Inspur Server User Manual

System Model i24

Node Model NS5162M5

Edition: 1.2
August,2021
Editon Statement:Updated Safety Instructions

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 this server's technical features, system installation and setup, which will help the user to understand how best to utilize the server and all its functions.

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. After the first login, please change the BMC user password in time.

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 Specifications 5
2.1 Introduction 5
2.2 Features and Specifications 6
2.3 Compatible Peripherals – AOC Cables 8
2.4 Power Efficiency 8

3 Component Identification 10
3.1 Front Panel Components 10
3.2 Rear Panel Components 11
3.3 Motherboard Components 12

4 Operations 14
4.1 Power up the Server 14
4.2 Power down the Server 14
4.3 Extend the Server from the Rack 14
4.4 Remove the Access Panel 15
4.5 Install the Access Panel 16
4.6 Remove the Node from the Chassis 16
4.7 Remove the Air Baffle 17
4.8 Remove the PCIE Riser Cage 18

5 Setup 21
5.1 Optimum Environment 21
5.2 Rack Warnings 23
5.3 Identifying the Contents of the Server Shipping Carton 24
5.4 Installing Hardware Options 24
5.5 Installing the Server into the Rack 24
5.6 Installing the Operating System 25

6 Hardware Options Installation 26
6.1 Introduction 26
6.2 Processor Option 26

6.3 Memory Option 28
6.4 Hot-plug HDD Option 29
6.5 Redundant Hot-plug Power Supply Option 31
6.6 Expansion Board Option 31
6.7 M.2 SSD Option 33
6.8 TPM Card Option 35
6.9 OCP/PHY Card Option 35

7 Cabling 37

8 BIOS Setup 38
8.1 Common Operations 38
8.2 BIOS Parameter Description 55
8.3 Firmware Update 97

9 BMC Settings 101
9.1 Introduction 101
9.2 Functional Modules 102
9.3 Web Interface Introduction 103
9.4 Remote Control 107
9.5 Power and Fan 114
9.6 BMC Settings 109
9.7 Logs 121
9.8 Fault Diagnosis 123
9.9 Administration 125
9.10 Command Line Function Introduction 129
9.11 Time Zone Table 134

10 CMC Settings 138
10.1 Introduction 138
10.2 Functional Modules 138
10.3 Web Interface Introduction 139
10.4 System Monitor 142
10.5 CMC Settings 146
10.6 Logs 153
10.7 FRU Information 156

10.8 System Maintenance 157
10.9 Command Line Function Introduction 160
10.10 Time Zone Table 162
10.11 Service & Protocol 164
10.12 User Management 165
10.13 BMC Firmware Update 166

11 Common Faults, Diagnosis and Troubleshooting 168
11.1 Hardware Problems 168
11.2 Software Problems 172

12 Battery Replacement 174

13 Regulatory Compliance Notices 175
13.1 Regulatory Compliance Identification Numbers 175
13.2 Federal Communications Commission Notice 175
13.3 European Union Regulatory Notice 176
13.4 Disposal of Waste Equipment by Users in the European Union 176
135 Korean Notice 177
13.6 Chinese Notice 177
13.7 Battery Replacement Notice 177
13.8 Battery Caution 178
13.9 Restricted Access Area 179

14 Electrostatic Discharge 180
14.1 Preventing Electrostatic Discharge 180
14.2 Grounding Methods to Prevent Electrostatic Discharge 180

15 Warranty 181
15.1 Introduction 181
15.2 Warranty Service 181
15.3 Warranty Exclusions 182

16 Appendix 183
16.1 Drive Neodymium Content Reference 183

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. Do not connect two or more power cords to each other. If a longer power cord is needed, contact Inspur Customer Service.
4. Please be sure to use the power supply components that come with the server, such as power cable, 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 cable 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 cables 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 cable plug from the power socket and contact Inspur's customer service department:

1) The power cords 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 motherboard, please power off the system and wait for five seconds, and then remove the components from the motherboard 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 dismounting the internal components, please pay attention to the followings:

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 dismounting the host cover or touching the internal components.

3) During the dismounting 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 Specifications

2.1 Introduction

Inspur i24 is a high-end, dual-socket and rack-mounted server, which is designed on the basis of the new generation of Intel® Xeon® scalable processors, to satisfy the requirements of cloud computing, big data, data mining, deep learning and other high-end IT applications. This server has high quality and high reliability on performance, storage and extension, and makes innovations and breakthroughs on computing performance, flexible configuration and intelligent management, particularly suitable for telecom operators, financial industry, internet companies and other large-scale enterprises.

- Main features:

▪ Ultimate computing, storage and expansion capability

Supports the new generation of Intel® Xeon® scalable processors and TDP 165W CPU;

16 DIMM sockets support RDIMM, LRDIMM and NVDIMM, which greatly improves the application performance, and improves 33 percent in the computing performance.

Achieves space's multidimensional extension, supports up to 12*3.5" drive or 24*2.5" drive in 2U space; supports up to 24*U.2 SSD or 16*U.2 SSD + 8*2.5" drive, providing high storage performance.

▪ Optimization oriented to different applications

The storage module, I/O module and network module can achieve different combinations for various application scenarios, providing flexible choices for users.

Provides abundant I/O and up to 2 PCI-E 3.0 X16 slots and OCP/PHY card in the limited space of 2U chassis and 4 nodes, to meet the users' requirements on system functionality and performance.

▪ Excellent low-noise and cooling design

With systematic low-noise design, the system can achieve "cool" operating under high load. The hot-swap fans have easy-maintainability and N+N redundant backup capability.

- 2.5"×24 Configuration (i.e. Full Configuration)

Supports 24*2.5"SAS/SATA/SSD in the front, as shown in the figure below.

Figure 2-1

- 3.5”×12 Configuration (i.e. Full Configuration)

Supports 12*2.5"/3.5" SAS/SATA/SSD in the front, as shown in the figure below.

Note: The 3.5" drive trays can hold 3.5"/2.5" drives.

Figure 2-2

2.2 Features and Specifications

Table 2-1

Processor	
Processor Type	Intel® Skylake, Cascadelake (supports up to two 165W processors)
Chipset	
Chipset Type	C622, C624, C627
Memory	
Memory Type	DDR4 Registered, LR DIMM, NVDIMM
Memory Slot Qty.	16
Total Memory Capacity	Supports up to 2.0TB (128GB per memory module)
I/O	
USB	2 rear USB 2.0 ports
VGA	1 rear VGA port

Serial Interface	2 rear serial interfaces
UID	1 UID LED and button (on the rear of the chassis)
Display	
Controller Type	Integrated in the Aspeed2500 chip, supports up to 1280*1024 resolution
SAS Backplane	
NVMe Backplane	Supports hot-plug SAS/SATA/SSD
NIC	
NIC Controller	The motherboard supports OCP/PCIE card, and supports 100G NIC.
Management	
Management Chip	It integrates 1 independent 1000Mbps network interface, special for IPMI remote management
PCI Expansion	• Onboard: 2 PCI Express 3.0 ×16 slots, used to support PCI-E Riser card • The Riser card only supports horizontal-inserted and HHHL cards • Standard configuration: PCIE0 slot (CPU0 out): 1 Riser card, supporting 1 PCI Express 3.0 ×16 slot • Full configuration 1: Riser slot1 (CPU0 out): 1 Riser card, supporting 1 PCI Express 3.0 ×16 slot Riser slot2 (CPU0 out): 1 Riser card, supporting 1 PCI Express 3.0 ×16 slot • Onboard: 1 Type A/C or A/B slot (for supporting OCP/PHY card)
Drive	
Drive Type	2.5”/3.5” SAS/SATA/SSD (The machine you purchased shall prevail)
External Storage Drive	
Optical Drive	Supports external USB drive
TF Card	Built-in TF card
Power	
Specifications	Single/dual power supply/supplies of 2000W output power; 1+1 conditional redundancy; 2 power modules; Supports PMBus power supply; Node Manager 4.0 function
Power Input	Please refer to the power input on the nameplate label of the host
Physical	
Size of Host Machine	Chassis (2.5” drive bays): 446 width × 87.5 height × 805 depth (unit: mm) Chassis (3.5” drive bays): 446 width × 87.5 height × 845 depth (unit: mm)
Product Weight	Full configuration: 12*3.5” drive bay (with 12 drives installed) Gross weight: 58kg (Gross weight includes: Host + Packing Box + Rails + Accessory Box) Full configuration: 24*2.5” drive bay (with 24 drives installed) Gross weight: 53kg (Gross weight includes: Host + Packing Box + Rails + Accessory Box)
Environmental	
Operating Temperature	10℃ -35℃
Storage & Transportation Temperature	-40℃ -60℃
Operating Humidity	20％ -80％ relative humidity
Storage & Transportation Humidity	20％ -93％ (40℃) relative humidity

2.3 Compatible Peripherals – AOC Cables

Table 2-2

Vendor	Vendor PN	Specifications
Gigalight	GSS-MDO100-003C	10G SFP+ AOC, 3m, orange
Gigalight	GSS-MDO100-005C	10G SFP+ AOC, 5m, orange
Gigalight	GSS-MDO100-007C	10G SFP+ AOC, 7m, orange
Gigalight	GSS-MDO100-010C	10G SFP+ AOC, 10m, orange
Finisar	FCBG110SD1C03	10G SFP+ AOC, 3m, black
Finisar	FCBG110SD1C05	10G SFP+ AOC, 5m, black
Finisar	FCBG110SD1C07	10G SFP+ AOC, 7m, black
Finisar	FCBG110SD1C10	10G SFP+ AOC, 10m, black
Avago	AFBR-2CAR03Z	10G SFP+ AOC, 3m, orange

2.4 Power Efficiency

Table 2-3

Efficiency Level	Rated Power	Efficiency			PF
		@20% Load	@50% Load	@100% Load	@50% Load
Platinum	2000W	90%	94%	91%	0.98

Table 2-4

EU Regulation 2019/424 Server configurations	High-end performance configuration	Low-end performance configuration
(h) idle state power	464.8W	329.4W
(i) list of all components for additional idle power allowances, if any (additional PSU, HDDs or SSDs, additional memory, additional buffered DDR channels, additional I/O devices);	1126.59W	400.44W
(j) maximum power, expressed in Watts and rounded to the first decimal place;	2063.7W	694.5W
(k) declared operating condition class, as detailed in Table 6;	A2	A2
(l) idle state power (Watts) at the higher boundary temperature of the declared operating condition class;	479.64W	341.72W
(m) the active state efficiency and the performance in active state of the server;	36.3	18.6

Table 2-5

(i) List of components for additional power allowance		High-end performance configuration	Low-end performance configuration
CPU Performance	1 socket: 10 × Perf CPU W		
	2 socket: 7 × Perf CPU W	364.35W	52.92W
Additional PSU	10 W per PSU	10W	10W
HDD or SSD	5.0 W per HDD or SSD	10W	10W
Additional memory	0.18 W per GB	552.24W	137.52W
Additional buffered DDR channel	4.0 W per buffered DDR channel	160W	160W
Additional I/O devices	< 1 Gb/s: No Allowance	0W	0W
	= 1 Gb/s: 2.0 W/Active Port		
	> 1 Gb/s and < 10 Gb/s: 4.0 W/Active Port		
	≥ 10 Gb/s and < 25Gb/s: 15.0 W/Active Port		
	≥ 25 Gb/s and < 50Gb/s: 20.0 W/Active Port		
	≥ 50 Gb/s 26.0 W/Active Port		
Total power		1126.59W	400.44W

3 Component Identification

3.1 Front Panel Components

- **3.5” × 12 Drive Bays**

Figure 3-1

Table 3-1

Item	Description	Status & Interpretation
1	Power button	Green: System on Orange: System in standby Long press it for 4s to force a shutdown.
2	UID|RST button	To turn ON/OFF the UID. Blue: ON Long press it for 6s to force a system reset.
3	System fault LED	OFF: Normal Steady red: Faulty Flashing red: Warning
4	CMC port	Mini USB to RJ45 port, CMC debug connector

- **2.5” × 24 Drive Bays**

Figure 3-2

- **Drive Tray LEDs**

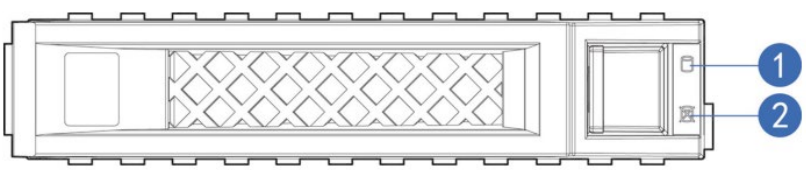


Figure 3-3

Table 3-2

Item	Description	Status & Interpretation
1	Fault alarm LED	Steady red: A HDD failure occurs Steady blue: Disk positioning Steady pink: RAID rebuilding
2	Activity status LED	Steady green: Normal Flashing green: Read and write activity

3.2 Rear Panel Components

- **Node Rear Panel Components**

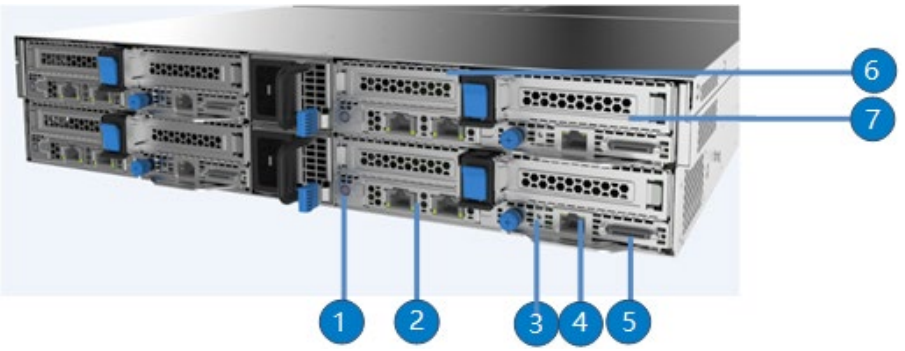


Figure 3-4

Table 3-3

Item	Description	Status & Interpretation
1	UID | RST button	To turn ON/OFF the UID. Blue: ON Long press it for 6s to force a system reset.
2	OCP or PHY	Optional OCP/PHY card
3	BMC Reset	BMC reset button
4	IPMI	Node management port
5	SUV	High-density port: Integrated USB2.0 port x2 Integrated VGA port x1 Integrated serial interface x2 (for BMC & for System)
6	PCIE GEN3 X16	To connect PCIE 3.0 X16 device
7	PCIE GEN3 X16	To connect PCIE 3.0 X16 device

- **Chassis Rear Panel Components**

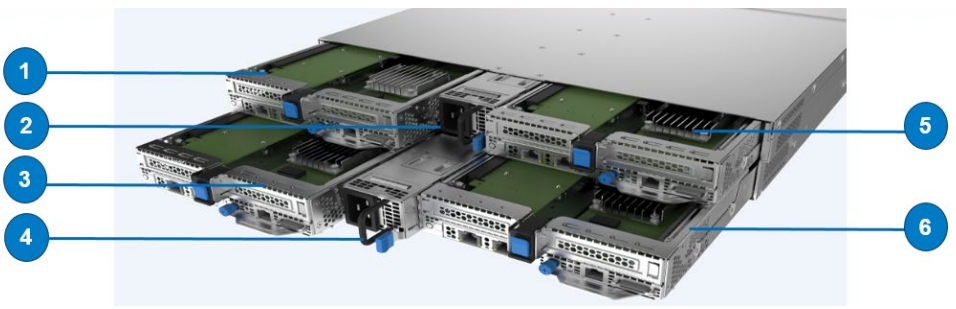


Figure 3-5

Table 3-4

Item	Description
1	NodeC
2	PSU0
3	NodeD
4	PSU1
5	NodeA
6	NodeB

- **Power Supply Unit LED**

Figure 3-6

Table 3-5

Item	Power Module Status/Condition	LED Status
1	Output-ON	Steady green
2	No AC power to all power supplies	OFF
3	AC present	1Hz blink green
4	AC cord unplugged or AC lost; with a second power supply on parallel still with AC input power	AC lost display amber
5	Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow FAN	2Hz blink amber
6	Power supply circuit event causing a shutdown; failure, OCP, OVP, FAN fail	Amber
7	PSU in cold standby mode	2Hz blink green
8	Bootload updating FW	Blink green

3.3 Motherboard Components

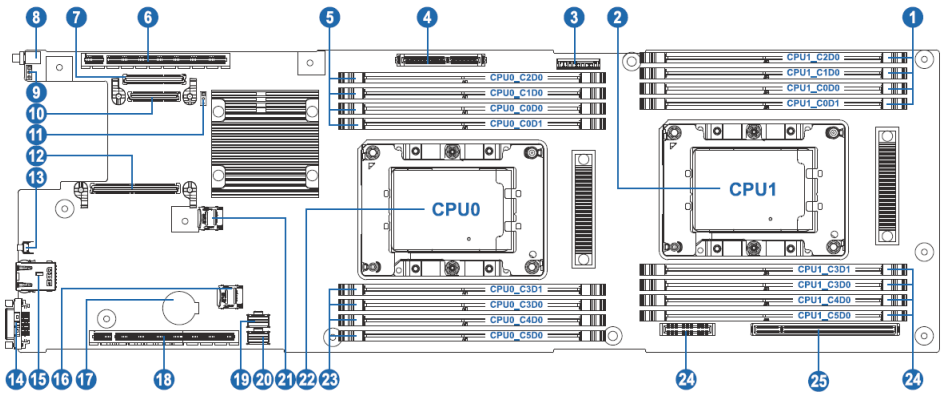


Figure 3-7

Table 3-6

Item	Description
1	DIMM slots (CPU1)
2	CPU1
3	TPM
4	M.2 RISER
5	DIMM slots (CPU0)
6	PCIE0_CPU0
7	OCPB_CPU0
8	UID RST
9	BMC_RELOAD
10	OCPC
11	CLR_COMS
12	OCPA_CPU0
13	BMC RST
14	SUV
15	MLAN
16	BMC_TF_SLOT
17	RTC battery
18	PCIE1_CPU0
19	SATA4-7
20	SATA0-3
21	SYS_TF_SLOT
22	CPU0
23	DIMM slots (CPU0)
24	EDGE_PWER
25	EDGE_PCIE
26	DIMM slots (CPU1)

● Motherboard Jumper Introduction

See [Motherboard Components] for the jumper position.

Table 3-7

Item	Description	Function
CLR_CMOS	CMOS clear jumper	Short-circuit pin1-2, restore to normal status; short-circuit 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 and Pin2 (the default status) of CLR_CMOS jumper with a jumper cap, 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 quick release levers on each side 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.

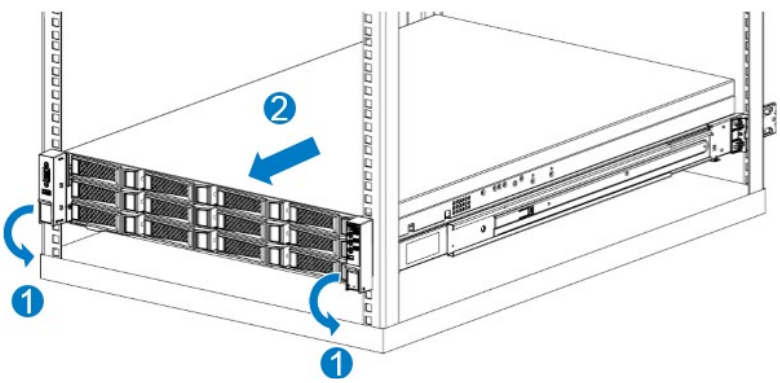


Figure 4-1

3. After performing the installation or maintenance procedure, slide the server back into the rack, and then push the server firmly into the rack to secure it 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.

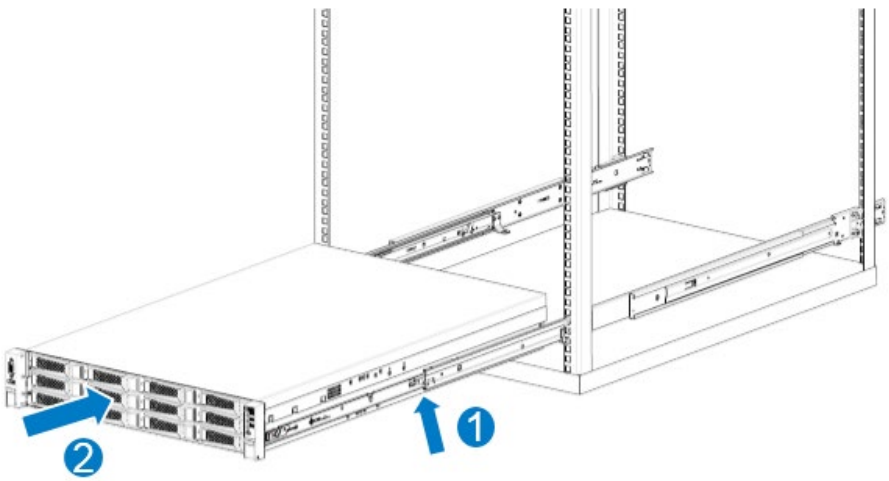


Figure 4-2

4.4 Remove the Access Panel

⚠ 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: For proper cooling, do not operate the server without the access panel, air baffle, or fan installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

To remove the component:

1. Power down the server if performing a non-hot-plug installation or maintenance procedure.
2. Extend the server from the rack.
3. Use the screwdriver to loosen the security screw on the hood latch.
4. Lift up on the hood latch handle, and then remove the access panel.

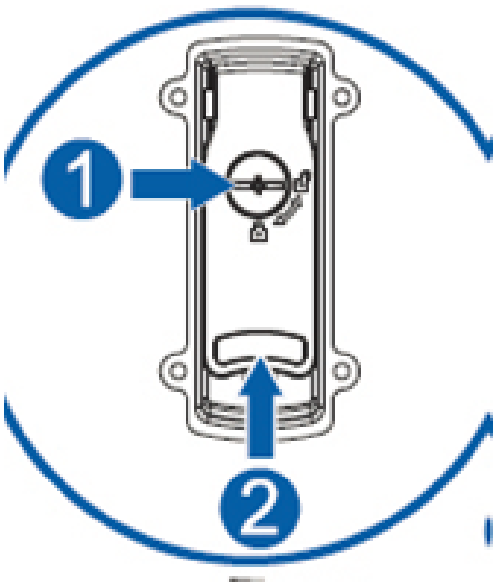


Figure 4-3

4.5 Install the Access Panel

1. Place the access panel on top of the server with the hood latch open. Allow the panel to extend past the rear of the server.
2. Push down on the hood latch. The access panel slides to a closed position.
3. Use the screwdriver to tighten the security screw on the hood latch.

4.6 Remove the Node from the Chassis

1. Use the screwdriver to loosen the screw on the node.
2. Pull out the node to remove it.
3. Install the node in the reverse order.

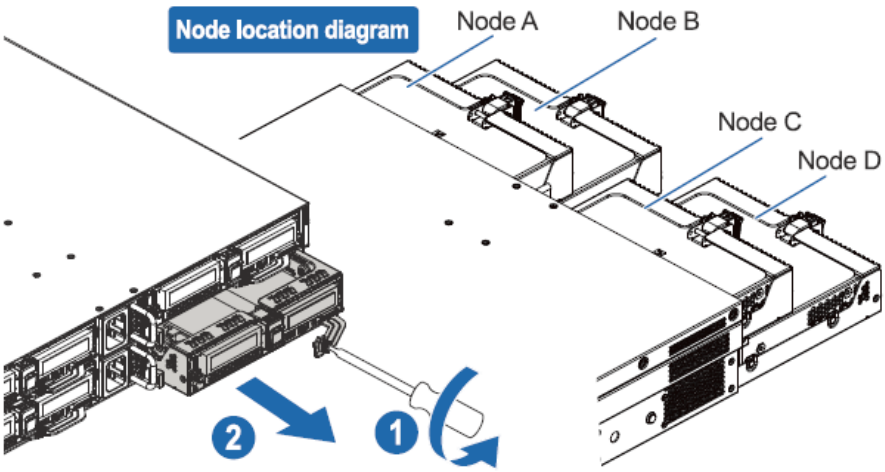


Figure 4-4

4.7 Remove the Air Baffle

CAUTION: For proper cooling, do not operate the server without the access panel, air baffle, or fan 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 or remove the server from the rack.
3. Remove the access panel.
4. Remove the air baffle.

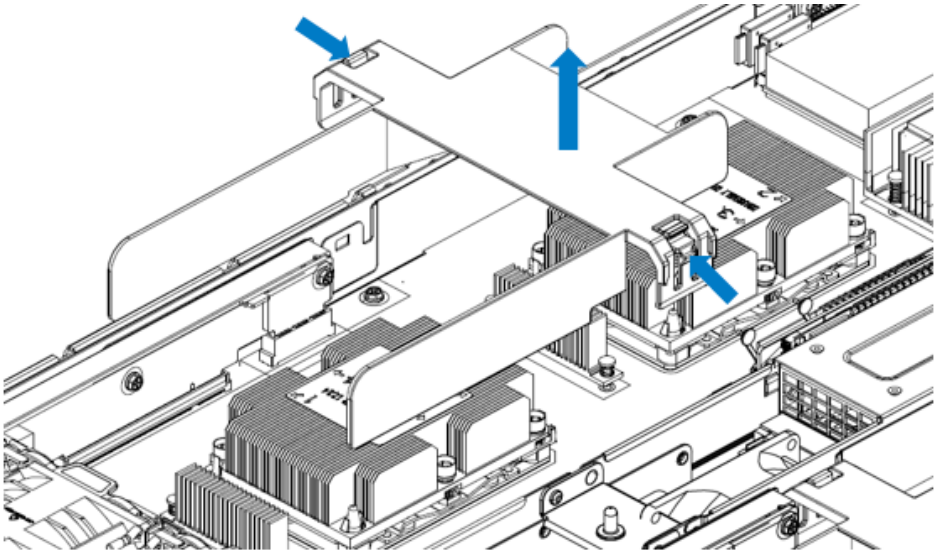


Figure 4-5

4.8 Remove the PCIE Riser Cage

⚠ CAUTION: For proper cooling, do not operate the server without the access panel, air baffle, or fan 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 corresponding node.
5. Press the latch of the riser cage as shown in the following figure.

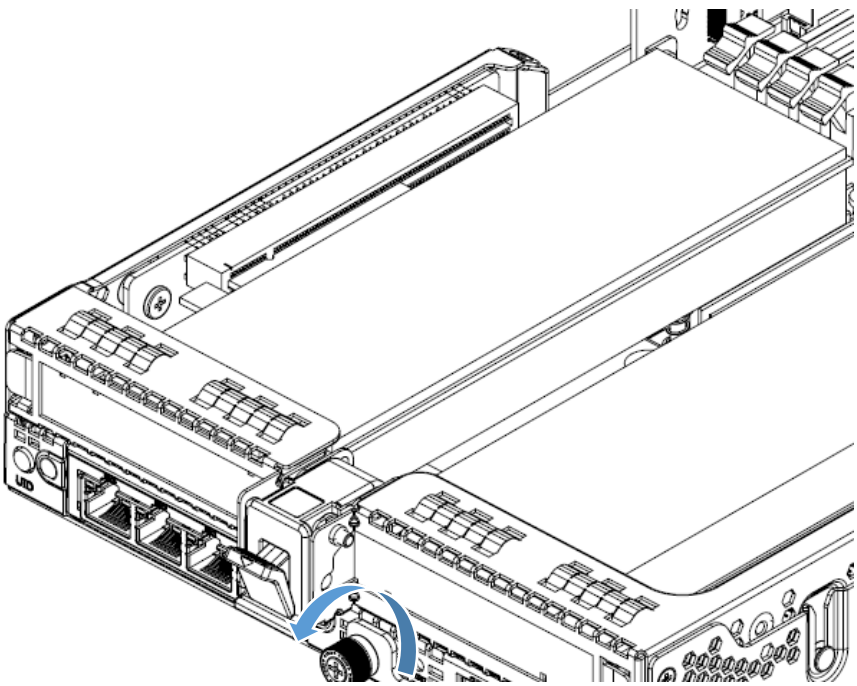


Figure 4-6

6. Open the latch and remove the riser cage vertically.

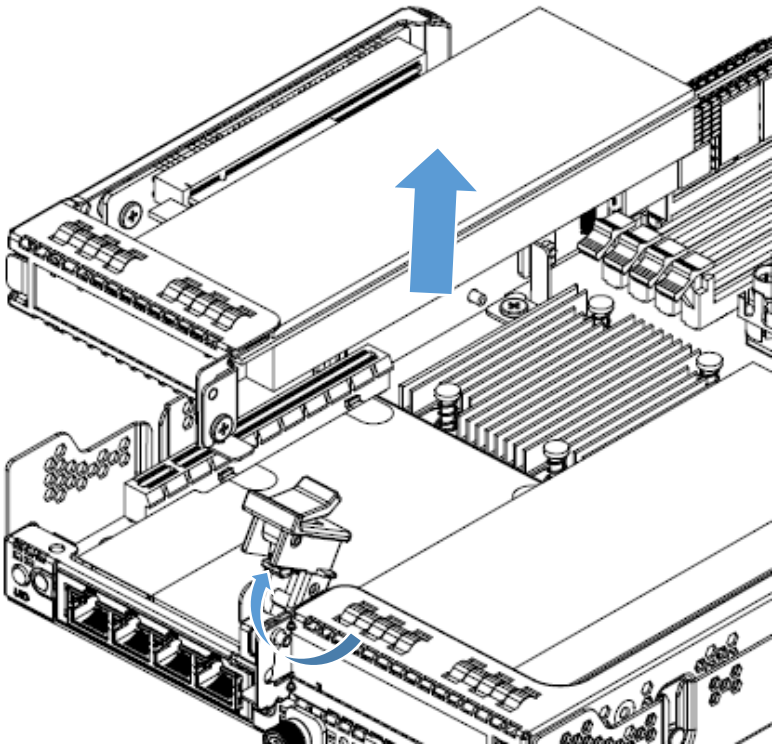


Figure 4-7

Note: The riser card types supported by the PCIE riser cage are shown as follows (there are two riser cards in the node: left one and right one).

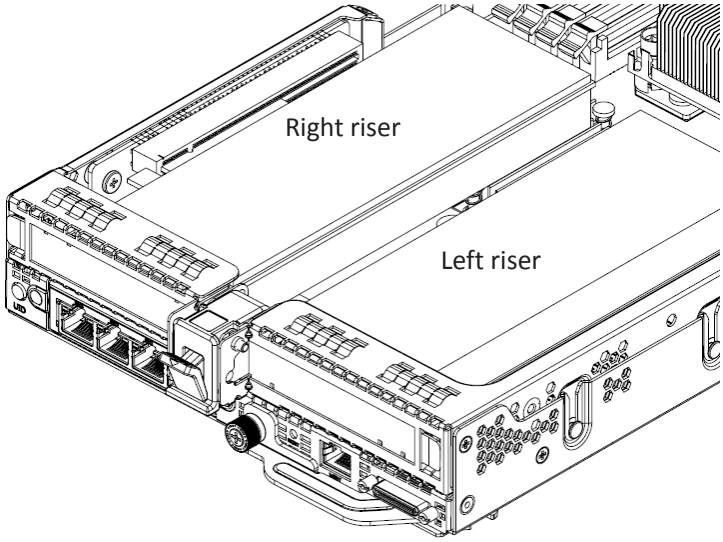


Figure 4-8

a. Left PCIE riser card

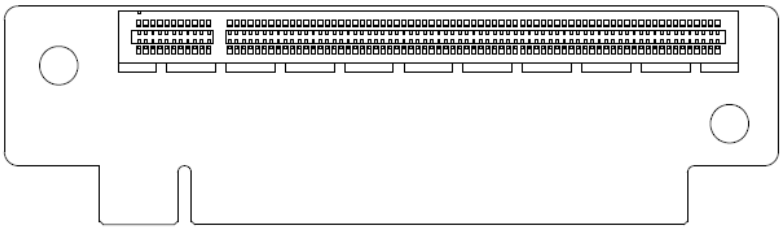


Figure 4-9

b. Right PCIE riser card

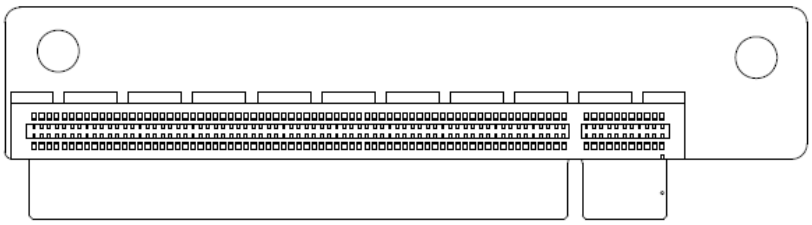


Figure 4-10

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 (containing the software driver TF card)
- 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 into the rack. For more information, see the installation instructions included with the 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://en. inspur.com/).

Methods to install an operating system on the server include:

Place the operating system into an external USB disk and then boot the server through the USB disk to install the system. This process may require you to obtain additional drivers from the Inspur website (http://en. inspur.com/).

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 node supports single- and dual-processor operation.

⚠ 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 configuration 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. Remove the processor:

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

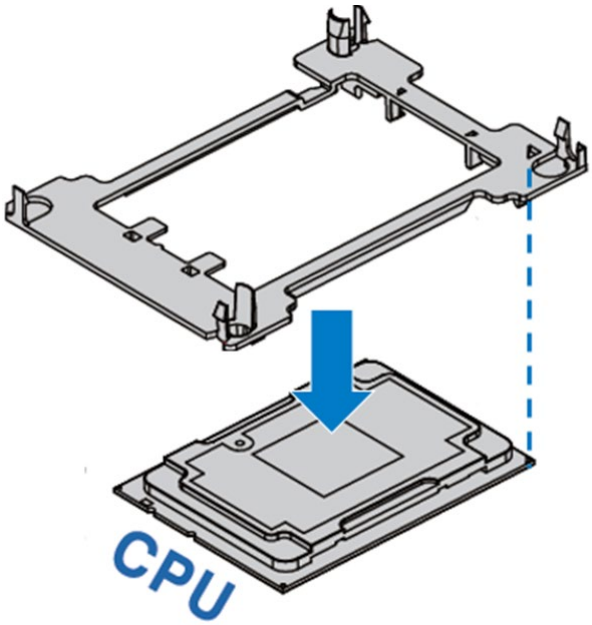


Figure 6-1

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.

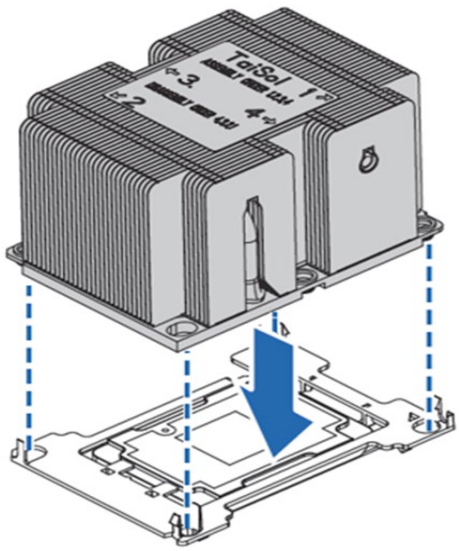


Figure 6-2

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.

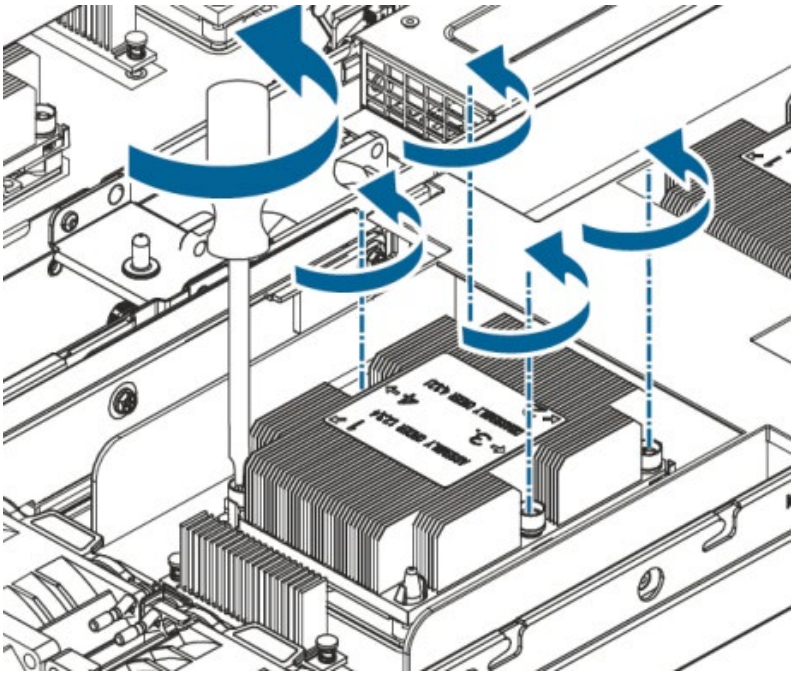


Figure 6-3

Notes:

- It is required to coat thermal grease evenly onto the contact position between CPU heatsink and CPU.
- During fixing CPU heatsink, it is required to fasten bolts according to the sequence accordingly.

6.3 Memory Option

RDIMMs and LRDIMMs can not be mixed.
AEPs can be mixed with RDIMMs or LRDIMMs.

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

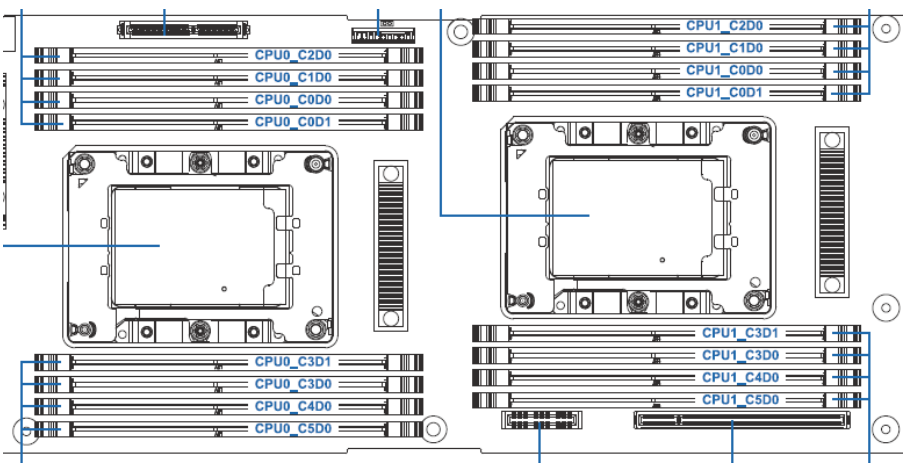


Figure 6-4

- DIMM population guidelines:

a. The white slots take the priority, while CPU1 DIMM shall be symmetrically installed with CPU0 DIMM.

b. For the single CPU, the DIMM population follows the screen printed sequence: CPU0_C0D0, CPU0_C1D0, CPU0_C2D0, CPU0_C3D0, CPU0_C4D0, CPU0_C5D0; CPU0_C0D1, CPU0_C3D1.

c. For dual CPUs, CPU0 DIMM population follows the screen printed sequence: CPU0_C0D0, CPU0_C1D0, CPU0_C2D0… ; CPU1 DIMM population follows the screen printed sequence: CPU1_C0D0, CPU1_C1D0, CPU1_C2D0 …

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.

