Vantageo Server

BMC User Guide (BMC V4)

LEGAL INFORMATION

disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. VANTAGEO PRIVATE LIMITED and its licensors shall not be liable for damages resulting from theuse of or reliance on the information contained herein.

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

VANTAGEO PRIVATE LIMITED reserves the right to upgrade or make technical change to this product without further notice.Users may visit the VANTAGEO technical support website https://support.Vantageo.com.cn to inquire for related information. The ultimate right to interpret this product resides in VANTAGEO PRIVATE LIMITED.

Statement on the Use of Third-Party Embedded Software:

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

About This Manual

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

Intended Audience

This manual is intended for:

- Network planning engineers
- Configuration engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters.

BMC Overview	Describes the operating principle and functions of the BMC, soft- ware security and operation interfaces.
Performing Client Commission- ing	Describes the debugging operations on the BMC Web portal logged in through a client.
Logging In to the Web Portal of the BMC	Describes how to log in to the Web portal of the BMC.
Common Operations	Describes common operations in the BMC.
System Management	Describes how to perform system management operations.
, Diagnosis and Maintenance	Describes how to perform diagnosis and maintenance opera- tions.
Service Management	Describes how to perform service management operations.
BMC Management	Describes how to perform BMC management operations.
User and Security	Describes how to perform user and security management opera- tions.

BMC Overview

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

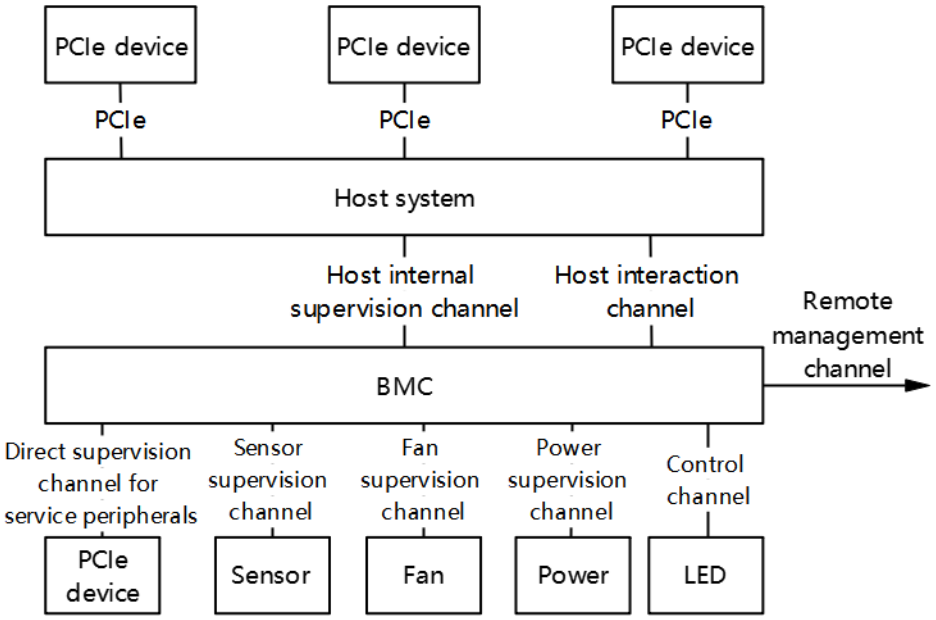
Operating Principle

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 func- tions. 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.

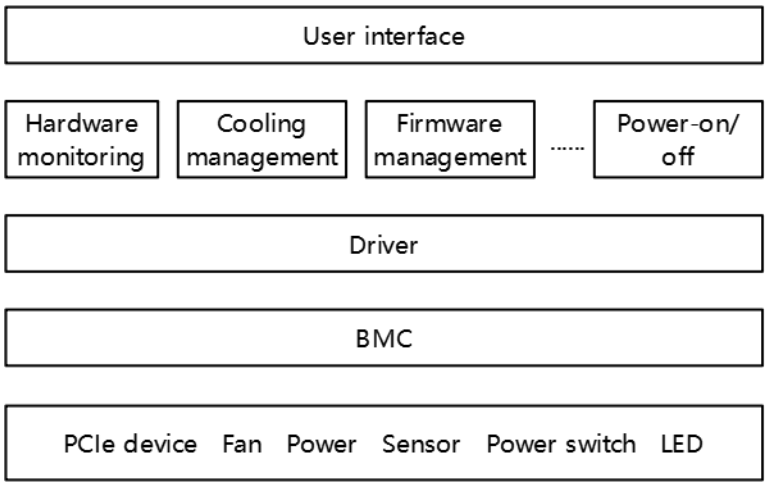
Table 1-1 BMC Hardware Channel Descriptions

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 IPMI protocol
Direct supervision channel for service peripherals	SMBUS and NC-SI	PCIe devices of a server
Sensor supervision channel	SMBUS, GPIO, and A/D	Temperature sensor, voltage sensor, current sensor, and presence sensor
Fan supervision channel	PWM	Fan
Power supervision channel	SMBUS	CRPS, and PMBUS power supply
Control channel	GPIO and SGPIO	Power-on, power-off, and indicator on/off
Remote management channel	Ethernet	Accesses the BMC management server

- Management software

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

Figure 1-2 BMC Management Software Architecture



Functions

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

- Server health status management: Checks the operational status of a server, analyzes historical data and actual monitoring data, and helps users to find and solve problems in advance, ensuring the highly reliable operation of the server.
  - → The 80-code recording function provides sufficient information for analyzing startup failures.
  - → When the system crashes, the last-screen capture function records the on-site scenario for analyzing system crashes.
  - → Screen snapshots and screen recording on preventive maintenance and operation processes facilitate follow-up audits.
  - → The alarm function supports precise fault diagnosis based on components, facilitating component fault locating and replacement.
  - → The CrashDump function facilitates further analysis of system errors.
  - → The BMC supports 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 BIOSs are supported to improve the reliability of BIOS upgrade and operation.
  - → The firmware (for example, the FRU and EPLD) upgrade function is supported.
- System cooling
  - → Monitors the temperature of important components on the server, and performs different cooling controls based on different hardware thermal characteristics.
  - → Supports the over-temperature power-off function to ensure that the server hardware is not damaged, extending the service life of components.
- Intelligent power consumption management
  - → The BMC supports the power capping technology, and provides the standard DCMI for centralized control by the NMS, improving the deployment density of servers.
  - → Energy-saving design reduces the operating costs of a server.
- BMC self-management
  - → Supports synchronizing the BMC time through the network and the host, meeting the requirements in different scenarios.
  - → Supports multiple authentication modes, which simplifies server management.
  - → Supports DHCP and DNS, which simplifies server deployment and management.
- Diversified management interfaces

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

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

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

Performing Client Commissioning

Abstract

In most cases, you can log in to the Web portal of the BMC on a client through the iPMI 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 iPMI 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

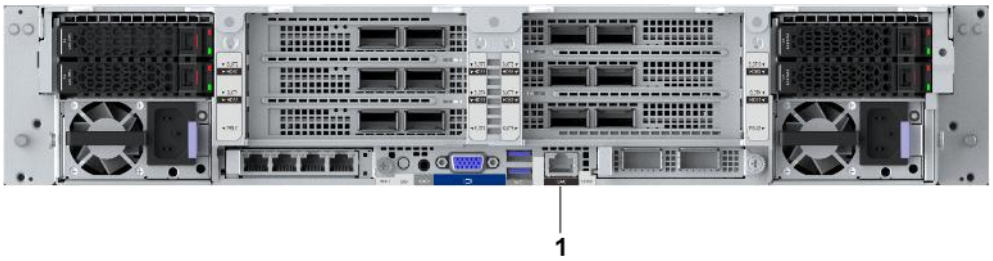
Note

Google Chrome 59 and later versions are recommended.

Context

The default IP address of the iPMI management network port of a server is 192.168.5.7. Figure 2-1 shows the position of the iPMI management network port on the rear panel of the server.

Figure 2-1 Position of the iPMI Management Network Port



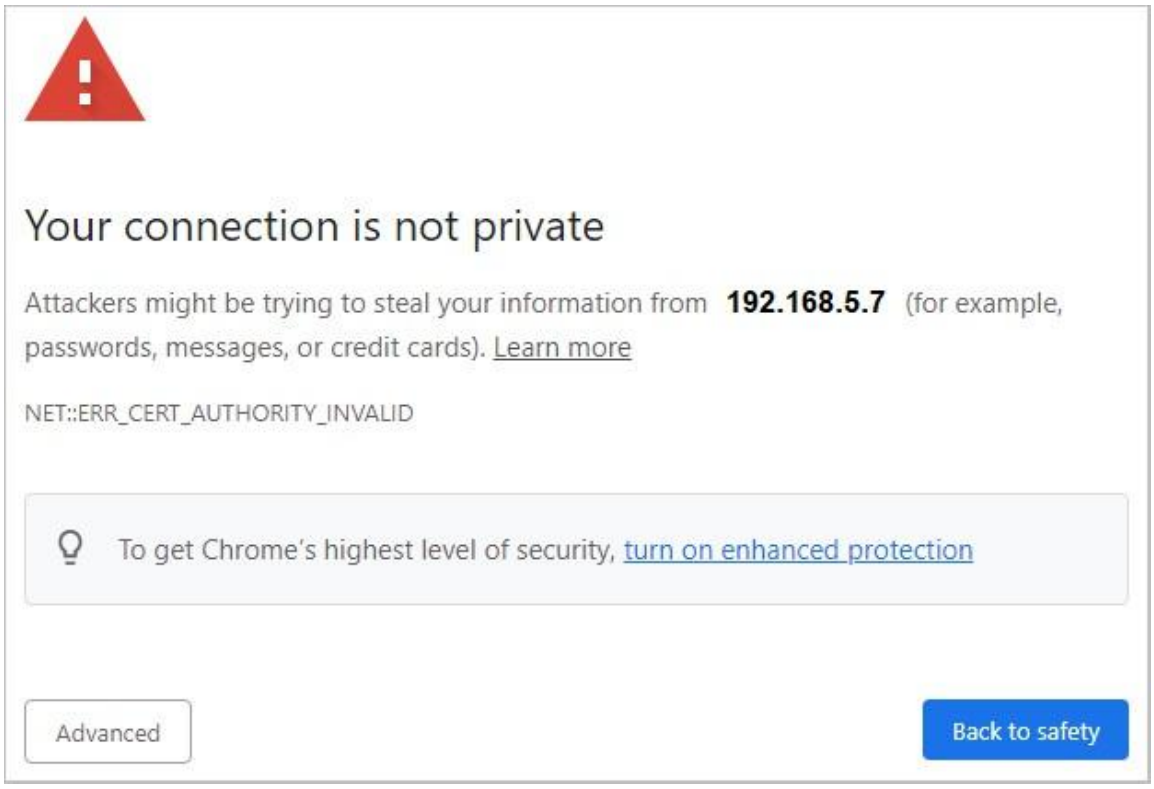
1. iPMI management network port

Steps

1. Connect the PC to the iPMI 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,

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,

7. Set the IP address of the iPMI management network port as planned, for example, 10.235.51.202.

   Note

   For how to set the IP address of the iPMI management network port, refer to 8.1.3 Configuring IP Addresses of Network Ports.

8. Record the IP address of the iPMI management network port.
9. Connect the iPMI management network port to the corresponding switch through a network cable.
10. 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 iPMI management network port belongs to.
11. Connect the PC to the corresponding switch through a network cable, so that the PC and the iPMI management network port are in the same LAN.
12. Run the **`ping`** command on the CLI of the PC to make sure that the PC can communicate with the iPMI management network port properly.

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 iPMI management network port is already obtained.

Steps

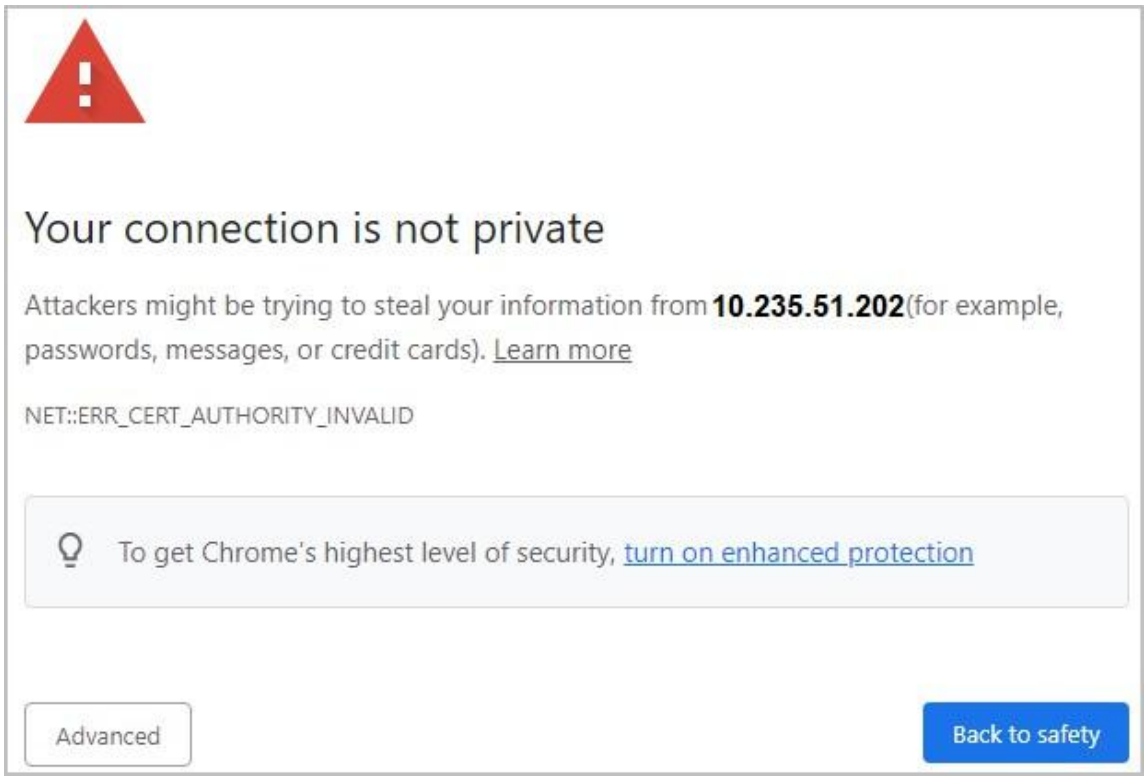
1. In the address bar of the browser, enter the address of the Web portal of the BMC, and press **Enter**. The page for login is displayed, see Figure 3-1.

Note

The address format of the Web portal of the BMC is as follows: *https://IP*. "IP" is the IP address of the iPMI 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,

For a description of the **Homepage**, refer to Table 3-1.

Table 3-1 Homepage Descriptions

No.	Name	Description
1	**Device Information**	Displays the detailed information and active alarm statistics of the server. ● To modify the asset flag of the server, click  . ● To view alarm details, click **Details**.
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	Displays the total number of active alarms. ● To view the number of alarms at each level, hover the mouse pointer over this button. ● To view alarm details, click this button.
4	UID button	Displays the UID indicator status of the server. To change the status of the UID indicator, click this button and select the corresponding shortcut menu. The shortcut menus include: ● **Steady on**: The UID indicator is lit, helping you to identify the current server among the servers in the equipment room.

No.	Name	Description
		● **Blink**: 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. ● **Off**: The UID indicator is off. The grayed shortcut menu indicates the current status of the UID indicator. For example, if the **Blink** shortcut menu is grayed, the UID indicator of the server is flashing.
5	Power button	Displays the power status of the server. To change the power status, click this button and select the corresponding shortcut menu. The shortcut menus include: ● **Power On**: Power on the server. ● **Normal Power Off**: Power off the server. ● **Forced Power Off**: Forcibly power off the server. ● **Power Reset**: Perform a warm reboot. Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline. ● **Power Cycle**: Perform a cold reboot. Cold reboot means that the server is started after it is shut down. During the restart, the server is offline. The grayed shortcut menu indicates the current power status of the server. For example, if the **Power On** shortcut menu is grayed, the server is in power-on status.
6	Language button	Displays the current language of the Web portal of the BMC. To change the language, click this button.
7	Current user	Displays the currently logged-in user. ● To view the details of the currently logged-in user, including the IP address and login time, click this button. ● To log out the currently logged-in user, click this button and then click **Log Out** in the detailed information box displayed.
8	**Shortcuts**	Displays the shortcut operation buttons on the Web portal of the BMC, including: ● **Firmware Upgrade**: upgrades firmware. For details, refer to 8.4 Upgrading Firmware. ● **Log**: queries BMC logs. For details, refer to 6.8 Querying BMC Logs. ● **Network**: configures network parameters. For details, refer to 8.1 Network Parameter Configuration. ● **Power**: queries server power-on/off information, and power supply and power consumption information. For details, refer to 5.7 Powering On/Off the Server and 5.13 Configuring Power Control Parameters.

No.	Name	Description
		● **One-Click Collection**: 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.
9	**Device List**	Displays the components in the server by category. To view the details of components of a category, click the category.
10	**Virtual Console**	Displays the operations related to the virtual console, including: ● To enable KVM preview in the **Virtual Console** area, click **Open Preview**. ● To disable KVM preview in the **Virtual Console** area, click **Close Preview**. ● To start the virtual console in HTML mode, click **Operate** and then select **Start HTML Virtual Console** from the shortcut menu. ● To start the virtual console in Java mode, click **Operate** and then select **Start Java Virtual Console** from the shortcut menu. ● To reset the virtual console, click **Operate** and then select **Reset Virtual Console** from the shortcut menu. ● Click **Settings**.
11	**System Monitoring**	Displays system monitoring information.

Common Operations

Logging In to the BMC Through SSH

Abstract

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

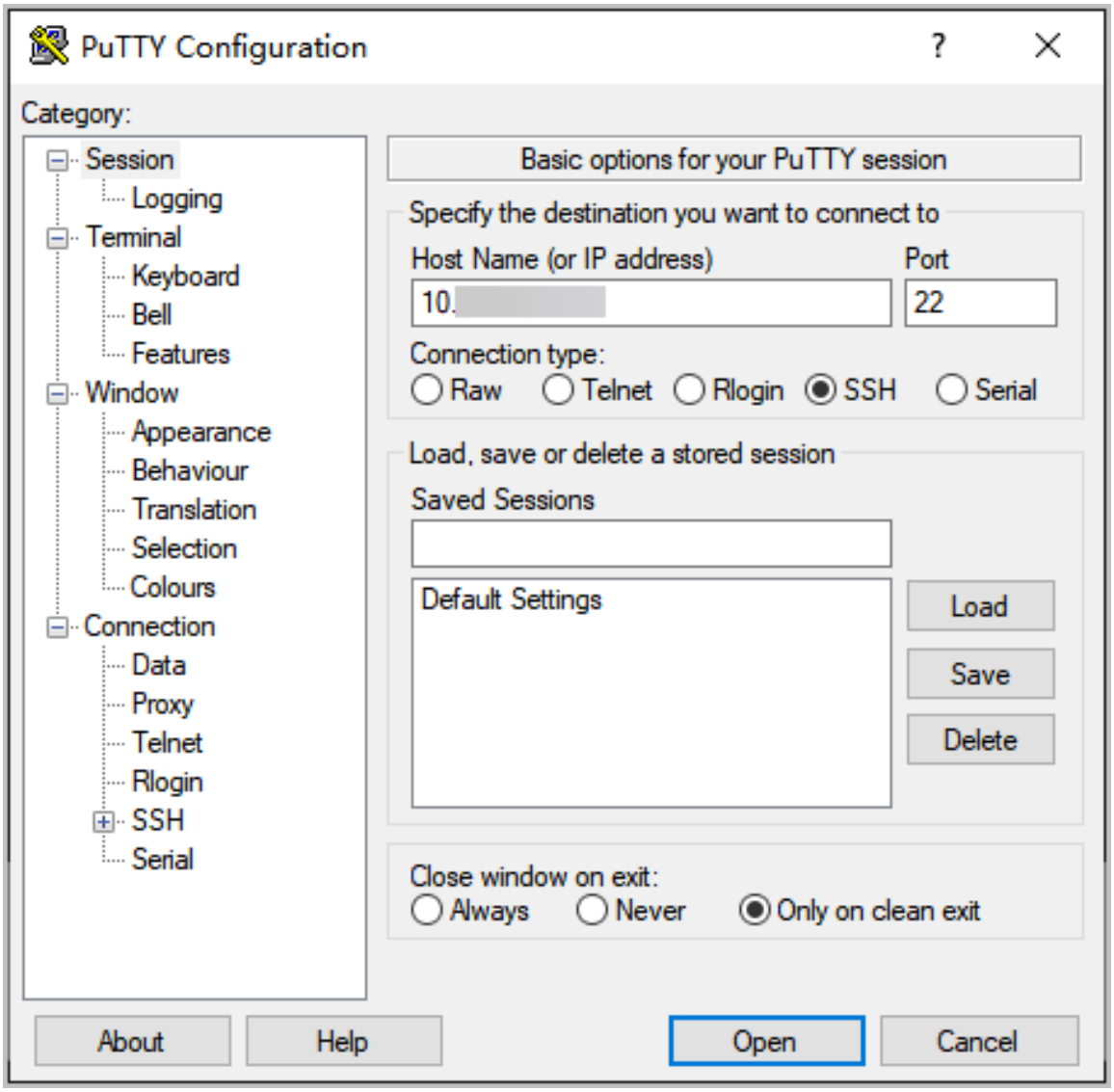
Prerequisite

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

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



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 **Session**.
Host Name (or IP address)	Enter the IP address of the iPMI management network port or shared network port.
Port	Enter *22*.

Parameter	Setting
Connection type	Select **SSH**.

2. Click **Open**. The CLI is displayed.
3. 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.

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

Modifying the BMC Address

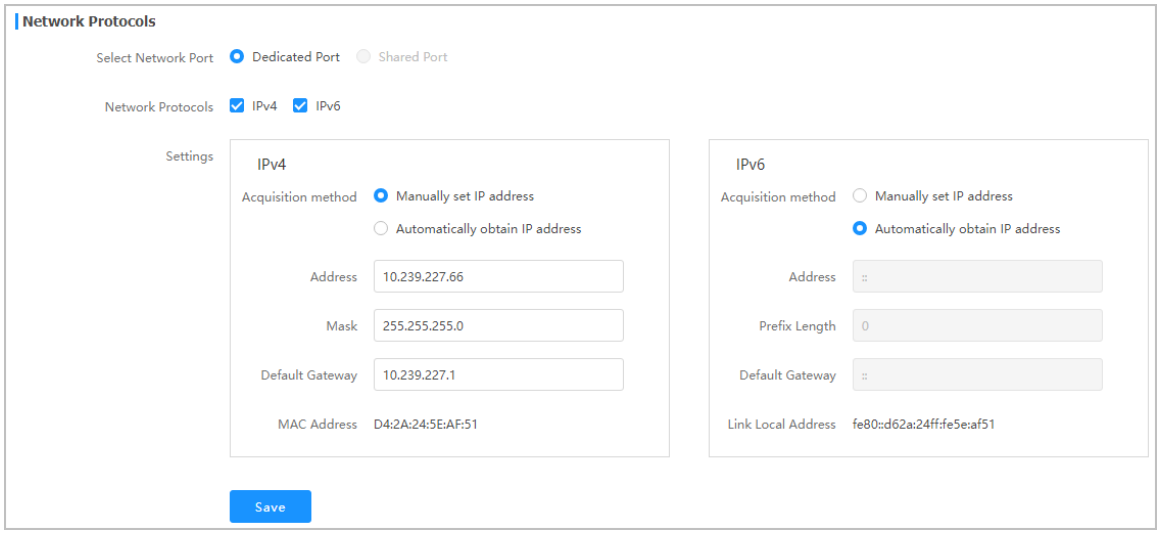
Abstract

To replan the IP address of the iPMI 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



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	This parameter can be set only if **Select Mode** is set to **Alone** in the **Network Port** area. Select the network port for which you want to configure an IP address. ● **Dedicated Port**: configures the IP address of the iPMI management network port.

Parameter	Setting
	● **Shared Port**: configures the IP address of the shared network port.
Network Protocols	Select the network protocol(s) for the network port. ● The IPv4 settings need to be configured if you select **IPv4** only. ● The IPv6 settings need to be configured if you select **IPv6** only. ● Both IPv4 settings and IPv6 settings need to be configured if you select **IPv4** and **IPv6**.
Acquisition method	Select the method of obtaining the IP address. The parameters below do not need to be configured if **Acquisition method** is set to **Automatically obtain IP address**.
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**.

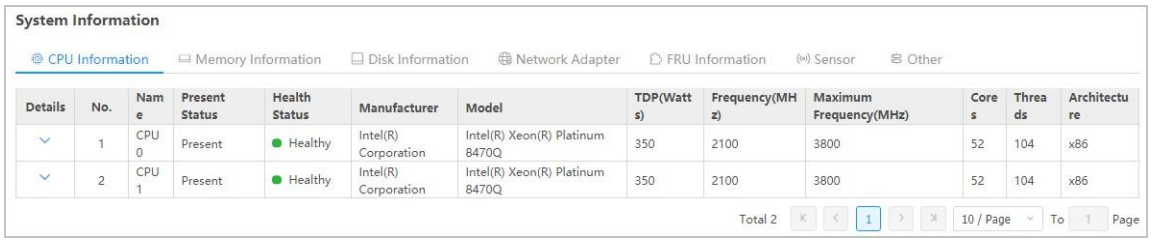
Checking Server Information

Abstract

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

- Serial number
- CPU
- Memory
- NIC
- Slot that a GPU is located

Figure 4-7 System Information Page



1. Perform the following operations as required.

To...	Do...
Check CPU information	Click **CPU Information** to switch to the **CPU Information** tab.
Check memory information	Click **Memory Information** to switch to the **Memory Information** tab.
Check NIC information	Click **Network Adapter** to switch to the **Network Adapter** tab.

Check GPU information	a. Click **Other**. The **Other** tab is displayed, as shown in Figure 4-8. b. Check the **Position** and **Device BDF** columns for each GPU.

Managing Storage Devices

Abstract

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

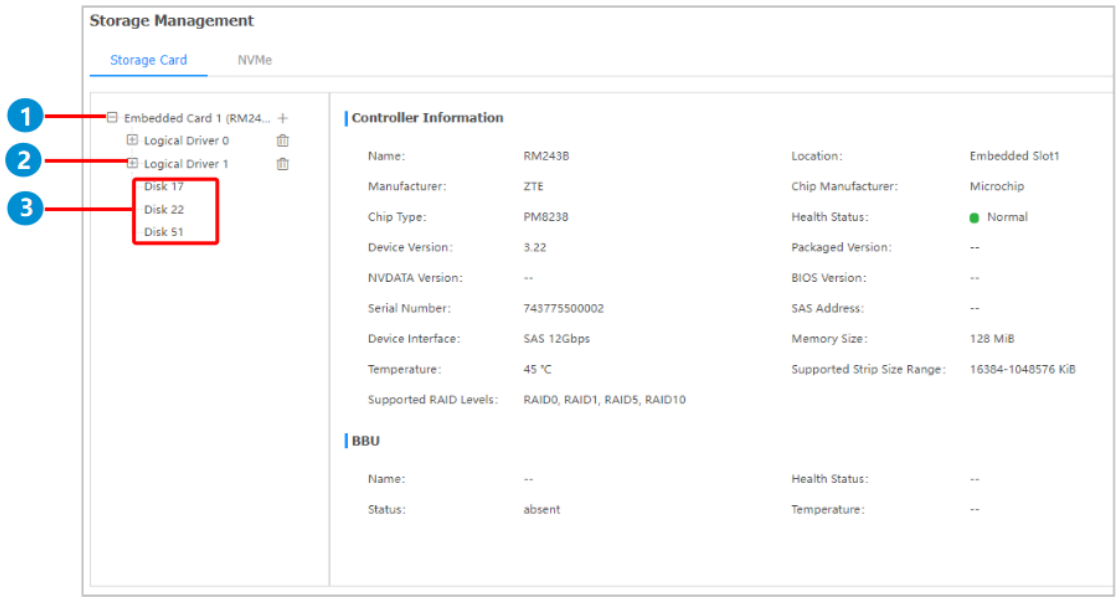
The physical disks managed by a RAID controller can be created as logical disks.

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 4-10.

Figure 4-10 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 BBU information	On the **Storage Card** tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the **Storage Card** tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, **Status** includes: ● **Optimal** ● **Degraded** ● **Part Degraded** ● **Offline**
Set the UID indicator of a logical disk	a. On the **Storage Card** tab, click the desired logical disk. b. Click **Settings** on the right. The **Logical Drive Setting** dialog box is displayed. c. Select **Open** or **Close**. ● **Open**: turns on the UID indicators of all member disks of the logical disk. ● **Off**: turns off the UID indicators of all member disks of the logical disk. d. Click **Submit**.
Check physical disk information	On the **Storage Card** tab, click the desired physical disk. The detailed physical disk information is displayed on the right.

To…	Do…
Create a logical disk	a. On the **Storage Card** tab, click **+** next to a RAID controller. The **Create Logical Drive** area is displayed on the right, see Figure 4-11. b. Configure the following parameters: ● **Logical disk name**: Enter the name of the logical disk. ● **RAID Level**: Select the corresponding RAID level. ● **Stripe Size**: Select a stripe size. ● **Physical Drive Configuration**: Select the member disks that form the logical disk. c. Click **Save**.
Query NVMe hard disk information	On the **Storage Management** page, click **NVMe** to switch to the **NVMe** tab. The detailed NVMe disk information is displayed.

4.1 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

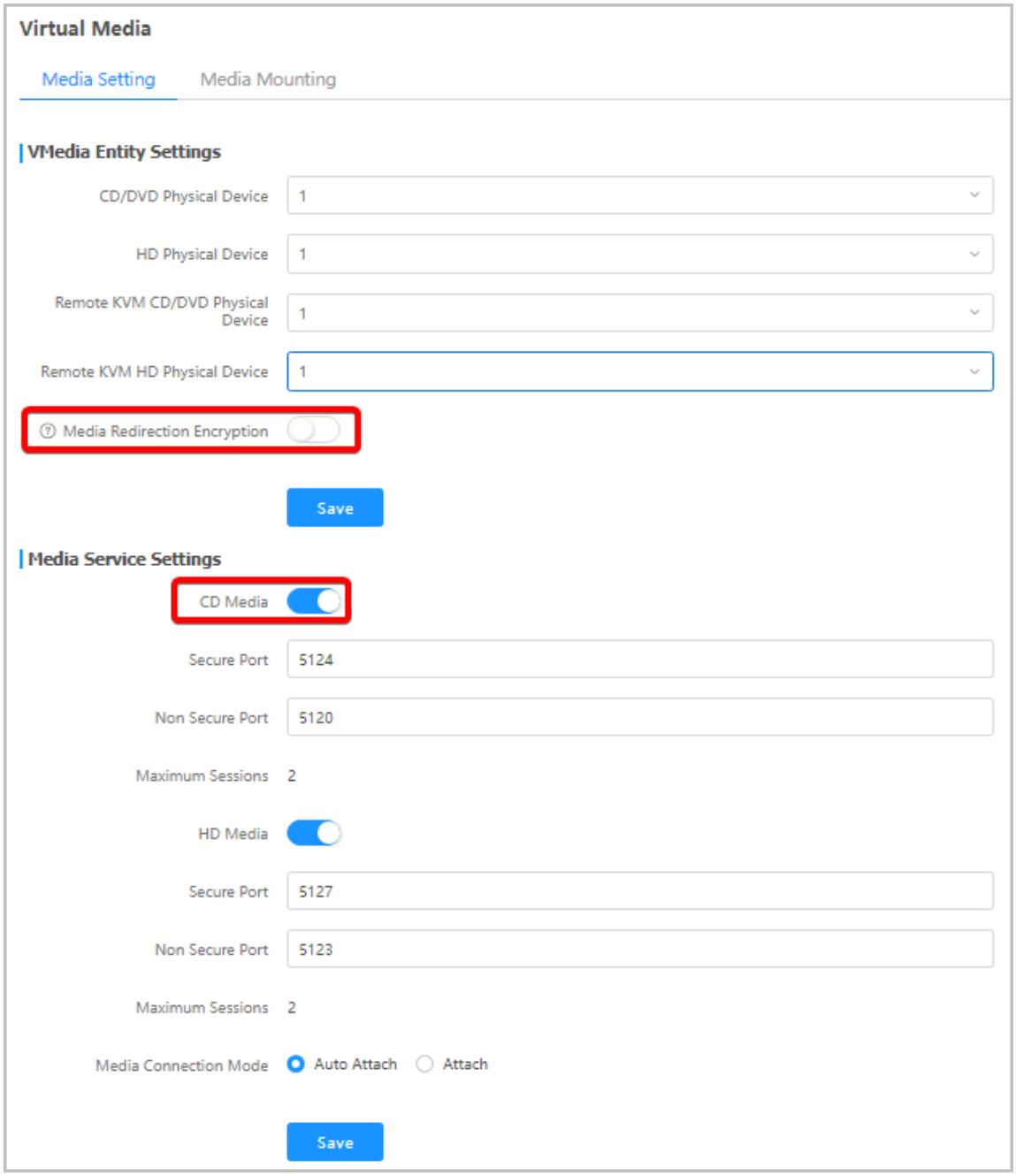
- The *iso* file of the OS is already obtained.
- The RAID configuration for the system disk of the server is already completed.
- If the KVM needs to be started in Java mode, JRE (for example, *jre-8u191*) is already installed on the PC.

