



Inspur Server User Manual

NF8480M5

© Copyright Inspur 2016. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Inspur.

The information in this manual is subject to change without notice.

Inspur is the registered trademark of Inspur. All the other trademarks or registered trademarks mentioned in this manual are the property of their respective holders.

Edition: 1.0

Jan. 2018

Abstract

This manual contains technical information such as specifications, hardware operations, software configuration, fault diagnosis, etc. that are relevant to the maintenance and operation of this server.

It is recommended that server installation, configuration, and maintenance is performed by experienced technicians only.

Target Audience

This manual is intended for:

- Technical support engineers
- Product maintenance engineers
- Technicians

Warnings:

This manual introduces the NF8480M5 server's technical features, system installation and setup, which will help the user to understand how best to utilize the server and all its functionalities.

1. For your safety, please do not disassemble the server's components arbitrarily. Please do not extend configuration or connect other peripheral devices arbitrarily. If needed, please contact Inspur for our support and guidance.
2. Before disassembling the server's components, please be sure to disconnect all the power cords connected to the server.
3. BIOS and BMC setup is a significant factor in correctly configuring your server. If there are no special requirements, it is suggested to use the Default Values and not alter the parameter settings arbitrarily.
4. Please install the product-compatible operating system and use the driver provided by Inspur. If you use an incompatible operating system or non-Inspur driver, it may cause compatibility issues and affect the normal use of the product, Inspur will not assume any responsibility or liability.

Inspur is not responsible for any damages, including loss of profits, loss of information, interruption of business, personal injury, and/or any damage or consequential damage without limitation, incurred before, during, or after the use of our products.


Contents

1 Safety Instructions	1
2 Product Specification	5
2.1 Introduction.....	5
2.2 Features and Specifications	5
3 Component Identification	7
3.1 Rear Panel Components	7
3.2 Motherboard Components.....	8
3.3 Motherboard Jumper Introduction	9
4 Operations.....	11
4.1 Power up the Server	11
4.2 Power down the Server	11
4.3 Extend the Server from the Rack.....	11
5 Setup	13
5.1 Optimum Environment.....	13
5.2 Rack Warnings	16
5.3 Identifying the Contents of the Server Shipping Carton.....	16
5.4 Installing Hardware Options	17
5.5 Installing the Server into the Rack.....	17
5.6 Installing the Operating System.....	18
6 Hardware Options Installation.....	19
6.1 Introduction.....	19
6.2 Processor Option	19
6.3 Memory Option	22
6.4 HDD Option	23
6.5 Redundant Hot-plug Power Supply Option	25

6.6 Expansion Board Option	26
6.7 Air Baffle Option	27
7 Cabling	29
8 BIOS Setup	30
8.1 Common Operations	30
8.2 BIOS Parameter Description	31
8.3 Firmware Update	70
9 BMC Settings	73
9.1 Introduction	73
9.2 Server System Overview	73
9.3 IPMI2.0	75
9.4 Management Web GUI	81
9.5 SNMP	84
9.6 Smash-Lite CLI	85
9.7 System Information and State	88
9.8 Device State Monitor and Diagnostic	98
9.9 Logs	101
9.10 Event Alerting	104
9.11 Diagnostics	106
9.12 BMC Self Recovery	108
9.13 LED	109
9.14 BMC Network	109
9.15 Users	112
9.16 Protocol and Ports	118
9.17 Time and NTP	119
9.18 BIOS and BMC	120
9.19 Storage	122
9.20 Server Control	125
9.21 Power Supply and Power Consumption	127

9.22 Fan Speed Control (FSC)	129
9.23 Firmware Update.....	130
9.24 Restore Factory Default	135
9.25 Serial Over LAN (SOL) and System Serial Log Recording.....	136
9.26 Console Redirection (KVM).....	138
9.27 Virtual Media.....	142
9.28 Redfish.....	144
9.29 Appendix	147
10 Common Faults, Diagnosis and Troubleshooting	148
10.1 Hardware Problems.....	148
10.2 Software Problems	152
11 Battery Replacement.....	154
12 Regulatory Compliance Notices.....	155
12.2 Federal Communications Commission Notice.....	155
12.3 European Union Regulatory Notice.....	156
12.4 Disposal of Waste Equipment by Users in the European Union	156
12.5 Korean Notice.....	157
12.6 Chinese Notice.....	157
12.7 Battery Replacement Notice	157
13 Electrostatic Discharge	159
13.1 Preventing Electrostatic Discharge	159
13.2 Grounding Methods to Prevent Electrostatic Discharge	159
14 Warranty.....	160
14.1 Introduction.....	160
14.2 Warranty Service	160
14.3 Warranty Exclusions	161

1 Safety Instructions

 **WARNING:** Please be advised to follow the instructions below for safety. Failure to do so could result to potential dangers that may cause property loss, personal injury or death.

1. The power supplies in the system may produce high voltages and energy hazards that may cause personal injury. For your safety, please do not attempt to remove the cover of the system to remove or replace any component without assistance provided by Inspur. Only service technicians trained by Inspur are authorized to remove the cover of the host, and to remove and replace internal components.
2. Please connect the equipment to the appropriate power supply. Use only power supplies with the correct voltage and electrical specifications according to the label. To protect your equipment from damages caused by a momentary spike or plunge of the voltage, please use relevant voltage stabilizing equipment, or uninterruptible power supplies.
3. If you must use an extension cable, please use a three-core cable with properly grounded plugs. Observe extension cable ratings. Ensure that the total rating of all equipment plugged into the extension cable does not exceed 80 percent of the ratings limit for the extension cable.
4. Please be sure to use the power supply components that come with the server, such as power lines, power socket (if provided with the server) etc. For your safety, please do not replace power cables or plugs randomly.
5. To prevent electric shock dangers caused by leakage in the system, please make sure that the power cables of the system and peripheral equipment are correctly connected to the earthed/grounded power socket. Please connect the three-core power line plug to the three-core AC power socket that is well earthed and easy to access. Be sure to use earthing /grounding pin of power lines and do not use the patch plug or the earthing/grounding pin unplugged with cables. In the case that the earthing/grounding conductors are not installed and it is uncertain whether there are appropriate earthing/grounding protections, please do not use or attempt to operate the equipment. Contact and consult an electrician.
6. Please do not push any objects into the openings of the system. Doing so may cause fire or electric shock.

7. Please place the system far away from the cooling plate and heat sources, and be sure not to block the air vents.
8. Please be sure not to scatter food or liquid in the system or on other components, and do not use the product in humid or dusty environments.
9. Using an incompatible battery may cause explosion. When battery replacement is required, please consult the manufacturer first, and choose batteries of the same or equivalent type. Do not disassemble, crush, puncture the batteries or make the external connection point short circuit, and do not expose them in the environment over 60°C. Never throw batteries into fire or water. Please do not attempt to open or repair the batteries. Dispose of used batteries according to instructions. For battery recycling, please contact the local waste recycling center.
10. Before installing equipment into the rack, please install all front and side stabilizers on the independent rack first. Please install the front stabilizers first, if connecting with other racks. Please install stabilizers before installing equipment into the rack. Failure to install the corresponding stabilizers before installing equipment into the rack may cause the cabinet to tip over, possibly resulting to severe injury. After installing the equipment and other components into the rack, only one component can be pulled out from the rack through its sliding part at one time. Pulling out several components at the same time may cause the rack to turn over, resulting to serious personal injury.
11. A minimum of two people are required to safely move a rack. The racks are extremely awkward and heavy, moving them without adequate, trained personnel could result in severe injury or death.
12. It is prohibited to directly short-circuit the copper busbar. Please do not touch the copper busbar when the rack is powered on.
13. This is Class A product, and may cause radio interference. In such case, users may need to take necessary measures to mitigate the interference.
14. The equipment is intended for installation in a Restricted Access Location.



Note: The following considerations may help avoid the occurrence of problems that could damage the components or cause data loss, etc.

1. In the event of the following, please unplug the power line plug from the power socket and contact Inspur's customer service department:

- 1) The power cables, extension cables or power plugs are damaged.
 - 2) The products get wet.
 - 3) The products have fallen or have been damaged.
 - 4) Other objects have fallen into the products.
 - 5) The products do not or are unable to function normally even when attempting to operate according to the instructions.
2. If the system becomes wet or damp, please follow these steps:
- 1) Power off the equipment, disconnect them with the power socket, wait for 10 to 20 seconds, and then open the host cover.
 - 2) Move the equipment to a well-ventilated place to dry the system at least for 24 hours and make sure that the system is fully dried.
 - 3) Close the host cover, reconnect the system to the power socket, and then power on.
 - 4) In case of operation failure or other abnormal situations, please contact Inspur and get technical support.
3. Pay attention to the position of system cables and power cables-avoid placing wires in high foot traffic locations. Please do not place objects on the cables.
4. Before removing the host cover, and/or touching the internal components, please allow for the equipment to cool first. To avoid damaging the mainboard, please power off the system and wait for five seconds, and then remove the components from the mainboard and/or disconnect the peripheral device from the system. Please remember that only service technicians trained by Inspur are authorized to remove the cover of the host, and to remove and replace internal components.
5. If there is modem, telecom or LAN options installed in the equipment, please pay attention to the followings:
- 1) In the case of thunder and lightning, please do not connect or use the modem.
 - 2) Never connect or use the modem in a damp environment.
 - 3) Never insert the modem or telephone cables into the socket of network interface controller (NIC).
 - 4) Before unpacking the product package, installing internal components, touching uninsulated cables or jacks of the modem, please disconnect the modem cables.
6. In order to prevent electrostatic discharge from damaging the electronic components in the equipment, please pay attention to the followings:
- 1) Please remove any static electricity on your body before dismounting or touching

- any electronic component in the equipment, to prevent the static electricity from conducting itself to the sensitive components. You may remove the static electricity on the body by touching the metal earthing objects (such as the unpainted metal surface on the rack).
- 2) Please do not take electrostatic sensitive components that are not ready to be installed for application out of the antistatic package materials.
 - 3) While working, please touch the earthing conductor or the unpainted metal surface on the cabinet regularly to remove any static electricity from the body that may damage the internal components.
 7. Upon receiving the proper authorization from Inspur and dismantling the internal components, please pay attention to the following:
 - 1) Switch the system power supply off and disconnect the cables, including all connections of the system. When disconnecting the cables, please hold the connector of the cables and slowly pull the plugs out. Never pull on the cables.
 - 2) The products need to completely cool down before dismantling the host cover or touching the internal components.
 - 3) During the dismantling process, avoid making large movement ranges to prevent damage to the components or scratching arms.
 - 4) Handle components and plug-in cards with care. Please do not touch the components or connection points on the plug-in cards. When handling the plug-in cards or components, firmly grab the edges of the plug-in cards and components, and/or their metal fixed supports.
 8. During the process of rack installation and application, please pay attention to the followings:
 - 1) After the rack installation is finished, please ensure that the stabilizers have been fixed to the rack and supported to ground, and the weight of the rack is firm on ground.
 - 2) Always load from the bottom up, and load the heaviest items first.
 - 3) When pulling out the components from the rack, apply slight force to keep the rack balanced.
 - 4) When pressing down the release latch and the rail of components is sliding, please be careful; as the sliding may hurt your fingers.
 - 5) Do not overload the AC power supply branch circuits in the rack. The total load of the rack should not exceed 80% of the ratings of the branch circuits.
 - 6) Ensure that components in the rack have good ventilation conditions.
 - 7) When repairing components in the rack, never step on any other components.

2 Product Specification

2.1 Introduction

Inspur NF8480M5 is a high-end, four-socket server with Intel® Xeon® scalable computing platform technology. It has powerful computing power, scalability and excellent RAS features. It is an ideal choice for memory database, ERP, CRM, business intelligence analysis system, large virtual applications and data-intensive applications.

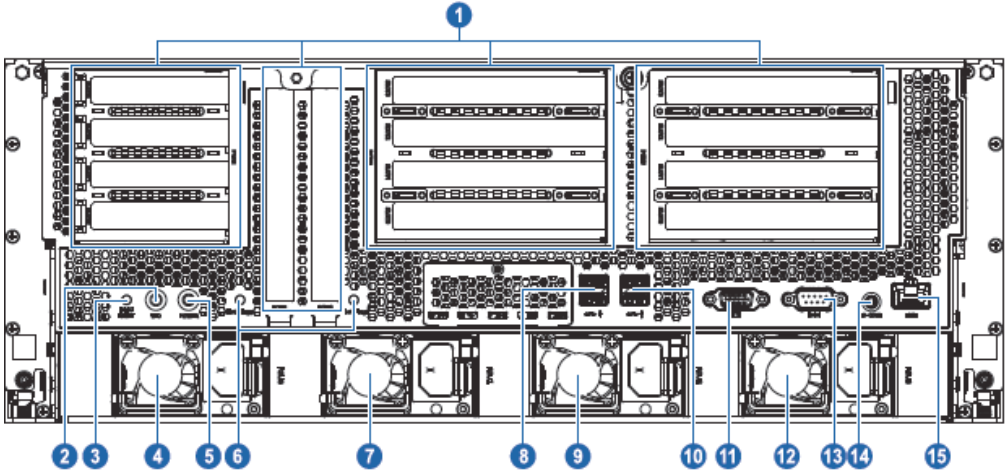
2.2 Features and Specifications

Processor	
Processor Type	2 or 4 Intel® Xeon® scalable processors (up to 205W)
Chipset	
Chipset Type	Intel® C620
Memory	
Memory Type	DDR4 RDIMM/LRDIMM, 2400/2666MHz memory
Memory Slot Qty.	48
Total Memory Capacity	Supports up to 3072GB (64GB per memory)
I/O	
USB	2 front USB 3.0 ports, 4 rear USB 3.0 ports
VGA	1 front VGA port, 1 rear VGA port
Serial Port	1 front RJ45 port, 1 rear DB9 port
Management Port	1 rear RJ45 IPMI port
Display	
Controller Type	Integrated in the Aspeed2500 chip, supports up to 1900*1200 resolution
HDD	
HDD Type	Supports SSD/SATA/SAS/NVME Supports up to 24 * 2.5" SSD/SAS/SATA disks; up to 12 * NVME disks
Power	
Specification	Supports the whole power network AC, and 240/336V DC input Supports 800/1300/1600W platinum CRPS Supports 1+1/2+1/2+2/3+1 redundancy modes
Power Input	Please refer to the power input on the nameplate label of the host.
Physical	
External Dimensions of Packing Box	714 width × 353 height × 1160 depth (unit: mm)

Size of Host Machine	448 width × 175.5 height × 812 depth (unit: mm)
Product Weight	Full configuration Gross weight: 60kg (Gross weight includes: Host + Packing Box + Rails + Accessory Box)
Environmental	
Operating Temperature	10°C -35°C
Storage & Transportation Temperature	-40°C -60°C
Operating Humidity	20% -80% relative humidity
Storage & Transportation Humidity	20% -93% (40°C) relative humidity

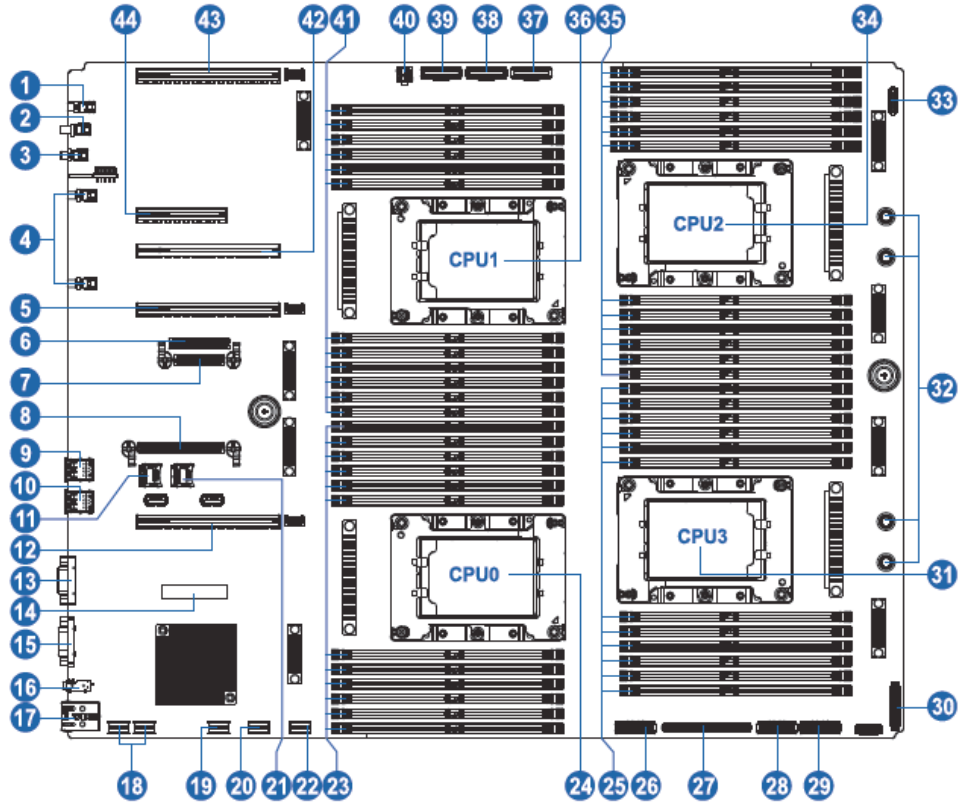
3 Component Identification

3.1 Rear Panel Components



Item	Description
1	PCIe slots
2	UID LED
3	BMC_RST button
4	PSU0
5	Power button
6	Hot-plug component start button
7	PSU1
8	USB3.0 ports (0 1)
9	PSU2
10	USB3.0 ports (2 3)
11	VGA port
12	PSU3
13	Serial port
14	BMC serial port
15	IPMI

3.2 Motherboard Components



Item	Description
1	BMC_RST button
2	UID LED
3	Power button
4	Hot-plug component start button
5	PCIe4 slot (CPU1)
6	OCPB connector (CPU1)
7	OCPB connector
8	OCPA connector (CPU1)
9	USB3.0 ports (0 1)
10	USB3.0 ports (2 3)
11	BMC TF slot
12	PCIe5 slot (CPU3)
13	VGA port
14	TPM/TCM connector
15	Serial port

16	BMC serial port
17	IPMI
18	SATA connectors (2)
19	M.2 HDD connector 0
20	M.2 HDD connector 1
21	SYS TF slot
22	Front control panel connector
23	DIMM slots (CPU0)
24	CPU0
25	DIMM slots (CPU3)
26	SLIM LINE2 connector (CPU3)
27	PCIE0 slot (CPU0)
28	SLIM LINE0 connector (CPU3)
29	SLIM LINE1 connector (CPU3)
30	Power board control signal connector
31	CPU3
32	Motherboard power connectors
33	Front control panel connector
34	CPU2
35	DIMM slots (CPU2)
36	CPU1
37	SLIM LINE0 connector (CPU2)
38	SLIM LINE1 connector (CPU2)
39	SLIM LINE2 connector (CPU2)
40	Standby power connector
41	DIMM slots (CPU1)
42	PCIE3 slot (CPU0)
43	PCIE1 slot (CPU2)
44	PCIE2 slot (CPU0)

3.3 Motherboard Jumper Introduction

See [3.2 Motherboard Components] for the jumper position.

Item	Description	Function
CLR_CMOS	CMOS clear jumper	Short-circuit J89 pin1-2, normal status; Short-circuit J89 pin2-3, clear CMOS.

**Note:**

It is required to shut down the system, as well as disconnect the power supply during CMOS clearing. Hold for 5 seconds after short-circuiting pin2-3, and then short-circuit pin1-2 (default setting) to restore to its original status.

4 Operations

4.1 Power up the Server

Insert the power cord plug, then press the Power Button.

4.2 Power down the Server



WARNING: To reduce the risk of personal injury, electric shock, or damage to the equipment, remove the power cord to remove power from the server. The front panel Power Button does not completely shut off system power. Portions of the power supply and some internal circuitry remain active until AC power is removed.

IMPORTANT: If installing a hot-plug device, it is not necessary to power down the server.

1. Back up the server data.
2. Shut down the operating system.
3. Disconnect the power cords.

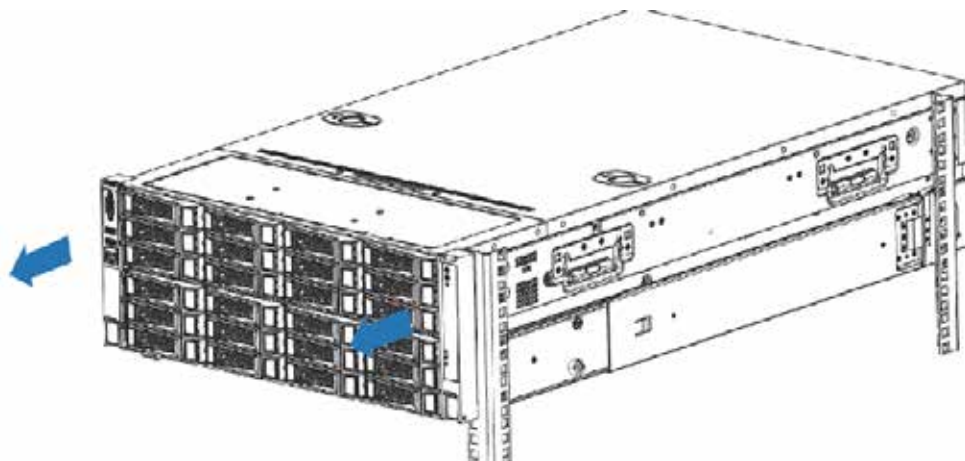
The system is now without power.

4.3 Extend the Server from the Rack


1. Pull down the two quick release levers on both sides of the server.
2. Extend the server from the rack.

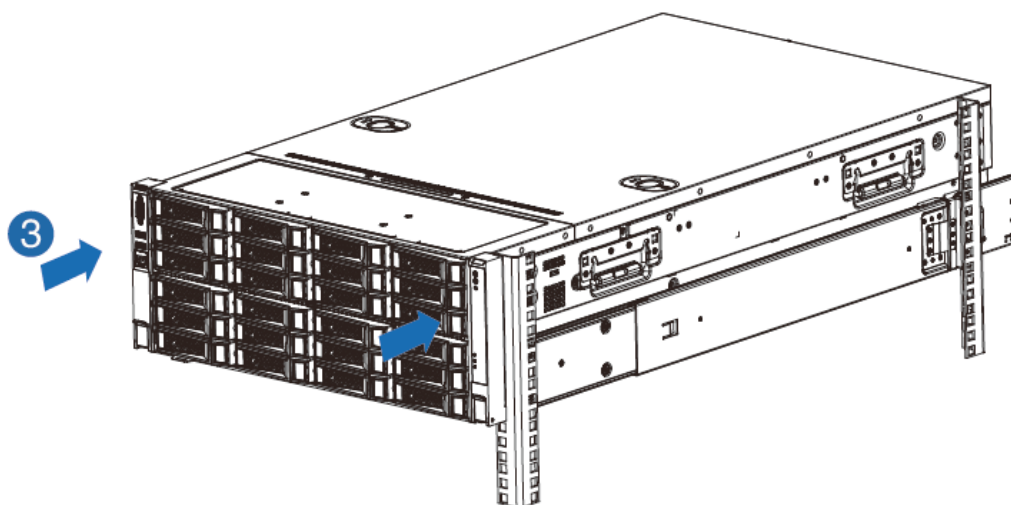


WARNING: To reduce the risk of personal injury or equipment damage, be sure that the rack is adequately stabilized before extending a component from the rack.



3. After performing the installation or maintenance procedure, slide the server back into the rack until it clicks into place. Tighten the screws to secure the chassis in place.

 **WARNING:** To reduce the risk of personal injury, be careful when sliding the server into the rack. The sliding rails could pinch your fingers.



5 Setup

5.1 Optimum Environment


When installing the server in a rack, select a location that meets the environmental standards described in this section.

5.1.1 Space and Airflow Requirements


To allow for servicing and adequate airflow, observe the following space and airflow requirements when deciding where to install a rack:


- Leave a minimum clearance of 63.5 cm (25 in) in front of the rack.
- Leave a minimum clearance of 76.2 cm (30 in) behind the rack.
- Leave a minimum clearance of 121.9 cm (48 in) from the back of the rack to the back of another rack or row of racks.

Inspur Servers draw in cool air through the front door and expel warm air through the rear door. Therefore, the front and rear rack doors must be adequately ventilated to allow ambient room air to enter the cabinet, and the rear door must be adequately ventilated to allow the warm air to escape from the cabinet.

 **CAUTION:** To prevent improper cooling and damage to the equipment, do not block the ventilation openings.

When vertical space in the rack is not filled by a server or rack component, the gaps between the components cause changes in airflow through the rack and across the servers. Cover all gaps with blanking panels to maintain proper airflow.

 **CAUTION:** Always use blanking panels to fill empty vertical spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

 **CAUTION:** If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:

- Front and rear doors—If the 42U rack includes closing front and rear doors, you must

allow 5,350 sq cm (830 sq in) of holes evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).

- Side—The clearance between the installed rack component and the side panels of the rack must be a minimum of 7 cm (2.75 in).
-

5.1.2 Temperature Requirements

To ensure continued safe and reliable equipment operation, install or position the system in a well-ventilated, climate-controlled environment.

The maximum recommended ambient operating temperature (TMRA) for most server products is 35°C (95°F). The temperature in the room where the rack is located must not exceed 35°C (95°F).



CAUTION: To reduce the risk of damage to the equipment when installing third-party options:


- Do not permit optional equipment to impede airflow around the server or to increase the internal rack temperature beyond the maximum allowable limits.
 - Do not exceed the manufacturer's TMRA.
-

5.1.3 Power Requirements

Installation of this equipment must comply with local and regional electrical regulations governing the installation of information technology equipment by licensed electricians. This equipment is designed to operate in installations covered by NFPA 70, 1999 Edition (National Electric Code) and NFPA-75, 1992 (code for Protection of Electronic Computer/Data Processing Equipment). For electrical power ratings on options, refer to the product rating label or the user documentation supplied with that option.



WARNING: To reduce the risk of personal injury, fire, or damage to the equipment, do not overload the AC supply branch circuit that provides power to the rack. Consult the electrical authority having jurisdiction over wiring and installation requirements of your facility.

 **CAUTION:** Protect the server from power fluctuations and temporary interruptions with a regulating uninterruptible power supply (UPS). This device protects the hardware from damage caused by power surges and voltage spikes and keeps the system in operation during a power failure.

When installing more than one server, you may need to use additional power distribution devices to safely provide power to all devices. Observe the following guidelines:

- Balance the server power load between available AC supply branch circuits.
- Do not allow the overall system AC current load to exceed 80 percent of the branch circuit AC current rating.
- Do not use common power outlet strips for this equipment.
- Provide a separate electrical circuit for the server.


5.1.4 Electrical Grounding Requirements

The server must be grounded properly for optimal operation and safety. In the United States, you must install the equipment in accordance with NFPA 70, 1999 Edition (National Electric Code), Article 250, as well as any local and regional building codes.


In Canada, you must install the equipment in accordance with Canadian Standards Association, CSA C22.1, and Canadian Electrical Code. In all other countries, you must install the equipment in accordance with any regional or national electrical wiring codes, such as the International Electrotechnical Commission (IEC) Code 364, parts 1 through 7. Furthermore, you must be sure that all power distribution devices used in the installation, such as branch wiring and receptacles, are listed or certified grounding-type devices.

Because of the high ground-leakage currents associated with multiple servers connected to the same power source, Inspur recommends the use of a PDU that is either permanently wired to the building's branch circuit or includes a nondetachable cord that is wired to an industrial-style plug. NEMA locking-style plugs or those complying with IEC 60309 are considered suitable for this purpose. Using common power outlet strips for the server is not recommended.

5.2 Rack Warnings

 **WARNING:** To reduce the risk of personal injury or damage to the equipment, please be sure of the following:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - The stabilizing feet are attached to the rack if it is a single-rack installation.
 - The racks are coupled together in multiple-rack installations.
 - Only one component is extended at a time. A rack may become unstable if more than one component is extended for any reason.
-

 **WARNING:** To reduce the risk of personal injury or equipment damage when unloading a rack:

- At least two people are needed to safely unload the rack from the pallet. An empty 42U rack can weigh as much as 115 kg (253 lb), can stand more than 2.1 m (7 ft) tall, and may become unstable when being moved on its casters.
 - Never stand in front of the rack when it is rolling down the ramp from the pallet. Always handle the rack from both sides.
-

5.3 Identifying the Contents of the Server Shipping Carton

Unpack the server shipping carton and locate the materials and documentation necessary for installing the server. All the rack mounting hardware necessary for installing the server into the rack is included with the rack or the server.

The contents of the server shipping carton include:

- Server
- Power cord
- Rack-mounting hardware


In addition to the supplied items, you may need:

- Operating system or application software
- Hardware options


5.4 Installing Hardware Options

Install any hardware options before initializing the server. For options installation information, refer to the option documentation. For server-specific information, refer to “Hardware options installation”.


5.5 Installing the Server into the Rack

 **CAUTION:** Always plan the rack installation so that the heaviest item is on the bottom of the rack. Install the heaviest item first, and continue to populate the rack from the bottom to the top.

1. Install the server and cable management arm into the rack. For more information, see the installation instructions included with the 1U Slide Rail System.
2. Connect peripheral devices to the server. For connector identification information, see “Rear panel components” in this guide.

 **WARNING:** To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into RJ-45 connectors.

3. Connect the power cord to the rear of the server.
4. Connect the power cord to the AC power source.

 **WARNING:** To reduce the risk of electric shock or damage to the equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.

5.6 Installing the Operating System


To operate properly, the server must have a supported operating system installed. For the latest information on supported operating systems, refer to the Inspur website (<http://www.inspur.com/eportal/ui?pagelId=2317460>).


To install the operating system on the server, you can download from the official website directly.

6 Hardware Options Installation

6.1 Introduction


If more than one option is being installed, read the installation instructions for all the hardware options and identify similar steps to streamline the installation process.

 **WARNING:** To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.


 **CAUTION:** To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause electrostatic discharge.


6.2 Processor Option

The server supports dual-and four-processor.

 **CAUTION:** To avoid damage to the processor and system board, only authorized personnel should attempt to replace or install the processor in this server.

To help avoid damage to the processor and system board, do not install the processor without using the processor installation tool.

 **CAUTION:** To prevent possible server malfunction and damage to the equipment, multiprocessor configurations must contain processors with the same part number.

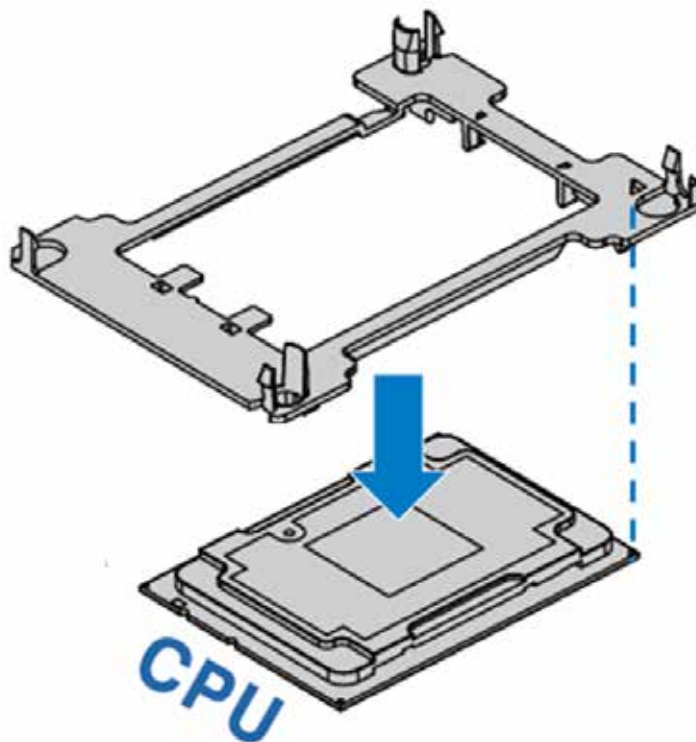
 **CAUTION:** To install a faster processor, update the system ROM before installing the processor.

To install the component:

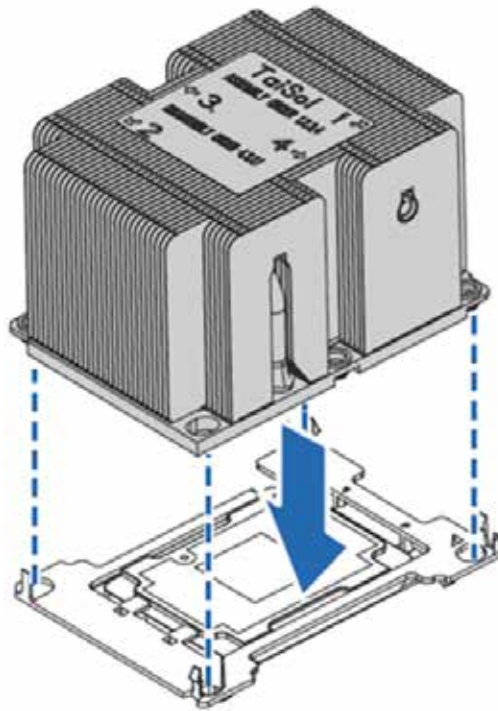
1. Power down the server.
2. Extend the server from the rack.
3. Remove the access panel.
4. Remove the air baffle.