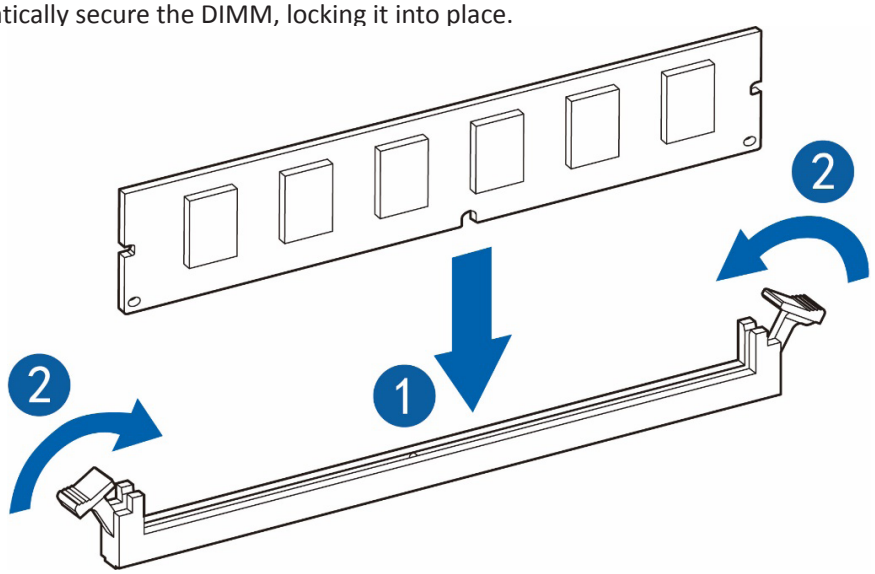


Figure 6-5

6.4 Hot-plug 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. Determine the status of the hard disk drive from the hot-plug HDD LED.
2. Back up all server data on the hard disk drive.
3. Remove the hard disk drive.

Installing a hot-plug HDD

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.

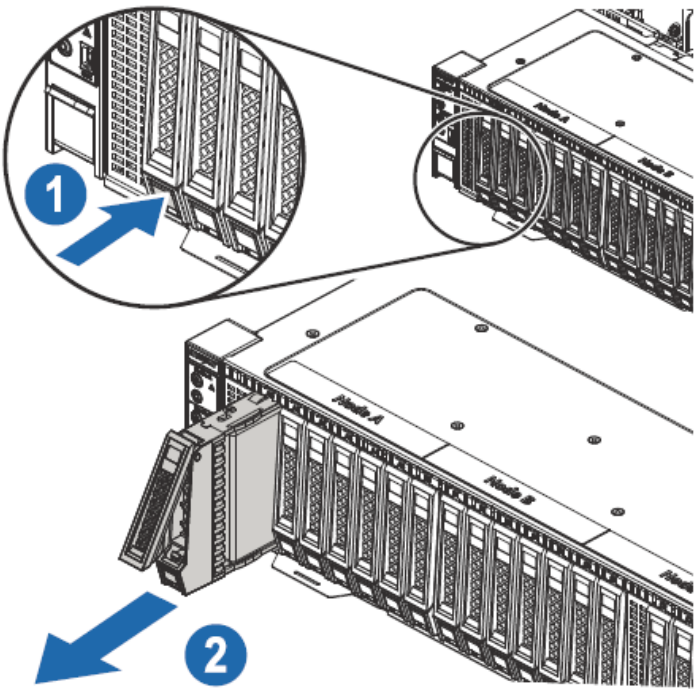


Figure 6-6

Step 3: Use four screws to fix the HDD into the tray.

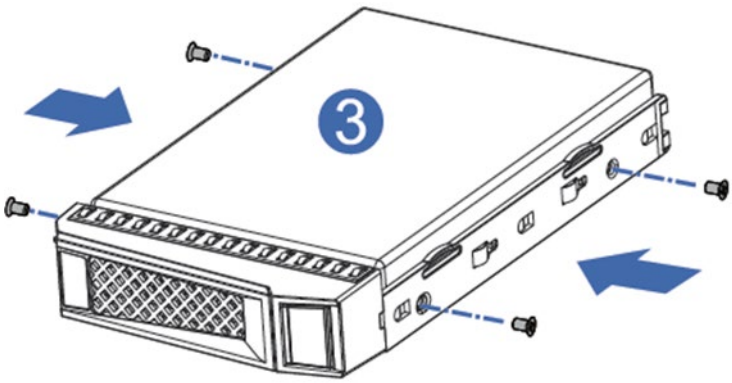


Figure 6-7

Step 4: Install the HDD into the chassis, and lock the lever firmly.

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, air baffle, or fan 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 corresponding node.
5. Press the latch of the riser cage as shown in the following figure.

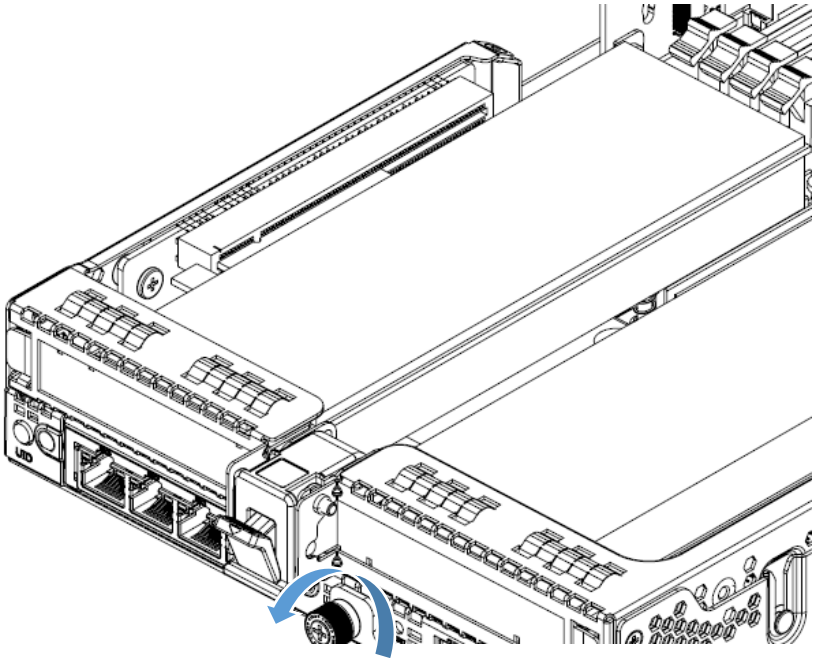


Figure 6-8

6. Open the latch and remove the riser cage vertically.

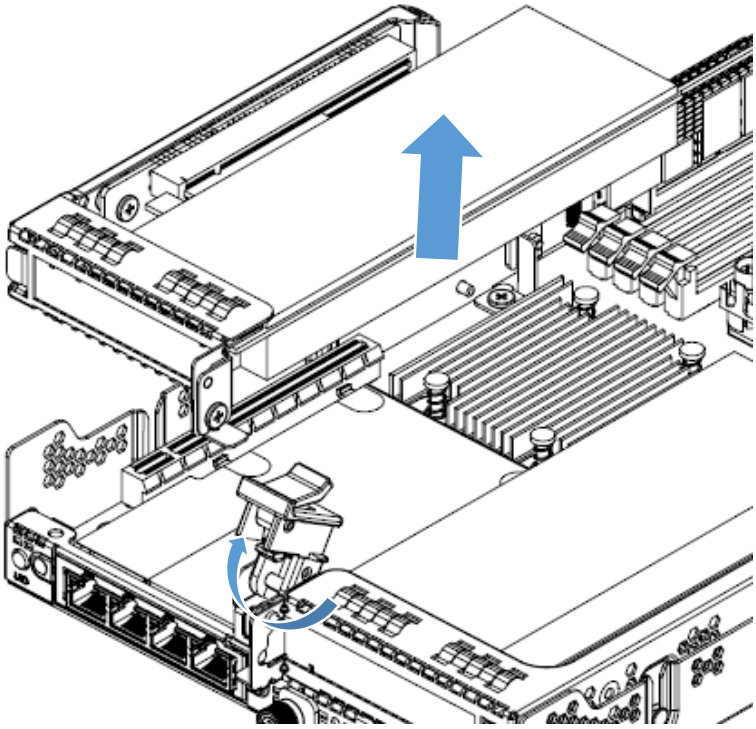


Figure 6-9

7. Remove the locking screw. Pull out the expansion board in the direction of the arrow, and replace it with a new one.

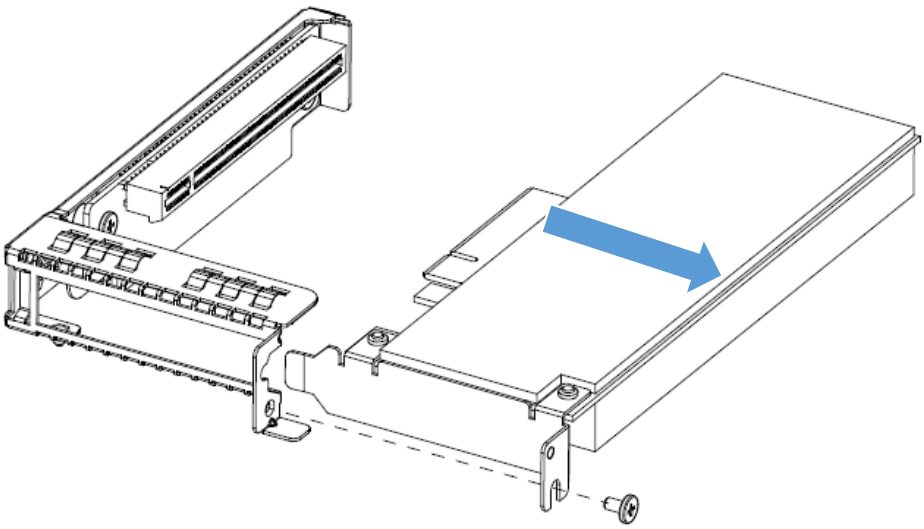


Figure 6-10

6.7 M.2 SSD 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, air baffle, or fan 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 corresponding node.
5. Remove the screw that secures the M.2 riser card to the motherboard, and remove the M.2 riser card vertically.

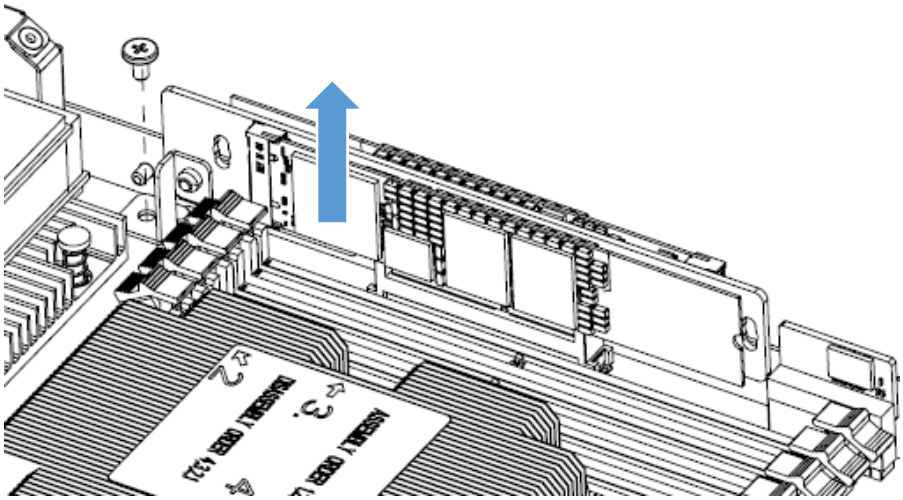


Figure 6-11

6. Remove the screw that secures the M.2 riser card to the bracket.

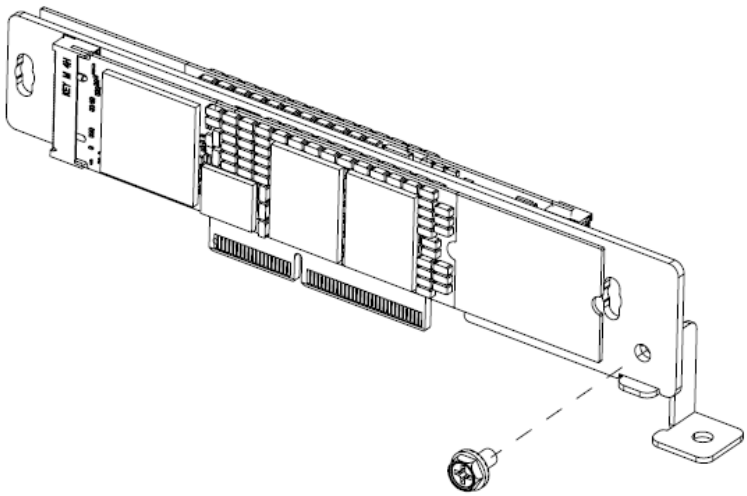


Figure 6-12

7. Open the fastener as shown below. Pull out the M.2 SSD in the direction of the arrow, and replace it with a new one.

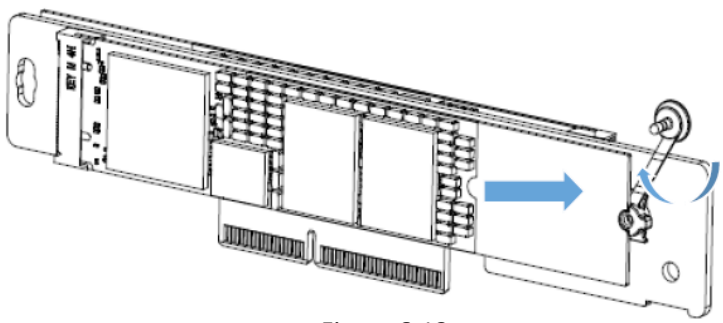


Figure 6-13

6.8 TPM Card 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, air baffle, or fan 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 corresponding node.
5. Remove the TPM card vertically, and replace it with a new one.

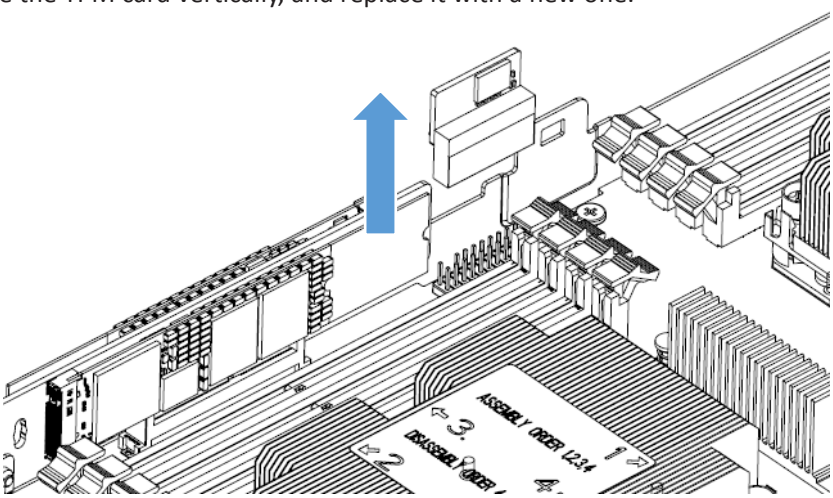


Figure 6-14

6.9 OCP/PHY Card 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, air baffle, or fan 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 corresponding node.
5. Remove the OCP/PHY card vertically, and replace it with a new one.

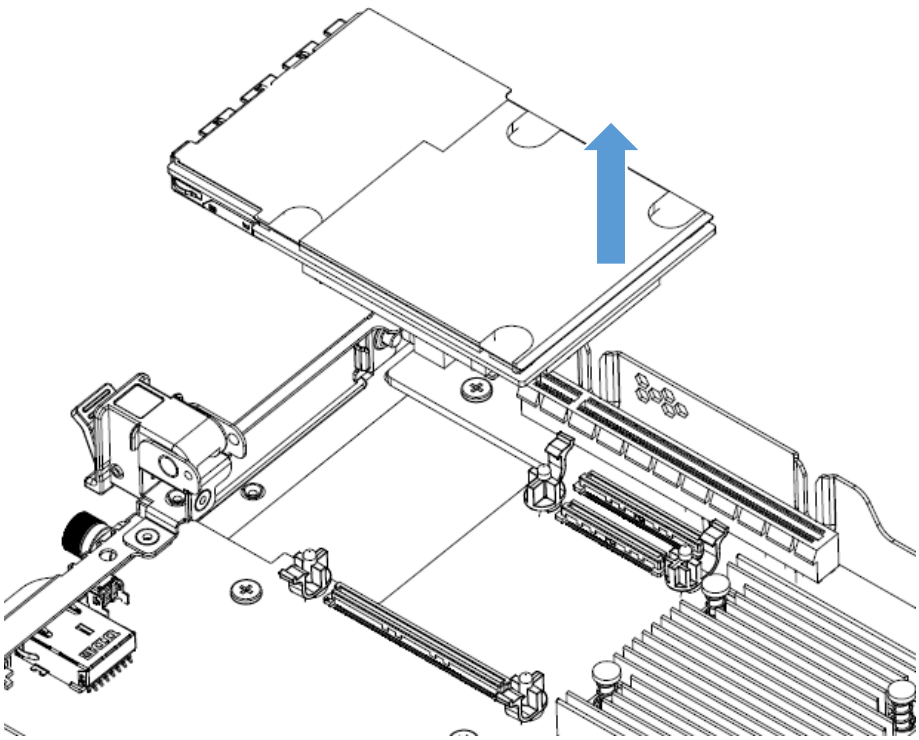


Figure 6-15

7 Cabling

Connect the cables between the power board and the HDD backplane as shown below

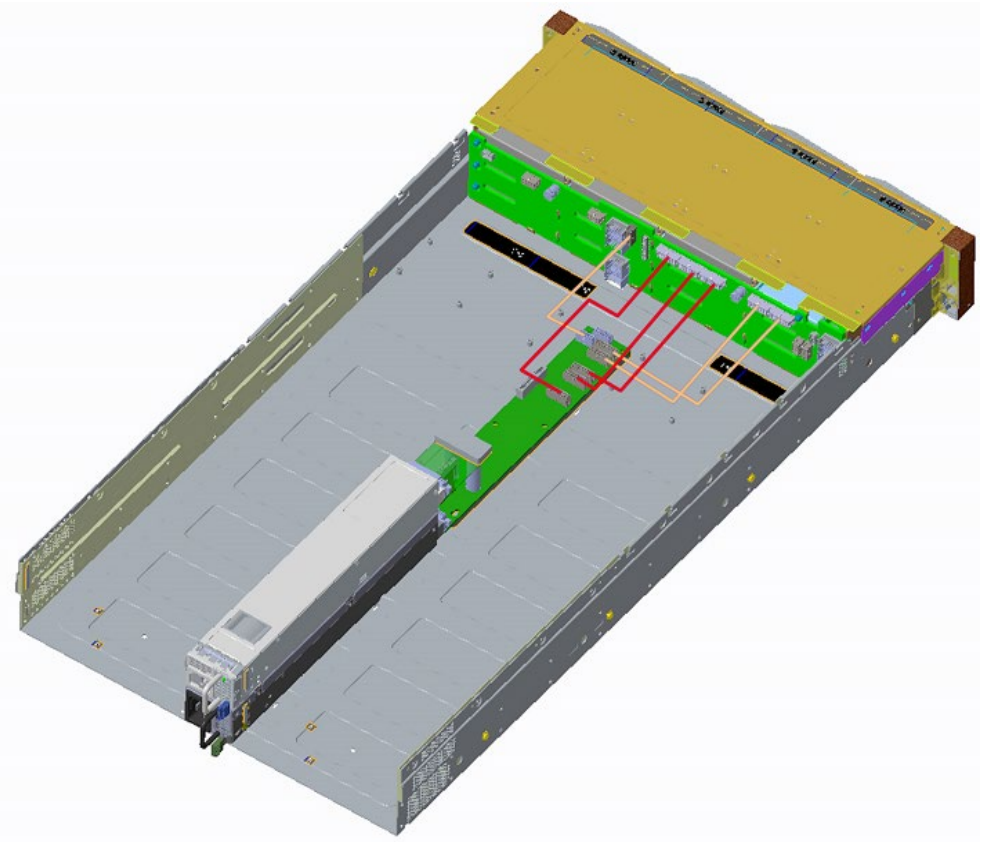


Figure 7-1

CAUTION: 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. If there is an exception, such as failure to boot, caused by changing the BIOS settings, users can try to recover it through the Clear CMOS operation.
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 the particular configuration 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 <DEL> to SETUP or <TAB> to POST 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 F2 to enter BIOS Setup interface.
- Press TAB to display the system information during POST.

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

Table 8-1 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
<Home> or <End>	Move the cursor to the top or bottom of the screen
<+> or <->	Select the previous or next numerical value or setting of the current one
<F1>	Help
<F2>	Restore to the last configuration
<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 sub-menu.

Figure 8-1

8.1.2 UEFI/Legacy Mode Switch

Login to the BIOS Setup interface, select "Advanced -> CSM Configuration". Press Enter, to set the Boot Mode (UEFI Mode/Legacy Mode). Set the Option ROM execution mode of

Network, Storage, Video OPROM Policy and Other PCI devices, as shown in the following figure.

At present, Inspur Purley platform servers are set to UEFI Mode by default. Compared with Legacy mode, UEFI mode has many advantages: it supports boot from the GPT disk bigger than 2.2T, supports IPv6/IPv4 PXE boot, and provides UEFI Shell environment. This option can be set according to customer's demand.

If the Boot Mode is set to Legacy Mode, the Option ROM execution mode of Network, Storage, Video OPROM Policy and Other PCI devices must be set to Legacy.

If the Boot Mode is set to UEFI Mode, the Option ROM execution mode of Network must be set to UEFI, and the Option ROM execution mode of Storage, Video OPROM Policy and Other PCI devices is suggested to set to UEFI. If there are special requirements, it can be set to Legacy.

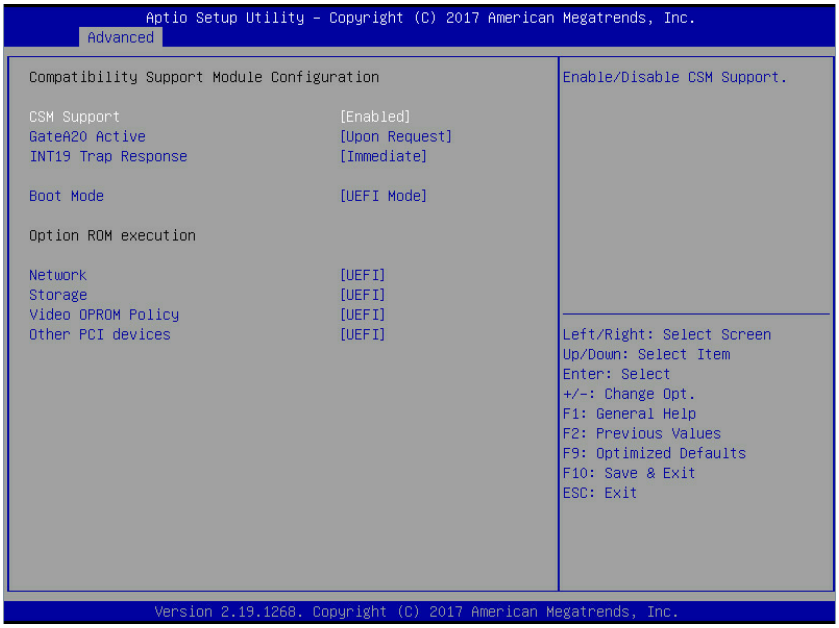


Figure 8-2

8.1.3 View System Information

Login to the BIOS Setup interface, and the Main menu displays the current system information, including BIOS/BMC/ME version, CPU/PCH SKU/RC version, memory and other information, as shown in the following figure.

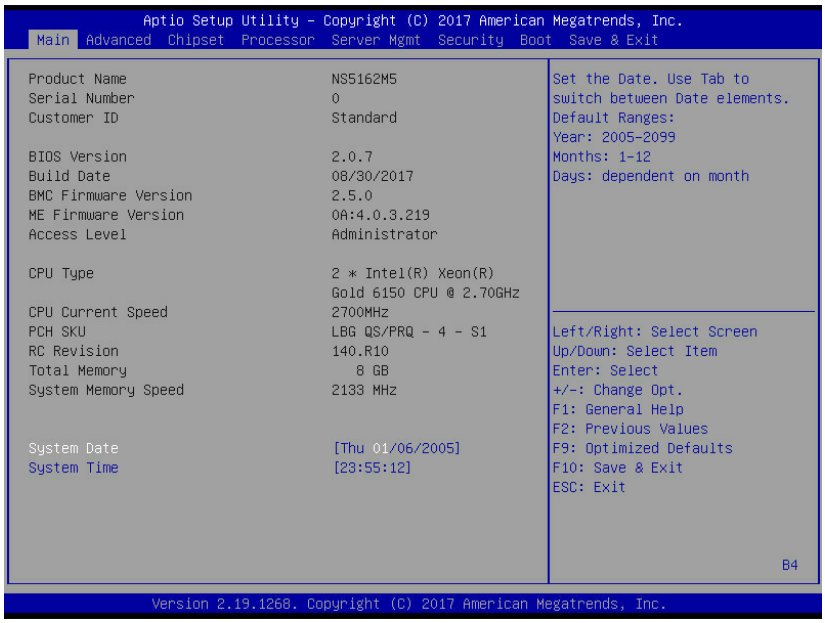


Figure 8-3

8.1.4 View CPU Information

Login to the BIOS interface, select “Processor -> Processor Configuration -> Processor Information”, and press Enter to display the CPU detailed information, as shown in the following figure.

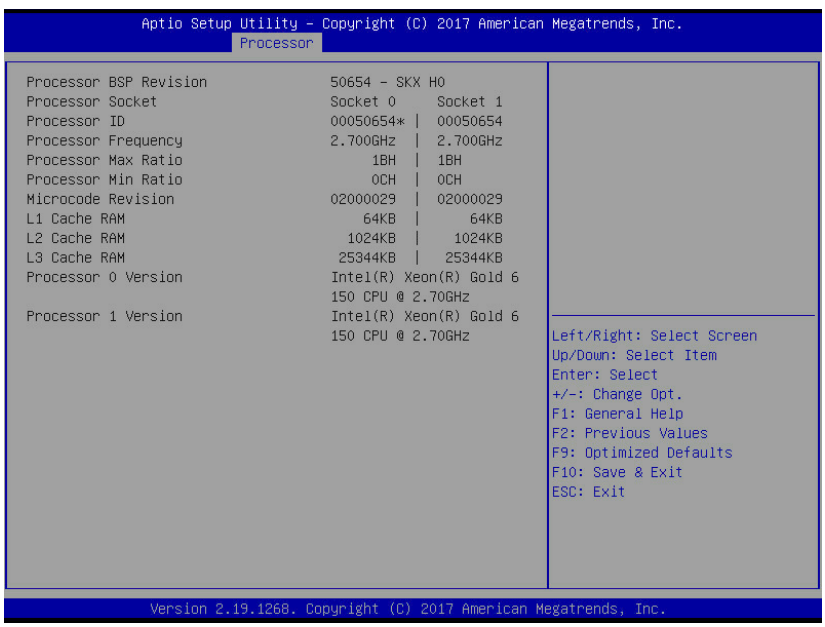


Figure 8-4

8.1.5 View Memory Information

Login to the BIOS interface, select “Processor -> Memory Configuration -> Memory Topology”, and press Enter to display the manufacturer, speed, capacity and other

information of the memories in position, as shown in the following figure.

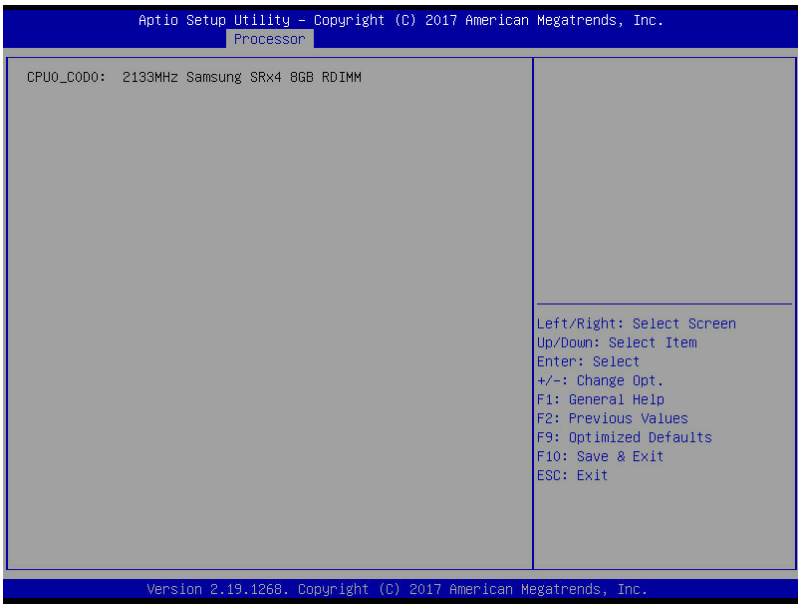


Figure 8-5

8.1.6 View HDD Information and RAID Configuration

8.1.6.1 View HDD Information

Login to the BIOS interface, select “Chipset -> PCH SATA Configuration/PCH sSATA Configuration”, and press Enter to display the HDD information of the current onboard SATA ports or sSATA ports, as shown in the following figures.

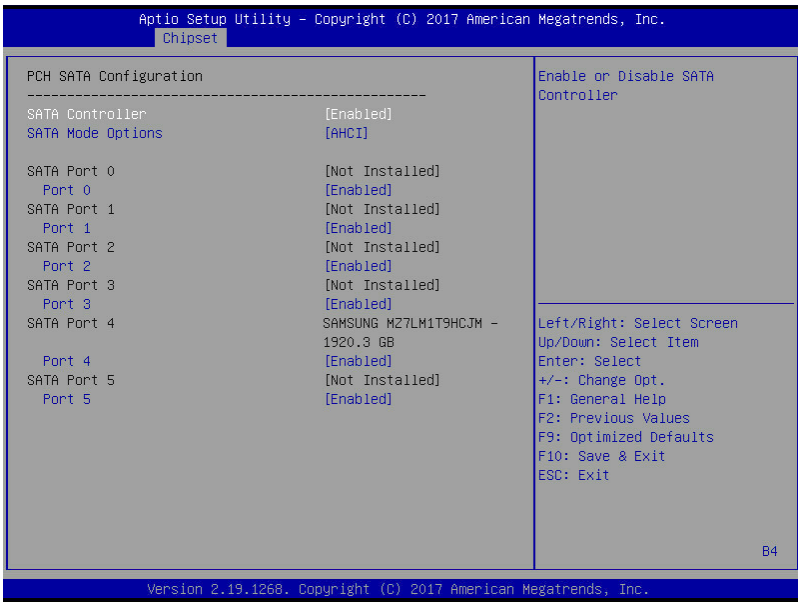


Figure 8-6

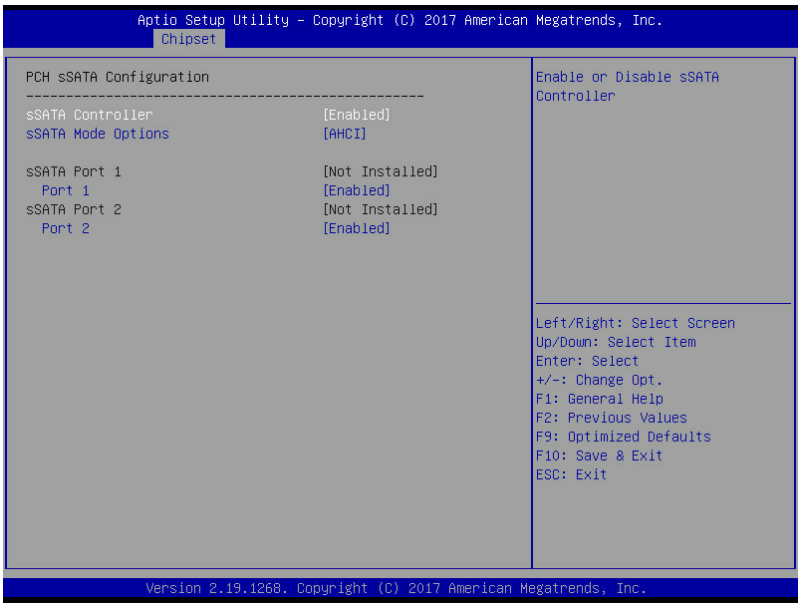


Figure 8-7

8.1.6.2 HDD RAID Mode Settings

1. Set the SATA Mode Option to [RAID], press F10 to save the setting, and the system reboots.
2. When Boot Mode is set to UEFI mode, in the BIOS Setup Advanced interface, there will be the Intel(R) RSTe SATA Controller menu, as shown in the following figure.

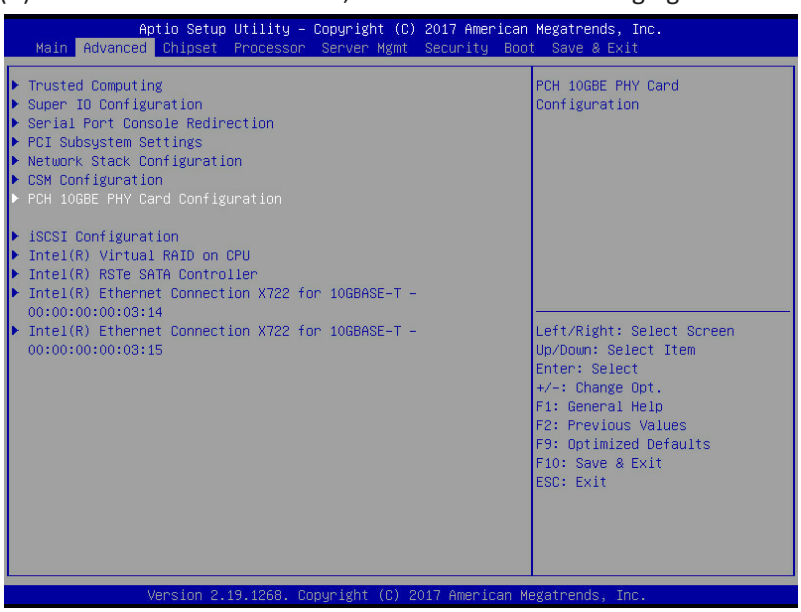


Figure 8-8

2.1 Press Enter, the executable operation and the current HDD information will be displayed, as shown in the following figure.

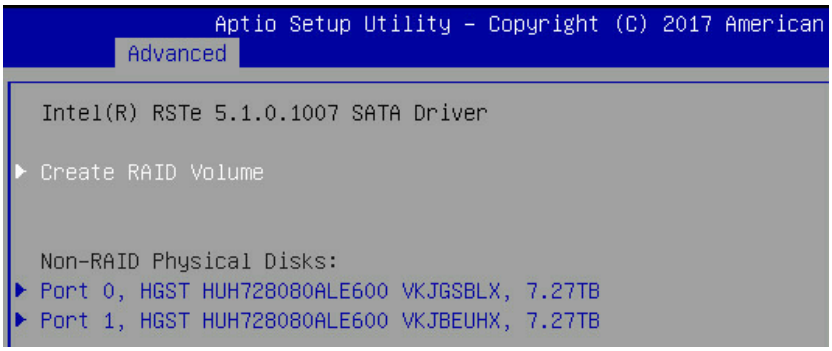


Figure 8-9

2.2 Create RAID volume. Select Create RAID Volume option, and press Enter, as shown in the following figure.

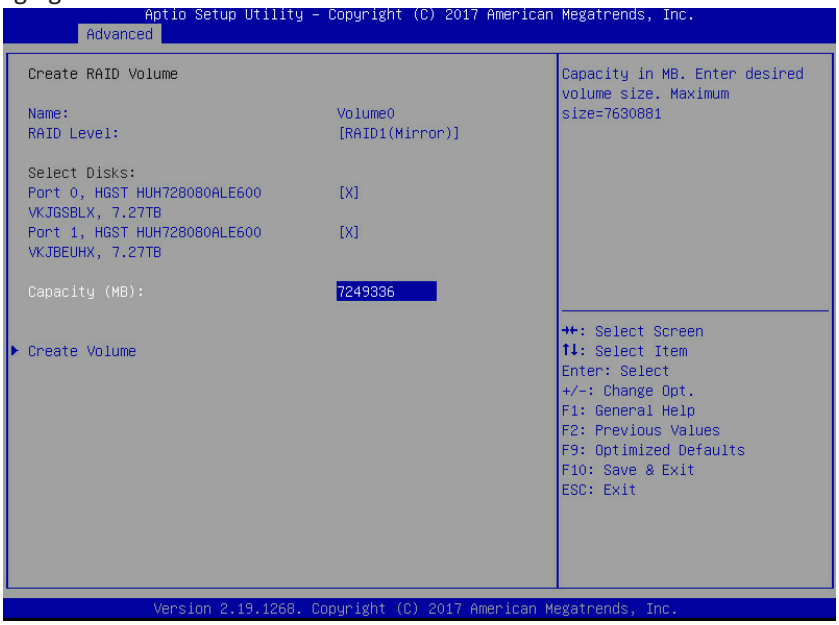


Figure 8-10

Table 8-2 Create RAID Menu Instruction Table

Interface Parameters	Function Description
Name	Please enter a volume name less than 16 characters without containing any special characters.
RAID Level	Please select the 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 the 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, and the maximum capacity is shown in the Help information on the right side.
Create Volume	After finishing the above settings, select this option to create RAID volume.

2.3 Delete RAID volume. Select a created RAID Volume, press Enter. Select “Delete”, there will be a prompt. To delete the volume, select “Yes” and press Enter; to cancel the deletion, select “No” and press Enter.

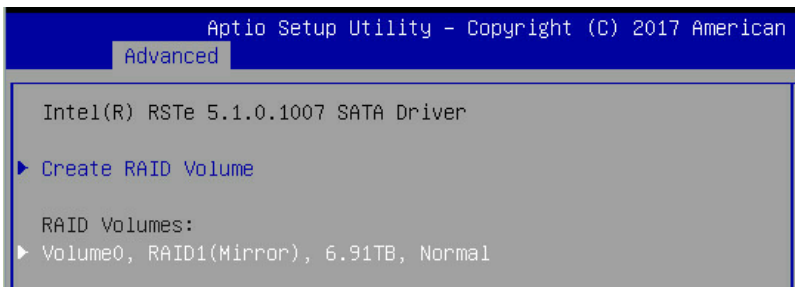


Figure 8-11

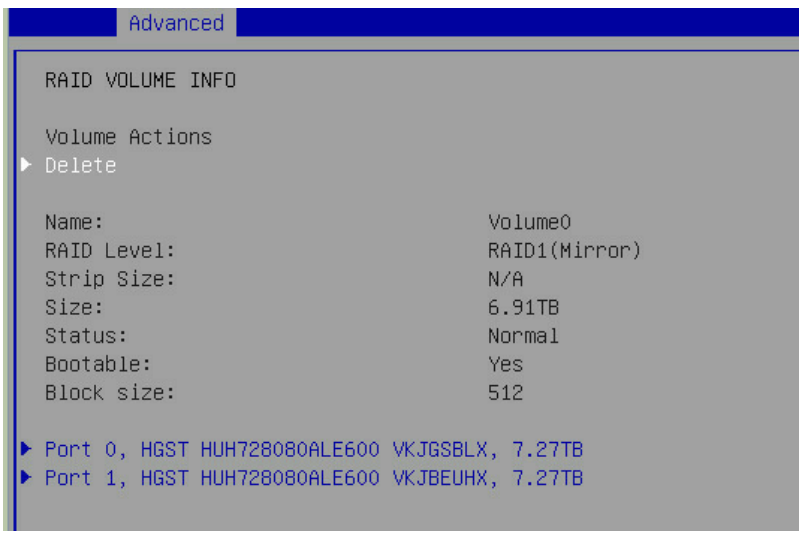


Figure 8-12

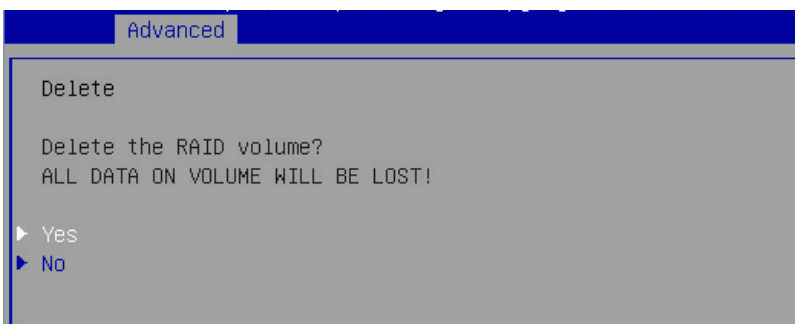


Figure 8-13

3. When Boot Mode is set to Legacy, a prompt “Press <CTRL-I> to enter Configuration Utility…” will appear on the screen during system booting. Press [Ctrl] and [I] keys at the same time to enter SATA RAID configuration, as shown in the following figure.