Steps

Disabling Media Redirection Configurations

1. Select **Services**. The **Services** page is displayed.
2. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed, see Figure 4-12.

Figure 4-12 Virtual Media Page



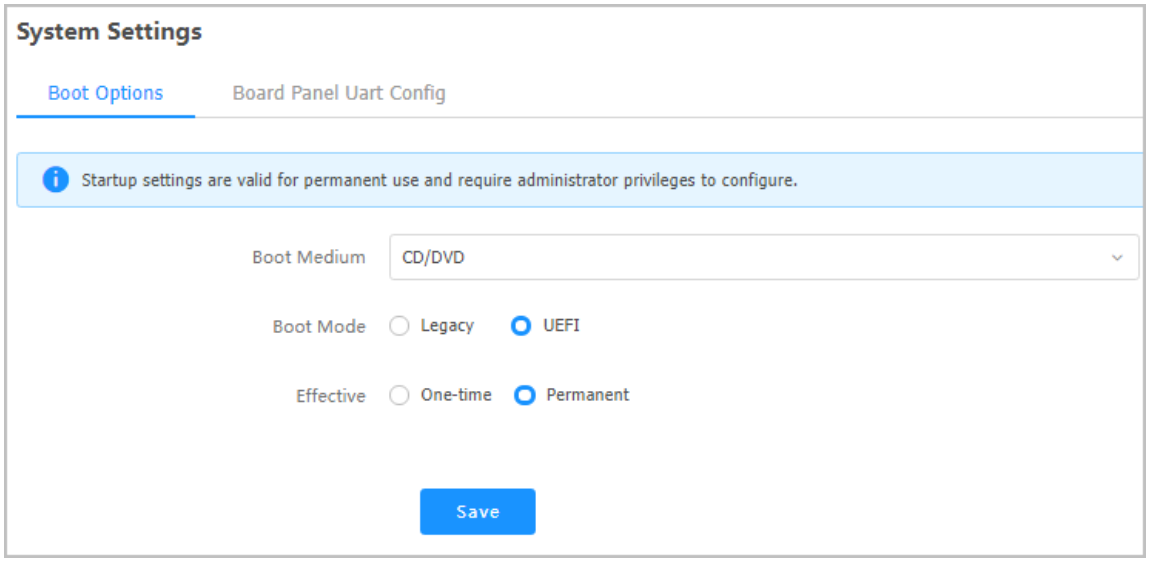
3. In the **VMedia Entity Settings** area, turn off **Media Redirection Encryption**, and click **Save**.
4. In the **Media Service Settings** area, turn on **CD Media**, and click **Save**.
5. From the navigation tree in the left pane, select **Virtual Console**. The **Virtual Console** page is displayed, .

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 4-14.

Figure 4-14 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 **CD/DVD**.
Boot Mode	Select **UEFI**.
Effective	Select **Permanent**.

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 KVM in HTML mode	a. Click **HTML Virtual Console**. The **HTML Virtual Console** page is displayed, see Figure 4-15. b. Click **Browse File** next to **CD Image**, and select the *iso* file from the PC. c. Click **Start Media** to load the *iso* file. d. Select **Power > Reset Server** to restart the server. The page for installing the OS is displayed.
Start the KVM in Java mode	a. In the search box in the lower left corner of the PC, enter *Java*. b. In the search result, select **Configure Java**. The **Java Control Panel** dialog box is displayed.

To…	Do…
	c. Click **Security**. The **Security** window is displayed. d. Click **Edit Site List**. The **Exception Site List** dialog box is displayed. e. Click **Add** to add the address of the Web portal of the BMC. f. Click **OK** to return to the **Security** window. g. Click **OK**. h. On the **Virtual Console** page of the Web portal of the BMC, click **Java Virtual Console**. A dialog box indicating whether to keep *jviewer.jnlp* is displayed. i. Click **Keep**. j. In the lower left corner of the browser, click *jviewer.jnlp*. A dialog box indicating whether to proceed is displayed. k. Click **Continue**. The **Do you want to run this application?** dialog box is displayed. l. Select **I accept the risk and want to continue to run this app.** and click **Run**. The **Untrusted Connection** dialog box is displayed. m. Click **Yes**. The **Java Console** page is displayed, see Figure 4-16. n. Select **Media > Virtual Media Wizard...**, and switch to the **CD/DVD** tab. o. Click **Browse**, and select the *iso* file from the PC. p. Click **Connect**. q. Select **Power > Reset Server** to restart the server. The page for installing the OS is displayed.

Note

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

Figure 4-15 HTML Console Page

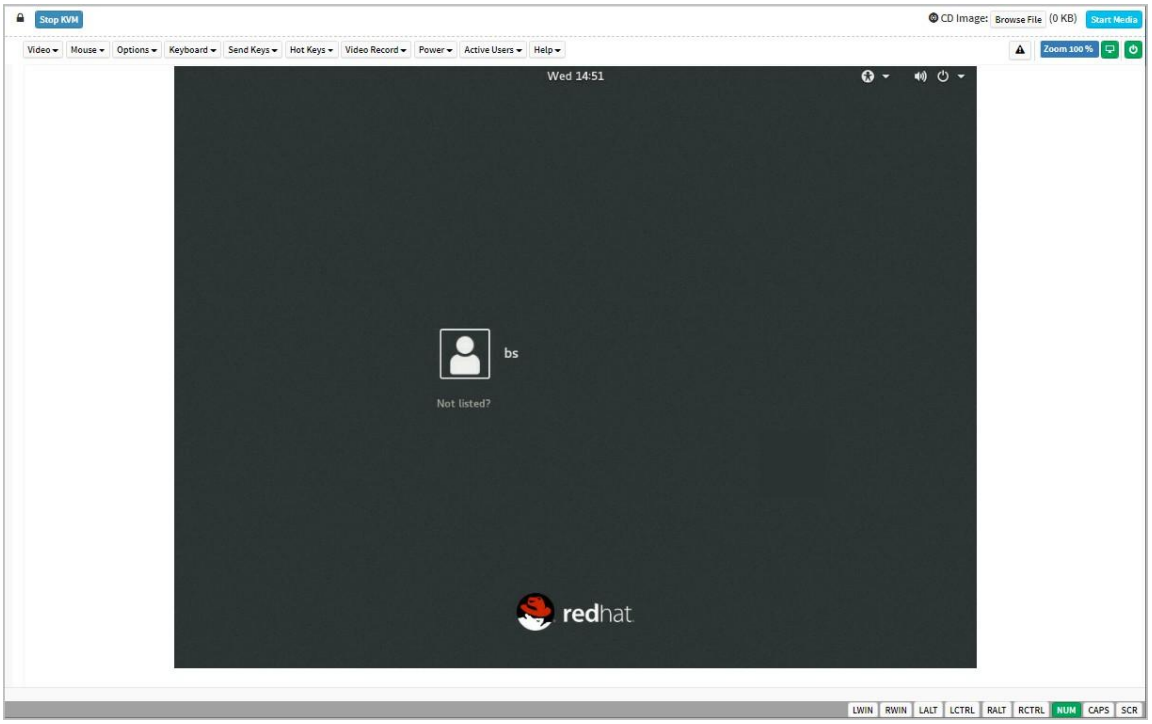
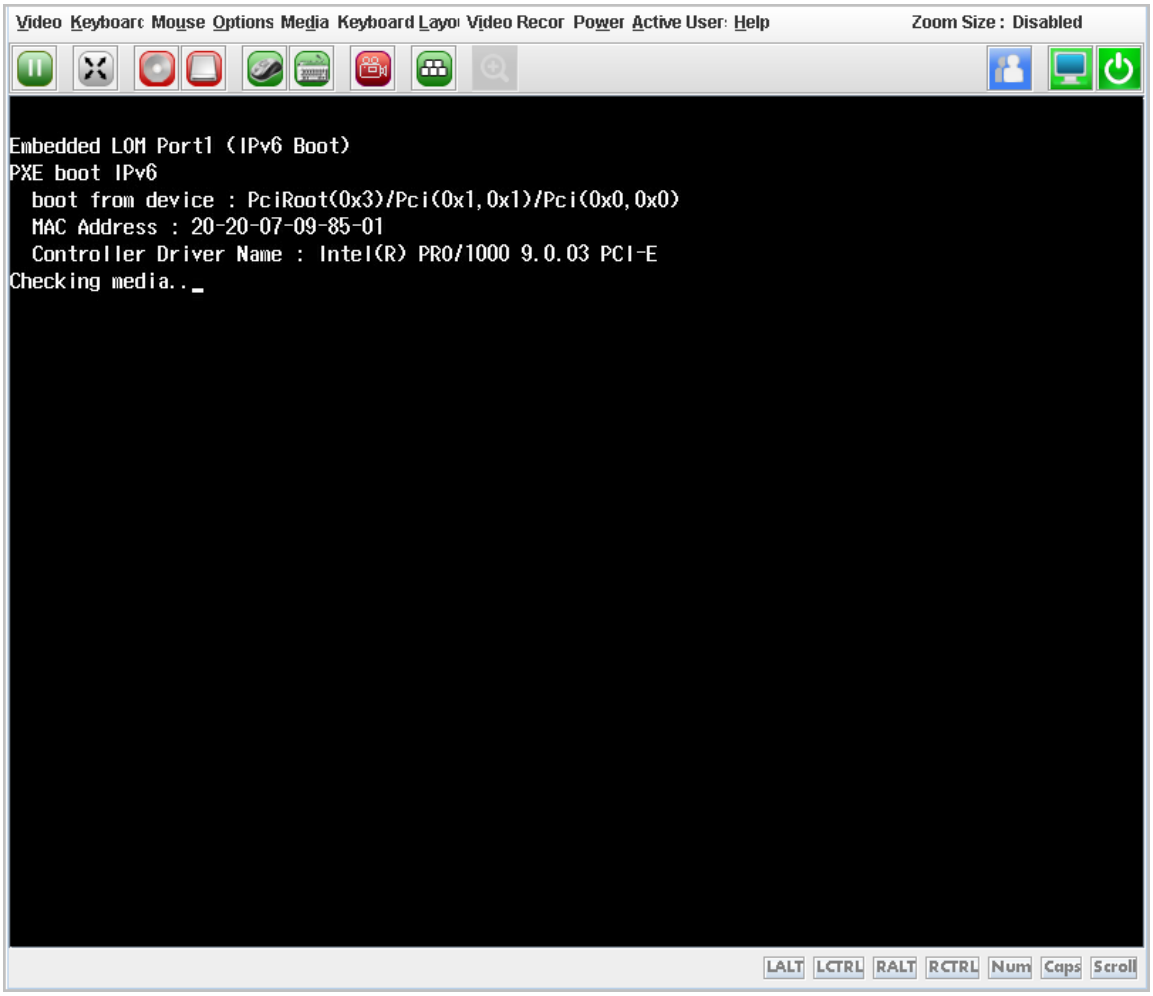


Figure 4-16 Java Console Page



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.

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.

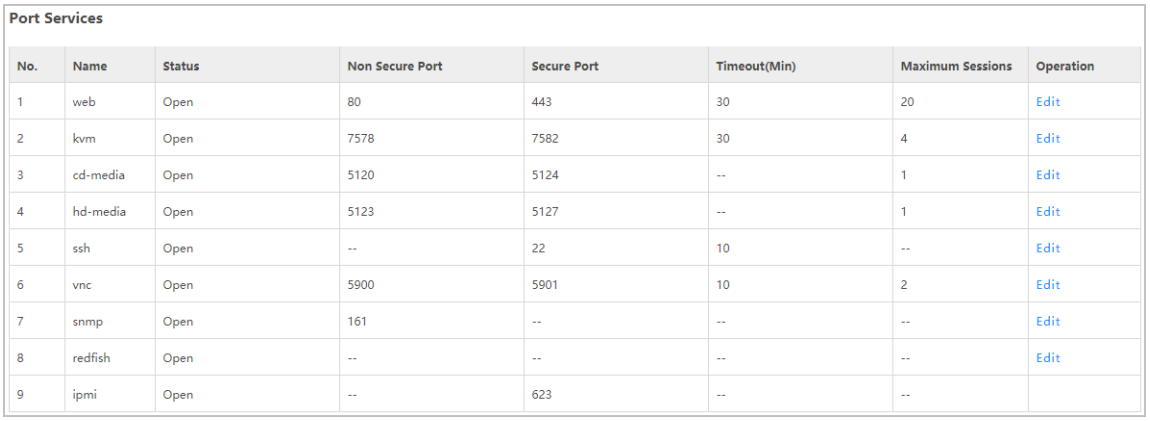
- **kvm**: controls, switches between, and manages multiple devices through a keyboard, display, or mouse, playing an important role in remote scheduling and monitoring.
- **cd-media**: a virtual media service that allows a KVM target server to access files on physical CD/DVD devices on a PC (acting 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 4-17.

Figure 4-17 Port Services Page



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	Enter the non-secure port number of the service. ● Default non-secure port number of the Web service: 80. ● Default non-secure port number of the KVM service: 7578. ● Default non-secure port number of the CD media service: 5120. ● Default non-secure port number of the HD media service: 5123. ● Default non-secure port number of the VNC service: 5900. ● Default non-secure port number of the SNMP service: 161. Other services do not support non-secure ports. Range of the non-secure port numbers: 1–65535.
Secure Port	Enter the secure port number of the service. ● Default secure port number of the Web service: 443. ● Default secure port number of the KVM service: 7582. ● Default secure port number of the CD media service: 5124. ● Default secure port number of the HD media service: 5127. ● Default secure port number of the SSH service: 22. ● Default secure port number of the VNC service: 5901. ● Default secure port number of the IPMI service: 623. Other services do not support secure ports. Range of the secure port numbers: 1–65535.
Timeout(Min)	The service exits if no operation is performed within the specified timeout period. Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).

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 *VANTAGEO Server Redfish Inter- face Description (BMC V4)*. For how to obtain the *VANTAGEO Server Redfish Interface De- scription (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 *VANTAGEO Server SNMP Interface Description (BMC V4)*. For how to obtain the *VANTAGEO Server SNMP Interface Description (BMC V4)* file, refer to 11 Reference: Accessing Documents.

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:

1. Enabling the NTP service: provides the NTP service for the devices whose time needs to be synchronized.
2. Modifying the registry: modifies the registry parameters related to the NTP service.
3. 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

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

Modifying the Registry

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

Table 4-6 Registry Parameter Descriptions

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

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

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**.

Configuring Trap Notification Parameters

Abstract

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

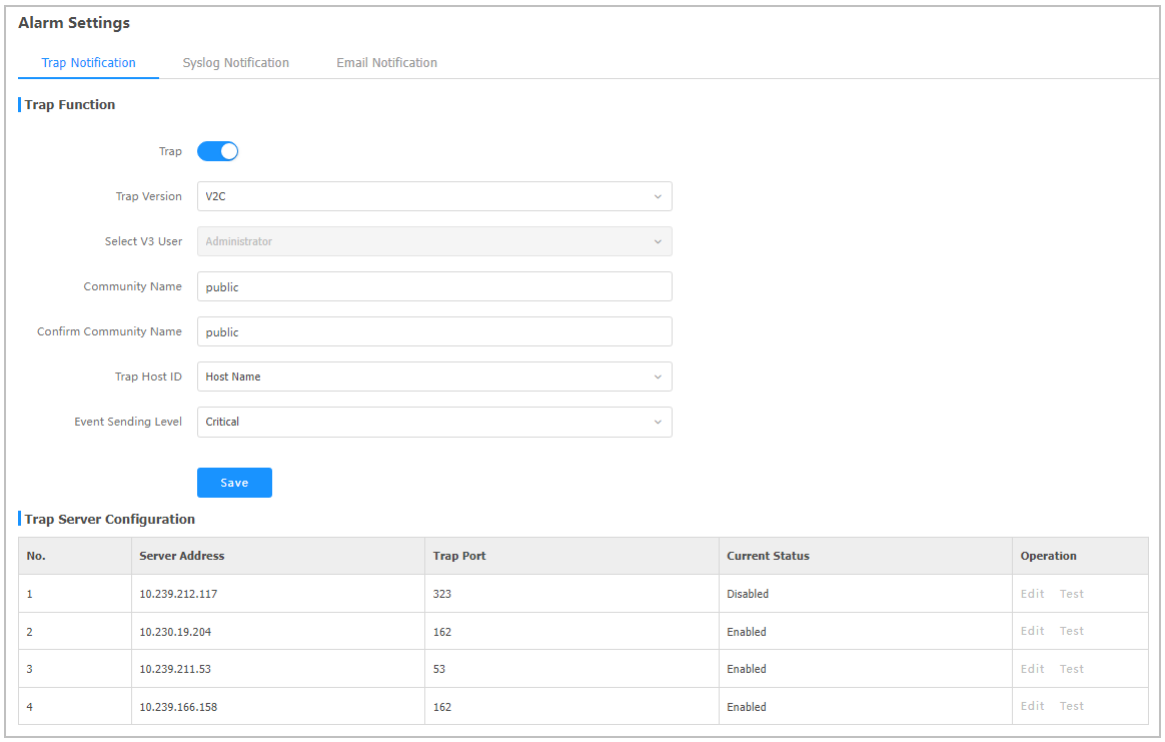
> **Note**
>
> Trap notification parameters are provided by the third-party NMS, so the values of trap notification parameters set on the Web portal of the BMC must be the same as those on the third-party NMS.

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 4-18.

Figure 4-18 Alarm Settings Page



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 **Trap** switch.
Trap Version	Select the SNMP version for traps. Options: **V1**, **V2C**, and **V3**.
Select V3 User	This parameter is required if **Trap Version** is set to **V3**. Select an SNMP user as the alarm sender. For how to create an SNMP user, refer to "4.16 Creating an SNMP User".
Community Name	This parameter is required if **Trap Version** is set to **V1** or **V2C**. Enter the trap community name.
Confirm Community Name	This parameter is required if **Trap Version** is set to **V1** or **V2C**. 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 **Event Sending Level** is set to **Critical**, 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 **Edit**, the parameter is activated. Enter the address of the server that receives alarms. An IPv4 address, IPv6 address, or domain name is supported.
Trap Port	After you click **Edit**, the parameter is activated. Enter the port number of the server that receives alarms. Range: 1–65535.
Current Status	After you click **Edit**, 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.

BMC Log Export

You can export BMC logs in the following ways:

- Exporting logs in one click through the Web portal

  .
- Exporting logs by category through the Web portal
- Exporting logs through SSH commands
- Export logs through a serial port

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.Vantageo.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 4-21.

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

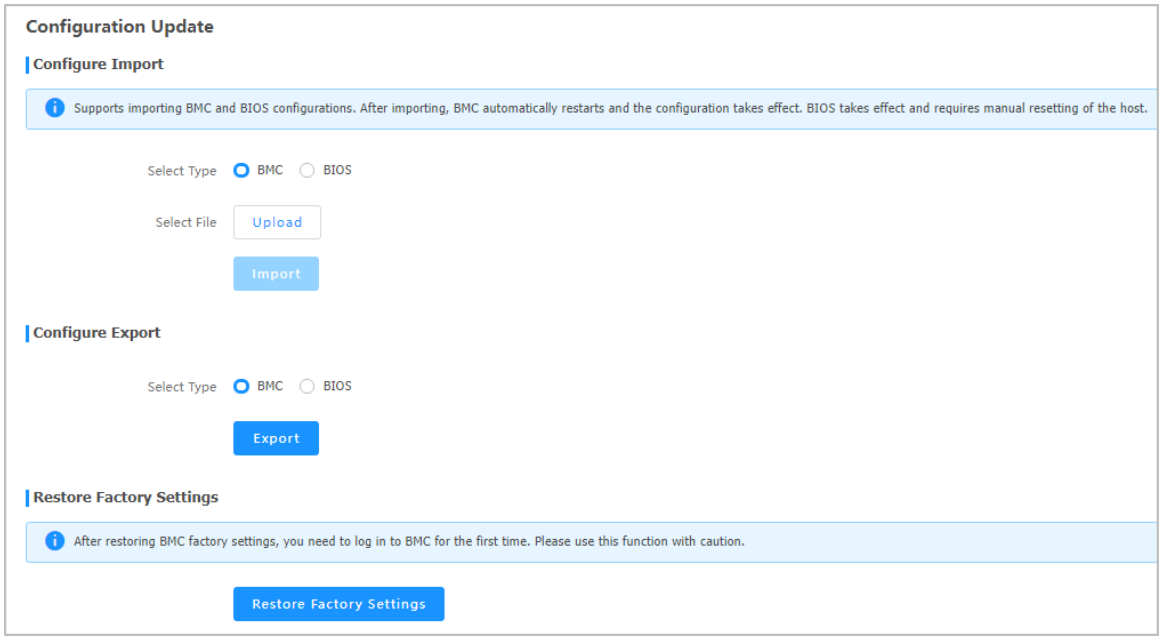
Do not perform any operation during restoration.
After the factory defaults are restored, the BMC will be restarted automatically.

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 4-22.

Figure 4-22 Configuration Update Page



3. Click **Restore Factory Settings**.

Backing Up BMC Configurations

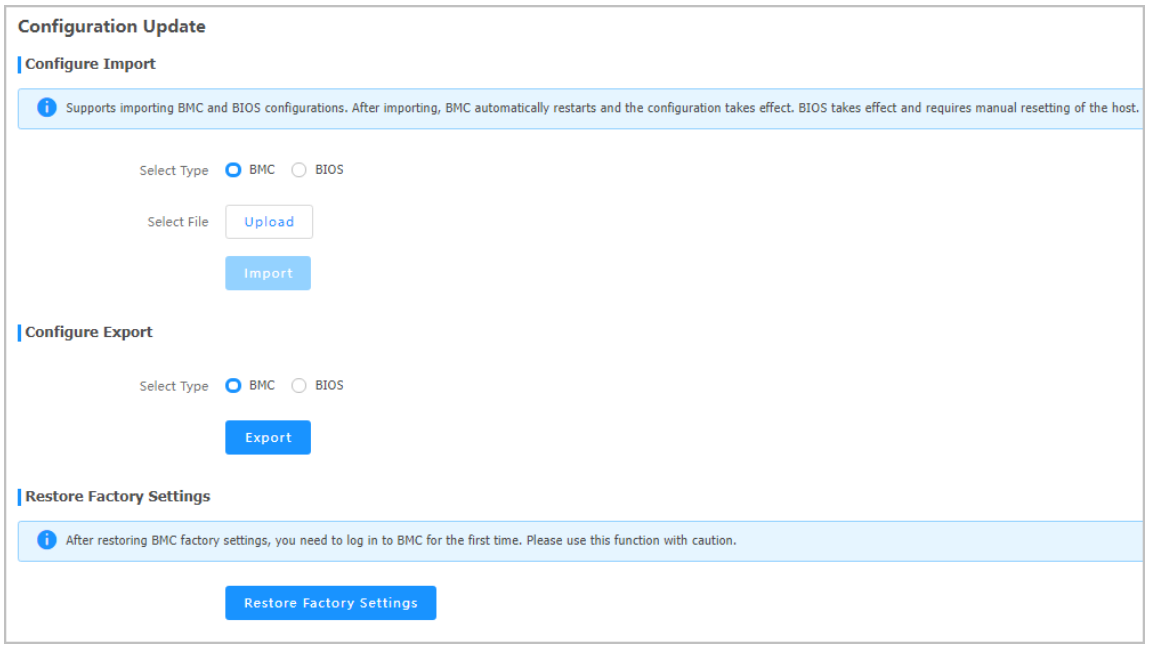
Abstract

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 4-23.

Figure 4-23 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.

1. .

System Management

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.

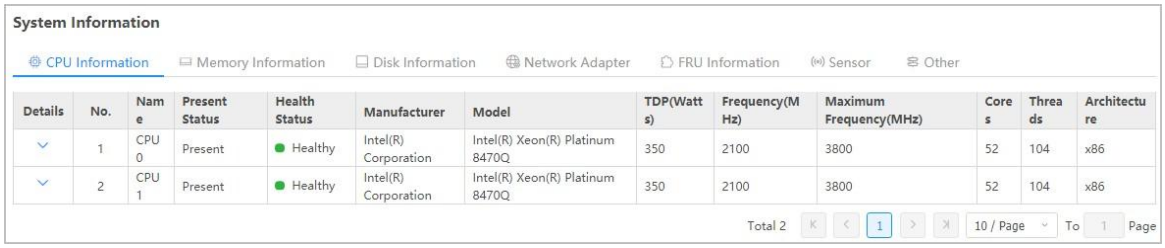
Note

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



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

5.1 Querying Performance Data

Abstract

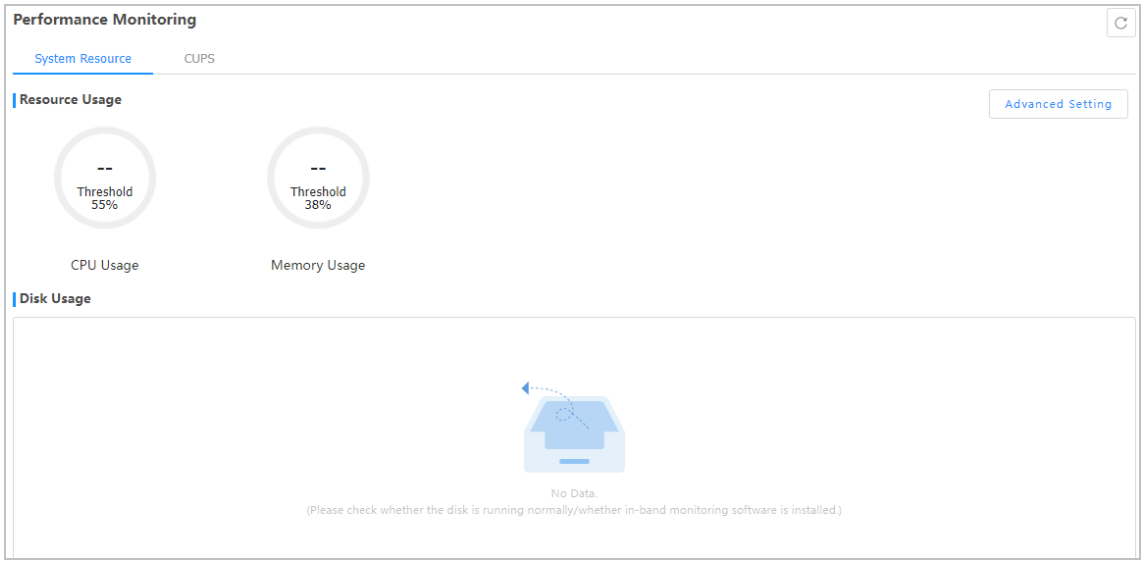
By querying performance data, you can learn about the following information:

- 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

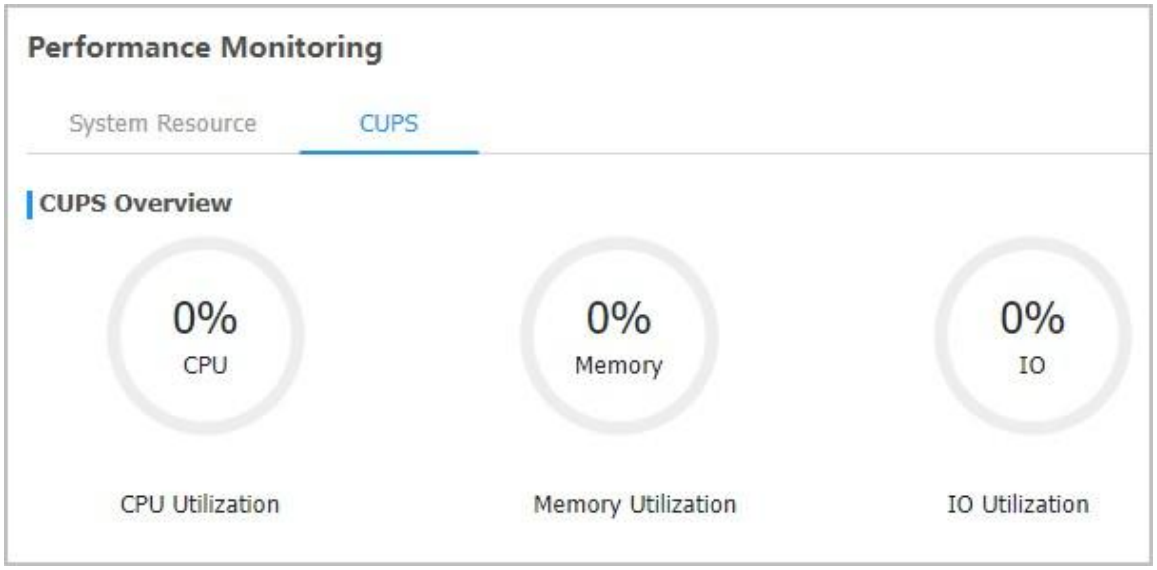


Note

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

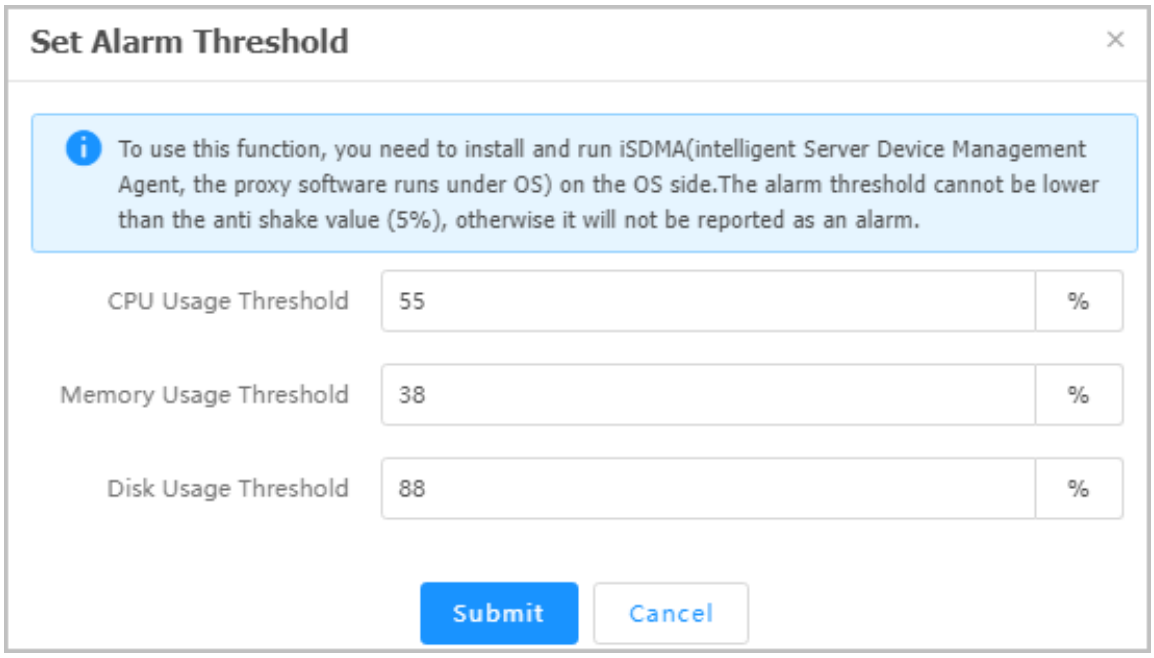
The dynamic CPU, memory, and I/O load ratios are displayed on the above tab.