5. Remove the heatsink.
6. Install the processor:

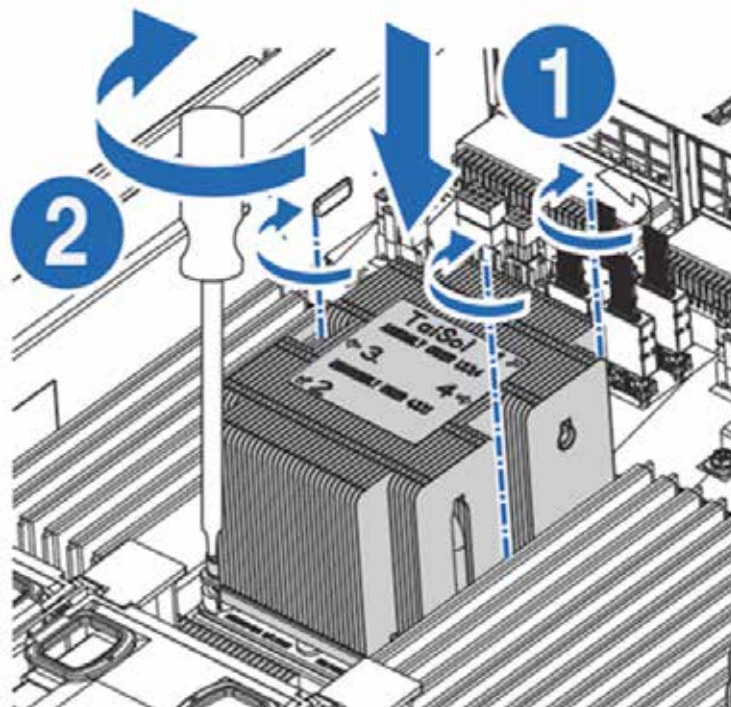
Step 1: Align the Clip's triangle mark with the CPU's corner mark, and then assemble the Clip and CPU together.



Step 2: Align the heatsink position marked by "1" with the Clip's triangle mark, vertically align the mounting holes on the heatsink with those on the Clip, and assemble the heatsink and Clip together.



Step 3: Install the assembled heatsink module onto the CPU socket, and the position marked by “1” should be aligned with the triangle mark on the CPU socket. Tighten the screws according to the sequence of 1, 2, 3, 4.



Notes:

- It is required to coat thermal grease evenly onto the contact position between CPU heatsink and CPU.
- The pins of the processor socket are easily damaged. If any pins are damaged, you may need to replace the motherboard.

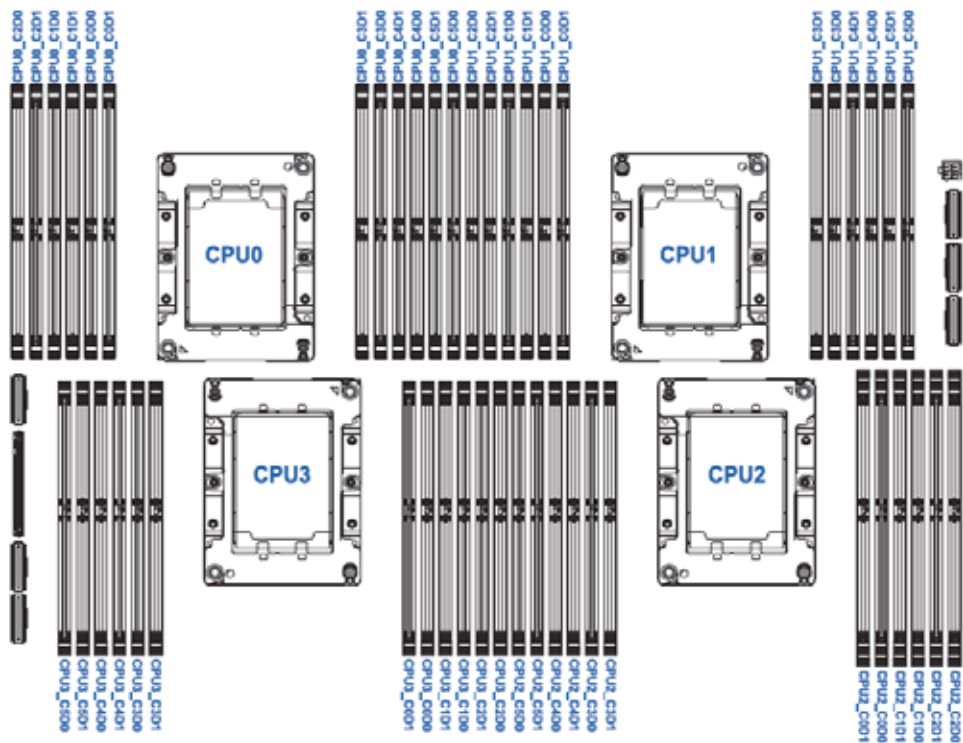
6.3 Memory Option

IMPORTANT:

This server does not support mixing DIMMs. Attempting to mix the DIMMs of different types may cause the server stops running during initialization.

All DIMMs installed in the server must be the same type.

- DIMM slot layout is as shown in the following figure:



- DIMM population guidelines:

Only DIMMs of the same type could be used in the same machine. Detailed DIMM population and combination principles are shown in the following figures:

• 4CPU Configuration - DIMM Quantity & Location (excluding the 12DIMM configuration)

2CPU Configuration - DIMM Quantity & Location (excluding the 12DIMM configuration)							
DIMM Qty.	1-2	3-4	5	7-8	9-10	11-12	13-14
CPU	DIMM0						
	Channel 0	Channel 3	Channel 1	Channel 4	Channel 2	Channel 5	Channel 0
CPU0	1	3	5	7	9	11	13
CPU1	2	4	●	8	10	12	14

• 2CPU Configuration - DIMM Quantity & Location (excluding the 6DIMM configuration)

2CPU Configuration - DIMM Quantity & Location (excluding the 6DIMM configuration)							
DIMM Qty.	1-2	3-4	5	7-8	9-10	11-12	13-14
CPU	DIMM0						
	Channel 0	Channel 3	Channel 1	Channel 4	Channel 2	Channel 5	Channel 0
CPU0	1	3	5	7	9	11	13
CPU1	2	4	●	8	10	12	14

• 4CPU 12DIMM Configuration

4CPU 12DIMM Configuration						
DIMM Qty.	12					
CPU	DIMM0					
	Channel 0	Channel 3	Channel 1	Channel 4	Channel 2	Channel 5
CPU0	1		5		9	
CPU1	2		6		10	
CPU2	3		7		11	
CPU3	4		8		12	

• 2CPU 6DIMM Configuration

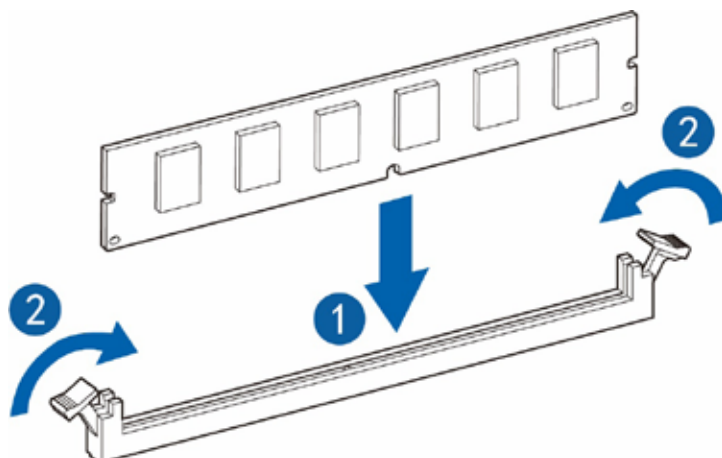
2CPU 6DIMM Configuration						
DIMM Qty.	6					
CPU	DIMM0					
	Channel 0	Channel 3	Channel 1	Channel 4	Channel 2	Channel 5
CPU0	1		3		5	
CPU1	2		4		6	

⚠ Population principle: C=Channel D=DIMM COD0=Channel0 DIMM0

1. Each CPU should be installed with 1 DIMM at least. If 1 DIMM, install it into C0-D0.
2. DIMMs are evenly distributed to each CPU by the amount of DIMM quantity/4. If the total number is not a multiple of 4, install them in order of CPU0/1/2/3.
3. ● indicates the installation position of the 12th or 6th DIMM.

Step 1: Open the lock tabs on both ends of the DIMM slot.

Step 2: Align the bottom key with the receptive point on the slot, press both ends of the DIMM with your thumbs. Insert the DIMM into the slot completely, and the lock tabs will automatically secure the DIMM, locking it into place.

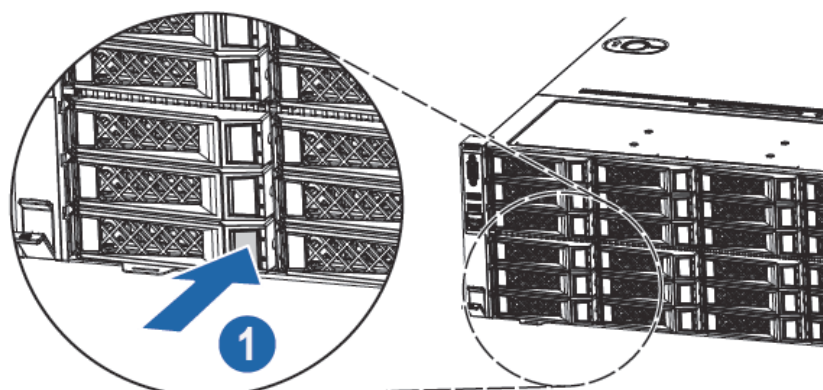


6.4 HDD Option

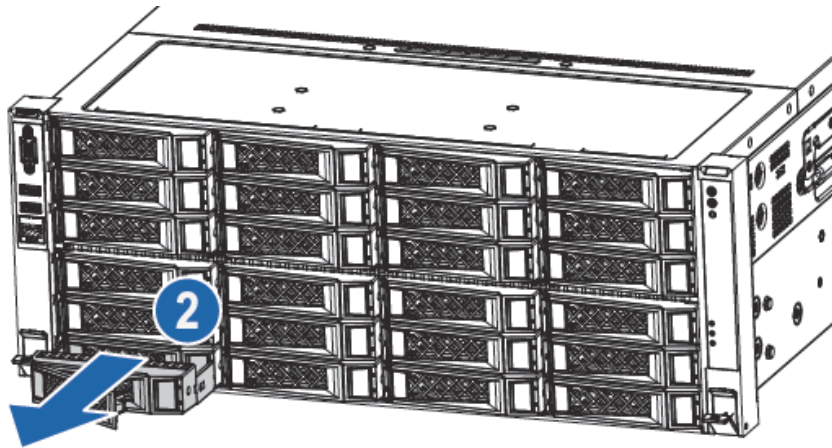
CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

1. Check the status of the hard disk drive from the hot-plug HDD LED.
2. Back up all data on the hard disk drive.
3. Remove the hard disk drive.

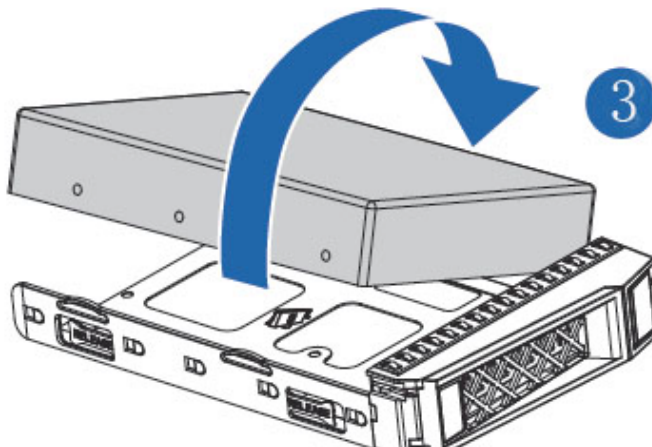
Step 1: Press the HDD panel button.



Step 2: The lever on HDD tray pops up automatically, pull it outwards and remove the HDD tray.



Step 3: Tilt and install the HDD into the tray.



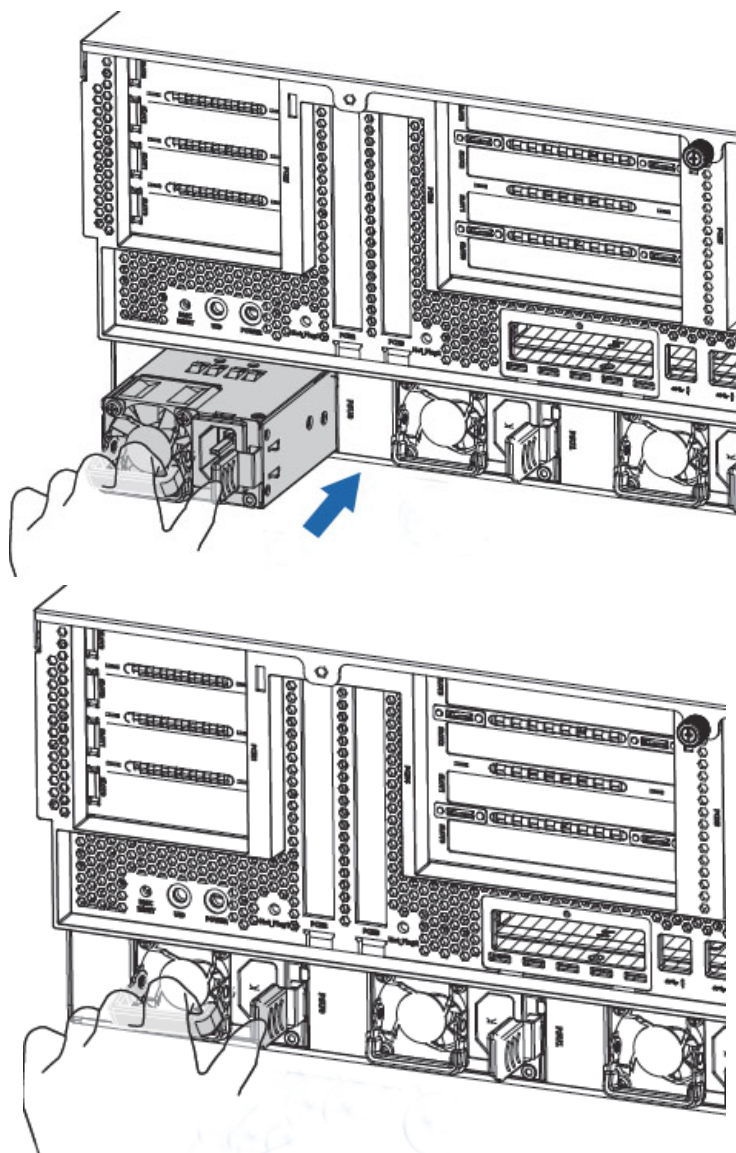
6.5 Redundant Hot-plug Power Supply Option

CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

1. Access the product rear panel.
2. Remove the power supply blank.


WARNING: To reduce the risk of personal injury from hot surfaces, allow the power supply or power supply blank to cool before touching it.

3. Install the power supply into the power supply bay.



4. Connect the power cord to the power supply.
5. Route the power cord through the power cord anchor or cable management arm.
6. Reposition the cable management arm into the operating position.
7. Connect the power cord to the power source.
8. Verify that the corresponding power supply LED is green.

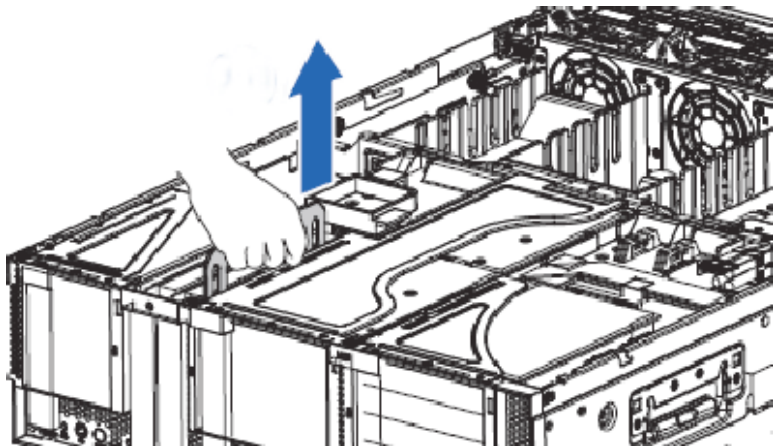
6.6 Expansion Board Option

 **CAUTION:** To prevent damage to the server or expansion boards, power down the server and remove all AC power cords before removing or installing the PCIe Riser cage.

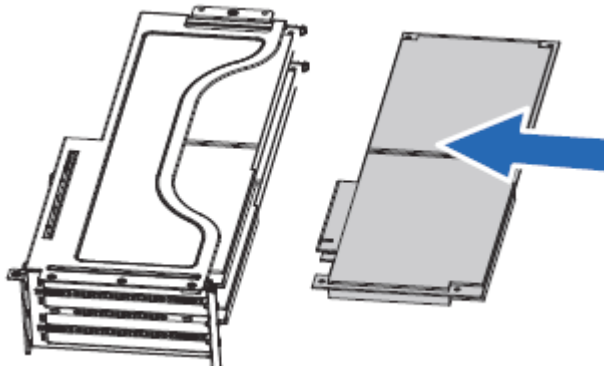
CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

1. Power down the server.
2. Extend the server from the rack.
3. Remove the access panel.
4. Remove the PCIE Riser cage according to tips on the label.

Step 1: Hold the handle on the PCIE Riser cage and remove it vertically.



Step 2: Install the expansion board to the PCIE Riser cage.




Step 3: Install the PCIE Riser cage back into the chassis.

6.7 Air Baffle Option

CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

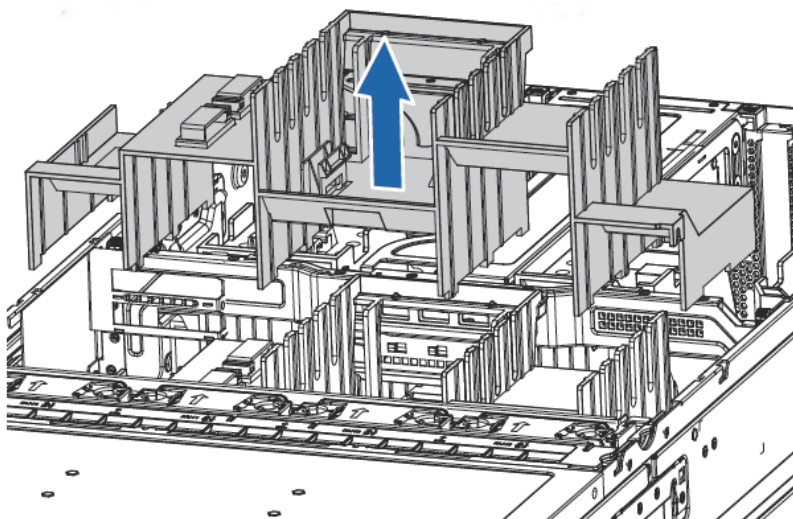
1. Power down the server.
2. Extend the server from the rack.

 **WARNING:** To reduce the risk of personal injury from hot surfaces, allow the machine to cool before touching it.

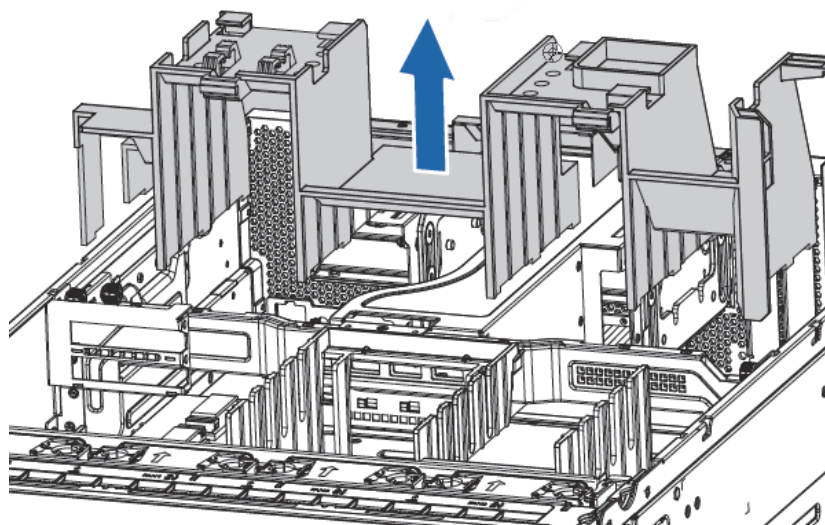
3. Remove the access panel.

Step 1: Remove the cables/capacitors above the air baffle.

Step 2: Remove the front air baffle vertically according to the following figure.

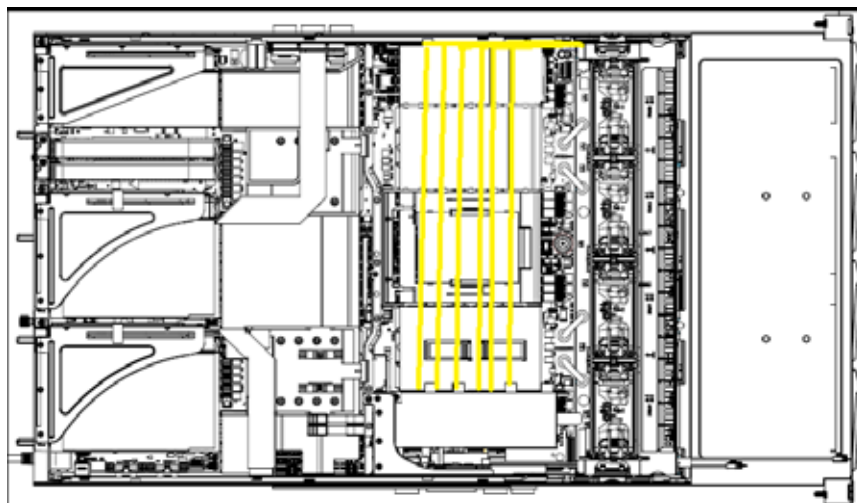


Step 3: Repeat step 2 to remove the rear air baffle.



7 Cabling

Schematic diagram of cabling using SAS/RAID/Expander card



Please route the cables according to the purchased machine configuration.

8 BIOS Setup

BIOS is the basic input/output system, which is the basic program code loaded in the motherboard chipset. It stores the computer's most important input/output program, POST program and system auto-boot program. It provides the most basic and most direct hardware settings and control, detects the boot device, boots the system or other preboot execution environment.

Inspur Purley platform server is developed on the basis of AMI Codebase, supporting Legacy and UEFI operating environments, with abundant in-band and out-of-band configuration functions and scalability. It can meet the customization needs of different customers.

Notes:

1. We recommend that you record the original BIOS settings before you modify them so it can safely revert to its previous state if required.
 2. The factory default settings are the optimal settings. It is advised not to alter the parameters before understanding their denotations.
 3. The common settings are introduced in detail in this chapter, but less common ones are not.
 4. The BIOS content varies according to different configurations of the products; hence the detailed introduction is elided.
-

8.1 Common Operations

8.1.1 Login to BIOS Interface

Power on the server. The system will then start to boot. When the following content appears below Inspur logo on the screen: "Press<ESC> to Front Page Press to Setup or <F11> to Boot Menu or <F12> to PXE Boot." Press DEL key. When "Entering Setup ..." appears in the lower right corner of the screen, it will enter the BIOS setup soon. In the BIOS main menu, you could select the subitem through direction keys to enter the submenu.


Other hotkeys function:

- Press ESC to enter BIOS Front Page interface.
- Press DEL to enter BIOS Setup interface.

- Press F11 to enter the boot management interface, select the boot device.
- Press F12 to boot the PXE.

BIOS Setup Interface Control Key Instruction Table

Key	Function
<Esc>	Exit or return from submenu to main menu
<<-> or <->>	Select a menu
<↑> or <↓>	Move the cursor up or down
<F1>	Help
<F5>/<F6>	Change the value
<F9>	Restore to the default configuration
<F10>	Save and exit
<Enter>	Execute commands or select a submenu

 Note: Options in grey are not available. Options with symbol “▶” have a submenu.

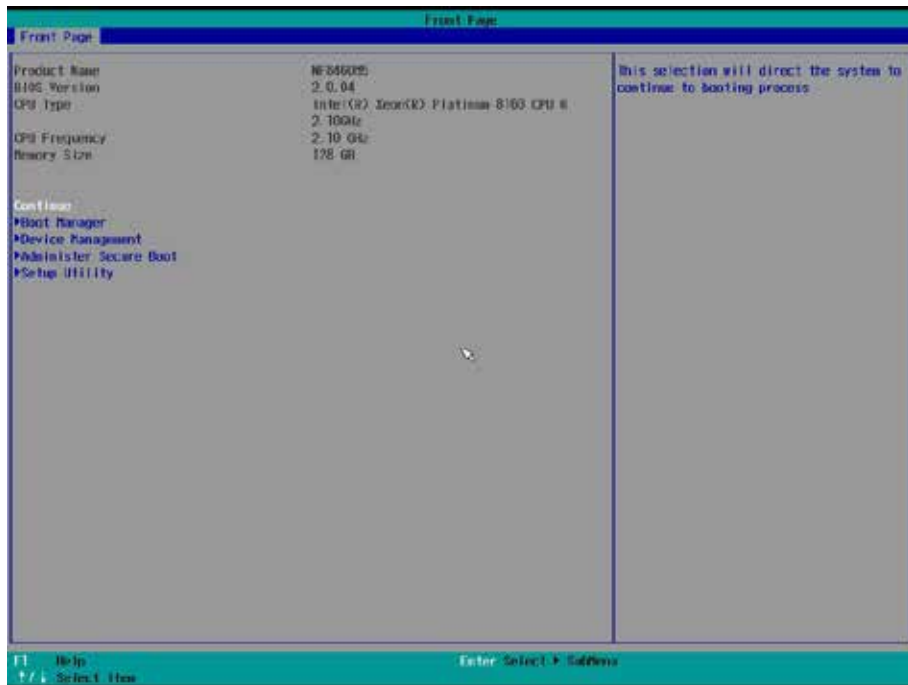


8.2 BIOS Parameter Description

8.2.1 Front Page

When Inspur Logo appears during system boot, press ESC to enter the Setup Front Page

interface, as shown in the following figure:



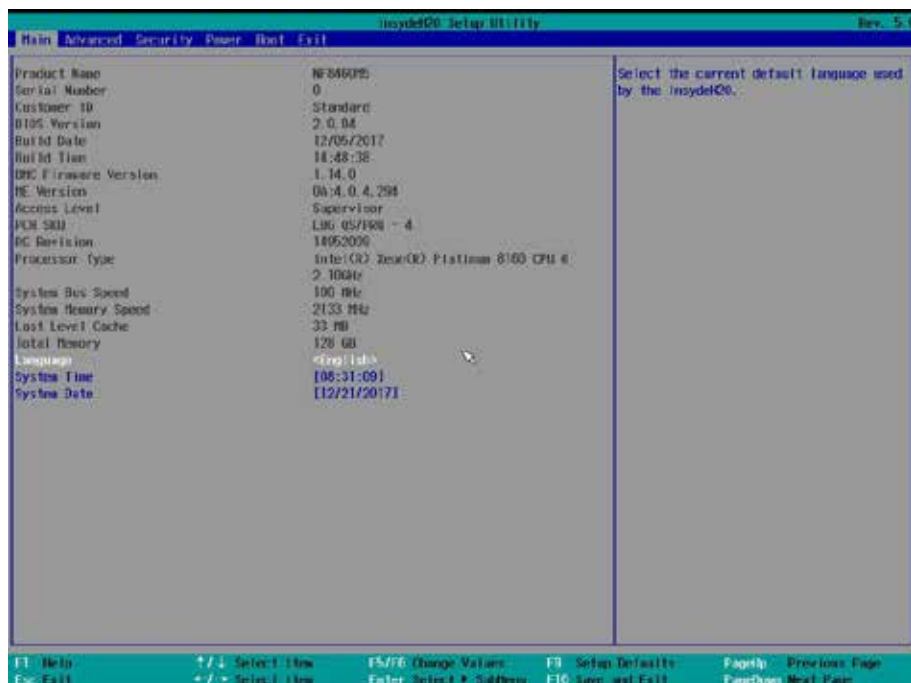
Front Page Interface Instruction Table

Interface Parameters	Function Description	Default Value
Product Name	Display the current product name	---
BIOS Version	Display BIOS version	---
CPU Type	Display CPU type	---
CPU Frequency	Display CPU nominal frequency	---
Memory Size	Display the current system memory size	---
Continue	Continue to boot option	---
Boot Manger	Boot device management option menu	---
Device Management	Device management option menu, including configuration option menus of PCH SATA/sSATA RAID, Intel NVME VMD RAID, SAS RAID and other devices in UEFI mode	---
Administer Secure Boot	Secure boot option settings	---
Setup Utility	BIOS setup interface	---

8.2.2 Main

When the logo appears, press DEL to enter the BIOS Setup Main interface, or select the Setup Utility option on the Front Page interface to enter the BIOS Setup Main interface. BIOS Main interface contains the basic information of BIOS system, the version information of BIOS, BMC and ME, CPU model information, total memory capacity information and system

time. The specific parameters are shown in the following table, and the Main interface is shown in the following figure.

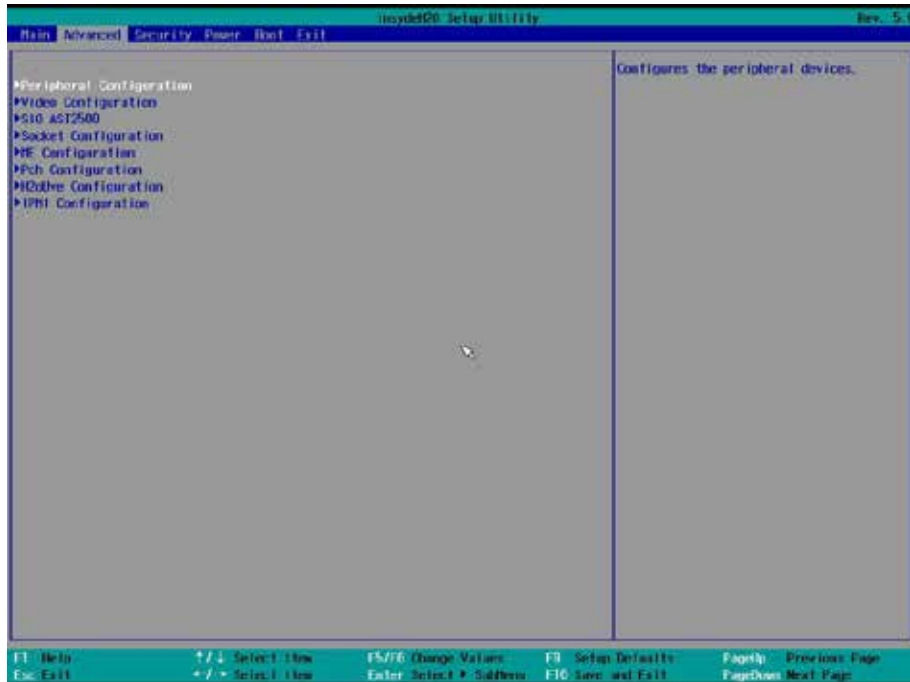


Main Interface Instruction Table

Interface Parameters	Function Description
Product Name	Display current product name
Serial Number	Display product serial number
Customer ID	Display the customer ID
BIOS Version	Display the BIOS version
Build Date	Display the build date for current BIOS Version
Build Time	Display the build time for current BIOS Version
BMC Firmware Version	Display the BMC firmware version
ME Version	Display the ME version
Access Level	Display the current access level
PCH SKU	Display the PCH revision
RC Revision	Display the reference code version
Processor Type	Display CPU type information
System Bus Speed	Display the speed of system bus
System Memory Speed	Display the memory speed
Last Level Cache	Display the last cache size
Total Memory	Display total memory size
Language	Display current Setup interface language
System Date	Display and set system date, allow changes, take effect immediately
System Time	Display and set system time, allow changes, take effect immediately

8.2.3 Advanced Menu

Advanced interface includes the BIOS system parameters and related function settings, as shown in the follow figure and table.

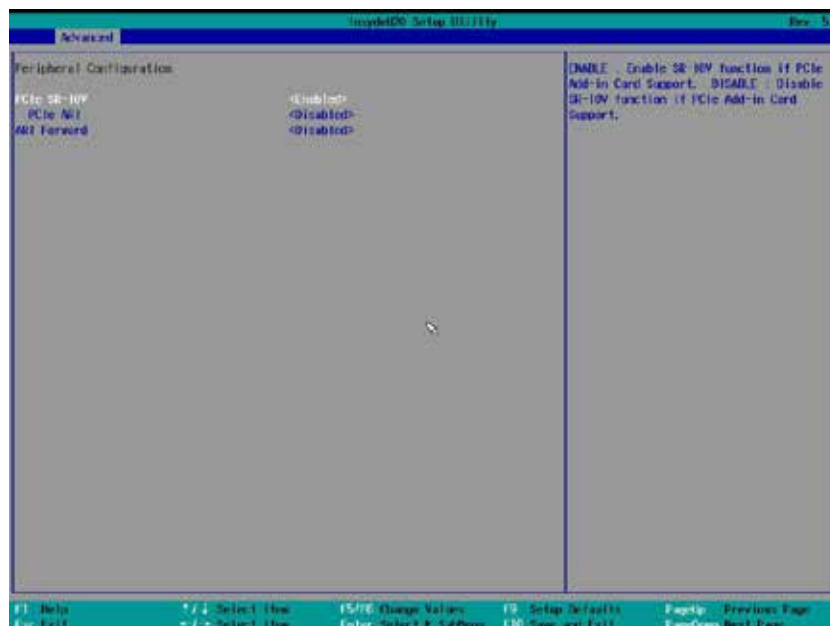


Advanced Interface Instruction Table

Interface Parameters	Function Description
Peripheral Configuration	Peripheral devices configuration submenu
Video Configuration	Video configuration submenu
SIO AST2500	SIO configuration submenu
Socket Configuration	Socket configuration submenu
ME Configuration	ME configuration submenu
PCH Configuration	PCH configuration submenu
IPMI Configuration	IPMI configuration submenu

8.2.3.1 Peripheral Configuration

Peripheral Configuration interface is used for system peripheral device settings, as shown in the follow figure and table.

