BMC User Manual

Document Version: V2.8

Release Date: October 28, 2022

Disclaimer

The purchased products, services and features shall be bound by the contract made between the customer and us. All or part of the products, services and features described herein may not be within your purchase or usage scope. Unless otherwise agreed in the contract, we make no express or implied statement or warranty on the contents herein. Images provided herein are for reference only and may contain information or features that do not apply to your purchased model. This manual is only used as a guide. We shall not be liable for any damage, including but not limited to loss of profits, loss of information, interruption of business, personal injury, or any consequential damage incurred before, during, or after the use of our products. We assume you have sufficient knowledge of servers and are well trained in protecting yourself from personal injury or preventing product damages during operation and maintenance. The information in this manual is subject to change without notice. We shall not be liable for technical or editorial errors or omissions contained in this manual.

Trademarks

All the trademarks or registered trademarks mentioned herein may be the property of their respective holders.

Support

Email	Technical Support	serversupport@aivres.com
	RMA/ARMA Support	serversupportusa@aivres.com
Web	Official Website	www.aivres.com
	Service Portal	service.aivres.com

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	A potential for serious injury, or even death if not properly handled
⚠ WARNING	A potential for minor or moderate injury if not properly handled

Symbol	Description
⚠ CAUTION	A potential loss of data or damage to equipment if not properly handled
ⓘ IMPORTANT	Operations or information that requires special attention to ensure successful installation or configuration
🗒 NOTE	Supplementary description of document information

Revision History

Version	Date	Description of Changes
V1.0	2021/02/07	Initial release.
V2.0	2021/06/23	Optimized the format and contents.
V2.1	2021/09/21	• Added the description that the Web GUI and some of the features may vary with different models. • Changed Section 3.12.3 Video Log to 3.12.3 Screen Recording. • Added instructions for viewing the multi-node server power supply information and fan management.
V2.2	2021/09/28	Optimized the format of Table 2-4.
V2.3	2021/10/27	Updated the query function description in Table 3-60.
V2.4	2021/11/16	Added 2 server models to Table 1-1.
V2.5	2022/01/18	Optimized some descriptions.
V2.6	2022/03/12	Unified the width of all tables.

Version	Date	Description of Changes
V2.7	2022/06/01	• Updated the default system timeout from 3 min to 30 min in 3.1.2. • Updated the latest system event log count from 9 to 10 in Table 3-3. • Added 2 server models to Table 1-1.
V2.8	2022/10/28	• Added description that JVIewer isn't supported on some models in 3.5.1.2 • Optimized the formats of some tables

Table of Contents

1 Overview

1.1 Purpose

This manual describes the functional specifications and other details of the Baseboard Management Controller (BMC).

1.2 Intended Audience

This manual is intended for:

- Technical support engineers
- Product maintenance engineers
- Server administrators

It is recommended that server installation, configuration, or maintenance is performed by only experienced technicians with knowledge in servers.

NOTE

Some interfaces and commands for production, assembly and return-to-depot, and advanced commands for locating faults, if used improperly, may cause equipment abnormality or business interruption. This is not described herein. Please contact us for such information.

1.3 Scope of Application

This manual applies to the following products:

Table 1-1 Product Model

Product Model	**Two-socket Server**	**Four-socket Server**	**AI Server**	**Multi-node Server**
NF8260M6		●		
NF8480M6		●		
NF5280M6	●			
NF5180M6	●			
NF5270M6	●			
NF5260M6	●			
NF5466M6	●			

Product Model	Two-socket Server	Four-socket Server	AI Server	Multi-node Server
NF5266M6	●			
NF5468M6	●		●	
NF5488M6	●		●	
NF5688M6	●		●	
i24M6	●			●
i48M6	●			●
SA5280M6	●			
SA5112M6	●			
SA5270M6	●			
SA5212M6	●			
i24LM6	●			●
NF5260FM6	●			

NOTE

The Web GUI and some of the features may vary with different models.

2 BMC Overview

2.1 Introduction

BMC is a versatile control unit for server management.

The BMC features include:

- IPMI 2.0 compliant with IPMI interfaces such as KCS, LANPLUS, and IPMB
- Management protocols such as IPMI 2.0, HTTPS, SNMP, and SMASH CLP
- Web GUI
- Redfish
- Management network port: Dedicated/NCSI
- Console redirection (KVM) and virtual media
- Serial Over LAN (SOL)
- Diagnostic logs: System Event Logs (SEL), audit logs, IDL and one-key collection logs
- BMC hardware watchdog: Fans will speed up to secure speeds for proper cooling if there is no response from BMC within 4 minutes.
- Intel® Intelligent Power Node Manager 4.0
- Event alerts: SNMP Trap (v1/v2c/v3), email alerts and syslog
- BMC firmware stored in dual flash
- Storage management: Monitors and configures RAID controller/drives/virtual drives
- Firmware update: BMC/BIOS/CPLD/FPGA/PSU
- Device status monitoring and diagnosis

2.2 Software Interfaces

2.2.1 IPMI 2.0

2.2.1.1 Interface Channel ID

Table 2-1 Interface Channel ID List

Channel ID	Interface	Purpose	Session Management Support
0x00	Primary IPMB	Unused	No
0x06	Secondary IPMB	ME access	No
0x0A	Third IPMB	Unused	No
0x01	Primary LAN	Dedicated Interface	Yes
0x08	Secondary LAN	NCSI Interface	Yes
0x0F	KCS/SMS	In-band IPMI communication	No

2.2.1.2 System Interface

The LPC interface is supported and used as the physical link for KCS messaging.

2.2.1.3 IPMB Interface

BMC supports Intel NM 4.0. Secondary IPMB is used as the communication interface.

2.2.1.4 LANPLUS Interface

BMC supports IPMI V2.0 and is compatible with V1.5. It supports receiving and sending IPMI messages based on RMCP or RMCP+ format.

BMC supports up to 2 network management interfaces (dedicated interface and shared interface).

The following table lists the supported cipher suites in IPMI:

Table 2-2 Supported Cipher Suites in IPMI

ID	Authentication Algorithm	Integrity Algorithm	Encryption Algorithm
1	RAKP-HMAC-SHA1	None	None
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	None
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128

ID	Authentication Algorithm	Integrity Algorithm	Encryption Algorithm
6	RAKP-HMAC-MD5	None	None
7	RAKP-HMAC-MD5	HMAC-MD5-128	None
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	None
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_SHA256	None	None
16	RAKP_HMAC_SHA256	HMAC-SHA256-128	None
17	RAKP_HMAC_SHA256	HMAC-SHA256-128	AES-CBC-128

2.2.1.5 IPMI Commands

The following tables define the IPMI commands that BMC supports.

IPMI Spec standard commands:

Table 2-3 IPMI NetFn

NetFn	App	Chassis	S/E	Storage	Transport	Bridge
Value	0x06	0x00	0x04	0x0A	0x0C	0x02

Table 2-4 IPMI Spec Standard Commands

Command	Function	NetFn	CMD	Support
IPMI Device “Global” Commands	Get Device ID	App	0x01	YES
	Broadcast ‘Get Device ID’ [1]	App	0x02	YES
	Cold Reset	App	0x03	YES
	Warm Reset	App	0x04	YES
	Get Self Test Results	App	0x05	YES
	Manufacturing Test On	App	0x06	YES
	Set ACPI Power State	App	0x07	YES
	Get ACPI Power State	App	0x08	YES
	Get Device GUID	App	0x09	YES
	Get NetFn Support	App	0x10	YES
	Get Command Support	App	0x0A	YES
	Get Command Sub-function Support	App	0x0B	YES
	Get Configurable Commands	App	0x0C	YES

Command	Function	NetFn	CMD	Support
	Get Configurable Command Sub-functions	App	0x0D	YES
	Set Command Enables	App	0x60	YES
	Get Command Enables	App	0x61	YES
	Set Command Sub-function Enables	App	0x62	YES
	Get Command Sub-function Enables	App	0x63	YES
	Get OEM NetFn IANA Support	App	0x64	YES
BMC Watchdog Timer Commands	Reset Watchdog Timer	App	0x22	YES
	Set Watchdog Timer	App	0x24	YES
	Get Watchdog Timer	App	0x25	YES
BMC Device and Messaging Commands	Set BMC Global Enables	App	0x2E	YES
	Get BMC Global Enables	App	0x2F	YES
	Clear Message Flags	App	0x30	YES
	Get Message Flags	App	0x31	YES
	Enable Message Channel Receive	App	0x32	YES
	Get Message	App	0x33	YES
	Send Message	App	0x34	YES
	Read Event Message Buffer	App	0x35	YES
	Get BT Interface Capabilities	App	0x36	YES
	Get System GUID	App	0x37	YES
	Set System Info Parameters	App	0x58	YES
	Get System Info Parameters	App	0x59	YES
	Get Channel Authentication Capabilities	App	0x38	YES
	Get Session Challenge	App	0x39	YES
	Activate Session	App	0x3A	YES
	Set Session Privilege Level	App	0x3B	YES
	Close Session	App	0x3C	YES
	Get Session Info	App	0x3D	YES
	Get AuthCode	App	0x3F	YES

Command	Function	NetFn	CMD	Support
	Set Channel Access	App	0x40	YES
	Get Channel Access	App	0x41	YES
	Get Channel Info Command	App	0x42	YES
	Set User Access Command	App	0x43	YES
	Get User Access Command	App	0x44	YES
	Set User Name	App	0x45	YES
	Get User Name Command	App	0x46	YES
	Set User Password Command	App	0x47	YES
	Activate Payload	App	0x48	YES
	Deactivate Payload	App	0x49	YES
	Get Payload Activation Status	App	0x4A	YES
	Get Payload Instance Info	App	0x4B	YES
	Set User Payload Access	App	0x4C	YES
	Get User Payload Access	App	0x4D	YES
	Get Channel Payload Support	App	0x4E	YES
	Get Channel Payload Version	App	0x4F	YES
	Get Channel OEM Payload Info	App	0x50	YES
	Master Write-Read	App	0x52	YES
	Get Channel Cipher Suites	App	0x54	YES
	Suspend/Resume Payload Encryption	App	0x55	YES
	Set Channel Security Keys	App	0x56	YES
	Get System Interface Capabilities	App	0x57	YES
	Firmware Firewall Configuration	App	0x60-0x64	NO
Chassis Device Commands	Get Chassis Capabilities	Chassis	0x00	YES
	Get Chassis Status	Chassis	0x01	YES
	Chassis Control	Chassis	0x02	YES

Command	Function	NetFn	CMD	Support
	Chassis Reset	Chassis	0x03	YES
	Chassis Identify	Chassis	0x04	YES
	Set Front Panel Button Enables	Chassis	0x0A	YES
	Set Chassis Capabilities	Chassis	0x05	YES
	Set Power Restore Policy	Chassis	0x06	YES
	Set Power Cycle Interval	Chassis	0x0B	YES
	Get System Restart Cause	Chassis	0x07	YES
	Set System Boot Options	Chassis	0x08	YES
	Get System Boot Options	Chassis	0x09	YES
	Get POH Counter	Chassis	0x0F	YES
Event Commands	Set Event Receiver	S/E	0x00	YES
	Get Event Receiver	S/E	0x01	YES
	Platform Event (a.k.a. “Event Message”)	S/E	0x02	YES
Sensor Device Commands	Get Device SDR Info	S/E	0x20	YES
	Get Device SDR	S/E	0x21	YES
	Reserve Device SDR Repository	S/E	0x22	YES
	Get Sensor Reading Factors	S/E	0x23	YES
	Set Sensor Hysteresis	S/E	0x24	YES
	Get Sensor Hysteresis	S/E	0x25	YES
	Set Sensor Threshold	S/E	0x26	YES
	Get Sensor Threshold	S/E	0x27	YES
	Set Sensor Event Enable	S/E	0x28	YES
	Get Sensor Event Enable	S/E	0x29	YES
	Re-arm Sensor Events	S/E	0x2A	YES
	Get Sensor Event Status	S/E	0x2B	YES
	Get Sensor Reading	S/E	0x2D	YES
	Set Sensor Type	S/E	0x2E	YES
	Get Sensor Type	S/E	0x2F	YES
	Set Sensor Reading And Event Status	S/E	0x30	YES
FRU Device Commands	Get FRU Inventory Area Info	Storage	0x10	YES
	Read FRU Data	Storage	0x11	YES
	Write FRU Data	Storage	0x12	YES

Command	Function	NetFn	CMD	Support
SDR Device Commands	Get SDR Repository Info	Storage	0x20	YES
	Get SDR Repository Allocation Info	Storage	0x21	YES
	Reserve SDR Repository	Storage	0x22	YES
	Get SDR	Storage	0x23	YES
	Add SDR	Storage	0x24	YES
	Partial Add SDR	Storage	0x25	YES
	Delete SDR	Storage	0x26	YES
	Clear SDR Repository	Storage	0x27	YES
	Get SDR Repository Time	Storage	0x28	YES
	Set SDR Repository Time	Storage	0x29	YES
	Enter SDR Repository Update Mode	Storage	0x2A	YES
	Exit SDR Repository Update Mode	Storage	0x2B	YES
	Run Initialization Agent	Storage	0x2C	YES
SEL Device Commands	Get SEL Info	Storage	0x40	YES
	Get SEL Allocation Info	Storage	0x41	YES
	Reserve SEL	Storage	0x42	YES
	Get SEL Entry	Storage	0x43	YES
	Add SEL Entry	Storage	0x44	YES
	Partial Add SEL Entry	Storage	0x45	YES
	Delete SEL Entry	Storage	0x46	YES
	Clear SEL	Storage	0x47	YES
	Get SEL Time	Storage	0x48	YES
	Set SEL Time	Storage	0x49	YES
	Get Auxiliary Log Status	Storage	0x5A	YES
	Set Auxiliary Log Status	Storage	0x5B	YES
	Get SEL Time UTC Offset	Storage	0x5C	YES
	Set SEL Time UTC Offset	Storage	0x5D	YES
LAN Device Commands	Set LAN Configuration Parameters	Transport	0x01	YES
	Get LAN Configuration Parameters	Transport	0x02	YES
	Suspend BMC ARPs	Transport	0x03	YES
	Get IP/UDP/RMCP Statistics	Transport	0x04	NO
Serial/Modem Device Commands	Set Serial/Modem Configuration	Transport	0x10	YES
	Get Serial/Modem Configuration	Transport	0x11	YES

Command	Function	NetFn	CMD	Support
	Set Serial/Modem Mux	Transport	0x12	YES
	Get TAP Response Codes	Transport	0x13	NO
	Set PPP UDP Proxy Transmit Data	Transport	0x14	NO
	Get PPP UDP Proxy Transmit Data	Transport	0x15	NO
	Send PPP UDP Proxy Packet	Transport	0x16	NO
	Get PPP UDP Proxy Receive Data	Transport	0x17	NO
	Serial/Modem Connection Active	Transport	0x18	NO
	Callback	Transport	0x19	YES
	Set User Callback Options	Transport	0x1A	YES
	Get User Callback Options	Transport	0x1B	YES
	Set Serial Routing Mux	Transport	0x1C	NO
	SOL Activating	Transport	0x20	NO
	Set SOL Configuration Parameters	Transport	0x21	YES
	Get SOL Configuration Parameters	Transport	0x22	YES
Command Forwarding Commands	Forwarded Command	Bridge	0x30	NO
	Set Forwarded Commands	Bridge	0x31	NO
	Get Forwarded Commands	Bridge	0x32	NO
	Enable Forwarded Commands	Bridge	0x33	NO
Bridge Management Commands (ICMB)	Get Bridge State	Bridge	0x00	NO
	Set Bridge State	Bridge	0x01	NO
	Get ICMB Address	Bridge	0x02	NO
	Set ICMB Address	Bridge	0x03	NO
	Set Bridge Proxy Address	Bridge	0x04	NO
	Get Bridge Statistics	Bridge	0x05	NO
	Get ICMB Capabilities	Bridge	0x06	NO
	Clear Bridge Statistics	Bridge	0x08	NO
	Get Bridge Proxy Address	Bridge	0x09	NO

Command	Function	NetFn	CMD	Support
	Get ICMB Connector Info	Bridge	0x0A	NO
	Get ICMB Connection ID	Bridge	0x0B	NO
	Send ICMB Connection ID	Bridge	0x0C	NO
Discovery Commands (ICMB)	PrepareForDiscovery	Bridge	0x10	NO
	GetAddresses	Bridge	0x11	NO
	SetDiscovered	Bridge	0x12	NO
	GetChassisDeviceId	Bridge	0x13	NO
	SetChassisDeviceId	Bridge	0x14	NO
Bridging Commands (ICMB)	BridgeRequest	Bridge	0x20	NO
	BridgeMessage	Bridge	0x21	NO
Event Commands (ICMB)	GetEventCount	Bridge	0x30	NO
	SetEventDestination	Bridge	0x31	NO
	SetEventReceptionState	Bridge	0x32	NO
	SendICMBEventMessage	Bridge	0x33	NO
	GetEventDestination (optional)	Bridge	0x34	NO
	GetEventReceptionState (optional)	Bridge	0x35	NO

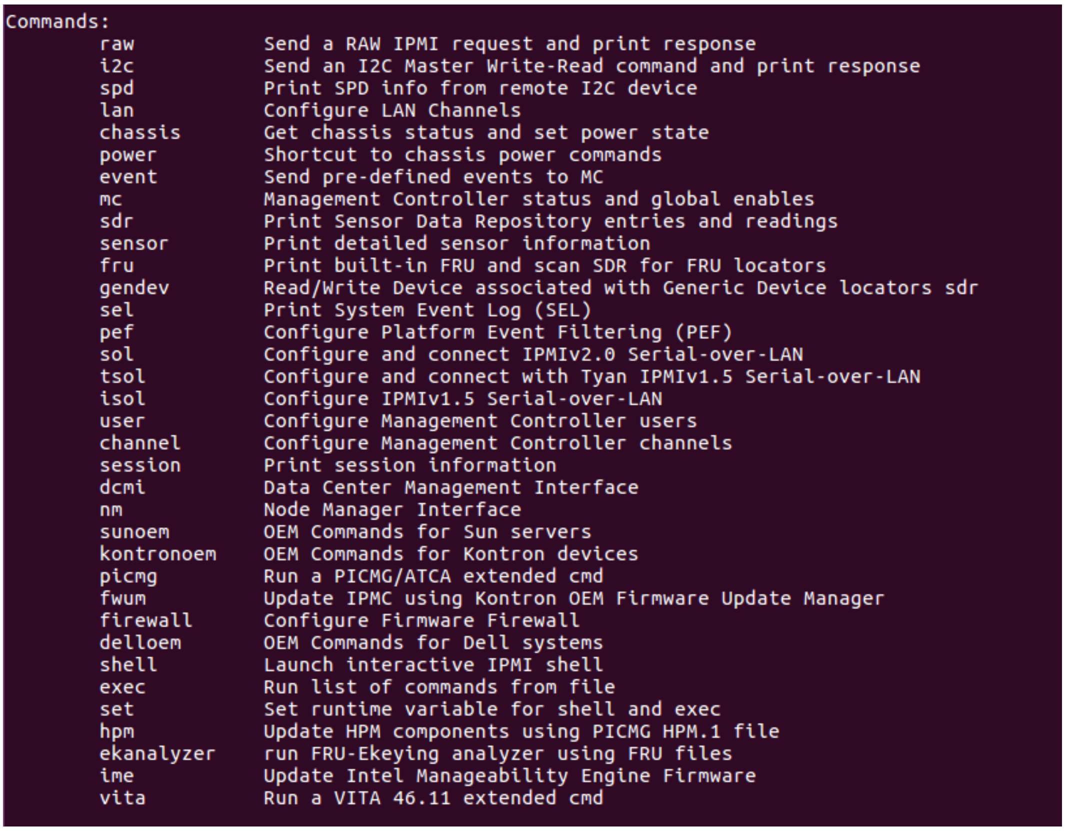
2.2.1.6 IPMI CMD Tool

IPMItool is usually used to send IPMI commands, including in-band commands over KCS interfaces from the host operating system, and out-of-band commands over LANPLUS interfaces from a remote system. IPMItool is available in Windows OS and Linux OS. See the official IPMI documentation for the use of IPMI commands.

Supported interfaces:

- Open interface: Linux OpenIPMI interface (default)
- LANPLUS interface: IPMI v2.0 RMCP+ LAN interface

Figure 2-1 IPMItool Commands



```
Commands:
        raw           Send a RAW IPMI request and print response
        i2c           Send an I2C Master Write-Read command and print response
        spd           Print SPD info from remote I2C device
        lan           Configure LAN Channels
        chassis       Get chassis status and set power state
        power         Shortcut to chassis power commands
        event         Send pre-defined events to MC
        mc            Management Controller status and global enables
        sdr           Print Sensor Data Repository entries and readings
        sensor        Print detailed sensor information
        fru           Print built-in FRU and scan SDR for FRU locators
        gendev        Read/Write Device associated with Generic Device locators sdr
        sel           Print System Event Log (SEL)
        pef           Configure Platform Event Filtering (PEF)
        sol           Configure and connect IPMIv2.0 Serial-over-LAN
        tsol          Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
        isol          Configure IPMIv1.5 Serial-over-LAN
        user          Configure Management Controller users
        channel       Configure Management Controller channels
        session       Print session information
        dcmi          Data Center Management Interface
        nm            Node Manager Interface
        sunoem        OEM Commands for Sun servers
        kontronoem    OEM Commands for Kontron devices
        picmg         Run a PICMG/ATCA extended cmd
        fwum          Update IPMC using Kontron OEM Firmware Update Manager
        firewall      Configure Firmware Firewall
        delloem       OEM Commands for Dell systems
        shell         Launch interactive IPMI shell
        exec          Run list of commands from file
        set           Set runtime variable for shell and exec
        hpm           Update HPM components using PICMG HPM.1 file
        ekanalyzer    run FRU-Ekeying analyzer using FRU files
        ime           Update Intel Manageability Engine Firmware
        vita          Run a VITA 46.11 extended cmd
```

2.2.2 Web GUI

You can access Web GUI with HTTPS (port 443). HTTP is disabled by default. Web GUI provides management interfaces for users to view system information, system events and status, and control the managed server.

Table 2-5 Supported Operating Systems and Browsers

Client OS	Browser Version
Windows 7.1 x64 Windows 8 x64 Windows 10 x64 Ubuntu 14.04.03 LTS x64	On Windows clients: Edge, Firefox 43+, Chrome 47+, and Internet Explorer 11+ On Linux clients: Firefox 43+ and Chrome 47+

See 3 Introduction to BMC Web GUI for more information about Web GUI.

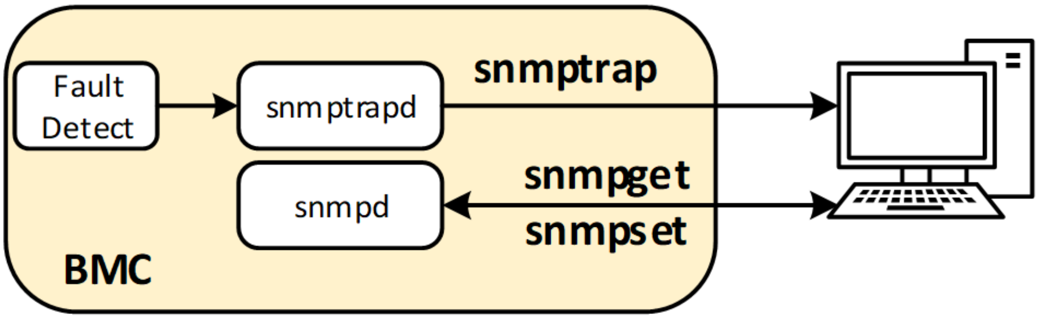
2.2.3 SNMP

SNMP is a network management standard based on the TCP/IP family and a standard protocol for managing nodes (such as servers, workstations, routers, and switches) on IP networks. Network administrators can learn about network problems by receiving notifications and alarm event reports from network nodes via SNMP.

A remote agent can access BMC via SNMP to get network information, user information, and server information (including temperature, voltage and fan speed), configure BMC parameters and manage servers via SNMP.

- SNMP Get/Set/Trap are supported.
- SNMP v1/v2c/v3 are supported.
- SNMP v3 supports the authentication algorithm MD5 or SHA. The encryption algorithm is DES or AES.
- SNMP enables users to query system health status, sensor status, hardware status, and device asset information.
- SNMP Set can be used to configure most BMC parameters.
- BMC sends alarms via SNMP Trap to the remote Trap receiver.

Figure 2-2 How SNMP Works



2.2.4 SMASH CLP CLI

SMASH CLP CLI is a command line tool with which you can perform some operations on BMC.

See 4 Introduction to SMASH CLP CLI Functions for details about SMASH CLP CLI. See 5 Terms and Abbreviations for the full name of SMASH and CLP.

2.2.5 Redfish

Redfish is a new management standard that uses hypermedia RESTful interface to represent data. Being model-oriented, it can express the relationships between components and the semantics of the services and components within them. The model is also easy to extend. For a server that supports Redfish, the client can obtain BMC information by sending HTTP requests or perform specified operations on BMC. The client can access the Redfish service through the HTTP client. Common request methods include GET, PUT, POST, PATCH and DELETE. Data is sent and received in JSON format.

For specific operations on BMC Redfish, refer to the Redfish user manual.

2.3 Security Management

2.3.1 Security Features

- User account security management

BMC account security policies include password length and complexity, password validity period, password history check, and lockout on login failures, as well as measures including old password verification for password change, and a prompt to change default password at first login to ensure account security.

- Security protocols and secure ports against attacks

BMC maintains a minimum number of network service ports and closes services not in use. By default, it uses the security protocol and closes the ports using the insecure protocol.

- Role-based access control

BMC supports multiple types of users, including IPMI, Web, SSH and SNMP users, who are assigned different privileges based on their roles in the principle of least privilege.

- Secure update and secure boot

The BMC image file is signed using the encryption algorithm with a secure key length, and firmware update and boot can be allowed only after the signature is verified so as to prevent the image from being tampered with. In addition, it provides a mismatch prevention mechanism to prevent the image files of different manufacturers, different product models and different firmware types from updating each other.

- Secure image backup

BMC supports dual flash with each flash storing an image file, and dual image update to ensure the availability of image files.

- Scenario-based access control

For security, the access to server management interfaces is minimized via control on IP address, port, time period, MAC, etc. Users can create whitelist access control rules based on scenarios to prevent unauthorized access.

- Log management

BMC records non-query operations of all interfaces, including such information as the time when the operation was performed, interface, source IP address, username, and operation. BMC supports log export through Web, log rotation and syslog forwarding to avoid log loss when log space is full. IDL is a log type unique to BMC and is used to record IPMI sensor-based event logs on the BMC device. A handling suggestion is provided for each log to help users with log diagnosis and analysis.

- Data encryption storage and transmission

Sensitive data stored in logs, files or cookies of BMC is encrypted using security algorithms. HTTPS is used for communication by default, and LDAP, AD, RADIUS and syslog data can also be transmitted over SSL to ensure secure data transmission. BMC also allows you to enable the KVM and VNC encryption functions, which encrypt data transmitted to and from the remote console.

- Certificate management

BMC allows you to generate and replace SSL certificates. To improve security, it is suggested that you replace the current certificate with your own certificate and public and private keys, and update the certificate in a timely manner to ensure its validity. You can also import an LDAP certificate to authenticate and encrypt data transmission, thus improving system security.

2.3.2 General Principles

- Manage and configure BMC using an internal private network other than the business network.
- Close unused service ports and use secure protocols for communication.
- Regularly audit BMC operation logs and install firmware security patches.

2.3.3 Security Hardening

2.3.3.1 Default User/Password

Refer to the following table for default passwords on BMC before getting started.

Table 2-6 Default User/Password

Default User/Password	Default Value	Description
BMC Default Username/Password	Username: admin Password: admin	The Admin user, under the role of administrator, has the highest level of privilege. To change the default password, please follow the password complexity requirements.
Uboot Password	root@u600t	U-Boot commands are debugging commands used to load underlying software and debug underlying devices. To change the password, please refer to the BMC configuration manual.
SNMP Community String	Public community string: root@0531 Private community string: root@0531	To change the default community string, please follow the password complexity requirements. The community string and password can be set by using IPMI commands.
BMC Debugging Serial Port User/Password	Username: sysadmin Password: superuser	Only login via the BMC debugging serial port is allowed for BMC debugging and maintenance.

NOTE

To ensure system security, it is recommended to modify the default values at first login.

2.3.3.2 User Management

BMC implements the role-based detail management of local users. System privileges are divided into 9 types: User Configuration, General Configuration, Power Control, Remote Media, Remote KVM, Security Configuration, Debug Diagnose, Query Function, and Itself Configuration. The "Administrator", "Operator" and "User" roles are set by default, whose privileges cannot be configured or modified. There are also 4 custom role groups (OEM1, OEM2, OEM3 and OEM4) available. The system administrator can assign privileges flexibly to a custom role according to business maintenance requirements.

It is recommended that the system administrator create an audit role and a maintenance role, and assign Security Configuration and Query Function privileges to the audit role and Debug Diagnose and Query Function privileges to the maintenance role. In addition, auditors can be created under the audit role, and maintainers under the maintenance role. For information on user creation, role assignment and privilege setting, refer to 3.11.2 User Detail Management.

2.3.3.3 Authentication Management

BMC supports local authentication and third-party remote authentication (LDAP/AD and Radius).

The local authentication mode is suitable for small-scale networking environments, such as small- and medium-sized enterprises. In this mode, username and password can be used for authentication, and public keys are recommended for authentication of auto logins via SSH to the BMC command line.

The third-party remote authentication methods such as LDAP are applicable to environments with a large number of users, as the number and privileges of users are set on the server side and are not subject to local settings (16 local users). Logging in to the BMC system with the user domain, group domain, and LDAP username and password belonging to the user domain in the domain controller can improve system security. LDAP users can access the BMC system by logging in to the BMC Web GUI, logging in to the BMC command line via SSH, or using Redfish interfaces. To secure the transmission of user authentication data and avoid LDAP server-side request forgery, it is recommended to enable LDAP over SSL and enable certificate authentication of remote controller line.

2.3.3.4 Service Management

BMC maintains network service ports based on the minimization principle, that is, network service ports used for BMC debugging must be closed when the BMC comes into use, ports using insecure protocols are closed by default, and unused network services must be closed. The services and ports are as follows:

Table 2-7 Services and Ports

Service	Non-Secure Port	Secure Port
Web	TCP/80	TCP/443
SSH	N/A	TCP/22
KVM	TCP/7578	TCP/7582
CD-Media	TCP/5120	TCP/5124
HD-Media	TCP/5123	TCP/5127
KVM on HTML5	TCP/80	TCP/443
VNC	TCP/5900	TCP/5901
SNMP	N/A	UDP/161
SNMP Multiplexer	N/A	TCP/199

Service	Non-Secure Port	Secure Port
IPMI	N/A	TCP, UDP/623

The services supported by BMC currently that have insecure ports include Web, KVM, CD-Media, HD-Media, and VNC, and their insecure ports should be closed according to the minimization principle.

Unused services are also recommended to be closed. When it is necessary to use these services, security configurations should be enabled, including session timeout and session limit. Session timeout threshold can be configured for Web, KVM, SSH, SOLSSH, VNC, etc. and can be set to different values depending on application scenarios. A value of no more than 300 seconds is recommended. The maximum number of sessions can be configured for Web, KVM, CD-Media, HD-Media, VNC, and so on, and this option is enabled by default.

You can set these in **BMC Settings** > **Services** by referring to Section 3.11.3 Services.

2.3.3.5 Password Policy

The BMC password policy involves password complexity, password validity period, history password record and lockout on login failures. To prevent password guessing and brute-force attack, a password should contain at least 8 characters of 3 or more types. Local users should enable password validity period check and history password record check. It is also recommended to enable the lockout on login failures.

You can set these in **BMC Settings** > **User Detail Management** by referring to Section 3.11.2 User Detail Management.

2.3.3.6 Access Control

The BMC access control mainly reduces attack surfaces through system firewalls, including IP address firewall, port firewall and MAC firewall. For security reasons, the access to server management interfaces is restricted to the minimum range from dimensions of time, location (IP/port/MAC) and behavior. You can create a whitelist for login as needed.

You can set these in **BMC Settings** > **System Firewall** by referring to 3.11.4 System Firewall.

2.3.3.7 Encryption Authentication

- LDAP

BMC supports the import of an LDAP certificate. To improve system security, it is recommended to enable LDAP/E-Directory authentication and select SSL or StartTLS encryption to authenticate and encrypt data transmission.

- KVM

It is recommended to configure VMedia instance settings and enable encrypt media redirection packets. See 3.5.3 Media Redirection Settings for details.

- SSL

Certificate management involves various operations for managing the SSL certificate. A self-signed SSL certificate is used by default, and the signature algorithm is SHA-256 or RSA-2048. For security reasons, we recommend that you replace the default custom certificate with your own certificate at first login to access BMC in a secure manner. See 3.11.6 SSL Settings for specific settings.

- Syslog over SSL

Syslog supports encryption during transmission. To ensure the security of data transmission, the TLS protocol should be configured for Syslog. See 3.6.2 Log Settings for details.

- SNMP

BMC supports SNMP SET/GET. The SNMP v3 with the authentication algorithm of SHA and encryption algorithm of AES is recommended. BMC also supports SNMP Trap. Users can enable the Trap receiver and set the Trap destination IP address on the BMC Web GUI, and BMC will automatically send an event it detects to the Trap receiver. See 3.6.7 SNMP Trap Settings for details.

- VNC

It is recommended to enable KVM encryption in remote session settings. See 3.5.3 Media Redirection Settings for details.

- Virtual Media

Media Redirection allows users to present various media devices and images via clients or remotely, and connect them as virtual USB to the server where BMC is located. Virtual media supports security (authentication or encryption) settings. See 3.5.3 Media Redirection Settings for details.

- SSH

BMC supports Smash-Lite CLI. Users can log in to BMC via SSH and enter Smash-Lite CLI. That is, log in to the CLI of the BMC via SSH. The CLI appears after login.

2.3.3.8 System Wiping

When a server device is to be scrapped or recycled, system wiping is required to protect data security and personal privacy. System wiping includes the following:

- Restore the default settings

BMC allows you to restore the system to default settings in the Web GUI. Log in to the Web GUI and go to **System Maintenance** > **Restore Factory Defaults** to restore default settings.

- Clear logs

System event log clearing: Log in to the Web GUI, go to **Logs & Alarms** > **System Event Log**, and click **Clear Event Logs** to delete all existing sensor log records.

IDL clearing: Go to **Logs & Alarms** > **IDL**, and click **Clear IDL** to delete all IDL logs on the BMC.

Alarm log clearing: When an alarm message is generated in the syslog, an alarm log is created. The alarm messages not handled are displayed on the **Logs & Alarms** > **Current Alarms** page. The alarm logs will be automatically cleared after the failures are removed.

- Clear screenshots

Log in to the Web GUI, and go to the **Fault Diagnosis** > **Capture Screen** page on which existing screenshots are displayed. Click **Delete Screen** to clear the screenshot files.

- Wipe drive data

ISQP and third-party tools can be used for drive data wiping. The data on drives will be securely and completely deleted and cannot be recovered.

2.3.3.9 System Recovery

- Automatic recovery

Watchdog mechanism: BMC supports automatic recovery in case of code execution exceptions. When the BMC kernel panics, or BMC runs out of resources or is unable to update firmware, the hardware watchdog's timeout reset mechanism enables BMC to automatically return to normal. In addition, BMC regularly detects the working status of internal services (such as IPMI, KVM and virtual media) through the software watchdog, and restarts the services in case of any exceptions in them.

Dual image mechanism: BMC supports dual flash with each flash storing an image file. When either of the images is damaged, the other flash is automatically used to ensure the availability of image file.

- Manual recovery

Users can manually restore various configurations of the BMC system by selecting the configuration file that has been backed up. Log in to the BMC Web GUI, go to **BMC Settings** > **Restore Configuration**, select the desired configuration file and restore it. See 3.11.8 Restore Configuration for details.

BMC allows rollback after firmware update failures. When the firmware update fails, users can carry out a rollback using the image file in the backup area to ensure the availability of firmware.

In addition, users can also restart BMC tasks through the Web or IPMI command in case of exceptions. See 3.12.4 Module Restart for specific operations.

2.3.3.10 Log Audit

To send BMC alarm messages to the remote Trap receiver securely using SNMP Trap, it is recommended to configure SNMP v3 for the Trap receiver, with SHA as the authentication protocol and AES as the encryption protocol, and the authentication and privacy passwords should follow the password complexity requirements. Meanwhile, the BMC sender should be set according to the parameters of the receiver. See 3.6.7 SNMP Trap Settings for the configuration method.

Since the local storage space of BMC is limited, to ensure log information is recorded normally, it is recommended to set a circular policy (default policy) for event logs, and use the syslog function to transmit the event logs and audit logs of BMC to the remote syslog server for storage. TLS protocol should be configured for syslog to ensure transmission security.

2.3.3.11 Others

We will release security bulletins and update patch packs from time to time for product security vulnerabilities discovered internally or externally. Please upgrade the BMC firmware as needed after assessing the risks according to actual application scenarios.

3 Introduction to BMC Web GUI

3.1 Getting Started

3.1.1 Basic Operations

Web GUI allows you to manage servers on visualized and user-friendly interfaces with online help.

You can perform basic operations, as shown in the following table, on the BMC Web GUI.

Table 3-1 Basic Operations

Operations	**Description**
Change language	You can change the language in the drop-down menu on the login page or other pages. Chinese and English are supported.
View system information	Select **Home** > **Information** > **System Information**. The **System Information** page displays the basic information of major server components, including CPU, Memory, Power Supply, Device Inventory, Hard Drive, Network Adapter, and Security Chip.
View online help	On a BMC Web GUI page, click ❓ to view the help information.
Refresh page	On a BMC Web GUI page, click ↻ to refresh the page.
View and log out the current user	On a BMC Web GUI page, click 👤 to display the user currently logged in, and click the drop-down arrow on the right to view this user and his/her privilege group or log out the user.

3.1.2 User Login

Description:

You can log in to the BMC Web GUI from the **User Login** page.

NOTE

For information on how to query the BMC IP address, see Section 2 Querying the IP Address of the Network Interface in the BMC configuration manual.

- A maximum of 20 users can log in to the Web GUI concurrently.
- The system timeout is 30 minutes by default. You will be automatically logged out after 30 minutes of inactivity in the Web GUI. In this case, you need to log in again using your username and password.
- You will be locked out after the specified number of failed login attempts. You cannot log in again until the set lockout duration expires.
- To ensure system security, change your password the first time you log in and at regular intervals thereafter.

Parameters:

Table 3-2 User Login

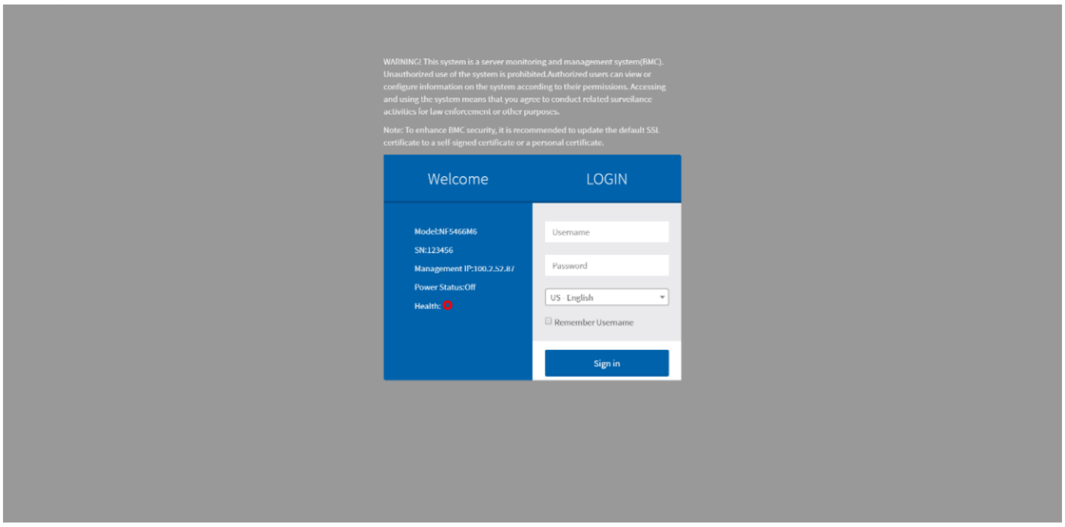
Parameter	Description
Username	The username for login to the BMC system.
Password	The password for login.
Language	The display language of the Web GUI.

Steps:

This document uses Chrome as an example to describe how to work with the BMC Web GUI.

1. Type **https://BMC_IP** in the browser address bar and press <Enter> to open the page as shown in Figure 3-1.

Figure 3-1 User Login



WARNING! This system is a server monitoring and management system(BMC). Unauthorized use of the system is prohibited.Authorized users can view or configure information on the system according to their permissions. Accessing and using the system means that you agree to conduct related surveilance activities for law enforcement or other purposes.

Note: To enhance BMC security, it is recommended to update the default SSL certificate to a self-signed certificate or a personal certificate.

Model:NF5466M6

SN:123456

Management IP:100.2.52.87

Power Status:Off

Health: ☒

NOTE

The port number can be changed (see the "3.11.3 Services" section). HTTP is available on port 80 (disabled by default) and HTTPS on port 443. If the port number has been changed, you need to specify it when logging in, for example, https://BMC_IP:sslport.

---

2. Enter the username and password for login to the BMC.
3. Select a display language of the Web GUI.
4. Click **Sign in**.

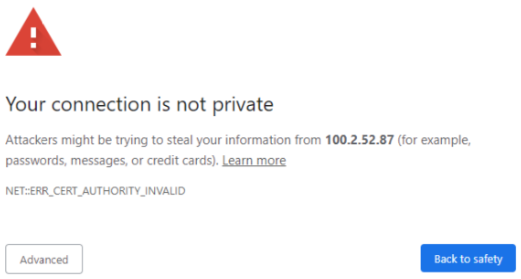
After successful login, the **General Information** page is displayed.

- End

NOTE

1. An IPv6 address must be enclosed in square brackets ([ ]). Examples:
   IPv4 address: "100.3.8.100"
   IPv6 address: "[fc00::64]"
2. A security warning will be displayed the first time you log in to the BMC Web GUI. In this case, click **Advanced** and select **Proceed to [IP address] (unsafe)** to continue. On the login page that appears, enter your username and password, and press <Enter> to log in.

