Inspur BMC
Product Specification and User Guide

Revision History

Date	Revision Number	Author	Modifications
10/25/2017	1.0	Inspur	Initial Release
11/9/2017	1.1	Inspur	Add smashclp user privilege, update Users section
11/23/2017	1.2	Inspur	Change figure BMC Hardware Architecture Add cipher suites description Add section IPMI CMD Tool Add audit log details Modify bonding description Update section BIOS Boot Options Add note for Soft shutdown Update section Power Supply and Power Consumption Update section BMC Firmware Update

目录

1. Introduction

This Specification describes the functional specifications for the Baseboard Management Controller (BMC). It also describes the feature's detail information.
In addition to common features, for each platform, there will be a section that contains platform-specific information.
This document is written for software developer, system integrators, testers, server management users.

2. Server System Overview

BMC is an independent system of host server system. This independent system has its own processor and memory; the host system can be managed by BMC system even if host hardware or OS hang or went down.

2.1. Main Feature

- Support IPMI 2.0, IPMI Interface include KCS, Lan, IPMB
- Management Protocol,IPMI2.0, HTTPS, SNMP, Smash CLI
- Web GUI
- Redfish
- Management Network Interface, Dedicated/NCSI
- Console Redirection(KVM) and Virtual Media
- Serial Over Lan(SOL)
- Diagnostic Logs, System Event Log (SEL), Blackbox Log, Audit Log
- Hardware watchdog timer, Fans will full speed when BMC no response in 4 mins
- Intel® Intelligent Power Node Manager 4.0 support
- Event Alert, SNMP Trap(v1/v2c/v3), Email Alert and Syslog
- Dual BMC firmware image support
- Storage, Monitor RAID Controller/HDD/Virtual HDD
- Firmware update, BMC/BIOS/CPLD
- Device State Monitor and Diagnostic
- RAID Monitor/Configure

2.2. Integrated BMC Hardware

ASPEED AST2500 Baseboard Management Controller, at the center of the server management subsystem is the ASPEED AST2500 integrated Baseboard Management Controller. This device provides support for many platform functions including system video capabilities, legacy Super I/O functions, hardware monitoring functions, and incorporates an ARM1176JZF-S 32-bit RISC CPU microcontroller to host an IPMI 2.0 compliant server management firmware stack.

The following functionality is integrated into the component:

- **Baseboard Management Controller (BMC) with peripherals**
- **Server class Super I/O (SIO)**
- **Graphics controller**
- **Remote KVM redirection, USB media redirection, and HW Encryption**

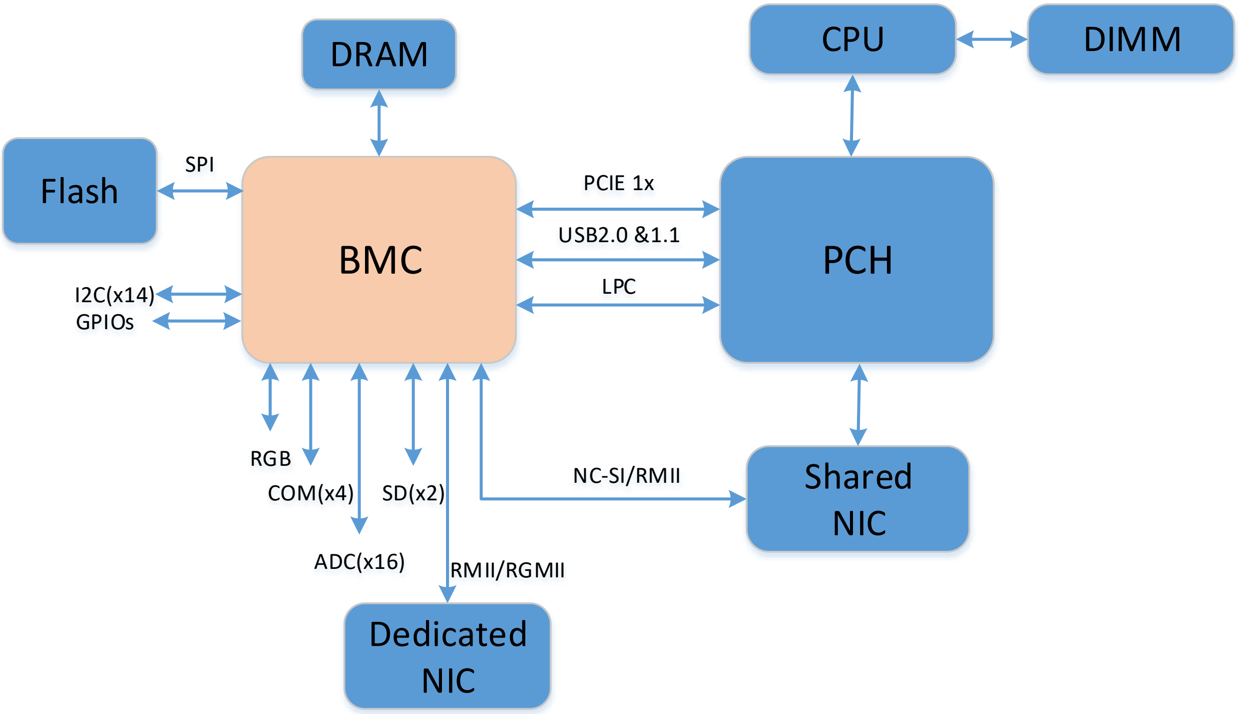


Figure 1 BMC Hardware Architecture

The eSPI/LPC interface to the host is used for SIO and BMC communication. The eSPI/LPC Bus interface provides IPMI Compliant KCS and BT interfaces.

The PCI Express interface is mainly used for the graphics controller interface to communicate with the host. The graphics controller is a VGA-compliant controller with 2D hardware acceleration and full bus master support. The graphics controller can support up to 1920x1200 32bpp@60Hz resolution at high refresh rates. The PCI Express interface is also used for BMC messaging to other system devices using MCTP protocol.

The USB 2.0 Hub interface is used for remote keyboard and mouse, and remote storage support. BMC supports various storage devices such as CDROM, DVDROM, CDROM (ISO image), floppy and USB flash disk. Any of the storage devices can be used as a boot device and the host can boot from this remote media via redirection over the USB interface.

For the main capabilities please refer to the AST2500 datasheet for more details.

3. IPMI2.0

3.1. Channel ID Assignment for each Interface

Table 1 Channel ID Assignment for each Interface

Channel ID	Interface	Support Sessions
0h	Primary IPMB	No
6h	Secondary IPMB	No
0Ah	Third IPMB	No
1h	Primary LAN	Yes
8h	Secondary LAN	Yes
0Fh	KCS / SMS	No

3.2. System Interface

AST2500 has an on-chip LPC interface. The LPC performs serial transfer of cycle type, address, and data, synchronized with the 33 MHz PCI clock. For IPMI application, LPC provides hardware path for KCS messaging.

3.3. IPMB Interface

BMC support one IPMB channel used to communicate with Intel NM. Now, **Secondary IPMB** is used.

3.4. LAN Interface

IPMI Specification v2.0 defines IPMI messages, encapsulated in RMCP/RMCP+ packet format, can be sent to and from the BMC.

BMC support up to 2 LAN Interface (Dedicated NIC and Shared NIC).

List of supported cipher suites in IPMI, user can use one of the suite to send IPMI CMD. If user sends IPMI CMD by ipmitool, default ID 3 suite is used, and user can specify cipher suite by option -C:

Table 2 Supported Cipher Suites in IPMI

ID	Authentication Algorithm	Integrity Algorithm	Confidentiality Algorithm
0	RAKP – NONE	NONE	NONE
1	RAKP-HMAC-SHA1	NONE	NONE
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
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

3.5. IPMI Commands

Tables below defines the IPMI commands supported by the BMC.
IPMI SPEC standard command：

Table 3 IPMI NetFn

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

Table 4 IPMI Spec Standard Command

IPMI Device “Global” Commands	NetFn	CMD	SUPPORT
Get Device ID	App	**01h**	YES
Broadcast ‘Get Device ID’ [1]	App	01h	YES
Cold Reset	App	02h	YES
Warm Reset	App	03h	YES
Get Self Test Results	App	04h	YES
Manufacturing Test On	App	05h	YES
Set ACPI Power State	App	06h	YES
Get ACPI Power State	App	07h	YES
Get Device GUID	App	08h	YES
Get NetFn Support	App	09h	YES
Get Command Support	App	0Ah	YES
Get Command Sub-function Support	App	0Bh	YES
Get Configurable Commands	App	0Ch	YES
Get Configurable Command Sub-functions	App	0Dh	YES
Set Command Enables	App	60h	YES
Get Command Enables	App	61h	YES
Set Command Sub-function Enables	App	62h	YES
Get Command Sub-function Enables	App	63h	YES
Get OEM NetFn IANA Support	App	64h	YES
BMC Watchdog Timer Commands			
Reset Watchdog Timer	App	22h	YES
Set Watchdog Timer	App	24h	YES
Get Watchdog Timer	App	25h	YES
BMC Device and Messaging Commands			
Set BMC Global Enables	App	2Eh	YES
Get BMC Global Enables	App	2Fh	YES
Clear Message Flags	App	30h	YES
Get Message Flags	App	31h	YES
Enable Message Channel Receive	App	32h	YES
Get Message	App	33h	YES
Send Message	App	34h	YES
Read Event Message Buffer	App	35h	YES
Get BT Interface Capabilities	App	36h	YES
Get System GUID	App	37h	YES
Set System Info Parameters	App	58h	YES
Get System Info Parameters	App	59h	YES
Get Channel Authentication Capabilities	App	38h	YES
Get Session Challenge	App	39h	YES

Activate Session	App	3Ah	YES
Set Session Privilege Level	App	3Bh	YES
Close Session	App	3Ch	YES
Get Session Info	App	3Dh	YES
Get AuthCode	App	3Fh	YES
Set Channel Access	App	40h	YES
Get Channel Access	App	41h	YES
Get Channel Info Command	App	42h	YES
Set User Access Command	App	43h	YES
Get User Access Command	App	44h	YES
Set User Name	App	45h	YES
Get User Name Command	App	46h	YES
Set User Password Command	App	47h	YES
Activate Payload	App	48h	YES
Deactivate Payload	App	49h	YES
Get Payload Activation Status	App	4Ah	YES
Get Payload Instance Info	App	4Bh	YES
Set User Payload Access	App	4Ch	YES
Get User Payload Access	App	4Dh	YES
Get Channel Payload Support	App	4Eh	YES
Get Channel Payload Version	App	4Fh	YES
Get Channel OEM Payload Info	App	50h	YES
Master Write-Read	App	52h	YES
Get Channel Cipher Suites	App	54h	YES
Suspend/Resume Payload Encryption	App	55h	YES
Set Channel Security Keys	App	56h	YES
Get System Interface Capabilities	App	57h	YES
Firmware Firewall Configuration	App	60h-64h	NO
Chassis Device Commands			
Get Chassis Capabilities	Chassis	00h	YES
Get Chassis Status	Chassis	01h	YES
Chassis Control	Chassis	02h	YES
Chassis Reset	Chassis	03h	YES
Chassis Identify	Chassis	04h	YES
Set Front Panel Button Enables	Chassis	0Ah	YES
Set Chassis Capabilities	Chassis	05h	YES
Set Power Restore Policy	Chassis	06h	YES
Set Power Cycle Interval	Chassis	0Bh	YES
Get System Restart Cause	Chassis	07h	YES
Set System Boot Options	Chassis	08h	YES
Get System Boot Options	Chassis	09h	YES
Get POH Counter	Chassis	0Fh	YES
Event Commands			
Set Event Receiver	S/E	00h	YES
Get Event Receiver	S/E	01h	YES
Platform Event (a.k.a. “Event Message”)	S/E	02h	YES

PEF and Alerting Commands			
Get PEF Capabilities	S/E	10h	YES
Arm PEF Postpone Timer	S/E	11h	YES
Set PEF Configuration Parameters	S/E	12h	YES
Get PEF Configuration Parameters	S/E	13h	YES
Set Last Processed Event ID	S/E	14h	YES
Get Last Processed Event ID	S/E	15h	YES
Alert Immediate	S/E	16h	YES
PET Acknowledge	S/E	17h	YES
Sensor Device Commands			
Get Device SDR Info	S/E	20h	YES
Get Device SDR	S/E	21h	YES
Reserve Device SDR Repository	S/E	22h	YES
Get Sensor Reading Factors	S/E	23h	YES
Set Sensor Hysteresis	S/E	24h	YES
Get Sensor Hysteresis	S/E	25h	YES
Set Sensor Threshold	S/E	26h	YES
Get Sensor Threshold	S/E	27h	YES
Set Sensor Event Enable	S/E	28h	YES
Get Sensor Event Enable	S/E	29h	YES
Re-arm Sensor Events	S/E	2Ah	YES
Get Sensor Event Status	S/E	2Bh	YES
Get Sensor Reading	S/E	2Dh	YES
Set Sensor Type	S/E	2Eh	YES
Get Sensor Type	S/E	2Fh	YES
Set Sensor Reading And Event Status	S/E	30h	YES
FRU Device Commands			
Get FRU Inventory Area Info	Storage	10h	YES
Read FRU Data	Storage	11h	YES
Write FRU Data	Storage	12h	YES
SDR Device Commands			
Get SDR Repository Info	Storage	20h	YES
Get SDR Repository Allocation Info	Storage	21h	YES
Reserve SDR Repository	Storage	22h	YES
Get SDR	Storage	23h	YES
Add SDR	Storage	24h	YES
Partial Add SDR	Storage	25h	YES
Delete SDR	Storage	26h	YES
Clear SDR Repository	Storage	27h	YES
Get SDR Repository Time	Storage	28h	YES
Set SDR Repository Time	Storage	29h	YES
Enter SDR Repository Update Mode	Storage	2Ah	YES
Exit SDR Repository Update Mode	Storage	2Bh	YES
Run Initialization Agent	Storage	2Ch	YES
SEL Device Commands			
Get SEL Info	Storage	40h	YES
Get SEL Allocation Info	Storage	41h	YES

Reserve SEL	Storage	42h	YES
Get SEL Entry	Storage	43h	YES
Add SEL Entry	Storage	44h	YES
Partial Add SEL Entry	Storage	45h	YES
Delete SEL Entry	Storage	46h	YES
Clear SEL	Storage	47h	YES
Get SEL Time	Storage	48h	YES
Set SEL Time	Storage	49h	YES
Get Auxiliary Log Status	Storage	5Ah	YES
Set Auxiliary Log Status	Storage	5Bh	YES
Get SEL Time UTC Offset	Storage	5Ch	YES
Set SEL Time UTC Offset	Storage	5Dh	YES
LAN Device Commands			
Set LAN Configuration Parameters	Transport	01h	YES
Get LAN Configuration Parameters	Transport	02h	YES
Suspend BMC ARPs	Transport	03h	YES
Get IP/UDP/RMCP Statistics	Transport	04h	NO
Serial/Modem Device Commands			
Set Serial/Modem Configuration	Transport	10h	YES
Get Serial/Modem Configuration	Transport	11h	YES
Set Serial/Modem Mux	Transport	12h	YES
Get TAP Response Codes	Transport	13h	NO
Set PPP UDP Proxy Transmit Data	Transport	14h	NO
Get PPP UDP Proxy Transmit Data	Transport	15h	NO
Send PPP UDP Proxy Packet	Transport	16h	NO
Get PPP UDP Proxy Receive Data	Transport	17h	NO
Serial/Modem Connection Active	Transport	18h	NO
Callback	Transport	19h	YES
Set User Callback Options	Transport	1Ah	YES
Get User Callback Options	Transport	1Bh	YES
Set Serial Routing Mux	Transport	1Ch	NO
SOL Activating	Transport	20h	NO
Set SOL Configuration Parameters	Transport	21h	YES
Get SOL Configuration Parameters	Transport	22h	YES
Command Forwarding Commands			
Forwarded Command	Bridge	30h	NO
Set Forwarded Commands	Bridge	31h	NO
Get Forwarded Commands	Bridge	32h	NO
Enable Forwarded Commands	Bridge	33h	NO
Bridge Management Commands (ICMB)			
Get Bridge State	Bridge	00h	NO
Set Bridge State	Bridge	01h	NO
Get ICMB Address	Bridge	02h	NO
Set ICMB Address	Bridge	03h	NO
Set Bridge ProxyAddress	Bridge	04h	NO
Get Bridge Statistics	Bridge	05h	NO
Get ICMB Capabilities	Bridge	06h	NO

Clear Bridge Statistics	Bridge	08h	NO
Get Bridge Proxy Address	Bridge	09h	NO
Get ICMB Connector Info	Bridge	0Ah	NO
Get ICMB Connection ID	Bridge	0Bh	NO
Send ICMB Connection ID	Bridge	0Ch	NO
Discovery Commands (ICMB)			
PrepareForDiscovery	Bridge	10h	NO
GetAddresses	Bridge	11h	NO
SetDiscovered	Bridge	12h	NO
GetChassisDeviceId	Bridge	13h	NO
SetChassisDeviceId	Bridge	14h	NO
Bridging Commands (ICMB)			
BridgeRequest	Bridge	20h	NO
BridgeMessage	Bridge	21h	NO
Event Commands (ICMB)			
GetEventCount	Bridge	30h	NO
SetEventDestination	Bridge	31h	NO
SetEventReceptionState	Bridge	32h	NO
SendICMBEventMessage	Bridge	33h	NO
GetEventDestination (optional)	Bridge	34h	NO
GetEventReceptionState (optional)	Bridge	35h	NO

3.6. IPMI CMD Tool

Normally, ipmitool is used to send IPMI cmd. ipmitool can be used in Host OS to send in-band IPMI CMD based on KCS interface, and can be used in remote PC to send IPMI CMD by Lan. ipmitool has Linux and Windows OS version.

Supported interface:

- OPEN interface, Linux OpenIPMI Interface, used to send in-band IPMI CMD in Linux OS.
- IMB interface, Intel IMB Interface, used to send bridge IPMI CMD to Intel ME.
- LAN interface, RMCP LAN interface, used to send out-band IPMI CMD to BMC.
- LANPLUS interface, RMCP+ LAN interface, RMCP+ allows for improved authentication and data integrity checks, as well as encryption and the ability to carry multiple types of payloads.

Options in ipmitool:

-a Prompt for the remote server password.

-A <authtype>

Specify an authentication type to use during IPMIv1.5 lan session activation. Supported types are NONE, PASSWORD, MD2, MD5, or OEM.

-b <channel>

Set destination channel for bridged request.

-B <channel>

Set transit channel for bridged request (dual bridge).

-b <channel>

Set destination channel for bridged request.

-B <channel>

Set transit channel for bridged request. (dual bridge)

-c Present output in CSV (comma separated variable) format. This is not available with all commands.

-C <ciphersuite>

The remote server authentication, integrity, and encryption algorithms to use for IPMIv2.0 lanplus connections. See table 22-19 in the IPMIv2.0 specification. The default is 3 which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.

-d N Use device number N to specify the /dev/ipmiN (or /dev/ipmi/N or /dev/ipmidev/N) device to use for in-band BMC communication.

Used to target a specific BMC on a multi-node, multi-BMC system through the ipmi device driver interface. Default is 0.

-e <sol_escape_char>

Use supplied character for SOL session escape character. The default is to use ~ but this can conflict with ssh sessions.

-E The remote server password is specified by the environment variable IPMI_PASSWORD or IPMITOOL_PASSWORD. The IPMITOOL_PASSWORD takes precedence.

-f <password_file>

Specifies a file containing the remote server password. If this option is absent, or if password_file is empty, the password will default to NULL.

-g Deprecated. Use: -o intelplus

-h Get basic usage help from the command line.

-H <address>

Remote server address, can be IP address or hostname. This option is required for lan and lanplus interfaces.

-I <interface>

Selects IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output.

-k <key>

Use supplied Kg key for IPMIv2.0 authentication. The default is not to use any Kg key.

-K Read Kg key from IPMI_KGKEY environment variable.

-l <lun>

Set destination lun for raw commands.

-L <privlvl>

Force session privilege level. Can be CALLBACK, USER, OPERATOR, ADMINISTRATOR. Default is ADMINISTRATOR. This value is ignored and always set to ADMINISTRATOR when combined with -t target address.

-m <local_address>

Set the local IPMB address. The local address defaults to 0x20 or is auto discovered on PICMG platforms when -m is not specified. There should be no need to change the local address for normal operation.

-N <sec>

Specify nr. of seconds between retransmissions of lan/lanplus messages. Defaults are 2 seconds for lan and 1 second for lanplus interfaces. Command raw uses fixed value of 15 seconds. Command sol uses fixed value of 1 second.

-o <oemtype>

Select OEM type to support. This usually involves minor hacks in place in the code to work around quirks in various BMCs from various manufacturers. Use -o list to see a list of current supported OEM types.

-O <sel oem>

Open selected file and read OEM SEL event descriptions to be used during SEL listings. See examples in contrib dir for file format.

-p <port>

Remote server UDP port to connect to. Default is 623.

-P <password>

Remote server password is specified on the command line. If supported it will be obscured in the process list. Note! Specifying the password as a command line option is not recommended.

-R <count>

Set the number of retries for lan/lanplus interface (default=4). Command raw uses fixed value of one try (no retries). Command hpm uses fixed value of 10 retries.

-s Deprecated. Use: -o supermicro

-S <sdr_cache_file>

Use local file for remote SDR cache. Using a local SDR cache can drastically increase performance for commands that require knowledge of the entire SDR to perform their function. Local SDR cache from a remote system can be created with the sdr dump command.

-t <target_address>

Bridge IPMI requests to the remote target address. Default is 32. The -L privlvl option is always ignored and value set to ADMINISTRATOR.

-T <address>
Set transit address for bridge request (dual bridge).

-T <transmit_address>
Set transit address for bridge request. (dual bridge)

-U <username>
Remote server username, default is NULL user.

-v Increase verbose output level. This option may be specified multiple times to increase the level of debug output. If given three times you will get hexdumps of all incoming and outgoing packets. Using it five times provides details on request andnexpected reply procesing. The hpm commands targetcap compprop abort upgstatus rollback rollbackstatus selftestresult increases the verbosity level

-V Display version information.

-y <hex key>
Use supplied Kg key for IPMIv2.0 authentication. The key is expected in hexadecimal format and can be used to specify keys with non-printable characters. E.g. '-k PASSWORD' and '-y 50415353574F5244' are equivalent. The default is not to use any Kg key.

-Y Prompt for the Kg key for IPMIv2.0 authentication.

-z <size>
Change Size of Communication Channel. (OEM)

Commands in ipmitool:

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
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

4. Management Web GUI

HTTPS(Port 443) is supported to access Management Web GUI. HTTP default disable, user can enable it by IPMI OEM CMD.

The Management Web GUI provides management interface for user to view the system information, system event and status, and to control the managed server.

The Management Web GUI is supported by following browsers:

Table 5 Supported Browsers

Client OS	Browser Versions
Windows 7.1 x64 Windows 8 x64 Windows 10 x64 Ubuntu 14.04.03 LTS x64 MAC OS X Fedora 23 x64 CentOS 7 x64	**On Windows Clients:** Edge ,Firefox 43, Chrome 47+, IE 11+ **On Linux Clients:** Firefox 43, Chrome 47+ **On MAC Client:** Safari

Step 1

Enter “https: // BMC_IP” in browser address bar. Port number is modifiable (see the "Services" section) and default the http port number is 80, https port number is 443. If you modify the port number, you need to specify the port number when login, such as https: // BMC_IP: sslport.

Step 2

In the WEB login interface, enter the user name and password, click the "Login" button to enter the home page, as the figure shows.

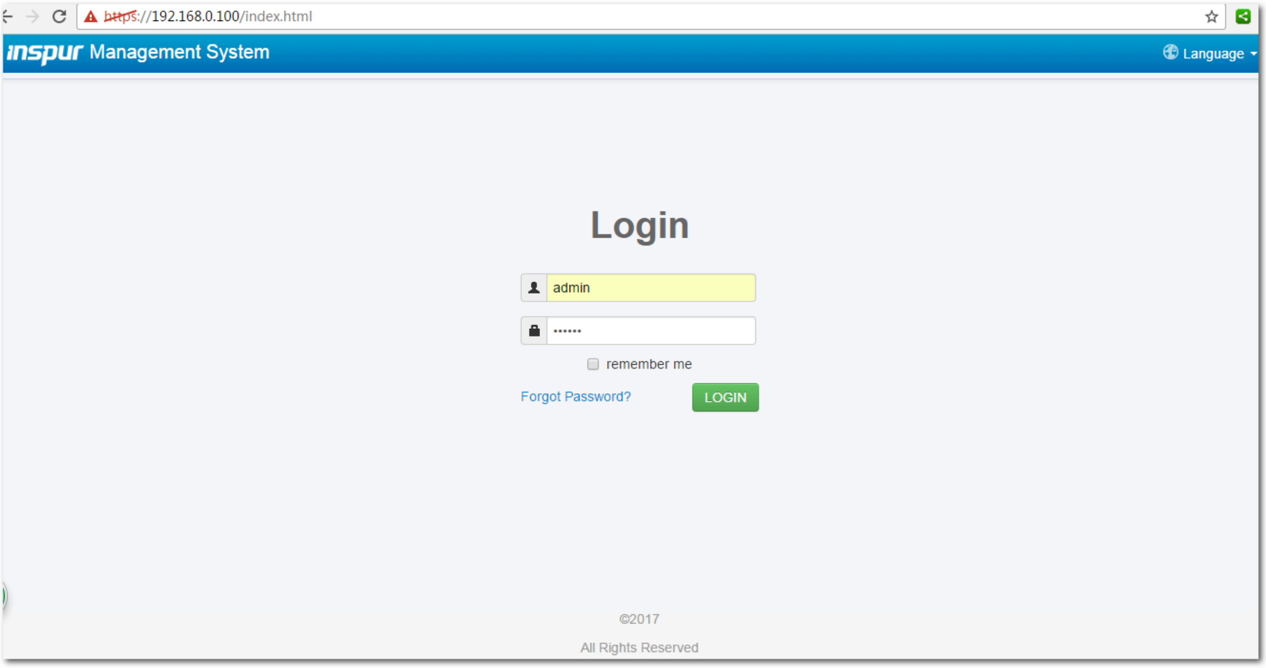


Figure 2 Web Login

When you forget password, you can click “Forgot Password?” link to get a new password by Email. The Email address MUST be configured in advance in “User management” page and configure SMPT server information in “SMTP” page.

Mean features supported in Web GUI.

Table 6 Features Supported in Web GUI.

Menus	Subdirectory	Auto Refresh Support	Main content
Overview Information	General Information	YES	System Running State
			BMC Information

			Quick Launch Tasks
			Active Session
			FW Version Information
			Recent System Event Log Information
Information	System Info	YES	Device asset info and health state, include: CPU Memory Device Inventory Network Hard Disk Power Supply Unit Fan Temperature Voltage
	BIOS Setup Options	NO	Display Main setup options
	History Record	YES	Last Day/Last Month/Last Year - Inlet history curve, and total power history curve, Current Power, Minimum Power, Maximum Power, Average Power
Storage	Controller	YES	RAID/SAS controller asset info and running state.
	Physical Drives	YES	Physical Drives lists， asset info and running state.
	Logical Drives	YES	Logical Drives lists, asset info and running state.
	Enclosure	YES	Topology of RAID/SAS controller.
Remote Control	Console Redirection	NO	HTML5 KVM; Java KVM ; Console Redirection Setting
	Locate Server	YES	Display UID status; Turn on/off UID.
	Virtual Media		Virtual Media settings
Power and Fan	Power Supply Monitor	YES	Display PSU present/health state, temperature, input/outputvoltage/current/power, firmware version.
	Power Supply Configure	YES	Manually Active/Standby switch
	Server Power Control	YES	Power on/off/soft off/reset/cycle Power Restore Setting
	Power Peak	NO	Server power on with random delay.
	Power Consumption	NO	Power limit setting.
	Fan Speed Control	YES	Display fan speed and state; Switch to manually fan control.
BMC Settings	BMC Network	NO	BMC Network Setting BMC DNS Setting Network Bonding Network Link Setting
	Services	NO	Supported service or protocol setting
	NTP	NO	BMC time setting
	SMTP	NO	SMTP setting for email alert
	Alerts	NO	SNMP Trap and email alert setting
	Threshold	NO	Threshold setting for sensors
	Access Control	NO	IP/MAC access limit policy.
	BMC Share NIC Switch	NO	NCSI NIC switch
	BIOS Boot Options	NO	BIOS Boot Options setting
Logs	System Event Log	YES	Display SEL
	BMC Audit Log	YES	Display audit Log

	Black Box Log	NO	Export Black Box Log
	Event Log Setting	NO	SEL Log store policy setting
	BMC Syslog Setting	NO	BMC Syslog setting
Fault Diagnosis	BMC Self-inspection Result	YES	Display BMC self-inspection result
	BMC Recovery	NO	Manually reset BMC or KVM.
	Capture Screen	NO	Auto Capture and Manual Capture
	Host POST Code	YES	Display current and history POST code
Administration	User Administration	NO	Local Users setting BMC System Administrator Directory Group setting
	Security	NO	LDAP setting AD setting
	Dual Image configuration	NO	Set image start order
	BMC Firmware Update	NO	Upgrade BMC firmware
	BIOS Firmware Update	NO	Upgrade BIOS firmware
	CPLD Update	NO	Upgrade CPLD
	Restore Factory Defaults	NO	Restore BMC settings to factory defaults

5. SNMP

Simple Network Management Protocol (SNMP), consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. It is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

In the BMC, the agent can obtain the server information such as network information, user information, temperature / voltage / fan speed and so on through the SNMP service. At the same time we can parameter configure parameters and manage the server through BMC.

- Support SNMP Get/Set/Trap
- Support V1/V2C/V3 version
- SNMPv3 support authentication algorithm MD5 or SHA, and encryption algorithm to DES or AES
- SNMP Get support query system health status, sensor status, hardware status, device asset information, etc.
- SNMP Set support local users or network user to switch machine and other operations.
- SNMP Trap supports IPM-based Trap messages

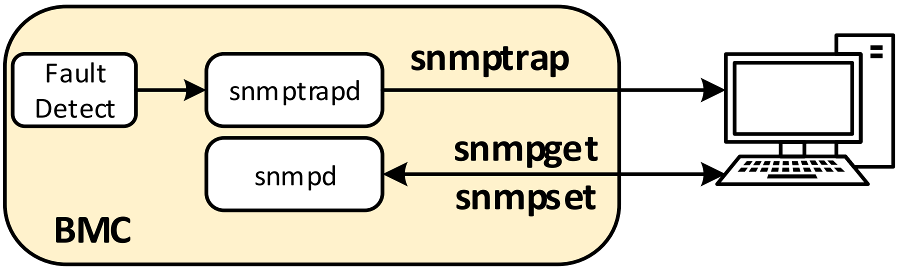
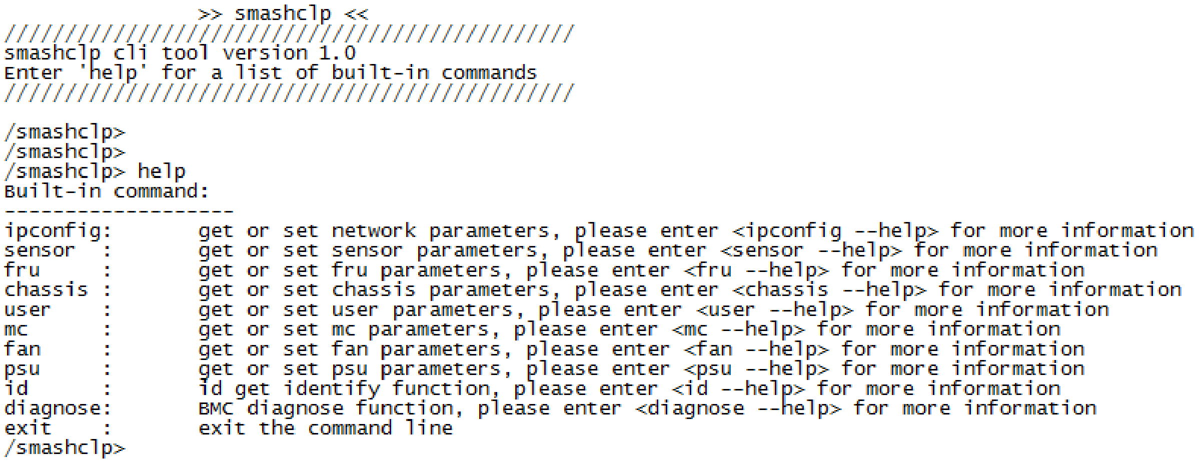


Figure 3 SNMP Schematic

6. Smashclp CLI

BMC support Smashclp CLI, users can login to BMC via SSH and enter Smashclp CLI. And it support ipconfig, sensor, fru, chassis, user, mc, fan, psu, id, diagnose commands, as the figure shows.