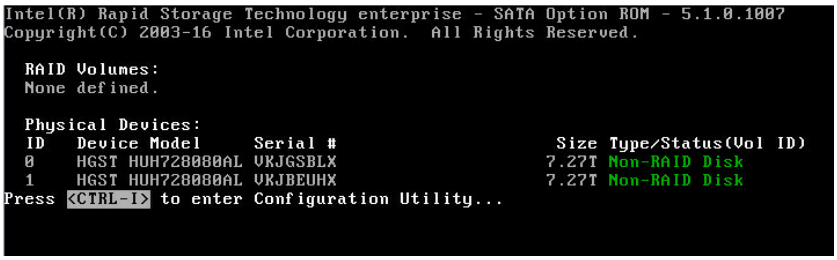


Figure 8-14

3.1 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.

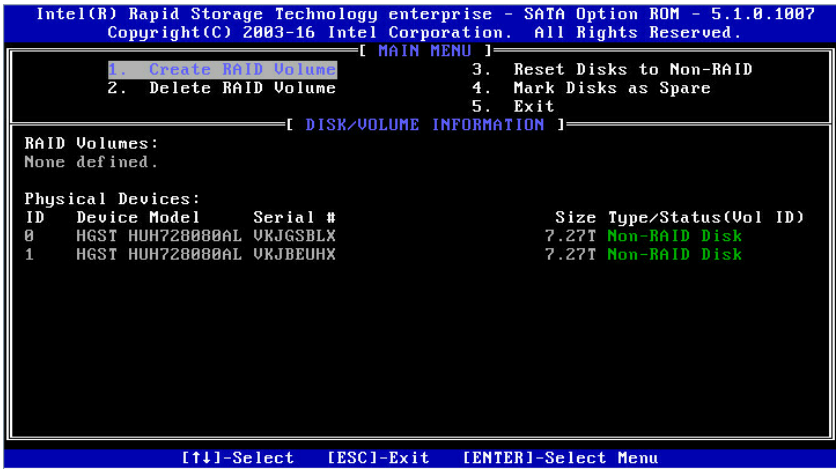


Figure 8-15

Table 8-3 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 sub-menu.

Table 8-4 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 HostRAID configuration interface.

3.2 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:

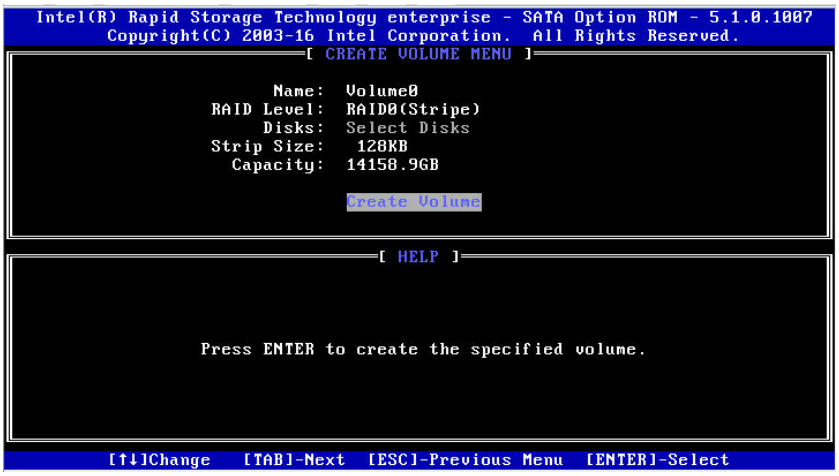


Figure 8-16

Table 8-5 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.

3.3 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”.

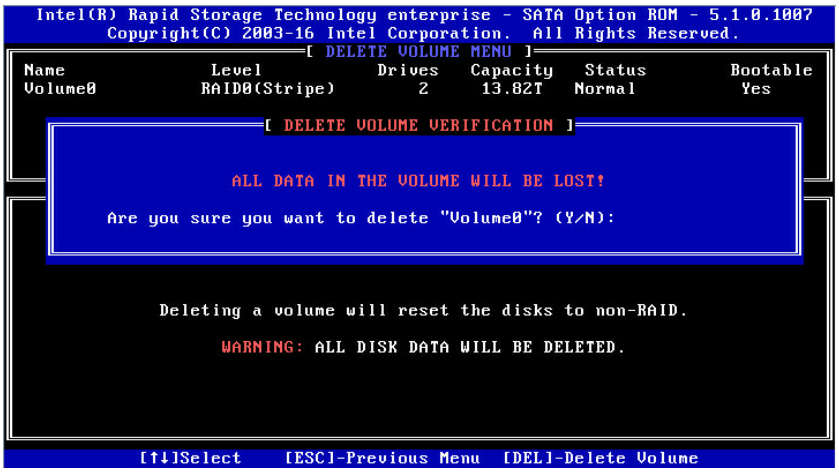


Figure 8-17

3.4 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.

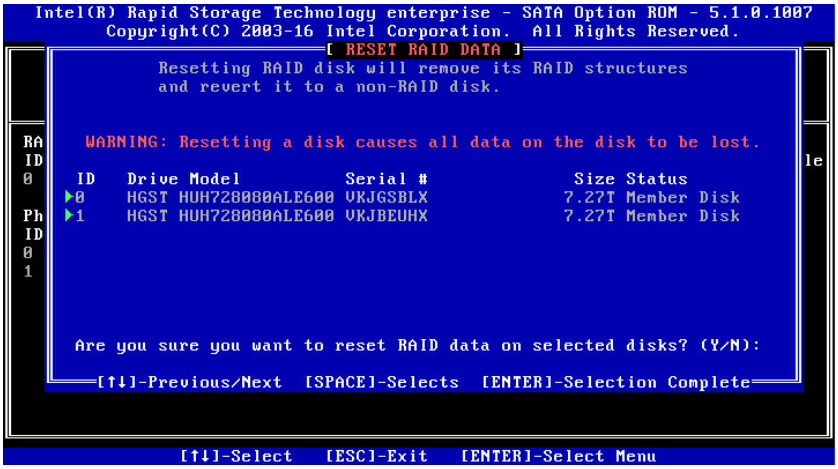


Figure 8-18

3.5 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.

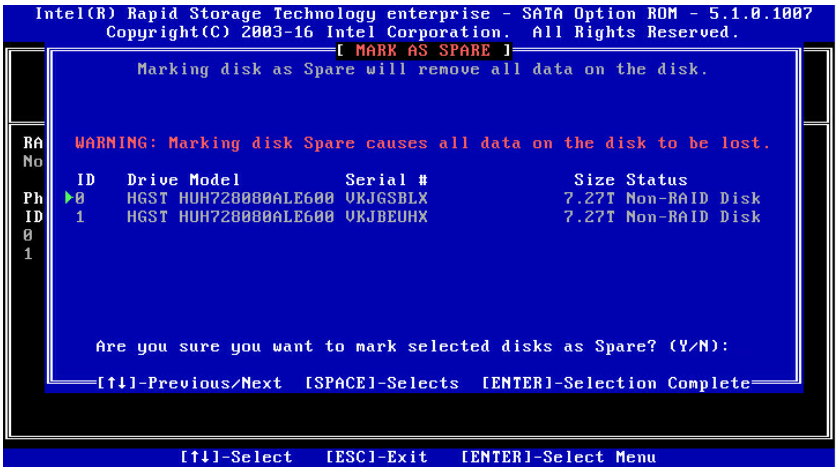


Figure 8-19

3.6 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.

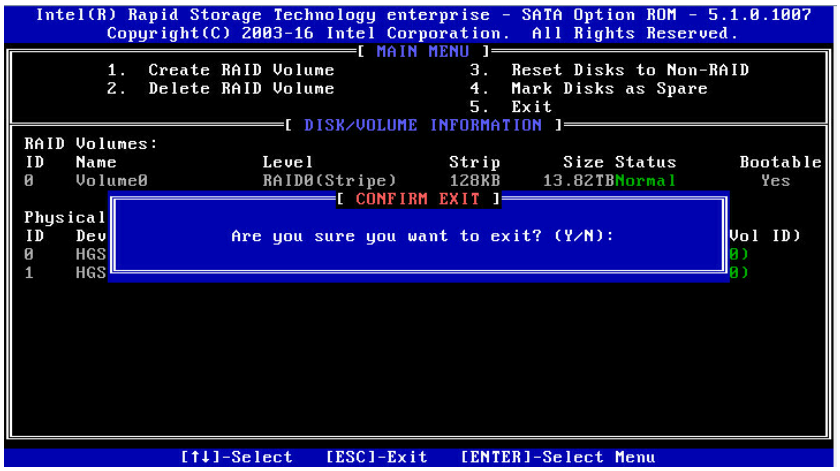


Figure 8-20

8.1.7 View and Set BMC Network Parameters

8.1.7.1 View BMC Network Parameters

Login to the BIOS interface, select “Server Mgmt -> BMC Network Configuration -> BMC IPv4 Network Configuration/BMC IPv6 Network Configuration”. Press Enter to view the current configuration of BMC IPv4 and BMC IPv6 network, as shown in the following figures.

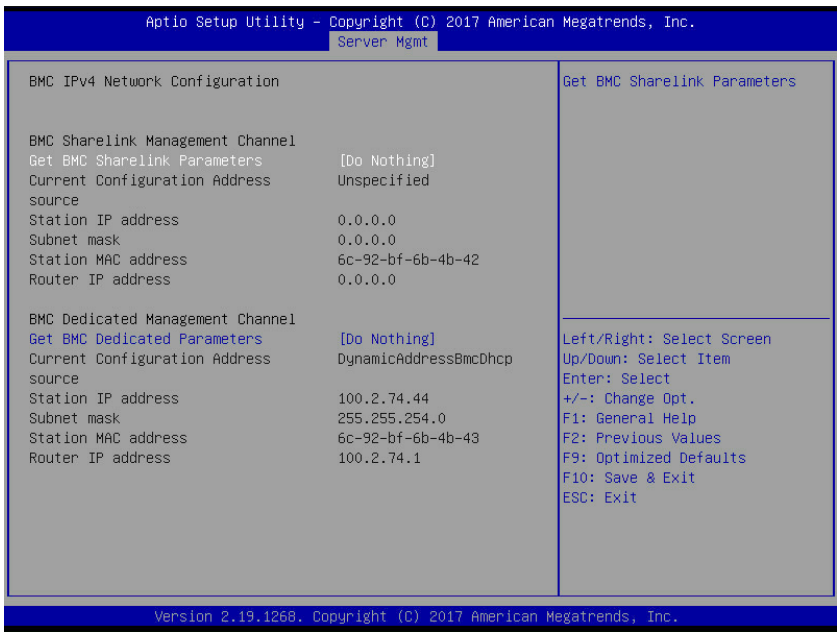


Figure 8-21

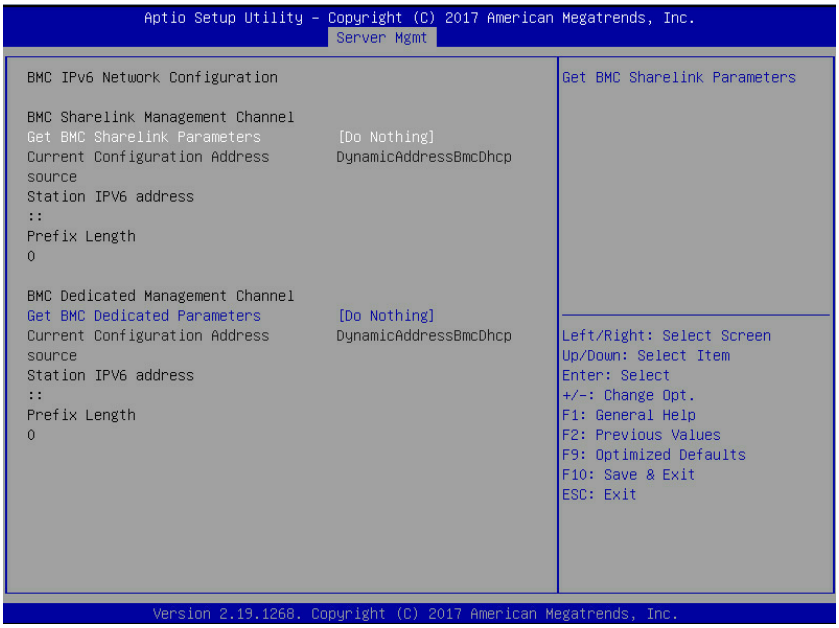


Figure 8-22

8.1.7.2 BMC Network Settings

Take BMC Sharelink port as an example to introduce the settings of BMC IPv4 network parameters, as shown in the following table.

Table 8-6 BMC Network Configuration Instruction Table

Interface Parameters	Function Description	Default Value
Get BMC Sharelink /Dedicated Parameters	Set the way to get BMC network parameters, options include: Do Nothing Auto Manual	Do Nothing
Configuration Address Source	Configure BMC network status parameters. When Get BMC Dedicated Parameters is set to [Manual], this option will be displayed. Options include: Unspecified Static DynamicBmcDhcp The static and dynamic settings take effect immediately.	Unspecified
Current Configuration Address	Display the current BMC network parameters configuration	----
Station IP address	BMC station IP address	----
Subnet mask	Subnet mask	----
Station MAC address	BMC station MAC address	----
Router IP address	BMC router IP address	----

8.1.7.3 Set BMC Static Network Parameters

Set the Configuration Address Source option to [Static]. If the setting succeeds, the system

will prompt “Set Static BMC IP Address Source Success!!”, as shown in the following figure.

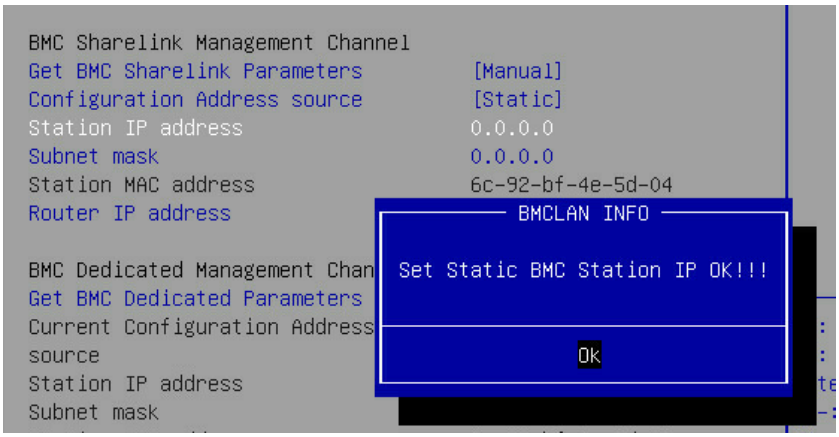


Figure 8-23

Select the Station IP Address option. Press Enter, the Station IP Address window pops up. Input the Static IP manually. After the setting is complete, press Enter to confirm, as shown in the following figures:

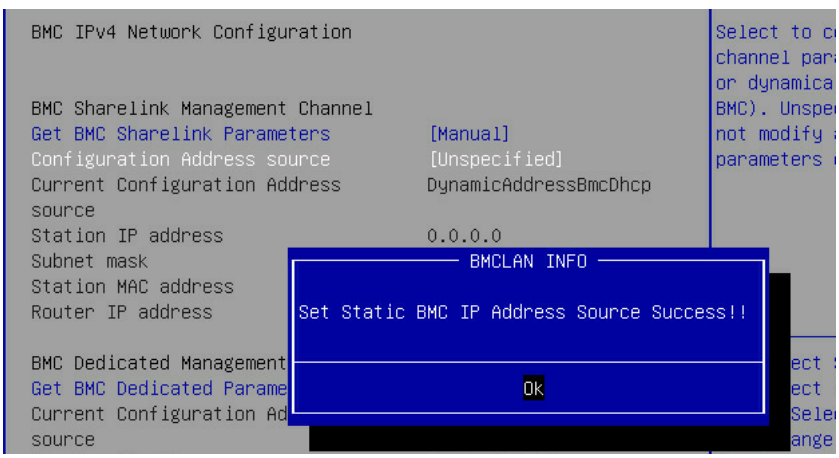


Figure 8-24

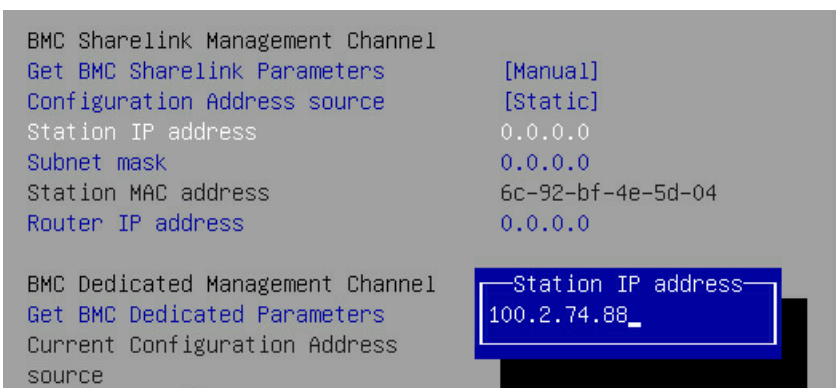


Figure 8-25

If the setting succeeds, the system prompts “Set Static BMC Station IP OK!!!” Press Enter to confirm, and the IP will take effect immediately.

If the setting fails, the system prompts “Set Static BMC Station IP Fail!!!”

If the IP does not change, the system prompts “Static BMC Station IP Not Change!!!”

If the input IP is invalid, the system prompts “Invalid Station IP Entered!!!”, and assign 0.0.0.0 to the IP address. The assignment only changes the IP address in BIOS Setup interface, and does not notify BMC to change the IP settings.

The prompts of Subnet mask and Router IP address settings are similar to those of Station IP address setting, there is no more detailed description here. As shown in the following figure, the BMC network parameters have taken effect, you can login to BMC Web interface to operate.

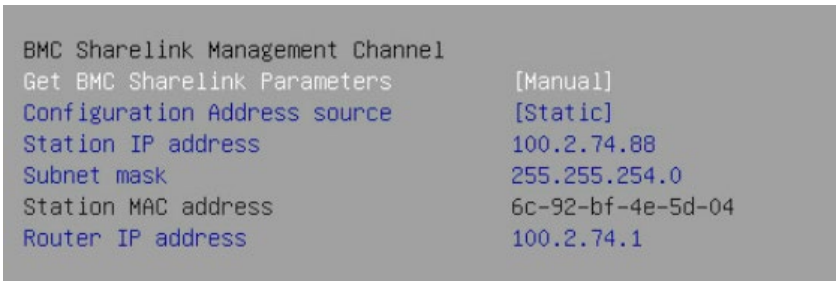


Figure 8-26

8.1.7.4 Set BMC Dynamic Network Parameters

Set the Configuration Address Source option to [DynamiBmcDhcp]. If the setting succeeds, the system will prompt “Set Dynamic BMC IP Address Source Success! Dynamic BMC Network Parameters are Getting Now, Please Wait a Moment!”, as shown in the following figure.

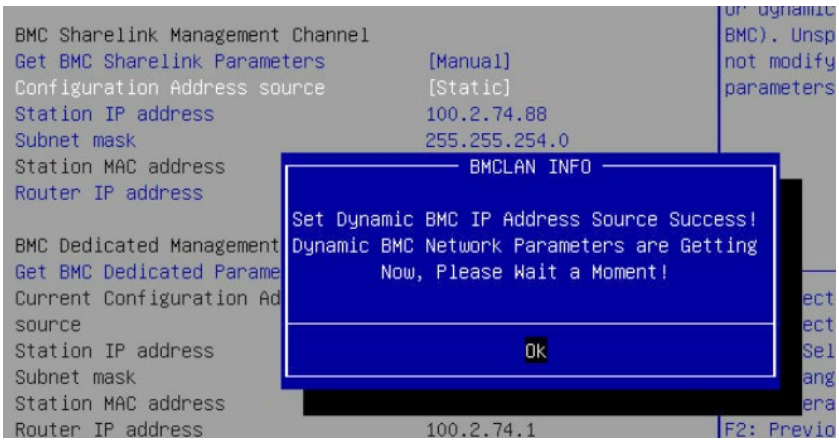


Figure 8-27

After pressing Enter to confirm, the following interface will stay for 30s, please wait patiently.

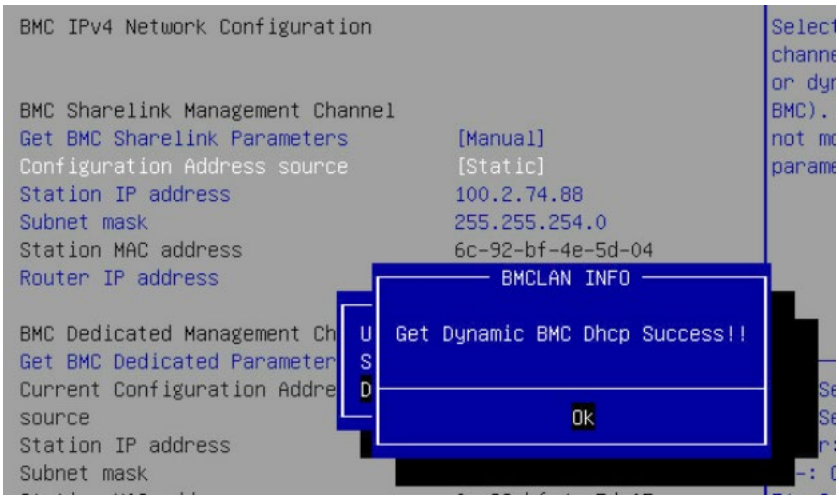


Figure 8-28

After the dynamic network takes effect, the system will prompt “Get Dynamic BMC Dhcp Success!!”, and the interface will be shown as the following figure.

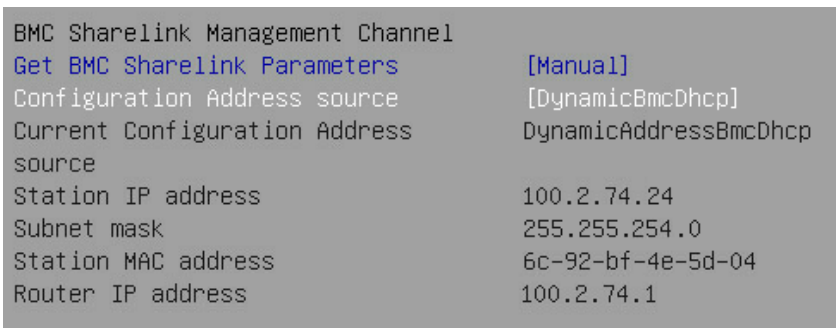


Figure 8-29

Note:

Please make sure that the BMC management port is connected to the network when you use the Manual setting options.

The options that take effect immediately in the BIOS Setup interface are implemented by calling the Callback function. Callback functions are only called when the options in the BIOS Setup interface are changed. Otherwise, the function will not take effect. For example, if you want to automatically get BMC parameters again, you need to set Get BMC Sharelink Parameters to [Do nothing] or [Manual], then set to [Auto], the function will take effect. The settings of BMC IPv6 network parameters are similar to this, which will be omitted here.

8.2 BIOS Parameter Description

8.2.1 Main

Main interface displays the basic information of BIOS system, including BIOS/BMC/ME version, CPU type, total memory capacity and system time.

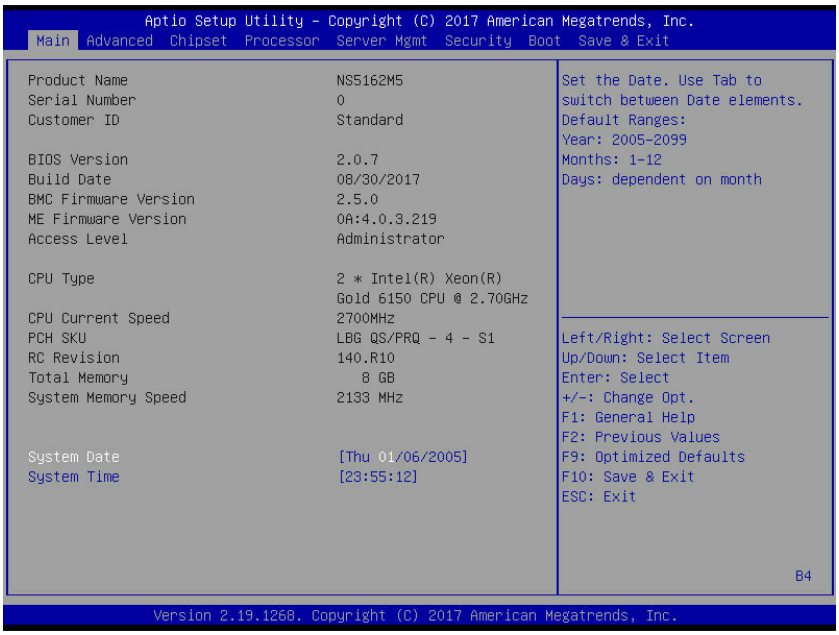


Figure 8-30

Table 8-7 Main Interface Instruction Table

Interface Parameters	**Function Description**
Product Name	Product name
Serial Number	Serial number
Customer ID	Customer ID
BIOS Version	BIOS version
Build Date	Build date
BMC Firmware Version	BMC Firmware version
ME Firmware Version	ME Firmware version
Access Level	Current access level
CPU Information	Display the current CPU's type, PCH SKU, RC version information.
Memory Information	Display the current total memory capacity and frequency information.
System Date (Day mm/dd/yyyy)	Display and set system date. Use [Tab] or [Enter] key to switch between system date and time, directly input the value or use +/- keys to change the value (Press + key, the value increases by 1, and press – key, the value decreases by 1).
System Time (hh/mm/ss)	Display and set system time. Use [Tab] or [Enter] key to switch between system date and time, directly input the value or use +/- keys to change the value (Press + key, the value increases by 1, and press – key, the value decreases by 1).

8.2.2 Advanced

Advanced interface includes the BIOS system parameters and related function settings, such as ACPI, serial port, PCI subsystem, CSM, USB, onboard NIC and so on.

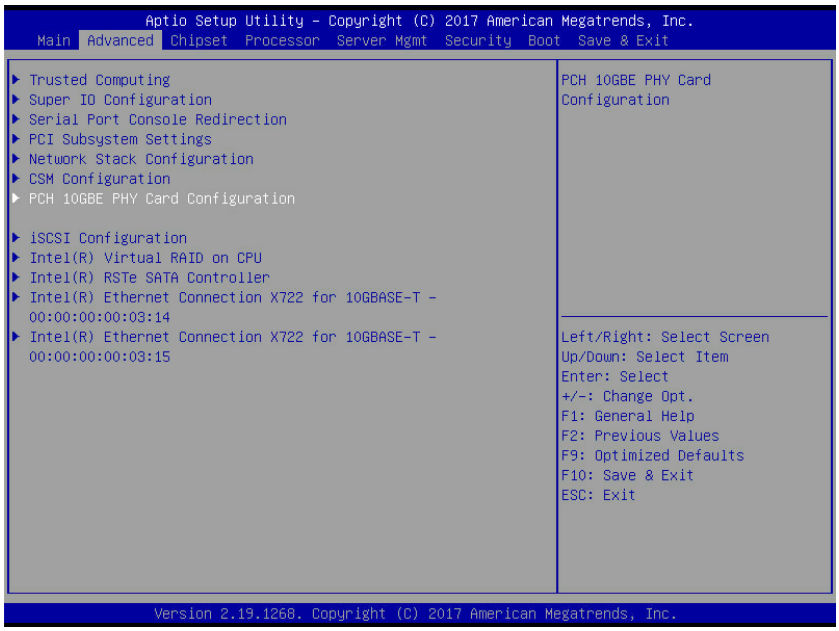


Figure 8-31

Table 8-8 Advanced Interface Instruction Table

Interface Parameters	**Function Description**
Trusted Computing	Trusted computing configuration
Super IO Configuration	AST2500 I/O chip parameter configuration
Serial Port Console Redirection	Serial port console redirection settings
PCI Subsystem Settings	PCI subsystem settings
Network Stack Configuration	Network stack configuration
CSM Configuration	CSM configuration
PCH 10GBE PHY Card Configuration	PCH 10GBE PHY card configuration
iSCSI Configuration	iSCSI configuration
Intel(R) Virtual RAID on CPU	Intel NVMe virtual RAID configuration
Intel® Enthernet Connection X722 for 10GbE SFP+XX:XX:XX:XX:XX:XX	Intel 10G NIC UEFI OPROM configuration

8.2.2.1 Trusted Computing

Trusted Computing interface is used to enable or disable BIOS support for security device.

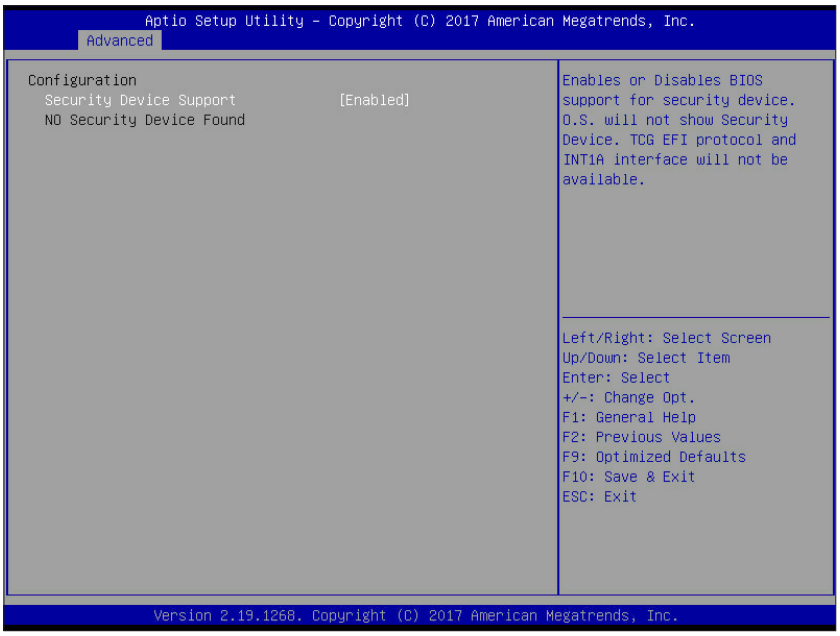


Figure 8-32

Table 8-9 Trusted Computing Interface Instruction Table

Interface Parameters	Function Description	Default Value
Security Device Support	Security device support settings. Options include: Enabled Disabled BIOS supports TPM TCG version 1.2/2.0. BIOS supports TPM module through TPM software binding, when the verification of software binding fails, BIOS will record the error to SEL.	Enabled
No Security Device Found	Display the status of security device. There is no information displayed at present, to enable this function, it needs to install TPM chip.	----

8.2.2.2 Super IO Configuration

Super IO Configuration interface is used to set the options related with I/O chip.

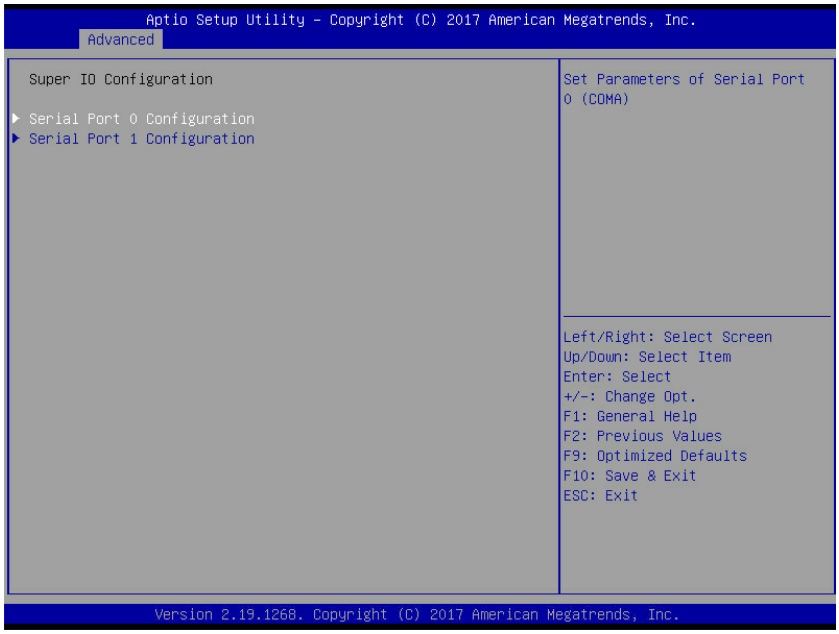


Figure 8-33

Table 8-10 Super IO Configuration Interface Instruction Table

Interface Parameters	Function Description
Serial Port 0 Configuration	Serial port 0 configuration, the configuration interface provides this serial port's on-off control and resource allocation control. Users can manually adjust the IO PORT and IRQ number that COM PORT uses.
Serial Port 1 Configuration	Serial port 1 configuration

8.2.2.3 Serial Port 0 Configuration

Serial Port 0 Configuration interface is used to set the options related with serial port 0.

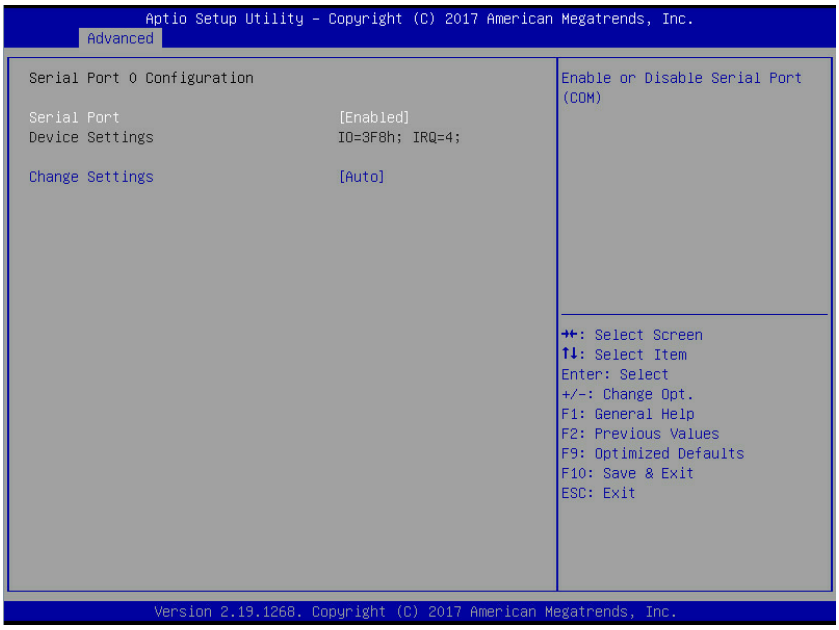


Figure 8-34

Table 8-11 Serial Port 0 Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Serial Port	Serial port 0 on-off settings. Options include: Enabled Disabled	Enabled
Change Settings	Select the optimal setting according to the demand. Options include: Auto I0=3F8h; IRQ=4; I0=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; I0=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; I0=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	Auto

8.2.2.4 Serial Port Console Redirection

Serial Port Console Redirection interface is used to set the options related with the serial port redirection.

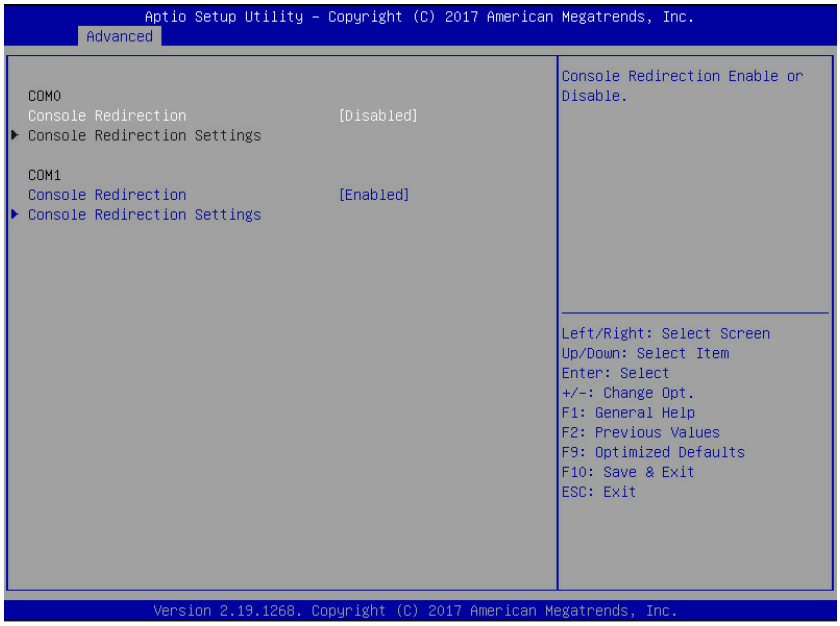


Figure 8-35

Table 8-12 Serial Port Console Redirection Interface Instruction Table

Interface Parameters	Function Description	Default Value
Console Redirection	Serial port console redirection on-off settings. Options include: Enabled Disabled	Disabled
Console Redirection Settings	Serial port console redirection parameter settings	----

8.2.2.5 Console Redirection Settings

When the Console Redirection is set to [Enabled], the Console Redirection Settings menu will be opened.