Figure 3-2 Security Warning

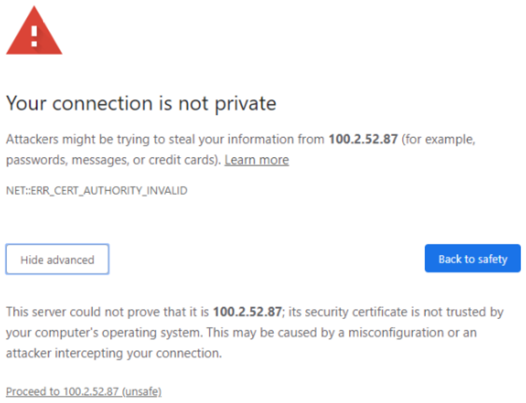


Your connection is not private

Attackers might be trying to steal your information from **100.2.52.87** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

Figure 3-3 Security Warning_Proceed to [IP address] (unsafe)



Your connection is not private

Attackers might be trying to steal your information from **100.2.52.87** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **100.2.52.87**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 100.2.52.87 (unsafe)

3.2 General Information

Description:

The **General Information** page provides:

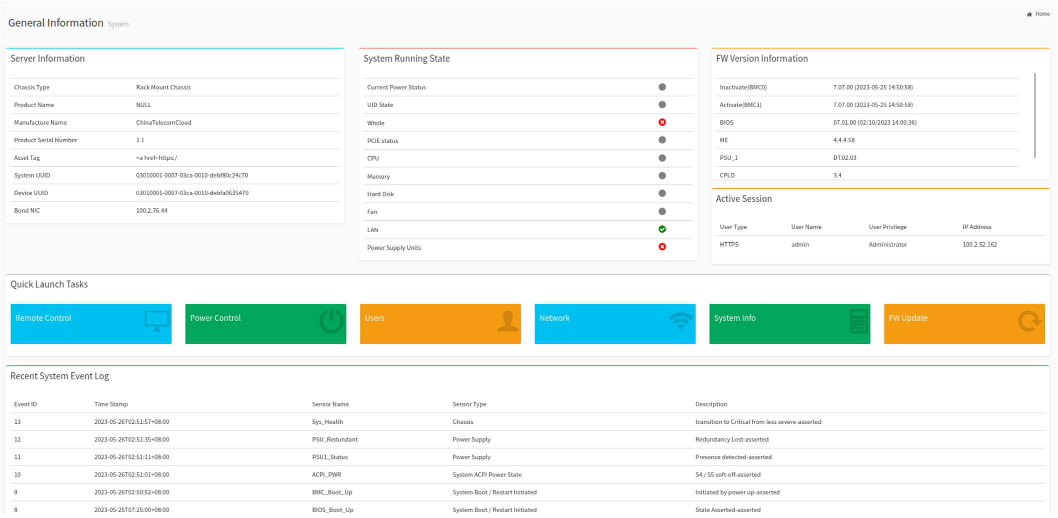
- Server Information

- System Running State
- FW Version Information
- Active Session
- Quick Launch Tasks
- Recent System Event Log

Screen description:

The **General Information** page is displayed after successful login. You can also go to this page by selecting **Information** > **General Information** in the navigation pane, as shown below.

Figure 3-4 General Information



General Information System

Server Information

Chassis Type	Rack Mount Chassis
Product Name	NULL
Manufacture Name	ChinaTelecomCloud
Product Serial Number	1 1
Asset Tag	<a href=https:/
System UUID	03010001-0007-03ca-0010-debf80c24c70
Device UUID	03010001-0007-03ca-0010-debfa0635470
Bond NIC	100.2.76.44

System Running State

Current Power Status	●
UID State	●
Whole	✗
PCIE status	●
CPU	●
Memory	●
Hard Disk	●
Fan	●
LAN	✓
Power Supply Units	✗

FW Version Information

Inactivate(BMC0)	7.07.00 (2023-05-25 14:50:58)
Activate(BMC1)	7.07.00 (2023-05-25 14:50:58)
BIOS	07.01.00 (02/10/2023 14:00:36)
ME	4.4.4.58
PSU_1	DT.02.03
CPLD	3.4

Active Session

User Type	User Name	User Privilege	IP Address
HTTPS	admin	Administrator	100.2.52.162

Quick Launch Tasks

Recent System Event Log

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
13	2023-05-26T02:51:57+08:00	Sys_Health	Chassis	transition to Critical from less severe-asserted
12	2023-05-26T02:51:35+08:00	PSU_Redundant	Power Supply	Redundancy Lost-asserted
11	2023-05-26T02:51:11+08:00	PSU1_Status	Power Supply	Presence detected-asserted
10	2023-05-26T02:51:01+08:00	ACPI_PWR	System ACPI Power State	S4 / S5 soft-off-asserted
9	2023-05-26T02:50:52+08:00	BMC_Boot_Up	System Boot / Restart Initiated	Initiated by power up-asserted
8	2023-05-25T07:25:00+08:00	BIOS_Boot_Up	System Boot / Restart Initiated	State Asserted-asserted

Parameters:

Table 3-3 General Information

Item	**Information**
Server Information	The basic information of the server, including: • **Chassis Type**: The server type • **Product Name**: The server name • **Manufacture Name**: The server manufacturer • **Product Serial Number**: The serial number of the server • **Asset Tag**: The asset tag of the server • **System UUID**: The system UUID of the server

Item	Information
	• **Device UUID**: The device UUID of the server • **Bond NIC**: IP address of the server's bond NIC
System Running State	The running state of the server, including: • **Current Power Status**: Indicates whether the server is powered on or off. • **UID State**: Indicates whether the UID LED is on or off. • **Whole**: The overall status of the server. • **CPU**: The health status of the CPU. • **Memory**: The health status of the memory modules. • **Hard Disk**: The health status of the drives. • **Fan**: The health status of the fans. • **LAN**: The health status of the network. • **Power Supply Units**: The health status of the PSUs. Note: The health status of each module may be: ✅ Normal/Present 🟢 LED on ⚠ Warning ❌ Critical ⚪ Absent/LED off
FW Version Information	The version information of the following firmware: • BMC • BIOS • ME • PSU • CPLD Note: Different firmware types may be displayed depending on the server model.
Active Session	The information of the user currently logged in to the BMC Web, including: • **User Type**: The login type, such as HTTPS and CLI

Item	Information
	• **User Name**: The username used for login to the BMC • **User Group**: The user group information of the user logged in to the BMC • **IP Address**: The IP address of the server from which the user has logged in to the BMC
Quick Launch Tasks	Shortcuts for direct access to the following pages: • **Remote Control**: Click this entry to open the **Remote Control** page. • **Power Control**: Click this entry to open the **Power Supply** > **Power Control** page. • **Users**: Click this entry to open the **BMC Settings** > **User Detail Management** page. • **Network**: Click this entry to open the **BMC Settings** > **Network** page. • **System Info**: Click this entry to open the **Information** > **System Information** page. • **FW Update**: Click this entry to open the **System Maintenance** > **HPM Firmware Update** page.
Recent System Event Log	Information on the latest 10 system event logs, including: • **Event ID**: The ID of the event log • **Time Stamp**: The time when the system event occurred • **Sensor Name**: The name of the sensor that triggered the system event • **Description**: The description of the system event Note: To query more event logs, go to the **Logs & Alarms** > **System Event Log** page.

3.3 Information

3.3.1 System Information

Description:

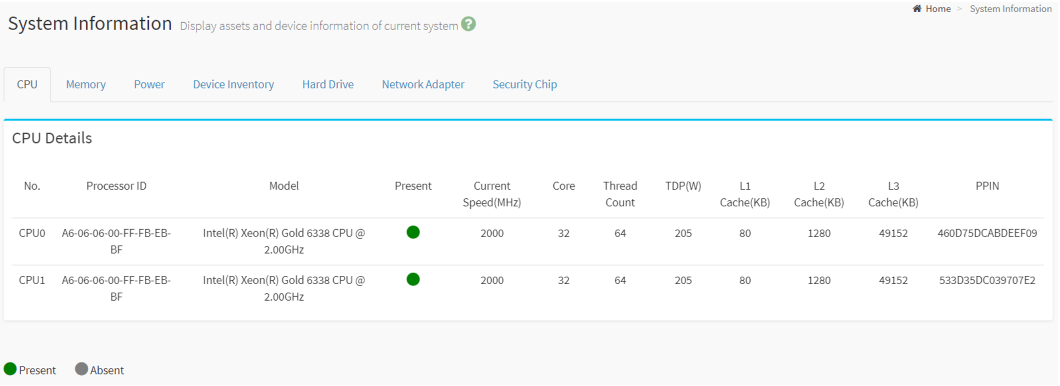
The **System Information** page displays basic information and health status of major server components, including CPU, Memory, Power, Device Inventory, Hard Drive, Network Adapter, and Security Chip.

3.3.1.1 CPU

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **CPU** tab to open the page as shown below.

Figure 3-5 CPU



Home > System Information
System Information Display assets and device information of current system
CPU
Memory
Power
Device Inventory
Hard Drive
Network Adapter
Security Chip

CPU Details

No.	Processor ID	Model	Present	Current Speed(MHz)	Core	Thread Count	TDP(W)	L1 Cache(KB)	L2 Cache(KB)	L3 Cache(KB)	PPIN
CPU0	A6-06-06-00-FF-FB-EB-BF	Intel(R) Xeon(R) Gold 6338 CPU @ 2.00GHz	●	2000	32	64	205	80	1280	49152	460D75DCABDEEF09
CPU1	A6-06-06-00-FF-FB-EB-BF	Intel(R) Xeon(R) Gold 6338 CPU @ 2.00GHz	●	2000	32	64	205	80	1280	49152	533D35DC039707E2

● Present ● Absent

Parameters:

Table 3-4 CPU

Parameter	Description
No.	Indicated with CPUx, where x represents the CPU No.
Processor ID	The CPU ID.
Model	The CPU model.
Present	The CPU status: ● Present ● Absent
Current Speed	The current speed of this CPU.
Core	The number of cores supported by this CPU.
Thread Count	The number of threads supported by this CPU.

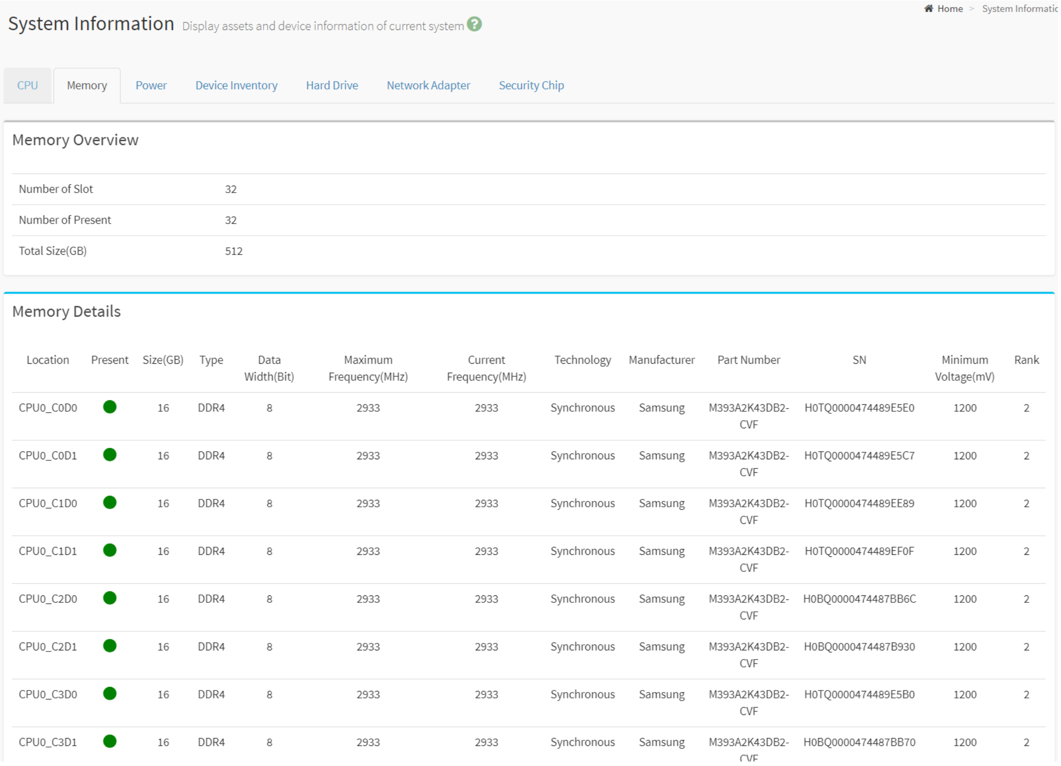
Parameter	Description
TDP	The thermal design power supported by this CPU.
L1 Cache	The L1 cache size supported by this CPU.
L2 Cache	The L2 cache size supported by this CPU.
L3 Cache	The L3 cache size supported by this CPU.
PPIN	The PPIN of the CPU.

3.3.1.2 Memory

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Memory** tab to open the page as shown below.

Figure 3-6 Memory



Memory Overview

Number of Slot	32
Number of Present	32
Total Size(GB)	512

Memory Details

Location	Present	Size(GB)	Type	Data Width(Bit)	Maximum Frequency(MHz)	Current Frequency(MHz)	Technology	Manufacturer	Part Number	SN	Minimum Voltage(mV)	Rank
CPU0_C0D0	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0TQ0000474489E5E0	1200	2
CPU0_C0D1	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0TQ0000474489E5C7	1200	2
CPU0_C1D0	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0TQ0000474489EE89	1200	2
CPU0_C1D1	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0TQ0000474489EF0F	1200	2
CPU0_C2D0	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0BQ0000474487BB6C	1200	2
CPU0_C2D1	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0BQ0000474487B930	1200	2
CPU0_C3D0	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0TQ0000474489E5B0	1200	2
CPU0_C3D1	●	16	DDR4	8	2933	2933	Synchronous	Samsung	M393A2K43DB2-CVF	H0BQ0000474487BB70	1200	2

Parameters:

Table 3-5 Memory Overview

Parameter	Description
Number of Slot	The total number of slots, which is the number of memory modules at full configuration.
Number of Present	The number of memory modules that are present.

Parameter	Description
Total Size (GB)	The total memory capacity (GB).

Table 3-6 Memory Details

Parameter	Description
Location	Indicated with CPUx_CyDz, where x represents the CPU No., y the channel No., and z the DIMM position.
Present	The memory status: 🟢 Present ⚪ Absent
Size (GB)	The memory capacity (GB).
Type	The memory type, such as DDR3 or DDR4.
Data Width (Bit)	The memory bit width.
Maximum Frequency (MHz)	The maximum memory frequency.
Current Frequency (MHz)	The current memory frequency.
Technology	The memory technology, such as synchronous.
Manufacturer	The memory manufacturer.
Part Number	The memory part number.
SN	The memory serial number.
Minimum Voltage (mV)	The minimum memory voltage.
Rank	The memory rank value.

3.3.1.3 Power

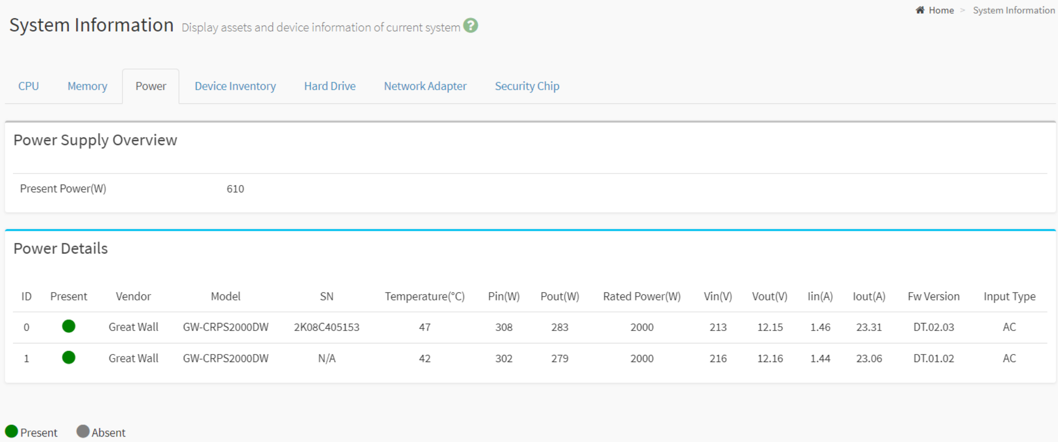
Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Power** tab to open the page as shown below.

NOTE

Refer to the CMC user manual for the power supply information of the multi-node server.

Figure 3-7 Power Supply



System Information Display assets and device information of current system

Power Supply Overview

Present Power(W)	610

Power Details

ID	Present	Vendor	Model	SN	Temperature(°C)	Pin(W)	Pout(W)	Rated Power(W)	Vin(V)	Vout(V)	Iin(A)	Iout(A)	Fw Version	Input Type
0	●	Great Wall	GW-CRPS2000DW	2K08C405153	47	308	283	2000	213	12.15	1.46	23.31	DT.02.03	AC
1	●	Great Wall	GW-CRPS2000DW	N/A	42	302	279	2000	216	12.16	1.44	23.06	DT.01.02	AC

● Present ● Absent

Parameters:

Table 3-7 Power Supply Overview

Parameter	Description
Present Power (W)	The total power consumption of the power supply.

Table 3-8 Power Details

Parameter	Description
ID	The power supply number.
Present	The power supply status: ● Present ● Absent
Vendor	The power supply vendor.
Model	The power supply model.
SN	The power supply serial number.
Temperature (°C)	The power supply temperature.
Pin (W)	The input power of the power supply.
Pout (W)	The output power of the power supply.
Rated Power (W)	The rated power of the power supply.
Vin (V)	The input voltage of the power supply.
Vout (V)	The output voltage of the power supply.
Iin (A)	The input current of the power supply.
Iout (A)	The output current of the power supply.
Fw Version	The firmware version of the power supply.

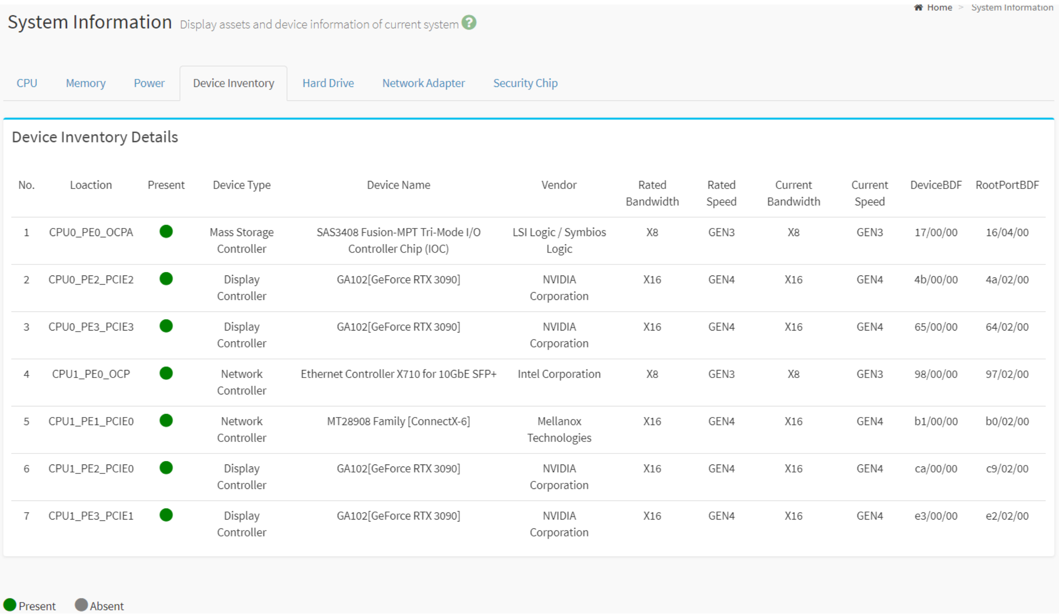
Parameter	Description
Input Type	The power input type: • AC • DC

3.3.1.4 Device Inventory

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Device Inventory** tab to open the page as shown below.

Figure 3-8 Device Inventory


Home > System Information
System Information Display assets and device information of current system
CPU
Memory
Power
Device Inventory
Hard Drive
Network Adapter
Security Chip

Device Inventory Details

No.	Loaction	Present	Device Type	Device Name	Vendor	Rated Bandwidth	Rated Speed	Current Bandwidth	Current Speed	DeviceBDF	RootPortBDF
1	CPU0_PE0_OCPA	●	Mass Storage Controller	SAS3408 Fusion-MPT Tri-Mode I/O Controller Chip (IOC)	LSI Logic / Symbios Logic	X8	GEN3	X8	GEN3	17/00/00	16/04/00
2	CPU0_PE2_PCIE2	●	Display Controller	GA102[GeForce RTX 3090]	NVIDIA Corporation	X16	GEN4	X16	GEN4	4b/00/00	4a/02/00
3	CPU0_PE3_PCIE3	●	Display Controller	GA102[GeForce RTX 3090]	NVIDIA Corporation	X16	GEN4	X16	GEN4	65/00/00	64/02/00
4	CPU1_PE0_OCP	●	Network Controller	Ethernet Controller X710 for 10GbE SFP+	Intel Corporation	X8	GEN3	X8	GEN3	98/00/00	97/02/00
5	CPU1_PE1_PCIE0	●	Network Controller	MT28908 Family [ConnectX-6]	Mellanox Technologies	X16	GEN4	X16	GEN4	b1/00/00	b0/02/00
6	CPU1_PE2_PCIE0	●	Display Controller	GA102[GeForce RTX 3090]	NVIDIA Corporation	X16	GEN4	X16	GEN4	ca/00/00	c9/02/00
7	CPU1_PE3_PCIE1	●	Display Controller	GA102[GeForce RTX 3090]	NVIDIA Corporation	X16	GEN4	X16	GEN4	e3/00/00	e2/02/00

● Present ● Absent

Parameters:

Table 3-9 Device Inventory

Parameter	Description
No.	The device number.
Location	Onboard slot number where the device is located
Present	The device status: ● Present ● Absent
Device Type	The type of the device.
Device Name	The name of the device.
Vendor	The device vendor.

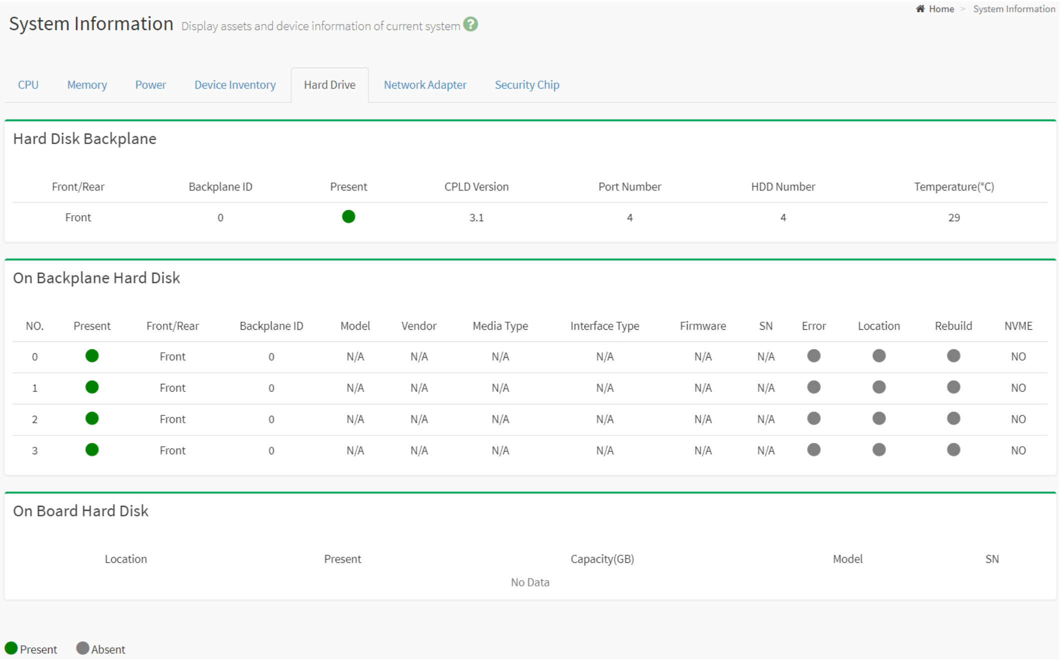
Parameter	Description
Rated Bandwidth	The rated bandwidth of the device.
Rated Speed	The rated speed of the device.
Current Bandwidth	The current bandwidth of the device.
Current Speed	The current speed of the device.
DeviceBDF	The Bus/Device/Function of the device.
RootPortBDF	The Bus/Device/Function of the device's RootPort.

3.3.1.5 Hard Drive

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Hard Drive** tab to open the page as shown below.

Figure 3-9 Hard Drive



Home > System Information

System Information Display assets and device information of current system

CPU | Memory | Power | Device Inventory | Hard Drive | Network Adapter | Security Chip

Hard Disk Backplane

Front/Rear	Backplane ID	Present	CPLD Version	Port Number	HDD Number	Temperature(°C)
Front	0	🟢	3.1	4	4	29

On Backplane Hard Disk

NO.	Present	Front/Rear	Backplane ID	Model	Vendor	Media Type	Interface Type	Firmware	SN	Error	Location	Rebuild	NVME
0	🟢	Front	0	N/A	N/A	N/A	N/A	N/A	N/A	⚫	⚫	⚫	NO
1	🟢	Front	0	N/A	N/A	N/A	N/A	N/A	N/A	⚫	⚫	⚫	NO
2	🟢	Front	0	N/A	N/A	N/A	N/A	N/A	N/A	⚫	⚫	⚫	NO
3	🟢	Front	0	N/A	N/A	N/A	N/A	N/A	N/A	⚫	⚫	⚫	NO

On Board Hard Disk

Location	Present	Capacity(GB)	Model	SN
		No Data		

🟢 Present ⚫ Absent

Parameters:

Table 3-10 On Backplane Hard Disk

Parameter	Description
Front/Rear	Indicates whether the drive is installed in the front or at the rear.
Backplane ID	The drive backplane number, in which x represents the device number.
Present	The drive status:

Parameter	Description
	🟢 Present ⚪ Absent
CPLD Version	The CPLD version of the driver.
Port Number	The number of drive ports.
HDD Number	The number of drives.
Temperature (°C)	The drive temperature.

Table 3-11 On Backplane Hard Disk

Parameter	Description
NO.	The drive number on the drive backplane, in which x represents the drive backplane number.
Present	The status of a drive on the drive backplane: 🟢 Present ⚪ Absent
Front/Rear	Indicates whether the drive is installed in the front or at the rear.
Backplane ID	The drive backplane number.
Model	The drive model.
Vendor	The drive vendor.
Media Type	The drive medium type, such as SSD, HHD, and HDD.
Interface Type	Indicates the drive interface type, including: • PCIe • OCP • Others
Firmware	Indicates the drive firmware version.
SN	Indicates the drive serial number.
Error	Indicates the drive error status, including: • ⚪ = Normal • ✓ = Drive error
Location	Drive Locate LED is on. Drive Active LED LED is off.
Rebuild	Indicates the rebuilding status of the drive, including: • Rebuilding • Not rebuilding

Parameter	Description
NVME	Indicates whether the drive is an NVMe drive, including: • Yes • No

Table 3-12 On Board Hard Disk

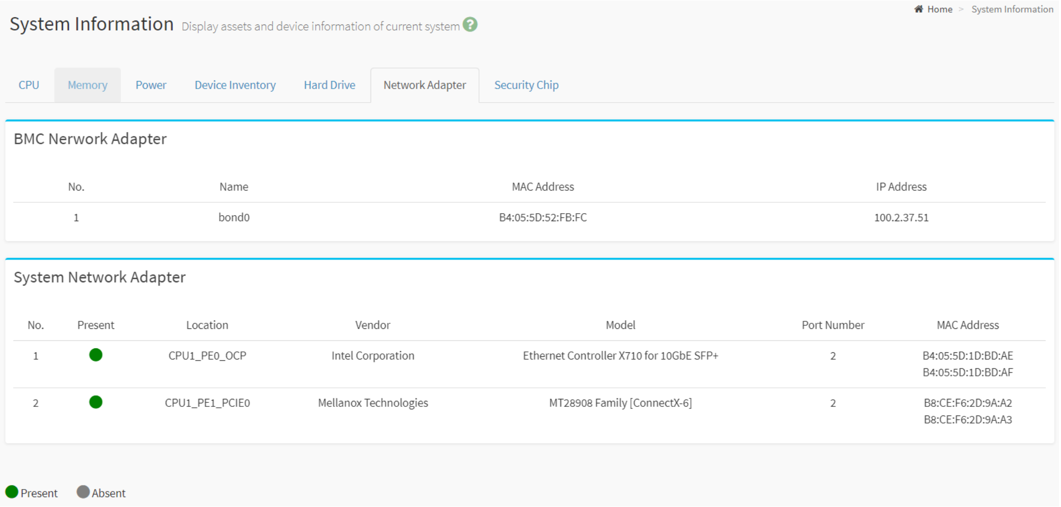
Parameter	Description
Location	Indicates the position of the onboard drive.
Present	Indicates the onboard drive status, including: ● Present ● Absent
Capacity (GB)	Indicates the capacity of the onboard drive.
Model	Indicates the model of the onboard drive.
SN	Indicates the serial number of the onboard drive.

3.3.1.6 Network Adapter

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Network Adapter** tab to open the page as shown below.

Figure 3-10 Network Adapter



System Information Display assets and device information of current system

BMC Nerwork Adapter

No.	Name	MAC Address	IP Address
1	bond0	B4:05:5D:52:FB:FC	100.2.37.51

System Network Adapter

No.	Present	Location	Vendor	Model	Port Number	MAC Address
1	●	CPU1_PE0_OCP	Intel Corporation	Ethernet Controller X710 for 10GbE SFP+	2	B4:05:5D:1D:BD:AE B4:05:5D:1D:BD:AF
2	●	CPU1_PE1_PCIE0	Mellanox Technologies	MT28908 Family [ConnectX-6]	2	B8:CE:F6:2D:9A:A2 B8:CE:F6:2D:9A:A3

● Present ● Absent

Parameters:

Table 3-13 BMC Network Adapter

Parameter	Description
No.	Indicates the network adapter number.
Name	Indicates the name of the network adapter, including: • eth0 • eth1
MAC Address	Indicates the MAC address.
IP Address	Indicates the IP address.

Table 3-14 System Network Adapter

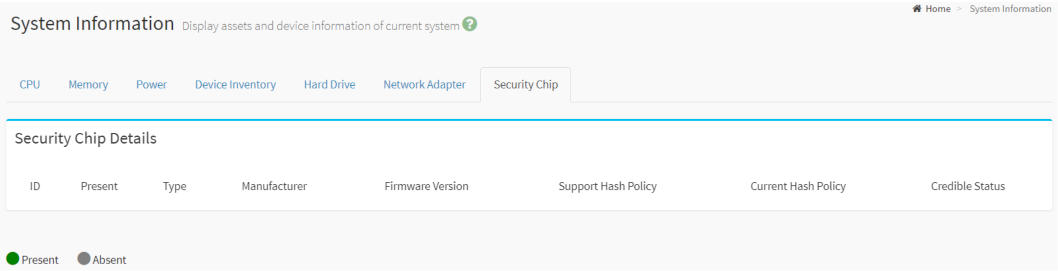
Parameter	Description
No.	Indicates the system network adapter number.
Present	Indicates the status of the system network adapter, including: ● Present ● Absent
Location	Indicates the position of the system network adapter.
Vendor	Indicates the vendor of the system network adapter.
Model	Indicates the model of the system network adapter.
Port Number	Indicates the number of the system network adapter ports.
MAC Address	Indicates the MAC address of the system network adapter.

3.3.1.7 Security Chip

Screen description:

In the navigation pane, select **Information** > **System Information**, and click the **Security Chip** tab to open the page as shown below.

Figure 3-11 Security Chip



System Information Display assets and device information of current system

Security Chip Details

ID	Present	Type	Manufacturer	Firmware Version	Support Hash Policy	Current Hash Policy	Credible Status

Parameters:

Table 3-15 Security Chip Details

Parameter	Description
ID	Indicates the security chip number.
Present	Indicates the status of the security chip, including: ● Present ● Absent
Type	Indicates the type of the security chip.
Manufacturer	Indicates the manufacturer of the security chip.
Firmware Version	Indicates the firmware version of the security chip.
Support Hash Policy	Indicates the Hash policy supported by the security chip.
Current Hash Policy	Indicates the current Hash policy of the security chip.
Credible Status	Indicates the trustworthiness of the security chip, which can be Yes or No.

3.3.2 FRU Information

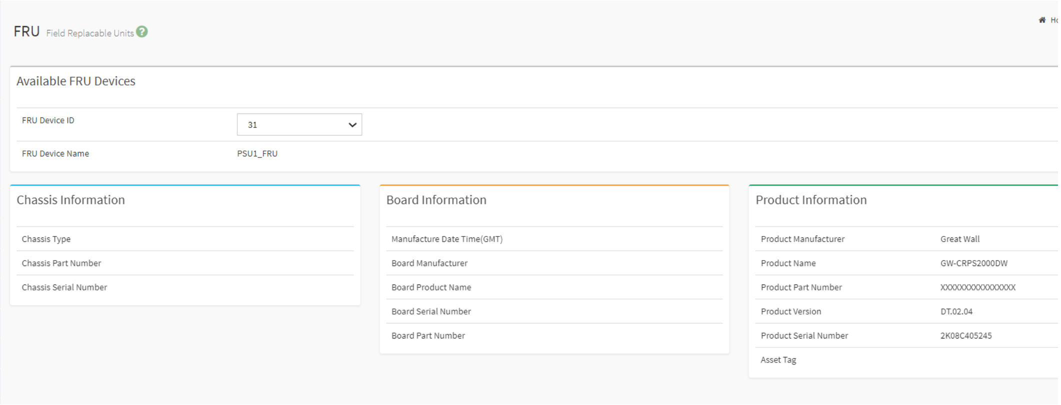
Description:

On the **FRU** page, you can obtain the field replacement unit (FRU) information of the server.

Screen description:

In the navigation pane, select **Information** > **FRU Information** to open the page as shown below, where you can see available FRU devices, chassis information, board information, and product information. Updating BMC firmware does not lead to the loss of FRU information.

Figure 3-12 FRU Information



FRU Field Replacable Units

Available FRU Devices

FRU Device ID	31
FRU Device Name	PSU1_FRU

Chassis Information

Chassis Type	
Chassis Part Number	
Chassis Serial Number	

Board Information

Manufacture Date Time(GMT)	
Board Manufacturer	
Board Product Name	
Board Serial Number	
Board Part Number	

Product Information

Product Manufacturer	Great Wall
Product Name	GW-CRPS2000DW
Product Part Number	XXXXXXXXXXXXXXXX
Product Version	DT.02.04
Product Serial Number	2K08C405245
Asset Tag	

Parameters:

Table 3-16 FRU Information

Type	Parameter
FRU Device ID	The FRU device ID, which can be selected from the drop-down list.
FRU Device Name	The FRU device name, such as BMC_FRU.
Chassis Information	Chassis Type (such as rack mount chassis)
	Chassis Part Number
	Chassis Serial Number
	Chassis Extra
Board Information	Manufacture Date Time (GMT)
	Board Manufacturer
	Board Product Name
	Board Serial Number
	Board Part Number
Product Information	Product Manufacturer
	Product Name
	Product Part Number
	Product Version
	Product Serial Number
	Asset Tag

3.3.3 History

Description:

On the **History** page, users can view historical data and administrators can learn about the actual usage of power and cooling resources based on the monitoring curve**.**

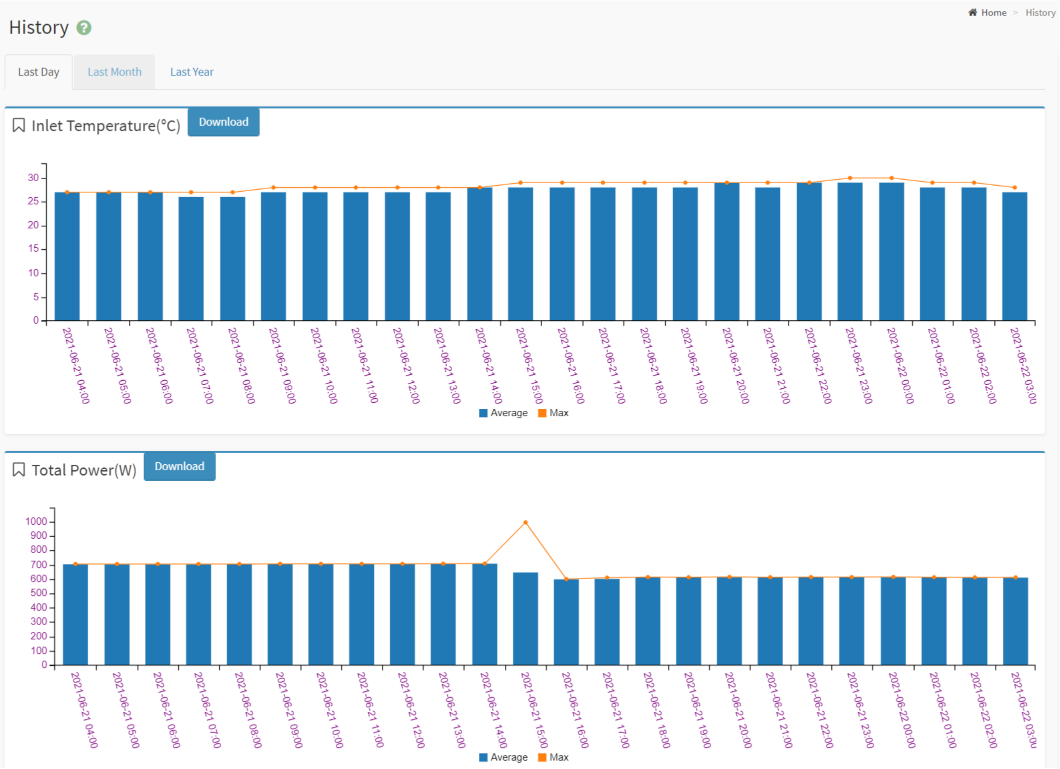
On the **History** page, you can:

- View the curve of the inlet temperature for the last day/last month/last year.
- Download the inlet temperature data for the last day/last month/last year.
- View the curve of the total power for the last day/last month/last year.
- Download the total power data for the last day/last month/last year.

Screen description:

In the navigation pane, select **Information** > **History** to open the page as shown below.

Figure 3-13 History



Parameters:

Table 3-17 History

Parameter	Description
Last Day	This tab displays the inlet temperature and the total power for the last day.
Last Month	This tab displays the inlet temperature and the total power for the last month.
Last Year	This tab displays the inlet temperature and the total power for the last year.
Download	Click the **Download** button to download the historical data of the inlet temperature and total power.

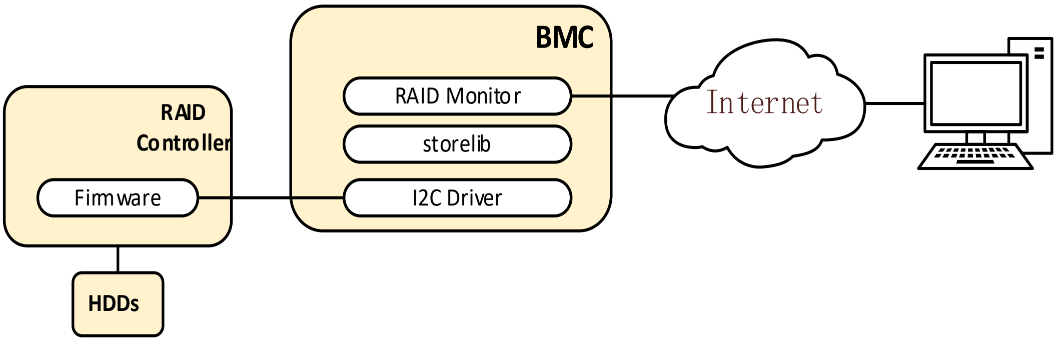
3.4 Storage

Description:

The server storage subsystem consists of expansion drives controlled by RAID or SAS controllers. BMC physically interacts with the RAID and SAS controllers through I^{2}C to obtain information on controllers, drives, and arrays, and to configure RAID.

The following shows how BMC accesses the RAID/SAS controller:

Figure 3-14 BMC Accessing RAID/SAS Controller



On the **Storage** page, you can view the controller of the current storage device and configure RAID.

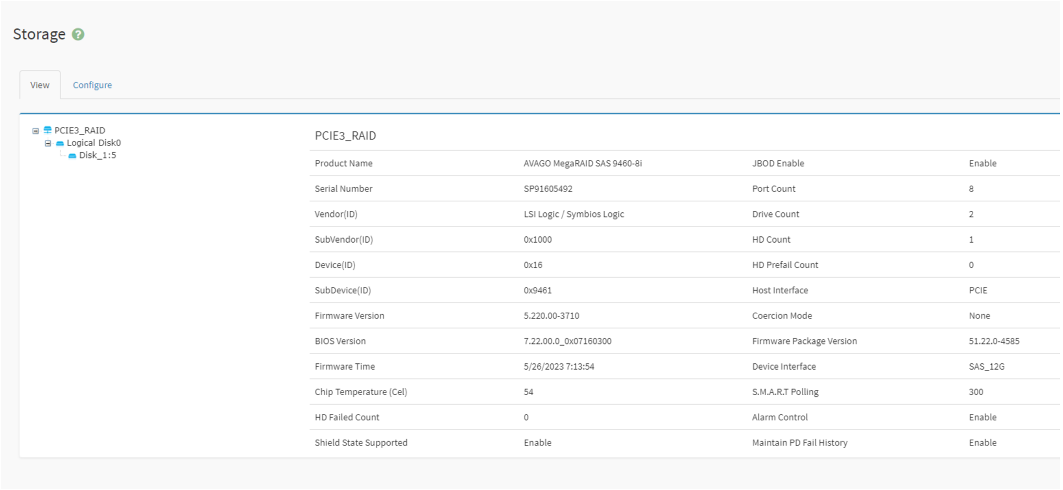
NOTE

The storage information is invalid when the system is powered off or being powered on. Every time the server and the system are powered on, BMC re-identifies all physical disks. If a physical disk is being rebuilt in this case, the disk will be identified later. Before the identification is completed, the disk information remains invalid.

Screen description:

In the navigation pane, select **Storage** > **View** to open the page as shown below, where you can view the details of controllers, logical disks, and physical disks.

Figure 3-15 Storage View

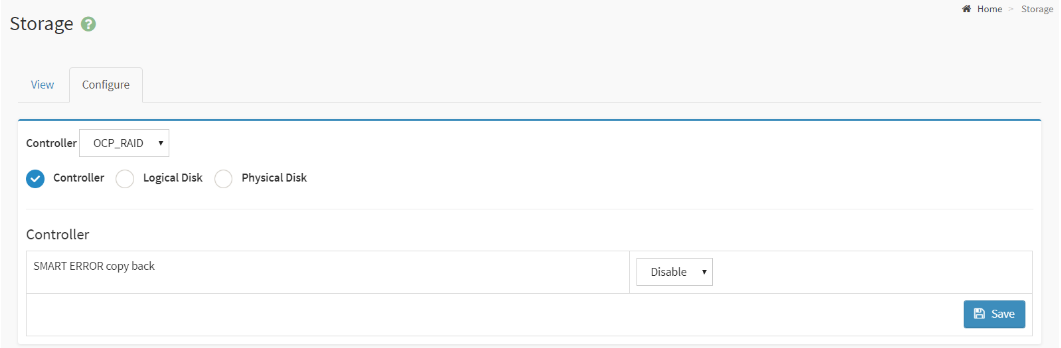


PCIE3_RAID

Product Name	AVAGO MegaRAID SAS 9460-8i	JBOD Enable	Enable
Serial Number	SP91605492	Port Count	8
Vendor(ID)	LSI Logic / Symbios Logic	Drive Count	2
SubVendor(ID)	0x1000	HD Count	1
Device(ID)	0x16	HD Prefail Count	0
SubDevice(ID)	0x9461	Host Interface	PCIE
Firmware Version	5.220.00-3710	Coercion Mode	None
BIOS Version	7.22.00.0_0x07160300	Firmware Package Version	51.22.0-4585
Firmware Time	5/26/2023 7:13:54	Device Interface	SAS_12G
Chip Temperature (Cel)	54	S.M.A.R.T Polling	300
HD Failed Count	0	Alarm Control	Enable
Shield State Supported	Enable	Maintain PD Fail History	Enable

In the navigation pane, select **Storage** > **Configure** to open the pages shown in Figure 3-16, Figure 3-17, and Figure 3-18.