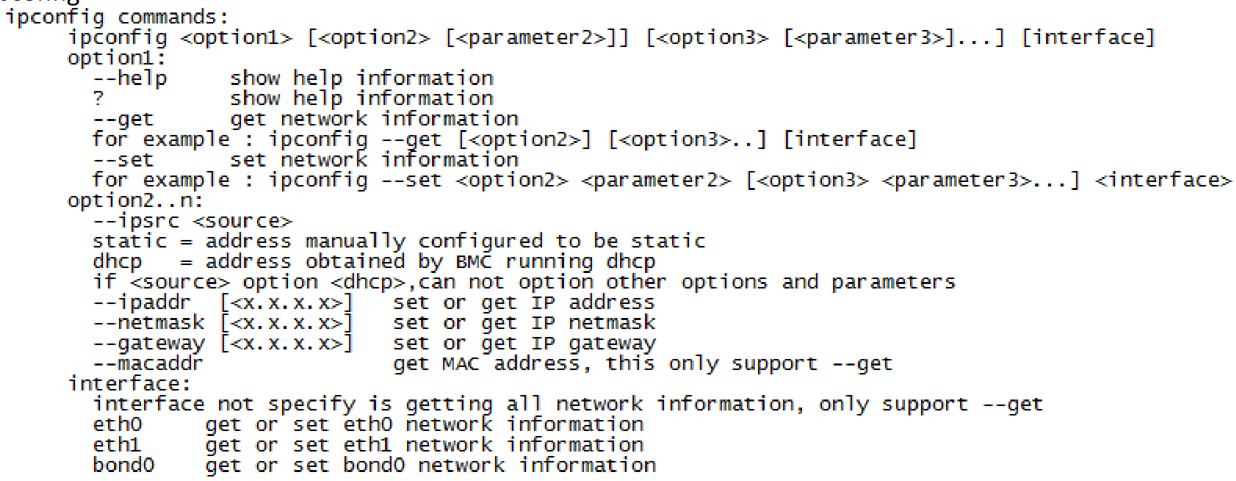
- Smashclp help:



```
                >> smashclp <<
///////////////////////////////////////////////
smashclp cli tool version 1.0
Enter 'help' for a list of built-in commands
///////////////////////////////////////////////

/smashclp>
/smashclp>
/smashclp> help
Built-in command:
-------------------
ipconfig:       get or set network parameters, please enter <ipconfig --help> for more information
sensor  :       get or set sensor parameters, please enter <sensor --help> for more information
fru     :       get or set fru parameters, please enter <fru --help> for more information
chassis :       get or set chassis parameters, please enter <chassis --help> for more information
user    :       get or set user parameters, please enter <user --help> for more information
mc      :       get or set mc parameters, please enter <mc --help> for more information
fan     :       get or set fan parameters, please enter <fan --help> for more information
psu     :       get or set psu parameters, please enter <psu --help> for more information
id      :       id get identify function, please enter <id --help> for more information
diagnose:       BMC diagnose function, please enter <diagnose --help> for more information
exit    :       exit the command line
/smashclp>
```

Figure 4 Smash Help

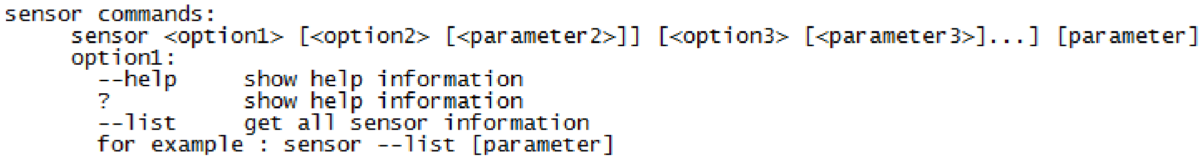
- Ipconfig



```
 ipconfig commands:
      ipconfig <option1> [<option2> [<parameter2>]] [<option3> [<parameter3>]...] [interface]
      option1:
        --help      show help information
        ?           show help information
        --get       get network information
        for example : ipconfig --get [<option2>] [<option3>..] [interface]
        --set       set network information
        for example : ipconfig --set <option2> <parameter2> [<option3> <parameter3>...] <interface>
      option2..n:
        --ipsrc <source>
        static = address manually configured to be static
        dhcp   = address obtained by BMC running dhcp
        if <source> option <dhcp>,can not option other options and parameters
        --ipaddr  [<x.x.x.x>]     set or get IP address
        --netmask [<x.x.x.x>]     set or get IP netmask
        --gateway [<x.x.x.x>]     set or get IP gateway
        --macaddr                 get MAC address, this only support --get
      interface:
        interface not specify is getting all network information, only support --get
        eth0     get or set eth0 network information
        eth1     get or set eth1 network information
        bond0    get or set bond0 network information
```

Figure 5 Ipconfig

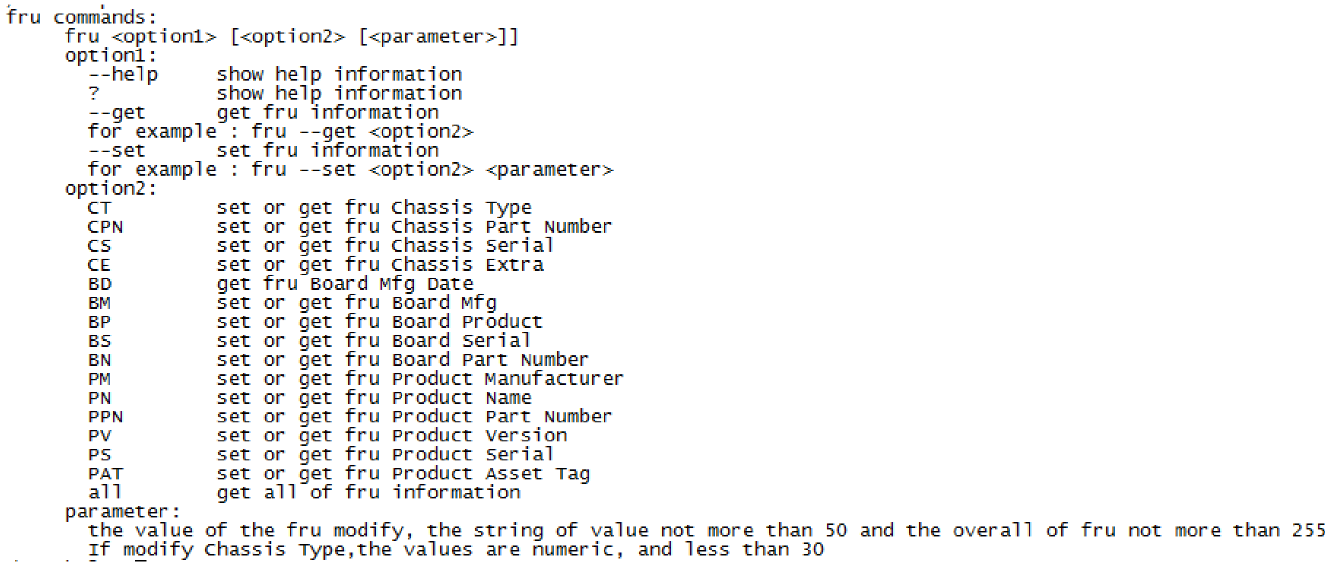
- sensor



```
sensor commands:
     sensor <option1> [<option2> [<parameter2>]] [<option3> [<parameter3>]...] [parameter]
     option1:
       --help      show help information
       ?           show help information
       --list      get all sensor information
       for example : sensor --list [parameter]
```

Figure 6 Sensor

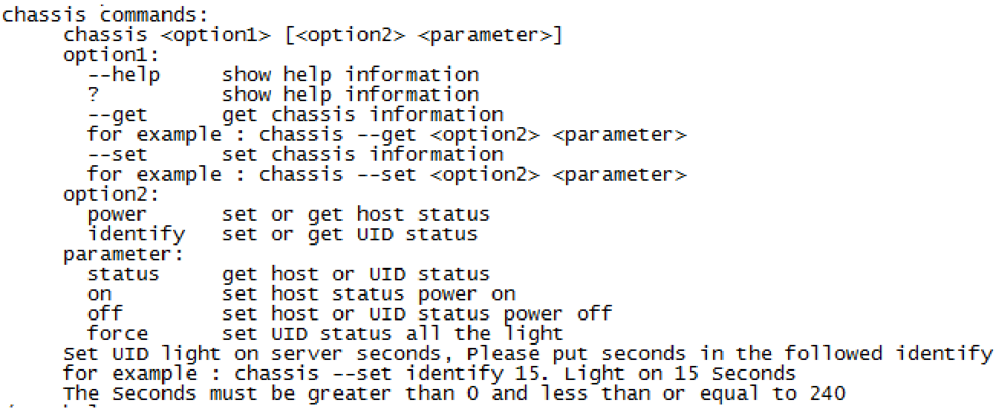
- fru



```
fru commands:
     fru <option1> [<option2> [<parameter>]]
     option1:
       --help      show help information
       ?           show help information
       --get       get fru information
       for example : fru --get <option2>
       --set       set fru information
       for example : fru --set <option2> <parameter>
     option2:
       CT          set or get fru Chassis Type
       CPN         set or get fru Chassis Part Number
       CS          set or get fru Chassis Serial
       CE          set or get fru Chassis Extra
       BD          get fru Board Mfg Date
       BM          set or get fru Board Mfg
       BP          set or get fru Board Product
       BS          set or get fru Board Serial
       BN          set or get fru Board Part Number
       PM          set or get fru Product Manufacturer
       PN          set or get fru Product Name
       PPN         set or get fru Product Part Number
       PV          set or get fru Product Version
       PS          set or get fru Product Serial
       PAT         set or get fru Product Asset Tag
       all         get all of fru information
     parameter:
       the value of the fru modify, the string of value not more than 50 and the overall of fru not more than 255
       If modify Chassis Type,the values are numeric, and less than 30
```

Figure 7 Fru

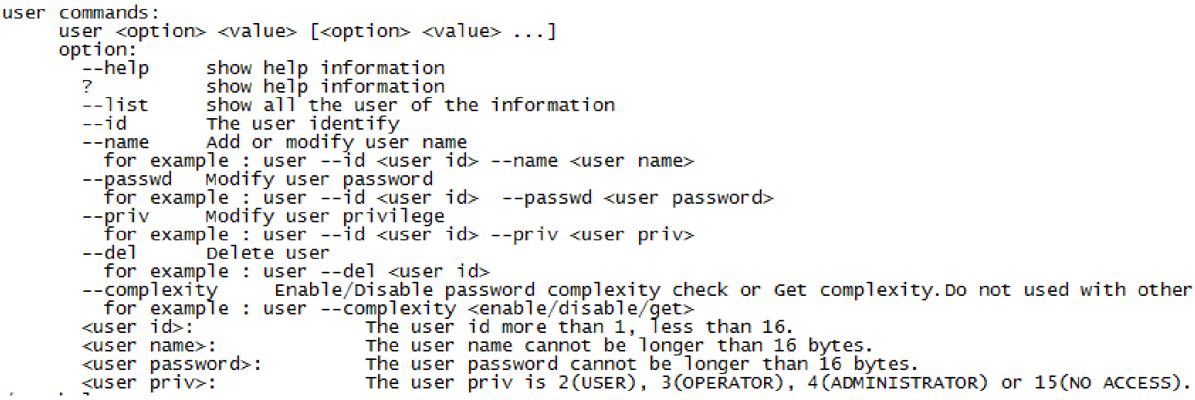
- chassis



```
chassis commands:
     chassis <option1> [<option2> <parameter>]
     option1:
       --help      show help information
       ?           show help information
       --get       get chassis information
       for example : chassis --get <option2> <parameter>
       --set       set chassis information
       for example : chassis --set <option2> <parameter>
     option2:
       power       set or get host status
       identify    set or get UID status
     parameter:
       status      get host or UID status
       on          set host status power on
       off         set host or UID status power off
       force       set UID status all the light
     set UID light on server seconds, Please put seconds in the followed identify
     for example : chassis --set identify 15. Light on 15 Seconds
     The Seconds must be greater than 0 and less than or equal to 240
```

Figure 8 Chassis

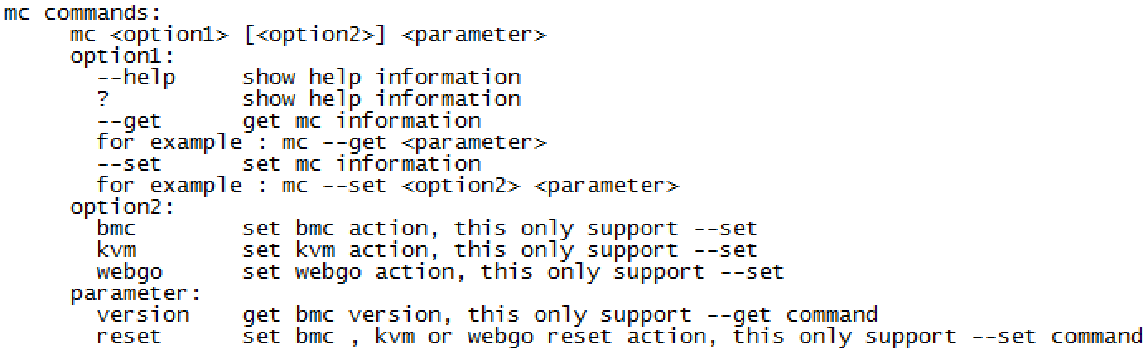
- user



```
user commands:
     user <option> <value> [<option> <value> ...]
     option:
       --help      show help information
       ?           show help information
       --list      show all the user of the information
       --id        The user identify
       --name      Add or modify user name
         for example : user --id <user id> --name <user name>
       --passwd    Modify user password
         for example : user --id <user id>  --passwd <user password>
       --priv      Modify user privilege
         for example : user --id <user id> --priv <user priv>
       --del       Delete user
         for example : user --del <user id>
       --complexity     Enable/Disable password complexity check or Get complexity.Do not used with other
         for example : user --complexity <enable/disable/get>
       <user id>:              The user id more than 1, less than 16.
       <user name>:            The user name cannot be longer than 16 bytes.
       <user password>:        The user password cannot be longer than 16 bytes.
       <user priv>:            The user priv is 2(USER), 3(OPERATOR), 4(ADMINISTRATOR) or 15(NO ACCESS).
```

Figure 9 User

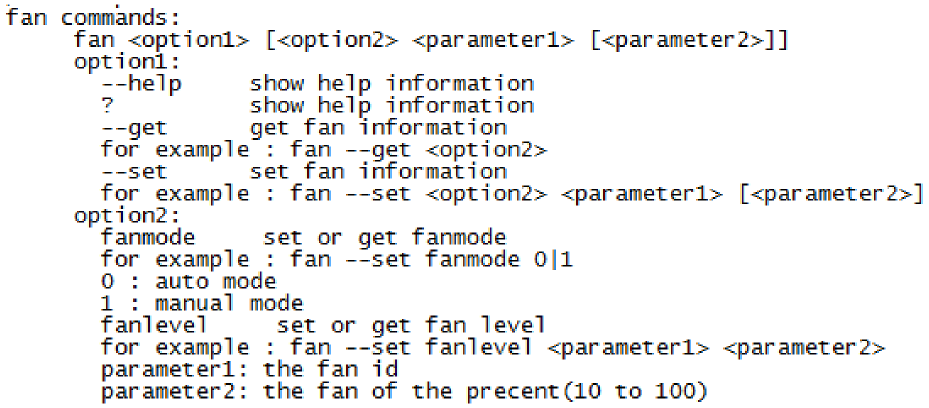
- mc



```
mc commands:
     mc <option1> [<option2>] <parameter>
     option1:
       --help      show help information
       ?           show help information
       --get       get mc information
       for example : mc --get <parameter>
       --set       set mc information
       for example : mc --set <option2> <parameter>
     option2:
       bmc         set bmc action, this only support --set
       kvm         set kvm action, this only support --set
       webgo       set webgo action, this only support --set
     parameter:
       version     get bmc version, this only support --get command
       reset       set bmc , kvm or webgo reset action, this only support --set command
```

Figure 10 MC

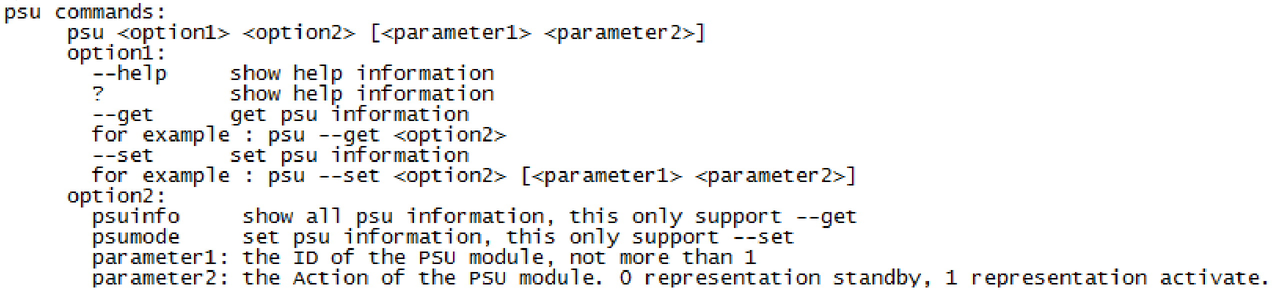
- fan



```
fan commands:
     fan <option1> [<option2> <parameter1> [<parameter2>]]
     option1:
       --help      show help information
       ?           show help information
       --get       get fan information
       for example : fan --get <option2>
       --set       set fan information
       for example : fan --set <option2> <parameter1> [<parameter2>]
     option2:
       fanmode      set or get fanmode
       for example : fan --set fanmode 0|1
       0 : auto mode
       1 : manual mode
       fanlevel      set or get fan level
       for example : fan --set fanlevel <parameter1> <parameter2>
       parameter1: the fan id
       parameter2: the fan of the precent(10 to 100)
```

Figure 11 Fan

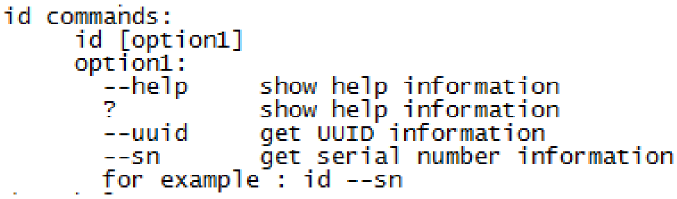
- psu



```
psu commands:
     psu <option1> <option2> [<parameter1> <parameter2>]
     option1:
       --help      show help information
       ?           show help information
       --get       get psu information
       for example : psu --get <option2>
       --set       set psu information
       for example : psu --set <option2> [<parameter1> <parameter2>]
     option2:
       psuinfo      show all psu information, this only support --get
       psumode      set psu information, this only support --set
       parameter1: the ID of the PSU module, not more than 1
       parameter2: the Action of the PSU module. 0 representation standby, 1 representation activate.
```

Figure 12 Psu

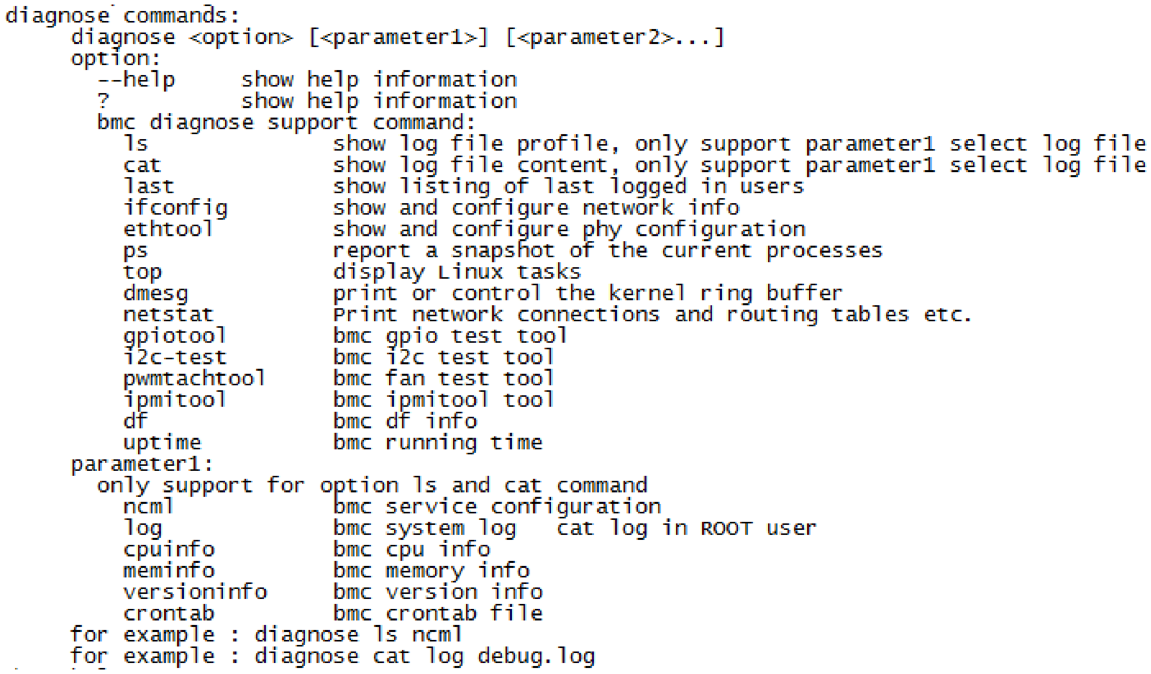
- id



```
id commands:
     id [option1]
     option1:
       --help      show help information
       ?           show help information
       --uuid      get UUID information
       --sn        get serial number information
       for example : id --sn
```

Figure 13 Id

- diagnose



```
diagnose commands:
     diagnose <option> [<parameter1>] [<parameter2>...]
     option:
       --help      show help information
       ?           show help information
       bmc diagnose support command:
         ls               show log file profile, only support parameter1 select log file
         cat              show log file content, only support parameter1 select log file
         last             show listing of last logged in users
         ifconfig         show and configure network info
         ethtool          show and configure phy configuration
         ps               report a snapshot of the current processes
         top              display Linux tasks
         dmesg            print or control the kernel ring buffer
         netstat          Print network connections and routing tables etc.
         gpiotool         bmc gpio test tool
         i2c-test         bmc i2c test tool
         pwmtachtool      bmc fan test tool
         ipmitool         bmc ipmitool tool
         df               bmc df info
         uptime           bmc running time
     parameter1:
       only support for option ls and cat command
         ncml             bmc service configuration
         log              bmc system log   cat log in ROOT user
         cpuinfo          bmc cpu info
         meminfo          bmc memory info
         versioninfo      bmc version info
         crontab          bmc crontab file
     for example : diagnose ls ncml
     for example : diagnose cat log debug.log
```

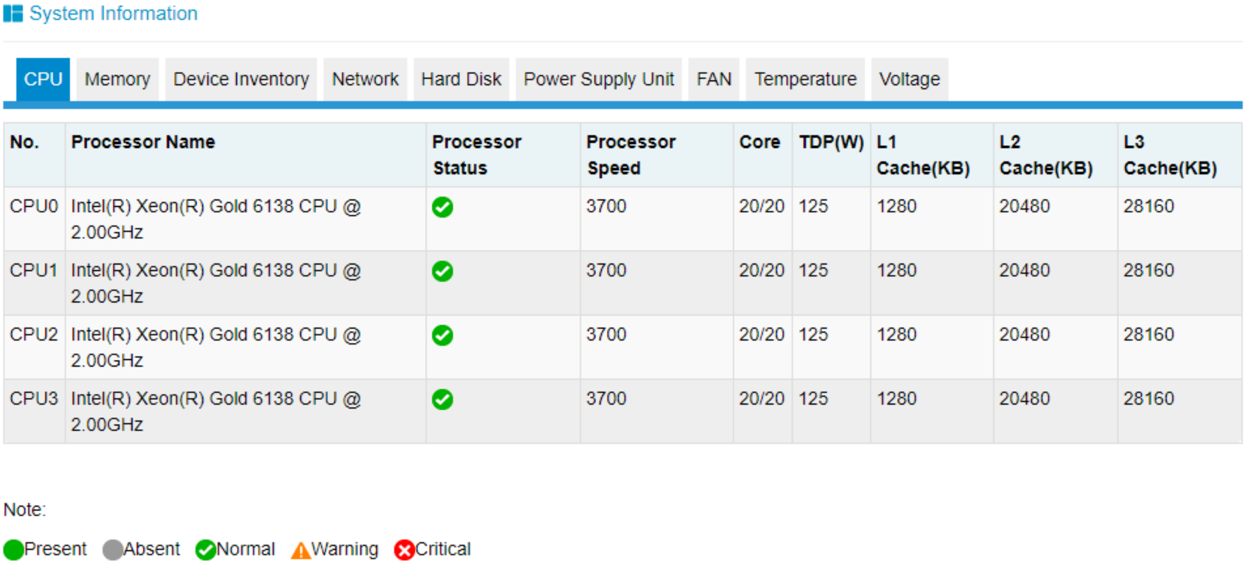
Figure 14 Diagnose

7. System Information and State

Login WEB GUI, go to page “Information->System Information”, this page displays information and health status of main components of platform, including CPU, Memory, PCIE Device, Network, Hard Disk Backplane, Power Supply Unit, Fan, Temperature, and Voltage.

7.1. CPU

Go to table “CPU” in System Information page.



No.	Processor Name	Processor Status	Processor Speed	Core	TDP(W)	L1 Cache(KB)	L2 Cache(KB)	L3 Cache(KB)
CPU0	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	✓	3700	20/20	125	1280	20480	28160
CPU1	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	✓	3700	20/20	125	1280	20480	28160
CPU2	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	✓	3700	20/20	125	1280	20480	28160
CPU3	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	✓	3700	20/20	125	1280	20480	28160

Note:

● Present ● Absent ✓ Normal ⚠ Warning ✖ Critical

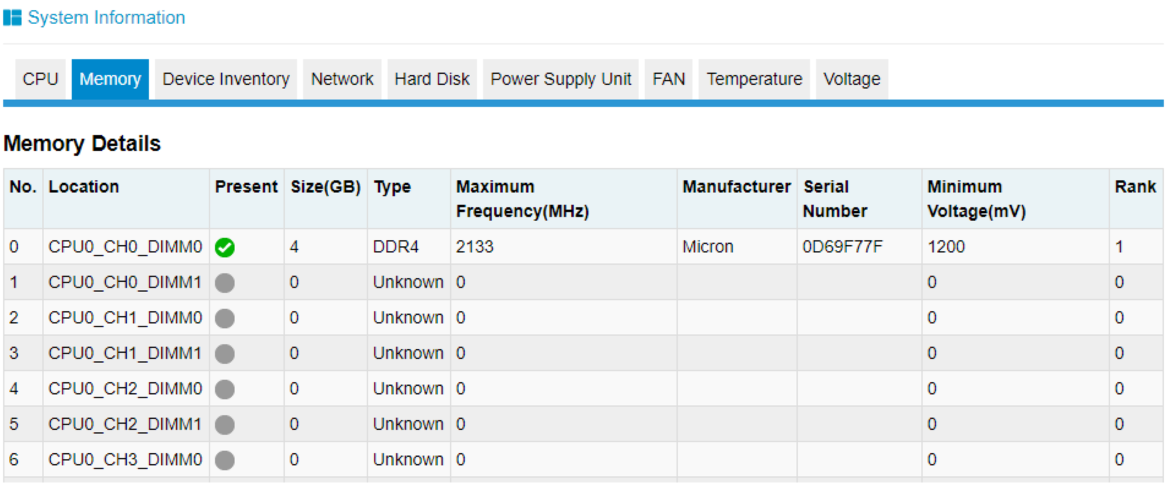
Figure 15 CPU Information

Table 7 CPU Information.

Attribute	Value
No.	CPUx, x is CPU No. based 0.
Processor Name	Product Model
Processor Status	✓ Normal State ⚠ Warning State ✖ Critical State ● State unavailable or current power is off. The State depends on CPUx_Status sensors.
Processor Speed(MHz)	Processor Speed
Core	x/y, x is Current Used Core Number, y is All Core Number
TDP	Rated Power
L1 Cache(KB)	L1 Cache
L2 Cache(KB)	L2 Cache
L3 Cache(KB)	L3 Cache

7.2. Memory

Go to table “Memory” in System Information page.



Memory Details

No.	Location	Present	Size(GB)	Type	Maximum Frequency(MHz)	Manufacturer	Serial Number	Minimum Voltage(mV)	Rank
0	CPU0_CH0_DIMM0	✓	4	DDR4	2133	Micron	0D69F77F	1200	1
1	CPU0_CH0_DIMM1	●	0	Unknown	0			0	0
2	CPU0_CH1_DIMM0	●	0	Unknown	0			0	0
3	CPU0_CH1_DIMM1	●	0	Unknown	0			0	0
4	CPU0_CH2_DIMM0	●	0	Unknown	0			0	0
5	CPU0_CH2_DIMM1	●	0	Unknown	0			0	0
6	CPU0_CH3_DIMM0	●	0	Unknown	0			0	0

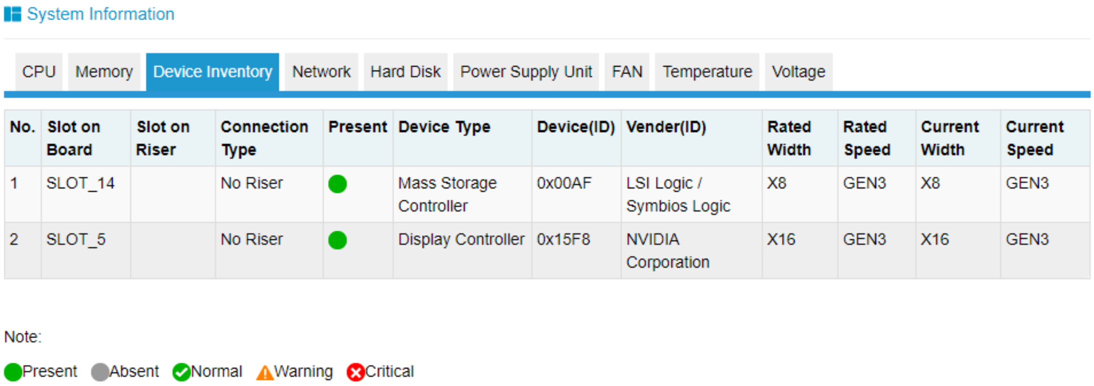
Figure 16 Memory Information

Table 8 Memory Information.

Attribute	Value
No.	x, x denotes the number of Memory.
Location	CPUx_CHy_DIMMz， x, y, z are based 0.
Present	✓ Normal State ⚠ Warning State ✖ Critical State ● Absent or power is off. The State depends on CPUx_CHy_DIMMz sensors
Size(GB)	Size of memory
Type	DDR3 or DDR4
Maximum Frequency(MHz)	Maximum Frequency
Manufacture	Manufacture
Serial Number	Serial Number
Rank	Rank

7.3. PCIE Devices

Go to table “PCIE Devices” in System Information page.