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**.

Querying Fan Information

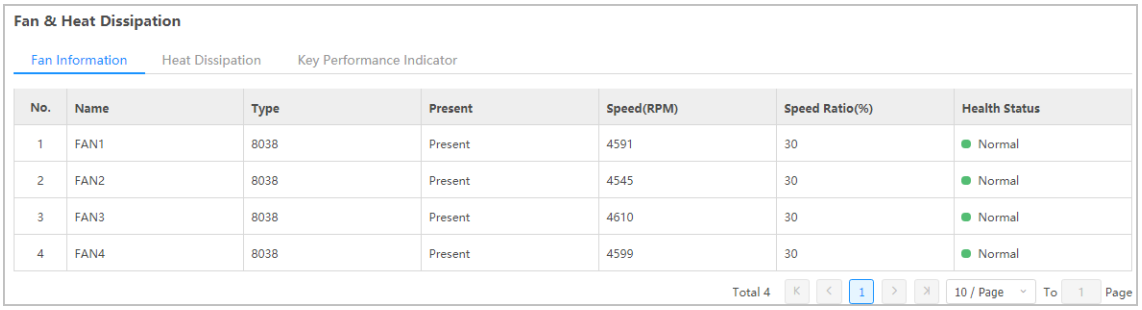
Abstract

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



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.

Configuring the Heat Dissipation Policy

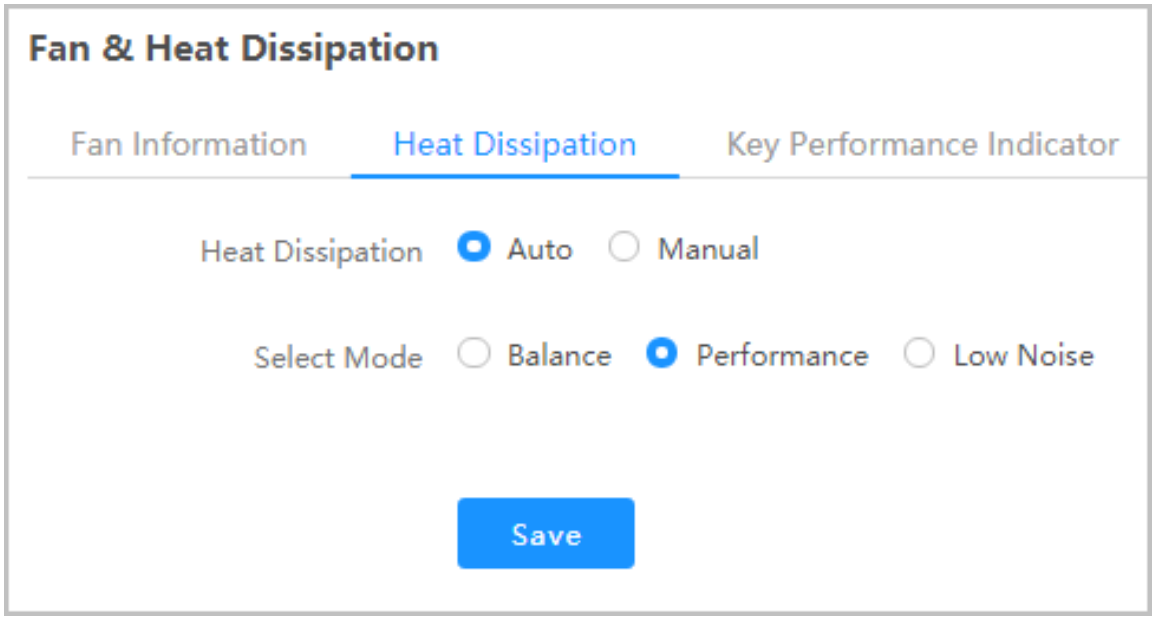
Abstract

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 **Heat Dissipation** to **Auto** and then set **Select Mode** to **Balance**.
Servers are stacked together, and there is no space between them	Set **Heat Dissipation** to **Auto** and then set **Select Mode** to **Performance**.
The server is placed in an office or other areas that are sensitive to noise	Set **Heat Dissipation** to **Auto** and then set **Select Mode** to **Low Noise**.
The fan speed needs to be set manually for the server	Set **Heat Dissipation** to **Manual** and then set **Speed Ratio**.

Note

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

5. Click **Save**.

Querying Temperature KPIs

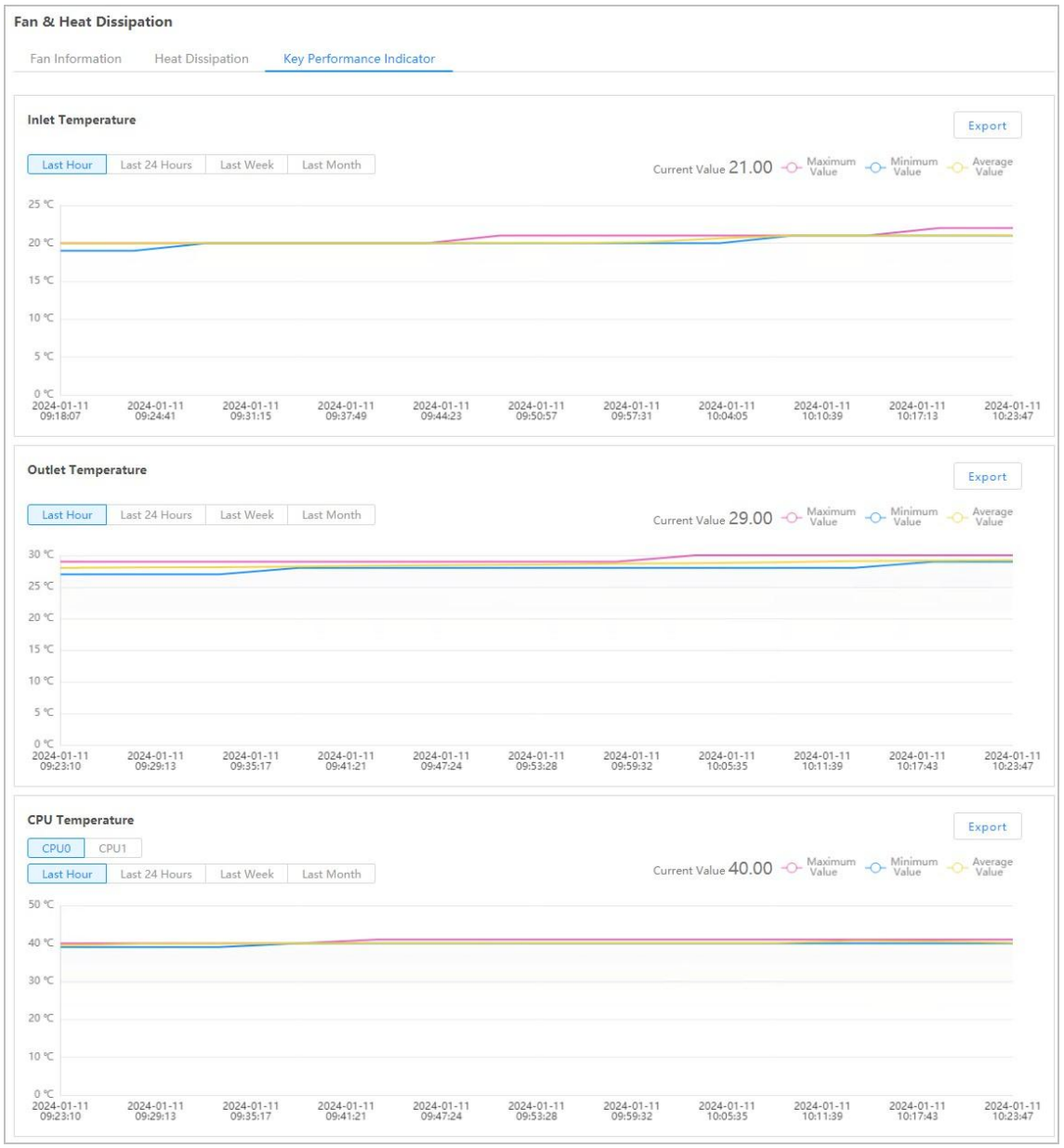
Abstract

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**.

Managing Storage Devices

Abstract

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

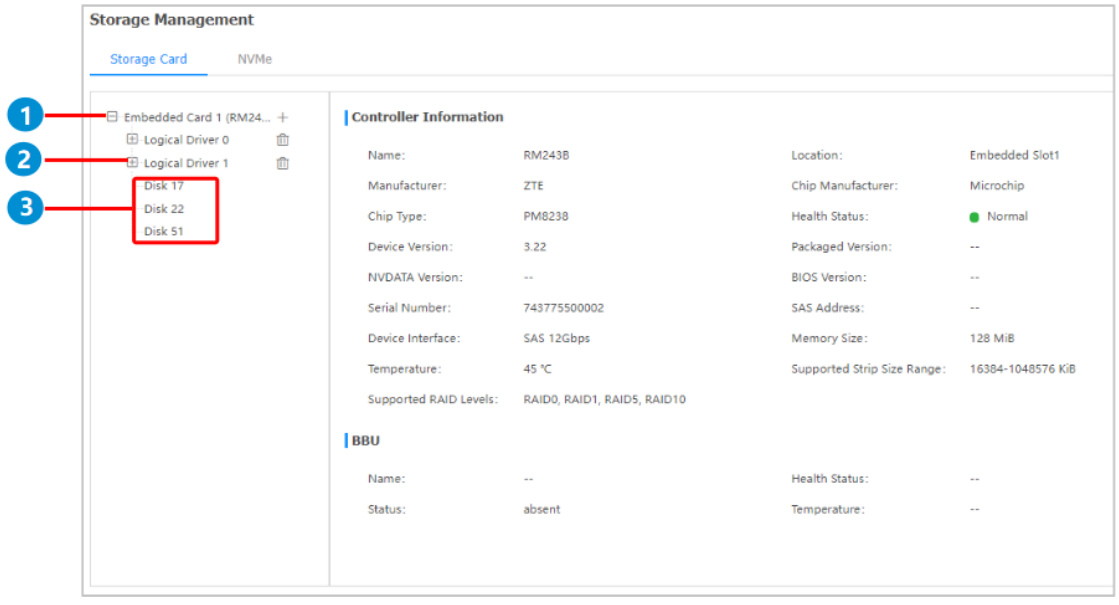
The physical disks managed by a RAID controller can be created as logical disks.

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

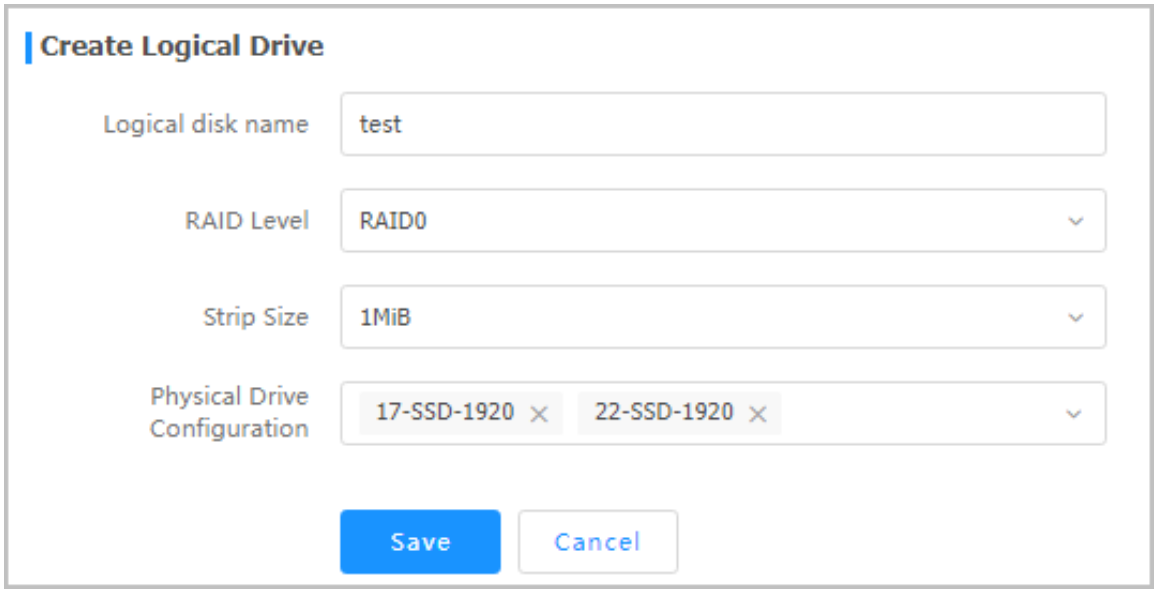


1. RAID controller
2. Logical disk
3. Physical disk

3. Perform the following operations as required.

To...	Do...
Check RAID controller and BBU information	On the **Storage Card** tab, click the desired RAID controller. The RAID controller and BBU information is displayed on the right.
Check logical disk information	On the **Storage Card** tab, click the desired logical disk. The detailed logical disk information is displayed on the right. In the logical disk information, **Status** includes: ● **Optimal** ● **Degraded** ● **Part Degraded** ● **Offline**
Set the UID indicator of a logical disk	a. On the **Storage Card** tab, click the desired logical disk. b. Click **Settings** on the right. The **Logical Drive Setting** dialog box is displayed. c. Select **Open** or **Close**. ● **Open**: lights up the UID indicators of all member disks of the logical disk. ● **Off**: lights off the UID indicators of all member disks of the logical disk. d. Click **Submit**.
Check physical disk information	On the **Storage Card** tab, click the desired physical disk. The detailed physical disk information is displayed on the right.
Create a logical disk	a. On the **Storage Card** tab, click **+** next to a RAID controller. The **Create Logical Drive** area is displayed on the right, see Figure 5-9. b. Configure the following parameters: ● **Logical disk name**: Enter the name of the logical disk. ● **RAID Level**: Select the corresponding RAID level. ● **Stripe Size**: Select a stripe size. ● **Physical Drive Configuration**: Select the member disks that form the logical disk. c. Click **Save**.
Check NVMe disk information	On the **Storage Management** page, click **NVMe** to switch to the **NVMe** tab. The detailed NVMe disk information is displayed.

Figure 5-9 Create Logical Drive Area



Note

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

5.2 Powering On/Off the Server

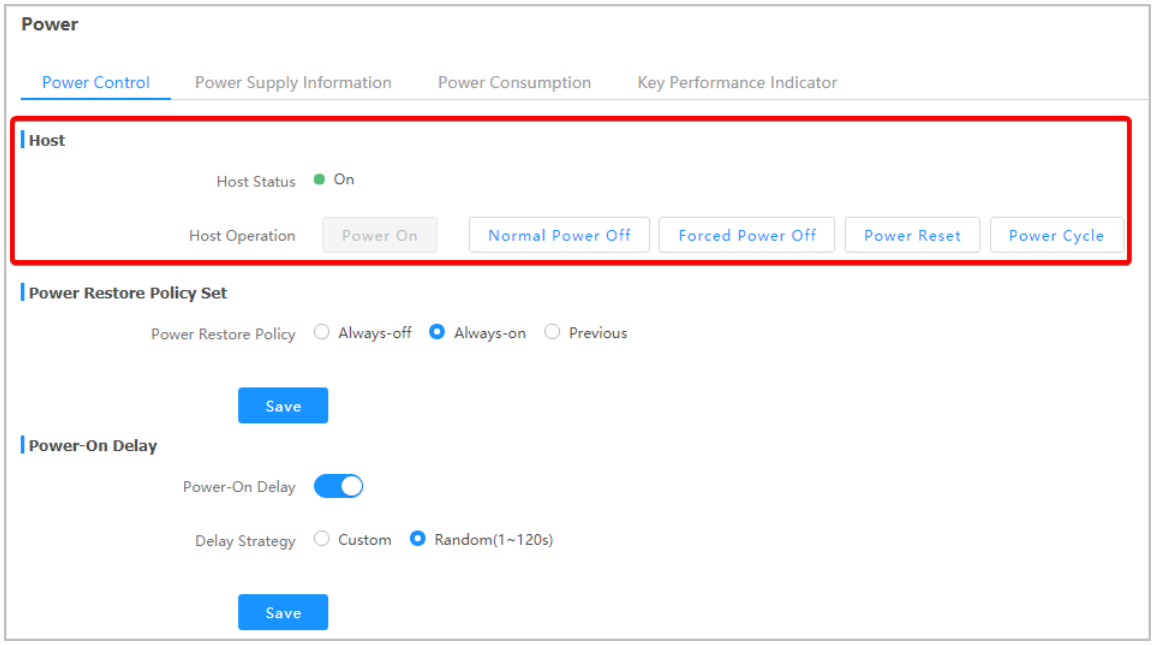
Abstract

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 **Power On**.
Power off the server	Click **Normal Power Off**. The prerequisite for selecting **Normal Power Off** to shut down the server is that **When the Power Button is Pressed** in the OS of the server is already set to **Power Off**. For details, refer to Related Tasks.
Forcibly power off the server	Click **Forced Power Off**.
Perform a warm reboot	Click **Power Reset**. 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 **Power Cycle**. 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.

Related Tasks

To set **When the Power Button is Pressed** to **Power Off**, perform the following operations:

Note

This procedure uses the Red Hat OS as an example. For other OSs, the operations are similar.
If an OS does not have a GUI, you need to install the ACPI service.

1. Log in to the OS through KVM.

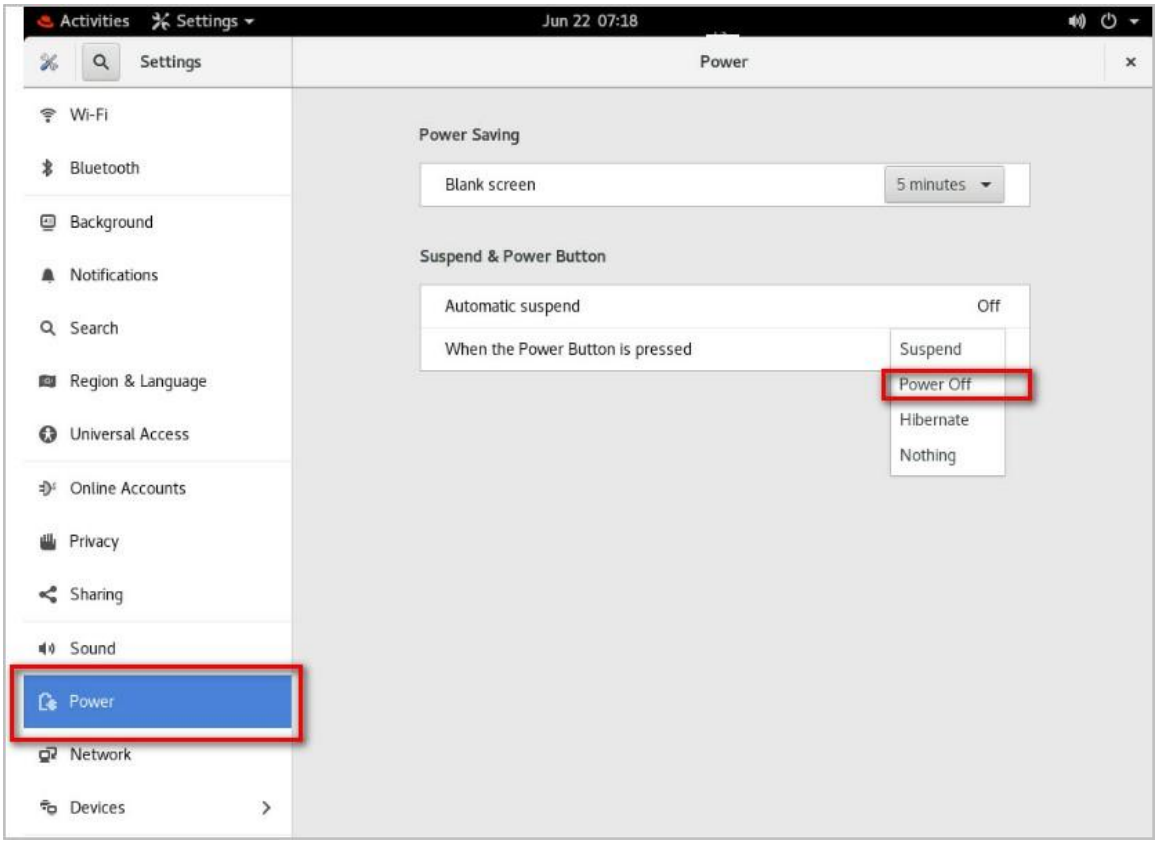
   If the screen is locked, you need to enter the password to log in to the OS.

2. Click . The **Activities** screen is displayed, as shown in Figure 5-11.

Figure 5-11 Activities Screen

3. Click **Settings**. The **Settings** screen is displayed, as shown in Figure 5-12.

Figure 5-12 Settings Screen



4. Set **When the Power Button is Pressed** to **Power Off**.

Configuring the Server Startup Policy

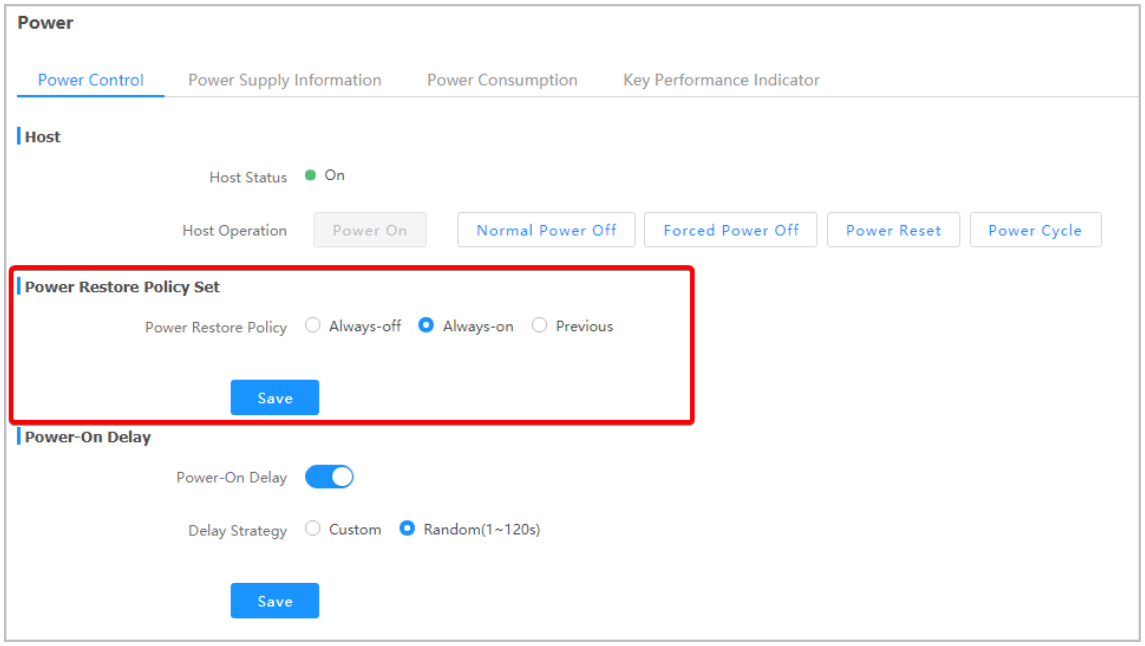
Abstract

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 5-13.

Figure 5-13 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**.

Configuring Power-On Delay Parameters

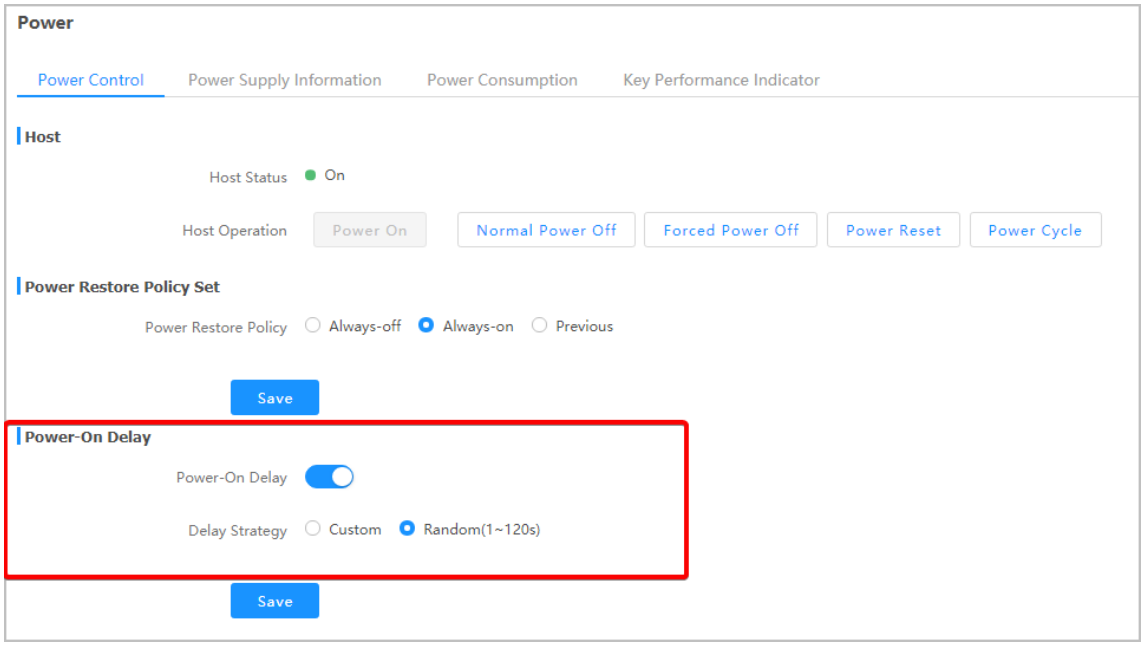
Abstract

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 5-14.

Figure 5-14 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. ● To enable the power-on delay function, turn the switch on. ● To disable the power-on delay function, turn the switch off.
Delay Strategy	Select the corresponding power-on delay mode. ● **Custom**: The power-on delay time is user-defined. If **Custom** is selected, set **Custom Delay Duration**. Range: 1–120, unit: seconds. ● **Random**: The power-on delay time is automatically generated by the system.

4. Click **Save**.

5.3 Querying Power Supply Information

Abstract

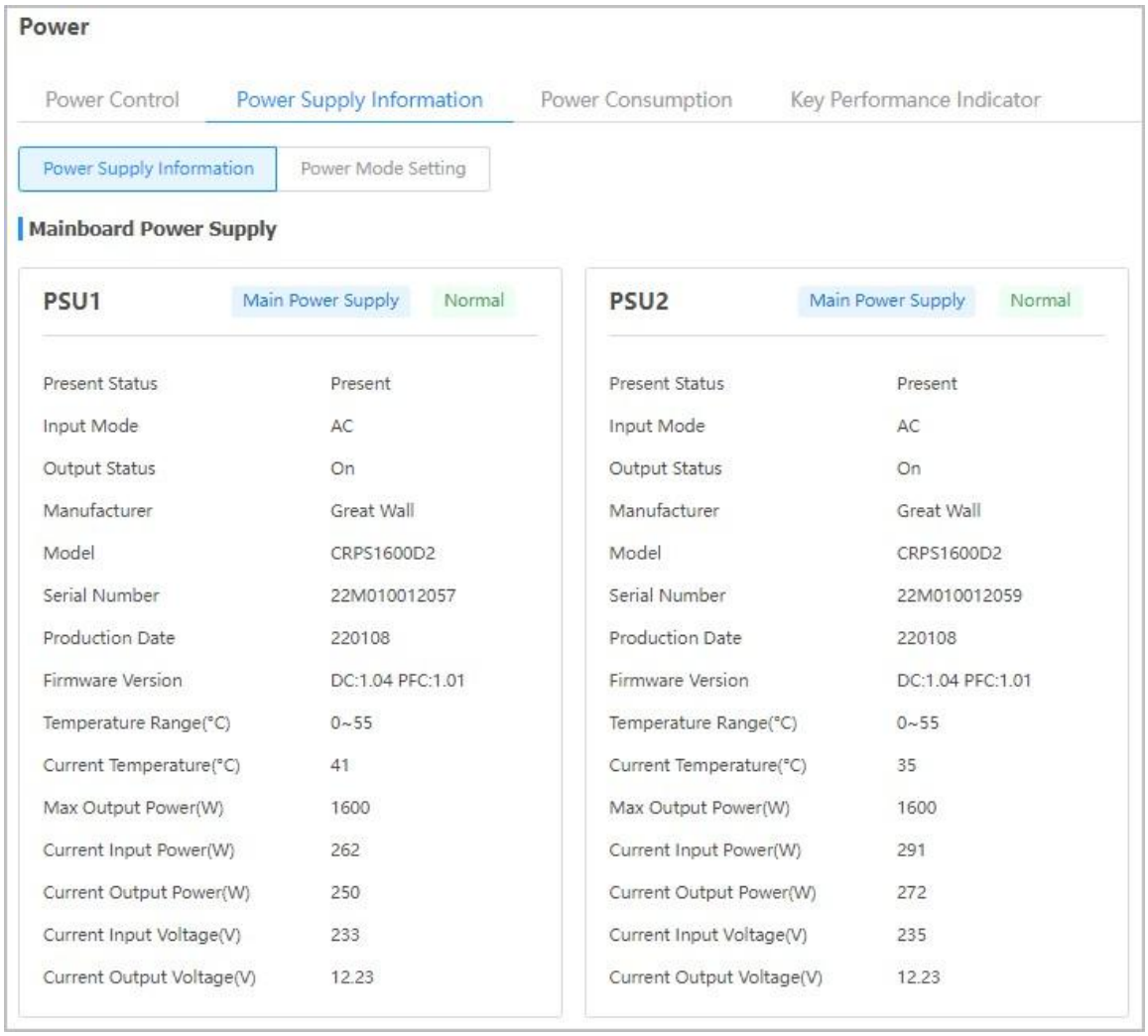
By querying power supply information, you can learn about the power supplies of the server.

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 5-15.

Figure 5-15 Power Supply Information Tab



Note

The power supply input modes include: AC, HVDC and LVDC.
For the R6900 G5 model, **Power Supply Information** also includes the power supply information about the GPU module.

Configuring the Power Mode

Abstract

The server power modes include:

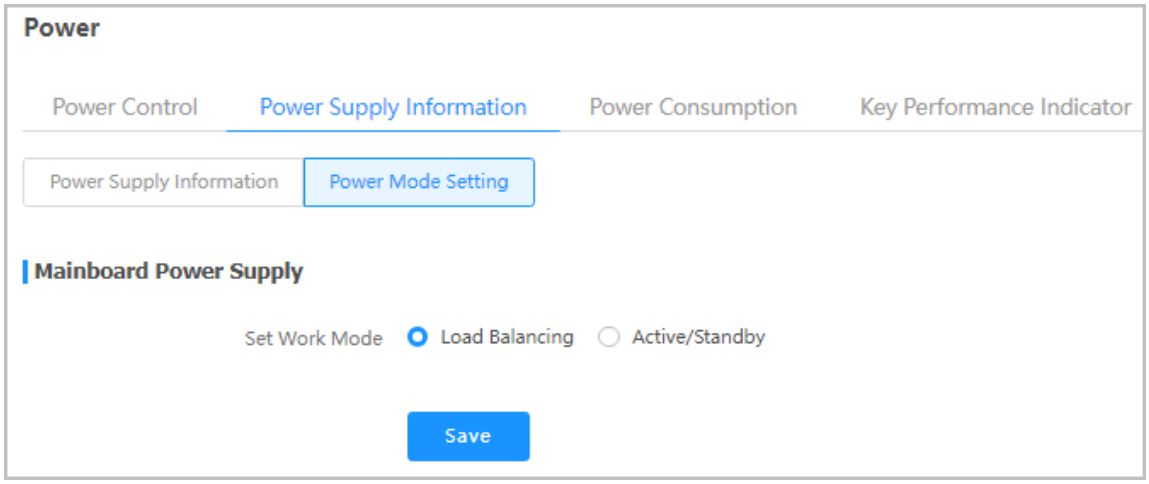
- **Load Balancing**: The power modules supply power in load-balancing mode.
- **Active/Standby**: The power modules supply power in active/standby mode.