Figure 3-16 Configure - Controller



Storage

Home > Storage

View | Configure

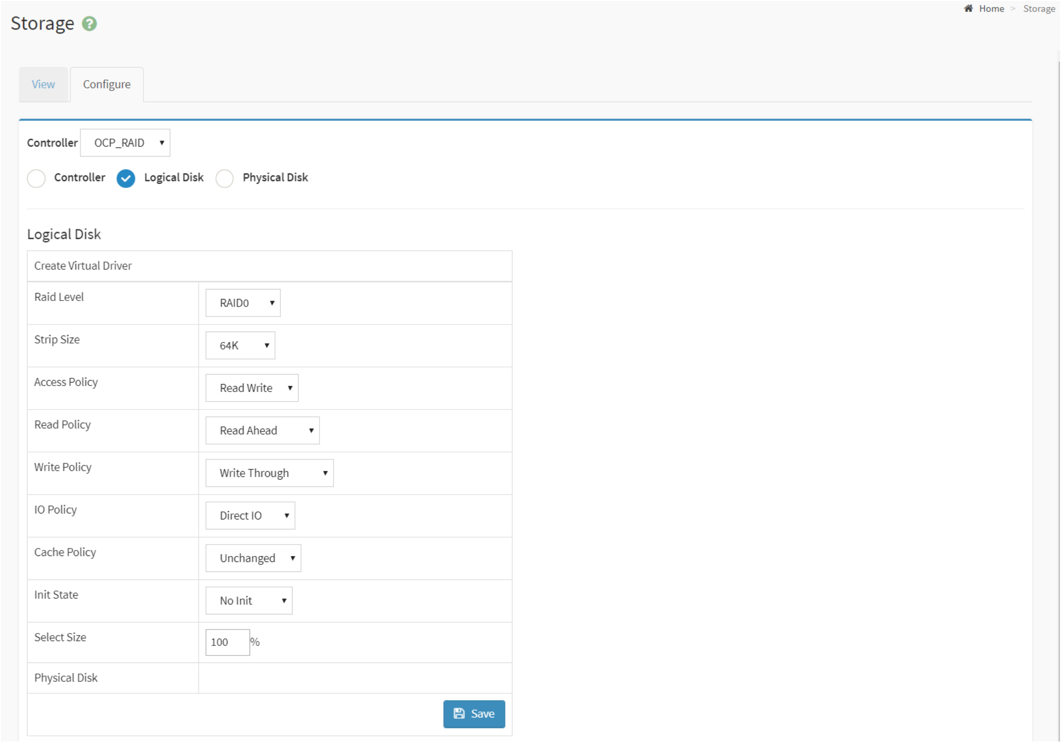
Controller: OCP_RAID

● Controller ○ Logical Disk ○ Physical Disk

Controller

SMART ERROR copy back	Disable

Figure 3-17 Configure - Logical Disk



Storage

Home > Storage

View | Configure

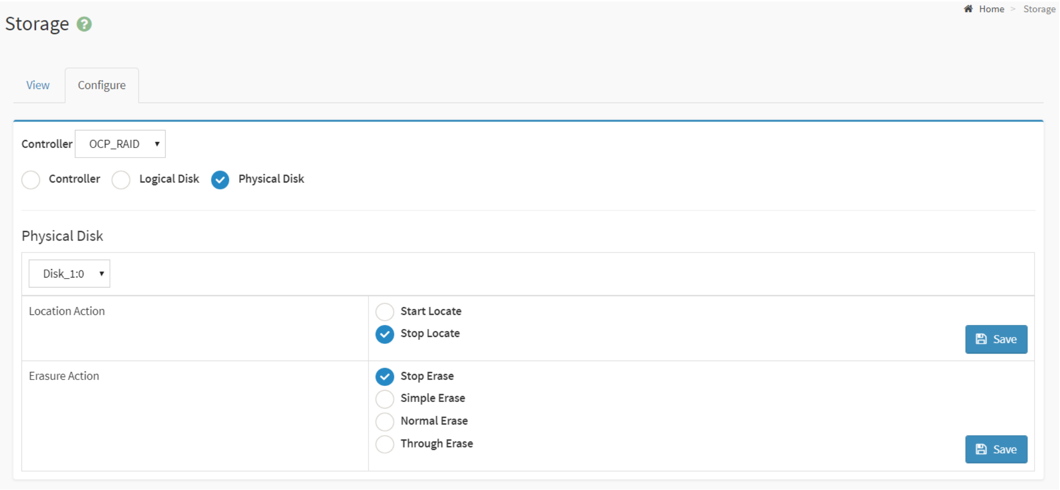
Controller: OCP_RAID

○ Controller ● Logical Disk ○ Physical Disk

Logical Disk

Create Virtual Driver	
Raid Level	RAID0
Strip Size	64K
Access Policy	Read Write
Read Policy	Read Ahead
Write Policy	Write Through
IO Policy	Direct IO
Cache Policy	Unchanged
Init State	No Init
Select Size	100 %
Physical Disk	

Figure 3-18 Configure - Physical Disk



Controller: OCP_RAID

○ Controller ○ Logical Disk ● Physical Disk

Physical Disk

Disk_1:0

Location Action: ○ Start Locate ● Stop Locate

Erasure Action: ● Stop Erase ○ Simple Erase ○ Normal Erase ○ Through Erase

NOTE

When a drive with no RAID enters the POWERSAVE mode after 30 minutes of idleness, the HDD_MAX_TEMP may not be identified. You can check this by running the ipmitool sdr elist command in the OS.

Parameters:

Table 3-18 Configure

Parameter	**Description**
Controller	
Controller	The name of the controller.
SMART ERROR copy back	Enables or disables copyback on SMART error. Disabled by default.
JBOD	Enables or disables the JBOD mode. Enabled by default.
Logical Disk	
Create Virtual Driver	Set the RAID level, stripe size, access policy, read policy, write policy, I/O policy, cache policy, init state, select size, and physical disk, and then click **Save**.
Other Actions	• Start locating logical disk • Stop locating logical disk • Quickly initialize logical disk • Slowly/Fully initialize logical disk

Parameter	Description
	• Stop initializing logical disk
Physical Disk	
Firmware Status	• UNCONFIGURED GOOD • UNCONFIGURED BAD • OFFLINE • ONLINE • JBOD
Location Action	• Start Locate • Stop Locate
Erasure Action	• Stop Erase • Simple Erase • Normal Erase • Thorough Erase

The following table lists some supported RAID and SAS controllers.

Table 3-19 Some Supported RAID and SAS Controllers

Type	Model	SAS Rate (Gbps)	Firmware Version
RAID	9361-8i/2G	12 Gbps	4.680.00-8527
RAID	9361-8i/1G	12 Gbps	4.680.00-8527
RAID	9361-8i/2G	12 Gbps	4.680.00-8527
RAID	9361-24i/4G	12 Gbps	4.740.00-8452
RAID	9460-8i/2G	12 Gbps	5.130.00-3170
SAS	9300-8e	12 Gbps	16.00.10.00
SAS	9300-8i	12 Gbps	16.00.10.00
SAS	9311-8i	12 Gbps	16.00.10.00
RAID	9341-8i	12 Gbps	4.680.01-8526
SAS	9305-24i	12 Gbps	16.00.00.00
SAS	9305-16i	12 Gbps	16.00.00.00
RAID	9361-16i/2G	12 Gbps	4.740.00-8452
SAS	9400-8i	12 Gbps	08.00.00.00
RAID	9440-8i	12 Gbps	5.130.01-3170
SAS	9400-8e	12 Gbps	08.00.00.00
SAS	9440-8i	12 Gbps	5.130.01-3170

Type	Model	SAS Rate (Gbps)	Firmware Version
SAS	9400-16i	12 Gbps	08.00.00.00
RAID	9460-8i/4G	12 Gbps	5.130.00-3170
RAID	9460-8i/2G	12 Gbps	5.130.00-3170
RAID	9460-16i/4G	12 Gbps	5.130.00-3170
RAID	8805	12 Gbps	33282
RAID	3152-8i/2G	12 Gbps	2.66
RAID	3152-8i	12 Gbps	2.66
RAID	3154-8i	12 Gbps	2.66
SAS	SmartHBA 2100-8i	12 Gbps	2.66
SAS	HBA1100-8i	12 Gbps	2.66
RAID	3154-24i/4G	12 Gbps	2.66

NOTE

The list of supported RAID and SAS controllers is subject to change due to version updates. This document only lists part of the supported controllers.

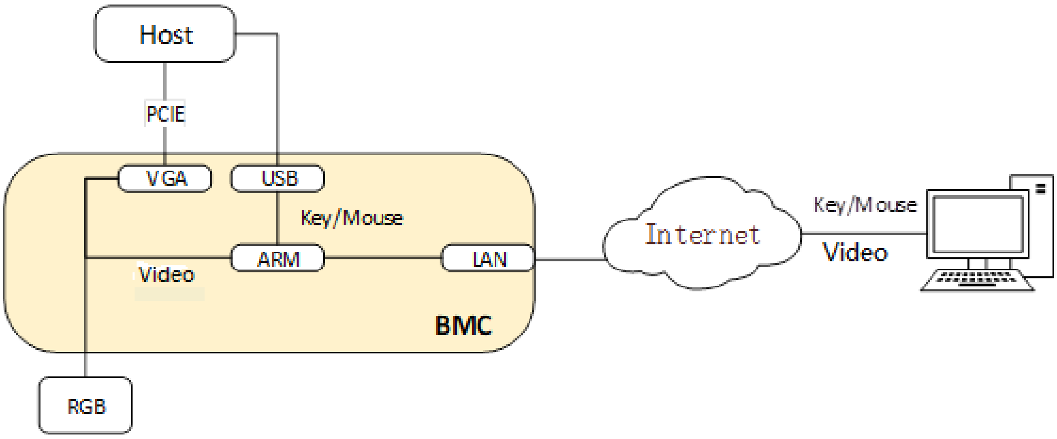
3.5 Remote Control

3.5.1 Console Redirection

Description:

Remote Control redirects the console of the server system to users' PC through BMC. When a user logs in to BMC and enables H5Viewer or JViewer Remote Control, the server screen will appear in the application. Then, the user can control the server with the keyboard and mouse of the PC.

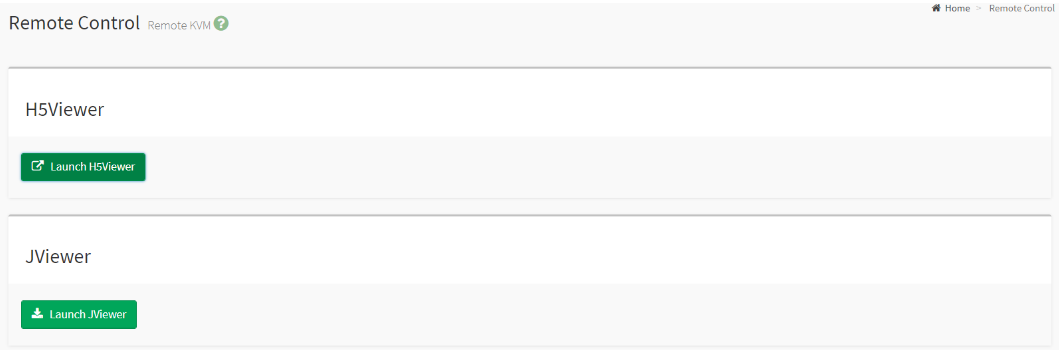
Figure 3-19 Console Redirection



Screen description:

In the navigation pane, select **Remote Control** > **Console Redirection** to open the page as shown below.

Figure 3-20 Remote Control



Parameters:

Table 3-20 Remote Control

Parameter	Description
Launch H5Viewer	Starts the HTML5 Integrated Remote Console.
Launch JViewer	Downloads the JViewer boot file.

3.5.1.1 H5Viewer

Description:

With the H5Viewer Integrated Remote Console, you can access and manage a server remotely, install or repair the operating system, and install drivers on the server.

- You can use the keyboard and mouse of the local PC to remotely manage the server on a real-time basis.
- You can enable the server to remotely access the local PC over a network using a virtual floppy drive or DVD/CD-ROM drive. For the server, the virtual floppy drive or DVD/CD-ROM drive can be used in the same way as the universal serial bus (USB) device inserted into the server.

Table 3-21 and Table 3-22 describe the menus and buttons in the KVM window.

Table 3-21 H5Viewer Menus

Menu	Secondary Menu	Function
Video	Pause Video Resume Video Refresh Video	Pauses the video. Resumes the video. Refreshes the video.
	Host Display Turn ON Host Display Turn OFF Host Display	Sets whether to display the host.
	Capture Screen	Captures the screen.
Mouse	Show Cursor Mouse Mode: Absolute Mouse Mode Relative Mouse Mode Other Mouse Mode	Sets the mouse mode and whether to display the mouse on the client.
Option	Zoom General Zoom In Zoom Out	Zooms in or out.
	Block Privilege Request Partial Permission	Sets the permissions.

Menu	Secondary Menu	Function
	No Permission	
	Auto Detect 256 Kbps 512 Kbps 1 Mbps 10 Mbps YUV 420 YUV 444 YUV 444+2 color VQ YUV 444+4 color VQ	Detects automatically.
	0Best Quality 1 2 3 4 5 6 7	Indicates the display quality.
Keyboard	Keyboard Layout English (United States) German Japan	Selects the keyboard type of the client.
Send Keys	Hold Right Ctrl Key Right Alt Key Right Windows Key Left Ctrl Key Left Alt Key Left Windows Key Press and Release Ctrl+Alt+Del Left Windows Key Right Windows Key Context Menu Print Screen	Indicates the keys for sending.
Hot Keys	Add Hot Keys	Adds custom shortcut keys.
Video Record	Start Record Stop Record Settings	Records a video. Stops recording. Recording settings: You can set the video length, video compression, and

Menu	Secondary Menu	Function
		whether to use a standard video resolution (1024 × 768).
PSU	Forced System Reset Forced Off Soft Shutdown On Power Cycle Set Boot Options	Performs power control actions.
Active Users	For example: admin(AD) 100.3.2.32	Shows users who are using H5Viewer.
Help	About H5Viewer	Shows H5Viewer version information.

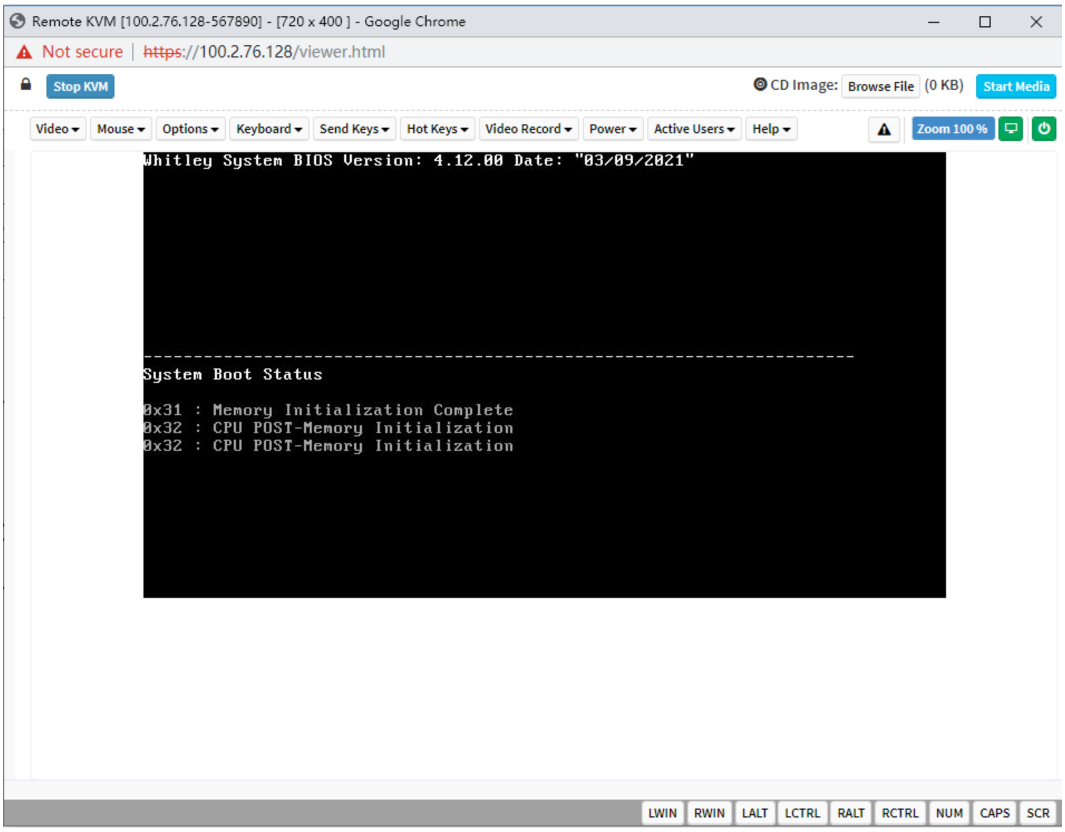
Table 3-22 H5Viewer Buttons

Icon	Description
Stop KVM	Stops the KVM.
Start Media	Starts media.
⏻	Powers on the server.
⚠	Unlocks the server display.
Zoom 100 %	The current zoom scale is 100%
🖥	Shows all received notifications.
◎ CD Image: Browse File	Selects the CD image file.

Screen description:

On the **Console Redirection** page, click the **Launch H5Viewer** button to start H5Viewer.

Figure 3-21 H5Viewer



Remote KVM [100.2.76.128-567890] - [720 x 400] - Google Chrome
Not secure | https://100.2.76.128/viewer.html
Stop KVM
CD Image: Browse File (0 KB) Start Media
Video Mouse Options Keyboard Send Keys Hot Keys Video Record Power Active Users Help
Zoom 100 %
LWIN RWIN LALT LCTRL RALT RCTRL NUM CAPS SCR

```
Whitley System BIOS Version: 4.12.00 Date: "03/09/2021"




-----------------------------------------------------------------------
System Boot Status

0x31 : Memory Initialization Complete
0x32 : CPU POST-Memory Initialization
0x32 : CPU POST-Memory Initialization
```

Table 3-23 H5Viewer

Item	Function
Address Bar (Top)	Shows the current KVM address.
Toolbar and Menu Area (Upper)	Shows menus and buttons.
Real-time Desktop (Middle)	Shows the real-time desktop of the server.
Status Bar (Bottom)	Shows shortcut keys.

NOTE

1. H5Viewer supported browsers: Google Chrome 58 or above and Internet Explorer 11 or above.
2. The H5Viewer does not depend on JAVA and .NET.

Steps:

Power On

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Power On** to turn on the server.

- End

Forced Off

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Forced Power Off** to forcibly turn off the server.

- End

Soft Shutdown

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Soft Shutdown** to shut down the server.

- End

Power Cycle

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Power Cycle** to forcibly turn off the server and then turn it on again.

- End

Forced System Reset

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Forced System Reset** to force restart the server.

- End

Set Boot Options

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **H5Viewer** button to turn on the KVM.
3. On the H5Viewer KVM page, select **Power** > **Set Boot Options**.

4. On the **Set Boot Options** page, select the boot options (**No Change, PXE, Hard Disk/USB**, and **BIOS Settings**) in the drop-down list, and select whether these items are applicable only to the next boot.

5. Restart the server.

- End

Mount CD

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **H5Viewer** button to turn on the KVM.

3. On the H5Viewer KVM page, click the file selection button ◎ CD Image: Browse File in the upper-right corner to select the image file, and then click the Start Media button.

- End

3.5.1.2 Jviewer

NOTE

JViewer is not supported on some server models due to hardware design. You can contact us for details.

Description:

With the JViewer Integrated Remote Console, you can access and manage a server remotely, install or repair the operating system, and install drivers on the server.

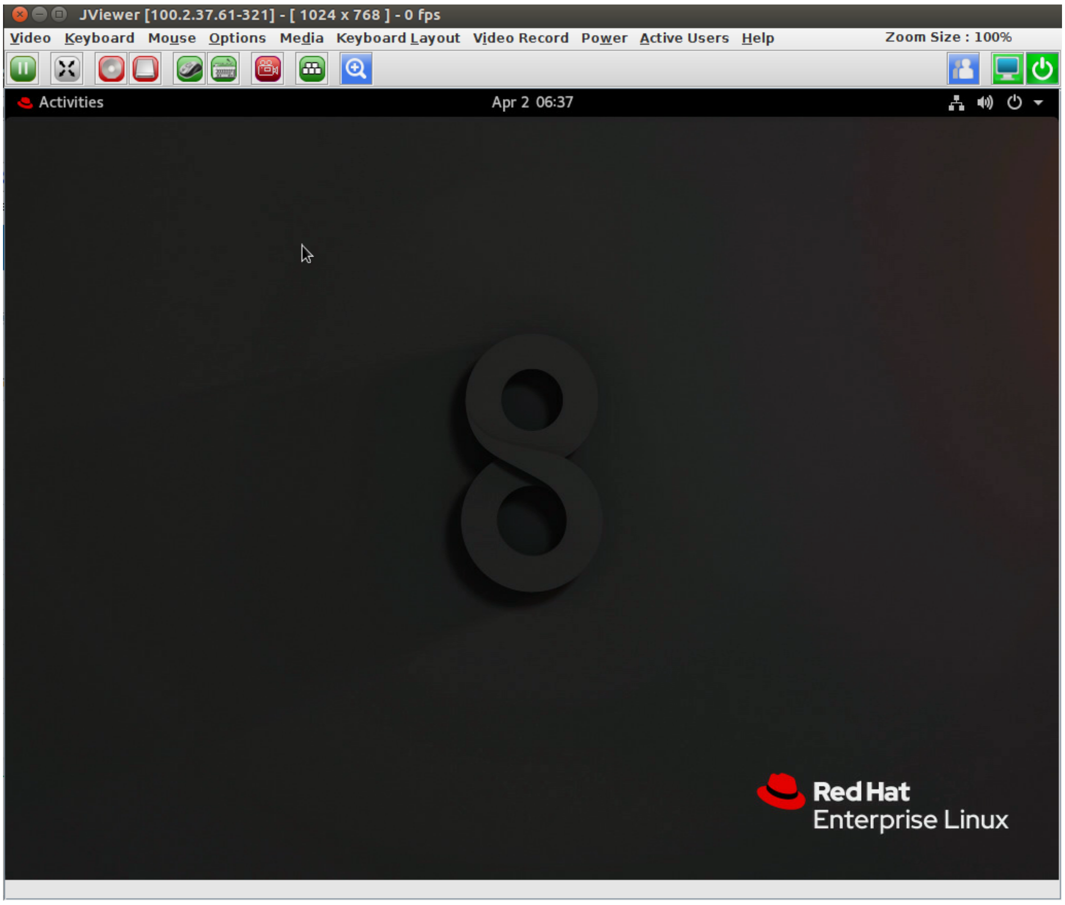
- You can use the keyboard and mouse of the local PC to remotely manage the server on a real-time basis.

- You can enable the server to remotely access the local PC over a network using a virtual floppy drive or DVD/CD-ROM drive. For the server, the virtual floppy drive or DVD/CD-ROM drive can be used in the same way as the universal serial bus (USB) device inserted into the server.

Table 3-24 and Table 3-25 describe the menus, buttons, and their functions in the **KVM** window.

On the **Console Redirection** page, click the **Launch JViewer** button to download the jviewer.jnlp file, and then open JViewer by running the javaws jviewer.jnlp command.

Figure 3-22 JViewer



NOTE

BMC supports JViewer. You need to download and open JNLP (Java Application), and prepare the JRE environment. OpenJDK 1.8 or above are supported.

NOTE

BMC cannot be accessed using proxy software, such as Nginx. You can open the BMC Web GUI using proxy software, but cannot open JViewer through the Java console.

Parameters:

Table 3-24 JViewer Buttons

Icon	Description
⏸	Pauses the display of the KVM page.
⛶	Shows the KVM page in full-screen mode.
💿	Opens the CD/DVD virtual media configuration page.
🖴	Opens the Hard Disk/USB virtual media settings page.
🖱	Shows the mouse.
🖱	Hides the mouse.
⌨	Opens the soft keyboard.
🎥	Starts recording.
🎥	Stops recording.
⌨	Shortcut keys.
🔍	Enables zoom.
🔍	Disables zoom.
👥	Active user information.
🖥	Unlocks the server display.
⏻	The server is powered off. Click the button to power on.
⏻	The server is powered on. Click the button to power off.

Table 3-25 JViewer Menus

Menu	Secondary Menu
Video	Pause Redirection Resume Redirection Refresh Video Turn ON Host Display Turn OFF Host Display Capture Screen Full Screen Compression Mode: YUV 420 YUV 444 YUV 444 + 2 colors VQ YUV 444 + 4 colors VQ DCT Quantization Table 0 Best Quality 1 2 3 4 5 6 7 Worst Quality Exit
Keyboard	Hold Right Ctrl Key Hold Right Alt Key Hold Left Ctrl Key Hold Left Alt Key Left Windows Key: Hold Down Press and Release Right Windows Key: Hold Down Press and Release Ctrl+Alt+Del Context Menu Hot Keys:

Menu	Secondary Menu
	Add Hot Keys Full Keyboard Support
Mouse	Show Cursor Mouse Calibration Mouse Mode: Absolute mouse mode Relative mouse mode Other mouse mode
Options	Bandwidth: Auto Detect 256 Kbps 512 Kbps 1 Mbps 10 Mbps 100 Mbps Keyboard/Mouse Encryption Zoom: Zoom In Zoom Out Actual Size Fit to Client Resolution Fit to Host Resolution Send IPMI Command GUI Languages English - [EN] Block Privilege Request： Allow only Video Deny Access
Media	Virtual Media Wizard
Keyboard Layout	Auto Detect Host Physical Keyboard: Host Platform English（United States） English（United Kingdom） French

Menu	Secondary Menu
	French（Belgium） German（Germany） German（Switzerland） Japanese Spanish Italian Danish Finnish Norwegian（Norway） Portuguese（Portugal） Swedish Dutch（Netherland） Dutch（Belgium） Tukish - F Tukish - G Soft Keyboard: English（United States） English（United Kingdom） Spanish French German（Germany） Italian Danish Finnish German（Switzerland） Norwegian（Norway） Portuguese（Portugal） Swedish Hebrew French（Belgium） Dutch（Netherland） Dutch（Belgium） Russsian（Russia） Japanese（QWERTY） Japanese（Hiragana） Japanese（Katakana） Tukish - F Tukish - G
Video Record	Start Record

Menu	Secondary Menu
	Stop Record Settings
Power	Forced System Reset Forced Power Off Soft Shutdown Power On Power Cycle Set Boot Options
Active Users	Eg: admin(ADMINISTRATOR): 100.2.76.103
Help	About JViewer

Steps:

Power On

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.
3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.
4. On the JViewer KVM page, select **Power** > **Power On** to turn on the server.

- End

Forced Off

1. In the navigation pane, select **Remote Control** > **Console Redirection**.
2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.
3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.
4. On the JViewer KVM page, Select **Power** > **Forced Power Off** to forcibly turn off the server.

- End

Soft Shutdown

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.

3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.

4. On the JViewer KVM page, select **Power** > **Soft Shutdown** to shut down the server.

- End

Power Cycle

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.

3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.

4. On the JViewer KVM page, Select **Power** > **Power Cycle** to forcibly turn off the server and then turn it on again.

- End

Forced System Reset

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.

3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.

4. On the JViewer KVM page, select **Power** > **Forced System Reset** to force restart the server.

- End

Set Boot Options

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.

3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.

4. On the JViewer KVM page, select **Power** > **Set Boot Options**.

5. On the **Set Boot Options** page, select the boot options (**No Change**, **PXE**, **Hard Disk/USB**, and **BIOS Settings**) in the drop-down list and check the **Next Boot Only** option as needed.

6. Restart the server.

- End

Mount CD

1. In the navigation pane, select **Remote Control** > **Console Redirection**.

2. On the page that appears, click the **JViewer** button to download the JViewer boot file, whose default file name is jviewer.jnlp.

3. Open the command line interface, go to the directory where the jnlp file was downloaded, and run the **javaws jviewer.jnlp** command to open the JViewer KVM page.

4. On the JViewer KVM page, click the 💿 button or choose **Media** > **Virtual Media Wizard** to open the configuration page.

5. Browse to select the image file, click the **Connect** button, and check that **CD/DVD Redirection Status** is **Connected** to make sure the image file has been mounted.

- End

3.5.2 Image Redirection

Description:

On the **Image Redirection** page, you can check the available image files for BMC and perform the following operations on the image files:

- Redirect
- Stop
- Clear

The image redirection has the following features:

- Only administrators have the privilege to redirect or clear redirection.
- Supported CD/DVD formats: ISO 9660 and UDF (v1.02 - v2.60).
- Supported CD/DVD image types: *.iso and *.nrg.
- Supported image types: *.img and *.ima.

Screen description:

In the navigation pane, select **Remote Control** > **Image Redirection** to open the pages shown in Figure 3-23 and Figure 3-24.

Figure 3-23 Image Redirection

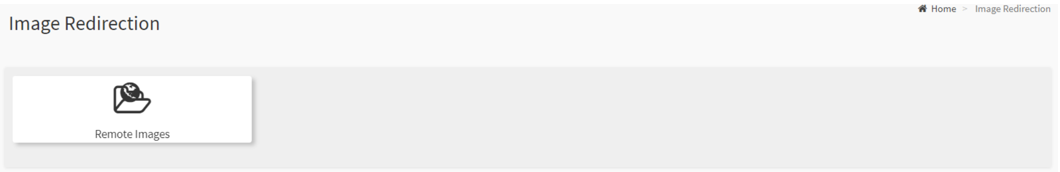
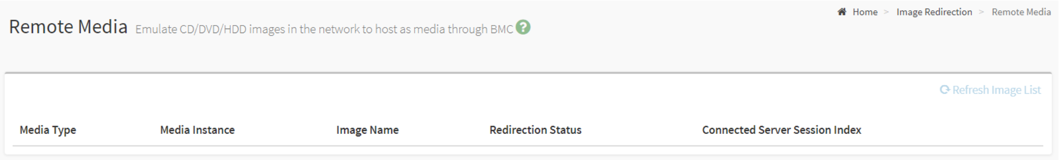


Figure 3-24 Remote Images


Remote Media
Emulate CD/DVD/HDD images in the network to host as media through BMC
Home > Image Redirection > Remote Media
Refresh Image List
Media Type
Media Instance
Image Name
Redirection Status
Connected Server Session Index

Parameters:

Table 3-26 Remote Images

Parameter	Description
Media Type	Indicates the media type (**CD/DVD, Hard Disk**, or **All**).
Media Instance	The media quantity.
Image Name	The name of the image.
Redirection Status	Indicates the media redirection status.
Connected Server Session Index	The session index.

3.5.3 Media Redirection Settings

Description:

On the **Media Redirection** page, you can configure the media redirection functions, including:

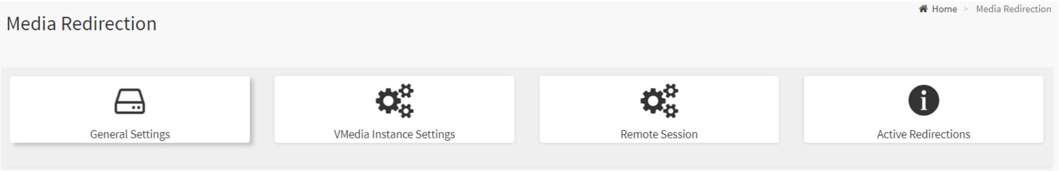
- General Settings
- VMedia Instance Settings

- Remote Session
- Active Redirections

Screen description:

In the navigation pane, select **Remote Control** > **Media Redirection** to open the page shown in Figure 3-25.

Figure 3-25 Media Redirection Settings



Parameters:

Table 3-27 Media Redirection

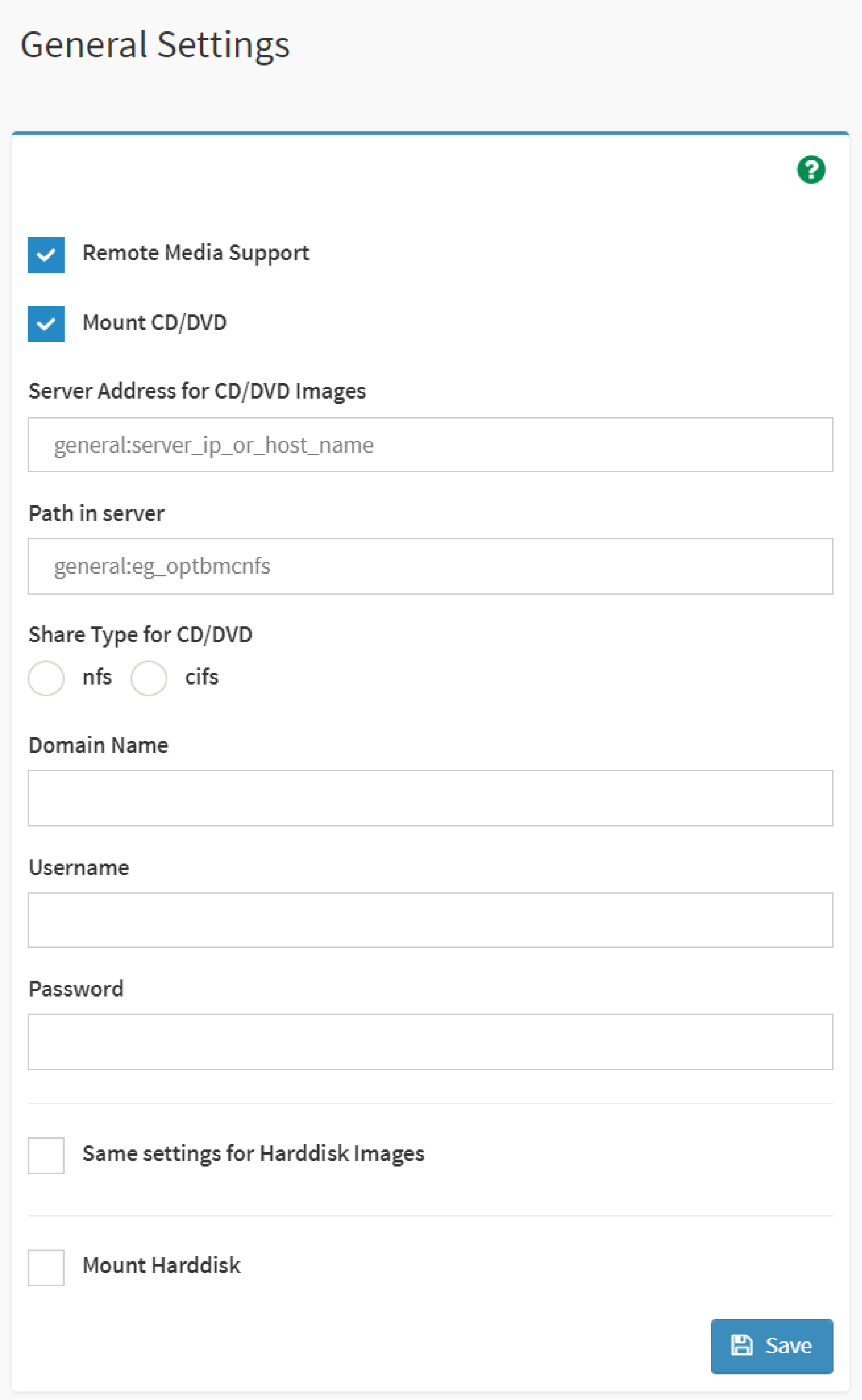
Parameter	Description
General Settings	Sets remote media support, including CDs/DVDs and drives.
VMedia Instance Settings	Sets the number of supported device instances, including CD/DVD instances, hard disk instances, remote KVM CD/DVD instances, and remote KVM hard disk instances. Sets the media encryption and power save mode.
Remote Session	Sets the KVM client type, Java KVM encryption, keyboard language, and server monitoring.
Active Redirections	Displays the list of redirecting media.

3.5.3.1 General Settings

Screen description:

In the navigation pane, select **Remote Control** > **Media Redirection** and click **General Settings** to open the pages shown in Figure 3-26 and Figure 3-27.

Figure 3-26 Mount CD/DVD in General Settings



General Settings

☑ Remote Media Support

☑ Mount CD/DVD

Server Address for CD/DVD Images

general:server_ip_or_host_name

Path in server

general:eg_optbmcnfs

Share Type for CD/DVD

○ nfs ○ cifs

Domain Name

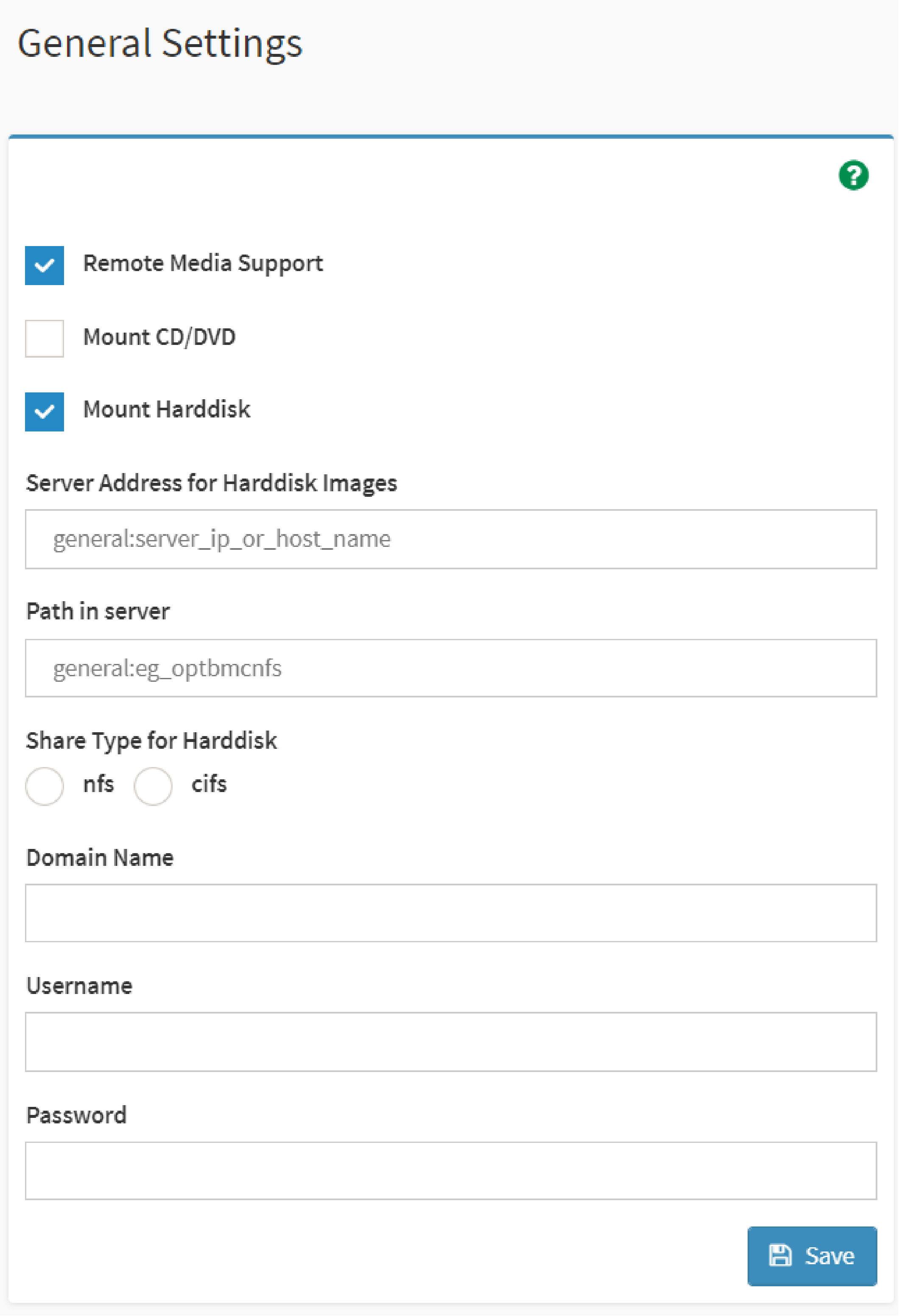
Username

Password

□ Same settings for Harddisk Images

□ Mount Harddisk

Figure 3-27 Mount Hard Disk in General Settings



General Settings

☑ Remote Media Support

□ Mount CD/DVD

☑ Mount Harddisk

Server Address for Harddisk Images

general:server_ip_or_host_name

Path in server

general:eg_optbmcnfs

Share Type for Harddisk

○ nfs ○ cifs

Domain Name

Username

Password

Parameters:

Table 3-28 General Settings

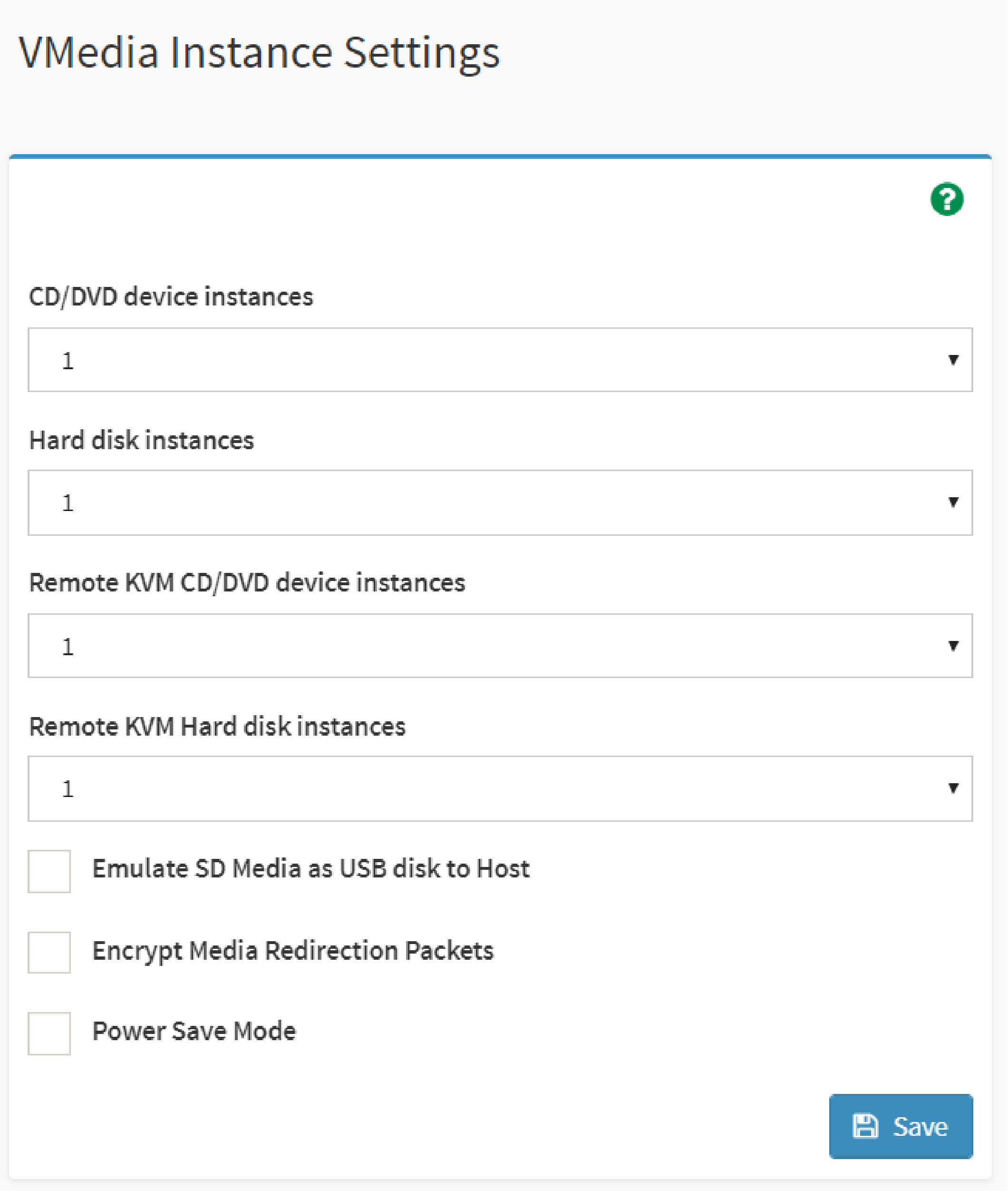
Parameter	Description
Remote Media Support	Check the box to enable Remote Media Support.
Mount CD/DVD	Check the box to enable **Mount CD/DVD**. To mount CD/DVD images, specify the **Server Address for CD/DVD Images**, **Path in server**, **Share Type for CD/DVD**, **Domain Name**, **Username**, **Password**, and **Same settings for Harddisk Images**
Mount Harddisk	Check the box to enable **Mount Hard Disk**. To mount hard disks, specify the **Server Address for Harddisk Images**, **Path in server**, and **Share Type for Harddisk**.