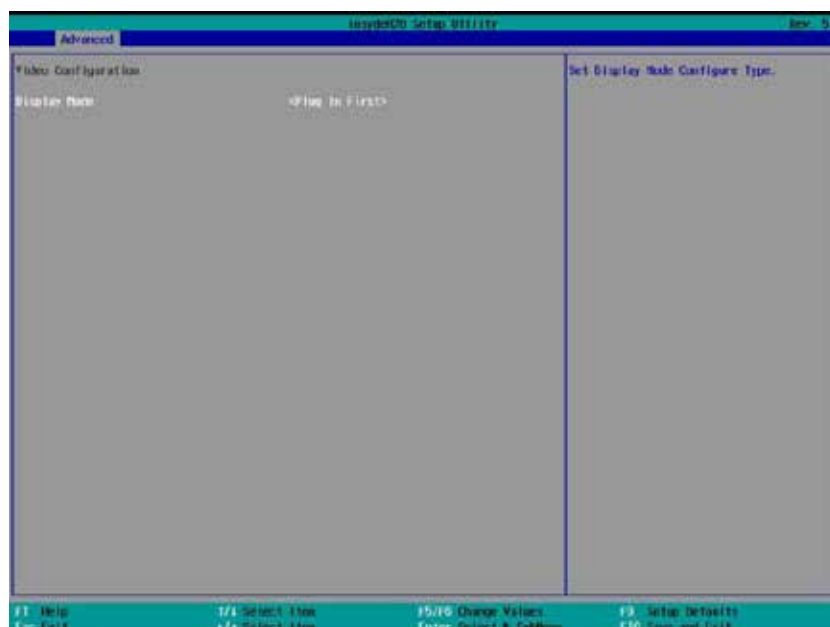


Peripheral Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
PCIe SR-IOV	PCIe device SR-IOV setting	Enabled
PCIe ARI	ARI capability setting	Disabled
ARI Forward	ARI forward setting	Disabled

8.2.3.2 Video Configuration

Video Configuration interface is used to set the system display mode, as shown in the following figure and table.

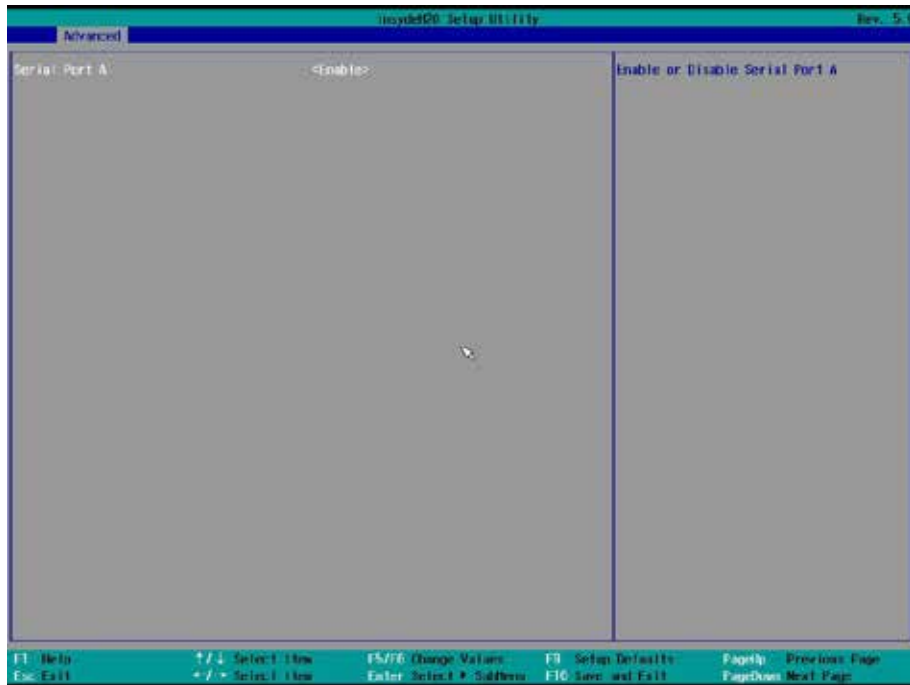


Video Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Display Mode	Set display mode configure type	Plug In First

8.2.3.3 SIO AST2500

SIO AST2500 interface is used for serial port settings, as shown in the following figure and table.

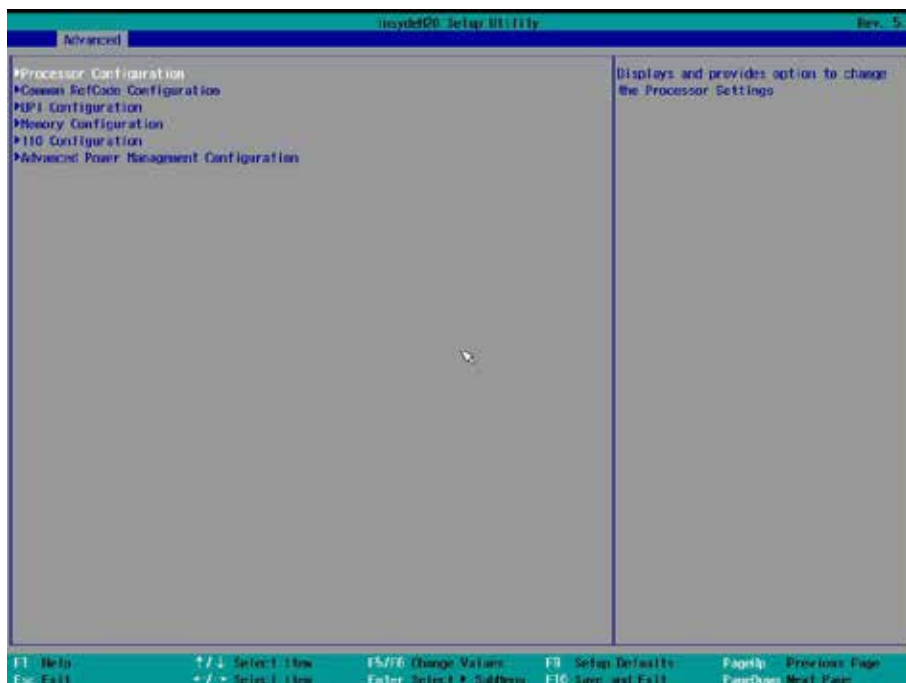


SIO AST2500 Interface Instruction Table

Interface Parameters	Function Description	Default Value
Serial Port A	Enable/disable serial port A	Enable

8.2.3.4 Socket Configuration

Socket Configuration interface is used for system processor and memory related settings, as shown in the following figure and table.

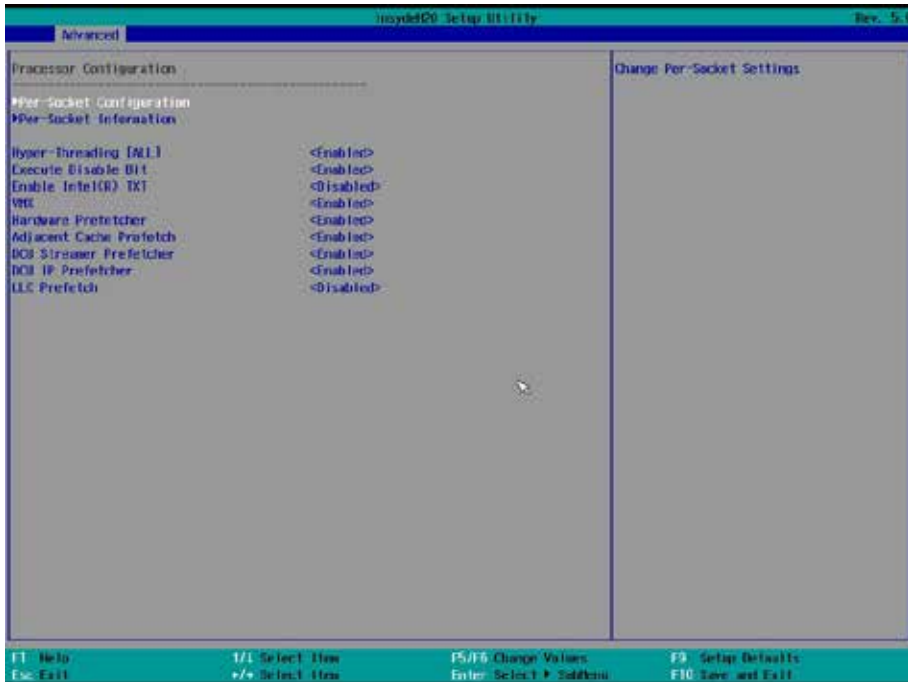


Socket Configuration Interface Instruction Table

Interface Parameters	Function Description
Processor Configuration	Processor configuration submenu
Common RefCode Configuration	Common reference code configuration submenu
UPI Configuration	UPI configuration submenu
Memory Configuration	Memory configuration submenu
IIO Configuration	IIO configuration submenu
Advanced Power Management Configuration	Advanced power management configuration submenu

8.2.3.4.1 Processor Configuration

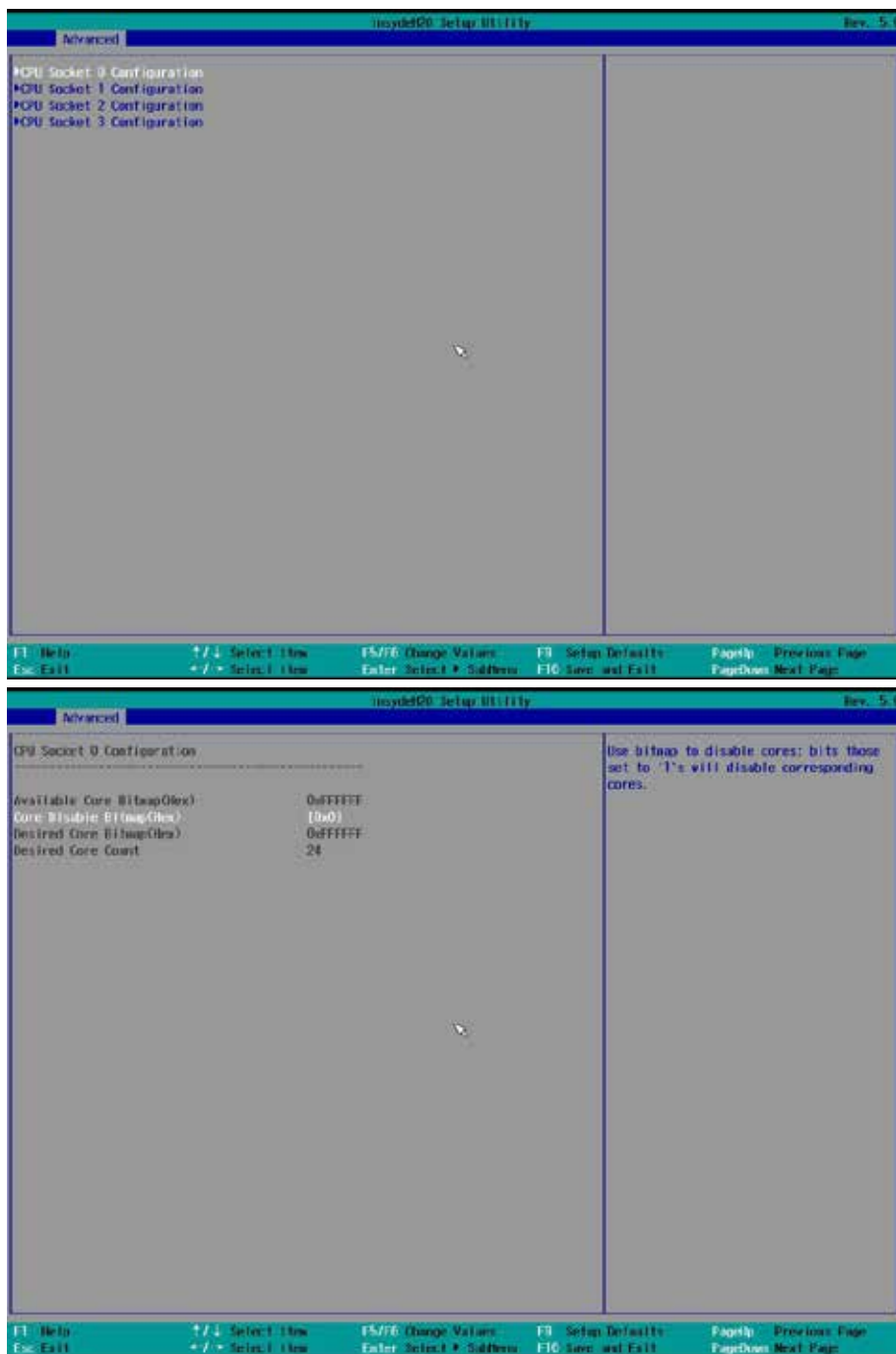
Processor Configuration interface is used for system processor related settings, as shown in the following figure and table.



Processor Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Per-Socket Configuration	Per-Socket setting submenu	--
Per-Socket Information	Per-Socket information display submenu	--
Hype-Threading [ALL]	Logical processor thread setting	Enabled
Execute Disable Bit	Virus protecting technology setting	Enabled
Enable Intel(R) TXT	Intel trustable execution technology setting	Disabled
VMX	Intel hardware-assisted virtualization technology settings	Enabled
Hardware Prefetcher	Hardware prefetch setting	Enabled
Adjacent Cache Prefetch	Adjacent high speed cache prefetch setting	Enabled
DCU Streamer Perfetcher	DCU streamer prefetch setting	Enabled
DCU IP Prefetcher	DCU IP prefetch setting	Enabled
LLC Prefetch	LLC prefetch setting	Disabled

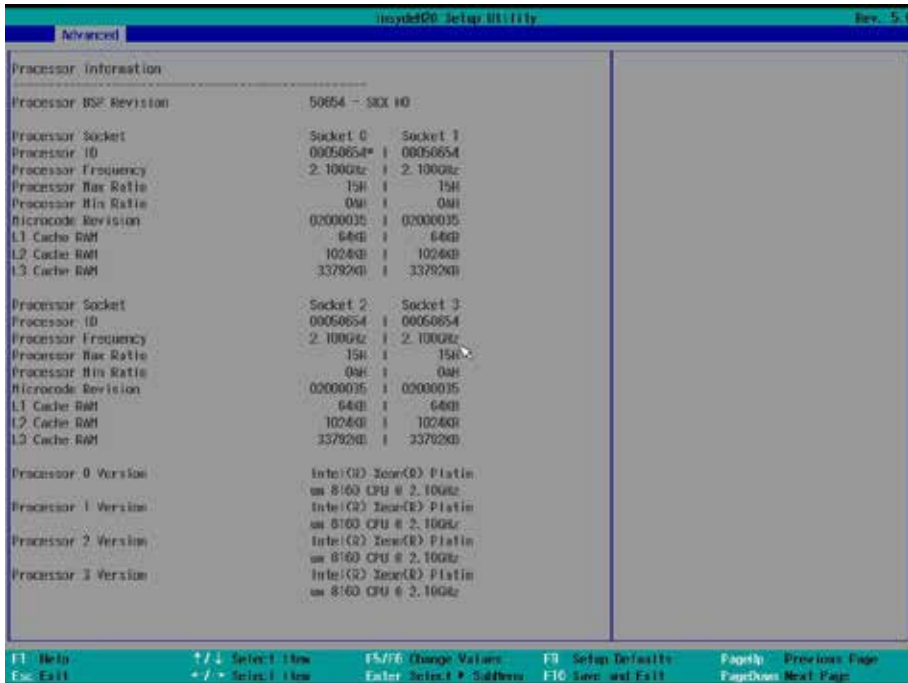
(a) Entering the Per-Socket Configuration submenu, core disable bitmap can be set, as shown in the following figures.



CPU Socket Configuration Interface Instruction Table

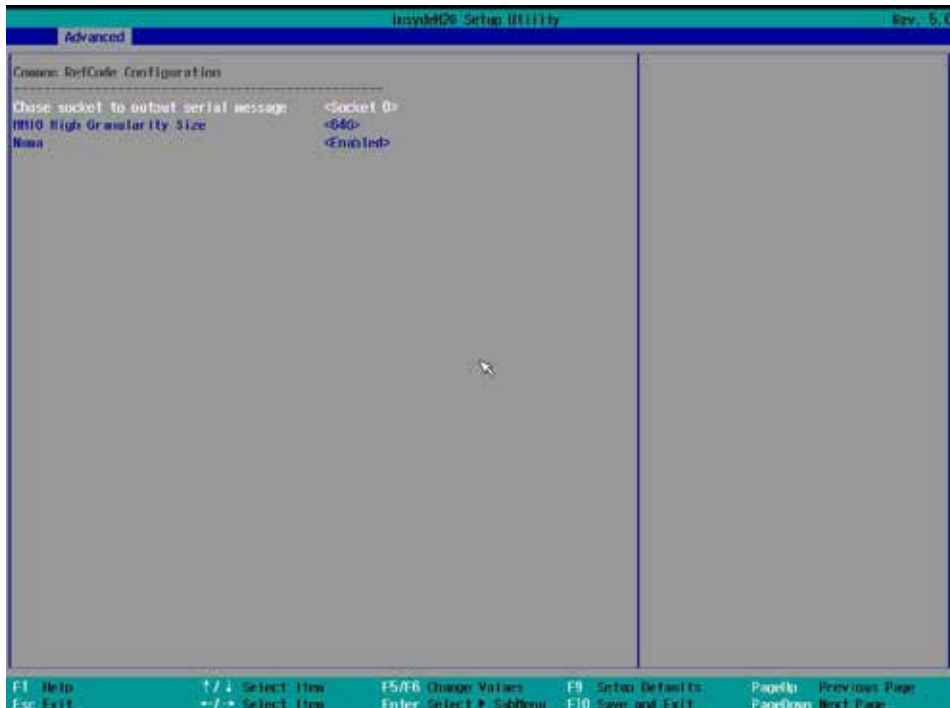
Interface Parameters	Function Description	Default Value
Available Core Bitmap(Hex)	Display the available core bitmap	--
Core Disable Bitmap(Hex)	Disabled core bitmap setting	0x0
Enable Core Bitmap(Hex)	Display the enable core bitmap	--
Desired Core Count	Display the number of enabled cores	--

(b) Information of all processors will be displayed by entering Per-Socket Information submenu.



8.2.3.4.2 Common RefCode Configuration

Common RefCode Configuration interface is used for common settings, as shown in the following figure and table.

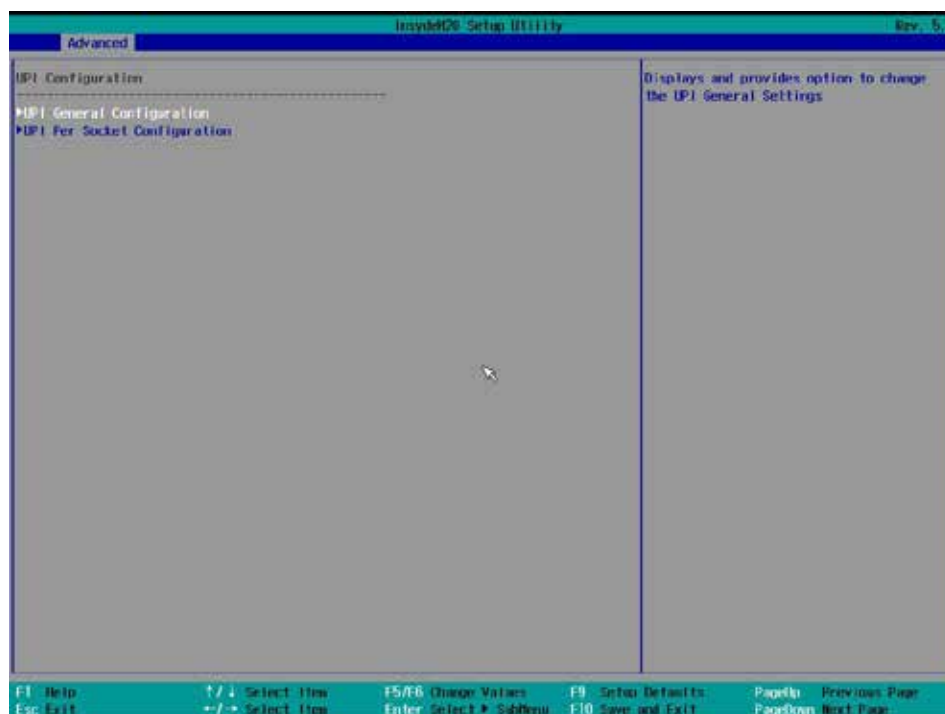


Common RefCode Configuration Interface Introduction

Interface Parameters	Function Description	Default Value
Chose socket to output serial message	MRC serial message display setting	Socket0
MMIO High Granularity Size	MMIO high resources granularity size setting	256G
Numa	Numa switching setting	Enabled

8.2.3.4.3 UPI Configuration

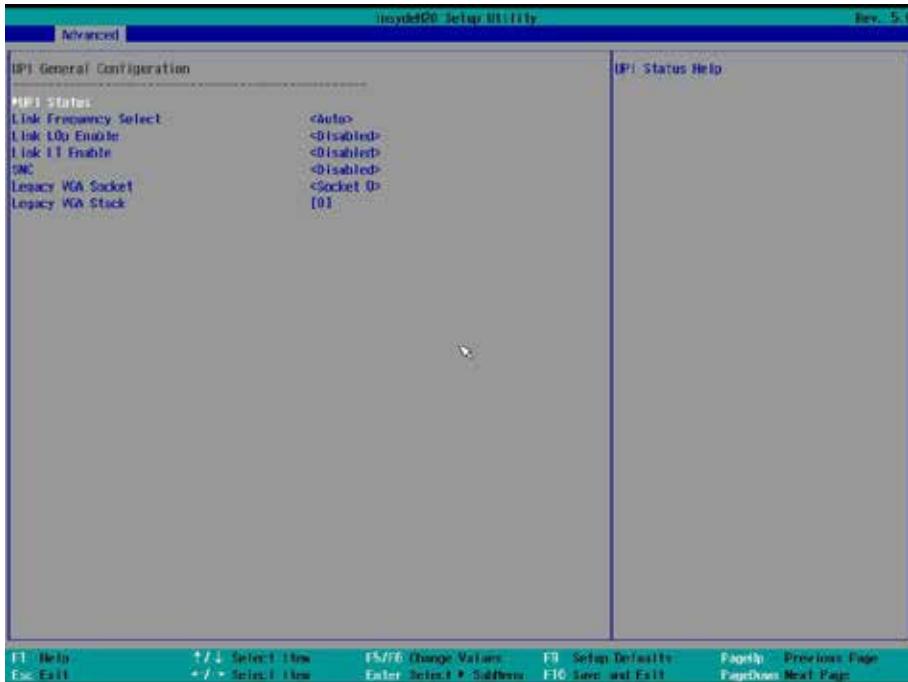
UPI Configuration interface is used for UPI related settings, as shown in the following figure and table.



UPI Configuration Interface Instruction Table

Interface Parameters	Function Description
UPI General Configuration	UPI general configuration submenu
UPI Per Socket Configuration	UPI per-socket configuration submenu

(a) It will display UPI general configuration menu by entering UPI General Configuration submenu.



UPI General Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
UPI Status	UPI status display submenu	--
Link Frequency Select	UPI link frequency setting	Auto
Link L0p Enable	UPI link power saving mode settings, which is made when bandwidth is half of the peak bandwidth.	Disabled
Link L1 Enable	In the case that system is extremely idle, turn off QPI Link.	Auto
SNC	SNC setting	Disabled
Legacy VGA Socket	Legacy VGA socket range setting	Socket0
Legacy VGA Stack	Legacy VGA stack range setting	0

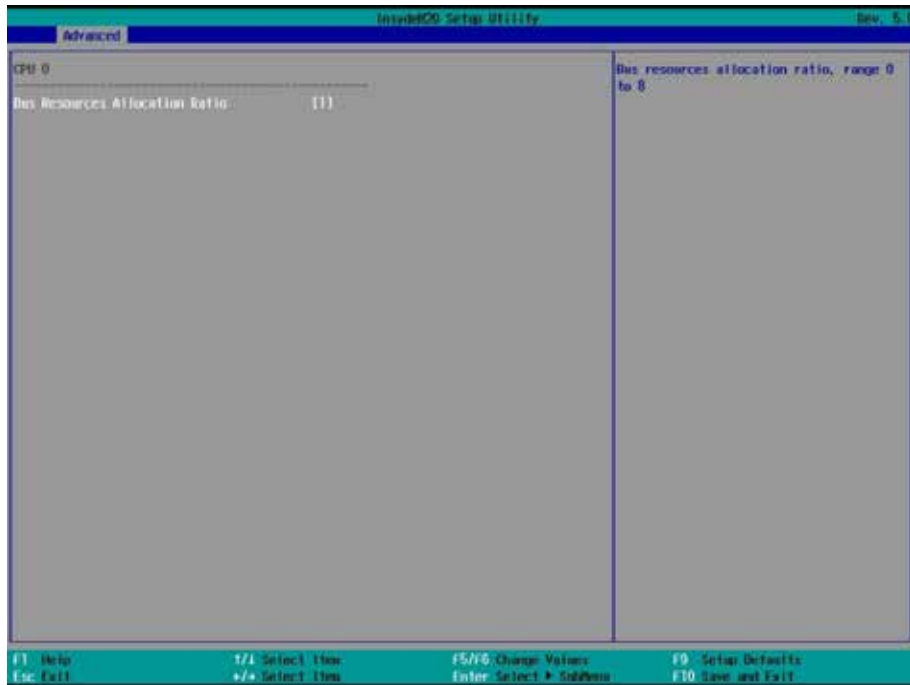
When using external VGA card, it needs to configure the Legacy VGA Socket/Legacy VGA Stack settings according to the rules in the following table:

External VGA Card Location & Parameters Settings

PCI-E	Usage	Socket	Stack
PCI-E1	Insert directly or use Slot0 of x16 Riser card	Socket 2	3
PCI-E4	Insert directly or use Slot0 of x16 Riser card	Socket 1	3
PCI-E4	Use Slot1 of x16 Riser card	Socket 2	2
PCI-E5	Insert directly or use Slot0 of x16 Riser card	Socket 3	2
PCI-E5	Use Slot1 of x16 Riser card	Socket 3	3

(b) Bus resources allocation ration can be configured by entering UPI Per Socket

Configuration submenu.

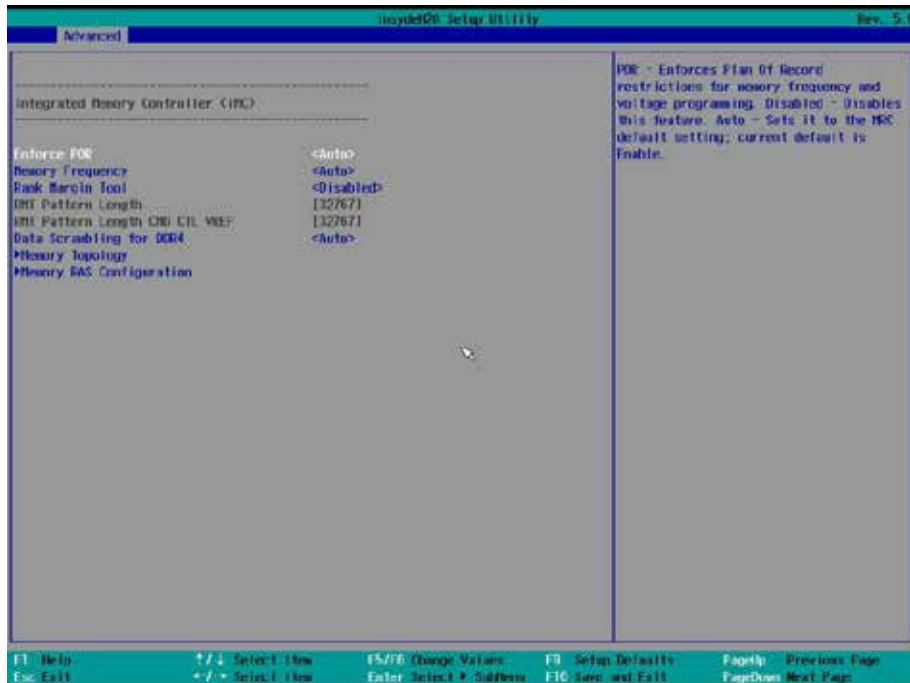


UPI Per Socket Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Bus Resources Allocation Ratio	Bus resources allocation ratio of each CPU	1

8.2.3.4.4 Memory Configuration

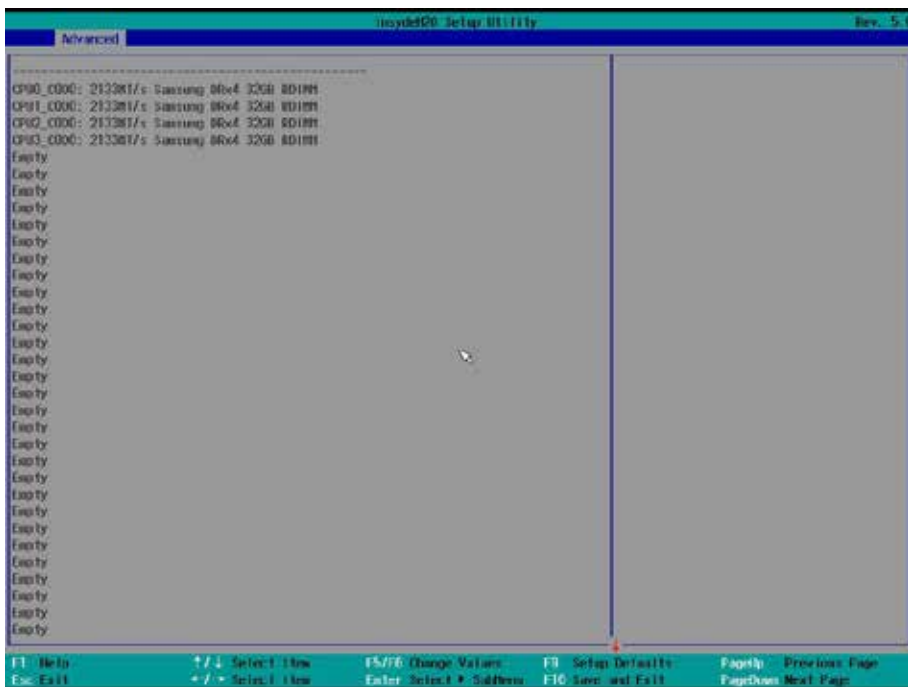
Memory Configuration interface is used for memory related settings, as shown in the following figure and table.



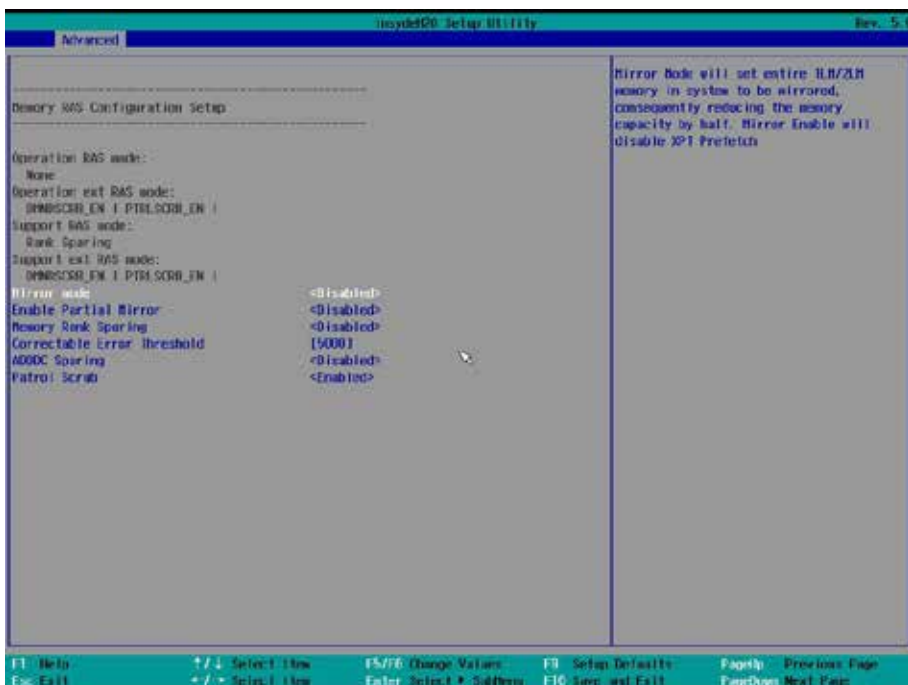
Memory Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Enforce POR	Enforce POR settings	Auto
Memory Configuration	Memory frequency select setting	Auto
Rank Margin Tool	Rank margin tool setting	Disabled
RMT Pattern Length	Set the pattern length for the rank margin tool when it's enabled	32767
RMT Pattern Length CMD CTL VREF	Set the pattern length for the rank margin tool (CMD CTL VREF step) when it's enabled	32767
Data Scrambling for DDR4	Data scrambling setting	Auto
Memory Topology	Memory topology submenu	--
Memory RAS Configuration	Memory RAS setting submenu	--

(a) It will display the memory topology information by entering the Memory Topology submenu.



(b) It will display the memory RAS configuration by entering the Memory RAS Configuration submenu.