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 5-16.

Figure 5-16 Power Mode Setting Tab



5. Click **Save**.

Querying Power Statistics

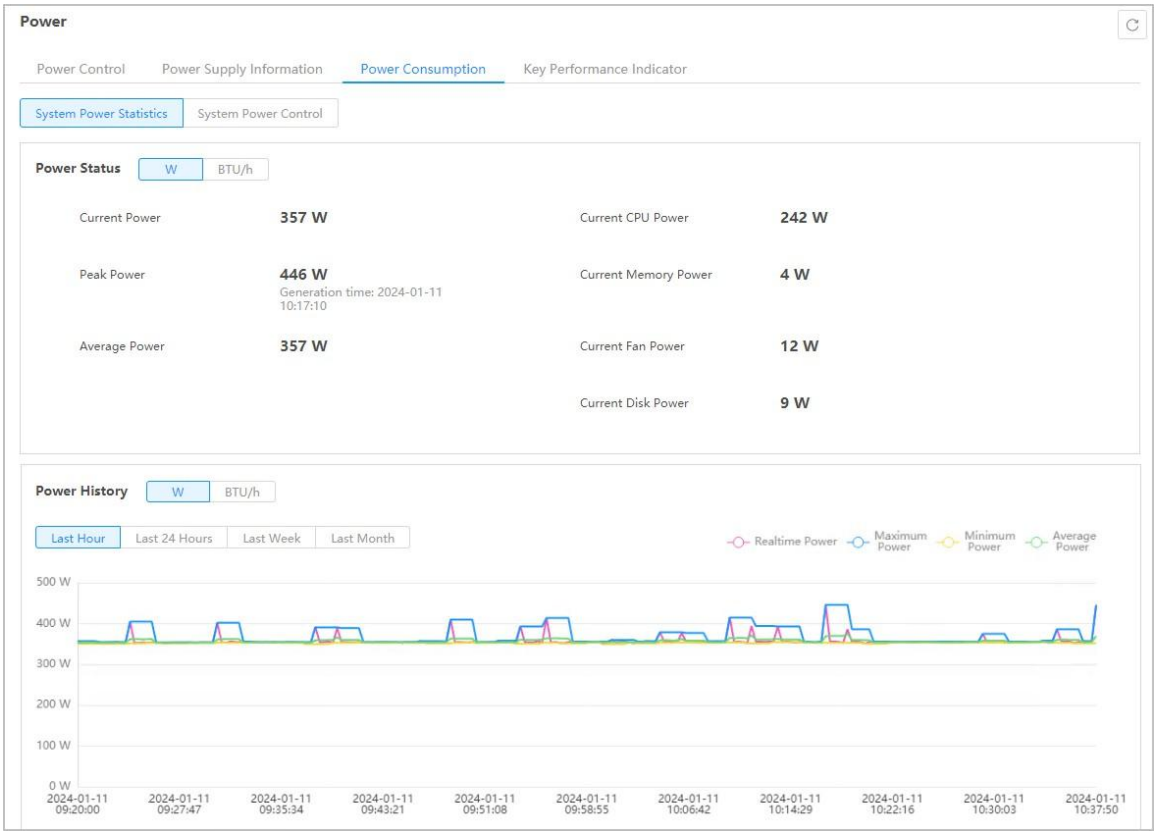
Abstract

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 5-17.

Figure 5-17 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.

Configuring Power Control Parameters

Abstract

The power control parameters include:

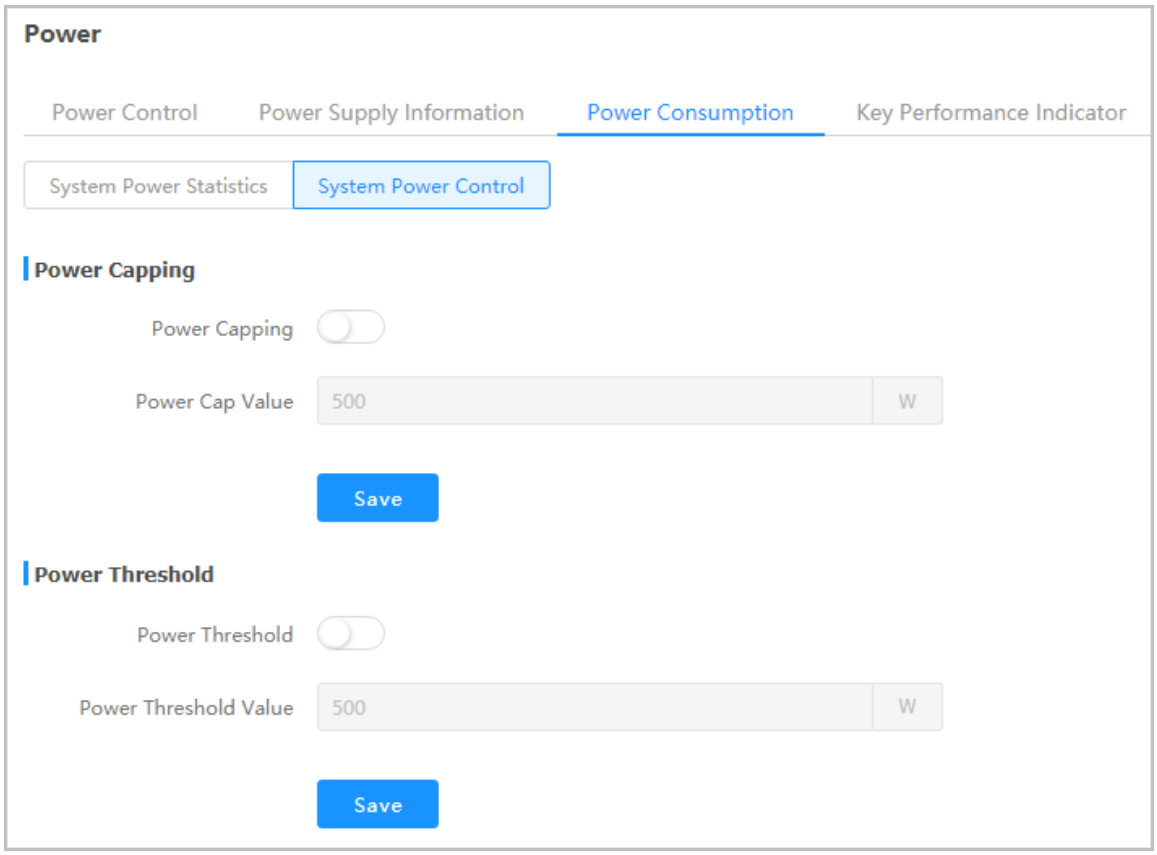
- **Power Capping**: The server power is limited to the power cap.
- **Power Threshold**: An alarm is raised when the server power exceeds the threshold.

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 5-18.

Figure 5-18 System Power Control Tab



5. Perform the following operations as required.

To…	Do…
Set the power cap	a. In the **Power Capping** area, turn on the **Power Capping** switch. b. In the **Power Cap Value** text box, set the power cap (range: 1–32767, unit: W). c. Click **Save**.
Set the power threshold	a. In the **Power Threshold** area, turn on the **Power Threshold** switch. b. In the **Power Threshold Value** text box, enter the power threshold (range: 5–32767, unit: W). c. Click **Save**.

Querying Power KPIs

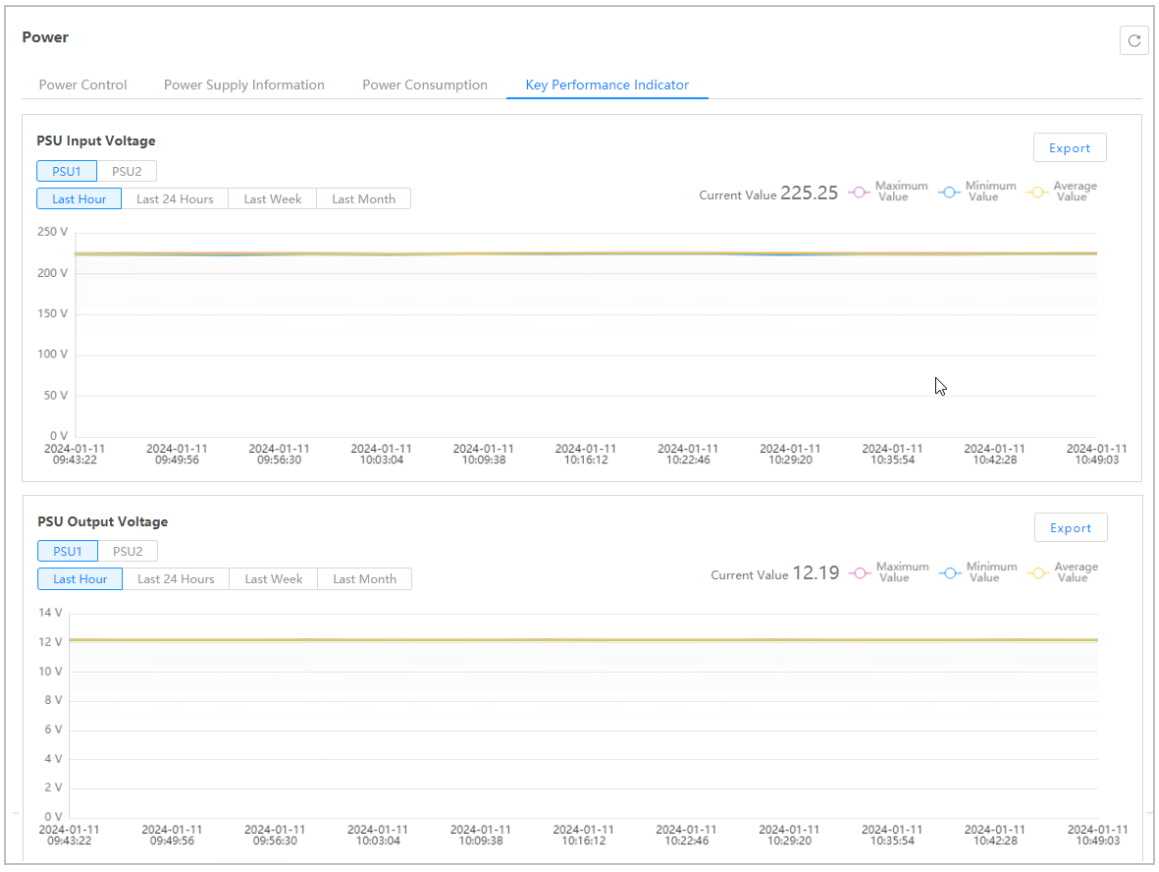
Abstract

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 5-19.

Figure 5-19 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**.

Configuring Boot Options

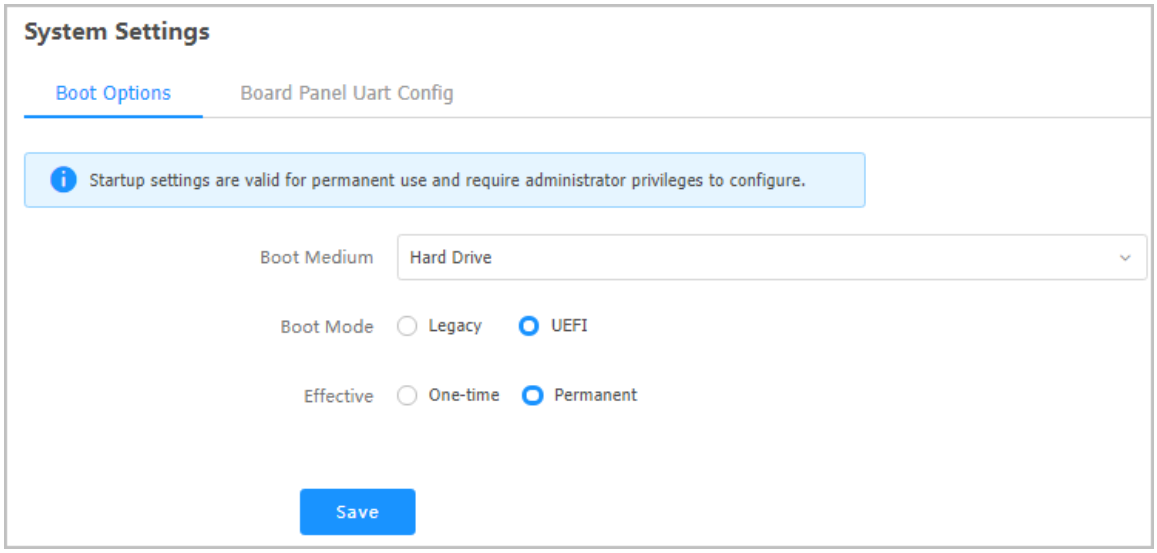
Abstract

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 5-20.

Figure 5-20 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. ● **No Override**: configures no boot device and uses the default boot device configured in the BIOS. ● **Hard Drive**: forcibly boots from a hard drive. ● **PXE**: forcibly boots from the PXE. ● **CD/DVD**: forcibly boots from the CD-ROM or DVD-ROM drive. ● **BIOS Setup**: enters the BIOS menu after the server is booted. ● **FDD/Removable Device**: forcibly boots from a floppy drive or removable device (for example, USB).
Boot Mode	Select a server boot mode.

Parameter	Setting
	● **Legacy**: a traditional boot mode with certain limitations, which supports the PXE boot only through a CPU-connected NIC. ● **UEFI**: a newer boot mode, which supports the PXE function in an IPv6/IPv4 network and provides the UEFI Shell environment. UEFI mode is recommended.
Effective	Select whether the reconfigured server boot options are applied to the current restart only. ● **One-time**: only effective for the current restart. ● **Permanent**: permanently effective.

4. Click **Save**.

Configuring the Serial Port Output Mode

Abstract

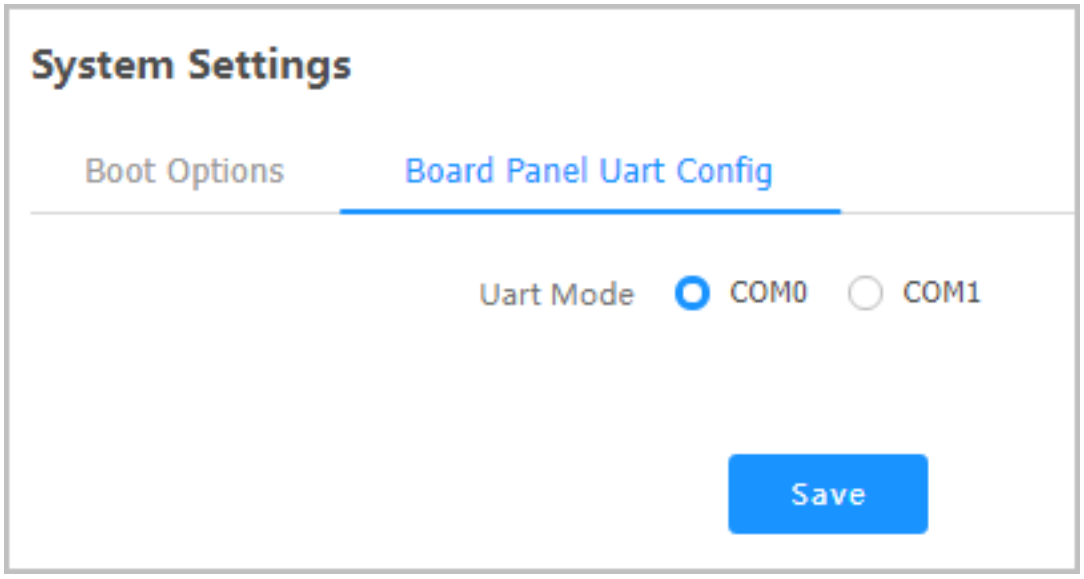
The serial port output modes on the panel include:

- COM0: The recorded information in the BIOS phase is output, which can be configured in the BIOS.
- COM1: 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 5-21.

4. **Figure 5-21 Board Panel Uart Config Tab**



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

Diagnosis and Maintenance

Querying Alarms

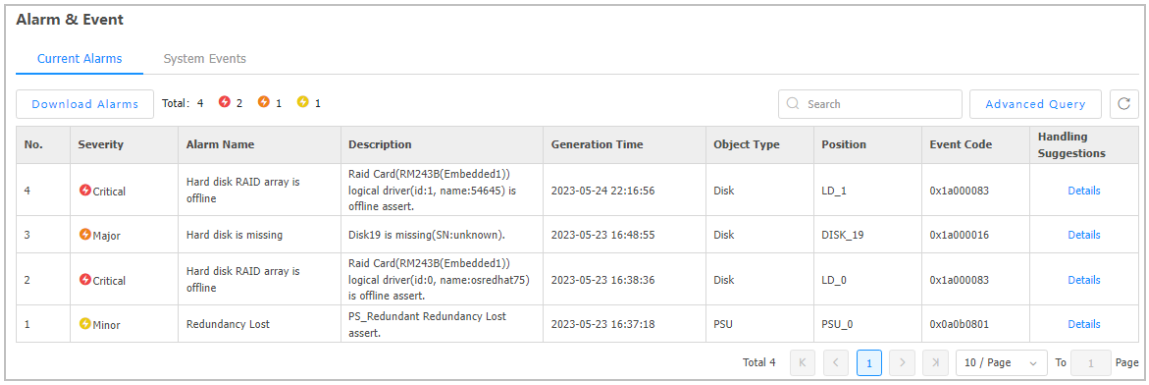
Abstract

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



3. Perform the following operations as required.

To…	Do…
Query alarms by keyword	In the **Search** box, enter a keyword.
Query alarms based on the advanced parameters	a. Click **Advanced Query**. Advanced query conditions are displayed. b. Set the query parameters. c. Click **Query**.
View the handling suggestions for an alarm	Click **Details** for the alarm.
Save alarm information to the local PC	Click **Download Alarms**.
Query system events	Click **System Events**. The **System Events** tab is displayed.

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.

Configuring Trap Notification Parameters

Abstract

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

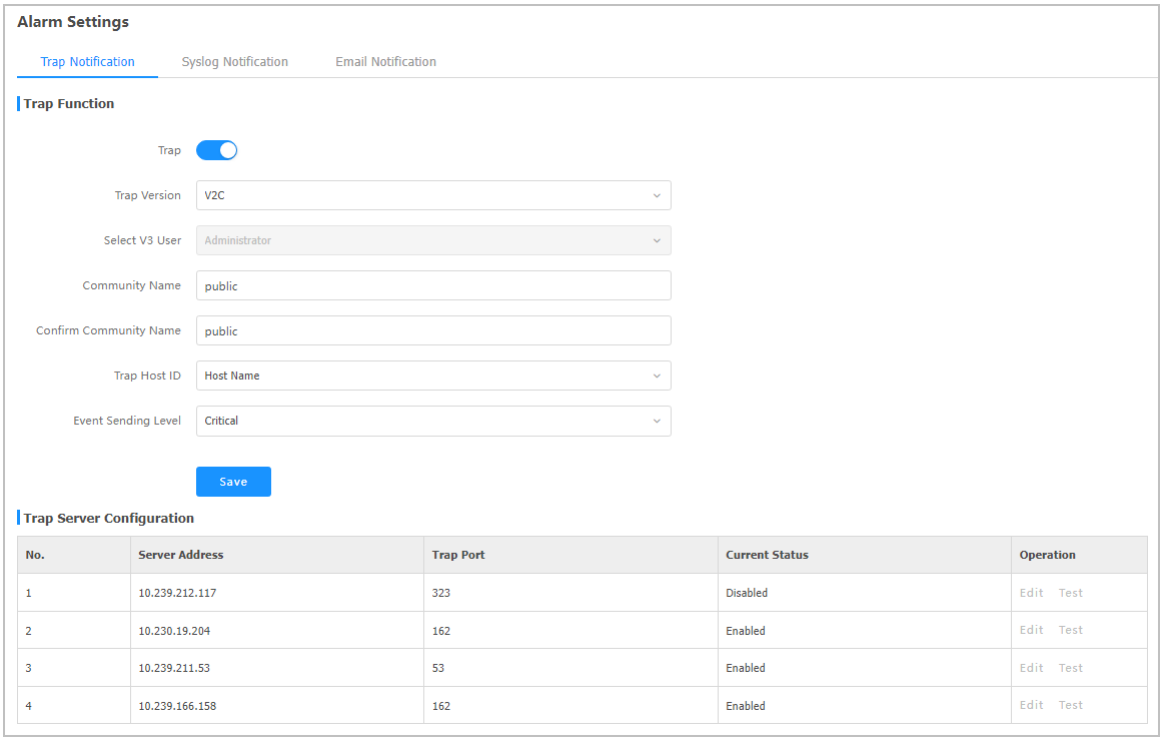
Note

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



3. 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

Parameter	Setting
Trap	Turn on the **Trap** switch.
Trap Version	Select the SNMP version for traps. Options: **V1**, **V2C**, and **V3**.

Parameter	Setting
Select V3 User	This parameter is required if **Trap Version** is set to **V3**. Select a user that has permission to send alarms through SNMP. For how to create an SNMP user, refer to "4.16 Creating an SNMP User".
Community Name	This parameter is required if **Trap Version** is set to **V1** or **V2C**. Enter the trap community name.
Confirm Community Name	This parameter is required if **Trap Version** is set to **V1** or **V2C**. 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 **Event Sending Level** is set to **Critical**, 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 **Edit**, the parameter is activated. Enter the address of the server that receives alarms. An IPv4 address, IPv6 address, or domain name is supported.
Trap Port	After you click **Edit**, the parameter is activated. Enter the port number of the server that receives alarms. Range: 1–65535.
Current Status	After you click **Edit**, 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.

Configuring Syslog Notification Parameters

Abstract

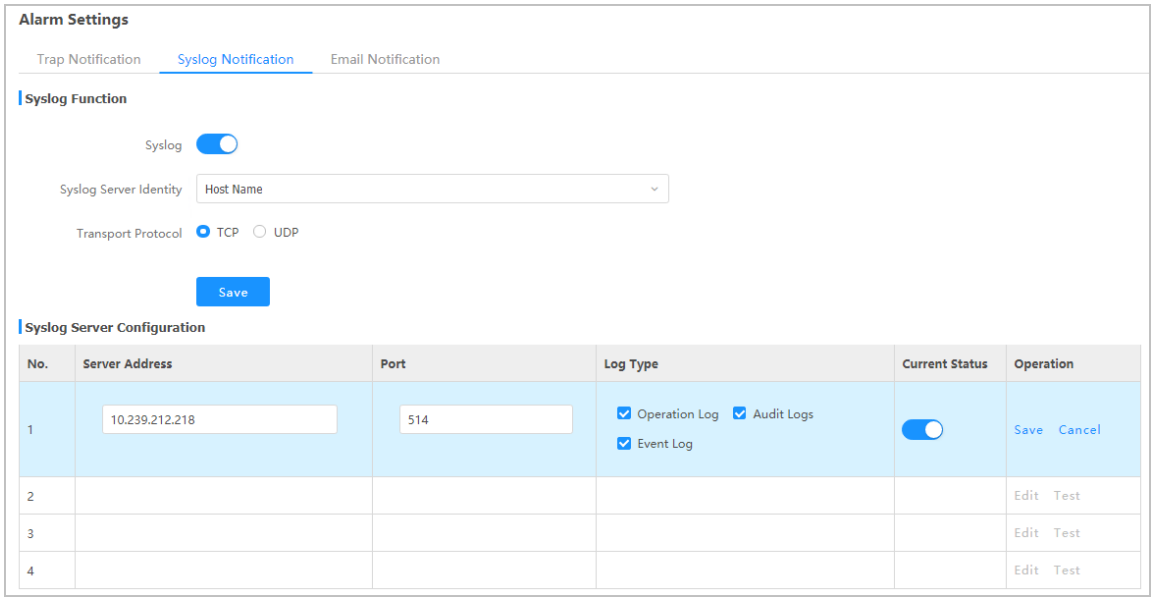
This procedure describes how to configure syslog notification parameters so that the BMC can send logs to the syslog server. The sent logs include:

- **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

8. Select **Maintenance**. The **Maintenance** page is displayed.
9. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
10. Click **Syslog Notification**. The **Syslog Notification** tab is displayed, see Figure 6-3.

Figure 6-3 Syslog Notification Tab



11. 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 **Syslog** switch.
Syslog Server Identity	Select the identifier of the syslog server to which logs are sent.
Transport Protocol	Select a log transmission protocol.

12. Click **Save**.
13. 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 **Edit**, the parameter is activated. Enter the address of the syslog server. An IPv4 address, IPv6 address, or domain name is supported.
Port	After you click **Edit**, the parameter is activated. Enter the port number of the syslog server. Range: 1–65535, default: 514.
Log Type	After you click **Edit**, the parameter is activated. Select one or more log types.
Current Status	After you click **Edit**, the parameter is activated. Select whether to enable the current syslog server to receive logs.

14. Click **Save**.

Note

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

15. (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.

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

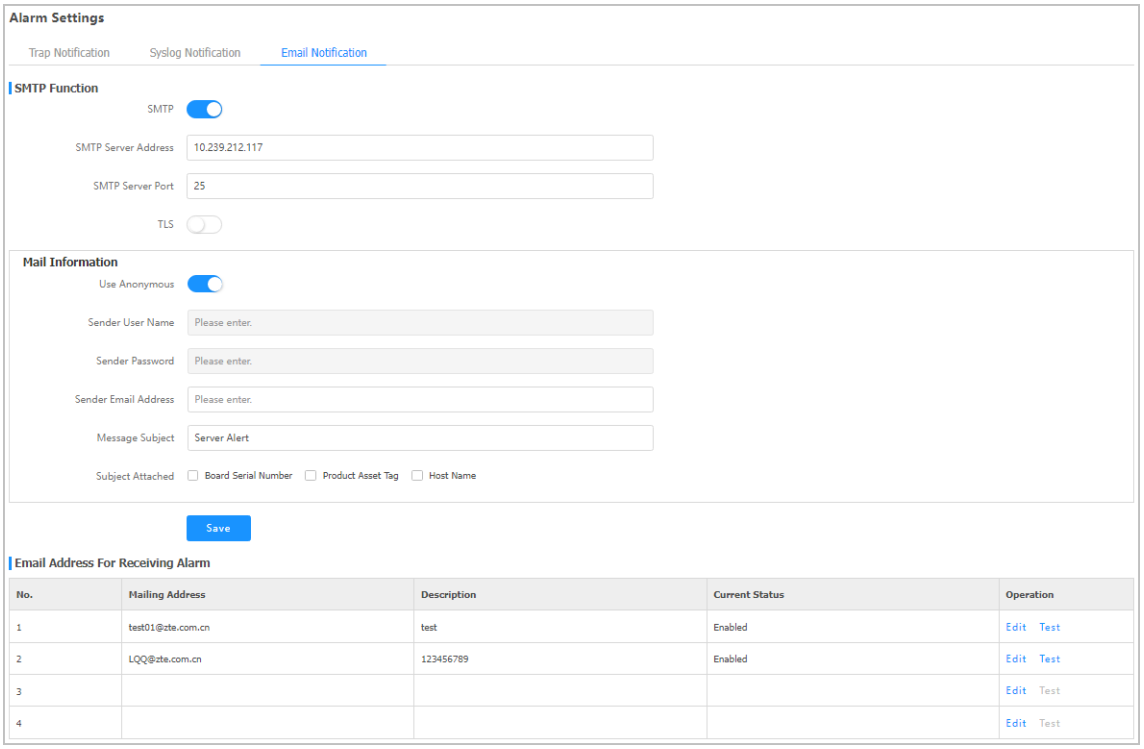
An SMTP server is already deployed. For details, refer to 4.10 Configuring an SMTP Server.

Abstract

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

17. From the navigation tree in the left pane, select **Alarm Settings**. The **Alarm Settings** page is displayed.
18. Click **Email Notification**. The **Email Notification** tab is displayed, see Figure 6-4.

Figure 6-4 Email Notification Tab



19. 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 **SMTP** switch.
SMTP Server Address	Enter the IP address of the SMTP server in IPv4 or IPv6 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 **Use Anonymous** switch is turned off. Enter the username for SMTP authentication.
Sender Password	Required if the **Use Anonymous** 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.

20. Click **Save**.
21. 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 **Edit**, the parameter is activated. Enter the email address to which alarms are sent.
Description	After you click **Edit**, the parameter is activated. Enter the description of the email address.
Current Status	After you click **Edit**, the parameter is activated. Select whether to enable the current email address to receive alarms.

22. Click **Save**.

Note

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

23. (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.

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".

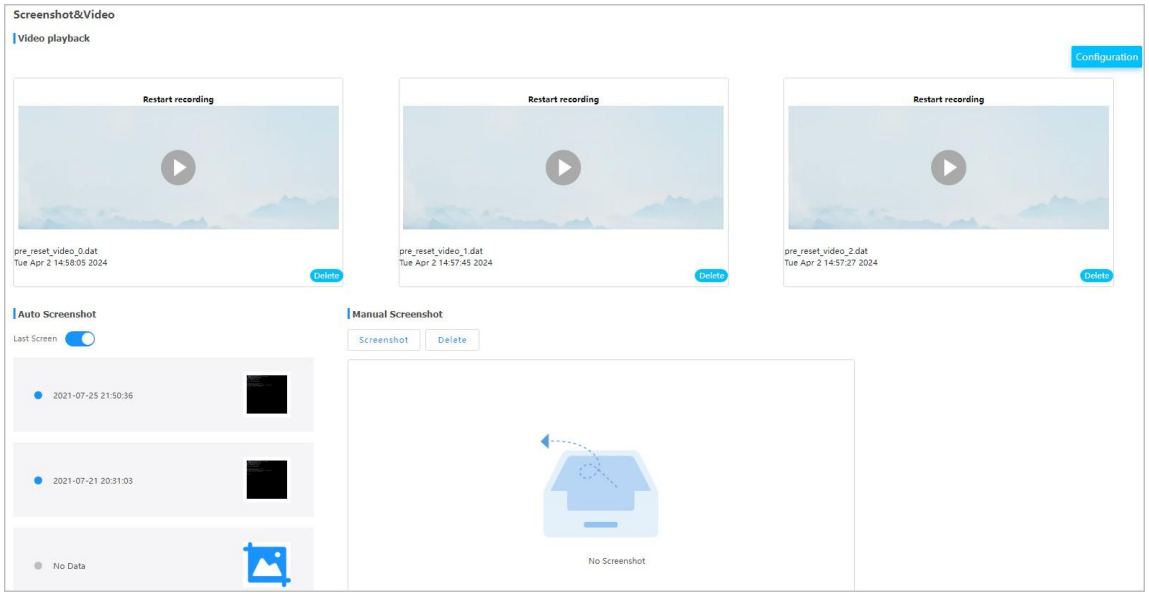
Note

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

Steps

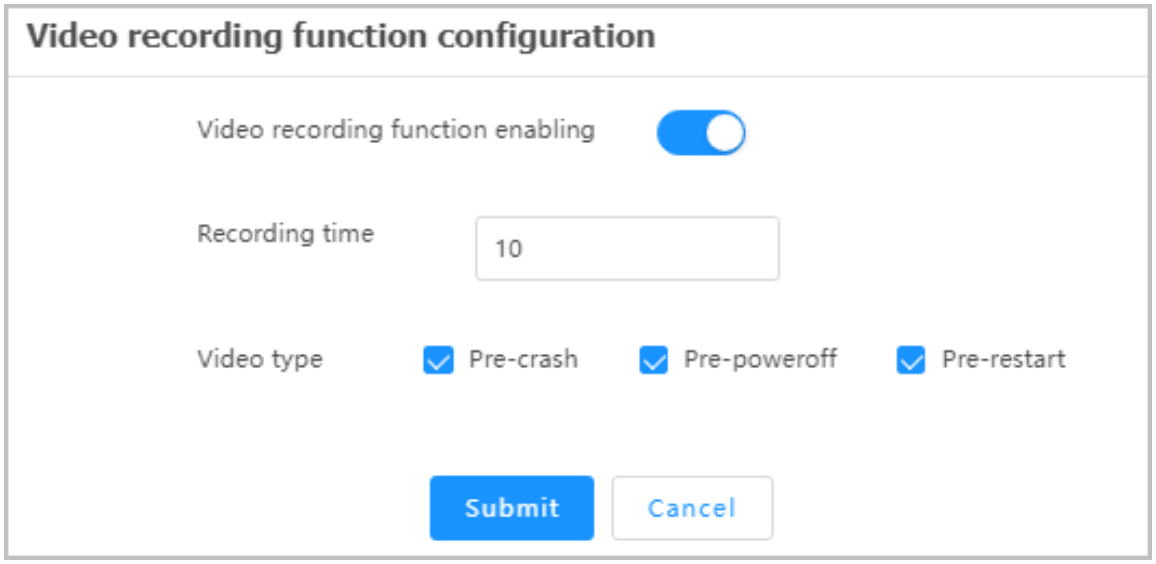
1. Select **Maintenance**. The **Maintenance** page is displayed.
2. From the navigation tree in the left pane, select **Screenshot&Video**. The **Screenshot&Video** page is displayed, as shown in Figure 6-5.