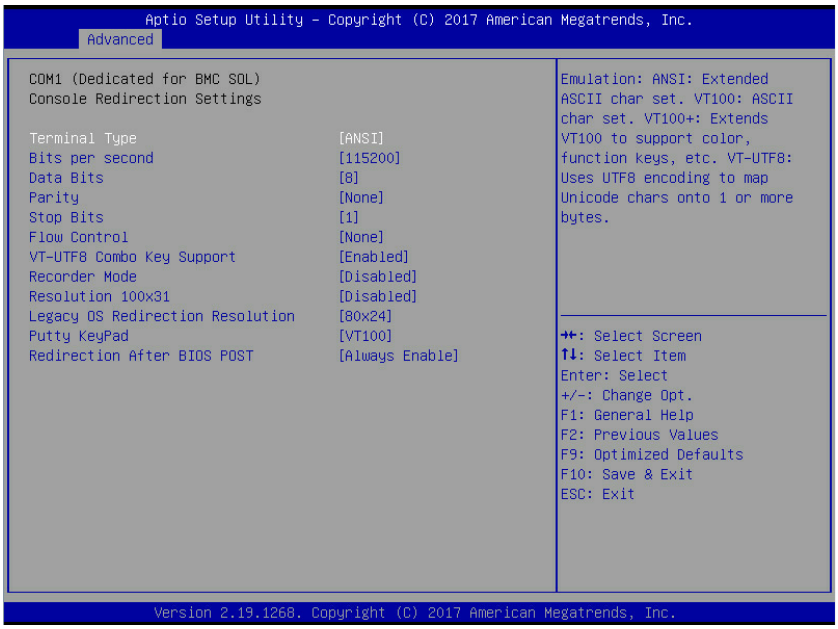


Figure 8-36

Table 8-13 Console Redirection Settings Interface Instruction Table

Interface Parameters	Function Description	Default Value
Terminal Type	Terminal type settings. Options include: VT100 VT100+ VT-UTF8 ANSI	ANSI
Bits per second	Baud rate settings. Options include: 9600 19200 38400 57600 115200	115200
Data Bits	Serial port data width settings. Options include: 7 8	8
Parity	Parity settings. Options include: None Even Odd Mark (odd-even check) Space (storage parity check)	None
Stop Bits	Stop bit settings. Options include: 1 2	1
Flow Control	Flow control settings. Options include: None Hardware RTS/CTS	None
VT-UTF8 Combo Key Support	VT-UTF8 combination key support on-off settings. Options include: Enabled Disabled	Enabled

Recorder Mode	Recorder mode on-off settings. Options include: Enabled Disabled	Disabled
Redirection 100×31	Expanded redirection resolution 100×31 on-off settings. Options include: Enabled Disabled	Disabled
Legacy OS Redirection Resolution	Legacy OS redirection resolution settings. Options include: 80×24 80×25	80×24
Putty KeyPad	Putty function keys and keyboard settings. Options include: VT100 LINUX XTERMR6 SCO ESCN VT400	VT100
Redirection After BIOS POST	Redirection after BIOS POST settings. Options include: Always Enable BootLoader	Always Enable

8.2.2.6 PCI Subsystem Settings

PCI Subsystem Settings interface is used to set the options related with PCI subsystem.

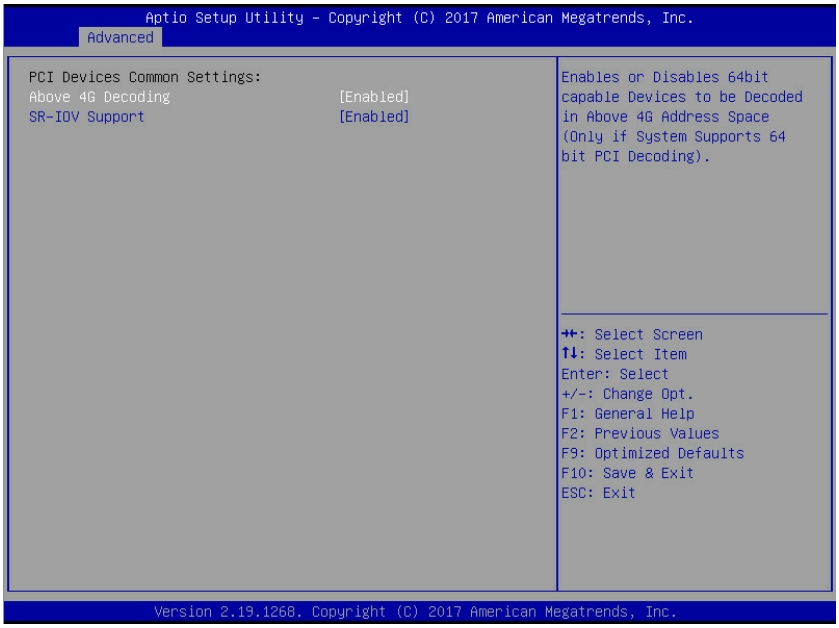


Figure 8-37

Table 8-14 PCI Subsystem Settings Interface Instruction Table

Interface Parameters	Function Description	Default Value
Above 4G Decoding	Above 4G memory access control on-off settings. Options include: Enabled Disabled	Enabled
SR-IOV Support	SR-IOV support on-off settings. Options include: Enabled Disabled	Enabled

8.2.2.7 Network Stack Configuration

Network Stack Configuration interface is used to set the options related with Network UEFI PXE.

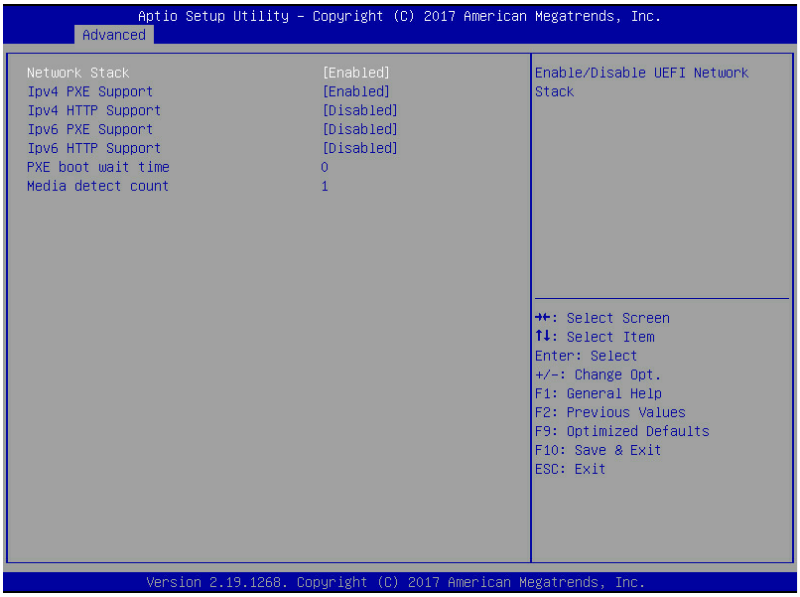


Figure 8-38

Table 8-15 Network Stack Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Network Stack	Network stack on-off settings. Options include: Enabled Disabled Only this option is enabled, the following options can be displayed and the functions can be set.	Enabled
Ipv4 PXE Support	UEFI Ipv4 PXE support on-off settings. Options include: Enabled Disabled	Enabled
Ipv4 HTTP Support	Ipv4 HTTP support on-off settings. Options include: Enabled Disabled	Disabled
Ipv6 PXE Support	UEFI Ipv6 PXE support on-off settings. Options include: Enabled Disabled	Disabled
Ipv6 HTTP Support	Ipv6 HTTP support on-off settings. Options include: Enabled Disabled	Disabled
PXE boot wait time	Set the wait time to cancel PXE boot after pressing ESC key, the setting range is 0~5.	0
Media detect count	Device detect count settings, the setting range is 1~50.	1

8.2.2.8 CSM Configuration

CSM Configuration interface is used to set the options related with the compatibility support module.

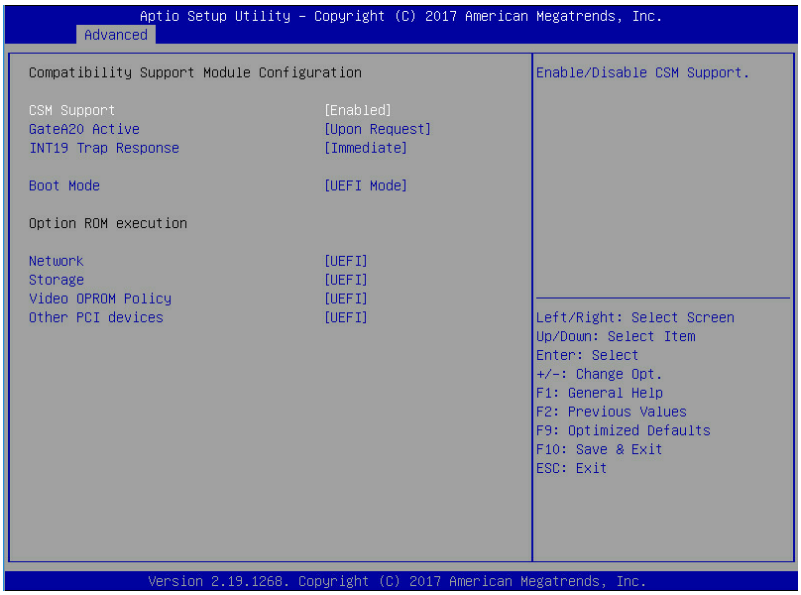


Figure 8-39

Table 8-16 CSM Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
CSM Support	CSM support on-off settings. Options include: Enabled Disabled	Disabled
GateA20 Active	A20 line control mode settings. Options include: Upon Request Always A20 is an address line, which controls the system how to access the memory space larger than 1MB.	Upon Request
INT19 Trap Response	Interrupt/Capture signal response settings. Options include: Immediate Postponed	Immediate
Boot Mode	Boot mode settings. Options include: UEFI Mode Legacy Mode	UEFI Mode
Network	NIC Option ROM execution mode settings. Options include: Do not launch Legacy UEFI	UEFI
Storage	Storage device Option ROM execution mode settings. Options include: Do not launch Legacy UEFI	UEFI
Video OPROM Policy	Video device Option ROM execution mode settings. Options include: Do not launch Legacy UEFI	UEFI
Other PCI devices	Other PCI devices Option ROM execution mode settings. Options include: Do not launch Legacy UEFI	UEFI

8.2.2.9 PCH 10GBE PHY Card Configuration

PCH 10GBE PHY Card Configuration interface is used to set the PCH 10GBE PHY Card PXE OPROM options.

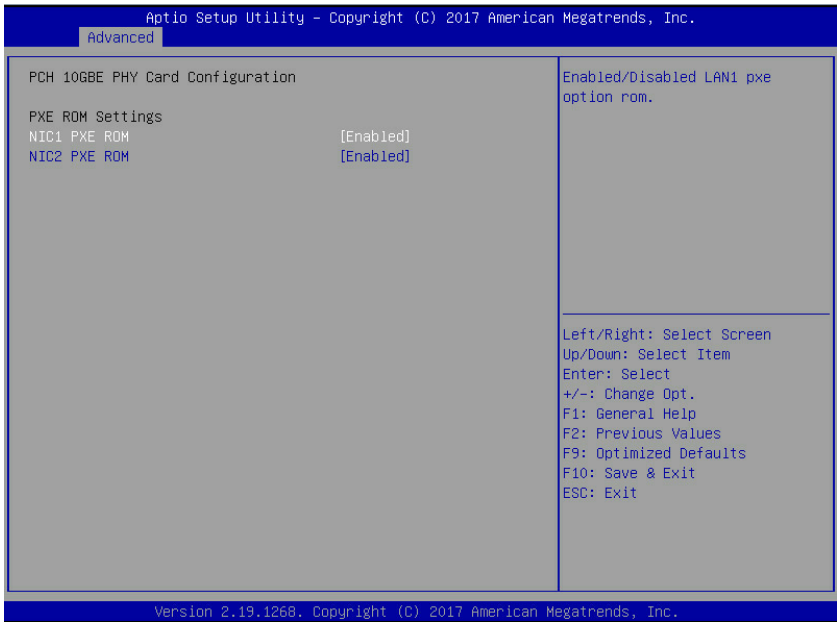


Figure 8-40

Table 8-17 PCH 10GBE PHY Card Configuration Instruction Table

Interface Parameters	Function Description	Default Value
NIC PXE ROM	PCH 10GBE PHY Card PXE ROM on-off settings. Options include: Enabled Disabled	Enabled

8.2.3 Chipset

Chipset interface includes the information settings and runtime error logging settings of PCH SATA/sSATA, USB and ME devices.

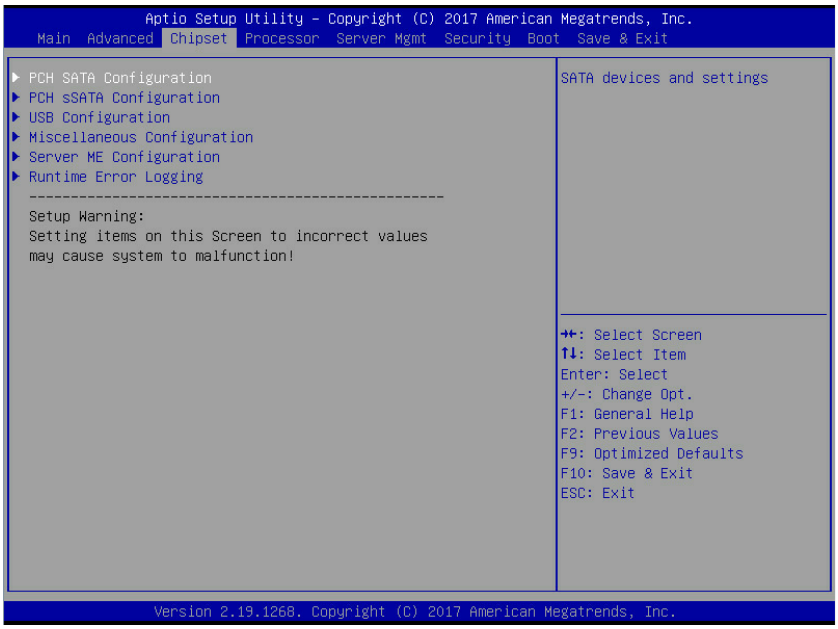


Figure 8-41

Table 8-18 Chipset Interface Instruction Table

Interface Parameters	**Function Description**
PCH SATA Configuration	PCH SATA configuration
PCH sSATA Configuration	PCH sSATA configuration
USB Configuration	USB configuration
Miscellaneous Configuration	Miscellaneous configuration
Server ME Configuration	Server ME configuration
Runtime Error Logging	Runtime error logging

8.2.3.1 PCH SATA Configuration/PCH sSATA Configuration

PCH sSATA Configuration and PCH SATA Configuration interfaces are used to set the options related with the onboard sSATA/SATA ports. Take PCH SATA Configuration menu as an example, as shown in the following figure.

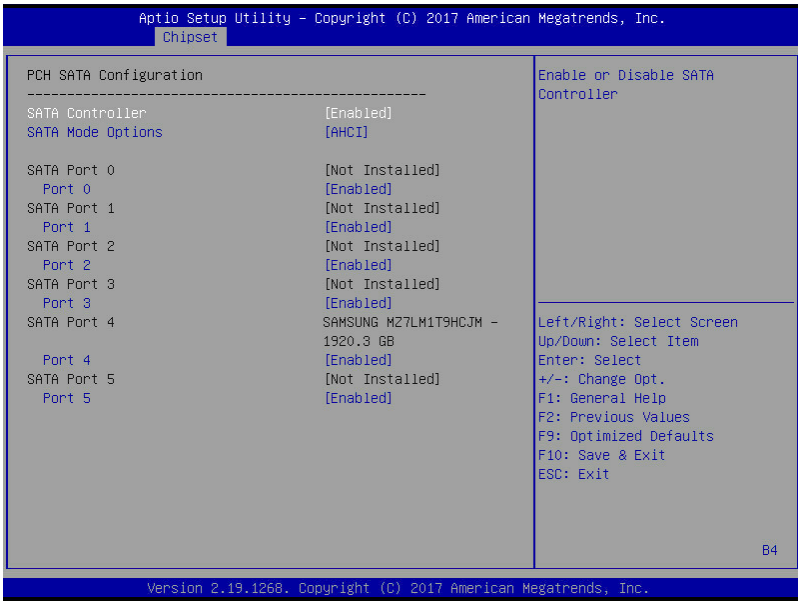


Figure 8-42

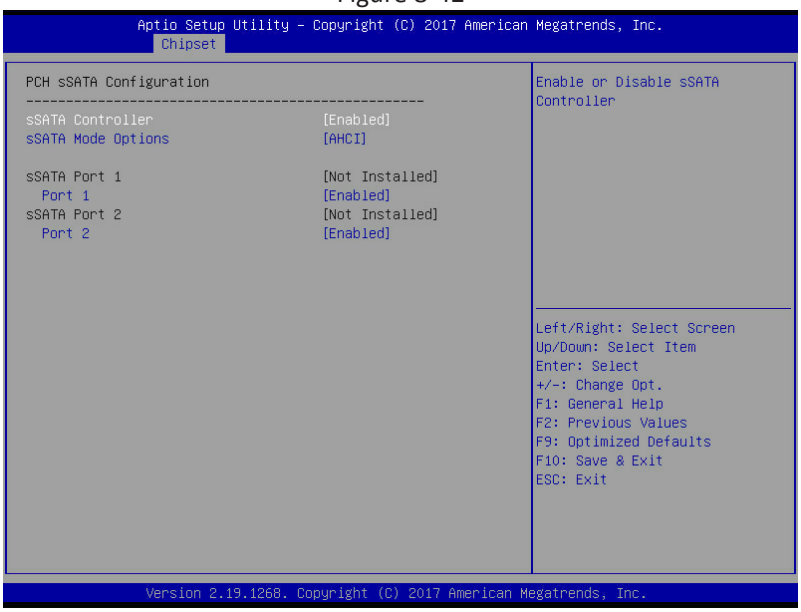


Figure 8-43

Table 8-19 PCH SATA Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
SATA Controller	SATA controller on-off settings. Options include: Enabled Disabled	Enabled
SATA Mode Options	SATA mode settings. Options include: AHCI RAID	AHCI
SATA Port 0~7	SATA port 0~7 HDD information	----
Port 0~7	SATA port on-off settings. Options include: Enabled Disabled	Enabled

PCH sSATA Configuration Interface Instruction Table is omitted here.

8.2.3.2 USB Configuration

USB Configuration is used to set the options related with the onboard USB ports.

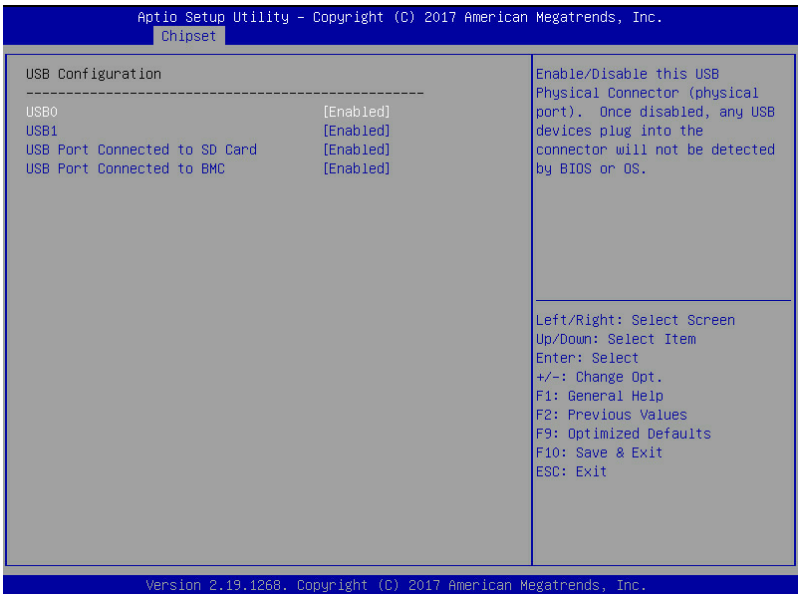


Figure 8-44

Table 8-20 USB Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
USB N	Onboard USB port on-off settings. Options include: Enabled Disabled	Enabled

8.2.3.3 Miscellaneous Configuration

Miscellaneous Configuration interface is used to set some other common options.

Figure 8-45

Table 8-21 Miscellaneous Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Restore AC Power Loss	Power state settings when restoring on AC power loss. Options include: Power OFF Last State Power ON	Power OFF
Max Page Table Size	The maximum page table size settings. Options include: 1GB 2MB For older OS, please select 2MB, otherwise, it may cause a problem.	1GB

8.2.3.4 Server ME Configuration

Server ME Configuration interface is used to display and set the options related with server ME configuration.

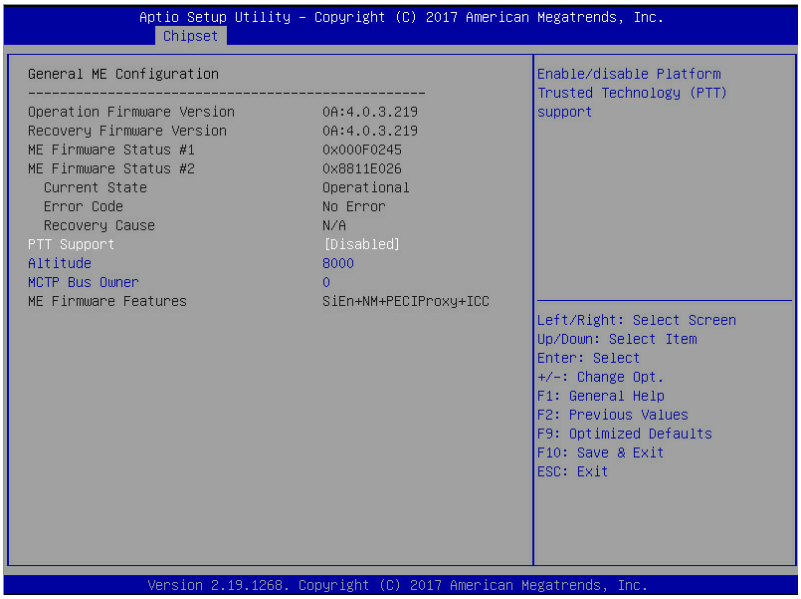


Figure 8-46

Table 8-22 Server ME Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Operational Firmware Version	Operational ME firmware version	----
Recovery Firmware Version	Recovery ME firmware version	----
ME Firmware Status #1	ME FW status value #1	----
ME Firmware Status #2	ME FW status value #2	----
Current State	Current state	----
Error code	ME FW error code	----
Recovery Cause	Recovery cause	N/A
PTT Support	PTT support on-off settings. Options include: Enabled Disabled	Disabled
Altitude	Altitude settings	8000
MCTP Bus Owner	MCTP bus owner is located in PCIe: [15:8] bus, [7:3] device, [2:0] function. If set to 0, it means disabled.	0
ME Firmware Features	ME FW features	----

8.2.3.5 Runtime Error Logging

Runtime Error Logging interface is used to set the runtime error logs.

Figure 8-47

Table 8-23 Runtime Error Logging Interface Instruction Table

Interface Parameters	Function Description	Default Value
System Errors	System error log record settings. Options include: Enabled Disabled	Enabled

8.2.4 Processor

Processor interface is used to set the options related with the processor and memory.

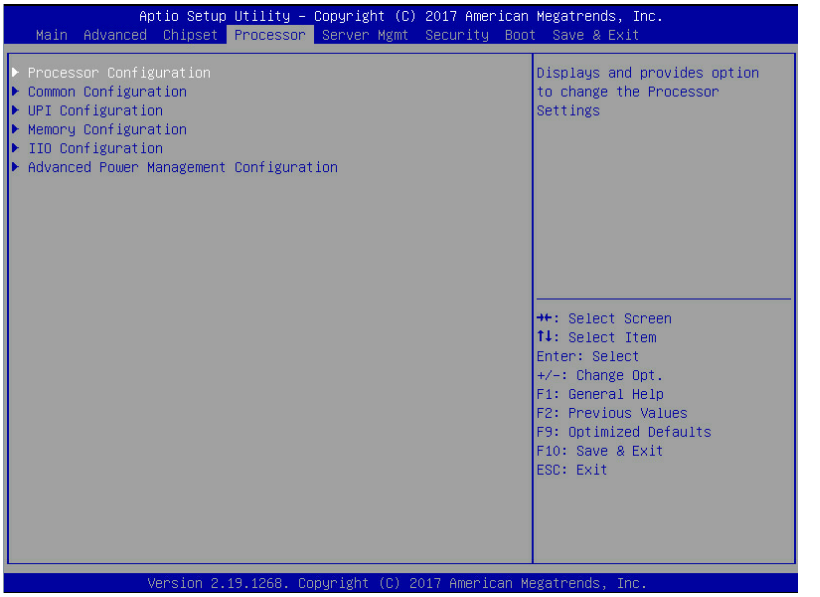


Figure 8-48

Table 8-24 Processor Interface Instruction Table

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

8.2.4.1 Processor Configuration

Processor Configuration interface is used to set the options related with the processor.

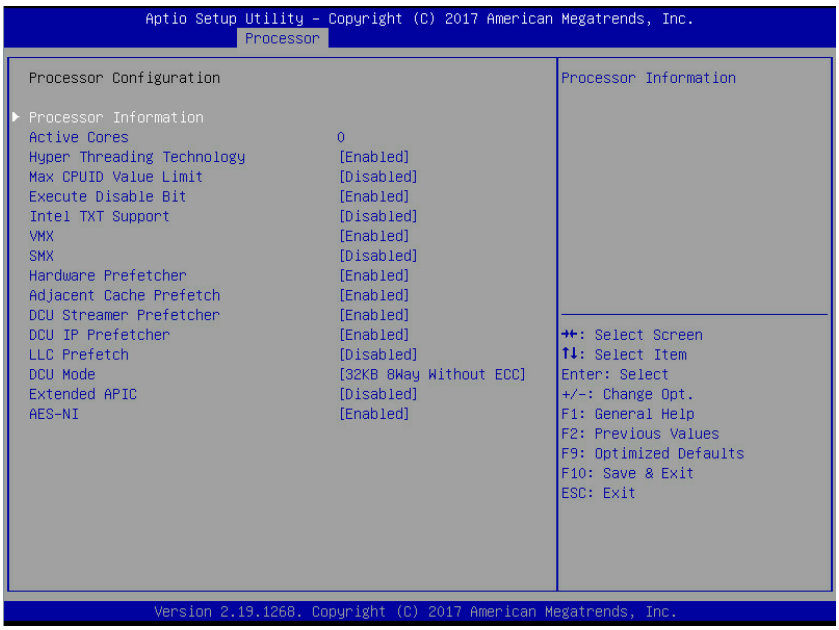


Figure 8-49

Table 8-25 Processor Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Processor Information	Processor information submenu, the processor's detailed information	----
Active Cores	CPU core settings. Input the number of CPU cores you want to enable. In the Help information, it will display the effective values you can set and the maximum number of physical cores according to the current CPU usage. The default value is 0, all cores enabled.	0
Hyper Threading Technology	Hyper threading technology on-off settings. Options include: Enabled Disabled	Enabled
Max CPUID Value Limit	The max CPUID value limit on-off settings. Enabled Disabled When the legacy OS boot does not support CPUID function, please enable this option.	Disabled

Execute Disable Bit	Execute disable bit on-off setting. Options include: Enabled Disabled	Enabled
Intel TXT Support	Intel trusted execution technology on-off settings. Options include: Enabled Disabled	Disabled
VMX	Intel virtual machine extensions technology on-off settings. Options include: Enabled Disabled	Enabled
SMX	Safe mode extension on-off settings. Options include: Enabled Disabled	Disabled
Hardware Prefetcher	Hardware prefetcher on-off settings. Options include: Enabled Disabled Before CPU processing instructions or data, it will prefetch these instructions or data from memory to L2 cache, to shorten the amount of time that reading memory takes, to help eliminate potential bottlenecks and to improve system performance.	Enabled
Adjacent Cache Prefetch	Adjacent cache prefetch on-off settings. Options include: Enabled Disabled If this function is enabled, during computer data reading, it will intelligently consider the adjacent data is needed as well, and it will prefetch these data during processing, to speed up the reading process.	Enabled
DCU Streamer Prefetcher	DCU streamer prefetcher on-off settings. Options include: Enabled Disabled This function can prefetch CPU data to shorten the data reading time.	Enabled
DCU IP Prefectcher	DCU IP prefectcher on-off settings. Options include: Enabled Disabled This function can judge whether there is data to prefetch, to shorten the data reading time.	Enabled
LLC Prefetcher	All threads LLC prefetcher on-off settings. Options include: Enabled Disabled	Disabled
DCU Mode	DCU mode settings. Options include: 32KB 8Way Without ECC 16KB 4Way With ECC	32KB 8Way Without ECC
Extended APIC	Extended APIC on-off settings. Options include: Enabled Disabled	Disabled
AES-NI	AES instruction on-off settings. Options include: Enabled Disabled This menu mainly controls whether the CPU supports AES instruction. These instructions are mainly used for system virtualization. Enable this instruction, system performance will be improved.	Enabled

8.2.4.2 Common Configuration

Common Configuration interface is used to set the common options.

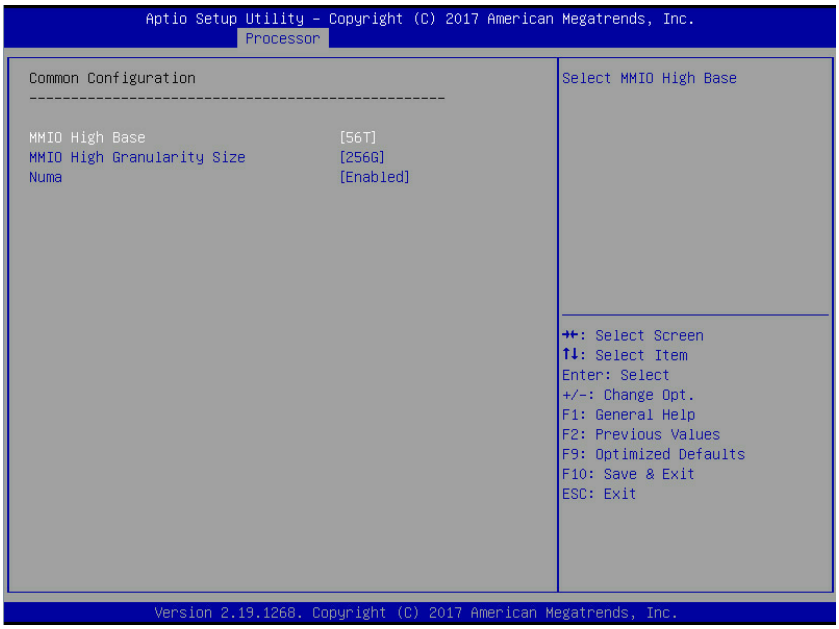


Figure 8-50

Table 8-26 Common Configuration Interface Instruction Table

Interface Parameters	**Function Description**	**Default Value**
MMIO High Base	MMIO high base settings. Options include: 56T 40T 24T 16T 4T 1T	56T
MMIO High Granularity Size	MMIO high granularity size settings. Options include: 1G 4G 16G 64G 256G 1024G	256G
Numa	Numa on-off settings. Options include: Enabled Disabled	Enabled

8.2.4.3 UPI Configuration

UPI Configuration interface is used to set the options related with UPI.

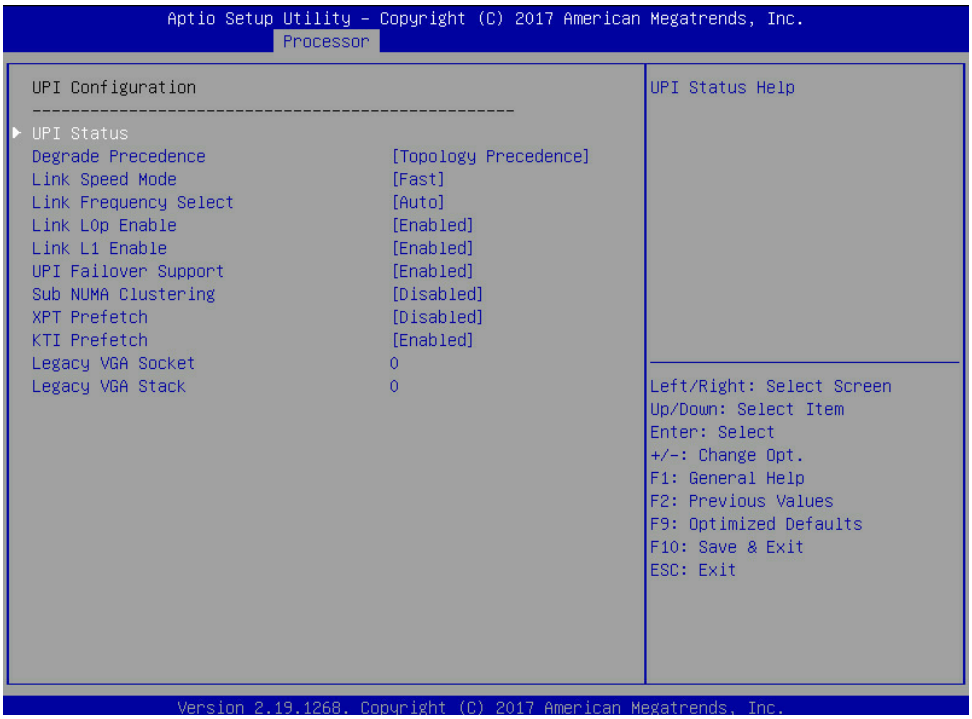


Figure 8-51

Table 8-27 UPI Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
UPI Status	UPI status submenu, displaying the current UPI link status	----
Degrade Precedence	Degrade precedence settings. Options include: Topology Precedence Feature Precedence When the system settings conflict, set it to Topology Precedence to reduce Feature; or set it to Feature Precedence to reduce Topology.	Topology Precedence
Link Speed Mode	Link speed mode settings. Options include: Fast Slow	Fast
Link Frequency Select	Link frequency select settings. Options include: Auto 9.6 GT/s 10.4GT/s Use Per Link Setting	Auto
Link L0p Enable	Link L0p on-off settings. Options include: Enabled Disabled Link power-saving mode setting, which is set when the bandwidth is half of the peak bandwidth	Enabled
Link L1 Enable	Link L1 on-off settings. Options include: Enabled Disabled In the case that system is extremely idle, turn off QPI Link.	Enabled

UPI Failover Support	UPI failover support on-off settings. Options include: Enabled Disabled	Enabled
Sub NUMA Clustering	Sub NUMA cluster settings. Options include: Auto: Support 1-cluster or 2-clusters according to IMC interleave. Enabled: Support all SNC clusters (2-clusters) and 1-way IMC interleave. Disabled: SNC function not supported.	Disabled
XPT Prefetch	XPT prefetch settings. Options include Disabled and Enabled.	Disabled
KTI Prefetch	KTI prefetch settings. Options include Disabled and Enabled.	Enabled
Legacy VGA Socket	Legacy VGA number settings, the range of effective values is 0~1.	0
Legacy VGA Stack	Legacy VGA stack number settings, the range of effective values is 0~6.	0

8.2.4.4 Memory Configuration

Memory Configuration interface is used to set the options related with the memory.

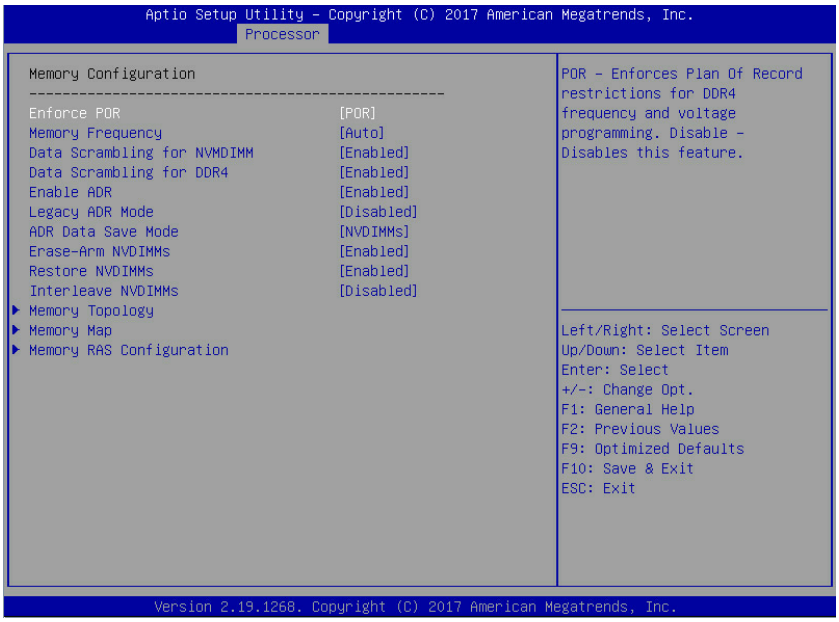


Figure 8-52

Table 8-28 Memory Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Enforce POR	Enforce POR settings. Options include: POR Disabled	POR
Memory Frequency	Memory frequency settings. Options include: Auto 1600 1866 2133 2400 2666 ……	Auto
Data Scrambling for NVMDIMM	NVMDIMM data scrambling on-off settings. Options include: Enabled Disabled	Enabled
Data Scrambling for DDR4	DDR4 data scrambling on-off settings. Options include: Auto Enabled Disabled	Enabled
Enable ADR	ADR on-off settings. Options include: Enabled Disabled	Enabled
Legacy ADR Mode	Legacy ADR mode on-off settings. Options include: Enabled Disabled	Enabled
ADR Data Save Mode	ADR data save mode settings. Options include: Disabled Batterybacked DIMMs NVDIMMs	NVDIM
Erase-Arm NVDIMMs	Erase-Arm NVDIMMs on-off settings. Options include: Enabled Disabled	Enabled
Restore NVDIMMs	Restore NVDIMMs on-off settings. Options include: Enabled Disabled	Enabled
Interleave NVDIMMs	Interleave NVDIMMs on-off settings. Options include: Enabled Disabled	Disabled
Memory Topology	Memory topology submenu, displaying the detailed information of the current installed memories.	----
Memory Map	Memory Map submenu	----
Memory RAS Configuration	Memory RAS configuration submenu	----

8.2.4.4.1 Memory Map

Memory Map interface is used to set some modes of the memory.

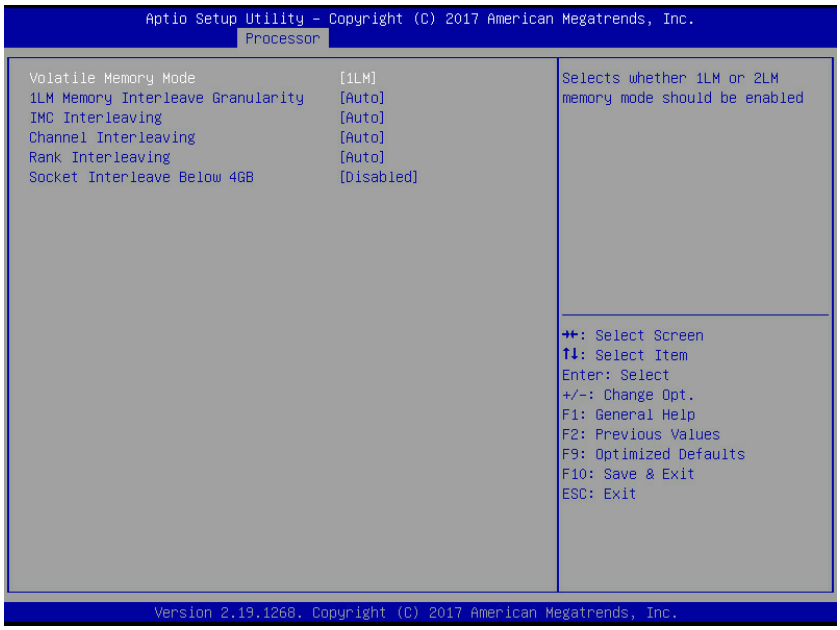


Figure 8-53

Table 8-29 Memory Map Interface Instruction Table

Interface Parameters	Function Description	Default Value
Volatile Memory Mode	Volatile memory mode settings. Options include: 1LM 2LM Auto	1LM
1LM Memory Interleave Granularity	1LM memory interleave granularity settings. Options include: Auto 256B Target, 256B Channel 64B Target, 64B Channel	Auto
IMC Interleaving	IMC interleaving settings. Options include: Auto 1-way Interleave 2-way Interleave	Auto
Channel Interleaving	Channel interleaving settings. Options include: Auto 1-way Interleave 2-way Interleave 3-way Interleave	Auto
Rank Interleaving	Rank interleaving settings. Options include: Auto 1-way Interleave 2-way Interleave 4-way Interleave 8-way Interleave	Auto
Socket Interleave Below 4GB	On-off settings of 4GB or less address space processor interleave. Options include: Enabled Disabled	Disabled

8.2.4.4.2 Memory RAS Configuration

Memory RAS Configuration interface is used to set the options related with the memory RAS feature.

