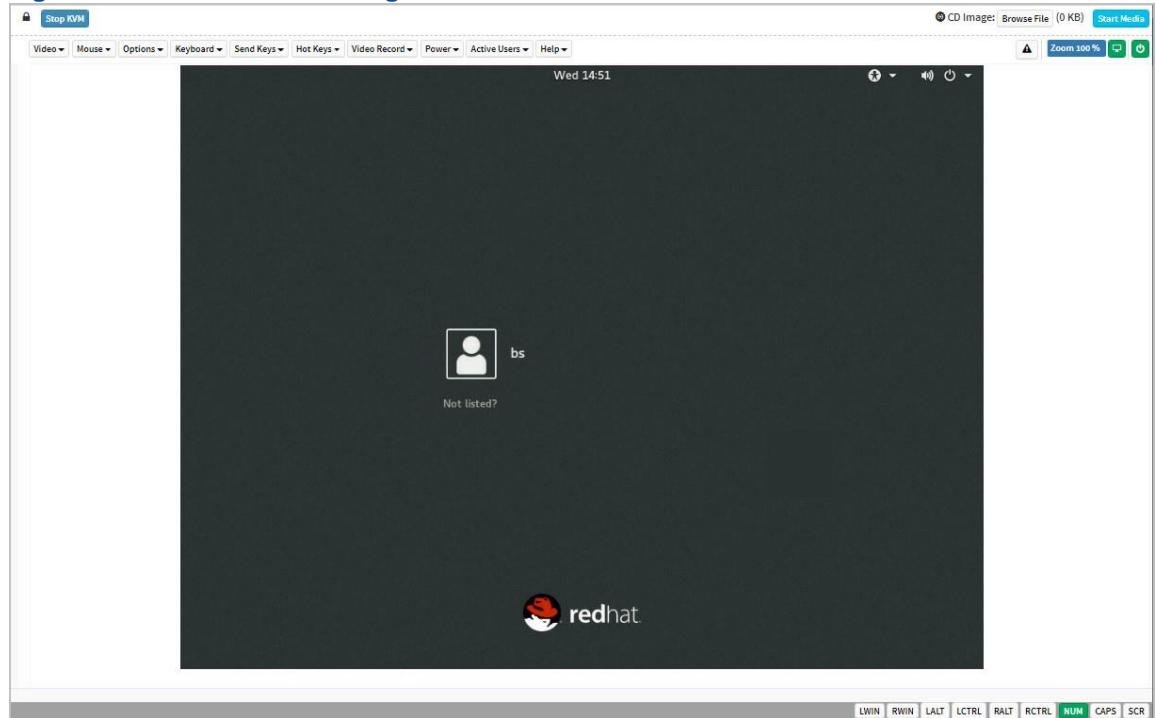
To...	Do...
Start the <b>KVM</b> in <b>HTML</b> mode	<ol style="list-style-type: none"> <li>Click <b>HTML Virtual Console</b>. The <b>HTML Virtual Console</b> page is displayed, see <a href="#">Figure 4-13</a>.</li> <li>Click <b>Browse File</b> next to <b>CD Image</b>, and select the <i>iso</i> file from the PC.</li> <li>Click <b>Start Media</b> to load the <i>iso</i> file.</li> <li>Select <b>Power &gt; Reset Server</b> to restart the server. The page for installing the OS is displayed.</li> </ol>

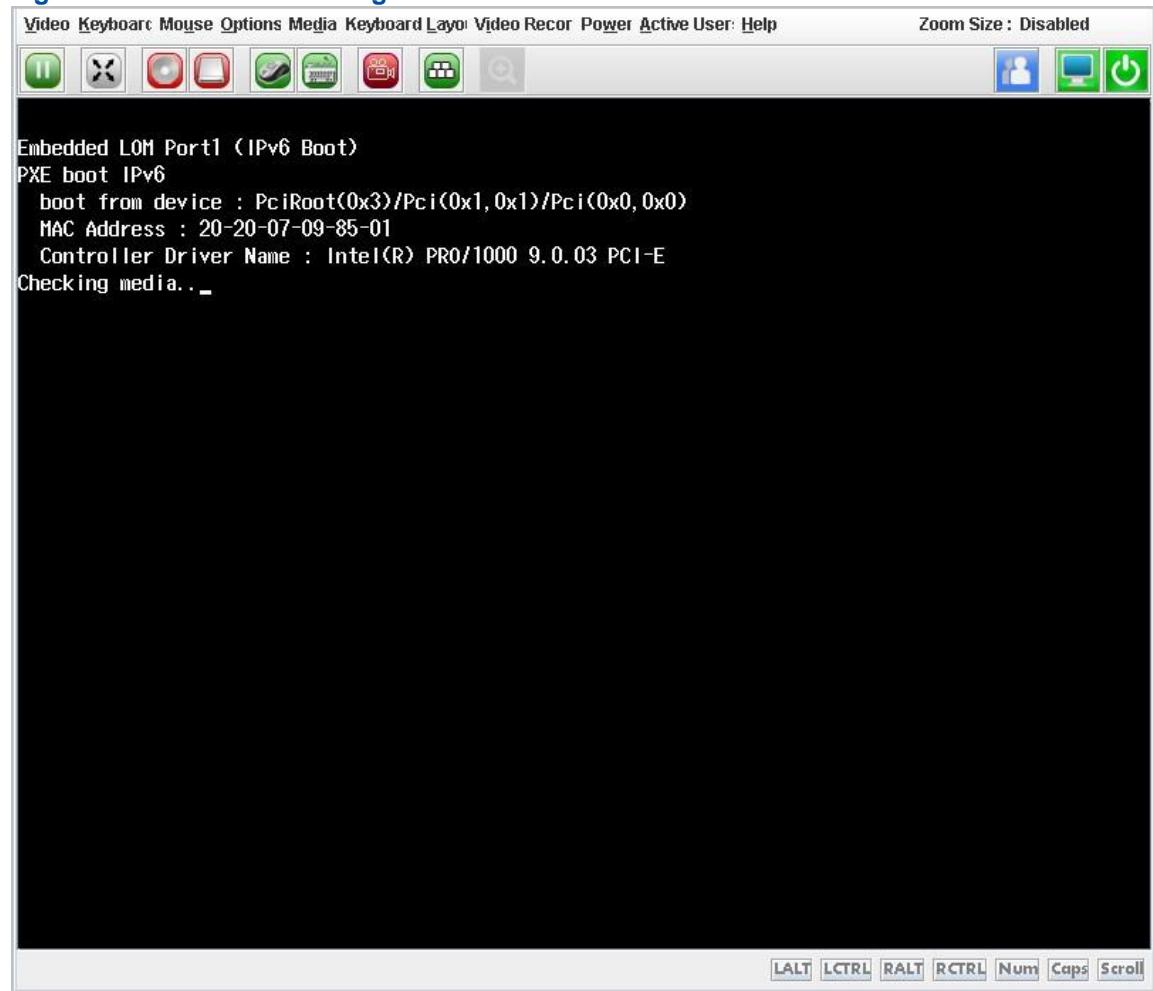
Start the KVM in Java mode	<ol style="list-style-type: none"> <li>a. In the search box in the lower left corner of the PC, enter <i>Java</i>.</li> <li>b. In the search result, select <b>Configure Java</b>. The <b>Java Control Panel</b> dialog box is displayed.</li> </ol>
<b>To...</b>	<b>Do...</b>
	<ol style="list-style-type: none"> <li>c. Click <b>Security</b>. The <b>Security</b> window is displayed.</li> <li>d. Click <b>Edit Site List</b>. The <b>Exception Site List</b> dialog box is displayed.</li> <li>e. Click <b>Add</b> to add the address of the Web portal of the BMC.</li> <li>f. Click <b>OK</b> to return to the <b>Security</b> window.</li> <li>g. Click <b>OK</b>.</li> <li>h. On the <b>Virtual Console</b> page of the Web portal of the BMC, click <b>Java Virtual Console</b>. A dialog box indicating whether to keep <i>jviewer.jnlp</i> is displayed.</li> <li>i. Click <b>Keep</b>.</li> <li>j. In the lower left corner of the browser, click <i>jviewer.jnlp</i>. A dialog box indicating whether to proceed is displayed.</li> <li>k. Click <b>Continue</b>. The <b>Do you want to run this application?</b> dialog box is displayed.</li> <li>l. Select <b>I accept the risk and want to continue to run this app.</b> and click <b>Run</b>. The <b>Untrusted Connection</b> dialog box is displayed.</li> <li>m. Click <b>Yes</b>. The <b>Java Console</b> page is displayed, see <a href="#">Figure 4-14</a>.</li> <li>n. Select <b>Media &gt; Virtual Media Wizard...</b>, and switch to the <b>CD/DVD</b> tab.</li> <li>o. Click <b>Browse</b>, and select the <i>iso</i> file from the PC.</li> <li>p. Click <b>Connect</b>.</li> <li>q. Select <b>Power &gt; Reset Server</b> to restart the server. The page for installing the OS is displayed.</li> </ol>



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 4-13 HTML Console Page



**Figure 4-14 Java Console Page**

## 4.7 Resetting the BMC When the Web Portal Is Unavailable

### Abstract

If you cannot log in to the Web portal of the [BMC](#), you need reset the BMC.

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

- Resetting the BMC by logging in to the server
- Resetting the BMC by using an [SSH](#) tool (for example, PuTTY)
- Resetting the BMC by using the ipmitool
- Resetting the BMC by powering off the server

### Prerequisite

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

## Steps

- Resetting 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
```
- Resetting the BMC by using an [SSH](#) tool
  1. Log in to the BMC by using the SSH tool Enter the following parameters for login:
    - Host address: address of the BMC → Username: sysadmin (the default administrator username)
    - Password: The default administrator password depends on server models and BMC versions. For details, refer to [10 Reference: Default Passwords](#).
    - Port number: 22
  2. Run the following command to reset the BMC:
 

```
# reboot
```
- Resetting the BMC by using the ipmitool
  1. In the ipmitool, run either of the following commands to reset the BMC:
    - Warm boot: `ipmitool -I lanplus -H 10.235.51.202 -U Administrator -P Superuser9! mc reset warm Sent warm reset command to MC`
    - Cold boot: `ipmitool -I lanplus -H 10.235.51.202 -U Administrator -P Superuser9! mc reset cold Sent cold reset command to MC`
 The parameters in the above commands are described as follows:
    - **10.235.51.202**: address of the BMC → **Administrator**: username → **Superuser9!**: password
- Resetting the BMC by powering off the server
  1. Power off the server without services.
  2. Power on the server.

## 4.8 Querying and Configuring Services

### Abstract

By default, the [BMC](#) provides the following services:

- **web**: a platform-independent, low-coupling, self-contained, programmable web-based application. You can use open [XML](#) standards for defining, publishing, discovering, coordinating, and configuring such applications, which are used to develop distributed and interoperable applications.

- **kvm**: controls, switches between, and manages multiple devices through a keyboard, display, or mouse, playing an important role in remote scheduling and monitoring.
- **cd-media**: a virtual media service that allows a **KVM** target server to access files on physical **CD/DVD** devices on a PC (acting as the client).
- **hd-media**: a virtual media service that allows a KVM target server to access files on physical **HD** devices on a PC (acting as the client).
- **ssh**: a protocol that provides secure remote access and other secure network services in an insecure network.
- **vnc**: a remote control tool, which consists of the application program (vncviewer) of the client and the application program (vncserver) of the server.
- **snmp**: a network management standard protocol widely used in **TCP/IP** networks. It provides unified interfaces to achieve the unified management of devices of different manufacturers.
- **redfish**: a server management specification. The Redfish Scalable Platforms Management **API** ("Redfish") uses RESTful interface semantics to access data defined in model format to perform out-of-band systems management. It is suitable for the management and deployment of large-scale server cloud environments.
- **ipmi**: a standard applied to server management system design.

This procedure describes how to query and modify the parameters of the services above.

## Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Port Services**. The **Port Services** page is displayed, see [Figure 4-15](#).

**Figure 4-15 Port Services Page**

Port Services								
No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation	
1	web	Open	80	443	30	20	<a href="#">Edit</a>	
2	kvm	Open	7578	7582	30	4	<a href="#">Edit</a>	
3	cd-media	Open	5120	5124	--	1	<a href="#">Edit</a>	
4	hd-media	Open	5123	5127	--	1	<a href="#">Edit</a>	
5	ssh	Open	--	22	10	--	<a href="#">Edit</a>	
6	vnc	Open	5900	5901	10	2	<a href="#">Edit</a>	
7	snmp	Open	161	--	--	--	<a href="#">Edit</a>	
8	redfish	Open	--	--	--	--	<a href="#">Edit</a>	
9	ipmi	Open	--	623	--	--		

3. Click **Edit** for a service to activate the parameters.
4. Set the parameters. For a description of the parameters, refer to [Table 4-5](#).

**Table 4-5 Port Service Parameter Descriptions**

Parameter	Setting
Status	Select whether to enable a service.
Non Secure Port	<p>Enter the non-secure port number of the service.</p> <ul style="list-style-type: none"> <li>● Default non-secure port number of the Web service: 80.</li> <li>● Default non-secure port number of the <a href="#">KVM</a> service: 7578.</li> <li>● Default non-secure port number of the CD media service: 5120.</li> <li>● Default non-secure port number of the HD media service: 5123.</li> <li>● Default non-secure port number of the <a href="#">VNC</a> service: 5900.</li> <li>● Default non-secure port number of the <a href="#">SNMP</a> service: 161.</li> </ul> <p>Other services do not support non-secure ports.</p> <p>Range of the non-secure port numbers: 1–65535.</p>
Secure Port	<p>Enter the secure port number of the service.</p> <ul style="list-style-type: none"> <li>● Default secure port number of the Web service: 443.</li> <li>● Default secure port number of the KVM service: 7582.</li> <li>● Default secure port number of the CD media service: 5124.</li> <li>● Default secure port number of the HD media service: 5127.</li> <li>● Default secure port number of the SSH service: 22.</li> <li>● Default secure port number of the VNC service: 5901.</li> <li>● Default secure port number of the <a href="#">IPMI</a> service: 623.</li> </ul> <p>Other services do not support secure ports.</p> <p>Range of the secure port numbers: 1–65535.</p>
Timeout(Min)	<p>The service exits if no operation is performed within the specified timeout period.</p> <p>Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).</p>

**Note**

You cannot configure the **Maximum Sessions** parameter.

5. Click **Save**.

**Verification**

- After enabling the Redfish service, you can query and configure the BMC through the Redfish interface.

For a detailed description of the Redfish interface, refer to the [NETAS Server Redfish Interface Description \(BMC V4\)](#). For how to obtain the [NETAS Server Redfish Interface Description \(BMC V4\)](#) file, refer to [11 Reference: Accessing Documents](#).

- After enabling the SNMP service and configuring a correct non-secure port, you can query and configure the BMC through the SNMP interface.

For a detailed description of the SNMP interface, refer to the [NETAS Server SNMP Interface Description \(BMC V4\)](#). For how to obtain the [NETAS Server SNMP Interface Description \(BMC V4\)](#) file, refer to [11 Reference: Accessing Documents](#).

## 4.9 Configuring an NTP Server

### Abstract

An [NTP](#) server is a time synchronization source of the [BMC](#). If the time of the [BMC](#) needs to be synchronized with an [NTP](#) server, you need to configure the NTP server.

To configure an NTP server, perform the following operations:

- Enabling the NTP service: provides the NTP service for the devices whose time needs to be synchronized.
- Modifying the registry: modifies the registry parameters related to the NTP service.
- Restarting the NTP service: applies the modified registry parameters.



### Note

This procedure uses the operations on a [PC](#) with the Windows Server 2012 R2 OS as an example. The operations on PCs with other Windows Server OSs are similar.

### Steps

#### Enabling the NTP Service

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

#### Modifying the Registry

- Press **Windows+R**. The **Run** dialog box is displayed.
- In the **Open** text box, enter *regedit*, and click **OK**. The **Registry Editor** window is displayed.
- 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
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	Type	NTP

### 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 executed, it indicates that the configuration is successful.

## 4.10 Configuring an SMTP Server

### Abstract

An **SMTP** server receives alarm emails from the **BMC**.

To configure an SMTP server, perform the following operations:

1. Installing the SMTP server: provides the SMTP service for the BMC.
2. Configuring the **IP** address and port number: sends alarm emails (if any) to the default path (*C:\inetpub\mailroot\Drop*) on the SMTP server after the IP address and port number of the SMTP server are configured on the Web portal of the BMC.



### Note

This procedure uses the operations on a **PC** with the Windows Server 2012 R2 OS as an example. The operations on PCs with other Windows Server OSs are similar.

**Steps****Installing an 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**.

## 4.11 Configuring Trap Notification Parameters

**Abstract**

Trap notification parameters are used by the **BMC** to report alarms to a third-party **NMS** through traps.



Trap notification parameters are provided by the third-party NMS, so the values of trap notification parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

## Abstract

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed, see [Figure 4-16](#).

**Figure 4-16 Alarm Settings Page**

The screenshot shows the 'Alarm Settings' page with the 'Trap Notification' tab selected. The 'Trap Function' section contains fields for Trap (switched on), Trap Version (V2C), Select V3 User (Administrator), Community Name (public), Confirm Community Name (public), Trap Host ID (Host Name), and Event Sending Level (Critical). A 'Save' button is at the bottom. The 'Trap Server Configuration' section shows a table with four entries:

No.	Server Address	Trap Port	Current Status	Operation
1	10.239.212.117	323	Disabled	Edit Test
2	10.230.19.204	162	Enabled	Edit Test
3	10.239.211.53	53	Enabled	Edit Test
4	10.239.166.158	162	Enabled	Edit Test

3. Set the parameters in the **Trap Function** area. For a description of the parameters, refer to [Table 4-7](#).

**Table 4-7 Trap Function Parameter Descriptions**

Parameter	Setting
Trap	Turn on the <b>Trap</b> switch.
Trap Version	Select the <b>SNMP</b> version for traps. Options: <b>V1</b> , <b>V2C</b> , and <b>V3</b> .
Select V3 User	This parameter is required if <b>Trap Version</b> is set to <b>V3</b> . Select a user that has permission to send alarms through SNMP.
Community Name	This parameter is required if <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b> . Enter the trap community name.

Confirm Community Name	This parameter is required if <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b> . Enter the trap community name.
Trap Host ID	Select the identifier of the host that reports alarms.
Event Sending Level	Select the level of events to be reported. For example, if <b>Event Sending Level</b> is set to <b>Critical</b> , only critical alarms are reported.

4. Click **Save**.
5. Set the parameters in the **Trap Server Configuration** area. For a description of the parameters, refer to [Table 4-8](#).

**Table 4-8 Parameter Descriptions for Trap Server Configuration**

Parameter	Setting
Server Address	After you click <b>Edit</b> , the parameter is activated. Enter the address of the server that receives alarms. An <a href="#">IPv4</a> address, <a href="#">IPv6</a> address, or domain name is supported.
Trap Port	After you click <b>Edit</b> , the parameter is activated. Enter the port number of the server that receives alarms. Range: 1–65535.
Current Status	After you click <b>Edit</b> , the parameter is activated. Select whether to enable the current server to receive alarms.

6. Click **Save**.



**Note**

After the **Edit** button is clicked, it is changed to the **Save** button.

7. (Optional) To send a test event to the server, click **Test**.



**Note**

If a message indicating "sent successfully" is displayed on the page, the trap is sent successfully.

## 4.12 BMC Log Export

You can export **BMC** logs in the following ways:

- Exporting logs in one click through the Web portal  
For details, refer to [4.12.1 Exporting Logs in One Click Through the Web Portal](#).
- Exporting logs by category through the Web portal

For details, refer to [4.12.2 Exporting Logs by Category Through the Web Portal](#).

- Exporting logs through [SSH](#) commands

For details, refer to [4.12.3 Exporting Logs Through the CLI \(SSH\)](#).

- Export logs through a serial port

For details, refer to [4.12.4 Exporting Logs Through the CLI \(Serial Port\)](#).

## 4.12.1 Exporting Logs in One Click Through the Web Portal

### Abstract

The Web portal of the [BMC](#) provides the one-click log export function. The exported log file is named `bmcinfo_<product serial number>.tar.gz` and stored in the default download directory of the browser.



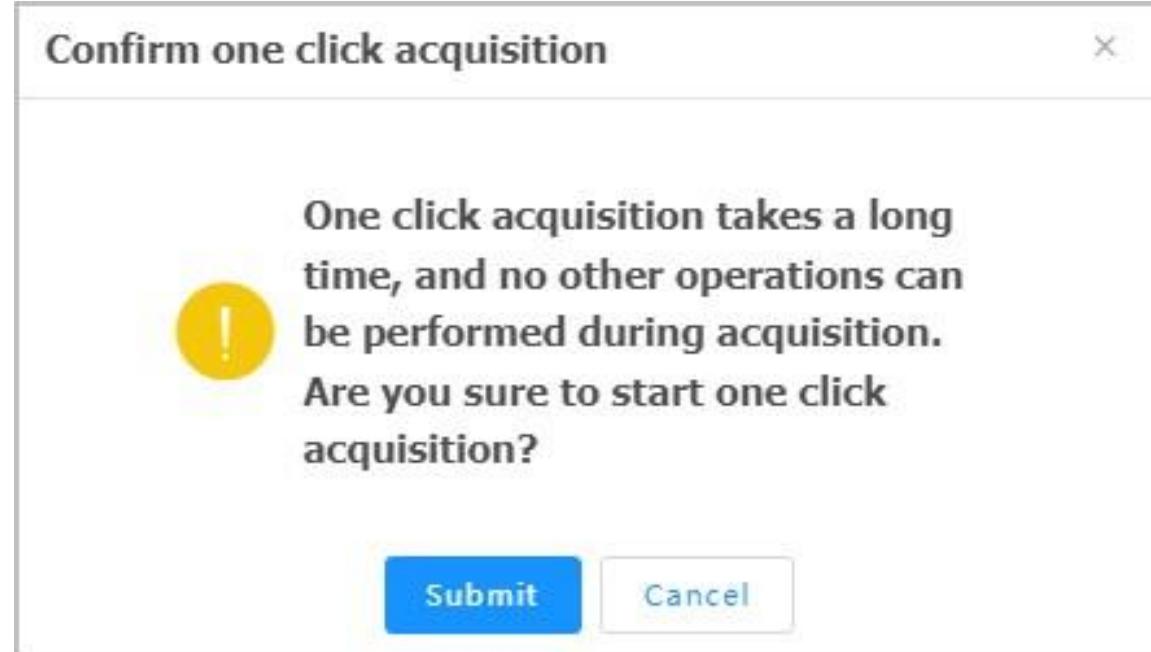
### Note

If the product serial number is not programmed, the filename is `bmcinfo_UnknownProductSN.tar.gz`.

### Steps

1. In the **Shortcuts** area on the [Homepage](#), click **One-Click Collection**. The **Confirm one click acquisition** dialog box is displayed, see [Figure 4-17](#).

[Figure 4-17 Confirm One Click Acquisition Dialog Box](#)



2. Click **Submit**.

**Note**

During the collection process, all Web interfaces of the BMC cannot be operated. If you shut down the browser by mistake and collect logs again after relogging in to the Web portal of the BMC, the **One click acquisition is being processed, please try again later.** prompt is displayed. In this case, you need to wait for about five minutes.

## 4.12.2 Exporting Logs by Category Through the Web Portal

### Abstract

Logs of the **BMC** include:

- **Operation Logs:** record the information about users' operations on the server, including manual server operations and remote server operations.
- **Audit Logs:** record users' login to and logout of the Web portal, BMC, and **KVM**.

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **BMC Logs**. The **BMC Logs** page is displayed, see [Figure 4-18](#).

**Figure 4-18 BMC Logs Page**

BMC Logs					
The page only displays about 100 logs generated recently. To view all the logs, please download the logs to view them locally.					
<a href="#">Operation Logs</a> <a href="#">Audit Logs</a>					
<a href="#">Download Logs</a> <input type="text"/> Search(Fuzzy search only s...)					
No.	Generation Time	Interface	User	Address	Details
112	2024-03-07 14:10:27	WEB	Administrator	10.	set time zone (Asia/Shanghai) successfully.
111	2024-03-07 14:10:27	WEB	Administrator	10.	disable NTP Server successfully.
110	2024-03-07 14:10:22	WEB	Administrator	10.	set bmc time to 2024-03-07 14:10:22 successfully.
109	2021-06-29 20:54:36	WEB	Administrator	10.	set asset tag: R8500 G5 successfully.
108	2021-06-29 20:36:52	WEB	Administrator	10.	set asset tag: R6900 G5 successfully.
107	2021-06-21 03:09:55	WEB	Administrator	10.	control chassis power on successfully.
106	2021-06-20 21:07:21	REDFISH	Administrator	10.	control chassis power cycle successfully.
105	2021-06-20 21:07:07	N/A	N/A	N/A	upgrade BIOS successfully.
104	2021-06-20 20:52:48	N/A	N/A	N/A	upgrade BIOS with preserve configuration successfully.
103	2021-06-20 20:52:47	REDFISH	N/A	N/A	begin upgrade BIOS successfully.

Total 112 [K](#) [<](#) [1](#) [2](#) [3](#) [4](#) [5](#) [>](#) [X](#) [10 / Page](#) [To](#) [1](#) [Page](#)

3. Perform the following operations as required.

To...	Do...
Export operation logs	<ol style="list-style-type: none"> <li>Click <b>Operation Logs</b> to switch to the <b>Operation Logs</b> tab.</li> <li>(Optional) In the <b>Search</b> box, enter a keyword.</li> <li>Click <b>Download Logs</b>.</li> </ol>

Export audit logs	<ol style="list-style-type: none"> <li>Click <b>Audit Logs</b> to switch to the <b>Audit Logs</b> tab.</li> <li>(Optional) In the <b>Search</b> box, enter a keyword.</li> <li>Click <b>Download Logs</b>.</li> </ol>
-------------------	---

### 4.12.3 Exporting Logs Through the CLI (SSH)

#### Abstract

If the Web portal of the **BMC** fails, you can log in to the BMC through **SSH** and export logs in one click through the CLI.

#### Steps

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

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



#### Note

After the logs are exported, they are stored in the `/var/bmcdata` directory.

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

```
# cd /var/bmcdata
# rm bmcinfo_.tar.gz
```

### 4.12.4 Exporting Logs Through the CLI (Serial Port)

#### Abstract

If the **BMC** cannot be accessed due to a network error, you can export logs in one click through the serial port.

#### Steps

1. Connect to the serial port of the BMC by using a serial cable.
2. Press and hold the **UID** button on the server panel for six seconds until the indicator flashes blue.
3. Connect to the serial port of the BMC by using a serial port tool.
4. After the connection is established, log in to the serial port with the corresponding username and password.
5. Run the following commands in the CLI to export logs:

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

**Note**

After the logs are exported, they are stored in the `/var/bmcdata` directory.

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