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**.

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

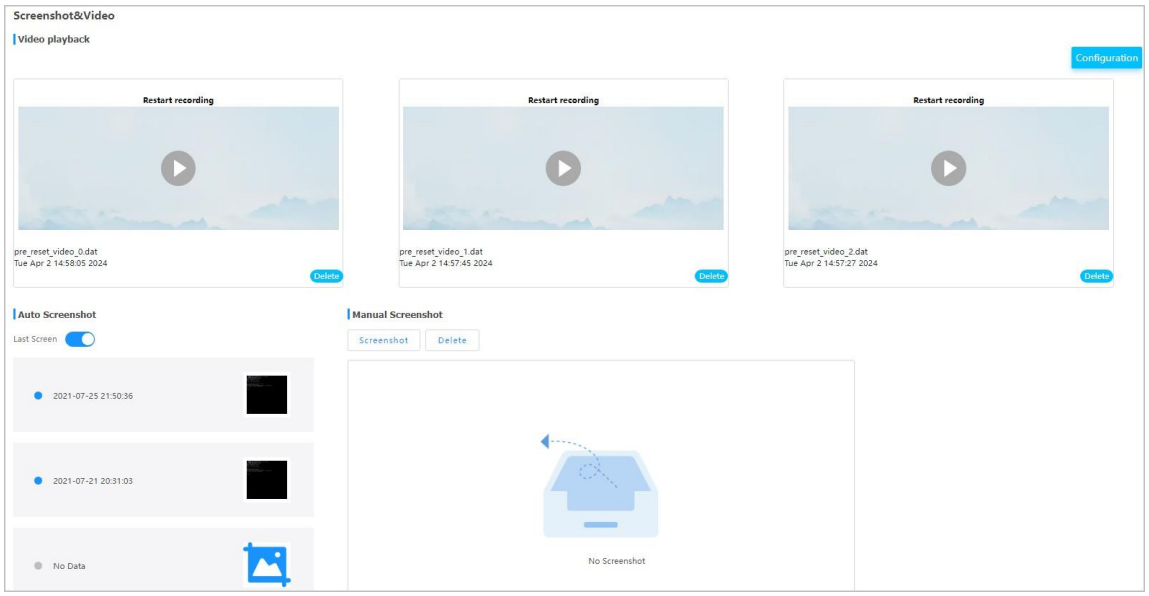
The screen recording function is enabled. For details, refer to "6.3 Configuring Screen Recording Parameters".

Steps

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

2. 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.

3. Click to play a recorded video.

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**.

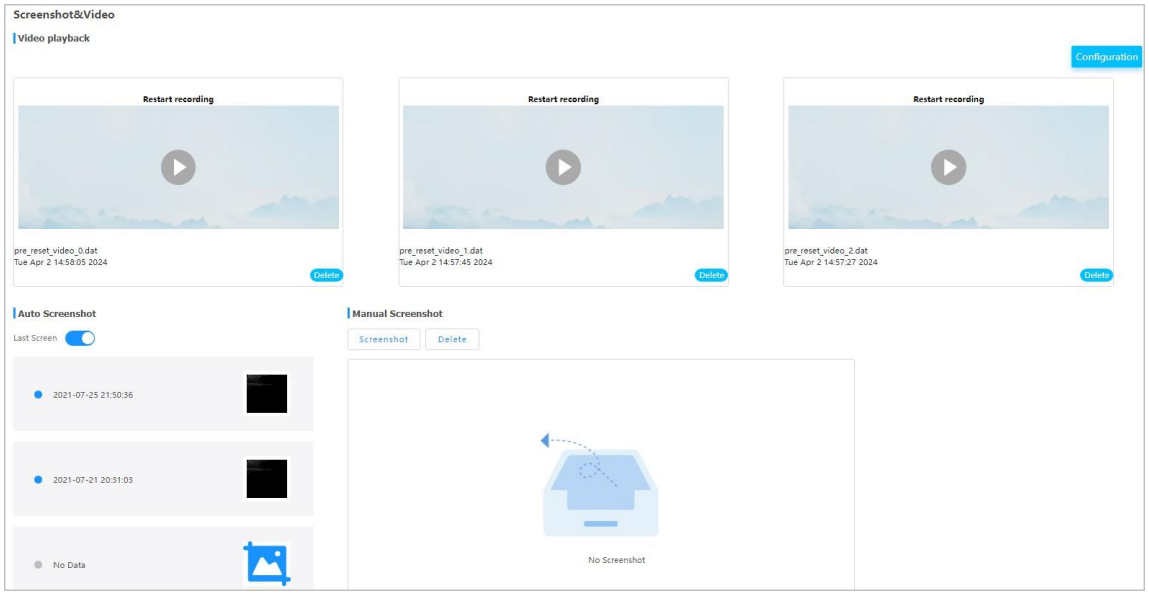
For a description of the power operations that can be triggered by the BMC, refer to 5.7 Powering On/Off the Server.

- 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 **Last Screen** switch.
Take a screenshot manually	Click **Screenshot**. The screenshot of the current screen is displayed at the bottom of the page. To delete the current screenshot, click **Delete**.

6.3 Viewing POST Codes

Abstract

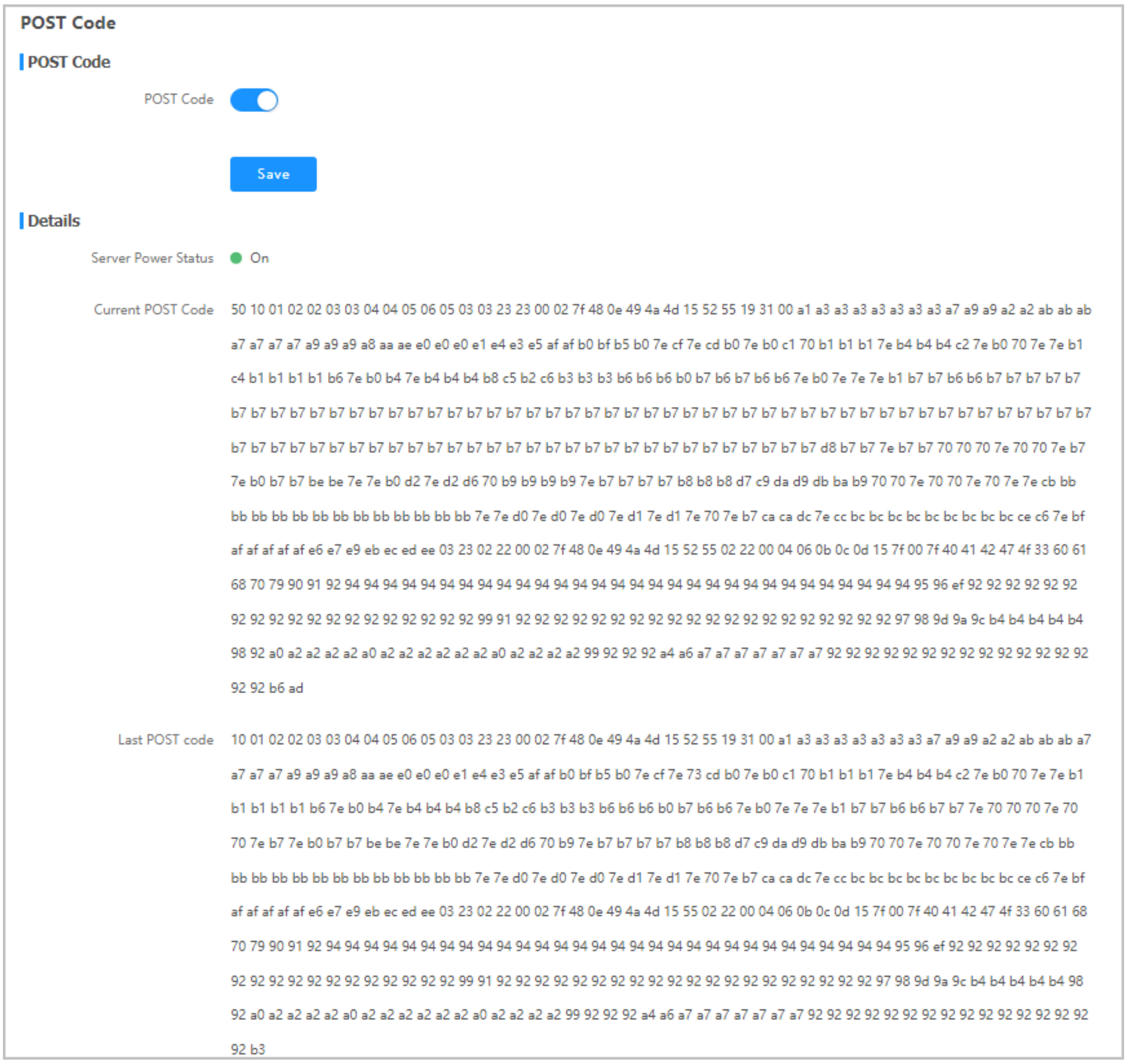
The POST code records the status of the server during power-on.

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**.

Downloading Server Logs

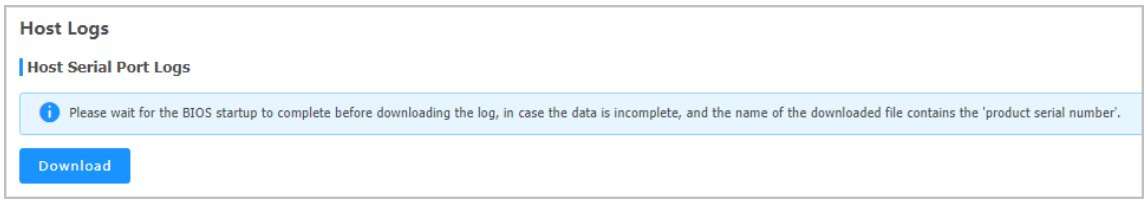
Abstract

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**.

Querying BMC Logs

Abstract

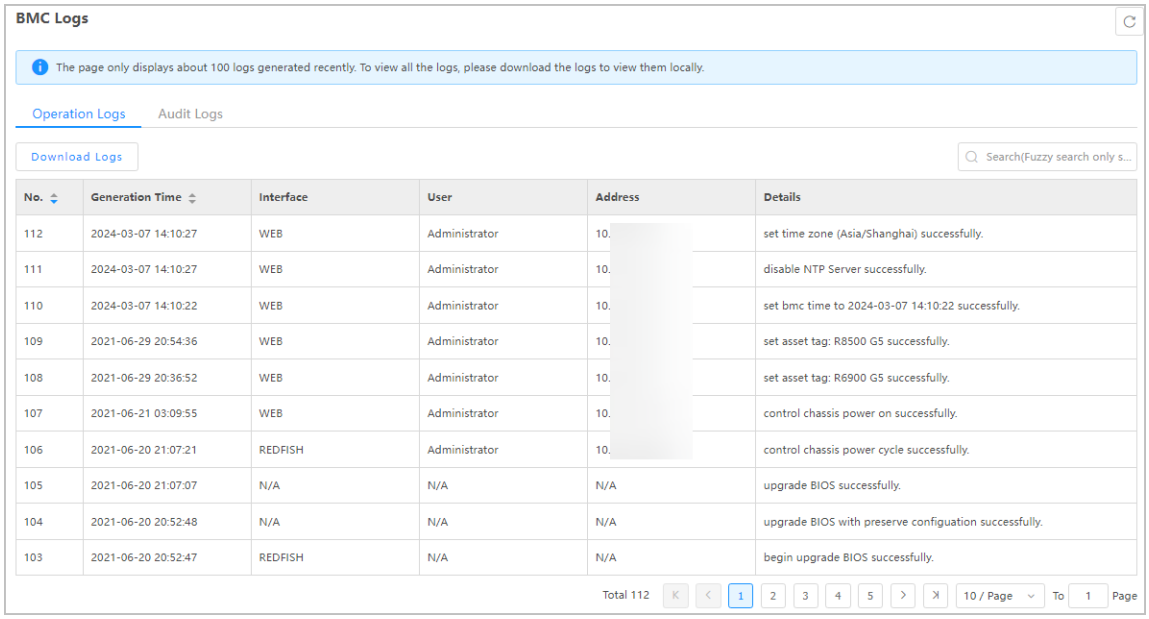
BMC logs include:

- **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



3. Perform the following operations as required.

To…	Do…
Query operation logs	a. Click **Operation Logs** to switch to the **Operation Logs** tab. b. (Optional) In the **Search** box, enter a keyword. c. (Optional) Click **Download Logs**.
Query audit logs	a. Click **Audit Logs** to switch to the **Audit Logs** tab. b. (Optional) In the **Search** box, enter a keyword. c. (Optional) Click **Download Logs**.

Querying SEL Logs

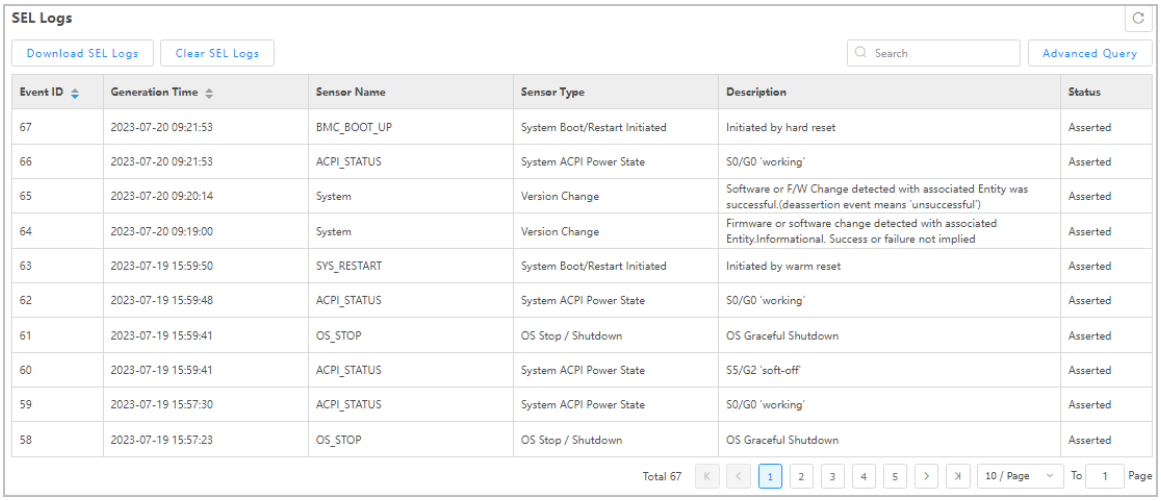
Abstract

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



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 **Download SEL Logs**.
Clear SEL Logs	Click **Clear SEL Logs**.

Service Management

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.

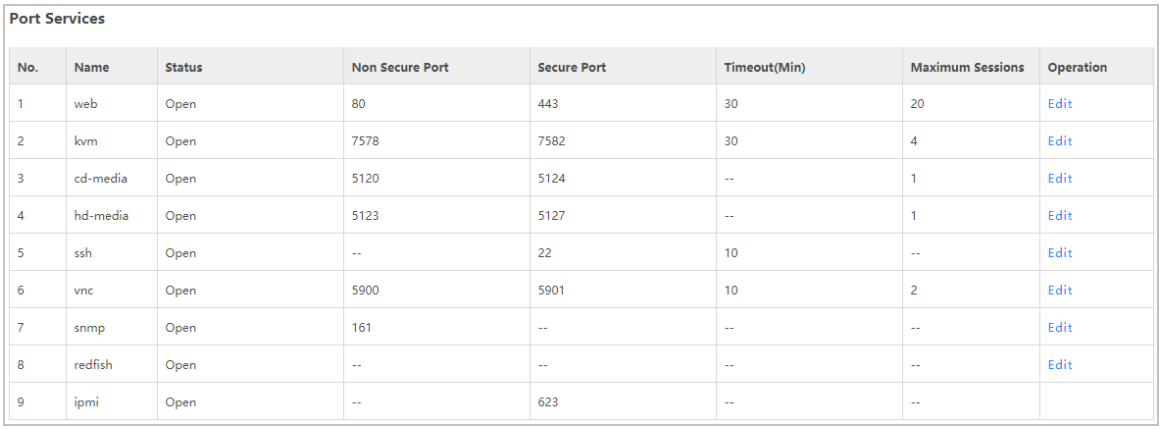
The parameters configured on the **Port Services** page are synchronized with the parameters configured on the following pages:

- **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	Enter the non-secure port number of the service. ● Default non-secure port number of the Web service: 80. ● Default non-secure port number of the KVM service: 7578. ● Default non-secure port number of the CD media service: 5120. ● Default non-secure port number of the HD media service: 5123. ● Default non-secure port number of the VNC service: 5900. ● Default non-secure port number of the SNMP service: 161. Other services do not support non-secure ports. Range of the non-secure port numbers: 1–65535.
Secure Port	Enter the secure port number of the service. ● Default secure port number of the Web service: 443. ● Default secure port number of the KVM service: 7582. ● Default secure port number of the CD media service: 5124. ● Default secure port number of the HD media service: 5127. ● Default secure port number of the SSH service: 22. ● Default secure port number of the VNC service: 5901. ● Default secure port number of the IPMI service: 623. Other services do not support secure ports. Range of the secure port numbers: 1–65535.
Timeout(Min)	Timeout period after which the service exits if no operation is performed. Enter the timeout period (in minutes). Range: 5–60 (for the VNC service) or 1–60 (for other services).

Note

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

5. Click **Save**.

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:

6. Configuring basic parameters
7. Uploading the SSL certificate to the browser
8. Uploading the SSL certificate to the Web portal of the BMC

Prerequisite

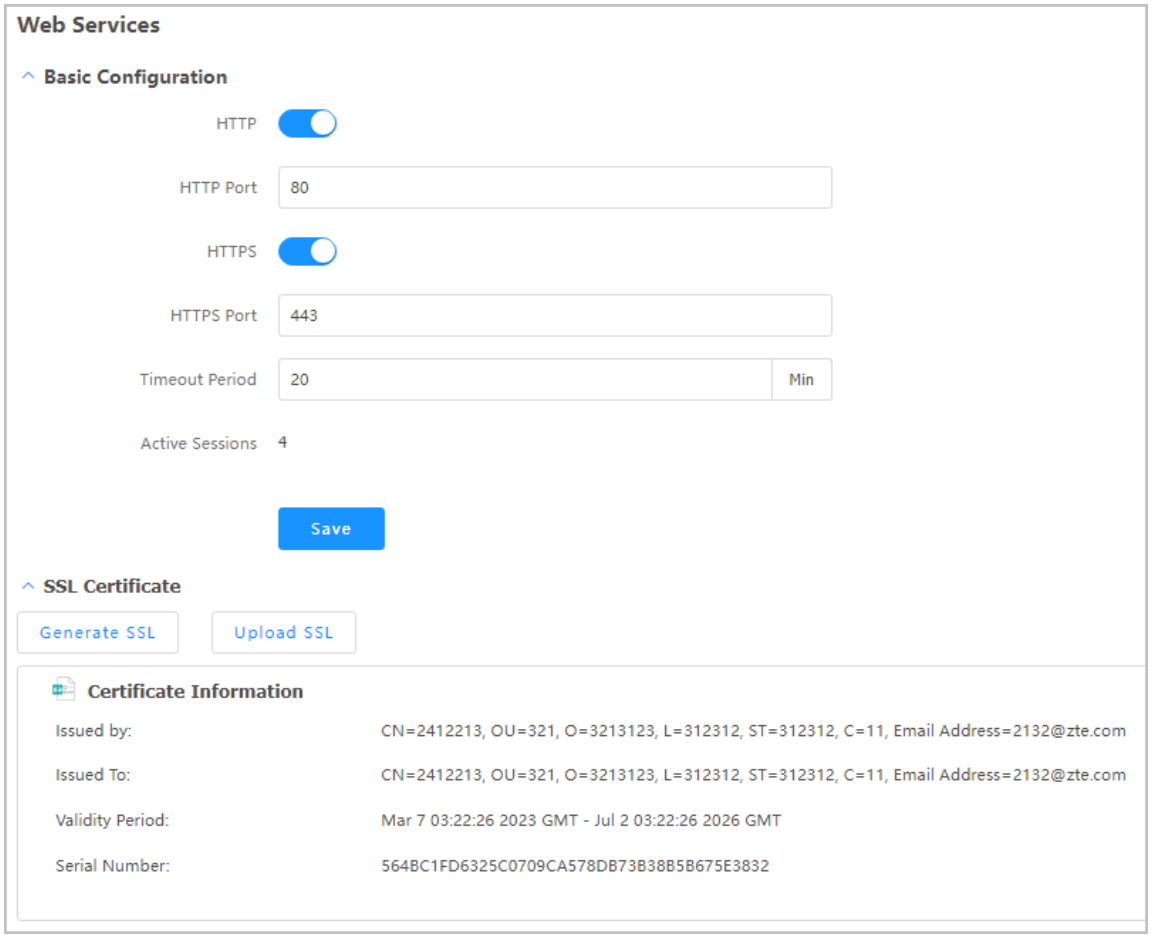
The *pem* file (containing the certificate file and private key file) is already obtained.

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



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 **HTTP** switch.
HTTP Port	Enter the non-secure port number of the Web service. Range: 1–65535, default: 80.
HTTPS	Turn on the **HTTPS** 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

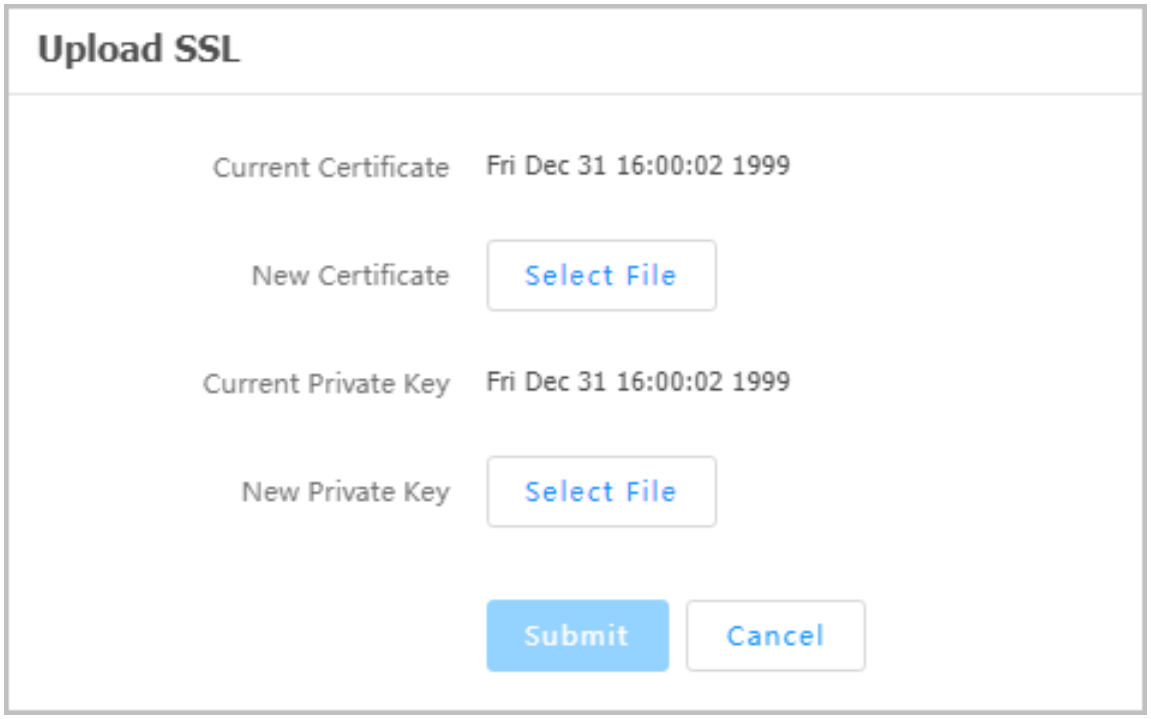
4. On the **Settings** page of the browser (for example, Google Chrome) on the PC, select **Privacy and security**. The **Privacy and security** page is displayed.

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

Configuring KVM Service Parameters

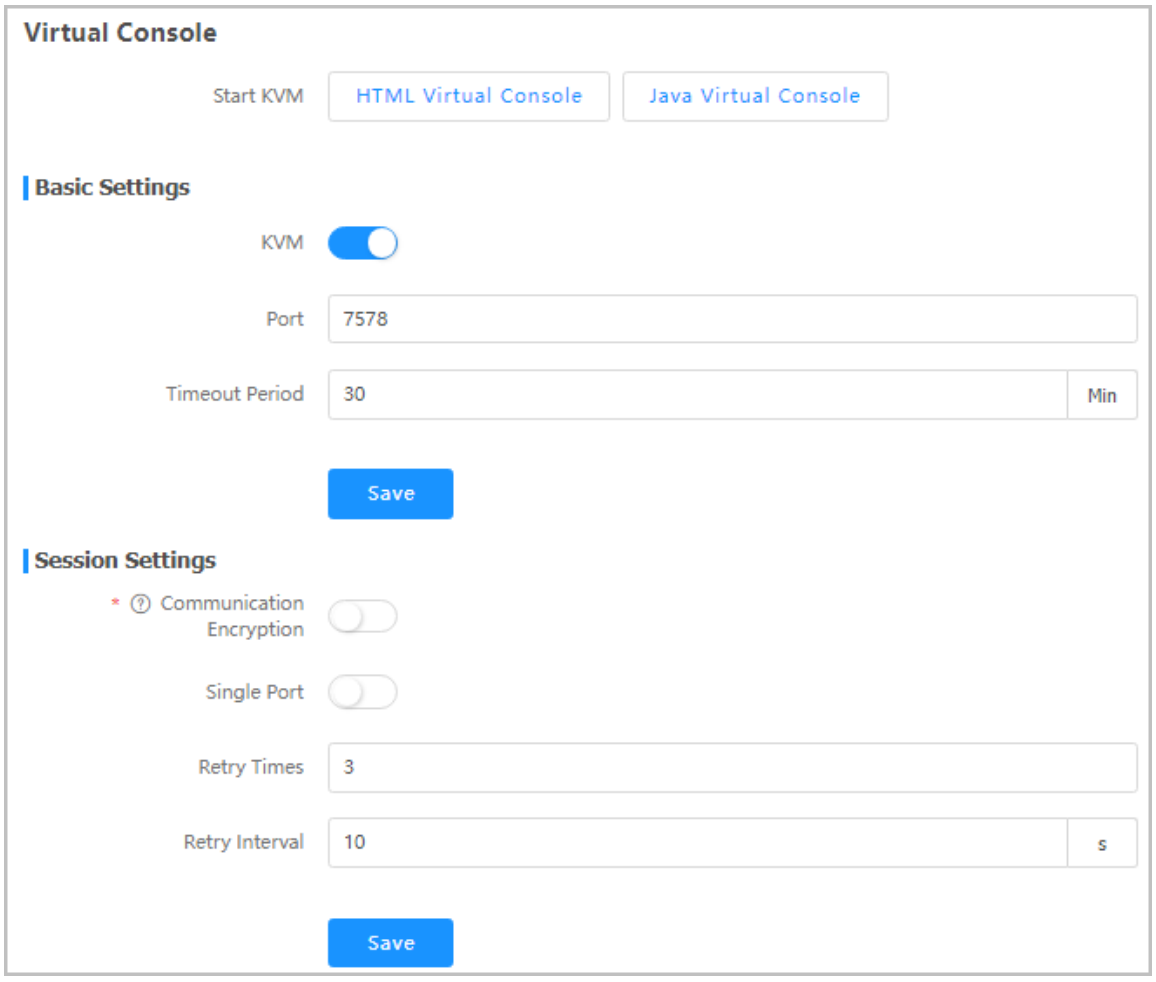
Abstract

Before starting the KVM, you need to configure the KVM service parameters.

Steps

9. Select **Services**. The **Services** page is displayed.
10. 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



11. 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 **KVM** switch.
Port	Enter the KVM service port number. ● If the **Communication Encryption** switch is turned off in the **Session Settings** area, enter a non-secure port number. ● If the **Communication Encryption** switch is turned on in the **Session Settings** area, enter a secure port number.
Timeout Period	The KVM service exits if no operation is performed within the specified timeout period. Enter the timeout period. Range: 1–30, unit: minutes.

12. Click **Save**.
13. 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 HTML mode. ● If the **Single Port** switch is turned on, port 443 is used in a unified manner. ● If the **Single Port** switch is turned off, port 443 is not used in a unified manner.
Retry Times	Enter the number of session retires. Range: 1–20.
Retry Interval	Enter the session retry interval. Range: 5–30, unit: seconds.

14. Click **Save**.

Starting the KVM

Abstract

When you are not on the customer site, you can start the KVM to remotely control the server.