No.	Slot on Board	Slot on Riser	Connection Type	Present	Device Type	Device(ID)	Vender(ID)	Rated Width	Rated Speed	Current Width	Current Speed
1	SLOT_14		No Riser	●	Mass Storage Controller	0x00AF	LSI Logic / Symbios Logic	X8	GEN3	X8	GEN3
2	SLOT_5		No Riser	●	Display Controller	0x15F8	NVIDIA Corporation	X16	GEN3	X16	GEN3

Note:

● Present ● Absent ✓ Normal ⚠ Warning ✖ Critical

Figure 17 PCIE Information

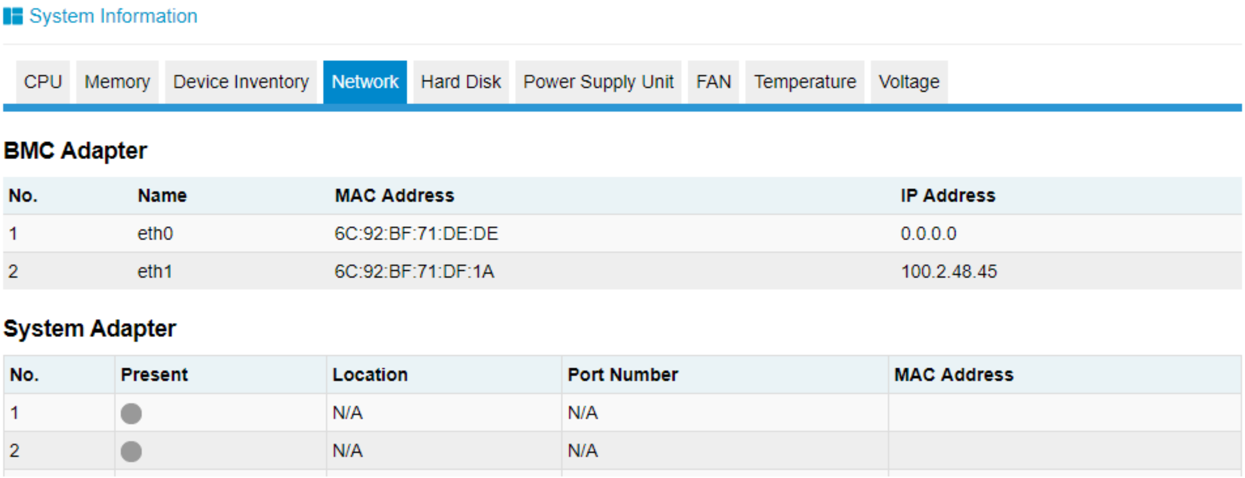
Table 9 PCIE Information.

Attribute	Value
No.	x, x is PCIE device number based 0.
Slot on Board	Onboard slot number where device is located.
Slot on Riser	Riser slot number where the device is located.
Connection Type	Connection Type.
Present	● Present

	● Absent or power is off.
Device Type	Device Type
Device(ID)	Device ID
Vender(ID)	Vendor ID
Rated Width	Rated Width
Rated Speed	Rated Speed
Current Width	Current Width
Current Speed	Current Speed

7.4. Network

Go to table “Network” in System Information page.



BMC Adapter

No.	Name	MAC Address	IP Address
1	eth0	6C:92:BF:71:DE:DE	0.0.0.0
2	eth1	6C:92:BF:71:DF:1A	100.2.48.45

System Adapter

No.	Present	Location	Port Number	MAC Address
1	●	N/A	N/A	
2	●	N/A	N/A	

Figure 18 Network Information

Table 10 BMC Adapter

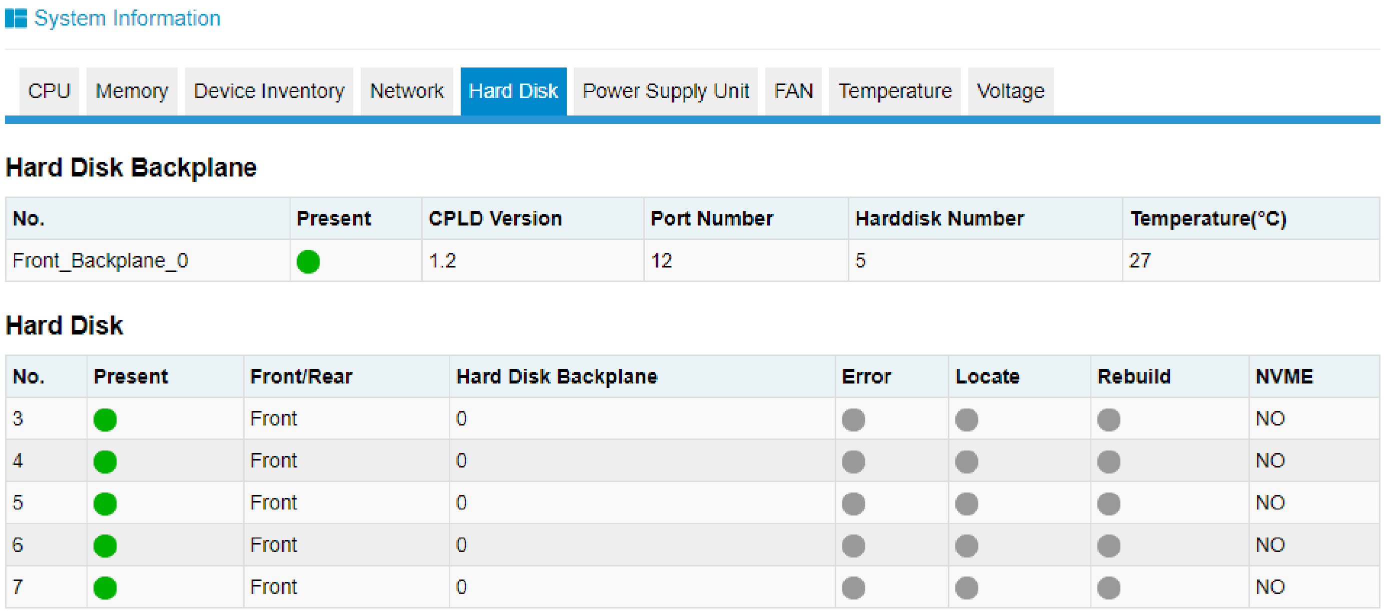
Attribute	Value
No.	x, x denotes the device number.
Name	eth0 or eth1
MAC Address	Mac Address
IP Address	IP Address
Status	●Link up ●Link down

Table 11 System Adapter

Attribute	Value
No.	x, x denotes the device number.
Present	●Present ●Absent
Location	Location
Port Number	Port Number
MAC Address	MAC Address

7.5. Hard Disk

Go to table “Hard Disk” in System Information page.



Hard Disk Backplane

No.	Present	CPLD Version	Port Number	Harddisk Number	Temperature(°C)
Front_Backplane_0	🟢	1.2	12	5	27

Hard Disk

No.	Present	Front/Rear	Hard Disk Backplane	Error	Locate	Rebuild	NVME
3	🟢	Front	0	●	●	●	NO
4	🟢	Front	0	●	●	●	NO
5	🟢	Front	0	●	●	●	NO
6	🟢	Front	0	●	●	●	NO
7	🟢	Front	0	●	●	●	NO

Figure 19 Hard Disk Information

Table 12 Hard Disk Backplane

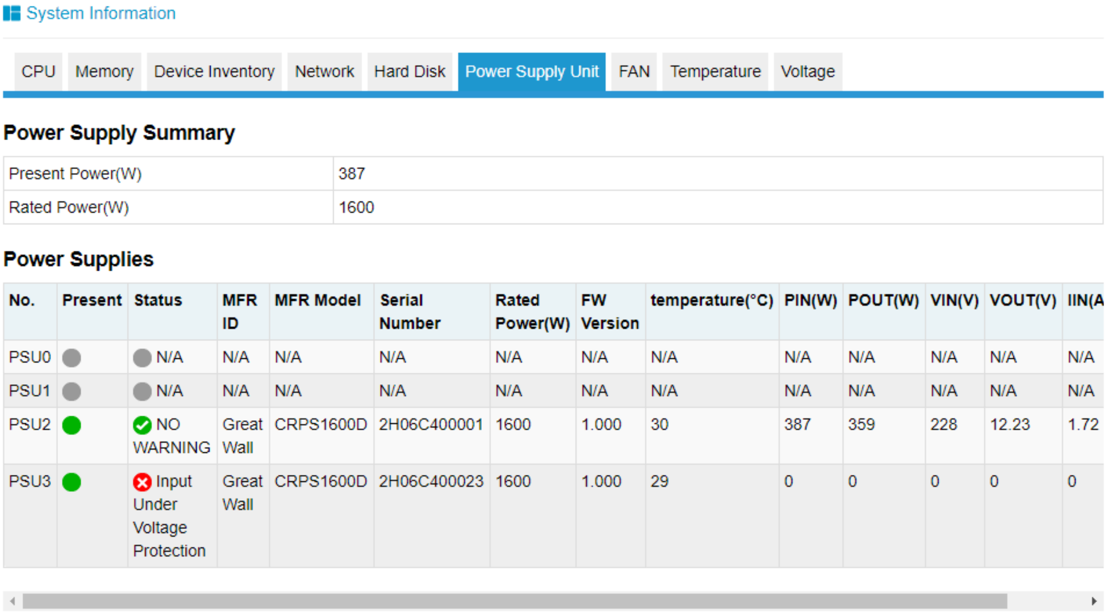
Attribute	Value
No.	x, x denotes the device number.
Present	🟢Present ●Absent
Port Number	Port Number
Hard disk Number	Hard disk Number

Table 13 Hard Disk

Attribute	Value
No.	x, x denotes the device number.
Present	🟢Present ●Absent
Front/Rear	Hard disk location, front or rear.
Hard Disk Backplane	Hard Disk Backplane Number
Error	✅ Normal State ❌ Error State ●Absent
Locate	🟢 Locating ●Absent or Non Locate
Rebuild	🟢 Rebuilding ●Absent or Non Locate
NVME	YES or NO, NVME or not.

7.6. Power Supply Summary

Go to table “Power Supply Unit” in System Information page.



Power Supply Summary

Present Power(W)	387
Rated Power(W)	1600

Power Supplies

No.	Present	Status	MFR ID	MFR Model	Serial Number	Rated Power(W)	FW Version	temperature(°C)	PIN(W)	POUT(W)	VIN(V)	VOUT(V)	IIN(A
PSU0	●	● N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PSU1	●	● N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
PSU2	●	✓ NO WARNING	Great Wall	CRPS1600D	2H06C400001	1600	1.000	30	387	359	228	12.23	1.72
PSU3	●	✗ Input Under Voltage Protection	Great Wall	CRPS1600D	2H06C400023	1600	1.000	29	0	0	0	0	0

Figure 20 Power Supply Unit Information

Table 14 Power Supply Summary

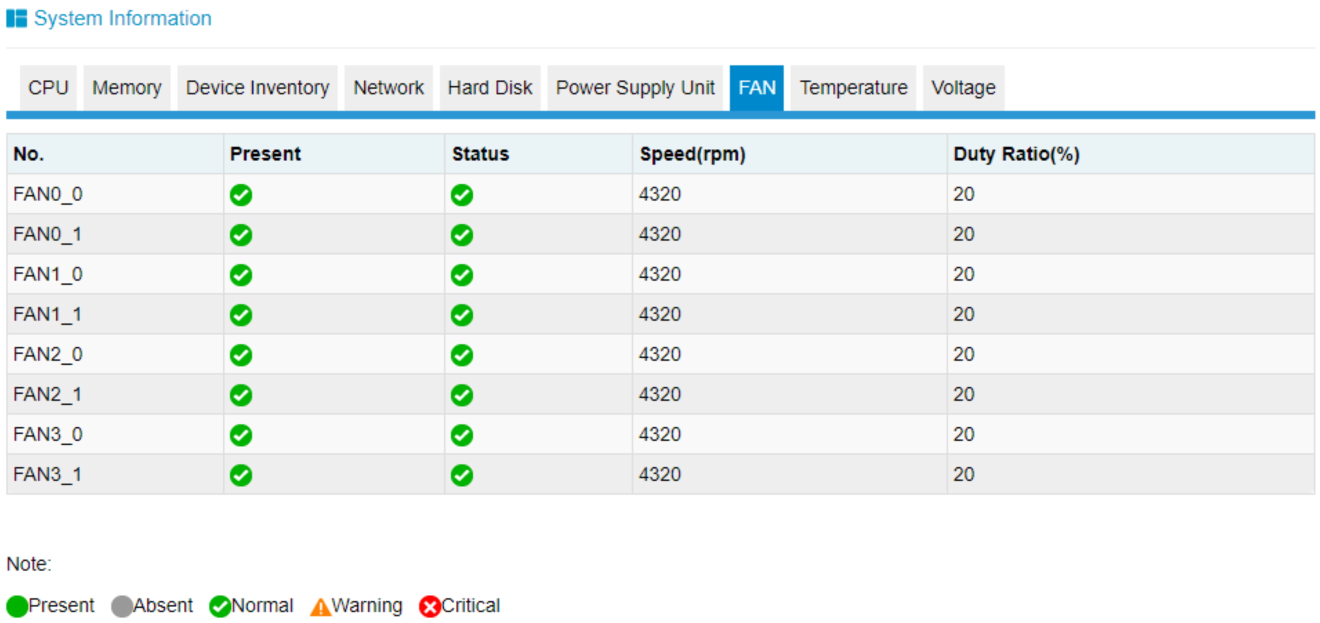
Attribute	**Value**
Present Power(W)	Total Power
Rated Power(W)	Rated Power
Power Status	Error Status

Table 15 Power Supplies

Attribute	**Value**
No.	PSUx, x denotes the power supply number
Present	● Present ● Absent
Status	Error Status, depends on PMBus Status Word command, 97h.
MFR ID	Manufacture ID
MFR Model	Manufacture Model
Serial Number	Serial Number
Rated Power(W)	Rated Power
FW Version	Firmware Version
Temperature(°C)	Temperature
PIN(W)	Input Power
POUT(W)	Output Power
VIN(V)	Input Voltage
VOUT(V)	Output Voltage
IIN(A)	Input current
IOUT(A)	Output current

7.7. FAN

Go to table “FAN” in System Information page.



System Information

No.	Present	Status	Speed(rpm)	Duty Ratio(%)
FAN0_0	✓	✓	4320	20
FAN0_1	✓	✓	4320	20
FAN1_0	✓	✓	4320	20
FAN1_1	✓	✓	4320	20
FAN2_0	✓	✓	4320	20
FAN2_1	✓	✓	4320	20
FAN3_0	✓	✓	4320	20
FAN3_1	✓	✓	4320	20

Note:

●Present ●Absent ✓Normal ⚠Warning ✗Critical

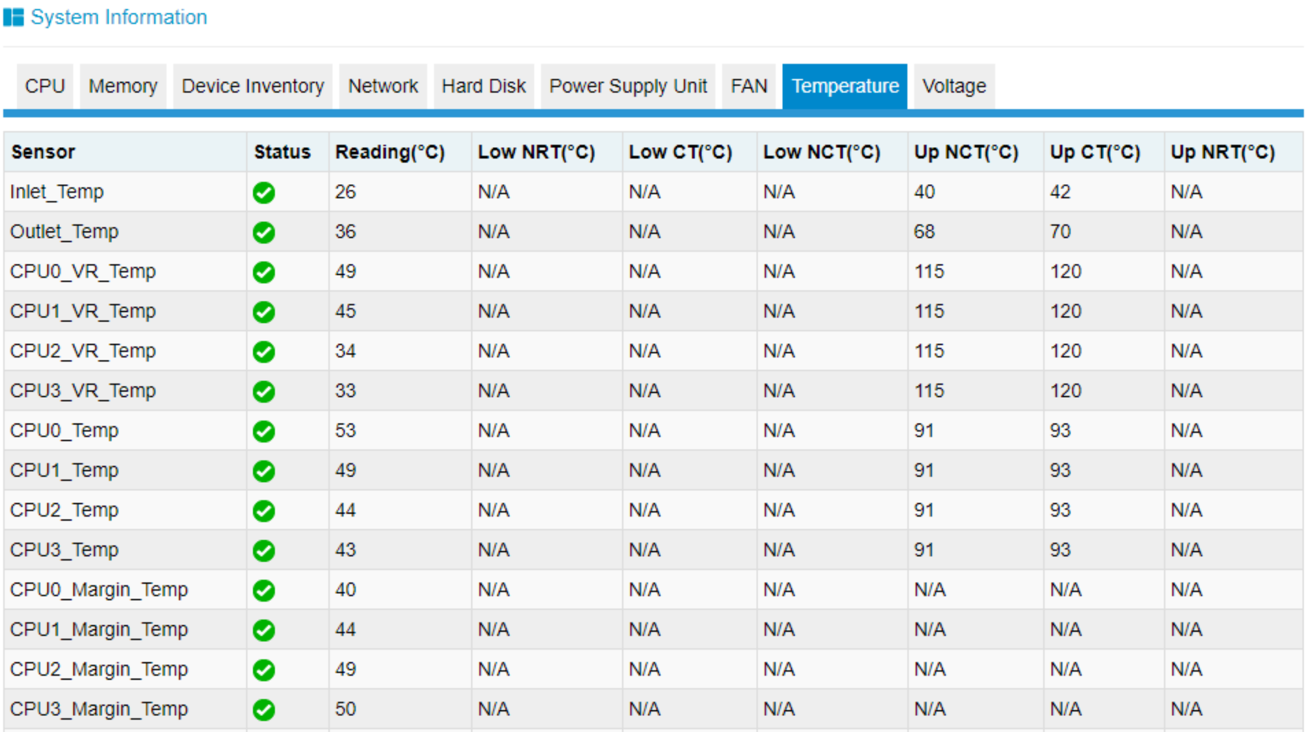
Figure 21 Fan Information

Table 16 Fan Information

Attribute	Value
No.	FANx_y, x denotes FAN or FAN group number, y denotes FAN number in group.
Present	●Present ●Absent
Status	✓ Normal State ✗ Critical State ● State unavailable or current power is off.
Speed(rpm)	Speed in rpm
Duty Ratio(%)	Speed in duty
Fan Power(Optional)	All FANs total power

7.8. Temperature

Go to table “Temperature” in System Information page.



Sensor	Status	Reading(°C)	Low NRT(°C)	Low CT(°C)	Low NCT(°C)	Up NCT(°C)	Up CT(°C)	Up NRT(°C)
Inlet_Temp	✓	26	N/A	N/A	N/A	40	42	N/A
Outlet_Temp	✓	36	N/A	N/A	N/A	68	70	N/A
CPU0_VR_Temp	✓	49	N/A	N/A	N/A	115	120	N/A
CPU1_VR_Temp	✓	45	N/A	N/A	N/A	115	120	N/A
CPU2_VR_Temp	✓	34	N/A	N/A	N/A	115	120	N/A
CPU3_VR_Temp	✓	33	N/A	N/A	N/A	115	120	N/A
CPU0_Temp	✓	53	N/A	N/A	N/A	91	93	N/A
CPU1_Temp	✓	49	N/A	N/A	N/A	91	93	N/A
CPU2_Temp	✓	44	N/A	N/A	N/A	91	93	N/A
CPU3_Temp	✓	43	N/A	N/A	N/A	91	93	N/A
CPU0_Margin_Temp	✓	40	N/A	N/A	N/A	N/A	N/A	N/A
CPU1_Margin_Temp	✓	44	N/A	N/A	N/A	N/A	N/A	N/A
CPU2_Margin_Temp	✓	49	N/A	N/A	N/A	N/A	N/A	N/A
CPU3_Margin_Temp	✓	50	N/A	N/A	N/A	N/A	N/A	N/A

Figure 22 Temperature Information

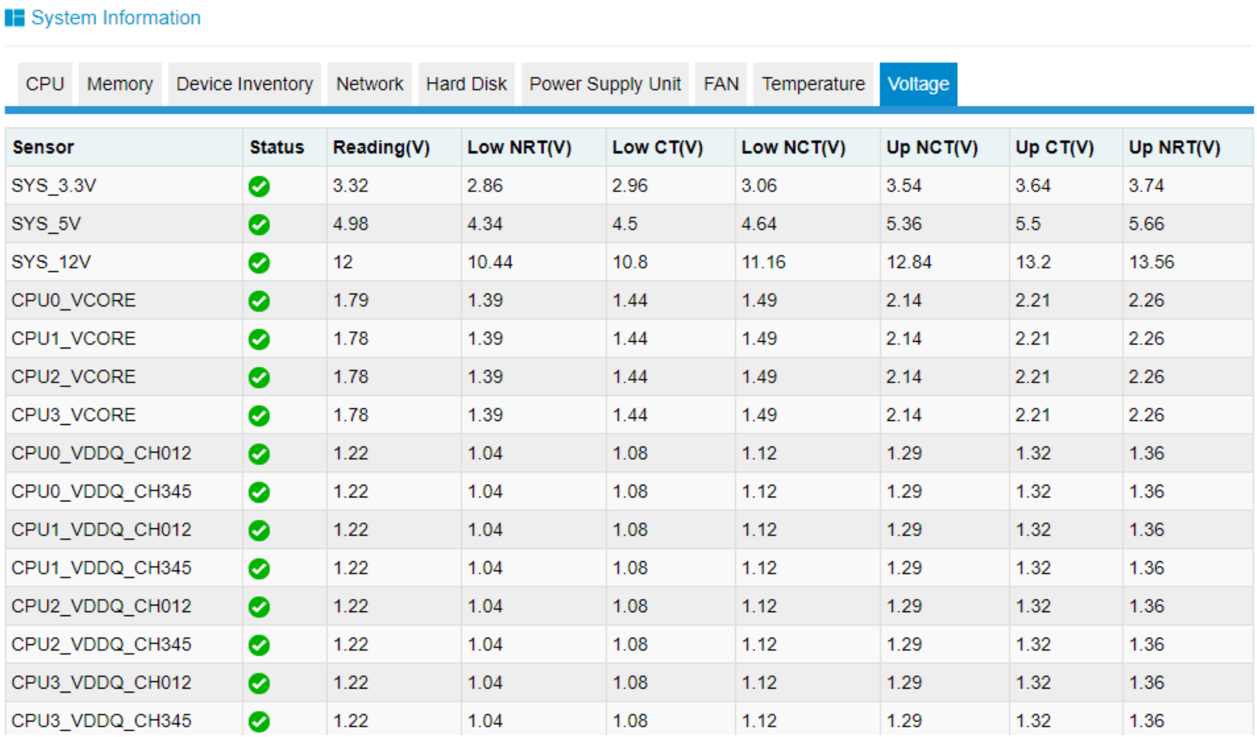
Table 17 Temperature Information

Attribute	Value
Sensor	Sensor Name
Status	✓ Normal State ⚠ Warning State ✖ Critical State ● State unavailable or current power is off.
Reading(°C)	Temperature Reading
Lower NRT(°C)	Lower Non Recoverable Threshold
Lower CT(°C)	Lower Critical Threshold
Lower NCT(°C)	Lower Non Critical Threshold
Up NCT (°C)	Up Non Critical Threshold
Up CT(°C)	Up Critical Threshold
Up NRT (°C)	Up Non Recoverable Threshold

Note：Threshold value N/A mean not configured

7.9. Voltage

Go to table “Voltage” in System Information page.



Sensor	Status	Reading(V)	Low NRT(V)	Low CT(V)	Low NCT(V)	Up NCT(V)	Up CT(V)	Up NRT(V)
SYS_3.3V	✓	3.32	2.86	2.96	3.06	3.54	3.64	3.74
SYS_5V	✓	4.98	4.34	4.5	4.64	5.36	5.5	5.66
SYS_12V	✓	12	10.44	10.8	11.16	12.84	13.2	13.56
CPU0_VCORE	✓	1.79	1.39	1.44	1.49	2.14	2.21	2.26
CPU1_VCORE	✓	1.78	1.39	1.44	1.49	2.14	2.21	2.26
CPU2_VCORE	✓	1.78	1.39	1.44	1.49	2.14	2.21	2.26
CPU3_VCORE	✓	1.78	1.39	1.44	1.49	2.14	2.21	2.26
CPU0_VDDQ_CH012	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU0_VDDQ_CH345	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU1_VDDQ_CH012	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU1_VDDQ_CH345	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU2_VDDQ_CH012	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU2_VDDQ_CH345	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU3_VDDQ_CH012	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36
CPU3_VDDQ_CH345	✓	1.22	1.04	1.08	1.12	1.29	1.32	1.36

Figure 23 Voltage Information

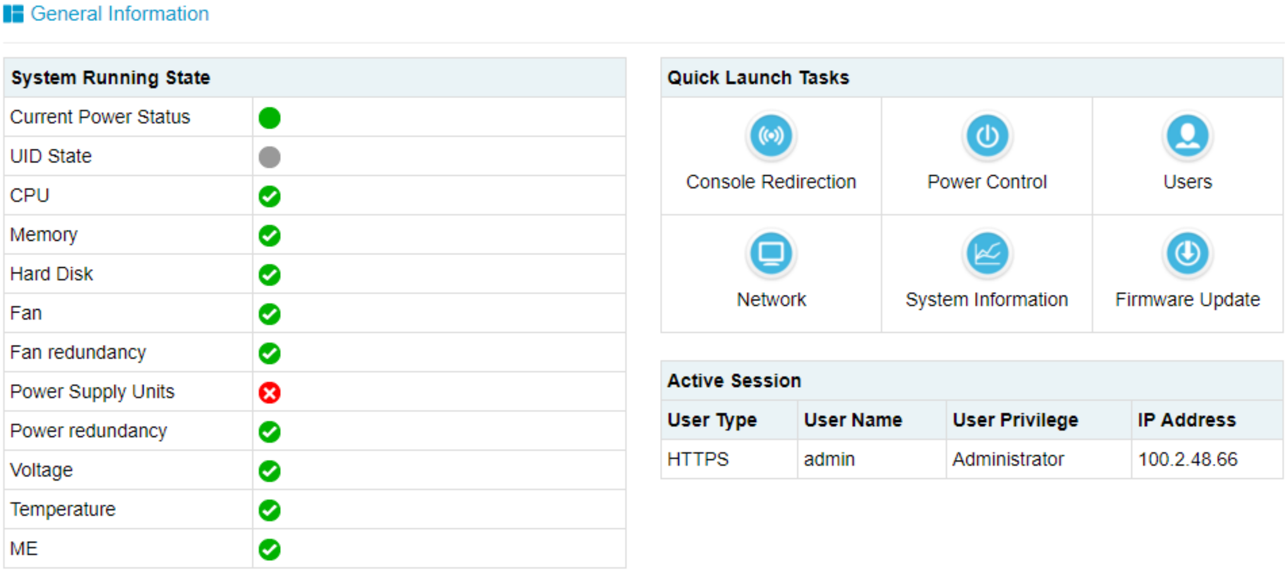
Table 18 Voltage Information

Attribute	Value
Sensor	Sensor Name
Status	✓ Normal State ⚠ Warning State ✖ Critical State ● State unavailable or current power is off.
Reading(V)	Temperature Reading
Lower NRT(V)	Lower Non Recoverable Threshold
Lower CT(V)	Lower Critical Threshold
Lower NCT(V)	Lower Non Critical Threshold
Up NCT (V)	Up Non Critical Threshold
Up CT(V)	Up Critical Threshold
Up NRT (V)	Up Non Recoverable Threshold

Note：Threshold value N/A mean not configured

7.10.Global Running State

Login WEB GUI, go to first page “Overview”, main devices global running state displayed.



System Running State	
Current Power Status	●
UID State	●
CPU	✓
Memory	✓
Hard Disk	✓
Fan	✓
Fan redundancy	✓
Power Supply Units	✗
Power redundancy	✓
Voltage	✓
Temperature	✓
ME	✓

Active Session

User Type	User Name	User Privilege	IP Address
HTTPS	admin	Administrator	100.2.48.66

Figure 24 Global Running State

Table 19 System Running State

Device	State Denotation
Current Power Status	● Power On ● Power Off
UID Status	● UID LED On ● UID LED Off
CPU	CPU Healthy state: ✓ Normal – All CPU Normal. ⚠ Warning State – One or more CPUx_Status warning. ✗ Critical State – One or more CPUx_Status critical. ● Power Off
Memory	Memory Healthy state: ✓ Normal – All Memory Normal. ⚠ Warning State – One or more CPUx_CHy_DIMMz warning. ✗ Critical State – One or more CPUx_CHy_DIMMz critical. ● Power Off
Hard Disk	Hard Disk Healthy state: ✓ Normal – All Disk Normal. ⚠ Warning State – One or more DISKx_Status warning. ✗ Critical State – One or more DISKx_Status critical. ● Power Off
Fan	Fan Healthy state: ✓ Normal – All Fan Normal. ✗ Critical State – One or more Fan failure. ● Power Off
Fan Redundancy	Fan Healthy state: ✓ Normal – All Fan Normal. ✗ Critical State – One or more Fan absent or cannot be read. ● Power Off
Power Supply Unit	PSU Healthy state: ✓ Normal State ⚠ Warning State – One or more PSUx_Status warning. ✗ Critical State – One or more PSUx_Status critical. ● Power Off
Power Redundancy	PSU Redundant state: ✓ Normal State ⚠ Warning State –PSU_Redundant Sensor warning. ✗ Critical State – PSU_Redundant Sensor critical.

	● Power Off
Voltage	Voltage Sensor state: ✓ Normal State ⚠ Warning State – One or more Voltage Sensor warning. ✖ Critical State – One or more Voltage Sensor critical. ● Power Off
Temperature	Temperature Sensor state: ✓ Normal State ⚠ Warning State – One or more Temperature Sensor warning. ✖ Critical State – One or more Temperature Sensor critical. ● Power Off
ME	ME state: ✓ Normal State ⚠ Warning State – ME_FW_Status Sensor warning ✖ Critical State – ME_FW_Status Sensor critical ● State unavailable or current power is off.

7.11.Firmware Version

Page “Firmware Version Information” displays version of firmware resides in the platform, including BMC, BIOS, ME, PSU, PCVVIN VR, PVCCIO VR, PVDDQ VR, CPLD and BP CPLD.

Table 20 All Firmware Which Monitored by BMC

Firmware	Revision information
BMC	Revision and Build Time
BIOS	Revision and Build Time
ME	Revision
CPLD	Revision
BP CPLD	Revision
PCVVIN VR	Revision
PVCCIO VR	Revision
PVDDQ VR	Revision
FPGA(if present)	Revision
PSOC(if present)	Revision

7.12.FRU

FRU stores in EEPROM, BMC will read FRU from EEPROM when BMC boot， FRU will not lose after BMC firmware upgraded.

Table 21 FRU Information

Category	Items
Basic Information	FRU Device ID: 0
	FRU Device Name: BMC_FRU
Chassis Information	Chassis Information Area Format Version: *
	Chassis Type: Tower
	Chassis Part Number: **
	Chassis Serial Number: **
Board Information	Board Information Area Format Version: *
	Language: *
	Manufacture Date Time: weekday month day time year
	Board Manufacturer: Inspur
	Board Product Name: *****
	Board Serial Number: **
	Board Part Number: **
	Board Extra: *****

Product Information	Product Information Area Format Version: *
	Language: *
	Manufacture Name: Inspur
	Product Name: *****
	Product Part Number: **
	Product Version: **
	Product Serial Number: **
	AssetTag: *

8. Device State Monitor and Diagnostic

8.1. Sensors

8.1.1. Physical Sensor

Physical sensors monitors main devices state change. The information gathered from physical sensors is translated into IPMI sensors.