```
# cp /var/bmcdata/bmcinfo_.tar.gz /mnt/nandflash0/
```

**Note**

After the network is restored, you can download the log file to the local PC by using the [SFTP](#) function.

## 4.13 Upgrading the BMC Firmware

**Abstract**

When the [BMC](#) firmware needs to be upgraded, you can upload the firmware online to upgrade it.

**Note**

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

**Prerequisite**

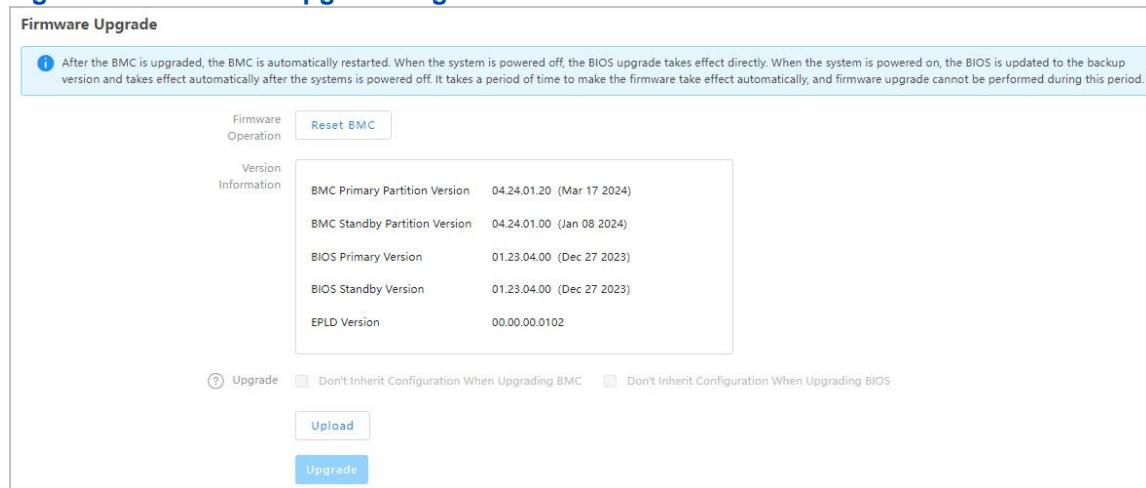
The BMC firmware is already obtained.

**Note**

The firmware upgrade file can be downloaded on the [Software Download](#) page on the Web portal of the servers and storage products (<https://enterprise.NETAS.com.cn>).

**Steps**

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Firmware Upgrade**. The **Firmware Upgrade** page is displayed, see [Figure 4-19](#).

**Figure 4-19 Firmware Upgrade Page**

3. Click **Upload** and select the firmware upgrade file.

**Note**

After the BMC firmware is successfully uploaded, the **Don't Inherit Configuration When Upgrading BMC** check box becomes activated.

4. (Optional) To restore the factory default settings of the BMC, select **Don't Inherit Configuration When Upgrading BMC**.
5. Click **Upgrade**.

**Notice**

During the firmware upgrade process, you cannot switch to another page. Otherwise, the upgrade process is interrupted.

## 4.14 Restoring Factory Defaults

### Abstract

This procedure describes how to restore the server configuration items (for example, the network, user, [SNMP](#) configuration, and boot mode) to factory defaults.

**Note**

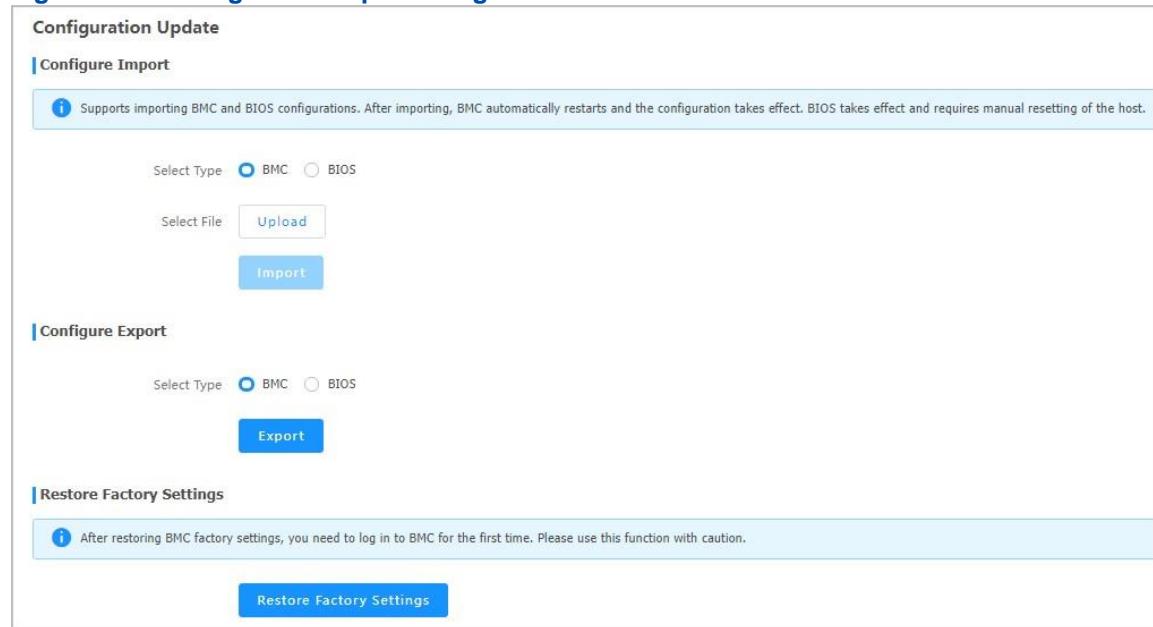
Do not perform any operation during restoration.

After the factory defaults are restored, the **BMC** will be restarted automatically.

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Configuration Update**. The **Configuration Update** page is displayed, see [Figure 4-20](#).

**Figure 4-20 Configuration Update Page**



3. Click **Restore Factory Settings**.

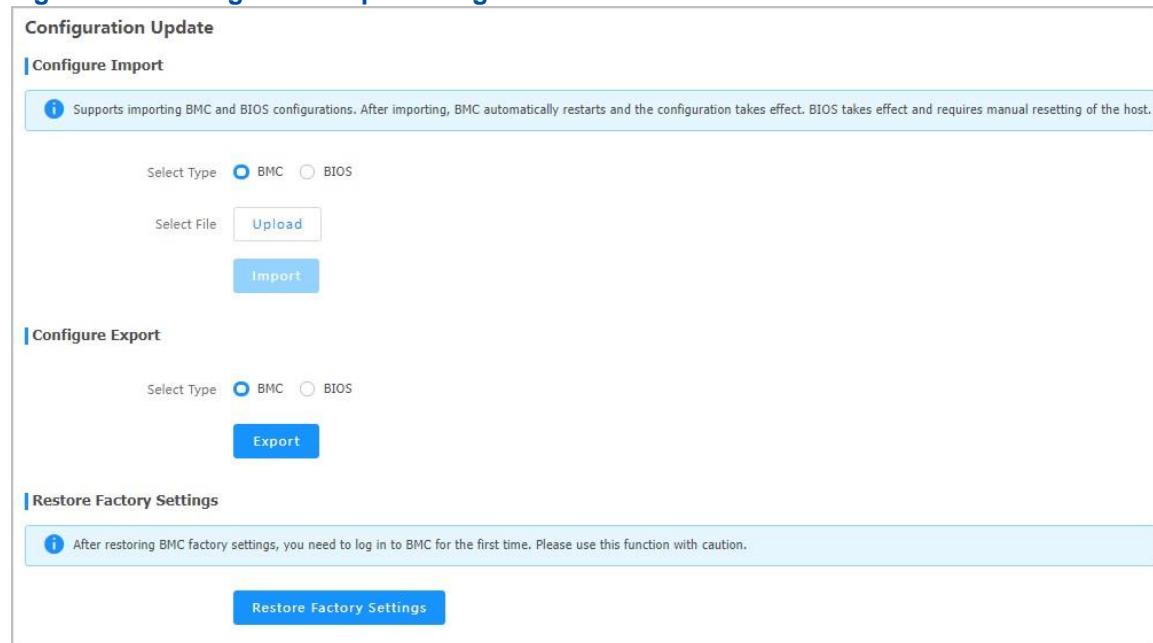
## 4.15 Backing Up BMC Configurations

### Abstract

Before replacing the mainboard of the server, you must export the **BMC** configurations. After replacing the mainboard, you need to import the BMC configurations.

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Configuration Update**. The **Configuration Update** page is displayed, see [Figure 4-21](#).

**Figure 4-21 Configuration Update Page**

3. Click **Export** to export the current BMC configurations to your local PC.
4. After replacing the mainboard, click **Upload**, and select the exported BMC configuration file in the displayed dialog box.
5. Click **Import**, and confirm the import in the displayed message box.

**Note**

After the BMC configurations are imported, the BMC is automatically restarted to apply the configurations. Do not perform any other operations until the BMC is restarted.

## 4.16 Creating an SNMP User

### Abstract

When configuring notification parameters for SNMPv3 trap messages, you need to select an **SNMP** user as the alarm sender. This procedure describes how to create an SNMP user.

### Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Local Users**. The **Local Users** page is displayed, as shown in [Figure 4-22](#).

**Figure 4-22 Local Users Page**

Local Users					Operation	
User ID	User Name	Role	Login Interfaces			Operation
1	anonymous	Administrator	SNMP	SSH	Redfish	Edit Enable Delete
2	Administrator	Administrator	SNMP	SSH	Redfish	Edit Disable Delete
					Total 2	Page

3. Click **Add User**. The **Add User** page is displayed, as shown in [Figure 4-23](#).

**Figure 4-23 Add User Page**

New User ID: 3

New UserName: testUser

New Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Role: Administrator

Login Interfaces:  SNMP  Redfish

Current User Password: \*\*\*\*\*

**Submit** **Cancel**

4. Set the parameters. For a description of the parameters, refer to [Table 4-9](#).

**Table 4-9 Parameter Descriptions for Adding a Local User**

Parameter	Description
New User ID	Select the ID of the new user. A maximum of 16 local users are supported, so the user ID ranges from 1 to 16. User 1 is a reserved user, and user 2 is the default administrator.
New UserName	Enter the name of the new user. The name contains a maximum of 16 characters, including digits, letters (case sensitive), and special characters. The new username cannot be the same as any existing one. The following cannot be used as a username: sshd, ntp, stunnel4, sysadmin, daemon, Administrator, and anonymous.

New Password	Enter the password of the new user. The password contains 8–20 characters, including digits, letters (case sensitive), and special characters.
<b>Parameter</b>	<b>Description</b>
	It must contain one special character and characters from at least two of the following types: digits, uppercase letters, and lowercase letters. Historical passwords cannot be used anymore.
Confirm Password	Enter the password again. It must be the same as <b>New Password</b> .
Role	Select the role of the new user.
Login Interfaces	Select one or more login interfaces available to the new user. <ul style="list-style-type: none"> <li>● <b>SNMP</b> is required. It indicates <b>SNMP</b> interface-based login.</li> <li>● For Redfish interface-based login, select <b>Redfish</b>.</li> </ul> <b>SSH</b> -based login is supported for all users by default.
Current User Password	Enter the password of the currently logged-in user of the Web portal of the BMC.

5. Click **Submit** to return to the **Local Users** page.
6. In the **Operation** column, click **Edit** for the new user. The **Edit** page is displayed, as shown in [Figure 4-24](#).

**Figure 4-24 Edit Page**

Local Users > **Edit**

User ID	3
User Name	testUser
Password	Please enter the password
Confirm Password	Please enter the password again
Role	Administrator
Login Interfaces	<input checked="" type="checkbox"/> SNMP <input type="checkbox"/> Redfish
SNMPv3 Authentication Algorithm	SHA256
SNMPv3 Encryption Algorithm	AES
Current User Password	*****
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

7. Set the parameters. For a description of the parameters, refer to [Table 4-10](#).

**Table 4-10 Parameter Descriptions for Editing a Local User**

Parameter	Description
SNMPv3 Authentication Algorithm	Select an authentication algorithm. <b>SHA256</b> , <b>SHA384</b> , or <b>SHA512</b> is recommended.
SNMPv3 Encryption Algorithm	Select an encryption algorithm. <b>AES</b> is recommended.
Current User Password	Enter the password of the currently logged-in user of the Web portal of the BMC.

8. Click **Submit**.

# Chapter 5

# System Management

---

## Table of Contents

Querying System Information.....	55
Querying Performance Data.....	56
Querying Fan Information.....	58
Configuring the Heat Dissipation Policy.....	59
Querying Temperature KPIs.....	60
Managing Storage Devices.....	62
Powering On/Off the Server.....	64
Configuring the Server Startup Policy.....	65
Configuring Power-On Delay Parameters.....	66
Querying Power Supply Information.....	67
Configuring the Power Mode.....	68
Querying Power Statistics.....	69
Configuring Power Control Parameters.....	70
Querying Power KPIs.....	72
Configuring Boot Options.....	73
Configuring the Serial Port Output Mode.....	74

## 5.1 Querying System Information

### Abstract

By querying system information, you can learn about the following information:

- [CPU](#) information
- Memory information
- Hard disk information
- [NIC](#) information, including Ethernet NIC and [FC](#) information
- [FRU](#) information
- Sensor information
- Other information, including [GPU](#), [PCIe](#) card information, and hard disk backplane information.



The operations for querying the above information are similar. This procedure uses how to query CPU information as an example.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **System Information**. The **System Information** page is displayed, see [Figure 5-1](#).

**Figure 5-1 System Information Page**

System Information													
CPU Information		Memory Information		Disk Information		Network Adapter		FRU Information		Sensor		Other	
Details	No.	Name	Present Status	Health Status	Manufacturer	Model	TDP(Watt/s)	Frequency(MHz)	Maximum Frequency(MHz)	Cores	Threads	Architecture	
▼	1	CPU 0	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86	
▼	2	CPU 1	Present	Healthy	Intel(R) Corporation	Intel(R) Xeon(R) Platinum 8470Q	350	2100	3800	52	104	x86	

Total 2 [navigation icons] 10 / Page [Page] To [Page]

3. (Optional) To view the details of a CPU, click  in the **Details** column for the CPU.

## 5.2 Querying Performance Data

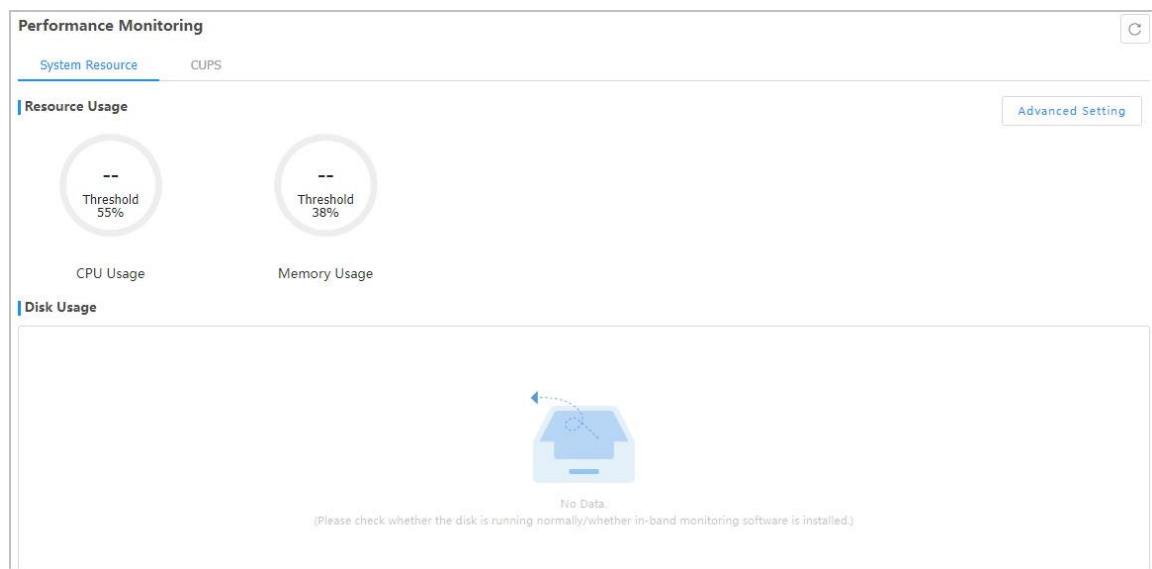
### Abstract

By querying performance data, you can learn about the following information:

- [CPU](#) usage
- [Memory](#) usage
- [Disk](#) usage
- Dynamic CPU load ratio: ratio of the currently used CPU resources to the total CPU resources of the server
- Dynamic memory load ratio: ratio of the currently used memory resources to the total memory resources of the server
- Dynamic [I/O](#) load ratio: ratio of the currently used I/O resources to the total I/O resources of the server

### Steps

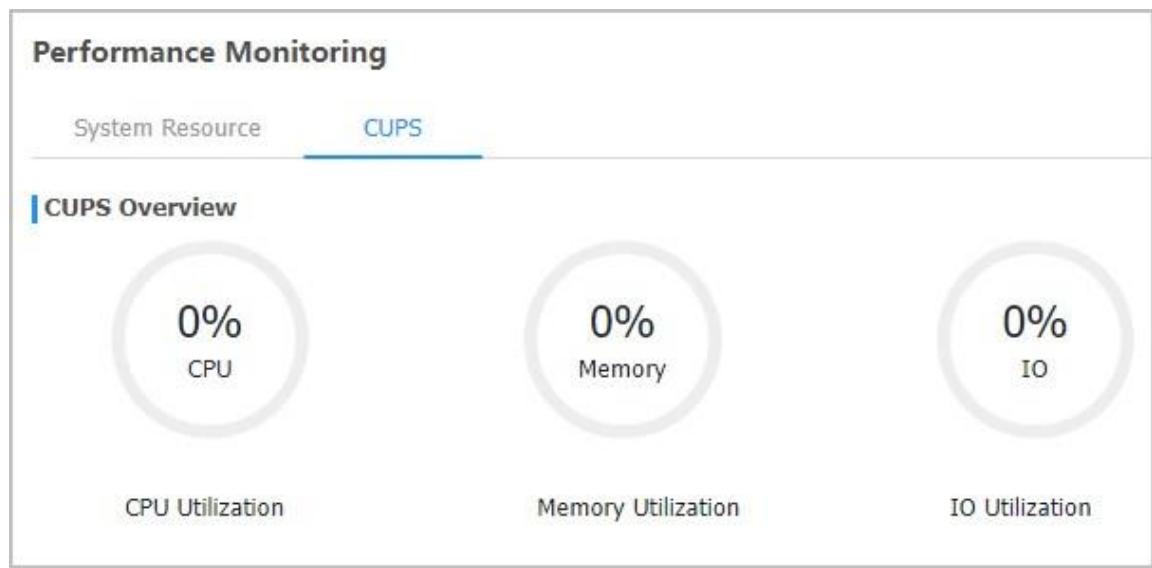
1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Performance Monitoring**. The **Performance Monitoring** page is displayed, see [Figure 5-2](#).

**Figure 5-2 Performance Monitoring Page**

### Note

The CPU usage, memory usage, and disk usage are displayed on the above page.

3. Click **CUPS**. The **CUPS** tab is displayed, see [Figure 5-3](#).

**Figure 5-3 CUPS Tab**

### Note

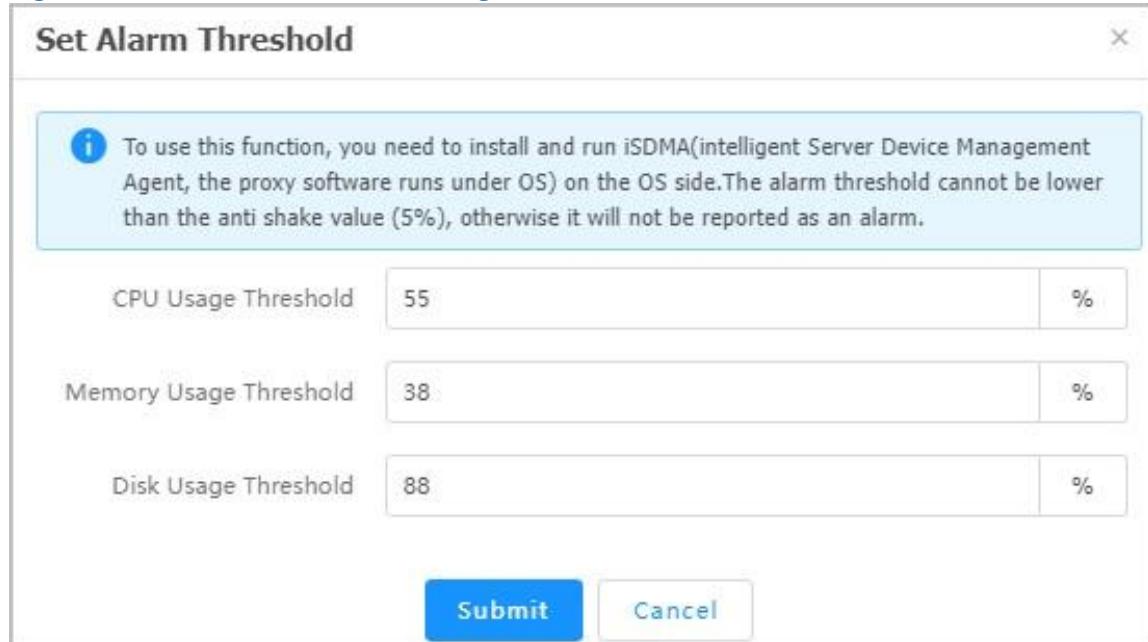
The dynamic CPU, memory, and I/O load ratios are displayed on the above tab.

## Related Tasks

To set the CPU usage, memory usage, and disk usage thresholds, perform the following operations:

1. On the **Performance Monitoring** page, click **Advanced Setting**. The **Set Alarm Threshold** dialog box is displayed, see [Figure 5-4](#).

**Figure 5-4 Set Alarm Threshold Dialog Box**



2. Set the alarm thresholds as required.
3. Click **Submit**.

## 5.3 Querying Fan Information

### Abstract

By querying fan information, you can learn about the operational status and detailed information of each fan in the server.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed, see [Figure 5-5](#).

**Figure 5-5 Fan & Heat Dissipation Page**

Fan & Heat Dissipation							
Fan Information		Heat Dissipation		Key Performance Indicator			
No.	Name	Type	Present	Speed(RPM)	Speed Ratio(%)	Health Status	
1	FAN1	8038	Present	4591	30	<span style="color: green;">●</span> Normal	
2	FAN2	8038	Present	4545	30	<span style="color: green;">●</span> Normal	
3	FAN3	8038	Present	4610	30	<span style="color: green;">●</span> Normal	
4	FAN4	8038	Present	4599	30	<span style="color: green;">●</span> Normal	

Total 4 K < 1 > X 10 / Page To 1 Page

**Note**

- The **Speed(RPM)** column indicates the current speed of each fan.
- The **Speed Ratio(%)** column indicates the ratio of the current speed of each fan to its maximum speed.

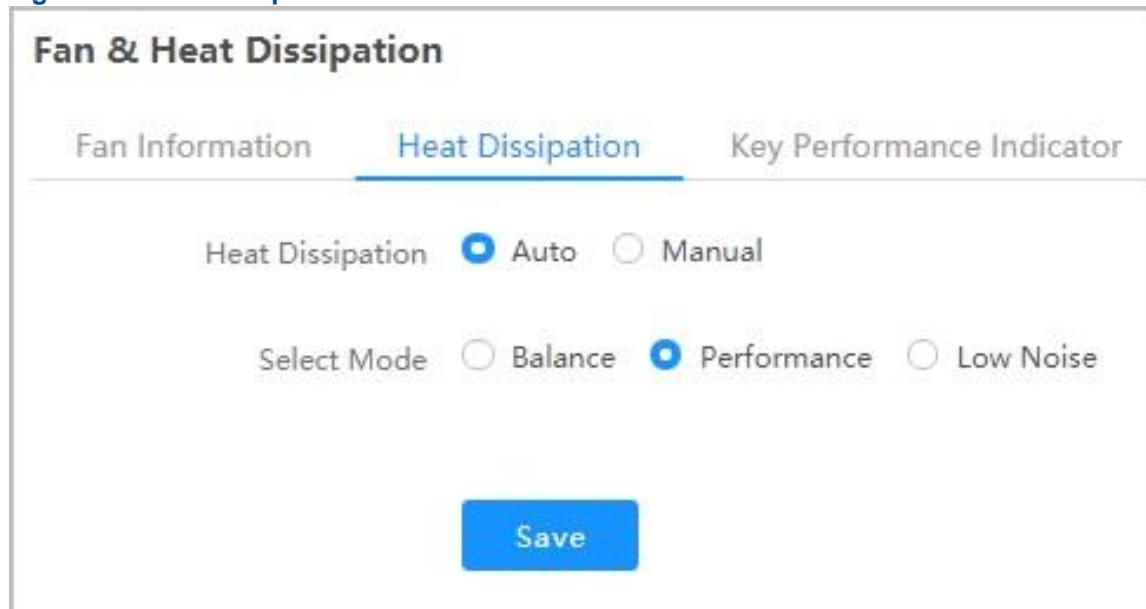
## 5.4 Configuring the Heat Dissipation Policy

### Abstract

A heat dissipation policy is configured in accordance with the environment where the server is held to ensure the performance and stability of the server.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed.
3. Click **Heat Dissipation**. The **Heat Dissipation** tab is displayed, see [Figure 5-6](#).

**Figure 5-6 Heat Dissipation Tab**

4. Perform the following operations as required.

If...	Then...
There is space above the top surface of the server, and the server is insensitive to noise	Set <b>Heat Dissipation</b> to <b>Auto</b> and then set <b>Select Mode</b> to <b>Balance</b> .
Servers are stacked together, and there is no space between them	Set <b>Heat Dissipation</b> to <b>Auto</b> and then set <b>Select Mode</b> to <b>Performance</b> .
The server is placed in an office or other areas that are sensitive to noise	Set <b>Heat Dissipation</b> to <b>Auto</b> and then set <b>Select Mode</b> to <b>Low Noise</b> .
The fan speed needs to be set manually for the server	Set <b>Heat Dissipation</b> to <b>Manual</b> and then set <b>Speed Ratio</b> .



#### Note

**Speed Ratio** indicates the ratio of the current speed of a fan to its maximum speed.

5. Click **Save**.

## 5.5 Querying Temperature KPIs

### Abstract

Air inlet temperatures, air outlet temperatures, and **CPU** temperatures of a server are **KPIs** related to fans and heat dissipation of the server. By querying these KPIs, you can learn about heat dissipation during the operation of the server.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Fan & Heat Dissipation**. The **Fan & Heat Dissipation** page is displayed.
3. Click **Key Performance Indicator**. The **Key Performance Indicator** tab is displayed, as shown in [Figure 5-7](#).

**Figure 5-7 Key Performance Indicator Tab**



4. Select a granularity period for a query.

**Note**

The data on the tab is automatically refreshed after the granularity period is selected.

5. (Optional) To export data, click **Export**.

## 5.6 Managing Storage Devices

### Abstract

The storage devices of a server refer to **RAID** controllers and hard disks.

The physical disks managed by a RAID controller can be created as logical disks.

On the **Storage Management** page, the **Storage Card** tab displays **SAS/SATA** disks, and the **NVMe** tab displays NVMe disks.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Storage Management**. The **Storage Management** page is displayed, see [Figure 5-8](#).

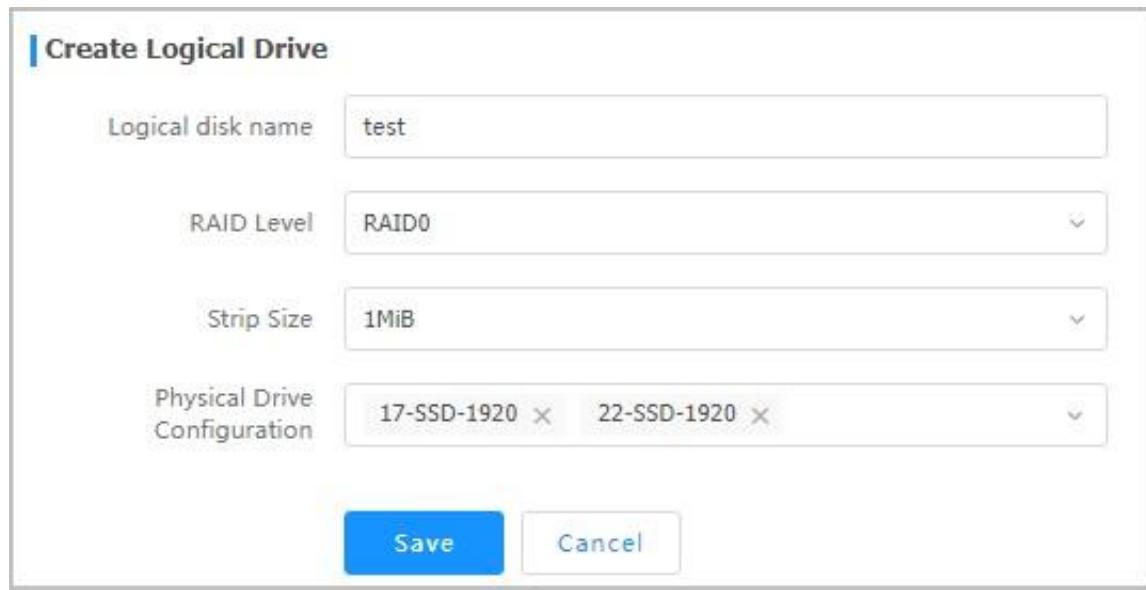
**Figure 5-8 Storage Management Page**

Controller Information			
Name:	RM243B	Location:	Embedded Slot1
Manufacturer:	ZTE	Chip Manufacturer:	Microchip
Chip Type:	PM8238	Health Status:	Normal
Device Version:	3.22	Packaged Version:	--
NVDATA Version:	--	BIOS Version:	--
Serial Number:	74377550002	SAS Address:	--
Device Interface:	SAS 12Gbps	Memory Size:	128 MiB
Temperature:	45 °C	Supported Strip Size Range:	16384-1048576 KiB
Supported RAID Levels:	RAID0, RAID1, RAID5, RAID10		

BBU			
Name:	--	Health Status:	--
Status:	absent	Temperature:	--

1. RAID controller
2. Logical disk
3. Physical disk
3. Perform the following operations as required.

To...	Do...
Check RAID controller and <b>BBU</b> information	On the <b>Storage Card</b> tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the <b>Storage Card</b> tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, <b>Status</b> includes: <ul style="list-style-type: none"> <li>● <b>Optimal</b></li> <li>● <b>Degraded</b></li> <li>● <b>Part Degraded</b></li> <li>● <b>Offline</b></li> </ul>
Set the UID indicator of a logical disk	<ol style="list-style-type: none"> <li>a. On the <b>Storage Card</b> tab, click the desired logical disk.</li> <li>b. Click <b>Settings</b> on the right. The <b>Logical Drive Setting</b> dialog box is displayed.</li> <li>c. Select <b>Open</b> or <b>Close</b>. <ul style="list-style-type: none"> <li>● <b>Open</b>: lights up the UID indicators of all member disks of the logical disk.</li> <li>● <b>Off</b>: lights off the UID indicators of all member disks of the logical disk.</li> </ul> </li> <li>d. Click <b>Submit</b>.</li> </ol>
Check physical disk information	On the <b>Storage Card</b> tab, click the desired physical disk. The detailed physical disk information is displayed on the right.
Create a logical disk	<ol style="list-style-type: none"> <li>a. On the <b>Storage Card</b> tab, click + next to a RAID controller. The <b>Create Logical Drive</b> area is displayed on the right, see <a href="#">Figure 5-9</a>.</li> <li>b. Configure the following parameters: <ul style="list-style-type: none"> <li>● <b>Logical disk name</b>: Enter the name of the logical disk.</li> <li>● <b>RAID Level</b>: Select the corresponding RAID level.</li> <li>● <b>Stripe Size</b>: Select a stripe size.</li> <li>● <b>Physical Drive Configuration</b>: Select the member disks that form the logical disk.</li> </ul> </li> <li>c. Click <b>Save</b>.</li> </ol>
Check <b>NVMe</b> disk information	On the <b>Storage Management</b> page, click <b>NVMe</b> to switch to the <b>NVMe</b> tab. The detailed NVMe disk information is displayed.

**Figure 5-9 Create Logical Drive Area**

The dialog box is titled 'Create Logical Drive'. It contains the following fields:

- Logical disk name: test
- RAID Level: RAID0
- Strip Size: 1MiB
- Physical Drive Configuration: 17-SSD-1920 X 22-SSD-1920 X

At the bottom are 'Save' and 'Cancel' buttons.



Different types of RAID controllers have different pages for creating logical disks.

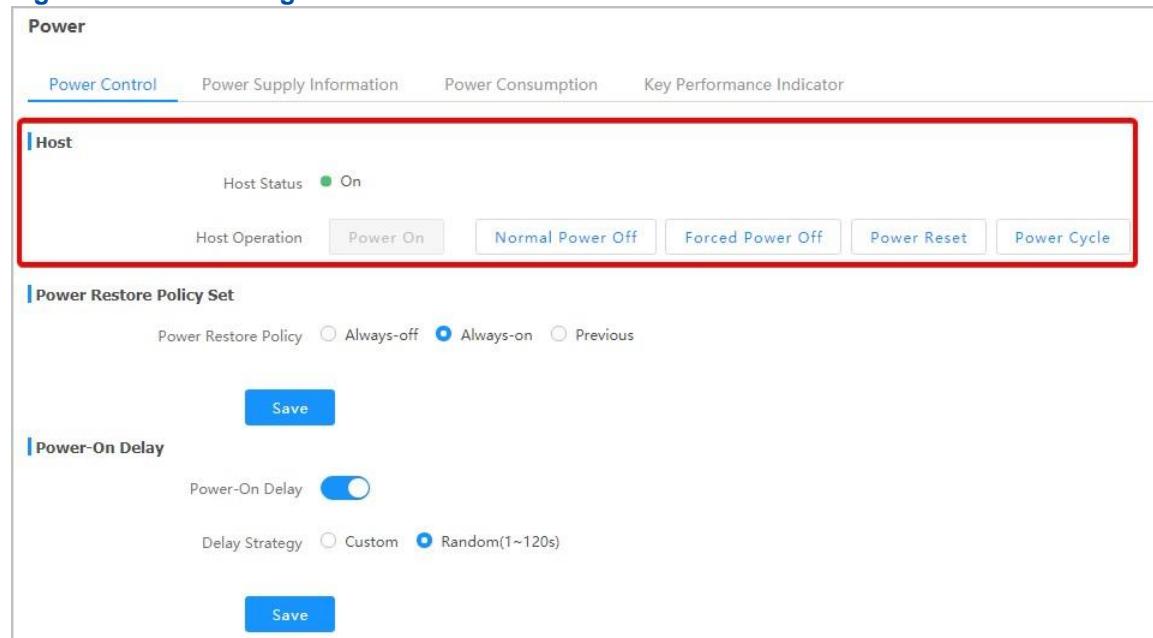
## 5.7 Powering On/Off the Server

### Abstract

When you are not on the customer site, you can remotely control the server on the PC to power on or off the server.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, see [Figure 5-10](#).

**Figure 5-10 Power Page**

3. In the **Host** area, check **Host Status**, and perform the following operations as required.

To...	Do...
Power on the server	Click <b>Power On</b> .
Power off the server	Click <b>Normal Power Off</b> .
Forcibly power off the server	Click <b>Forced Power Off</b> .
Perform a warm reboot	Click <b>Power Reset</b> . Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
Perform a cold reboot	Click <b>Power Cycle</b> . Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.

**Note**

The grayed button indicates the current power status of the server. For example, if the **Power On** button is grayed, the server is powered on.

## 5.8 Configuring the Server Startup Policy

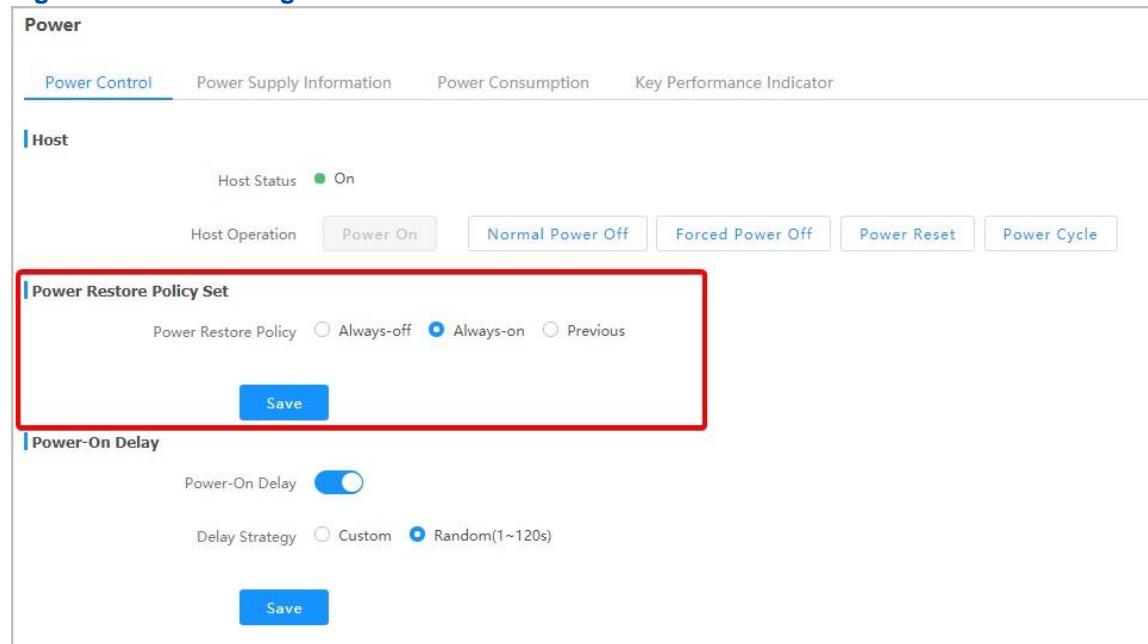
### Abstract

This procedure describes how to configure the server startup policy to specify the power status of the server after power is restored.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, see [Figure 5-11](#).

**Figure 5-11 Power Page**



3. In the **Power Restore Policy Set** area, set the server startup policy after the power is restored.
  - **Always-off**: The server remains powered off after power is restored.