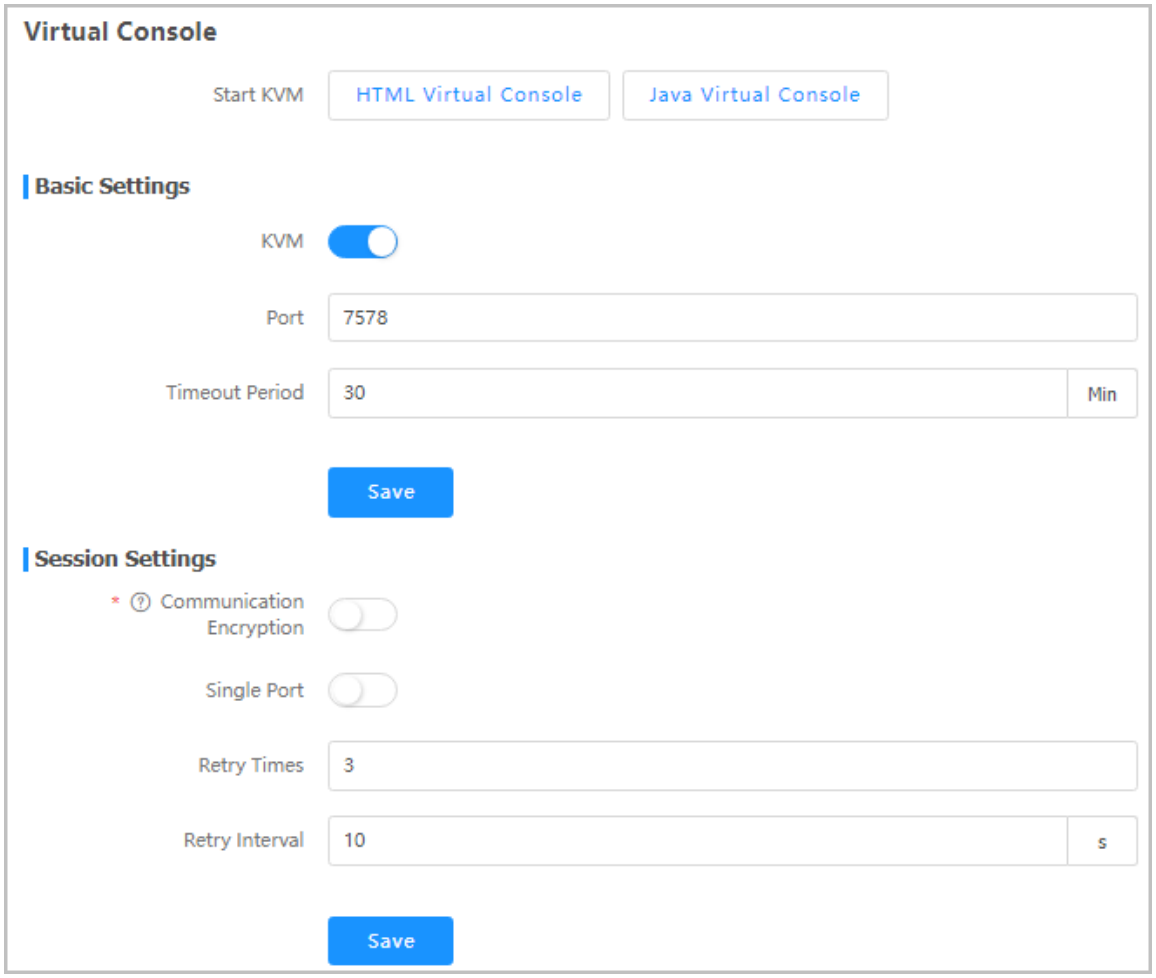
Prerequisite

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

15. Select **Services**. The **Services** page is displayed.
16. 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



17. Perform the following operations as required.

To…	Do…
Start the KVM in HTML mode	a. Click **HTML Virtual Console**. The **Remote KVM (HTML)** page is displayed, see Figure 7-8. b. Perform the following operations as required. For a description of the operations, refer to Table 7-5.
Start the KVM in Java mode	a. In the search box in the lower left corner of the PC, enter *Java*. b. In the search result, select **Java**. The **Java Control Panel** dialog box is displayed. c. Click **Security**. The **Security** window is displayed. d. Click **Edit Site List**. The **Exception Site List** dialog box is displayed.

To…	Do…
	e. Click **Add** to add the address of the Web portal of the BMC. f. Click **OK** to return to the **Security** window. g. Click **OK**. h. On the **Virtual Console** page of the Web portal of the BMC, click **Java Virtual Console**. A dialog box indicating whether to keep *jviewer.jnlp* is displayed. i. Click **Keep**. j. In the lower left corner of the browser, click *jviewer.jnlp*. A dialog box indicating whether to proceed is displayed. k. Click **Continue**. The **Do you want to run this application?** dialog box is displayed. l. Select **I accept the risk and want to continue to run this app.** and click **Run**. The **Untrusted Connection** dialog box is displayed. m. Click **Yes**. The **Remote KVM (JAVA)** page is displayed, see Figure 7-9. n. Perform the following operations as required. For a description of the operations, refer to Table 7-6.

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)

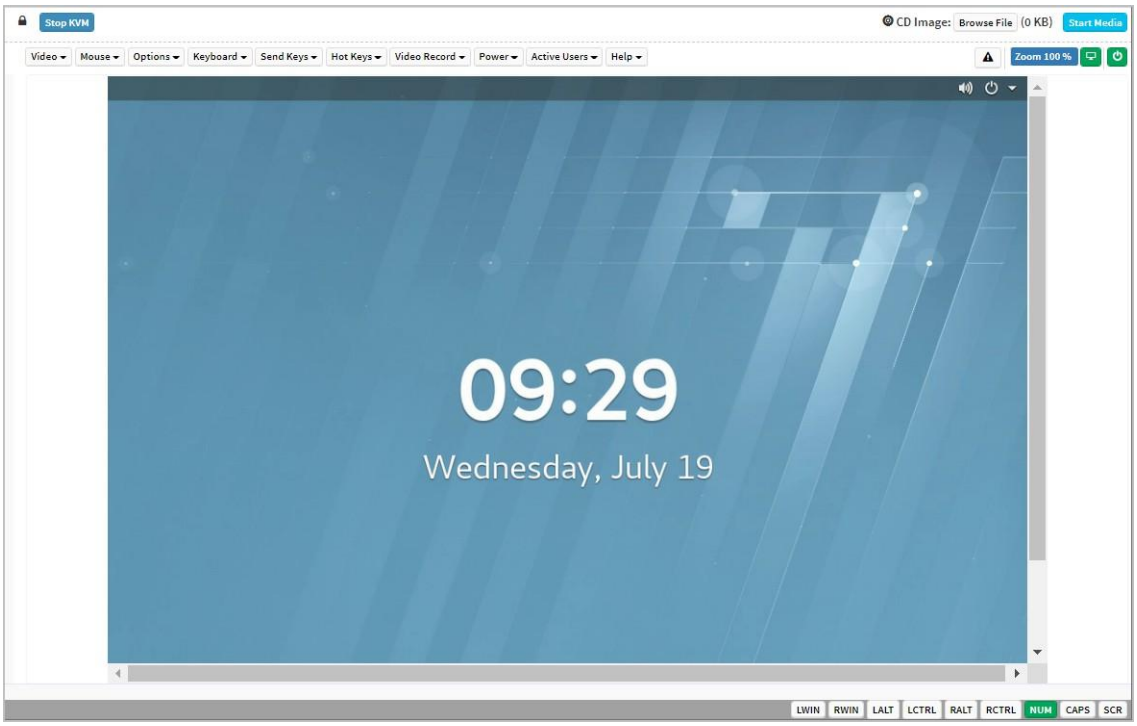


Table 7-5 Descriptions for the Remote KVM (HTML) Operations

Operation	Description
Stop the KVM	Click **Stop KVM** to exit the **Remote KVM (HTML)** page.
Mount a local *iso* file	a. Click **Browse File** next to **CD Image**, and select the *iso* file from the PC. b. Click **Start Media**.
Display the notifications received	Click  .
Lock the display of the server	Lock the server display through either of the following ways: ● Click  . ● Select **Video > Display OFF**. 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.
Unlock the server display	Unlock the server display through either of the following ways: ● Click  . ● Select **Video > Display ON**.  is converted to  .
Pause a remote control screen	Select **Video > Pause Video**.
Resume a remote control screen	Select **Video > Resume Video**.
Refresh a remote control screen	Select **Video > Refresh Video**.
Capture the current screen	Select **Video > Capture Screen**.
Display or hide the mouse pointer on the server screens	● To display the mouse pointer on the server screens, click **Mouse**, and select **Show Client Cursor**. ● To hide the mouse pointer on the server screens, click **Mouse**, and clear **Show Client Cursor**.
Set the mouse mode	Click **Mouse**, and select **Absolute Mouse Mode**. In absolute mouse mode, the absolute position of the local mouse is transferred to the server to make the mouse on the server move.
Set keyboard layout	a. Select **Keyboard**. b. In the displayed submenu, select the keyboard layout, including **English U.S**, **German** and **Japanese**. **English U.S** is selected by default.

Operation	Description
Set video recording time length	a. Select **Video Record > Record Settings**. The **Record Settings** dialog box is displayed. b. Set the video recording time length with a range of 1–1800 seconds. c. Click **OK**.
Record videos	Select **Video Record > Record Video**.
Stop recording	Select **Video Record > Stop Recording**.
Shut down the server	Shut down the server through either of the following ways: ● Select **Power > Orderly shutdown**. ● Click  .
Start the server	Start the server through either of the following ways: ● Select **Power > Power On Server**. ● Click  .
Perform a cold reboot	Select **Power > Power Cycle Server**. Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.
Perform a warm reboot	Select **Power > Reset Server**. Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
View the users that are using remote control	Select **Active Users**.

Figure 7-9 Remote KVM (Java) Page

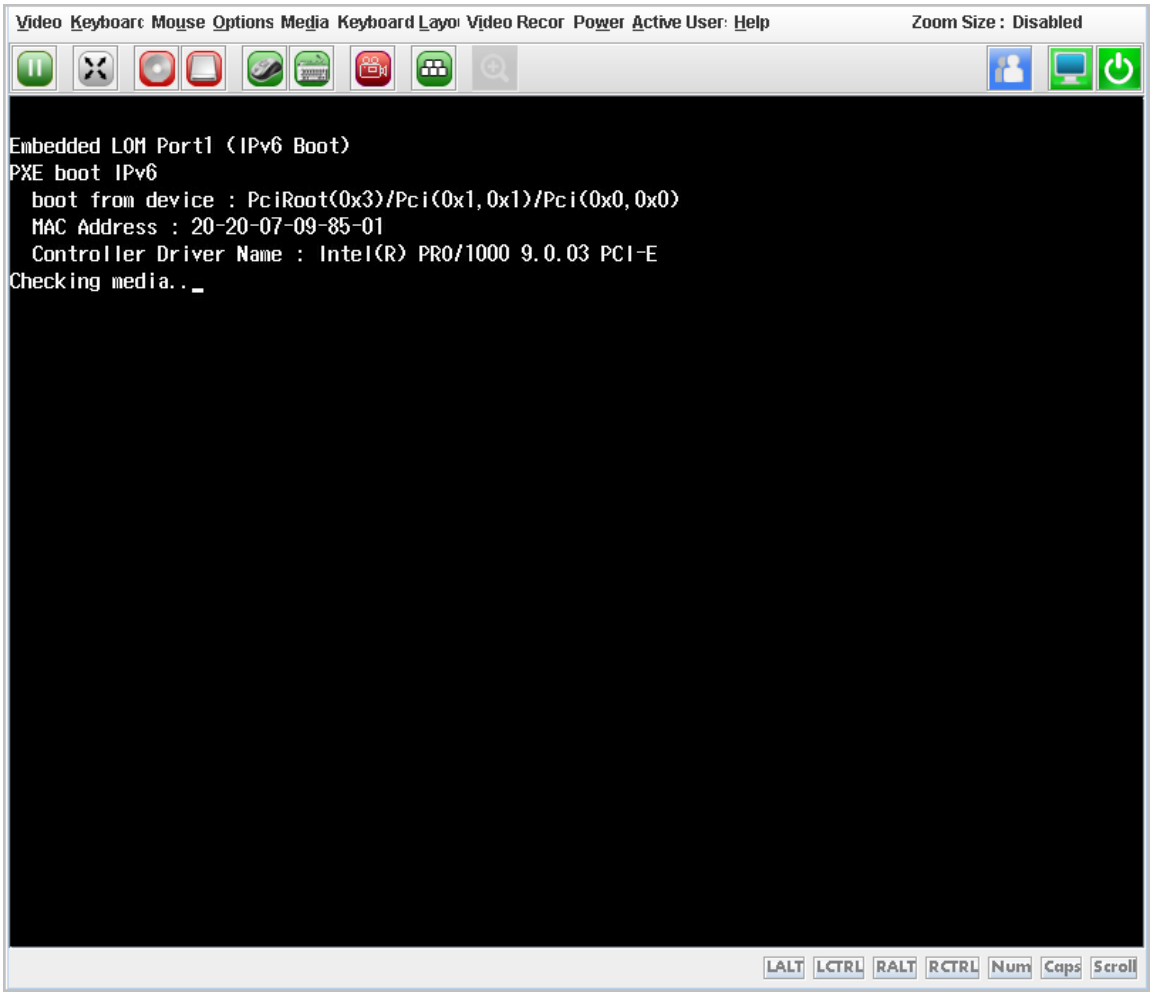


Table 7-6 Descriptions for the Remote KVM (JAVA) Operations

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

Operation	Description
	● To not display the remote screen on the host, select **Video > Turn OFF Host Display**. Note: You can use either of the following methods to rapidly switch between the remote screen display modes of the host. ● Click  . ● Press **Alt+N**.
Capture the current screen	Capture the current screen through either of the following ways: ● Select **Video > Capture Screen**. ● Press **Alt+S**.
Set a video decoding mode	a. Select **Video > Compression Mode**. b. Select a video decoding mode from the displayed submenu.
Set the video display quality	a. Select **Video > DCT Quantization Table**. b. Select the video display quality from the displayed submenu. The video display quality is divided into eight levels from 0 through 7, with video quality degraded in turn.
Define a key combination	a. Select **Keyboard > Hot Keys > add Hot Keys**. The **User Defined Macros** page is displayed. b. Click **add**. The **Add Macros** page is displayed. c. Press and then release the user-defined key combination. d. Click **OK**.
Enable full keyboard support	● To enable full keyboard support, click **Keyboard**, and select **Full Keyboard Support**. ● To disable full keyboard support, click **Keyboard**, and clear **Full Keyboard Support**.
Display or hide the mouse pointer	● To display the mouse pointer, click **Mouse**, and select **Show Client Cursor**. ● To hide the mouse pointer, click **Mouse**, and clear **Show Client Cursor**. You can use either of the following methods to rapidly change the mouse display modes on the PC. ● Press **Alt+C**. ● Click  .
Set the network bandwidth	a. Select **Options > Bandwidth**. b. Select the desired network bandwidth from the displayed submenu.
Change the encryption status of the mouse/keyboard	● To enable mouse/keyboard encryption, click **Options**, and select **Keyboard/Mouse Encryption**. ● To disable mouse/keyboard encryption, click **Options**, and clear **Keyboard/Mouse Encryption**.

Operation	Description
Set the scaling mode of a remote screen	a. Select **Options > Zoom**. b. In the displayed submenu, set the zoom scale of the remote screen. ● **Zoom In**: zooms in the remote screen. ● **Zoom Out**: zooms out the remote screen. ● **Actual Size**: displays the remote screen in the proportion of 100%. ● **Fit to Client Resolution**: displays the remote screen in the resolution of the local client system. ● **Fit to Host Resolution**: displays the remote screen in the resolution of the remote server system.
Send an IPMI command to the server	a. Select **Options > Send IPMI Command**. The **IPMI Command Dialog** window is displayed. b. Enter the IPMI command. c. Click **Send**. The IPMI command supports hex format and ASCII format.
Set the GUI language	a. Select **Options > GUI Languages**. b. Select the GUI language from the displayed submenu.
Set the privilege request mode	a. Select **Options > Block Privilege Request**. b. Select a privilege request block mode from the displayed submenu. ● **Allow only Video**: The permission for viewing the information displayed on the server is automatically granted to the user who initiates a privilege request. ● **Deny Access**: Privilege requests in the system are blocked.
Mount a local `iso` file	a. Open the **Virtual Media** window in either of the following ways: ● Select **Media > Virtual Media Wizard...**, and switch to the **CD/DVD** tab. ● Click  . b. Click **Browse** and select a local `iso` file. c. Click **Connect**.
Mount a local folder	a. Create an `iso` file on the PC. b. Open the **Virtual Media** window in either of the following ways: ● Select **Media > Virtual Media Wizard...**, and switch to the **Hard Disk/USB** tab. ● Click  . c. Select **physical drive > folder path**. d. Click **Browse** and select a local folder path. e. Set **Size** and **folder path**. f. Click **Connect**. The value of **Size** must be 2^n, such as 2, 4 and 8. The path specified by **folder path** needs to be the same as that of the new `iso` file.

Operation	Description
Set keyboard layout	a. Select **Keyboard Layout**. b. Select the keyboard layout from the displayed submenu.
Open the soft keyboard	Click  .
Configure video recording	a. Select **Video Record > Settings**. The **Video Record** window is displayed. b. Set the video recording time length in seconds and the video storage position. c. Click **OK**. The video recording time length ranges from 1 through 1800 seconds.
Record videos	a. Start recording a video in either of the following ways: ● Select **Video Record > Start Record**. ● Click  . b. (Optional) Stop recording a video in either of the following ways: ● Select **Video Record > Stop Record**. ● Click  . c. After the preset recording time length is reached or the recording is stopped manually, click **OK**. The recorded video file is saved to the `VideoCaptures` folder in the preset path.
Set the server power mode	a. Select **Power**. b. Select a server power option from the displayed submenu. The server power options are as follows: ● **Reset Server**: restarts the system without shutting down the power supply (warm reboot). ● **Immediate Shutdown**: shuts down the server immediately by shutting down the power supply. ● **Orderly Shutdown**: shuts down the server in order through program control. ● **Power On Server**: starts the server. ● **Power Cycle Server**: shuts down the server and restarts it (cold reboot).
Check active users	View the users using remote control in either of the following ways: ● Select **Active Users**. ● Click  .

Configuring Virtual Media Parameters

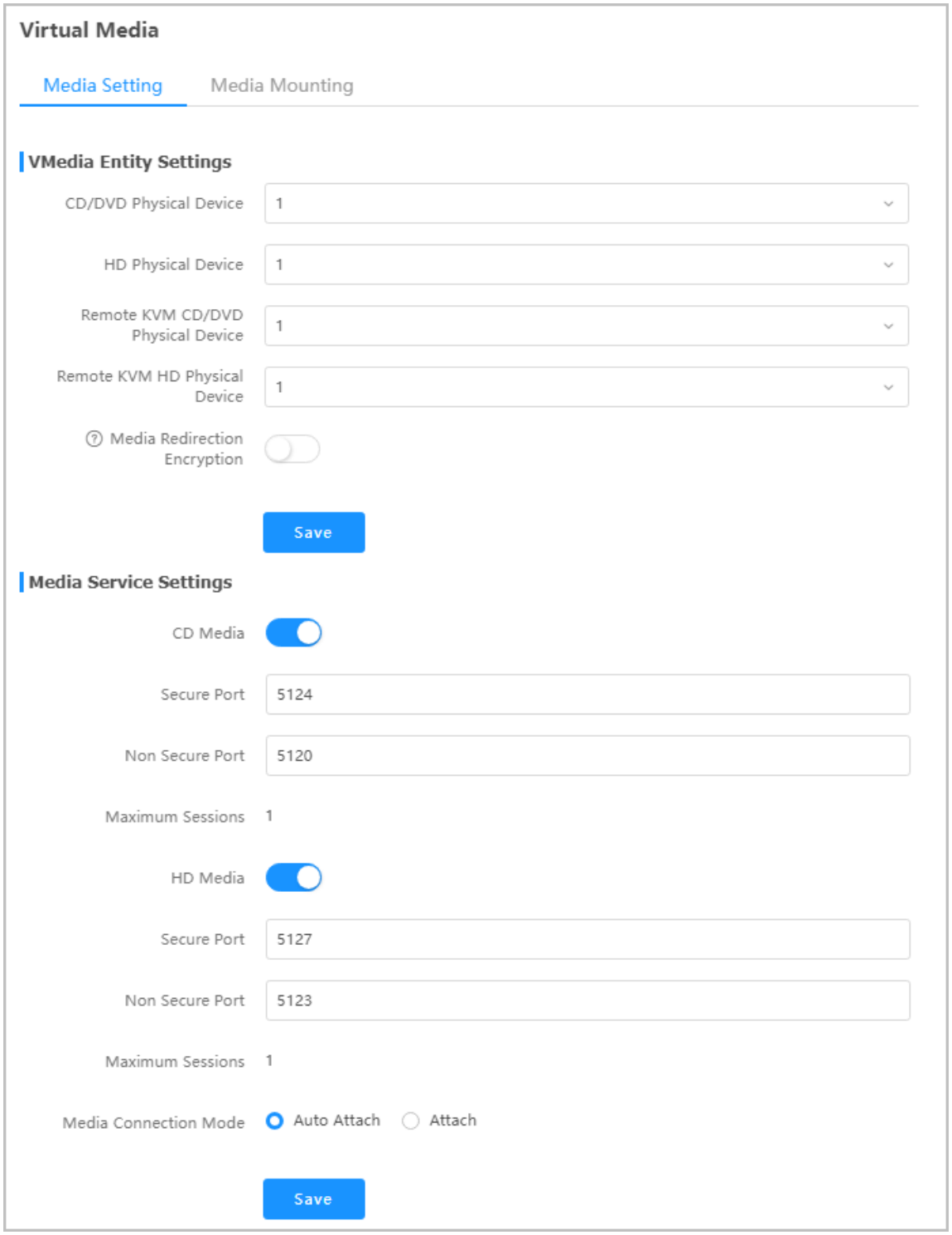
Abstract

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

Steps

18. Select **Services**. The **Services** page is displayed.
19. 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



20. Set the parameters in the **VMedia Entity Settings** area. For a description of the parameters, refer to Table 7-7.

Table 7-7 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 **Media Redirection Encryption** switch.

21. Click **Save**.
22. Set the parameters in the **Media Service Settings** area. For a description of the parameters, refer to Table 7-8.

Table 7-8 Parameter Descriptions for Media Service Settings

Parameter	Setting
CD Media	● To enable the CD media service, turn on the **CD Media** switch. ● To disable the CD media service, turn off the **CD Media** switch.
Secure Port	This parameter can be set when the **CD Media** 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 **CD Media** switch is turned on. Enter the non-secure port number of the CD media service. Range: 1–65535, default: 5120.
HD Media	● To enable the HD media service, turn on the **HD Media** switch. ● To disable the HD media service, turn off the HD Media switch.
Secure Port	This parameter can be set when the **HD Media** 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 **HD Media** 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. ● **Auto Attach**: reconnects automatically. ● **Attach**: does not reconnect automatically.

23. Click **Save**.

Mounting a Virtual Media Device

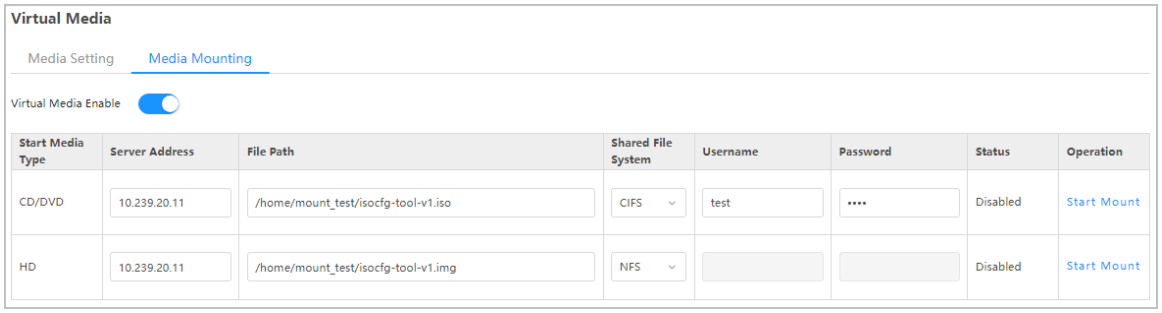
Abstract

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

Steps

24. Select **Services**. The **Services** page is displayed.
25. From the navigation tree in the left pane, select **Virtual Media**. The **Virtual Media** page is displayed.
26. Click **Media Mounting**. The **Media Mounting** tab is displayed, as shown in Figure 7-11.

Figure 7-11 Virtual Media Page—Media Mounting Tab



27. Set the parameters. For a description of the parameters, refer to Table 7-9.

Table 7-9 Parameter Descriptions for Mounting a Virtual Media Device

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

Parameter	Description
	● If **Start Media Type** is **CD/DVD**, the suffix of the image filename must be *iso*. ● If **Start Media Type** is **HD**, the suffix of the image filename must be *img* or *ima*.
Shared File System	Select a file system protocol for file sharing. Options: **NFS**, **CIFS**, and **HTTPS**. ● If **Start Media Type** is **CD/DVD**, **NFS**, **CIFS**, and **HTTPS** are supported. ● If **Start Media Type** is **HD**, **NFS** and **CIFS** are supported.
Username	Enter the username for logging in to the remote server. This parameter does not need to be set if **Shared File System** is set to **NFS**.
Password	Enter the password for logging in to the remote server. This parameter does not need to be set if **Shared File System** is set to **NFS**.

28. 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.

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.

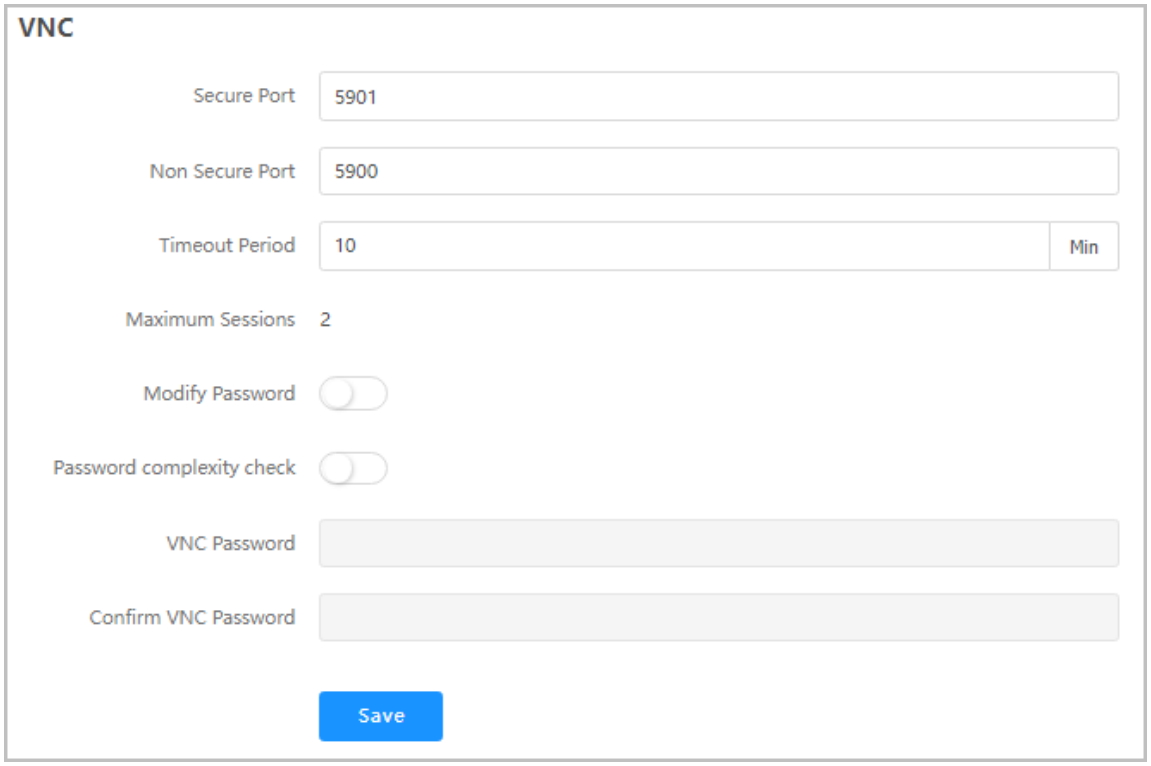
Note

For KVM-related parameter configuration, refer to 7.3 Configuring KVM Service Parameters. For KVM-based remote server control operations, refer to 7.4 Starting the KVM.

Steps

29. Select **Services**. The **Services** page is displayed.
30. From the navigation tree in the left pane, select **VNC**. The **VNC** page is displayed, see Figure 7-12.

Figure 7-12 VNC Page



31. Set the parameters. For a description of the parameters, refer to Table 7-10.

Table 7-10 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	The VNC service exits if no operation is performed within the specified timeout period. Enter the timeout period. Range: 5–30, unit: minutes.
Modify Password	Whether to modify the VNC password. ● To modify the VNC password, turn on the **Modify Password** switch. ● To not modify the VNC password, turn off the **Modify Password** switch.
Password complexity check	Whether to check the complexity of the VNC password. ● To check the complexity of the VNC password, turn on the **Password complexity check** switch. ● To not check the complexity of the VNC password, turn off the **Password complexity check** switch.

Parameter	Setting
VNC Password	This parameter can be set when the **Modify Password** switch is turned on. Enter the new VNC password. The requirements for the VNC password are as follows: ● The password contains a maximum of eight characters. ● The password must contain at least one special character except spaces. ● The password must contain at least two of the following types: upper-case letters, lowercase letters, and digits. If the configuration is null, the default password is restored.
Confirm VNC Password	This parameter can be set when the **Modify Password** switch is turned on. Confirm the new VNC password, which must be the same as **VNC Password**.

32. Click **Save**.

Configuring SNMP Parameters

Abstract

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

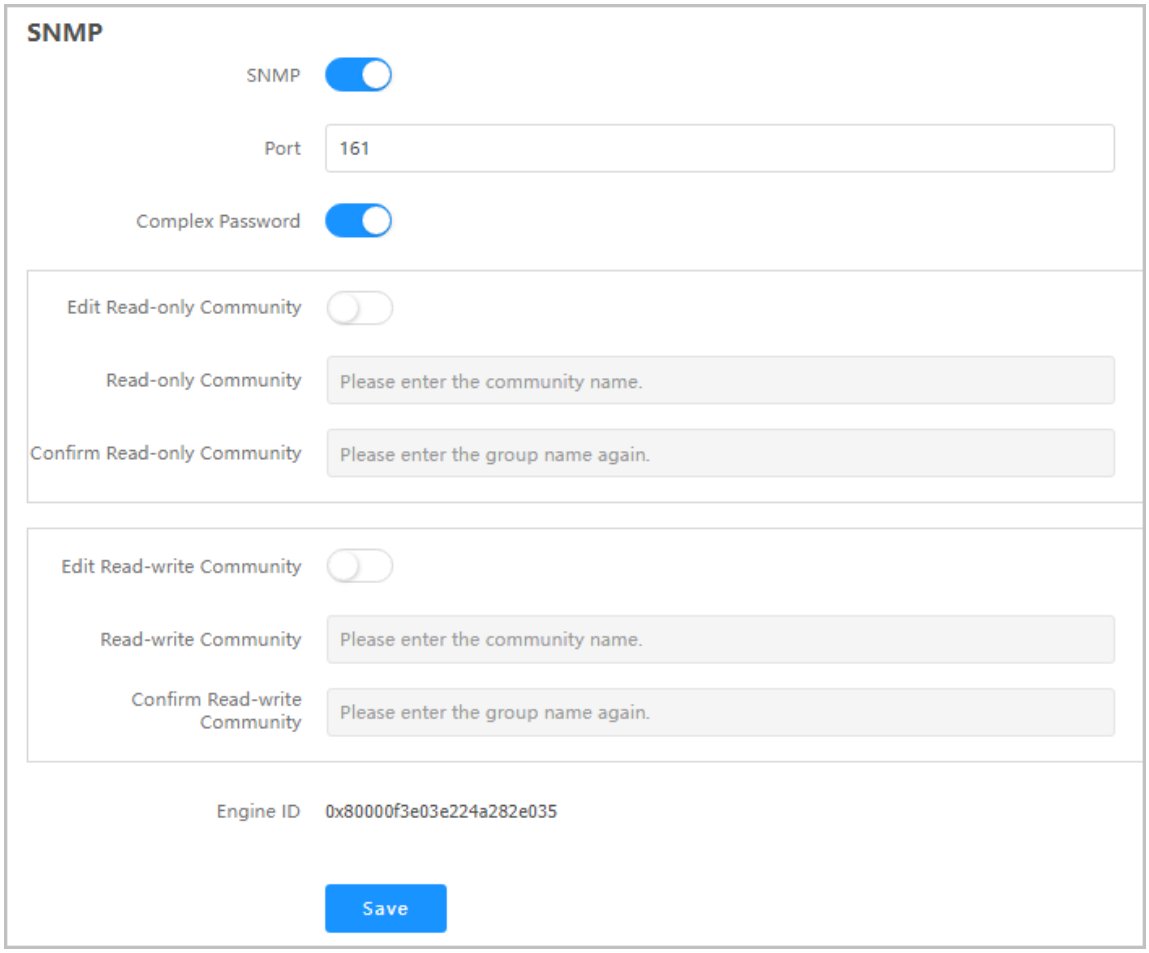
Note

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

33. Select **Services**. The **Services** page is displayed.
34. From the navigation tree in the left pane, select **SNMP**. The **SNMP** page is displayed, see Figure 7-13.

Figure 7-13 SNMP Page



35. Set the parameters. For a description of the parameters, refer to Table 7-11.

Table 7-11 SNMP Parameter Descriptions

Parameter	Setting
SNMP	Turn on the **SNMP** 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. ● To enable the complex password function, turn on the **Complex Password** switch. ● To disable the complex password function, turn off the **Complex Password** switch.
Edit Read-only Community	Whether to edit the read-only community name. ● To edit the read-only community name, turn on the **Edit Read-only Community** switch. ● To not edit the read-only community name, turn off the **Edit Read-only Community** switch.