- Device State Sensors: BMC monitors CPU/DIMM/PSU/HDD error state based on IPMI Sensor type.
- Temperature: BMC monitors temperature of system components like, CPU, PCH, DIMM, PSU and HSBP, and monitors Inlet/Outlet temperatures.
- Voltage: System P12V, P5V, P3V3, PVNN, PVDDQ, PVCCIO, PVCCIN.
- Fan Speed: System fan.
- Power Consumption: BMC monitors Total Power, CPU Power, Memory Power, PSU Input Power. Fan Power and HDD Power are platform-specific.
- System Main Component Health: BMC monitors system component's health like, CPU Status, PCH Status, MEM Hot, HDD Status, PSU Supply, ME FW Status.
- Intrusion: Optional - An assertion event will be logged, when chassis cover is opened.
- Button: An assertion event will be logged, when Power Button or Reset Button is pressed.

8.1.2. Virtual Sensor

BMC also reports various system state changes by maintaining virtual sensors that are not specifically tied to physical hardware.

- IPMI Watchdog: BMC supports an IPMI Watchdog sensor as a means to log SEL events due to expirations of the IPMI 2.0 compliant Watchdog Timer.
- EventLog: The Event Log sensor is used to indicate when the event log is cleared. An assertion event is logged against this sensor when the SEL is cleared. This discrete sensor also supports offsets that indicate when the SEL is full and almost full.
- Clear CMOS: If BIOS CMOS is cleared by BMC, an assertion event will be logged.
- System Restart: When system is cold reset, or hard reset, an assertion event will be logged indicating system ever being cold reset or hard reset.
- BMC Boot Up: When BMC boots up, an assertion event will be logged.
- BIOS Boot: When BIOS boots up and host boot to OS, an assertion event will be logged.

8.1.3. Event-Only Sensor

Event-Only discrete sensors are used for event generation only and are not accessible through IPMI sensor commands like the Get Sensor Reading(IPMI command). BIOS/OS or Other third-part client use Add SEL Entry(IPMI command) to add event log to SEL.

8.1.4. Sensor Attribute

- Sensor Type: Please refer to *Sensor Type Codes* table in IPMI Specification, Version 2.0.
- Event Type: Please refer to *Event/reading Type Code Ranges* table in IPMI Specification, Version 2.0.
- Event Offset:

  If sensor event type is generic, please refer to *Generic Event/Reading Type Code* table in IPMI Specification, Version 2.0.

If sensor event type is sensor-specific, please refer to *Sensor Type Code* tables in IPMI Specification, Version 2.0.

- Assertion/De-assertion
- Assertion and de-assertion indicators reveal the type of events this sensor generates:

8.2. CPU

Table 22 CPU Health State Monitored.

State	Level	Related Model
Present	Info	SDR/SEL
Thermal Trip	Critical	SDR/SEL
Processor Hot	Critical	SDR/SEL
Catt Error	Critical	SDR/SEL
Error0	Warning	Blackbox
Error1	Warning	Blackbox
Error2	Critical	Blackbox
CPU VR Hot	Critical	Blackbox
PCH Thermal Trip	Critical	Blackbox

8.3. Memory

Table 23 Memory Health State Monitored.

State	Level	Related Model
Mem Hot	Critical	Blackbox
Mem VR Hot	Critical	Blackbox
ECC	Warning	SDR/SEL
Uncorrectable ECC	Critical	SDR/SEL

8.4. HDD

Table 24 HDD Health State Monitored

State	Level	Related Model
Present	Info	SDR/SEL
Error	Critical	SDR/SEL
Rebuild	Warning	SDR/SEL

8.5. PSU

Table 25 PSU Health State Monitored

State	Level	Related Model
Present	Info	SDR/SEL/ Blackbox
Power Supply Failure	Critical	SDR/SEL/ Blackbox
Predictive Failure	Warning	SDR/SEL/ Blackbox
Power Supply AC lost	Critical	SDR/SEL/ Blackbox

9. Logs

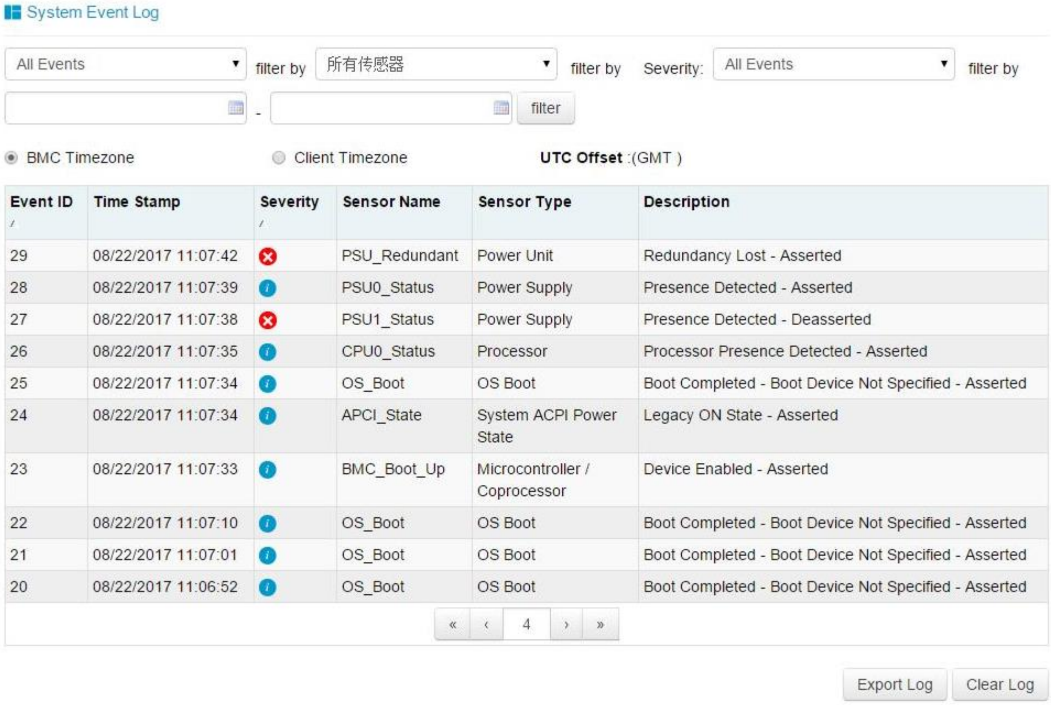
Logs provides the history record of main devices state change, used to fault diagnostic.

9.1. System Event Log

BMC provide the ability to record IPMI sensor based event history. System event log output following items and user can get the sensor event information by WEB or IPMI CMD.

- Support Up to 3639 items.
- Support Linear mode. When SEL is full, new log will be discard.
- Support Cycle mode, default mode. When SEL is full, oldest log will be discard.
- When SEL is almost full(75%), then Almost full log will be record in SEL.
- When SEL is full in linear mode, Full log will be record in SEL.
- When SEL is clear, Clear log will be record in SEL.
- Support export SEL by WEB or IPMI CMD
- Support inform event to remote client by SNMP Trap, Email Alert, Syslog.

Go to page “Logs->System Event Log” in Web GUI, all sensor based log displayed, user can filter event by event severity, time, or senor.



System Event Log

All Events ▾ filter by 所有传感器 ▾ filter by Severity: All Events ▾ filter by

- filter

● BMC Timezone ○ Client Timezone UTC Offset :(GMT)

Event ID	Time Stamp	Severity	Sensor Name	Sensor Type	Description
29	08/22/2017 11:07:42	✖	PSU_Redundant	Power Unit	Redundancy Lost - Asserted
28	08/22/2017 11:07:39	ⓘ	PSU0_Status	Power Supply	Presence Detected - Asserted
27	08/22/2017 11:07:38	✖	PSU1_Status	Power Supply	Presence Detected - Deasserted
26	08/22/2017 11:07:35	ⓘ	CPU0_Status	Processor	Processor Presence Detected - Asserted
25	08/22/2017 11:07:34	ⓘ	OS_Boot	OS Boot	Boot Completed - Boot Device Not Specified - Asserted
24	08/22/2017 11:07:34	ⓘ	APCI_State	System ACPI Power State	Legacy ON State - Asserted
23	08/22/2017 11:07:33	ⓘ	BMC_Boot_Up	Microcontroller / Coprocessor	Device Enabled - Asserted
22	08/22/2017 11:07:10	ⓘ	OS_Boot	OS Boot	Boot Completed - Boot Device Not Specified - Asserted
21	08/22/2017 11:07:01	ⓘ	OS_Boot	OS Boot	Boot Completed - Boot Device Not Specified - Asserted
20	08/22/2017 11:06:52	ⓘ	OS_Boot	OS Boot	Boot Completed - Boot Device Not Specified - Asserted

Figure 25 System Event Log

Table 26 SEL Attributes

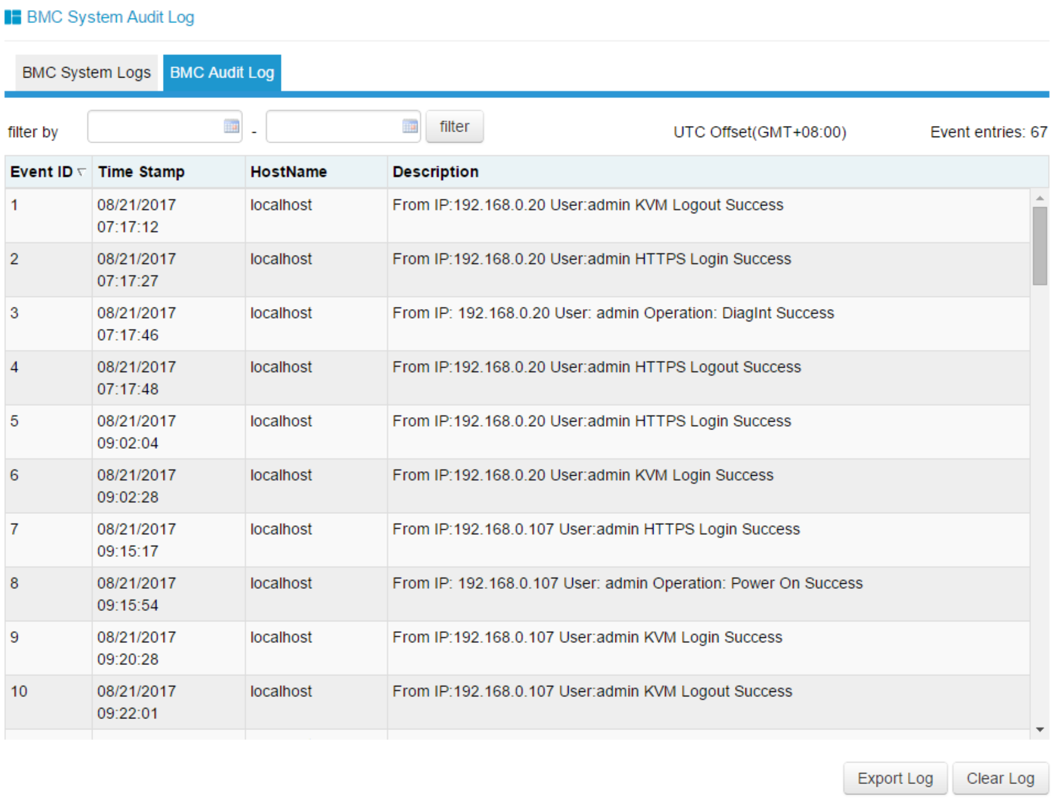
Event ID	Event ID in SEL
Time Stamp	Event generate time
Severity	Event error level, include Error, Warning, Information
Sensor Name	Sensor Name, locate the device
Sensor Type	Sensor Type defined in IPMI2.0
Description	Event details

9.2. Audit Log

BMC provide ability to record BMC system audit log.

- All Web setting operating actions will be recorded.
- Web/SSH/Telnet login and logout will be recorded.

- Audit log supported size is 50K, if more than 50K, log will be cleared.
- Support export log by Web.



UTC Offset(GMT+08:00)   Event entries: 67

Event ID	Time Stamp	HostName	Description
1	08/21/2017 07:17:12	localhost	From IP:192.168.0.20 User:admin KVM Logout Success
2	08/21/2017 07:17:27	localhost	From IP:192.168.0.20 User:admin HTTPS Login Success
3	08/21/2017 07:17:46	localhost	From IP: 192.168.0.20 User: admin Operation: DiagInt Success
4	08/21/2017 07:17:48	localhost	From IP:192.168.0.20 User:admin HTTPS Logout Success
5	08/21/2017 09:02:04	localhost	From IP:192.168.0.20 User:admin HTTPS Login Success
6	08/21/2017 09:02:28	localhost	From IP:192.168.0.20 User:admin KVM Login Success
7	08/21/2017 09:15:17	localhost	From IP:192.168.0.107 User:admin HTTPS Login Success
8	08/21/2017 09:15:54	localhost	From IP: 192.168.0.107 User: admin Operation: Power On Success
9	08/21/2017 09:20:28	localhost	From IP:192.168.0.107 User:admin KVM Login Success
10	08/21/2017 09:22:01	localhost	From IP:192.168.0.107 User:admin KVM Logout Success

Figure 26 BMC Audit log

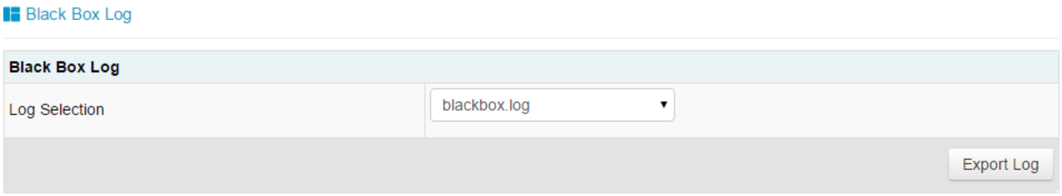
Table 27 Audit Log Attributes:

Event ID	Event ID
Time Stamp	Event generate time
Host Name	BMC host name
Description	Event details, including event source, username, service name, operation, success or fail.

9.3. Blackbox Log

BMC support blackbox function used to record some details when event occurred.

- Record each CPU’s MSR, CSR Registers, used to fault diagnostic. CPU Catterr, Thermal Trip, Error2, Uncorrectable ECC will trigger record CPU Registers.
- Record event details for Non-IPMI events, used to diagnostic.
- When more than 3M, log will loop to store, and the old log content will be deleted.
- Support export log by WEB



Log Selection: blackbox.log

Figure 27 Blackbox Log

9.4. System Serial Log

Reference to section “Serial over LAN (SOL) and System Serial Log Recording”.

10. Event Alerting

BMC supports SNMP Trap and SMTP email alerts.

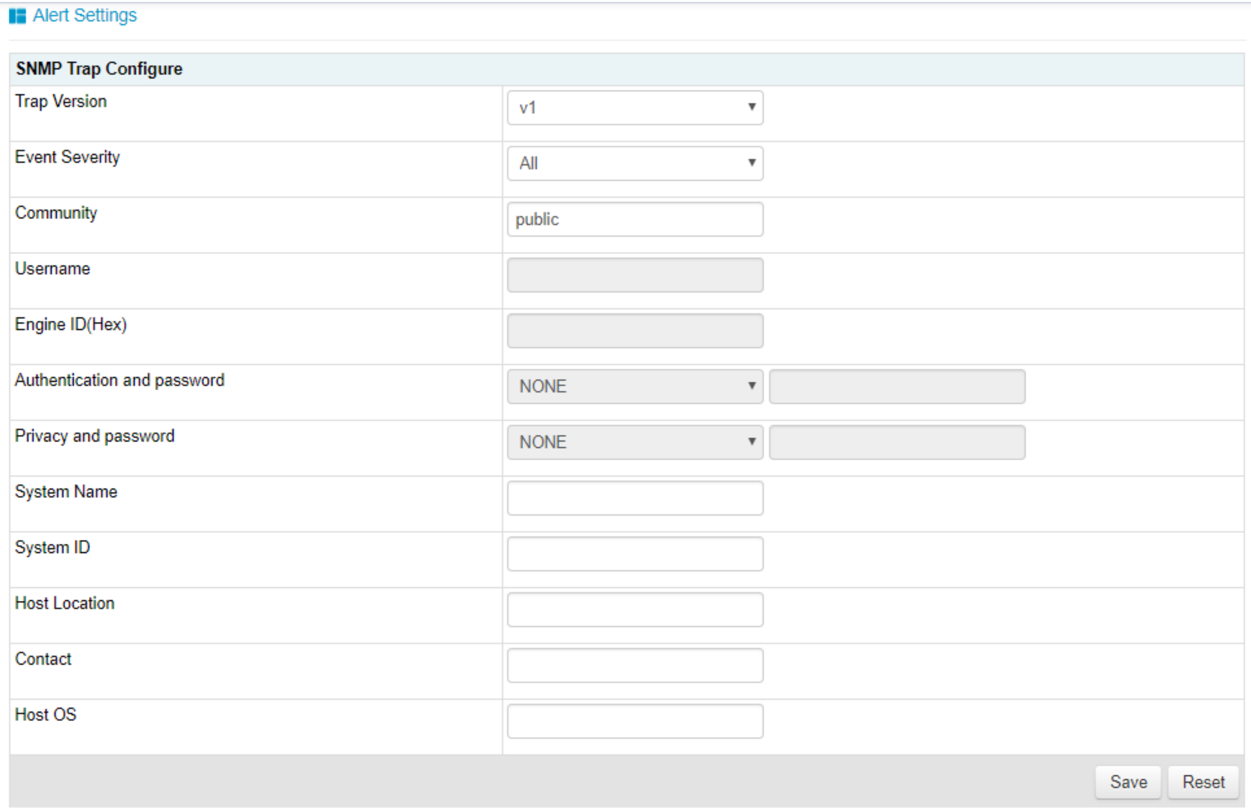
10.1.SNMP Trap Alert

BMC support SNMP Trap, user opens trap receiver, set trap destination IP in BMC Web GUI, when BMC detect event, BMC sends event to the trap receiver.

- BMC supports SNMP v1, v2, v3 traps. Default Trap v1.
- A Modular Information Block (MIB) file associated with the traps should be provided with the BMC firmware to help SNMP Trap receiver to translate the trap.
- SNMP default port number is 162, user can set port in Chapter “Service”.
- Only IPMI sensor based log support SNMP Traps.

Step 1

Set SNMP Trap protocol,   including Trap version, event severity filtering, and community .etc. As bellow:



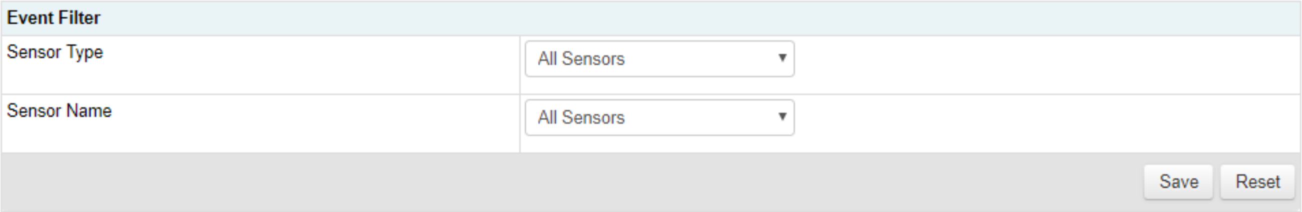
SNMP Trap Configure

Trap Version	v1 ▾	
Event Severity	All ▾	
Community	public	
Username		
Engine ID(Hex)		
Authentication and password	NONE ▾	
Privacy and password	NONE ▾	
System Name		
System ID		
Host Location		
Contact		
Host OS		

Figure 28 Alert Settings

Step 2

Set event filter, user can select sensor type or sensor name.



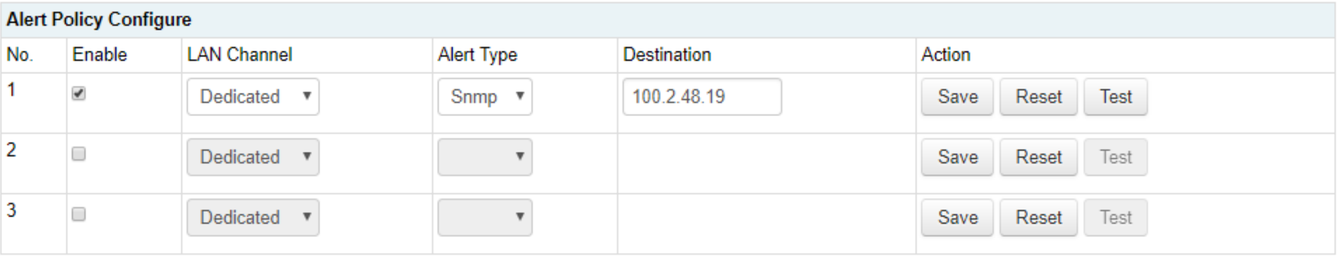
Event Filter

Sensor Type	All Sensors ▾
Sensor Name	All Sensors ▾

Figure 29 Event Filter

Step 3

Set alert type and destination. Firstly enable one of three items. If SNMP selected, user should set destination to his IP, if Email selected, user should set LAN Channel to dedicated or shared network, then set destination to an user configured email.



Alert Policy Configure

No.	Enable	LAN Channel	Alert Type	Destination	Action
1	☑	Dedicated ▾	Snmp ▾	100.2.48.19	Save Reset Test
2	□	Dedicated ▾	▾		Save Reset Test
3	□	Dedicated ▾	▾		Save Reset Test

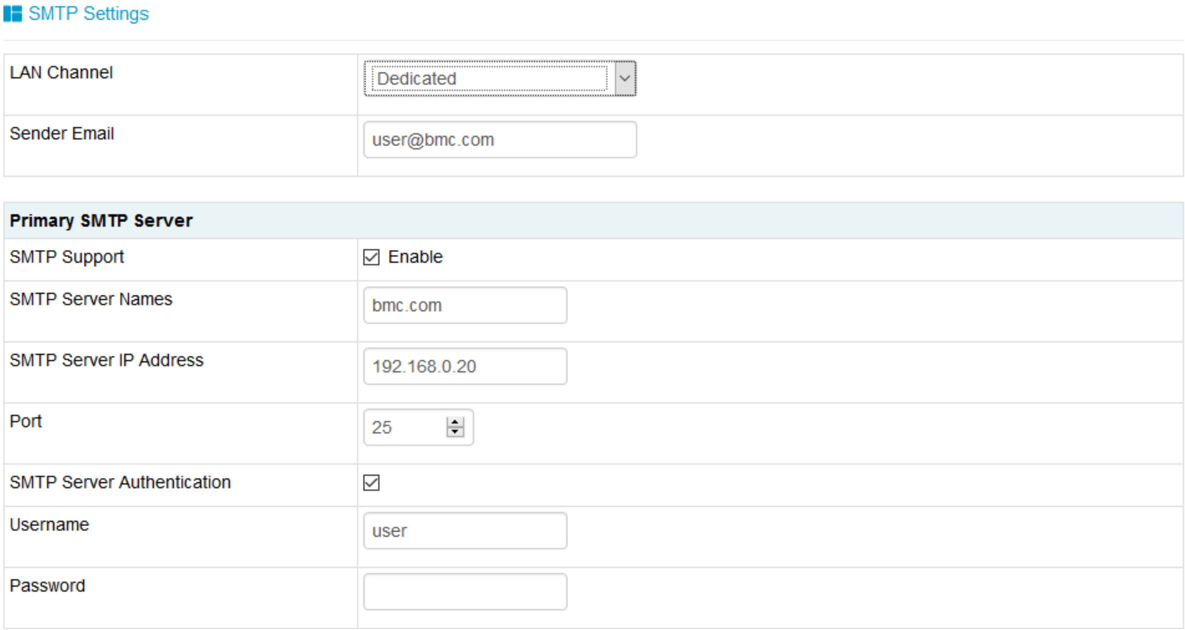
Figure 30 Alert Policy Configure

10.2.SMTP Email Alert

SMTP (Simple Mail Transport Protocol, defined in RFC821) email alert is supported. The email alert provides text information about the event.

Step 1

Configure SMTP settings, user should set SMTP server for used LAN channel, if event alert, Sender Email will send an email to destination email.



SMTP Settings

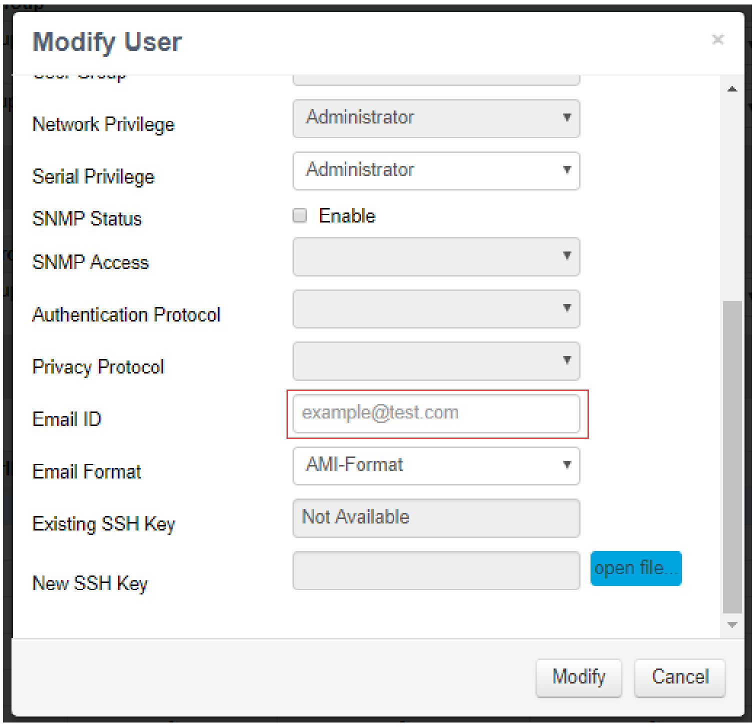
LAN Channel	Dedicated
Sender Email	user@bmc.com

Primary SMTP Server	
SMTP Support	☑ Enable
SMTP Server Names	bmc.com
SMTP Server IP Address	192.168.0.20
Port	25
SMTP Server Authentication	☑
Username	user
Password	

Figure 31 SMTP Settings

Step 2

Configure destination email for related user.



Modify User

Network Privilege	Administrator ▾
Serial Privilege	Administrator ▾
SNMP Status	□ Enable
SNMP Access	▾
Authentication Protocol	▾
Privacy Protocol	▾
Email ID	example@test.com
Email Format	AMI-Format ▾
Existing SSH Key	Not Available
New SSH Key	open file...

Figure 32 Email Settings

Step 3

Set destination in Figure “Alert Policy Configure” like SNMP Trap Alert Step 3.

10.3.Syslog

Syslog supports on/off, supports log level filtering, supports 4 receiving target and every target can configure the receiving server address (IPv4 / IPv6 / FQDN), port number, log type, enable status and Send test information. Report log support security log, operation log and system event log and it is configurable. These logs carry host log. Considering security, Syslog report logs support TLS encryption, and support bidirectional authentication based on import certificate

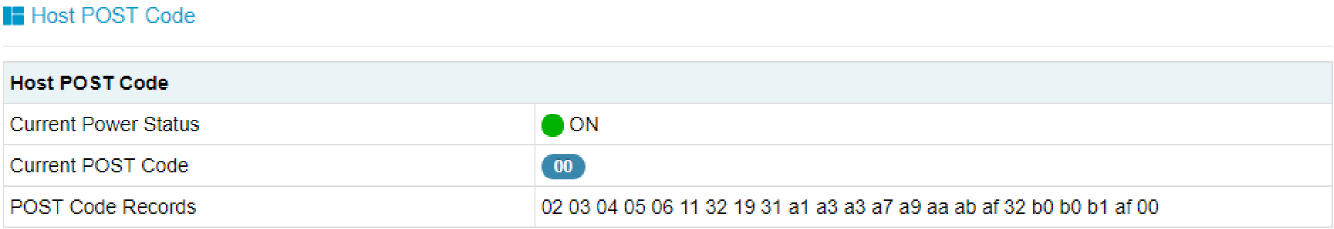
11. Diagnostics

Diagnostic tool provide the ability of check and verification for BMC or Host system to investigate whether there is something out of function or something does not work correctly.

11.1.BIOS Post Code(Port 80h)

BIOS send Post code to IO port 80h. If there is any errors during power on, the last post code is on port 80h. BMC is able to trace post code via port 80h to investigate the cause of issue happened.

BMC could record max 255 POST storage in buffer, if buffer full oldest POST code will be deleted.



Host POST Code

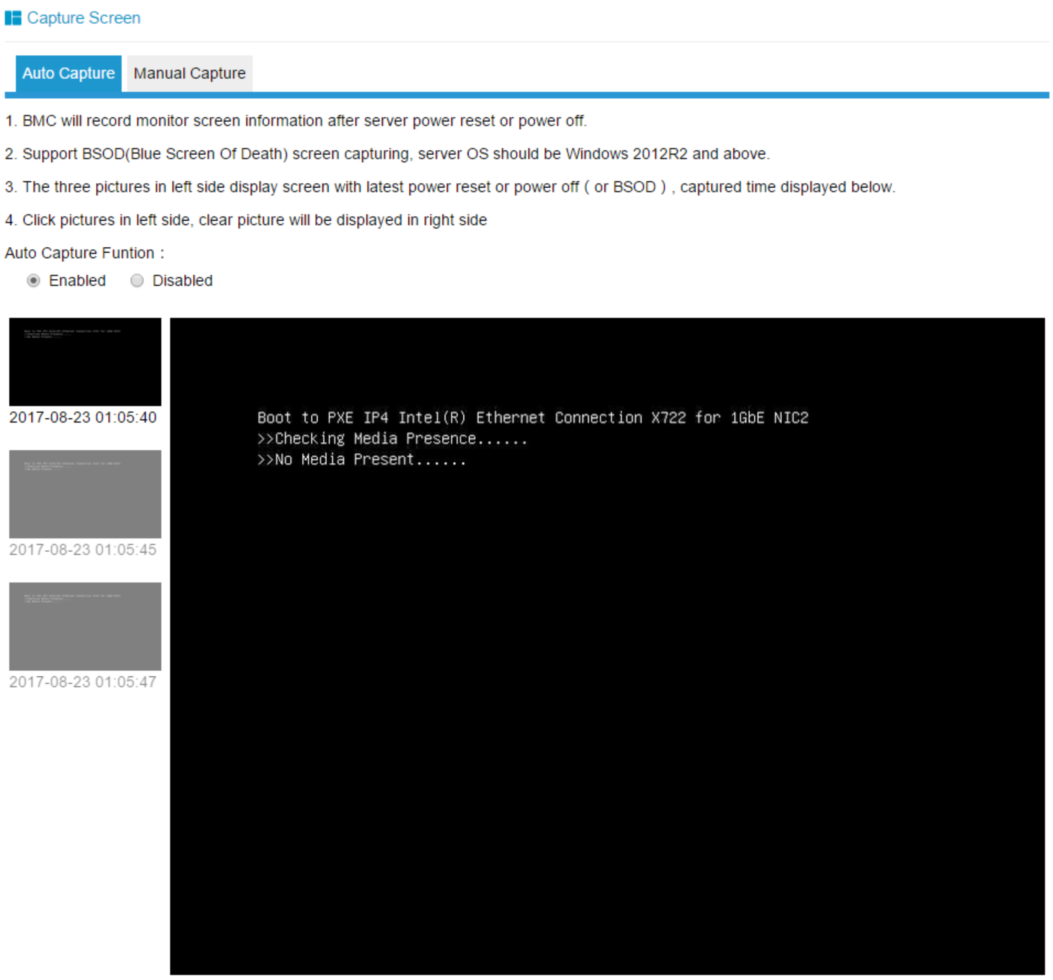
Host POST Code	
Current Power Status	● ON
Current POST Code	00
POST Code Records	02 03 04 05 06 11 32 19 31 a1 a3 a3 a7 a9 aa ab af 32 b0 b0 b1 af 00

Figure 33 BIOS Post Code

11.2.Screen Capture

BMC will record monitor screen after server power reset or power off. BMC also support BSOD (Blue Screen of Death) screen capturing, server OS should be Windows 2012R2 and above.

Default auto-capture is enabled, user could disable in Web GUI.