3.5.3.2 VMedia Instance Settings

Screen description:

In the navigation pane, select **Remote Control** > **Media Redirection** and click **VMedia Instance Settings** to open the page as shown below.

Figure 3-28 VMedia Instance Settings



VMedia Instance Settings

CD/DVD device instances

1 ▾

Hard disk instances

1 ▾

Remote KVM CD/DVD device instances

1 ▾

Remote KVM Hard disk instances

1 ▾

□ Emulate SD Media as USB disk to Host

□ Encrypt Media Redirection Packets

□ Power Save Mode

Parameters:

Table 3-29 VMedia Instance Settings

Parameter	Description
CD/DVD device instances	Selects the number of CD/DVD drives that support virtual media redirection in the drop-down list.
Hard disk instances	Selects the number of drives that support virtual media redirection.

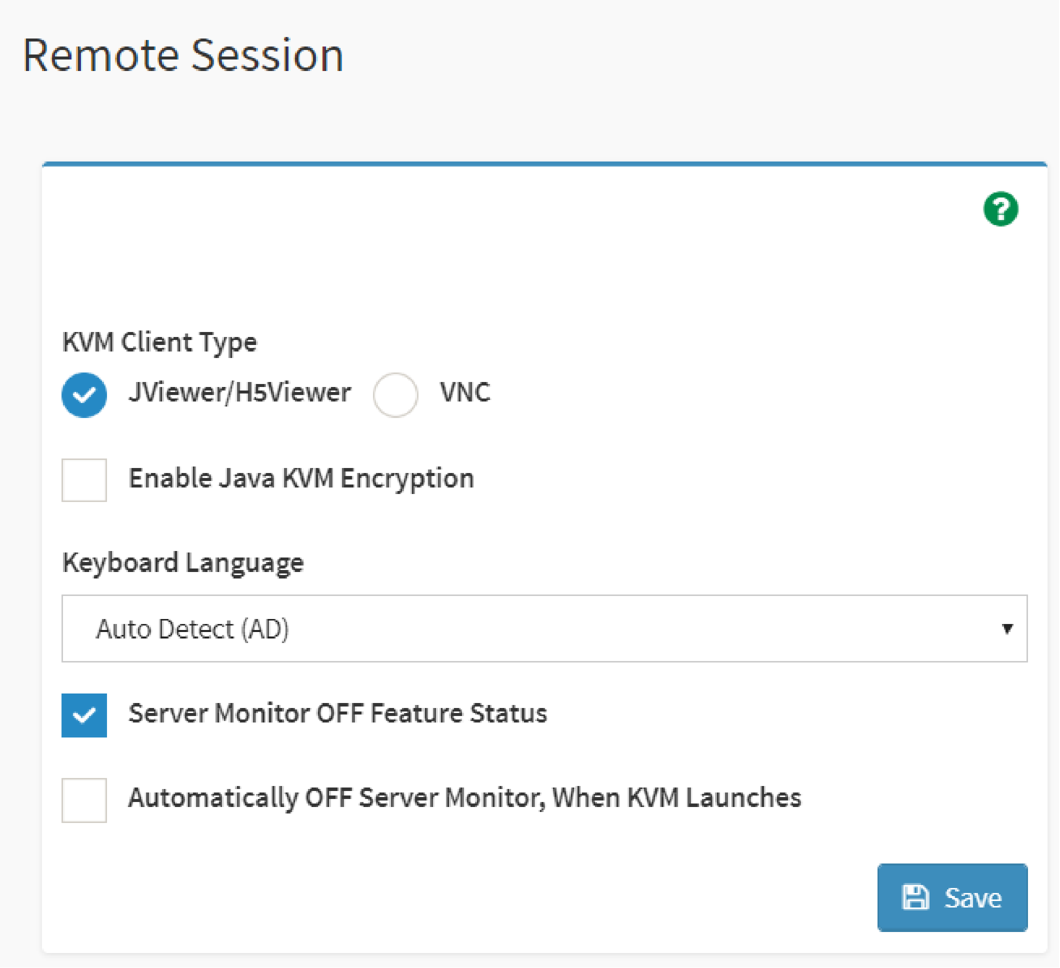
Parameter	Description
Remote KVM CD/DVD device instances	Selects the number of KVM CD/DVD drives that support virtual media redirection in the drop-down list with a maximum of 2 for HTML5 and 5 for Java.
Remote KVM Hard disk instances	Selects the number of remote KVM drives that support virtual media redirection.
Emulate SD Media as USB disk to Host	Enables or disables SD card media support.
Encrypt Media Redirection Packets	Check the box to enable BMC media encryption support. Note: If media redirection settings are available, this option can be changed. When non-secure communication is not allowed, media encryption cannot be disabled.
Power Save Mode	Check the box to enable the BMC Power Save Mode.

3.5.3.3 Remote Session

Screen description:

In the navigation pane, select **Remote Control** > **Media Redirection** and click **Remote Session** to open the page as shown below.

Figure 3-29 Remote Session



Remote Session

KVM Client Type

● JViewer/H5Viewer ○ VNC

□ Enable Java KVM Encryption

Keyboard Language

Auto Detect (AD) ▾

☑ Server Monitor OFF Feature Status

□ Automatically OFF Server Monitor, When KVM Launches

Parameters:

Table 3-30 Remote Session

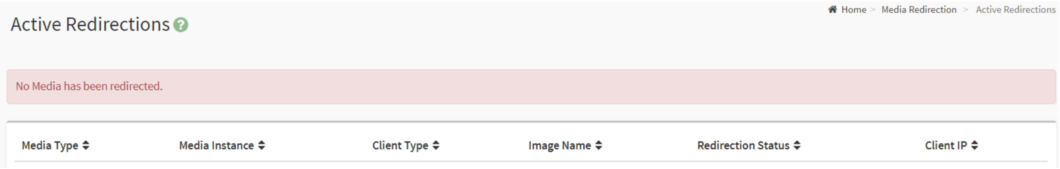
Parameter	Description
KVM Client Type	Indicates the KVM client type (**JViewer/H5Viewer** and **VNC)**.
Enable Java KVM Encryption	Enables KVM encryption when JViewer is launched.
Keyboard Language	Selects the keyboard language in the drop-down list.
Server Monitor OFF Feature Status	Check the box to turn off server monitor.
Automatically OFF Server Monitor, When KVM Launches	Check the box to automatically turn off server monitor when the KVM launches.

3.5.3.4 Active Redirections

Screen description:

In the navigation pane, select **Remote Control** > **Media Redirection** and click **Active Redirections** to open the page as shown below.

Figure 3-30 Active Redirections



Active Redirections

Home > Media Redirection > Active Redirections

No Media has been redirected.

Media Type	Media Instance	Client Type	Image Name	Redirection Status	Client IP

Parameters:

Table 3-31 Active Redirections

Parameter	Description
Media Type	Indicates the media type (**CD/DVD, Hard Disk**, or **All**).
Media Instance	Indicates the total number of media instances.
Client Type	Indicates the client type.
Image Name	Indicates the default image name on the server.
Redirection Status	Indicates the media redirection status.
Client IP	Indicates the IP address of the client.

3.5.4 Server Location UID Control

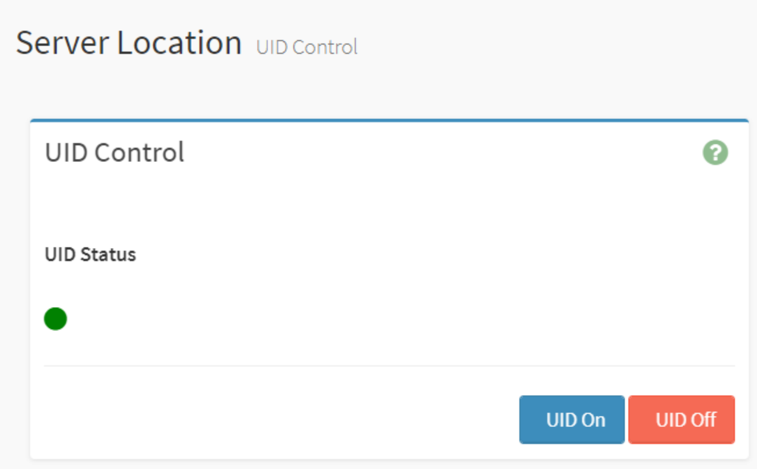
Description:

On the **Server Location** page, you can locate the server by turning the UID on and off.

Screen description:

In the navigation pane, select **Remote Control** > **Server Location UID Control** to open the page as shown below.

Figure 3-31 Server Location



Parameters:

Table 3-32 Server Location UID

Parameter	Description
UID Status	🟢 The current server UID LED is on. ⚪ The current server UID LED is off.
UID On	Turns on the current server UID.
UID Off	Turns off the current server UID.

3.6 Logs & Alarms

Description:

Logs & Alarms provide the change history of major devices and system alarms for fault diagnosis and analysis.

3.6.1 System Event Log

Description:

On the **System Event Log** page, you can view, download, and clear the BMC event logs. The System Event Log (SEL) has the following features:

- Up to 3,639 entries are supported.
- The circular mode is supported. When the SEL is full, previous logs will be discarded (oldest first).
- When the log is cleared, a **SEL Cleared** entry will be added to the SEL.
- You can export the SEL through Web or IPMI CMD.
- You can report events to the remote client through SNMP Trap and Syslog.

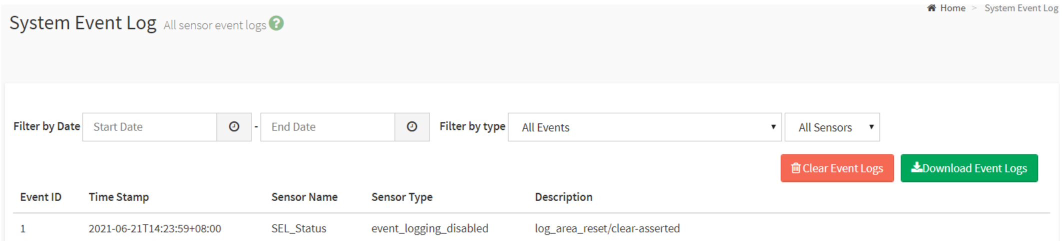
NOTE

You can also access the SEL through IPMI CMD.

Screen description:

In the navigation pane, select **Logs & Alarms** > **System Event Log** to open the page as shown below.

Figure 3-32 System Event Log



Event ID	Time Stamp	Sensor Name	Sensor Type	Description
1	2021-06-21T14:23:59+08:00	SEL_Status	event_logging_disabled	log_area_reset/clear-asserted

Parameters:

Table 3-33 SEL Parameters

Parameter	Description
Event ID	The event ID in the SEL.
Time Stamp	The time when the SEL was generated.
Sensor Name	Sensor names. You can query the names of all sensors on the device by running **ipmitool sdr elist**.
Sensor Type	Sensor types defined in IPMI 2.0, including: Temperature: Temperature sensor

Parameter	Description
	Voltage: Voltage sensor Processor: CPU status sensor Power Unit: Sensor that detects the status of PSUs Memory: Memory status sensor Drive Slot: Drive status sensor Critical Interrupt: PCIe status sensor
Description	The details of the event.

Table 3-34 System Event Log Operations

Parameter	Description
Filter	Filters by the event type, sensor, and start and end dates. Action: You can use filter options (the event type, sensor name, start and end dates) to query specific events recorded in the device.
Download Event Logs	Click to download event logs to the local computer.
Clear Event Logs	Click to delete all existing sensor log entries.

3.6.2 Log Settings

Description:

On the **Log Settings** page, you can configure Syslog to allow the BMC system to send logs to the third-party server as Syslog messages.

Screen description:

In the navigation pane, select **Logs & Alarms** > **Log Settings** to open the page shown in Figure 3-33. Click **Syslog Settings** to open the page shown in Figure 3-34.

Figure 3-33 Log Settings

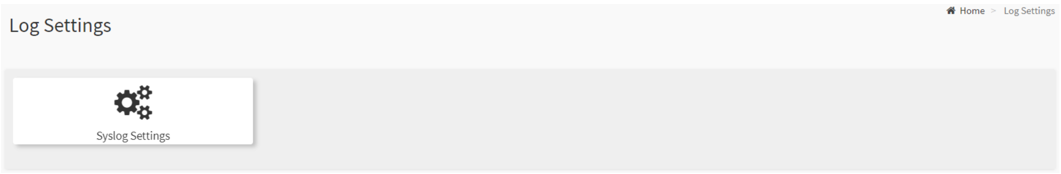
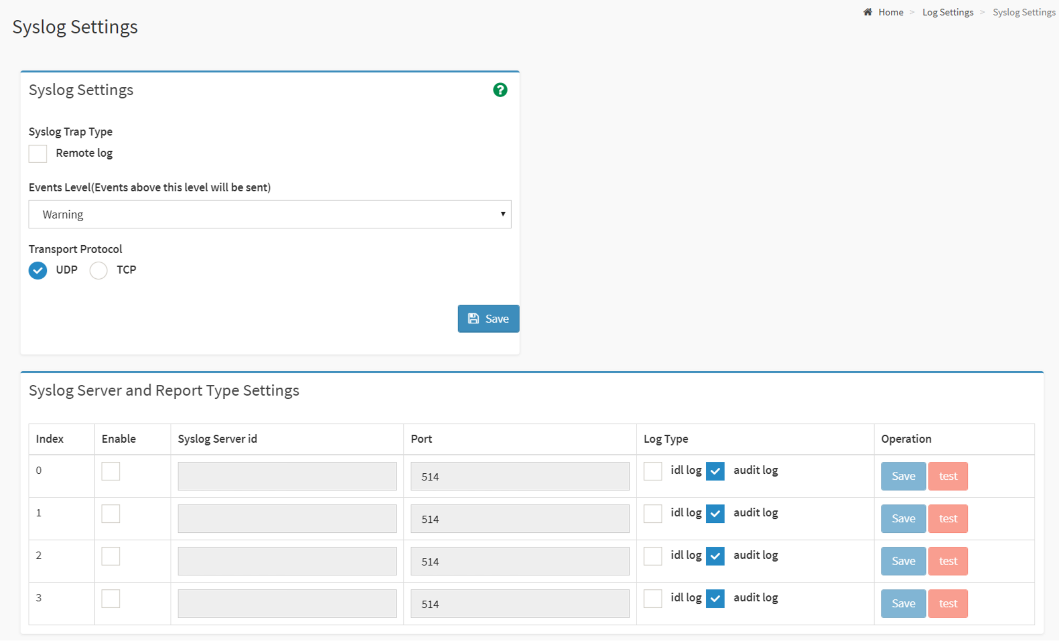


Figure 3-34 Syslog Settings



Syslog Settings

Home > Log Settings > Syslog Settings

Syslog Settings

Syslog Trap Type

□ Remote log

Events Level(Events above this level will be sent)

Warning ▾

Transport Protocol

● UDP ○ TCP

Save

Syslog Server and Report Type Settings

Index	Enable	Syslog Server id	Port	Log Type	Operation
0	□		514	□ idl log ☑ audit log	Save test
1	□		514	□ idl log ☑ audit log	Save test
2	□		514	□ idl log ☑ audit log	Save test
3	□		514	□ idl log ☑ audit log	Save test

Parameters:

Table 3-35 Syslog Settings

Parameter	Description
Remote log	The location where the Syslog alarm log is stored. You can choose whether to store logs on a remote server. When Remote Log is enabled, BMC stores logs in the remote Syslog server and local log files. Otherwise, logs are stored only in local log files.
Events Level	Events above this level will be sent. Options include: • Info: Send alarms of the Info, Warning, and Critical levels. • Warning: Send alarms of the Warning and Critical levels. • Critical: Send only alarms of the Critical level.
Transport Protocol	The transport protocol used when Syslog messages are transmitted between the BMC system and the Syslog server. Options include: • UDP: Refers to a connectionless protocol. No connection needs to be established between the source and destination before you transmit data.

Parameter	Description
	• TCP: Refers to a connection-oriented protocol. It requires a reliable connection between the source and destination before you transmit data.

Table 3-36 Syslog Server and Message Settings

Parameter	Description
Index	The serial number.
Enable	Enables or disables automatic Syslog message sending.
Syslog Server id	The address of the Syslog server.
Port	The port number of the Syslog server.
Log Type	The log type that needs to be sent in a Syslog message. Options include: idl log, audit log, or both.
Operation	● Save: Saves the information about the Syslog server and messages. ● Test: Tests whether the Syslog channel is available.

3.6.3 Audit Log

Description:

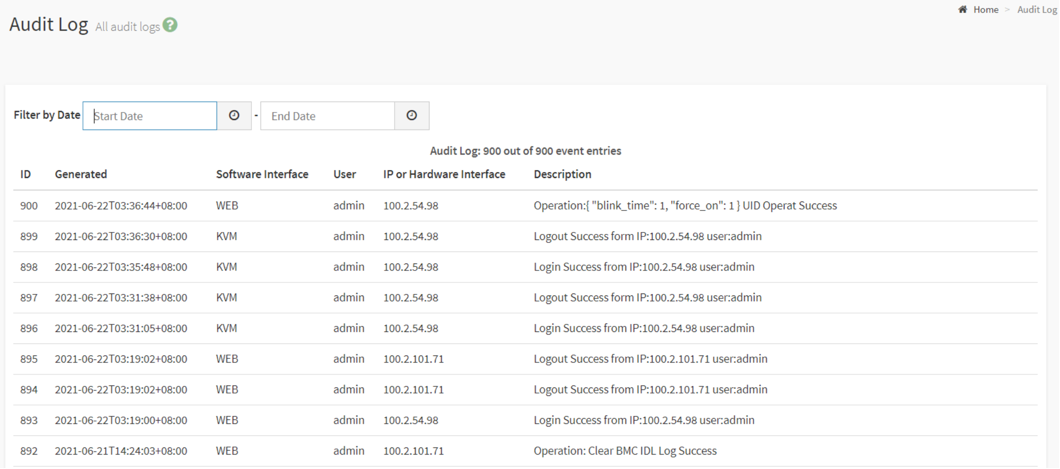
On the **Audit Log** page, you can view the BMC audit logs, The BMC audit logs have the following features:

- Key behaviors via SSH, Web, IPMI, and Redfish interfaces will be recorded, including but not limited to login, logout, user management, password management, authorization management, and changes to core security configuration (such as access control policies, automatic update policies, security monitoring policies, and audit functions), firmware updates, and recovery.
- The maximum size of an audit log is 200 KB. When the size exceeds 200 KB, earlier audit logs will be backed up to the BMC. You can view the current audit log through Web and download earlier logs by using the one-key log collection function.

Screen description:

In the navigation pane, select **Logs & Alarms** > **Audit Log** to open the page as shown below.

Figure 3-35 Audit Log



Audit Log All audit logs

Filter by Date Start Date - End Date

Audit Log: 900 out of 900 event entries

ID	Generated	Software Interface	User	IP or Hardware Interface	Description
900	2021-06-22T03:36:44+08:00	WEB	admin	100.2.54.98	Operation:{ "blink_time": 1, "force_on": 1 } UID Operat Success
899	2021-06-22T03:36:30+08:00	KVM	admin	100.2.54.98	Logout Success form IP:100.2.54.98 user:admin
898	2021-06-22T03:35:48+08:00	KVM	admin	100.2.54.98	Login Success from IP:100.2.54.98 user:admin
897	2021-06-22T03:31:38+08:00	KVM	admin	100.2.54.98	Logout Success form IP:100.2.54.98 user:admin
896	2021-06-22T03:31:05+08:00	KVM	admin	100.2.54.98	Login Success from IP:100.2.54.98 user:admin
895	2021-06-22T03:19:02+08:00	WEB	admin	100.2.101.71	Logout Success from IP:100.2.101.71 user:admin
894	2021-06-22T03:19:02+08:00	WEB	admin	100.2.101.71	Logout Success from IP:100.2.101.71 user:admin
893	2021-06-22T03:19:00+08:00	WEB	admin	100.2.54.98	Login Success from IP:100.2.54.98 user:admin
892	2021-06-21T14:24:03+08:00	WEB	admin	100.2.101.71	Operation: Clear BMC IDL Log Success

Parameters:

Table 3-37 Audit Log Parameters

Parameter	Description
ID	The serial number of an audit log. A log with a smaller serial number was generated earlier.
Generated	The time when the audit log was generated.
Software Interface	Options include: • Web • CLI • IPMI • KVM • VMEDIA_CD • VMEDIA_HD
User	The user who triggered the log event such as admin, sysadmin, or NA.
IP or Hardware Interface	The IP address or the hardware interface. Hardware interfaces include Serial, HOST, IPMB, USB, and SSIF.
Description	The details of the event.

Table 3-38 Parameters of Audit Logs and System Logs

Parameter	Description
Filter	Filters by start and end dates.

Parameter	Description
	Action: You can use filter options (the start and end dates) to query specific events recorded in the device.

3.6.4 IDL

Description:

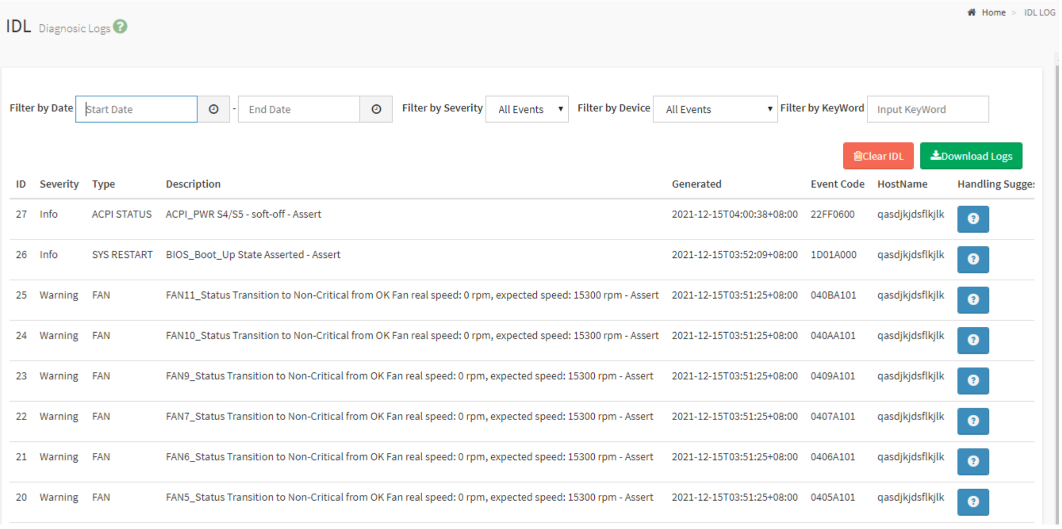
IDL is a unique log type of BMC to record events on BMC devices based on IPMI sensors. An IDL corresponds to a system event log. But compared with system logs, IDLs provide more comprehensive and complete information. Each log entry has a handling suggestion, which can help you diagnose and analyze logs more effectively. IDL entries can be filtered by date, severity, device, and keyword. You can download and clear the logs. Click the ? button for each log entry to view its handling suggestion and processing steps.

On the **IDL** page, you can view the list of BMC IDLs on the device. Click the **Handling Suggestion** button on the right of each event to view the specific suggestion.

Screen description:

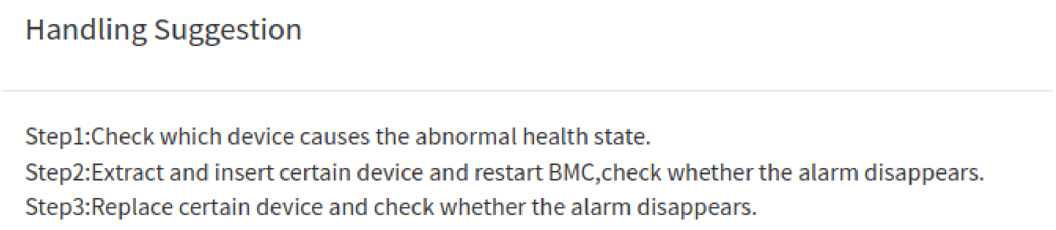
In the navigation pane, select **Logs & Alarms** > **IDL** to open the page shown in Figure 3-36. Then, click ? to open the page for specific handling suggestion, as shown in Figure 3-37.

Figure 3-36 IDL



ID	Severity	Type	Description	Generated	Event Code	HostName	Handling Sugge:
27	Info	ACPI STATUS	ACPI_PWR S4/S5 - soft-off - Assert	2021-12-15T04:00:38+08:00	22FF0600	qasdjkjdsflkjlk	?
26	Info	SYS RESTART	BIOS_Boot_Up State Asserted - Assert	2021-12-15T03:52:09+08:00	1D01A000	qasdjkjdsflkjlk	?
25	Warning	FAN	FAN11_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	040BA101	qasdjkjdsflkjlk	?
24	Warning	FAN	FAN10_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	040AA101	qasdjkjdsflkjlk	?
23	Warning	FAN	FAN9_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	0409A101	qasdjkjdsflkjlk	?
22	Warning	FAN	FAN7_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	0407A101	qasdjkjdsflkjlk	?
21	Warning	FAN	FAN6_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	0406A101	qasdjkjdsflkjlk	?
20	Warning	FAN	FAN5_Status Transition to Non-Critical from OK Fan real speed: 0 rpm, expected speed: 15300 rpm - Assert	2021-12-15T03:51:25+08:00	0405A101	qasdjkjdsflkjlk	?

Figure 3-37 Handling Suggestion



Handling Suggestion

Step1:Check which device causes the abnormal health state.
Step2:Extract and insert certain device and restart BMC,check whether the alarm disappears.
Step3:Replace certain device and check whether the alarm disappears.

Parameters:

Table 3-39 IDL Configuration Parameters

Parameter	Description
ID	The event ID of the IDL.
Severity	The event severity (Info/Warning/Critical).
Type	The component associated with the alarm event. Component types include: • FAN • INTRUSION • CPU • PSU • ADDIN CARD • MEMORY • DISK • SYS FW PROGRESS • EVENT LOG • WATCHDOG1 • SYSTEM EVENT • POWER BUTTON • MAINBOARD • PCIe • BMC • PCH • CABLE

Parameter	Description
	• SYS RESTART • BOOT ERROR • BIOS BOOT • OS STATUS • ACPI STATUS • IPMI WATCHDOG • LAN • SUB SYSTEM • BIOS OPTIONS • GPU • RAID • FW UPDATE • Cable • SYSTEM • SNMP TEST • SMTP TEST
Description	The detailed description of the alarm event.
Generated	The time when the IDL was generated.
Event Code	The unique fault code of the event with a length of 8 bytes. For details about IDL event codes, see Table 3-41.
HostName	The name of the server.
Handling Suggestion	Suggestion on how to solve the alarm event.

Table 3-40 IDL Operations

Parameter	Description
Filter	Filters by severity and start and end dates. Action: You can use filter options (the severity, date, and keyword) to query specific events recorded in the device.
Download Logs	Downloads the IDL to the local computer.
Clear Logs	Click the **Clear IDL** button to clear all IDLs recorded on BMC.

Table 3-41 IDL Event Codes

Byte	Description
6 - 7	The component type. A hexadecimal number corresponds to a component type: • 04: FAN • 05: INTRUSION • 07: CPU • 08: PSU • 0B: ADDIN_CARD • 0C: MEMORY • 0D: DISK
4 - 5	The serial number of the component, which indicates the serial number for this component type.
2 - 3	The offset of the event indicates the type of the event. Particular offsets are specified in IPMI protocol for events of different types of sensors.
0 - 1	The event level. A hexadecimal number corresponds to an event level: • 00: INFO • 01: WARNING • 02: CRITICAL • 03: ALERT

3.6.5 One-key Collection Log

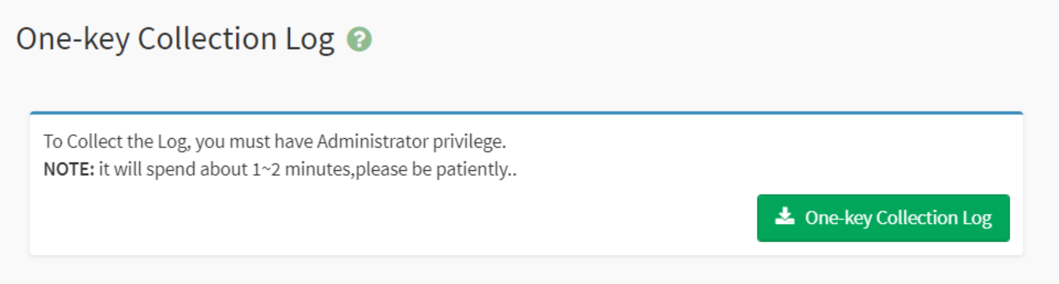
Description:

On the **One-key Collection Log** page, you can collect all the information required for fault diagnosis and analysis with one click, including logs, running data, BMC configuration, and components. It takes about 1 to 2 minutes to complete the log collection.

Screen description:

In the navigation pane, select **Logs & Alarms** > **One-key Collection Log** to open the page as shown below.

Figure 3-38 One-key Collection Log



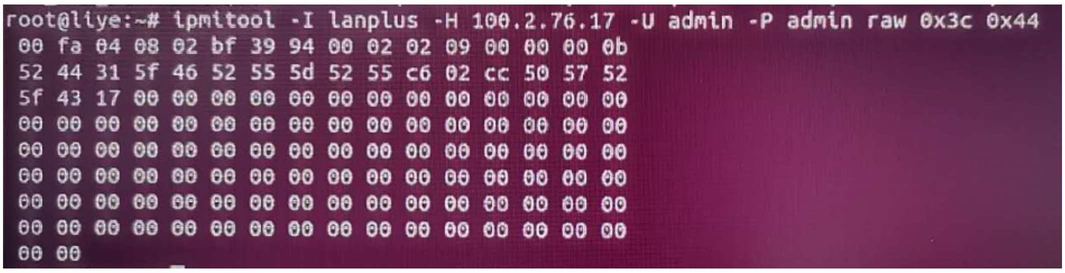
One-key Collection Log

To Collect the Log, you must have Administrator privilege.
NOTE: it will spend about 1~2 minutes,please be patiently..

You can query the progress of the one-key collection log by running the **ipmitool** command. For example:

ipmitool -I lanplus -H 100.2.76.17 -U admin -P admin raw 0x3C 0x44

Figure 3-39 Querying the Status of One-key Collection Log



```
root@liye:~# ipmitool -I lanplus -H 100.2.76.17 -U admin -P admin raw 0x3c 0x44
 00 fa 04 08 02 bf 39 94 00 02 02 09 00 00 00 0b
 52 44 31 5f 46 52 55 5d 52 55 c6 02 cc 50 57 52
 5f 43 17 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00
```

Parameters:

Table 3-42 Commands for Querying the Progress of One-key Collection Log

Get Onekeylog Rate		
	Byte	Data Field
NetFn	0x3C	
Cmd	0x44	
Request Data	N/A	
Response Data	Byte0	completecode. 00h = Ok, normal, complete. C1h = Command is invalid.
	Byte1	rate = The collection progress in hexadecimal.
	Byte2	status = The collection status. 0xfc = Collection completed. 0xfe = Collection in progress. 0xfb = Failed to compress the file. 0xfa = Collection is not yet started. 0xfd = The collection begins. 0xf1 = Failed to delete the existing folder.

Get Onekeylog Rate		
	Byte2-129	file_name. The file name identified with ASCII code.

After the logs are collected, the downloaded items are shown in the table below, including logs, running data, configuration, and components.

Table 3-43 Item List of One-key Collection Log

Category	Item	Path in One-key Collection Log File
Log	SEL	onekeylog/log/selelist.csv
	Audit log	onekeylog/log/audit.log, audit.log1
	IDL	onekeylog/log/idl.log
	System log	onekeylog/log/info.log, info.log1 onekeylog/log/warning.log, warning.log1 onekeylog/log/err.log, onekeylog/log/err.log.1 onekeylog/log/crit.log onekeylog/log/alert.log onekeylog/log/emerg.log
	Maintenance log	onekeylog/log/maintenance.log, maintenance.log.1
	PSU fault history	onekeylog/log/psuFaultHistory.log
	RAID log	onekeylog/log/raid%d.log (%d ranges from 0 to 7)
	Serial port log	onekeylog/sollog/solHostCaptured.log, onekeylog/sollog/solHostCaptured.log.1
	BMC UART log	onekeylog/sollog/BMCUart.log, onekeylog/sollog/BMCUart.log.1
	NIC log	onekeylog/sollog/NetCard.log, onekeylog/sollog/NetCard.log.1
	Crash screenshot	onekeylog/log/CaptureScreen/IERR/IERR_Capture.jpeg
	Crash screen recording	onekeylog/log/CaptureScreen/MCERR/MCE_Error2_Capture1.jpeg MCE_Error2_Capture2.jpeg
	Linux kernel log	onekeylog/log/dmesg
	BMC SEL	onekeylog/log/BMC1/SEL.dat
	Flash status log	onekeylog/log/flash_status
	SNMP Trap statistical log	onekeylog/log/index.log

Category	Item	Path in One-key Collection Log File
	Notice log	onekeylog/log/notice.log, onekeylog/log/notice.log.1
	Parsing log after fault diagnosis	onekeylog/log/ErrorAnalyReport.json onekeylog/log/RegRawData.json
Running Data	CPLD register	onekeylog/runningdata/cpldinfo.log
	MCA register	onekeylog/runningdata/RegRawData.json
	POST code	onekeylog/runningdata/rundatainfo.log
	BMC time	onekeylog/runningdata/rundatainfo.log
	BMC CPU utilization	onekeylog/runningdata/rundatainfo.log
	BMC memory utilization	onekeylog/runningdata/rundatainfo.log
	BMC flash utilization	onekeylog/runningdata/rundatainfo.log
	Voltage, temperature, current, speed, and power	onekeylog/runningdata/rundatainfo.log
	Sensor information	onekeylog/runningdata/rundatainfo.log
	Process information	onekeylog/runningdata/rundatainfo.log
	Memory information	onekeylog/runningdata/meminfo.log
	Fan information	onekeylog/runningdata/faninfo.log
	Interruption information	onekeylog/runningdata/interrupts
	I^{2}C channel information	onekeylog/runningdata/rundatainfo.log
	Real-time data from the EEPROM and register by I^{2}C	onekeylog/runningdata/rundatainfo.log
	Power statistics	onekeylog/runningdata/rundatainfo.log
	SMBIOS	onekeylog/runningdata/smbios.dmp
	Files created during runtime	onekeylog/runningdata/var/
	Online session information	onekeylog/runningdata/racsessioninfo

Category	Item	Path in One-key Collection Log File
	Current BMC network information	onekeylog/runningdata/rundatainfo.log
	Current BMC routing information	onekeylog/runningdata/rundatainfo.log
	Packet sending and receiving information of network interfaces	onekeylog/runningdata/rundatainfo.log
	Cumulative running time of BMC	onekeylog/runningdata/rundatainfo.log
	Driver information	onekeylog/runningdata/rundatainfo.log
Configuration	User information	onekeylog/configuration/config.log
	DNS	onekeylog/configuration/conf/dns.conf
	BMC network	onekeylog/configuration/config.log
	SSHD configuration	onekeylog/configuration/conf/ssh_server_config
	Service (SSH/Web/KVM/IPMI LAN) configuration	onekeylog/configuration/conf/ncml.conf
	Configuration of BIOS menu items	onekeylog/configuration/conf/redfish/bios/BiosAttributeRegistry0.24.00.0.24.0.json
	Power capping configuration	onekeylog/configuration/conf/redfish/bios/bios_current_settings.json
	Email configuration	onekeylog/configuration/conf/redfish/bios//bios_future_settings.json"
	SNMP Trap configuration	onekeylog/configuration/conf/SnmTrapCfg.json
	SMTP configuration file	onekeylog/configuration/conf/SmtpCfg.json
	Syslog configuration	onekeylog/configuration/conf/syslog.conf
Component	CPU	onekeylog/configuration/conf/dhcp.preip_4
	Memory	onekeylog/configuration/conf/dhcp6c.confonekeylog/configuration/conf/dhcp6c_duid

Category	Item	Path in One-key Collection Log File
	Drive	onekeylog/configuration/conf/dcmi.conf
	PSU	onekeylog/component/component.log
	Fan	onekeylog/component/component.log
	PCIe card	onekeylog/component/component.log
	RAID card	onekeylog/component/component.log
	NIC	onekeylog/component/component.log
	BMC	onekeylog/component/component.log
	Motherboard	onekeylog/component/component.log
	Drive backplane	onekeylog/component/component.log
	PCIe Riser card	onekeylog/component/component.log
	Firmware version information	onekeylog/component/component.log

For more details, contact the BMC developer. Items in **One-Key Collection Log** may vary with different server models.

3.6.6 Current Alarms

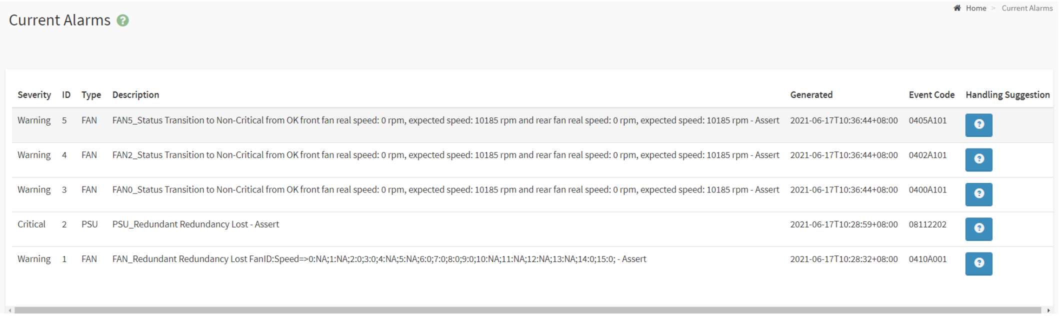
Description:

When an alarm is generated in the system log, an alarm log entry will be added. On the **Current Alarms** page, you can view the system alarms that have not been solved. Click the ? button for each log entry to view its handling suggestion and processing steps.

Screen description:

In the navigation pane, select **Logs & Alarms** > **Current Alarms** to open the page as shown below.

Figure 3-40 Current Alarms



Severity	ID	Type	Description	Generated	Event Code	Handling Suggestion
Warning	5	FAN	FAN5_Status Transition to Non-Critical from OK front fan real speed: 0 rpm, expected speed: 10185 rpm and rear fan real speed: 0 rpm, expected speed: 10185 rpm - Assert	2021-06-17T10:36:44+08:00	0405A101	?
Warning	4	FAN	FAN2_Status Transition to Non-Critical from OK front fan real speed: 0 rpm, expected speed: 10185 rpm and rear fan real speed: 0 rpm, expected speed: 10185 rpm - Assert	2021-06-17T10:36:44+08:00	0402A101	?
Warning	3	FAN	FAN0_Status Transition to Non-Critical from OK front fan real speed: 0 rpm, expected speed: 10185 rpm and rear fan real speed: 0 rpm, expected speed: 10185 rpm - Assert	2021-06-17T10:36:44+08:00	0400A101	?
Critical	2	PSU	PSU_Redundant Redundancy Lost - Assert	2021-06-17T10:28:59+08:00	08112202	?
Warning	1	FAN	FAN_Redundant Redundancy Lost FanID:Speed=>0:NA;1:NA;2:0;3:0;4:NA;5:NA;6:0;7:0;8:0;9:0;10:NA;11:NA;12:NA;13:NA;14:0;15:0; - Assert	2021-06-17T10:28:32+08:00	0410A001	?

Parameters:

Table 3-44 Current Alarms

Parameter	Description
Severity	The alarm severity (Info/Warning/Critical).
ID	The alarm ID.
Type	The component associated with the alarm event. Component types include: • FAN • INTRUSION • CPU • PSU • ADDIN CARD • MEMORY • DISK • SYS FW PROGRESS • EVENT LOG • WATCHDOG1 • SYSTEM EVENT • POWER BUTTON • MAINBOARD • PCIe • BMC • PCH • CABLE • SYS RESTART • BOOT ERROR • BIOS BOOT • OS STATUS • ACPI STATUS • IPMI WATCHDOG

Parameter	Description
	• LAN • SUB SYSTEM • BIOS OPTIONS • GPU • RAID • FW UPDATE • SYSTEM • SNMP TEST • SMTP TEST
Description	The detailed description of the alarm event.
Generated	The time when the alarm event was generated.
Event Code	The unique fault code of the alarm event. Refer to Table 3-41 IDL Event Codes.
Handling Suggestion	Suggestion on how to solve the alarm event.

3.6.7 SNMP Trap Settings

Description:

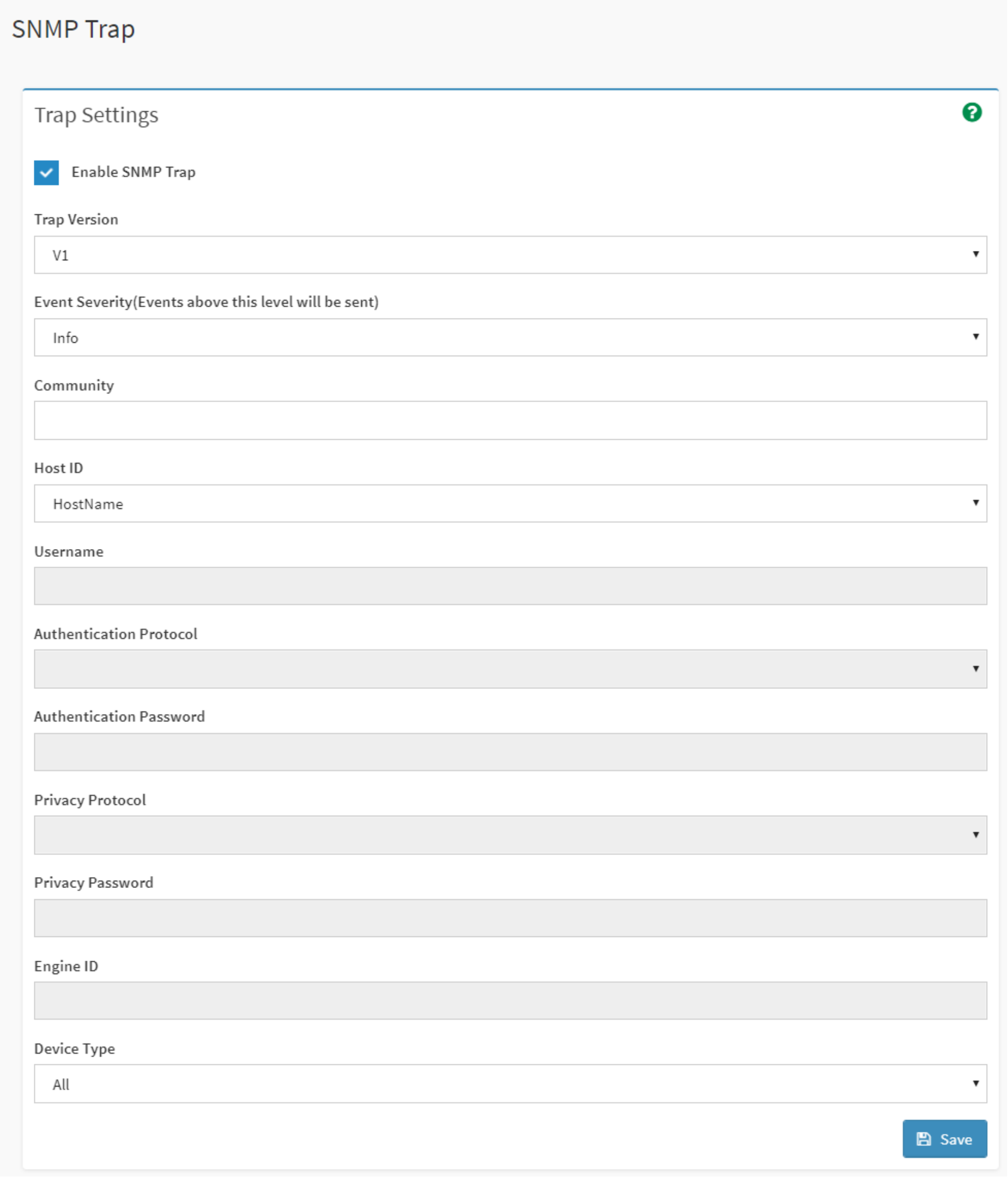
On the **SNMP Trap** page, you can:

- Enable SNMP Trap.
- Set alarm policies.