Parameter	Setting
Read-only Community	This parameter can be set when the **Edit Read-only Community** switch is turned on. Enter the read-only community name (default: roAdmin9!).
Confirm Read-only Community	This parameter can be set when the **Edit Read-only Community** switch is turned on. Confirm the read-only community name, which must be the same as that specified by **Read-only Community**.
Edit Read-write Community	Whether to edit the read-write community name. ● To edit the read-write community name, turn on the **Edit Read-write Community** switch. ● To not edit the read-only community name, turn off the **Edit Read-write Community** switch.
Read-write Community	This parameter can be set when the **Edit Read-write Community** switch is turned on. Enter the read-write community name (default: rwAdmin9!).
Confirm Read-write Community	This parameter can be set when the **Edit Read-write Community** switch is turned on. Confirm the read-write community name, which must be the same as that specified by **Read-write Community**.

36. Click **Save**.

BMC Management

Network Parameter Configuration

Configuring the Host Name

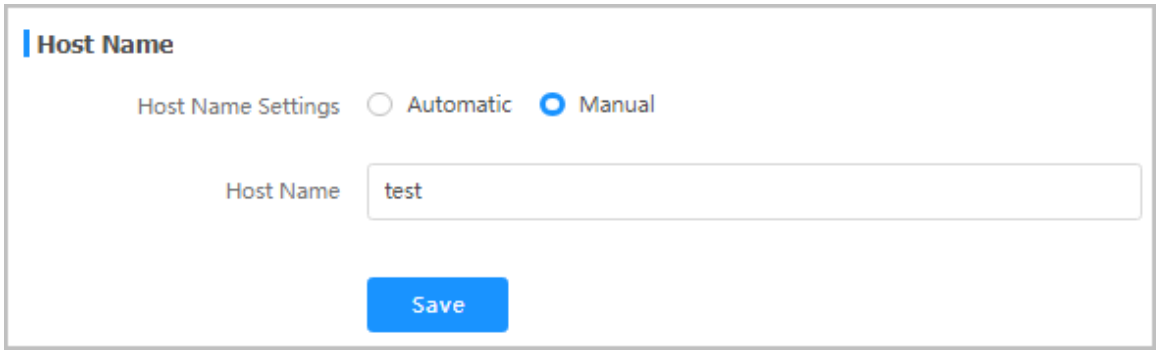
Abstract

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



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. ● **Automatic**: A host name is automatically set by the system. ● **Manual**: A host name needs to be manually entered in the **Host Name** text box.
Host Name	This parameter is required if **Host Name Settings** is set to **Manual**. 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**.

Configuring the Network Port Mode

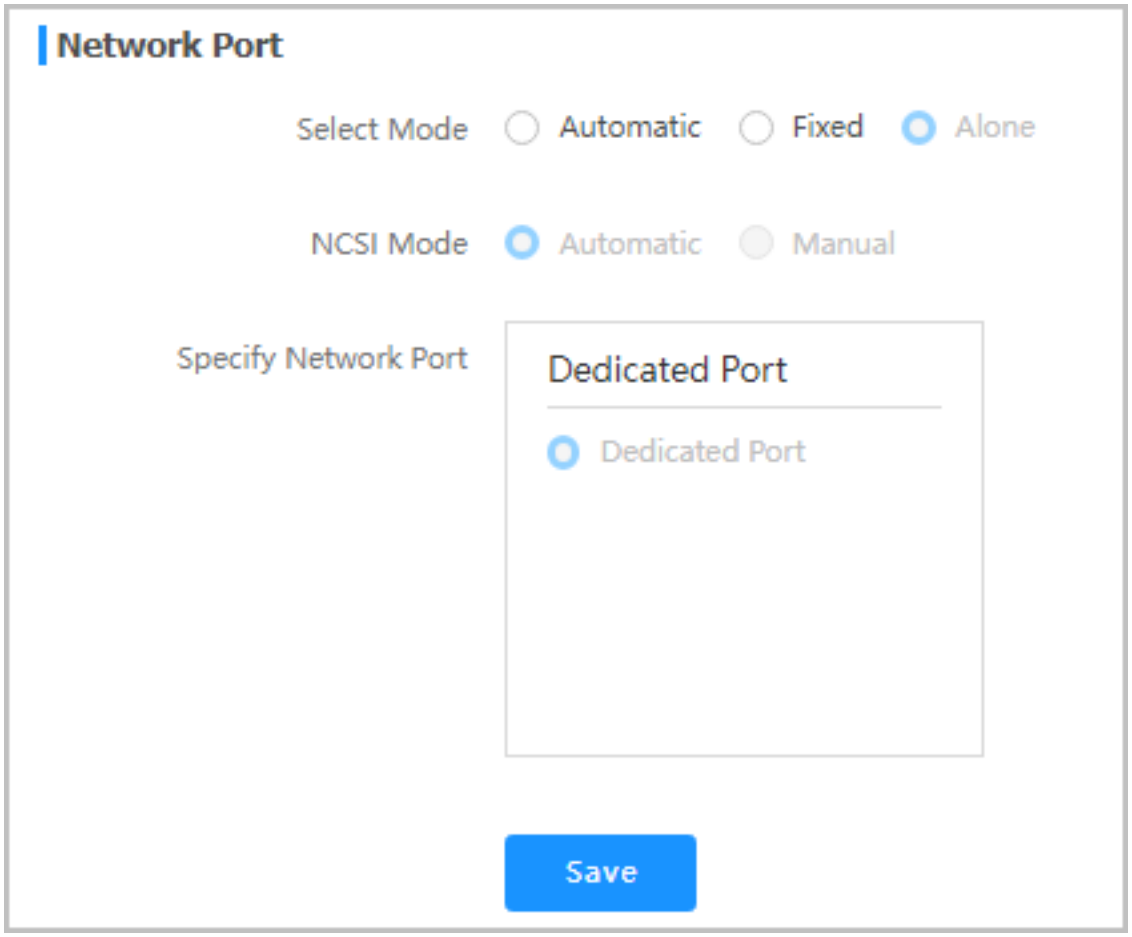
Abstract

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

Steps

5. Select **BMC Settings**. The **BMC Settings** page is displayed.
6. 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



7. 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	Select the desired network port mode. ● **Automatic**: The dedicated network port (namely the iPMI network port) is preferentially used as the management network port. If the dedicated network port does not operate properly, an onboard NCSI that is operating properly is automatically used as the management network port to replace the dedicated network port. ● **Fixed**: A network port (the dedicated network port or an onboard NCSI) specified in the **Dedicated Port** box in the **Specify Network Port** area is used as the management network port. ● **Alone**: 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.

Parameter	Setting
	If **Select Mode** is set to **Automatic**, the following parameters do not need to be configured.
NCSI Mode	This parameter is required when **Alone** is selected. Select the desired shared network port mode. ● **Automatic**: If the shared network port does not operate properly, an onboard **NCSI** that is operating properly is automatically used as the shared network port to replace the faulty shared network port. ● **Manual**: An onboard NCSI specified in the **Network Card** box in the **Specify Network Port** area is used as the shared network port. If **NCSI Mode** is set to **Automatic**, no shared network port needs to be specified.
Specify Network Port	● If **Select Mode** is set to **Automatic**, no network port needs to be specified. ● If **Select Mode** is set to **Fixed**, a network port (the dedicated network port or an onboard NCSI) needs to be specified as the management network port. ● If **Select Mode** is set to **Alone** and **NCSI Mode** is set to **Manual**, the dedicated network port is used as the management network port, and an onboard NCSI needs to be specified in the **Network Card** box as the shared network port.

8. Click **Save**.

Configuring IP Addresses of Network Ports

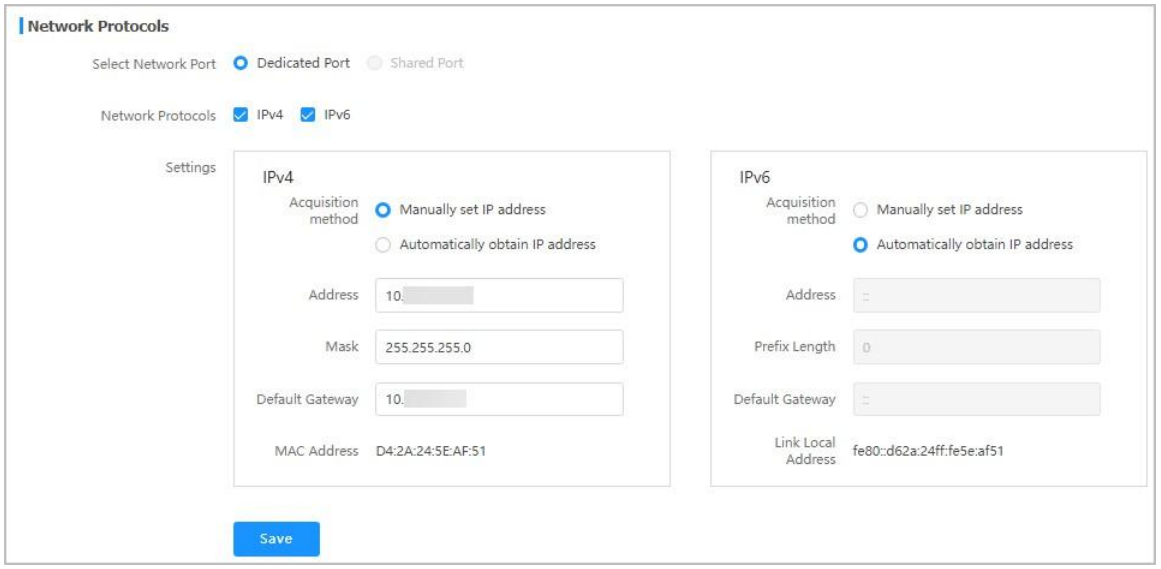
Abstract

To replan the IP address of the iPMI 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

9. Select **BMC Settings**. The **BMC Settings** page is displayed.
10. 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



11. 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	This parameter can be set only if **Select Mode** is set to **Alone** in the **Network Port** area. Select the network port for which you want to configure an IP address. ● **Dedicated Port**: configures the IP address of the iPMI management network port. ● **Shared Port**: configures the IP address of the shared network port.
Network Protocols	Select the network protocol(s) for the network port. ● The IPv4 settings need to be configured if you select **IPv4** only. ● The IPv6 settings need to be configured if you select **IPv6** only. ● Both IPv4 settings and IPv6 settings need to be configured if you select **IPv4** and **IPv6**.
Acquisition method	Select the method of obtaining the IP address. The parameters below do not need to be configured if **Acquisition method** is set to **Automatically obtain IP address**.
Address	Enter the address of the BMC as planned.
Mask	Enter the mask.
Default Gateway	Enter the IP address of the default gateway.

12. Click **Save**.

Configuring the DNS

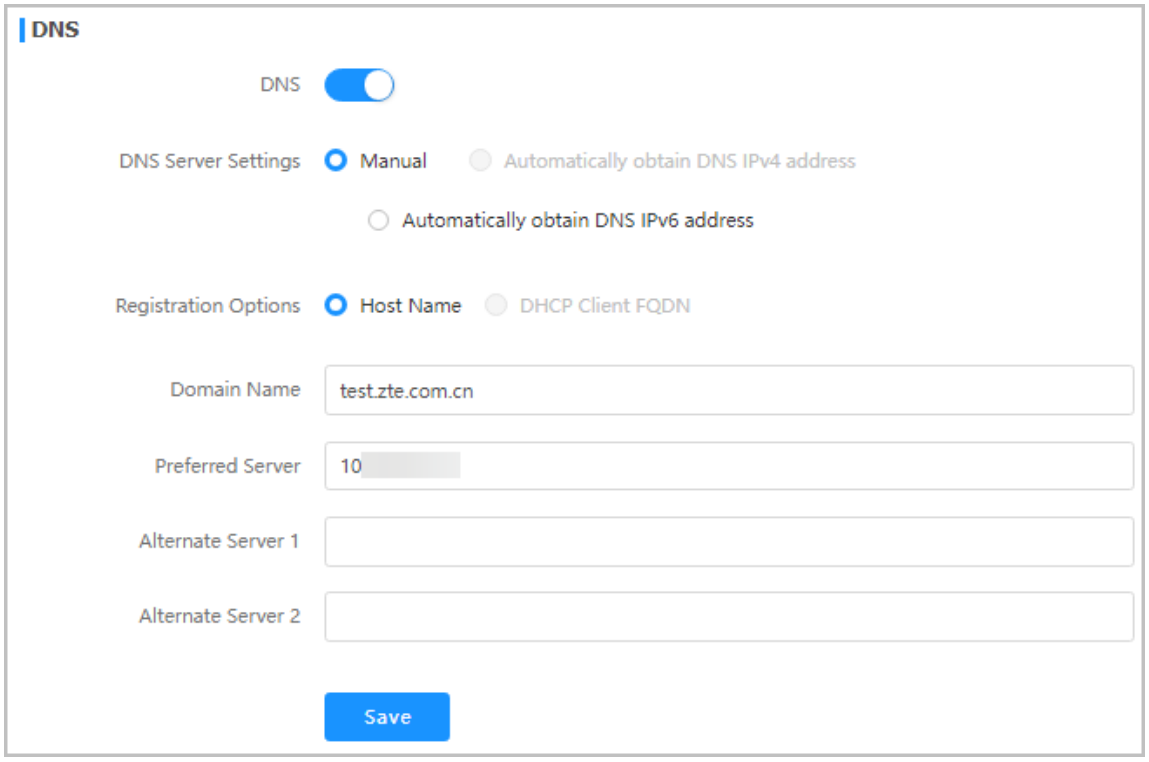
Abstract

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

Steps

13. Select **BMC Settings**. The **BMC Settings** page is displayed.
14. 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



15. 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	Select whether to enable the DNS service. ● To enable the DNS service, turn on the **DNS** switch. In this case, the following parameters need to be configured. ● To disable the DNS service, turn off the **DNS** switch. In this case, the following parameters do not need to be configured.
DNS Server Settings	Select the desired DNS setting method.

Parameter	Setting
	● **Manual**: If **Acquisition method** is set to **Manually set IP address** in the **Network Protocols** area, this parameter must be set to **Manual**. When **Manual** is selected, you need to configure the following parameters. ● **Automatically obtain DNS IPv4 address**: If **Acquisition method** is set to **Automatically obtain IP address** and **Network Protocols** is set to **IPv4** in the **Network Protocols** area, this parameter must be set to **Automatically obtain DNS IPv4 address**. When **Automatically obtain DNS IPv4 address** is selected, you do not need to configure the following parameters. ● **Automatically obtain DNS IPv6 address**: If **Acquisition method** is set to **Automatically obtain IP address** and **Network Protocols** is set to **IPv6** in the **Network Protocols** area, this parameter must be set to **Automatically obtain DNS IPv6 address**. When **Automatically obtain DNS IPv6 address** is selected, you do not need to configure the following parameters.
Registration Options	Select the option used to register with the DNS. ● **Host Name**: uses DHCP option 12 to register with the DNS. ● **DHCP Client FQDN**: uses DHCP option 81 to register with the DNS. If the DHCP server does not support DHCP option 81, select **Host Name**. If **DNS Server Settings** is set to **Manual**, only **Host Name** can be selected. If **DNS Server Settings** is set to **Automatically obtain DNS IPv4 address** or **Automatically obtain DNS IPv6 address**, **Host Name** or **DHCP Client FQDN** can be selected.
Domain Name	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.
Preferred Server	Enter the IP address of the preferred DNS server. This parameter is required if **DNS Server Settings** is set to **Manual**.
Alternate Server 1	Enter the IP address of alternate DNS server 1. This parameter is optional if **DNS Server Settings** is set to **Manual**.
Alternate Server 2	Enter the IP address of alternate DNS server 2. This parameter is optional if **DNS Server Settings** is set to **Manual**.

16. Click **Save**.

Configuring an iPMI VLAN

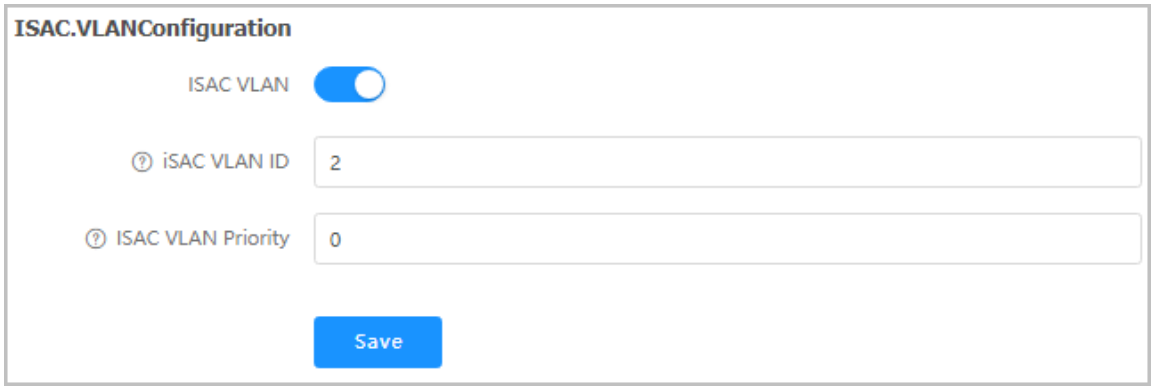
Abstract

This procedure describes how to configure an iPMI VLAN so that the iPMI management network port can be added to the VLAN.

Steps

17. Select **BMC Settings**. The **BMC Settings** page is displayed.
18. 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



19. Set the parameters in the **IPMI VLAN Configuration** area. For a description of the parameters, refer to Table 8-5.

Table 8-5 iPMI VLAN Parameter Descriptions

Parameter	Setting
iPMI VLAN	Select whether to enable the iPMI VLAN function. ● To enable the iPMI VLAN function, turn on the **iPMI VLAN** switch. In this case, the following parameters need to be configured. ● To disable the iPMI VLAN function, turn off the **iPMI VLAN** switch. In this case, the following parameters do not need to be configured. **iPMI VLAN** can be enabled if one of the following conditions is met: ● The **Select Mode** parameter in the **Network Port** area is set to **Automatic**, and the iPMI management network port is connected. ● The **Select Mode** parameter is set to **Fixed** in the **Network Port** area, and the iPMI management network port is specified as the management network port.
iPMI VLAN ID	Enter the iPMI VLAN ID. Range: 2–4094.
IPMI VLAN Priority	Enter the iPMI VLAN priority. Range: 0–7. A greater value indicates a higher priority.

20. Click **Save**.

Configuring an NCSI VLAN

Abstract

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

Steps

21. Select **BMC Settings**. The **BMC Settings** page is displayed.
22. From the navigation tree in the left pane, select **Network Settings**. The **Network Settings** page is displayed, see Figure 8-6.

Figure 8-6 Network Settings Page

23. Set the parameters in the **NCSI VLAN Configuration** area. For a description of the parameters, refer to Table 8-6.

Table 8-6 NCSI VLAN Parameter Descriptions

Parameter	Setting
NCSI VLAN	Select whether to enable the VLAN function. ● To enable the VLAN function, turn on the **VLAN** switch. In this case, the following parameters need to be configured. ● To disable the VLAN function, turn off the **VLAN** switch. In this case, the following parameters do not need to be configured. The VLAN function can be enabled if any of the following conditions is met: ● The **Select Mode** parameter is set to **Automatic** in the **Network Port** area, and an onboard NCSI is connected. ● The **Select Mode** parameter is set to **Fixed** in the **Network Port** area, and an onboard NCSI is specified as the management network port.
NCSI VLAN ID	Enter the VLAN ID. Range: 2–4094.

Parameter	Setting
NCSI VLAN Priority	Enter the VLAN priority. Range: 0–7. A greater value indicates a higher priority.

24. Click **Save**.

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:

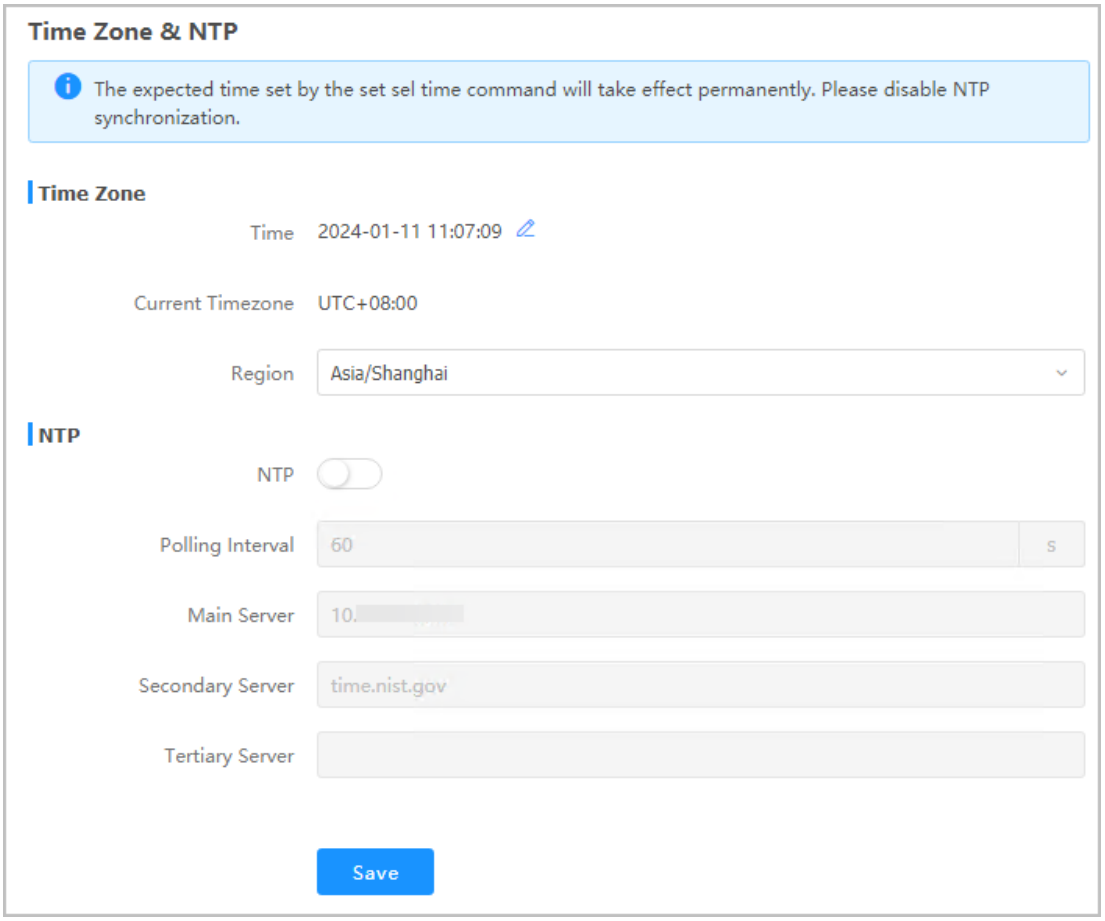
- Setting time manually
- Synchronizing time with an NTP server

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 8-7.

Figure 8-7 Time Zone & NTP Page



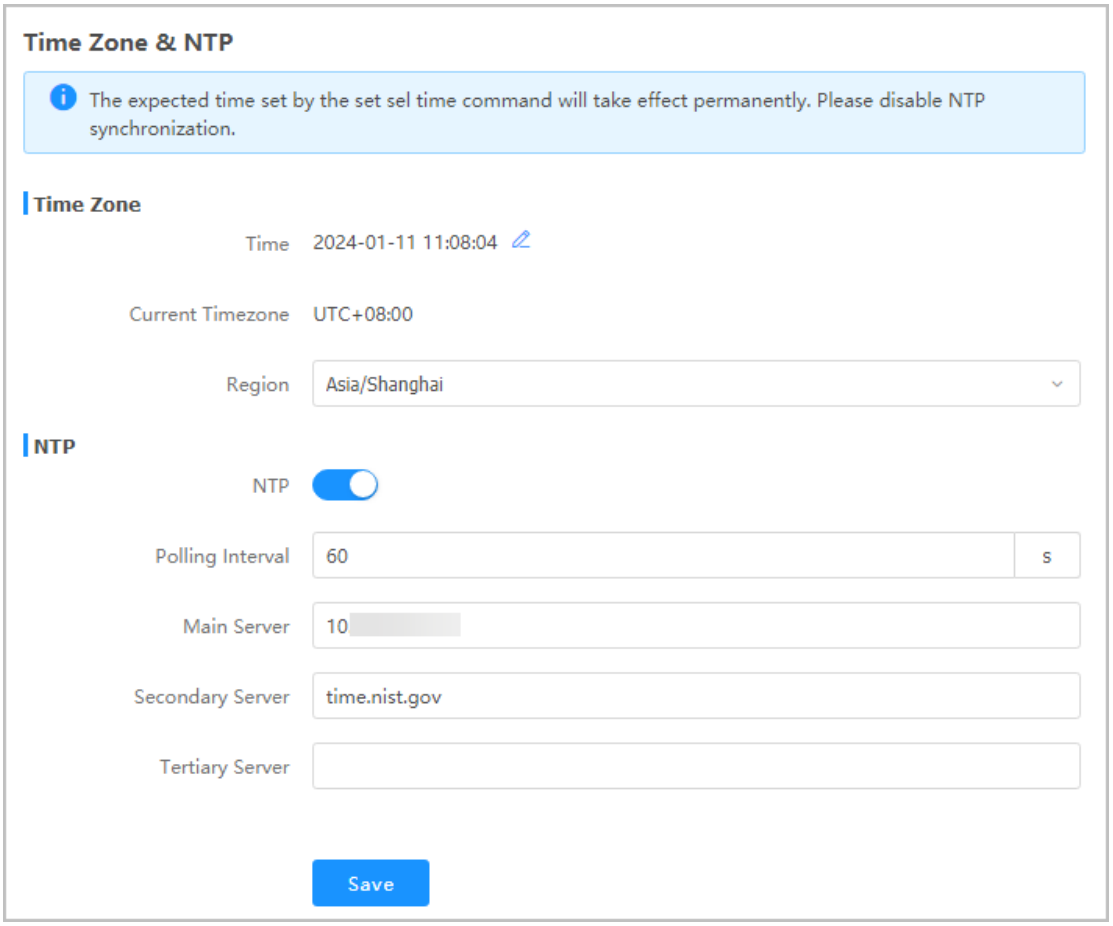
3. Click and then set the time.

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 8-8.

Figure 8-8 Time Zone & NTP Page



3. Set the parameters in the **NTP** area. For a description of the parameters, refer to Table 8-7.

Table 8-7 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 FQDN 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.

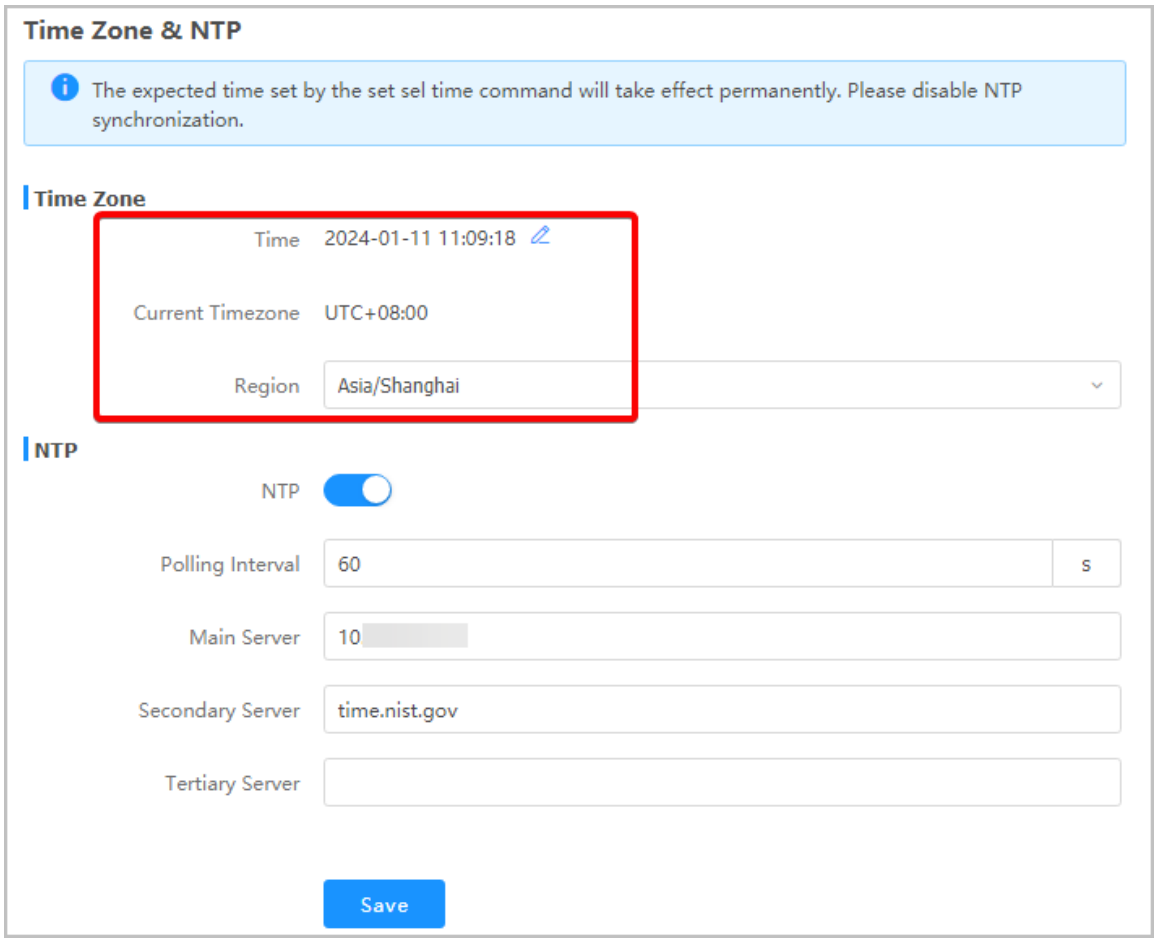
4. Click **Save**.

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 8-9.

Figure 8-9 Time Zone & NTP Page



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

Resetting the BMC on the Web Portal of the BMC

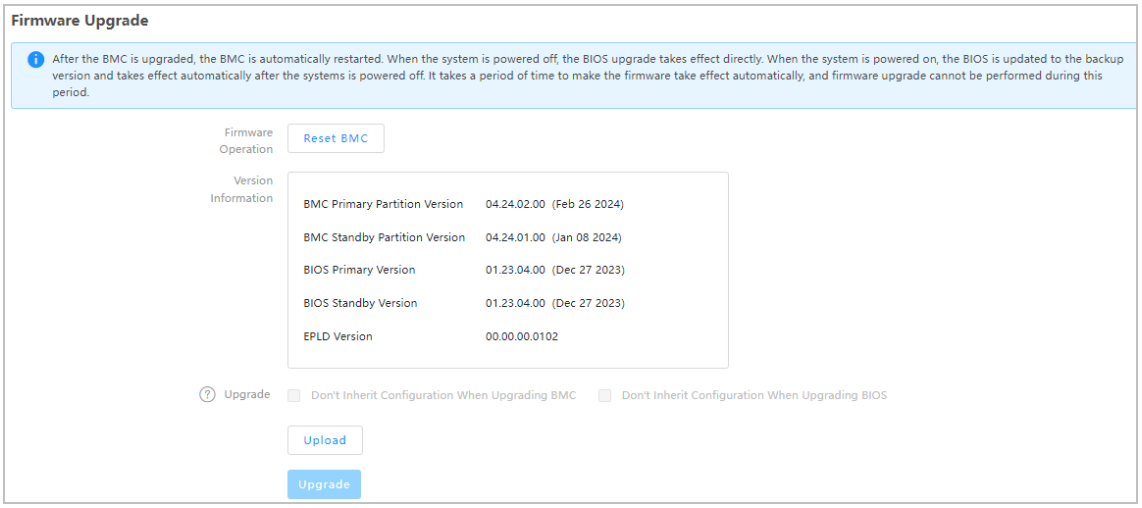
Abstract

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 8-10.