Capture Screen

1. BMC will record monitor screen information after server power reset or power off.
2. Support BSOD(Blue Screen Of Death) screen capturing, server OS should be Windows 2012R2 and above.
3. The three pictures in left side display screen with latest power reset or power off (or BSOD) , captured time displayed below.
4. Click pictures in left side, clear picture will be displayed in right side

Auto Capture Funtion :

● Enabled ○ Disabled

2017-08-23 01:05:40

2017-08-23 01:05:45

2017-08-23 01:05:47

```
Boot to PXE IP4 Intel(R) Ethernet Connection X722 for 1GbE NIC2
>>Checking Media Presence......
>>No Media Present......
```

Figure 34 Screen Capture

11.3.BMC Watchdog for System

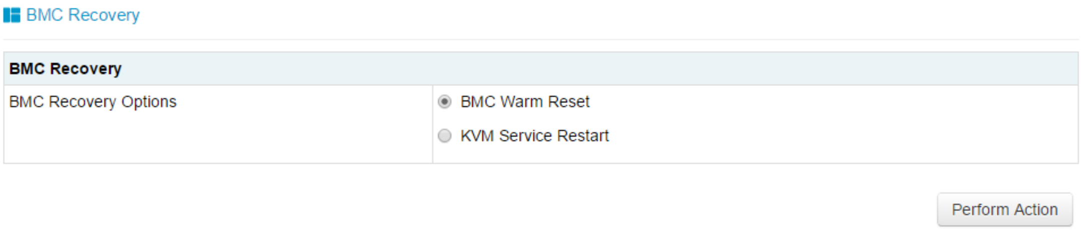
Software watchdog can be used for a number of system timeout function by system management or by BIOS. If software watchdog triggered, the following actions are available.

- System Reset
- System Power Off
- System Power Cycle
- When BMC watchdog working, BMC will record SEL log.

11.4.BMC and Task Reset

User can do BMC task reset from WEB or IPMI interface to make BMC recovery if any unexpected situations occurred.

- Warm reset BMC, use “ipmitool mc reset warm”, IPMI Server, KVM Server, WEB Server will be reset.
- Cold reset BMC, use WEB or “ipmtool mc reset cold”, BMC will be full reset
- KVM reset, user WEB, KVM Server will be reset



BMC Recovery

BMC Recovery	
BMC Recovery Options	● BMC Warm Reset ○ KVM Service Restart

Figure 35 BMC Recovery

12. BMC Self Recovery

BMC Self Recovery provides the ability of automatic repair operations as well if necessary.

12.1.Hardware watchdog

Known fault scene:

- Kernel panic
- System resources exhausted or error, system can’t create a new task, but the original task can continue to run

Hardware watchdog:

- Watchdog start when uboot load kernel, and the timeout is 5 minutes. If BMC boot timeout， BMC will reset。
- After the BMC system starts, the main process resets the Watchdog every minute. If the timeout is more than 1 minute, the BMC will reset.
- When enter the flash mode, set watchdog time to 20 mins, if timeout BMC will reset automatically. When start flashing image, the watchdog will update to 20 mins, if timeout BMC will reset automatically.

12.2.Software watchdog

BMC regularly detect the working status of internal services, and progress abnormal, BMC will restart the corresponding service:

- IPMI Server
- KVM Server
- Virtual Media Server

13. LED

The system provided LED to indicating the health of the system.

Table 28 LED to Indicating the Health of the System

LED name	Color	Status	Description
SYS LED	Red	OFF	1. When system is off than SYS LED is OFF. 2. System working fine than the SYS LED is OFF.
SYS LED	Red	ON	CPU has below event occur： 1.CPU IERR 2.CPU Thermal Trip 3. PCIE Error
SYS LED	Red	BLINK	CPU appears the following warning： Processor Automatically Throttled
Power LED	Yellow	ON	Plug in power but not Power on
Power LED	Green	ON	1.Power on 2.Power button is pressed
BMC Heartbeat	Green	BLINK	BMC status OK
BMC Heartbeat	Green	ON/OFF	BMC has error
DIMM Error	Red	ON	DIMM Ecc or Uncorrectable ECC occurred
PSU Error	Red	ON	PSU Sensors error
FAN Error	Red	ON	Fan sensors error
CPU Hot	Red	ON	CPU Proc Hot PIN detected

14. BMC Network

14.1. LAN Interface

BMC usually support a LAN controller dedicated to BMC and a LAN controller shared for both BMC and system.

- Maximum bandwidth: Dedicated NIC – 1000M, Shared NIC – 100M
- BMC network interface compatible support IPV4 and IPV6, support automatic access or manually set the IP address and MAC address is stored in the EEPROM.
- Support vlan.
- Default, IPMI LAN channels are assigned as below

Table 29 BMC LAN Interface

Channel ID	Interface	Support Sessions
1h	Primary LAN(eth1)	Yes
8h	Secondary LAN(eth0)	Yes

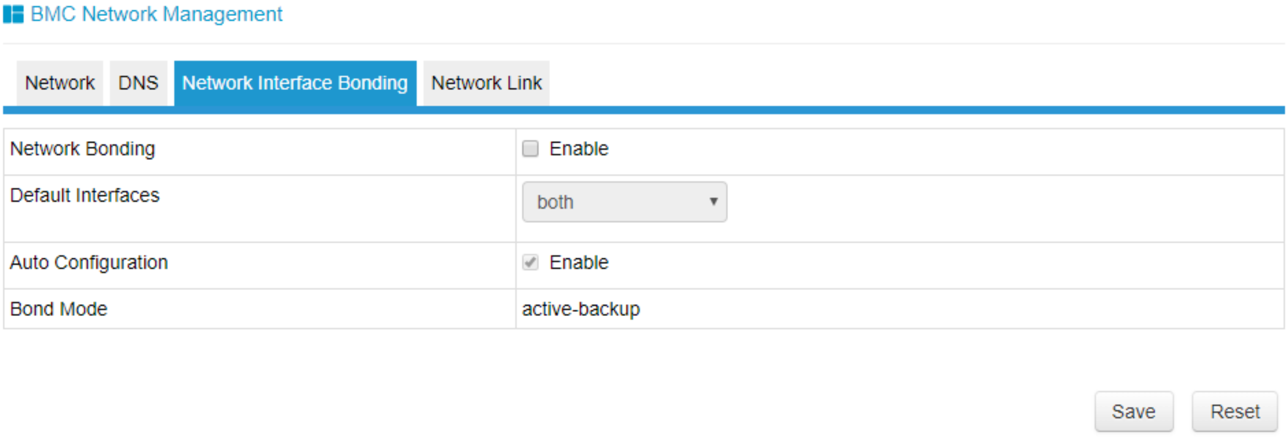
- BMC network interface support enable/disable; and default enable.

14.2. BMC Network Bonding

Bonding feature provide a method for aggregating multiple network interfaces into a single logical bonded network interface. Although multiple network interfaces are bonded, only one is active available at a time. In run-time, the netif_carrier (network link state) is monitored by polling periodically.

- Default disable bonding, user can enable it in WEB GUI or IPMI CMD.
- Only support Active-backup bonding mode. Default bonding on both NIC(Dedicated and Shared NIC), means network will be working on the NIC plugged cable. If both NICs plugged cable before BMC boot up, shared NIC will be primary network to be working. If one NIC plugged cable before BMC boot up, then anther plugged later, first NIC will be working.
- After bonding, bonding interface use **shared** NIC's MAC to access network, include bonding to both, dedicated or shared NIC.

In WEB GUI, go to page "BMC Settings->BMC Network->Network Interface Bonding" to check and configure bonding function.



Network Bonding	□ Enable
Default Interfaces	both ▾
Auto Configuration	☑ Enable
Bond Mode	active-backup

Figure 36 Network Bonding

Network Bonding: Enable/Disable the Network Bonding. If VLAN is enable, Network Bonding cannot be enable.
Default Interface: Select the default network interface.
Auto Configuration: Enable/Disable Auto Configuration.
If Auto Configuration is disabled, then interface service can be configured via IPMI command.
If Auto Configuration is enabled, then all service will restart automatically.
Bond Mode: Display the current Bonding mode. (This field is read-only.)

14.3. NCSI

NC-SI ("Network Controller Sideband Interface") is an electrical interface and protocol defined by the Distributed Management Task Force (DMTF), which enables the connection of a Baseboard Management Controller (BMC) to a set of Network Interface Controller (NICs) in server computer systems for the purpose of enabling out-of-band remote manageability. It mainly includes: a management controller (MC), one or more (NCSI electrical characteristics support up to 4) network controller (NC). The network controller, on the one hand, connects the external network interface to the internal host interface, and on the other hand, there is an out-of-band interface between the management controllers.

The network management module structure of the server is shown as bellow.

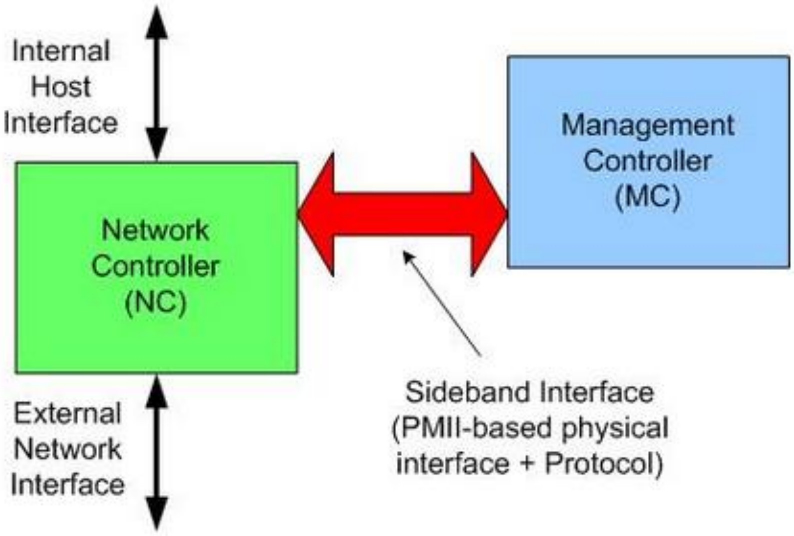

Internal Host Interface
Network Controller (NC)
Management Controller (MC)
External Network Interface
Sideband Interface (PMII-based physical interface + Protocol)

Figure 37 Network Management Module Structure

Table 30 Server Support NCSI

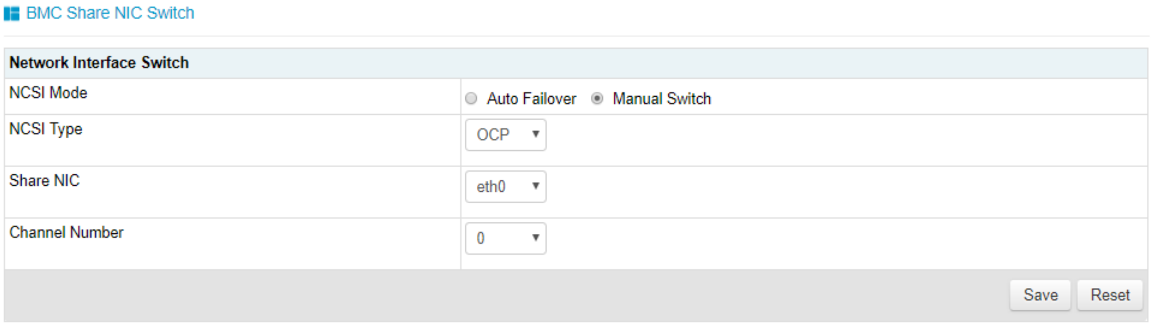
Feature	Detail	NF8460M5	Vancouver	Suva
NCSI	OCP	YES	NO	YES
	PCIE(Not OCP)	NO	NO	NO
	Onboard NIC	NO	YES	NO

14.3.1. Shared NIC Switch

Normally BMC support two or more NCSI NICs, only allowed one NIC on NCSI bus, if switch NCSI to anther NIC, user should set in Web GUI.

Supported NCSI card, On PURLEY platform, includes onboard NIC, PHY card, OCP A/B/C card, Inspur designed PCIE NIC supported NCSI. Different projects support one or more of the NCSI cards.

Login Management Web GUI, enter “BMC Settings > BMC Shared NIC Switch” as shown below.



BMC Share NIC Switch

Network Interface Switch	
NCSI Mode	○ Auto Failover ● Manual Switch
NCSI Type	OCP
Share NIC	eth0
Channel Number	0

Figure 38 BMC Shared NIC Switch

NCSI Type: Select NIC type you wanted to switch to then click Save. The available types are “PHY”, “OCP” and “PCIE”.

14.3.2. NCSI Auto-Failover

Normally, NCSI NIC have two or more ports, BMC supports Auto-Failover to switch to other port when working port link down.

Default NCSI mode is Manual Switch to port0.

NCSI Failover setting as figure “BMC Shared NIC Switch”.

NCSI Mode: Select the NCSI mode supported. The available modes are “Auto Failover”, and “Manual Switch”.
BMC Shared NIC: Select the port of shared NIC. The available port is eth0
Channel Number: Select the channel number of the selected NIC. Channel 0, 1, 2, or 3 can be selected.

15. Users

BMC support multiple type users, include IPMI, WEB, BMC OS and SNMP users.

- BMC supports unified user management mechanism to manage IPMI, WEB, BMC OS user. User created by IPMI or WEB will have IPMI, WEB and BMC OS user privilege. As BMC OS user, it only has common user privilege, not has root user privilege.
- Sysadmin is BMC OS root user, only have BMC OS root privilege, cannot access IPMI and WEB.
- SNMP user is used for SNMP Get/Set.

15.1.IPMI/WEB/BMC OS Unified User

- BMC supports IPMI 2.0 user model. Unified user could be created by IPMI CMD or Web GUI.
- Up to 16 users are supported.
- The 16 users can be assigned to any channel include dedicated LAN and NCSI LAN.
- All of the created users can login simultaneously.
- The available user privilege levels are Administrator, Operator, User, No Access.

Table 31 IPMI Users

User ID	User Name	Password	Status	Default Privilege	Characteristics
1	admin	admin	Enabled	Administrator	User Name fixed(cannot be changed), password can be changed
2- 16	undefined	undefined	Disabled	Administrator	User Name/Password can be changed

15.1.1. User Security

Username

- User Name is a string of 1 to 16 alpha-numeric characters, including '-','_'and'@'.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters ','(comma), '.'(period), ':'(colon), ';'(semicolon), ' '(space), '/'(slash), '\\'(backslash), '(' (left bracket) ,')'(right bracket)and so on are not allowed.

Password Authentication

- Password encryption scheme: 64Bit Blowfish. Password is encrypted to store in BMC flash.

Password Complexity

- At password complexity check disabled, Password must be 1-16 character long.
- At password complexity check enabled, Password must include special, uppercase, lowercase character and number, 8-16 characters long.
- Default disable complexity check, we strongly suggest you enable this function for security.

Password Expiration

- Password Expiration, the range of the expiration is 0~90 days, and 0 presents forever.
- Default disable, we strongly suggest you enable this function for security.

- If enable, you need change password in expiration time. If password will be expired less than 15 days, when login Web GUI, Web will alert “From the password expiration remaining days:xx ”.
- If password expired, you need disable this function in HOST OS by OEM IPMI CMD.
- *Password Expiration* only supported in Web GUI.

Password Failed Locking

- Login Fail Retry Count: the retry count should be a number between 0 and 5.
- Lock Time: the range of the time is 5 ~ 60 minutes.
- If login failed time reach *Login Fail Retry Coun*t, Web will alert “Input Error Password more than limit, user is locked, please retry later!”, and user will be locked for *Lock Time*.
- Default disable, we strongly suggest you enable this function for security.
- *Password Failed Locking* only supported in Web GUI.

Password History Record

- -Password History Records: the range is 0 ~ 5.
- Default disable. If enable, you could not set password same to Password History Records(last N passwords).
- *Password History Record* only supported in Web GUI.

15.2.BMC System Root User

System root user in BMC Linux OS, can be used to access smashcli by ssh or telnet.
User name: sysadmin(Fixed, cannot be changed)
Default password: superuser

15.2.1. User Security

Username and Password Security
- Username is fixed, cannot be changed.
- Password must be at least 8 characters long.
- Password must be include Special, Uppercase, Lowercase characters and Numbers.
- White space is not allowed.
- Not allow more than 64 characters.

15.3.SNMP User

SNMP user used to support SNMP Get/Set.

- Default read community: cmccread and inspur@0531
- Default write community: cmccwrite
- SNMPV3 support user authentication, supported authentication algorithm is SHA and MD5;
- SNMPV3 support user privacy , supported privacy algorithm is DES and AES;
- Default SNMPV3 user is **sysadmin**, authentication algorithm is **MD5**, authentication password is **rootuser**; privacy algorithm is **DES**, privacy password is **rootuser.**

15.3.1. User Security

- SNMPV3 support user authentication, supported authentication algorithm is SHA and MD5;
- SNMPV3 support user privacy , supported privacy algorithm is DES and AES;

15.4.User Privilege

15.4.1. User privilege for IPMI

BMC has two ways to receive IPMI CMD, out-band and in-band.

- **Out-band** mode means sending IPMI CMD to BMC by LAN, BMC will authenticate user and password.
- **In-band** mode means sending IPMI CMD in HOST OS. In this mode, IPMI CMD no need authenticating user and password, because he will get highest privilege if someone access HOST OS. So if user forget password or password expired, this is a way to change password or disable password security rules.

Please refer to IPMI 2.0 Spec, Appendix G - Command Assignments. Common privilege as below:

Table 32 User Privilege for IPMI

User Privilege	Supported Operation
Administrator	Write/Read
Operator	Read Only
User	Read Only
No Access	Non

15.4.2. User privilege for Management Web GUI

Only IPMI/WEB/BMC OS Unified User supports Web GUI.

Table 33 User Privilege for Management Web GUI

Menu	Subdirectory	N	U	O	A
Information	System Information	NA	RO	RO	RW
	History Record	NA	RO	RO	RW
Remote Control	Console Redirection	NA	NA	NA	RW
	Locate Server	NA	NA	NA	RW
	Remote Session	NA	RO	RO	RW
	Virtual Media	NA	RO	RO	RW
	Mouse Mode	NA	RO	RO	RW
Power and Fan	Power Supply Monitor	NA	RO	RO	RW
	Server Power Control	NA	RO	RO	RW
	Power Peak	NA	RO	RO	RW
	Fan Speed Control	NA	RO	RO	RW
BMC Setting	BMC Network	NA	NA	RO	RW
	Services	NA	RO	RO	RW
	NTP	NA	RO	RO	RW
	SMTP	NA	NA	NA	RW
	Alerts	NA	NA	RO	RW
	BMC Share NIC Switch	NA	NA	NA	RW
	BIOS Boot Options	NA	RO	RO	RW
Logs	System Event Log	NA	RO	RO	RW
	BMC System Audit Log	NA	RO	RO	RW
	Black Box Log	NA	NA	RO	RW
	Event Log Setting	NA	RO	RO	RW
	BMC System Audit Log Setting	NA	RO	RO	RW
Fault Diagnosis	BMC Self-inspection Result	NA	RO	RO	RW
	BMC Recovery	NA	RO	RO	RW
	Capture Screen	NA	NA	NA	RW
	Host POST Code	NA	RO	RO	RW
Administrator	User Administration	NA	NA	RO	RW
	Security	NA	RO	RO	RW
	Dual Image configuration	NA	NA	NA	RW
	Dual Firmware Update	NA	NA	NA	RW
	BIOS FW Update	NA	NA	NA	RW
	CPLD Update	NA	NA	NA	RW
	PSOC Update	NA	NA	NA	RW
	Restore Factory Default	NA	NA	NA	RW

Note

N = No Access Privilege level
U = User Privilege level
O = Operator Privilege level
A = Administrator Privilege level

RW = Support Read and Write operation
RO = Support Read operation only

For “Operator” and “User” privilege, if with RO attribute, the settings are visible, but the input fields and buttons are disabled, so user cannot modify the settings; if with NA attribute, the settings are invisible and no operation can be taken. When “No Access” privilege cannot login Web GUI.

15.4.3. User privilege for Smashclp

CMD	Sub CMD	N	U	O	A	R
ipconfig	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
sensor	get	NO	YES	YES	YES	YES
fru	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
chassis	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
user	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
mc	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
fan	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
psu	get	NO	YES	YES	YES	YES
	set	NO	NO	NO	YES	YES
password	get	NO	NO	NO	NO	YES
sol	get	NO	NO	NO	YES	YES
id	set	NO	YES	YES	YES	YES
register	get	NO	NO	NO	YES	YES
	set	NO	NO	NO	YES	YES
diagnose	get	NO	NO	NO	YES	YES
diaglog	get	NO	NO	NO	NO	YES

Note

N = No Access Privilege level of Unified User
U = User Privilege level of Unified User
O = Operator Privilege level of Unified User
A = Administrator Privilege level of Unified User
R = Root user - sysadmin of BMC OS

YES = Support
NO = Not Support

16. Protocol and ports

BMC support network connection manager library to configure networking services configuration in run-time. RCMP+, HTTP/HTTPS, KVM, CD-MEDIA, FD-MEDIA, HD-MEDIA, SSH, TELNET and SOLSSH services are supported so far. User can enable or disable theses services, configure communication port, the session timeout value of the service and the maximum number of allowed sessions for the services.

Table 34 Protocol and Ports

Service	Usage	Default State	Non-Security Port	Security Port	Default Port	Timeout(s)	Max Session
RMCP+	IPMI	Enable	623	N/A	N/A	1800	20
HTTP/HTTPS	Web GUI	Enable	80(Http)	443(Https)	443(Https)	1800	20

Service	Usage	Default State	Non-Security Port	Security Port	Default Port	Timeout(s)	Max Session
KVM	Console Redirection	Enable	7578	7582	7578	1800	4
cd-media	Virtual Media	Enable	5120	5124	5120	N/A	4
fd-media	Virtual Media	Enable	5122	5126	5122	N/A	4
hd-media	Virtual Media	Enable	5123	5127	5123	N/A	4
Ssh	ssh	Disable	N/A	22	22	600	N/A
telnet	telnet	Disable	23	N/A	23	600	N/A
solssh	sol by ssh	Enable	52123	N/A	N/A	60	N/A

Note1: Http/Https(WEB) Timeout, if there is no web request in Timeout, web session will be delete, and new web request will not respond, if web page have not auto update, web will logout when you change page or refresh page.

Note2: Telnet is a non-security protocol, if not used, we suggest you disable it.

Fixed Protocols could not be configured.

Table 35 Fixed Protocols

Service	Usage	State	Port
SNMP	SNMP Get/Set	Enable	161
syslog	syslog	Enable	514
Websockify	KVM on HTML5	Enable	9666
Websockify	Virtual Media on HTML5	Enable	9999
srvloc	Sever location	Enable	427
smux		Enable	199

17. Time and NTP

BMC support that system describes instants in time. It's defined as the number of seconds have elapsed since 00:00:00 1970/01/01 and time can be referenced as timestamp for other BMC application.

By interface such as WEB UI, user is able to get current system date and time information or configure either date and time or synchronize date and time through NTP.

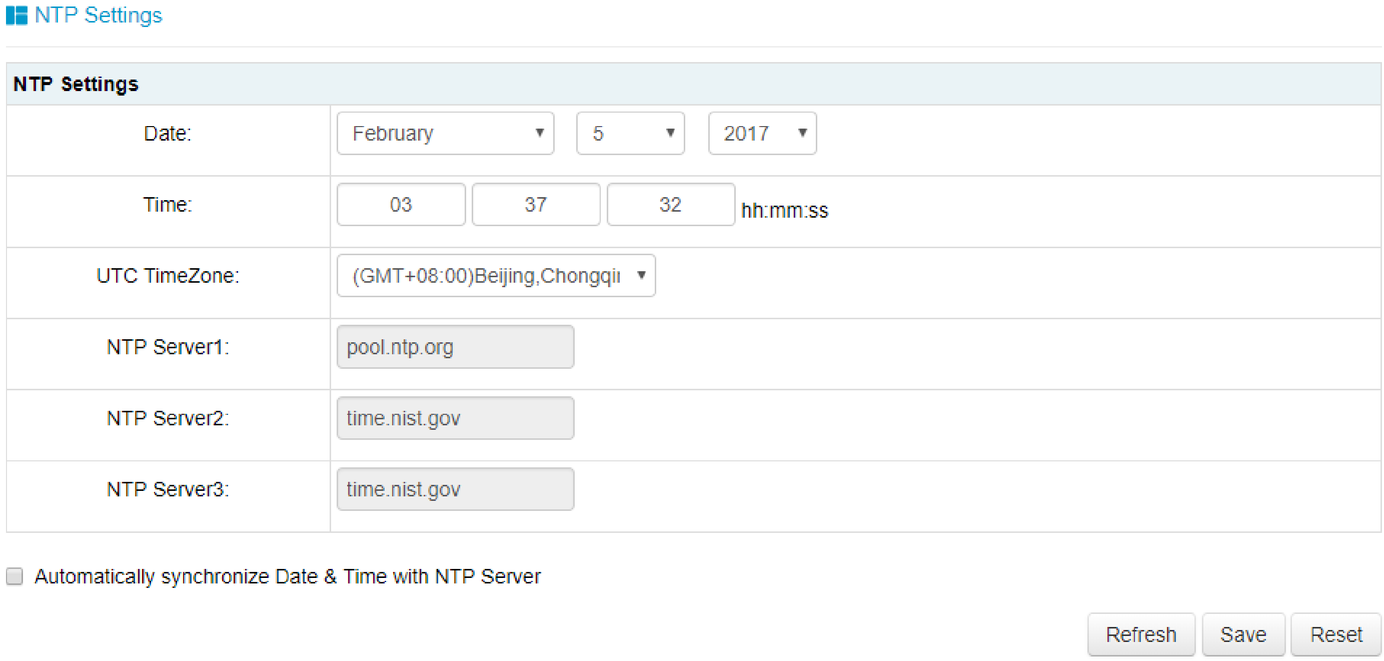
Table 36 Time and NTP

Mode	State	UTC Timezone	NTP Server1	NTP server2	NTP Server3
Manual	Disable	N/A	N/A	N/A	N/A
NTP	Enable	GMT+8	pool.ntp.org	time.nist.gov	time.nist.gov

Time Synchronization

- BMC will synchronize time with ME after BMC running.
- BIOS will synchronize time to BMC when beginning of BIOS POST.
- If NTP Enabled and NTP servers are accessible, BMC will synchronize time with NTP servers per hour.

Page "BMC Settings->NTP" in Web GUI displays current BMC time and NTP settings.



NTP Settings

NTP Settings

Date:	February ▾ 5 ▾ 2017 ▾
Time:	03 37 32 hh:mm:ss
UTC TimeZone:	(GMT+08:00)Beijing,Chongqi ▾
NTP Server1:	pool.ntp.org
NTP Server2:	time.nist.gov
NTP Server3:	time.nist.gov

□ Automatically synchronize Date & Time with NTP Server

Figure 39 NTP

18. BIOS and BMC

BIOS and BMC cooperate very closely in the server. BIOS use IPMI command to communicate with BMC by means of KCS interface on LPC bus.

BIOS provides following features to BMC.

- Sync Host RTC time with BMC by "Set SEL Time Command".
- Provide BMC information and configure BMC in BIOS Setup Menu.
- Provide System Inventory information, like CPU and DIMM to BMC.

BMC provides following features to BIOS.

- FRB2 supported by means of IPMI Watchdog Timer Command (Please refer BMC Watchdog Chapter.)
- BIOS firmware update and ME firmware update
- BIOS Setup Menu Configuration
- SEL repository device for System event logging
- BIOS Port80 POST code redirection to certain BMC GPIO group

- NMI to PCH, Non Maskable Interrupt. The highest priority interrupt in the system, after SMI. This interrupt has traditionally been used to notify the operating system fatal system hardware error conditions, such as parity errors and unrecoverable bus errors. It is also used as a Diagnostic Interrupt for generating diagnostic traces and ‘core dumps’ from the operating system.

The AST2500 SOC also acts as a Super I/O (SIO), which provides system serial port to host. When SOL is activated, BMC redirect the System UART to BMC UART to reach SOL feature. For details, please refer to “Serial over LAN” Chapter.

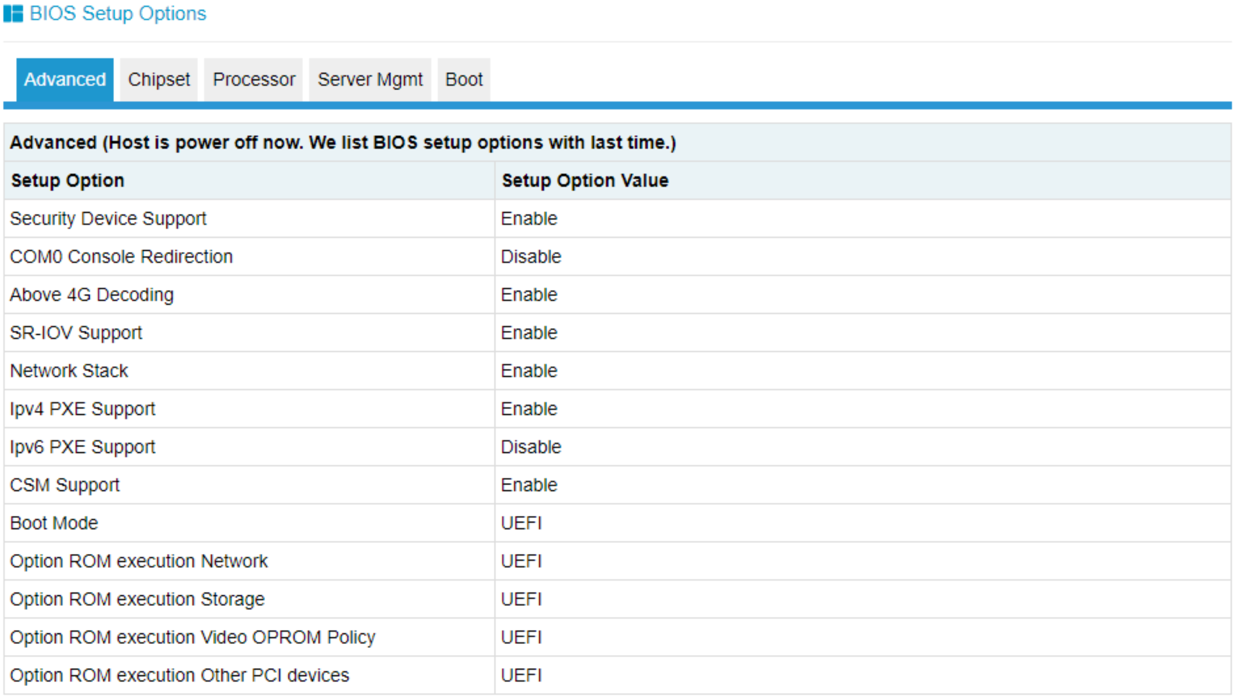
Note The LPC interface to the host is used for SIO and BMC communication. The LPC addressing of SIO and BMC could be different. For example, the BMC LPC addressing is 0x2E, and the SIO addressing is 0x4E.

18.1.BIOS Setup Options

BMC support BIOS Setup Option getting and setting.

- BIOS sends BIOS Setup Options to BMC When BIOS POST Complete.
- User can use IPMI OEM CMD to change setup option value. BIOS will update setup option after next system restart.

Page “Information-> BIOS Setup Options” in Web GUI displays BIOS Setup Options.



Advanced (Host is power off now. We list BIOS setup options with last time.)