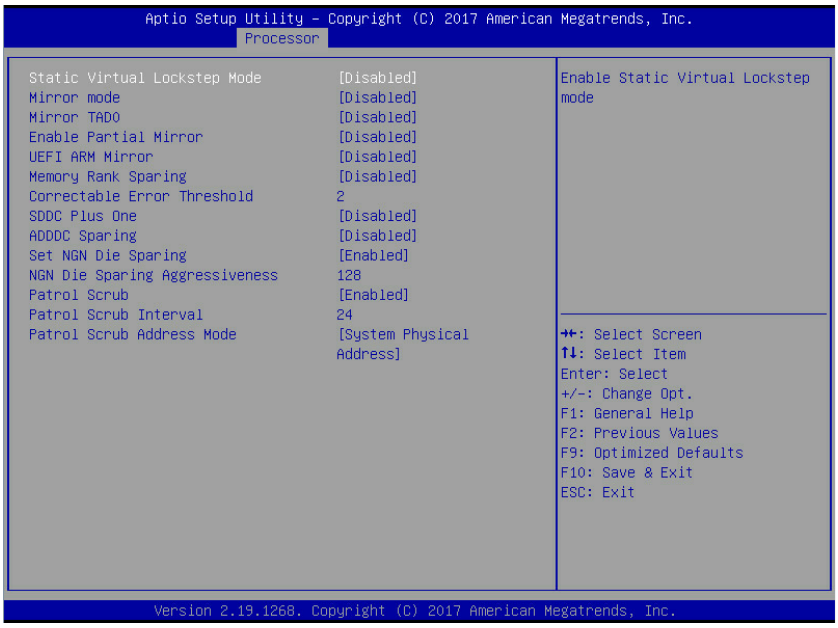


Figure 8-54

Table 8-30 Memory RAS Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Static Virtual Lockstep Mode	Static virtual lockstep mode on-off settings. Options include: Enabled Disabled	Disabled
Mirror Mode	Mirror mode settings. Options include: Disabled Mirror Mode 1LM Mirror Mode 2LM	Disabled
Mirror TAD0	Mirror TAD0 mode on-off settings. Options include: Enabled Disabled	Disabled
Enable Partial Mirror	Enable partial mirror mode. Options include: Disabled Partial Mirror mode 1LM Partial Mirror mode 2LM	Disabled
UEFI ARM Mirror	UEFI ARM mirror mode on-off settings. Options include: Enabled Disabled	Disabled
Memory Rank Sparing	Memory Rank sparing on-off settings. Options include: Enabled Disabled When it is set to Enabled, users can select the memory sparing mode. It is a kind of memory channel sparing in Rank, the total memory capacity varies with sparing modes, and it supports at most half of the memory capacity to be used for sparing.	Disabled

Correctable Error Threshold	Correctable error threshold settings	5000
SDDC Plus One	SDDC+1 on-off settings. Options include: Enabled Disabled	Disabled
ADDDC Sparing	ADDDC sparing on-off settings. Options include: Enabled Disabled	Disabled
Set NGN Die Sparing	NGN Die sparing on-off settings. Options include: Enabled Disabled	Enabled
NGN Die Sparing Aggressiveness	NGN Die sparing aggressiveness settings, the value range is 0~255, and 0 means no sparing Die.	128
Patrol Scrub	Patrol Scrub on-off settings. Options include: Enabled Disabled	Enabled
Patrol Scrub Interval	Patrol Scrub interval settings, the unit is hour and the range is 0~24.	24
Patrol Scrub Address Mode	Patrol Scrub address mode settings. Options include: System Physical Address Reverse Address	System Physical Address

8.2.4.5 IIO Configuration

IIO Configuration interface is used to set the options related with the PCIe sockets.

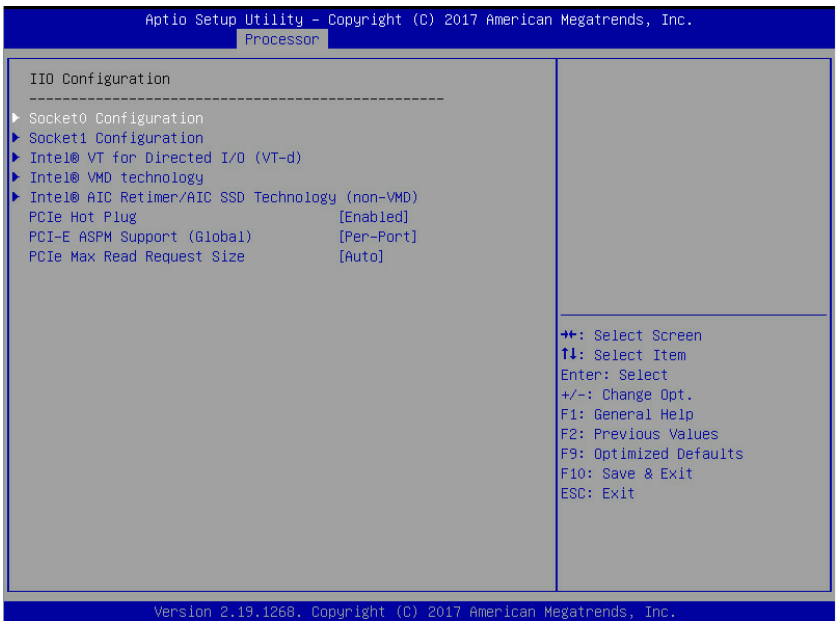


Figure 8-55

Table 8-31 IIO Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
SocketN Configuration	Socket N configuration submenu, used to set the Link speed, Max Payload Size and ASPM of the CPU0's PCIE device, and to display the link status, maximum link and current link speed of the PCIE port.	----
Intel VT for Directed I/O (VT-d)	Intel VT-d settings submenu, Intel VT-d on-off settings	----
Intel VMD Technology	Intel VMD settings submenu, VMD on-off settings of each PStack of each CPU.	----
Intel AIC Rtimer/AIC SSD Technology (Non-VMD)	Intel AIC Retimer/AIC SSD settings submenu, AIC Retimer/AIC SSD on-off settings of each PStack of each CPU.	----
PCIe Hot Plug	PCIe hot plug on-off settings. Options include: Enabled Disabled	Enabled
PCI-E ASPM Support (Global)	PCIE ASPM support on-off settings. Options include: Disabled Per-Port L1 Only	Per-Port
PCIe Max Read Request Size	PCIe max read request size settings. Options include: Auto 128B 256B 512B 1024B 2048B 4096B	Auto

8.2.4.6 Advanced Power Management Configuration

Advanced Power Management Configuration interface is used to set the options related with the CPU power management.

Figure 8-56

Table 8-32 Advanced Power Management Configuration Interface Instruction Table

Interface Parameters	Function Description
Power/Performance Profile	Mode settings, options include: Maximum Performance, Minimum Power and Custom. The default value is Custom.
CPU P State Control	CPU P state control submenu
Hardware PM State Control	Hardware PM state control submenu
CPU C State Control	CPU C state control submenu
Package C State Control	Package C state control submenu
CPU-Advanced PM Tuning	CPU power-saving performance tuning submenu
Socket RAPL Configuration	Socket RAPL configuration submenu

8.2.4.6.1 CPU P State Control

CPU P State Control interface is used to set the options related with the CPU P state.

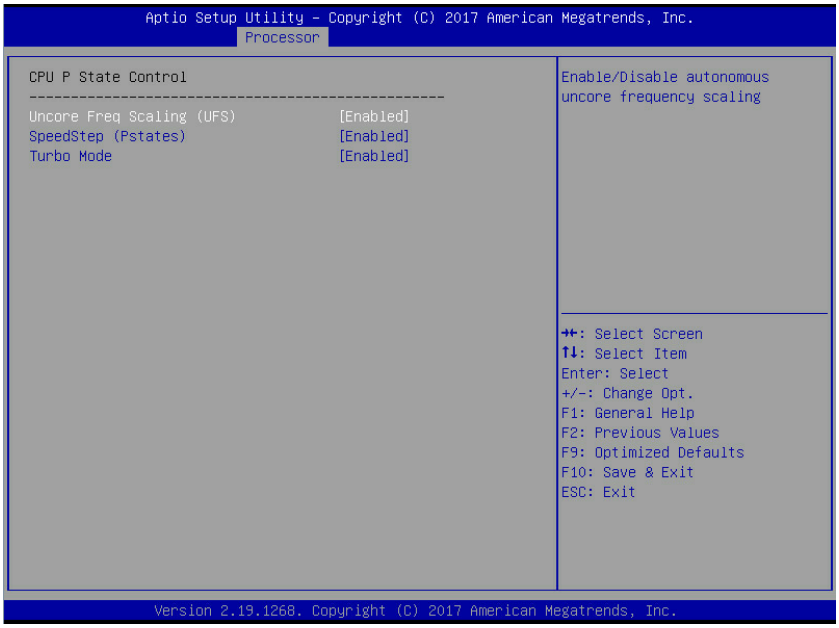


Figure 8-57

Table 8-33 CPU P State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Uncore Freq Scaling (UFS)	Uncore frequency scaling settings. Options include: Enabled Disabled (Min Frequency) Disabled (Max Frequency) Custom	Enabled
Uncore Frequency	Uncore frequency settings. The range is 1300-2300, displayed when Uncore Freq Scaling (UFS) is set to Custom.	1300
SpeedStep (Pstates)	SpeedStep on-off settings. Options include: Enabled Disabled	Enabled
Turbo Mode	Turbo mode on-off settings. Options include: Enabled Disabled	Enabled

8.2.4.6.2 Hardware PM State Control

Hardware PM State Control interface is used to set the options related with the hardware PM state.

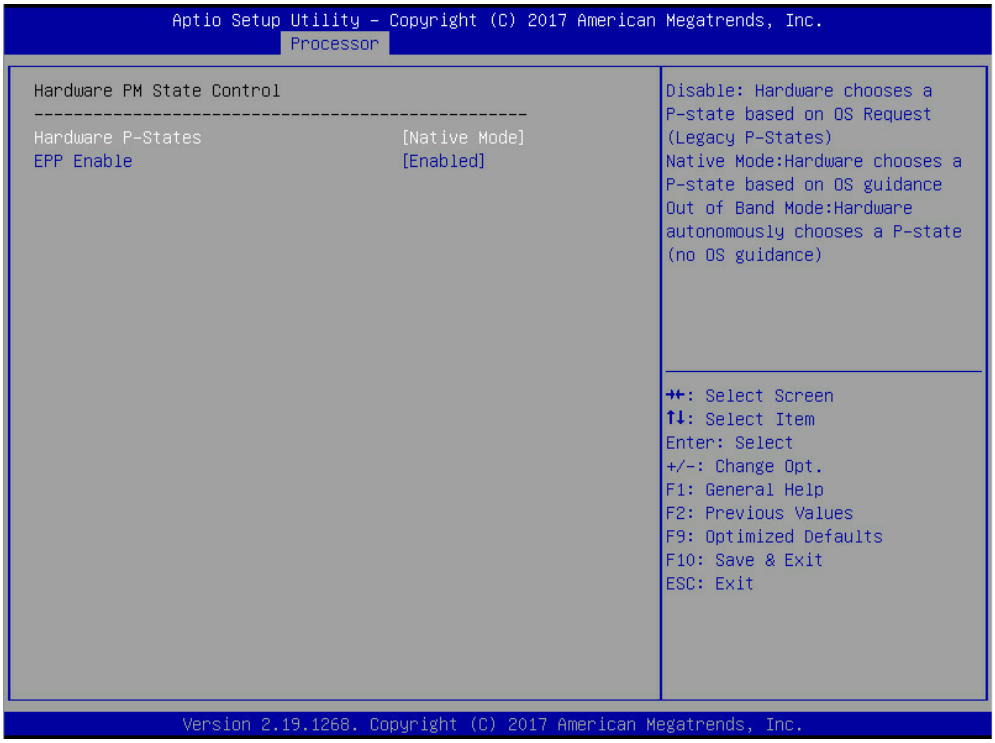


Figure 8-58

Table 8-34 Hardware PM State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Hardware P-States	Hardware P-States is set by OS automatically or not, the default value is decided based on the actual test. Options include: Disabled: based on legacy OS request Native Mode: based on legacy OS boot Out of Band Mode: hardware auto select, no OS boot Native Mode with No Legacy Support	Native Mode
EPP Enable	EPP on-off settings. Options include: Enabled Disabled	Enabled

8.2.4.6.3 CPU C State Control

CPU C State Control interface is used to set the options related with the CPU C state, for controlling the power consumption of CPU in idle state.

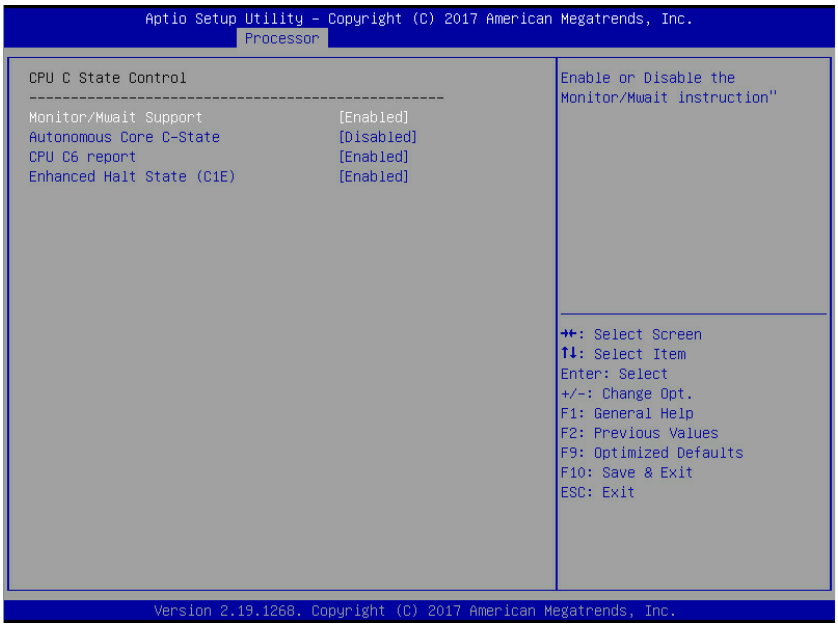


Figure 8-59

Table 8-35 CPU C State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Monitor/Mwait Support	Monitor/Mwait support on-off settings. Options include: Enabled Disabled	Enabled
Autonomous Core C-State	Autonomous core C-state on-off settings. Options include: Enabled Disabled	Disabled
CPU C6 report	On-off settings of reporting C6 state to OS. Options include: Enabled Disabled	Disabled
Enhanced Halt State (C1E)	C1E on-off settings. Options include: Enabled Disabled	Disabled

8.2.4.6.4 Package C State Control

Package C State Control interface is used with set the options related with the Package C state.

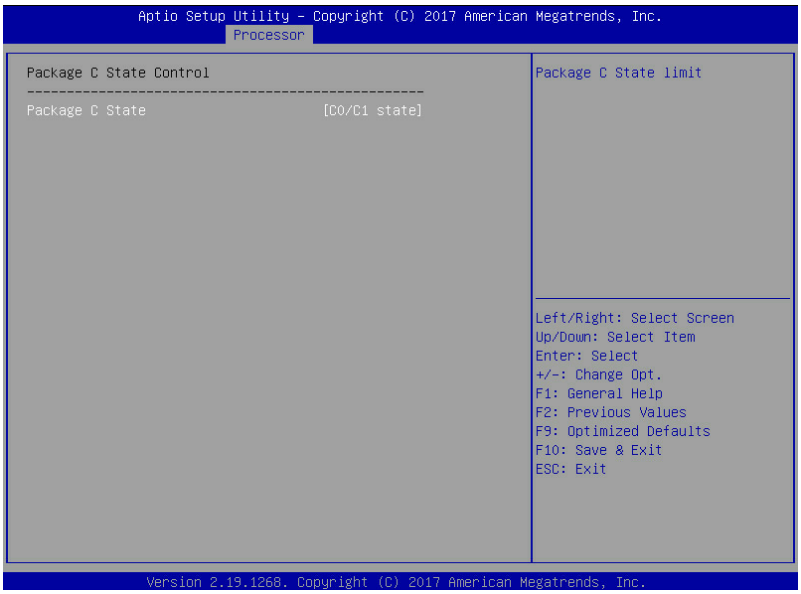


Figure 8-60

Table 8-36 Package C State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Package C State	Package C state settings. Options include: C0/C1 state C2 state C6 (Non Retention) state C6 (Retention) state No Limit	C0/C1 state

8.2.4.6.5 CPU-Advanced PM Tuning

CPU-Advanced PM Tuning interface is used to set the options related with the CPU power-saving performance, with an Energy Perf BIAS submenu.

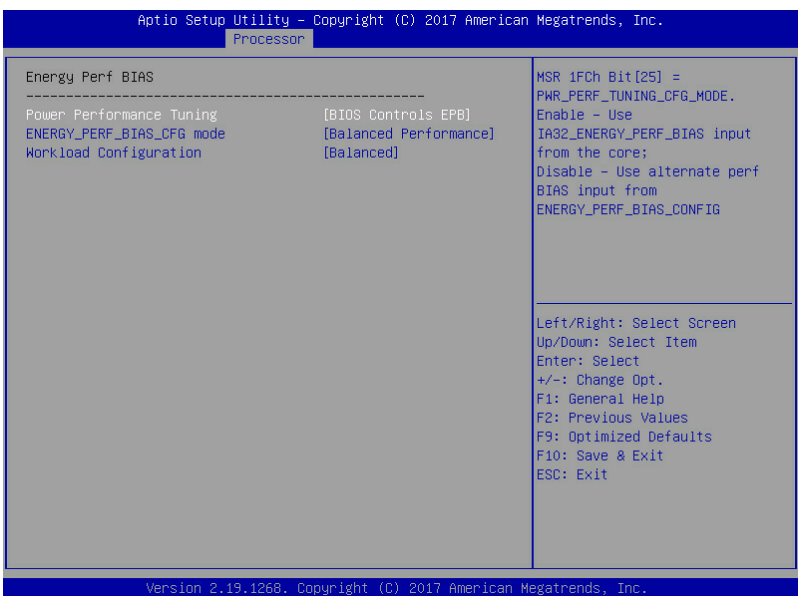


Figure 8-61

Table 8-37 Energy Perf BIAS Interface Instruction Table

Interface Parameters	Function Description	Default Value
Power Performance Tuning	Power performance tuning settings. Options include: OS Controls EPB BIOS Controls EPB	BIOS Controls EPB
ENERGY_PERF_BIAS_CFG Mode	Power performance management settings. Options include: Performance Balanced Performance Balanced Power Power When the Power Performance Tuning is set to BIOS Controls EPB, this option can be set.	Balanced Performance
Workload Configuration	Workload optimization settings. Options include: Balanced I/O Sensitive	Balanced

8.2.4.6.6 SOCKET PARL Config

SOCKET RAPL Config interface is used to set the Power Limit.

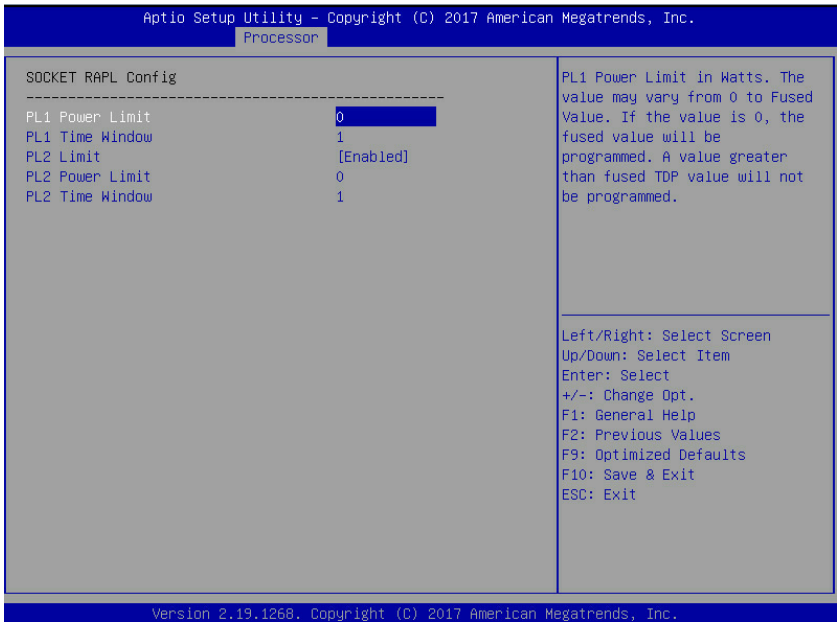


Figure 8-62

Table 8-38 SOCKET RAPL Config Interface Instruction Table

Interface Parameters	Function Description	Default Value
PL1 Power Limit	PL1 Power Limit parameter settings	0
PL1 Time Window	PL1 time settings	1
PL2 Power	PL2 Power on-off settings. Options include: Enabled Disabled	Enabled
PL2 Power Limit	PL2 Power Limit parameter settings	0
PL2 Time Window	PL2 time settings	1

8.2.5 Server Mgmt

Server Mgmt interface is used to set the options related with server management, including watchdog, BMC network configuration, BMC user settings, system health information, etc.

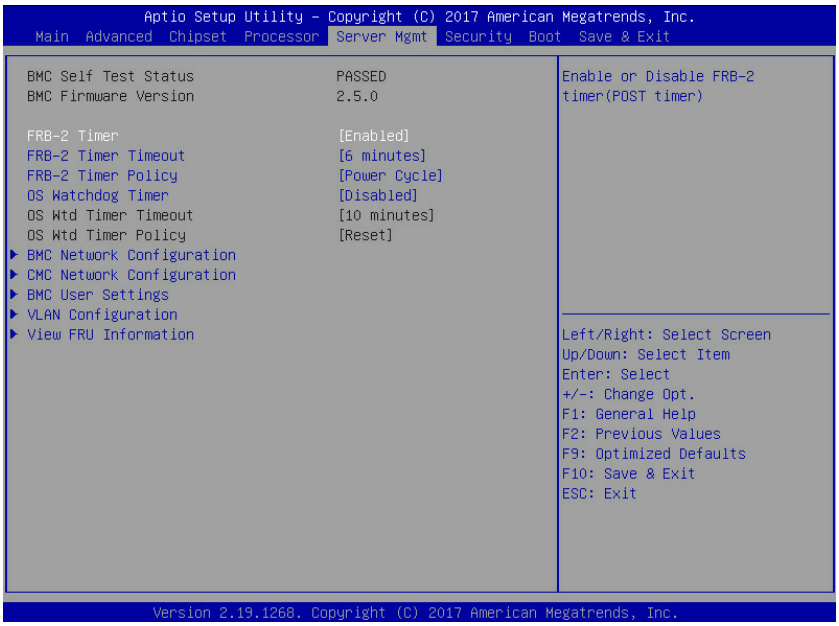


Figure 8-63

Table 8-39 Server Mgmt Interface Instruction Table

Interface Parameters	Function Description	Default Value
BMC Self Test Status	BMC self-test status	----
BMC Firmware Version	Current motherboard's BMC firmware version	----
FRB-2 Timer	FRB-2 timer on-off settings. Options include: Enabled Disabled	Enabled
FRB-2 Timer Timeout	FRB-2 timer timeout settings. Options include: 3 minutes 4 minutes 5 minutes 6 minutes	6 minutes
FRB-2 Timer Policy	FRB-2 timer policy settings. Options include: Do Nothing Reset Power Down Power Cycle	Power Cycle
OS Watchdog Timer	OS watchdog timer settings. Options include: Enabled Disabled	Disabled
OS Wtd Timer Timeout	OS watchdog timer timeout settings. Options include: 5 minutes 10 minutes 15 minutes 20 minutes	10 minutes

OS Wtd Timer Policy	OS watchdog timer policy settings. Options include: Do Nothing Reset Power Down Power Cycle	Reset
BMC Network Configuration	BMC network configuration submenu	----
CMC Network Configuration	CMC network configuration submenu	----
BMC User Settings	BMC user settings submenu	----
VLAN Configuration	VLAN configuration submenu	----
View FRU Information	View FRU information submenu	----

8.2.5.1 BMC Network Configuration

BMC Network Configuration interface is used to configure the BMC network through BIOS.

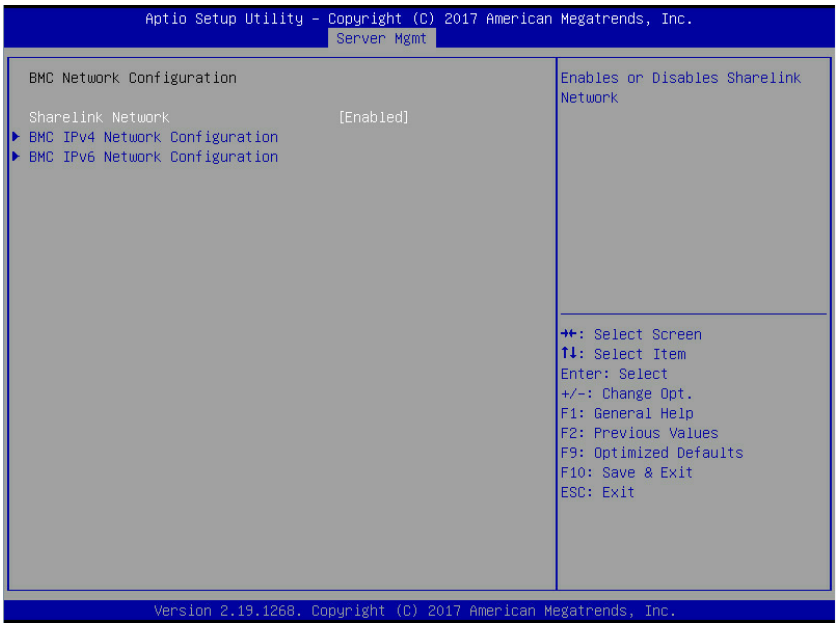


Figure 8-64

Table 8-40 BMC Network Configuration Interface Instruction Table

Interface Parameters	**Function Description**	**Default Value**
Sharelink Network	BMC Sharelink network on-off settings, take effect immediately.	Enabled
BMC IPv4 Network Configuration	BMC IPv4 network configuration	----
BMC IPv6 Network Configuration	BMC IPv6 network configuration	----

8.2.5.1.1 BMC IPv4 Network Configuration

BMC IPv4 Network Configuration interface is used to configure the BMC IPv4 management network through BIOS.

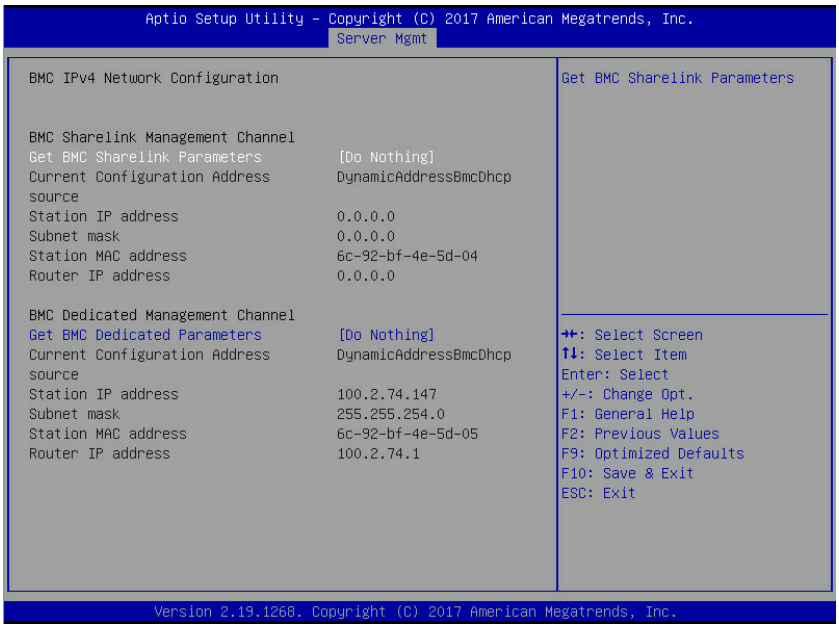


Figure 8-65

Table 8-41 BMC IPv4 Network Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Get BMC Sharelink/Dedicated Parameters	Set the method to get the BMC sharelink/dedicated parameters. Options include: Do Nothing Auto Manual	Do Nothing
Configuration Address Source	Set BMC network status. Options include: Unspecified Static DynamicBmcDhcp The setting takes effect immediately.	Unspecified
Current Configuration Address	Current BMC configuration address status	----
Station IP address	Station IP address	----
Subnet mask	Subnet mask	----
Station MAC address	Station MAC address	----
Router IP address	Router IP address	----

8.2.5.1.2 BMC IPv6 Network Configuration

BMC IPv6 Network Configuration interface is used to configure the BMC IPv6 management network through BIOS.

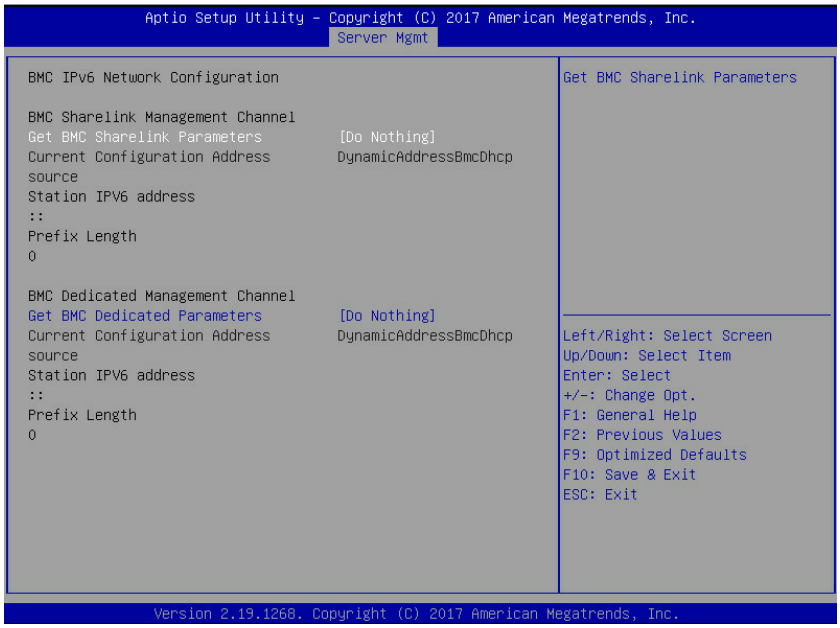


Figure 8-66

Table 8-42 BMC IPv6 Network Configuration Interface Instruction Table

Interface Parameters	**Function Description**	**Default Value**
Get BMC Sharelink/Dedicated Parameters	Set the method to get the BMC sharelink/dedicated parameters. Options include: Do Nothing Auto Manual	Do Nothing
Configuration Address Source	Set BMC network status. Options include: Unspecified Static DynamicBmcDhcp The setting takes effect immediately.	Unspecified
Current Configuration Address	Current BMC configuration address status	----
Station IPv6 address	Station IPv6 address	----
Prefix Length	IPv6 prefix length	----

8.2.5.2 CMC Network Configuration

CMC Network Configuration interface is used to configure the CMC network through BIOS.

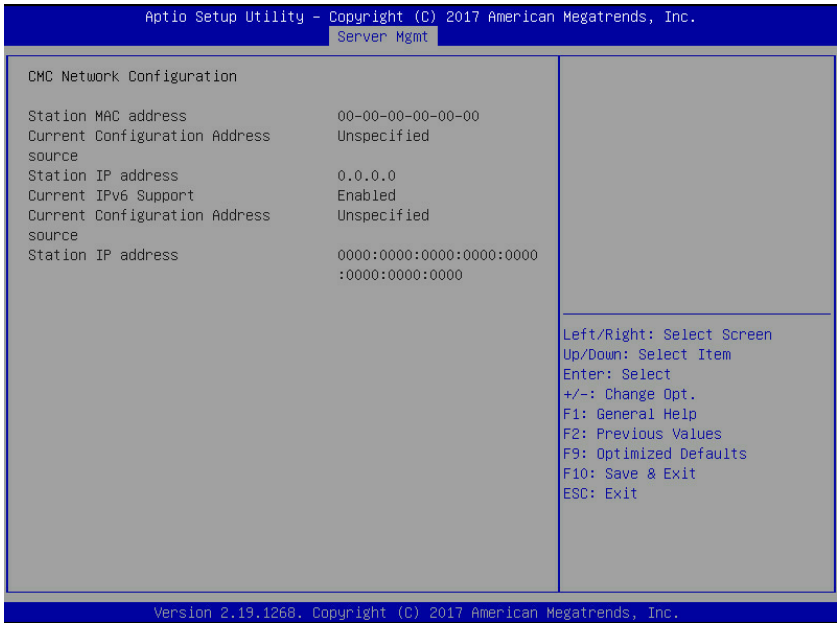


Figure 8-67

Table 8-43 CMC Network Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Station MAC address	CMC Mac address	----
Current Configuration Address Source	CMC IP Info source	Unspecified
Station IP address	CMC IP address	----
Current IPv6 support	The current IPv6 supports or not	Enabled
Current Configuration Address Source	CMC IPv6 Info source	Unspecified
Station IP address	CMC IPv6 address	----

8.2.5.3 BMC User Settings

BMC User Settings interface is used to configure BMC users through BIOS.

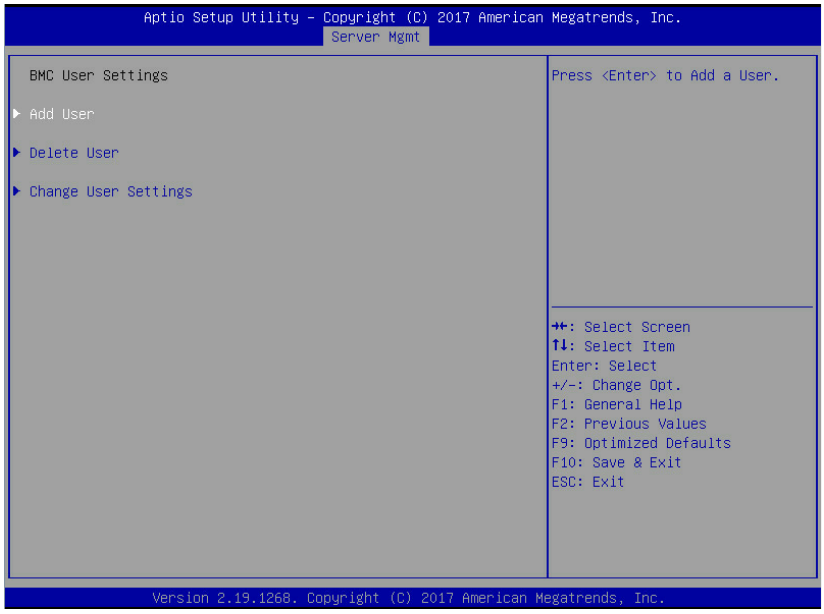


Figure 8-68

Table 8-44 BMC User Settings Interface Instruction Table

Interface Parameters	Function Description
Add User	Add user submenu
Delete User	Delete user submenu
Change User Settings	Change user settings submenu

8.2.5.3.1 Add User

Add User interface is used to add a BMC user through BIOS. The addition takes effect immediately, and the user will be added to the BMC user list.

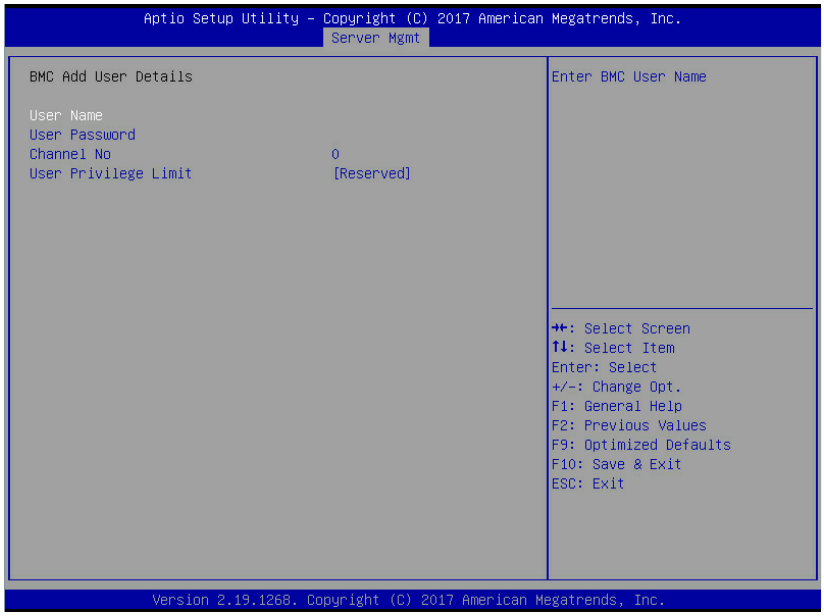


Figure 8-69

Table 8-45 Add User Interface Instruction Table

Interface Parameters	Function Description	Default Value
User Name	Set user name, supporting up to 16 characters.	----
User Password	Set user password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.	----
Channel NO	Set BMC channel, input 1 or 8.	----
User Privilege Limit	User privilege settings. Options include: Reserved Callback User Operator Administrator If the setting succeeds, it will prompt “Set User Access Command Passed”, and the BMC User takes effect immediately.	Reserved

Note: To enable the new user, it needs to set the User option in the Change User Settings interface to [Enabled], and then this user can login to the BMC Web interface.

8.2.5.3.2 Delete User

Delete User interface is used to delete a BMC user through BIOS. The deletion takes effect immediately, and this user can not login to the BMC Web interface any more.

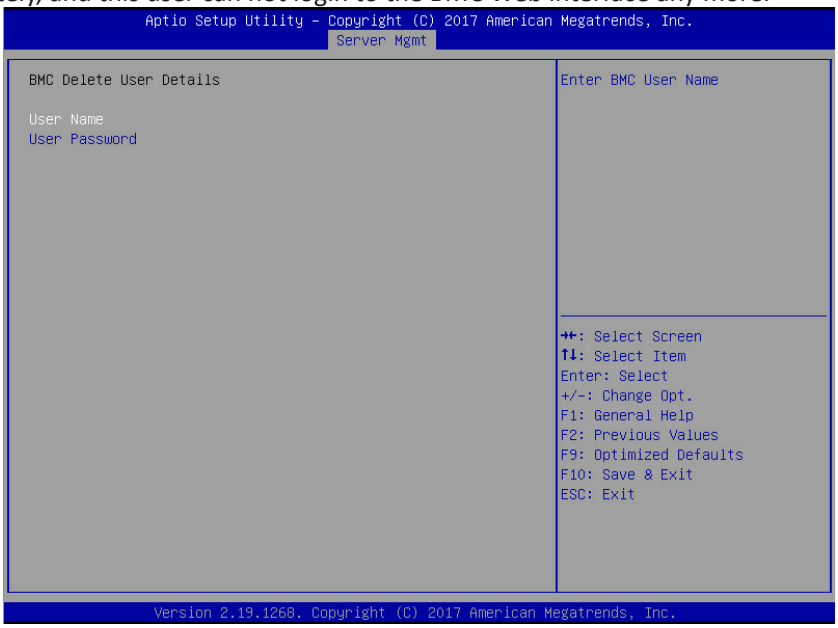


Figure 8-70

Table 8-46 Delete User Interface Instruction Table

Interface Parameters	Function Description
User Name	Input the name of user to delete
User Password	Input the password of user to delete. If the password is correct, it pops up “User Deleted!!!” The deletion takes effect immediately in BMC, and this user can not login to the BMC Web interface any more.