Steps:

1. In the navigation pane, select **Logs & Alarms** > **SNMP Trap** to open the page as shown below.

Figure 3-41 SNMP Trap Settings



SNMP Trap

Trap Settings

☑ Enable SNMP Trap

Trap Version: V1

Event Severity(Events above this level will be sent): Info

Community:

Host ID: HostName

Username:

Authentication Protocol:

Authentication Password:

Privacy Protocol:

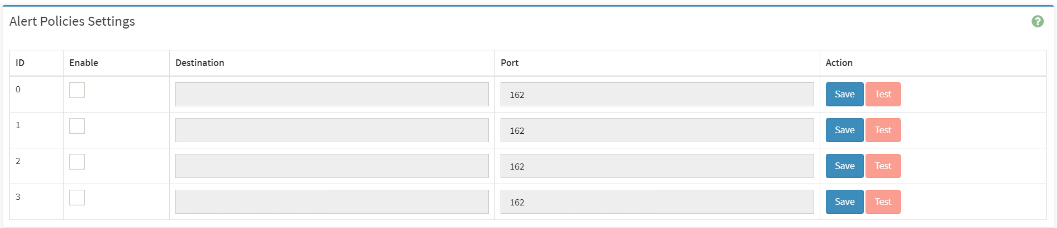
Privacy Password:

Engine ID:

Device Type: All

2. Check **Enable SNMP Trap** and then configure information such as **Trap Version**, **Event Severity**, and **Community**.
3. On the **Alert Policies Settings** page, check **Enable**, enter the IP address of the Syslog server in **Destination**, set the **Port**, and then click **Save**.

Figure 3-42 Alert Policies Settings



Alert Policies Settings

ID	Enable	Destination	Port	Action
0	☐		162	Save Test
1	☐		162	Save Test
2	☐		162	Save Test
3	☐		162	Save Test

NOTE

1. SNMP port is 162 by default.
2. BMC supports SNMP Trap. You need to open the Trap receiver and set the Trap destination IP address on the BMC Web GUI. An event detected by BMC will be automatically sent to the Trap receiver.

3.6.8 Mail Alarm

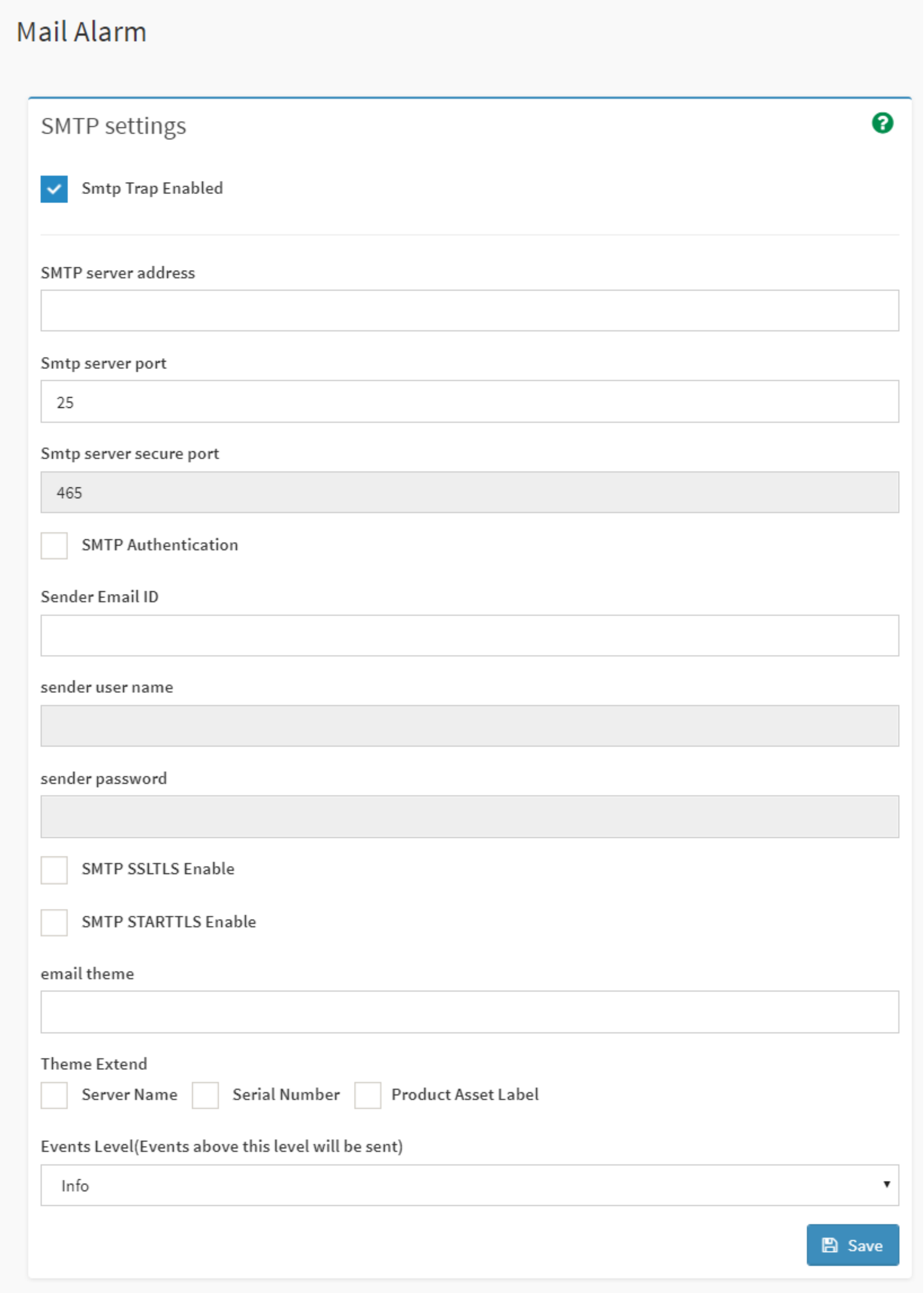
Description:

On the **Mail Alarm** page, you can enable or disable the SMTP Trap and configure related information.

Screen description:

In the navigation pane, select **Logs & Alarms** > **Mail Alarm** to open the pages shown in Figure 3-43 and Figure 3-44.

Figure 3-43 SMTP Settings



Mail Alarm

SMTP settings

☑ Smtp Trap Enabled

SMTP server address

Smtp server port

25

Smtp server secure port

465

□ SMTP Authentication

Sender Email ID

sender user name

sender password

□ SMTP SSLTLS Enable

□ SMTP STARTTLS Enable

email theme

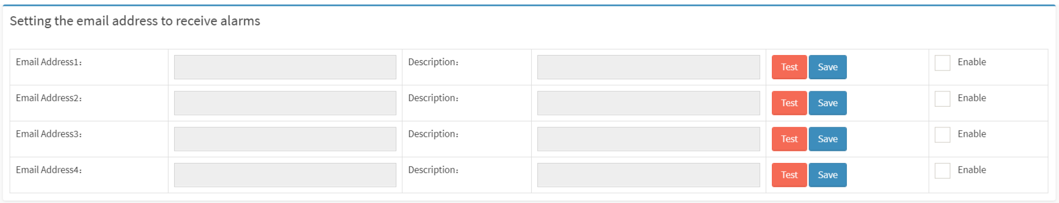
Theme Extend

□ Server Name □ Serial Number □ Product Asset Label

Events Level(Events above this level will be sent)

Info ▾

Figure 3-44 Setting the Email Address to Receive Alarms



Setting the email address to receive alarms

Email Address1:		Description:		Test Save	□ Enable
Email Address2:		Description:		Test Save	□ Enable
Email Address3:		Description:		Test Save	□ Enable
Email Address4:		Description:		Test Save	□ Enable

Parameters:

Table 3-45 Mail Alarm

Parameter	Description
SMTP Trap Enabled	Check it to enable the SMTP email alarm function, and the following parameters should be specified: SMTP server address, SMTP server port, SMTP server secure port, SMTP authentication, sender Email ID, sender user name, sender password, SMTP SSL/TLS Enable, SMTP STARTTLS Enable, email theme, Theme Extend, and Events Level.
Email Address	The email address for receiving alarms.
Description	The description of the email address.

Table 3-46 Operations on Mail Alarm

Parameter	Description
Test	Tests whether the email address can receive alarms.
Save	Saves the configured email address and its description.
Enable	Enables this email address to receive alarms.

3.7 Sensor

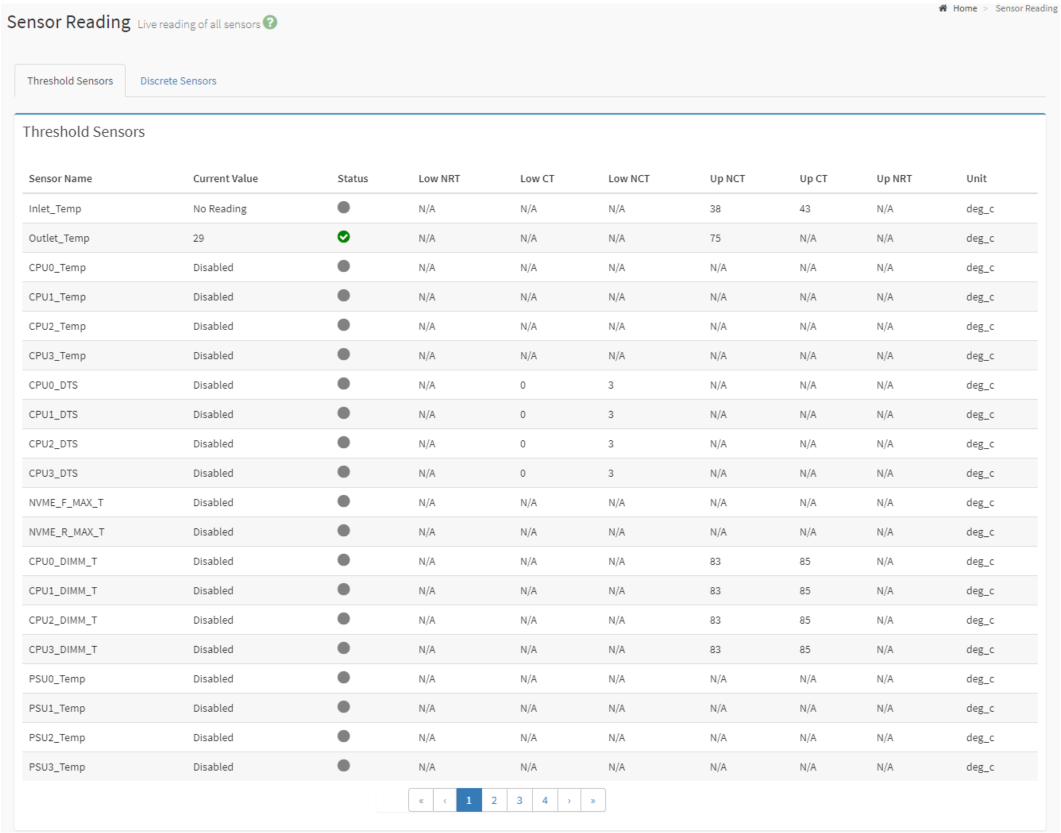
Description:

On the **Sensor** page, you can view the information of all sensors supported by the current system. You can also double-click the line of a sensor on the **Threshold Sensors** page to go to the sensor threshold modification page. The **Sensor** page includes two tabs: **Threshold Sensors** and **Discrete Sensor**s.

Screen description:

In the navigation pane, select **Sensor** and then **Threshold Sensors** to open the page as shown below.

Figure 3-45 Threshold Sensors



Threshold Sensors

Sensor Name	Current Value	Status	Low NRT	Low CT	Low NCT	Up NCT	Up CT	Up NRT	Unit
Inlet_Temp	No Reading	●	N/A	N/A	N/A	38	43	N/A	deg_c
Outlet_Temp	29	✓	N/A	N/A	N/A	75	N/A	N/A	deg_c
CPU0_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
CPU1_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
CPU2_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
CPU3_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
CPU0_DTS	Disabled	●	N/A	0	3	N/A	N/A	N/A	deg_c
CPU1_DTS	Disabled	●	N/A	0	3	N/A	N/A	N/A	deg_c
CPU2_DTS	Disabled	●	N/A	0	3	N/A	N/A	N/A	deg_c
CPU3_DTS	Disabled	●	N/A	0	3	N/A	N/A	N/A	deg_c
NVME_F_MAX_T	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
NVME_R_MAX_T	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
CPU0_DIMM_T	Disabled	●	N/A	N/A	N/A	83	85	N/A	deg_c
CPU1_DIMM_T	Disabled	●	N/A	N/A	N/A	83	85	N/A	deg_c
CPU2_DIMM_T	Disabled	●	N/A	N/A	N/A	83	85	N/A	deg_c
CPU3_DIMM_T	Disabled	●	N/A	N/A	N/A	83	85	N/A	deg_c
PSU0_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
PSU1_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
PSU2_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c
PSU3_Temp	Disabled	●	N/A	N/A	N/A	N/A	N/A	N/A	deg_c

Parameters:

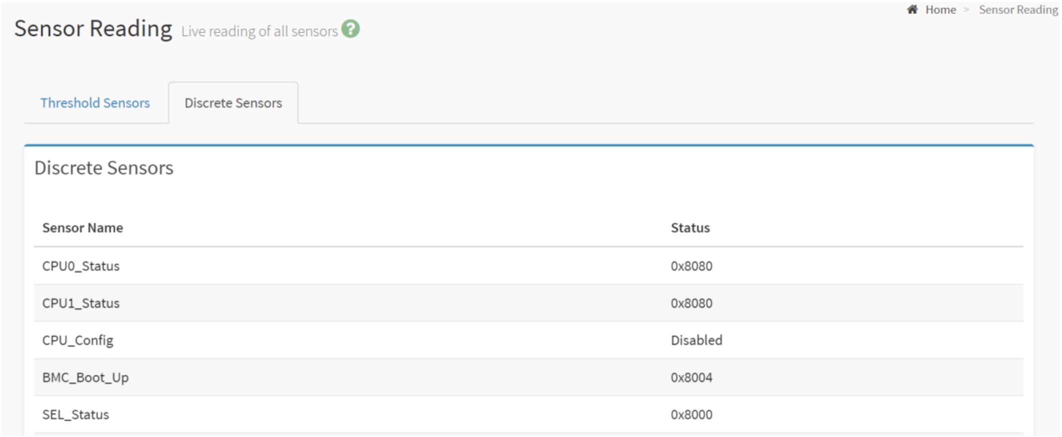
Table 3-47 Threshold Sensors

Parameter	Description
Sensor Name	The name of the sensor.
Current Value	The current reading of the sensor.
Status	The status of the sensor.
Low NRT	The low non-recoverble threshold of the sensor.
Low CT	The low critical threshold of the sensor.
Low NCT	The low non-critical threshold of the sensor.
Up NCT	The high non-critical threshold of the sensor.
Up CT	The high critical threshold of the sensor.
Up NRT	The high non-recoverble threshold of the sensor.
Unit	The unit of the sensor reading.

Screen description:

In the navigation pane, click **Sensor** and select **Discrete Sensors** to open the page as shown below.

Figure 3-46 Discrete Sensors



Discrete Sensors

Sensor Name	Status
CPU0_Status	0x8080
CPU1_Status	0x8080
CPU_Config	Disabled
BMC_Boot_Up	0x8004
SEL_Status	0x8000

Parameters:

Table 3-48 Discrete Sensors

Parameter	Description
Sensor Name	The name of the sensor.
Status	The status of the sensor.

3.8 PSU

3.8.1 Power Control

Description:

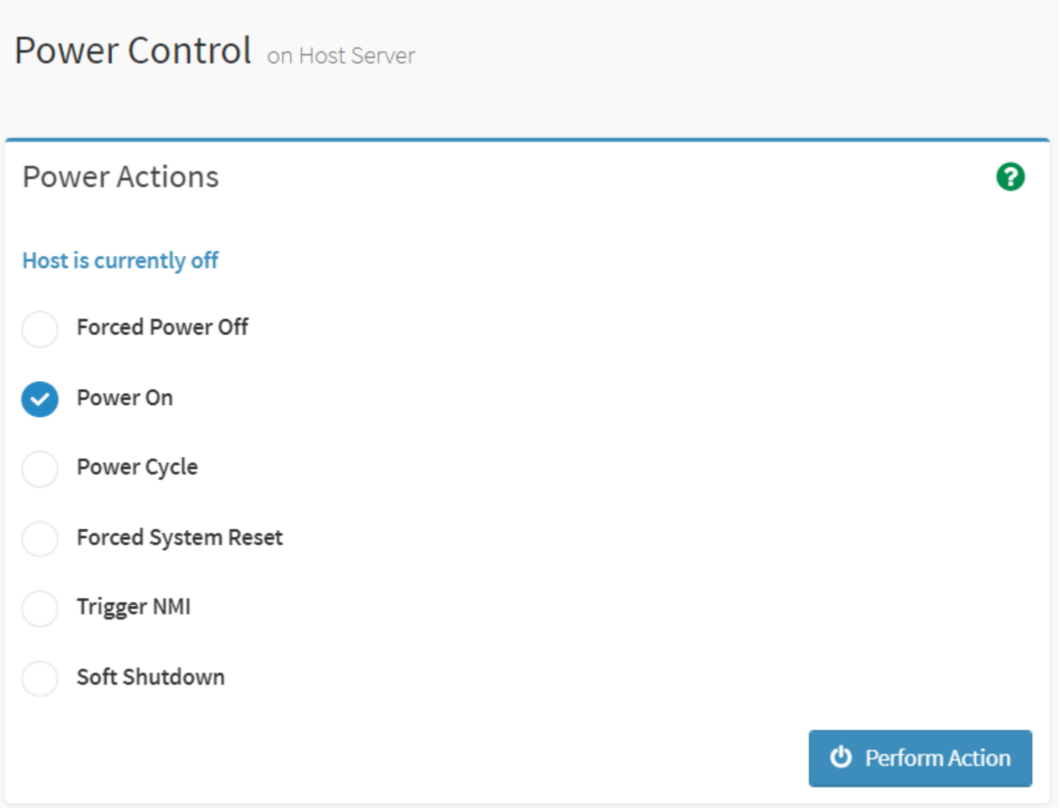
On the **Power Control** page, you can perform these operations:

- Power On
- Forced Off
- Power Cycle
- Forced System Reset
- Trigger NMI
- Soft Shutdown

Screen description:

In the navigation pane, select **Power Supply** > **Power Control** to open the page as shown below.

Figure 3-47 Power Control


Power Control on Host Server

Power Actions

Host is currently off

○ Forced Power Off

● Power On

○ Power Cycle

○ Forced System Reset

○ Trigger NMI

○ Soft Shutdown

Parameters:

Table 3-49 Power Control

Parameter	Description
Power On	Powers the server on, same to short pressing the power button.
Forced Power Off	Powers the server off forcibly, same to long pressing the power button.
Power Cycle	Power off the server, wait for 10s, and then power it on.
Forced System Reset	Same to pressing the reset button (if available).
Trigger NMI	Triggers NMI (Non-Maskable Interrupt).
Soft Shutdown	Performs an orderly shutdown, same to short pressing the power button.

3.9 Fan Management

Description:

On the **Fan Management** page, you can view its status, current speed, duty ratio, and other information of a fan module. You can also select the fan control mode, and preset the speed for each fan module in the **Manual Fan Control** mode.

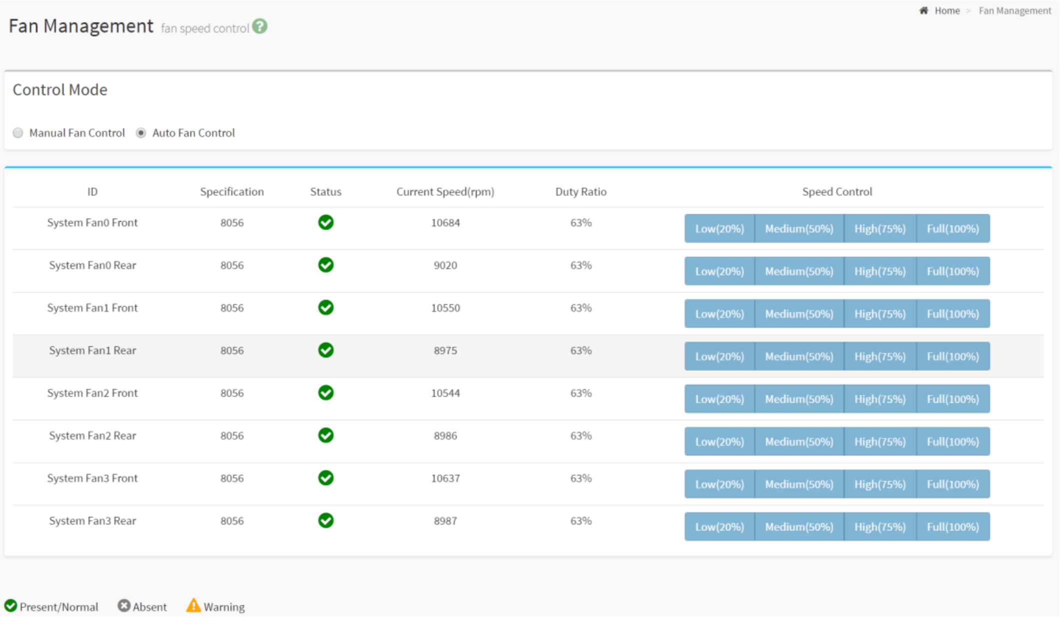
NOTE

Refer to the CMC user manual for the fan management of the multi-node server.

Screen description:

In the navigation pane, click **Fan Management** to open the page as shown below.

Figure 3-48 Fan Management



Fan Management fan speed control

Control Mode

○ Manual Fan Control ● Auto Fan Control

ID	Specification	Status	Current Speed(rpm)	Duty Ratio	Speed Control
System Fan0 Front	8056	✓	10684	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan0 Rear	8056	✓	9020	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1 Front	8056	✓	10550	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan1 Rear	8056	✓	8975	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2 Front	8056	✓	10544	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan2 Rear	8056	✓	8986	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3 Front	8056	✓	10637	63%	Low(20%) Medium(50%) High(75%) Full(100%)
System Fan3 Rear	8056	✓	8987	63%	Low(20%) Medium(50%) High(75%) Full(100%)

✓ Present/Normal ⊗ Absent ⚠ Warning

NOTE

The MCU or CPLD monitors BMC fan control tasks by receiving BMC watchdog signals. Failure to receive the watchdog signal within 4 minutes indicates that the current fan control task is running improperly. All fans are set to secure speeds to prevent system overheating.

Parameters:

Table 3-50 Fan Management

Parameter	Description
Control Mode	Options: **Manual Fan Control** or **Auto Fan Control**

Parameter	Description
	In the **Manual Fan Control** mode, you can manually adjust the speed of each fan.
ID	The fan ID.
Specification	The specification of the fan, such as 8056 or 8038.
Status	The status of the fan: ✅ Present/Normal ⚠ Warning ● Absent/LED off
Current Speed	The current speed of the fan.
Duty Ratio	The current duty ratio of the fan.
Speed Control	In the **Manual Fan Control** mode, you can set the speed to: • Low (20%) • Medium (50%) • High (75%) • Full (100%)

3.10 System Settings

3.10.1 BIOS Boot Options

Description:

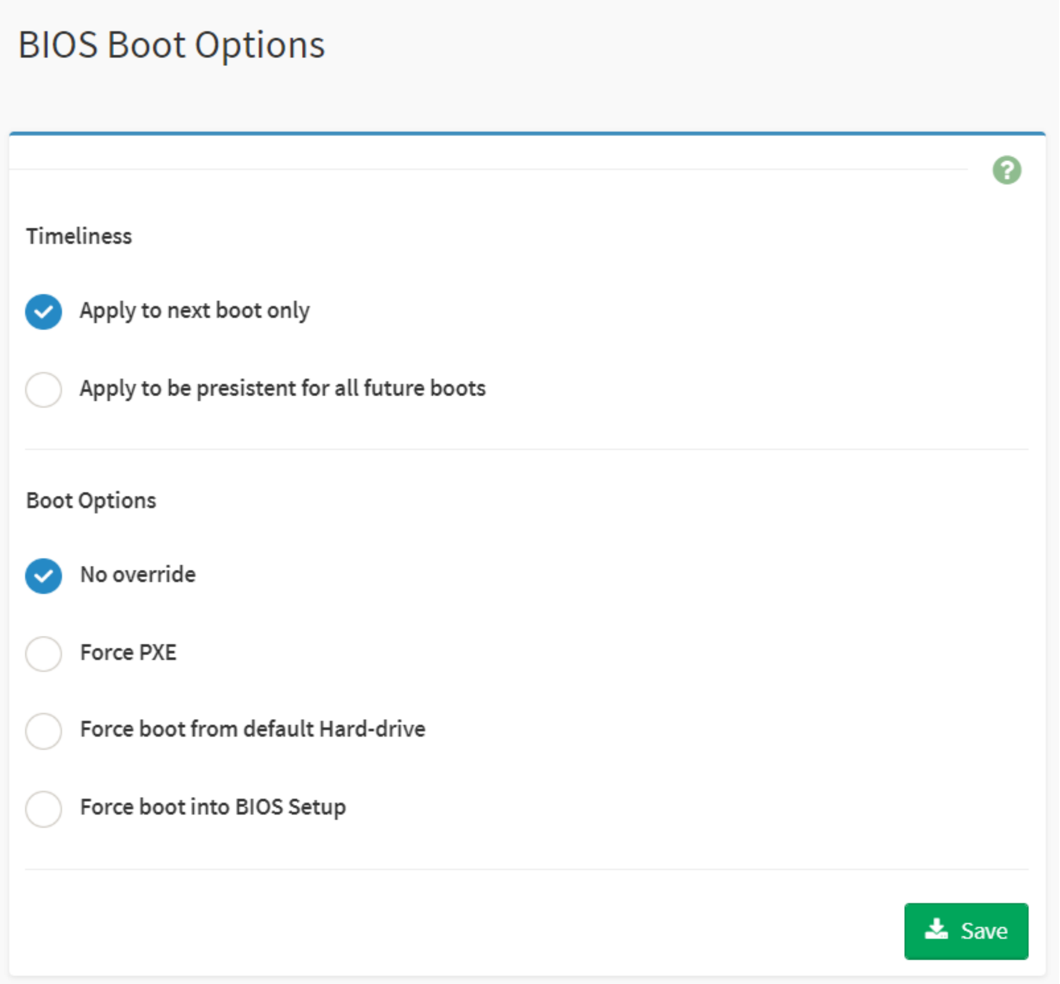
On the **BIOS Boot Options** page, you can:

- Set boot options
- Set timeliness

Screen description:

In the navigation pane, select **System Settings** > **BIOS Boot Options** to open the page as shown below.

Figure 3-49 BIOS Boot Options



BIOS Boot Options

Timeliness

● Apply to next boot only

○ Apply to be presistent for all future boots

Boot Options

● No override

○ Force PXE

○ Force boot from default Hard-drive

○ Force boot into BIOS Setup

Parameters:

Table 3-51 BIOS Boot Options

Parameter	Option
Timeliness	Apply to next boot only Apply to be persistent for all future boots
Boot Options	No override Force PXE Force boot from default Hard-drive Force boot into BIOS Setup

3.11 BMC Settings

3.11.1 Network

3.11.1.1 Network Settings

Description:

On the **Network Setup** page, you can query and configure the BMC management network settings, including:

- NCSI mode
- The interface bound to the network and the binding mode
- Network IP Settings
- VLAN properties

Properties of network settings:

- BMC supports an LAN controller dedicated to BMC and an LAN controller shared by both BMC and OS.
- Maximum bandwidth: 1000 Mbps for dedicated NICs and 100 Mbps for shared NICs.
- The BMC network interfaces support IPv4 and IPv6. You can set an IP address via DHCP or manually.
- The MAC address is stored in EEPROM.
- VLAN is supported.
- BMC supports Adaptive Mode (default) and Standalone Mode for networking.
  - Adaptive Mode: Both the dedicated NIC and shared NIC share the same MAC address. The dedicated NIC is accessible only if its network cable is connected. In this case, the shared NIC is disabled.
  - Standalone Mode: Both the dedicated NIC and shared NIC are independent of each other using different MAC addresses.
- By default, IPMI LAN channels are allocated as follows:

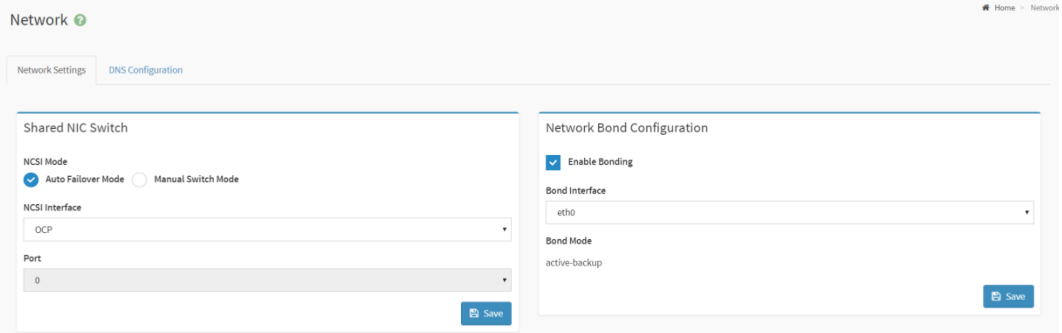
Table 3-52 BMC LAN Interfaces

Channel ID	Interface	Session Support
0x01	Primary LAN (dedicated)	Yes
0x08	Secondary LAN (shared)	Yes

Screen description:

In the navigation pane, select **BMC Settings** > **Network**, and click **Network Settings** to open the pages shown in Figure 3-50 and Figure 3-51.

Figure 3-50 Network Adaptation Configuration



Network

Home > Network

Network Settings | DNS Configuration

Shared NIC Switch

NCSI Mode
● Auto Failover Mode ○ Manual Switch Mode

NCSI Interface
OCP

Port
0

Save

Network Bond Configuration

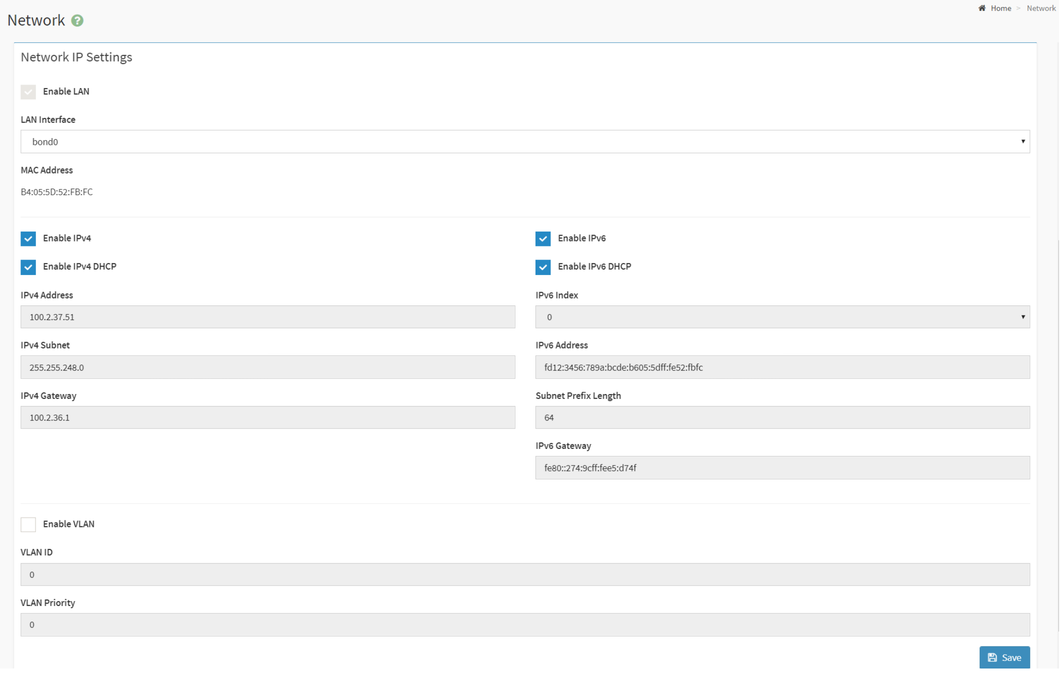
☑ Enable Bonding

Bond Interface
eth0

Bond Mode
active-backup

Save

Figure 3-51 Network IP Settings



Network

Home > Network

Network IP Settings

☑ Enable LAN

LAN Interface
bond0

MAC Address
B4:05:5D:52:FB:FC

☑ Enable IPv4

☑ Enable IPv4 DHCP

IPv4 Address
100.2.37.51

IPv4 Subnet
255.255.248.0

IPv4 Gateway
100.2.36.1

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index
0

IPv6 Address
fd12:3456:789a:bcde:b605:5dff:fe52:fbfc

Subnet Prefix Length
64

IPv6 Gateway
fe80::274:9cff:fee5:d74f

□ Enable VLAN

VLAN ID
0

VLAN Priority
0

Save

Parameters:

Table 3-53 Network Settings

Parameter	**Description**
Shared NIC Switch	
NCSI mode	Options: **Auto Failover Mode** and **Manual Switch Mode** The **Auto Failover Mode** is selected by default. Note: After the NCSI mode is changed, you need to manually restart BMC to make the change effective.

Parameter	Description
NCSI NIC	In the **Manual Switch Mode**, you can select the NCSI NIC.
Port	In the **Manual Switch Mode**, select a port for the selected NIC.
Network Bond Configuration	
Enable Bonding	Check this option to enable binding.
Bond Interface	Available options: **eth0** (dedicated NIC) and **eth1** (shared NIC).
Bond Mode	The network binding mode, which is non-configurable.
Network IP Settings	
Enable LAN	Check this option to enable LAN
LAN Interface	Options: **eth0** (dedicated NIC) and **eth1** (shared NIC)
MAC Address	The MAC address.
Enable IPv4	Check this option to enable IPv4 support for the selected interface.
Enable IPv4 DHCP	Check this option to configure a dynamic IPv4 address via DHCP. If it is not checked, you need to specify the information of the static IPv4 address, including **IPv4 Address**, **IPv4 Subnet**, and **IPv4 Gateway**.
Enable IPv6	Check this option to enable IPv6 support for the selected interface.
Enable IPv6 DHCP	Check this option to configure a dynamic IPv6 address via DHCP. If it is not checked, you need to specify the information of the static IPv6 address, including **IPv6 Index, IPv6 Address**, **Subnet Prefix Length**, and **IPv6 Gateway**.
Enable VLAN	You can enable or disable the VLAN properties of the management network interface by checking or unchecking this option. It is disabled by default. Note: In case of VLAN change, you must restart the system.
VLAN ID	The VLAN of the management network interface. Value range: 0 - 7
VLAN Priority	The VLAN priority.

3.11.1.2 DNS Configuration

Description:

On the **DNS Configuration** page, you can query and configure DNS, including:

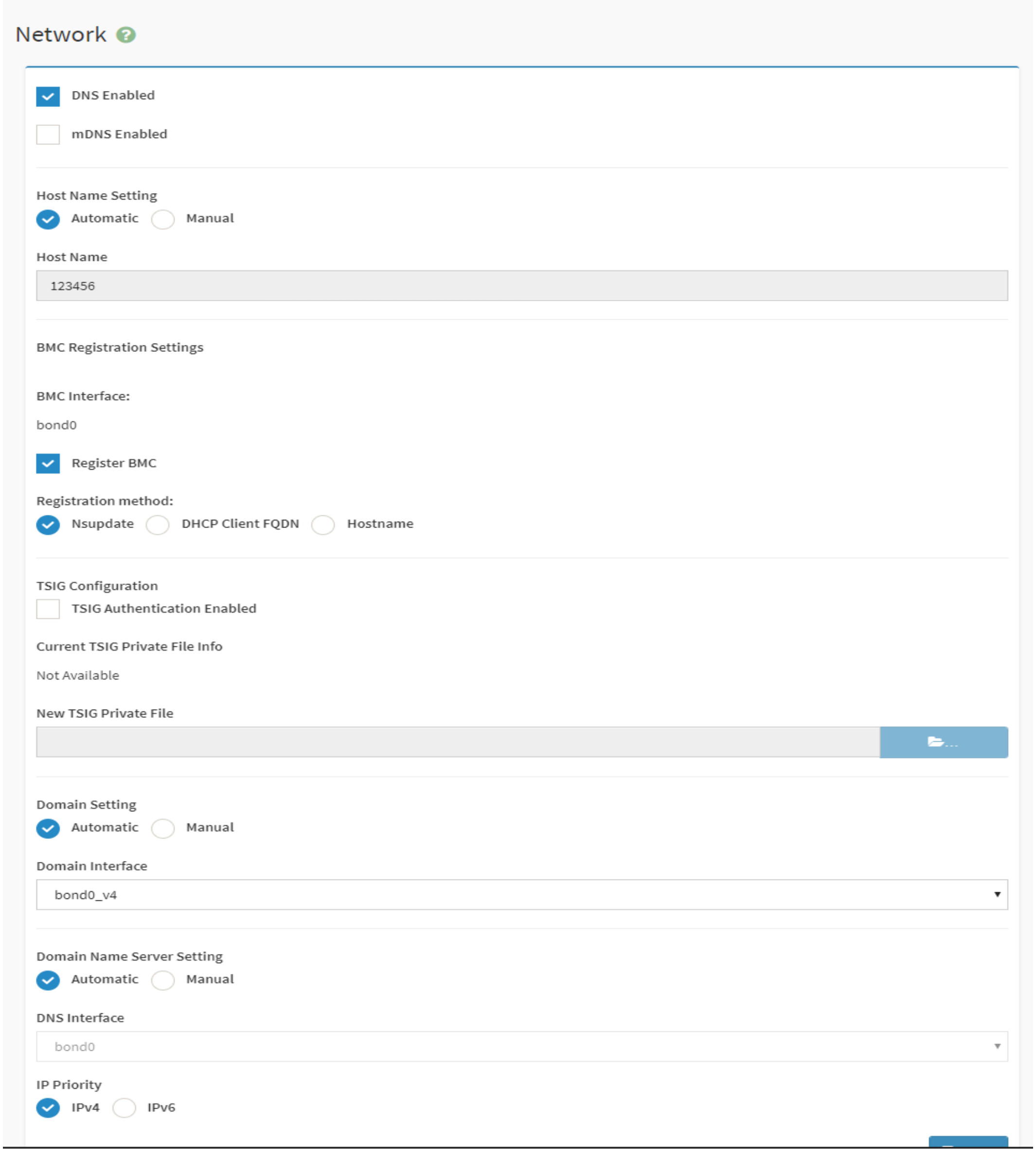
- Host settings

- Domain settings
- Domain server settings

Screen description:

In the navigation pane, select **BMC Settings** > **Network**, and click **DNS Configuration** to open the page as shown below.

Figure 3-52 DNS Configuration



Network

☑ DNS Enabled

□ mDNS Enabled

Host Name Setting

● Automatic ○ Manual

Host Name

123456

BMC Registration Settings

BMC Interface:

bond0

☑ Register BMC

Registration method:

● Nsupdate ○ DHCP Client FQDN ○ Hostname

TSIG Configuration

□ TSIG Authentication Enabled

Current TSIG Private File Info

Not Available

New TSIG Private File

Domain Setting

● Automatic ○ Manual

Domain Interface

bond0_v4

Domain Name Server Setting

● Automatic ○ Manual

DNS Interface

bond0

IP Priority

● IPv4 ○ IPv6

Parameters:

Table 3-54 DNS Configuration

Parameter	Description
DNS Enabled	Enables DNS.

Parameter	Description
mDNS Enabled	Enables mDNS.
Host Name Setting	Configures the server name. Options: **Automatic** and **Manual** If **Automatic** is selected, the default host name will be displayed. If **Manual** is selected, you need to enter the host name manually.
BMC Registration Settings	**Register BMC**: Check this option to register BMC. Options for **Registration method**: **Nsupdate** **DHCP Client FQDN** **Hostname** **Nsupdate** is selected by default.
TSIG Configuration	**TSIG Authentication Enabled**: Check this option to enable authentication for TSIG. It is disabled by default. **Current TSIG Private File Info**: The current TSIG private files are displayed. **New TSIG Private File:** A new TSIG private profile can be uploaded.
Domain Setting	**Automatic** or **Manual**. **Domain Interface**, which can be bond0_v4 or bond0_v6.
Domain Name Server Setting	**Automatic** or **Manual**. **DNS Interface**, which is displayed automatically. If **Manual** is selected, you need to enter the DNS server address.
IP Priority	**IPv4** or **IPv6**.

3.11.2 User Detail Management

Description:

On the **User Detail Management** page, you can:

- Enable Password Check

- Change user group privileges
- Add a User
- Delete a User
- Modify a User

BMC user management features:

- BMC supports a centralized user management mechanism for managing IPMI, Web, SSH, and Redfish users. Users created via IPMI or Web will be granted the IPMI, Web, Redfish, and SSH user privileges. You can access the Smash-Lit CLI via SSH.
- Sysadmin is used to access the BMC debugging serial port rather than IPMI, Web, Redfish, and SSH.
- BMC supports the IPMI 2.0 user model. Users can be created using the IPMI command or the Web GUI.
- Up to 16 users are supported.
- These 16 users can be assigned to any channel, including dedicated LAN and shared LAN
- All created users can log in at the same time.
- The available user privilege levels include Administrator, Operator, User, and No Privilege. Tables 3-55, 3-56, and 3-57 describe IPMI, Web GUI, and Smash-Lite CLI user privileges.

Table 3-55 IPMI User Privileges

User Privilege	**Supported Operation**
Administrator	Read/Write
Operator	Read
User	Read

Table 3-56 Web GUI User Privileges

User Group	**Privilege**
Administrator	User Configuration, General Configuration, Power Control, Remote Media, Remote KVM, Security Configuration, Debug Diagnose, Query Function, and Itself Configuration.
Operator	General Configuration, Power Control, Remote Media, Remote KVM, Query Function, and Itself Configuration.
User	Query Function and Itself Configuration.