Setup Option	Setup Option Value
Security Device Support	Enable
COM0 Console Redirection	Disable
Above 4G Decoding	Enable
SR-IOV Support	Enable
Network Stack	Enable
Ipv4 PXE Support	Enable
Ipv6 PXE Support	Disable
CSM Support	Enable
Boot Mode	UEFI
Option ROM execution Network	UEFI
Option ROM execution Storage	UEFI
Option ROM execution Video OPROM Policy	UEFI
Option ROM execution Other PCI devices	UEFI

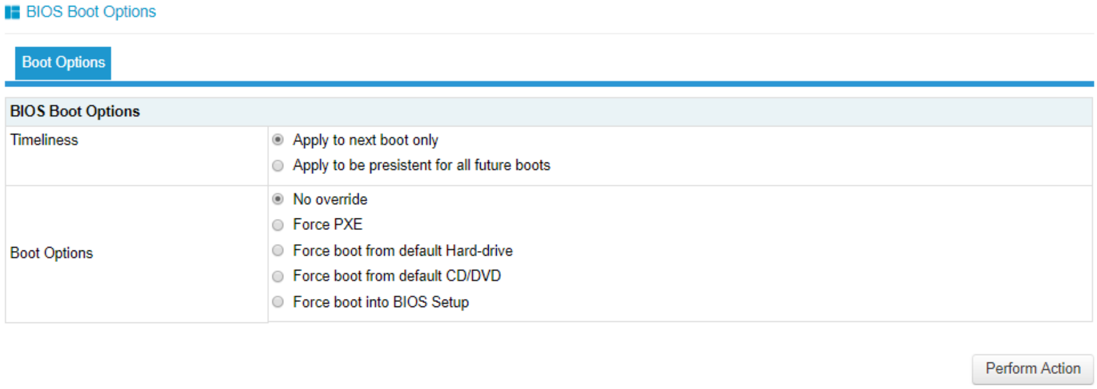
Figure 40 BIOS Setup Options

18.2.BIOS Boot Options

BMC provide a method to set BIOS Boot Option by out-band.

- BMC sets boot option parameters by “Set System Boot Options Command” or WEB GUI. It is used to set parameters that direct the system boot following a system power up or reset.
- The boot flags only apply for one system restart. When BIOS POST, BIOS reads boot option parameters by “Get System Boot Options Command”, and modify boot device to related device. And then BIOS clear boot options parameters by “Set System Boot Options Command”.
- Boot flags will be cleared in 60s after setting boot option by BMC. So, system must restart within 60 seconds, otherwise the BIOS startup option action will be invalid.
- BIOS will get mode and boot device by “Get System Boot Options Command”. Two mode supported:
  - **Apply to next boot only**, means BIOS uses configured boot device only one time, and next boot, BIOS will first boot on last configured device in BIOS Setup.
  - **Apply to be persistent for all future boots**, means BIOS will change first boot option to configured device in BIOS Setup, and then BIOS will boot on the device all future boots if BIOS Setup not changed. Note: In this mode, BIOS Setup will be changed.
- Boot Devices Options:
  - No override
  - Force PXE
  - Force boot from default Hard-drive
  - Force boot from default CD/DVD
  - Force boot into BIOS Setup.

Enter “BMC settings->BIOS Boot Options” page to check and set BIOS Boot Options.



BIOS Boot Options

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 from default CD/DVD ○ Force boot into BIOS Setup

Figure 41 Boot Option

19. Storage

Server storage subsystem generally consists by the RAID, SAS control expand hard disks, BMC physically through the I2C link and access RAID, SAS controller interaction, to access the controller, disk, array and other information, and set up RAID.

Table 37 Currently Supported RAID and SAS

Model	Type	Manufacturer	Speed(G)	Firmware Version
9361-8i	RAID	Broadcom	12	ALL
3108	RAID	Broadcom	12	ALL
3008 IT	SAS	Broadcom	12	14.00.02.00
3008 IR	SAS	Broadcom	12	14.00.02.00
3008 iMR	RAID	Broadcom	12	ALL
9305-16i	SAS	Broadcom	12	
9361-16i	RAID	Broadcom	12	
2208-8i	RAID	Broadcom	6	X
9364-8i	RAID	Broadcom	12	ALL

8060	RAID	Microsemi	12	33083 and above
9300-8e	SAS	Broadcom	12	
9305-24i	SAS	Broadcom	12	
9460-8i	RAID	Broadcom	12	
9460-16i	RAID	Broadcom	12	
9400-8i	SAS	Broadcom	12	
9400-16i	SAS	Broadcom	12	
9440-8i	RAID	Broadcom	12	
9440-16i	RAID	Broadcom	12	
3408 IT	SAS	Broadcom	12	
3408 iMR	RAID	Broadcom	12	
3508	RAID	Broadcom	12	
3154-8i	RAID	Broadcom	12	
HBA1100	SAS	Microsemi	12	
SmartHBA2100	SAS	Microsemi	12	
3152-8i	RAID	Microsemi	12	
3154-8i	RAID	Microsemi	12	

Schematic that BMC access RAID/SAS controller:

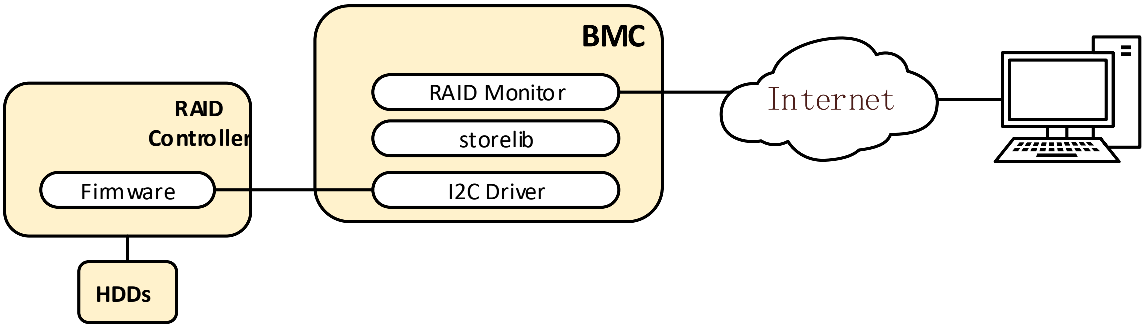


Figure 42 Schematic that BMC Access RAID/SAS Controller

Table 38 Storage Management Information

Device	Monitored Information
RAID controller	Product Name Serial Number Vendor(ID) SubVendor(ID) Device(ID) SubDevice(ID) Host Interface Firmware Version WebBIOS Version BIOS Version Firmware Package Version Firmware Time Device Interface Chip Temperature (Cel) Unconfigured Good Spin Down Hot Spare Spin Down Cluster Mode NCQ Coercion Mode Alarm Control

	Smart Copyback Enabled Auto Rebuild SAS Address Port Count Drive Count Virtual Drive Count NVRAM Size(KB) Memory Size(MB) Flash Size(MB) Min Strip Size(KB) Max Strip Size(KB) Spin Down Time(Minutes) Rebuild Rate Back Ground Init(BGI) Rate Consistency Check(CC) Rate Reconstruction Rate S.M.A.R.T Polling Cache Flush Interval(s) Spinup Drive Count Spinup Delay Controller BIOS Shield State Supported Maintain PD Fail History Battery Warning
Hard disk	Device ID Enclosure ID Firmware State Media Type Vendor(ID) Product Revision Level Max Speed (Gbps) Temperature (Cel) Raw Size (GB) Media Error Count User Data Block Size (B) Certified Disabled for Removal FW Download Allowed Security Rebuild Locate Copy Back Slot Number Connected Port Power State Device Interface Product ID Vendor Specific Info Negotiated Link Speed (Gbps) SAS Address Coerced size (GB) Predictive Fail Count Emulated Block Size (B) Is Path Broken FDE Capable Emergency Spare Commissioned Hotspare

	Clear All Data Secure Erase Patrol Read
Enclosure	Device ID Enclosure is Faulty Slot Count Internal Index Enclosure Type Drive Count

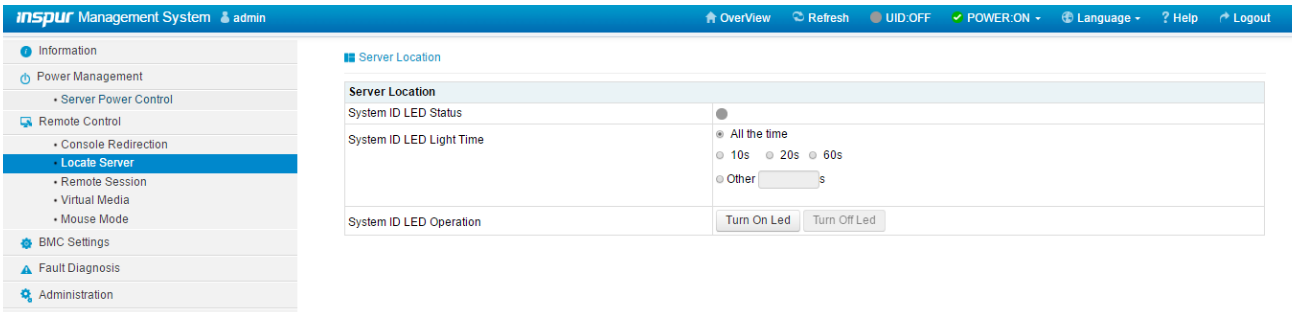
20. Server Control

20.1.Server Location

The managed server can be located by means of UID LED.

- User can control UID LED by BMC IPMI CMD and UID Button separately.
- UID should be turned on/off by UID Button even BMC crashed.

In the “Remote Control -> Locate Server” page, show the status of UID.
Turn on UID: Specify the light time period, and click “Turn On Led” button to turn on UID for specified time.
Turn on UID: Click “Turn Off Led” button to turn on UID.



Server Location	
System ID LED Status	●
System ID LED Light Time	◉ All the time ○ 10s ○ 20s ○ 60s ○ Other s
System ID LED Operation	Turn On Led Turn Off Led

Figure 43 Server Location

20.2.Server Virtual Power Button

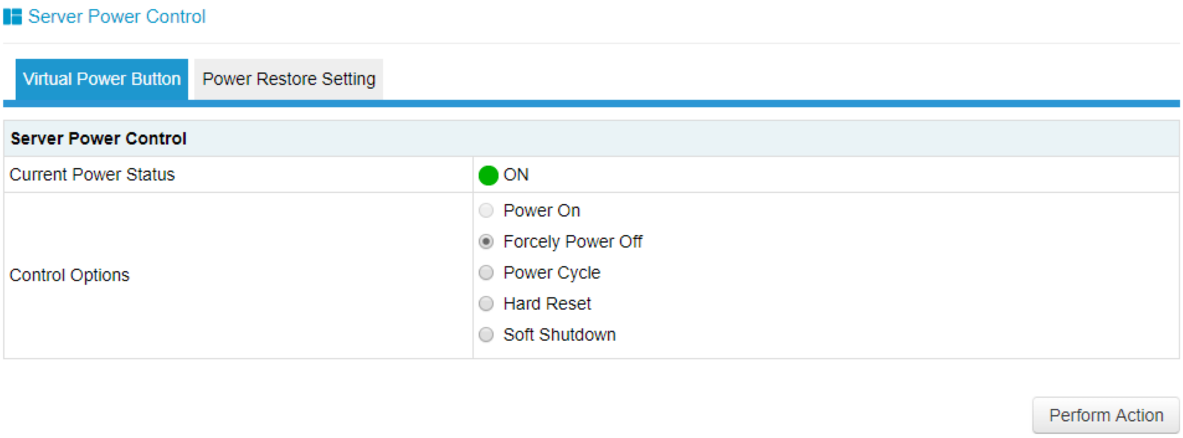
This function allows user to power on, off, and reset the managed server via BMC.

- Power on, same to short time pressing power button.
- Power off, forcedly power off, same to long time (more than 4s) pressing power button.
- Soft shutdown, orderly power off, same to short time pressing power button. Note: Soft shutdown will be available after Power Button Policy setting correctly in OS.
- Power reset, same to short time pressing reset button (if present).
- Power cycle, Power off, delay 10s, Power on.

Supported:

Web GUI
IPMI command based on IPMI2.0.

Page “Remote Control -> Server Power Control” shows current power status. User can perform power control actions.



Server Power Control

Server Power Control	
Current Power Status	● ON
Control Options	○ Power On ● Forcely Power Off ○ Power Cycle ○ Hard Reset ○ Soft Shutdown

Figure 44 Virtual Power Button

21. Power Supply and Power Consumption

21.1.Power Supply Redundancy

BMC usually support PSU Redundancy, means if one or more PSU cannot normally output power, server will work normally powered by other power supply, but redundancy sensor will alert event.

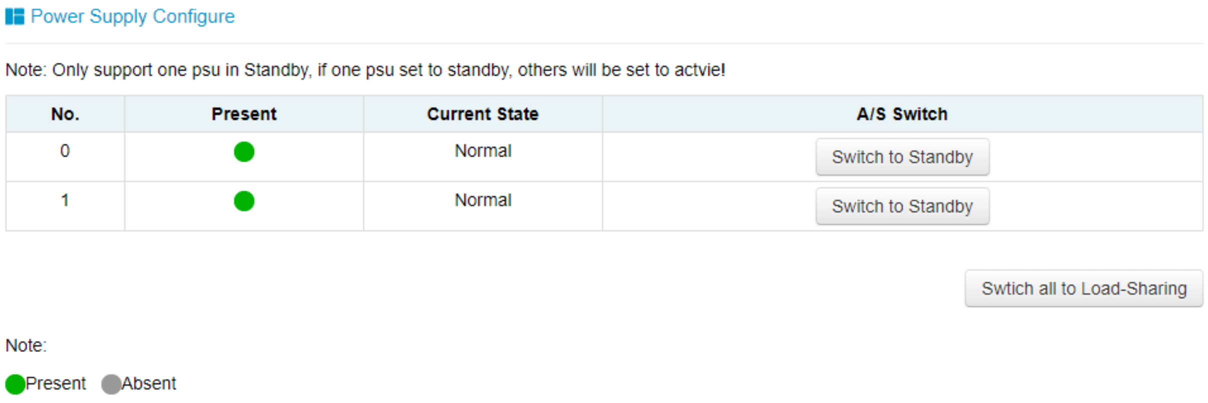
21.2.PSU Active Standby

In the case of meeting the normal work, BMC provides a way to manually set the power supply to standby to improve power conversion efficiency.

PSU defaults Activate-Activate mode, and if switch to Active-Standby mode, as the power supply is critical, the work need to do under the guidance of professional engineer.

In the case of meeting business power consumption, reduce part of the power supply by 0.3V, suppress the standby current output by the voltage difference, and the system powered by the main power system. The power supply is in a hot standby state, once the main power supply is abnormal, standby power switch to the main power supply smoothly without affecting the service

Conditions that standby power switch to the main power:
1. Main power supply are pulled out;
2. Main power supply output voltage is low or no output；
3. Main power supply temperature is too high, input loss, overcurrent, or overvoltage;
4. System power as a percentage of main power supply rated power reach the upper limit



Power Supply Configure

Note: Only support one psu in Standby, if one psu set to standby, others will be set to actvie!

No.	Present	Current State	A/S Switch
0	●	Normal	Switch to Standby
1	●	Normal	Switch to Standby

Note:
● Present ● Absent

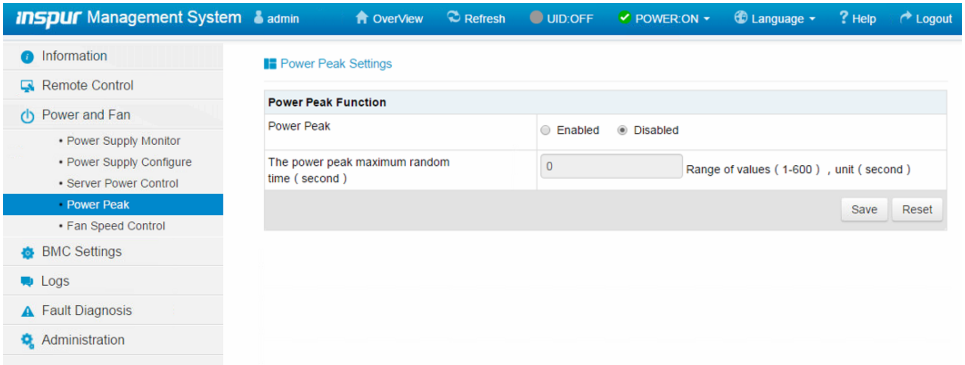
Figure 45 PSU Active Standby

21.3.Power Peak

Power peak is used to prevent many servers from being started at the same time when first time A/C power is restored, which would cause heavy power loading.

- Power peak could be enabled or disabled. Default disabled.
- When it is enabled, user can configure maximum random time.
- BMC will power on server with a random time delay within the time configured.

Click Power and Fan -> Power Peak to go to the configuration page.



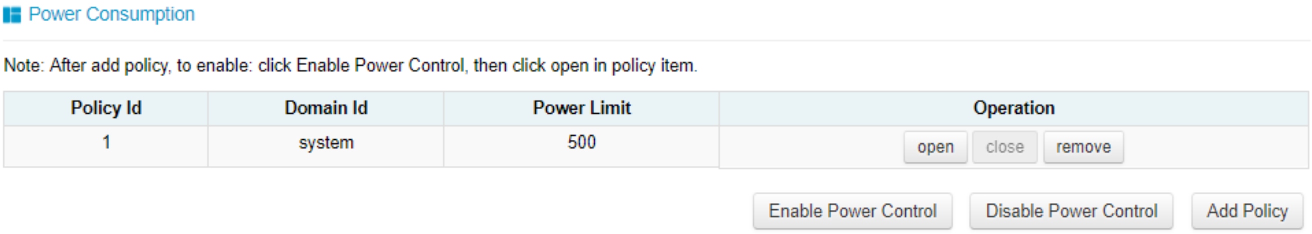
Power Peak Function	
Power Peak	○ Enabled ● Disabled
The power peak maximum random time (second)	0 Range of values (1-600) , unit (second)

Figure 46 Power Peak

21.4.Power Limit

BMC provides power cap function, power cap function sets the power limit for the system, and when the system power exceeds this upper limit, Intel ME will slow down the CPU to reduce power consumption. Power cap will affect the server performance, professional maintenance personnel will operate when needed.

WEB GUI, go to page “Power and Fan->Power Consumption” to check and configure



Note: After add policy, to enable: click Enable Power Control, then click open in policy item.

Policy Id	Domain Id	Power Limit	Operation
1	system	500	open close remove

Figure 47 Power Limits

21.5.Power Consumption Statistics and History Record

BMC provides inlet temperature, power monitoring and statistical data calculated based on the curve. Administrators can gain insight into the actual use of electricity and cooling resources through energy monitoring devices. Users can optimize the server's energy savings based on historical data

WEB GUI, go to page “Power Management-> Power statistics”, and this page displays the system current power, CPU total power, total memory power and a specific period of peak power, average power, the cumulative power consumption.

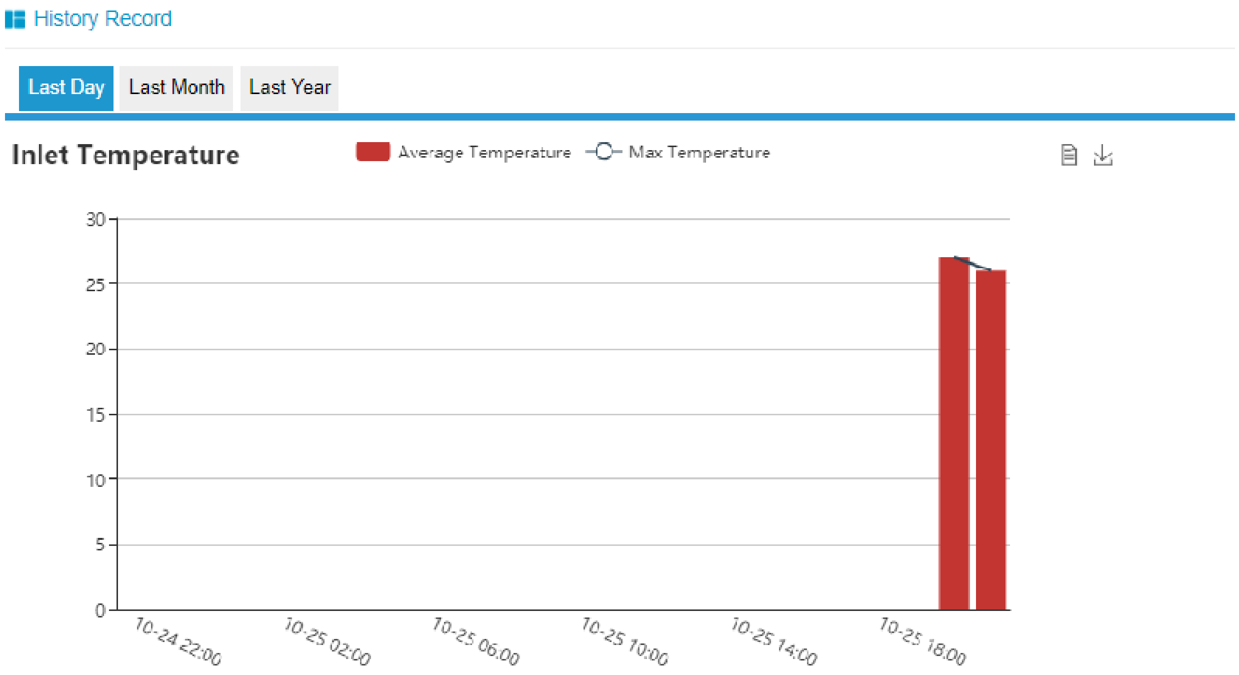
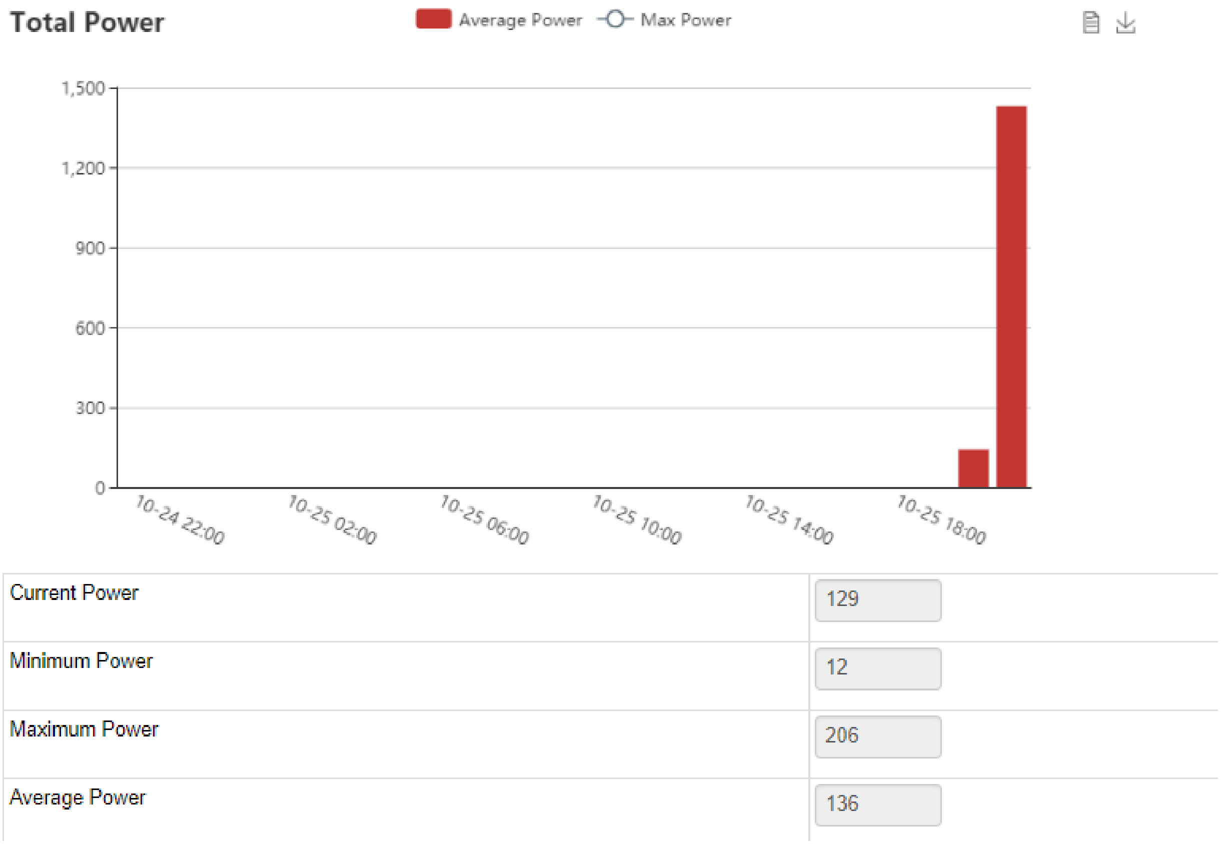


Figure 48 Inlet Temperature History Record



Current Power	129
Minimum Power	12
Maximum Power	206
Average Power	136

Figure 49 Total Power History Record

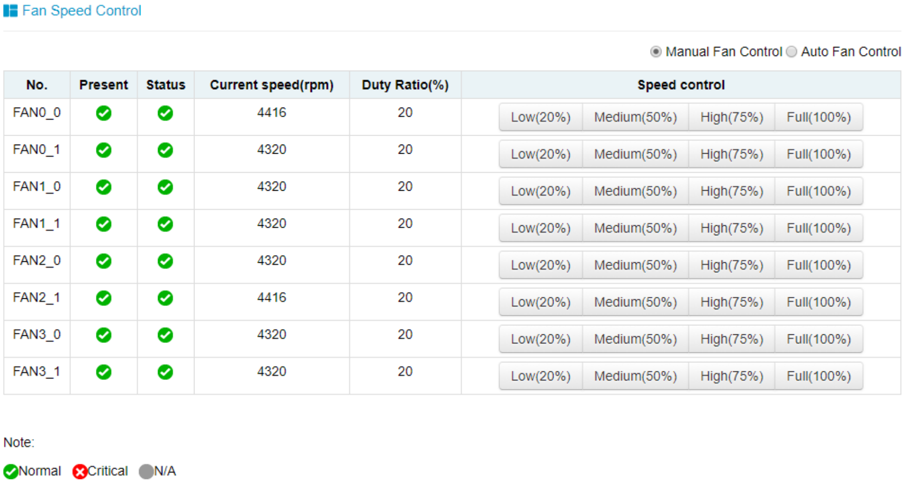
22. Fan Speed Control (FSC)

22.1.Fan Speed Control

BMC default support Auto Fan Control, the fan module speed is control by the algorithm provided by thermal team.

User can enable Manually Fan Control in Web GUI, if enabled, user can select one of four fan speed predefined for each fan module. These predefined fan speed are Low, Medium, High and Full. Manual configuration is store in EEPROM, will be available after BMC reset or FW Upgraded.

Click Power and Fan > Fan Speed Control to go to the configuration page. Select Manually Fan Control, and click the fan speed you want. In the Duty Ratio filed, user can see the duty ratio of the fan module. In this page, user can know the presence of the fan module, and their status as well.



Fan Speed Control

● Manual Fan Control ○ Auto Fan Control

No.	Present	Status	Current speed(rpm)	Duty Ratio(%)	Speed control
FAN0_0	✓	✓	4416	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN0_1	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN1_0	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN1_1	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN2_0	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN2_1	✓	✓	4416	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN3_0	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)
FAN3_1	✓	✓	4320	20	Low(20%) Medium(50%) High(75%) Full(100%)

Note:

✓Normal ✗Critical ●N/A

Figure 50 Fan Speed Control

22.2.Fan Speed Control (FSC) Watchdog

MCU or CPLD will monitor BMC Fan control task by receiving BMC watchdog signal.
If MCU or CPLD cannot receive watchdog signal in 4 Mins, all Fans will be set to full speed to avoid system over hot.

23. Firmware Update

23.1.BMC Firmware Update

BMC support dual BMC firmware image. BMC flash contains two images(BMC flash size is 64M, BMC firmware image size is 32M).
Supported Upgrade mode:

- WEB update, user login Web GUI and enter flash page to update firmware. This is a sideband mode, supports Firmware Integrity Checking and preserve configurations. It is a suggested update mode.
- SOCflash tool update, SOCflash tool used in DOS/Windows/Linux OS. SOCflash will directly erase and overwrite flash with new image without Firmware Integrity Checking. All configuration will be erased. This is an inband mode, user should accept user permission.

23.1.1. Firmware Integrity Checking

Each firmware image have a MD5 code calculated by MD5 tool(Hash.exe). Before update firmware, user must check integrity using MD5 tool to make sure the firmware image file is the correct one.

23.1.2. Dual image

Dual image means BMC supporting two images in flash, when active image cannot boot, 5 minutes later, BMC will try another image to boot.

23.1.3. WEB Update

BMC firmware update is supported via the Management Web GUI.

- Support hardware watchdog, reference to “Hardware watchdog” in section “BMC Self Recovery”.

When updating BMC firmware, user can specify which image area to update.

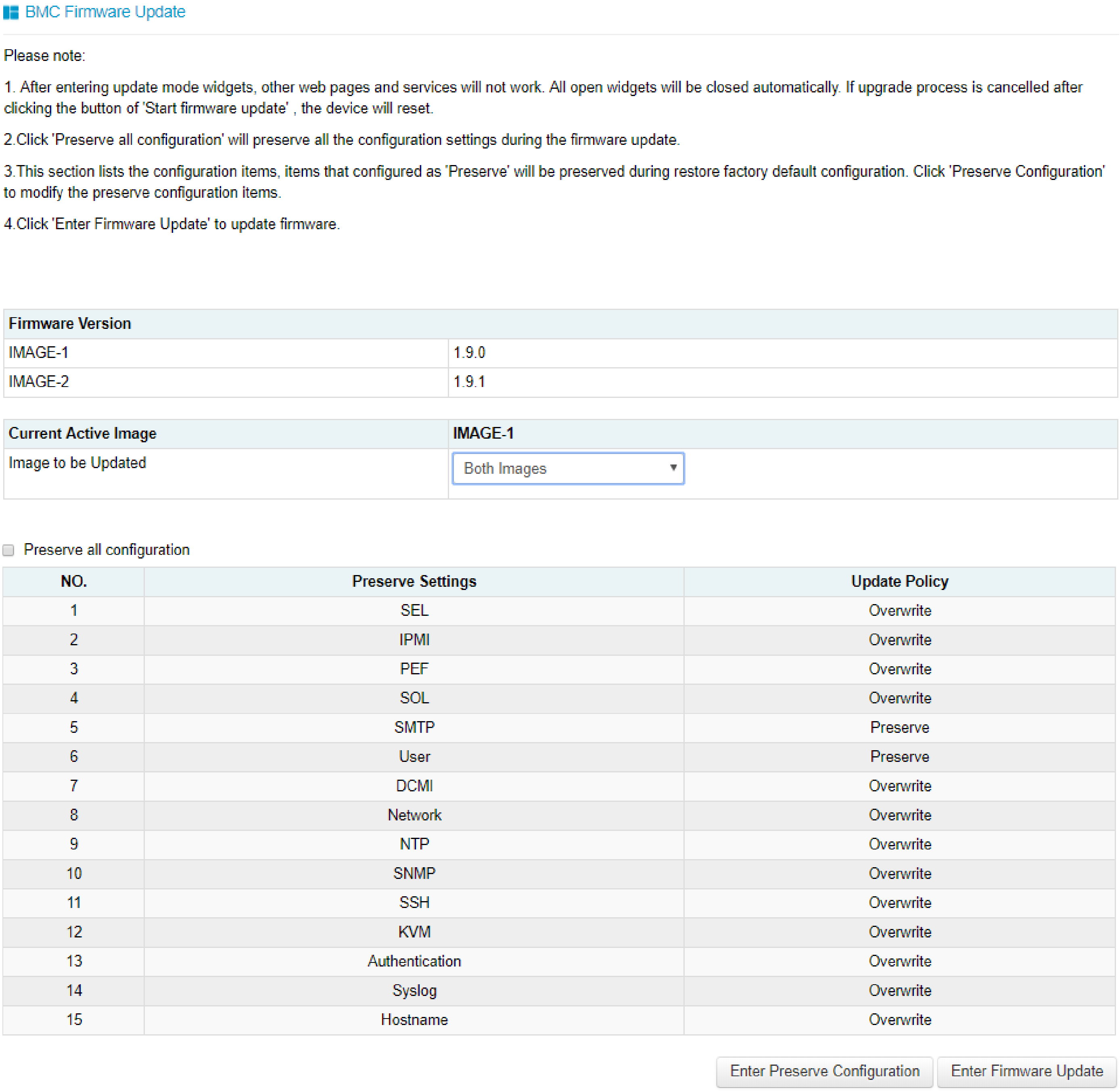
- Image-1
- Image-2
- Inactive image
- Both images(Default)

Configurations can be preserved separately. Reference to Section “Restore Factory Default”.