8.2.5.3.3 Change User Settings

Change User Settings interface is used to modify the BMC user settings through BIOS.

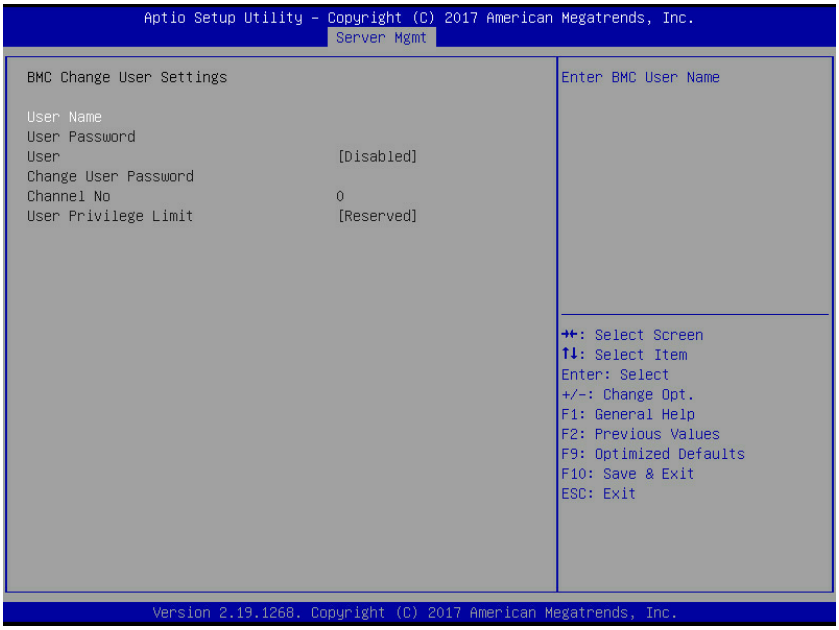


Figure 8-71

Table 8-47 Change User Settings Interface Instruction Table

Interface Parameters	Function Description	Default Value
User Name	Input the name of user to modify.	----
User Password	Input the password of user to modify. Only both the name and password are correct, the following options can be modified.	----
User	User privilege on-off settings. Options include: Enabled Disabled	Disabled
Change User Password	Change the user password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.	----
Channel NO	Set BMC channel, input 1 or 8.	0
User Privilege Limit	Modify the user privilege. Options include: Reserved Callback User Operator Administrator	Reserved

8.2.5.4 VLAN Configuration

VLAN Configuration interface is used to set the BMC VLAN parameters through BIOS.

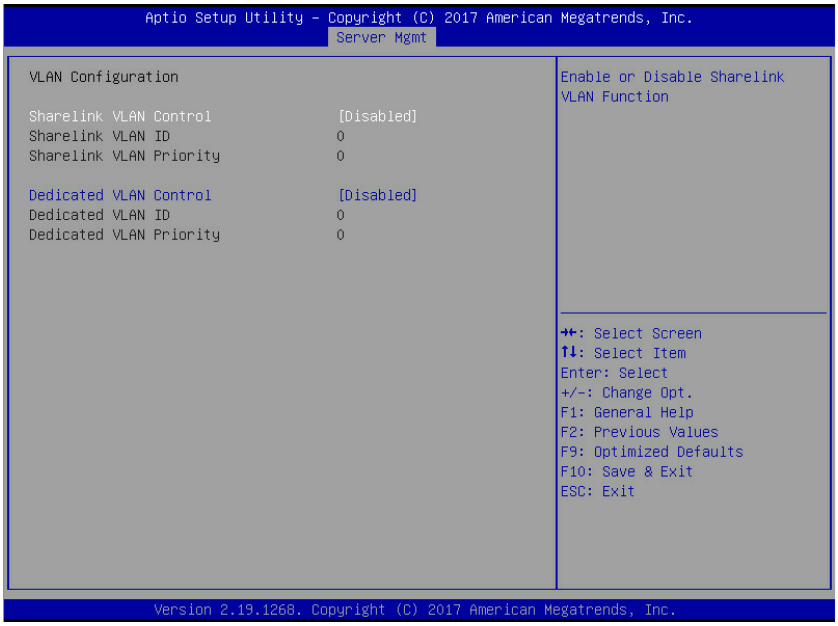


Figure 8-72

Table 8-48 VLAN Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Sharelink/Dedicated VLAN Control	BMC sharelink/dedicated VLAN control on-off settings. Options include: Enabled Disabled To enable VLAN, it needs to set the VLAN ID first.	Disabled
Sharelink/Dedicated VLAN ID	BMC sharelink/dedicated VLAN ID settings, the range is 2~4094. The setting takes effect immediately.	0
Sharelink/Dedicated VLAN Priority	BMC sharelink/dedicated VLAN priority settings, the range is 1~7. The setting takes effect immediately.	0

8.2.5.5 View FRU Information

View FRU Information interface displays the BMC FRU information read by BIOS. On each system reboot, BIOS interacts with BMC to keep the FRU information synchronized.

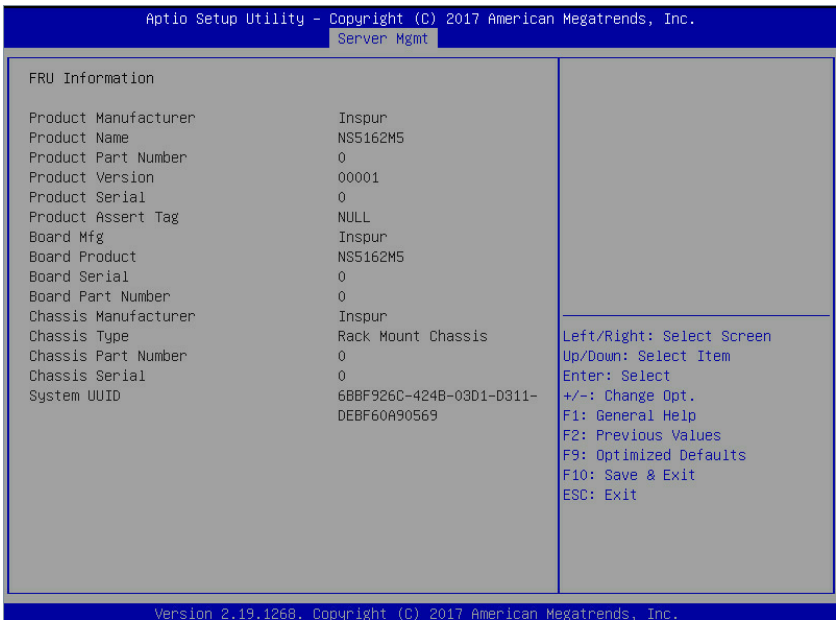


Figure 8-73

Table 8-49 View FRU Information Interface Instruction Table

Interface Parameters	**Function Description**
Product Manufacturer	Product manufacturer
Product Name	Product name
Product Part Number	Product part number
Product Version	Product version
Product Serial	Product serial number
Product Asset Tag	Product asset tag
Board Mfg	Board manufacturer
Board Product	Board product name
Board Serial	Board serial number
Board Part Number	Board part number
Chassis Manufacturer	Chassis manufacturer
Chassis Type	Chassis type
Chassis Product Name	Chassis product name
Chassis Serial	Chassis serial number
System UUID	System serial number

8.2.6 Security

Security interface is used to set the password of the administrator and user. It defaults to no password for the BIOS, users can set the password according to the requirement when using

the machine.

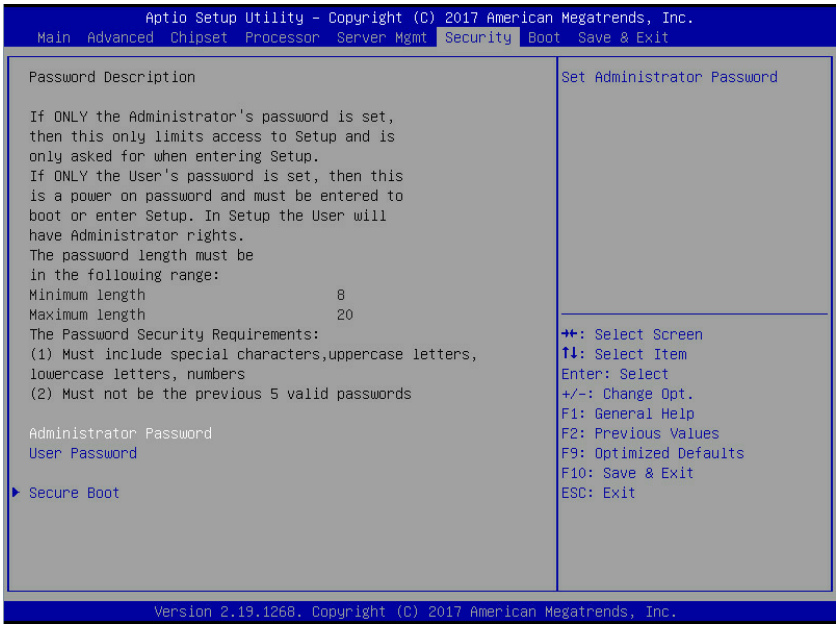


Figure 8-74

Table 8-50 Security Interface Instruction Table

Interface Parameters	**Function Description**
Administrator Password	Create an administrator password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.
User Password	Create a user password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.
Secure Boot	Secure boot menu

8.2.7 Boot Menu

Boot interface is used to set the options related with system boot, including boot mode, boot priority, boot procedure, etc.

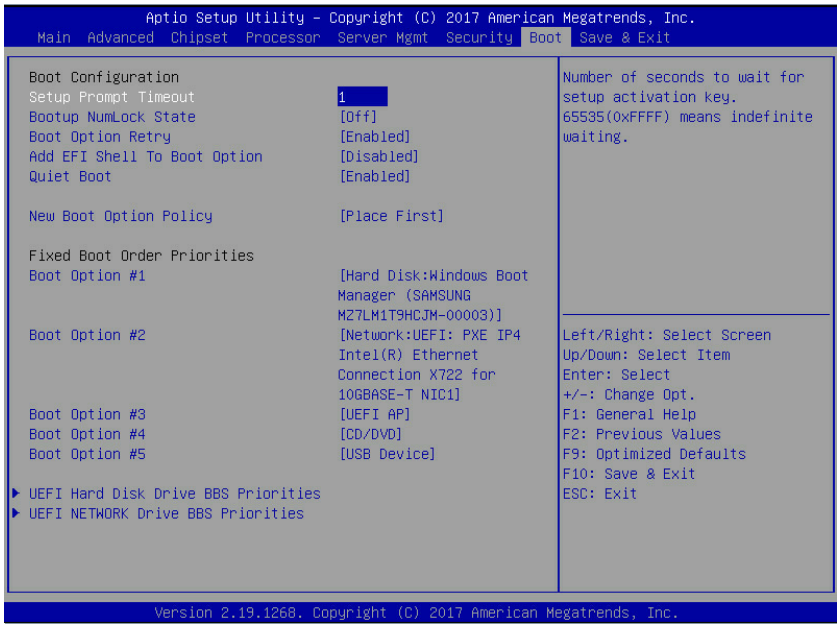


Figure 8-75

Table 8-51 Boot Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Setup Prompt Timeout	Setup prompt timeout settings. Set the time to wait for the Setup activate key, and the maximum value is 65535 seconds.	1
Bootup NumLock State	Bootup Numlock state on-off settings. Options include: On Off	Off
Boot Options Retry	Boot options retry on-off settings. Options include: Enabled Disabled	Enabled
Add EFI Shell To Boot Option	Add UEFI Shell to Boot Option or not, options include: Enabled Disabled	Disabled
Quiet Boot	Quite boot on-off settings. Options include: Enabled Disabled If it is set to Enabled, the boot logo displays as that set by manufacturer, if set to Disabled, the boot screen displays as the text-mode POST interface.	Enabled
New Boot Option Policy	New UEFI boot option policy settings. Options include: Default Place First Place Last	Place First
Fixed Boot Order Priorities Boot Option #X	Boot options priority settings	----
XXXX Driver BBS Priorities	XXXX driver BBS priority settings	---

8.2.8 Save & Exit

Save & Exit interface is used to set the options related with BIOS parameters saving and exit.

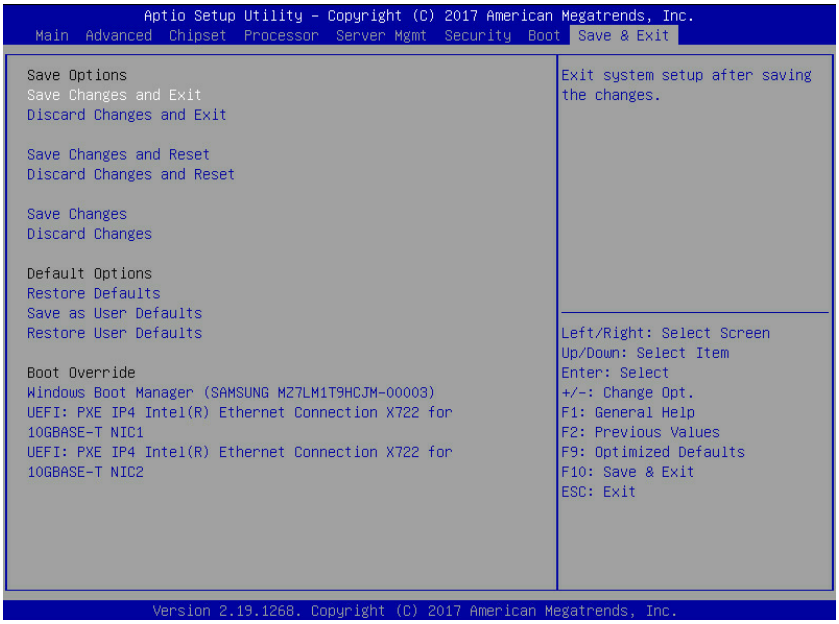


Figure 8-76

Table 8-52 Save & Exit Interface Instruction Table

Interface Parameters	**Function Description**
Save Changes and Exit	To save changes and exit
Discard Changes and Exit	To discard changes and exit
Save Changes and Reset	To save changes and reset
Discard Changes and Reset	To discard changes and reset
Save Changes	To save changes
Discard Changes	To discard changes
Restore Defaults	To restore defaults
Save as User Defaults	To save as user defaults
Restore User Defaults	To restore user defaults
Boot Override	To override the boot option, you could select the boot device from the following options

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 on the screen during system booting, there is a prompt “Press <DEL> to SETUP or <TAB> to POST or <F11> to Boot Menu or <F12> to PXE Boot” below. Press F11 key to open the Boot Menu, as shown in the following figure. Enter the item: UEFI: Built-in EFI Shell.

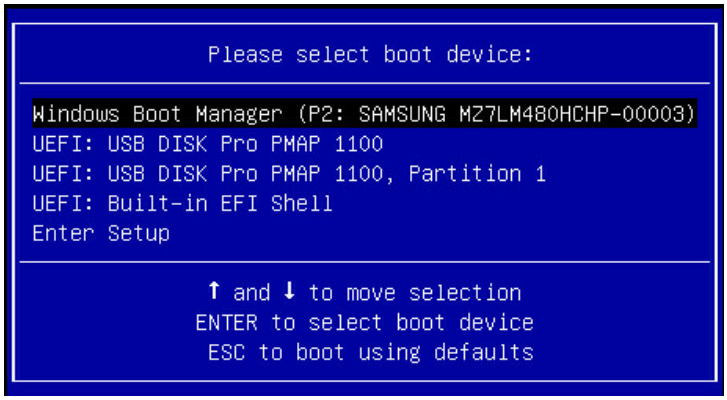


Figure 8-77

2) Enter the disk where the AfuEfi64 package resides, and enter the AfuEfi64 folder. The BIOS.bin file is the 32M BIOS+ME file to update, as shown in the following figure.

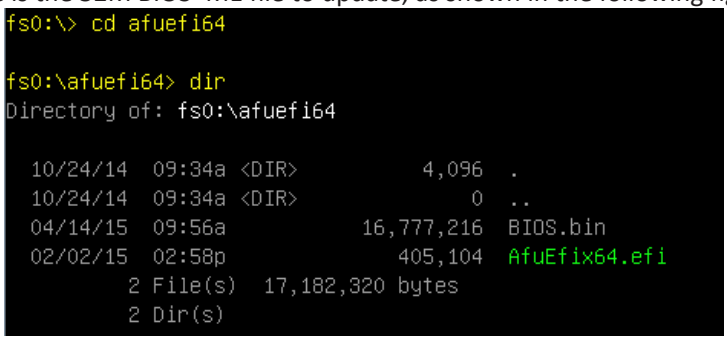


Figure 8-78

3) When there is no change in ME part, execute the command to update 16M BIOS: AfuEfix64.efi BIOS.bin /b /p /n /x /k /l, and the process is as shown in the following figure. After the update is complete, it is recommended to power cycle the system.

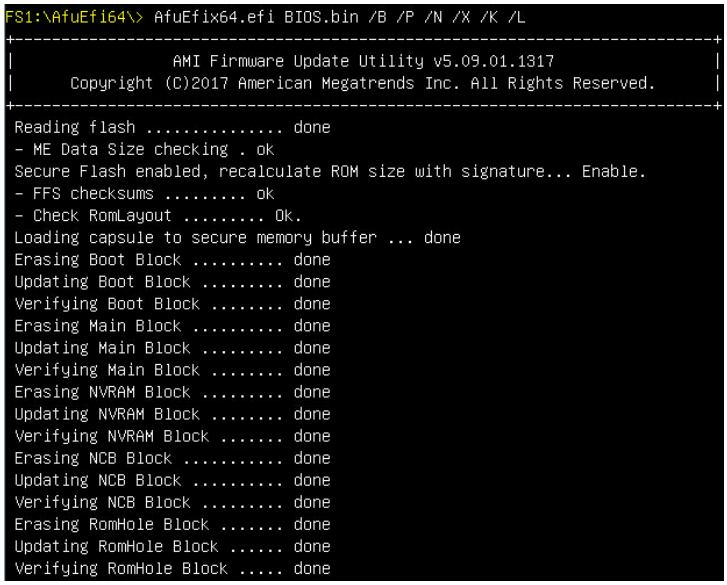


Figure 8-79

4) If there are any changes in ME part, execute the command to update 32M ME+BIOS:

AfuEfix64.efi BIOS.bin /b /p /n /x /k /l /me, and the process is as shown in the following figure.

Parameter instructions:

- /B Program Boot Block
- /P Program main bios image
- /N Program NVRAM
- /X Do not check ROM ID
- /K Program all non-critical blocks
- /L Program all ROM Holes
- /ME Program ME Entire Firmware Block

```
FS1:\AfuEfi64\> AfuEfix64.efi BIOS.bin /B /P /N /X /K /L /ME
+--------------------------------------------------------------------------+
|                AMI Firmware Update Utility v5.09.01.1317                 |
|      Copyright (C)2017 American Megatrends Inc. All Rights Reserved.     |
+--------------------------------------------------------------------------+
 Reading flash ..... done
 - ME Data Size checking . ok
 Secure Flash enabled, recalculate ROM size with signature... Enable.
 - FFS checksums ..... ok
 - Check RomLayout ..... Ok.
 Loading capsule to secure memory buffer ... done
 Erasing Boot Block ..... done
 Updating Boot Block ..... done
 Verifying Boot Block ..... done
 Erasing Main Block ..... done
 Updating Main Block ..... done
 Verifying Main Block ..... done
 Erasing NVRAM Block ..... done
 Updating NVRAM Block ..... done
 Verifying NVRAM Block ..... done
 Erasing NCB Block ..... done
 Updating NCB Block ..... done
 Verifying NCB Block ..... done
 Erasing RomHole Block ..... done
 Updating RomHole Block ..... done
 Verifying RomHole Block ..... done
 - Update success for FDR
 - Update success for GBER |
 - Update success for DER. |
 - Update success for GBEA... |
 - PTT is locked, skip updating.
 - Successful Update Recovery Loader to OPRx!!
 - Successful Update MFSB!!|
 - Successful Update FTPR!!|
 - Successful Update MFS, IVB1 and IVB2!!
 - Successful Update FLOG and UTOK!!
 - ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!
```

Figure 8-80

Note: After the update is complete, 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

There are 32bit and 64bit Linux OS afulnx tools. Taking Linux 64bit OS as an example, use

the afulnx_64 tool to enter the directory containing afulnx_64 tool. Meanwhile, put the corresponding BIOS bin file into this folder.

When there is no change in ME part, execute the command to update BIOS: ./afulnx_64 BIOS.bin /b /p /n /x /k /l, as shown in the following figure.

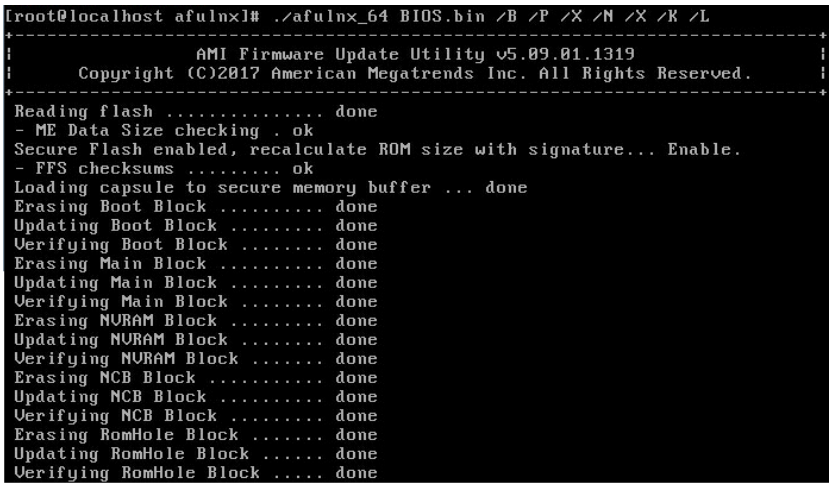


Figure 8-81

If there are any changes in ME part, execute the command to update BIOS and ME simultaneously: ./afulnx_64 BIOS.bin /b /p /n /x /k /l /me, as shown in the following figure.

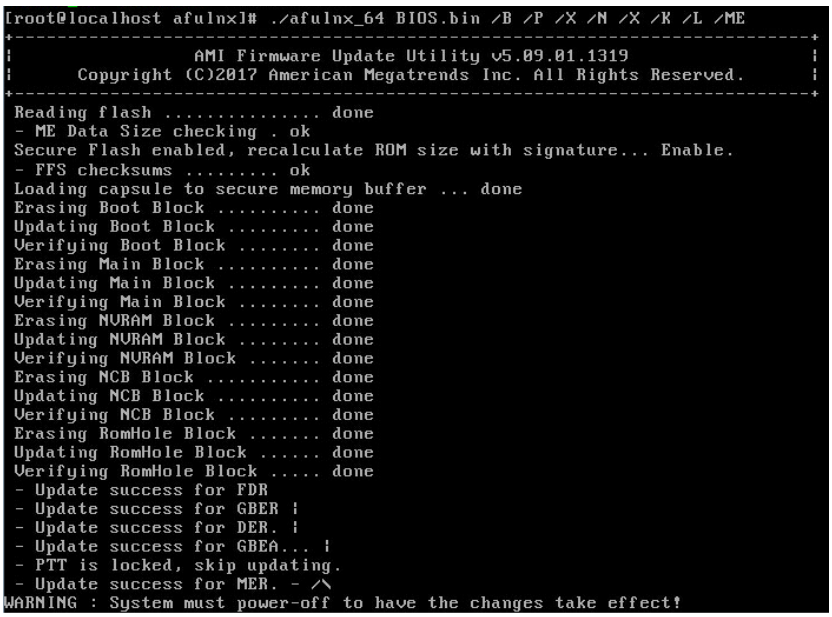


Figure 8-82

Notes:

1. For Linux system, it needs to run the afulnx_64 tool as root.
2. After the update is complete, please power off the machine, and confirm that there is no residual electricity on the motherboard, and then power it on.

9 BMC Settings

9.1 Introduction

This section introduces the specifications that the management software follows and its main functions.

The Inspur Server Management System is a control unit for server management, which is compatible with the standard IPMI2.0 specification.

Below are the main functions of the Inspur Server Management System:

- Remote control

Achieves server control via functions such as KVM (Keyboard Video and Mouse), SOL (Serial Over LAN), virtual media, etc.

⚠ **Note:** SOL function must be implemented via third-party tools, such as IPMITool.

- Warning management

Reports warning message in real time, and carries out corresponding solutions according to the information.

- State monitoring

Monitors the running states of all monitoring units in real time.

- Device information management

Provides device version, model and asset information.

- Heat dissipation control

It could adjust fan speed dynamically according to the ambient temperature and workload.

- Supports IPMITool management

Supports the command operation sent by IPMITool.

- Supports WEB interface management

Provides a friendly and visual interface management. Configuration can quickly be completed as well as query tasks, by simply clicking on the interface.

- Supports account centralized management

It is supported to store accounts in the Active Directory server, direct the authentication

process to server, and achieve management system login with domain accounts.

9.2 Functional Modules

This chapter introduces the Inspur Server Management System module composition, as well as the functions of these modules.

9.2.1 Module Composition

The Inspur Server Management System is mainly composed of IPMI module, command line module, WEB module, KVM Over IP and virtual media.

- The command line module attains the calling of IPMI module. The user performs the operation on IPMI module via command lines.
- The WEB module attains daily management on server in the form of visual interface via calling IPMI commands, and the WEB module integrates functions of KVM and virtual media.

Note: BMC out-of-band access control is enabled by default, allowing WEB or ipmitool out-of-band access.

9.2.2 IPMI Module Introduction

IPMI module attains management of the server system according to the IPMI2.0 standard. The functions of the IPMI module include:

- System real-time monitoring

Provides the alarm report and alarm indication in the event of fault detection.

- System remote control

Meets the management requirements such as remote power-on/off, and business system reset via command lines and Web.

9.2.3 Command Line Function Introduction

The command line module includes query and setting commands for network, sensor, fan, user management, system and server.

9.2.4 Remote Control Module Introduction

The remote control module includes:

- KVM Over IP: A management method that carries out monitoring and control on remote devices via local video, keyboard and mouse to the client, enabling the operation of remote

devices in real-time.

- Virtual Media: A method of providing remote access on local media (CD-ROM, floppy drive or CD/floppy disk iso file) in the form of virtual CD driver and floppy drive on server via the internet.

To use the remote control function, the client should be equipped with appropriate browser and Java runtime environment.

9.3 Web Interface Introduction

This section introduces the Web interface of the management system, as well as operation steps to login the Web interface.

- Login Web interface: Introduces the method to login the Web interface.
- Web interface introduction: Introduces the Web interface layout.

9.3.1 Login Web Interface

This guide introduces the operation steps to login the Web management interface, taking Windows Operating System and Firefox browser as an example.

⚠ **Note:** When carrying out interface operation via Web, a maximum of 20 users can be logged in at the same time.

Step 1: Ensure the management network ports on the client and server are connected to the internet.

Step 2: Open the browser, and enter “http://ipaddress” in the address bar (ipaddress is the actual IP address of the management port. The default login mode is https, and safe operation configuration is needed).

Step 3: The login interface should appear as shown below:

1. Enter the user name and password.

⚠ **Note:** The system provides a default user “admin” in administer user group, and the default password is “admin”. Please change the default password in time after the first login.

2. Click “Login”, to enter the management interface.

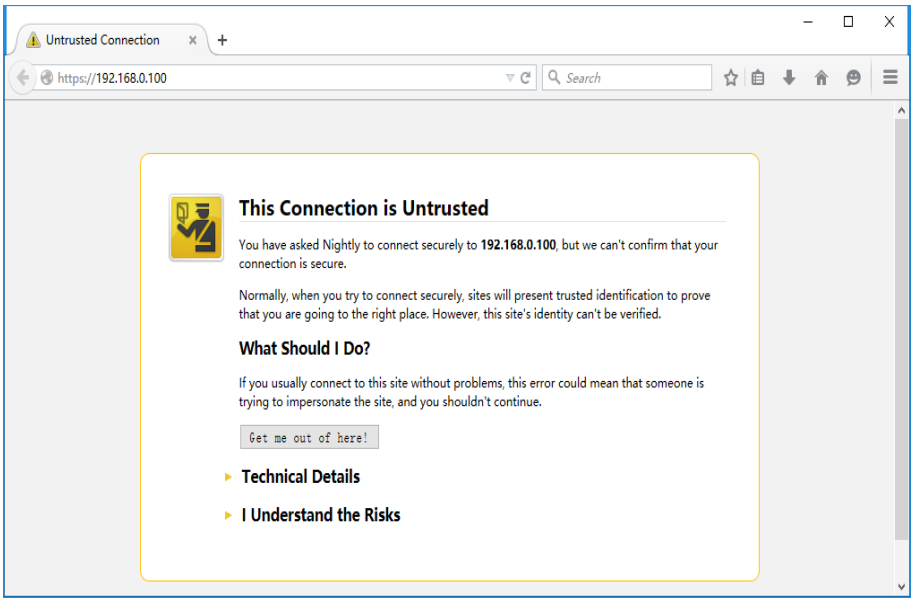


Figure 9-1

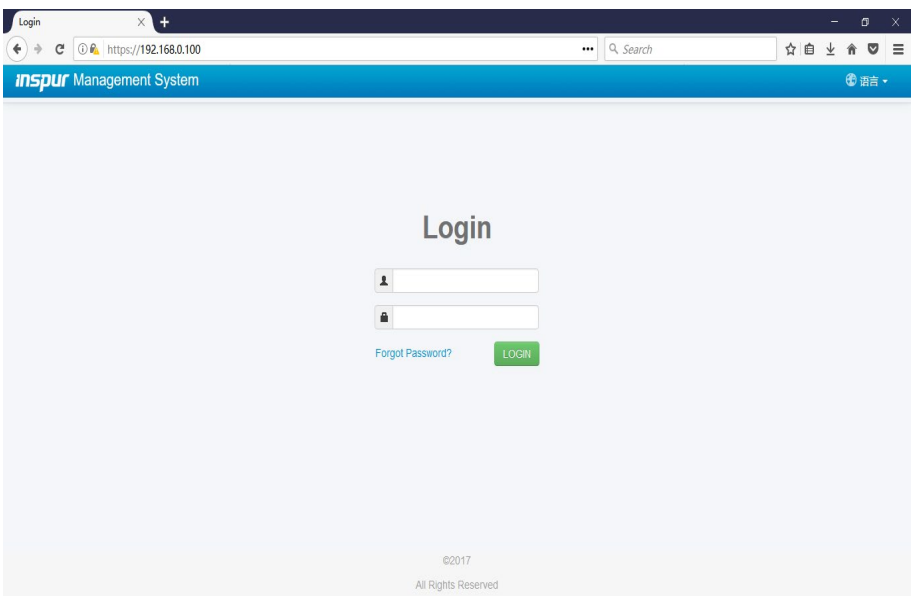


Figure 9-2

9.3.2 Web Interface Introduction

The Web interface helps users accomplish server management. The Web interface also has a help function so users can click the help button 

in the case that they may need it.

The Web interface is divided into several parts, as shown in the following figure.

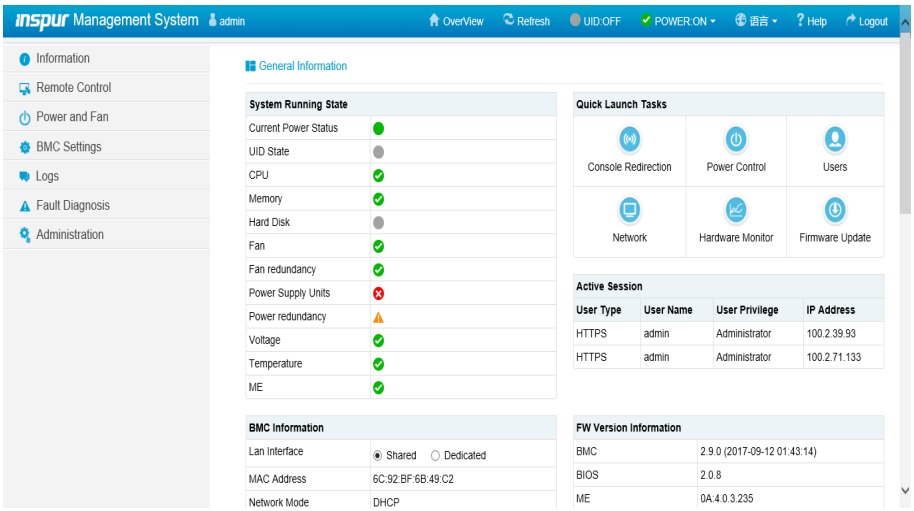


Figure 9-3

- The name of the Web interface is displayed on top left of the interface.
- The meanings of all buttons on top right of the interface:

◇ OverView Click on the Overview button, to return to the overview page.

◇ Refresh Click on the Refresh button, to refresh the page.

◇ UID:ON Click on the UID button, to turn on/off the UID LED.

◇ POWER:ON Click on the Power button, to turn on/off the server.

◇ 语言 Click on the Language button, to change the language (which supports Chinese and English).

◇ Logout Click on the Help button to query help information on the corresponding page.

◇ Help Click on the Logout button, to return to the login page.

- The navigation tree is on the left. Via the nodes on the tree, you can select different functional interfaces. The following functions are included:

◇ View overall situation

◇ View system information

◇ Remote control

◇ Power management

◇ Event and log query

◇ Real-time monitoring

- ◇ Diagnosis and orientation
- ◇ System maintenance
- ◇ System configuration

For detailed introduction on all functions, please refer to the following chapters.

- Specific operation interface is on the right of the interface.

9.3.3 Overview

Click on Overview to open the “General Information” interface, as shown below.

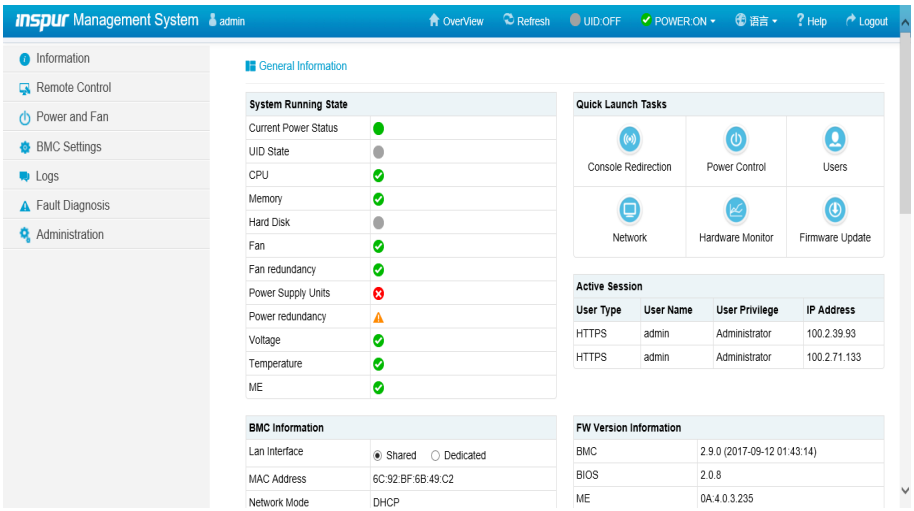


Figure 9-4

9.3.4 Information

Select “Information” on the navigation tree. It contains two interfaces of system information and BIOS setup options, as shown in the following figures below.

System Information: This page shows asset information of the system. You can get different device information via related TAB, including the following devices:

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

- Voltage

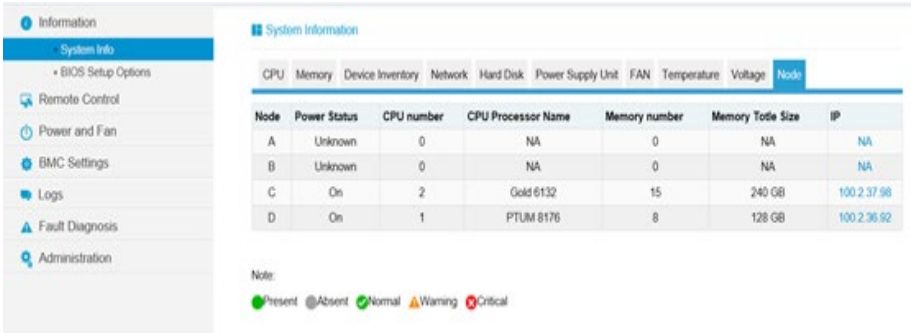


Figure 9-5

BIOS Setup Options: This page displays some important BIOS Setup Options.

- Advanced
- Chipset
- Processor
- Server Mgmt
- Boot

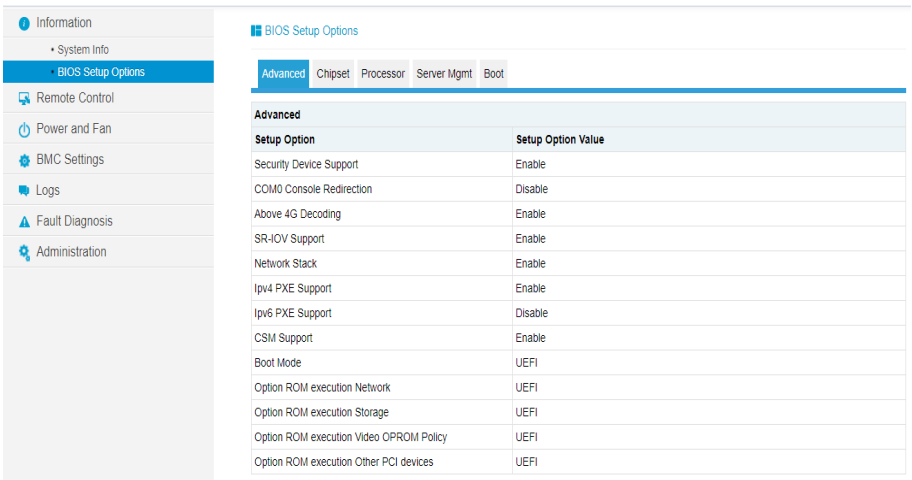


Figure 9-6

9.4 Remote Control

Select “Remote Control” on the navigation tree to open the remote control interface, which contains five interfaces of console redirection (KVM)”, server location, configure remote session, virtual media devices and mouse mode settings, as shown in the following figures.

- Console redirection (KVM): The KVM console window will pop up, Java KVM and HTML5 KVM are supported.
- Server location: To turn on/off the system ID LED.
- Configure remote session: To set the KVM session encryption, media encryption and

virtual media connection methods.

- Virtual media devices: To set the quantity of virtual media (floppy devices, CD/DVD devices and hard disk drives, etc.).
- Mouse mode settings: To set the mouse working mode for KVM remote console.

9.4.1 Console redirection (KVM)

Launch the remote console redirection window from this page. To launch it, you must have Administrator privileges.

Note: A compatible JRE must be installed in the system prior to the launch of JNLP file.

Actions

Launch KVM HTML5 Viewer

Click 'Launch KVM HTML5 Viewer', one new page will be displayed.

Launch KVM Java Viewer

Click 'Launch KVM' which will cause the jviewer.jnlp file to be downloaded. Once the file is downloaded and launched, a Java redirection window will be displayed.

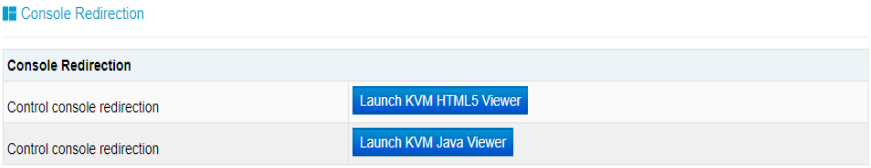


Figure 9-7

9.4.2 Locate Server

This page will help you to view System ID LED Status, and open or close the LED.