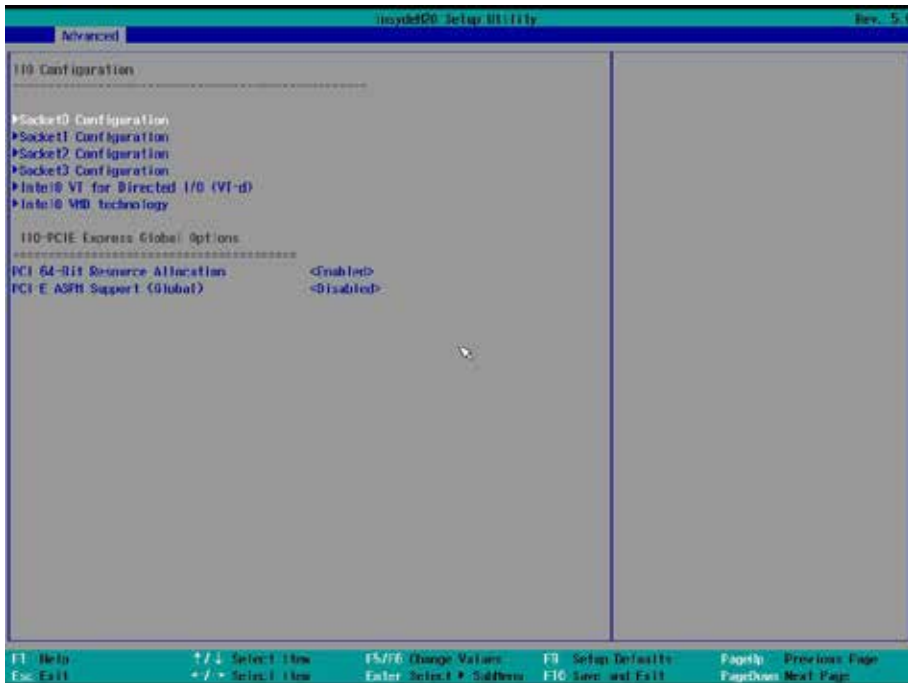


Memory RAS Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Operation RAS mode	Display current operation RAS mode	--
Operation ext RAS mode	Display current operation extra RAS mode	--
Support RAS mode	Display supported RAS mode	--
Support ext RAS mode	Display supported extra RAS mode	--
Mirror Mode	Mirror mode setting	Disabled
Enable Partial Mirror	Partial mirror mode setting	Disabled
Memory Rank Sparing	Memory Rank hot sparing setting	Disabled
Correctable Error Threshold	Correctable error threshold setting	5000
ADDDC Sparing	ADDDC sparing setting	Disabled
Patrol Scrub	Patrol scrub setting	Enabled

8.2.3.4.5 IIO Configuration

IIO Configuration interface is used for PCIe slot settings, as shown in the following figure and table.

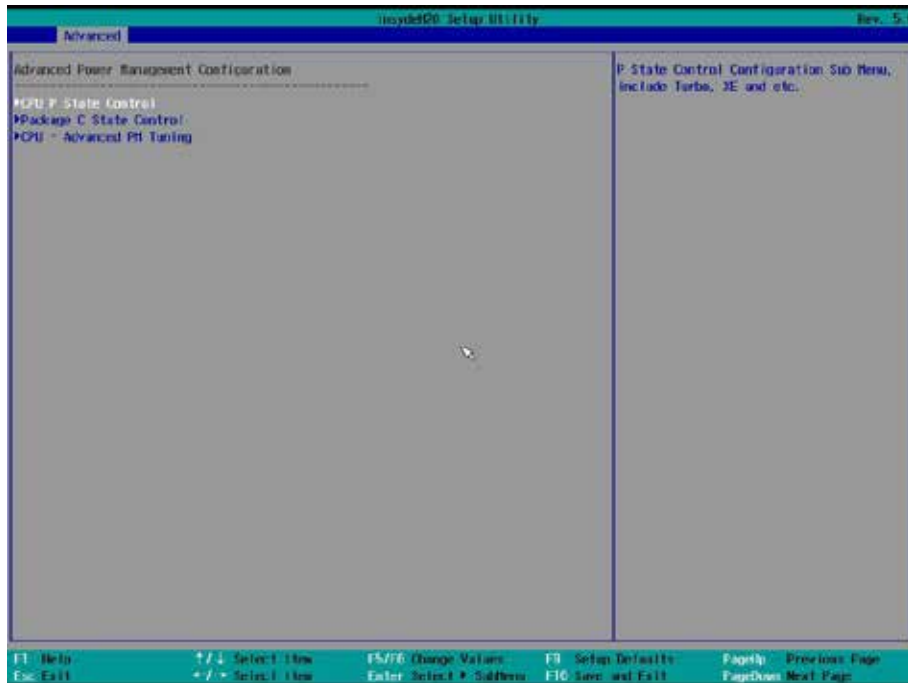


IIO Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Socket# Configuration	Socket# IIO Configuration setting submenu	--
Intel VT for Directed I/O (VT-d)	Intel VT-d switching setting submenu	--
Intel VMD Technology	Intel VMD setting, to enable/disable the VMD of each Pstack on the CPU	
PCI 64-Bit Resource Allocation	PCI 64-bit resource allocation setting	Enabled
PCI-E ASPM Support (Global)	Global PCIe device ASPM support setting	Disabled

8.2.3.3.6 Advanced Power Management Configuration

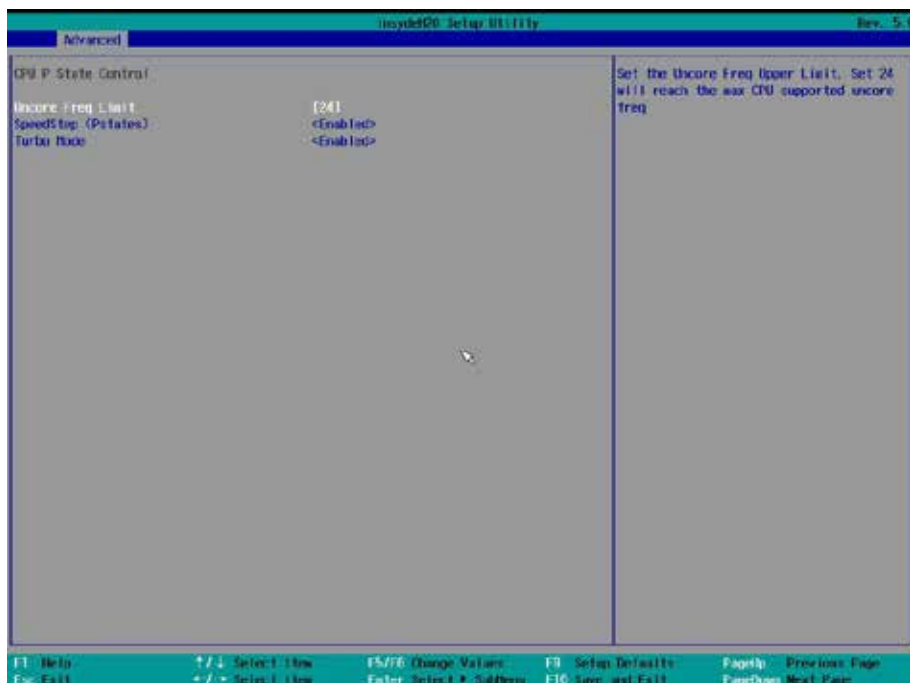
Advanced Power Management Configuration interface is used for CPU power management settings, as shown in the following figure and table.



Advanced Power Management Configuration Interface Instruction Table

Interface Parameters	Function Description
CPU P State Control	CPU P state control configuration submenu
Package C State Control	Package C state setting submenu
CPU-Advanced PM Tuning	CPU advanced PM turning setting submenu

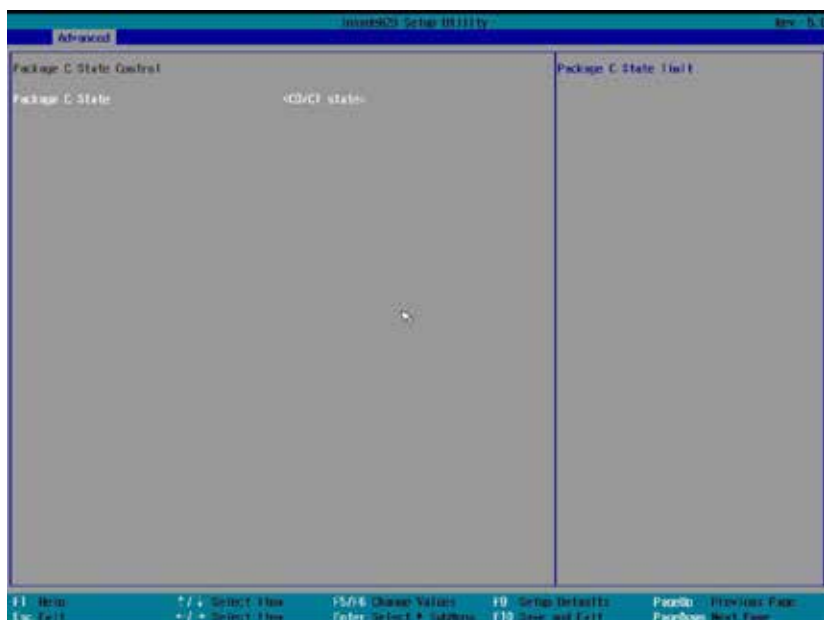
(a) It will display the CPU P state configuration menu by entering CPU P State Control submenu.



CPU P State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Uncore Fre Limit	Uncore frequency limit setting	24
SpeedStep (Pstates)	CPU P state setting	Enabled
Turbo Mode	Turbo mode setting	Enabled

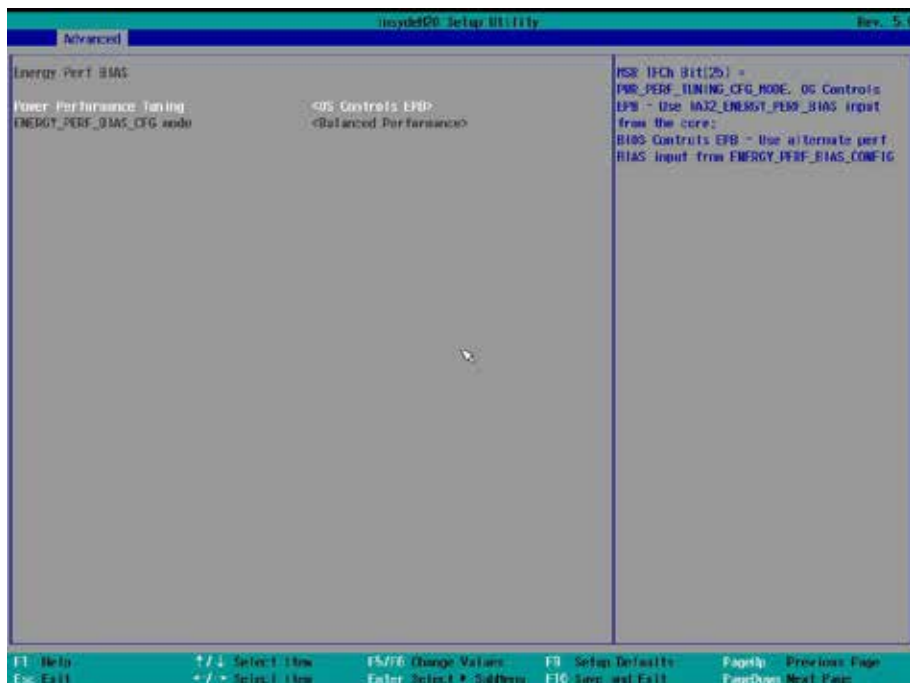
(b) It will display the package C state configuration menu by entering Package C State Control submenu.



Package C State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Package C State	Package C state setting	C0/C1 State

(c) Select CPU Advanced PM Tuning menu, select Energy Perf BIAS, and enter power performance setting interface, as shown below:

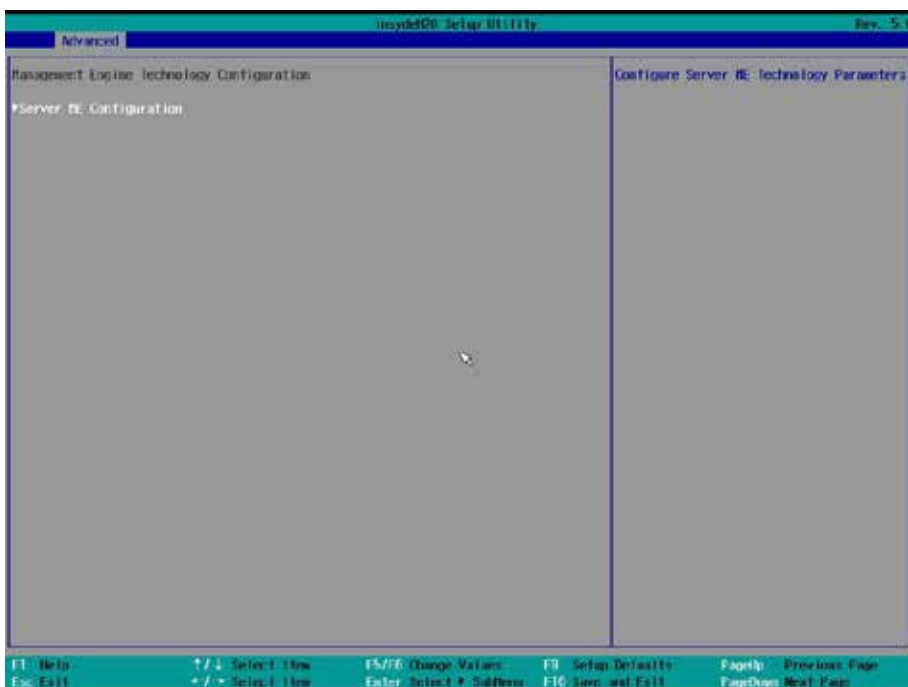


Energy Perf BIAS Interface Instruction Table

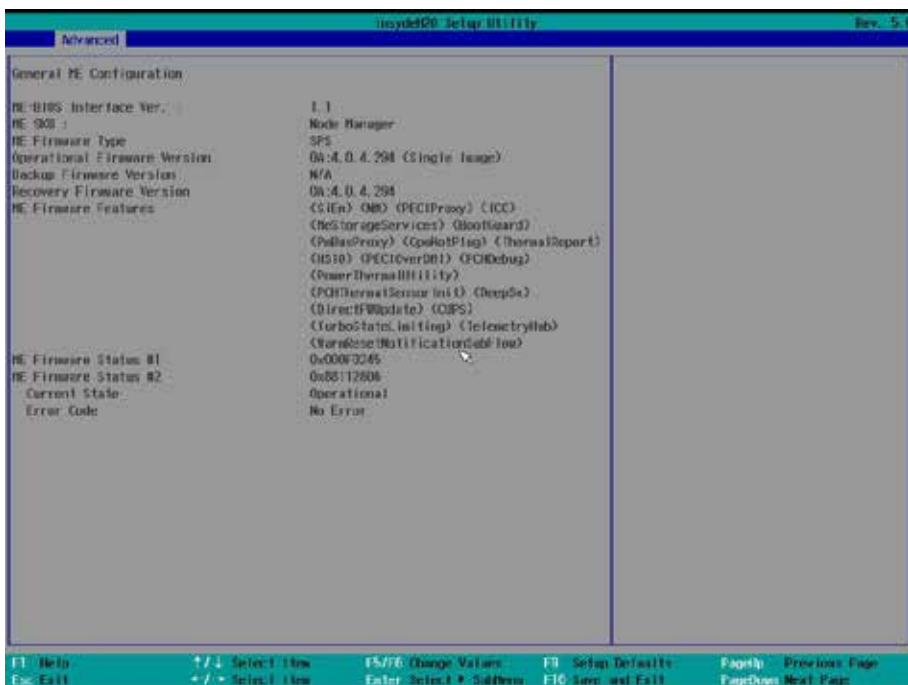
Interface Parameters	Function Description	Default Value
Power Performance Tuning	Power performance tuning setting	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Performance setting	Balanced Performance

8.2.3.5 ME Configuration

ME Configuration interface displays the information related with ME configuration.



The general information of ME configuration will be displayed by entering Server ME Configuration submenu.

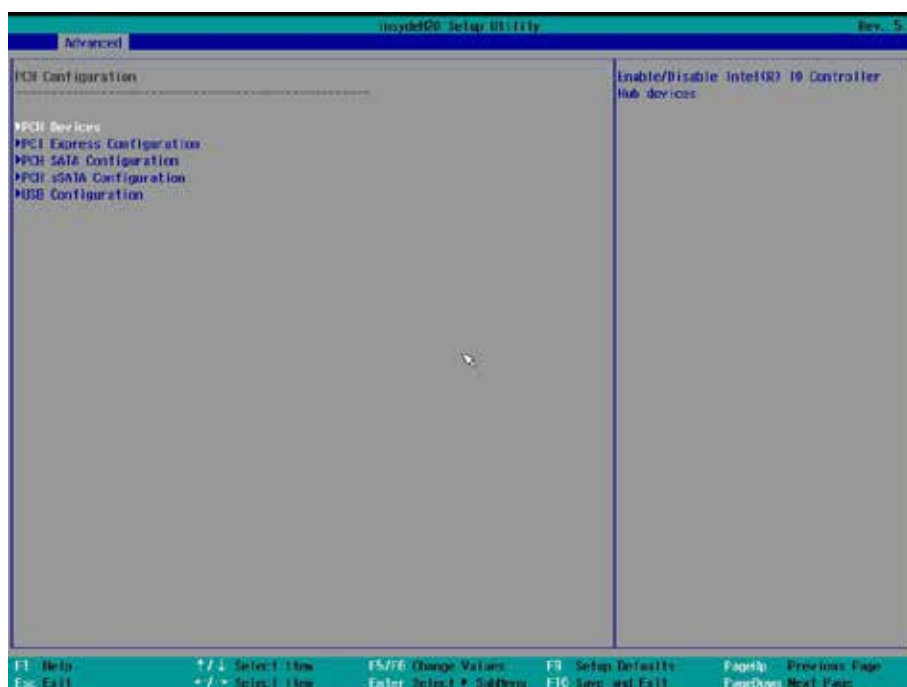


Sever ME Configuration Interface Instruction Table

Interface Parameters	Function Description
ME-BIOS Interface Ver.	ME BIOS interface version
ME SKU	ME SKU
ME Firmware Type	ME FW type
Operational Firmware Version	Current operational ME FW version
Backup Firmware Version	Backup ME FW version
Recovery Firmware Version	Recovery ME FW version
ME Firmware Features	ME FW features
ME Firmware Status#1	ME FW status1
ME Firmware Status#2	ME FW status 2
Current State	ME current state
Error Code	ME error code

8.2.3.6 PCH Configuration

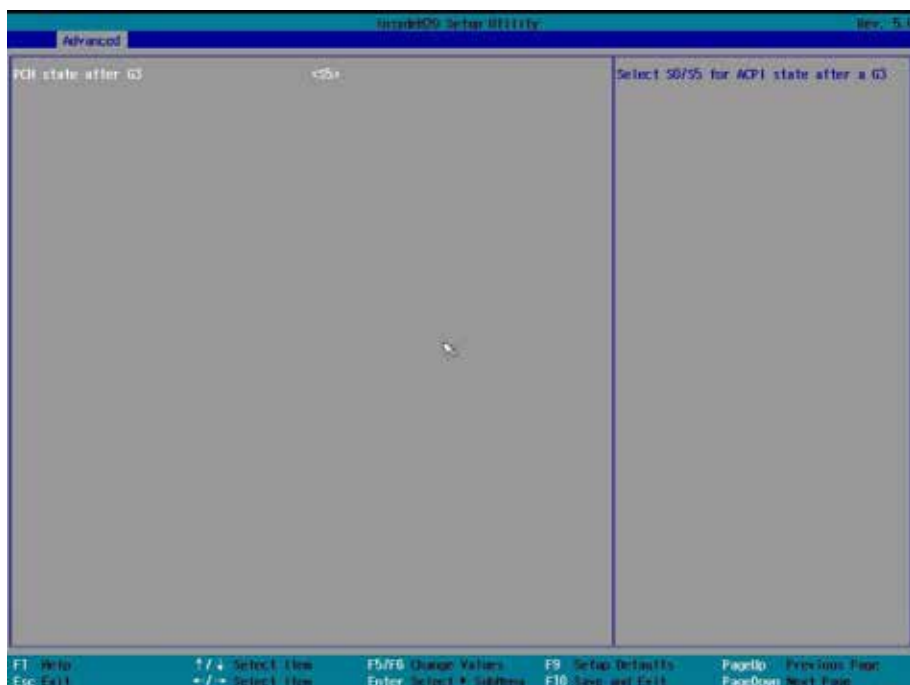
PCH Configuration interface is used to set the PCH related devices, including SATA/sSATA, USB options, etc., as shown in the following figure and table.



PCH Configuration Interface Instruction Table

Interface Parameters	Function Description
PCH Devices	Intel IO control hub device setting submenu
PCH Express Configuration	PCH Express devices display and setting submenu
PCH SATA Configuration	PCH SATA configuration submenu
PCH sSATA Configuration	PCH sSATA configuration submenu
USB Configuration	PCH USB configuration submenu

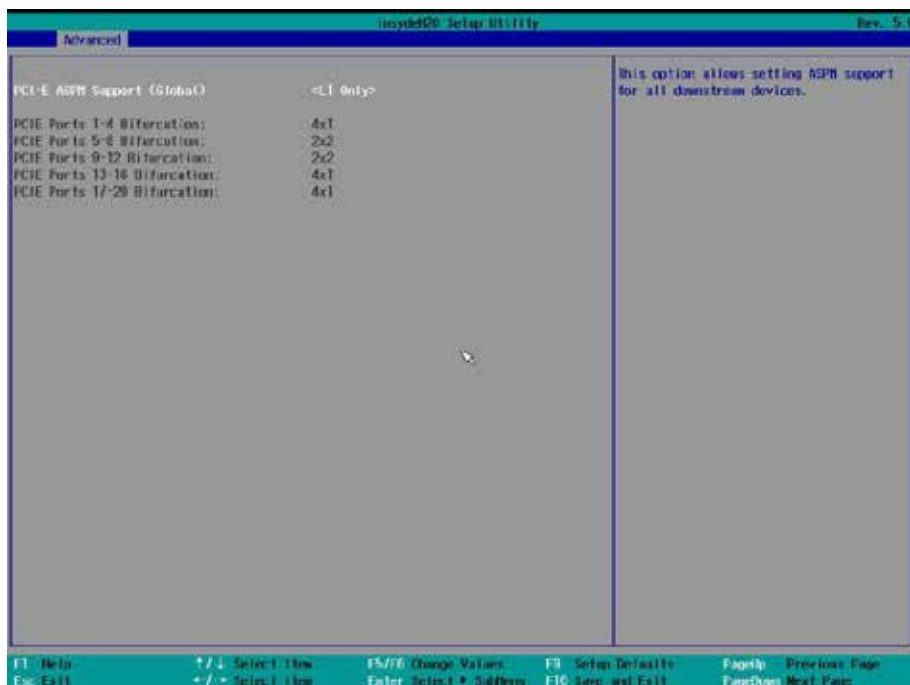
8.2.3.6.1 PCH Devices



PCH Devices Interface Instruction Table

Interface Parameters	Function Description	Default Value
PCH state after G3	Select S0/S5 for ACPI state after a G3	S5

8.2.3.6.2 PCI Express Configuration

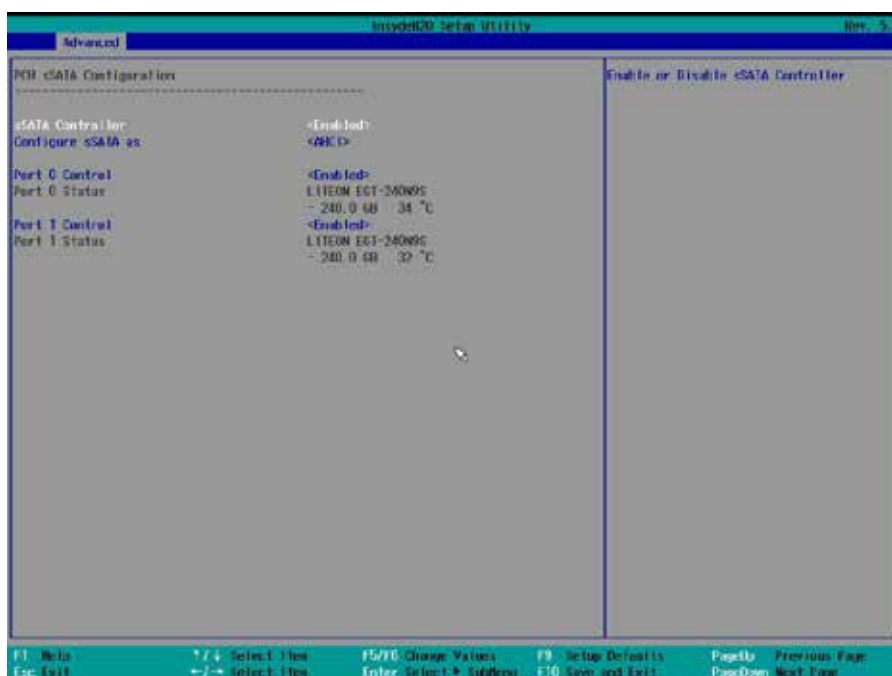
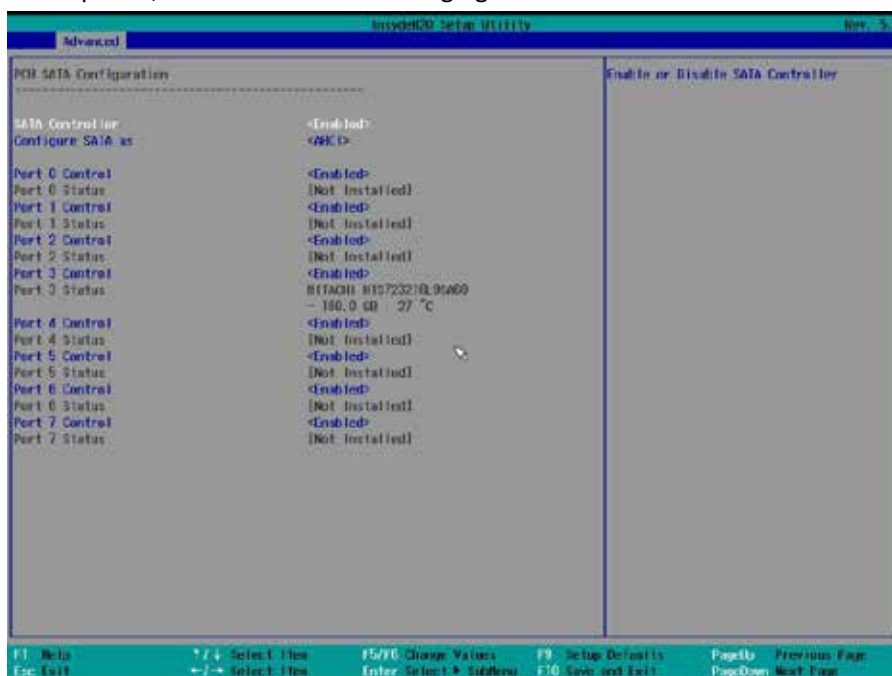


PCI Express Configuration Menu Interface Instruction Table

Interface Parameters	Function Description	Default value
PCI-E ASPM Support (Global)	Setting ASPM support for all downstream devices	L1 Only
PCI-E Ports X Bifurcation	Bifurcation of PCIe port X	--

8.2.3.6.3 PCH SATA Configuration/PCH sSATA Configuration

PCH SATA Configuration/PCH sSATA Configuration interface is used to set the onboard PCH SATA/sSATA options, as shown in the following figures.



PCH SATA Configuration Menu Interface Instruction Table

Interface Parameters	Function Description	Default value
SATA Controller	Enable or disable SATA controller	Enabled
Configure SATA as	Set the SATA Controller as AHCI or RAID	AHCI
Port X Control	Enable or disable SATA port X	Enabled
Port X Status	SATA port X status	--

PCH SATA/sSATA RAID mode setting

SATA/sSATA controller is set to RAID mode. When the Boot Type is UEFI, take sSATA setting as an example. When the Boot Type is Legacy, take SATA setting as an example. Under the same Boot Type, sSATA is set in the same way as SATA.

1. Set the Configure SATA /sSATA as option to [RAID], press F10 to save the setting, and the system reboots.



Notes:

When the SATA/sSATA Mode option is set to RAID, you can choose whether to enable the Load EFI Driver for RAID option. When the Boot Type is UEFI mode, the setting is Enabled. However, when the Boot Type is Legacy mode, you need to set Load EFI Driver for RAID to Disabled.

When the Boot Type is UEFI mode and the Load EFI Driver for RAID is set to Enabled, the system will load Intel RSTe SATA/sSATA Controller to manage the SATA/sSATA RAID after

pressing F10 and system reboot. When the logo appears during system startup, press ESC to enter the Front Page interface, enter the Device Management configuration interface, and select Intel RSTe SATA/sSATA Controller to configure RAID.

When the Boot Type is Legacy mode and the Load EFI Driver for RAID is set to Disabled, the system will load Legacy Option ROM to manage the SATA/sSATA RAID after pressing F10 and system reboot. During system startup, the screen will prompt: Press <CTRL-I> to enter Configuration Utility...then press <Ctrl> and <I> simultaneously to enter the SATA/sSATA RAID configuration interface for RAID configuration.

2. Take SATA RAID configuration in Legacy Mode as an example to introduce the SATA RAID configuration. During system startup, the screen will prompt: Press <CTRL-I> to enter Configuration Utility... Press <Ctrl> and <I> simultaneously to enter the SATA RAID configuration, as shown in the following figure.

```

Intel(R) Rapid Storage Technology enterprise - SATA Option ROM - 5.1.0.1007
Copyright(C) 2003-16 Intel Corporation. All Rights Reserved.

RAID Volumes:
None defined.

Physical Devices:
ID Device Model Serial # Size Type/Status(Vol ID)
0 HGST HUH720000AL UKJGSDLX 7.27T Non-RAID Disk
1 HGST HUH720000AL UKJBEUHX 7.27T Non-RAID Disk
Press <CTRL-I> to enter Configuration Utility...

```

2.1 After entering SATA RAID configuration interface, it will display the main menu list, the information (HDD ID, HDD type, HDD capacity, volume member or not) of HDDs connected to SATA controller, and the existed RAID volumes information (including volume ID, name, RAID level, capacity, status, bootable or not). There are 5 executable menus in the SATA RAID configuration interface, as shown in the following figure.

```

Intel(R) Rapid Storage Technology enterprise - SATA Option ROM - 5.1.0.1007
Copyright(C) 2003-16 Intel Corporation. All Rights Reserved.

[ MAIN MENU ]
1. Create RAID Volume
2. Delete RAID Volume
3. Reset Disks to Non-RAID
4. Mark Disks as Spare
5. Exit

[ DISK/VOLUME INFORMATION ]

RAID Volumes:
None defined.

Physical Devices:
ID Device Model Serial # Size Type/Status(Vol ID)
0 HGST HUH720000AL UKJGSDLX 7.27T Non-RAID Disk
1 HGST HUH720000AL UKJBEUHX 7.27T Non-RAID Disk

[↑] Select [ESC] Exit [ENTER] Select Menu

```

Key Instruction Table

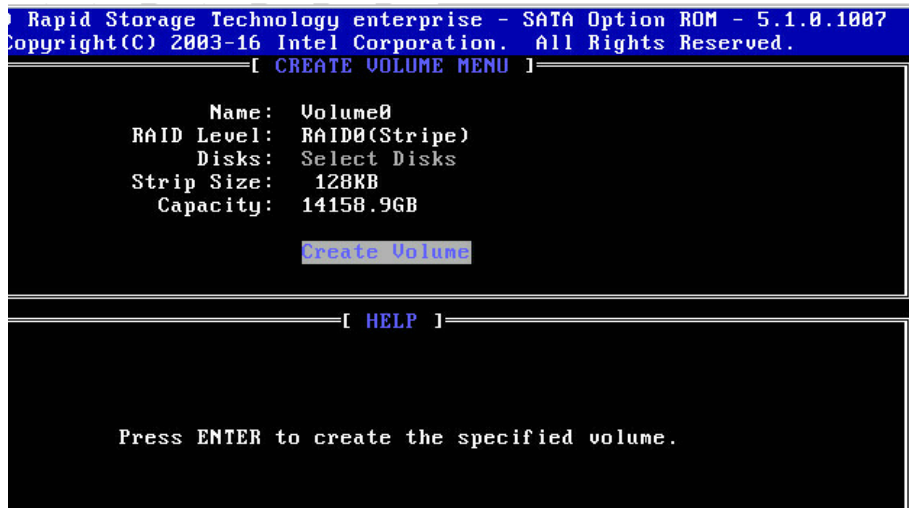
Key	Description
↑↓	Used to move cursor in different menus or to change values of menu options.
TAB	To select the next menu option.
Enter	To select a menu.
Esc	To exit menu or return to previous menu from submenu.

Menu Instruction Table

Create RAID Volume	To create an RAID volume.
Delete RAID Volume	To delete an existed RAID volume.
Reset Disks to Non-RAID	To reset HDDs in RAID volume, and to restore them to non-RAID status.
Mask Disk as Spare	To mask the HDDs as spare disks. The data will be cleared, and these HDDs can not be selected during RAID setting. It can be restored through the Reset Disks to Non-RAID menu.
Exit	To exit SATA Host RAID configuration interface.

2.2 Create RAID Volume menu. After entering SATA RAID configuration interface, you could use up and down arrow keys to select this menu, and then press Enter to enter the Create RAID Volume menu, or directly input the number before the menu to enter the Create RAID Volume menu. For other menu operations that are similar, it will not be repeated here.