Note: The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.
Once you enter into Update Mode and choose to cancel the firmware flash operation, BMC must be reset. This means that you must close the Internet browser and log back onto the BMC before you can perform any other types of operations.
The default boot image configure is higher version booting the two image. You can change the value from the web-GUI.

Step 1

Go to flash page “Administration->Dual Image Update”, select image to upgrade, default Both Images, means both image will be upgraded. If configuration should be preserved, click “Enter Preserve Configuration” to select items need to be preserved. Click “Enter Update Mode” to go to upgrade page.



BMC Firmware Update

Please note:

1. After entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled after clicking the button of 'Start firmware update' , the device will reset.

2.Click 'Preserve all configuration' will preserve all the configuration settings during the firmware update.

3.This section lists the configuration items, items that configured as 'Preserve' will be preserved during restore factory default configuration. Click 'Preserve Configuration' to modify the preserve configuration items.

4.Click 'Enter Firmware Update' to update firmware.

Firmware Version	
IMAGE-1	1.9.0
IMAGE-2	1.9.1

Current Active Image	IMAGE-1
Image to be Updated	Both Images ▾

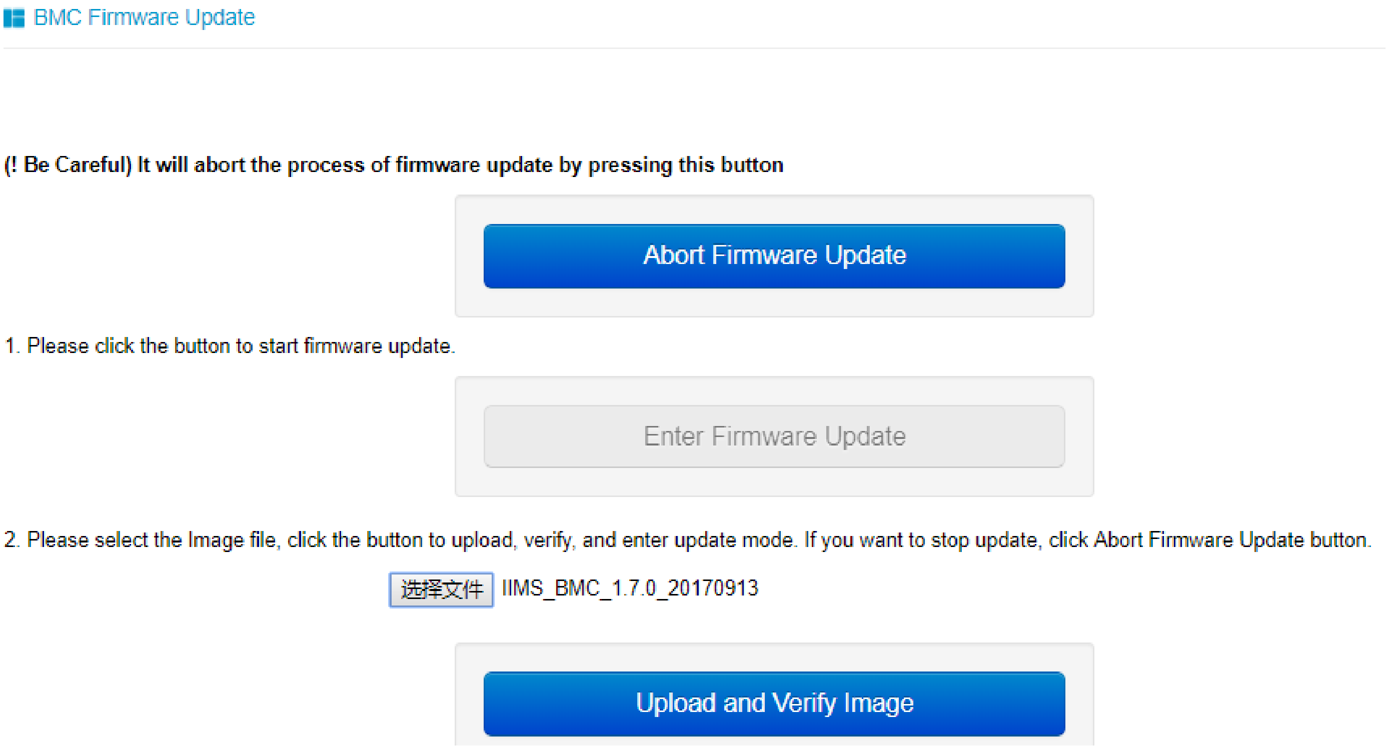
□ Preserve all configuration

NO.	Preserve Settings	Update Policy
1	SEL	Overwrite
2	IPMI	Overwrite
3	PEF	Overwrite
4	SOL	Overwrite
5	SMTP	Preserve
6	User	Preserve
7	DCMI	Overwrite
8	Network	Overwrite
9	NTP	Overwrite
10	SNMP	Overwrite
11	SSH	Overwrite
12	KVM	Overwrite
13	Authentication	Overwrite
14	Syslog	Overwrite
15	Hostname	Overwrite

Figure 51 BMC Upgrade Step 1

Step 2

Select image file, push Upload button to upload file, BMC will go to flash mode after upload file, IPMI service will stop, and then BMC will verify image. Verify:
Size should be 32M
Verify image integrity, it will make sure this is BMC image.
If verify failed, BMC will stop flash and restart.



(! Be Careful) It will abort the process of firmware update by pressing this button

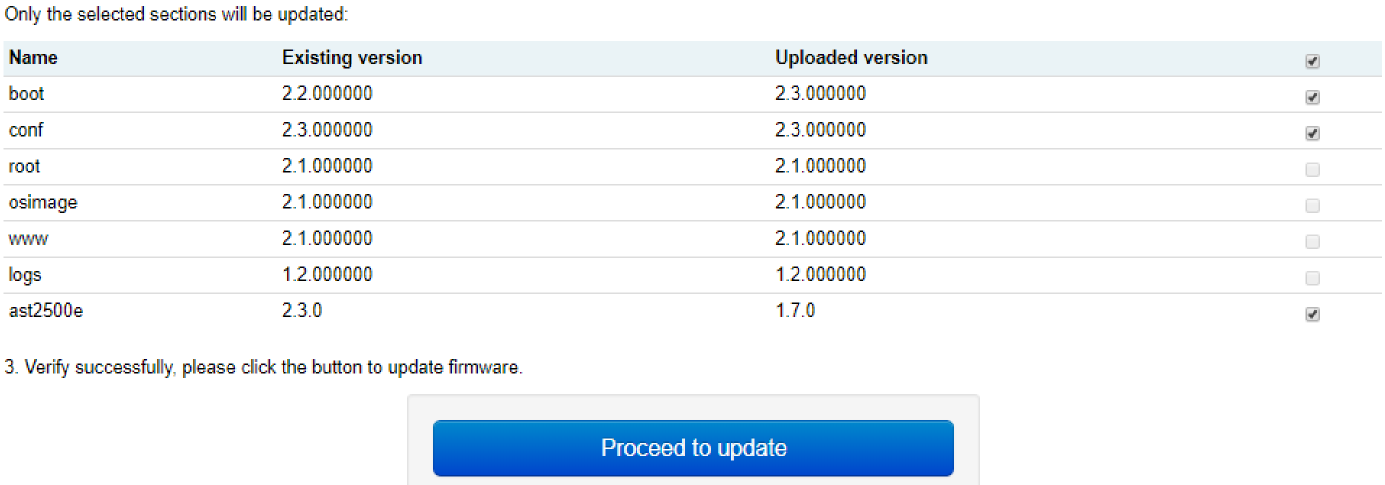
1. Please click the button to start firmware update.

2. Please select the Image file, click the button to upload, verify, and enter update mode. If you want to stop update, click Abort Firmware Update button.

Figure 52 BMC Upgrade Step 2

Step 3

Check image version and current image version, then click “Proceed to Update” button to start upgrading.
Wait about 15mins(2 images), then flash done.


Only the selected sections will be updated:

Name	Existing version	Uploaded version	☑
boot	2.2.000000	2.3.000000	☑
conf	2.3.000000	2.3.000000	☑
root	2.1.000000	2.1.000000	☐
osimage	2.1.000000	2.1.000000	☐
www	2.1.000000	2.1.000000	☐
logs	1.2.000000	1.2.000000	☐
ast2500e	2.3.0	1.7.0	☑

3. Verify successfully, please click the button to update firmware.

Figure 53 BMC Upgrade Step 3

23.1.4. SOC Flash Update

SOCflash tool will directly erase and overwrite flash with new image without Firmware Integrity Checking. All configuration will be erased.
Windows/linux/DOS update BMC, enter DOS or linux shell or windows cmd line, execute following CMDs:

socflash if=Imagefile offset=0x2000000 will update the Image2;
socflash if=Imagefile will update the Image1;

23.2.BIOS Firmware Update

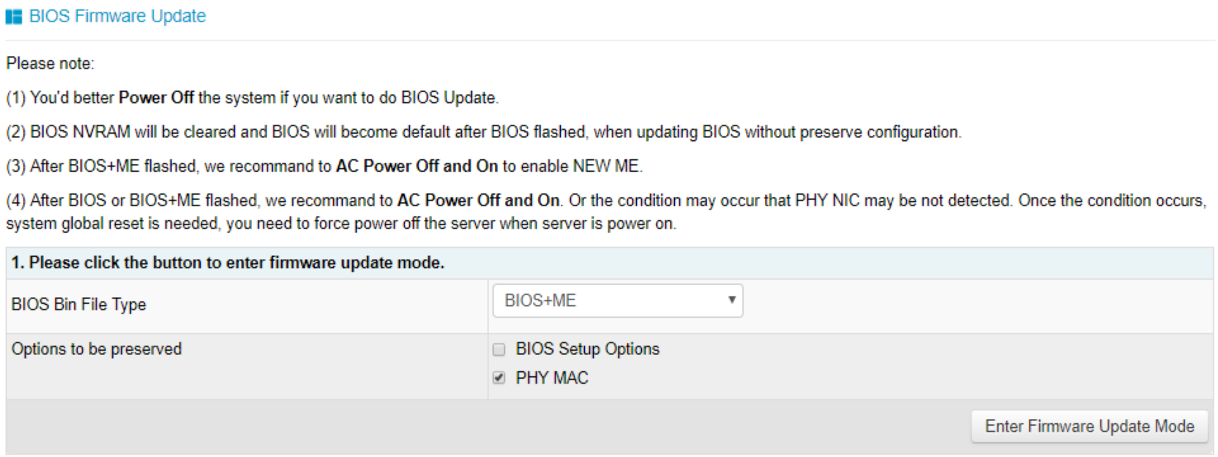
BMC support BIOS Firmware update via the Management Web GUI.

Intel ME firmware is packaged with BIOS firmware as a single firmware image.

- Support two upgrade mode “BIOS+ME” and “BIOS Only”
- Power off the system before perform BIOS firmware update.
- After update BIOS firmware, BIOS NVRAM will be clear, all BIOS configurations will rest to default.
- If we update both BIOS and ME image, in order to make ME firmware take effort, suggest to AC power off the system.

Step 1

Login Management Web GUI, enter “Administrator > BIOS Firmware Update” as shown below. Select BIOS+ME or BIOS only, default BIOS+ME. If you want to preserve BIOS setup options, user need select “BIOS Setup Options”. PHY MAC default selected to be preserved. Click “Enter Firmware Update Mode” button to enter update mode.



BIOS Firmware Update

Please note:

(1) You'd better **Power Off** the system if you want to do BIOS Update.

(2) BIOS NVRAM will be cleared and BIOS will become default after BIOS flashed, when updating BIOS without preserve configuration.

(3) After BIOS+ME flashed, we recommand to **AC Power Off and On** to enable NEW ME.

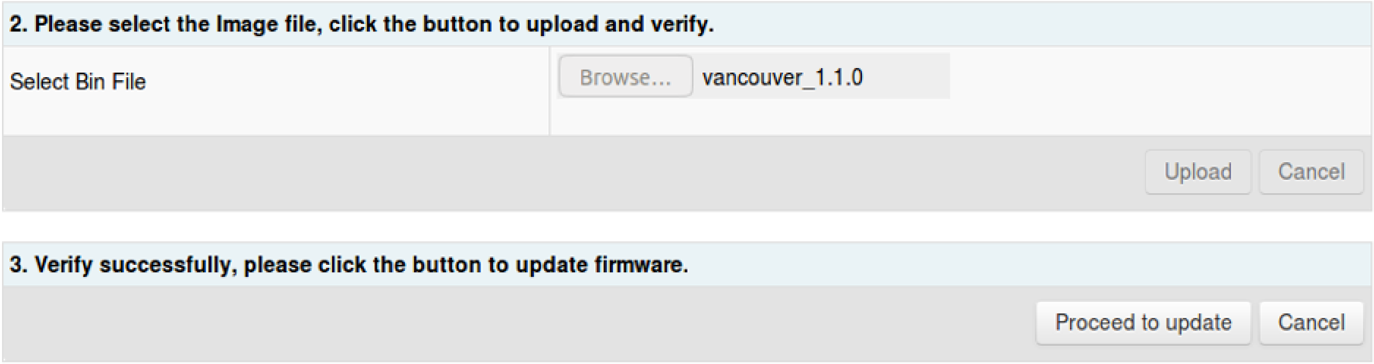
(4) After BIOS or BIOS+ME flashed, we recommand to **AC Power Off and On**. Or the condition may occur that PHY NIC may be not detected. Once the condition occurs, system global reset is needed, you need to force power off the server when server is power on.

1. Please click the button to enter firmware update mode.

BIOS Bin File Type	BIOS+ME ▾
Options to be preserved	□ BIOS Setup Options ☑ PHY MAC

Figure 54 BIOS Upgrade Step 1

Step 2



2. Please select the Image file, click the button to upload and verify.

Select Bin File: vancouver_1.1.0

3. Verify successfully, please click the button to update firmware.

Figure 55 BIOS Upgrade Step 2

Select image file, click “Upload” button to upload file, ME will go to recovery mode, and then BMC will verify image. Verify:

Size should be 32M
Verify image integrity, it will make sure this is BIOS image.

If verify failed, BMC will stop flash, and will change ME to Normal mode.

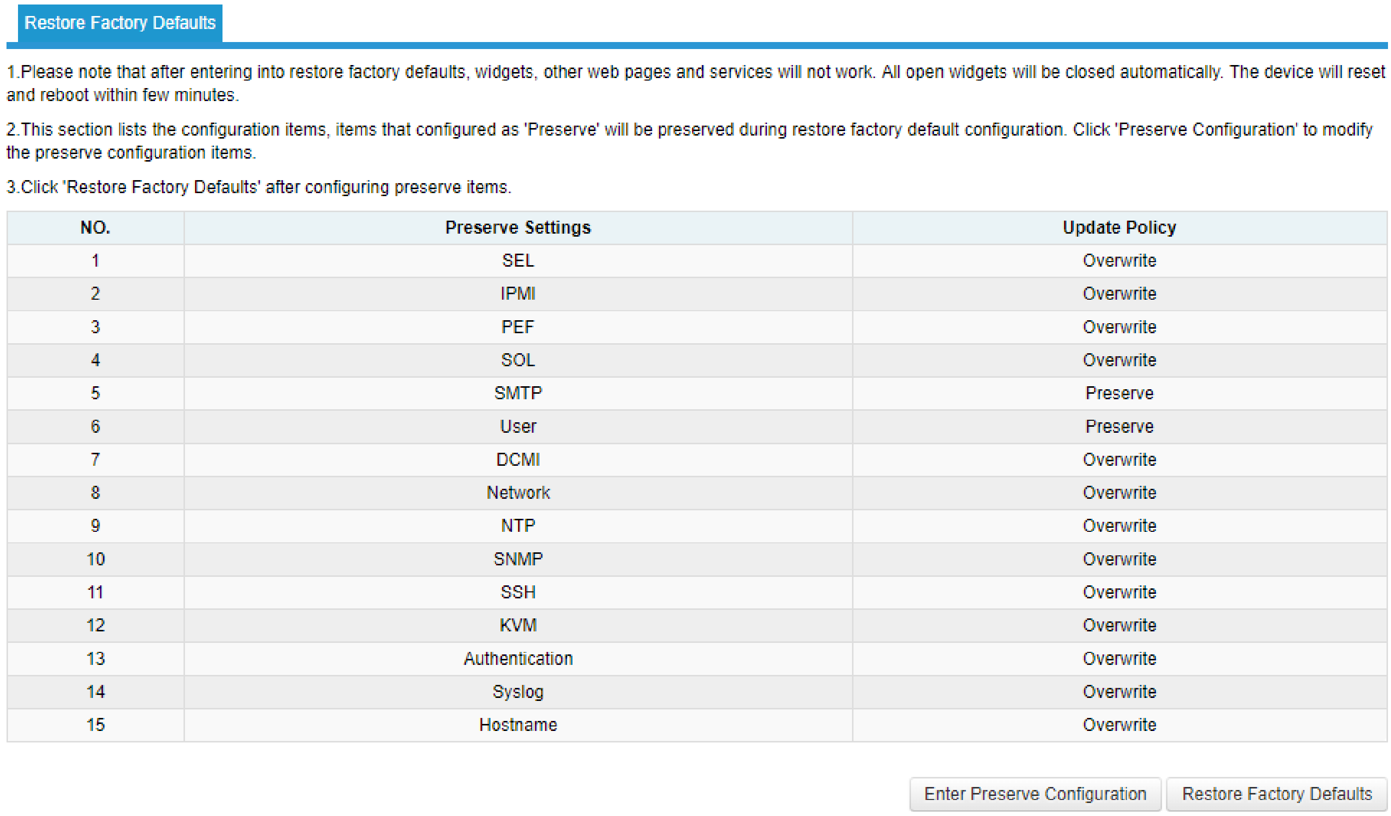
If verify succeed, click “Proceed to update” to start upgrade. Wait about 3 mins, then flash done.

23.3.CPLD FW update

BMC uses JTAG to update CPLD. Support Web GUI update.

24. Restore Factory Default

BMC support restore factory default in Web GUI. Go to page “Administration->Restore Factory Defaults” to check and configure.



1.Please note that after entering into restore factory defaults, widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

2.This section lists the configuration items, items that configured as 'Preserve' will be preserved during restore factory default configuration. Click 'Preserve Configuration' to modify the preserve configuration items.

3.Click 'Restore Factory Defaults' after configuring preserve items.

NO.	Preserve Settings	Update Policy
1	SEL	Overwrite
2	IPMI	Overwrite
3	PEF	Overwrite
4	SOL	Overwrite
5	SMTP	Preserve
6	User	Preserve
7	DCMI	Overwrite
8	Network	Overwrite
9	NTP	Overwrite
10	SNMP	Overwrite
11	SSH	Overwrite
12	KVM	Overwrite
13	Authentication	Overwrite
14	Syslog	Overwrite
15	Hostname	Overwrite

Figure 56 Restore Factory Default

Note: Update policy “Overwirte” means selected item will be overwritten to default after click “Restore Factory Default” or Upgrade BMC; “Preserve” means selected item will be restored after click “Restore Factory Default” or Upgrade BMC.

Table 39 Restore Factory Default

Items	Preserved configuration	Note
SEL	SEL Log	
IPMI	IPMI, include PEF data ,SOL data, IPMI user information ,SMTP,DCMI data etc.	
PEF	PEF	Select IPMI option while include this configuration.
SOL	SOL	Select IPMI option while include this configuration
SMTP	SMTP	Select IPMI option while include this configuration
User	IPMI User	Select IPMI option while include this configuration
DCMI	DCMI	DCMI, Select IPMI option while include this configuration
Network	BMC Network	
NTP	NTP	
SNMP	SNMP	
SSH	SSH	
KVM	KVM and Virtual Media Devices	

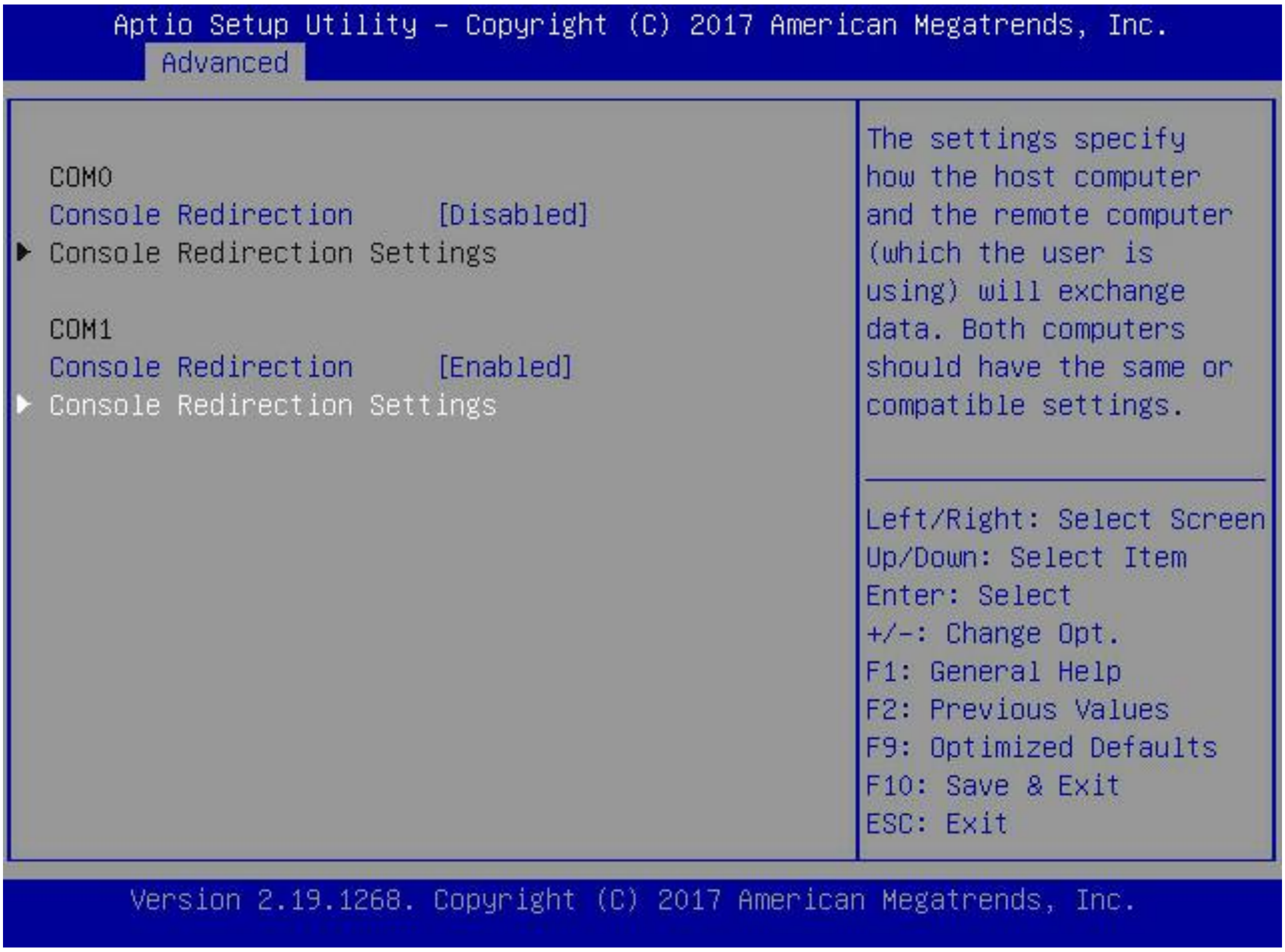
Authentication	Authentication, include LADP and superuser	
Syslog	Syslog	
Hostname	Hostname	

25. Serial Over LAN (SOL) and System Serial Log Recording

25.1.Serial Over LAN

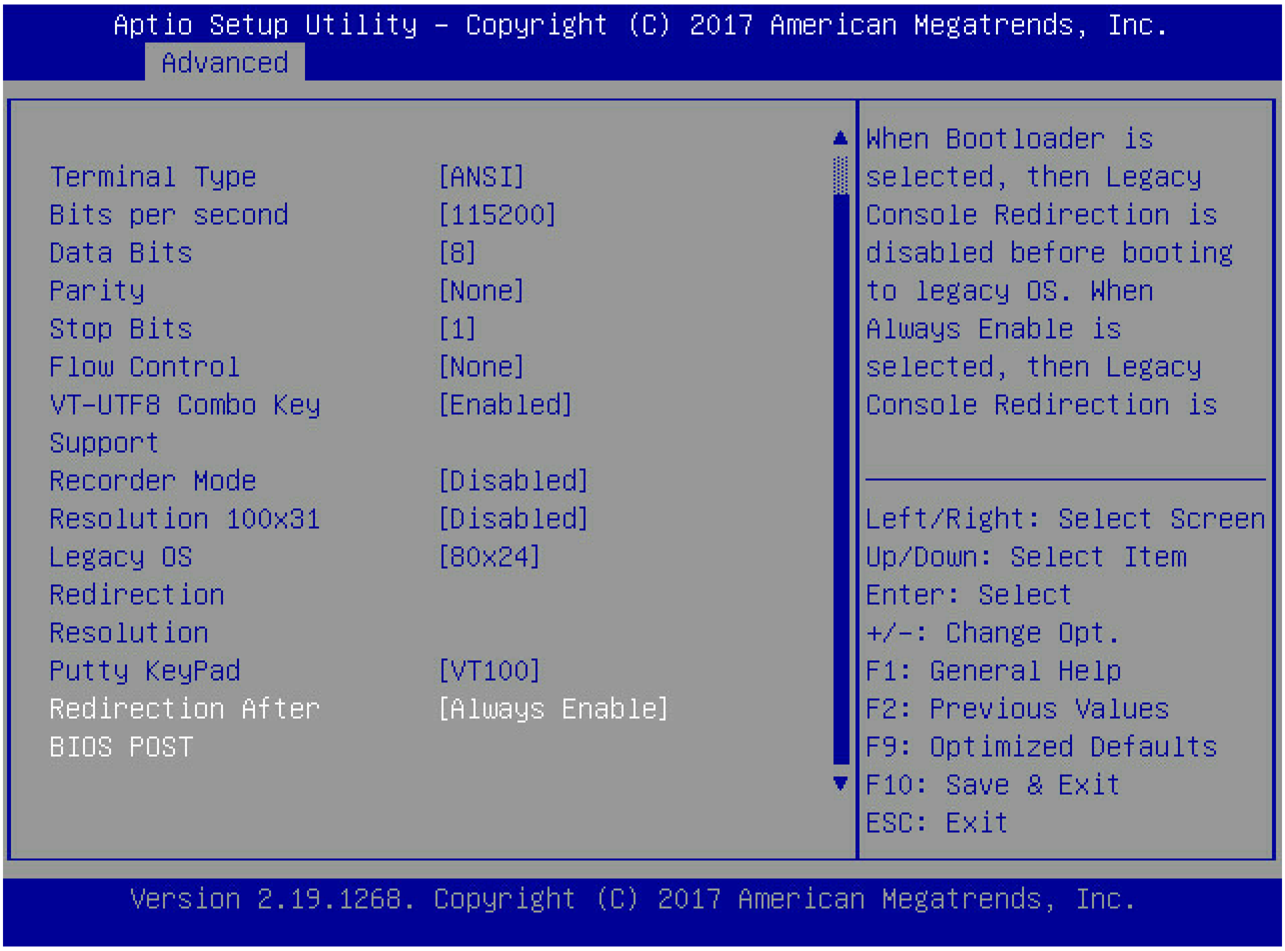
Serial Over LAN(SOL) redirects the system serial port to the remote network client. Users connect to the BMC on the local PC, open the serial port redirection function with the standard IPMI command (sol activate) then view the system serial output, and enter the system serial port.

- COM0 and COM1 both support SOL. COM0 port has connector on the motherboard. The COM1 port is dedicated for SOL function.
- SOL default enable on COM0(some projects on COM1), user should configure SOL in BIOS Setup(Serial Port Console Redirection), if needed.



```
      Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
              Advanced

   COM0                                       The settings specify
   Console Redirection     [Disabled]         how the host computer
 ► Console Redirection Settings               and the remote computer
                                              (which the user is
   COM1                                       using) will exchange
   Console Redirection     [Enabled]          data. Both computers
 ► Console Redirection Settings               should have the same or
                                              compatible settings.

                                              Left/Right: Select Screen
                                              Up/Down: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              F1: General Help
                                              F2: Previous Values
                                              F9: Optimized Defaults
                                              F10: Save & Exit
                                              ESC: Exit

       Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 57 SOL Setting in BIOS



```
     Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
          Advanced

                                                      ▲ When Bootloader is
  Terminal Type              [ANSI]                     selected, then Legacy
  Bits per second            [115200]                   Console Redirection is
  Data Bits                  [8]                        disabled before booting
  Parity                     [None]                     to legacy OS. When
  Stop Bits                  [1]                        Always Enable is
  Flow Control               [None]                     selected, then Legacy
  VT-UTF8 Combo Key          [Enabled]                  Console Redirection is
  Support
  Recorder Mode              [Disabled]
  Resolution 100x31          [Disabled]                 Left/Right: Select Screen
  Legacy OS                  [80x24]                    Up/Down: Select Item
  Redirection                                           Enter: Select
  Resolution                                            +/-: Change Opt.
  Putty KeyPad               [VT100]                    F1: General Help
  Redirection After          [Always Enable]            F2: Previous Values
  BIOS POST                                             F9: Optimized Defaults
                                                      ▼ F10: Save & Exit
                                                        ESC: Exit

        Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 58 Default serial setting.

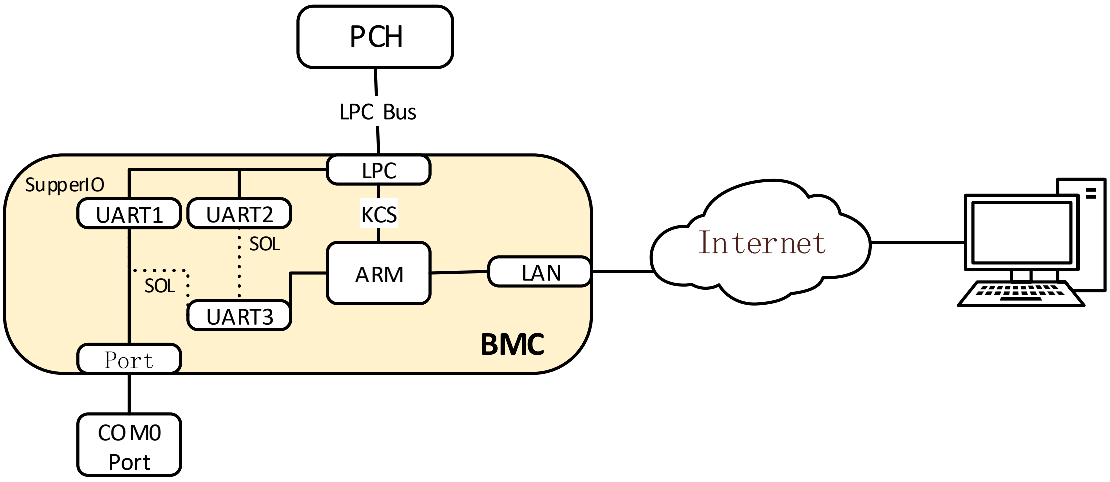


Figure 59 SOL Schematic

25.2.System Serial Log Recording

BMC can record system serial information. The logs BIOS or OS sends to the serial port will be recorded to the BMC's DDR, and keep up to 2M bytes of system serial log content. When more than 2M, log will loop to store, and the old log content will be deleted. When the system downtime or restart, system serial log can be exported, and fault information help diagnose the fault

26. Console Redirection(KVM)

Remote KVM redirect the host system's console to user's PC by BMC, user login BMC and open KVM, then host's screen will be open in KVM application, user PC's keyboard and mouse can be used to control server.