  - **Always-on**: The server is powered on automatically after power is restored.
  - **Previous**: The server goes back to the previous power status after power is restored.
4. Click **Save**.

## 5.9 Configuring Power-On Delay Parameters

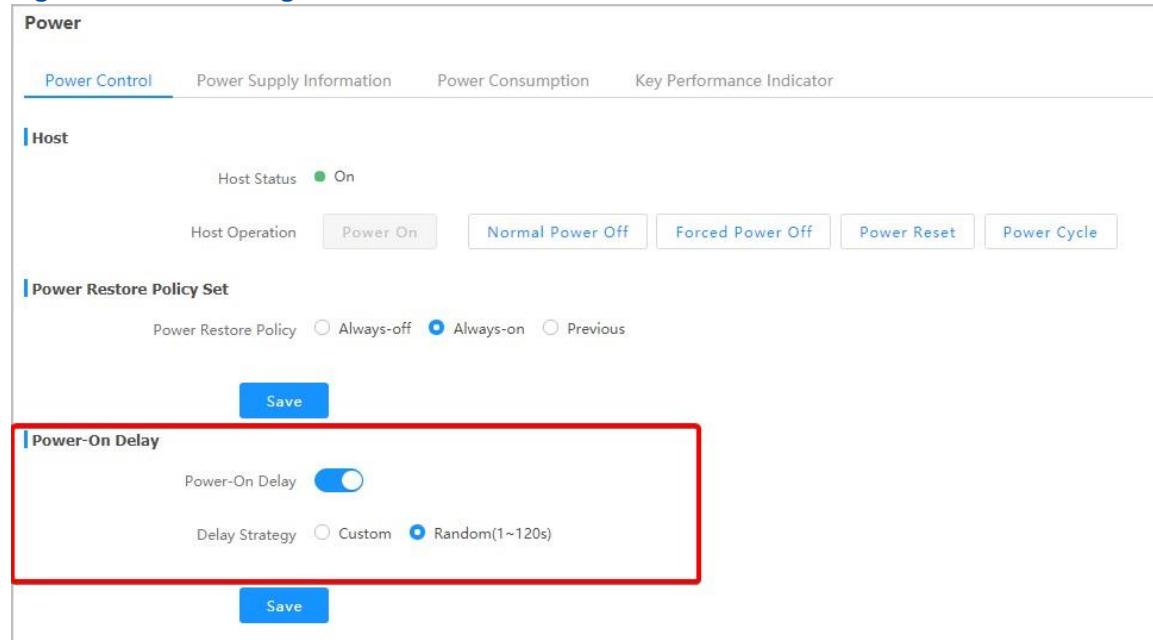
### Abstract

This procedure describes how to configure power-on delay parameters to stagger the power-on of servers.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed, see [Figure 5-12](#).

**Figure 5-12 Power Page**



3. Set the parameters in the **Power-On Delay** area. For a description of the parameters, refer to [Table 5-1](#).

**Table 5-1 Power-On Delay Parameter Descriptions**

Parameter	Setting
Power-On Delay	Select whether to enable the power-on delay function. <ul style="list-style-type: none"> <li>● To enable the power-on delay function, turn the switch on.</li> <li>● To disable the power-on delay function, turn the switch off.</li> </ul>
Delay Strategy	Select the corresponding power-on delay mode. <ul style="list-style-type: none"> <li>● <b>Custom:</b> The power-on delay time is user-defined. If <b>Custom</b> is selected, set <b>Custom Delay Duration</b>. Range: 1–120, unit: seconds.</li> <li>● <b>Random:</b> The power-on delay time is automatically generated by the system.</li> </ul>

4. Click **Save**.

## 5.10 Querying Power Supply Information

### Abstract

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

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
3. Click **Power Supply Information**. The **Power Supply Information** tab is displayed, see [Figure 5-13](#).

**Figure 5-13 Power Supply Information Tab**

Power		Power Control		Power Supply Information		Power Consumption		Key Performance Indicator	
				Power Supply Information		Power Mode Setting			
PSU1		Main Power Supply		Normal		PSU2			
Present Status	Present					Present Status	Absent		
Input Mode	AC					Input Mode	--		
Output Status	On					Output Status	--		
Manufacturer	Great Wall					Manufacturer	--		
Model	CRPS1200D					Model	--		
Serial Number	22M080011397					Serial Number	--		
Production Date	220913					Production Date	--		
Device Version	DC:1.02 PFC:1.01					Device Version	--		
Temperature Range(°C)	0~55					Temperature Range(°C)	--		
Current Temperature(°C)	26					Current Temperature(°C)	--		
Max Output Power(W)	1200					Max Output Power(W)	--		
Current Input Power(W)	353					Current Input Power(W)	--		
Current Output Power(W)	329					Current Output Power(W)	--		
Current Input Voltage(V)	224					Current Input Voltage(V)	--		
Current Output Voltage(V)	12.19					Current Output Voltage(V)	--		



### Note

The power supply input modes include:

- AC
- HVDC
- LVDC

## 5.11 Configuring the Power Mode

### Abstract

The server power modes include:

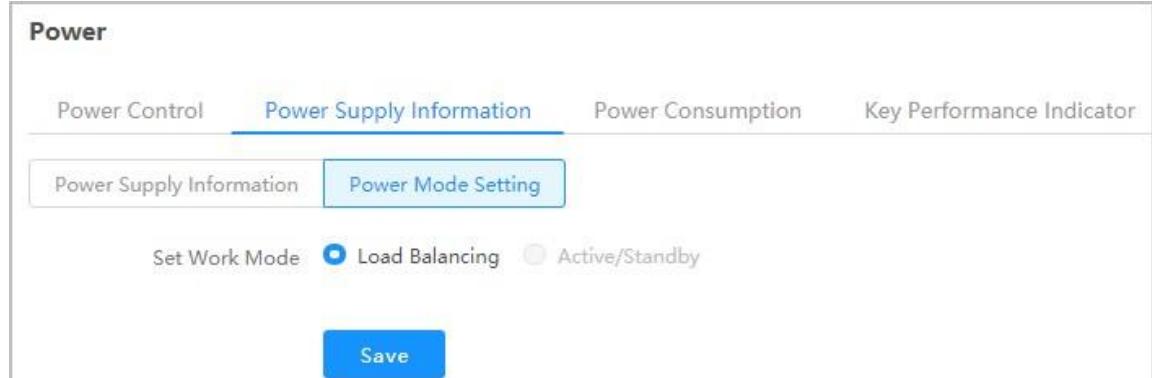
- **Load Balancing:** The power modules supply power in load-balancing mode.
- **Active/Standby:** The power modules supply power in active/standby mode.

A proper power mode enables the power modules to supply power to the server in a reasonable manner.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
3. Click **Power Supply Information**. The **Power Supply Information** tab is displayed.
4. Click **Power Mode Setting**. The **Power Mode Setting** tab is displayed, see [Figure 5-14](#).

[Figure 5-14 Power Mode Setting Tab](#)



5. Select a power mode.



### Note

The **Active/Standby** mode can be selected only when two or more power modules are present and in **Normal** state.

6. Click **Save**.

## 5.12 Querying Power Statistics

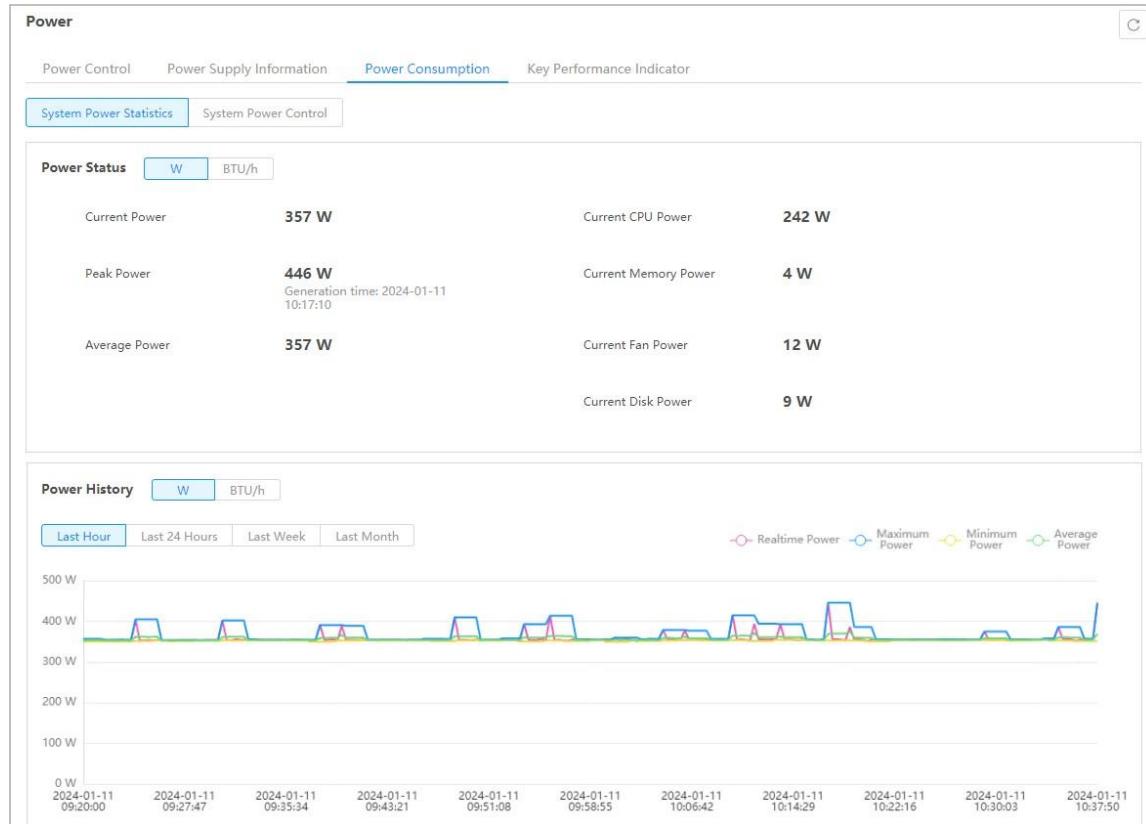
### Abstract

By querying power statistics, you can learn about the current power status of the server and the power changes within the specified time period.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
3. Click **Power Consumption**. The **Power Consumption** tab is displayed, see [Figure 5-15](#).

**Figure 5-15 Power Consumption Tab**



### Note

- The current power statistics of the server are displayed in the **Power Status** area.
- The historical power statistics of the server are displayed in the **Power History** area. You can specify a time range to query the corresponding power statistics.

## 5.13 Configuring Power Control Parameters

### Abstract

The power control parameters include:

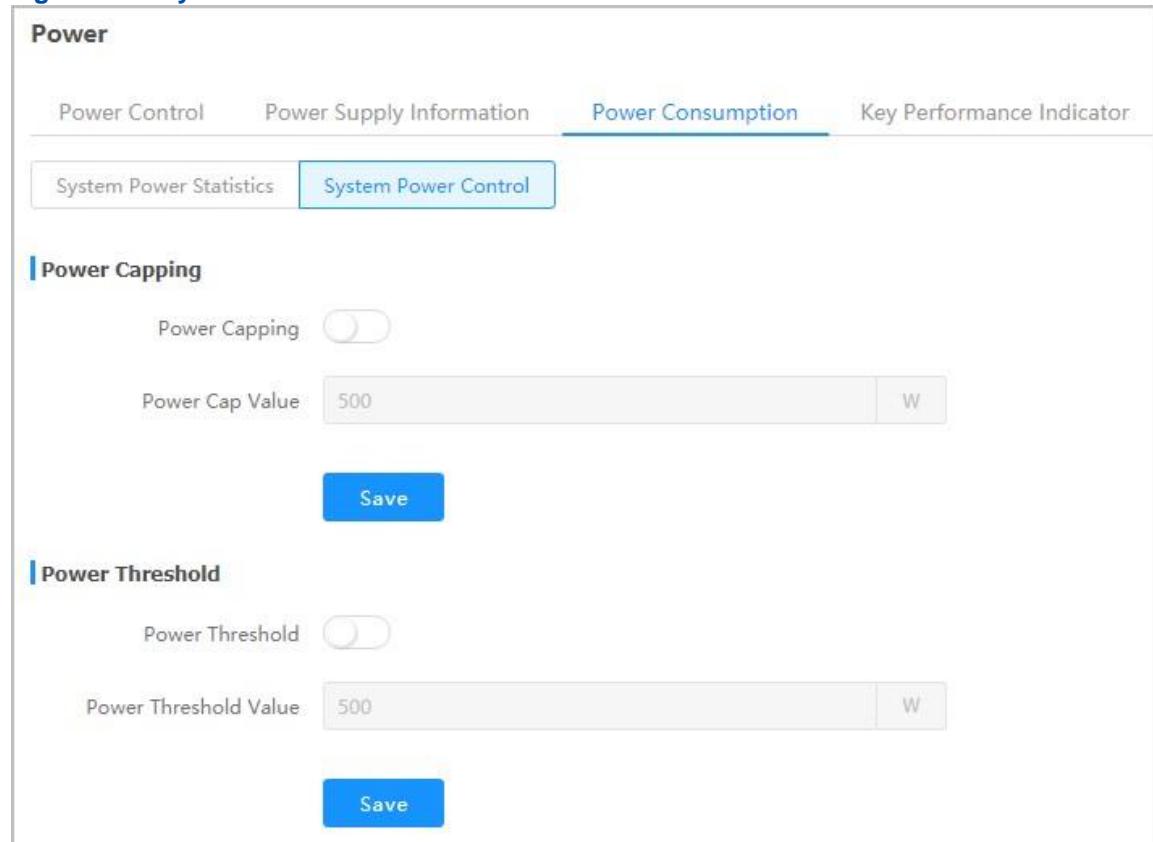
- **Power Capping**: The server power is limited to the power cap.
- **Power Threshold**: An alarm is raised when the server power exceeds the threshold.

This procedure describes how to configure the power control parameters.

## Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
3. Click **Power Consumption**. The **Power Consumption** tab is displayed.
4. Click **System Power Control**. The **System Power Control** tab is displayed, see [Figure 5-16](#).

**Figure 5-16 System Power Control Tab**



5. Perform the following operations as required.

To...	Do...
Set the power cap	<ol style="list-style-type: none"> <li>In the <b>Power Capping</b> area, turn on the <b>Power Capping</b> switch.</li> <li>In the <b>Power Cap Value</b> text box, set the power cap (range: 1–32767, unit: W).</li> <li>Click <b>Save</b>.</li> </ol>
Set the power threshold	<ol style="list-style-type: none"> <li>In the <b>Power Threshold</b> area, turn on the <b>Power Threshold</b> switch.</li> <li>In the <b>Power Threshold Value</b> text box, enter the power threshold (range: 5–32767, unit: W).</li> <li>Click <b>Save</b>.</li> </ol>

## 5.14 Querying Power KPIs

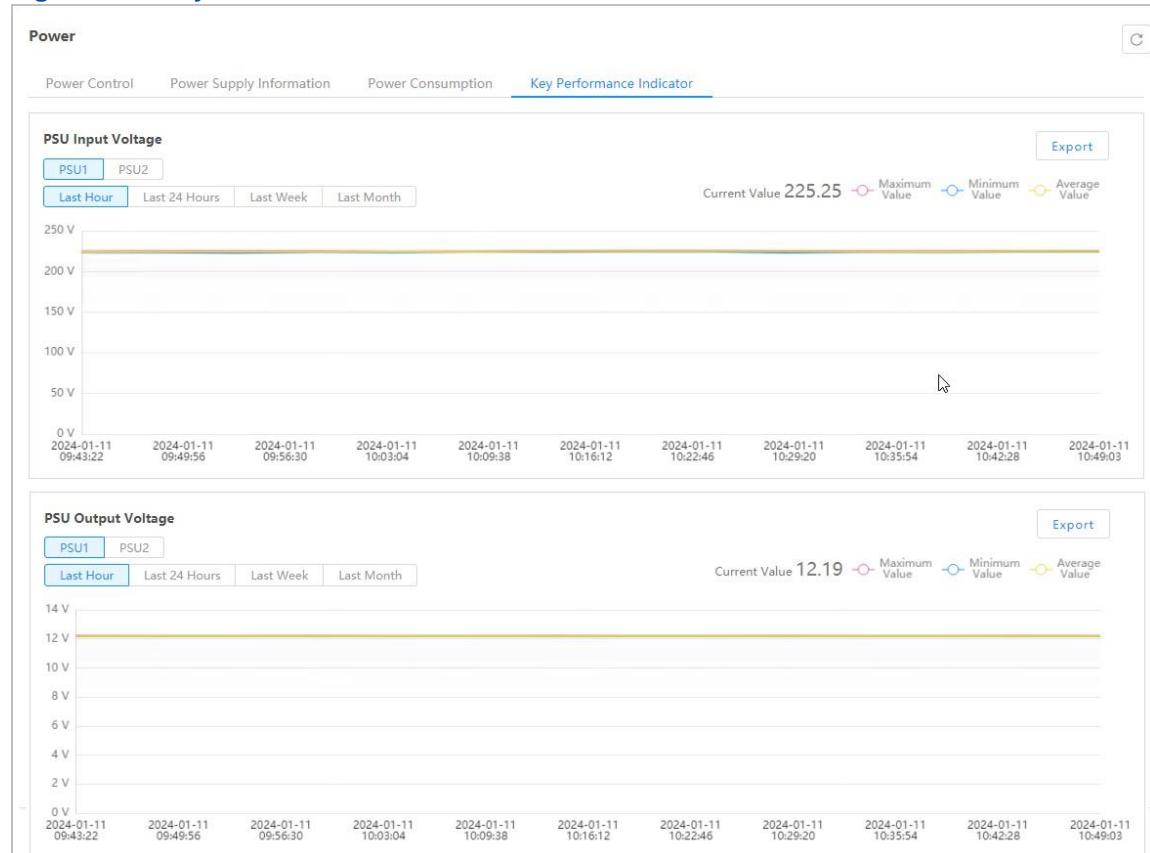
### Abstract

Input voltage and output voltage of a server are **KPIs** related to power modules and energy consumption of the server. By querying these KPIs, you can learn about power supply during the operation of the server.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **Power**. The **Power** page is displayed.
3. Click **Key Performance Indicator**. The **Key Performance Indicator** tab is displayed, as shown in [Figure 5-17](#).

**Figure 5-17 Key Performance Indicator Tab**



4. Select a granularity period for a query.



### Note

The data on the tab is automatically refreshed after the granularity period is selected.

5. (Optional) To export data, click **Export**.

## 5.15 Configuring Boot Options

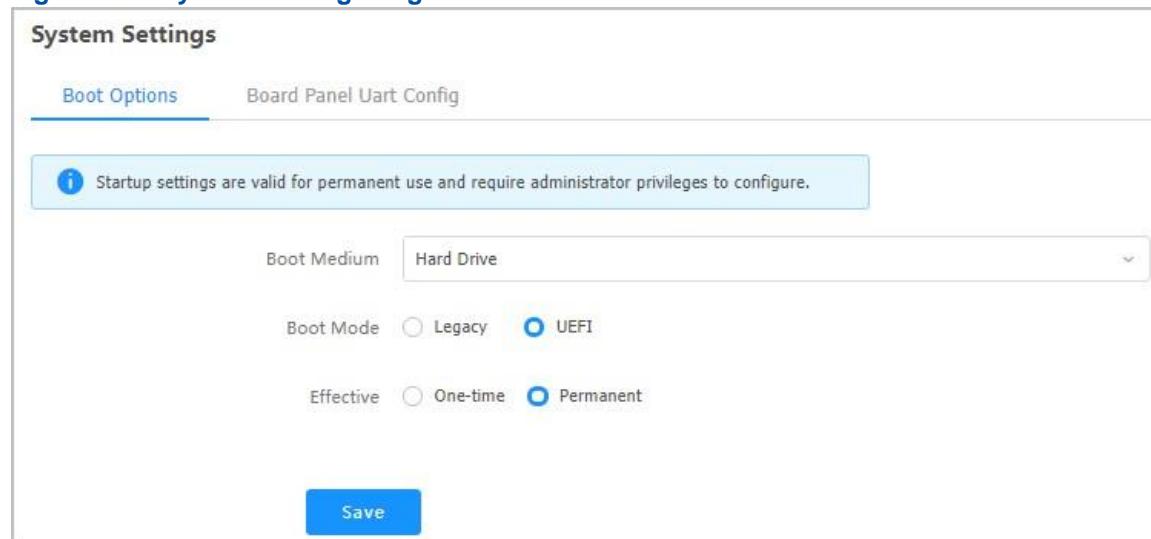
### Abstract

This procedure describes how to configure the boot device, boot mode, and boot option effectiveness for the server.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **System Settings**. The **System Settings** page is displayed, see [Figure 5-18](#).

**Figure 5-18 System Settings Page**



3. Set the parameters. For a description of the parameters, refer to [Table 5-2](#).

**Table 5-2 Boot Option Parameter Descriptions**

Parameter	Setting
Boot Medium	Select the device used to boot the server. <ul style="list-style-type: none"> <li>● <b>No Override</b>: configures no boot device and uses the default boot device configured in the <a href="#">BIOS</a>.</li> <li>● <b>Hard Drive</b>: forcibly boots from a hard drive.</li> <li>● <b>PXE</b>: forcibly boots from the <a href="#">PXE</a>.</li> <li>● <b>CD/DVD</b>: forcibly boots from the CD-ROM or DVD-ROM drive.</li> <li>● <b>BIOS Setup</b>: enters the BIOS menu after the server is booted.</li> <li>● <b>FDD/Removable Device</b>: forcibly boots from a floppy drive or removable device (for example, <a href="#">USB</a>).</li> </ul>
Boot Mode	Select a server boot mode.
Parameter	Setting

	<ul style="list-style-type: none"> <li>● <b>Legacy</b>: a traditional boot mode, which has some limitations.</li> <li>● <b>UEFI</b>: a newer boot mode, which supports the <a href="#">PXE</a> function in an <a href="#">IPv6/IPv4</a> network and provides the <a href="#">UEFI</a> Shell environment.</li> </ul> <p>UEFI mode is recommended.</p>
Effective	<p>Select whether the reconfigured server boot options are applied to the current restart only.</p> <ul style="list-style-type: none"> <li>● <b>One-time</b>: only effective for the current restart.</li> <li>● <b>Permanent</b>: permanently effective.</li> </ul>

4. Click **Save**.

## 5.16 Configuring the Serial Port Output Mode

### Abstract

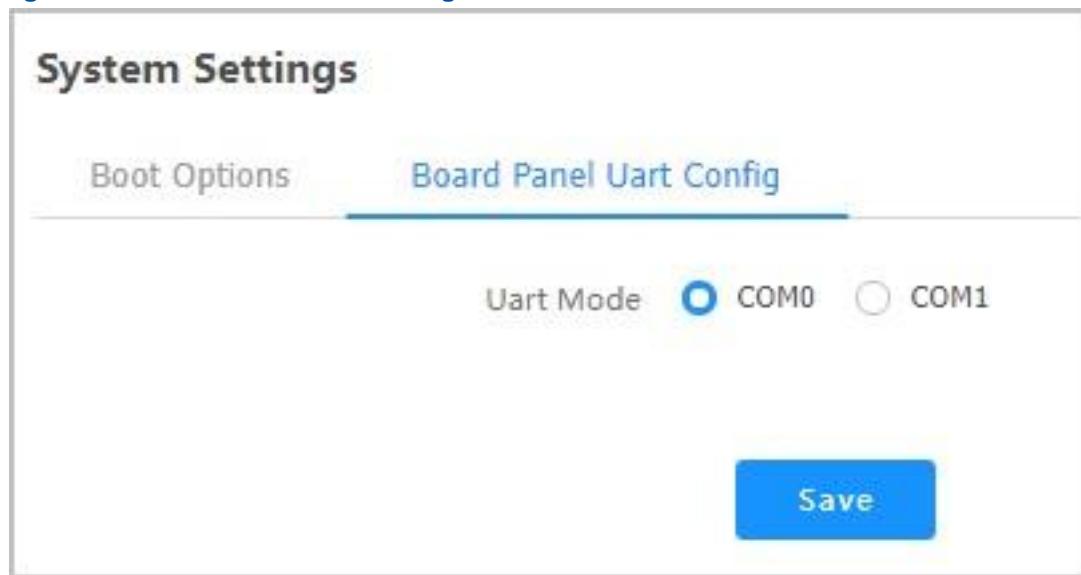
The serial port output modes on the panel include:

- COM1: The recorded information in the [BIOS](#) phase is output, which can be configured in the BIOS.
- COM2: There is no output in the BIOS phase and the system hot key cannot be responded. The recorded information in the [OS](#) phase is output.

### Steps

1. Select **System**. The **System** page is displayed.
2. From the navigation tree in the left pane, select **System Settings**. The **System Settings** page is displayed.
3. Click **Board Panel Uart Config**. The **Board Panel Uart Config** tab is displayed, see [Figure 5-19](#).

## 4. Figure 5-19 Board Panel Uart Config Tab



5. Select a serial port output mode.
6. Click **Save**.

# Chapter 6

# Diagnosis and

# Maintenance

---

## Table of Contents

Querying Alarms.....	76
Alarm Reporting Parameter Configuration.....	77
Configuring Screen Recording Parameters.....	83
Viewing Recorded Videos.....	85
Taking a Screenshot.....	86
Viewing POST Codes.....	87
Downloading Server Logs.....	88
Querying BMC Logs.....	89
Querying SEL Logs.....	90

## 6.1 Querying Alarms

### Abstract

By querying alarms, you can learn about the active alarms and system events of the server. System events include notifications and cleared alarms.

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Alarm & Event**. The **Alarm & Event** page is displayed, see [Figure 6-1](#).

**Figure 6-1 Alarm & Event Page**

Alarm & Event								
Current Alarms			System Events					
Download Alarms			Total: 4		Search		Advanced Query	
No.	Severity	Alarm Name	Description	Generation Time	Object Type	Position	Event Code	Handling Suggestions
4	<span style="color: red;">●</span> Critical	Hard disk RAID array is offline	Raid Card(RM243B(Embedded1)) logical driver(id:1, name:54645) is offline assert.	2023-05-24 22:16:56	Disk	LD_1	0x1a000083	<a href="#">Details</a>
3	<span style="color: orange;">●</span> Major	Hard disk is missing	Disk19 is missing(SN:unknown).	2023-05-23 16:48:55	Disk	DISK_19	0x1a000016	<a href="#">Details</a>
2	<span style="color: red;">●</span> Critical	Hard disk RAID array is offline	Raid Card(RM243B(Embedded1)) logical driver(id:0, name:osredhat75) is offline assert.	2023-05-23 16:38:36	Disk	LD_0	0x1a000083	<a href="#">Details</a>
1	<span style="color: yellow;">●</span> Minor	Redundancy Lost	PS_Redundant Redundancy Lost assert.	2023-05-23 16:37:18	PSU	PSU_0	0x0a0b0801	<a href="#">Details</a>

3. Perform the following operations as required.

To...	Do...
Query alarms by keyword	In the <b>Search</b> box, enter a keyword.
Query alarms based on the advanced parameters	<ol style="list-style-type: none"> <li>Click <b>Advanced Query</b>. Advanced query conditions are displayed.</li> <li>Set the query parameters.</li> <li>Click <b>Query</b>.</li> </ol>
View the handling suggestions for an alarm	Click <b>Details</b> for the alarm.
Save alarm information to the local PC	Click <b>Download Alarms</b> .
Query system events	Click <b>System Events</b> . The <b>System Events</b> tab is displayed.

## 6.2 Alarm Reporting Parameter Configuration

Alarms can be reported in the following ways:

- Reported through trap packets

For how to configure trap notification parameters, refer to [6.2.1 Configuring Trap Notification Parameters](#).

- Reported through syslog packets

For how to configure syslog notification parameters, refer to [6.2.2 Configuring Syslog Notification Parameters](#).

- Reported through emails

For how to configure email notification parameters, refer to [6.2.3 Configuring Email Notification Parameters](#).

## 6.2.1 Configuring Trap Notification Parameters

### Abstract

Trap notification parameters are used by the **BMC** to report alarms to a third-party **NMS** through traps.



### Note

Trap notification parameters are provided by the third-party NMS, so the values of trap notification parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

### Abstract

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed, see [Figure 6-2](#).

**Figure 6-2 Alarm Settings Page**

No.	Server Address	Trap Port	Current Status	Operation
1	10.239.212.117	323	Disabled	Edit Test
2	10.230.19.204	162	Enabled	Edit Test
3	10.239.211.53	53	Enabled	Edit Test
4	10.239.166.158	162	Enabled	Edit Test

Parameter	Setting
Trap	Turn on the <b>Trap</b> switch.

Trap Version	Select the <b>SNMP</b> version for traps. Options: <b>V1</b> , <b>V2C</b> , and <b>V1</b> .
<b>Parameter</b>	<b>Setting</b>
Select V3 User	This parameter is required if <b>Trap Version</b> is set to <b>V3</b> . Select a user that has permission to send alarms through SNMP.
Community Name	This parameter is required if <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b> . Enter the trap community name.
Confirm Community Name	This parameter is required if <b>Trap Version</b> is set to <b>V1</b> or <b>V2C</b> . Enter the trap community name.
Trap Host ID	Select the identifier of the host that reports alarms.
Event Sending Level	Select the level of events to be reported. For example, if <b>Event Sending Level</b> is set to <b>Critical</b> , only critical alarms are reported.

4. Click **Save**.
5. Set the parameters in the **Trap Server Configuration** area. For a description of the parameters, refer to [Table 6-2](#).

**Table 6-2 Parameter Descriptions for Trap Server Configuration**

Parameter	Setting
Server Address	After you click <b>Edit</b> , the parameter is activated. Enter the address of the server that receives alarms. An <b>IPv4</b> address, <b>IPv6</b> address, or domain name is supported.
Trap Port	After you click <b>Edit</b> , the parameter is activated. Enter the port number of the server that receives alarms. Range: 1–65535.
Current Status	After you click <b>Edit</b> , the parameter is activated. Select whether to enable the current server to receive alarms.

---

1. Set the parameters in the **Trap Function** area. For a description of the parameters, refer to [Table 6-1](#).

**Table 6-1 Trap Function Parameter Descriptions**

---

6. Click **Save**.

**Note**

After the **Edit** button is clicked, it is changed to the **Save** button.

---

7. (Optional) To send a test event to the server, click **Test**.

**Note**

If a message indicating "sent successfully" is displayed on the page, the trap is sent successfully.

## 6.2.2 Configuring Syslog Notification Parameters

### Abstract

This procedure describes how to configure syslog notification parameters so that the **BMC** can send logs to the syslog server. The sent logs include:

- **Operation Log:** records the information about users' operations on hardware devices, including manual operations and remote operations.
- **Audit Log:** records users' login to and logout of the Web portal of the **BMC**, BMC, and **KVM**.
- **Event Log:** records log and alarm information generated during the operation of the server.

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
3. Click **Syslog Notification**. The **Syslog Notification** tab is displayed, see [Figure 6-3](#).

**Figure 6-3 Syslog Notification Tab**

4. Set the parameters in the **Syslog Function** area. For a description of the parameters, refer to [Table 6-3](#).

**Table 6-3 Syslog Function Parameter Descriptions**

Parameter	Setting
Syslog	Turn on the <b>Syslog</b> switch.
Syslog Server Identity	Select the identifier of the syslog server to which logs are sent.
Transport Protocol	Select a log transmission protocol.

5. Click **Save**.

6. Set the parameters in the **Syslog Server Configuration** area. For a description of the parameters, refer to [Table 6-4](#).

**Table 6-4 Syslog Server Parameter Descriptions**

Parameter	Setting
Server Address	After you click <b>Edit</b> , the parameter is activated. Enter the address of the syslog server. An <a href="#">IPv4</a> address, <a href="#">IPv6</a> address, or domain name is supported.
Port	After you click <b>Edit</b> , the parameter is activated. Enter the port number of the syslog server. Range: 1–65535, default: 514.
Log Type	After you click <b>Edit</b> , the parameter is activated. Select one or more log types.

Current Status	After you click <b>Edit</b> , the parameter is activated. Select whether to enable the current syslog server to receive logs.
----------------	--

7. Click **Save**.

**Note**

After the **Edit** button is clicked, it is changed to the **Save** button.

8. (Optional) To send a test log to the syslog server, click **Test**.

**Note**

If a message indicating "sent successfully" is displayed on the page, the test log is sent successfully.

## 6.2.3 Configuring Email Notification Parameters

**Abstract**

This procedure describes how to configure email notification parameters so that the **BMC** can send emails to the specified mailbox.

**Prerequisite**

An **SMTP** server is already deployed. For details, refer to [4.10 Configuring an SMTP Server](#).

**Abstract**

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
3. Click **Email Notification**. The **Email Notification** tab is displayed, see [Figure 6-4](#).

**Figure 6-4 Email Notification Tab**

No.	Mailing Address	Description	Current Status	Operation
1	test01@zte.com.cn	test	Enabled	<a href="#">Edit</a> <a href="#">Test</a>
2	LQQ@zte.com.cn	123456789	Enabled	<a href="#">Edit</a> <a href="#">Test</a>
3				<a href="#">Edit</a> <a href="#">Test</a>
4				<a href="#">Edit</a> <a href="#">Test</a>

4. Set the parameters in the **SMTP Function** area. For a description of the parameters, refer to [Table 6-5](#).

**Table 6-5 SMTP Function Parameter Descriptions**

Parameter	Setting
SMTP	Turn on the <b>SMTP</b> switch.
SMTP Server Address	Enter the IP address of the SMTP server in <a href="#">IPv4</a> or <a href="#">IPv6</a> format.
SMTP Server Port	Enter the port number of the SMTP server. Range: 1–65535, default: 25.
TLS	Select whether to enable the encryption function.
Use Anonymous	Select whether emails are sent anonymously.