A Create RAID Volume instance is shown in the following figure:

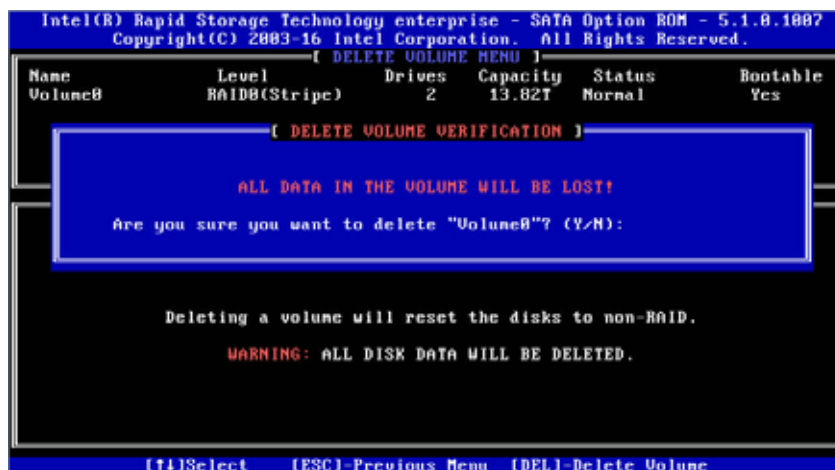


Create RAID Menu Instruction Table

Interface Parameters	Function Description
Name	Please enter a volume label name less than 16 characters without containing any special characters.
RAID Level	Please select RAID volume level. If no volume has been created at present, there are four volume levels of RAID0 (Stripe), RAID1 (Mirror), RAID10 (RAID0+1) and RAID5 (Parity) for selection. Please select volume level according to actual requirements. RAID0: This RAID volume is allowed to be made on 2 or above HDDs. RAID1: This RAID volume is allowed to be made on 2 HDDs. RAID10: This RAID volume is allowed to be made on 4 HDDs, which is only available when HDD quantity is 4 or above. RAID5 (Parity): This RAID volume is allowed to be made on 3 or above HDDs.
Select Disks	Select HDDs to make RAID volume, press Enter, select X, and then press Enter to return to Create RAID Volume interface.
Strip Size	Please select the strip size, only RAID0 and RAID5 volumes could enable this option.
Capacity	Set the volume capacity.

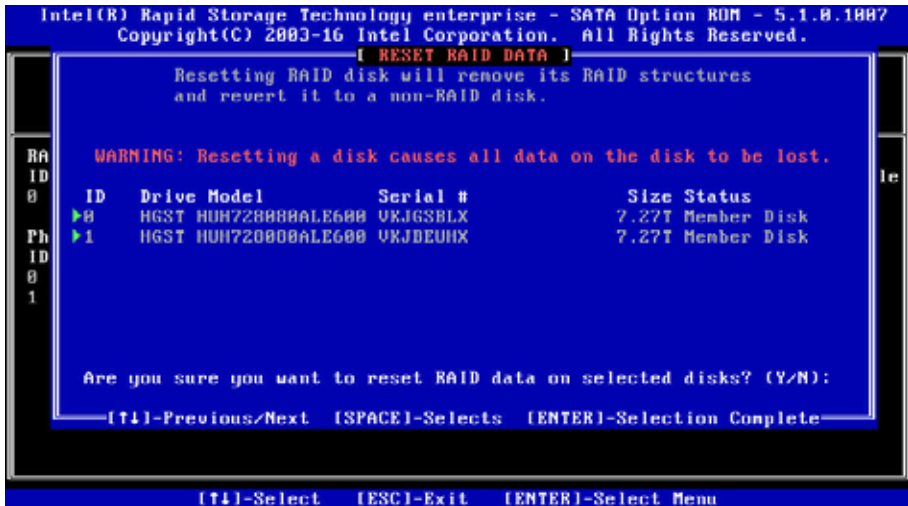
After completing the above settings, please select [Create Volume], and press Enter. The system will prompt “WARNING: ALL DATA ON THE SELECTED DISKS WILL BE LOST. Are you sure you want to create this volume? (Y/N)”. To create an RAID volume, please enter “Y”. A volume will be created, and all data on the selected disks will be lost. Otherwise, please enter “N”, to exit volume creation. Here we enter “Y” to create an RAID volume. After the creation is completed, return to MAIN MENU interface, the created RAID volume will be displayed.

2.3 Delete RAID Volume menu. After entering Delete RAID Volume menu, press [DEL] to delete the selected RAID volume, and the system will prompt “ALL DATA IN THE VOLUME WILL BE LOST! Are you sure you want to delete “Volume0*”? (Y/N)”. To delete this RAID volume, please enter “Y”, to cancel the deletion, please enter “N”.

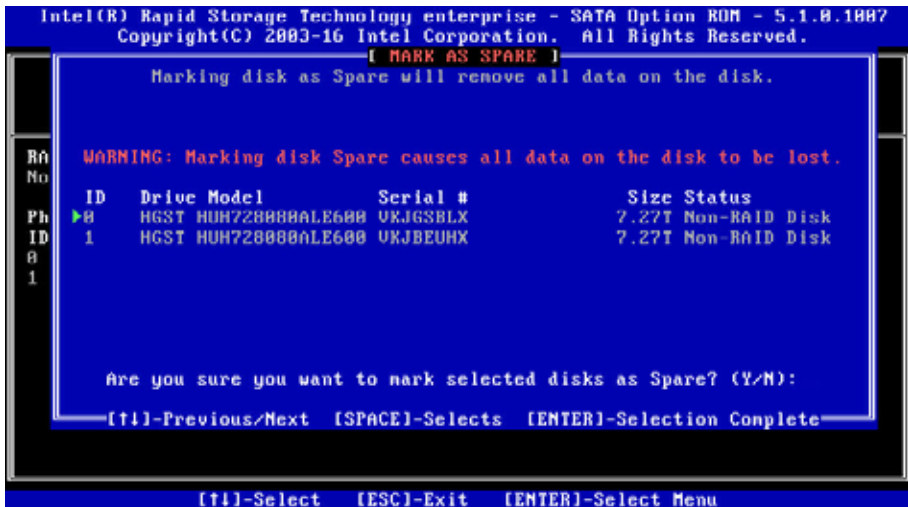


2.4 Reset Disks to Non-RAID menu. After entering Reset Disks to Non-RAID menu, system will display all HDDs in RAID volume. Please use the space key to select the HDD to reset

according to the actual demand, and then press Enter to reset the HDD. The system will prompt “Are you sure you want to reset RAID data on selected disks? (Y/N)” again, enter “Y” or “N” according to the prompt. It is to be noted that all data on this disk will be lost after reset. Meanwhile, this disk will not belong to RAID volume any more.

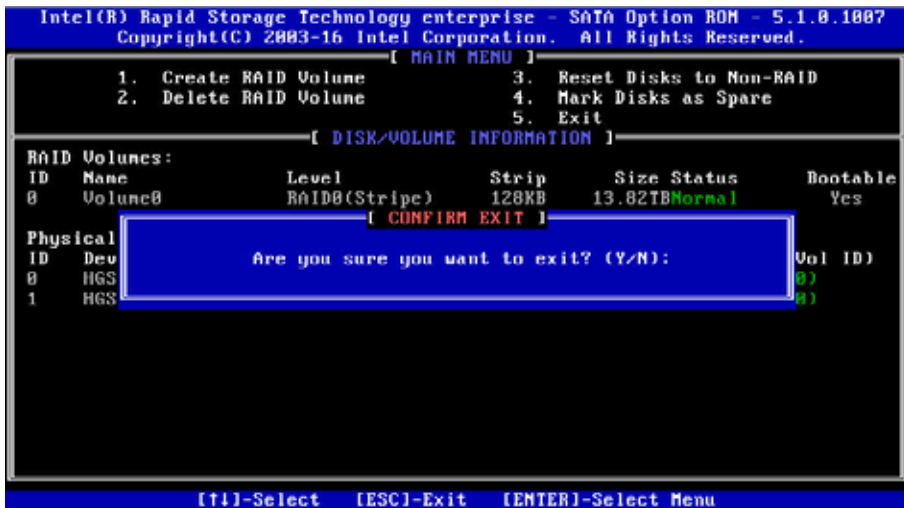


2.5 Mask Disk as Spare menu. After entering Mask Disk as Spare menu, system will display the HDDs not in RAID volume. Please use the space key to select the HDDs according to the actual demand, and then press Enter. The system will prompt “Are you sure you want to mask selected disks as Spare? (Y/N)”, enter “Y” or “N” according to the prompt. It is to be noted that all data on this disk will be lost as the spare disk.



2.6 Exit menu. Select Exit menu through up and down keys, or press ESC to exit SATA RAID configuration interface, as shown in the following figure. The system will prompt “Are you

sure you want to exit? (Y/N)", enter "Y" to exit, or enter "N" to cancel the exit operation.

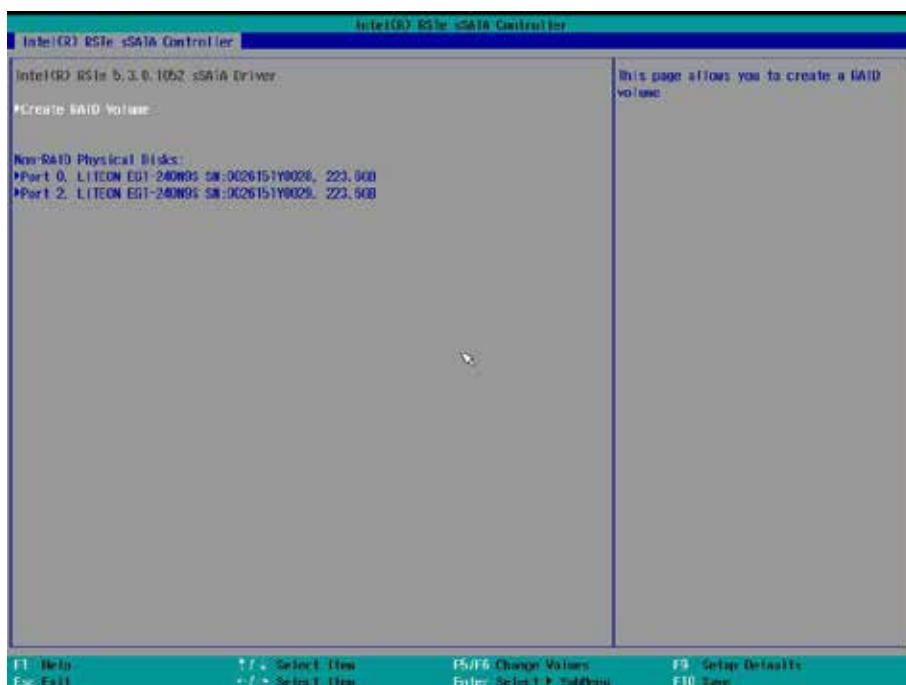


3. Take sSATA RAID configuration in Legacy Mode as an example to introduce the sSATA RAID configuration. When the logo appears during system startup, press ESC to enter the Front Page interface, enter the Device Management configuration interface, and select Intel RSTe sSATA Controller to configure RAID.

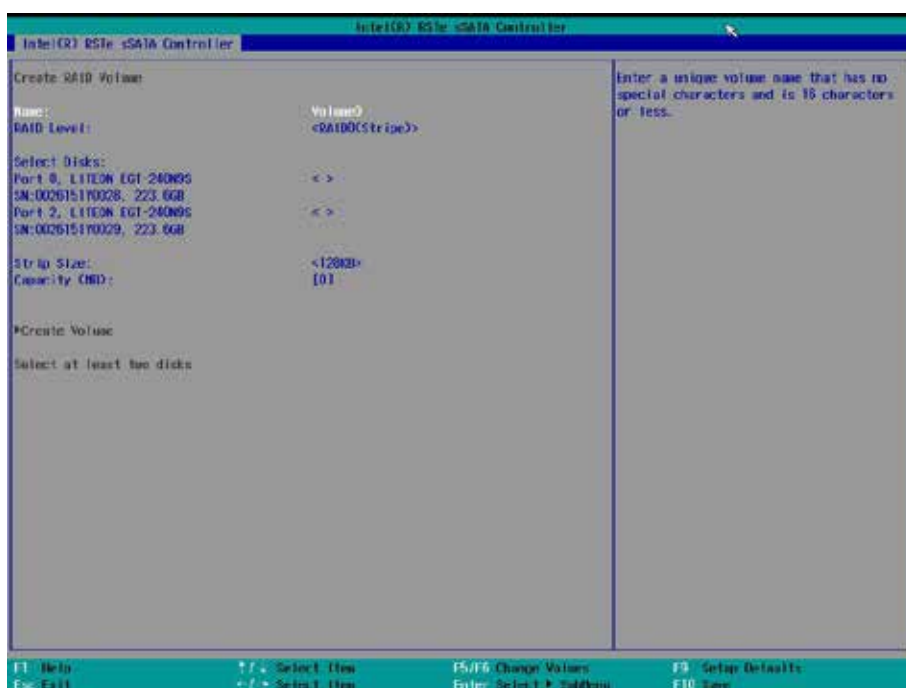


3.1 After entering sSATA RAID configuration interface, it will display the Create RAID Volume option, the existed RAID volumes (if present) information and non-RAID physical disks

information.



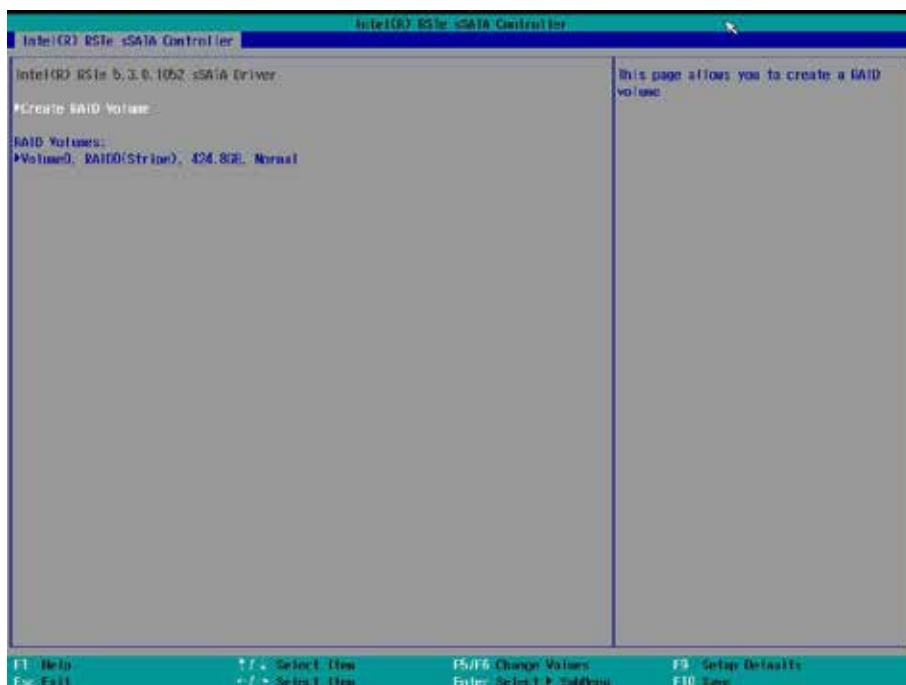
3.2 Create RAID Volume. Enter this menu interface, as shown below.



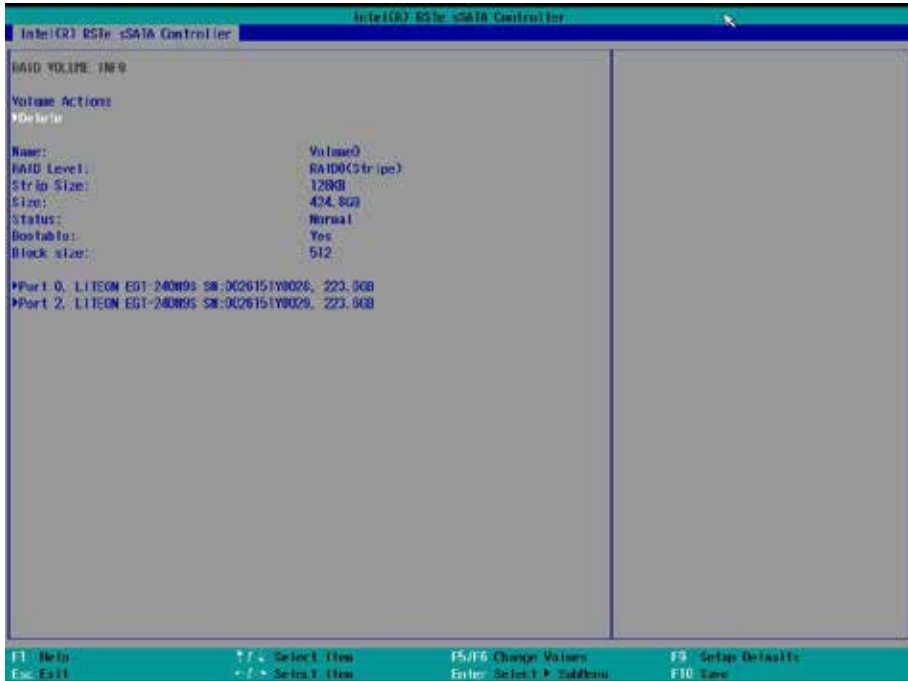
Create RAID Menu Instruction Table

Interface Parameters	Function Description
Name	Please enter a volume label name less than 16 characters without containing any special characters.
RAID Level	Please select RAID volume level. If no volume has been created at present, there are four volume levels of RAID0 (Stripe), RAID1 (Mirror), RAID10 (RAID0+1) and RAID5 (Parity) for selection. Please select volume level according to actual requirements. RAID0: This RAID volume is allowed to be made on 2 or above HDDs. RAID1: This RAID volume is allowed to be made on 2 HDDs. RAID10: This RAID volume is allowed to be made on 4 HDDs, which is only available when HDD quantity is 4 or above. RAID5 (Parity): This RAID volume is allowed to be made on 3 or above HDDs.
Select Disks	Select HDDs to make RAID volume, press Enter, select X, and then press Enter to return to Create RAID Volume interface.
Strip Size	Please select the strip size, only RAID0 and RAID5 volumes could enable this option.
Capacity	Set the volume capacity.

After completing the above settings, please select [Create Volume], and press Enter. After the creation is completed, it will return to RAID configuration interface, the created RAID volume will be displayed.

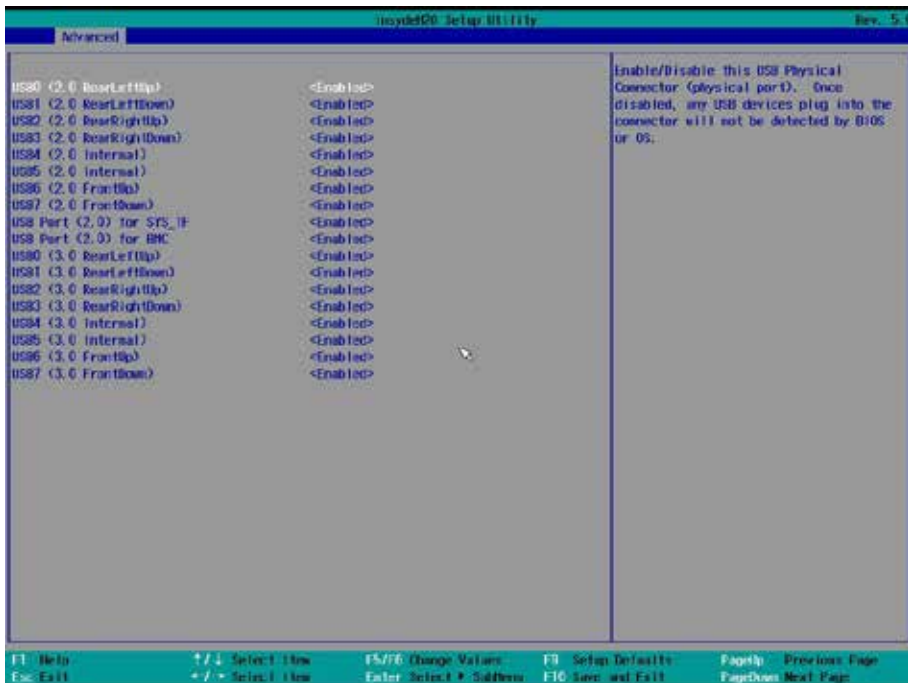


3.3 Delete RAID Volume. Select a created RAID volume, and press Enter to view the RAID volume information. If you want to delete the RAID volume, select Delete, and press Enter to confirm it.



8.2.3.6.4 USB Configuration

USB Configuration interface is used to set USB related options, as shown in the following figure and table.

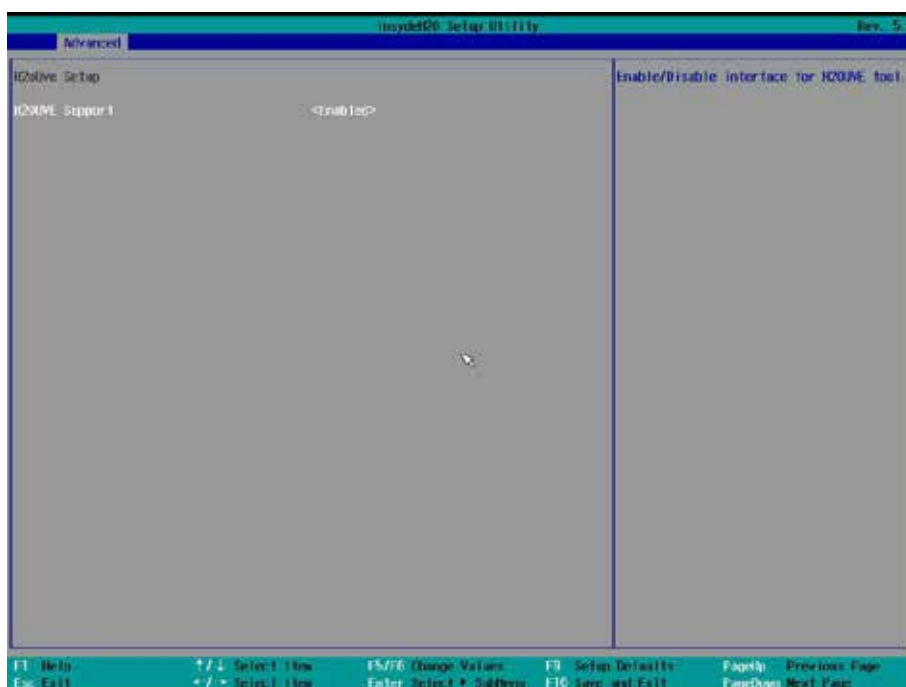


USB Configuration Interface Instruction Table

Interface Parameters	Function Description	Default value
USB0 (2.0 RearLeftUp)	USB0 (2.0 RearLeftUp) setting	Enabled
USB1 (2.0 RearLeftDown)	USB1 (2.0 RearLeftDown) setting	Enabled
USB2 (2.0 RearRightUp)	USB2 (2.0 RearRightUp) setting	Enabled
USB3 (2.0 RearRightDown)	USB3 (2.0 RearRightDown) setting	Enabled
USB4 (2.0 Internal)	USB4 (2.0 Internal) setting	Enabled
USB5 (2.0 Internal)	USB5 (2.0 Internal) setting	Enabled
USB6 (2.0 FrontUp)	USB6 (2.0 FrontUp) setting	Enabled
USB7 (2.0 FrontDown)	USB7 (2.0 FrontDown) setting	Enabled
USB Port (2.0) for SYS_TF	USB Port (2.0) for SYS_TF setting	Enabled
USB Port (2.0) for BMC	USB Port (2.0) for BMC setting	Enabled
USB0 (3.0 RearLeftUp)	USB0 (3.0 RearLeftUp) setting	Enabled
USB1 (3.0 RearLeftDown)	USB1 (3.0 RearLeftDown) setting	Enabled
USB2 (3.0 RearRightUp)	USB2 (3.0 RearRightUp) setting	Enabled
USB3 (3.0 RearRightDown)	USB3 (3.0 RearRightDown) setting	Enabled
USB4 (3.0 Internal)	USB4 (3.0 Internal) setting	Enabled
USB5 (3.0 Internal)	USB5 (3.0 Internal) setting	Enabled
USB6 (3.0 FrontUp)	USB6 (3.0 FrontUp) setting	Enabled
USB7 (3.0 FrontDown)	USB7 (3.0 FrontDown) setting	Enabled

8.2.3.6.5 H2oUve Configuration

H2oUve Configuration interface is used to set the H2OUVE support option, as shown in the following figure and table.



H2oUve Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
H2OUVE Support	Enable/disable H2OUVE support	Enabled

8.2.3.6.6 IPMI Configuration

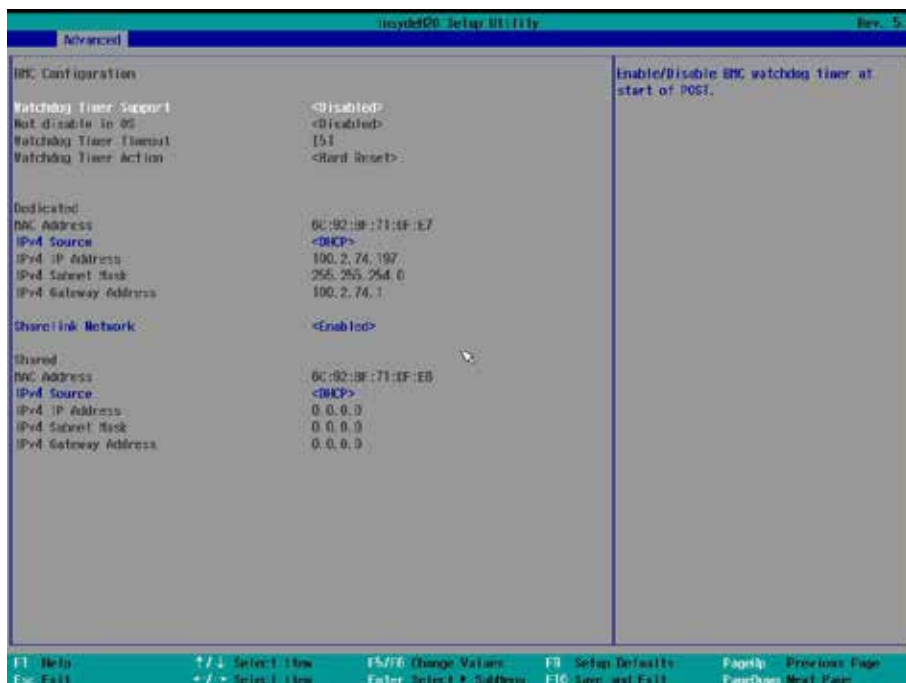
IPMI Configuration interface is used to set IPMI related options, as shown in the following figure and table.



IPMI Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
IPMI Support	IPMI support switch setting	Enabled
System Interface Type	System interface type of connecting BMC display	--
BMC Status	Current BMC status display	--
BMC Firmware Version	BMC firmware version	--
IPMI Specification Version	IPMI specification version	--
BMC Warmup Time	A maximum waiting time period from POST to BMC ready	30
Boot Option Support	IPMI boot optional function setting	Disabled
BMC Configuration	BMC Configuration setting submenu	--

Select BMC Configuration to enter the BMC configuration interface, as shown in the following figure.



BMC Configuration Menu Interface Instruction Table

Interface Parameters	Function Description	Default Value
Watchdog Timer Support	Enable or disable BMC watchdog timer at start of POST	Disabled
Not disable in OS	Enable or disable BMC watchdog timer when boot to OS	Disabled
Watchdog Timer Timeout	Watchdog expiration time setting	5
Watchdog Timer Action	Watchdog timeout action setting	Hard Reset
Dedicated MAC Address	MAC address of dedicated port	--
Dedicated Ipv4 Source	Ipv4 address source of dedicated port setting	--
Dedicated Ipv4 IP Address	Ipv4 IP address of dedicated port setting	--
Dedicated Ipv4 Subnet Mask	Ipv4 subnet mask of dedicated port setting	--
Dedicated Ipv4 Gateway Address	Ipv4 gateway address of dedicated port setting	--
Sharelink Network	Enable or disable sharelink network	Enabled
Shared MAC Address	MAC address of share link port display	--
Shared Ipv4 Source	Ipv4 address source of share link port setting	--
Shared Ipv4 IP Address	Ipv4 IP address of share link port setting	--
Shared Ipv4 Subnet Mask	Ipv4 subnet mask of share link port setting	--
Shared Ipv4 Gateway Address	Ipv4 gateway address of share link port setting	--

(a) BMC dynamic IP setting method:

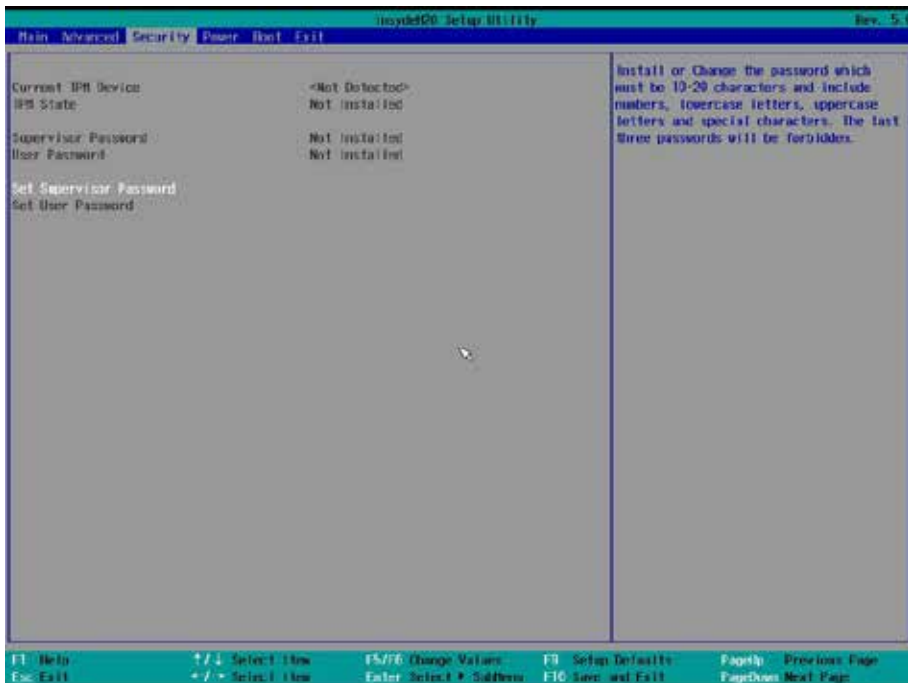
(1) Select Dedicated or Share BMC port.

(2) Modify the IP address acquisition mode of this port to DHCP through IPV4 source.

- (3) Select Exit -> Save Change Without Exit option to save, it takes effect immediately.
- (b) BMC static IP setting method:
 - (1) Select Dedicated or Share BMC port.
 - (2) Modify the IP address acquisition mode of this port to Static through IPV4 source.
 - (3) Select IPV4 IP Address, press Enter, input IP, and press Enter to confirm; then set IPV4 Subnet Mask and IPV4 Gateway Address in the same way.
 - (4) Select Exit -> Save Change Without Exit option to save, it takes effect immediately.

8.2.4 Security

Security interface is used to set the options related with administrative security, including TPM, supervisor and user password settings, as shown in the following figure and table.

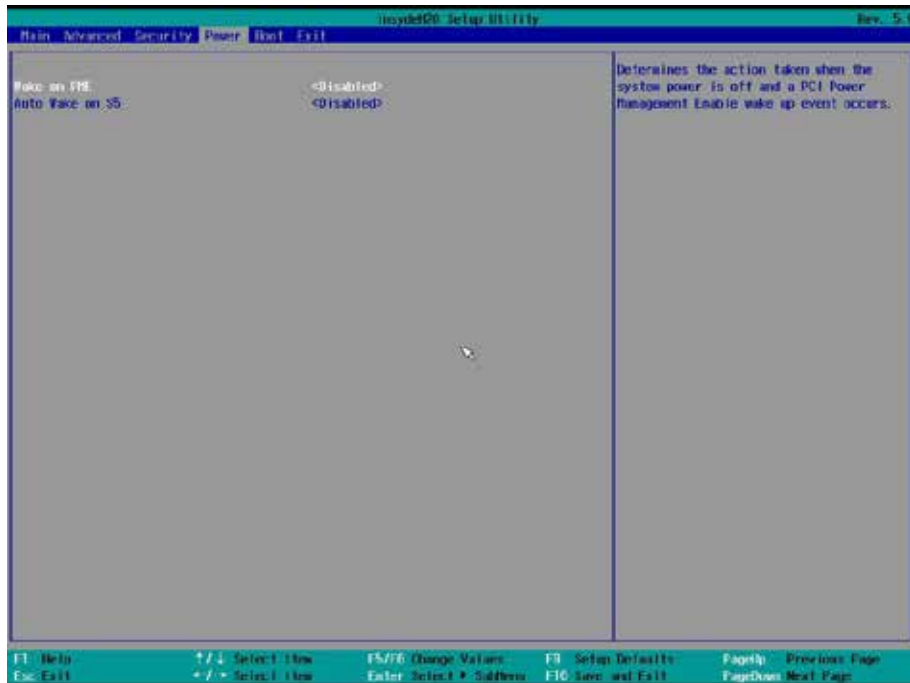


Security Interface Instruction Table

Interface Parameters	Function Description
Current TPM Device	Display current TPM device
TPM State	Display current TPM device status
Supervisor Password	Display supervisor password status
User Password	Display user password status
Set Supervisor Password	Set a supervisor password. The password length should be 10-20 characters, and it must include uppercase letters, lowercase letters, numbers and special characters at the same time.
Set User Password	Set a user password. The password length should be 8 characters, and it must include uppercase letters, lowercase letters, numbers and special characters at the same time.

8.2.5 Power

Power interface is used to set the options related with system power status, as shown in the following figure and table.