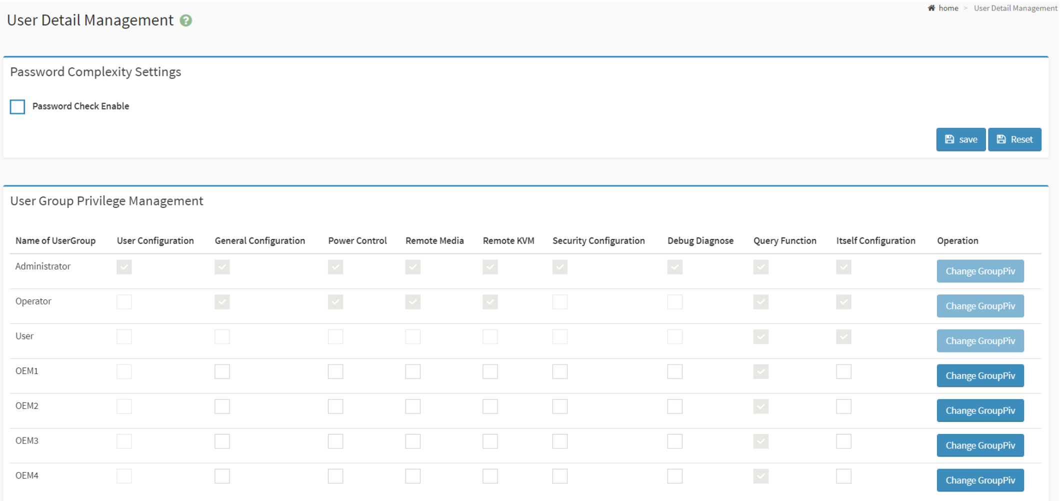
Table 3-57 Smash-Lite CLI User Privileges

Command	Subcommand	User	Operator	Administrator
bmclog	get	Yes	Yes	Yes
	set	No	No	Yes
chassis	get	Yes	Yes	Yes
	set	No	No	Yes
mc	get	Yes	Yes	Yes
	set	No	No	Yes
diagnose	ls cat last ifconfig ethtool ps top dmesg netstat gpiotool i2c-test pwmtachtool ipmitool df uptime	No	No	Yes

Screen description:

In the navigation pane, select **BMC Settings** > **User Detail Management** to open the pages shown in Figure 3-53 and Figure 3-54.

Figure 3-53 Password Complexity Settings and User Group Privilege Management



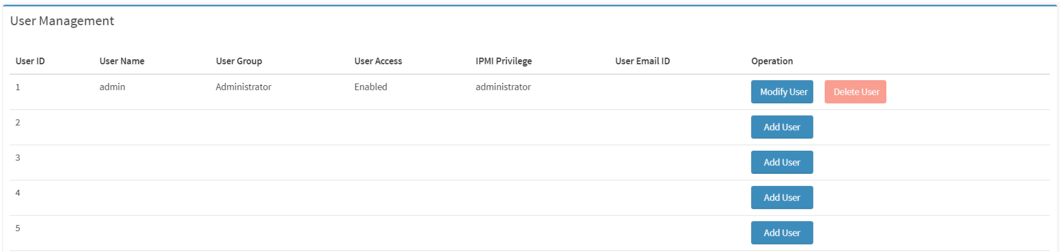
Password Complexity Settings

□ Password Check Enable

User Group Privilege Management

Name of UserGroup	User Configuration	General Configuration	Power Control	Remote Media	Remote KVM	Security Configuration	Debug Diagnose	Query Function	Itself Configuration	Operation
Administrator	☑	☑	☑	☑	☑	☑	☑	☑	☑	Change GroupPiv
Operator	□	☑	☑	☑	☑	□	□	☑	☑	Change GroupPiv
User	□	□	□	□	□	□	□	☑	☑	Change GroupPiv
OEM1	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM2	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM3	□	□	□	□	□	□	□	☑	□	Change GroupPiv
OEM4	□	□	□	□	□	□	□	☑	□	Change GroupPiv

Figure 3-54 User Management



User Management

User ID	User Name	User Group	User Access	IPMI Privilege	User Email ID	Operation
1	admin	Administrator	Enabled	administrator		Modify User Delete User
2						Add User
3						Add User
4						Add User
5						Add User

Parameters:

Table 3-58 Password Complexity Settings

Parameter	Description
Password Check Enable	Check this option to enable password complexity. Password complexity is disabled if it is not checked.
Password Min Length	It defaults to 8. An integer between 8 and 16 can be selected.
Password Complexity Enable	Check this option to select the following characters for a password: uppercase letters, lowercase letters, numbers, and special characters. For example, select **Uppercase Letters** if uppercase letters are required in a password. Password complexity is disabled if this option is not checked.
Password Validity Period (days)	You can set the validity period (days) of the password. After the validity period expires, users can no longer log in.
Password History Record	You can store a maximum of 5 most recently used passwords, which are prohibited from reuse. Value range: 0 - 5
Retry Controls for Login Failure	You can set the maximum number of retries that a user is allowed to retry their password after login failure. The user will be locked out after a specified number of failed login attempts. Value range: 0 - 5
Locking Period (min)	It defaults to 5. Value range: 5 - 60

Table 3-59 User Group Privilege Management

User Group	Privilege
Administrator	User Configuration, General Configuration, Power Control, Remote Media, Remote KVM, Security Configuration, Debug Diagnose, Query Function, and Itself Configuration.
Operator	General Configuration, Power Control, Remote Media, Remote KVM, Query Function, and Itself Configuration.
User	Query Function and Itself Configuration
OEM	OEM1, OEM2, OEM3, and OEM4 are reserved user groups that have query privilege and can configure custom privileges by default. You can also select other privileges to configure.

Table 3-60 User Group Privileges Description

Privilege	Description
User Configuration	User Group Management, User Management, Service Session, General LDAP Settings, and Role Groups.
General Configuration	DNS Configuration, Password Complexity Settings, IDL Clearing, System Event Log Clearing, Services Configuration, General Firewall Settings, IP Address Firewall Rules, Port Firewall Rules, Date & Time, PAM Sequence, Save Configuration, SEL Setting Policy, Syslog Settings, SNMP Trap Settings, SNMP Set/Get Settings, Mailbox Alarm, Sensor Threshold, HPM Firmware Update, Firmware Image Location, Restore Factory Defaults, Restore Configuration, Power Key Settings of Front Control Panel, Fan Management, Network Adaptive Configuration, Shared NIC Switch, Network Bond Configuration, Network IP Settings, and BIOS Boot Options.
Power Supply Control	Controls the power supply.
Remote Media	KVM Mouse Settings, Local Image, Remote Image, General Settings, VMedia Instance Device Settings, Remote Session, VNC, and Active Redirections.
Remote KVM	H5Viewer and JViewer.
Security Configuration	Generate SSL Certificate, Upload SSL Certificate, System Administrator, and Audit Log.

Privilege	Description
Debug Diagnose	Downtime Screenshot, Manual Screenshot, Video Trigger Settings, Video Remote Storage, Pre-Event Video Recording, Module Restart, and One-Key Collection Log.
Query Function	You can log in and view information other than the security configuration.
Itself Configuration	You can configure your own password and email address, and manage the SSH public key.

Table 3-61 User Management

Parameter	Description
User ID	The user ID.
User Name	The user name.
User Access	Indicates whether the user is enabled. Options include: • Enabled • Disabled
IPMI Privilege	The user's IPMI privilege.
User Email ID	The user's email address.
Operation	You can perform the following operations: • Add User • Modify User • Delete User

3.11.3 Services

Description:

On the **Services** page, you can view and modify the basic information of the running BMC services, including the Status, Non Secure Port, Secure Port, Timeout, and Maximum Sessions.

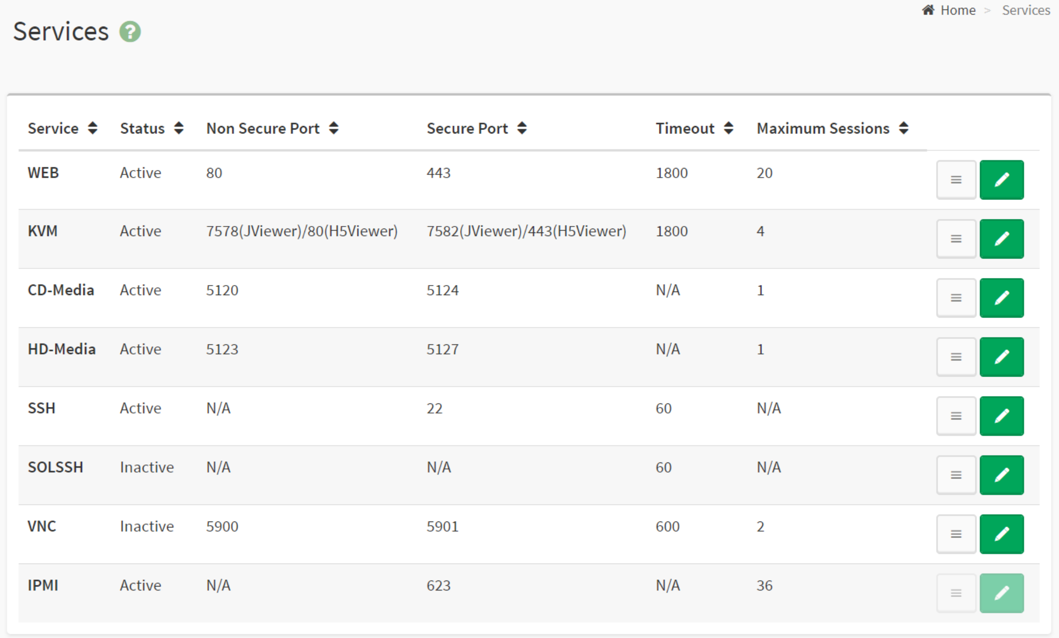
NOTE

1. Only the administrator has the privilege to modify service information.
2. To ensure the security of the system, we recommend that you disable unnecessary services and close their ports.
3. In addition to modifiable services, BMC also uses some ports with fixed protocols. For details, see Table 3-63 Fixed Protocols. Fixed protocols cannot be configured.

Screen description:

In the navigation pane, select **BMC Settings** > **Services** to open the page as shown below.

Figure 3-55 Protocols and Ports



Service	Status	Non Secure Port	Secure Port	Timeout	Maximum Sessions
WEB	Active	80	443	1800	20
KVM	Active	7578(JViewer)/80(H5Viewer)	7582(JViewer)/443(H5Viewer)	1800	4
CD-Media	Active	5120	5124	N/A	1
HD-Media	Active	5123	5127	N/A	1
SSH	Active	N/A	22	60	N/A
SOLSSH	Inactive	N/A	N/A	60	N/A
VNC	Inactive	5900	5901	600	2
IPMI	Active	N/A	623	N/A	36

Parameters:

Table 3-62 Services

Parameter	Description
Service	The service name.
Status	Active or Inactive.
Non Secure Port	The non-secure port.
Secure Port	The secure port.
Timeout	The timeout period (in seconds).
Maximum Sessions	The maximum number of sessions supported by each service, which cannot be changed.

Table 3-63 Fixed Protocols

Service	Purpose	Status	Port No.	TCP/UDP
SMUX	SNMP Multiplexer	Active	199	TCP
DHCP V6 Client	DHCP V6 Client	Active	546	UDP
Websockify	KVM on HTML5	Active	443	TCP
Websockify	Virtual Media on HTML5	Active	443	TCP
IPMI	IPMI	Active	623	UDP

3.11.4 System Firewall

Description:

On the **System Firewall** page, you can view and modify firewall rules, including:

- IP Address Firewall Rules
- Port Firewall Rules
- MAC Firewall Rules

Screen description:

In the navigation pane, select **BMC Settings** > **System Firewall** to open the pages shown in Figure 3-56, Figure 3-57, Figure 3-58, and Figure 3-59.

Figure 3-56 System Firewall

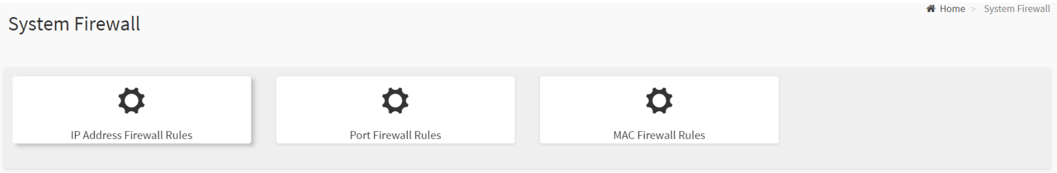
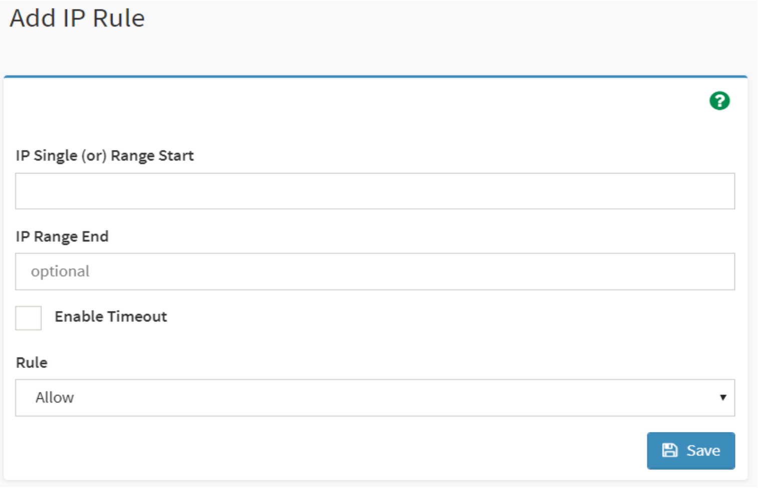


Figure 3-57 Add IP Rule


Add IP Rule

IP Single (or) Range Start

IP Range End

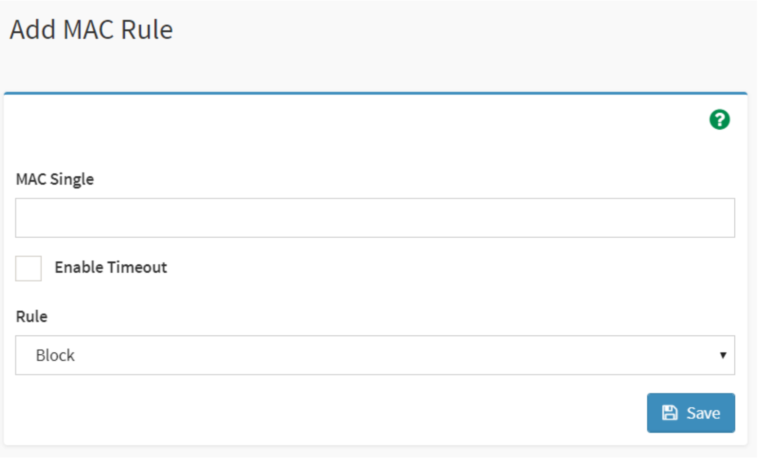
optional

□ Enable Timeout

Rule

Allow

Figure 3-58 Add MAC Rule


Add MAC Rule

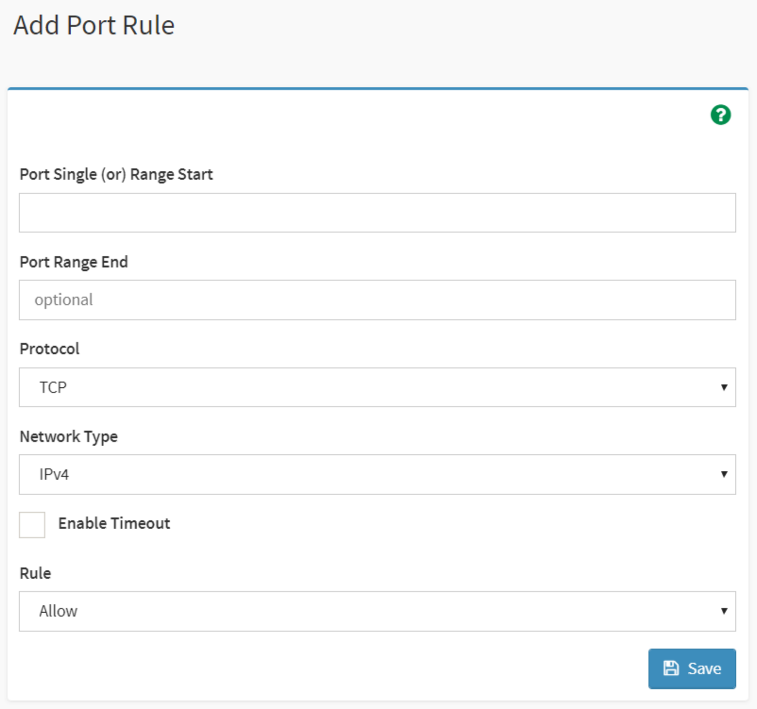
MAC Single

□ Enable Timeout

Rule

Block

Figure 3-59 Add Port Rule



Add Port Rule

Port Single (or) Range Start

Port Range End

optional

Protocol

TCP

Network Type

IPv4

□ Enable Timeout

Rule

Allow

Parameters:

Table 3-64 System Firewall

Parameter	Description
Existing IP Rules	Shows the existing IP rules.
Add IP Rule	Adds an IP rule. Specify the following parameters: • IP Single (or) Range Start • IP Range End • Enable Timeout If this option is not checked, the rule will take effect immediately and will not expire. If this option is checked, you need to specify the validity period of the rule. • Rule: Allow or Block
Port Firewall Rules	The existing port rules.
Add Port Rule	Adds a port rule. Specify the following parameters:

Parameter	Description
	• Port Single (or) Range Start • Port Range End • Protocol: TCP, UDP or Both • Network Type: IPv4, IPv6, or Both • Enable Timeout If this option is not checked, the rule will take effect immediately and will not expire. If this option is checked, you need to specify the validity period of the rule. • Rule: Allow or Block
MAC Firewall Rules	The existing MAC rules.
Add MAC Rule	Adds a MAC rule. Specify the following parameters: • MAC Single • Enable Timeout If this option is not checked, the rule will take effect immediately and will not expire. If this option is checked, you need to specify the validity period of the rule. • Rule: Allow or Block

3.11.5 Date & Time

Description:

On the **Date & Time** page, you can query and configure:

- BMC system timezone
- NTP information

Here are the BMC time synchronization rules:

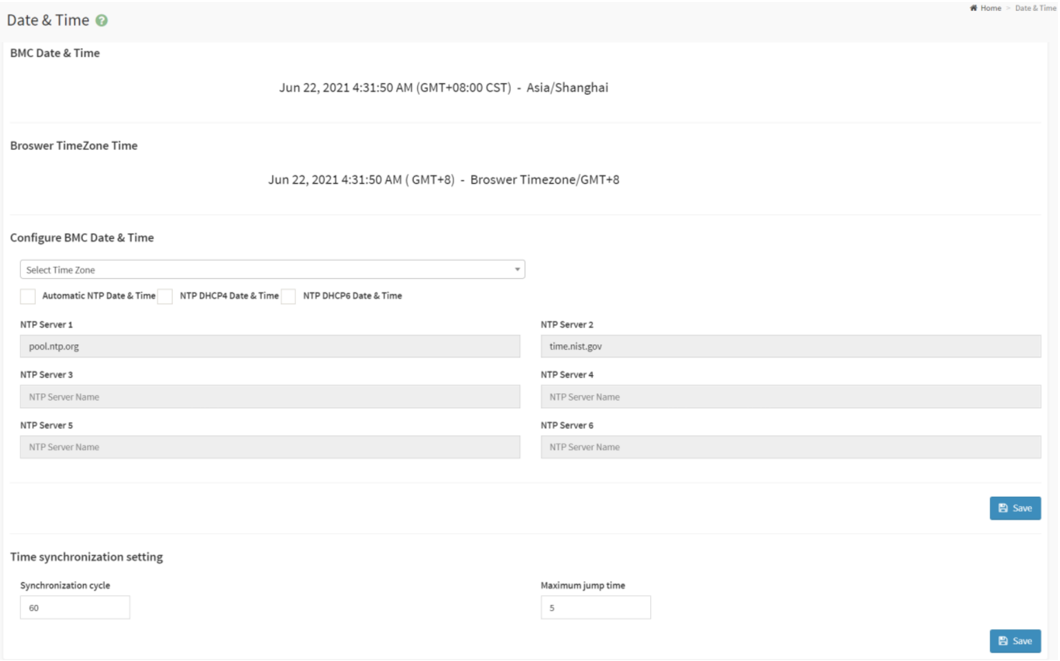
- After BMC starts, it will send a request to ME to obtain the system RTC time.

- During BIOS boot, it sends a time setting request to BMC, which then synchronizes with the BIOS time.
- The BMC time is equal to the BIOS time plus the time in BMC timezone, and the time difference between the BIOS and the OS depends on their respective settings.
- If NTP is enabled and the NTP server is operating normally, then BMC will synchronize the time with the NTP server every hour.

Screen description:

In the navigation pane, select **BMC Settings** > **Date & Time** to open the page as shown below.

Figure 3-60 Date & Time



Date & Time

BMC Date & Time

Jun 22, 2021 4:31:50 AM (GMT+08:00 CST) - Asia/Shanghai

Broswer TimeZone Time

Jun 22, 2021 4:31:50 AM (GMT+8) - Broswer Timezone/GMT+8

Configure BMC Date & Time

Select Time Zone

□ Automatic NTP Date & Time □ NTP DHCP4 Date & Time □ NTP DHCP6 Date & Time

NTP Server 1: pool.ntp.org

NTP Server 2: time.nist.gov

NTP Server 3: NTP Server Name

NTP Server 4: NTP Server Name

NTP Server 5: NTP Server Name

NTP Server 6: NTP Server Name

Time synchronization setting

Synchronization cycle: 60

Maximum jump time: 5

Parameters:

Table 3-65 Date & Time

Parameter	Description
BMC Date & Time	The BMC date and time.
Browser TimeZone Time	The time in the browser timezone.
Configure BMC Date & Time	Select Timezone. Select one of the following modes of refreshing date and time by NTP: • Auto NTP Date & Time • NTP DHCP4 Date & Time

Parameter	Description
	- NTP DHCP6 Date & Time Enter the NTP server address.
Time synchronization setting	Synchronization Cycle Maximum jump time

3.11.6 SSL Settings

Description:

The SSL certificate establishes a secure SSL channel (where the access method is HTTPS) between the client browser and the web server to transmit encrypted data between them, to prevent data leakage. SSL secures the information transmitted between both ends. Users can verify if the website they are visiting is genuine and trustworthy using the server certificate. The SSL certificate can be replaced. To improve security, we recommend you replace the current certificate with your own certificate and public and private keys, and update the certificate in a timely manner to ensure its validity.

On the **SSL Settings** page, you can:

- View SSL certificate
- Generate SSL certificate
- Upload SSL certificate

Screen description:

In the navigation pane, select **BMC Settings** > **SSL Settings** to open the pages shown in Figure 3-61, Figure 3-62, Figure 3-63, and Figure 3-64.

Figure 3-61 SSL Settings

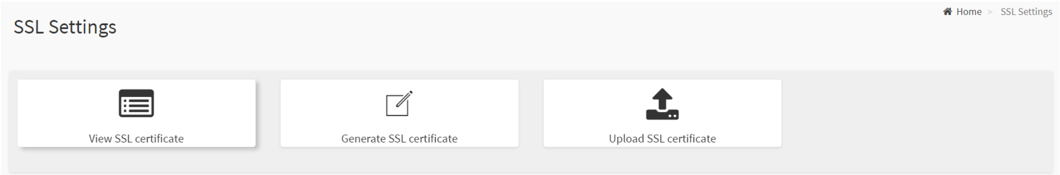
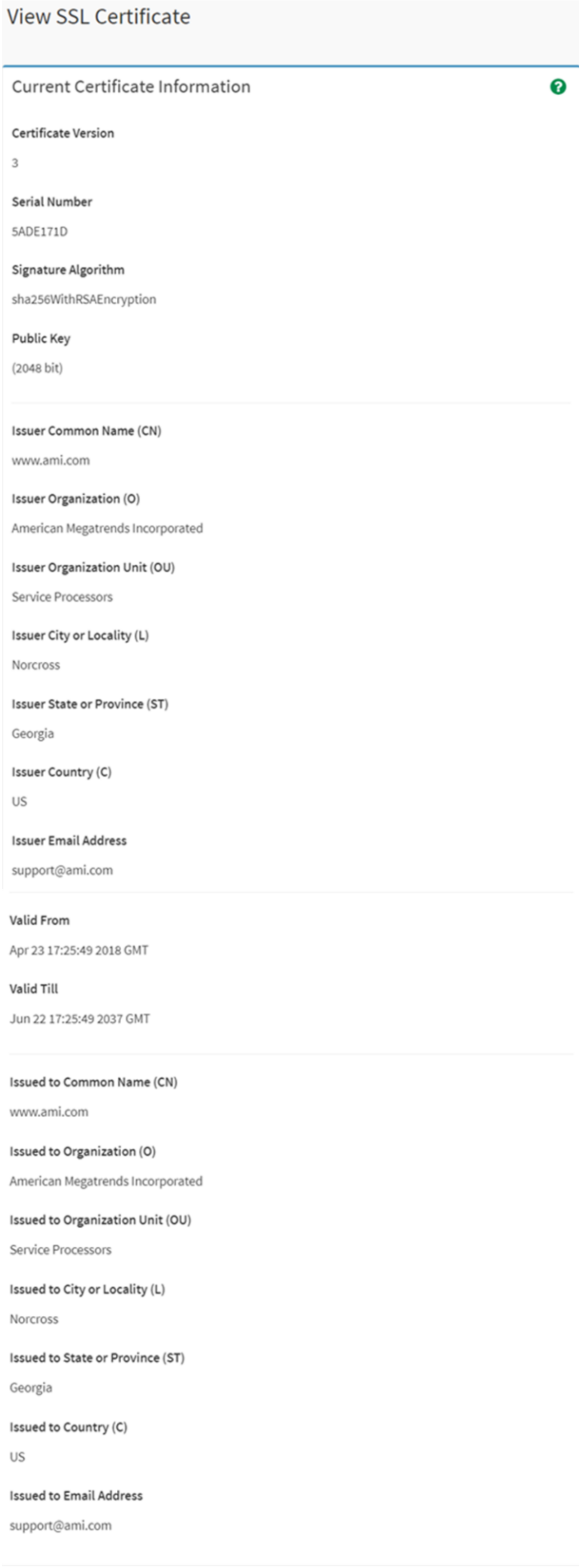


Figure 3-62 View SSL Certificate



View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

5ADE171D

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

www.ami.com

Issuer Organization (O)

American Megatrends Incorporated

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Norcross

Issuer State or Province (ST)

Georgia

Issuer Country (C)

US

Issuer Email Address

support@ami.com

Valid From

Apr 23 17:25:49 2018 GMT

Valid Till

Jun 22 17:25:49 2037 GMT

Issued to Common Name (CN)

www.ami.com

Issued to Organization (O)

American Megatrends Incorporated

Issued to Organization Unit (OU)

Service Processors

Issued to City or Locality (L)

Norcross

Issued to State or Province (ST)

Georgia

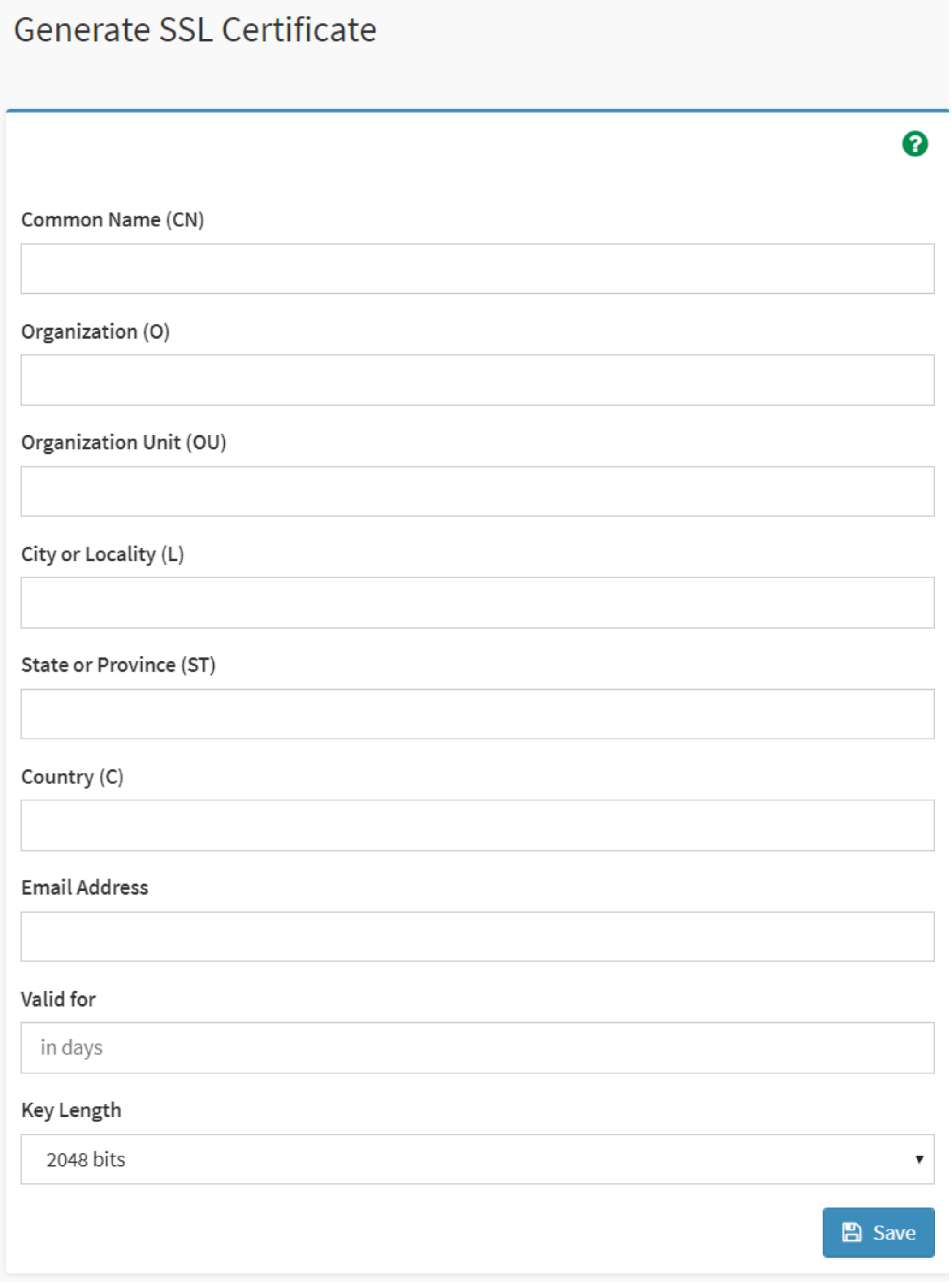
Issued to Country (C)

US

Issued to Email Address

support@ami.com

Figure 3-63 Generate SSL Certificate



Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

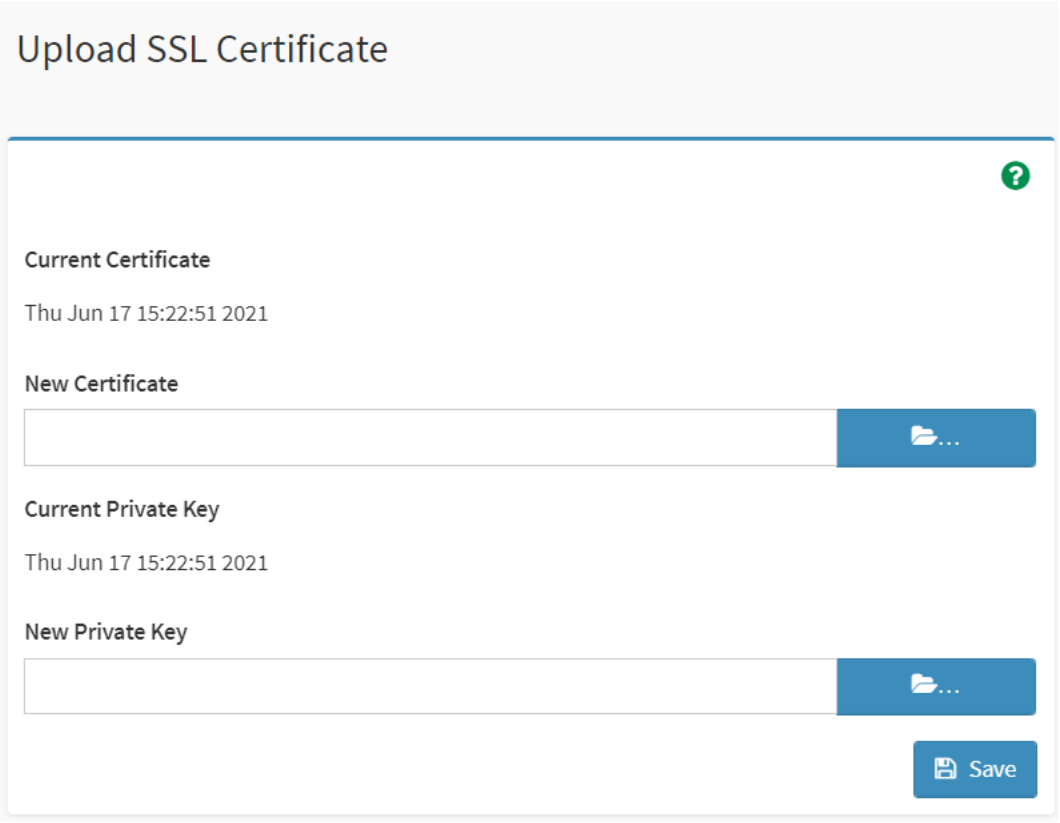
Valid for

in days

Key Length

2048 bits ▾

Figure 3-64 Upload SSL Certificate



Upload SSL Certificate

Current Certificate

Thu Jun 17 15:22:51 2021

New Certificate

Current Private Key

Thu Jun 17 15:22:51 2021

New Private Key

Parameters:

Table 3-66 SSL Settings

Parameter	Description
Common Name (CN)	The common name
Organization (O)	The organization
Organization Unit (OU)	The organization unit
City or Locality (L)	The city or location
State or Province (ST)	The state or province
Country (C)	The country
Email Address	The email address
Valid for	Total days of validity, ranging from 1 to 3,650 days
Key Length	The key length

3.11.7 Backup Configuration

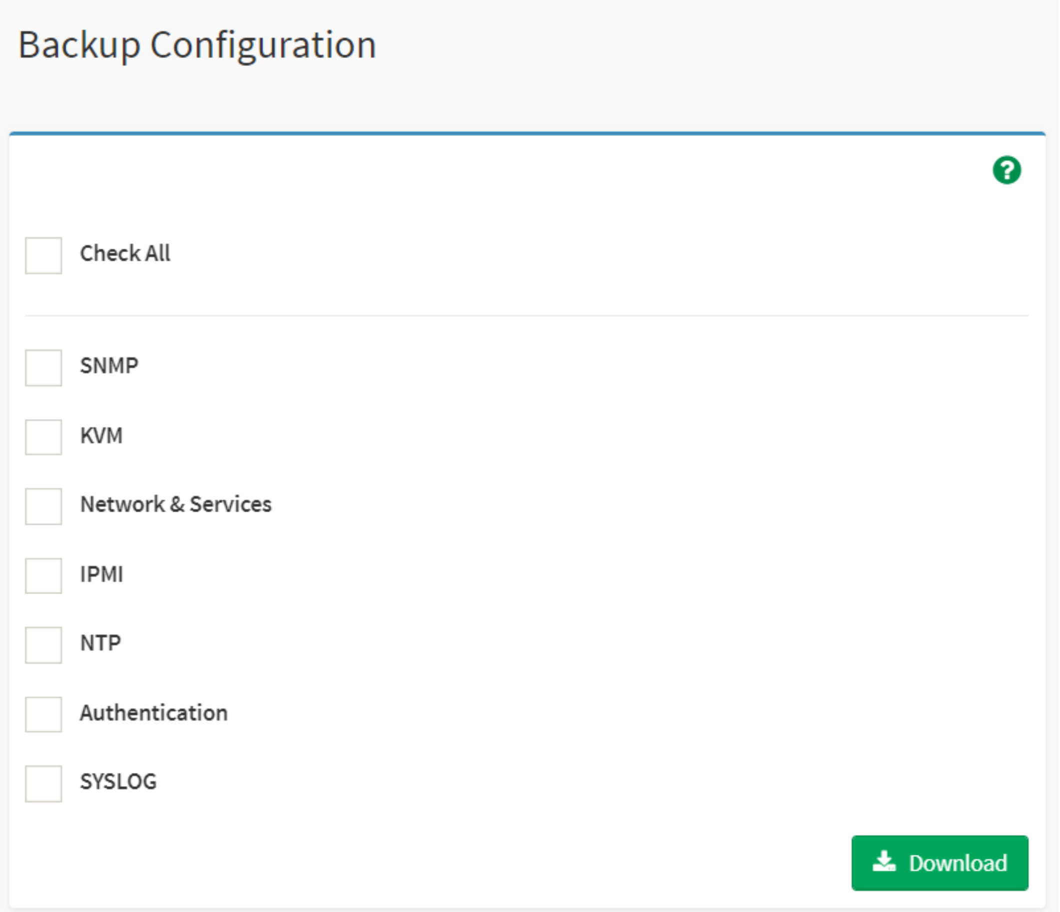
Description:

On the **Backup Configuration** page, you can back up the existing system configurations and download the configuration file to the local computer.

Screen description:

In the navigation pane, select **BMC Settings** > **Backup Configuration** to open the page as shown below.

Figure 3-65 Backup Configuration



Backup Configuration

□ Check All

□ SNMP

□ KVM

□ Network & Services

□ IPMI

□ NTP

□ Authentication

□ SYSLOG

Parameters:

Table 3-67 Backup Configuration

Parameter	Description
SNMP	Backs up SNMP configuration.
KVM	Backs up KVM configuration.
Network & Services	Backs up network and service configuration.
IPMI	Backs up IPMI configuration.

Parameter	Description
NTP	Backs up NTP configuration.
Authentication	Backs up authentication configuration.
SYSLOG	Backs up syslog configuration.

3.11.8 Restore Configuration

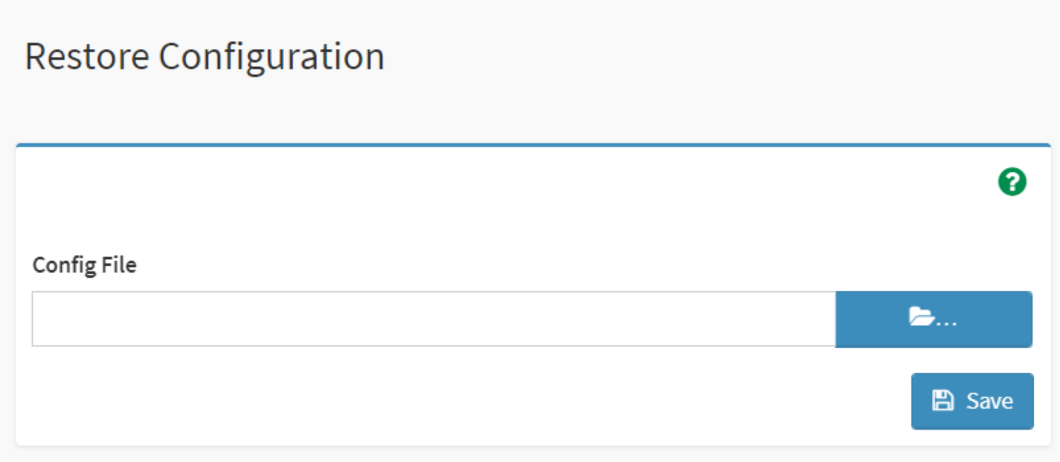
Description:

On the **Restore Configuration** page, you can restore the existing system configurations.

Screen description:

In the navigation pane, select **BMC Settings** > **Restore Configuration** to open the page as shown below.

Figure 3-66 Restore Configuration



Parameters:

Table 3-68 Restore Configuration

Parameter	Description
Config File	Select a local configuration file to restore the existing system configurations.

3.12 Fault Diagnosis

The diagnostic tool checks and verifies the BMC or host system for any dysfunctions or anomalies.

3.12.1 Host POST Code

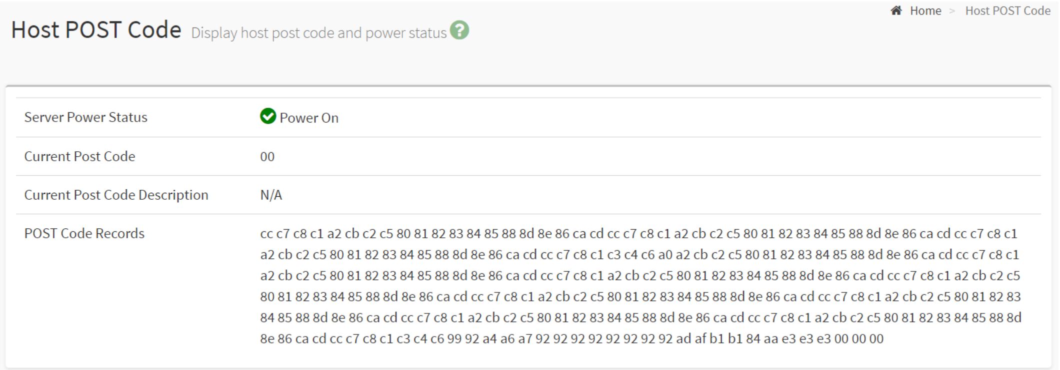
Description:

On the **Host POST Code** page, you can view the server power status, the current POST codes and its description, and historical POST codes.

Screen description:

In the navigation pane, select **Fault Diagnosis** > **Host POST Code** to open the page as shown below.

Figure 3-67 Host POST Code



Home > Host POST Code

Host POST Code Display host post code and power status

Server Power Status	✓ Power On
Current Post Code	00
Current Post Code Description	N/A
POST Code Records	cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 c3 c4 c6 a0 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 a2 cb c2 c5 80 81 82 83 84 85 88 8d 8e 86 ca cd cc c7 c8 c1 c3 c4 c6 99 92 a4 a6 a7 92 92 92 92 92 92 92 92 ad af b1 b1 84 aa e3 e3 e3 00 00 00

Parameters:

Table 3-69 Host POST Code

Parameter	Description
Server Power Status	The power status of the server. Values include: ● On ● Off
Current POST Code	The existing POST code.
Current POST Code Description	Description of the existing POST code.
POST Code Records	The historical POST codes.

3.12.2 Captured Screenshot

Description:

On the **Captured Screenshot** page, you can:

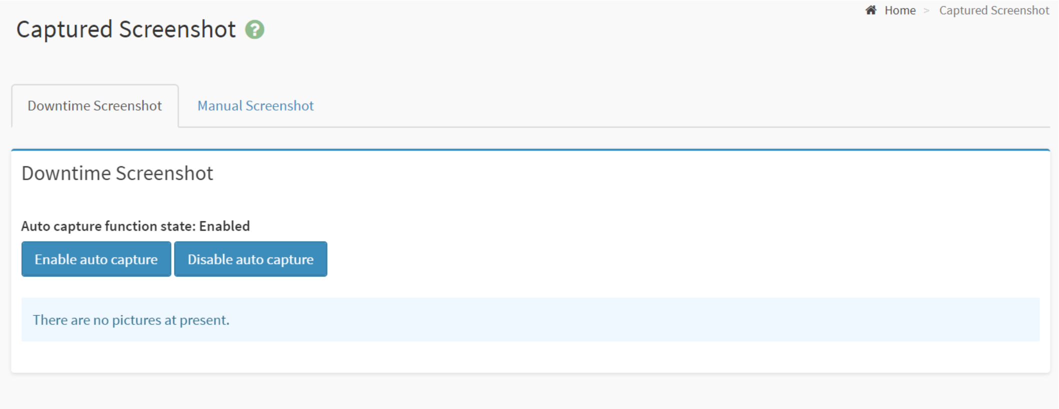
- Enable auto capture, allowing the system to automatically capture the last screen before system downtime due to IERR.