System ID LED Status

Shows the current System ID LED Status. ON: System ID LED open, OFF: System ID LED closed.

System ID LED Light Time

- All the time: System ID LED will be open all the time.
- 10s: System ID LED will be closed after 10s.
- 20s: System ID LED will be closed after 20s.
- 60s: System ID LED will be closed after 60s.
- Other: You can enter 1 to 255 seconds. System ID LED will be closed after configured seconds.

System ID LED Operation

- Turn On Led
- Turn Off Led

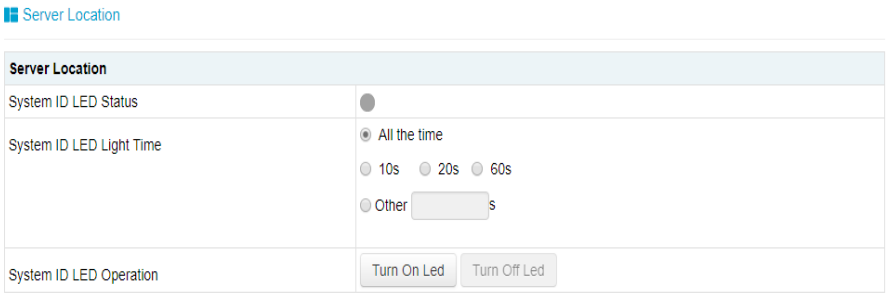


Figure 9-8

9.4.3 Remote Session

This page is used to configure virtual media configuration settings for the next redirection session.

Encrypt H5Viewer KVM packets

Check this option to enable Encrypt H5Viewer KVM packets.

Keyboard Language

To select the Keyboard Language.

Virtual Media Attach Mode

Two types of VM attach mode are available:

- Attach - Immediately attaches Virtual Media to the server upon bootup.
- Auto Attach - Attaches Virtual Media to the server only when a virtual media session is started.

Retry Count

Number of times to be retried in case a KVM failure occurs. Retry count ranges from 1 to 6.

Retry Time Interval (Seconds)

Number of seconds to wait for subsequent retries. Time interval ranges from 5 to 30 seconds.

Server Monitor OFF Feature Status

Check this option to enable Server Monitor OFF Feature Status.

Automatically OFF Server Monitor, When KVM Launches

Check this option to enable Automatically OFF Server Monitor, When KVM Launches.

Actions

Save

Click ‘Save’ to save the current changes.

Note: It will automatically close the existing remote redirection either KVM or Virtual media sessions, if any.

Reset

Click ‘Reset’ to reset the modified changes.

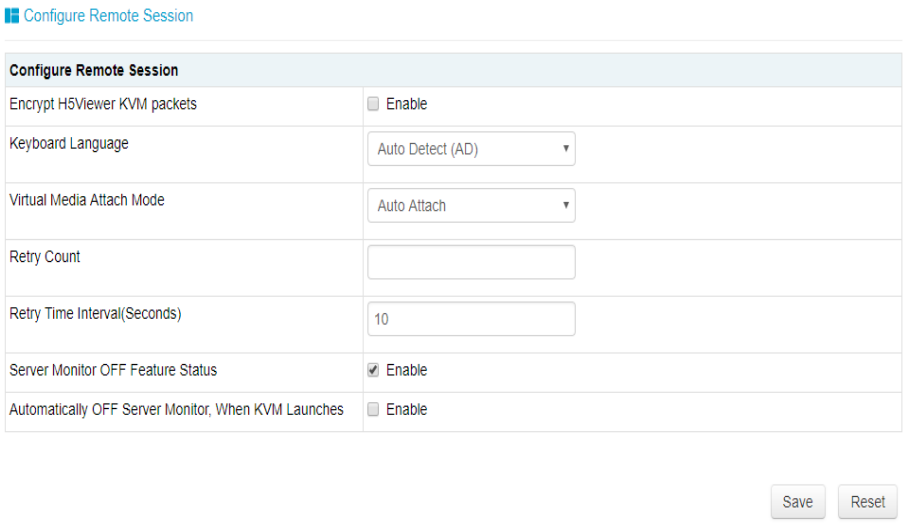


Figure 9-9

9.4.4 Virtual Media

9.4.4.1 Virtual Media Setup

Local Media Support

To enable or disable local media support, check or uncheck the checkbox respectively.

Remote Media Support

To enable or disable remote media support, check or uncheck the checkbox respectively. If it is selected, then following remote media types will be displayed.

- CD/DVD
- Floppy
- Hard disk

On selecting the individual media types, its respective configuration will be displayed. Users can configure different settings for different remote media types.

Mount CD/DVD

Check this option to enable mount CD/DVD.

Server Address for CD/DVD Images

Address of the server where the remote media images are stored.

Path in server

Source path to the remote media images.

Share Type for CD/DVD

Share Type of the remote media server either NFS or Samba (CIFS).

Username, Password and Domain Name

- If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
- Note: Domain Name field is optional.

Same Settings for Floppy/Hard disk Images

If Same Settings for Floppy/Hard disk Images option is selected, then the entered CD/DVD media type data configuration will be same for Floppy and Hard disk remote media types.

Mount Floppy

Check this option to enable mount floppy.

Server Address for Floppy Images

Address of the server where the remote media images are stored.

Path in server

Source path to the remote media images.

Username, Password and Domain Name

- If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
- Note: Domain Name field is optional.

Mount Hard disk

Check this option to enable mount hard disk.

Server Address for Hard disk Images

Address of the server where the remote media images are stored.

Path in server

Source path to the remote media images.

Username, Password and Domain Name

- If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
- Note: Domain Name field is optional.

Actions

Save

Click ‘Save’ to save the configured settings.

Reset

Click ‘Reset’ to reset the previously-saved values.

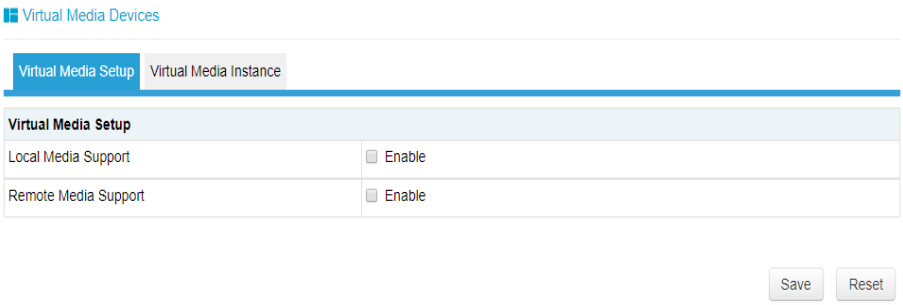


Figure 9-10

9.4.4.2 Virtual Media Instance

Floppy devices

Select the number of floppy devices that support for virtual media redirection.

CD/DVD devices

Select the number of CD/DVD devices that support for virtual media redirection.

Hard disk devices

Select the number of hard disk devices that support for virtual media redirection.

Remote KVM floppy devices

Select the number of Remote KVM floppy devices that support for virtual media redirection.

Remote KVM CD/DVD devices

Select the number of KVM CD/DVD devices that support for virtual media redirection.

Remote KVM hard disk devices

Select the number of KVM hard disk devices that support for virtual media redirection.

SD media support

Check this option to enable SD media support in BMC.

Encrypt media redirection packets

Check this option to enable encrypt media redirection packets.

Power save mode

Check this option to enable the power save mode in BMC.

Actions

Save

Click ‘Save’ to save the configured settings.

Reset

Click ‘Reset’ to reset the previously-saved values.

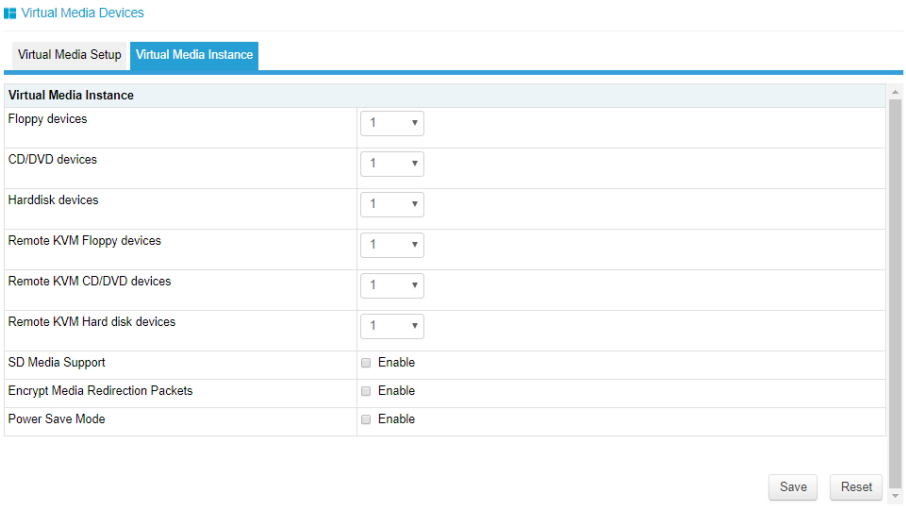


Figure 9-11

9.4.5 Mouse Mode Settings

The Redirection Console handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure this option.

- - Relative Mouse mode
- - Absolute Mouse mode
- - Other Mouse mode

Options

Relative Mouse mode

The relative position of the local mouse is sent to the server.

To select this mode select the "Set mode to Relative" option.

Absolute Mouse mode

The absolute position of the local mouse is sent to the server. To select this mode select the "Set mode to Absolute" option.

Other Mouse mode

Select other mode to have the calculated displacement from the local mouse in the center position, sent to the server.

Use this mode for SLES 11 Linux OS installation.

Actions

Save

Click 'Save' to save any changes made.

Reset

Click 'Reset' to reset the modified changes.

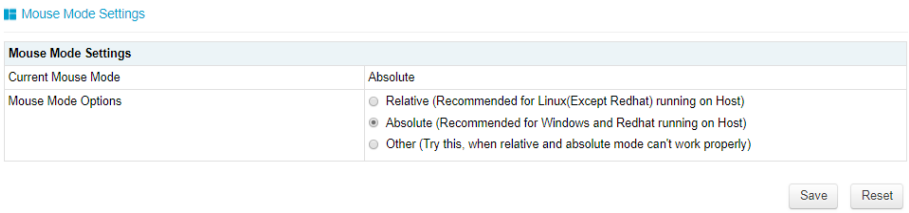


Figure 9-12

9.5 Power and Fan

Select “Power Supply and Fan” on the navigation tree to open the power supply and fan interface. It contains four interfaces of power supply monitor, server power control, power peak settings and fan speed control, as shown in the following figures.

- Power supply monitor: Contains present state, alert, temperature, input power, output power, input voltage, output voltage, input current, output current and firmware version information.
- Server power control: Contains the server’s power on/off and reset, as well as the power policy on AC power loss.
- Power peak settings: To enable or disable the power peak, and set the maximum random time.
- Power consumption: To enable or disable power control, or to add policy.
- Fan speed control: Contains fan status, current speed and speed control function.

9.5.1 Power Supply Monitor

This page displays the status of power supply on the host. You can get the following information for a single power supply unit:

- ID
- Present
- Alert: Alert Information
- Temp(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

- FW Version: FW Version of power supply unit

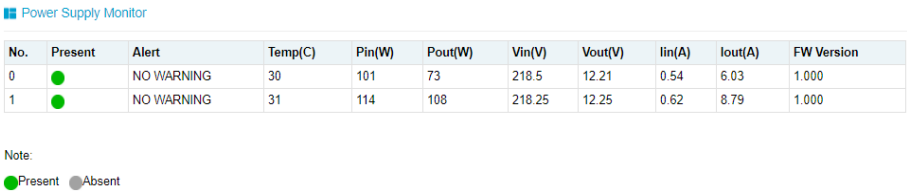


Figure 9-13

9.5.2 Server Power Control

- Virtual power button
- Power restore setting

Virtual Power Button

This tab helps you to view or perform any host power cycle operation.

Power On

Select this option to power on the server.

Power Off

Select this option to immediately power off the server.

Power Cycle

Select this option to first power off, and then reboot the system (cold boot).

Hard Reset

Select this option to reboot the system without powering off (warm boot).

ACPI Power Off

Select this option to initiate operating system shutdown prior to the shutdown.

Actions

Perform Action

Click ‘Perform Action’ to perform the selected option.

Power Restore Setting

This tab can be used to configure the power restore policy. The power restore policy determines how the system or chassis behaves when AC power returns after AC power loss.

Always Power On

Chassis always powers up after AC/mains is applied or returns.

Always Power Off

Chassis always stays powered off after AC/mains is applied, power pushbutton or command required to power on system.

Restore Last Power State

After AC/mains is applied or returns, power is restored to the state that was in effect when AC/mains was removed or lost.

Actions

Perform Action

Click 'Perform Action' to perform the selected option.

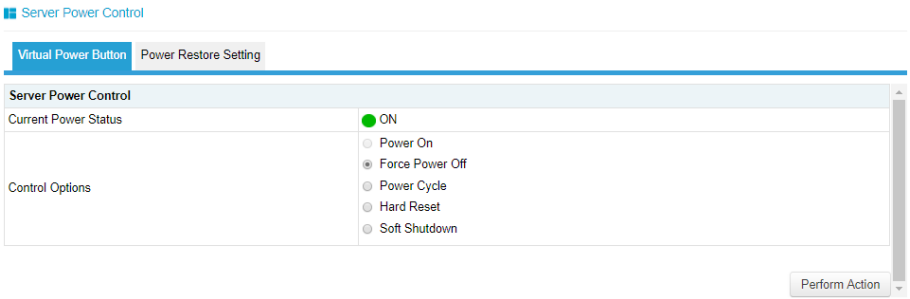


Figure 9-14

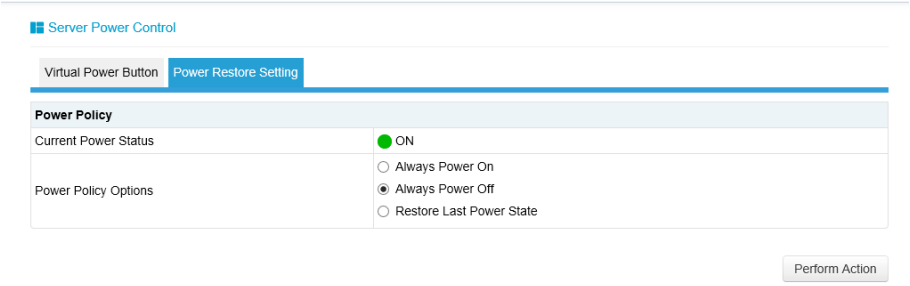


Figure 9-15

9.5.3 Power Peak Settings

The displayed table shows the Power Peak status. You can modify the Power Peak time from here.

Actions

Power Peak

-Select "Enabled" to enable Power Peak function.

-Select "Disabled" to disable Power Peak function.

The power peak maximum random time

-You can set power peak maximum random time from here, the range of time is 1s-600s.

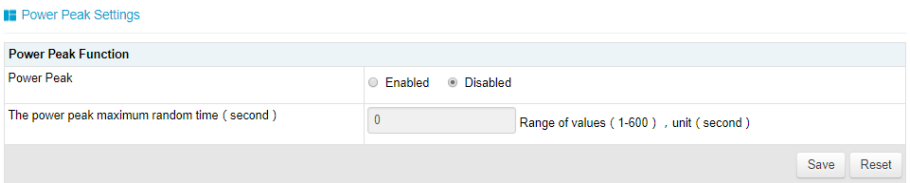


Figure 9-16

9.5.4 Power Consumption

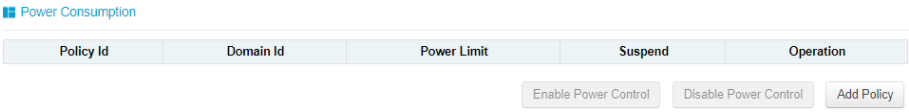


Figure 9-17

9.5.5 Fan Speed Control

This page shows system fan status and fan speed, and you can manually set fan speed in this page.

Manual fan control

Enable/Disable Manual fan control mode.

Speed control

There are four levels for every fan. You can click different level for setting fan speed.

- Low: Set fan duty to 20%.
- Medium: Set fan duty to 50%.
- High: Set fan duty to 75%.
- Full: Set fan duty to 100%.

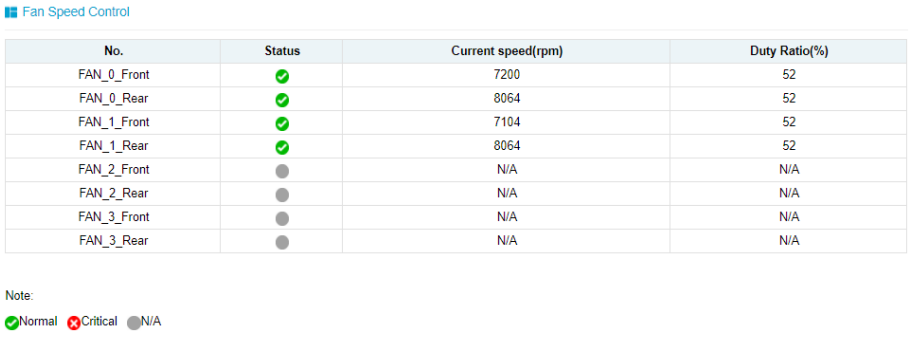


Figure 9-18

9.6 BMC Settings

Select “BMC Settings” on the navigation tree to open the BMC Settings interface. It contains seven interfaces of BMC network management, services, NTP settings, SMTP settings, alert settings, BMC share NIC switch and BIOS boot options, as shown in the following figures.

- BMC network management: Contains BMC network (static IP and DHCP), DNS settings and network interface bonding and network link information.
- Services: To configure the BMC’s Web service, KVM service, ssh service, telnet service, etc.
- NTP settings: To set the BMC time, which has two methods:
  - Synchronize from NTP server.

➢ Sets time manually.

- SMTP settings: To set the SMTP server information related to alert.
- Alert settings: To set the alert event filtering and alert targets of BMC management module.
- BMC share NIC switch: Contains NCSI type switch, NCSI mode switch and channel switch.
- BIOS boot options: To set the boot option after BIOS reset.

9.6.1 BMC Network Settings

This page contains BMC network (static IP and DHCP), DNS settings and network interface bonding and network link information.

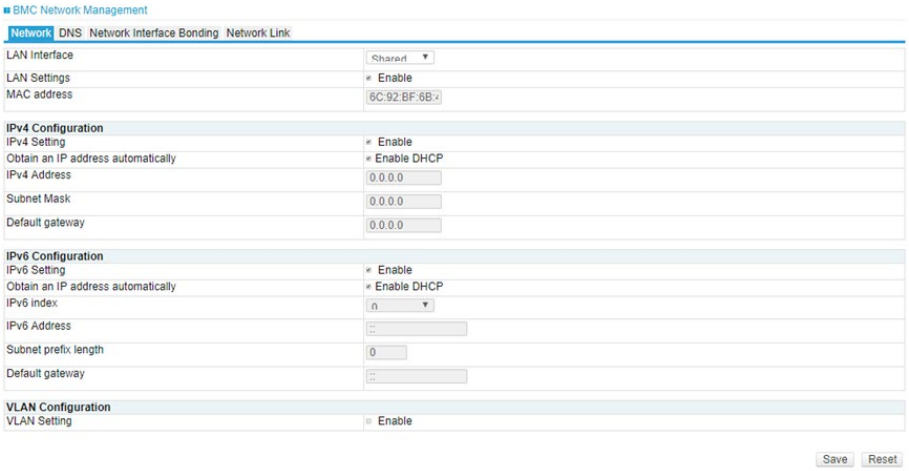


Figure 9-19

9.6.2 Services

This page is displays the basic information about services running in the BMC. To modify a service, user must be an Administrator.

Services

#	Service Name	Current State	Interfaces	Nonsecure Port	Secure Port	Timeout(s)	Maximum Sessions	Active Sessions
1	web	Active	both	80	443	1800	20	2
2	kvm	Active	both	7578	7582	1800	4	0
3	cd-media	Active	both	5120	5124	N/A	4	0
4	fd-media	Active	both	5122	5126	N/A	4	0
5	hd-media	Active	both	5123	5127	N/A	4	0
6	ssh	Active	N/A	N/A	22	600	N/A	0
7	telnet	Inactive	N/A	23	N/A	600	N/A	0
8	solssh	Inactive	N/A	52123	N/A	60	N/A	0

Figure 9-20

Note: Web, kvm, cd-media, fd-media, hd-media and ssh services are enabled by default. Telnet and solssh services are disabled by default.

9.6.3 NTP Settings

This page displays the device's current Date & Time Settings. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

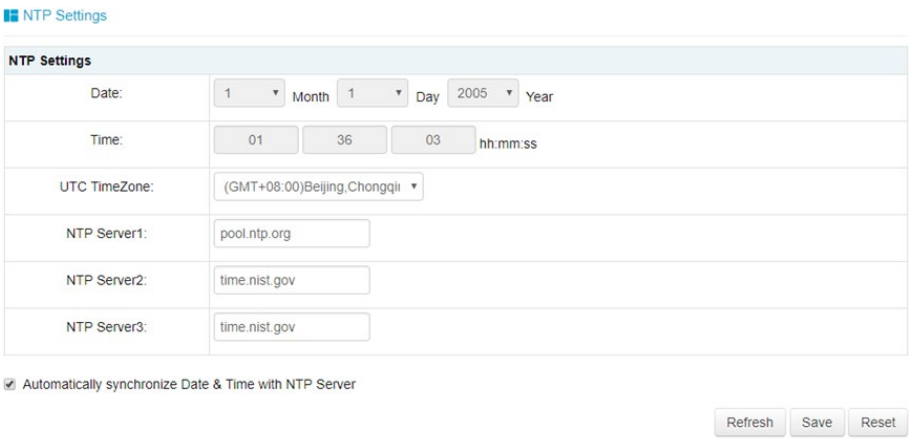


Figure 9-21

9.6.4 SMTP Settings

This page is used to configure the SMTP settings.

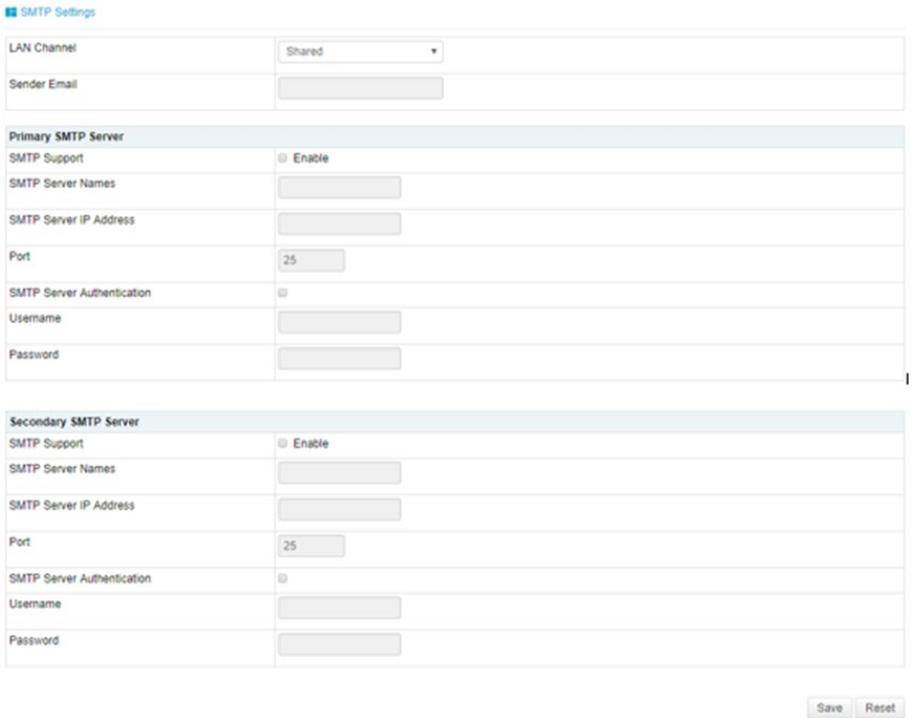


Figure 9-22

9.6.5 Alert Settings

You can configure snmp trap alert and smtp alert in this page.

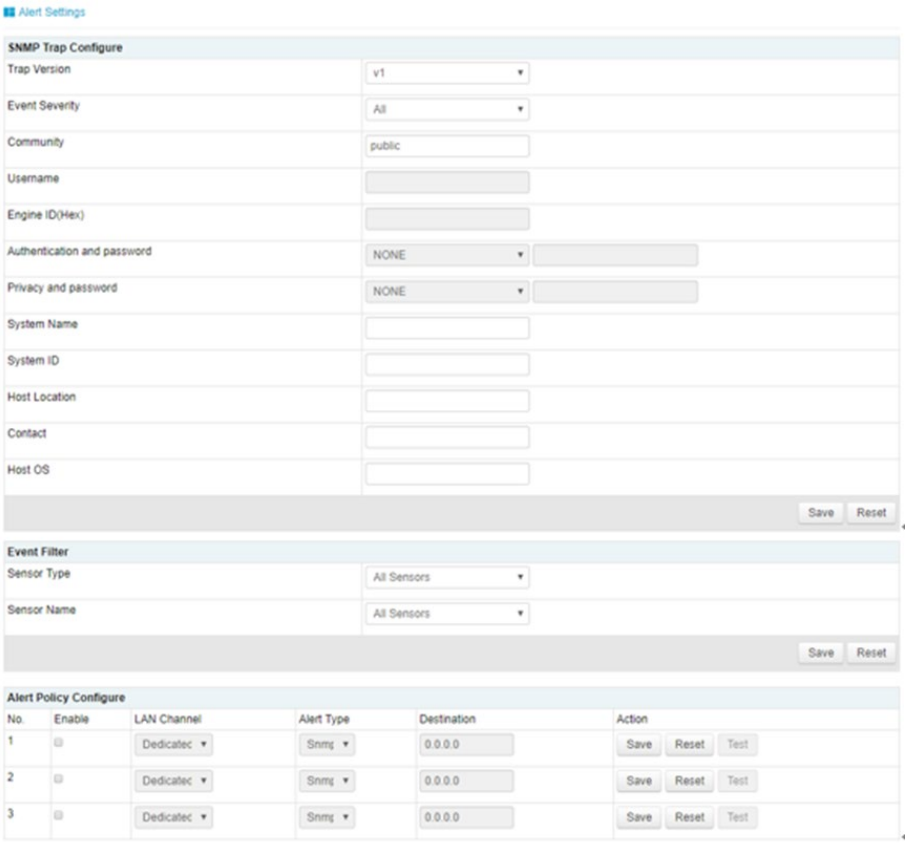


Figure 9-23

9.6.6 BMC Share NIC Switch

This page is used to switch BMC Share NIC.

Actions

NCSI Mode

Select this radio button to change NCSI Mode to Auto Failover Mode or Manual Switch Mode.

Share NIC Switch

It lists the interface names in list box. Choose the particular interface name that you wanted.

NCSI Type

Choose the NCSI Card Type.

Channel Number

Choose the channel number to be configured for the selected interface name.

Package ID

Choose the package ID to be configured for the selected interface name.

Save

Click ‘Save’ to save the current changes.

Reset

Click ‘Reset’ to reset the modified changes.

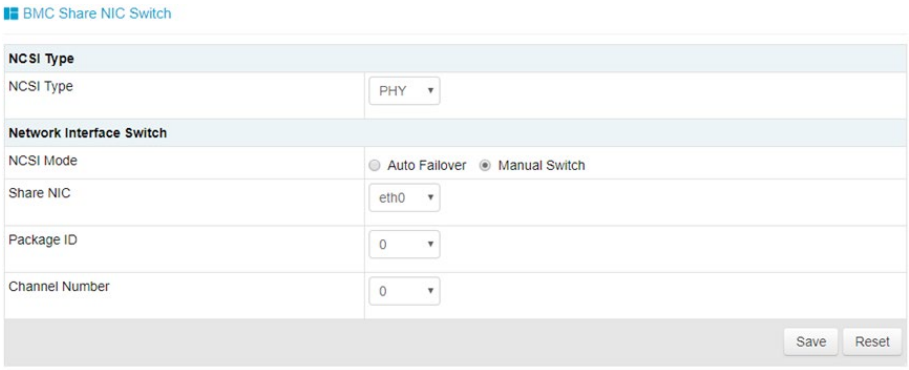


Figure 9-24

9.6.7 BIOS Boot Options

This page shows the system boot option. You can set parameters that direct the system boot following a system power up or reset.

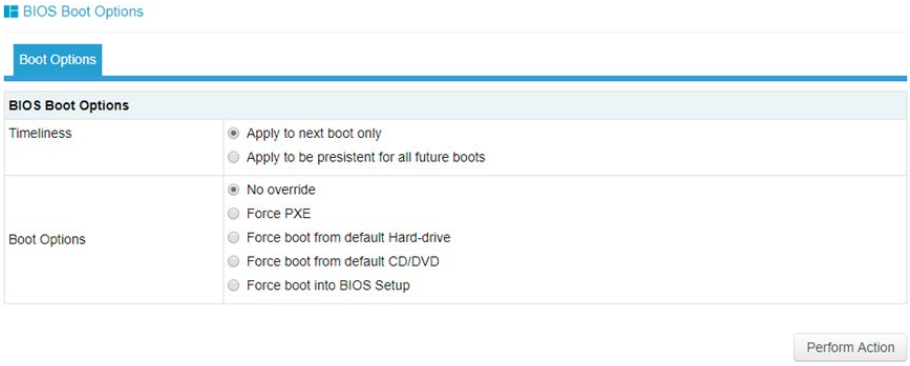


Figure 9-25

9.7 Logs

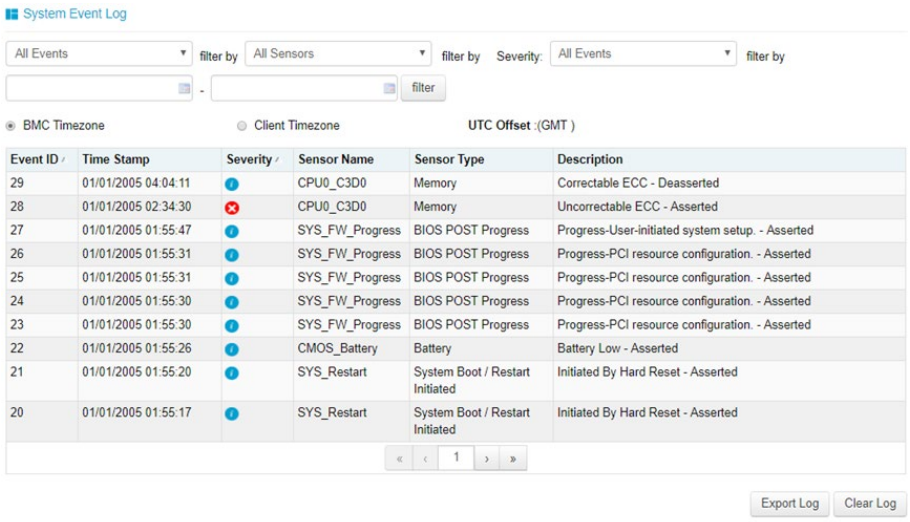
Select “Logs” on the navigation tree to open the related log interface. It contains five interfaces of system event log, BMC system audit log, black box log, event log setting and system and audit log settings, as shown in the following figures.

- System event log: Displays various event logs generated by the server.
- BMC system audit log: Displays system logs and audit logs of BMC.
- Black box log: Used to import fault logs. The black box logs are encrypted by default, and need to be decrypted to view.

- Event log setting: To set the BMC log storage policy:
  - ➢ Linear strategy: To clear all logs after log storage is full and record again.
  - ➢ Circular strategy: To record circularly after log record is full.
- System and audit log settings: To set the log type, file size and other information of BMC system audit logs.

9.7.1 System Event log

This page displays the list of events incurred by different sensors on this device.

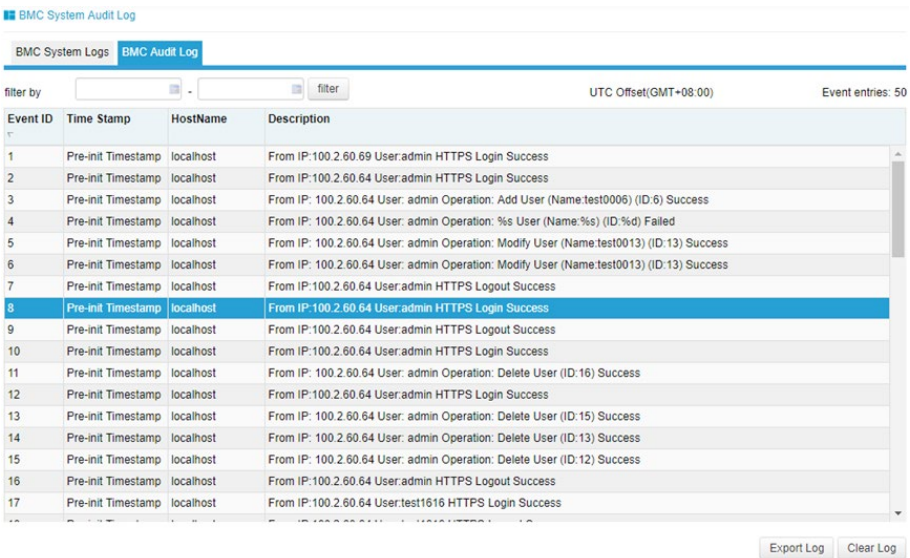


Event ID	Time Stamp	Severity	Sensor Name	Sensor Type	Description
29	01/01/2005 04:04:11		CPU0_C3D0	Memory	Correctable ECC - Deasserted
28	01/01/2005 02:34:30		CPU0_C3D0	Memory	Uncorrectable ECC - Asserted
27	01/01/2005 01:55:47		SYS_FW_Progress	BIOS POST Progress	Progress-User-initiated system setup. - Asserted
26	01/01/2005 01:55:31		SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
25	01/01/2005 01:55:31		SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
24	01/01/2005 01:55:30		SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
23	01/01/2005 01:55:30		SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
22	01/01/2005 01:55:26		CMOS_Battery	Battery	Battery Low - Asserted
21	01/01/2005 01:55:20		SYS_Restart	System Boot / Restart Initiated	Initiated By Hard Reset - Asserted
20	01/01/2005 01:55:17		SYS_Restart	System Boot / Restart Initiated	Initiated By Hard Reset - Asserted

Figure 9-26

9.7.2 BMC System & Audit logs

If configured, these logs display all the system and audit events that occurred on this device.



Event ID	Time Stamp	HostName	Description
1	Pre-init Timestamp	localhost	From IP:100.2.60.69 User:admin HTTPS Login Success
2	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Login Success
3	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Add User (Name:test0006) (ID:6) Success
4	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: %s User (Name:%s) (ID:%d) Failed
5	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Modify User (Name:test0013) (ID:13) Success
6	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Modify User (Name:test0013) (ID:13) Success
7	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Logout Success
8	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Login Success
9	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Logout Success
10	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Login Success
11	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Delete User (ID:16) Success
12	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Login Success
13	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Delete User (ID:15) Success
14	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Delete User (ID:13) Success
15	Pre-init Timestamp	localhost	From IP: 100.2.60.64 User: admin Operation: Delete User (ID:12) Success
16	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:admin HTTPS Logout Success
17	Pre-init Timestamp	localhost	From IP:100.2.60.64 User:test1616 HTTPS Login Success

Figure 9-27

9.7.3 Black Box Log

You can export Black Box Log in this page. You should select the log and click 'Export Log' to get the log you wanted.

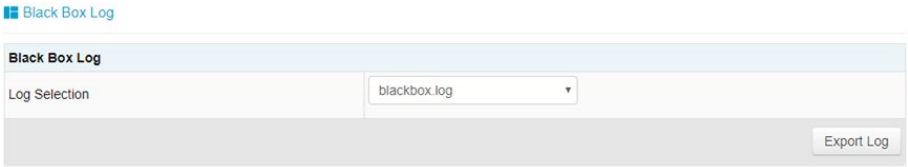


Figure 9-28

9.7.4 Event Log Setting

This page is used to configure the System Event log information.

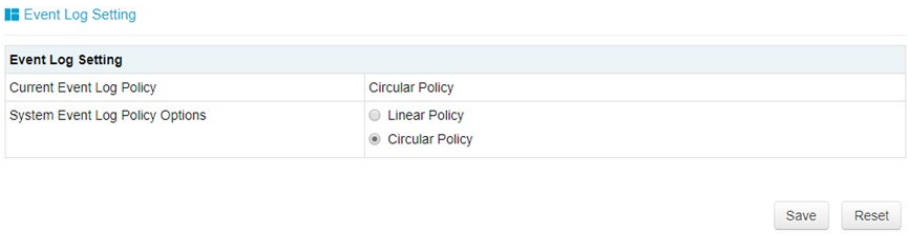


Figure 9-29

9.7.5 System & Audit Log Settings

This page is used to configure the System and Audit log settings.

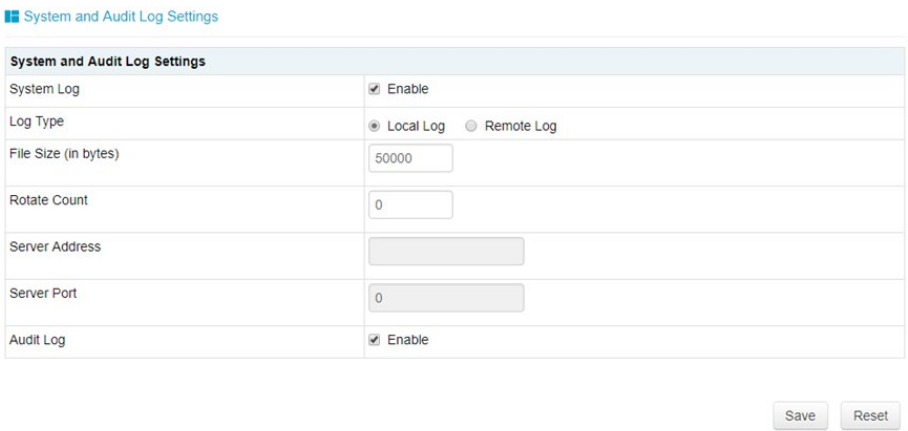


Figure 9-30

9.8 Fault Diagnosis

Select "Fault Diagnosis" on the navigation tree to open the fault diagnosis interface. It contains four interfaces of BMC self-inspection result, BMC recovery, capture screen and host POST code, as shown in the following figures.

- BMC self-inspection result: To view the BMC self-inspection result.
- BMC recovery: Contains two functions of BMC warm reset and KVM service restart.
- Capture screen: Used to record the information on the last screen at system crash.

Note: To support BSOD (Blue Screen Of Death) screen capturing, server OS should be Windows 2012R2 and above.

- Host POST code: Displays POST code during system startup.

9.8.1 BMC Self-inspection Result

This page shows current BMC Self-inspection Result.

Figure 9-31

9.8.2 BMC Recovery

You can reset BMC function modules below.