Sender User Name	Required if the <b>Use Anonymous</b> switch is turned off. Enter the username for SMTP authentication.
Sender Password	Required if the <b>Use Anonymous</b> switch is turned off. Enter the password of the email sender.
Sender Email Address	Enter the email address of the sender.
Parameter	Setting

Message Subject	Enter the subject of alarm emails.
Subject Attached	Select the information to be attached to the email subject. One or more options can be selected.

5. Click **Save**.
6. Set the parameters in the **Email Address For Receiving Alarm** area. For a description of the parameters, refer to [Table 6-6](#).

**Table 6-6 Mailbox Address Parameter Descriptions**

Parameter	Setting
Mailing Address	After you click <b>Edit</b> , the parameter is activated. Enter the email address to which alarms are sent.
Description	After you click <b>Edit</b> , the parameter is activated. Enter the description of the email address.
Current Status	After you click <b>Edit</b> , the parameter is activated. Select whether to enable the current email address to receive alarms.

7. Click **Save**.

**Note**

After the **Edit** button is clicked, it is changed to the **Save** button.

8. (Optional) To send a test alarm email to the email address, click **Test**.

**Note**

If a message indicating "sent successfully" is displayed on the page, the alarm email is sent successfully.

## 6.3 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 **Screenshot&Video** page.

## Prerequisite

Before enabling the screen recording function, you need to enable the KVM service. For details, refer to "[7.3 Configuring KVM Service Parameters](#)".



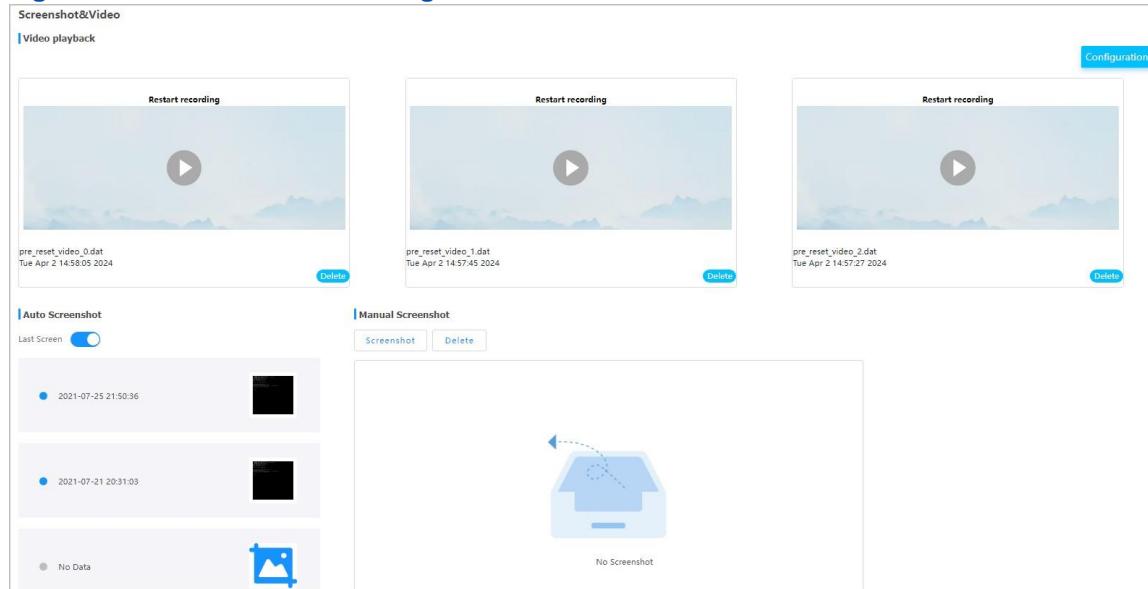
### Note

The launch of a KVM or [VNC](#) session temporarily disables recording. After the KVM or VNC session is closed, recording is automatically resumed.

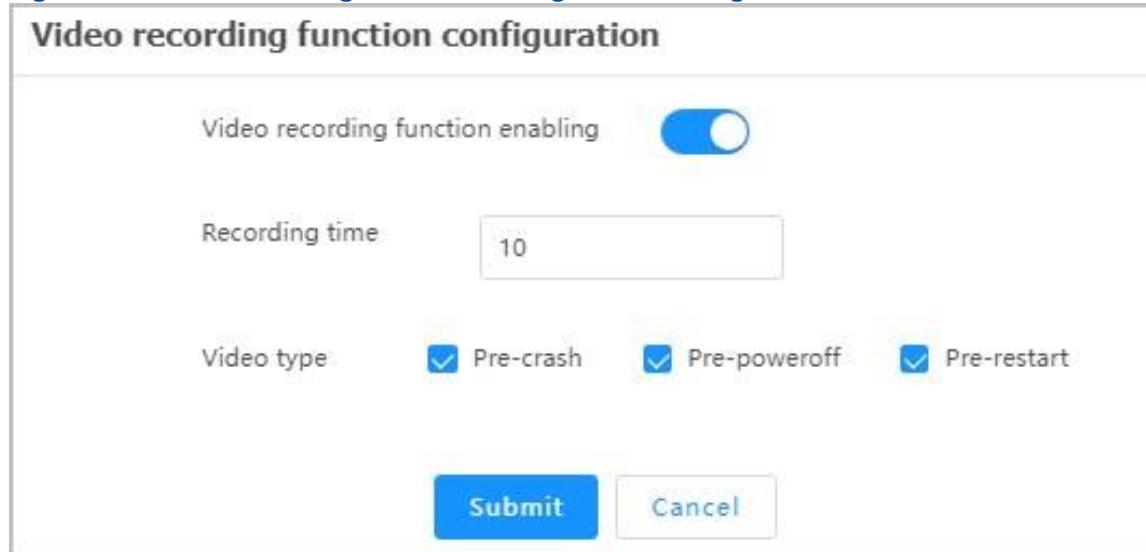
## Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Screenshot&Video**. The **Screenshot&Video** page is displayed, as shown in [Figure 6-5](#).

**Figure 6-5 Screenshot&Video Page**



3. Click **Configuration** in the upper right corner. The **Video recording function configuration** dialog box is displayed, as shown in [Figure 6-6](#).

**Figure 6-6 Video Recording Function Configuration Dialog Box**

4. Set the parameters. For a description of the parameters, refer to [Table 6-7](#).

**Table 6-7 Parameter Descriptions for the Screen Recording Function**

Parameter	Description
Video recording function enabling	Turn on the toggle switch.
Recording time	Enter the screen recording duration. Options: 10, 20, 30, 40, 50, and 60. Unit: seconds.
Video type	Select the events that trigger screen recording.

5. Click **Submit**.

## 6.4 Viewing Recorded Videos

### Abstract

After the screen recording function is enabled, the system automatically records the screen in accordance with the configured recording parameters before the server crashes, restarts, or powers off. You can view the recorded videos for fault diagnosis.

### Prerequisite

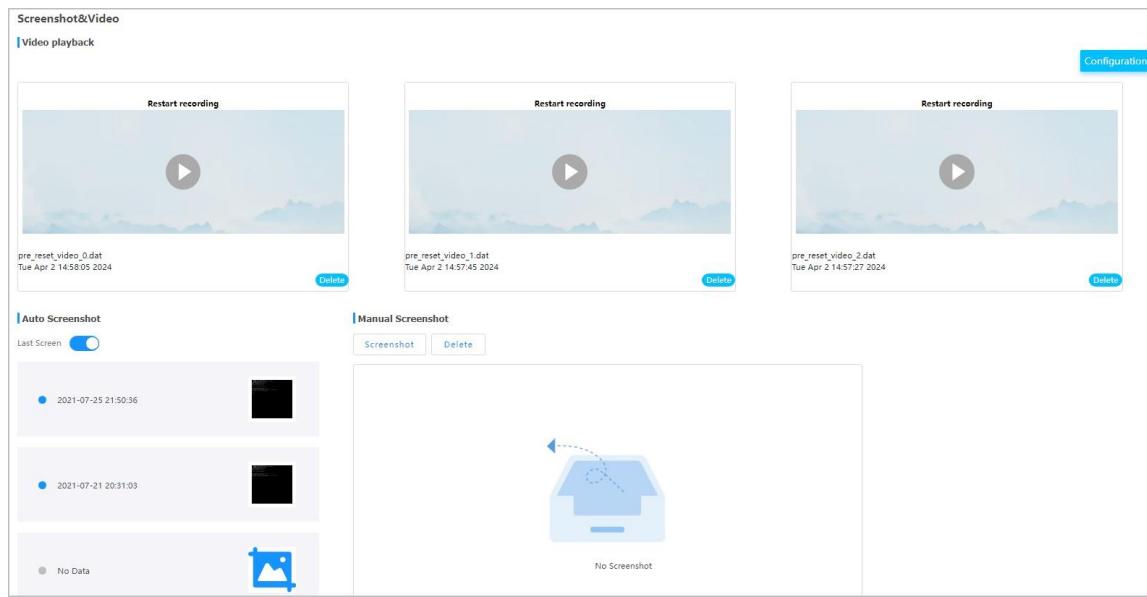
The screen recording function is enabled. For details, refer to "[6.3 Configuring Screen Recording Parameters](#)".

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.

- From the navigation tree in the left pane, select **Screenshot&Video**. The **Screenshot&Video** page is displayed, as shown in [Figure 6-7](#).

**Figure 6-7 Screenshot&Video Page**



### Note

The **Video playback** area displays the latest three recorded videos.

- Click to play a recorded video.

## 6.5 Taking a Screenshot

### Abstract

The screenshot function is used for fault diagnosis.



### Note

Before using the screenshot function, you must disable the [KVM](#) function.

Screenshots can be taken in the following ways:

- Automatic

Automatic screenshot is triggered when one of the following conditions is met:

→ The server is restarted after a fatal error (for example, a [CPU](#) fault) occurs. → The [BMC](#) triggers **Power Reset**. → The BMC triggers **Power Cycle**. → The BMC triggers **Forced Power Off**.

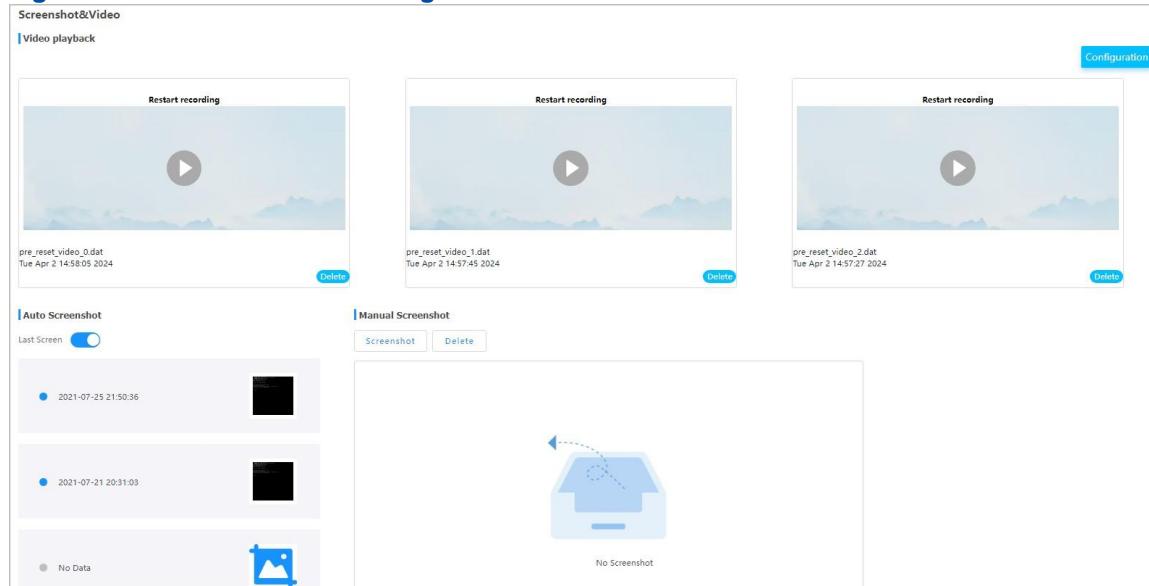
For a description of the power operations that can be triggered by the BMC, refer to [5.7 Powering On/Off the Server](#).

- Manual

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Screenshot&Video**. The **Screenshot&Video** page is displayed, see [Figure 6-8](#).

**Figure 6-8 Screenshot&Video Page**



3. Perform the following operations as required.

To...	Do...
Take screenshots automatically	Turn on the <b>Last Screen</b> switch.
Take a screenshot manually	Click <b>Screenshot</b> . The screenshot of the current screen is displayed at the bottom of the page. To delete the current screenshot, click <b>Delete</b> .

## 6.6 Viewing POST Codes

### Abstract

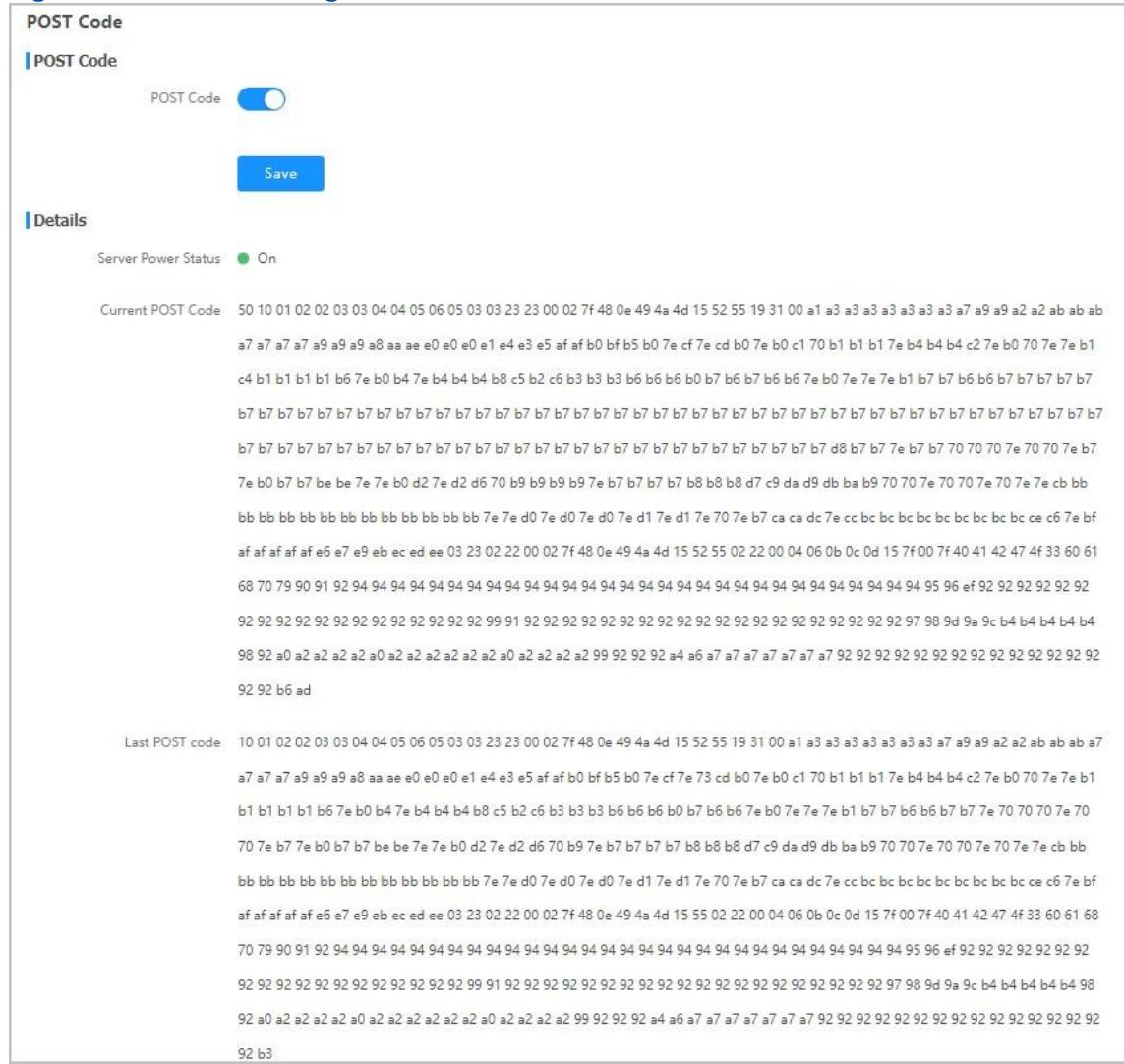
The **POST** code records the status of the server during power-on.

Check the POST code for fault diagnosis.

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **POST Code**. The **POST Code** page is displayed, see [Figure 6-9](#).

## Figure 6-9 POST Code Page



3. (Optional) If the POST code is not enabled, open **POST Code** and click **Save**.
4. View **Server Power Status**, **Current POST Code**, and **Last POST Code**.

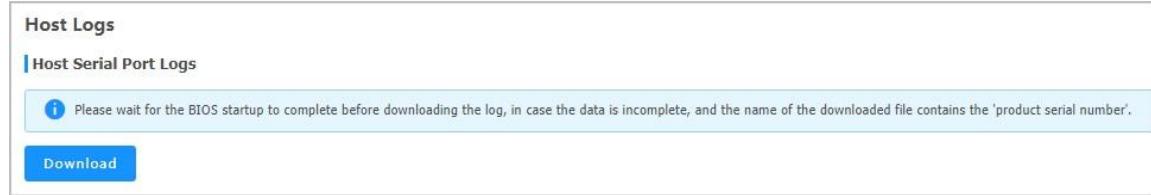
## 6.7 Downloading Server Logs

## Abstract

When a fault occurs, the server logs are written to the serial port. You can download these logs for fault diagnosis.

## Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Host Logs**. The **Host Logs** page is displayed, see [Figure 6-10](#).

**Figure 6-10 Host Log Page**

3. Click **Download**.

## 6.8 Querying BMC Logs

### Abstract

BMC logs include:

- **Operation Logs:** record the information about users' operations on the server, including manual operations and remote operations.
- **Audit Logs:** record users' login to and logout of the Web portal of the BMC, BMC, and [KVM](#).

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **BMC Logs**. The **BMC Logs** page is displayed, see [Figure 6-11](#).

**Figure 6-11 BMC Logs Page**

BMC Logs					
The page only displays about 100 logs generated recently. To view all the logs, please download the logs to view them locally.					
Operation Logs		Audit Logs			
Download Logs					Search(Fuzzy search only ... )
No.	Generation Time	Interface	User	Address	Details
112	2024-03-07 14:10:27	WEB	Administrator	10.	set time zone (Asia/Shanghai) successfully.
111	2024-03-07 14:10:27	WEB	Administrator	10.	disable NTP Server successfully.
110	2024-03-07 14:10:22	WEB	Administrator	10.	set bmc time to 2024-03-07 14:10:22 successfully.
109	2021-06-29 20:54:36	WEB	Administrator	10.	set asset tag: R8500 G5 successfully.
108	2021-06-29 20:56:52	WEB	Administrator	10.	set asset tag: R6900 G5 successfully.
107	2021-06-21 03:09:55	WEB	Administrator	10.	control chassis power on successfully.
106	2021-06-20 21:07:21	REDFISH	Administrator	10.	control chassis power cycle successfully.
105	2021-06-20 21:07:07	N/A	N/A	N/A	upgrade BIOS successfully.
104	2021-06-20 20:52:48	N/A	N/A	N/A	upgrade BIOS with preserve configuration successfully.
103	2021-06-20 20:52:47	REDFISH	N/A	N/A	begin upgrade BIOS successfully.

Total 112 10 / Page 1 Page

3. Perform the following operations as required.

To...	Do...

Query operation logs	<ol style="list-style-type: none"> <li>Click <b>Operation Logs</b> to switch to the <b>Operation Logs</b> tab.</li> <li>(Optional) In the <b>Search</b> box, enter a keyword.</li> <li>(Optional) Click <b>Download Logs</b>.</li> </ol>
Query audit logs	<ol style="list-style-type: none"> <li>Click <b>Audit Logs</b> to switch to the <b>Audit Logs</b> tab.</li> <li>(Optional) In the <b>Search</b> box, enter a keyword.</li> <li>(Optional) Click <b>Download Logs</b>.</li> </ol>

## 6.9 Querying SEL Logs

### Abstract

The **SEL** logs record event logs reported by sensors in the server system.

### Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **SEL Logs**. The **SEL Logs** page is displayed, see [Figure 6-12](#).

**Figure 6-12 SEL Logs Page**

SEL Logs					
		<a href="#">Download SEL Logs</a>	<a href="#">Clear SEL Logs</a>	<input type="text"/> <a href="#">Search</a>	<a href="#">Advanced Query</a>
Event ID	Generation Time	Sensor Name	Sensor Type	Description	Status
67	2023-07-20 09:21:53	BMC_BOOT_UP	System Boot/Restart Initiated	Initiated by hard reset	Asserted
66	2023-07-20 09:21:53	ACPI_STATUS	System ACPI Power State	S0/G0 'working'	Asserted
65	2023-07-20 09:20:14	System	Version Change	Software or F/W Change detected with associated Entity was successful.(deassertion event means 'unsuccessful')	Asserted
64	2023-07-20 09:19:00	System	Version Change	Firmware or software change detected with associated Entity.Informational. Success or failure not implied	Asserted
63	2023-07-19 15:59:50	SYS_RESTART	System Boot/Restart Initiated	Initiated by warm reset	Asserted
62	2023-07-19 15:59:48	ACPI_STATUS	System ACPI Power State	S0/G0 'working'	Asserted
61	2023-07-19 15:59:41	OS_STOP	OS Stop / Shutdown	OS Graceful Shutdown	Asserted
60	2023-07-19 15:59:41	ACPI_STATUS	System ACPI Power State	S5/G2 'soft-off'	Asserted
59	2023-07-19 15:57:30	ACPI_STATUS	System ACPI Power State	S0/G0 'working'	Asserted
58	2023-07-19 15:57:23	OS_STOP	OS Stop / Shutdown	OS Graceful Shutdown	Asserted

Total 67 [K](#) [<](#) [1](#) [2](#) [3](#) [4](#) [5](#) [>](#) [X](#) [10 / Page](#) [To](#) [1](#) [Page](#)

3. (Optional) Click **Advanced Query**, set the query conditions, and click **Query**.
4. Perform the following operations as required.

To...	Do...
Download SEL Logs	Click <b>Download SEL Logs</b> .
Clear SEL Logs	Click <b>Clear SEL Logs</b> .

# Chapter 7

# Service Management

---

## Table of Contents

Configuring Port Service Parameters.....	92
Configuring Web Service Parameters.....	94
Configuring KVM Service Parameters.....	97
Starting the KVM.....	99
Configuring Virtual Media Parameters.....	108
Mounting a Virtual Media Device.....	111
Configuring VNC Parameters.....	112
Configuring SNMP Parameters.....	114

## 7.1 Configuring Port Service Parameters

### Abstract

By configuring port service parameters, you can configure the status, secure port, non-secure port, and timeout period of each service of the **BMC**.

The parameters configured on the **Port Services** page are synchronized with the parameters configured on the following pages:

- **Web Services** page
- **Virtual Console** page
- **Virtual Media** page
- **VNC** page
- **SNMP** page

### Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Port Services**. The **Port Services** page is displayed, see [Figure 7-1](#).

**Figure 7-1 Port Services Page**

Port Services							
No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation
1	web	Open	80	443	30	20	Edit
2	kvm	Open	7578	7582	30	4	Edit
3	cd-media	Open	5120	5124	--	1	Edit
4	hd-media	Open	5123	5127	--	1	Edit
5	ssh	Open	--	22	10	--	Edit
6	vnc	Open	5900	5901	10	2	Edit
7	snmp	Open	161	--	--	--	Edit
8	redfish	Open	--	--	--	--	Edit
9	ipmi	Open	--	623	--	--	

3. Click **Edit** for a service to activate the parameters.
4. Set the parameters. For a description of the parameters, refer to **Table 7-1**.

**Table 7-1 Port Service Parameter Descriptions**

Parameter	Setting
Status	Select whether to enable a service.
Non Secure Port	<p>Enter the non-secure port number of the service.</p> <ul style="list-style-type: none"> <li>● Default non-secure port number of the Web service: 80.</li> <li>● Default non-secure port number of the <b>KVM</b> service: 7578.</li> <li>● Default non-secure port number of the CD media service: 5120.</li> <li>● Default non-secure port number of the HD media service: 5123.</li> <li>● Default non-secure port number of the <b>VNC</b> service: 5900.</li> <li>● Default non-secure port number of the <b>SNMP</b> service: 161.</li> </ul> <p>Other services do not support non-secure ports.</p> <p>Range of the non-secure port numbers: 1–65535.</p>
Secure Port	<p>Enter the secure port number of the service.</p> <ul style="list-style-type: none"> <li>● Default secure port number of the Web service: 443.</li> <li>● Default secure port number of the KVM service: 7582.</li> <li>● Default secure port number of the CD media service: 5124.</li> <li>● Default secure port number of the HD media service: 5127.</li> <li>● Default secure port number of the SSH service: 22.</li> <li>● Default secure port number of the VNC service: 5901.</li> <li>● Default secure port number of the <b>IPMI</b> service: 623.</li> </ul> <p>Other services do not support secure ports.</p> <p>Range of the secure port numbers: 1–65535.</p>
Timeout(Min)	<p>Timeout period after which the service exits if no operation is performed.</p> <p>Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).</p>

**Note**

You cannot configure the **Maximum Sessions** parameter.

5. Click **Save**.

## 7.2 Configuring Web Service Parameters

### Abstract

By configuring the Web service parameters, you can securely access the Web portal of the BMC through the local PC.

To configure the Web service parameters, perform the following operations:

1. Configuring basic parameters
2. Uploading the [SSL](#) certificate to the browser
3. Uploading the SSL certificate to the Web portal of the BMC

### Prerequisite

The *pem* file (containing the certificate file and private key file) is already obtained.

### Steps

#### Configuring Basic Parameters

1. On the Web portal of the BMC, select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Web Services**. The **Web Services** page is displayed, see [Figure 7-2](#).

**Figure 7-2 Web Services Page**

The screenshot shows the 'Web Services' configuration page. It includes sections for 'Basic Configuration' (HTTP and HTTPS ports, timeout period, active sessions, and a 'Save' button), 'SSL Certificate' (generate or upload), and 'Certificate Information' (displaying the certificate's issued by, issued to, validity period, and serial number). The 'HTTP' port is set to 80, and the 'HTTPS' port is set to 443.

3. Set the parameters. For a description of the parameters, refer to [Table 7-2](#).

**Table 7-2 Basic Parameter Descriptions**

Parameter	Setting
HTTP	Turn on the <b>HTTP</b> switch.
HTTP Port	Enter the non-secure port number of the Web service. Range: 1–65535, default: 80.
HTTPS	Turn on the <b>HTTPS</b> switch.
HTTPS Port	Enter the secure port number of the Web service. Range: 1–65535, default: 443.
Timeout Period	The Web service exits if no operation is performed within the specified timeout period. Enter the timeout period. Range: 1–30, unit: minutes.

#### Uploading the SSL Certificate to the Browser

4. On the **Settings** page of the browser (for example, Google Chrome) on the PC, select **Privacy and security**. The **Privacy and security** page is displayed.

5.

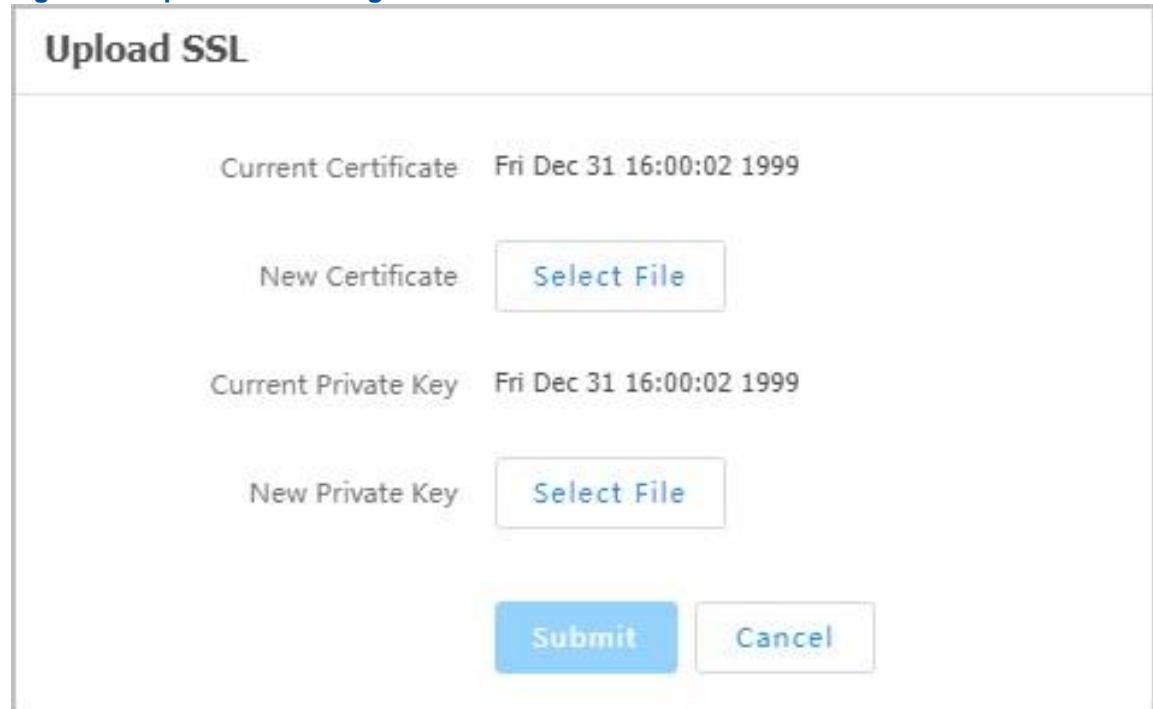


Click on the right of **Manage certificates** and upload the SSL certificate.

#### [Uploading the SSL Certificate to the Web Portal of the BMC](#)

6. On the **Web Services** page on the Web portal of the BMC, click **Upload SSL**. The **Upload SSL** dialog box is displayed, see [Figure 7-3](#).

[Figure 7-3 Upload SSL Dialog Box](#)



7. Select the prepared certificate file and private key file.
8. Click **Submit**.

#### **Verification**

In the address bar of your browser, enter the address of the Web portal of the BMC, and press **Enter** to see if the login page is displayed directly and there is no "Not secure" warning displayed, see [Figure 7-4](#).

[Figure 7-4 Secure Access](#)



[Figure 7-5](#) shows the "Not secure" warning displayed in the address bar of the browser.

**Figure 7-5 Insecure Access**

## 7.3 Configuring KVM Service Parameters

### Abstract

Before starting the [KVM](#), you need to configure the KVM service parameters.

### Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see [Figure 7-6](#).

**Figure 7-6 Virtual Console Page**

The screenshot shows the 'Virtual Console' configuration page. It includes sections for 'Basic Settings', 'Session Settings', and 'Keyboard & Mouse Settings'. The 'Basic Settings' section contains a 'KVM' switch (on), 'Port' (7585), 'Timeout Period' (30 Min), and a 'Save' button. The 'Session Settings' section contains 'Communication Encryption' (off), 'Single Port' (off), 'Retry Times' (3), 'Retry Interval' (10 s), and a 'Save' button. The 'Keyboard & Mouse Settings' section contains 'Keyboard Language' (Automatic Detection(AD)) and a 'Save' button.

3. Set the parameters in the **Basic Settings** area. For a description of the parameters, refer to [Table 7-3](#).

**Table 7-3 Basic Setting Parameter Descriptions**

Parameter	Setting
KVM	Turn on the <b>KVM</b> switch.
Port	Enter the KVM service port number. <ul style="list-style-type: none"> <li>● If the <b>Communication Encryption</b> switch is turned off in the <b>Session Settings</b> area, enter a non-secure port number.</li> <li>● If the <b>Communication Encryption</b> switch is turned on in the <b>Session Settings</b> area, enter a secure port number.</li> </ul>

Timeout Period	The KVM service exits if no operation is performed within the specified timeout period.
<b>Parameter</b>	<b>Setting</b>
	Enter the timeout period. Range: 1–30, unit: minutes.

4. Click **Save**.
5. Set the parameters in the **Session Settings** area. For a description of the parameters, refer to [Table 7-4](#).

**Table 7-4 Session Setting Parameter Descriptions**

Parameter	Setting
Communication Encryption	Select whether to encrypt KVM communication.
Single Port	Select whether to use port 443 in a unified manner when the KVM is started in <a href="#">HTML</a> mode. <ul style="list-style-type: none"> <li>● If the <b>Single Port</b> switch is turned on, port 443 is used in a unified manner.</li> <li>● If the <b>Single Port</b> switch is turned off, port 443 is not used in a unified manner.</li> </ul>
Retry Times	Enter the number of session retries. Range: 1–20.
Retry Interval	Enter the session retry interval. Range: 5–30, unit: seconds.

6. Click **Save**.