- Manually capture the current system image at any time when OS wakes up and KVM is turned off.
- Delete captured screenshots.

Screen description:

In the navigation pane, select **Fault Diagnosis** > **Captured Screenshot** to open the pages shown in Figure 3-68 and Figure 3-69.

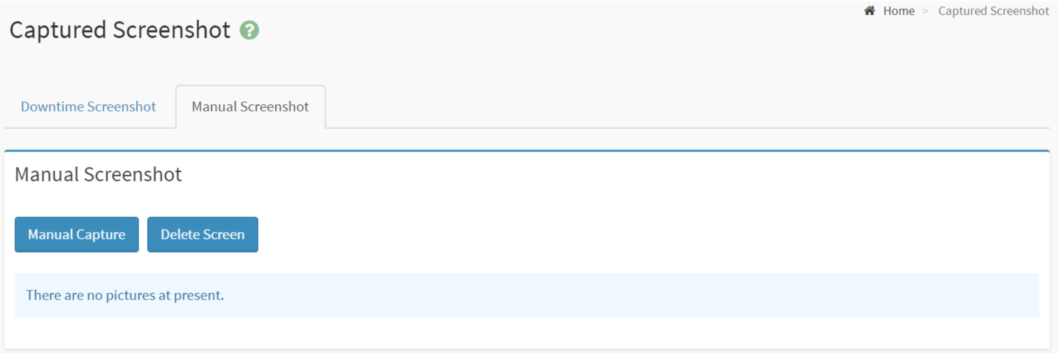
Figure 3-68 Downtime Screenshot



Auto capture function state: Enabled

There are no pictures at present.

Figure 3-69 Manual Screenshot



There are no pictures at present.

Parameters:

Table 3-70 Captured Screenshot

Parameter	**Description**
Auto capture function state	Displays the state of the auto capture function. Options include: • On • Off

Parameter	Description
Enable auto capture	Enables the auto capture function. Captures the last screen before system downtime due to IERR.
Disable auto capture	Disables the auto capture function.
Manual Capture	Manually captures and displays the current system screen at any time.
Delete Screen	Deletes the existing manually captured screenshots.

3.12.3 Screen Video

Description:

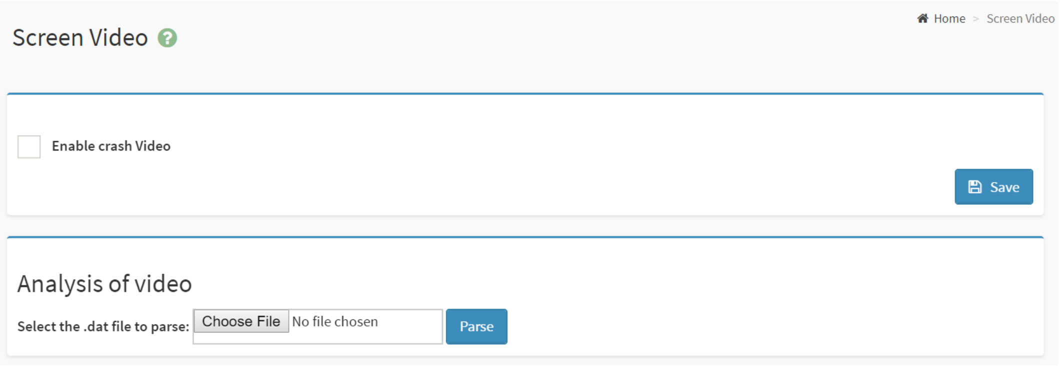
On the **Screen Video** page, you can:

- Start video recording at system downtime.
- Analyse videos.
- Display video files recorded at downtime.

Screen description:

In the navigation pane, select **Fault Diagnosis** > **Screen Video** to open the page as shown below.

Figure 3-70 Screen Recording



Screen Video

Home > Screen Video

□ Enable crash Video

Analysis of video

Select the .dat file to parse: No file chosen

Parameters:

Table 3-71 Screen Recording

Parameter	Description
Enable crash video	Starts screen recording at system downtime, allowing the system to record the last video before system downtime

Parameter	Description
	due to IERR. Note: The system can record the video at the system downtime only after KVM is off.
Analysis of video	You can analyse the .dat file downloaded locally from BMC as an .avi file here. You can download the video (.dat format) by One-key Collection Log if the system is enabled to record a video and system downtime occurred.
Downtime video	Displays video files recorded when the system is enabled to record a video at downtime.

3.12.4 Module Restart

Description:

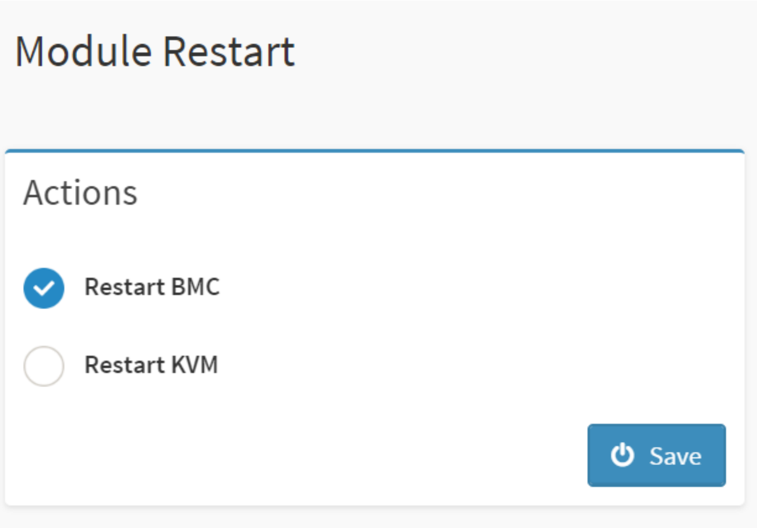
On the **Module Restart** page, you can:

- Restart the BMC.
- Restart the KVM.

Screen description:

In the navigation pane, select **Fault Diagnosis** > **Module Restart** to open the page as shown below.

Figure 3-71 Module Restart



Module Restart

Actions

☑ Restart BMC

○ Restart KVM

Parameters:

Table 3-72 Module Restart

Parameter	Description
Restart BMC	Restart the BMC.
Restart KVM	Restart the KVM.

3.13 System Maintenance

3.13.1 HPM Firmware Update

Description:

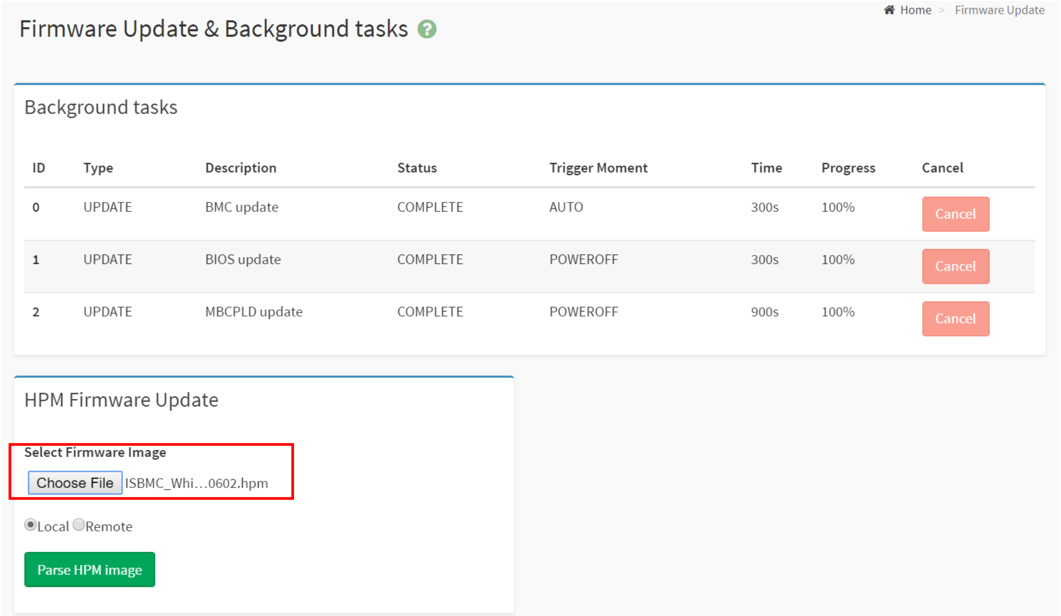
On the **HPM Firmware Update** page, you can update HPM firmware including BIOS, BMC, CPLD, PSU, and FPGA. The BMC contains two 64 MB flash, each of which stores a 64 MB firmware image. It supports dual-image update. An update can be performed via Web and YafuFlash. When performing an update, you can choose whether to preserve the configuration. HPM firmware update is safer and can prevent your data from being updated accidentally.

The following shows how to update the BMC, BIOS, and CPLD.

3.13.1.1 Updating BMC

1. In the navigation pane, select **System Maintenance** > **HPM Firmware Update**. On the page, select a BMC image.

Figure 3-72 Selecting Firmware Images



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
0	UPDATE	BMC update	COMPLETE	AUTO	300s	100%	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	COMPLETE	POWEROFF	900s	100%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File ISBMC_Whi...0602.hpm

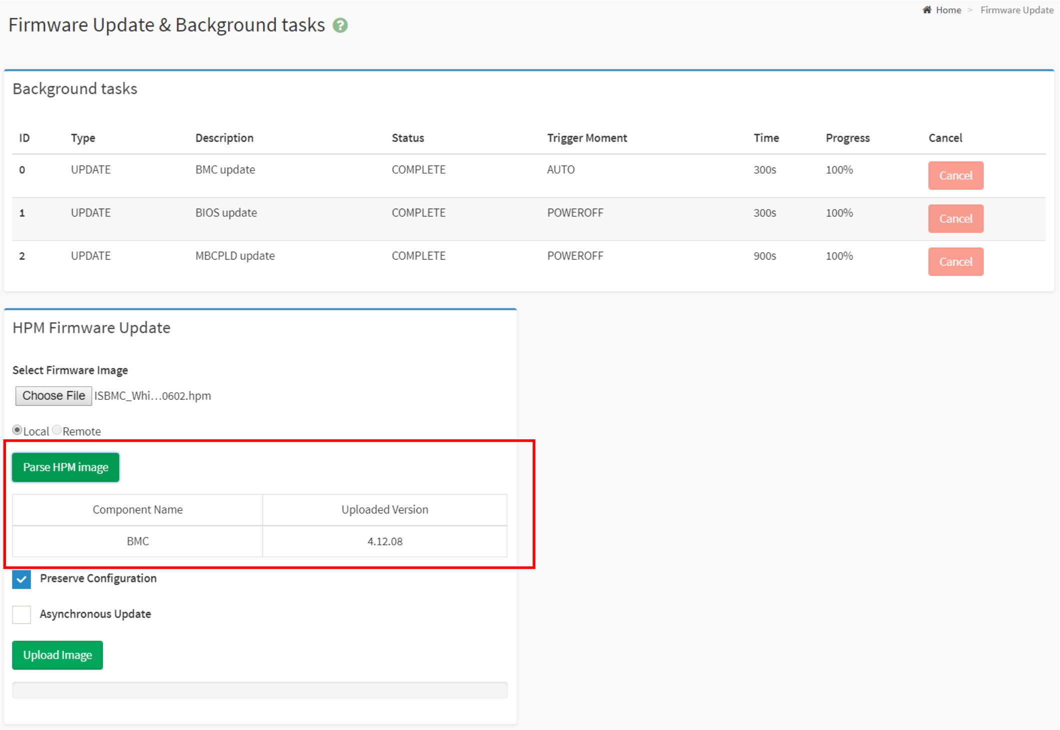
● Local ○ Remote

Table 3-73 Selecting Firmware Image Parameters

Parameter	Description
Local	Select a local image.
Remote	Select a remote image. Protocol: NFS/SFTP/SCP. NFS has no username and password. Use NA by default.

2. Parse the HPM image.

Figure 3-73 Parsing HPM Image



Home > Firmware Update

Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
0	UPDATE	BMC update	COMPLETE	AUTO	300s	100%	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	COMPLETE	POWEROFF	900s	100%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File ISBMC_Whi…0602.hpm

● Local ○ Remote

Parse HPM image

Component Name	Uploaded Version
BMC	4.12.08

☑ Preserve Configuration

□ Asynchronous Update

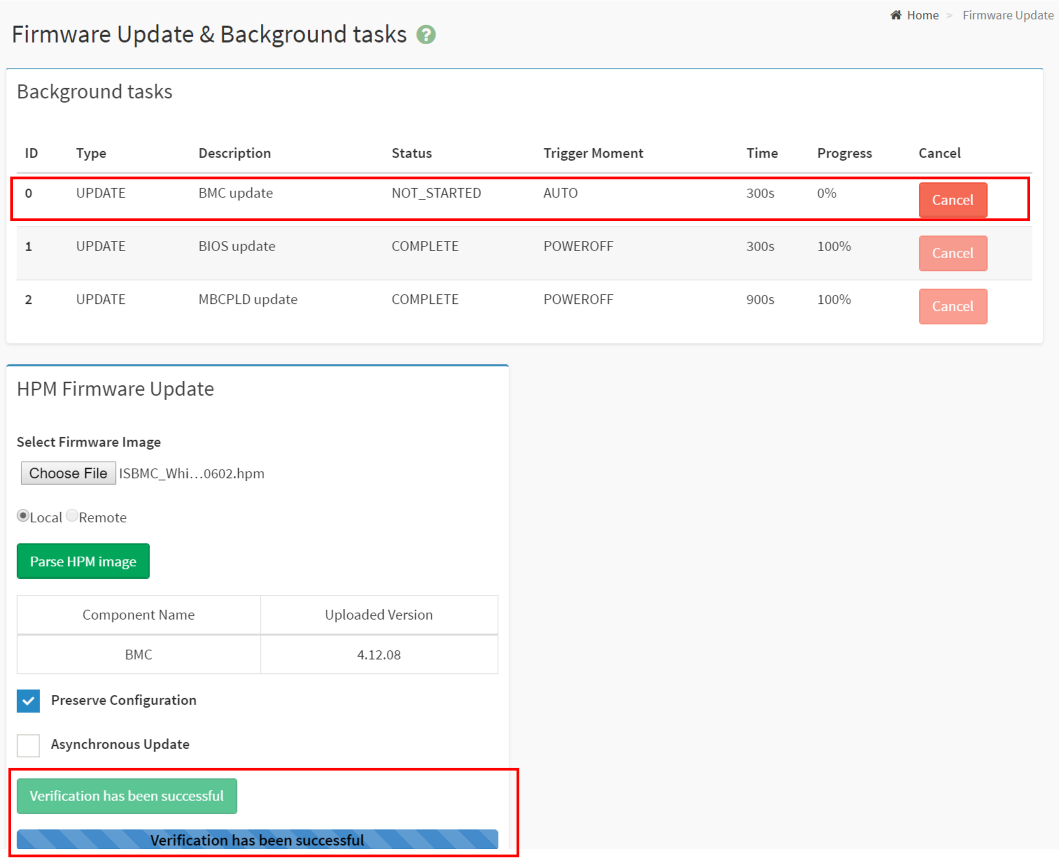
Upload Image

3. The component name and uploaded version are displayed after image parsing. Confirm the information, select whether to preserve the configuration and enable asynchronous update, click **Upload Image**, wait for successful verification.

NOTE

Asynchronous Update is available only when **Preserve Configuration** is selected.

Figure 3-74 Image Verification



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
0	UPDATE	BMC update	NOT_STARTED	AUTO	300s	0%	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	COMPLETE	POWEROFF	900s	100%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File ISBMC_Whi…0602.hpm

● Local ○ Remote

Parse HPM image

Component Name	Uploaded Version
BMC	4.12.08

☑ Preserve Configuration

□ Asynchronous Update

Verification has been successful

Verification has been successful

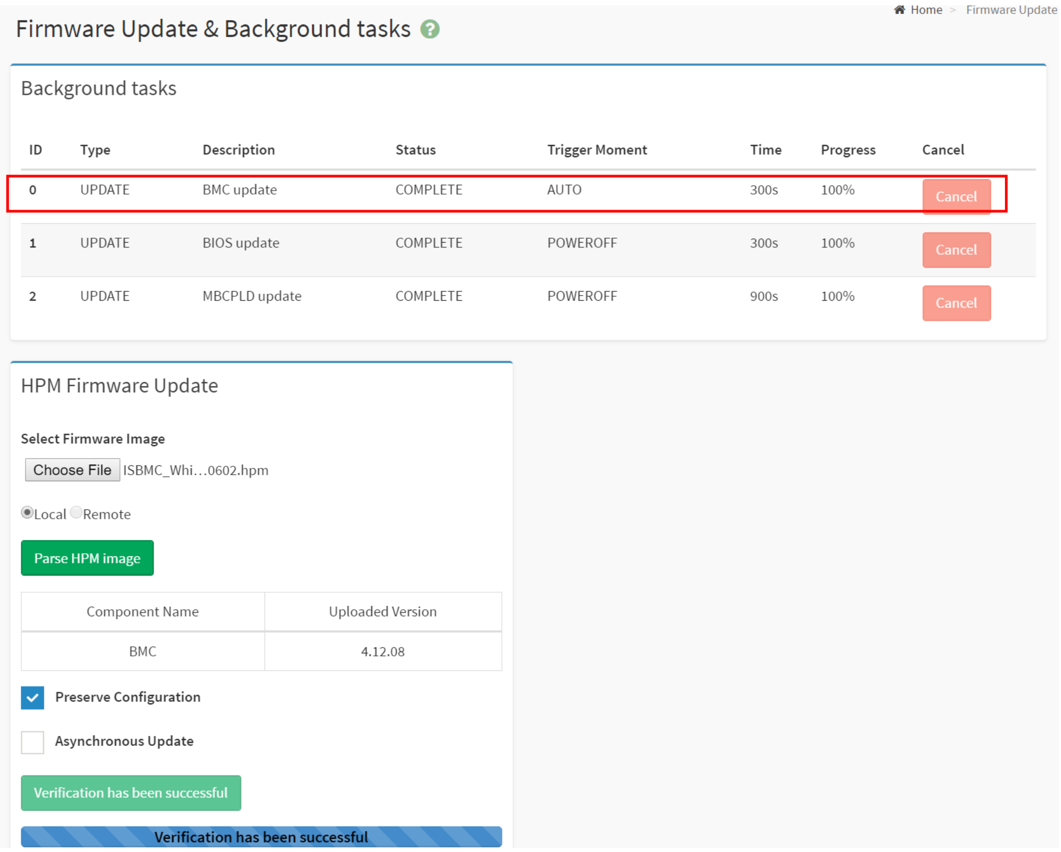
Table 3-74 Update Options Parameter

Parameter	Description
Preserve Configuration	• If checked, SDR, FRU, SEL policy settings, IPMI, network configuration, NTP, SNMP Set/Get settings, SSH, KVM, authentication, Syslog settings, Web, Extlog, and the BIOS configuration sent via Redfish will be preserved. • If not checked, all configurations are restored to factory settings.
Asynchronous Update	• If checked, the BMC will not reboot automatically after the update is completed. When you reboot the BMC manually, the image will switch to the new version. The other image

Parameter	Description
	will also be updated to the newest version. • If not checked, the BMC will reboot immediately after the update. After the system reboots, the image will switch to the new version. The other image will also be updated to the newest version.

4. The update starts automatically as a background task after the image is uploaded. You can view the progress and estimated completion time in the background taskbar. The update is successful when the progress is 100%.

Figure 3-75 Image Upload and Auto Update



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
0	UPDATE	BMC update	COMPLETE	AUTO	300s	100%	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	COMPLETE	POWEROFF	900s	100%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File ISBMC_Whi…0602.hpm

● Local ○ Remote

Component Name	Uploaded Version
BMC	4.12.08

☑ Preserve Configuration

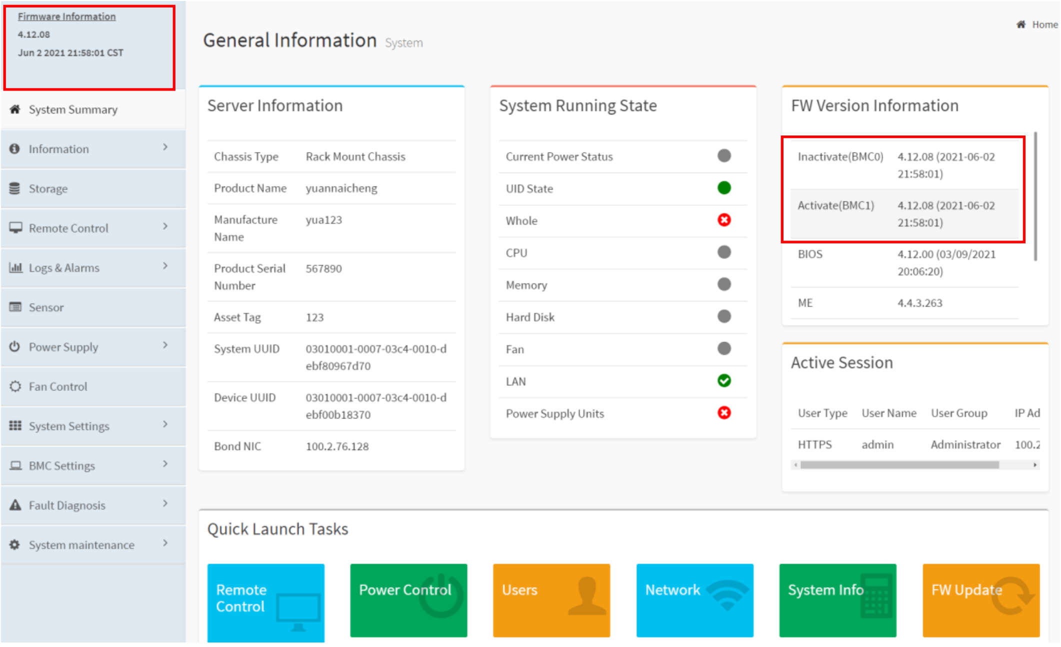
□ Asynchronous Update

Verification has been successful

Verification has been successful

5. After the BMC reboots, check its firmware version. Log in to the BMC Web GUI again, and check the firmware version in the upper-left corner of the page. If the BIOS or CPLD is updated, view the firmware version on the right for details.

Figure 3-76 Viewing Firmware Version



General Information System

Server Information

Chassis Type	Rack Mount Chassis
Product Name	yuannaicheng
Manufacture Name	yua123
Product Serial Number	567890
Asset Tag	123
System UUID	03010001-0007-03c4-0010-debf80967d70
Device UUID	03010001-0007-03c4-0010-debf00b18370
Bond NIC	100.2.76.128

System Running State

Current Power Status	●
UID State	●
Whole	☒
CPU	●
Memory	●
Hard Disk	●
Fan	●
LAN	✓
Power Supply Units	☒

FW Version Information

Inactivate(BMC0)	4.12.08 (2021-06-02 21:58:01)
Activate(BMC1)	4.12.08 (2021-06-02 21:58:01)
BIOS	4.12.00 (03/09/2021 20:06:20)
ME	4.4.3.263

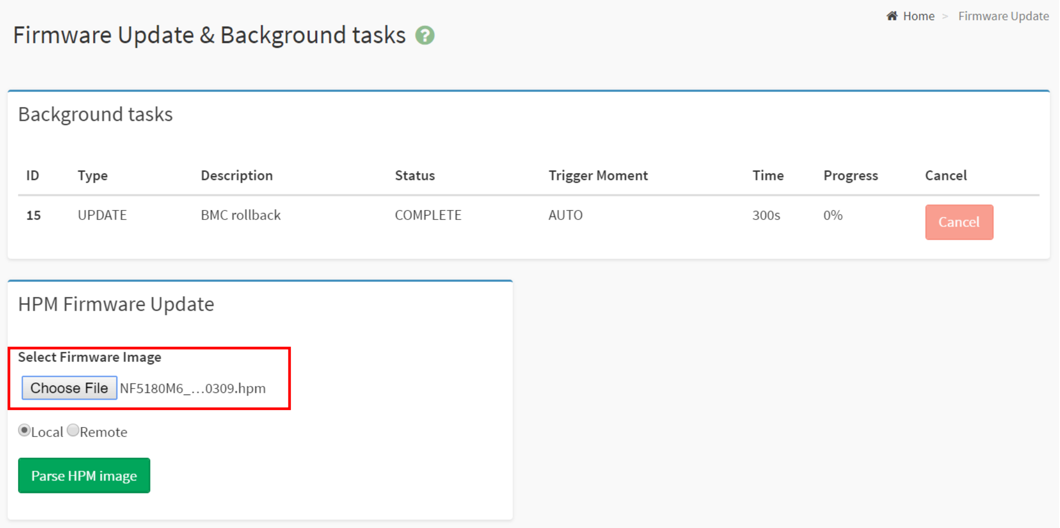
Active Session

User Type	User Name	User Group	IP Ad
HTTPS	admin	Administrator	100.2

3.13.1.2 Updating the BIOS

1. In the navigation pane, select **System Maintenance** > **HPM Firmware Update**. On the page, select a BIOS image.

Figure 3-77 BIOS Update_Select Firmware Image



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

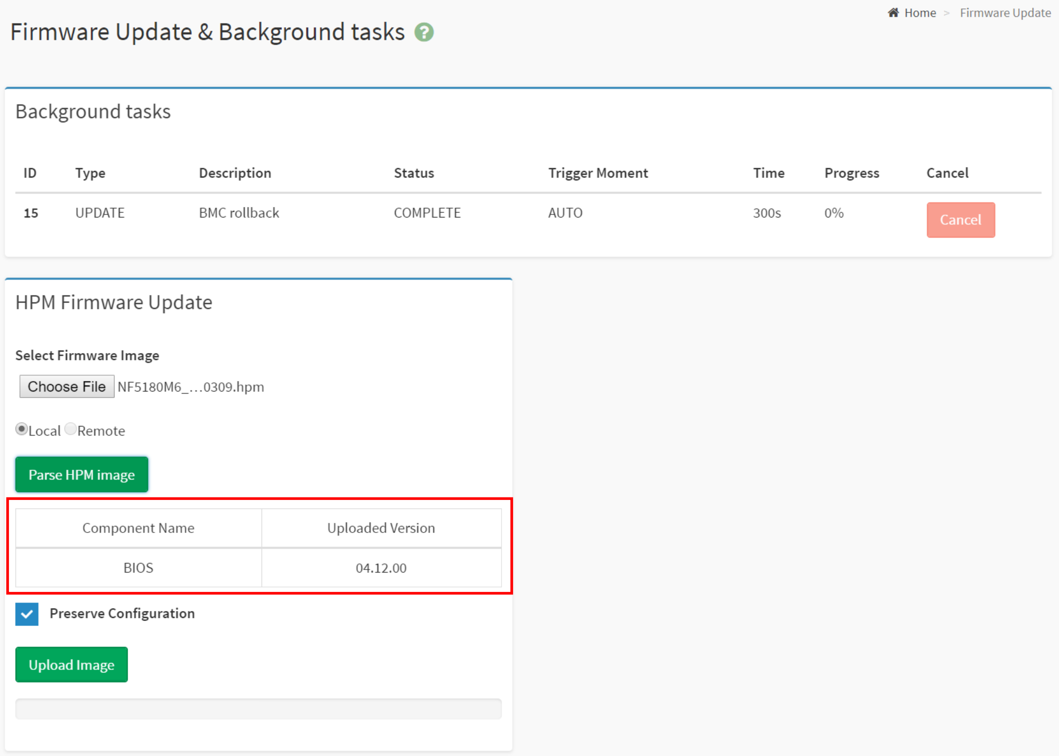
HPM Firmware Update

Select Firmware Image: NF5180M6_....0309.hpm

● Local ○ Remote

2. Click **Parse HPM image** and select whether to preserve configuration.

Figure 3-78 BIOS Update_Parse HPM Image



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File NF5180M6_...0309.hpm

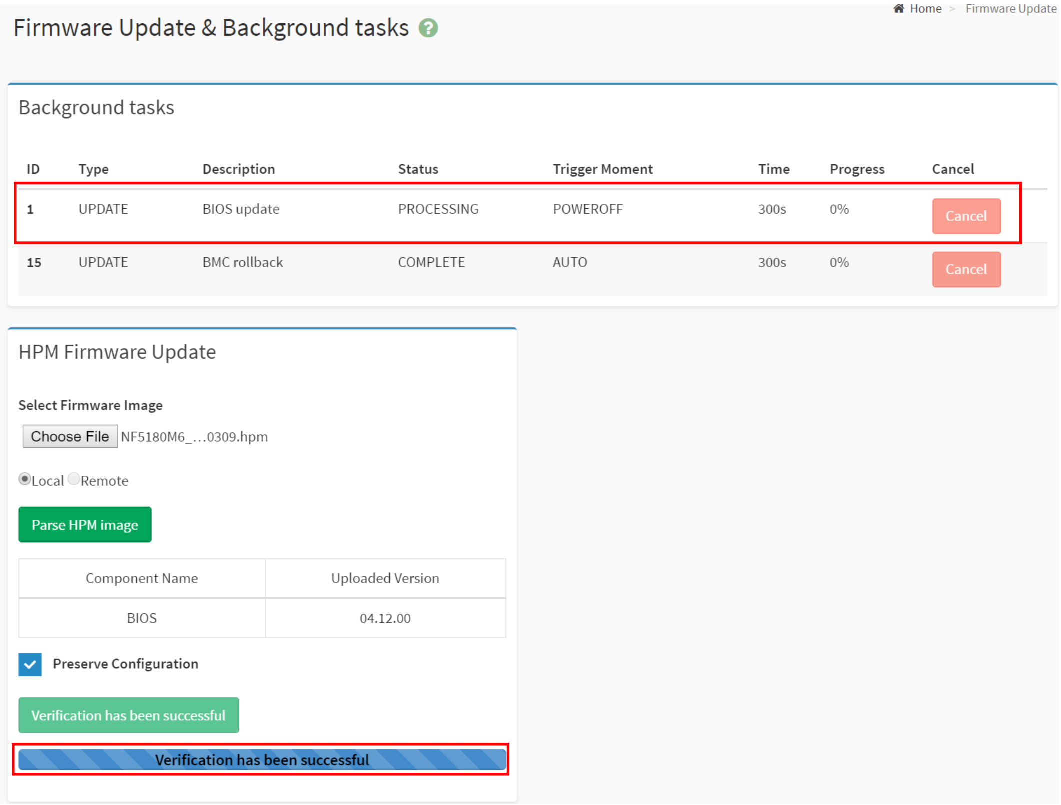
● Local ○ Remote

Component Name	Uploaded Version
BIOS	04.12.00

☑ Preserve Configuration

3. After the file is parsed, the component name and uploaded version will be displayed. If the information is correct, click **Upload Image** and wait until the file is verified successfully.

Figure 3-79 BIOS Update_Image Verification



Home > Firmware Update

Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	PROCESSING	POWEROFF	300s	0%	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File NF5180M6_...0309.hpm

● Local ○ Remote

Parse HPM image

Component Name	Uploaded Version
BIOS	04.12.00

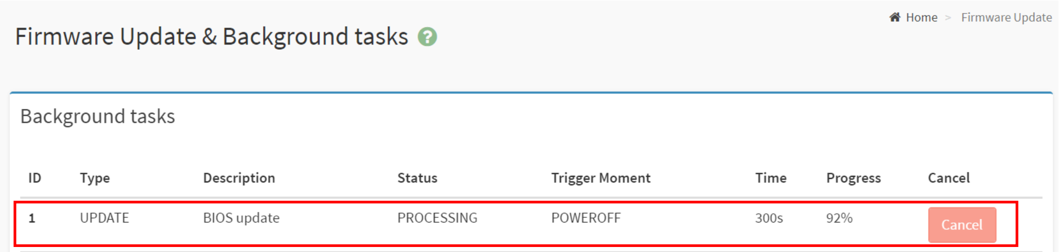
☑ Preserve Configuration

Verification has been successful

Verification has been successful

4. The update starts automatically as a background task after the image is uploaded. You can view the progress and estimated completion time in the background taskbar. The update is successful when the progress is 100%. Note: The BIOS update is triggered under the **POWEROFF** condition. No update is triggered when the existing power supply is on. To update BIOS, you should power off the server by running the **ipmitool power off** command. It is recommended to power off the server before updating the BIOS.

Figure 3-80 BIOS Update_Background Task Execution



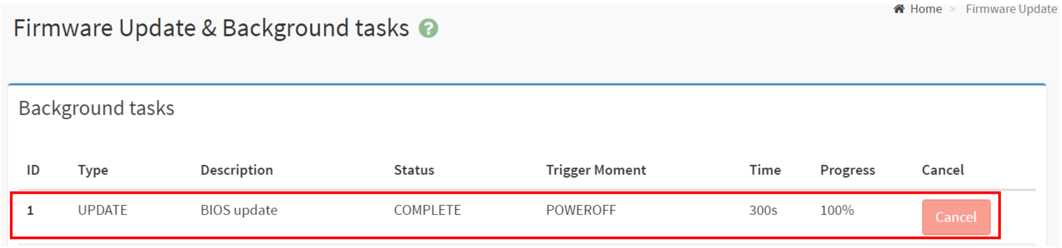
Home > Firmware Update

Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	PROCESSING	POWEROFF	300s	92%	Cancel

Figure 3-81 BIOS Update_Update Completed



Home > Firmware Update

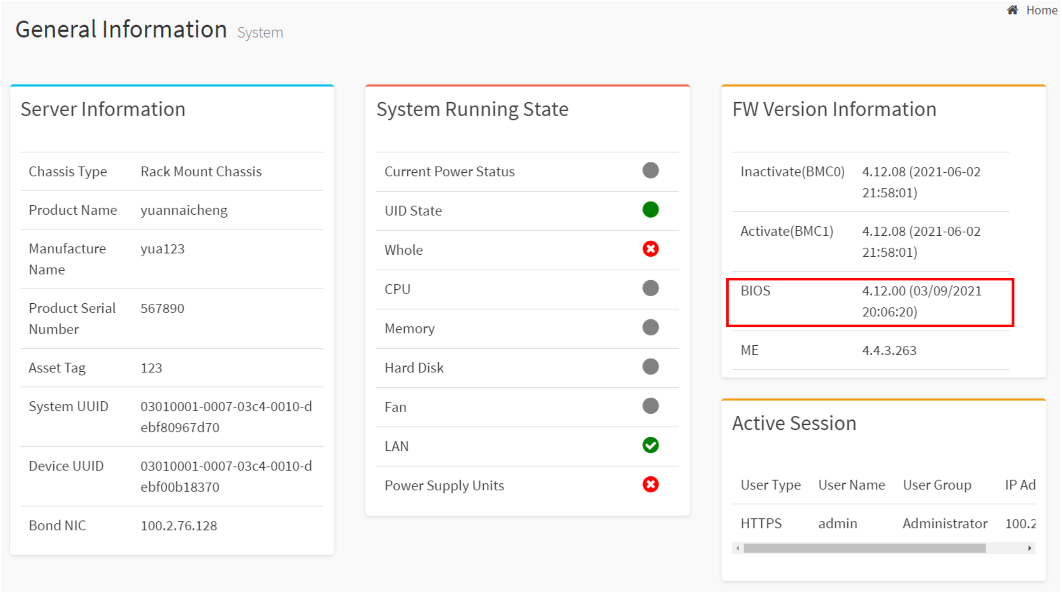
Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel

5. Log in to BMC Web GUI again after the operating system reboots and check the BIOS firmware version on the right.

Figure 3-82 BIOS Update_Version Check



Home

General Information System

Server Information

Chassis Type	Rack Mount Chassis
Product Name	yuannaicheng
Manufacture Name	yua123
Product Serial Number	567890
Asset Tag	123
System UUID	03010001-0007-03c4-0010-debf80967d70
Device UUID	03010001-0007-03c4-0010-debf00b18370
Bond NIC	100.2.76.128

System Running State

Current Power Status	●
UID State	●
Whole	✗
CPU	●
Memory	●
Hard Disk	●
Fan	●
LAN	✓
Power Supply Units	✗

FW Version Information

Inactivate(BMC0)	4.12.08 (2021-06-02 21:58:01)
Activate(BMC1)	4.12.08 (2021-06-02 21:58:01)
BIOS	4.12.00 (03/09/2021 20:06:20)
ME	4.4.3.263

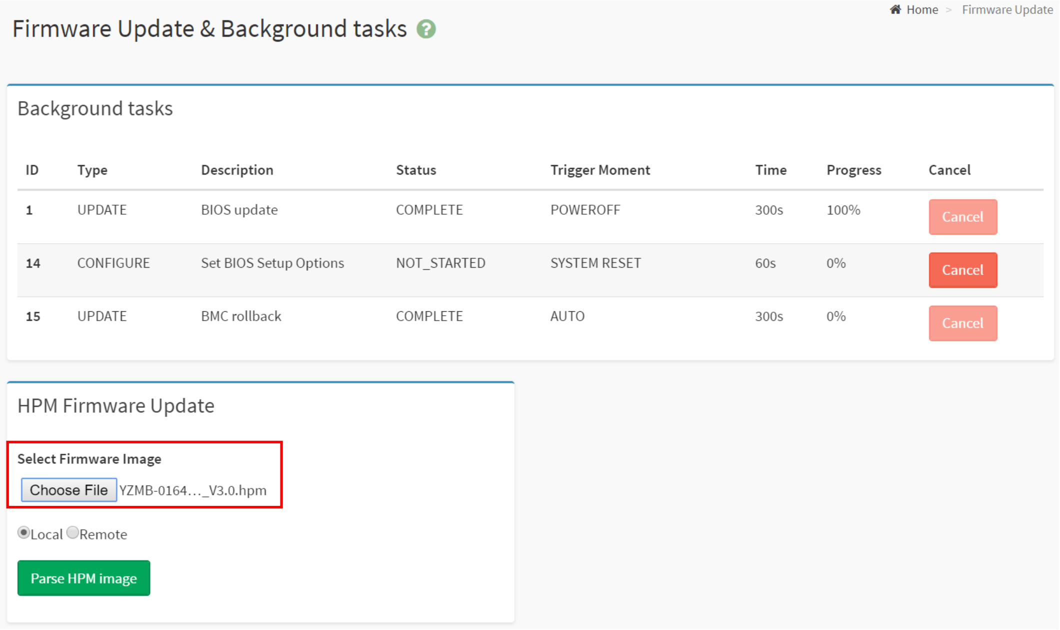
Active Session

User Type	User Name	User Group	IP Ad
HTTPS	admin	Administrator	100.2

3.13.1.3 Updating the CPLD

1. In the navigation pane, select **System Maintenance** > **HPM Firmware Update**. On the page, select a CPLD image.

Figure 3-83 CPLD Update_Select Firmware Image



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
14	CONFIGURE	Set BIOS Setup Options	NOT_STARTED	SYSTEM RESET	60s	0%	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

HPM Firmware Update

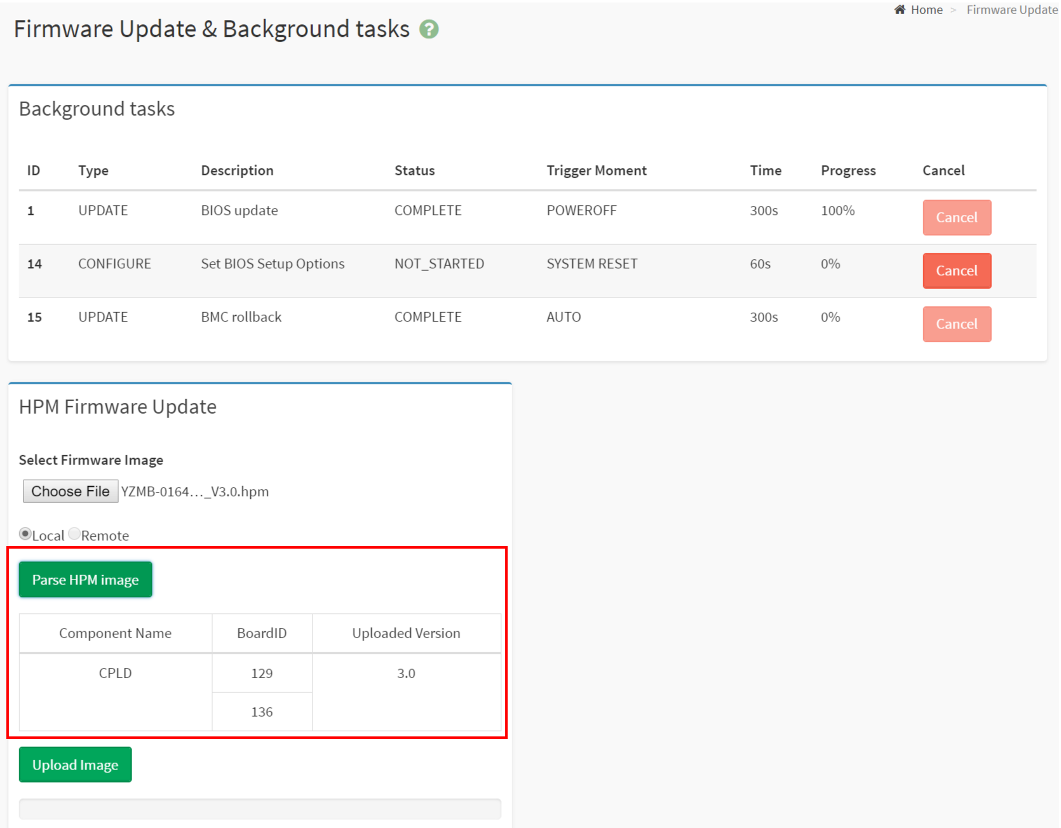
Select Firmware Image

Choose File YZMB-0164..._V3.0.hpm

● Local ○ Remote

2. Click **Parse HPM image**. After the file is parsed, the component name and version are displayed. If the information is correct, click **Upload Image** and wait until the file is verified successfully.