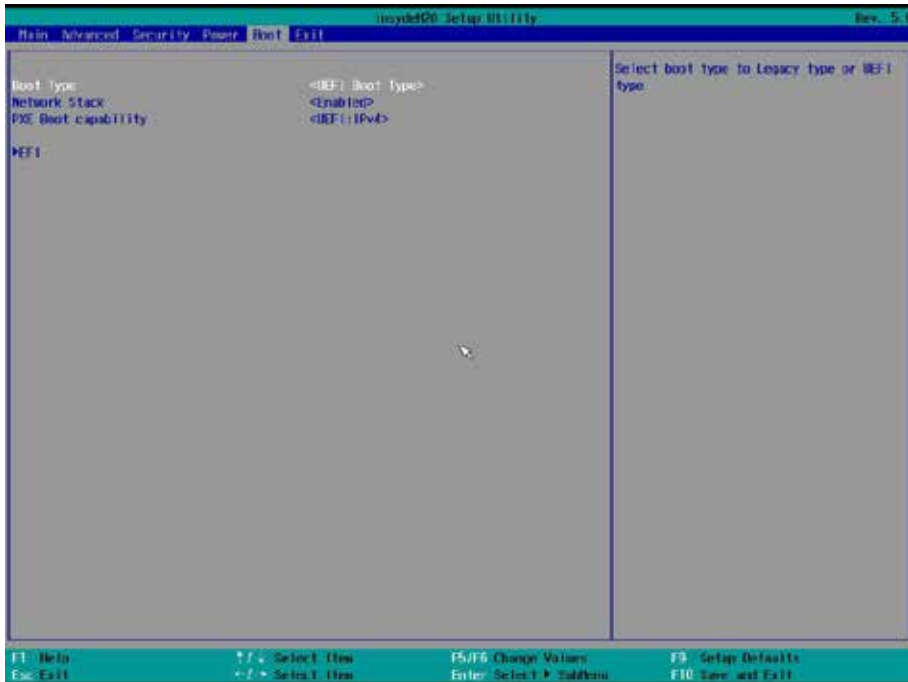


Power Interface Instruction Table

Interface Parameters	Function Description	Default Value
Auto Wake on S5	Auto wake on S5 setting. When set to Enabled, you can set to wake up the machine from S5 state automatically at a certain time.	Disabled

8.2.6 Boot

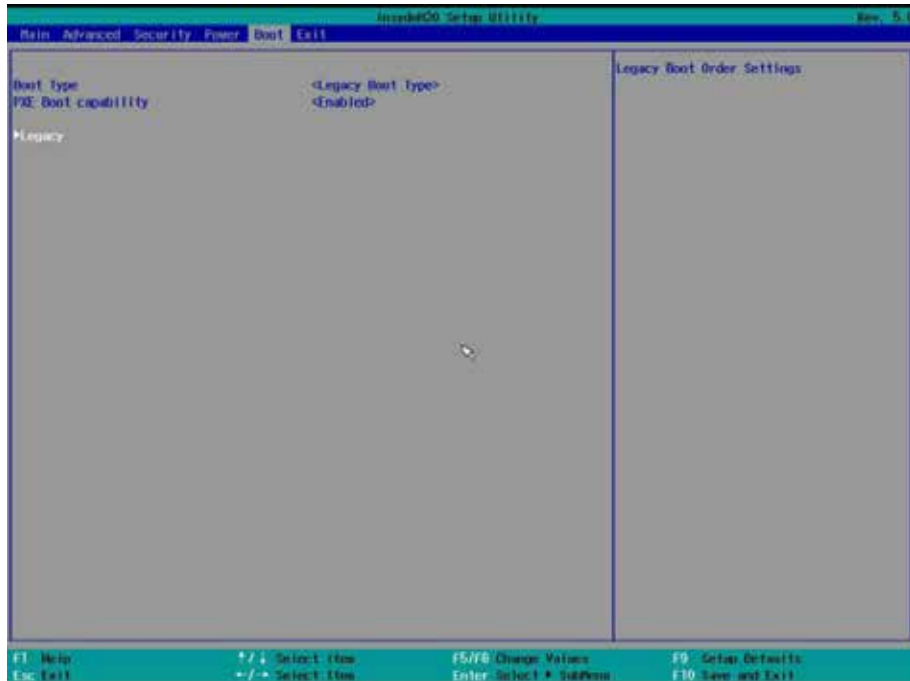
Boot interface is used to set system boot options, including boot type, boot priority, etc. The BIOS boot type defaults to UEFI mode, as shown in the following figure and table.



Boot Interface Instruction Table

Interface Parameters	Function Description	Default Value
Boot Type	Select boot type	UEFI Boot Type
Network Stack	Network stack support setting	Enabled
PXE Boot capability	PXE boot setting	UEFI:IPv4
EFI	EFI boot option setting submenu, the boot priority can be adjusted and set	--

When Boot Type is set to Legacy Boot Type, save the setting and reboot the system. Enter the Boot interface again, you can enter the Legacy Boot Configuration interface, as shown in the following figure.

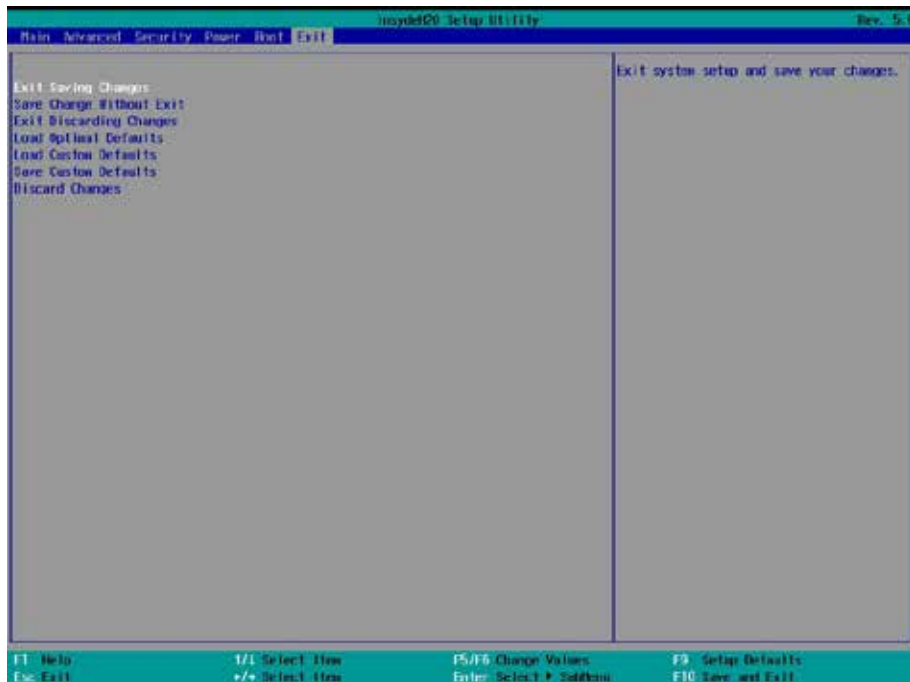


Legacy Boot Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Boot Type	Select boot type	Legacy Boot Type
PXE Boot capability	PXE boot setting	Enabled
Legacy	Legacy boot option setting submenu, the boot priority can be adjusted and set	---

8.2.7 Exit

Exit interface is used to set the options related with save and exit after changing BIOS parameters, as shown in the following figure and table.



Exit Menu Interface Instruction Table

Interface Parameters	Function Description
Exit Saving Changes	To save changes and exit system setup
Save Change Without Exit	To save changes and do not exit system setup
Exit Discarding Changes	To abandon changes and exit system setup
Load Optional Defaults	To load the optional default setting of the system setup
Load Custom Defaults	To load the custom default setting of the system setup
Save Custom Defaults	To save as custom default setting of the system setup
Discard Changes	To abandon changes.

8.3 Firmware Update

For BIOS update, you could select to update in UEFI shell or OS.

8.3.1 Update BIOS in UEFI shell


- 1) When Inspur Logo appears during system startup, there is a prompt “Press <ESC> to Front Page or to Setup or <F11> to Boot Menu or <F12> to PXE Boot.” on the bottom of the screen. Press F11 to start the Boot Menu, and enter EFI shell.
- 2) Enter the disk in which the BIOS flash toolkit H2OFFT-Sx64.efi resides, enter the flash toolkit folder, and BIOS.bin is the 32M BIOS+ME file to be updated. Execute the command H2OFFT-Sx64.efi XXXX.bin -ALL -SSB to flash BIOS+ME, and execute H2OFFT-Sx64.efi XXXX.

bin -ALL -BIOS -SSB to flash BIOS only, as shown in the following figure.

```

UEFI Interactive Shell v2.1
UEFI II
UEFI v2.50 (INSYDE Corp., 0x56510028)
Mapping table
FS0: Alias(s):HD1h0b:;BLK3:
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)/HD(1,MBR,0xCAD4E8EA,0x100,0x1C105214)
BLK0: Alias(s):
    PciRoot(0x0)/Pci(0x11,0x5)/Sata(0x0,0x0,0x0)
BLK1: Alias(s):
    PciRoot(0x0)/Pci(0x11,0x5)/Sata(0x2,0x0,0x0)
BLK2: Alias(s):
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)
BLK4: Alias(s):
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0xB,0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> H2OFFT 5x64.efi BIOS.bin -ALL -SSB_

```

 **Note:** After updating ME+BIOS, please power off the machine, confirm that there is no residual electricity on the motherboard, and then power it on.

8.3.2 Update BIOS in Linux OS

There're 32bit and 64bit Linux OS H2OFFT tools. Here take Linux 64bit OS as an example, using H2OFFTx64.sh tool. Enter the directory containing H2OFFTx64.sh tool, meanwhile, put the bin file of corresponding BIOS into this folder. Execute the command `./H2OFFTx64.sh -ALL -SSB` to flash BIOS+ME, and execute `./H2OFFTx64.sh -ALL -BIOS -SSB` to flash BIOS only, as shown in the following figure.

```

root@localhost:~/inspur/H2OFFT_005_1.0B004_000_00_00_15.00_15
#SGG.kip root@root:~/inspur/H2OFFT_005_1.0B004_000_00_00_15.00_15
root@localhost:~/inspur/H2OFFT_005_1.0B004_000_00_00_15.00_15# cd /mnt
mkdir C:\15\media\01 01 0-514-617-006_01\0111 Previous-Backup-FIT.Linux\inspur\H2OFFT_005_1.0B004_000_00_00_15-drive1 clone
mkdir11: Entering directory ~\mnt\c:\15\media\01\01 0-514-617-006_01\
mkdir11: Loading files\006 ~\mnt\c:\15\media\01\01 0-514-617-006_01\
01 0-514-617-006_01
mkdir C:\15\media\01\01 0-514-617-006_01\0111 Previous-Backup-FIT.Linux\inspur\H2OFFT_005_1.0B004_000_00_00_15-drive1 Clone CPFF111 media
mkdir11: Entering directory ~\mnt\c:\15\media\01\01 0-514-617-006_01\
D:\01\ Previous-Backup-FIT.Linux\inspur\H2OFFT_005_1.0B004_000_00_00_15-drive1\0111
Building media file: stage 2:
Mounting 1 media file:
D:\01\ Previous-Backup-FIT.Linux\inspur\H2OFFT_005_1.0B004_000_00_00_15-drive1\0111\0111
D:\01\01\ Previous-Backup-FIT.Linux\inspur\H2OFFT_005_1.0B004_000_00_00_15-drive1\0111\0111\0111
mkdir11: Loading files\006 ~\mnt\c:\15\media\01\01 0-514-617-006_01\
root@localhost:~/inspur/H2OFFT_005_1.0B004_000_00_00_15
Read file successfully. path: platform.tst
Read file successfully. path: img_img.tst
Warning
Connect get AC Plug info.
Information
Please do not remove the AC power

inspur H2OFFT (F) Jack Firmware Build Version (202) 000-00-00-15
Copyright (c) 2012 - 2020, Inspur Software Corp. All Rights Reserved.

Initializing
Warning
New BIOS version data and New Hall access rights. (NE)
Current BIOS Model name: H20000
New BIOS Model name: H20000S
Current BIOS version: 2.0.00
New BIOS version: 2.0.00

root@localhost:~/inspur/H2OFFT_005_1.0B004_000_00_00_15
1 Updating block of FIT/0000_0701_

```

! Notes:

1. For Linux system, it needs to run the H2OFFT tool as root.
2. After updating ME+BIOS, please power off the machine, confirm that there is no residual electricity on the motherboard, and then power it on.

9 BMC Settings

9.1 Introduction

This Specification describes the functional specifications for the Baseboard Management Controller (BMC). It also describes the feature's detail information.

This document is written for software developers, system integrators, testers, server management users.

9.2 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.

9.2.1 Main Feature

- Support IPMI 2.0, IPMI Interface includes 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

9.2.2 Integrated BMC Hardware

ASPEED AST2500 is the processor of server management subsystem, based on

ARM1176JZF-S 32-bit RISC CPU microcontroller.

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

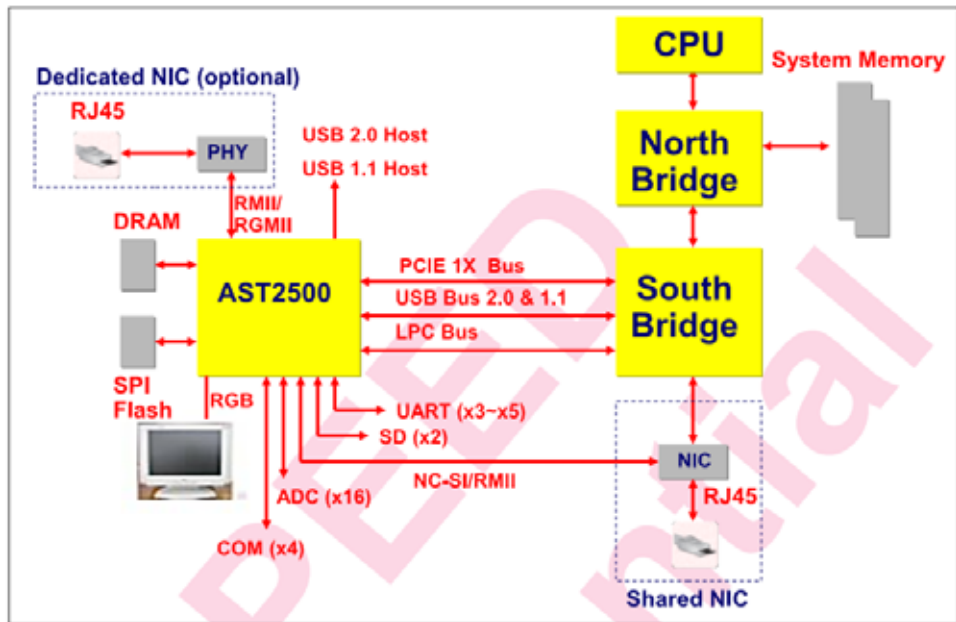


Figure 1 BMC Hardware Architecture

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.

9.3 IPMI2.0

9.3.1 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

9.3.2 System Interface

Support LPC interface, and LPC provides hardware path for KCS messaging.

9.3.3 IPMB Interface

BMC supports Intel NM4.0. Now, Secondary IPMB is used as the communication interface.

9.3.4 LAN Interface

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

BMC supports up to 2 LAN Interfaces (Dedicated NIC and Shared NIC).

List of supported cipher suites in IPMI:

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

9.3.5 IPMI Commands

Tables below define 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 Proxy Address	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)			
Prepare For Discovery	Bridge	10h	NO
Get Addresses	Bridge	11h	NO
Set Discovered	Bridge	12h	NO
Get Chassis Device Id	Bridge	13h	NO
Set Chassis Device Id	Bridge	14h	NO
Bridging Commands (ICMB)			
Bridge Request	Bridge	20h	NO
Bridge Message	Bridge	21h	NO
Event Commands (ICMB)			
Get Event Count	Bridge	30h	NO
Set Event Destination	Bridge	31h	NO
Set Event Reception State	Bridge	32h	NO
Send ICMB Event Message	Bridge	33h	NO
Get Event Destination (optional)	Bridge	34h	NO
Get Event Reception State (optional)	Bridge	35h	NO

9.4 Management Web GUI

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

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

The Web GUI is supported by following browsers:

Table 5 Supported Browsers

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

Step 1

Enter “https: // BMC_IP” in browser address bar. Port number is modifiable (See the “Services” section) and 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.

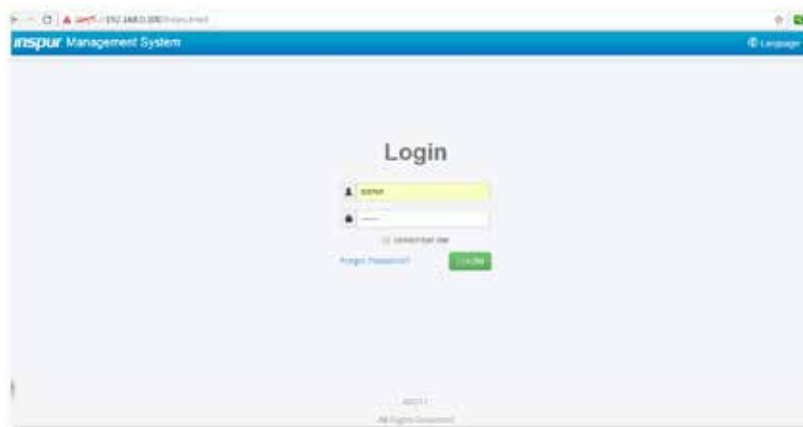


Figure 2 Web Login

When you forget password, you can click “Forgot Password?” link to get a new password by Email. Be sure to configure the Email address in advance in “User Management” page and configure SMTP server information in “SMTP” page.

Main 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
	BOIS 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/output voltage/current/power, firmware version
	Power Supply Configure	YES	Manually Active/Standby switch
	Server Power Control	YES	Power on/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

9.5 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 configure parameters and manage the server through BMC.

- Support SNMP Get/Set/Trap.
- Support V1/V2C/V3 version.
- SNMPv3 supports authentication algorithm MD5 or SHA, and encryption algorithm to DES or AES.
- SNMP Get supports querying system health status, sensor status, hardware status, device asset information, etc.

- SNMP Set supports local users or network users to switch machine and other operations.
- SNMP Trap supports IPM-based Trap messages.

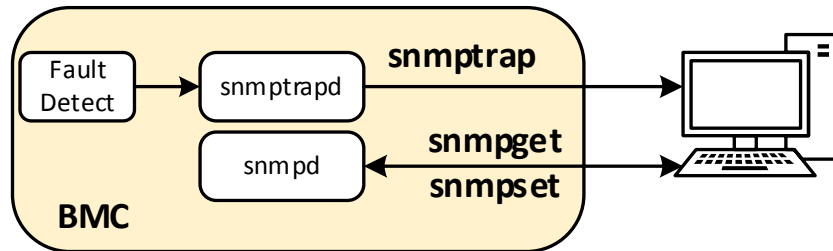


Figure 3 SNMP Schematic

9.6 Smash-Lite CLI

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

- Smash-Lite help:

```

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

/smashcli>
/smashcli>
/smashcli> 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
/smashcli>

```

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 [<xx.x.x.x>] set or get IP address
--netmask [<xx.x.x.x>] set or get IP netmask
--gateway [<xx.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.
gpitool    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

9.7 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.

9.7.1 CPU

Go to table “CPU” in System Information page.

System Information

CPU Memory Device Inventory Network Hard Disk Power Supply Unit FAN Temperature Voltage

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	Normal	3700	20/20	125	1280	20480	28160
CPU1	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	Normal	3700	20/20	125	1280	20480	28160
CPU2	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	Normal	3700	20/20	125	1280	20480	28160
CPU3	Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz	Normal	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., starting from 0.
Processor Name	Product Model
Processor Status	<ul style="list-style-type: none"> ✔ 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

9.7.2 Memory

Go to table “Memory” in System Information page.

No.	Location	Present	Size(GB)	Type	Maximum Frequency(MHz)	Manufacturer	Serial Number	Minimum Voltage(mV)	Rank
0	CPU0_CH0_DIMM0	✔	4	DDR4	2133	Micron	0069F77F	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 starting from 0.
Present	<ul style="list-style-type: none"> ● Present ● Absent or power is off
Size (GB)	Size of memory
Type	DDR3 or DDR4
Maximum Frequency (MHz)	Maximum Frequency
Manufacture	Manufacture
Serial Number	Serial Number
Rank	Rank

9.7.3 Device Inventory

Go to table “Device Inventory” in System Information page.

System Information

System Information											
CPU		Memory	Device Inventory	Network	Hard Disk	Power Supply Unit	FAN	Temperature	Voltage		
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, starting from 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

9.7.4 Network

Go to table “Network” in System Information page.

System Information

System Information											
CPU		Memory	Device Inventory	Network	Hard Disk	Power Supply Unit	FAN	Temperature	Voltage		
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		100.2.45.45							
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

Table 11 System Adapter

Attribute	Value
No.	x, x denotes the device number.
Present	<input checked="" type="radio"/> Present <input type="radio"/> Absent
Location	Location
Port Number	Port Number
MAC Address	MAC Address

9.7.5 Hard Disk

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

The screenshot shows the 'System Information' page with the 'Hard Disk' tab selected. It contains two tables: 'Hard Disk Backplane' and 'Hard Disk'.

System Information								
CPU	Memory	Device Inventory	Network	Hard Disk	Power Supply Unit	FAN	Temperature	Voltage
Hard Disk Backplane								
No.	Present	CPLD Version	Port Number	Harddisk Number	Temperature(°C)			
Front_Backplane_0	<input checked="" type="radio"/>	1.2	12	5	27			
Hard Disk								
No.	Present	Front/Rear	Hard Disk Backplane	Error	Locate	Rebuild	NVME	
3	<input checked="" type="radio"/>	Front	0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO	
4	<input checked="" type="radio"/>	Front	0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO	
5	<input checked="" type="radio"/>	Front	0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO	
6	<input checked="" type="radio"/>	Front	0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO	
7	<input checked="" type="radio"/>	Front	0	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	NO	

Figure 19 Hard Disk Information

Table 12 Hard Disk Backplane

Attribute	Value
No.	x, x denotes the device number.
Present	<input checked="" type="radio"/> Present <input type="radio"/> 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	<input checked="" type="radio"/> Present <input type="radio"/> Absent
Front/Rear	Hard disk location, front or rear
Hard Disk Backplane	Hard Disk Backplane Number
Error	<input checked="" type="radio"/> Normal State <input checked="" type="radio"/> Error State <input type="radio"/> Absent
Locate	<input checked="" type="radio"/> Locating <input type="radio"/> Absent or Non Locate
Rebuild	<input checked="" type="radio"/> Rebuilding <input type="radio"/> Absent or Non Locate
NVME	YES or NO

9.7.6 Power Supply Unit

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

System Information

CPU Memory Device Inventory Network Hard Disk **Power Supply Unit** FAN Temperature Voltage

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)
PSU2	<input type="radio"/>	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	<input type="radio"/>	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	<input checked="" type="radio"/>	NO WARNING	Great Wall	CRPS1600D	2H06C400001	1600	1.000	30	387	359	228	12.23	1.72
PSU3	<input checked="" type="radio"/>	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

Table 15 Power Supplies

Attribute	Value
No.	PSUx, x denotes the power supply number.
Present	<input checked="" type="radio"/> Present <input type="radio"/> 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

9.7.7 FAN

Go to table “FAN” in System Information page.

System Information

CPU Memory Device Inventory Network Hard Disk Power Supply Unit **FAN** Temperature Voltage

No.	Present	Status	Speed(rpm)	Duty Ratio(%)
FAN0_0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN0_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN1_0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN1_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN2_0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN2_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN3_0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4320	20
FAN3_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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	<ul style="list-style-type: none"> ● Present ● Absent
Status	<ul style="list-style-type: none"> ✔ 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

9.7.8 Temperature

Go to table “Temperature” in System Information page.


System Information

System Information									
CPU Memory Device Inventory Network Hard Disk Power Supply Unit FAN Temperature Voltage									
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	<ul style="list-style-type: none"> ✔ 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 means not configured.

9.7.9 Voltage

Go to table “Voltage” in System Information page.


System Information

System Information									
CPU	Memory	Device Inventory	Network	Hard Disk	Power Supply Unit	FAN	Temperature	Voltage	
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	<ul style="list-style-type: none"> ✔ 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 means not configured.

9.7.10 Global Running State





















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



Figure 24 Global Running State

Table 19 System Running State

Device	State Denotation
Current Power Status	<ul style="list-style-type: none"> ● Power On ● Power Off
UID Status	<ul style="list-style-type: none"> ● UID LED On ● UID LED Off
CPU	<p>CPU Healthy state:</p> <ul style="list-style-type: none"> ✓ Normal – All CPU Normal ⚠ Warning State – One or more CPUx_Status warning ✗ Critical State – One or more CPUx_Status critical ● Power Off
Memory	<p>Memory Healthy state:</p> <ul style="list-style-type: none"> ✓ 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	<p>Hard Disk Healthy state:</p> <ul style="list-style-type: none"> ✓ Normal – All Disk Normal. ⚠ Warning State – One or more DISKx_Status warning ✗ Critical State – One or more DISKx_Status critical ● Power Off
Fan	<p>Fan Healthy state:</p> <ul style="list-style-type: none"> ✓ Normal – All Fan Normal. ✗ Critical State – One or more Fan failure ● Power Off
Fan Redundancy	<p>Fan Healthy state:</p> <ul style="list-style-type: none"> ✓ 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

9.7.11 Firmware Version

Page “Firmware Version Information” displays version of firmware residing 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

9.7.12 FRU

FRU stores in EEPROM, BMC will read FRU from EEPROM when BMC boots, 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: **
Asset Tag: *	

9.8 Device State Monitor and Diagnostic

9.8.1 Sensors

9.8.1.1 Physical Sensor

Physical sensors monitor main devices state change. The information gathered from physical sensors is transmitted 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.

9.8.1.2 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.
- Event Log: 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 boots to OS, an assertion event will be logged.

9.8.1.3 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 uses Add SEL Entry (IPMI command) to add event log to SEL.

9.8.1.4 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.

9.8.2 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

9.8.3 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

9.8.4 HDD

Table 24 HDD Health State Monitored

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

9.8.5 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

9.9 Logs

Logs provide the history record of main devices state changes, used for fault diagnostic.

9.9.1 System Event Log

BMC provides the ability to record IPMI sensor based event history. System event log outputs 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 discarded.
- Support cycle mode, default mode. When SEL is full, oldest log will be discarded.
- When SEL is almost full (75%), then Almost full log will be recorded in SEL.
- When SEL is full in linear mode, Full log will be recorded in SEL.
- When SEL is clear, Clear log will be recorded in SEL.
- Support exporting SEL by WEB or IPMI CMD.
- Support informing event to remote client by SNMP Trap, Email Alert, Syslog.

Go to page “Logs -> System Event Log” in Web GUI, all sensor based logs are displayed, users can filter events by event severity, time, or sensor.

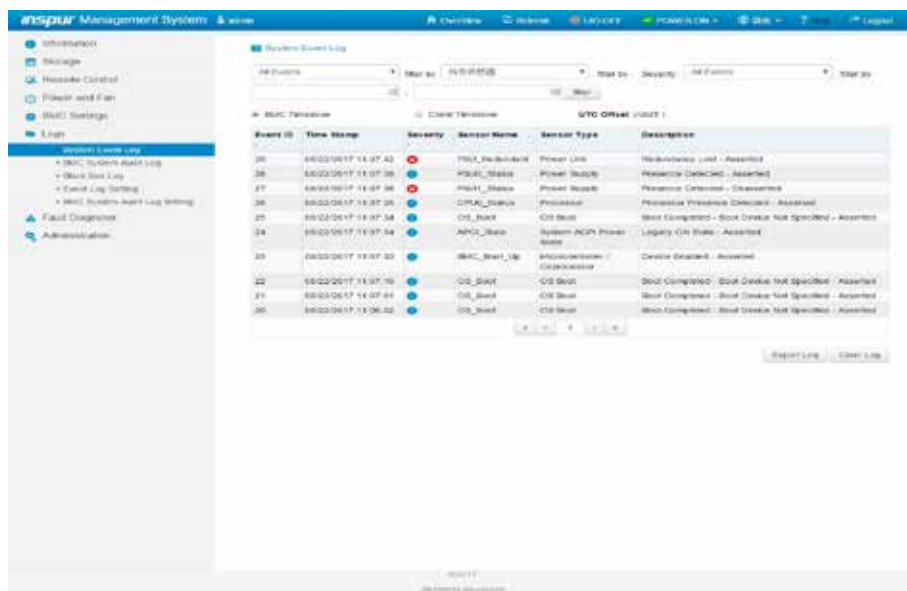


Figure 24 System Event Log

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

9.9.2 Audit Log

BMC provides 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 exporting log by Web.

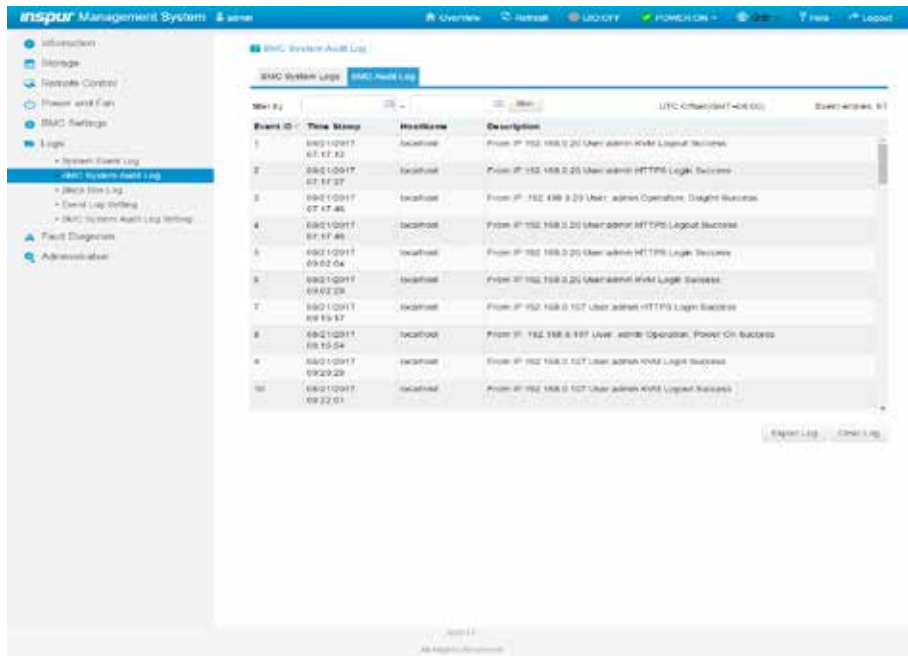


Figure 25 BMC Audit log

Table 27 Audit Log Attributes

Event ID	Event ID
Time Stamp	Event generate time
Host Name	BMC host name
Description	Event details

9.9.3 Blackbox Log

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

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



Figure 26 Blackbox Log

9.9.4 System Serial Log

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

9.10 Event Alerting

BMC supports SNMP Trap and SMTP email alerts.

9.10.1 SNMP Trap Alert

BMC supports SNMP Trap. Users open trap receiver and set trap destination IP in BMC Web GUI. When BMC detects event, BMC will send 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, users can set port in Chapter “Service”.
- Only IPMI sensor based log supports 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 27 Alert Settings

Step 2

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



Event Filter

Sensor Type: All Sensors

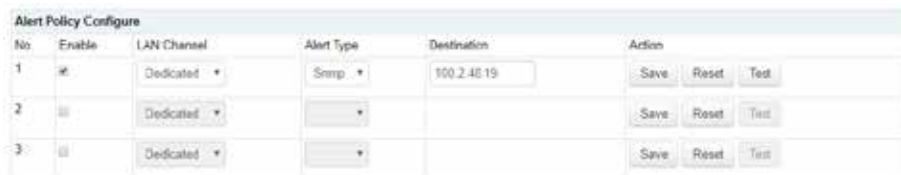
Sensor Name: All Sensors

Save Reset

Figure 28 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 a user configured email.



No.	Enable	LAN Channel	Alert Type	Destination	Action
1	<input checked="" type="checkbox"/>	Dedicated	Smmp	100.2.48.19	Save Reset Test
2	<input type="checkbox"/>	Dedicated			Save Reset Test
3	<input type="checkbox"/>	Dedicated			Save Reset Test

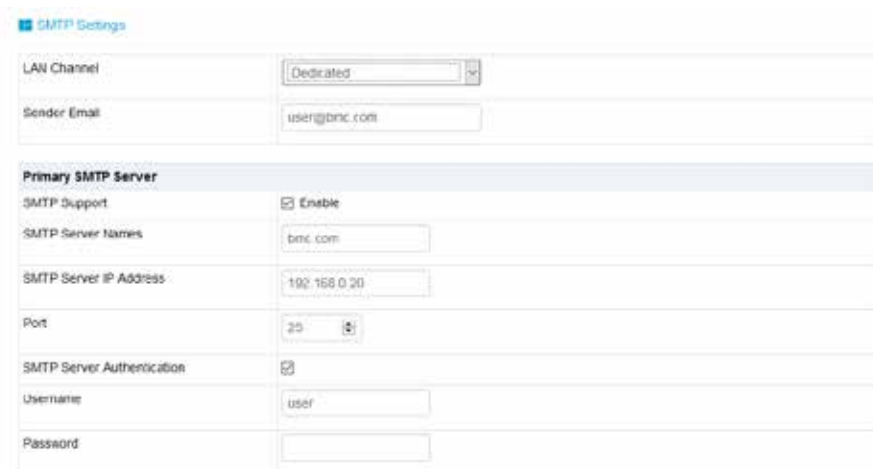
Figure 29 Alert Policy Configure

9.10.2 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. Users should set SMTP server for used LAN channel, if an event occurs, 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 30 SMTP Settings

Step 2

Configure destination email for related user.