7. Set the parameters in the **Keyboard & Mouse Settings** area. For a description of the parameters, refer to [Table 7-5](#).

**Table 7-5 Keyboard & Mouse Setting Parameter Descriptions**

Parameter	Setting
Keyboard language	Select the keyboard language for remote KVM.

8. Click **Save**.

## 7.4 Starting the KVM

### Abstract

When you are not on the customer site, you can start the [KVM](#) to remotely control the server.

## Prerequisite

If the KVM needs to be started in Java mode, [JRE 8](#) or a later version (for example, `jre-8u191`) is already installed on the PC.

## Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, see [Figure 7-7](#).

**Figure 7-7 Virtual Console Page**

**Virtual Console**

Start KVM [HTML Virtual Console](#) [Java Virtual Console](#)

**Basic Settings**

KVM

Port

Timeout Period  Min

**Session Settings**

\* [Communication Encryption](#)

Single Port

Retry Times

Retry Interval  s

**Keyboard & Mouse Settings**

Keyboard Language

3. Perform the following operations as required.

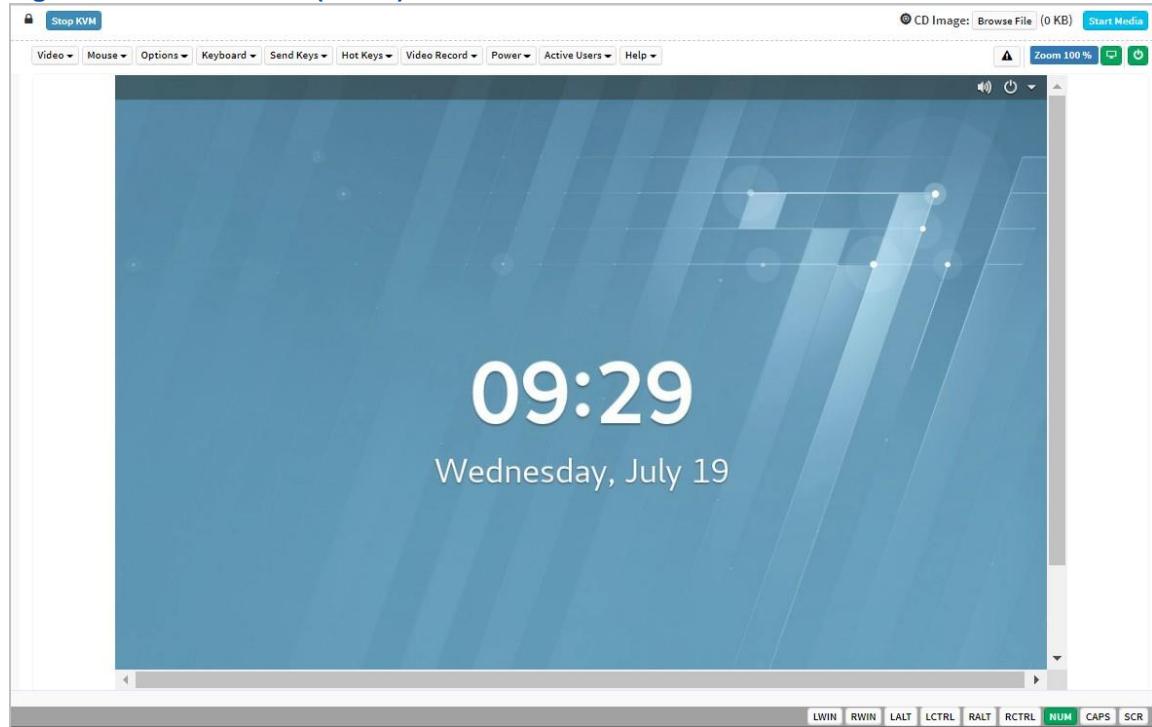
To...	Do...

Start the KVM in <a href="#">HTML</a> mode	<ol style="list-style-type: none"> <li>Click <b>HTML Virtual Console</b>. The <b>Remote KVM (HTML)</b> page is displayed, see <a href="#">Figure 7-8</a>.</li> <li>Perform the following operations as required. For a description of the operations, refer to <a href="#">Table 7-6</a>.</li> </ol>
Start the KVM in Java mode	<ol style="list-style-type: none"> <li>In the search box in the lower left corner of the PC, enter <i>Java</i>.</li> <li>In the search result, select <b>Java</b>. The <b>Java Control Panel</b> dialog box is displayed.</li> <li>Click <b>Security</b>. The <b>Security</b> window is displayed.</li> </ol>
To...	<b>Do...</b>
	<ol style="list-style-type: none"> <li>Click <b>Edit Site List</b>. The <b>Exception Site List</b> dialog box is displayed.</li> <li>Click <b>Add</b> to add the address of the Web portal of the BMC.</li> <li>Click <b>OK</b> to return to the <b>Security</b> window.</li> <li>Click <b>OK</b>.</li> <li>On the <b>Virtual Console</b> page of the Web portal of the BMC, click <b>Java Virtual Console</b>. A dialog box indicating whether to keep <i>jviewer.jnlp</i> is displayed.</li> <li>Click <b>Keep</b>.</li> <li>In the lower left corner of the browser, click <i>jviewer.jnlp</i>. A dialog box indicating whether to proceed is displayed.</li> <li>Click <b>Continue</b>. The <b>Do you want to run this application?</b> dialog box is displayed.</li> <li>Select <b>I accept the risk and want to continue to run this app.</b> and click <b>Run</b>. The <b>Untrusted Connection</b> dialog box is displayed.</li> <li>Click <b>Yes</b>. The <b>Remote KVM (JAVA)</b> page is displayed, see <a href="#">Figure 7-9</a>.</li> <li>Perform the following operations as required. For a description of the operations, refer to <a href="#">Table 7-7</a>.</li> </ol>



### 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.

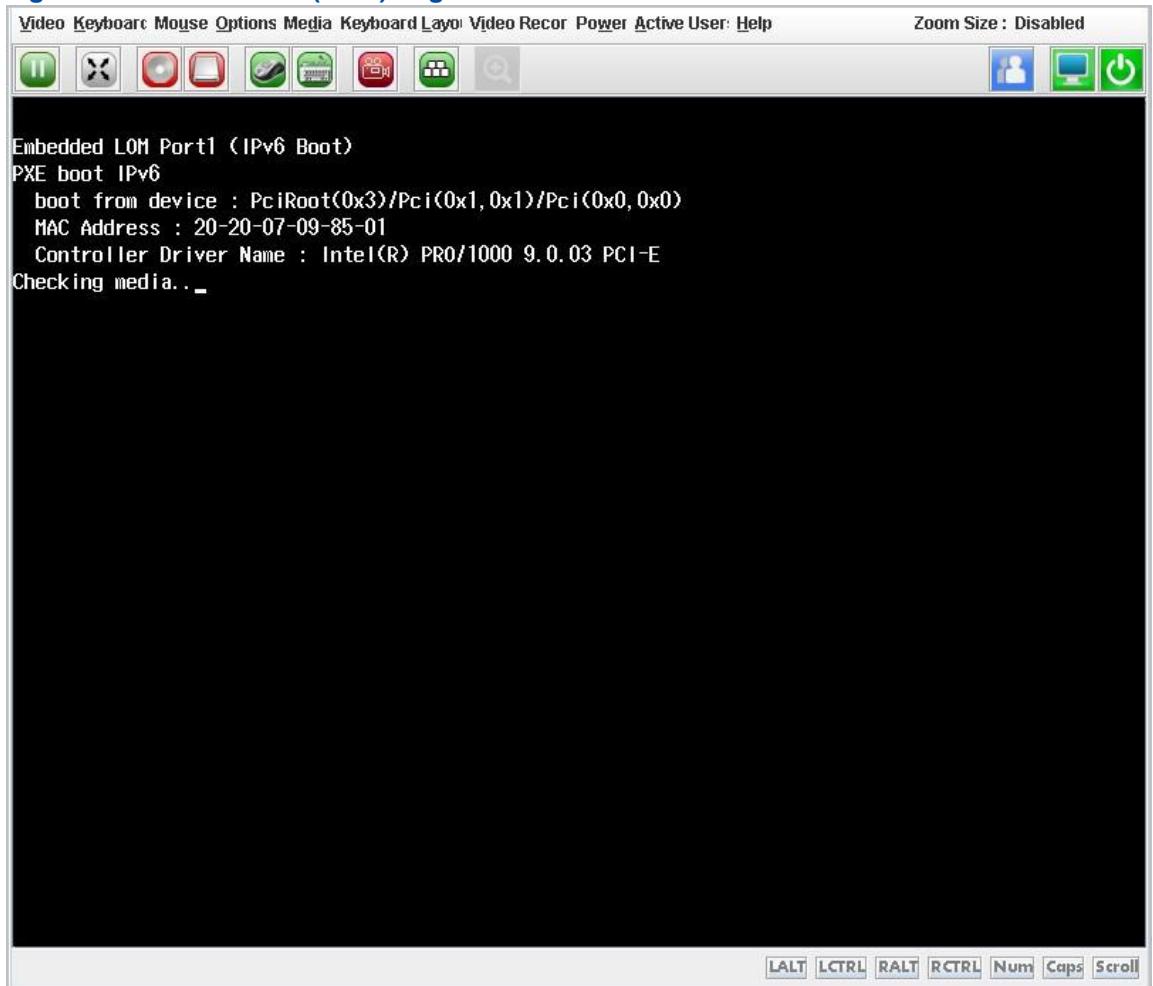
**Figure 7-8 Remote KVM (HTML)****Table 7-6 Descriptions for the Remote KVM (HTML) Operations**

Operation	Description
Stop the KVM	Click <b>Stop KVM</b> to exit the <b>Remote KVM (HTML)</b> page.
Mount a local <i>iso</i> file	<ol style="list-style-type: none"> <li>Click <b>Browse File</b> next to <b>CD Image</b>, and select the <i>iso</i> file from the PC.</li> <li>Click <b>Start Media</b>.</li> </ol>
Display the notifications received	Click  .
Lock the display of the server	<p>Lock the server display through either of the following ways:</p> <ul style="list-style-type: none"> <li>Click .</li> <li>Select <b>Video &gt; Display OFF</b>.</li> </ul> <p>After the server display is locked, if another user wants to view a server screen, a permission request is sent to the current active user. The user can view the server screen only after being authorized by the current active user.</p>

Unlock the server display	<p>Unlock the server display through either of the following ways:</p> <ul style="list-style-type: none"> <li>Click </li> <li>Select <b>Video &gt; Display ON</b>.  is converted to </li> </ul>
---------------------------	--

Operation	Description
Pause a remote control screen	Select <b>Video &gt; Pause Video</b> .
Resume a remote control screen	Select <b>Video &gt; Resume Video</b> .
Refresh a remote control screen	Select <b>Video &gt; Refresh Video</b> .
Capture the current screen	Select <b>Video &gt; Capture Screen</b> .
Display or hide the mouse pointer on the server screens	<ul style="list-style-type: none"> <li>To display the mouse pointer on the server screens, click <b>Mouse</b>, and select <b>Show Client Cursor</b>.</li> <li>To hide the mouse pointer on the server screens, click <b>Mouse</b>, and clear <b>Show Client Cursor</b>.</li> </ul>
Set the mouse mode	<p>Click <b>Mouse</b>, and select <b>Absolute Mouse Mode</b>.</p> <p>In absolute mouse mode, the absolute position of the local mouse is transferred to the server to make the mouse on the server move.</p>
Set keyboard layout	<ol style="list-style-type: none"> <li>Select <b>Keyboard</b>.</li> <li>In the displayed submenu, select the keyboard layout, including <b>English U.S</b>, <b>German</b> and <b>Japanese</b>. <b>English U.S</b> is selected by default.</li> </ol>
Set video recording time length	<ol style="list-style-type: none"> <li>Select <b>Video Record &gt; Record Settings</b>. The <b>Record Settings</b> dialog box is displayed.</li> <li>Set the video recording time length with a range of 1–1800 seconds.</li> <li>Click <b>OK</b>.</li> </ol>
Record videos	Select <b>Video Record &gt; Record Video</b> .
Stop recording	Select <b>Video Record &gt; Stop Recording</b> .
Shut down the server	<p>Shut down the server through either of the following ways:</p> <ul style="list-style-type: none"> <li>Select <b>Power &gt; Orderly shutdown</b>.</li> <li>Click </li> </ul>

Start the server	Start the server through either of the following ways: <ul style="list-style-type: none"><li>● Select <b>Power &gt; Power On Server</b>.</li><li>● Click </li></ul>
Perform a cold reboot	Select <b>Power &gt; Power Cycle Server</b> . 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 <b>Power &gt; Reset Server</b> . Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
<b>Operation</b>	<b>Description</b>
View the users that are using remote control	Select <b>Active Users</b> .

**Figure 7-9 Remote KVM (Java) Page**

**Table 7-7 Descriptions for the Remote KVM (JAVA) Operations**

Operation	Description
Pause a remote control screen	<p>Pause a remote control screen through one of the following ways:</p> <ul style="list-style-type: none"> <li>● Select <b>Video &gt; Pause Redirection</b>.</li> <li>●  Click</li> <li>● Press <b>Alt+P</b>.</li> </ul>
Resume a remote control screen	<p>Resume the remote control screen through one of the following ways:</p> <ul style="list-style-type: none"> <li>● Select <b>Video &gt; Resume Redirection</b>.</li> <li>●  Click</li> <li>● Press <b>Alt+R</b>.</li> </ul>

Operation	Description
Refresh a remote control screen	<p>Refresh the remote control screen through either of the following ways:</p> <ul style="list-style-type: none"> <li>● Select <b>Video &gt; Refresh Video</b>.</li> <li>● Press <b>Alt+E</b>.</li> </ul>
Switch the host screen display mode	<ul style="list-style-type: none"> <li>● To display the remote screen on the host, select <b>Video &gt; Turn ON Host Display</b>.</li> <li>● To not display the remote screen on the host, select <b>Video &gt; Turn OFF Host Display</b>.</li> </ul> <p>Note: You can use either of the following methods to rapidly switch between the remote screen display modes of the host.</p> <ul style="list-style-type: none"> <li>●  Click</li> <li>● Press <b>Alt+N</b>.</li> </ul>
Capture the current screen	<p>Capture the current screen through either of the following ways:</p> <ul style="list-style-type: none"> <li>● Select <b>Video &gt; Capture Screen</b>.</li> <li>● Press <b>Alt+S</b>.</li> </ul>
Set a video decoding mode	<ol style="list-style-type: none"> <li>Select <b>Video &gt; Compression Mode</b>.</li> <li>Select a video decoding mode from the displayed submenu.</li> </ol>
Set the video display quality	<ol style="list-style-type: none"> <li>Select <b>Video &gt; DCT Quantization Table</b>.</li> <li>Select the video display quality from the displayed submenu.</li> </ol> <p>The video display quality is divided into eight levels from 0 through 7, with video quality degraded in turn.</p>

Define a key combination	<ol style="list-style-type: none"> <li>Select <b>Keyboard &gt; Hot Keys &gt; add Hot Keys</b>. The <b>User Defined Macros</b> page is displayed.</li> <li>Click <b>add</b>. The <b>Add Macros</b> page is displayed.</li> <li>Press and then release the user-defined key combination.</li> <li>Click <b>OK</b>.</li> </ol>
Enable full keyboard support	<ul style="list-style-type: none"> <li>To enable full keyboard support, click <b>Keyboard</b>, and select <b>Full Keyboard Support</b>.</li> <li>To disable full keyboard support, click <b>Keyboard</b>, and clear <b>Full Keyboard Support</b>.</li> </ul>
Display or hide the mouse pointer	<ul style="list-style-type: none"> <li>To display the mouse pointer, click <b>Mouse</b>, and select <b>Show Client Cursor</b>.</li> <li>To hide the mouse pointer, click <b>Mouse</b>, and clear <b>Show Client Cursor</b>.</li> </ul> <p>You can use either of the following methods to rapidly change the mouse display modes on the PC.</p> <ul style="list-style-type: none"> <li>Press <b>Alt+C</b>.</li> <li> Click .</li> </ul>
Set the network bandwidth	<ol style="list-style-type: none"> <li>Select <b>Options &gt; Bandwidth</b>.</li> </ol>

Operation	Description
	<ol style="list-style-type: none"> <li>Select the desired network bandwidth from the displayed submenu.</li> </ol>
Change the encryption status of the mouse/keyboard	<ul style="list-style-type: none"> <li>To enable mouse/keyboard encryption, click <b>Options</b>, and select <b>Keyboard/Mouse Encryption</b>.</li> <li>To disable mouse/keyboard encryption, click <b>Options</b>, and clear <b>Keyboard/Mouse Encryption</b>.</li> </ul>
Set the scaling mode of a remote screen	<ol style="list-style-type: none"> <li>Select <b>Options &gt; Zoom</b>.</li> <li>In the displayed submenu, set the zoom scale of the remote screen. <ul style="list-style-type: none"> <li><b>Zoom In</b>: zooms in the remote screen.</li> <li><b>Zoom Out</b>: zooms out the remote screen.</li> <li><b>Actual Size</b>: displays the remote screen in the proportion of 100%.</li> <li><b>Fit to Client Resolution</b>: displays the remote screen in the resolution of the local client system.</li> <li><b>Fit to Host Resolution</b>: displays the remote screen in the resolution of the remote server system.</li> </ul> </li> </ol>

Send an <b>IPMI</b> command to the server	<ol style="list-style-type: none"> <li>Select <b>Options &gt; Send IPMI Command</b>. The <b>IPMI Command Dialog</b> window is displayed.</li> <li>Enter the <b>IPMI</b> command.</li> <li>Click <b>Send</b>.</li> </ol> <p>The IPMI command supports hex format and <b>ASCII</b> format.</p>
Set the <b>GUI</b> language	<ol style="list-style-type: none"> <li>Select <b>Options &gt; GUI Languages</b>.</li> <li>Select the GUI language from the displayed submenu.</li> </ol>
Set the privilege request mode	<ol style="list-style-type: none"> <li>Select <b>Options &gt; Block Privilege Request</b>.</li> <li>Select a privilege request block mode from the displayed submenu.             <ul style="list-style-type: none"> <li>● <b>Allow only Video</b>: The permission for viewing the information displayed on the server is automatically granted to the user who initiates a privilege request.</li> <li>● <b>Deny Access</b>: Privilege requests in the system are blocked.</li> </ul> </li> </ol>
Mount a local <i>iso</i> file	<ol style="list-style-type: none"> <li>Open the <b>Virtual Media</b> window in either of the following ways:             <ul style="list-style-type: none"> <li>● Select <b>Media &gt; Virtual Media Wizard...</b>, and switch to the <b>CD/DVD</b> tab.</li> <li>●  Click .</li> </ul> </li> <li>Click <b>Browse</b> and select a local <i>iso</i> file.</li> <li>Click <b>Connect</b>.</li> </ol>
Mount a local folder	<ol style="list-style-type: none"> <li>Create an <i>iso</i> file on the PC.</li> <li>Open the <b>Virtual Media</b> window in either of the following ways:             <ul style="list-style-type: none"> <li>● Select <b>Media &gt; Virtual Media Wizard...</b>, and switch to the <b>Hard Disk/USB</b> tab.</li> <li>●  Click .</li> </ul> </li> <li>Select <b>physical drive &gt; folder path</b>.</li> </ol>

Operation	Description
	<ol style="list-style-type: none"> <li>Click <b>Browse</b> and select a local folder path.</li> <li>Set <b>Size</b> and <b>folder path</b>.</li> <li>Click <b>Connect</b>.</li> </ol> <p>The value of <b>Size</b> must be <math>2^n</math>, such as 2, 4 and 8. The path specified by <b>folder path</b> needs to be the same as that of the new <i>iso</i> file.</p>
Set keyboard layout	<ol style="list-style-type: none"> <li>Select <b>Keyboard Layout</b>.</li> <li>Select the keyboard layout from the displayed submenu.</li> </ol>
Open the soft keyboard	 Click .

Configure video recording	<ol style="list-style-type: none"> <li>Select <b>Video Record &gt; Settings</b>. The <b>Video Record</b> window is displayed.</li> <li>Set the video recording time length in seconds and the video storage position.</li> <li>Click <b>OK</b>.</li> </ol> <p>The video recording time length ranges from 1 through 1800 seconds.</p>
Record videos	<ol style="list-style-type: none"> <li>Start recording a video in either of the following ways: <ul style="list-style-type: none"> <li>Select <b>Video Record &gt; Start Record</b>.</li> <li>Click </li> </ul> </li> <li>(Optional) Stop recording a video in either of the following ways: <ul style="list-style-type: none"> <li>Select <b>Video Record &gt; Stop Record</b>.</li> <li>Click </li> </ul> </li> <li>After the preset recording time length is reached or the recording is stopped manually, click <b>OK</b>. The recorded video file is saved to the <i>VideoCaptures</i> folder in the preset path.</li> </ol>
Set the server power mode	<ol style="list-style-type: none"> <li>Select <b>Power</b>.</li> <li>Select a server power option from the displayed submenu.</li> </ol> <p>The server power options are as follows:</p> <ul style="list-style-type: none"> <li><b>Reset Server</b>: restarts the system without shutting down the power supply (warm reboot).</li> <li><b>Immediate Shutdown</b>: shuts down the server immediately by shutting down the power supply.</li> <li><b>Orderly Shutdown</b>: shuts down the server in order through program control.</li> <li><b>Power On Server</b>: starts the server.</li> <li><b>Power Cycle Server</b>: shuts down the server and restarts it (cold reboot).</li> </ul>
Check active users	<p>View the users using remote control in either of the following ways:</p> <ul style="list-style-type: none"> <li>Select <b>Active Users</b>.</li> <li>Click </li> </ul>

## 7.5 Configuring Virtual Media Parameters

### Abstract

Before mounting a **CD/DVD** or **HD** of the PC to the server through the **KVM**, you must configure virtual media parameters.

## Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed, see [Figure 7-10](#).

**Figure 7-10 Virtual Media Page**

The screenshot shows the 'Virtual Media' configuration page. The 'Media Setting' tab is active. The 'VMedia Entity Settings' section contains fields for CD/DVD Physical Device (value 1), HD Physical Device (value 1), Remote KVM CD/DVD Physical Device (value 1), and Remote KVM HD Physical Device (value 1). A toggle switch for 'Media Redirection Encryption' is shown as off. A 'Save' button is located below this section. The 'Media Service Settings' section contains two sets of settings for CD and HD media. For CD media, 'CD Media' is enabled (blue toggle), 'Secure Port' is 5124, and 'Non Secure Port' is 5120. For HD media, 'HD Media' is enabled (blue toggle), 'Secure Port' is 5127, and 'Non Secure Port' is 5123. Both sets have a 'Maximum Sessions' value of 1. The 'Media Connection Mode' section shows 'Auto Attach' selected (radio button). A 'Save' button is located at the bottom of the 'Media Service Settings' section.

3. Set the parameters in the **VMedia Entity Settings** area. For a description of the parameters, refer to [Table 7-8](#).

**Table 7-8 Parameter Descriptions for VMedia Instance Settings**

Parameter	Setting
-----------	---------

CD/DVD Physical Device	Select the number of CD/DVD devices on the PC. Keep the default value 1.
HD Physical Device	Select the number of HD devices on the PC. Keep the default value 1.
Remote KVM CD/DVD Physical Device	Select the number of CD/DVD devices to be mounted through the KVM. The number cannot exceed the number of CD/DVD physical device. Keep the default value 1.
Remote KVM HD Physical Device	Select the number of HD devices to be mounted through the KVM. The number cannot exceed the number of HD physical device. Keep the default value 1.
Media Redirection Encryption	Turn off the <b>Media Redirection Encryption</b> switch.

4. Click **Save**.
5. Set the parameters in the **Media Service Settings** area. For a description of the parameters, refer to [Table 7-9](#).

**Table 7-9 Parameter Descriptions for Media Service Settings**

Parameter	Setting
CD Media	<ul style="list-style-type: none"> <li>● To enable the CD media service, turn on the <b>CD Media</b> switch.</li> <li>● To disable the CD media service, turn off the <b>CD Media</b> switch.</li> </ul>
Secure Port	This parameter can be set when the <b>CD Media</b> switch is turned on. Enter the secure port number of the CD media service. Range: 1–65535, default: 5124.
Non Secure Port	This parameter can be set when the <b>CD Media</b> switch is turned on. Enter the non-secure port number of the CD media service. Range: 1–65535, default: 5120.
HD Media	<ul style="list-style-type: none"> <li>● To enable the HD media service, turn on the <b>HD Media</b> switch.</li> <li>● To disable the HD media service, turn off the <b>HD Media</b> switch.</li> </ul>