Figure 3-84 CPLD Update_Parse HPM Image



Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
14	CONFIGURE	Set BIOS Setup Options	NOT_STARTED	SYSTEM RESET	60s	0%	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

HPM Firmware Update

Select Firmware Image

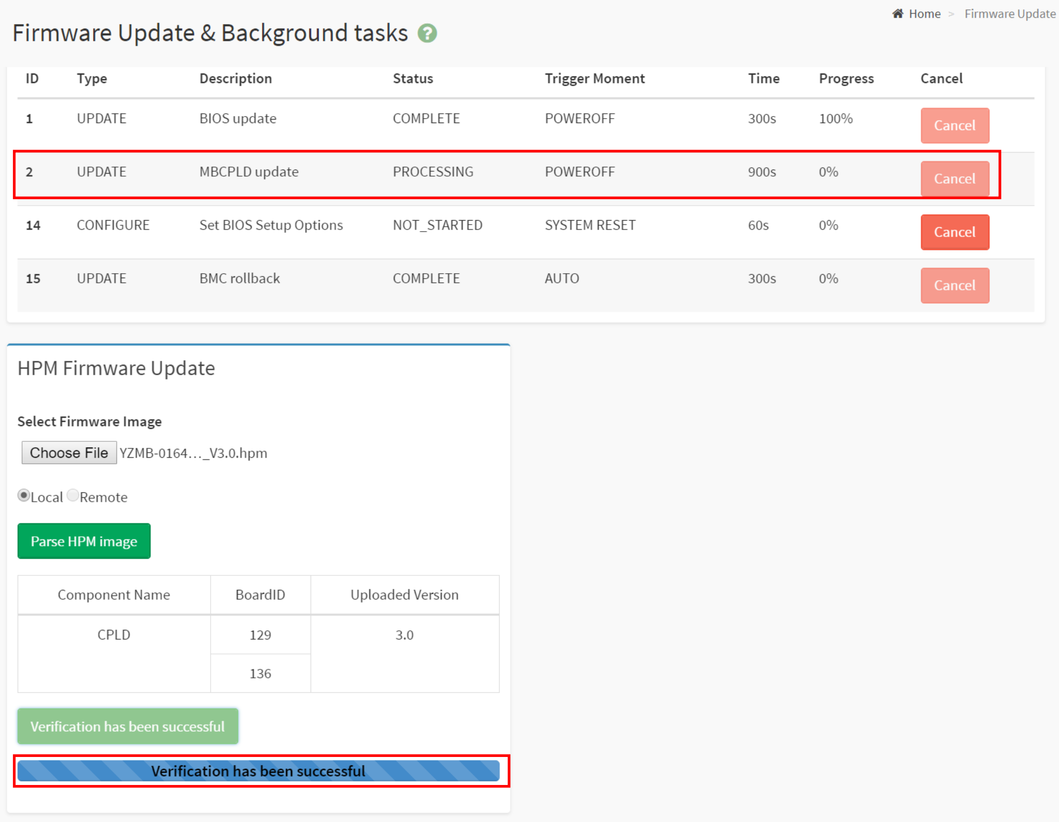
Choose File YZMB-0164..._V3.0.hpm

● Local ○ Remote

Component Name	BoardID	Uploaded Version
CPLD	129 136	3.0

3. The update starts automatically as a background task after the image is uploaded. You can view the progress and estimated completion time in the background taskbar. The update is successful when the progress is 100%. Note: The CPLD update is triggered under the **POWEROFF** condition. No CPLD update is triggered when the existing power supply is on. To trigger a CPLD update, you must power off the server by running the **ipmitool power off** command. It is recommended to power off the server before updating the CPLD.

Figure 3-85 CPLD Update_Image Verification



Firmware Update & Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	PROCESSING	POWEROFF	900s	0%	Cancel
14	CONFIGURE	Set BIOS Setup Options	NOT_STARTED	SYSTEM RESET	60s	0%	Cancel
15	UPDATE	BMC rollback	COMPLETE	AUTO	300s	0%	Cancel

HPM Firmware Update

Select Firmware Image

Choose File YZMB-0164..._V3.0.hpm

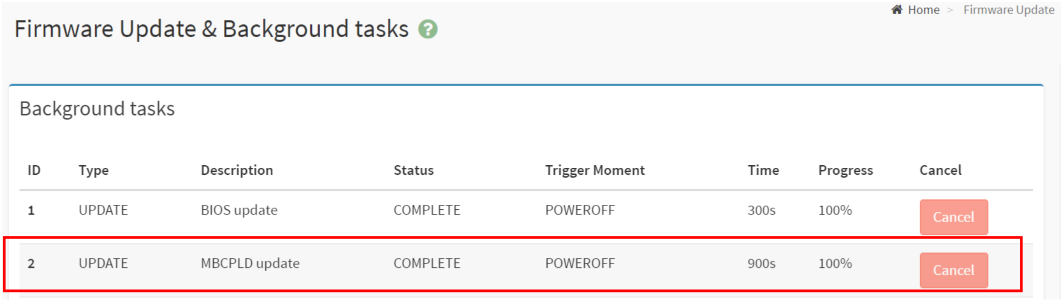
● Local ○ Remote

Component Name	BoardID	Uploaded Version
CPLD	129 136	3.0

Verification has been successful

Verification has been successful

Figure 3-86 CPLD Update_Update Completed



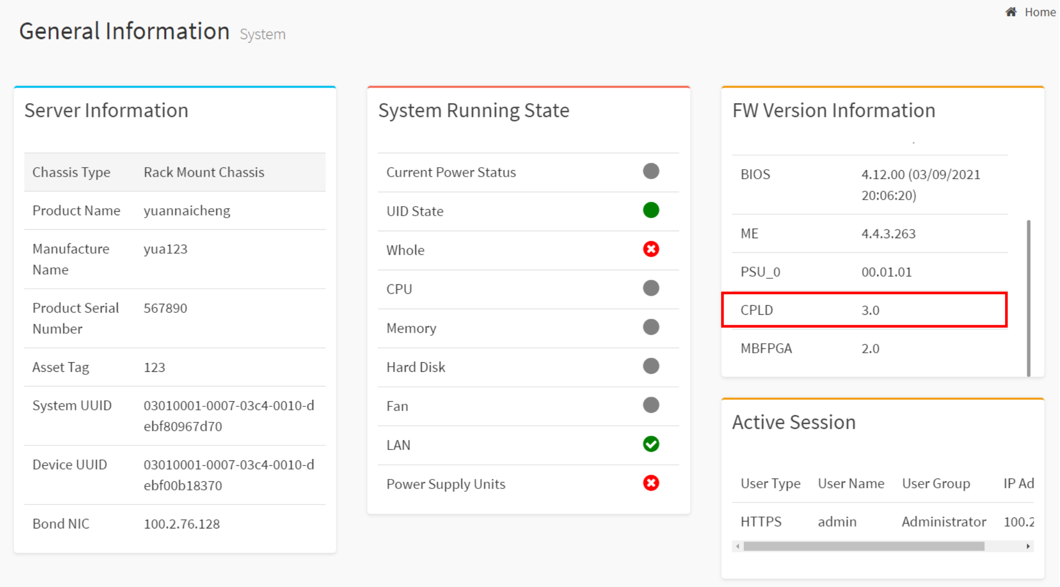
Firmware Update & Background tasks

Background tasks

ID	Type	Description	Status	Trigger Moment	Time	Progress	Cancel
1	UPDATE	BIOS update	COMPLETE	POWEROFF	300s	100%	Cancel
2	UPDATE	MBCPLD update	COMPLETE	POWEROFF	900s	100%	Cancel

4. Log in to the BMC Web GUI again and check the CPLD firmware version on the right.

Figure 3-87 CPLD Update_Version Check



General Information System

Home

Server Information

Chassis Type	Rack Mount Chassis
Product Name	yuannaicheng
Manufacture Name	yua123
Product Serial Number	567890
Asset Tag	123
System UUID	03010001-0007-03c4-0010-debf80967d70
Device UUID	03010001-0007-03c4-0010-debf00b18370
Bond NIC	100.2.76.128

System Running State

Current Power Status	●
UID State	●
Whole	✖
CPU	●
Memory	●
Hard Disk	●
Fan	●
LAN	✓
Power Supply Units	✖

FW Version Information

BIOS	4.12.00 (03/09/2021 20:06:20)
ME	4.4.3.263
PSU_0	00.01.01
CPLD	3.0
MBFPGA	2.0

Active Session

User Type	User Name	User Group	IP Ad
HTTPS	admin	Administrator	100.2

3.13.2 Firmware Image Location

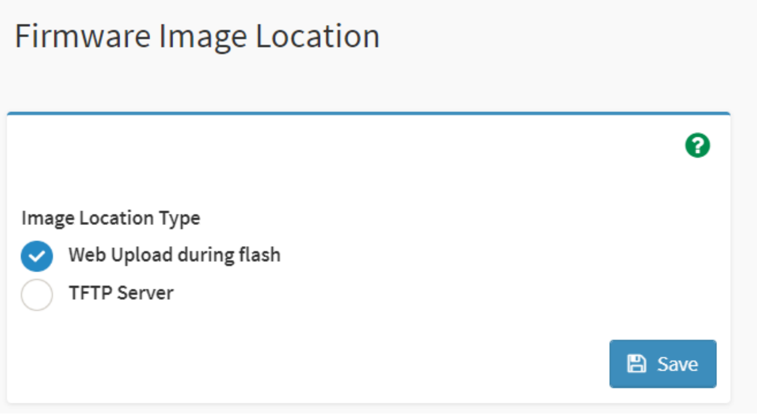
Description:

On the **Firmware Image Location** page, you can select the protocol for sending firmware image to BMC. The image location types include **Web Upload during flash** and **TFTP Server**.

Screen description:

In the navigation pane, select **System Maintenance** > **Firmware Image Location** to open the page as shown below.

Figure 3-88 Firmware Image Location



Firmware Image Location

Image Location Type

☑ Web Upload during flash

○ TFTP Server

Parameters:

Table 3-75 Firmware Image Location

Parameter	Description
Web Upload during flash	Web Upload during flash.
TFTP Server	Select a TFTP server and upload the firmware image to the server. When you select a TFTP server, specify the address, image name, and the number of retries of the TFTP server.

3.13.3 Firmware Information

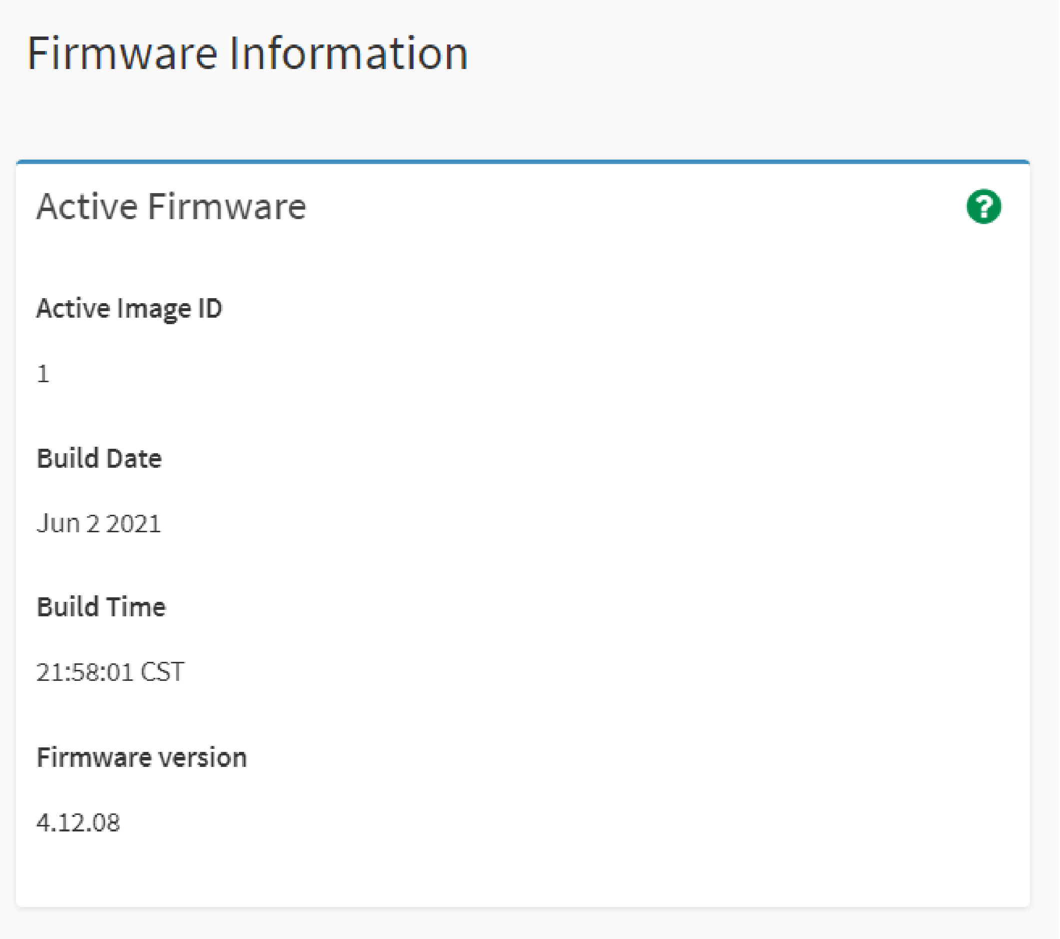
Description:

On the **Firmware Information** page, you can view the BMC firmware information, including **Active Image ID**, **Build Date**, **Build Time**, and **Firmware Version**.

Screen description:

In the navigation pane, select **System Maintenance** > **Firmware Information** to open the page as shown below.

Figure 3-89 Firmware Information



Firmware Information

Active Firmware

Active Image ID

1

Build Date

Jun 2 2021

Build Time

21:58:01 CST

Firmware version

4.12.08

Parameters:

Table 3-76 Firmware Information

Parameter	Description
Active Image ID	The ID of the BMC image being used.
Build Date	The date when the BMC image was created.
Build Time	The time when the BMC image was created.
Firmware version	The firmware version of the BMC image.

3.13.4 Restore Factory Defaults

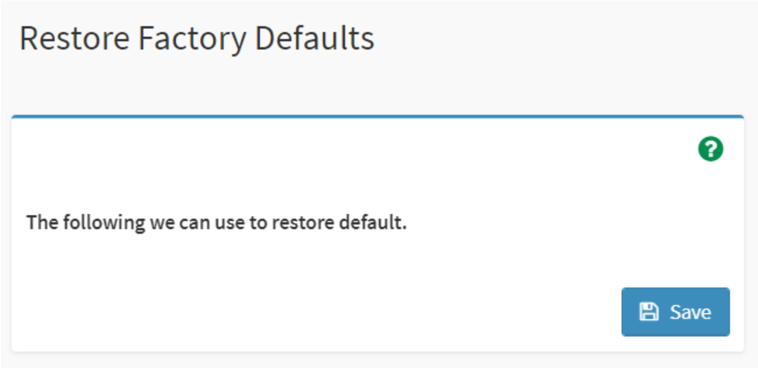
Description:

On the **Restore Factory Defaults** page, you can restore the BMC to its factory settings.

Screen description:

In the navigation pane, select **System Maintenance** > **Restore Factory Defaults** to open the page as shown below.

Figure 3-90 Restoring Factory Defaults



Restore Factory Defaults

The following we can use to restore default.

Parameters:

Table 3-77 Restoring Factory Defaults

Parameter	Description
Save	Click **Save** to restore BMC to factory settings.

NOTE

All user configurations will be lost after being restored to factory settings. Please proceed with caution.

4 Introduction to SMASH CLP CLI Functions

4.1 Overview

4.1.1 Commands

SMASH CLP CLI supports the following commands.

Table 4-1 Commands Supported by SMASH CLP CLI

Command	Description
bmclog	Obtains and clears BMC SELs.
chassis	Queries and controls the status of the chassis power supply and UID LED of the server.
mc	Queries and controls the status of the management controller.
diagnose	Provides various diagnostic tools.

4.1.2 Formats

A command line is generally composed of a command word followed by one or more command options, such as:

command [<option1>] [<option2>] ...

Table 4-2 Command Line Formats

Format	Description
[ ]	Commands enclosed in square brackets "[ ]" are optional during configuration.
<option>	Select one from the parameters.
<x|y|...>	Select one from the two or more options.

4.1.3 Help Information

Two types of help information can be displayed: a command list and detailed help information of a command.

You can view the command list using the help command.

```
/smashclp> help

Built-in command:

-------------------

bmclog    :    get or set bmclog parameters, please enter <bmclog --help> for
more information

chassis : get or set chassis parameters, please enter <chassis --help> for more
information

mc        :    get or set mc parameters, please enter <mc --help> for more
information

diagnose:    BMC diagnose function, please enter <diagnose --help> for more
information

exit      : exit the command line
```

Append **--help** to a command to view the command details. Example of the help information of bmclog:

```
/smashclp> bmclog --help

bmclog commands:

    bmclog <option1> [option2]

    option1:

        --help              show help information

        ?                   show help information

        --get               get bmc log

        --set               set bmc log

    option2:

        sel [clear]       get SEL or clear SEL
```

Append **--help** to a command to view the command details. Example of the help information of netstat:

```
/smashclp> diagnose netstat --help

BusyBox v1.21.1 (2021-04-01 09:46:39 CST) multi-call binary.


Usage: netstat [-ral] [-tuwx] [-en]


Display networking information


        -r    Routing table

        -a    All sockets

        -l    Listening sockets

              Else: connected sockets

        -t    TCP sockets

        -u    UDP sockets

        -w    Raw sockets

        -x    Unix sockets

              Else: all socket types

        -e    Other/more information

        -n    Don't resolve names
```

4.2 Login and Logout

4.2.1 Login to SMASH CLP CLI

You can log in to the BMC via SSH and then open Smash-Lite CLI. That is, log in to the CLI of the BMC via SSH. The CLI appears after login. Then, you can log in to the CLI by using the username and password of the BMC system.

```
root@desktop:~# ssh admin@100.2.76.64

The authenticity of host '100.2.76.64 (100.2.76.64)' can't be established.

RSA key fingerprint is 81:9d:31:77:42:c3:d7:98:95:42:6d:cb:2b:37:9e:f4.
```

```
Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '100.2.76.64' (RSA) to the list of known hosts.

admin@100.2.76.64's password:



          >> smashclp <<

///////////////////////////////////////////////

smashclp cli tool version 1.0

Enter 'help' for a list of built-in commands

///////////////////////////////////////////////


/smashclp>
```

4.2.2 Logout of SMASH CLP CLI

Run the **exit** command to log out of SMASH CLP CLI.

```
/smashclp> exit

Connection to 100.2.76.59 closed.
```

4.3 bmclog Command

4.3.1 Querying and Clearing SEL Logs

Function:

The **sel** command is used to query and clear SEL logs.

Format:

bmclog --get sel

bmclog --set sel clear

Parameters:

None

User Guide:

None

Examples:

# Query SEL logs.

```
/smashclp> bmclog --get sel
ID      |RecordTy   |TimeS          |GenID      |EvmRev     |SensorT   |Sensor#   |Evt DT
|Data1      |Data2      |Data3
553     |0x02       |0x60478f53   |0x20       |0x04       |0x18       |0xde       |0x07
|0x01       |0000       |0000
552     |0x02       |0x60478f35   |0x20       |0x04       |0x08       |0x8c       |0x0b
|0x01       |0000       |0000
551     |0x02       |0x60478f26   |0x20       |0x04       |0x04       |0x9f       |0x07
|0x01       |0000       |0000
550     |0x02       |0x60478f26   |0x20       |0x04       |0x04       |0x9d       |0x07
|0x01       |0000       |0000
```

# Clear SEL logs. If you query SEL logs again, you can view only one log that recorded this clearing operation.

```
/smashclp> bmclog --set sel clear
/smashclp> bmclog --get sel
ID      |RecordTy   |TimeS          |GenID      |EvmRev     |SensorT   |Sensor#   |Evt DT
|Data1      |Data2      |Data3
1       |0x02       |0x60563d6a   |0x20       |0x04       |0x10       |0x6f       |0x6f
|0x02       |0xff       |0xff
```

4.4 chassis Command

4.4.1 Querying and Controlling the Server Power Status

Function:

The **power** command is used to query and control the power status of the server.

Format:

chassis --get power status

chassis --set power <poweroption>

Table 4-3 Parameter Description

Parameter	Description	Value
poweroption	Turns on/off the server.	• on • off

User Guide:

None

Examples:

# Query the power status of the server.

```
/smashclp> chassis --get power status

The host status is off
```

# Turn on the server.

```
/smashclp> chassis --set power on

Power status successfully.
```

# Turn off the server.

```
/smashclp> chassis --set power off

Power status successfully.
```

4.4.2 Querying and Controlling the UID LED Status

Function:

The **identify** command is used to query and control the status of the UID LED.

Format:

chassis --get identify status

chassis --set identify <force | value>

Table 4-4 Parameter Description

Parameter	Description	Value
force	Force the UID LED to remain on.	N/A
value	Duration of UID LED flashes.	An integer in seconds. Value range: 0 - 240. The value 0 indicates that the LED is turned off.

User Guide:

None

Examples:

# Query the UID LED status.

```
/smashclp> chassis identify status

The UID status is off
```

# Force the UID LED to remain on.

```
/smashclp> chassis --set identify force

Identify UID successfully.
```

# Flash the UID LED for 15 seconds.

```
/smashclp> chassis --set Didentify 15

Identify UID successfully.
```

4.5 mc Command

4.5.1 Obtaining the BMC System Version

Function:

Display the version of the existing BMC system.

Format:

mc --get version

Parameters:

None

User Guide:

None

Examples:

# Obtain the BMC system version.

```
/smashclp> mc --get version
Device ID                  : 32
Device Revision            : 1
Firmware Revision          : 4.11.5
IPMI Version               : 2.0/dev/ram3                    6116        6116
0 100% /usr/local/www
/dev/shm                   205200      8904      196296    4% /usr/local/bin
```

4.5.2 Restarting Service

Function:

Restart the BMC system or a service in the BMC system.

Format:

mc --set <servicename> reset

Table 4-5 Parameter Description

Parameter	Description	Value
servicename	Service name	• BMC • KVM • Web

User Guide:

None

Examples:

# Restart the KVM module in the BMC.

```
/smashclp> mc --set kvm reset
KVM reset OK!
```

# Restart the BMC system.

```
/smashclp> mc --set bmc reset


Broadcast message from sysadmin@ProductSN (Mon Apr 13 21:56:13 2020):


The system is going down for reboot NOW!

MC reset OK!
```

4.5.3 Factory Reset

Function:

Restore BMC to factory settings. The BMC system restarts after the command is executed successfully.

Format:

mc --set factorydefaults restore

Parameters:

None

User Guide:

None

Examples:

# Restore to factory settings.

```
/smashclp> mc --set factorydefaults restore

/smashclp>
```

4.5.4 Dual-Image Boot Configuration

Function:

Display and modify the dual-image boot configuration of the existing BMC system.

Format:

mc --get dualimgconf

mc --set dualimgconf [boot_number]

Table 4-6 Parameter Description

Parameter	Description	Value
boot_number	The image from which the boot process starts.	• 0: Higher firmware version • 1: IMAGE-1 • 2: IMAGE-2 • 3: Lower firmware version • 4: Newest updated firmware • 5: Not newest updated firmware

User Guide:

None

Examples:

# Obtain the existing dual-image boot configuration of the BMC system.

```
/smashclp> mc --get dualimgconf

Current active image: Image2

Current active image version: 4.10.12

Current standby image: Image1

Current standby image version: 4.10.12
```

# Set the BMC system to boot using a higher version.

```
/smashclp> mc --set dualimgconf 0

Setting dual image configuration OK! The specified boot image is Higher
firmware version

Set bmc boot image OK!
```

4.6 diagnose Command

4.6.1 Listing Log File Attributes

Function:

The **ls** command in the Linux system is used to display the log directory or file under a directory.

Format:

diagnose ls <logfile>

Table 4-7 Parameter Description

Parameter	Description	Value
logfile	Log file	• ncml bmc service configuration • log bmc system log • cpuinfo bmc cpu info • meminfo bmc memory info • versioninfo bmc version info • crontab bmc crontab file

User Guide:

None

Examples:

# Display the cpuinfo file.

```
/smashclp> diagnose ls cpuinfo

/proc/cpuinfo
```

# Display the log directory.

```
/smashclp> diagnose ls log

BMC1                         ErrorAnalyReport.json    archive
audit.log.1               index.log                    psuFaultHistory.log

CaptureScreen             RegRawData.json          audit.log                     idl.log
maintenance.log           sollog
```

4.6.2 Viewing Log File

Function:

The **cat** command in the Linux system is used to display the content of a log file.

Format:

diagnose cat <logfile>

Table 4-8 Parameter Description

Parameter	Description	Value
logfile	Log file	• ncml bmc service configuration • log bmc system log • cpuinfo bmc cpu info • meminfo bmc memory info • versioninfo bmc version info • crontab bmc crontab file

User Guide:

None

Examples:

# List the contents in the audit.log file.

```
/smashclp> diagnose cat log audit.log

<142>    2000-01-07T01:56:45.760000+08:00 ProductSN adviserd:    [3176 : 3182 INFO]|KVM|100.2.54.118|admin|Logout Success form IP:100.2.54.118 user:admin

<142>    2000-01-03T09:23:01.740000+08:00 ProductSN sshd[11564]:    [11564 : 11564 INFO]|CLI|100.2.54.244|admin|Login Success from IP:100.2.54.244 user:admin

<142>    2000-01-03T09:31:04.930000+08:00 ProductSN sshd[11564]:    [11564 : 11564 INFO]|CLI|100.2.54.244|admin|Logout Success from IP:100.2.54.244 user:admin

<142>    2000-01-03T09:31:27.320000+08:00 ProductSN spx_restservice:    [3227 : 3227 INFO]|WEB|100.2.54.244|admin|Login Success from IP:100.2.54.244 user:admin

<142>    2000-01-03T09:42:28.140000+08:00 ProductSN sshd[15679]:    [15679 : 15679 INFO]|CLI|100.2.54.244|admin|Login Success from IP:100.2.54.244 user:admin

/smashclp>
```

# List the contents in the cpuinfo file.

```
/smashclp> diagnose cat cpuinfo

processor       : 0

model name : ARMv6-compatible processor rev 7 (v6l)

Features: swp half fastmult edsp java tls

CPU implementer : 0x41

CPU architecture: 7

CPU variant   : 0x0

CPU part: 0xb76

CPU revision  : 7



Hardware        : AST2500EVB

Revision : 0000

Serial             : 0000000000000000
```

# List the contents in the meminfo file.

```
/smashclp> diagnose cat meminfo

MemTotal:             410404 kB

MemFree:               179400 kB

MemAvailable:        237160 kB

Buffers:                24752 kB

Cached:                  49228 kB

SwapCached:                  0 kB

Active:               149900 kB

Inactive:              38756 kB

Active (anon):        115320 kB

Inactive (anon):       10084 kB

Active (file):        34580 kB

Inactive (file):     28672 kB

Unevictable:                0 kB
```

```
Mlocked:                 0 kB
SwapTotal:               0 kB
SwapFree:                0 kB
Dirty:                   0 kB
Writeback:               0 kB
AnonPages:          114704 kB
Mapped:              17864 kB
Shmem:               10728 kB
Slab:                 5560 kB
SReclaimable:         1812 kB
SUnreclaim:           3748 kB
KernelStack:          1424 kB
PageTables:           1832 kB
NFS_Unstable:            0 kB
Bounce:                  0 kB
WritebackTmp:            0 kB
CommitLimit:        205200 kB
Committed_AS:      1078224 kB
VmallocTotal:       581632 kB
VmallocUsed:         51020 kB
VmallocChunk:       344060 kB
```

4.6.3 Viewing Recently Logged in Users (last)

Function:

The **last** command in the Linux system is used to display the users who have recently logged in to the existing BMC system.

Format:

diagnose last

Parameters:

None

User Guide:

None

Examples:

# Display users who have recently logged in to the BMC system.

```
/smashclp> diagnose last
admin     pts/0        100.2.54.244     Sat Mar 13 16:40    still logged in
admin     pts/0        100.2.54.244     Sat Mar 13 16:40 - 16:40 (0+00:00)
admin     pts/0        100.2.54.244     Sat Mar 13 16:21 - 16:40 (0+00:18)
admin     pts/0        100.2.54.244     Sat Mar 13 14:50 - 14:50 (0+00:00)
admin     pts/0        100.2.54.244     Sat Mar 13 10:40 - 14:50 (0+04:10)
admin     pts/0        100.2.54.244     Sat Mar 13 10:10 - 10:37 (0+00:26)
admin     pts/0        100.2.54.244     Sat Mar 13 10:10 - 10:10 (0+00:00)
admin     pts/2        100.2.54.244     Fri Mar 12 17:35 - 10:09 (0+16:34)
sysadmin pts/1         100.2.53.75      Fri Mar 12 17:14 - 03:26 (0+10:12)
sysadmin pts/0         100.2.53.75      Fri Mar 12 15:40 - 03:28 (0+11:48)
sysadmin pts/2         100.2.53.101     Fri Mar 12 10:37 - 15:53 (0+05:16)
sysadmin pts/1         100.2.53.101     Fri Mar 12 09:49 - 15:52 (0+06:03)
```

4.6.4 Viewing and Setting Network Devices (ifconfig)

Function:

The **ifconfig** command in the Linux system is used to display and set the network devices in the existing BMC system.

Format:

diagnose ifconfig [interface]

Table 4-9 Parameter Description

Parameter	Description	Value
interface	Physical network interface	• bond0 • eth0 • eth1

User Guide:

None

Examples:

# List information of all network devices.

```
/smashclp> diagnose ifconfig
bond0       Link encap:Ethernet    HWaddr B4:05:5D:9B:27:4A
          inet addr:100.2.76.134    Bcast:100.2.76.255    Mask:255.255.255.0
          inet6 addr: fe80::b605:5dff:fe9b:274a/64 Scope:Link
          inet6 addr: fdbd:dc02:108:1318::209/64 Scope:Global
          UP BROADCAST RUNNING MASTER MULTICAST    MTU:1500    Metric:1
          RX packets:30347376 errors:90 dropped:131859 overruns:0 frame:90
          TX packets:499701 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2083961985 (1.9 GiB)    TX bytes:216037733 (206.0 MiB)

eth0       Link encap:Ethernet    HWaddr B4:05:5D:9B:27:4A
          UP BROADCAST RUNNING SLAVE MULTICAST    MTU:1500    Metric:1
          RX packets:30347376 errors:90 dropped:14 overruns:0 frame:90
          TX packets:499494 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2083961985 (1.9 GiB)    TX bytes:216028211 (206.0 MiB)
          Interrupt:3

eth1       Link encap:Ethernet    HWaddr B4:05:5D:9B:27:4A
          UP BROADCAST SLAVE MULTICAST    MTU:1500    Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:9522 (9.2 KiB)
          Interrupt:2

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:18113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2925785 (2.7 MiB)  TX bytes:2925785 (2.7 MiB)

usb0      Link encap:Ethernet  HWaddr 5E:F5:F7:34:4B:A9
          inet addr:169.254.0.17  Bcast:169.254.15.255  Mask:255.255.240.0
          inet6 addr: fe80::5cf5:f7ff:fe34:4ba9/64 Scope:Link
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:7 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:648 (648.0 B)
```

# List information of the network device eth0.

```
/smashclp> diagnose ifconfig eth0
eth0      Link encap:Ethernet  HWaddr B4:05:5D:9B:27:4A
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
          RX packets:30348184 errors:90 dropped:14 overruns:0 frame:90
          TX packets:499527 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2084019516 (1.9 GiB)  TX bytes:216037909 (206.0 MiB)
          Interrupt:3
```

4.6.5 Viewing and Setting NIC Parameters (ethtool)

Function:

The **ethtool** command in the Linux system is used to display and set NIC parameters in the existing BMC system.

Format:

diagnose ethtool <interface>

Table 4-10 Parameter Description

Parameter	Description	Value
interface	Physical network interface	• eth0 • eth1

User Guide:

None

Examples:

# List parameters of the NIC eth0.

```
/smashclp> diagnose ethtool eth0
Settings for eth0:
        Supported ports: [ TP MII ]
        Supported link modes:     10baseT/Half 10baseT/Full
                                  100baseT/Half 100baseT/Full
                                  1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Advertised link modes:    10baseT/Half 10baseT/Full
                                  100baseT/Half 100baseT/Full
                                  1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes

        Speed: 1000 Mb/s

        Duplex: Full

        Port: Twisted Pair

        PHYAD: 0

        Transceiver: internal

        Auto-negotiation: on

        MDI-X: Unknown

Cannot get wake-on-lan settings: Operation not permitted

        Link detected: yes
```

4.6.6 Obtaining BMC System Processes (ps)

Function:

The **ps** command in the Linux system is used to display processes in the existing BMC system.

Format:

diagnose ps

Parameters:

None

User Guide:

None

Examples:

# List processes in the existing system.

```
/smashclp> diagnose ps

   PID TTY          TIME CMD

14730 pts/0    00:00:00 smashclp

15452 pts/0    00:00:00 sh

15453 pts/0    00:00:00 ps
```

4.6.7 Viewing Resource Utilization of BMC System Processes (top)

Function:

The **top** command in the Linux system is used to display resource utilization of processes running in the existing BMC system.

Format:

diagnose top [-b] [-nCOUNT] [-dSECONDS] [-m]

Table 4-11 Parameter Description

Parameter	Description	Value
-nCOUNT	The number of repetitions before exit	1 - n
q	Exit the command.	NA

User Guide:

None

Examples:

# Display resource utilization of the BMC system processes once and then exit.

```
/smashclp> diagnose top -n 1


Mem: 231580K used, 178824K free, 0K shrd, 605464K buff, 605512K cached

CPU: 15.0% usr 30.0% sys   0.0% nic 50.0% idle   0.0% io   0.0% irq   5.0% sirq

Load average: 4.86 4.87 4.87 3/182 15374

  PID  PPID USER      STAT    VSZ %VSZ CPU %CPU COMMAND

15371 15369 sysadmin R       3344   0.8    0 20.0 top -n 1

15374 15370 admin     R       2812   0.6    0 20.0 /usr/bin/top -n 1

  775     1 sysadmin S      434m108.3    0   0.0 {init_rai}
/usr/local/bin/IPMIMain --daemonize --reg-with-procmgr
```

4.6.8 Viewing Kernel Buffer Logs (dmesg)

Function:

The **dmesg** command in the Linux system is used to display the dmesg log in the existing BMC system.

Format:

diagnose dmesg

Parameters:

None

User Guide:

None

Examples:

# Display the dmesg log in the BMC system.

```
/smashclp> diagnose dmesg
[    1.340000] sdhci: Copyright(c) Pierre Ossman
[    1.430000] mmc0: SDHCI controller on ast_sdhci1 [ast_sdhci1.0] using ADMA
[    1.480000] mmc1: SDHCI controller on ast_sdhci2 [ast_sdhci2.0] using ADMA
[    1.480000] AST SoC SD/MMC Driver Init Success
[    1.490000] Netfilter messages via NETLINK v0.30.
[    1.490000] nfnl_acct: registering with nfnetlink.
[    1.500000] xt_time: kernel timezone is -0000
```

4.6.9 Obtaining Network Information (netstat)

Function:

The **netstat** command in the Linux system is used to display the network information in the existing BMC system.

Format:

diagnose netstat [-ral] [-tuwx] [-en]

Table 4-12 Parameter Description

Parameter	Description
-a	Displays all sockets.
-n	Skips domain name resolution.

User Guide:

None

Examples:

# Display all network connections to the current system.

```
/smashclp> diagnose netstat -an

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address           Foreign Address         State

tcp        0      0 0.0.0.0:199             0.0.0.0:*               LISTEN

tcp        0      0 0.0.0.0:5900              0.0.0.0:*               LISTEN

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN

tcp        0    0 100.2.76.59:22          100.2.54.244:43331
ESTABLISHED
```

4.6.10 Debugging BMC GPIO Devices

Function:

Debug GPIO devices in the existing BMC system.

Format:

diagnose gpiotool <gpionumber> <option>

Table 4-13 Parameter Description

Parameter	Description	Value
gpionumber	GPIO device ID	0-227
option	Supported commands	• --get-dir • --get-data

User Guide:

This tool must be used under the guidance of qualified professionals to prevent system errors.

Examples:

# Obtain input/output directions of GPIO 10.

```
/smashclp> diagnose gpiotool 10 --get-dir
Inside Get Dir


Input Pin
```

# Obtain the input status of GPIO 10.

```
/smashclp> diagnose gpiotool 10 --get-data
Inside Read gpio.


Pin is High
```

4.6.11 Debugging BMC I^{2}C Devices

Function:

Debug I^{2}C devices in the existing BMC system.

Format:

diagnose i2c-test -b <bus number> --scan

diagnose i2c-test -b <bus number> -s slave -rc count -d < bytes >

diagnose i2c-test -b <bus number> -s slave -w -d < bytes >

Table 4-14 Parameter Description

Parameter	Description	Value
bus number	Bus number	0 - 13
slave	7-bit slave address	0-0x7F
count	Number of bytes to read	1 by default
bytes	Data to be sent	

User Guide:

This tool must be used under the guidance of qualified professionals to prevent system errors.

Examples:

# Scan all slave addresses of bus 1 of the I^{2}C device.

```
/smashclp> diagnose i2c-test -b 1 --scan

Scanning the I2C Bus...this may take a while...

.

................................................................................X......

..........................................

Done!   Found 1 valid slave address(es)

Slave list:

0xa0
```

# Read 32 bytes from the 7-bit slave address 0x50 of bus 1 of the I^{2}C device.

```
/smashclp> diagnose i2c-test -b 1 -s 0x50 -rc 32 -d 0 0

i2c_dev = /dev/i2c1

Bytes read:   32

b4 05 5d 4d f8 94 ff ff ff ff ff ff ff ff ff ff

ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Bytes written:     2

00 00
```

4.6.12 Debugging BMC PWM Fans

Function:

Debug PWM fans in the BMC system.

Format:

diagnose pwmtachtool <device_id> <command-option> <fannum>

Table 4-15 Parameter Description

Parameter	Description	Value
device_id	Device ID	Usually 0
command-option	Supported commands	• --get-fan-speed • --get-pwm-dutycycle
fannum	The serial number of the fan	[1-n], depending on the actual number of fans.

User Guide:

This tool must be used under the guidance of qualified professionals to prevent system errors.

Examples:

# Obtain the rotational speed of fan 0 of device 0.

```
/smashclp> diagnose pwmtachtool 0 --get-fan-speed 0

Fan 0 speed is 7498
```

# Obtain the duty of fan 2 of device 0.

```
/smashclp> diagnose pwmtachtool 0 --get-pwm-dutycycle 2

PWM 2 Dutycycle is 26
```

4.6.13 Accessing BMC IPMI Devices

Function:

The **ipmitool** command is used to access the IPMI devices in the existing BMC system.

Format:

diagnose ipmitool -H 127.0.0.1 <command>

Table 4-16 Parameter Description

Parameter	Description	Value
command	The ipmitool command.	• fru • Sensor

Parameter	Description	Value
		- sdr - sel - sel list

User Guide:

None

Examples:

# Obtain the FRU information in the BMC system.

```
/smashclp> diagnose ipmitool -H 127.0.0.1 fru
FRU Device Description : Builtin FRU Device (ID 0)
 Chassis Type              : Rack Mount Chassis
 Chassis Part Number   : ChassisPN
 Chassis Serial            : ChassisSN
 Chassis Extra             : ChassisExtra
```

# Obtain the SDR information in the BMC system.

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sdr
Inlet_Temp          | 24 degrees C        | ok
Outlet_Temp         | 35 degrees C        | ok
CPU0_Temp           | disabled            | ns
CPU1_Temp           | disabled            | ns
CPU0_DTS            | disabled            | ns
CPU1_DTS            | disabled            | ns
CPU0_DDR_DIMM_T     | disabled            | ns
CPU0_BPS_DIMM_T     | disabled            | ns
CPU1_DDR_DIMM_T     | disabled            | ns
CPU1_BPS_DIMM_T     | disabled            | ns
```

# Obtain the sensor information in the BMC system.

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sensor
Inlet_Temp       | 23.000     | degrees C  | ok    | na        | na        | na
| 42.000    | 47.000    | na
Outlet_Temp      | 35.000     | degrees C  | ok    | na        | na        | na
| 75.000    | na        | na
CPU0_Temp        | na         | degrees C  | na    | na        | na        | na
| na        | na        | na
CPU1_Temp        | na         | degrees C  | na    | na        | na        | na
| na        | na        | na
```

# Obtain the SEL summary in the BMC system.

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sel
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
Entries          : 1737
Free Space       : 34236 bytes
Percent Used     : 44%
Last Add Time    : 01/01/2000 08:02:13
Last Del Time    : Not Available
Overflow         : false
Supported Cmds   : 'Delete' 'Partial Add' 'Reserve' 'Get Alloc Info'
# of Alloc Units : 3639
Alloc Unit Size  : 18
# Free Units     : 1902
Largest Free Blk : 1902
Max Record Size  : 7
```

# Obtain the SEL list information in the BMC system.

```
/smashclp> diagnose ipmitool -H 127.0.0.1 sel elist
   1 | 01/01/2000 | 08:00:41 | System Boot Initiated BMC_Boot_Up | Initiated by
power up | Asserted
```

```
     2 | 01/01/2000 | 08:00:49 | System ACPI Power State ACPI_PWR | S0/G0:
working | Asserted

     3 | 01/01/2000 | 08:01:18 | Button Power_Button | Power Button pressed |
Asserted
```

4.6.14 Obtaining Disk Usage of the File System (df)

Function:

The **df** command in the Linux system is used to display the usage of the file system in the existing BMC system.

Format:

diagnose df [-Pkmhai]

Parameters:

None

User Guide:

None

Examples:

# Obtain the usage of the existing file system.

```
/smashclp> diagnose df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root                59868     59868         0 100% /
devtmpfs                171080         0    171080   0% /dev
/dev/shm                205200      8904    196296   4% /var
/dev/shm                205200        64    205136   0% /run
/dev/mtdblock7            1984       316      1668  16% /bkupsync
/dev/mtdblock1            1984       304      1680  15% /conf
/dev/mtdblock2            1984       332      1652  17% /bkupconf
/dev/mtdblock3           10176      2124      8052  21% /extlog
/dev/mtdblock9           10176      2108      8068  21% /bkupextlog
/dev/mtdblock4           10176       388      9788   4% /usr/local/lmedia
/dev/ram3                 6116      6116         0 100% /usr/local/www
/dev/shm                205200      8904    196296   4% /usr/local/bin
```

4.6.15 Obtaining System Runtime (uptime)

Function:

The **uptime** command in the Linux system is used to display the runtime of the existing BMC system.

Format:

diagnose uptime

Parameters:

None

User Guide:

None

Examples:

# Obtain the runtime of the existing system.

```
/smashclp> diagnose uptime
 16:54:02 up 4 days,  1:48,  1 users,  load average: 4.06, 4.03, 4.09
```

5 Terms and Abbreviations

B	
BIOS	Basic Input Output System
BMC	Baseboard Management Controller
C	
CLI	Command-Line Interface
CLP	Command Line Protocol
CPU	Central Processing Unit
D	
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual-Inline-Memory-Modules
DNS	Domain Name System
F	
FMA	Failure Mode Analysis
G	
GPU	Graphics Processing Unit
GUI	Graphical User Interface
H	
HDD	Hard Disk Drive
HTML	Hyper Text Markup Language
I	
I/O	Input/Output
IOPS	Input/Output Operations Per Second
IPMI	Intelligent Platform Management Interface

M	
MC	Management Controller
N	
NIC	Network Interface Controller
NTP	Network Time Protocol
O	
OCP	Open Compute Project
P	
PCH	Platform Controller Hub
PCIe	Peripheral Component Interconnect express
PSU	Power Supply Unit
R	
RAID	Redundant Arrays of Independent Drives
RDIMM	Registered Dual In-line Memory Module
RST	Reset
S	
SATA	Serial Advanced Technology Attachment
SAS	Serial Attached SCSI
SMTP	Simple Mail Transfer Protocol
SMASH	Systems Management Architecture for Server Hardware
SNMP	Simple Network Management Protocol
SSD	Solid State Disk
SSH	Secure Shell
T	
TCO	Total Cost of Ownership
TDP	Thermal Design Power

U	
UEFI	Unified Extensible Firmware Interface
UID	User Identification
UPI	User Program Interface
USB	Universal Serial Bus

6 Appendix

6.1 BMC POST Codes

Table 6-1 Host POST Code

POST Code	Description
0x55	SFT_CODE_OK
0x56	SFT_CODE_NOT_IMPLEMENTED
0x57	SFT_CODE_DEV_CORRUPTED
0x58	SFT_CODE_FATAL_ERROR
0xff	SFT_CODE_RESERVED
0x80	SEL_ERROR
0x40	SDR_ERROR
0x20	FRU_ERROR
0x10	IPMB_ERROR
0x08	SDRR_EMPTY
0x04	INTERNAL_USE
0x02	FW_BOOTBLOCK
0x01	FW_CORRUPTED