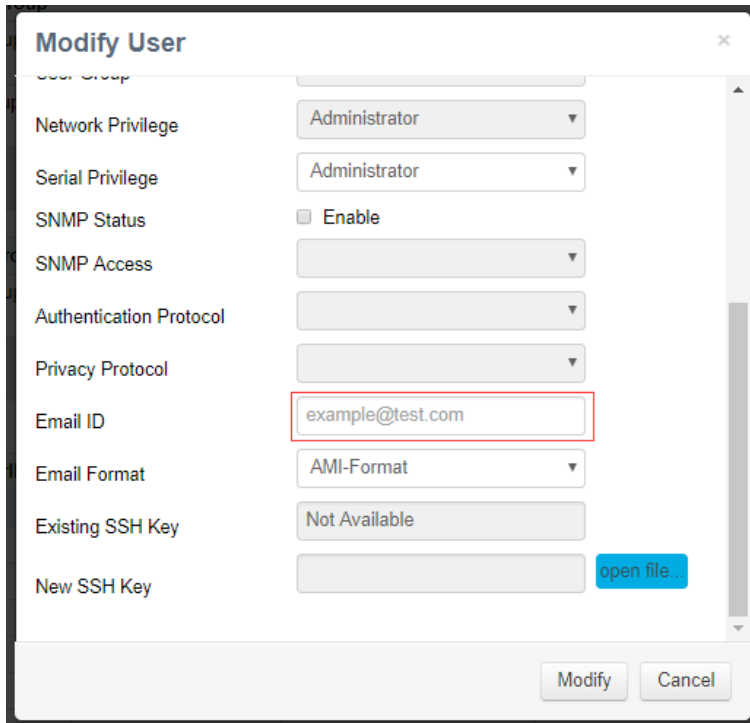


Figure 31 Email Settings

Step 3

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

9.10.3 Syslog

Syslog supports on/off, supports log level filtering, supports 4 receiving targets and every target can configure the receiving server address (IPv4 / IPv6 / FQDN), port number, log type, enable status and send test information. Report log supports 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 imported certificate.

9.11 Diagnostics

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

9.11.1 BIOS Post Code (Port 80h)

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



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 b1 af 00

Figure 32 BIOS Post Code

9.11.2 Screen Capture

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

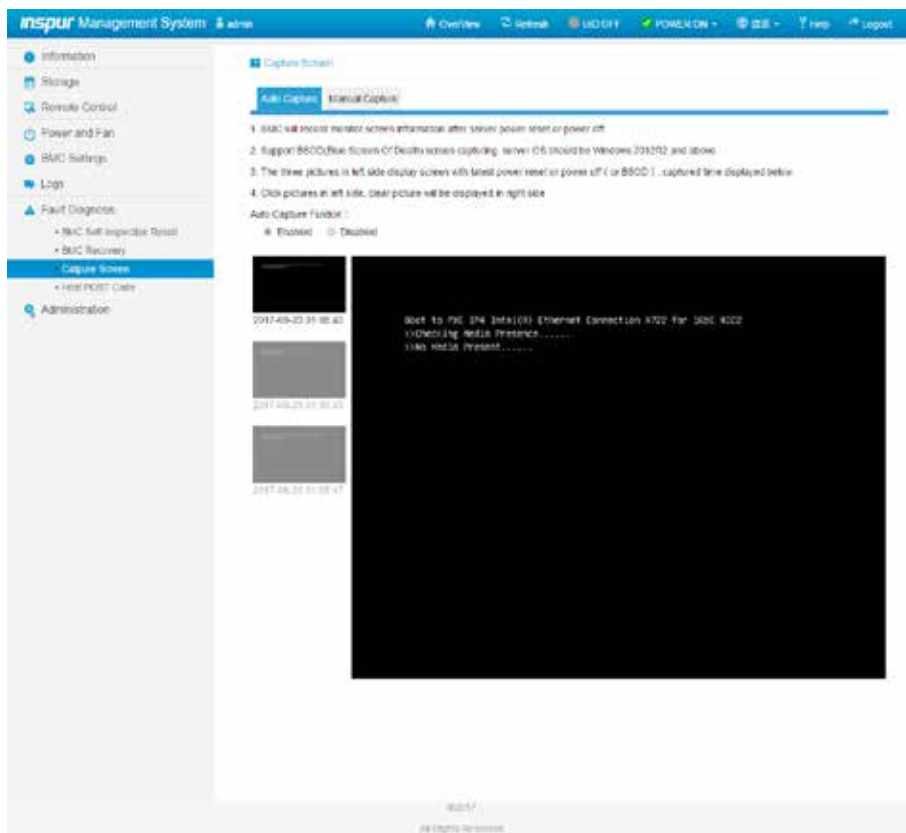


Figure 33 Screen Capture

9.11.3 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 is triggered, the following actions are available.

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

9.11.4 BMC Recovery

Users can reset BMC from WEB or IPMI interface in case of abnormal situation.

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



Figure 34 BMC Recovery

9.12 BMC Self Recovery

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

9.12.1 Hardware Watchdog

Known fault scenarios:

- 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 starts when uboot loads kernel, and the timeout is 5 minutes. If BMC boot timeout occurs, BMC will reset.
- After the BMC system starts, the main process resets the Watchdog every minute. If the

timeout is more than 1 minute, BMC will reset.

- When entering the flash mode, set watchdog time to 20 mins, if timeout BMC will reset automatically. When flashing image starts, the watchdog will update to 20 mins, if timeout BMC will reset automatically.

9.12.2 Software Watchdog

BMC regularly detects the working status of internal services. When the progress is abnormal, BMC will restart the corresponding service:

- IPMI Server
- KVM Server
- Virtual Media Server

9.13 LED

The system provides LEDs to indicate the health of the system.

Table 28 LEDs Indicating the Health of the System

LED name	Color	Status	Description
SYS LED	Red	OFF	1. When system is off, SYS LED is OFF. 2. System works fine, SYS LED is OFF.
SYS LED	Red	ON	The following CPU events occur: 1. CPU IERR 2. CPU Thermal Trip 3. PCIE Error
SYS LED	Red	BLINK	The following warning about CPU appears: Processor Automatically Throttled
Power LED	Yellow	ON	Power plugged in, but not powered 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 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

9.14 BMC Network

9.14.1 LAN Interface

BMC usually supports an LAN controller dedicated to BMC and an LAN controller shared for both BMC and system.

- Maximum bandwidth: Dedicated NIC – 1000M, Shared NIC – 100M.
- BMC network interface compatibly supports IPV4 and IPV6, supports automatic access or IP address manual setting, and MAC address is stored in the EEPROM.
- Support VLAN.
- By 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 supports enable/disable, enabled by default.

9.14.2 BMC Network Bonding

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

- Bonding function is disabled by default, users can enable it in WEB GUI or IPMI CMD.
- Only support Active-backup bonding mode. Default bonding on both NICs (Dedicated and Shared NICs), means network will be working on the NIC plugged with cable. If both NICs plugged with cable before BMC bootup, shared NIC will be primary network to be working. If one NIC plugged with cable before BMC bootup, then another plugged later, the first NIC will be working.
- After bonding, bonding interface uses shared NIC’s MAC to access network, including bonding to dedicated or shared NIC.

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

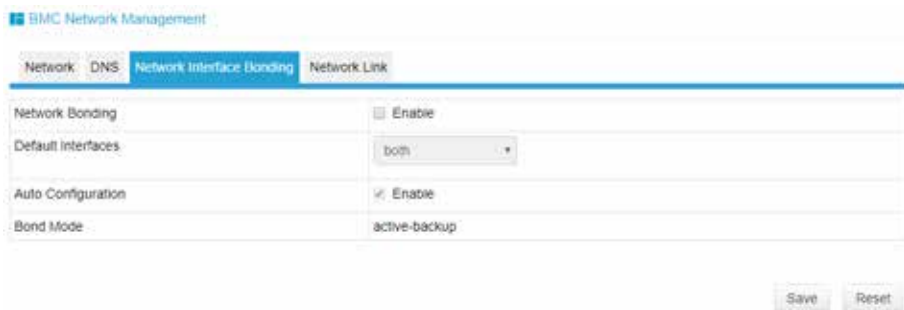


Figure 35 Network Bonding

Network Bonding: Enable/Disable the Network Bonding. If VLAN is enabled, Network Bonding cannot be enabled.

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 services will restart automatically.

Bond Mode: Display the current bond mode. (This field is read-only.)

9.14.3 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 Controllers (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 (support up to 4 NCSI electrical characteristics) network controllers (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.

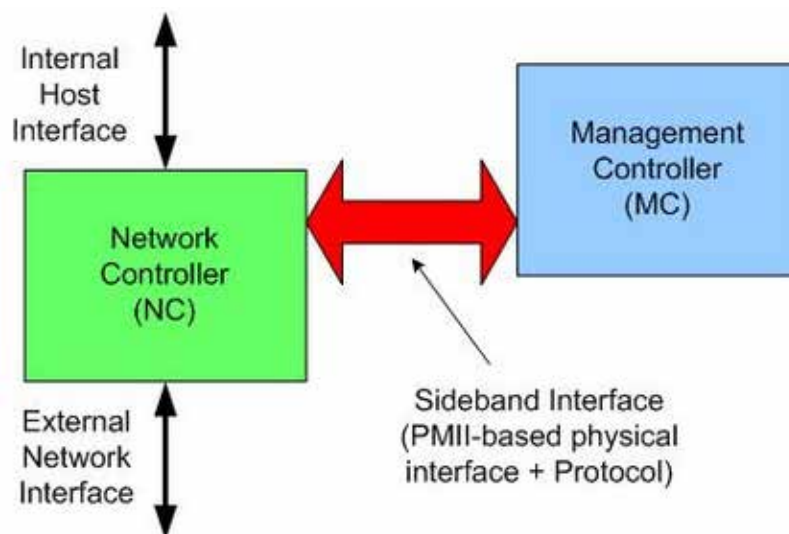


Figure 36 Network Management Module Structure

9.14.3.1 Shared NIC Switch

Normally BMC supports two or more NCSI NICs, and only allows one NIC on NCSI bus. If it

needs to switch NCSI to another NIC, user should set in Web GUI.

Supported NCSI cards on PURLEY platform, include onboard NIC, PHY card, OCP A/B/C card, Inspur designed and NCSI-supported PCIE NIC. Different projects support one or more NCSI cards.

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



Figure 37 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”.

9.14.3.2 NCSI Auto-Failover

Normally, NCSI NIC has two or more ports, and BMC supports Auto-Failover to switch to other port when working port link is disconnected.

Default NCSI mode is Manual Switch to port0.

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

NCSI Mode: Select the supported NCSI mode. 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.

9.15 Users

BMC supports multiple types of users, including IPMI, WEB, BMC OS and SNMP users.

- BMC supports unified user management mechanism to manage IPMI, WEB and BMC

OS users. Users created by IPMI or WEB will have IPMI, WEB and BMC OS user privilege. As BMC OS user, it only has common user privilege, without root user privilege.

- Sysadmin is BMC OS root user, it only has BMC OS root privilege, and cannot access IPMI and WEB.
- SNMP user is used for SNMP Get/Set.

9.15.1 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, including 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 30 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

9.15.1.1 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

- When password complexity check is disabled, password must be 1-16 characters long.
- When password complexity check is enabled, password must include special characters, uppercase and lowercase letters, and numbers, 8-16 characters long.

- Complexity check is disabled by default, 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.
- Disabled by default, we strongly suggest you enable this function for security.
- If enabled, you need change password in expiration time. If password will be expired less than 15 days, when you login Web GUI, Web will alert “Days until password expires: xx”.
- If password expired, you need disable this function in HOST OS by OEM IPMI CMD.
- Password Expiration is 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 reaches Login Fail Retry Count, Web will alert “Input times of wrong password exceeds the limit, user is locked, please retry later!”, and the user will be locked for Lock Time.
- Disabled by default, we strongly suggest you enable this function for security.
- Password Failed Locking is only supported in Web GUI.

Password History Record

- Password History Records: The range is 0 ~ 5.
- Disabled by default. If enabled, you could not set password same to Password History Records (last N passwords).
- Password History Record is only supported in Web GUI.

9.15.2 BMC System Root User

System root user in BMC Linux OS, can be used to access BMC by ssh or telnet.

User name: sysadmin (Fixed, cannot be changed)

Default password: superuser

9.15.2.1 User Security

Username and Password Security

- Username is fixed, cannot be changed.
- Password must be at least 8 characters long.
- Password must include special characters, uppercase/lowercase letters and numbers.

- White space is not allowed.
- No more than 64 characters.

9.15.3 SNMP User

SNMP user is used to support SNMP Get/Set.

- Default read community: cmccread and inspur@0531
- Default write community: cmccwrite
- SNMPV3 supports user authentication, supported authentication algorithm is SHA and MD5;
- SNMPV3 supports 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.

9.15.3.1 User Security

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

9.15.4 User Privilege

9.15.4.1 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 does not need to authenticate user and password, because he will get the highest privilege if someone accesses the HOST OS. So if the user forgets password or password expires, 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 31 User Privilege for IPMI

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

9.15.4.2 User Privilege for Management Web GUI

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

Table 32 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 users 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.

9.15.4.3 User Privilege for Smash-Lite

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	NPO	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

9.16 Protocol and Ports

BMC supports 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. Users can enable or disable these services, configure communication port, session timeout value of the service and the maximum number of allowed sessions for the services.

Table 33 Protocols and Ports

Service	Usage	Default State	Non-Security Port	Security Port	Default Portz	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
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 deleted, and new web request will not respond. If the web page has no auto update, it will be logged out when you switch pages or refresh the page after timeout.

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

Fixed protocols can not be configured.

Table 34 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

9.17 Time and NTP

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

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

Table 35 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+/-0	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 is enabled and NTP servers are accessible, BMC will synchronize time with NTP servers per hour.

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

Figure 38 NTP

9.18 BIOS and BMC

BIOS and BMC cooperate very closely in the server. BIOS uses 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 redirects the System UART to BMC UART to reach SOL feature. For details, please refer to “Serial over LAN” chapter.

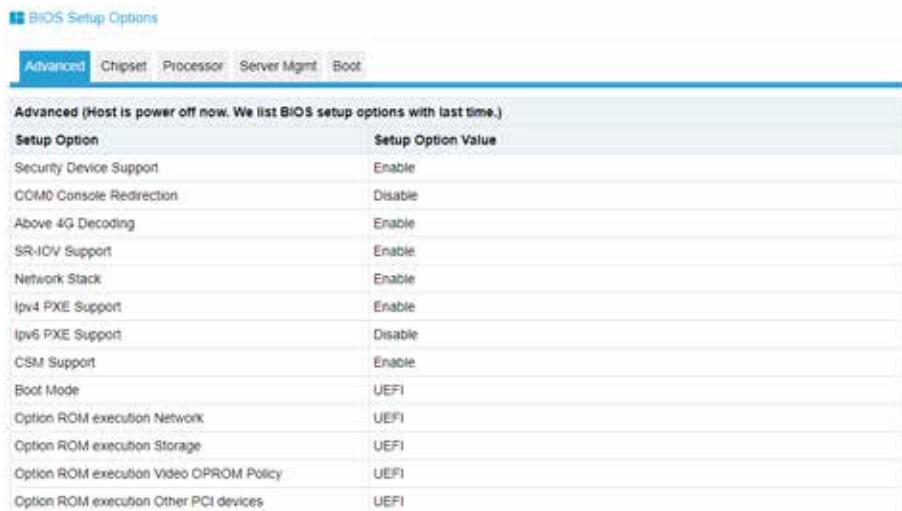
 **Note:** The LPC interface to the host is used for SIO and BMC communication. The LPC addressing of SIO and BMC could be different. For example, the BMC LPC addressing is 0x2E, and the SIO addressing is 0x4E.

9.18.1 BIOS Setup Options

BMC supports BIOS Setup Option getting and setting.

- BIOS sends BIOS Setup Options to BMC When BIOS POST completes.
- Users 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.



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 39 BIOS Setup Options

9.18.2 BIOS Boot Options

BMC supports BIOS startup options, including timeliness and startup options.

- BMC must restart within 60 seconds, otherwise the BIOS startup option action will be invalid.
- Timeliness: Selectable timeliness is only used for the next boot or applies to all boot.
- Startup 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.

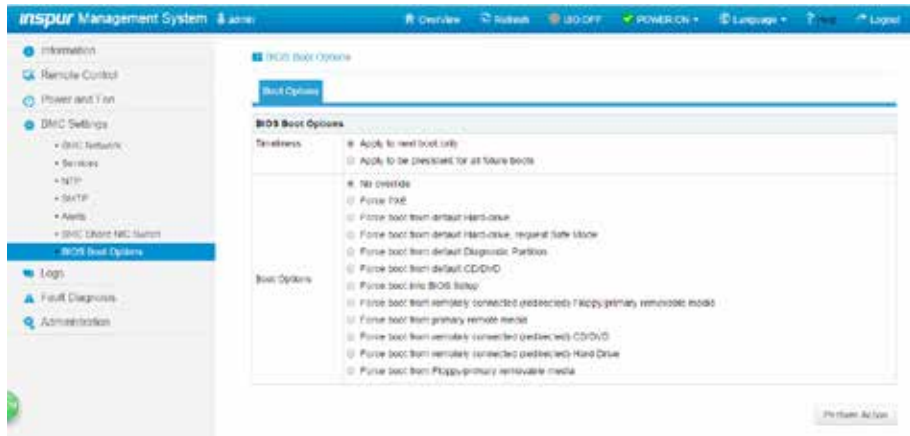


Figure 40 Boot Option

9.19 Storage

Server storage subsystem generally consists of RAID and SAS hard disks. BMC physically interacts with the RAID and SAS controllers through I2C to obtain information such as controllers, disks, and arrays, and to set RAID.

Table 36 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:

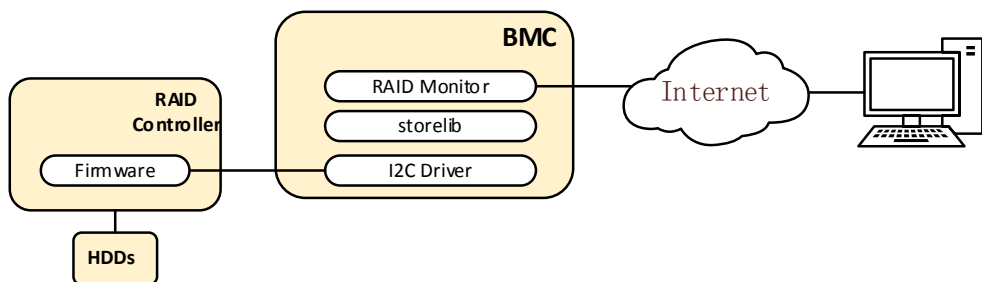


Figure 41 Schematic that BMC Access RAID/SAS Controller

Table 37 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
Array	
Enclosure	Device ID Enclosure is Faulty Slot Count Internal Index Enclosure Type Drive Count

9.20 Server Control

9.20.1 Server Location

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

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

The “Remote Control -> Locate Server” page shows 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 off UID: Click “Turn Off Led” button to turn off UID.



Figure 42 Server Location

9.20.2 Server Virtual Power Button

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

- Power on, same to short time pressing power button.
- Forcedly power off, same to long time pressing power button.
- Power cycle, power off, delay 10s, power on.
- Hard reset, same to short time pressing reset button (if present).
- Soft shutdown, orderly power off, same to short time pressing power button.

Supported:

Web GUI

IPMI command based on IPMI2.0.

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

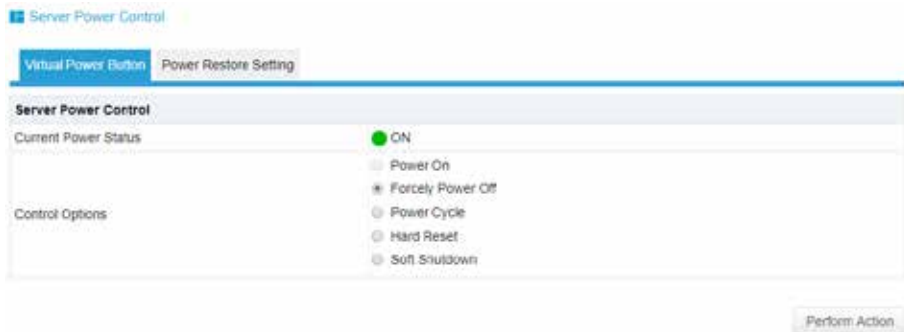


Figure 43 Virtual Power Button

9.21 Power Supply and Power Consumption

9.21.1 Power Supply Redundancy

BMC usually supports PSU Redundancy, which means if one or more PSUs cannot normally output power, server will work normally powered by other power supply.

9.21.2 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 to Activate-Activate mode, and if it need 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 will be powered by the main power system. The power supply is in a hot standby state, once the main power supply is abnormal, standby power will switch to the main power supply smoothly without affecting the service.

Conditions that standby power switches to the main power:

1. Main power supply is 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 reaches the upper limit.



Figure 44 PSU Active Standby

9.21.3 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 can be enabled or disabled. Disabled by default.
- When it is enabled, users can configure the 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.

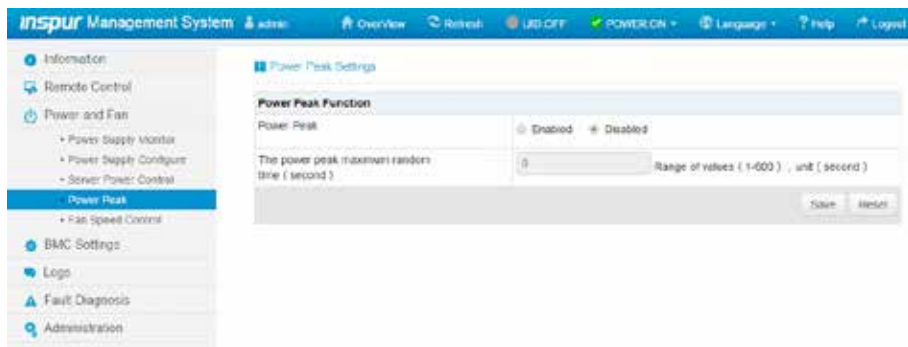


Figure 45 Power Peak

9.21.4 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.



Figure 46 Power Limits

9.21.5 Power Consumption Statistics and History Record

BMC provides curve-based inlet temperature and power monitoring statistics.

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.

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.

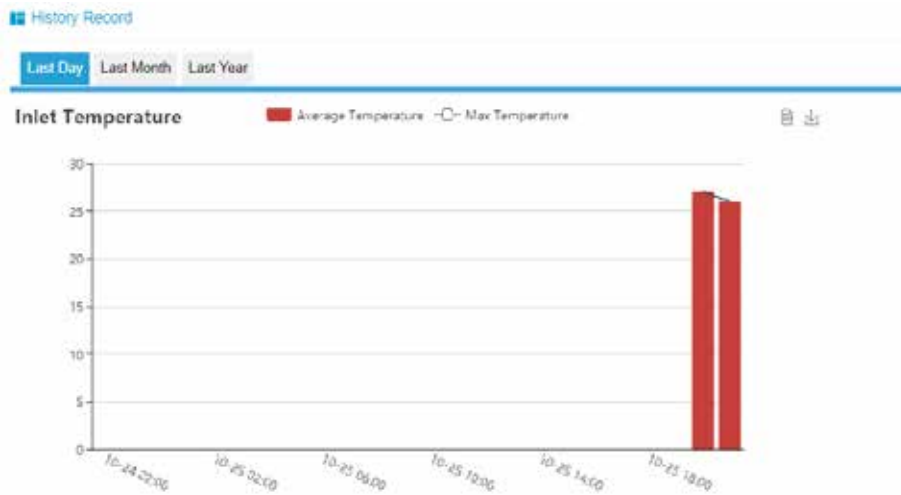


Figure 47 Inlet Temperature History Record

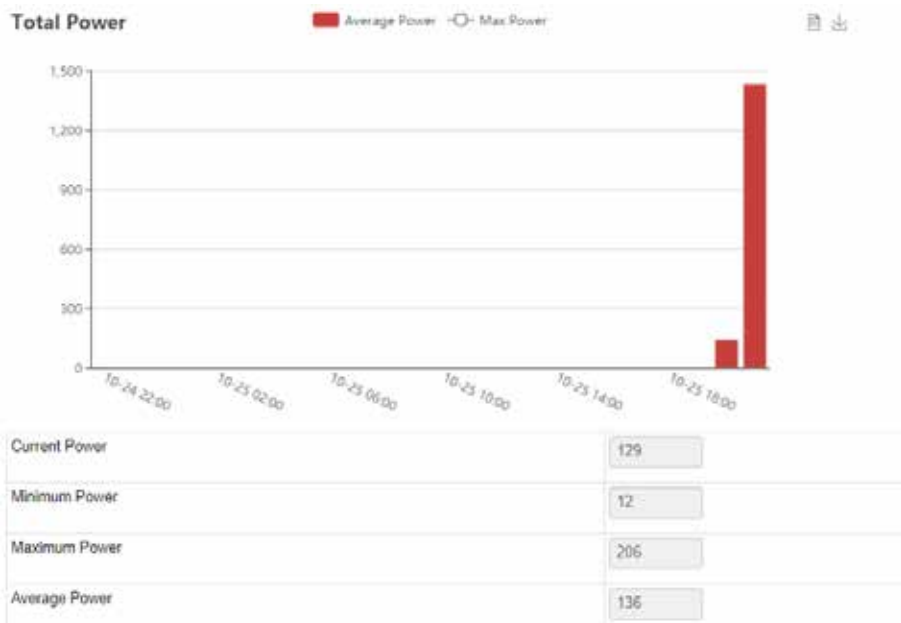


Figure 48 Total Power History Record

9.22 Fan Speed Control (FSC)

9.22.1 Fan Speed Control

BMC supports Auto Fan Control by default, and the fan module speed is controlled by the algorithm provided by thermal team.

Users can enable Manually Fan Control in Web GUI, if enabled, users can select one of four fan speeds predefined for each fan module. These predefined fan speed are Low, Medium, High and Full.

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, users can see the duty ratio of the fan module. In this page, users 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 49 Fan Speed Control

9.22.2 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 overheating.

9.23 Firmware Update

9.23.1 BMC Firmware Update

BMC supports dual BMC firmware image. BMC flash contains two images (BMC flash size is 64M, BMC firmware image size is 32M).

Supported update modes:

- WEB update, users login Web GUI and enter flash page to update firmware. This is a sideband mode, it supports Firmware Integrity Checking and preserving configurations. It is a suggested update mode.
- SOCflash tool update, SOCflash tool is 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, users should accept user permission.

9.23.1.1 Firmware Integrity Checking

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

9.23.1.2 Dual image

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

9.23.1.3 WEB Update


BMC firmware update is supported via the Management Web GUI.

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

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

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

Configurations can be preserved separately. Please refer 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.

It defaults to boot the higher version of the two images. You can change the value from the Web GUI.

Step 1

Go to “Administration->Dual Image Update” page, and select image to update. It defaults

to Both Images, which means both image will be updated. If configuration should be preserved, click “Enter Preserve Configuration” to select items that need to be preserved. Click “Enter Update Mode” to go to update page.

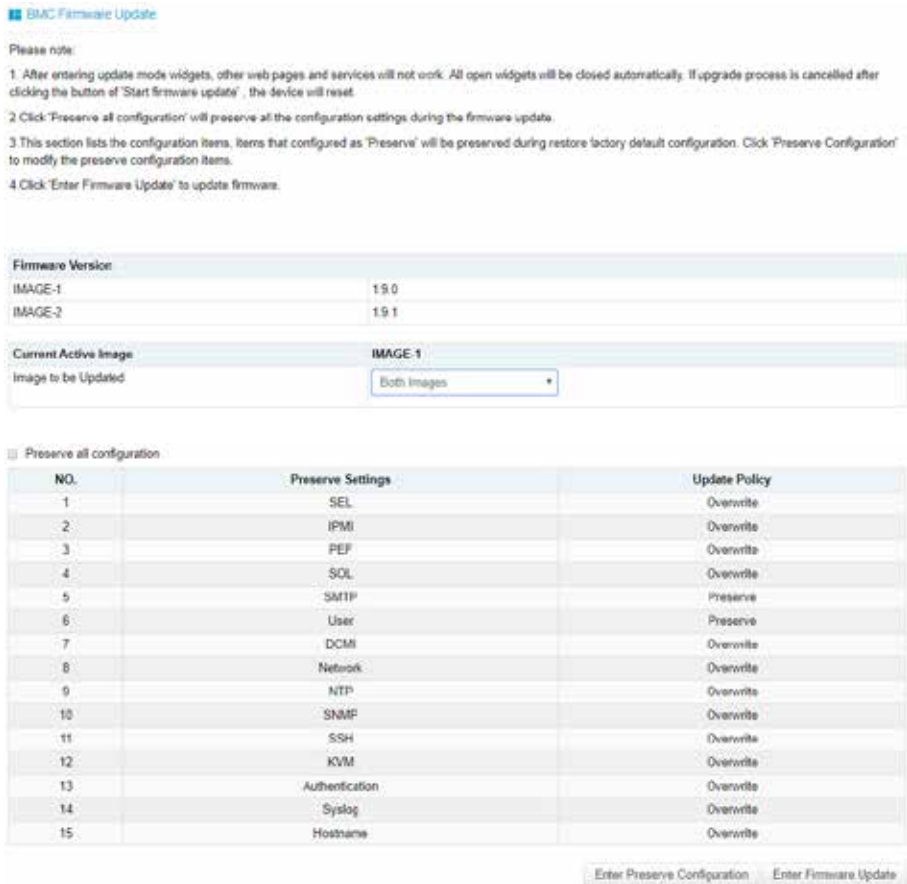


Figure 50 BMC Update Step 1

Step 2

Select image file, click Upload button to upload file, BMC will enter flash mode, 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 the verification fails, BMC will stop flash and restart.



Figure 51 BMC Update Step 2

Step 3

Check image version and current image version, then click “Proceed to Update” button to start update.

Wait for about 15mins (both images), then flash is complete.

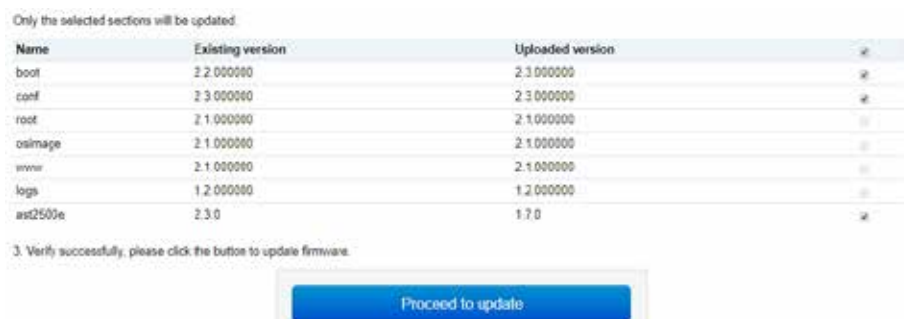


Figure 52 BMC Update Step 3

9.23.1.4 SOC Flash Update

SOCflash tool will directly erase and overwrite flash with new image without Firmware Integrity Checking. All configuration will be erased.

To update BMC in Windows/Linux/DOS, enter DOS or Linux shell or Windows cmd line, execute the following CMDs:

socflash if=Imagefile will update the Image1;

socflash if=Imagefile offset=0x2000000 will update the Image2.

9.23.2 BIOS Firmware Update

BMC supports BIOS Firmware update via the Management Web GUI.

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

- Support two upgrade modes: “BIOS+ME” and “BIOS Only”.
- Power off the system before performing BIOS firmware update.
- After BIOS firmware update, BIOS NVRAM will be cleared, all BIOS configurations will be reset to defaults.
- If we update both BIOS and ME images, in order to make ME firmware take effect, it is suggested to start the server after AC power off.

Step 1

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



Figure 53 BIOS Update Step 1

Step 2

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

Size should be 32M.

Verify image integrity, it will make sure this is BIOS image.

If the verification fails, BMC will stop flash and change ME to normal mode.

If the verification succeeds, click “Proceed to Update” button to start update. Wait for about 3mins, then the flash is complete, and ME will enter the normal mode.



Figure 54 BIOS Update Step 2

9.23.3 CPLD FW update

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

9.24 Restore Factory Default

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

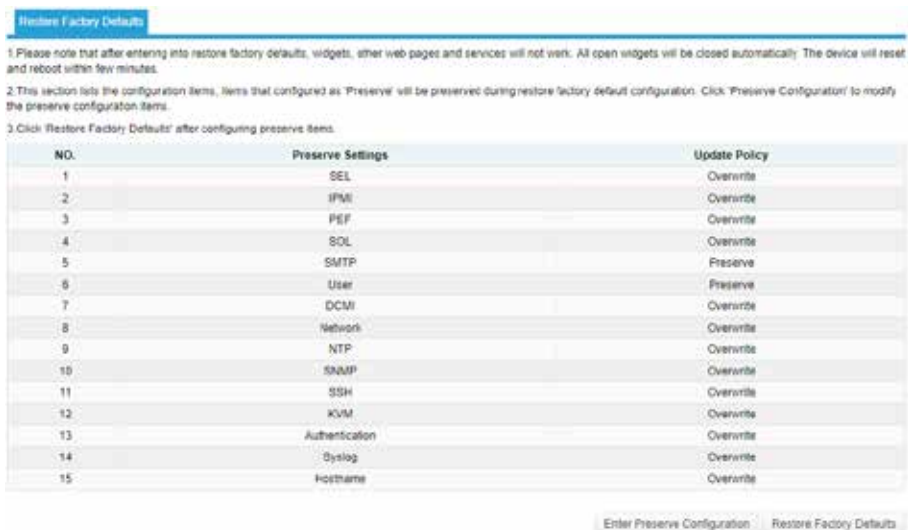


Figure 55 Restore Factory Default

Note: Update policy “Override” means selected items will be overwritten to defaults after clicking “Restore Factory Default” or upgrading BMC; “Preserve” means selected items will be restored after clicking “Restore Factory Default” or upgrading BMC.