Figure 8-10 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.

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.

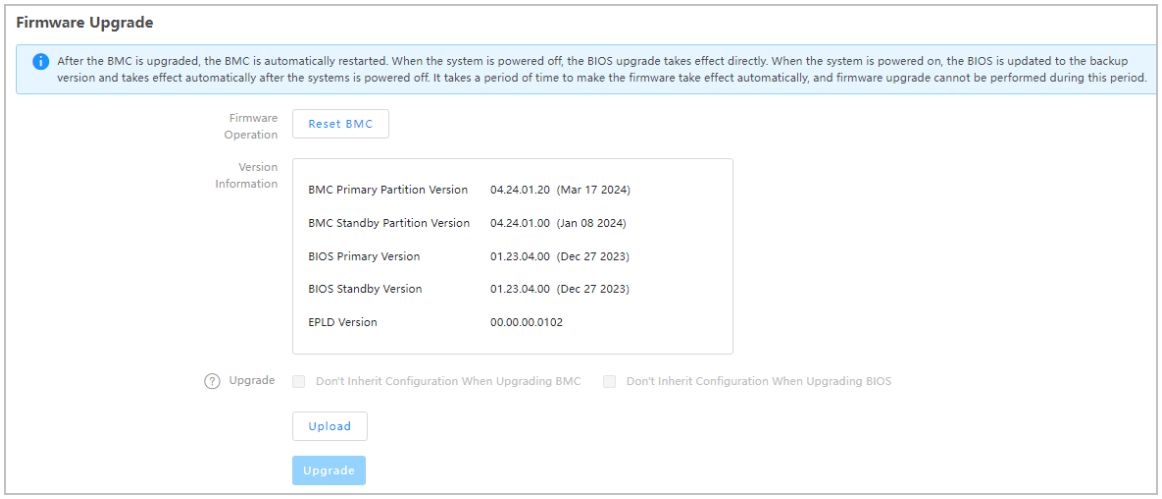
Note

Firmware files can be obtained on the **Software Download** page on the Web portal of the servers and storage products (https://enterprise.Vantageo.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 8-11.

Figure 8-11 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 to switch to another page. Otherwise, the upgrade process is interrupted.

Updating BMC Configurations

Abstract

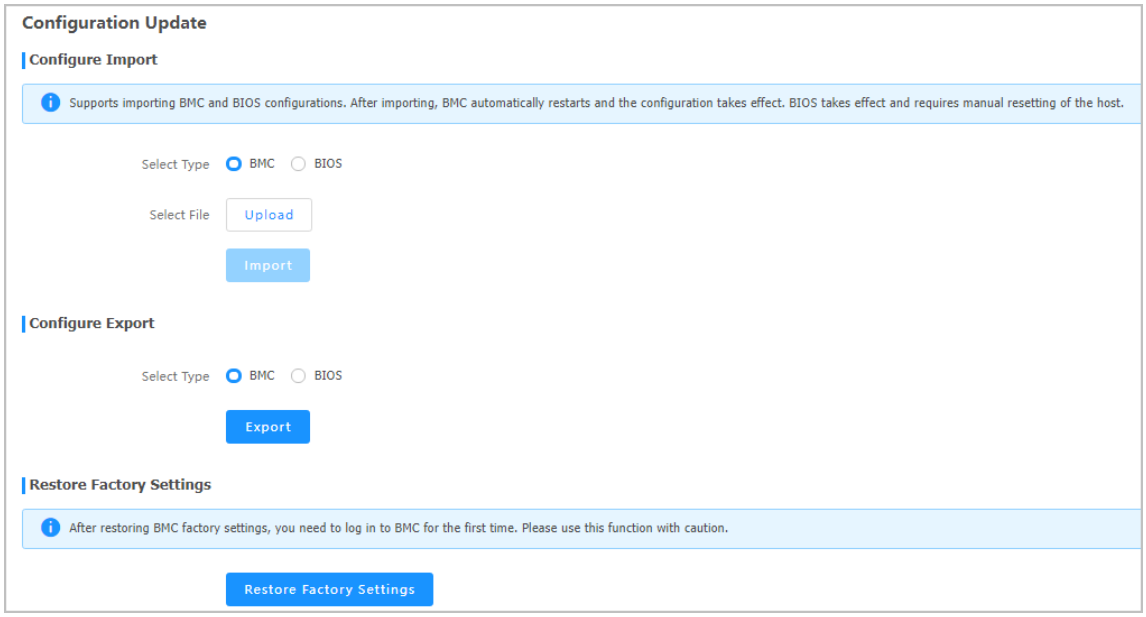
This procedure describes how to update BMC configurations online.

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 8-12.

Figure 8-12 Configuration Update Page



3. Perform the following operations as required.

If…	Then…
There is an existing BMC configuration file	a. Click **Upload**, and select the BMC configuration file in the displayed dialog box. b. Click **Import**, and confirm the import in the displayed message box.
There is no BMC configuration file	a. Click **Export** to export the current BMC configurations to your local PC. b. Edit the exported BMC configuration file. c. Click **Upload**, and select the BMC configuration file in the displayed dialog box. d. 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.

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.

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.

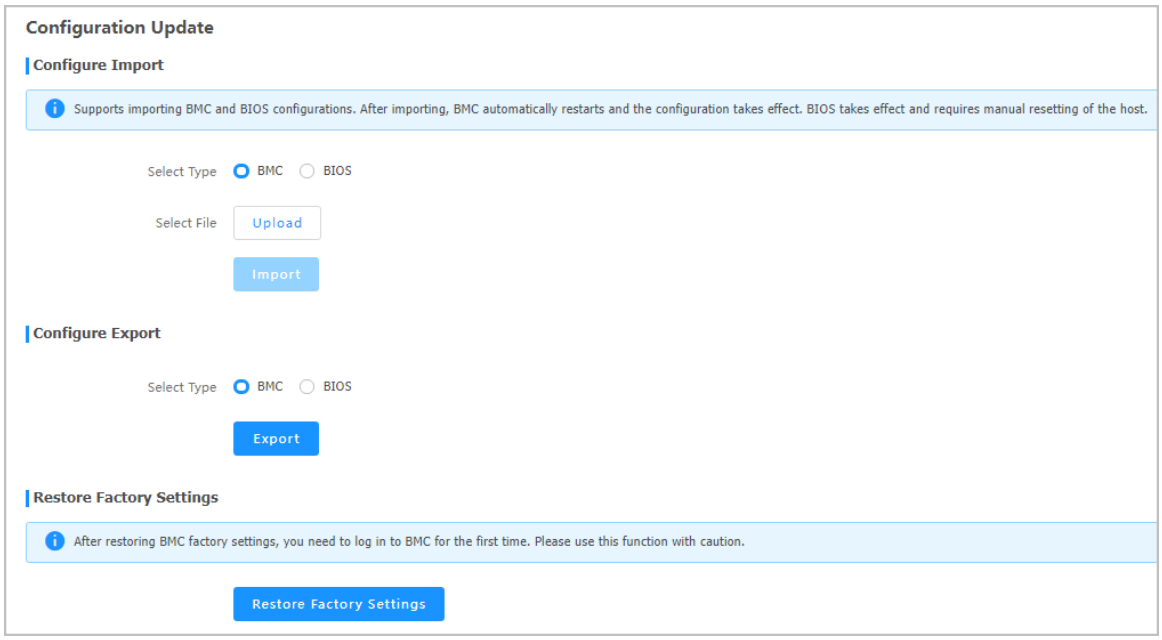
Note

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 8-13.

Figure 8-13 Configuration Update Page



3. Click **Restore Factory Defaults**.

User and Security

Adding a Local User

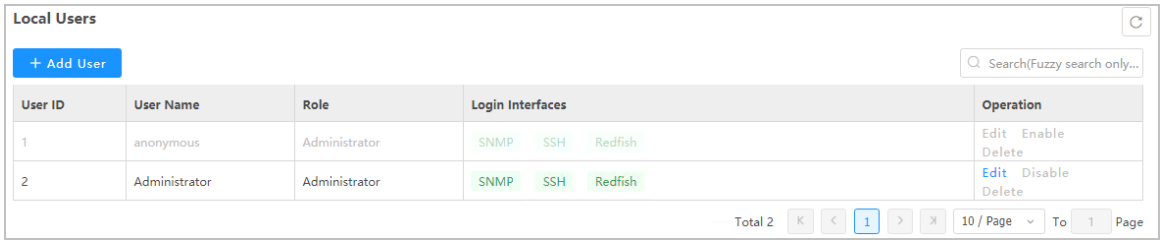
Abstract

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

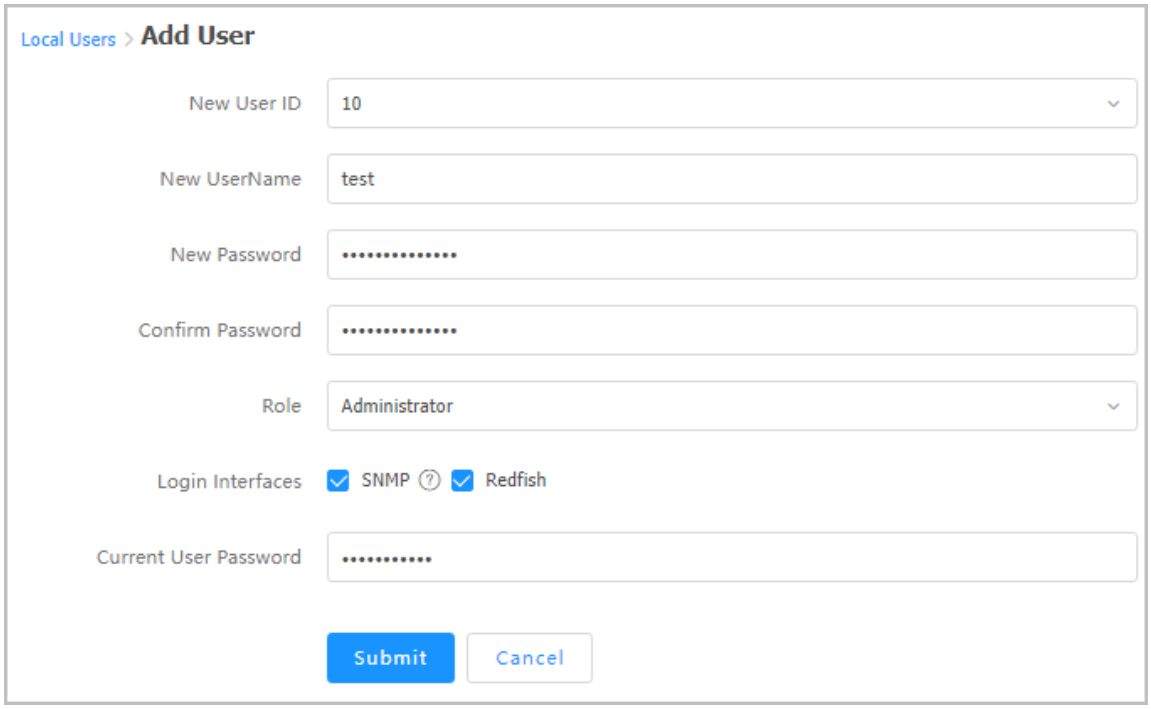
1. Select **User & Security**. The **User & Security** page is displayed.
2. From the navigation tree in the left pane, select **Local Users**. The **Local Users** page is displayed, see Figure 9-1.

Figure 9-1 Local Users Page



3. Click **Add User**. The **Add User** page is displayed, see Figure 9-2.

Figure 9-2 Add User Page



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. The allowed special characters include hyphens (-), underscores (_), and at symbols (@).
New Password	Enter the password of the new user. The password contains 5–20 characters (If **Login Interfaces** is set to **SNMP**, the password contains 8–20 characters.), including digits, letters (case sensitive), and special characters. It must contain one special character and characters from at least two of the following types: digits, uppercase letters, and lowercase letters. The allowed special characters include `, ~, !, @, $, %, ^, &, *, (,), -, _, =, +, \, |, [, {, },], :, ', ", ,, <, ., >, /, ?, #, ;. Historical passwords cannot be used anymore.

Parameter	Setting
	The password cannot be the same as the username in reverse order. For example, if the username is test, the password cannot be tset.
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. ● For SNMP interface–based login, select **SNMP**. ● For Redfish interface–based login, select **Redfish**. SSH-based login is supported for all users by default.
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	1. In the **Operation** column, click **Disable** for the user. The **Confirm** dialog box is displayed. 2. Enter the password of the currently logged-in user. 3. Click **Submit**.
Delete a local user	1. In the **Operation** column, click **Delete** for the user. The **Confirm** dialog box is displayed. 2. Enter the password of the currently logged-in user. 3. Click **Submit**.

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.

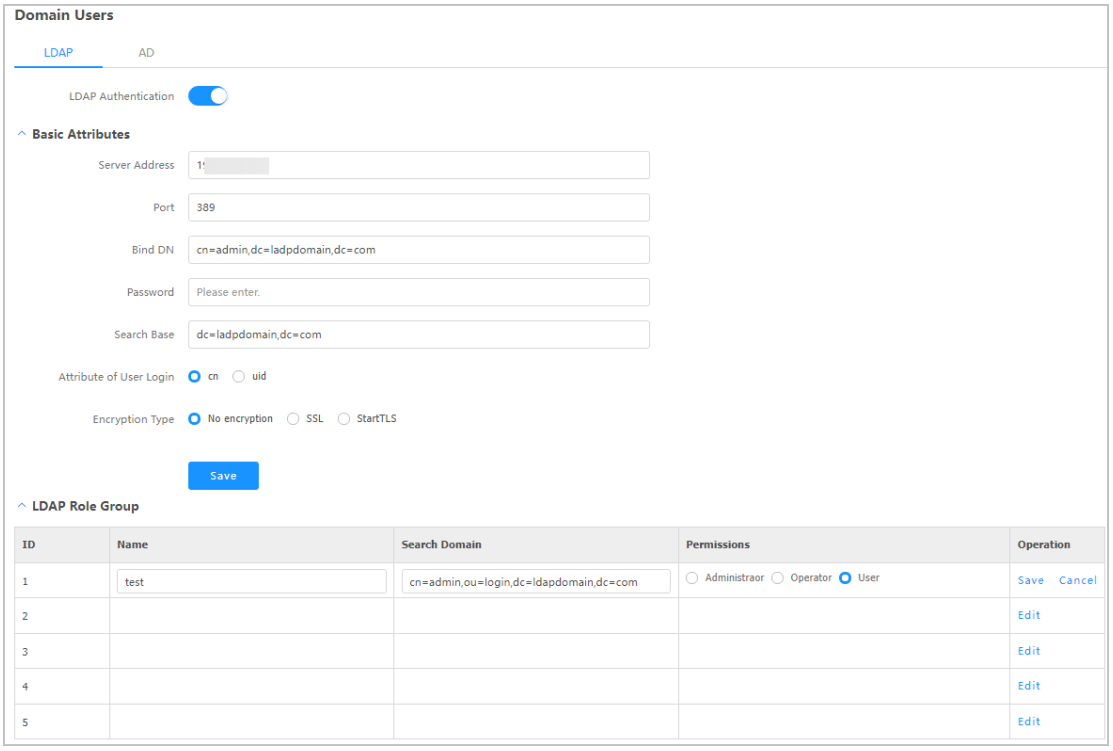
Prerequisite

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.
  2. 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



  3. Turn on the **LDAP Authentication** switch.
  4. 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 IP address or FQDN of the LDAP server.
Port	Enter the port number. Range: 1–65535. Default: 389. If **Encryption Type** is set to **SSL**, enter the port number *636*.
Bind DN	Enter the DN of the LDAP server, for example, *cn=admin,dc=ldap-domain,dc=com*.
Password	Enter the password for logging in to the LDAP server. It cannot be left blank. Range: 1–47 characters. **Bind DN** and **Password** are used to access the LDAP server.

Parameter	Setting
Search Base	Enter the storage location of the user information on the LDAP server, for example, *dc=ldapdomain,dc=com*.
Attribute of User Login	Select the user login attribute identified by the LDAP server. → If **Bind DN** contains cn, select **cn**. → If **Bind DN** contains uid, select **uid**.
Encryption Type	Select the type of encryption used by the LDAP server. → **No encryption**: indicates that no encryption is used. → **SSL**: indicates that SSL encryption is used. → **StartTLS**: indicates that StartTLS encryption is used.
Upload certificate	Click the corresponding certificate button and upload the certificate. If **Encryption Type** is set to **No encryption**, 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.

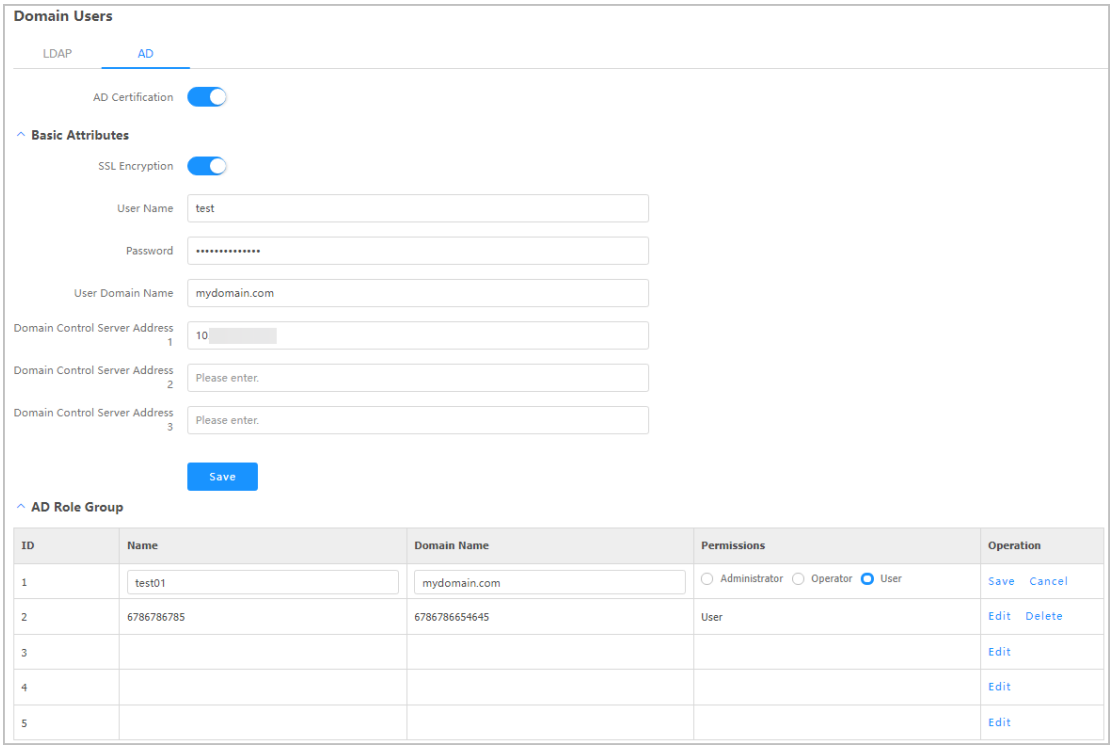
Table 9-3 LDAP Role Group Parameter Descriptions

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, *cn=admin,ou=login,dc=ldapdomain,dc=com*.
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



4. Turn on the **AD Authentication** switch.
5. 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 **SSL Encryption** switch. → To disable SSL encryption, turn off the **SSL Encryption** 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, *mydomain.com*, and is required.

Parameter	Setting
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, *mydomain.com*.
Permissions	Select the operation permissions of the role group on the BMC.

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

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

7. Select **User & Security**. The **User & Security** page is displayed.
8. 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

9. (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.

Note

You cannot delete yourself.

Configuring Permissions for a Customized Role

Abstract

The following roles exist in the system by default:

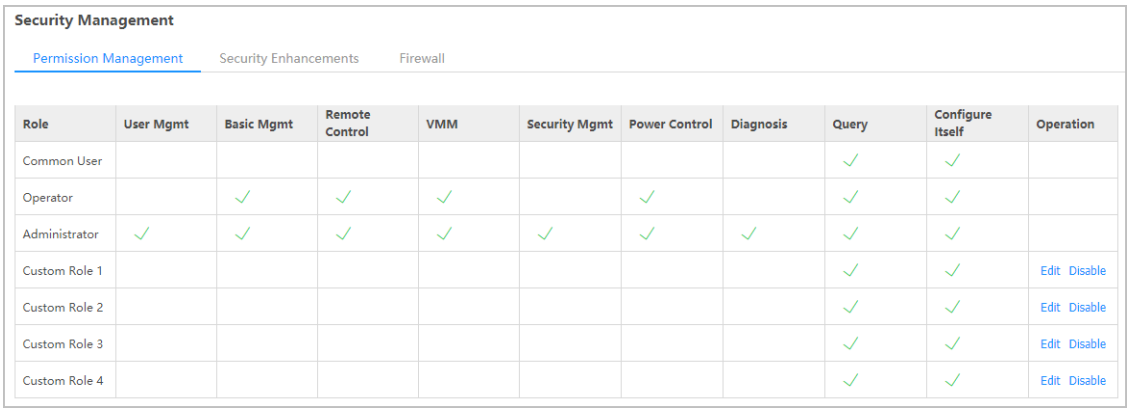
- Common user
- Operator
- Administrator
- Customized roles 1–4

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

Steps

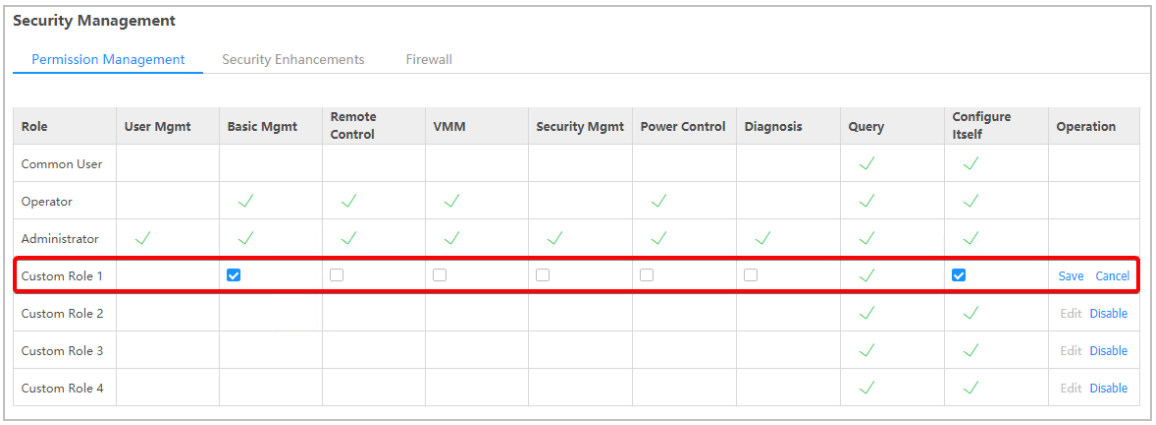
10. Select **User & Security**. The **User & Security** page is displayed.
11. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed, see Figure 9-6.

Figure 9-6 Security Management Page



12. 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



13. Select the corresponding permissions.
14. 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.

Note

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

Configuring Security Enhancement Parameters

Abstract

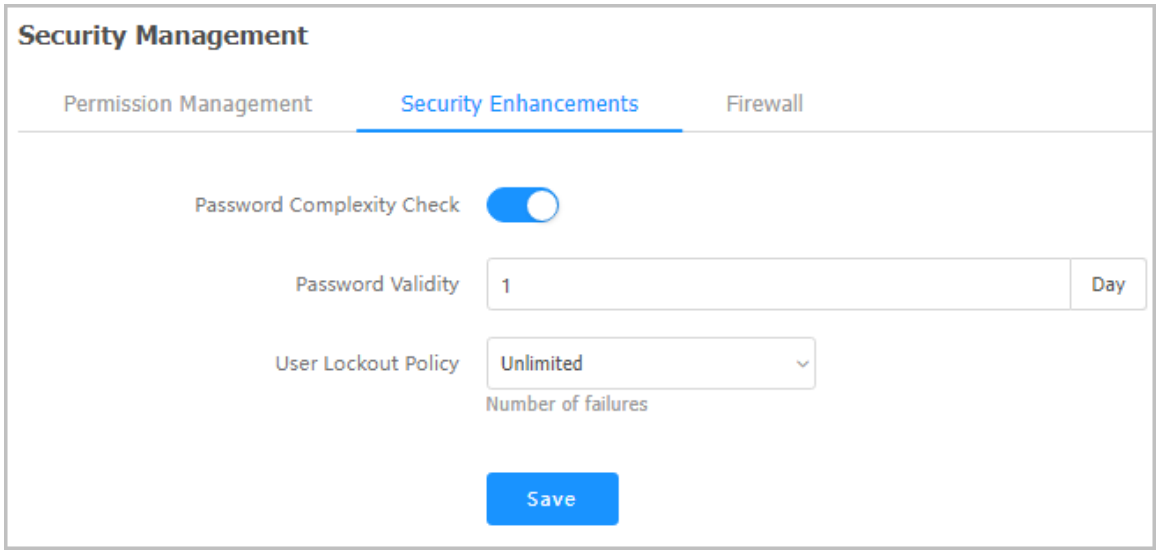
To enhance user login security, you can configure security enhancement parameters, including:

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

Steps

15. Select **User & Security**. The **User & Security** page is displayed.
16. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
17. Click **Security Enhancements**. The **Security Enhancements** tab is displayed, see Figure 9-8.

Figure 9-8 Security Enhancements Tab



18. 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. ● To enable password complexity check, turn on the **Password Complexity Check** switch. ● To disable password complexity check, turn off the **Password Complexity Check** switch.
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.

19. Click **Save**.

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.

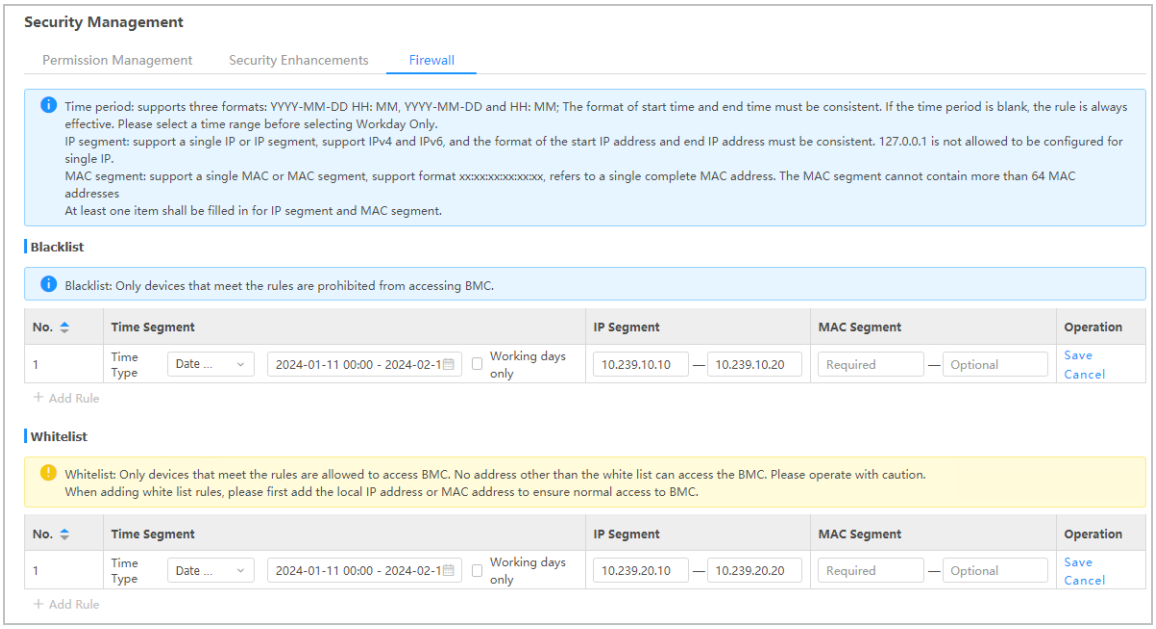
Note: When enabling the whitelist policy, you must first add the IP or MAC address of your local PC (acting as a client PC) to the whitelist to ensure that your local PC can access the Web portal of the BMC.

This procedure describes how to configure firewall parameters.

Steps

20. Select **User & Security**. The **User & Security** page is displayed.
21. From the navigation tree in the left pane, select **Security Management**. The **Security Management** page is displayed.
22. Click **Firewall**. The **Firewall** tab is displayed, as shown in Figure 9-9.

Figure 9-9 Firewall Tab



23. Perform the following operations as needed.

To…	Do…
Add an item to the blacklist	a. In the **Blacklist** area, click **Add Rule**. The blacklist parameters are activated. b. Set the parameters. For a description of the parameters, refer to Table 9-7. c. Click **Save**.
Add an item to the whitelist	a. In the **Whitelist** area, click **Add Rule**. The whitelist parameters are activated. b. Set the parameters. For a description of the parameters, refer to table 9-7. c. Click **Save**.

Table 9-7 Blacklist/Whitelist Parameter Descriptions

Parameter	Description
Time Segment	From the **Time Type** list, select the desired time type, and set the time period accordingly. The format of the start time and end time must be the same. Before selecting **Working days only**, 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.
IP Segment	Enter an IP address or an IP address segment. IPv4 or IPv6 format is supported. For a single IP address, 127.0.0.1 is disallowed. For an IP address segment, the format of the start address and end address must be the same.
MAC Segment	Enter a MAC address or a MAC address segment. The format is xx:xx:xx:xx:xx:xx. A MAC address segment can contain a maximum of 64 MAC addresses. At least one of the **IP Segment** and **MAC Segment** parameters must be set.

Configuring Two-Factor Authentication

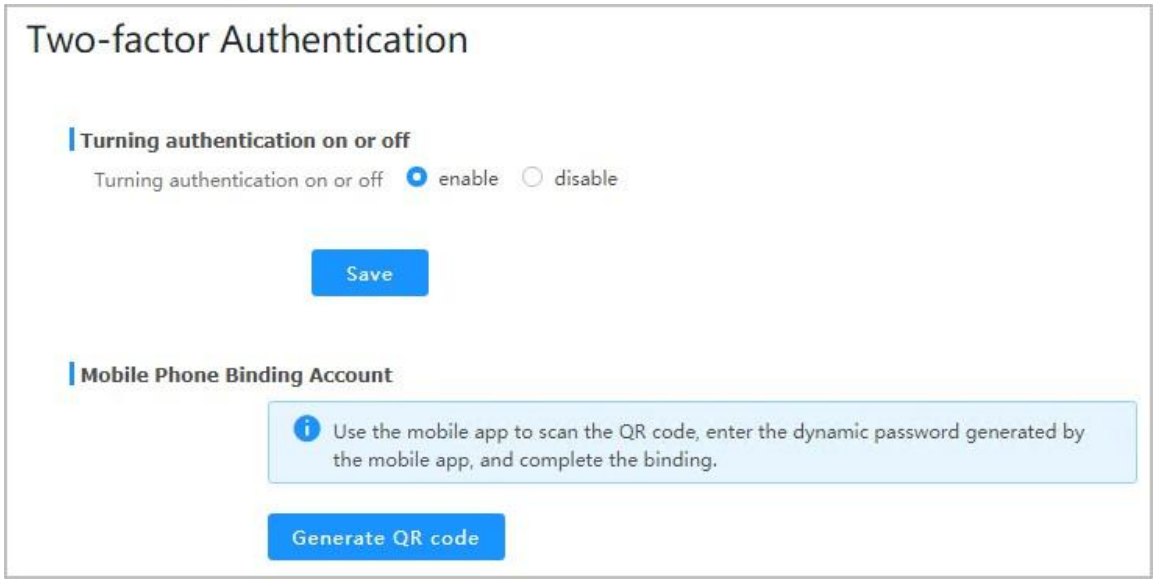
Abstract

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

Steps

24. Select **User & Security**. The **User & Security** page is displayed.
25. 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



26. Select whether to enable two-factor authentication. Options:
    - **enable**: enables two-factor authentication.
    - **disable**: disables two-factor authentication.
27. Click **Save**.
28. (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.