Secure Port	This parameter can be set when the <b>HD Media</b> switch is turned on. Enter the secure port number of the HD media service. Range: 1–65535, default: 5127.
Non Secure Port	This parameter can be set when the <b>HD Media</b> switch is turned on. Enter the non-secure port number of the HD media service. Range: 1–65535, default: 5123.

Media Connection Mode	Select the desired media connection mode. <ul style="list-style-type: none"> <li>● <b>Auto Attach:</b> reconnects automatically.</li> <li>● <b>Attach:</b> does not reconnect automatically.</li> </ul>
-----------------------	--

6. Click **Save**.

## 7.6 Mounting a Virtual Media Device

### Abstract

This procedure describes how to enable the virtual media function and remotely mount a virtual media device.

### Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed.
3. Click **Media Mounting**. The **Media Mounting** tab is displayed, as shown in [Figure 7-11](#).

[Figure 7-11 Virtual Media Page—Media Mounting Tab](#)

Virtual Media								
Media Setting		Media Mounting						
<input checked="" type="checkbox"/> Virtual Media Enable								
Start Media Type	Server Address	File Path	Shared File System	Username	Password	Status	Operation	
CD/DVD	10.239.20.11	/home/mount_test/isocfg-tool-v1.iso	CIFS	test	***	Disabled	Start Mount	
HD	10.239.20.11	/home/mount_test/isocfg-tool-v1.img	NFS			Disabled	Start Mount	

4. Set the parameters. For a description of the parameters, refer to [Table 7-10](#).

[Table 7-10 Parameter Descriptions for Mounting a Virtual Media Device](#)

Parameter	Description
Virtual Media Enable	Turn on the toggle switch. If the <b>Virtual Media Enable</b> switch is turned off, the mounted virtual media devices are cleared.
Start Media Type	The number of virtual media devices in the <b>Start Media Type</b> column must be the same as that of the devices set in <b>Remote KVM CD/DVD Physical Device</b> and <b>Remote KVM HD Physical Device</b> on the <b>Media Setting</b> tab. For example, if <b>Remote KVM CD/DVD Physical Device</b> is set to 1, there is only one <b>CD/DVD</b> entry displayed in the <b>Start Media Type</b> column.

Server Address	Enter the IP address of the server that provides the remote image mounting service. Domain names are not supported.
File Path	Enter the storage path of the image file on the remote server. A maximum of 256 characters can be entered. The name of each mounted image file must be unique.
<b>Parameter</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• If <b>Start Media Type</b> is <b>CD/DVD</b>, the suffix of the image filename must be <i>iso</i>.</li> <li>• If <b>Start Media Type</b> is <b>HD</b>, the suffix of the image filename must be <i>img</i> or <i>ima</i>.</li> </ul>
Shared File System	Select a file system protocol for file sharing. Options: <b>NFS</b> , <b>CIFS</b> , and <b>HTTPS</b> . <ul style="list-style-type: none"> <li>• If <b>Start Media Type</b> is <b>CD/DVD</b>, <b>NFS</b>, <b>CIFS</b>, and <b>HTTPS</b> are supported.</li> <li>• If <b>Start Media Type</b> is <b>HD</b>, <b>NFS</b> and <b>CIFS</b> are supported.</li> </ul>
Username	Enter the username for logging in to the remote server. This parameter does not need to be set if <b>Shared File System</b> is set to <b>NFS</b> .
Password	Enter the password for logging in to the remote server. This parameter does not need to be set if <b>Shared File System</b> is set to <b>NFS</b> .

5. In the **Operation** column, click **Start Mount** for the desired virtual media device.



#### Note

After the virtual media device is successfully mounted, its status in the **Status** column is changed to **Enabled**.

#### Related Tasks

To disable a mounted virtual media device, click **End Mount** in the **Operation** column for it.

## 7.7 Configuring VNC Parameters

#### Abstract

A server can be remotely controlled through the **KVM** and **VNC**. Before remotely controlling the server in VNC mode, you must configure the VNC parameters.



#### Note

For KVM-related parameter configuration, refer to [7.3 Configuring KVM Service Parameters](#). For KVMbased remote server control operations, refer to [7.4 Starting the KVM](#).

## Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **VNC**. The **VNC** page is displayed, see [Figure 7-12](#).

**Figure 7-12 VNC Page**

The screenshot shows the 'VNC' configuration page. It includes the following fields:

- Secure Port: 5901
- Non Secure Port: 5900
- Timeout Period: 25 (with a 'Min' label)
- Maximum Sessions: 2
- Modify Password: Off (toggle switch)
- VNC Password: (password field)
- Confirm VNC Password: (password field)

A 'Save' button is located at the bottom of the form.

3. Set the parameters. For a description of the parameters, refer to [Table 7-11](#).

**Table 7-11 VNC Parameter Descriptions**

Parameter	Setting
Secure Port	Enter the secure port number of the VNC service. Range: 1–65535, default: 5901.
Non Secure port	Enter the non-secure port number of the VNC service. Range: 1–65535, default: 5900.
Timeout Period	<p>The VNC service exits if no operation is performed within the specified timeout period.</p> <p>Enter the timeout period. Range: 5–30, unit: minutes.</p>

Modify Password	Whether to modify the VNC password. <ul style="list-style-type: none"> <li>● To modify the VNC password, turn on the <b>Modify Password</b> switch.</li> <li>● To not modify the VNC password, turn off the <b>Modify Password</b> switch.</li> </ul>
VNC Password	This parameter can be set when the <b>Modify Password</b> switch is turned on.  Enter the new VNC password. A VNC password consists of a maximum of eight characters, including digits, letters, and special characters except spaces. If this parameter is left blank, the default password is restored.
Confirm VNC Password	This parameter can be set when the <b>Modify Password</b> switch is turned on.
Parameter	Setting
	Confirm the new VNC password, which must be the same as <b>VNC Password</b> .

4. Click **Save**.

## 7.8 Configuring SNMP Parameters

### Abstract

This procedure describes how to configure **SNMP** parameters for communication between the **BMC** and a third-party NMS.



### Note

SNMP parameters are provided by the third-party NMS, so the values of SNMP parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

### Steps

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **SNMP**. The **SNMP** page is displayed, see [Figure 7-13](#).

**Figure 7-13 SNMP Page**

The screenshot shows the SNMP configuration page. At the top, the 'SNMP' section is active, indicated by a blue toggle switch. The 'Port' is set to 161. The 'Complex Password' switch is also turned on. Below this, the 'Edit Read-only Community' switch is off, and the 'Read-only Community' field is empty with a placeholder 'Please enter the community name.' The 'Confirm Read-only Community' field is also empty with the same placeholder. The 'Edit Read-write Community' switch is off, and the 'Read-write Community' and 'Confirm Read-write Community' fields are both empty with the same placeholder. At the bottom, the 'Engine ID' is listed as 0x80000f3e03e224a282e035, and a blue 'Save' button is located at the bottom center.

3. Set the parameters. For a description of the parameters, refer to [Table 7-12](#).

**Table 7-12 SNMP Parameter Descriptions**

Parameter	Setting
SNMP	Turn on the <b>SNMP</b> switch.
Port	Enter the non-secure port number of the SNMP service. Range: 1–65535, default: 161.
Complex Password	Whether to enable the complex password function. <ul style="list-style-type: none"> <li>• To enable the complex password function, turn on the <b>Complex Password</b> switch.</li> <li>• To disable the complex password function, turn off the <b>Complex Password</b> switch.</li> </ul>

Edit Read-only Community	<p>Whether to edit the read-only community name.</p> <ul style="list-style-type: none"> <li>● To edit the read-only community name, turn on the <b>Edit Read-only Community</b> switch.</li> <li>● To not edit the read-only community name, turn off the <b>Edit Read-only Community</b> switch.</li> </ul>
<b>Parameter</b>	<b>Setting</b>
Read-only Community	<p>This parameter can be set when the <b>Edit Read-only Community</b> switch is turned on.</p> <p>Enter the read-only community name (default: roAdmin9!).</p>
Confirm Read-only Community	<p>This parameter can be set when the <b>Edit Read-only Community</b> switch is turned on.</p> <p>Confirm the read-only community name, which must be the same as that specified by <b>Read-only Community</b>.</p>
Edit Read-write Community	<p>Whether to edit the read-write community name.</p> <ul style="list-style-type: none"> <li>● To edit the read-write community name, turn on the <b>Edit Read-write Community</b> switch.</li> <li>● To not edit the read-only community name, turn off the <b>Edit Readwrite Community</b> switch.</li> </ul>
Read-write Community	<p>This parameter can be set when the <b>Edit Read-write Community</b> switch is turned on.</p> <p>Enter the read-write community name (default: rwAdmin9!).</p>
Confirm Read-write Community	<p>This parameter can be set when the <b>Edit Read-write Community</b> switch is turned on.</p> <p>Confirm the read-write community name, which must be the same as that specified by <b>Read-write Community</b>.</p>

4. Click **Save**.

# Chapter 8

# BMC Management

---

## Table of Contents

Network Parameter Configuration.....	117
Setting the Time of the BMC.....	127
Resetting the BMC on the Web Portal of the BMC.....	130
Upgrading Firmware.....	131
Updating BMC Configurations.....	133
Restoring Factory Defaults.....	135

## 8.1 Network Parameter Configuration

### 8.1.1 Configuring the Host Name

#### Abstract

This procedure describes how to configure the host name to identify the server.

#### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 8-1](#).

**Figure 8-1 Network Settings Page**

**Network Settings**

**Host Name**

Host Name Settings  Automatic  Manual

Host Name

**Save**

**Network Port**

**Save**

**Network Protocols**

**Save**

**DNS**

**Save**

**NCSI VLAN Configuration**

**Save**

3. Set the parameters in the **Host Name** area. For a description of the parameters, refer to [Table 8-1](#).

**Table 8-1 Host Name Parameter Descriptions**

Parameter	Setting
Host Name Settings	Select the desired host name setting mode. <ul style="list-style-type: none"> <li><b>Automatic:</b> A host name is automatically set by the system.</li> <li><b>Manual:</b> A host name needs to be manually entered in the <b>Host Name</b> text box.</li> </ul>
Host Name	This parameter is required if <b>Host Name Settings</b> is set to <b>Manual</b> . Enter the host name. The host name contains a maximum of 64 characters, including digits, letters, and hyphens. The host name cannot begin or end with hyphens.

4. Click **Save**.

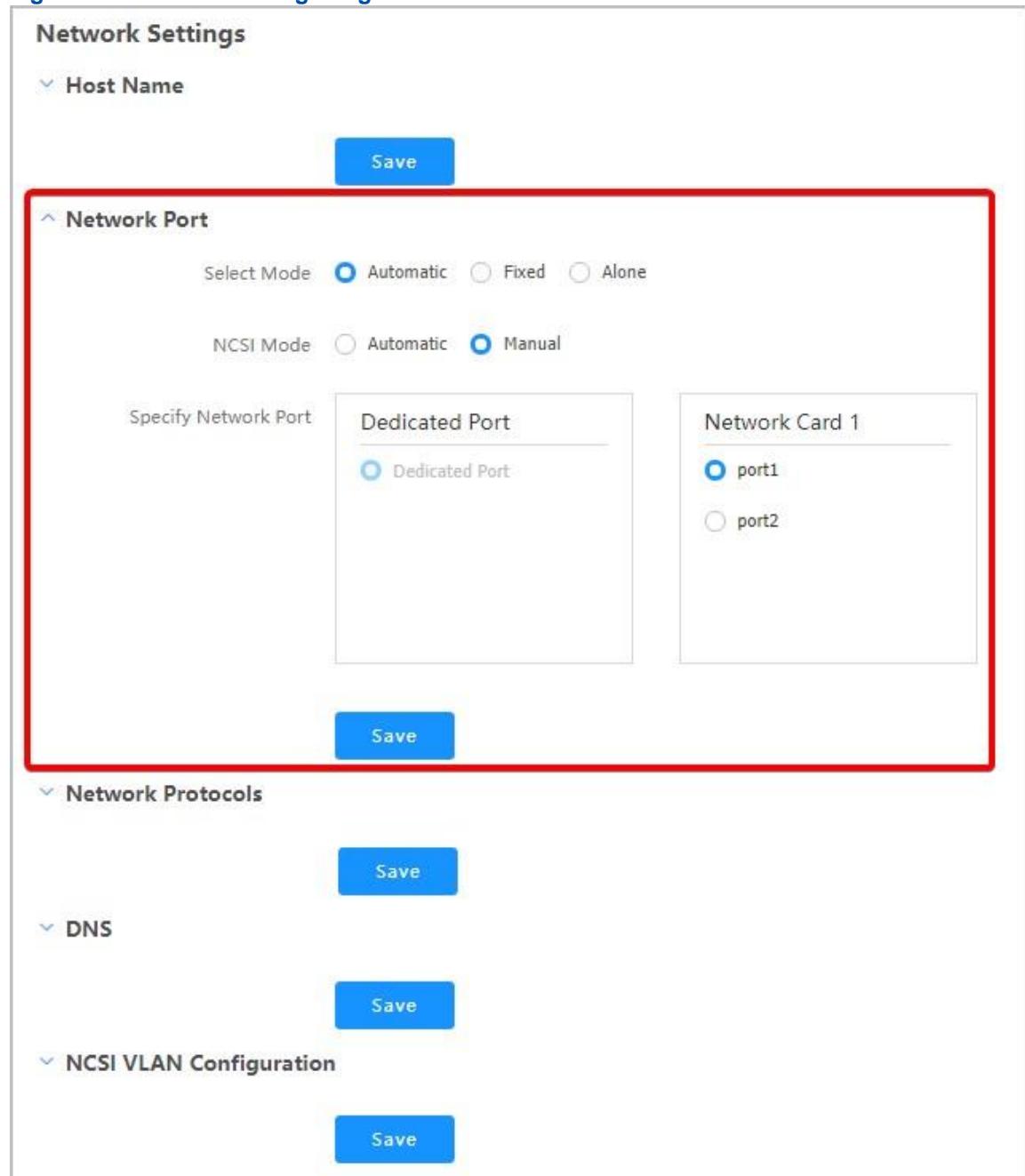
## 8.1.2 Configuring the Network Port Mode

### Abstract

This procedure describes how to configure the network port mode to specify the management network port and shared network port.

### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 8-2](#).

**Figure 8-2 Network Settings Page**

3. Set the parameters in the **Network Port** area. For a description of the parameters, refer to [Table 8-2](#).

**Table 8-2 Parameter Descriptions for Configuring a Network Port Mode**

Parameter	Setting
Select Mode	<p>Select the desired network port mode.</p> <ul style="list-style-type: none"> <li>● <b>Automatic:</b> The dedicated network port (namely the <a href="#">iSAC</a> network port) is preferentially used as the management network port. If the dedicated network port does not operate properly, an onboard <a href="#">NCSI</a></li> </ul>

Parameter	Setting
	<p>that is operating properly is automatically used as the management network port to replace the dedicated network port.</p> <ul style="list-style-type: none"> <li>● <b>Fixed:</b> A network port (the dedicated network port or an onboard NCSI) specified in the <b>Dedicated Port</b> box in the <b>Specify Network Port</b> area is used as the management network port.</li> <li>● <b>Alone:</b> The management network port and shared network port are configured separately. The dedicated network port is used as the management network port, and an onboard NCSI is used as the shared network port.</li> </ul> <p>If <b>Select Mode</b> is set to <b>Automatic</b>, the following parameters do not need to be configured.</p>
<b>NCSI</b> Mode	<p>This parameter is required when <b>Alone</b> is selected.</p> <p>Select the desired shared network port mode.</p> <ul style="list-style-type: none"> <li>● <b>Automatic:</b> If the shared network port does not operate properly, an onboard <b>NCSI</b> that is operating properly is automatically used as the shared network port to replace the faulty shared network port.</li> <li>● <b>Manual:</b> An onboard NCSI specified in the <b>Network Card</b> box in the <b>Specify Network Port</b> area is used as the shared network port. If <b>NCSI Mode</b> is set to <b>Automatic</b>, no shared network port needs to be specified.</li> </ul>
Specify Network Port	<ul style="list-style-type: none"> <li>● If <b>Select Mode</b> is set to <b>Automatic</b>, no network port needs to be specified.</li> <li>● If <b>Select Mode</b> is set to <b>Fixed</b>, a network port (the dedicated network port or an onboard NCSI) needs to be specified as the management network port.</li> <li>● If <b>Select Mode</b> is set to <b>Alone</b> and <b>NCSI Mode</b> is set to <b>Manual</b>, the dedicated network port is used as the management network port, and an onboard NCSI needs to be specified in the <b>Network Card</b> box as the shared network port.</li> </ul>

4. Click **Save**.

### 8.1.3 Configuring IP Addresses of Network Ports

#### Abstract

To replan the **IP** address 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.

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 8-3](#).

**Figure 8-3 Network Settings Page**

The screenshot shows the BMC Management interface. The 'Network Settings' page is open. The 'Network Protocols' section is highlighted with a red box. This section contains settings for 'IPv4' and 'IPv6'. Under 'IPv4', the 'Acquisition method' is set to 'Manually set IP address', with fields for 'Address' (10.255.255.0), 'Mask' (255.255.255.0), and 'Default Gateway' (10.255.255.1). The 'MAC Address' is listed as E2:24:A2:82:E0:35. Under 'IPv6', the 'Acquisition method' is set to 'Automatically obtain IP address', with fields for 'Address' (empty), 'Prefix Length' (0), and 'Default Gateway' (empty). The 'Link Local Address' is listed as fe80::e024:a2ff:fe82:e035. Other sections visible include 'Host Name', 'Network Port', 'DNS', and 'NCSI VLAN Configuration', each with a 'Save' button.

3. Set the parameters in the **Network Protocols** area. For a description of the parameters, refer to [Table 8-3](#).

**Table 8-3 Network Protocol Parameter Descriptions**

Parameter	Setting
Select Network Port	<p>This parameter can be set only if <b>Select Mode</b> is set to <b>Alone</b> in the <b>Network Port</b> area.</p> <p>Select the network port for which you want to configure an IP address.</p> <ul style="list-style-type: none"> <li>● <b>Dedicated Port</b>: configures the IP address of the iSAC management network port.</li> <li>● <b>Shared Port</b>: configures the IP address of the shared network port.</li> </ul>

Network Protocols	Select the network protocol(s) for the network port. <ul style="list-style-type: none"> <li>• The IPv4 settings need to be configured if you select <b>IPv4</b> only.</li> <li>• The IPv6 settings need to be configured if you select <b>IPv6</b> only.</li> <li>• Both IPv4 settings and IPv6 settings need to be configured if you select <b>IPv4</b> and <b>IPv6</b>.</li> </ul>
<b>Parameter</b>	<b>Setting</b>
Acquisition method	Select the method of obtaining the IP address. The parameters below do not need to be configured if <b>Acquisition method</b> is set to <b>Automatically obtain IP address</b> .
Address	Enter the address of the BMC as planned.
Mask	Enter the mask.
Default Gateway	Enter the IP address of the default gateway.

4. Click **Save**.

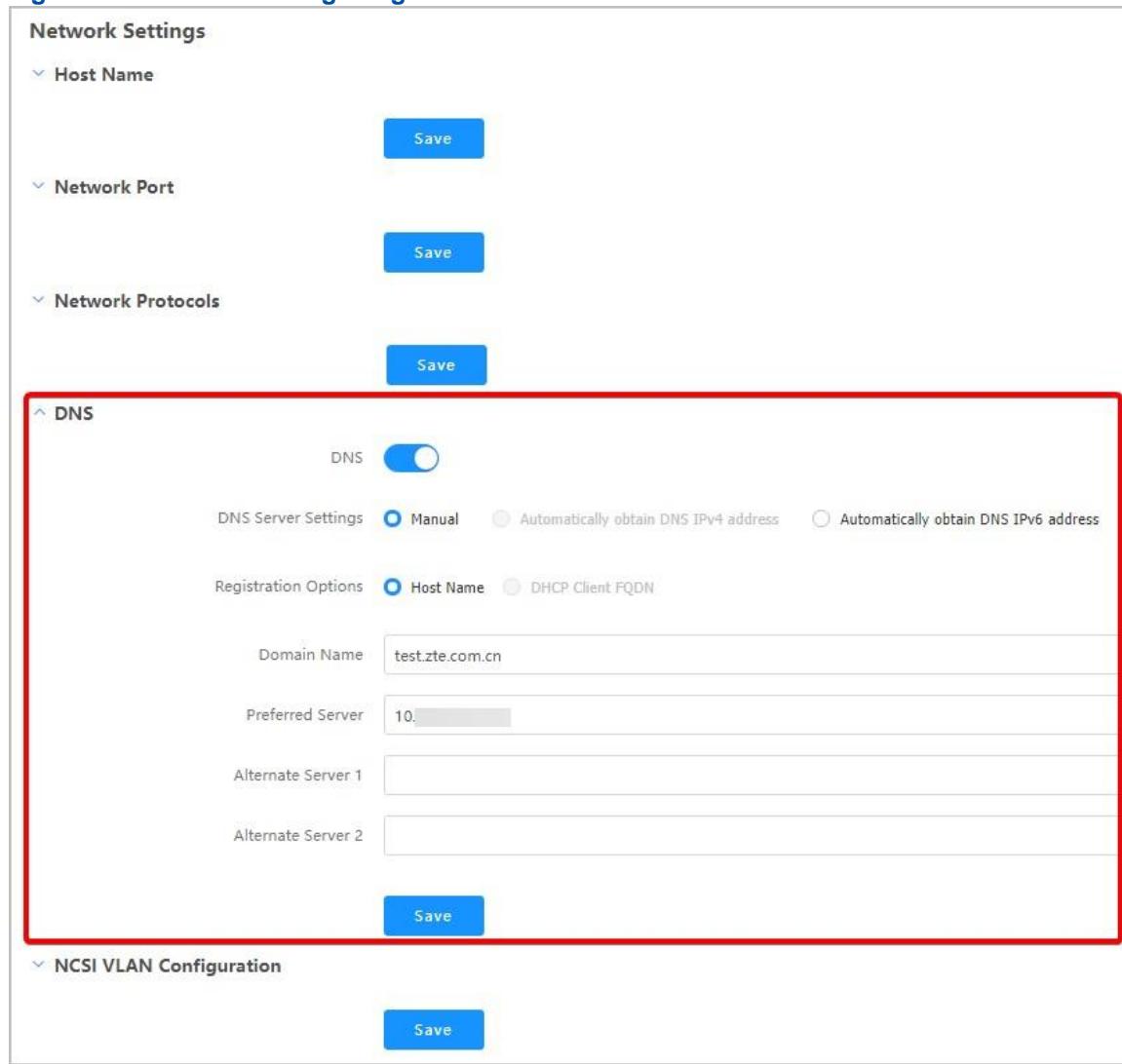
## 8.1.4 Configuring the DNS

### Abstract

To access the Web portal of the **BMC** through a **FQDN**, you must configure the **DNS** information about the server.

### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 8-4](#).

**Figure 8-4 Network Settings Page**


The screenshot shows the 'Network Settings' page with a red box highlighting the 'DNS' configuration area. The 'DNS' section contains the following fields:

- DNS:** A toggle switch that is turned on (blue).
- DNS Server Settings:** A radio button group with three options:  Manual,  Automatically obtain DNS IPv4 address, and  Automatically obtain DNS IPv6 address.
- Registration Options:** A radio button group with two options:  Host Name and  DHCP Client FQDN.
- Domain Name:** A text input field containing 'test.zte.com.cn'.
- Preferred Server:** A text input field containing '10. [redacted]'
- Alternate Server 1:** An empty text input field.
- Alternate Server 2:** An empty text input field.

Below the DNS section, there are other collapsed sections: 'Host Name', 'Network Port', 'Network Protocols', and 'NCSI VLAN Configuration', each with a 'Save' button.

3. Set the parameters in the **DNS** area. For a description of the parameters, refer to [Table 8-4](#).

**Table 8-4 DNS Parameter Descriptions**

Parameter	Setting
DNS	<p>Select whether to enable the DNS service.</p> <ul style="list-style-type: none"> <li>● To enable the DNS service, turn on the <b>DNS</b> switch. In this case, the following parameters need to be configured.</li> <li>● To disable the DNS service, turn off the <b>DNS</b> switch. In this case, the following parameters do not need to be configured.</li> </ul>
DNS Server Settings	<p>Select the desired DNS setting method.</p> <ul style="list-style-type: none"> <li>● <b>Manual:</b> If <b>Acquisition method</b> is set to <b>Manually set IP address</b> in the <b>Network Protocols</b> area, this parameter must be set to <b>Manual</b>. When <b>Manual</b> is selected, you need to configure the following parameters.</li> </ul>