Table 38 Restore Factory Default

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

9.25 Serial Over LAN (SOL) and System Serial Log Recording

9.25.1 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), 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 is enabled on COM0 (some projects on COM1) by default, users should configure SOL in BIOS Setup (Serial Port Console Redirection), if needed.

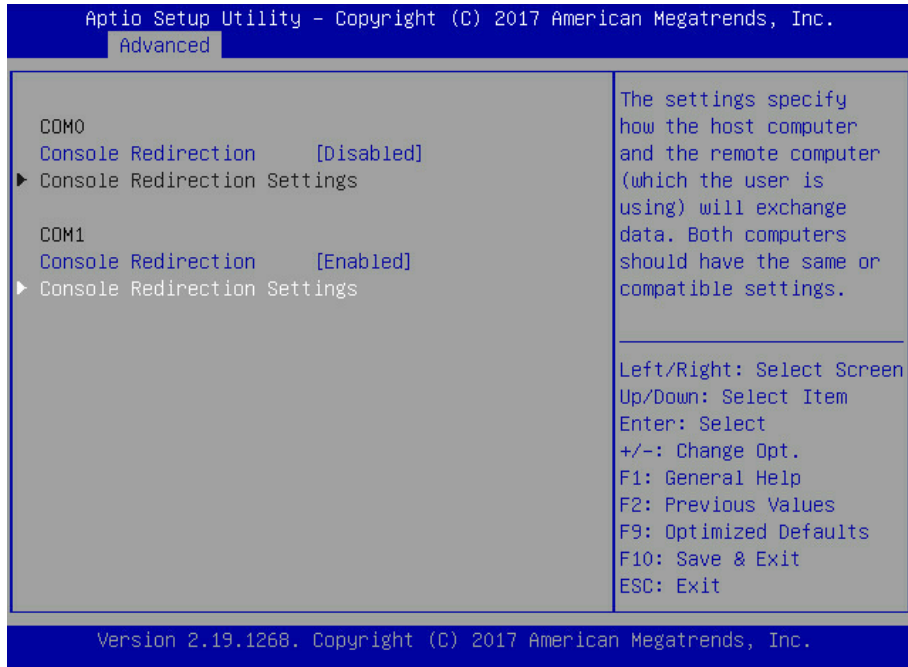


Figure 56 SOL Setting in BIOS

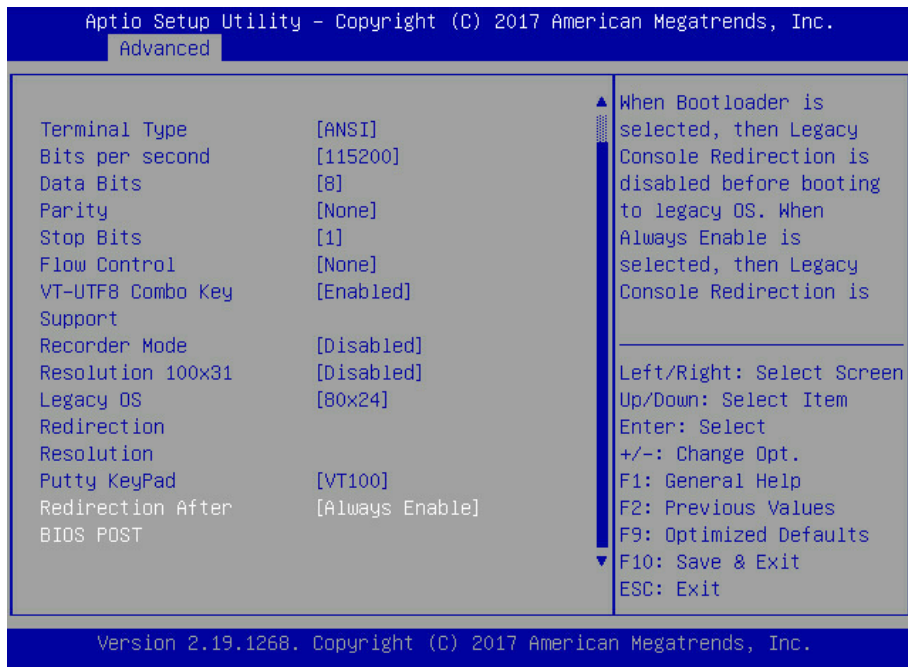


Figure 57 Default Serial Setting

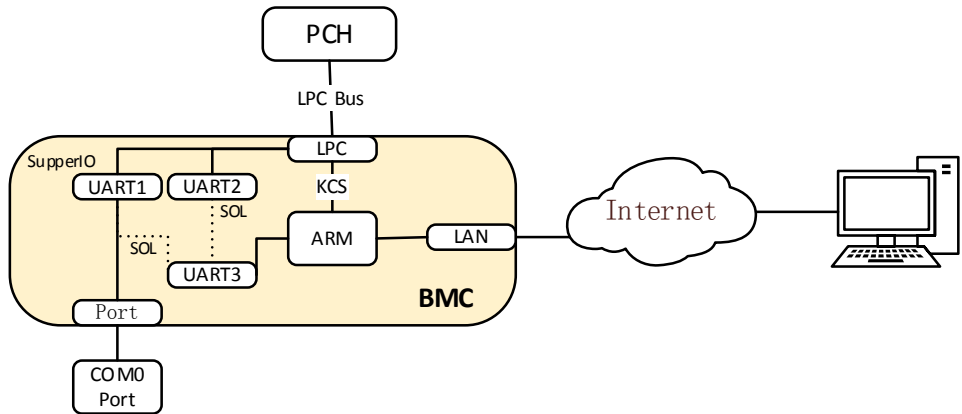


Figure 58 SOL Schematic

9.25.2 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 logs. When more than 2M, log will loop to store, and the old log content will be deleted. When the system crashes or restarts, system serial log can be exported, and fault information can be used for fault diagnosis.

9.26 Console Redirection (KVM)

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

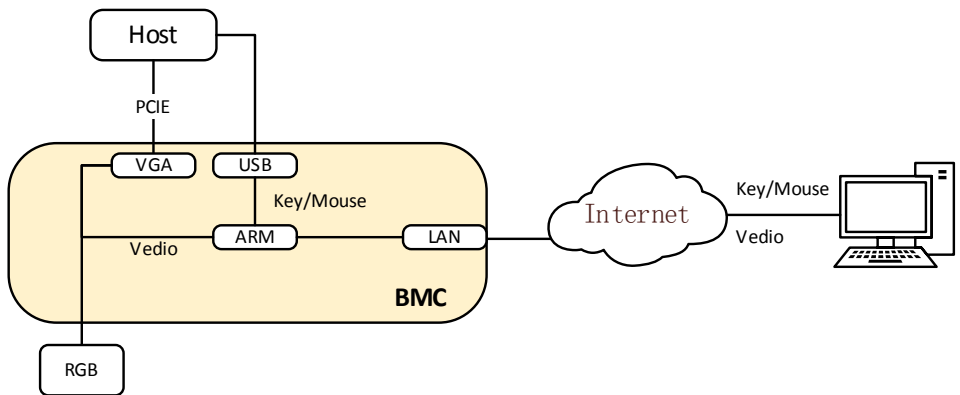


Figure 59 KVM Schematic

9.26.1 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.

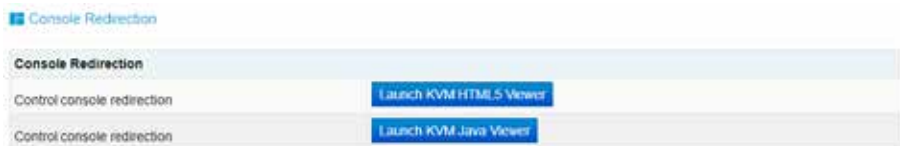


Figure 60 Console Redirection

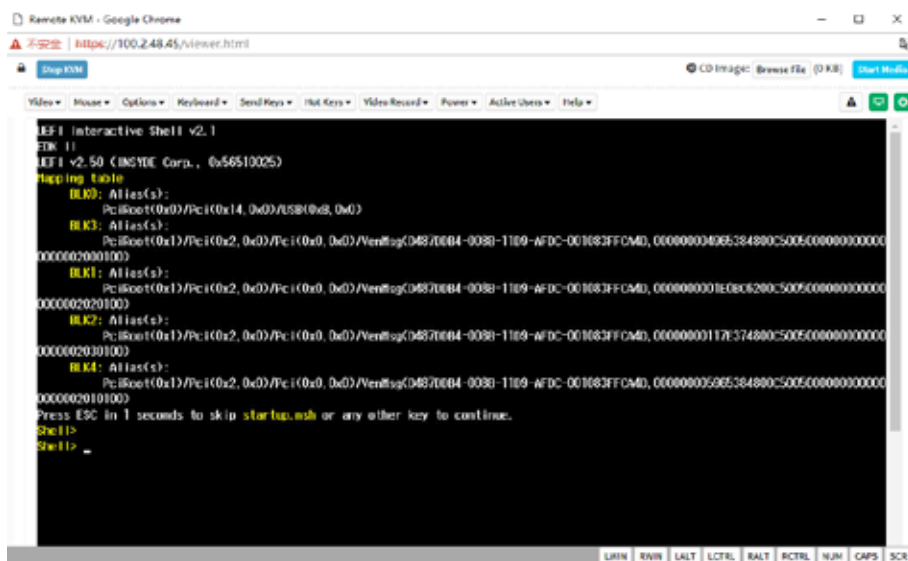


Figure 61 KVM Screen

9.26.2 Java KVM

Support Java KVM, users should download and open JNLP (Java Application), and 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.

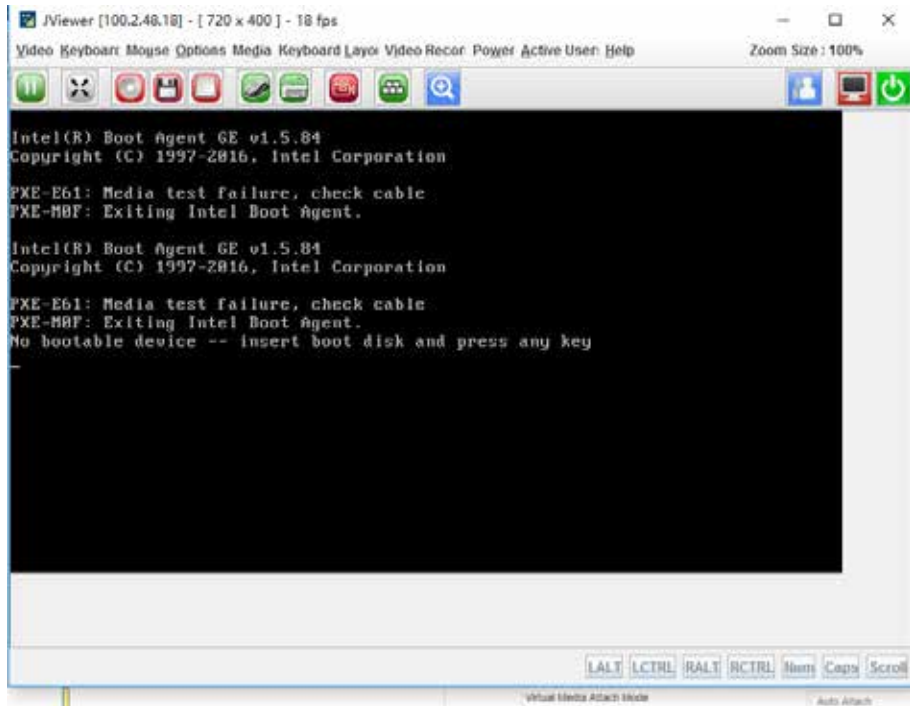


Figure 62 Java KVM

9.26.3 KVM Reconnect

Support reconnection after network disconnection, the retry count is 3 by default, and the retry time interval is 10s. Users 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.

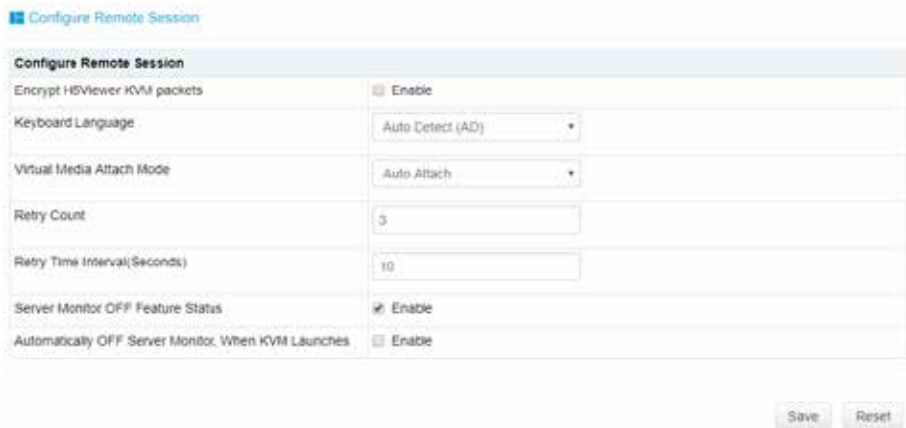


Figure 63 KVM Reconnect

9.26.4 Mouse Mode

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

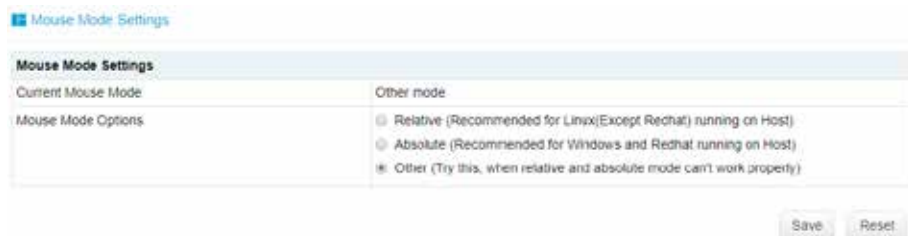


Figure 64 Mouse Mode Settings

Table 39 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

9.27 Virtual Media

The media redirection will allow users 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.

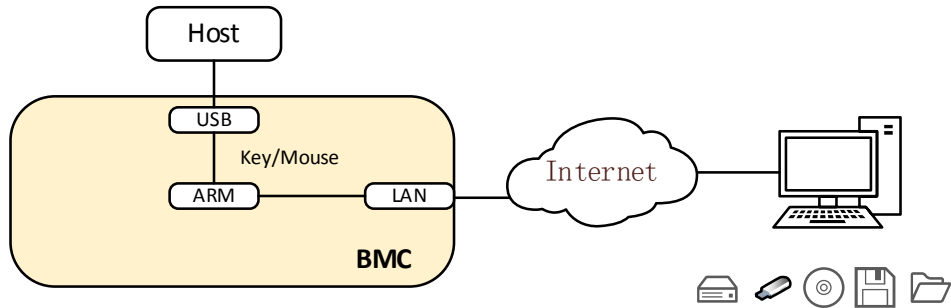


Figure 65 Virtual Media Schematic

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



Figure 66 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/Hard disk Images.

Users can mount virtual media in KVM as below.

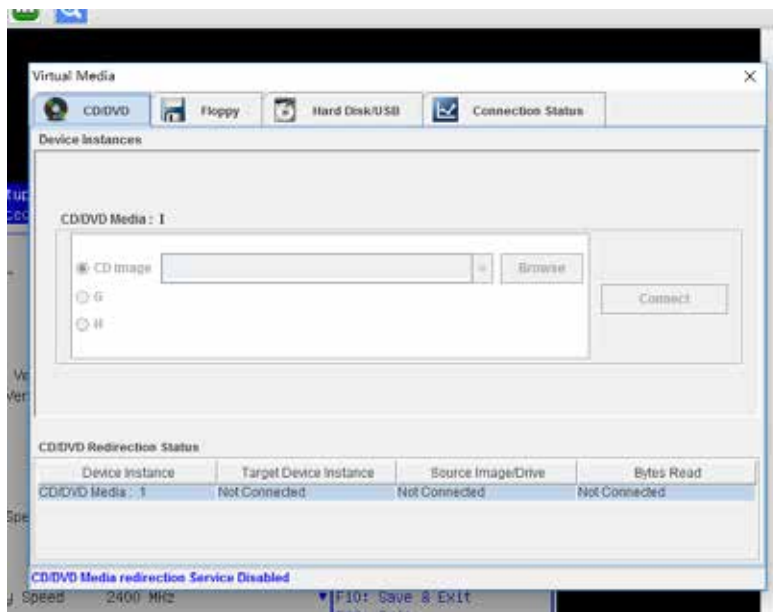


Figure 67 Virtual Media in KVM

9.28 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. The sending and receiving data are all in json format.

The username and password below must be BMC users with administrator privileges.

9.28.1 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://IP/redfish/v1/Chassis
```

9.28.2 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://IP/redfish/v1/Systems/System1/Actions/ComputerSystem.Reset -X POST -H 'Content-Type: application/json' -d '{"ResetType":"ForceOff"}
```

Note:

https://IP/redfish/v1/Systems/System1/Actions/ComputerSystem.Reset is the requested URL.

-H The parameter is the format of the requested data.

-d The parameter is the requested data.

9.28.3 DELETE

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

```
curl -k -u username:password https://IP/redfish/v1/SessionService/Sessions/2e630a6d590834cc06tTbziU5Wzqzg -X DELETE
```

Note:

https://IP/redfish/v1/SessionService/Sessions/2e630a6d590834cc06tTbziU5Wzqzg is the

deleted address.

9.28.4 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://IP/redfish/v1
```

Response:

```
{
  "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
  "@odata.id": "/redfish/v1/",
  "@odata.type": "#ServiceRoot.v1_0_2.ServiceRoot",
  "AccountService": {
    "@odata.id": "/redfish/v1/AccountService"
  },
  "Chassis": {
    "@odata.id": "/redfish/v1/Chassis"
  },
  "Id": "RootService",
  "Links": {
    "Sessions": {
      "@odata.id": "/redfish/v1/SessionService/Sessions"
    }
  },
  "Managers": {
    "@odata.id": "/redfish/v1/Managers"
  },
  "Name": "Root Service",
  "Oem": {},
  "RedfishVersion": "1.0.2",
  "SessionService": {
    "@odata.id": "/redfish/v1/SessionService"
  },
  "Systems": {
    "@odata.id": "/redfish/v1/Systems"
  },
  "UUID": "4ebf926c-045d-03ec-b211-d21d60da821c"
}
```

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:

```
{
  "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
  "@odata.id": "/redfish/v1/",
  "@odata.type": "#ServiceRoot.v1_0_2.ServiceRoot",
  "AccountService": {
    "@odata.id": "/redfish/v1/AccountService"
  },
  "Chassis": {
    "@odata.id": "/redfish/v1/Chassis"
  },
  "Id": "RootService",
  "Links": {
    "Sessions": {
      "@odata.id": "/redfish/v1/SessionService/Sessions"
    }
  },
  "Managers": {
    "@odata.id": "/redfish/v1/Managers"
  },
  "Name": "Root Service",
  "Oem": {},
  "RedfishVersion": "1.0.2",
  "SessionService": {
    "@odata.id": "/redfish/v1/SessionService"
  },
  "Systems": {
    "@odata.id": "/redfish/v1/Systems"
  },
  "UUID": "4ebf926c-045d-03ec-b211-d21d60da821c"
}
```

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://IP/redfish/v1/Chassis/Chassis1

Response:

```
{
  "@odata.context": "/redfish/v1/$metadata#Chassis.Chassis",
  "@odata.id": "/redfish/v1/Chassis/Chassis1",
  "@odata.type": "#Chassis.v1_2_0.Chassis",
  "AssetTag": "NULL",
  "ChassisType": "RackMount",
  "Id": "1U",
  "IndicatorLED": "Off",
  "Links": {
    "ComputerSystems": [
      {
        "@odata.id": "/redfish/v1/Chassis/Chassis1/Thermal"
      }
    ]
  }
}
```



```

    }
  ],
  "ManagedBy": [
    {
      "@odata.id": "/redfish/v1/Managers/BMC"
    }
  ],
  "ManagersInChassis": [
    {
      "@odata.id": "/redfish/v1/Managers/BMC"
    }
  ],
  "PCleDevices": [],
},
"Manufacturer": "Inspur",
"Model": "NF5280M5",
"Name": "NF5280M5",
"PartNumber": "M01",
"Power": {
  "@odata.id": "/redfish/v1/Chassis/Chassis1/Power",
  "Health": "NA"
},
"PowerState": "On",
"SerialNumber": "PS",
"Status": {
  "Health": "OK",
  "State": "Enabled"
},
"Thermal": {
  "@odata.id": "/redfish/v1/Chassis/Chassis1/Thermal"
}
}
}

```

Figure 71 Response of Get the URL for Chassis Specific Information

9.29 Appendix

Table 40 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

10 Common Faults, Diagnosis and Troubleshooting

This chapter introduces the common server faults, as well as corresponding diagnosis and troubleshooting suggestions.

10.1 Hardware Problems

1) Power-on failure at startup

Description: After pressing the power button, the LED (power status LED, HDD status LED) on server's front control panel is off. Meanwhile, no KVM (display) output is displayed, and server chassis fans do not rotate.

Suggestions:

- a. Check the power supply situation: If the power module LED is on, it indicates normal power supply. If the power module LED is off or red, please check whether the power supply is normal, and whether the power cord is connected well.
- b. If the power supply is normal, insert the power module again, and then power on for verification.
- c. If there is a machine and a power module of the same type, you could change the power module to test whether there is a power module fault.
- d. If the instructions above do not resolve the problem, please contact Inspur customer service.

2) No display after power on

Description: After pressing the power button, the power LED on server's front control panel is on, the chassis fans rotate normally, but there's no output on the display.

Suggestions:

- a. Firstly check whether the monitor is powered up normally.
- b. If the monitor is powered up normally, check whether it is connected normally with the server's VGA port.

- c. Test on another monitor.
- d. If there is no output on the new monitor, login to the BMC Web interface. Open BMC remote KVM to check whether there is output on the monitor. If there is normal output, it indicates the VGA port may be abnormal, please contact Inspur customer service.
- e. If above operations could not resolve the problem, please contact Inspur customer service.

3) Status LED on front panel is abnormal

Description: The server is under normal operation, but the status LED on front panel turns red.

Suggestions:

- a. Firstly confirm which LED is abnormal according to the previous chapter about the LEDs on the front panel.
- b. If the system failure LED is abnormal, check whether the system runs normally; if the system runs normally, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.
- c. If the power failure LED is abnormal, check whether the power module LED is normal; if the power module LED is normal, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.
- d. If other LEDs are abnormal, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.
- e. If above operations could not resolve the problem, please contact Inspur customer service.

4) Power module LED is off or red

Description: The server is under normal operation, but a certain power module LED is off or red.

Suggestions:

- a. Firstly check whether all power cables are normal, and plug in the power cables again.
- b. If the fault still exists, insert the power module again.
- c. If shutdown is allowed, you could exchange the two power modules to judge whether it is a power module fault.
- d. If above operations could not resolve the problem, please contact Inspur customer

service.

5) HDD status LED is abnormal

Description: The server is under normal operation, but the HDD status LED is off or red.

Suggestions:

- a. If it is caused by manual operations, restore the array through RAID configuration.
- b. If there is no manual operations, check whether the HDDs are identified normally. If the server is configured with an RAID card, login to the RAID management interface to check whether there is an HDD failure.
- c. If there is an HDD failure, or the above operations could not resolve the problem, please contact Inspur customer service.

Note: Hot-plugging HDD allows users to take out or replace the HDD without system shutdown and power off, which improves the system disaster recovery capability, scalability and flexibility. It only means the hot-plug HDD can be plugged in and out online without damage, and the following two items need to be noticed: ① Depending on the RAID level, hot plugging the HDD in the RAID will cause RAID degradation or failure. When installing a new HDD, different RAID cards have different policies, you may need to login to the RAID card management interface for recovery. ② Remove the HDD until the HDD motor stops completely, to prevent damage to the motor. For the operations on the RAID card management interface, please refer to Inspur technical website: www.4008600011.com.

6) Chassis fans make excessive noise

Suggestions:

- a. Firstly check whether the chassis fans operate at a high speed caused by the over-temperature chassis.
- b. If the chassis has a high temperature, check the temperature of server room, if it is excessively high, open the air conditioner to cool the room.
- c. If the server room's temperature is normal, check whether the front panel or chassis interior is jammed with dust, or the air inlet is blocked. It needs to improve the server room's environment, to avoid server over-temperature running because of too much dust.
- d. Check whether the server runs under high load.

e. If above operations could not resolve the problem, please contact Inspur customer service.

7) There is alarm sound during startup

Suggestions:

Firstly identify the source of alarm sound:

a. If the alarm sound comes from the power supply, check the power LED's status. If the power LED is abnormal, refer to item 3) to handle it.

b. If the alarm sound comes from the chassis interior, open the chassis to identify the specific source.

c. If the alarm sound comes from the RAID card, check the HDD LED status or login to the RAID management interface to check the HDD status. For the operations about the RAID management interface, please refer to Inspur technical website: www.4008600011.com.

d. If above operations could not resolve the problem, please contact Inspur customer service.

8) Keyboard and mouse are not available

Description: Neither keyboard nor mouse could be operated normally.

Suggestions:

a. Make sure the keyboard or mouse has been connected correctly and firmly.

b. Replace other parts to test whether it is a mouse or keyboard fault.

c. Power cycle the server and retest.

d. Reboot and enter BIOS or RAID configuration interface to test keyboard or mouse performance. When tested in a non-system situation, if the keyboard or mouse performance turns out to be normal, a system fault could be considered. If the keyboard or mouse fault still exists, a mainboard interface fault could be considered, and Inspur technical hotline can be called for support.

9) USB interface problem

Description: Unable to use devices with a USB interface.

Suggestions:

a. Make sure the operating system on server supports USB devices.

b. Make sure the system has been installed with correct USB device driver.

c. Power off the server, and then power on again to test.

d. Check whether the USB device is normal when connected to other hosts.

e. If the USB device is normal when connected to other hosts, the server may be abnormal:

please contact Inspur customer service.

f. If the USB device turns out to be abnormal when connecting to other hosts, please replace the USB device.

10.2 Software Problems

1) System installation problems

Description: It fails to load the RAID driver or to create partitions larger than 2T during system installation, C disk utilization is too large, and other problems.

Suggestions:

a. If it fails to load the driver during system installation, check the RAID driver's version, please visit Inspur website (<http://www.inspur.com>) to download the correct RAID driver.

For some RAID drivers, it needs to load several times.

b. If it fails to create 2T partitions, check BIOS Advance -> CSM Configuration-> Boot option filter, enable the UEFI option, and select UEFI mode to boot the system. It needs to enter the CMD command line to change the HDD format to GPT, and then partitions larger than 2T can be created.

c. If the C disk utilization is too large after system installation, open Computer Property-> Advanced System Property-> Advanced-> Performance-> Settings-> Change Virtual Memory, turn down the virtual memory or allocate the virtual memory to other partitions.

d. If above operations could not resolve the problem, please contact Inspur customer service.

2) Abnormal memory capacity

Description: The memory capacity displayed in the OS and the physical memory capacity are inconsistent.

Suggestions:

a. Check the OS version, the supported memory capacity varies with the version of Windows OS. Enter BIOS Setup to view the memory capacity, if the memory is identified completely, the operating system may have limits to the memory capacity, e.g. Windows server 2008 x86 supports 4G memory at most.

b. If the memory is not identified completely in BIOS Setup, confirm that the corresponding slots have been installed with memories of correct type.

c. If above operations could not resolve the problem, please contact Inspur customer service.

3) Abnormal network

Description: The network is disconnected, or the rate is lower than the actual rate of the network port.

Suggestions:

a. Check whether the network cable is connected well and whether the network LED flashes normally, re-insert the network cable to test again.

b. If the problem still exists, use a computer to connect with the server directly. If the direct connection is normal, check whether the network cable or the switch port is normal.

c. If the direct connection is abnormal, please visit Inspur website (<http://www.inspur.com>) to download the latest NIC driver.

d. If above operations could not resolve the problem, please contact Inspur customer service.

11 Battery Replacement

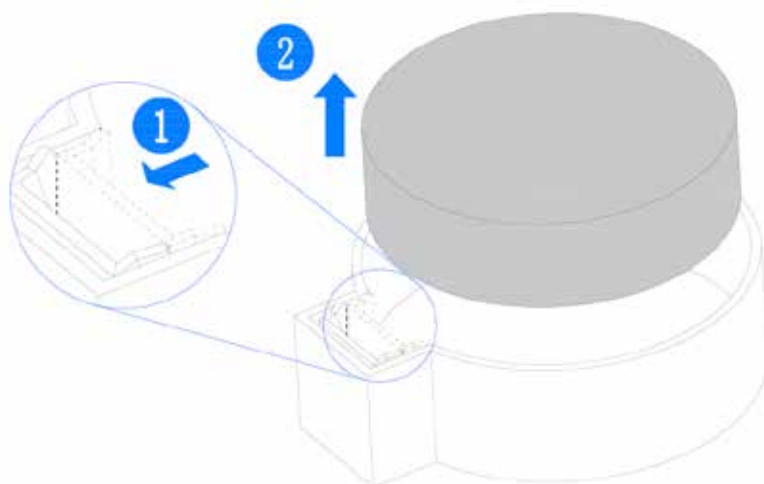
If the server no longer automatically displays the correct date and time, you may need to replace the battery that provides power to the real-time clock.

⚠ WARNING: The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose the battery to temperatures higher than 60°C (140°F).
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.
- Replace only with the spare designated for this product.

To remove the component:

1. Power down the server.
2. Extend the server from the rack.
3. Remove the access panel.
4. Remove the full-length expansion board retainer if any full-length expansion boards are installed.
5. Remove the PCI riser cage.
6. Remove the air baffle.
7. Remove the battery.



12 Regulatory Compliance Notices

12.1 Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, this product has been assigned a unique regulatory model number. The regulatory model number can be found on the product nameplate label, along with all required approval markings and information. When requesting compliance information for this product, always refer to this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

12.2 Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

12.2.1 FCC Rating Label

The FCC rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or ID on the label. Class A devices do not have an FCC logo or ID on the label. After you determine the class of the device, refer to the corresponding statement.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and,

if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

12.3 European Union Regulatory Notice

Products bearing the CE marking comply with the following EU Directives:

- Low Voltage Directive 2014/35/EU
- EMC Directive 2014/30/EU

CE compliance of this product is valid if powered with the correct CE-marked AC adapter provided by INSPUR.

Compliance with these directives implies conformity to applicable harmonized European standards (European Norms) that are listed in the EU Declaration of Conformity issued by INSPUR for this product or product family and available (in English only) within the product documentation.

The compliance is indicated by one of the following conformity markings placed on the product:



Please refer to the regulatory label provided on the product.

12.4 Disposal of Waste Equipment by Users in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.



12.5 Korean Notice

Class A Equipment

A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.
-----------------------	-------------------------------------------------------------------------------------------

Class B Equipment

B급 기기 (가정용 방송통신기기)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.
-----------------------	------------------------------------------------------------------------------

12.6 Chinese Notice

Class A Equipment

声明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取可行的措施。

12.7 Battery Replacement Notice



WARNING: The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose the battery to temperatures higher than 60°C (140°F).
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.



Batteries, battery packs, and accumulators should not be disposed of together with the general household waste. To forward them to recycling or proper disposal, use the public collection system or return them to Inspur, an authorized Inspur Partner, or their agents.

13 Electrostatic Discharge

13.1 Preventing Electrostatic Discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

13.2 Grounding Methods to Prevent Electrostatic Discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

For more information on static electricity or assistance with product installation, contact Inspur Customer Service.

14 Warranty

14.1 Introduction

Inspur warrants that all Inspur-branded hardware products shall provide a period of three (3) year warranty. This document describes Warranty Service, including a detailed description of service-level.

The warranty terms and conditions may vary by country, and some services and/or parts may not be available in all countries. For more information about warranty services in your country, contact Inspur technical support or Inspur local office.

14.2 Warranty Service

14.2.1 Service Overview

Type	Duration
Remote Services	3 years
RMA Services	3 years

14.2.2 Warranty Service Terms & Conditions

i. Remote Services

Inspur provides 24x7 remote service through Hotline, E-mail and Website. Through Hotline and E-mail Services, Inspur engineer helps customers determine the cause of the malfunction and provide solution. Website service provides a number of resources to help customers resolve problems, and learn about our products, such as product manuals, drivers and Firmware.

Below is how to obtain our remote service:

Type	Description	Response time
Hotline	1-844-860-0011(English) 1-646-517-4966(English) 86-800-860-0011(Chinese)	Within 2hrs
E-mail	serversupport@inspur.com	Within 2hrs
Website	http://en.inspur.com/	

ii. RMA Services

Customers could return defective parts to the designated Inspur site after submitting a

service request. Inspur may, at its discretion, repair or replace the defective parts. Repair or replacement parts may be new, used, or equivalent to new in performance and reliability. Replaced or repaired parts are warranted to be free of defects in material or workmanship for ninety (90) calendar days or, for the remainder of the warranty period of the product, whichever is longer.

14.3 Warranty Exclusions

Inspur does not guarantee that there will be no interruptions or mistakes during the use of the products. Inspur will not undertake any responsibility for the losses arising from any operation not conducted according to Inspur Hardware Products.

The Warranty Service Terms & Conditions do not apply to consumable parts, as well as any products the serial number of which falls off, is damaged or obscure for the following reasons:

- Accident, misuse, abuse, defiling, improper maintenance or calibration or other external causes
- Operating beyond the parameters as stipulated in the user documentation
- Use of the software, interface, parts or supplies not provided by Inspur
- Improper preparation place or maintenance
- Virus infection
- Loss or damage in transit
- Alterations or repairs have been made by unauthorized persons, or service organizations

Inspur does not undertake any responsibility for the damages or losses of any application, data or removable storage medium. Except for the software installed by Inspur in its production of this product, Inspur is not responsible for the restoration or reinstallation of any programs or data.