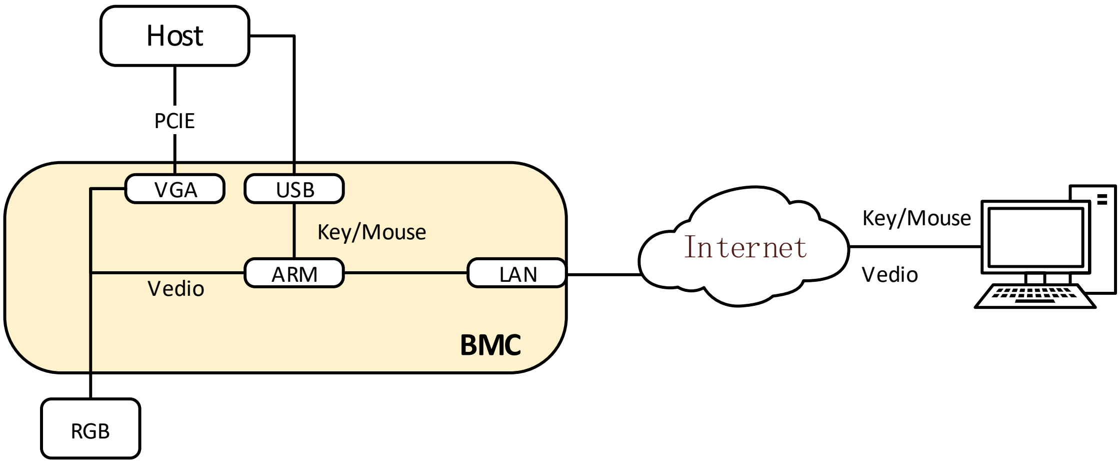
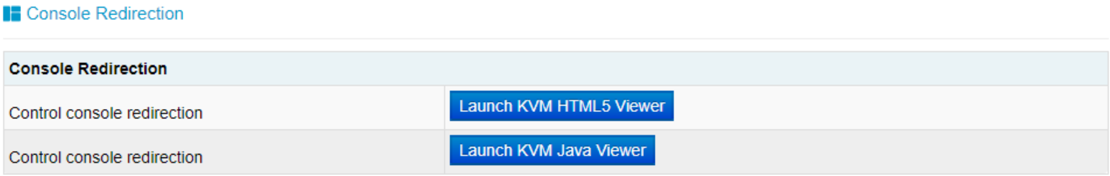


Figure 60 KVM Schematic

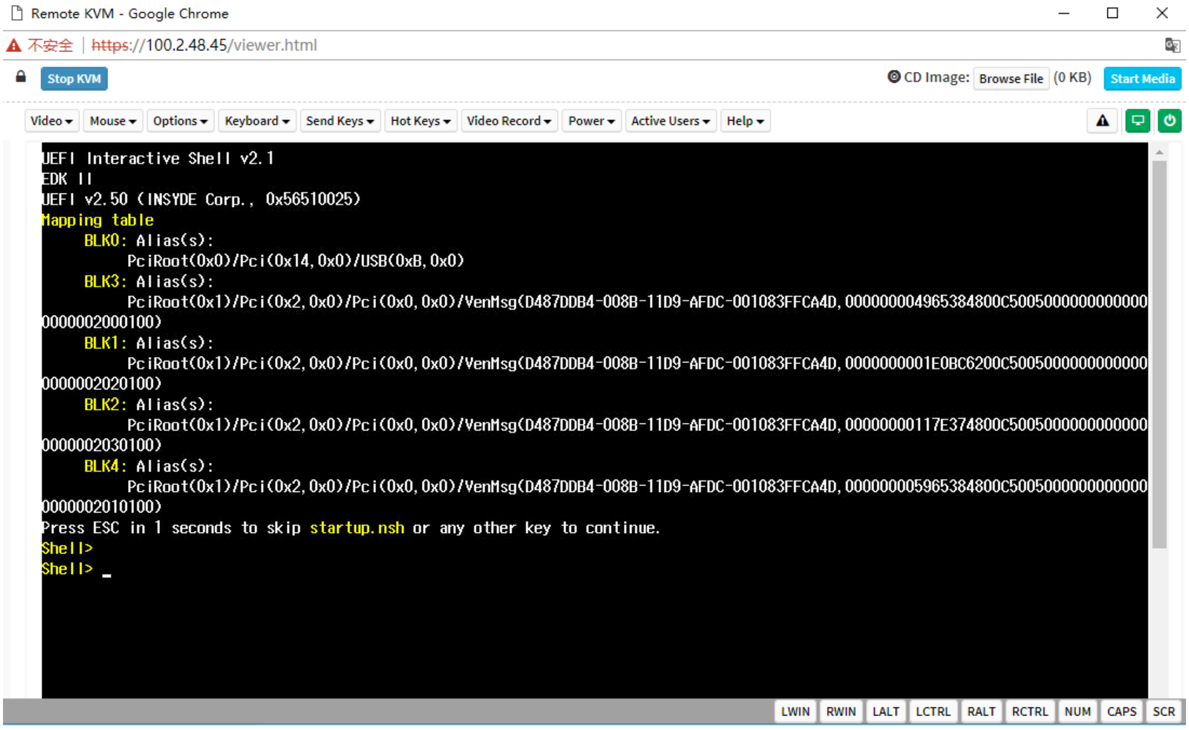
26.1.HTML5 KVM

BMC supports HTML5 KVM, supported on Chrome 58 and above, IE 11 and above. Not depend on JAVA, .NET. Go to “Remote Control > Console Redirection” in WEB GUI, click “Launch KVM HTML5 Viewer” to launch HTML5 KVM.



Console Redirection	
Control console redirection	Launch KVM HTML5 Viewer
Control console redirection	Launch KVM Java Viewer

Figure 61 Console Redirection



```
UEFI Interactive Shell v2.1
EDK II
UEFI v2.50 (INSYDE Corp., 0x56510025)
Mapping table
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0xB,0x0)
     BLK3: Alias(s):
          PciRoot(0x1)/Pci(0x2,0x0)/Pci(0x0,0x0)/VenMsg(D487DDB4-008B-11D9-AFDC-001083FFCA4D,000000004965384800C5005000000000000000
0000002000100)
     BLK1: Alias(s):
          PciRoot(0x1)/Pci(0x2,0x0)/Pci(0x0,0x0)/VenMsg(D487DDB4-008B-11D9-AFDC-001083FFCA4D,0000000001E0BC6200C5005000000000000000
0000002020100)
     BLK2: Alias(s):
          PciRoot(0x1)/Pci(0x2,0x0)/Pci(0x0,0x0)/VenMsg(D487DDB4-008B-11D9-AFDC-001083FFCA4D,00000000117E374800C5005000000000000000
0000002030100)
     BLK4: Alias(s):
          PciRoot(0x1)/Pci(0x2,0x0)/Pci(0x0,0x0)/VenMsg(D487DDB4-008B-11D9-AFDC-001083FFCA4D,000000005965384800C5005000000000000000
0000002010100)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell>
Shell> _
```

Figure 62 KVM Screen

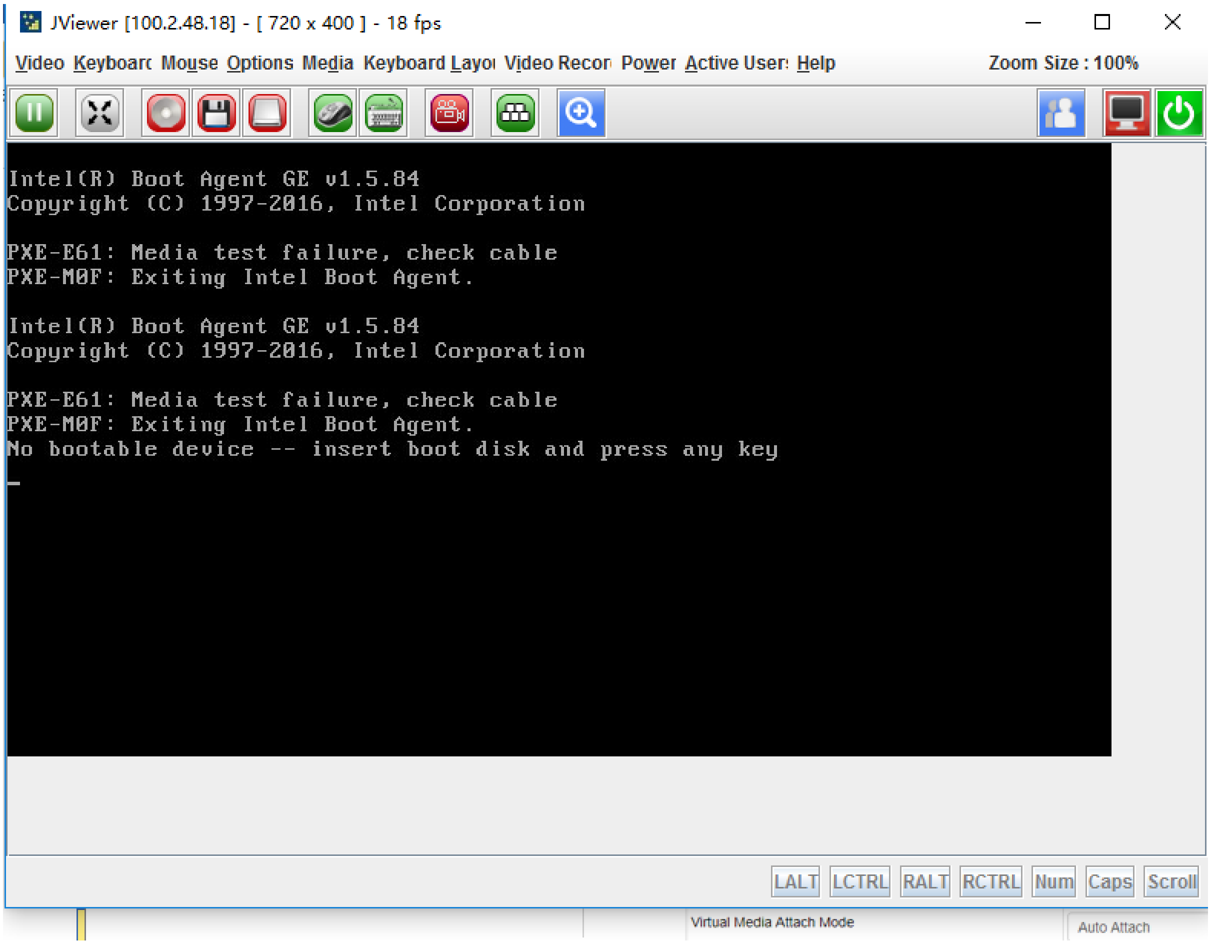
26.2.Java KVM

Support Java KVM, user should download and open JNLP(Java Application), JRE environment should be ready. Supported JRE version:

jre-7u40 and above;

jre-8u45 and above;

Go to “Remote Control > Console Redirection” in WEB GUI, click “Launch KVM Java Viewer” to launch Java KVM.

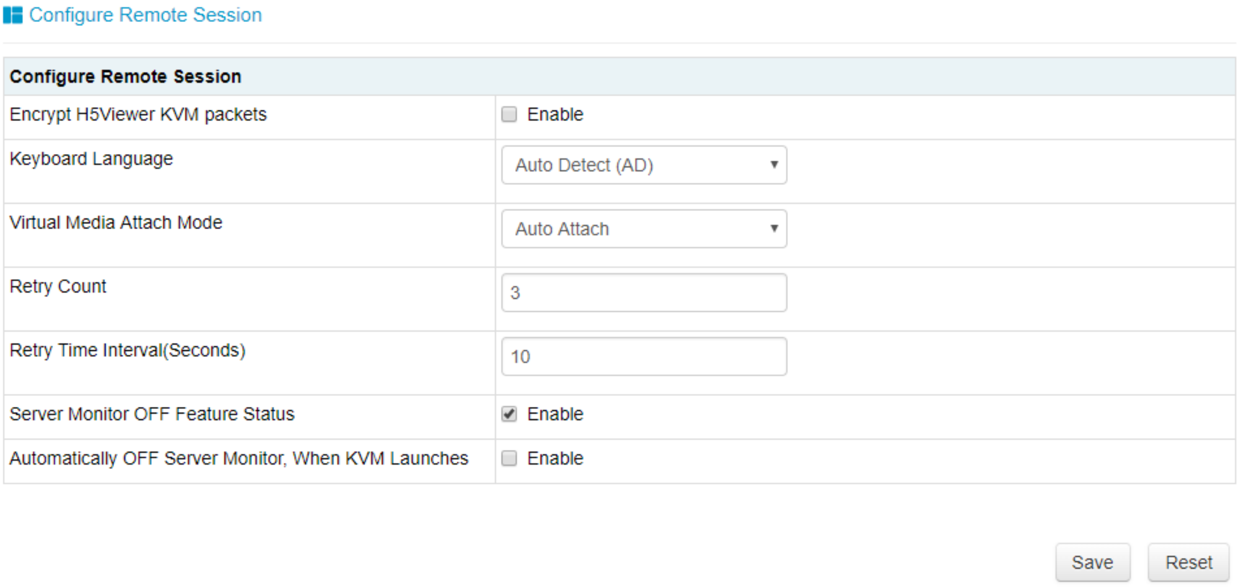

JViewer [100.2.48.18] - [720 x 400] - 18 fps
Video Keyboarc Mouse Options Media Keyboard Layoi Video Recor Power Active User: Help
Zoom Size : 100%
LALT
LCTRL
RALT
RCTRL
Num
Caps
Scroll
Virtual Media Attach Mode
Auto Attach

```
Intel(R) Boot Agent GE v1.5.84
Copyright (C) 1997-2016, Intel Corporation

PXE-E61: Media test failure, check cable
PXE-M0F: Exiting Intel Boot Agent.

Intel(R) Boot Agent GE v1.5.84
Copyright (C) 1997-2016, Intel Corporation

PXE-E61: Media test failure, check cable
PXE-M0F: Exiting Intel Boot Agent.
No bootable device -- insert boot disk and press any key
_
```

Figure 63 Java KVM

26.3.KVM Reconnect

Support reconnect after network disconnection, default retry count is 3, retry time interval is 10s. User could change reconnect setting in page “Remote Control->Configure Remote Session”. Retry count ranges from 1 to 6, time interval ranges from 5 to 30 seconds.



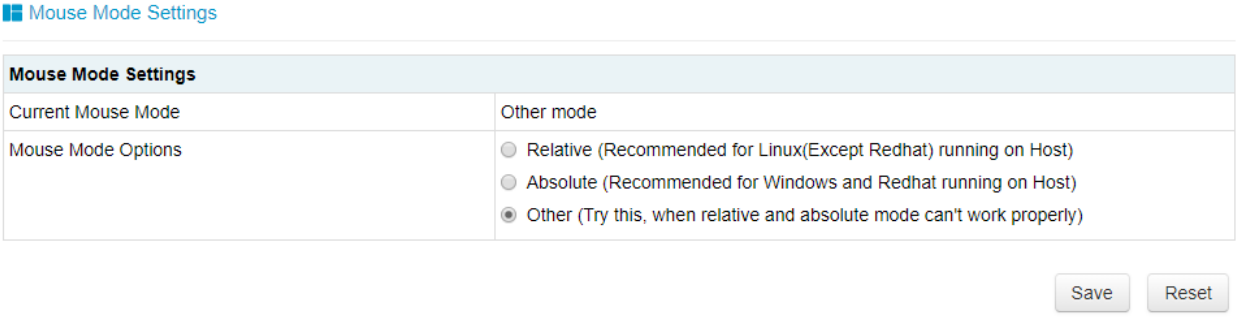
Configure Remote Session

Configure Remote Session	
Encrypt H5Viewer KVM packets	□ Enable
Keyboard Language	Auto Detect (AD) ▾
Virtual Media Attach Mode	Auto Attach ▾
Retry Count	3
Retry Time Interval(Seconds)	10
Server Monitor OFF Feature Status	☑ Enable
Automatically OFF Server Monitor, When KVM Launches	□ Enable

Figure 64 KVM Reconnect

26.4.Mouse Mode

To open KVM Mouse setting page, click “Remote Control -> Mouse Mode”.



Mouse Mode Settings

Mouse Mode Settings	
Current Mouse Mode	Other mode
Mouse Mode Options	○ Relative (Recommended for Linux(Except Redhat) running on Host) ○ Absolute (Recommended for Windows and Redhat running on Host) ● Other (Try this, when relative and absolute mode can't work properly)

Figure 65 Mouse Mode Settings

Table 40 Table KVM Mouse Mode

Host OS	Client OS			
	Windows 8	**Windows 7**	**Windows Server 2012**	**Windows Server 2008 R2**
RHEL 5.2	Relative	Relative	Relative	Relative
RHEL 5.4	Relative	Relative	Relative	Relative
RHEL 5.6	Relative	Relative	Relative	Relative
RHEL 6.0	Absolute	Absolute	Absolute	Absolute
RHEL 6.4	Absolute	Absolute	Absolute	Absolute
RHEL 7.0	Absolute	Absolute	Absolute	Absolute
Fedora10	Relative	Relative	Relative	Relative
Fedora11	Absolute	Absolute	Absolute	Absolute
Fedora12	Absolute	Absolute	Absolute	Absolute
Fedora14	Absolute	Absolute	Absolute	Absolute
Fedora15	Absolute	Absolute	Absolute	Absolute
Fedora18	Absolute	Absolute	Absolute	Absolute
Fedora19	Absolute	Absolute	Absolute	Absolute
Fedora 20	Absolute	Absolute	Absolute	Absolute
Cent OS 5.4	Absolute	Absolute	Absolute	Absolute
Cent OS 6.0	Relative	Relative	Relative	Relative
Cent OS 6.1	Absolute	Absolute	Absolute	Absolute
Cent OS 6.2	Absolute	Absolute	Absolute	Absolute
Ubuntu 8.10	Absolute	Absolute	Absolute	Absolute
Ubuntu 9.10	Absolute	Absolute	Absolute	Absolute
Ubuntu 11.04	Absolute	Absolute	Absolute	Absolute
Ubuntu 12.04	Absolute	Absolute	Absolute	Absolute

Ubuntu 14.04	Absolute	Absolute	Absolute	Absolute
OpenSuse 11.1	Absolute	Absolute	Absolute	Absolute
OpenSuse 12.1	Relative	Relative	Relative	Relative
Windows 2008	Absolute	Absolute	Absolute	Absolute
Windows server 2012	Absolute	Absolute	Absolute	Absolute

27. Virtual Media

The media redirection will allow user to take various media devices and images that presented on the client side (Local Media Support) or remote (Remote Media Support), and attach them as virtual USB on the server side in which the BMC is resident.

The virtual media supports:

- Simultaneous Hard disk, Floppy, USB key, CD/DVD, Folder redirection.
- Efficient USB 2.0 based CD/DVD redirection with a typical speed of 20XCD.
- Completely secured (Authenticated or Encrypted).
- The media image can be mounted on NFS or CIFS server as Remote Media Support.

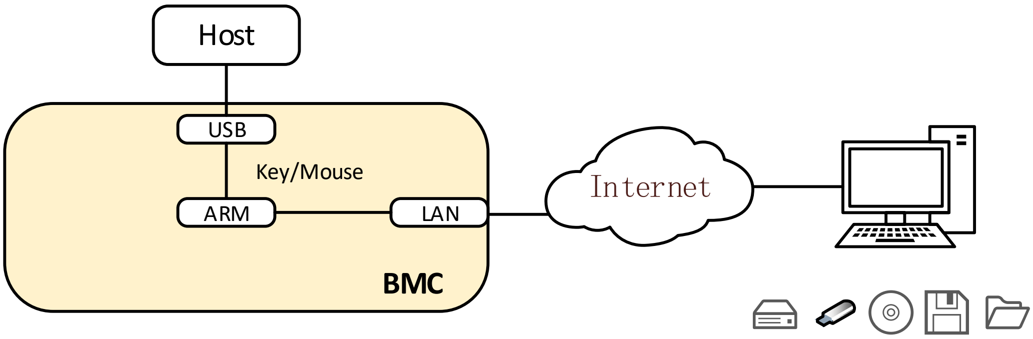
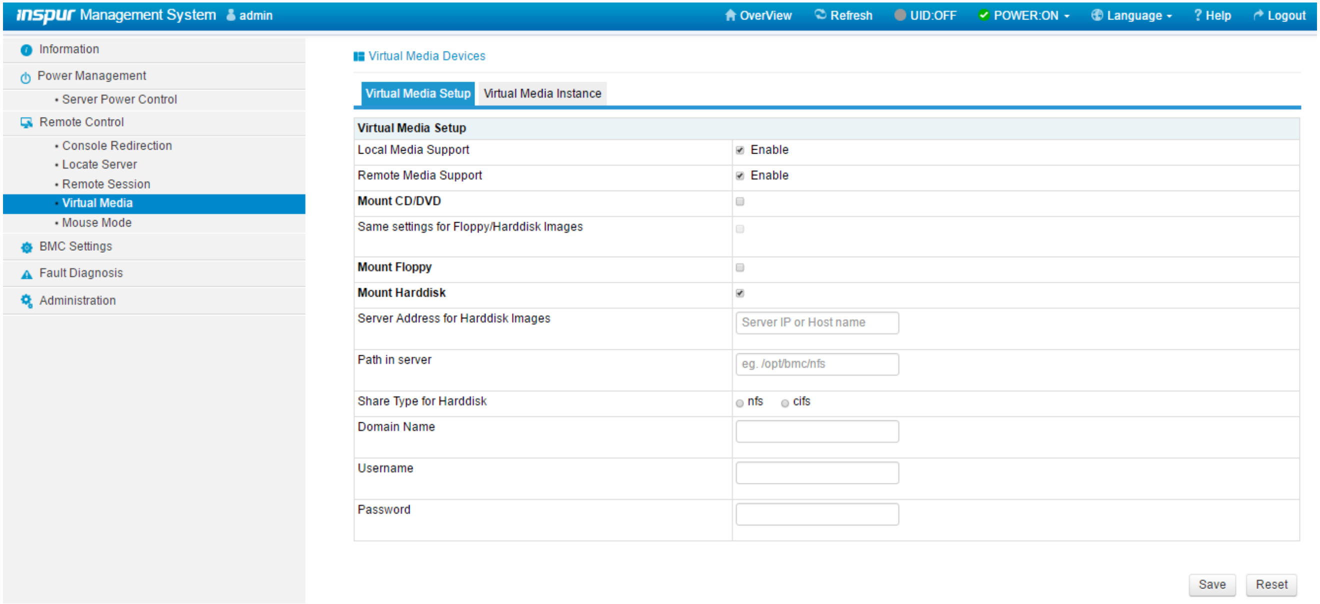


Figure 66 Virtual Media Schematic

To open virtual media configuration, click “Remote Control -> Virtual Media”.



Virtual Media Setup	
Local Media Support	☑ Enable
Remote Media Support	☑ Enable
Mount CD/DVD	□
Same settings for Floppy/Harddisk Images	□
Mount Floppy	□
Mount Harddisk	☑
Server Address for Harddisk Images	Server IP or Host name
Path in server	eg. /opt/bmc/nfs
Share Type for Harddisk	○ nfs ○ cifs
Domain Name	
Username	
Password	

Figure 67 Virtual Media Settings

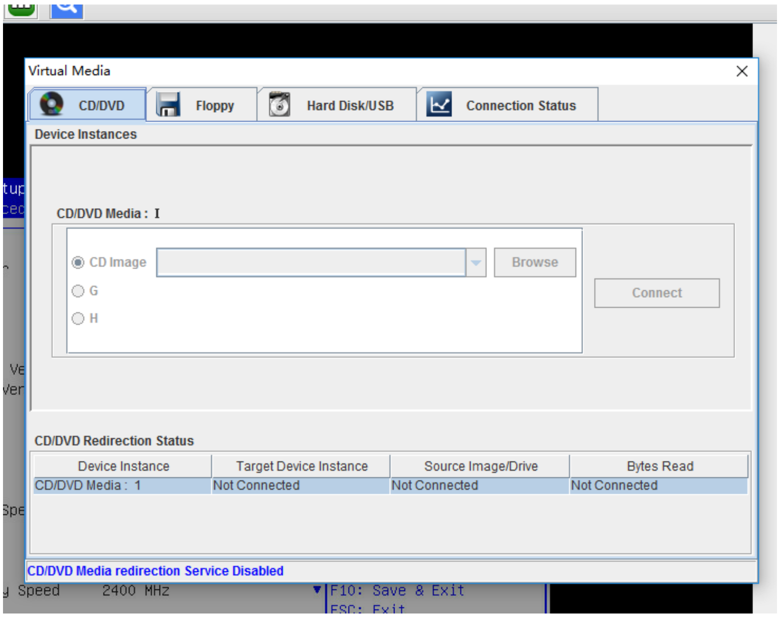
Local Media Support: To enable or disable Local Media support, check/uncheck the 'Enable' check box.

Remote Media Support: To enable or disable Remote Media support, check/uncheck the 'Enable' check box.
***Mount CD/DVD**:*

To enable or disable Mount CD/DVD support, check/uncheck the 'Enable' check box.
Note: You can also select all the media types simultaneously.
Server Address for CD/DVD Images: Displays the address of the server where the remote media images are stored.
Path in server: Displays the Source path to the remote media images.
Share Type for CD/DVD: Displays the Share Type of the remote media server either NFS or CIFS.
Domain Name, Username, and Password: If share Type is Samba(CIFS), then enter user credentials to authenticate on the server.

Same settings for Floppy/Harddisk Images.

User can mount virtual media in KVM as below.



Device Instance	Target Device Instance	Source Image/Drive	Bytes Read
CD/DVD Media : 1	Not Connected	Not Connected	Not Connected

CD/DVD Media redirection Service Disabled

Figure 68 Virtual Media in KVM

28. Redfish

Redfish is a new management standard that uses the hypermedia RESTful interface to express data. It is oriented to the model, can express the relationship between modern system components and the semantics of services and components, and be easy to expand. For servers that provide Redfish, the client can obtain the BMC information by sending HTTP request and specify the operation for the BMC.

The client can access the Redfish service through the HTTP client. The following is the use of curl in Linux to send the request to access redfish. The usual request operation is "GET", "PUT", "POST", "PATCH", "DELETE" and so on. Sending and Receiving data are all json format.
The username and password below must be BMC users with administrator privileges.

28.1.GET

The client gets the data of the specified URL via HTTP GET. The basic format is as follows
curl -k -u username:password https://BMC_IP:8080/redfish/v1/Chassis/1

28.2.POST

The client sends data to the specified URL via HTTP POST, and the server is configured according to the POST data. The basic format is as follows:

```
curl -k  -u username:password
https://BMC_IP:8080/redfish/v1/Systems/System1/Actions/ComputerSystem.Reset -X POST -H 'Content-Type:
application/json' -d '{"ResetType":"ForceOff"}'
```

Note:

https://BMC_IP:8080/redfish/v1/Systems/System1/Actions/ComputerSystem.Reset is the request URL

-H The parameter is the format of the requested data

-d The parameter is the requested data

28.3.DELETE

The client deletes the data for the specified URL via HTTP DELTE, and the server delete configurations according to the URL. The basic format is as follows:

```
curl -k  -u username:password https://BMC_IP:8080/redfish/v1/SessionService/Sessions/1 -X DELETE
```

Note:

https://BMC_IP:8080/redfish/v1/SessionService/Sessions/1 is the deleted address

28.4.Steps

1. Get the resources provided by Redfish, Redfish's root directory visit does not require authorization. Get the accessible resource URL through visiting the Redfish root directory

Request:

```
curl -k  -u username:password https://BMC_IP:8080/redfish/v1/
```

Response:

```
{
 "@Redfish.Copyright": "Copyright 2014-2016 Distributed Management Task Force,
Inc. (DMTF). For the full DMTF copyright policy, see
http://www.dmtf.org/about/policies/copyright.",
 "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
 "@odata.id": "/redfish/v1/",
 "@odata.type": "#ServiceRoot.v1_1_0.ServiceRoot",
 "AccountService": {
  "@odata.id": "/redfish/v1/AccountService"
 },
 "Chassis": {
  "@odata.id": "/redfish/v1/Chassis"
 },
 "EventService": {
  "@odata.id": "/redfish/v1/EventService"
 },
 "Id": "RootService",
 "Links": {
  "Sessions": {
   "@odata.id": "/redfish/v1/SessionService/Sessions"
  }
 },
 "Managers": {
  "@odata.id": "/redfish/v1/Managers"
 },
 "Name": "Root Service",
 "Oem": {},
 "RedfishVersion": "1.1.0",
 "SessionService": {
  "@odata.id": "/redfish/v1/SessionService"
```

```
      },
      "Systems": {
        "@odata.id": "/redfish/v1/Systems"
      },
      "Tasks": {
        "@odata.id": "/redfish/v1/TaskService"
      },
      "UUID": "92384634-2938-2342-8820-489239905423"
    }
```

Figure 69 Response of Get the Accessible Resource URL

2. Get the URL of the device category based on the acquired resource

Eg: Get the URL for the Chassis category: / redfish / v1 / Chassis:

Request:

```
curl -k  -u username:password https://BMC_IP:8080/redfish/v1/Chassis
```

Response:

```
    {
     "@Redfish.Copyright": "Copyright 2014-2016 Distributed Management Task Force,
    Inc.    (DMTF).    For    the    full    DMTF    copyright    policy,    see
    http://www.dmtf.org/about/policies/copyright.",
     "@odata.context": "/redfish/v1/$metadata#ChassisCollection.ChassisCollection",
     "@odata.id": "/redfish/v1/Chassis",
     "@odata.type": "#ChassisCollection.ChassisCollection",
     "Members": [
       {
        "@odata.id": "/redfish/v1/Chassis/1"
       }
     ],
     "Members@odata.count": 1,
     "Name": "Chassis Collection"
    }
```

Figure 70 Response of Get the URL for the Chassis Category

3. Access the URL of the resource that is ultimately needed by step-by-step access

Eg: Get the URL for Chassis specific information: /redfish/v1/Chassis/Chassis1:

Request:

```
curl -k  -u username:password https://BMC_IP:8080/redfish/v1/Chassis/Chassis1
```

Response:

```
{
   "@odata.type": "#Chassis.v1_2_0.Chassis",
   "Id": "1",
   "Name": "Computer System Chassis",
   "ChassisType": "RackMount",
   "AssetTag": "5280",
   "Manufacturer": "Inspur",
   "Model": "5280",
   "SKU": "8675309",
   "SerialNumber": "5280",
   "PartNumber": "224071-J23",
   "PowerState": "On",
   "IndicatorLED": "Lit",
   "Status": {
     "State": "Enabled",
     "Health": "OK"
   },
   "Thermal": {
     "@odata.id": "/redfish/v1/Chassis/1/Thermal"
   },
   "Power": {
     "@odata.id": "/redfish/v1/Chassis/1/Power"
   },
   "Links": {
     "ComputerSystems": [
       {
         "@odata.id": "/redfish/v1/Systems/5280"
       }
     ],
     "ManagedBy": [
       {
         "@odata.id": "/redfish/v1/Managers/BMC"
       }
     ],
     "ManagersInChassis": [
       {
         "@odata.id": "/redfish/v1/Managers/BMC"
       }
     ]
   },
   "@odata.context": "/redfish/v1/$metadata#Chassis.Chassis",
   "@odata.id": "/redfish/v1/Chassis/1",
   "@Redfish.Copyright": "Copyright 2014-2016 Distributed Management Task Force, Inc.
(DMTF). For the full DMTF copyright policy, see http://www.dmtf.org/about/policies/copyright."
}
```

Figure 71 Response of Get the URL for Chassis Specific Information

29. Appendix

Table 41 BMC Self-Inspection Code Table

Self-Inspection 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