Parameter	Setting
	<ul style="list-style-type: none"> <li>● <b>Automatically obtain DNS IPv4 address:</b> If <b>Acquisition method</b> is set to <b>Automatically obtain IP address</b> and <b>Network Protocols</b> is set to <b>IPv4</b> in the <b>Network Protocols</b> area, this parameter must be set to <b>Automatically obtain DNS IPv4 address</b>. When <b>Automatically obtain DNS IPv4 address</b> is selected, you do not need to configure the following parameters.</li> <li>● <b>Automatically obtain DNS IPv6 address:</b> If <b>Acquisition method</b> is set to <b>Automatically obtain IP address</b> and <b>Network Protocols</b> is set to <b>IPv6</b> in the <b>Network Protocols</b> area, this parameter must be set to <b>Automatically obtain DNS IPv6 address</b>. When <b>Automatically obtain DNS IPv6 address</b> is selected, you do not need to configure the following parameters.</li> </ul>
Registration Options	<p>Select the option used to register with the DNS.</p> <ul style="list-style-type: none"> <li>● <b>Host Name:</b> uses <b>DHCP</b> option 12 to register with the DNS.</li> <li>● <b>DHCP Client FQDN:</b> uses <b>DHCP</b> option 81 to register with the DNS.</li> </ul> <p>If the <b>DHCP</b> server does not support <b>DHCP</b> option 81, select <b>Host Name</b>. If <b>DNS Server Settings</b> is set to <b>Manual</b>, only <b>Host Name</b> can be selected. If <b>DNS Server Settings</b> is set to <b>Automatically obtain DNS IPv4 address</b> or <b>Automatically obtain DNS IPv6 address</b>, <b>Host Name</b> or <b>DHCP Client FQDN</b> can be selected.</p>
Domain Name	<p>Enter a domain name. The domain name consists of a maximum of 67 characters, including digits, letters, hyphens, and dots. It cannot start with a hyphen or dot or end with a hyphen. No more than 63 characters are allowed between any two dots.</p>
Preferred Server	<p>Enter the <b>IP</b> address of the preferred DNS server. This parameter is required if <b>DNS Server Settings</b> is set to <b>Manual</b>.</p>
Alternate Server 1	<p>Enter the IP address of alternate DNS server 1. This parameter is optional if <b>DNS Server Settings</b> is set to <b>Manual</b>.</p>
Alternate Server 2	<p>Enter the IP address of alternate DNS server 2. This parameter is optional if <b>DNS Server Settings</b> is set to <b>Manual</b>.</p>

4. Click **Save**.

## 8.1.5 Configuring a VLAN

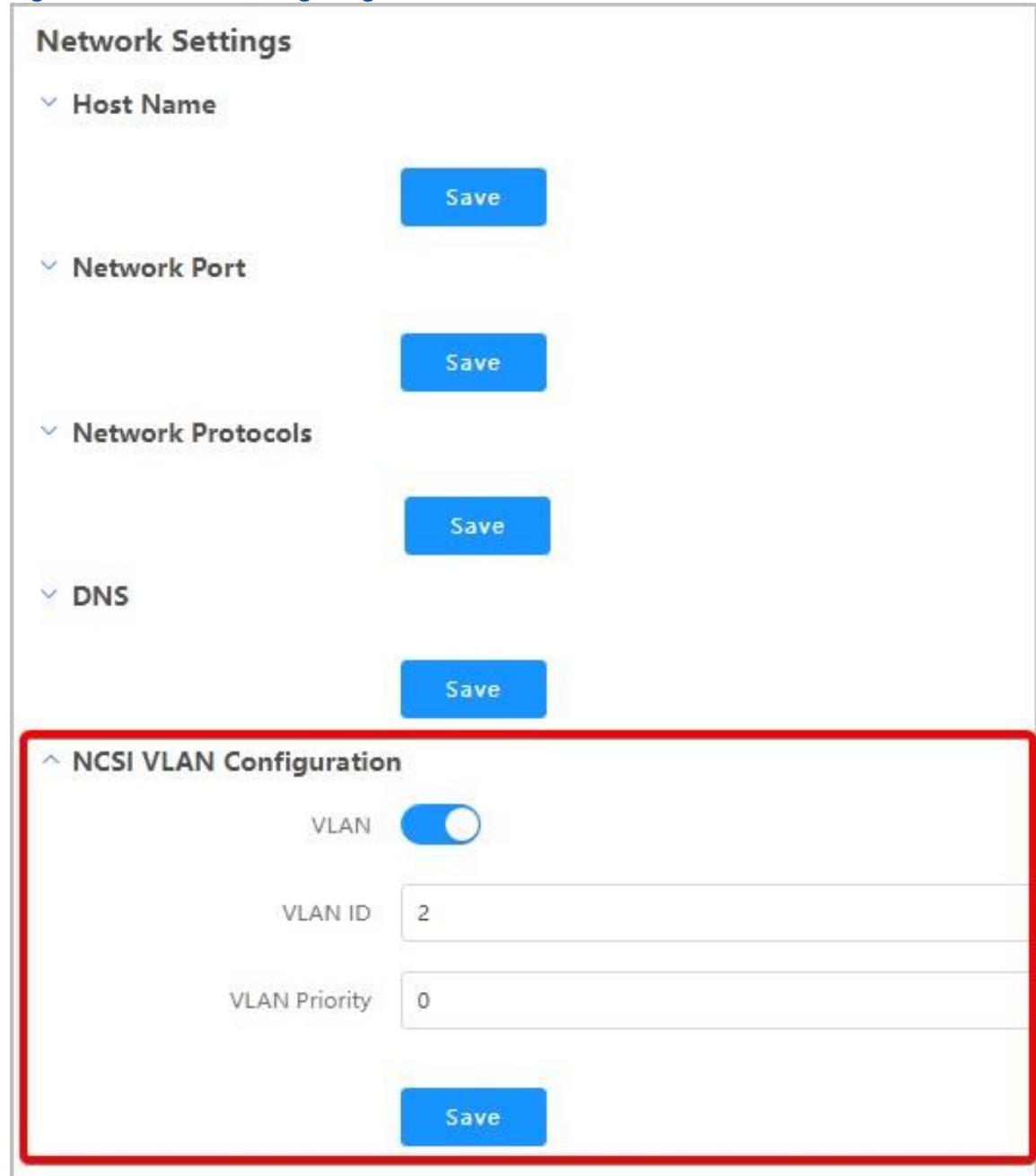
### Abstract

This procedure describes how to configure a **VLAN** so that an onboard **NCSI** can be added to the **VLAN**.

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see [Figure 8-5](#).

[Figure 8-5 Network Settings Page](#)



The screenshot shows the 'Network Settings' page with the following structure:

- Host Name**: Contains a 'Save' button.
- Network Port**: Contains a 'Save' button.
- Network Protocols**: Contains a 'Save' button.
- DNS**: Contains a 'Save' button.
- NCSI VLAN Configuration**: This section is highlighted with a red box and contains the following fields:
  - VLAN**: A toggle switch that is turned on (blue).
  - VLAN ID**: A text input field containing the value '2'.
  - VLAN Priority**: A text input field containing the value '0'.

3. Set the parameters in the **NCSI VLAN Configuration** area. For a description of the parameters, refer to [Table 8-5](#).

**Table 8-5 NCSI VLAN Parameter Descriptions**

Parameter	Setting
VLAN	<p>Select whether to enable the VLAN function.</p> <ul style="list-style-type: none"> <li>● To enable the VLAN function, turn on the <b>VLAN</b> switch. In this case, the following parameters need to be configured.</li> <li>● To disable the VLAN function, turn off the <b>VLAN</b> switch. In this case, the following parameters do not need to be configured.</li> </ul> <p>The VLAN function can be enabled if any of the following conditions is met:</p> <ul style="list-style-type: none"> <li>● The <b>Select Mode</b> parameter is set to <b>Automatic</b> in the <b>Network Port</b> area, and an onboard NCSI is connected.</li> <li>● The <b>Select Mode</b> parameter is set to <b>Fixed</b> in the <b>Network Port</b> area, and an onboard NCSI is specified as the management network port.</li> </ul>
VLAN ID	Enter the VLAN ID. Range: 2–4094.
VLAN Priority	Enter the VLAN priority. Range: 0–7. A greater value indicates a higher priority.

4. Click **Save**.

## 8.2 Setting the Time of the BMC

### Abstract

The time of the **BMC** must be correct.

This procedure describes how to set the time of the BMC in either of the following ways:

- Setting time manually
- Synchronizing time with an **NTP** server

To make the manually set time permanently valid, you need to disable NTP-based time synchronization.

### Steps

- Setting Time Manually

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Time Zone & NTP**. The **Time Zone & NTP** page is displayed, as shown in [Figure 8-6](#).

**Figure 8-6 Time Zone & NTP Page**

**Time Zone & NTP**

**Time Zone**

Time 2024-01-11 11:07:09

Current Timezone UTC+08:00

Region

**NTP**

NTP

Polling Interval

Main Server

Secondary Server

Tertiary Server

**Save**

3. Click and then set the time.

**Note**

The time is automatically saved on the page after being set.

- Synchronizing Time with an NTP Server
  1. Select **BMC Settings**. The **BMC Settings** page is displayed.
  2. From the navigation tree in the left pane, select **Time Zone & NTP**. The **Time Zone & NTP** page is displayed, as shown in [Figure 8-7](#).

**Figure 8-7 Time Zone & NTP Page**

3. Set the parameters in the **NTP** area. For a description of the parameters, refer to [Table 8-6](#).

**Table 8-6 NTP Parameter Descriptions**

Parameter	Description
NTP	Enable NTP.
Polling Interval	Enter the time synchronization period. Range: 60–65535, unit: seconds.
Main Server	Enter the IP address or <a href="#">FQDN</a> of the primary NTP server. The length cannot exceed 127 characters. This parameter is required.
Secondary Server	Enter the IP address or FQDN of the secondary NTP server. The length cannot exceed 127 characters. This parameter is optional.
Tertiary Server	Enter the IP address or FQDN of the tertiary NTP server. The length cannot exceed 127 characters. This parameter is optional.

**Note**

The BMC first synchronizes time with the primary NTP server. If the synchronization fails, it synchronizes time with the secondary NTP server and tertiary NTP server in turn.

4. Click **Save**.

**Verification**

If NTP-based time synchronization is used, perform the following operations:

1. On the **Time Zone & NTP** page, view the date and time, as shown in [Figure 8-8](#).

**Figure 8-8 Time Zone & NTP Page**

**Time Zone & NTP**

**Time Zone**

Time 2024-01-11 11:09:18

Current Timezone UTC+08:00

Region Asia/Shanghai

**NTP**

NTP

Polling Interval 60 s

Main Server 10

Secondary Server time.nist.gov

Tertiary Server

**Save**

2. On the NTP server, check whether the time is the same as the time of the BMC.

## 8.3 Resetting the BMC on the Web Portal of the BMC

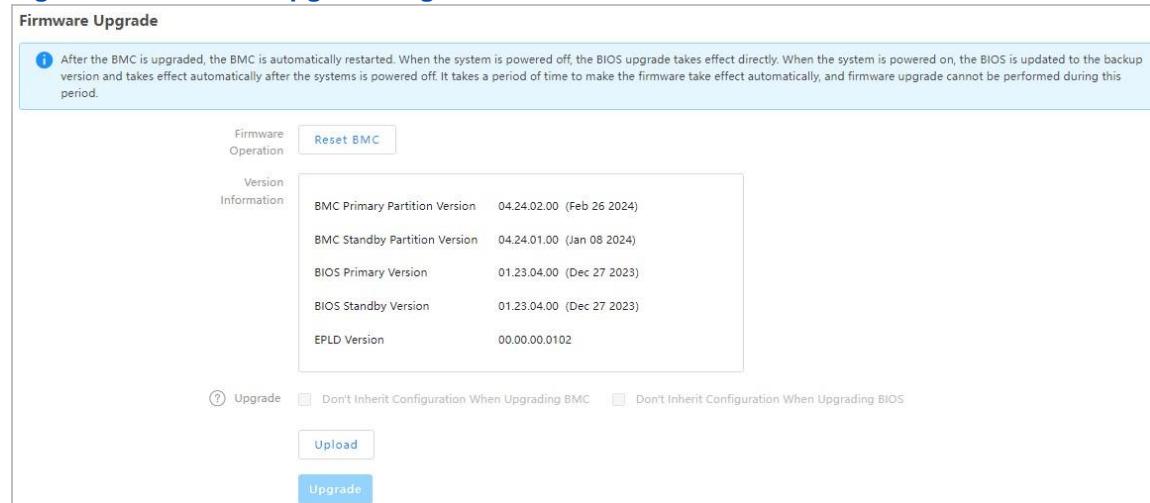
### Abstract

After some configurations (for example, **MAC** address and chassis information programming), you must reset the **BMC** to apply the changes.

### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Firmware Upgrade**. The **Firmware Upgrade** page is displayed, see [Figure 8-9](#).

**Figure 8-9 Firmware Upgrade Page**



3. Click **Reset BMC**, and confirm the reset in the displayed message box.



### Note

Relogin is allowed only after the BMC is reset.

## 8.4 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

The firmware to be upgraded is already obtained.

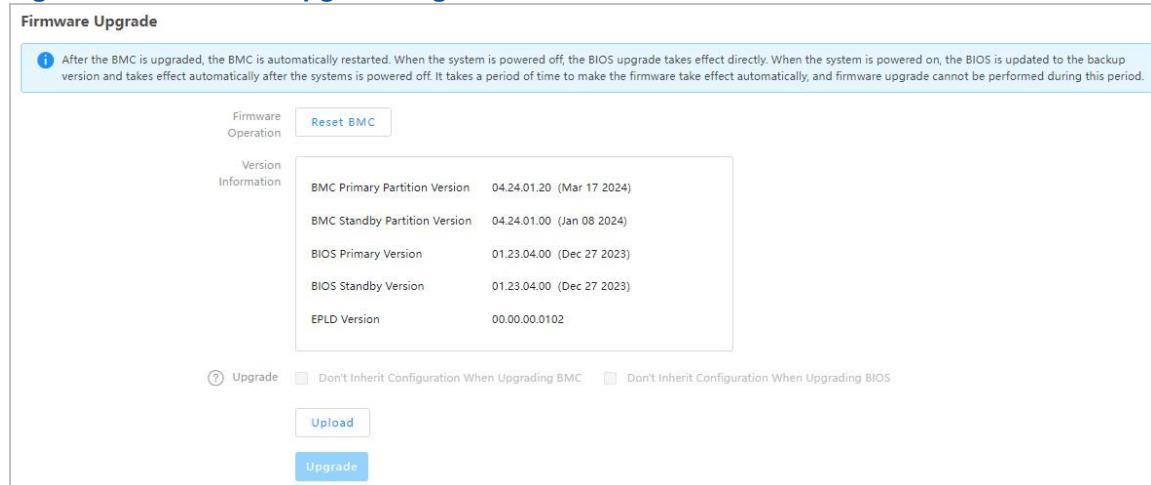


### Note

Firmware files can be obtained on the **Software Download** page on the Web portal of the servers and storage products ([https://enterprise.NETA\\$ .com.cn](https://enterprise.NETA$ .com.cn)).

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Firmware Upgrade**. The **Firmware Upgrade** page is displayed, see [Figure 8-10](#).

**Figure 8-10 Firmware Upgrade Page**

3. Click **Upload** and select the firmware file in the displayed dialog box.

**Note**

Only one firmware file can be selected at a time. During the firmware upgrade process, the firmware file automatically matches the firmware type.

After the BMC or BIOS firmware is successfully uploaded, the **Don't Inherit Configuration When Upgrading BMC** or **Don't Inherit Configuration When Upgrading BIOS** check box becomes activated.

4. (Optional) Perform either of the following operations:
  - To restore the factory default settings of the BMC, select **Don't Inherit Configuration When Upgrading BMC**.
  - To restore the factory default settings of the BIOS, select **Don't Inherit Configuration When Upgrading BIOS**.
5. Click **Upgrade**.

**Notice**

During the firmware upgrade process, you cannot switch to another page. Otherwise, the upgrade process is interrupted.

## 8.5 Updating BMC Configurations

### Abstract

This procedure describes how to update **BMC** configurations online.

Before replacing the mainboard of a server, you can back up the BMC configurations by using the BMC configuration update function.

## Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Configuration Update**. The **Configuration Update** page is displayed, see [Figure 8-11](#).

**Figure 8-11 Configuration Update Page**

Configuration Update

**Configure Import**

Supports importing BMC and BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the host.

Select Type  BMC  BIOS

Select File  Upload

Import

**Configure Export**

Select Type  BMC  BIOS

Export

**Restore Factory Settings**

After restoring BMC factory settings, you need to log in to BMC for the first time. Please use this function with caution.

Restore Factory Settings

3. Perform the following operations as required.

If...	Then...
There is an existing BMC configuration file	<ol style="list-style-type: none"> <li>Click <b>Upload</b>, and select the BMC configuration file in the displayed dialog box.</li> <li>Click <b>Import</b>, and confirm the import in the displayed message box.</li> </ol>
There is no BMC configuration file	<ol style="list-style-type: none"> <li>Click <b>Export</b> to export the current BMC configurations to your local PC.</li> <li>Edit the exported BMC configuration file.</li> <li>Click <b>Upload</b>, and select the BMC configuration file in the displayed dialog box.</li> <li>Click <b>Import</b>, and confirm the import in the displayed message box.</li> </ol>



After the BMC configurations are imported, the BMC is automatically restarted to apply the configurations. Do not perform any other operations until the BMC is restarted.

## Related Tasks

To back up BMC configurations, perform the following operations:

1. Click **Export** to export the current BMC configurations to your local PC.
2. After replacing the mainboard, click **Upload**, and select the exported BMC configuration file in the displayed dialog box.
3. Click **Import**, and confirm the import in the displayed message box.

## 8.6 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 the factory defaults are restored, the [BMC](#) will be restarted automatically.

### Steps

1. Select **BMC Settings**. The **BMC Settings** page is displayed.
2. From the navigation tree in the left pane, select **Configuration Update**. The **Configuration Update** page is displayed, see [Figure 8-12](#).

**Figure 8-12 Configuration Update Page**

**Configuration Update**

**Configure Import**

Supports importing BMC and BIOS configurations. After importing, BMC automatically restarts and the configuration takes effect. BIOS takes effect and requires manual resetting of the host.

Select Type  BMC  BIOS

Select File  Upload

Import

**Configure Export**

Select Type  BMC  BIOS

Export

**Restore Factory Settings**

After restoring BMC factory settings, you need to log in to BMC for the first time. Please use this function with caution.

Restore Factory Settings

3. Click **Restore Factory Defaults**.

# Chapter 9

# User and Security

---

## Table of Contents

Adding a Local User.....	136
Configuring Authentication Parameters for Domain Users.....	138
Querying Online Users.....	142
Configuring Permissions for a Customized Role.....	143
Configuring Security Enhancement Parameters.....	144
Configuring Firewall Parameters.....	145
Configuring Two-Factor Authentication.....	147

## 9.1 Adding a Local User

### Abstract

Local users refer to users of the **BMC** itself. This procedure describes how to add a local user to configure and manage the BMC.

### Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Local Users**. The **Local Users** page is displayed, see [Figure 9-1](#).

**Figure 9-1 Local Users Page**

Local Users						C
<a href="#">+ Add User</a>						<input type="text"/> Search(Fuzzy search only...)
User ID	User Name	Role	Login Interfaces			Operation
1	anonymous	Administrator	SNMP	SSH	Redfish	<a href="#">Edit</a> <a href="#">Enable</a> <a href="#">Delete</a>
2	Administrator	Administrator	SNMP	SSH	Redfish	<a href="#">Edit</a> <a href="#">Disable</a> <a href="#">Delete</a>

Total 2 [K](#) [<](#) [1](#) [>](#) [X](#) 10 / Page [To](#) [1](#) Page

3. Click **Add User**. The **Add User** page is displayed, see [Figure 9-2](#).

**Figure 9-2 Add User Page**

Local Users > **Add User**

New User ID: 10

New UserName: test

New Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Role: Administrator

Login Interfaces:  SNMP ?  Redfish

Current User Password: \*\*\*\*\*

**Submit** **Cancel**

4. Set the parameters. For a description of the parameters, refer to [Table 9-1](#).

**Table 9-1 Parameter Descriptions for Adding a Local User**

Parameter	Setting
New User ID	Select the ID of the new user. A maximum of 16 local users are supported, so the user ID ranges from 1 to 16. User 1 is a reserved user, and user 2 is the default administrator.
New UserName	Enter the name of the new user. The name contains a maximum of 16 characters, including digits, letters (case sensitive), and special characters. The new username cannot be the same as another existing username. The following cannot be used as a username: sshd, ntp, stunnel4, sysadmin, daemon, Administrator, and anonymous.
New Password	Enter the password of the new user. The password contains 5–20 characters, including digits, letters (case sensitive), and special characters. Historical passwords cannot be used anymore.
Confirm Password	Enter the same password again for confirmation.
Role	Select the role of the new user.

Login Interfaces	Select one or more login interfaces available to the new user. <ul style="list-style-type: none"> <li>For <b>SNMP</b> interface-based login, select <b>SNMP</b>.</li> <li>For Redfish interface-based login, select <b>Redfish</b>.</li> </ul> <b>SSH</b> -based login is supported for all users by default.
<b>Parameter</b>	<b>Setting</b>
Current User Password	Enter the password of the currently logged-in user.

5. Click **Submit**.
6. (Optional) If **Login Interfaces** is set to **SNMP**, click **Edit** in the **Operation** column for the new user. The **Edit** page is displayed. Set **SNMPv3 Authentication Algorithm** and **SNMPv3 Encryption Algorithm**.

### Related Tasks

Perform either of the following operations as needed.

To...	Do...
Disable a local user	<ol style="list-style-type: none"> <li>1. In the <b>Operation</b> column, click <b>Disable</b> for the user. The <b>Confirm</b> dialog box is displayed.</li> <li>2. Enter the password of the currently logged-in user.</li> <li>3. Click <b>Submit</b>.</li> </ol>
Delete a local user	<ol style="list-style-type: none"> <li>1. In the <b>Operation</b> column, click <b>Delete</b> for the user. The <b>Confirm</b> dialog box is displayed.</li> <li>2. Enter the password of the currently logged-in user.</li> <li>3. Click <b>Submit</b>.</li> </ol>

## 9.2 Configuring Authentication Parameters for Domain Users

### Abstract

Domain users are not the users of the **BMC** itself. The detailed information about domain users is stored on an **LDAP** server or **AD** server.

This procedure describes how to configure authentication parameters for domain users to authenticate them through an LDAP or AD server.

### Prerequisite

The parameters of the LDAP server or AD server are already obtained.

### Steps

- Configuring LDAP Server Authentication Parameters
  1. Select **User & Security**. The **User & Security** page is displayed.

- From the navigation tree in the left pane, select **Domain Users**. The **Domain Users** page is displayed, see [Figure 9-3](#).

**Figure 9-3 Domain Users Page**

ID	Name	Search Domain	Permissions	Operation
1	test	cn=admin,ou=login,dc=ldapdomain,dc=com	<input type="radio"/> Administrator <input type="radio"/> Operator <input checked="" type="radio"/> User	<a href="#">Save</a> <a href="#">Cancel</a>
2				<a href="#">Edit</a>
3				<a href="#">Edit</a>
4				<a href="#">Edit</a>
5				<a href="#">Edit</a>

- Turn on the **LDAP Authentication** switch.
- Set the parameters in the **Basic Attributes** area. For a description of the parameters, refer to [Table 9-2](#).

**Table 9-2 Parameter Descriptions for Basic LDAP Authentication Attributes**

Parameter	Setting
Server Address	Enter the <b>IP</b> address or <b>FQDN</b> of the LDAP server.
Port	Enter the port number. Range: 1–65535. Default: 389. If <b>Encryption Type</b> is set to <b>SSL</b> , enter the port number 636.
Bind DN	Enter the DN of the LDAP server, for example, <code>cn=admin,dc=ldapdomain,dc=com</code> .
Password	Enter the password for logging in to the LDAP server. It cannot be left blank. Range: 1–47 characters. <b>Bind DN</b> and <b>Password</b> are used to access the LDAP server.
Search Base	Enter the storage location of the user information on the LDAP server, for example, <code>dc=ldapdomain,dc=com</code> .

Attribute of User Login	Select the user login attribute identified by the LDAP server. → If <b>Bind DN</b> contains cn, select <b>cn</b> . → If <b>Bind DN</b> contains uid, select <b>uid</b> .
Encryption Type	Select the type of encryption used by the LDAP server. → <b>No encryption</b> : indicates that no encryption is used.
Parameter	<b>Setting</b>
	→ <b>SSL</b> : indicates that <b>SSL</b> encryption is used. → <b>StartTLS</b> : indicates that StartTLS encryption is used.
Upload certificate	Click the corresponding certificate button and upload the certificate. If <b>Encryption Type</b> is set to <b>No encryption</b> , no certificate needs to be uploaded.

5. Click **Save**.
6. In the **LDAP Role Group** area, click **Edit** in the **Operation** column for a role group to activate role group parameters.
7. Set the role group parameters. For a description of the parameters, refer to [Table 9-3](#).

**Table 9-3 LDAP Role Group Parameter Descriptions**

Parameter	Setting
Name	Enter the name of the role group that domain users belong to. The name contains a maximum of 64 characters, including digits, letters, spaces, and special characters. It cannot begin with a space. The allowed special characters include hyphens and underscores.
Search Domain	Enter the storage location of the user group information on the LDAP server, for example, <i>cn=admin,ou=login,dc=ldapdomain,dc=com</i> .
Permissions	Select the operation permissions of the role group on the BMC.

8. Click **Save** in the **Operation** column.
- Configuring AD Server Authentication Parameters
  1. Select **User & Security**. The **User & Security** page is displayed.
  2. From the navigation tree in the left pane, select **Domain Users**. The **Domain Users** page is displayed.
  3. Click **AD**. The **AD** tab is displayed, see [Figure 9-4](#).

**Figure 9-4 AD Tab**

ID	Name	Domain Name	Permissions	Operation
1	test01	mydomain.com	<input type="radio"/> Administrator <input type="radio"/> Operator <input checked="" type="radio"/> User	Save Cancel
2	6786786785	6786786654645	User	Edit Delete
3				Edit
4				Edit
5				Edit

- Turn on the **AD Authentication** switch.
- Set the parameters in the **Basic Attributes** area. For a description of the parameters, refer to [Table 9-4](#).

**Table 9-4 Parameter Descriptions for Basic AD Authentication Attributes**

Parameter	Setting
SSL Encryption	Select whether SSL encryption is used when logging in to the AD server. → To enable SSL encryption, turn on the <b>SSL Encryption</b> switch. → To disable SSL encryption, turn off the <b>SSL Encryption</b> switch.
User Name	Enter the username for logging in to the AD server. The username contains a maximum of 64 characters, including digits, letters (case sensitive), spaces, and special characters. It must begin with a letter. The allowed special characters include hyphens and underscores. If the username and password are not required, leave this parameter blank.
Password	Enter the password for logging in to the AD server. Range: 6–127 characters. If the username and password are not required, leave this parameter blank.

User Domain Name	Enter the domain name of the AD server, for example, <i>mydomain.com</i> , and is required.
<b>Parameter</b>	<b>Setting</b>
Domain Control Server Address 1	Enter the IP address of AD server 1, which supports IPv4 and IPv6 formats, and is required.
Domain Control Server Address 2	Enter the IP address of AD server 2, which supports IPv4 and IPv6 formats, and is optional.
Domain Control Server Address 3	Enter the IP address of AD server 3, which supports IPv4 and IPv6 formats, and is optional.

6. Click **Save**.
7. In the **AD Role Group** area, click **Edit** in the **Operation** column for a role group to activate role group parameters.
8. Set the role group parameters. For a description of the parameters, refer to [Table 9-5](#).

**Table 9-5 AD Role Group Parameter Descriptions**

Parameter	Setting
Name	Enter the name of the role group that domain users belong to. The name contains a maximum of 64 characters, including digits, letters, spaces, and special characters. It cannot begin with a space. The allowed special characters include hyphens and underscores.
Domain Name	Enter the domain name of the role group, for example, <i>mydomain.com</i> .
Permissions	Select the operation permissions of the role group on the BMC.

9. Click **Save** in the **Operation** column.

## 9.3 Querying Online Users

### Abstract

By querying online users, administrator can learn about all online users, including their **IDs**, **usernames**, **login modes**, **login IP addresses**, and **login time**.



### Note

The ID is the serial number of a user's connection session rather than the user ID.

## Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Online Users**. The **Online Users** page is displayed, see [Figure 9-5](#).

**Figure 9-5 Online Users Page**



The screenshot shows a table with the following data:

ID	User Name	Login Method	Login IP	Login Time	Operation
12	Administrator	Web HTTPS	10. [redacted]	2024-03-07 15:06:15	<a href="#">Delete</a>

Below the table, there is a navigation bar with buttons for sorting (K, <, >, X), page selection (1), and page size (10 / Page, To, 1 Page).

3. (Optional) To force a user to log out of the Web portal of the BMC, click **Delete** in the **Operation** column for the user, and click **Submit** in the displayed message box.

## 9.4 Configuring Permissions for a Customized Role

### Abstract

The following roles exist in the system by default:

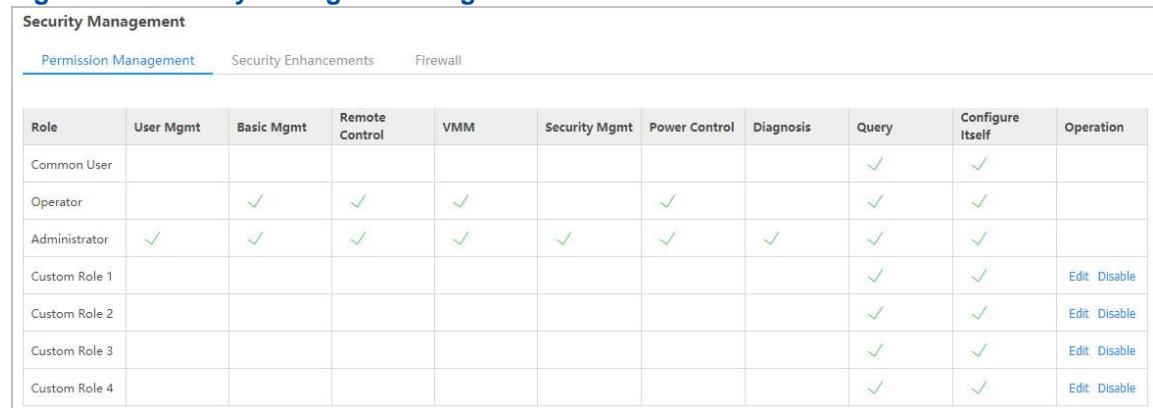
- Common user
- Operator
- Administrator
- Customized roles 1–4

The permissions of common users, operators, and administrators cannot be configured, while the permissions of customized roles can be configured.

## Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed, see [Figure 9-6](#).

**Figure 9-6 Security Management Page**

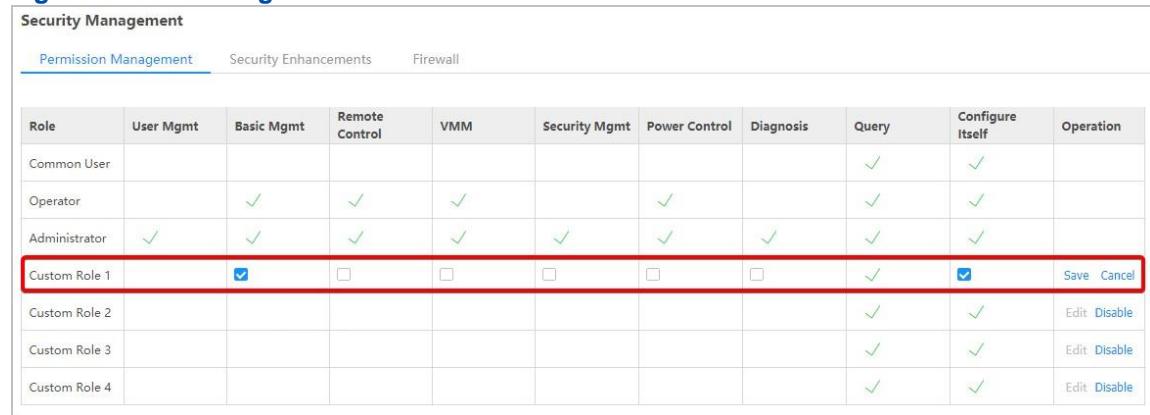


The screenshot shows a table with the following data:

Security Management											
Permission Management			Security Enhancements			Firewall					
Role	User Mgmt	Basic Mgmt	Remote Control	VMM	Security Mgmt	Power Control	Diagnosis	Query	Configure Itself	Operation	
Common User								✓	✓		
Operator		✓	✓	✓		✓		✓	✓		
Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Custom Role 1								✓	✓		<a href="#">Edit</a> <a href="#">Disable</a>
Custom Role 2								✓	✓		<a href="#">Edit</a> <a href="#">Disable</a>
Custom Role 3								✓	✓		<a href="#">Edit</a> <a href="#">Disable</a>
Custom Role 4								✓	✓		<a href="#">Edit</a> <a href="#">Disable</a>

3. In the **Operation** column, click **Edit** for a customized role to activate the permission check boxes, see [Figure 9-7](#).

**Figure 9-7 Activating the Permission Check Boxes**



Security Management											
Permission Management		Security Enhancements			Firewall						
Role	User Mgmt	Basic Mgmt	Remote Control	VMM	Security Mgmt	Power Control	Diagnosis	Query	Configure Itself	Operation	
Common User									✓	✓	
Operator		✓	✓	✓		✓		✓	✓		
Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Custom Role 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	✓	<input checked="" type="checkbox"/>	<a href="#">Save</a> <a href="#">Cancel</a>						
Custom Role 2								✓	✓	<a href="#">Edit</a> <a href="#">Disable</a>	
Custom Role 3								✓	✓	<a href="#">Edit</a> <a href="#">Disable</a>	
Custom Role 4								✓	✓	<a href="#">Edit</a> <a href="#">Disable</a>	

4. Select the corresponding permissions.

5. Click **Save**.

### Related Tasks

To disable or enable a customized role, perform the following operations:

- In the **Operation** column, click **Disable** to disable the customized role.
- In the **Operation** column, click **Enable** to enable the customized role.



You cannot disable or enable common users, operators, and administrators.

## 9.5 Configuring Security Enhancement Parameters

### Abstract

To enhance user login security, you can configure security enhancement parameters, including:

- **Password Complexity Check** • **Password Validity** • **User Lockout Policy**

### Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
3. Click **Security Enhancements**. The **Security Enhancements** tab is displayed, see [Figure 9-8](#).

**Figure 9-8 Security Enhancements Tab**

4. Set the parameters. For a description of the parameters, refer to [Table 9-6](#).

**Table 9-6 Security Enhancement Parameter Descriptions**

Parameter	Setting
Password Complexity Check	Select whether to enable password complexity check. <ul style="list-style-type: none"> <li>• To enable password complexity check, turn on the <b>Password Complexity Check</b> switch.</li> <li>• To disable password complexity check, turn off the <b>Password Complexity Check</b> switch.</li> </ul>
Password Validity	Enter the password validity period. Range: 0–365, unit: days. If the password validity period is 0, there is no limit to the validity period.
User Lockout Policy	Select the maximum number of login failures and enter the locking duration. If the maximum number is exceeded, a user is locked.

5. Click **Save**.

## 9.6 Configuring Firewall Parameters

### Abstract

By configuring firewall parameters, you can add IP or MAC addresses to the blacklist and whitelist to control access to the [BMC](#).

- The devices in the blacklist are forbidden to access the BMC all the time or within the specified time period.
- The devices in the whitelist are allowed to access the BMC all the time or within the specified time period.

Note: When enabling the whitelist policy, you must first add the **IP** or **MAC** address of your local **PC** (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

## Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
3. Click **Firewall**. The **Firewall** tab is displayed, as shown in [Figure 9-9](#).

**Figure 9-9 Firewall Tab**

No. <span style="font-size: small;">▲</span>	Time Segment	IP Segment	MAC Segment	Operation
1	Time Type <input type="button" value="Date ..."/> 2024-01-11 00:00 - 2024-02-11 <input type="checkbox"/> Working days only	10.239.10.10 — 10.239.10.20	Required <input type="checkbox"/> — Optional <input type="checkbox"/>	<a href="#">Save</a> <a href="#">Cancel</a>

No. <span style="font-size: small;">▲</span>	Time Segment	IP Segment	MAC Segment	Operation
1	Time Type <input type="button" value="Date ..."/> 2024-01-11 00:00 - 2024-02-11 <input type="checkbox"/> Working days only	10.239.20.10 — 10.239.20.20	Required <input type="checkbox"/> — Optional <input type="checkbox"/>	<a href="#">Save</a> <a href="#">Cancel</a>

4. Perform the following operations as needed.

To...	Do...
Add an item to the blacklist	<ol style="list-style-type: none"> <li>In the <b>Blacklist</b> area, click <b>Add Rule</b>. The blacklist parameters are activated.</li> <li>Set the parameters. For a description of the parameters, refer to <a href="#">Table 9-7</a>.</li> <li>Click <b>Save</b>.</li> </ol>
Add an item to the whitelist	<ol style="list-style-type: none"> <li>In the <b>Whitelist</b> area, click <b>Add Rule</b>. The whitelist parameters are activated.</li> <li>Set the parameters. For a description of the parameters, refer to <a href="#">Table 9-7</a>.</li> <li>Click <b>Save</b>.</li> </ol>

**Table 9-7 Blacklist/Whitelist Parameter Descriptions**

Parameter	Description
Time Segment	<p>From the <b>Time Type</b> list, select the desired time type, and set the time period accordingly.</p> <p>The format of the start time and end time must be the same.</p> <p>Before selecting <b>Working days only</b>, you must specify a time period. If the time period is left blank, the devices in the blacklist are permanently forbidden to access the BMC or those in the whitelist are permanently allowed to access the BMC.</p>
IP Segment	<p>Enter an IP address or an IP address segment. IPv4 or IPv6 format is supported.</p> <p>For a single IP address, 127.0.0.1 is disallowed.</p> <p>For an IP address segment, the format of the start address and end address must be the same.</p>
MAC Segment	<p>Enter a MAC address or a MAC address segment. The format is xx:xx:xx:xx:xx:xx.</p> <p>A MAC address segment can contain a maximum of 64 MAC addresses. At least one of the <b>IP Segment</b> and <b>MAC Segment</b> parameters must be set.</p>

## 9.7 Configuring Two-Factor Authentication

### Abstract

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

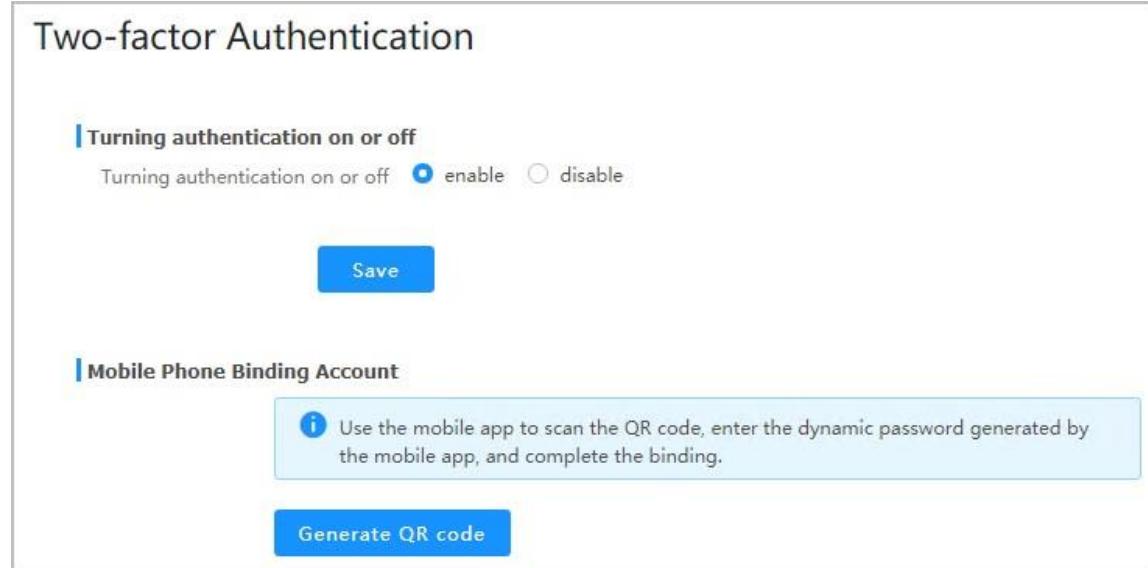


### Note

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

### Steps

1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Two-factor Authentication**. The **Two-factor Authentication** page is displayed, as shown in [Figure 9-10](#).

**Figure 9-10 Two-factor Authentication Page**

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 to.

**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.

# Chapter 10

## 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 10-1](#).

**Table 10-1 Default Password Descriptions**

Server Model	BMC Version	Default Password
NCS6712 N4 NCS6742 N4	Versions earlier than V04.23.01.02P1	superuser
	V04.23.01.02P1 and later	Superuser@123
NCS6722 N4 NCS6742G N4	Versions earlier than V04.23.02.01	superuser
	V04.23.02.01 and later	Superuser@123
R5301 G5	Versions earlier than V04.23.04.00	superuser
	V04.23.04.00 and later	Superuser@123
R5310 G3	Versions earlier than V04.23.01.02	superuser
	V04.23.01.02 and later	Superuser@123
NCS6722A N4	Versions earlier than V04.23.01.01P2	superuser
	V04.23.01.01P2 and later	Superuser@123
NCS6744 N4	Versions earlier than V04.23.01.01	superuser
	V04.23.01.01 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 11

# Reference: Accessing Documents

---

## Abstract

Documents are readily available at [NETAŞ-Server and Storage](#).



This procedure uses NETAŞ Server Redfish Interface Description (BMC V4) as an example, and other documents can be accessed by similar steps.

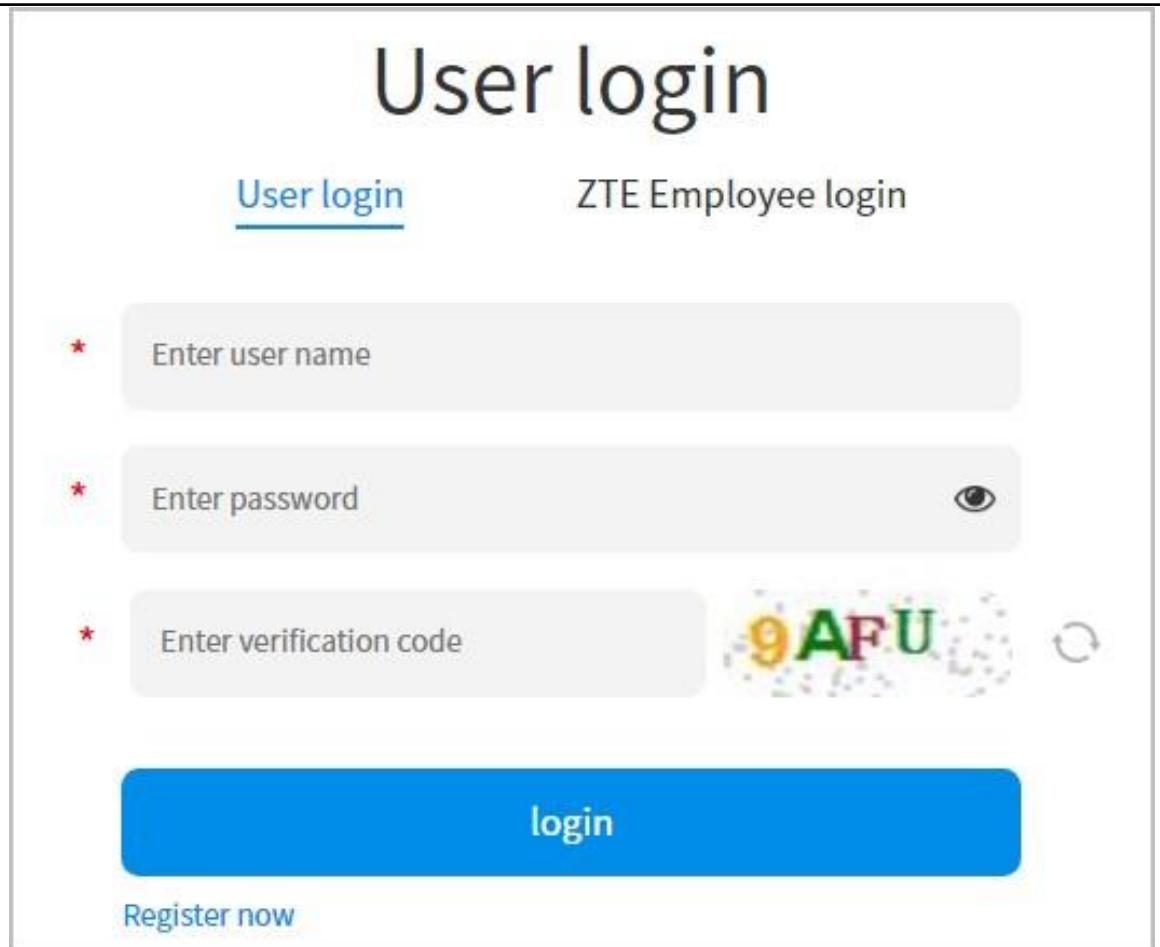
## Prerequisite

You have registered successfully at [NETAŞ-Server and Storage](#).

## Steps

1. In the address bar of your browser, enter <https://destek.netas.com.tr> and press **Enter**. The home page is displayed.
2. Click **Login** in the upper right corner. The **User Login** page is displayed, see [Figure 11-1](#).

Figure 11-1 User Login Page



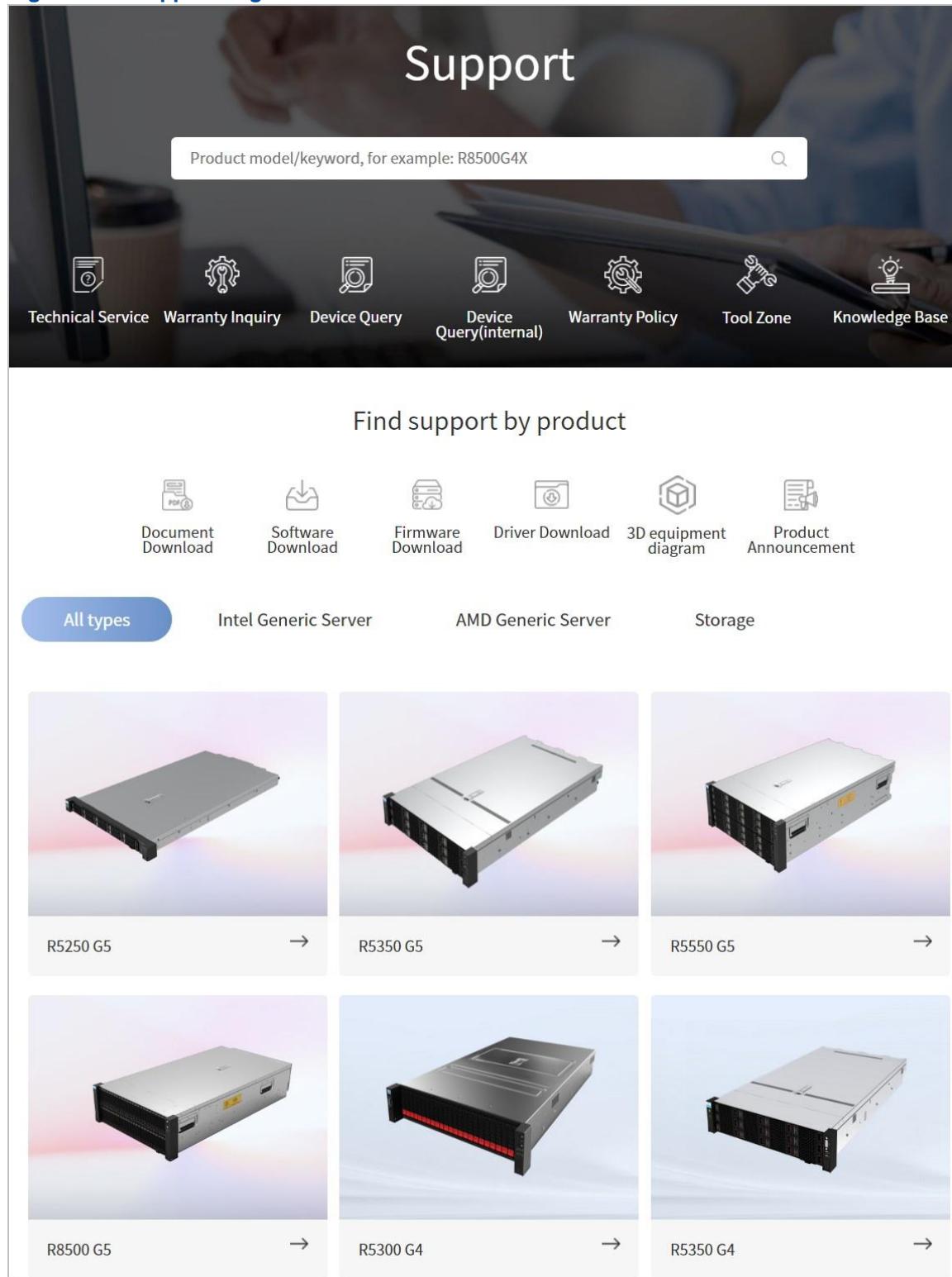
The screenshot shows the 'User login' page. At the top, there are two tabs: 'User login' (underlined in blue) and 'ZTE Employee login'. Below the tabs are three input fields with red asterisks indicating required fields:

- Enter user name
- Enter password (with an eye icon to toggle visibility)
- Enter verification code (with a refresh icon and a CAPTCHA image showing '9AFU' over a grid of colored dots)

A large blue 'login' button is at the bottom, and a 'Register now' link is at the bottom left.

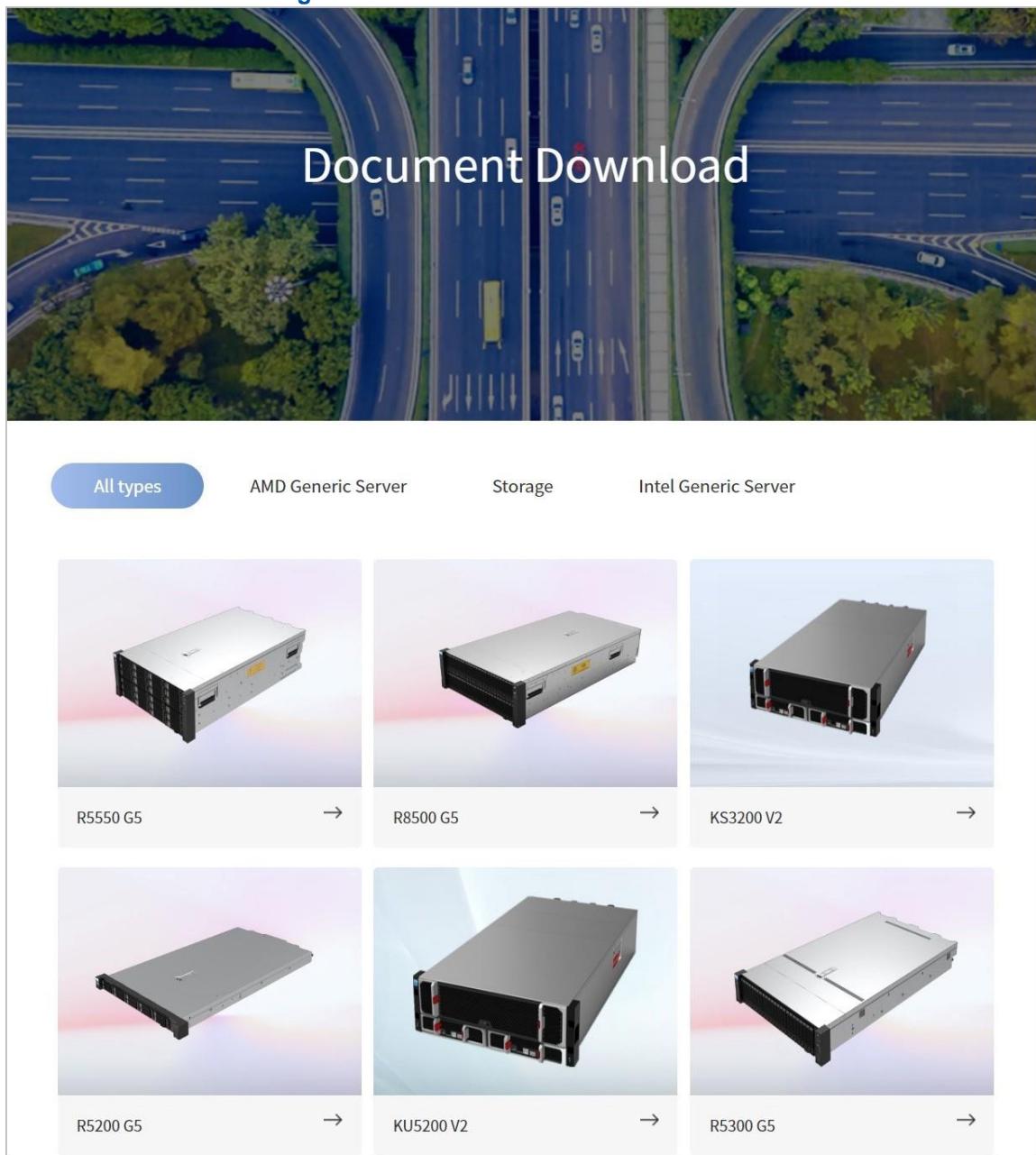
3. Enter the username, password, and verification code.
4. Click **Login** to log in the **NETAŞ-Server and Storage** website.
5. Select **Support** on the menu. The **Support** page is displayed, see [Figure 11-2](#).

Figure 11-2 Support Page



6. Click **Document Download**. The **Document Download** page is displayed, see [Figure 11-3](#).

Figure 11-3 Document Download Page



7. On the server list of servers at the lower part of the page, click the server that the document to be accessed is about.
8. In the **document** list, select **Interface Description**, and all the documents about interface description are display on the right side of the page.
9. Click **Download** to the right of **NETAS Server Redfish Interface Description (BMC V4)**, and download the document.

# Glossary

---

## **A/D**

- Analog to Digital

## **AC**

- Alternating Current

## **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

## **CD**

- Compact Disk

## **CLI**

- Command Line Interface

## **CPU**

- Central Processing Unit

**CRPS**

- Common Redundant Power Supplies

**DCMI**

- Data Center Manageability Interface

**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

**FTP**

- File Transfer Protocol

**GPIO**

- General Purpose Input Output

**GPU**

- Graphics Processing Unit

**GUI**

- Graphical User Interface

## **HD**

- Hard disk

## **HTML**

- HyperText Markup Language

## **HTTP**

- Hypertext Transfer Protocol

## **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

## **JRE**

- Java Runtime Environment

## **KPI**

- Key Performance Indicator

## **KVM**

- Keyboard, Video and Mouse

## **LAN**

- Local Area Network

## **LDAP**

- Lightweight Directory Access Protocol

## **LPC**

- Lower order Path Connection

## **LVDC**

- Low-Voltage Direct Current

## **MAC**

- Media Access Control

## **NCSI**

- Network Controller Sideband Interface

## **NIC**

- Network Interface Card

## **NMS**

- Network Management System

## **NTP**

- Network Time Protocol

## **NVMe**

- Non-Volatile Memory Express

## **OS**

- Operating System

## **PC**

- Personal Computer

## **PCIe**

- Peripheral Component Interconnect Express

## **PECI**

- Platform Environment Control Interface

## **POST**

- Power-On Self-Test

## **PWM**

- Pulse-Width Modulation

## **PXE**

- Preboot eXecution Environment

## **RAID**

- Redundant Array of Independent Disks

## **RMCP**

- Remote Management Control Protocol

## **RPM**

- Rotations Per Minute

## **SAS**

- Serial Attached SCSI

## **SATA**

- Serial ATA

## **SEL**

- System Event Log

**SFTP**

- Secure File Transfer Protocol

**SGPIO**

- Serial GPIO

**SHA**

- Secure Hash Algorithm

**SMBUS**

- System Management BUS

**SMTP**

- Simple Mail Transfer Protocol

**SNMP**

- Simple Network Management Protocol

**SSH**

- Secure Shell

**SSL**

- Secure Sockets Layer

**TCP**

- Transmission Control Protocol

**TLS**

- Transport Layer Security

**UEFI**

- Unified Extensible Firmware Interface

**UID**

- Unit Identification Light

**USB**

- Universal Serial Bus

**VLAN**

- Virtual Local Area Network

**VNC**

- Virtual Network Console

**VR**

- Voltage Regulator

**XML**

- Extensible Markup Language

**NETAŞ**

- Zhongxing Telecommunications

**EquipmentiSAC**

- Integrated Server Administrator Controller