- BMC Warm Reset
- KVM Service Restart

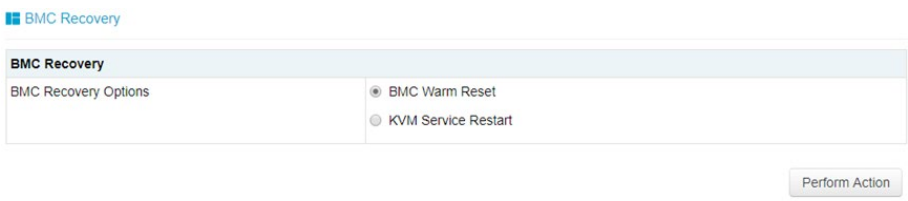


Figure 9-32

9.8.3 Capture Screen

This page displays the screens captured after power reset or power off. Support BSOD (Blue Screen Of Death) screen capturing, server OS should be Windows 2012R2 and above. Go to Manual Capture tab to capture current server screen.

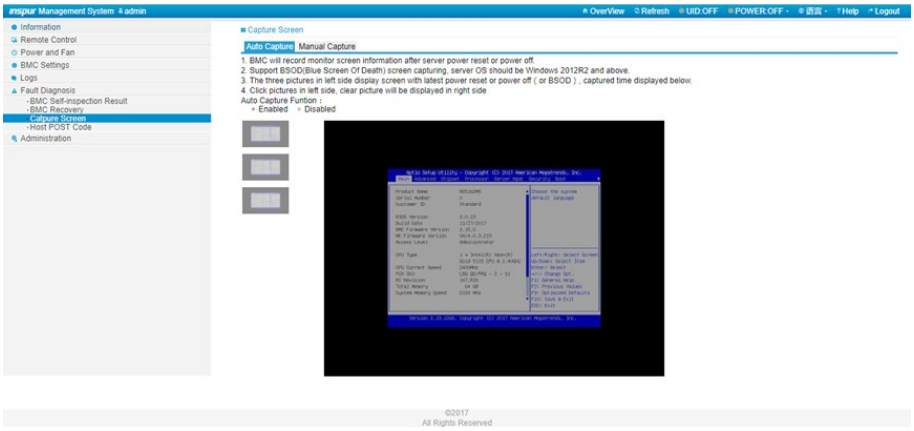


Figure 9-33

9.8.4 Host POST Code

This page shows current Host POST from system port 80.

- POST Code
- POST Records

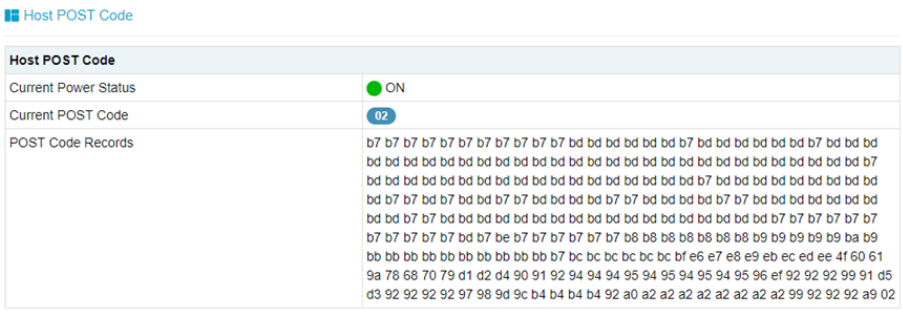


Figure 9-34

9.9 Administration

Select “Administration” on the navigation tree to open the administration interface. It contains six interfaces of user administration, security, dual image configuration, BMC firmware update, BIOS firmware update and restore factory defaults, as shown in the following figures.

- User administration: To add, delete or modify users via BMC Web interface.
- Security: To configure LDAP and AD servers via BMC Web interface.
- Dual image configuration: To configure the boot options in dual image mode via BMC Web interface.
- Dual firmware update: To update BMC FW via BMC Web interface.
- BIOS firmware update: To update BIOS FW via BMC Web interface.

- Restore factory defaults: To restore BMC's configuration to factory state.

Note: BMC supports the force reset operation via the Reset button on the rear of the chassis, and supports the force factory reset operation via the jumper on the motherboard.

9.9.1 User Administration

This page is used to configure the System Administrator configuration.

Options

Username

Username of System Administrator is displayed (read only).

Change Password

To change the user's password, check the 'Change Password' option. This will enable the password fields.

Password, Confirm Password

Enter and confirm the new password here.

- - Password must be at least 8 characters long.
- - Password must be include Special, Uppercase, Lowercase characters and Numbers.
- - White space is not allowed.

Note: This field will not allow more than 64 characters.

Actions

Save

Click 'Save' to save the new configuration for system administrator.

Reset

Click 'Reset' to reset the modified changes.

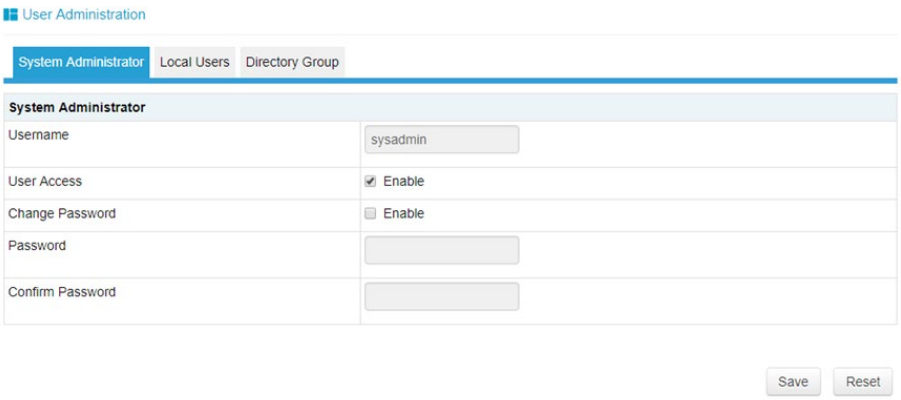


Figure 9-35

9.9.2 Security

Use this page to configure advanced LDAP/AD settings.

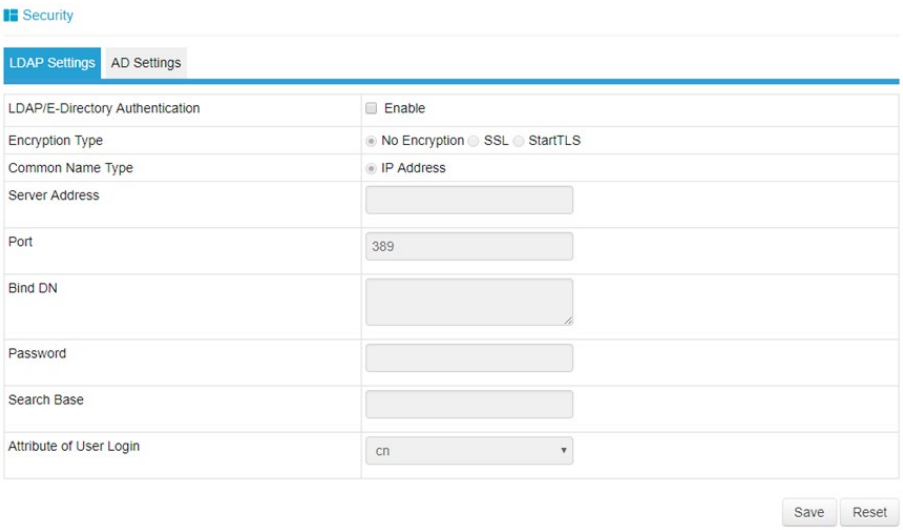


Figure 9-36

9.9.3 Dual Image configuration

This page helps you to view or perform dual image configuration.

Firmware Version

It displays the firmware version of image.

State

It displays the current state of image.

Image to be booted from upon reset

Check this option to boot image-1 in the next boot up process.

Higher firmware version

Check this option to boot higher firmware version image among the dual images in the next boot up process.

Lower firmware version

Check this option to boot lower firmware version image among the dual images in the next boot up process.

Newest updated firmware

Check this option to boot the newest updated firmware image among the dual images in the next boot up process.

Not newest updated firmware

Check this option to boot not the newest updated firmware image among the dual images in the next boot up process

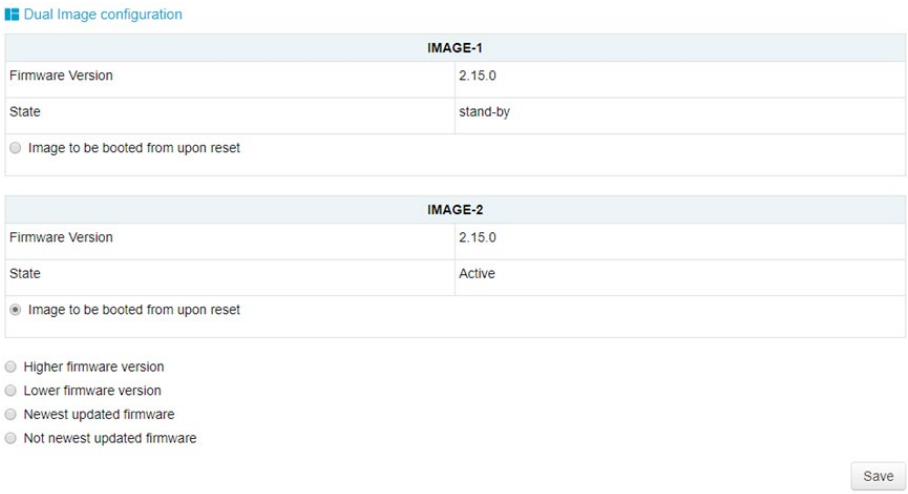


Figure 9-37

9.9.4 BMC Firmware Update

This wizard takes you through the process of firmware upgradation

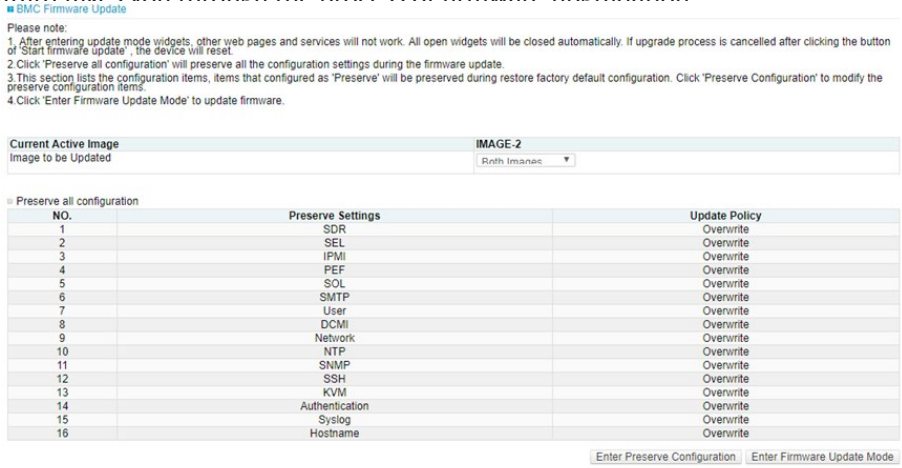


Figure 9-38

9.9.5 BIOS Firmware Update

You can update BIOS firmware in this page. Please follow the steps in the page.

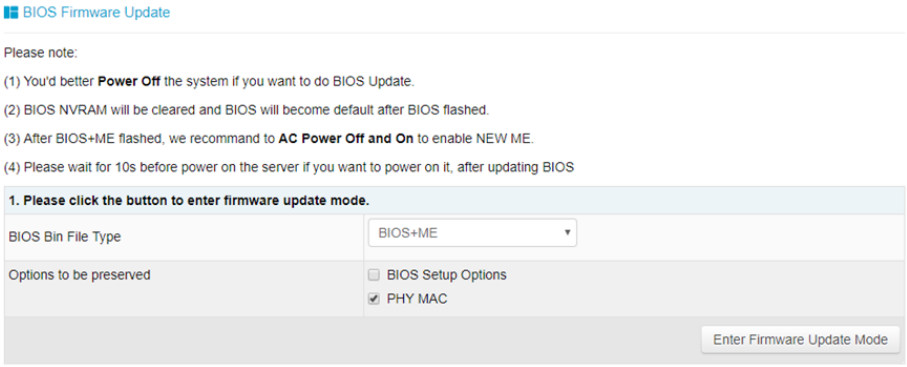


Figure 9-39

9.9.6 Restore Factory Defaults

This page helps to restore the factory defaults of the device.

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

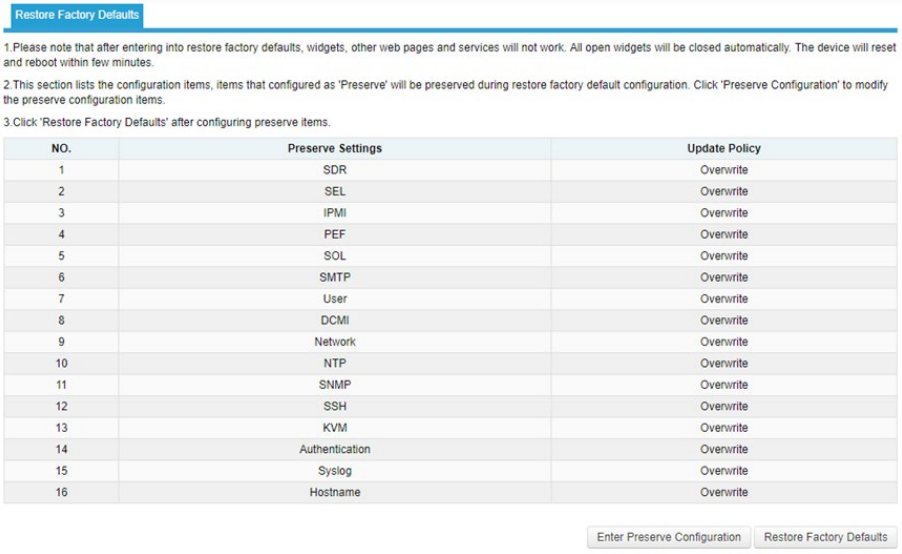


Figure 9-40

9.10 Command Line Function Introduction

This chapter introduces Web interface of the management system, as well as operation steps to login the Web interface.

- Login command line

Introduces methods of login command line.

- Command line function introduction

Introduces command line functions.

9.10.1 Command Line Login

Login to BMC Command line through ssh. After login, enter the command line interface:

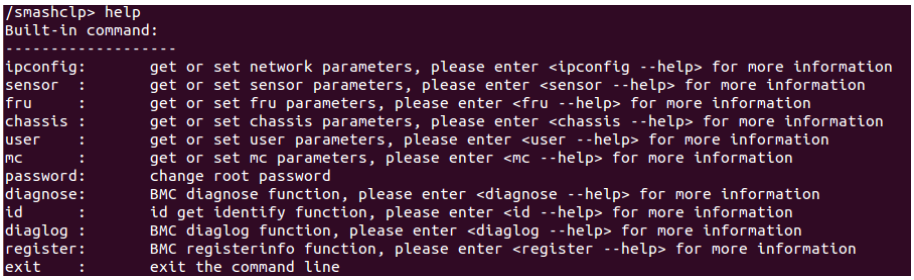


Figure 9-41

Enter help to view the online help information:

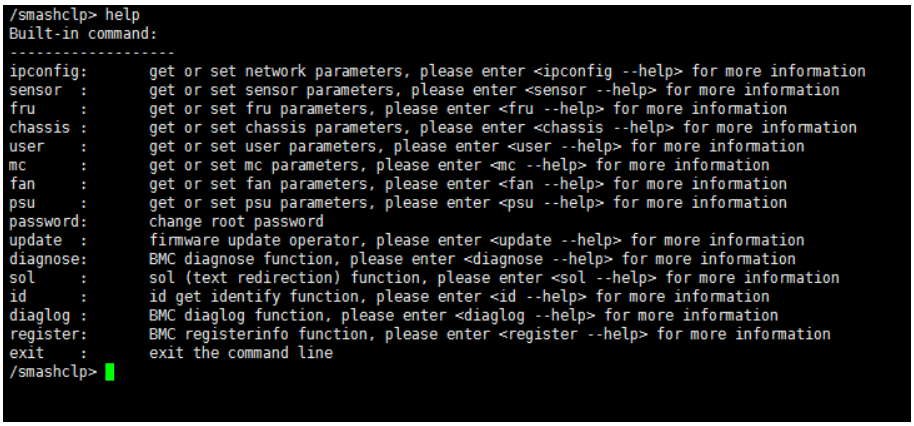


Figure 9-42

9.10.2 Command Line Function Introduction

9.10.2.1 Get and Set Network Information

Via ipconfig command, get and set BMC's network information:

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

Figure 9-43

9.10.2.2 Get Sensor Information

Via sensor command, get the information list of all sensors:

```
/smashclp> sensor --help
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]
/smashclp>
/smashclp> sensor --list
sensor name      | num | value     | unit       | status | lnr       | lc        | lnc       | unc       | uc        | unr
CPU0_Temp        | 19h | na        | degrees C  | na     | na        | na        | na        | 102.000   | 112.000   | na
CPU1_Temp        | 1Ah | na        | degrees C  | na     | na        | na        | na        | 102.000   | 112.000   | na
PCH_Temp         | 1Dh | na        | degrees C  | na     | na        | na        | na        | 100.000   | 110.000   | na
DIMMG0_Temp      | 1Eh | na        | degrees C  | na     | na        | na        | na        | 95.000    | 105.000   | na
DIMMG1_Temp      | 1Fh | na        | degrees C  | na     | na        | na        | na        | 95.000    | 105.000   | na
System_Temp      | 01h | na        | degrees C  | na     | na        | na        | na        | na        | na        | na
Inlet_Temp       | 02h | na        | degrees C  | na     | na        | na        | na        | 40.000    | 50.000    | na
Outlet_Temp      | 00h | na        | degrees C  | na     | na        | na        | na        | na        | na        | na
SYS_VCCIO        | 40h | na        | Volts      | na     | 0.690     | 0.770     | 0.850     | 1.170     | 1.250     | 1.330
SYS_12V          | 43h | na        | Volts      | na     | 9.024     | 9.776     | 10.528    | 13.536    | 14.288    | 15.040
SYS_3.3V         | 44h | na        | Volts      | na     | 2.660     | 2.800     | 2.940     | 3.657     | 3.797     | 3.938
SYS_5V           | 47h | na        | Volts      | na     | 3.888     | 4.176     | 4.464     | 5.544     | 5.832     | 6.120
PCH_P1V05        | 41h | na        | Volts      | na     | 0.770     | 0.850     | 0.930     | 1.170     | 1.250     | 1.330
PCH_P1V5         | 42h | na        | Volts      | na     | 1.180     | 1.260     | 1.340     | 1.670     | 1.750     | 1.830
CPU0_VCORE       | 45h | na        | Volts      | na     | 1.040     | 1.120     | 1.200     | 2.300     | 2.380     | 2.460
CPU1_VCORE       | 46h | na        | Volts      | na     | 1.040     | 1.120     | 1.200     | 2.300     | 2.380     | 2.460
```

Figure 9-44

9.10.2.3 Get and Set FRU Information

Via FRU command, get the FRU configuration information:

```
/smashclp> fru --help
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
/smashclp>
```

Figure 9-45

9.10.2.4 Get and Control Chassis Status

Via chassis command, get and control the system power status:

```
/smashclp> chassis --help
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
/smashclp>
```

Figure 9-46

9.10.2.5 Get User List and Add/Delete User

Via user command, get the user list, add or delete users:

```
/smashclp> user --help
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
         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).
/smashclp>
/smashclp> user --list
ID  Name             Channel Priv Limit
1   root             ADMINISTRATOR
2   admin            ADMINISTRATOR
3                    NO ACCESS
```

Figure 9-47

9.10.2.6 Get BMC Version and Reset BMC

Via mc command, get BMC version information and reset BMC:

```
/smashclp> mc --help
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
/smashclp>
/smashclp> mc --get version
Device ID                 : 32
Device Revision           : 1
Firmware Revision         : 4.2.0
IPMI Version              : 2.0
/smashclp>
```

Figure 9-48

9.10.2.7 Change Root Password

Via password command, change the root user's password:

Figure 9-49

9.10.2.8 Fault Diagnosis

Via diagnose command, execute the tools and commands integrated in BMC to view the BMC status:

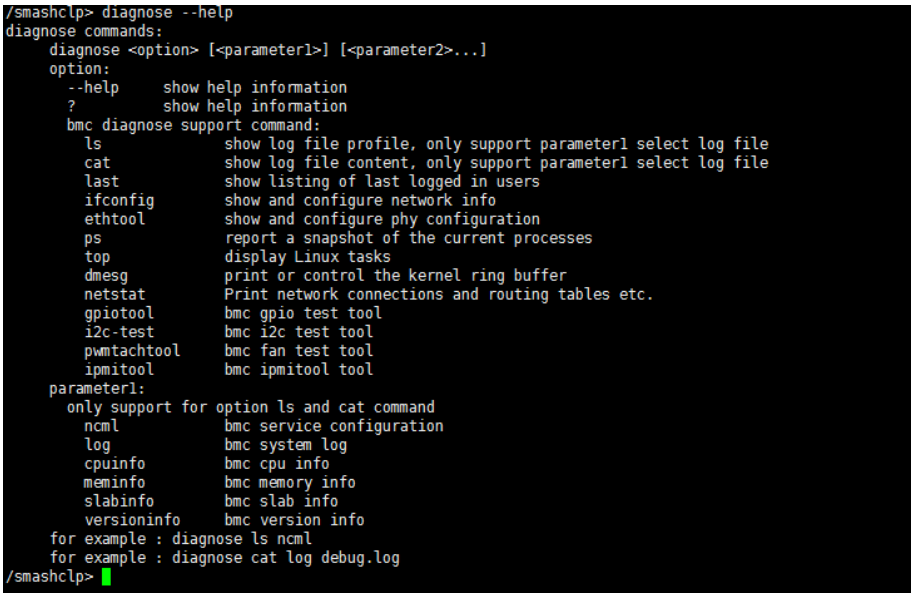


Figure 9-50

9.10.2.9 Collect Fault Logs

Via dialog command, trigger the fault logs collection function. When the server fails, it can quickly collect the fault logs information stored in BMC. The collected fault logs can be downloaded through the browser or wget.

Figure 9-51

9.10.2.10 Serial Over LAN

Via sol command, perform the serial port redirection operation, to view the POST information of the serial ports during system startup.

```
/smashclp> sol --help
sol commands:
     sol <option1>
     option1:
       --help     show help information
       ?          show help information
       --start     start sol (text redirection)
       for example : sol --start
/smashclp>
/smashclp>
/smashclp> sol --start

SOL (text redirection) is going to be executed.
Please remember the exit sequence: ~.

Press any key to continue.
 Notice: SOL (Text Redirection) Starts Successully.
 Please Remember, Exit Sequence: ~.
```

Figure 9-52

9.11 BMC Firmware Update

9.11.1 Firmware Integrity Check

Each firmware image can generate MD5 check code (Hash.exe) through the MD5 tool. Before updating the firmware, MD5 tool must be used to check the image's integrity to ensure that the firmware image file is correct.

9.11.2 WEB Update

The BMC firmware can be updated through the management interface in the web interface. BMC firmware update is configured with watchdog, to avoid that the program stays in the update mode and fails to restore when an exception occurs, and the watchdog time is 20 minutes. When entering the flash mode, the watchdog will be activated, it will automatically reset BMC after 20 minutes timeout. When the image starts to flash, the watchdog timeout will be updated to 20 minutes again.

Supports dual-image firmware update

When updating the BMC firmware, the user can specify the image to update, you can choose:

- Image 1
- Image 2
- Alternate image
- Dual images (default)

⚠ **Note:**

The firmware update process is a critical operation, once you enter the update mode and choose to cancel the firmware update operation, the BMC must reboot, which means that you must close the browser and login to the BMC again before any other action can be

performed.

It defaults to use the higher version of the two images, which you can modify through the interface.

Firmware update steps:

- Go to the update page.
- Choose the image file, and click Upload button to upload the file. BMC will enter the update mode after the file is uploaded. IPMI service will stop, and BMC will check the image's size, which should be 32M, and check the image's integrity to ensure it is the BMC image.

If the check fails, BMC will stop the update and reboot.

- Check the image version and the existed image version, after confirmation, click Update button to start the update.

9.11.3 SOCFlash Update

In Windows/Linux/Dos OS, it uses socflash tool to update the firmware. The steps are as follows:

- Execute the command socflash if=Imagefile to update image1;
- Execute the command socflash if=Imagefile offset=0x2000000 to update image2.

9.12 Time Zone Table

Table 9-1

Name of Time Zone	Time
Dateline Standard Time	(GMT-12:00) International Date Line West
Samoa Standard Time	(GMT-11:00) Midway Island, Samoa
Hawaiian Standard Time	(GMT-10:00) Hawaii
Alaskan Standard Time	(GMT-09:00) Alaska
Pacific Standard Time	(GMT-08:00) Pacific Time (US and Canada); Tijuana
Mountain Standard Time	(GMT-07:00) Mountain Time (US and Canada)
Mexico Standard Time 2	(GMT-07:00) Chihuahua, La Paz, Mazatlan
U.S. Mountain Standard Time	(GMT-07:00) Arizona
Central Standard Time	(GMT-06:00) Central Time (US and Canada
Canada Central Standard Time	(GMT-06:00) Saskatchewan
Mexico Standard Time	(GMT-06:00) Guadalajara, Mexico City, Monterrey

Central America Standard Time	(GMT-06:00) Central America
Eastern Standard Time	(GMT-05:00) Eastern Time (US and Canada)
U.S. Eastern Standard Time	(GMT-05:00) Indiana (East)
S.A. Pacific Standard Time	(GMT-05:00) Bogota, Lima, Quito
Atlantic Standard Time	(GMT-04:00) Atlantic Time (Canada)
S.A. Western Standard Time	(GMT-04:00) Caracas, La Paz
Pacific S.A. Standard Time	(GMT-04:00) Santiago
Newfoundland and Labrador Standard Time	(GMT-03:30) Newfoundland and Labrador
E. South America Standard Time	(GMT-03:00) Brasilia
S.A. Eastern Standard Time	(GMT-03:00) Buenos Aires, Georgetown
Greenland Standard Time	(GMT-03:00) Greenland
Mid-Atlantic Standard Time	(GMT-02:00) Mid-Atlantic
Azores Standard Time	(GMT-01:00) Azores
Cape Verde Standard Time	(GMT-01:00) Cape Verde Islands
GMT Standard Time	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Greenwich Standard Time	(GMT) Casablanca, Monrovia
Central Europe Standard Time	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Central European Standard Time	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Romance Standard Time	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
W. Europe Standard Time	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
W. Central Africa Standard Time	(GMT+01:00) West Central Africa
E. Europe Standard Time	(GMT+02:00) Bucharest
Egypt Standard Time	(GMT+02:00) Cairo
FLE Standard Time	(GMT+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
GTB Standard Time	(GMT+02:00) Athens, Istanbul, Minsk
Israel Standard Time	(GMT+02:00) Jerusalem
South Africa Standard Time	(GMT+02:00) Harare, Pretoria
Russian Standard Time	(GMT+03:00) Moscow, St. Petersburg, Volgograd
Arab Standard Time	(GMT+03:00) Kuwait, Riyadh
E. Africa Standard Time	(GMT+03:00) Nairobi
Arabic Standard Time	(GMT+03:00) Baghdad

Iran Standard Time	(GMT+03:30) Tehran
Arabian Standard Time	(GMT+04:00) Abu Dhabi, Muscat
Caucasus Standard Time	(GMT+04:00) Baku, Tbilisi, Yerevan
Transitional Islamic State of Afghanistan Standard Time	(GMT+04:30) Kabul
Ekaterinburg Standard Time	(GMT+05:00) Ekaterinburg
West Asia Standard Time	(GMT+05:00) Islamabad, Karachi, Tashkent
India Standard Time	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
Nepal Standard Time	(GMT+05:45) Kathmandu
Central Asia Standard Time	(GMT+06:00) Astana, Dhaka
Sri Lanka Standard Time	(GMT+06:00) Sri Jayawardenepura
N. Central Asia Standard Time	(GMT+06:00) Almaty, Novosibirsk
Myanmar Standard Time	(GMT+06:30) Yangon Rangoon
S.E. Asia Standard Time	(GMT+07:00) Bangkok, Hanoi, Jakarta
North Asia Standard Time	(GMT+07:00) Krasnoyarsk
China Standard Time	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi
Singapore Standard Time	(GMT+08:00) Kuala Lumpur, Singapore
Taipei Standard Time	(GMT+08:00) Taipei
W. Australia Standard Time	(GMT+08:00) Perth
North Asia East Standard Time	(GMT+08:00) Irkutsk, Ulaanbaatar
Korea Standard Time	(GMT+09:00) Seoul
Tokyo Standard Time	(GMT+09:00) Osaka, Sapporo, Tokyo
Yakutsk Standard Time	(GMT+09:00) Yakutsk
A.U.S. Central Standard Time	(GMT+09:30) Darwin
Cen. Australia Standard Time	(GMT+09:30) Adelaide
A.U.S. Eastern Standard Time	(GMT+10:00) Canberra, Melbourne, Sydney
E. Australia Standard Time	(GMT+10:00) Brisbane
Tasmania Standard Time	(GMT+10:00) Hobart
Vladivostok Standard Time	(GMT+10:00) Vladivostok
West Pacific Standard Time	(GMT+10:00) Guam, Port Moresby
Central Pacific Standard Time	(GMT+11:00) Magadan, Solomon Islands, New Caledonia
Fiji Islands Standard Time	(GMT+12:00) Fiji Islands, Kamchatka, Marshall Islands
New Zealand Standard Time	(GMT+12:00) Auckland, Wellington
Tonga Standard Time	(GMT+13:00) Nuku'alofa

10 CMC Settings

10.1 Introduction

This section introduces the specifications that the management software follows and its main functions.

The Inspur Server Management System is a control unit for server management, which is compatible with the standard IPMI2.0 specification.

Below are the main functions of the Inspur Server Management System:

- System monitor

Monitors the fan module and power module.

- System configuration

To set the configuration related with CMC network, services and alert, etc.

- Log information

Displays the various event log information, and users can set the options related with the event logs.

- FRU information

Displays the information about CMC and nodes.

- Support IPMI Tool management

Supports the command operation sent by IPMI Tool, you could download IPMI Tool by yourself.

- Support WEB interface management

Provides a friendly and visual interface management, you could quickly complete configuration and query tasks via simple clicking on the interface.

- Support account centralized management

It is supported to store accounts in Active Directory server, and direct authentication process to server, so as to realize management system login with domain accounts.

10.2 Functional Modules

This chapter introduces Inspur server management system module composition as well as functions of these modules.

10.2.1 Module Composition

The Inspur Server Management System is mainly composed of IPMI module, command line module and WEB module.

- The command line module attains the calling of IPMI module. The user performs the operation on IPMI module via command lines.
- The WEB module attains daily management on server in the form of visual interface via calling IPMI commands.

10.2.2 IPMI Module Introduction

IPMI module attains management of the server system according to the IPMI2.0 standard. The functions of the IPMI module include:

- System real-time monitoring

Provides the alarm report and alarm indication in the event of fault detection.

- System remote control

Meets the management requirements such as remote power-on/off, and business system reset via command lines and Web.

10.2.3 Command Line Function Introduction

Command line module includes query and setting commands.

10.3 Web Interface Introduction

This section introduces the Web interface of the management system, as well as operation steps to login the Web interface.

- Login Web interface: Introduces the method to login the Web interface.
- Web interface introduction: Introduces the Web interface layout.

10.3.1 Login Web Interface

It introduces methods to login the Web interface.

This guide introduces operation steps to login Web management interface, taking Windows operating system and Firefox browser as examples.

⚠ **Note:** When carrying out interface operation via Web, a maximum of 20 users can be logged in at the same time.

Step 1: Ensure the management network ports on the client and server are connected to the internet.

Step 2: Open the browser, and enter “http://ipaddress” in the address bar (ipaddress is the actual IP address of the management port. The default login mode is https, and safe operation configuration is needed).

Step 3: The login interface should appear as shown below:

1. Enter the user name and password.

Note: The system provides a default user “admin” in administer user group, and the default password is “admin”. Please change the default password in time after the first login.

2. Click “Login”, to enter the management interface.

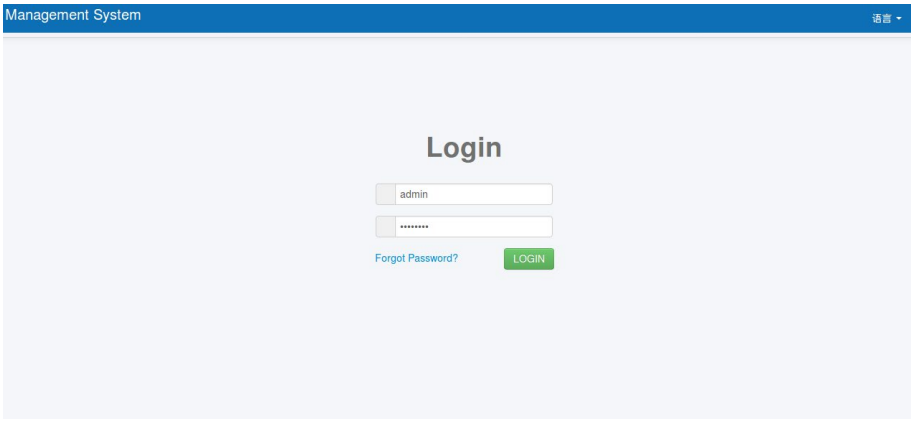


Figure 10-1

10.3.2 Web Interface Introduction

The Web interface helps users accomplish server management. The Web interface has a help function so users can click the help button 

in the case that they may need it. The Web interface is divided into several parts, as shown in the following figure.

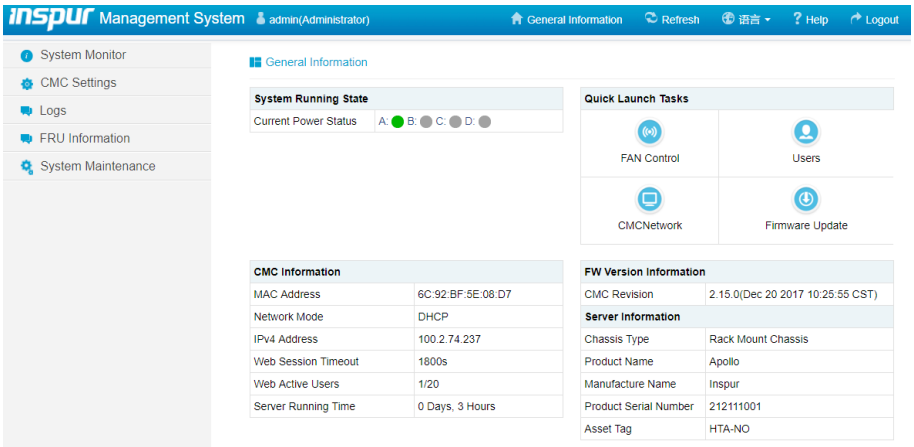


Figure 10-2

- The name of the Web interface is displayed on top left of the interface.
- The meanings of all buttons on top right of the interface:

◇ OverView Click on the Overview button, to return to the overview page.

◇ Refresh Click on the Refresh button, to refresh the page.

◇ Language Click on the Language button, to change the language (which supports Chinese and English).

◇ Help Click on the Help button to query help information on the corresponding page.

◇ Logout Click on the Logout button, to return to the login page.

- The navigation tree is on the left. Via the nodes on the tree, you can select different functional interfaces. The following functions are included:

- View the overall situation
- System monitor
- CMC settings
- Logs
- FRU information
- System maintenance

For detailed introduction on all functions, please refer to the following chapters.

- Specific operation interface is on the right of the interface.

10.3.3 Overview

Click General Information to open the “General Information” interface, as shown in the following figure. This page displays some Quick Launch Tasks: fan control, users, CMC network and firmware update. This page also contains some summary information: CMC information, FW version information and recent system event log.

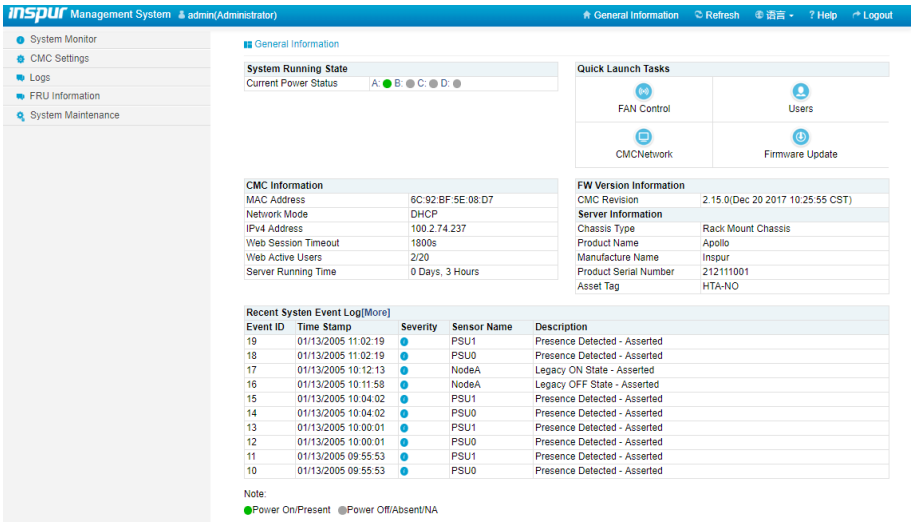


Figure 10-3

10.4 System Monitor

Select “System Monitor” on the navigation tree. It includes the interfaces of node module, fan module, power module, history record and chassis view, as shown in the following figures.

- Node module: Displays the node information, including present status, power status, BMC IP. Users can perform actions to nodes, including power on, power off, power reset, BMC reset.
- Fan module: Displays fans’ No., status, current speed, manual control and speed control.
- Power module: Contains PSU monitor, power monitor and power control.
- History record: Displays the history record of the total power.
- Chassis view: Displays the front panel view, rear panel view and vertical view of the chassis.

10.4.1 Node Module

This page displays the node information, including present status, power status, BMC IP, etc. Users can perform actions to nodes, including power on, power off, power reset and BMC reset.

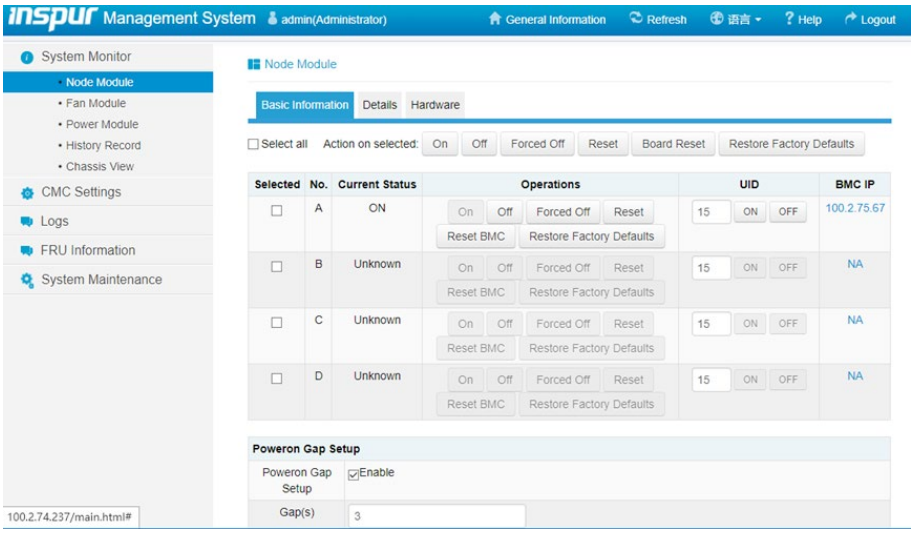


Figure 10-4

Details tab displays the node's present status, power status, related temperature information, CPU, memory and hardware information.

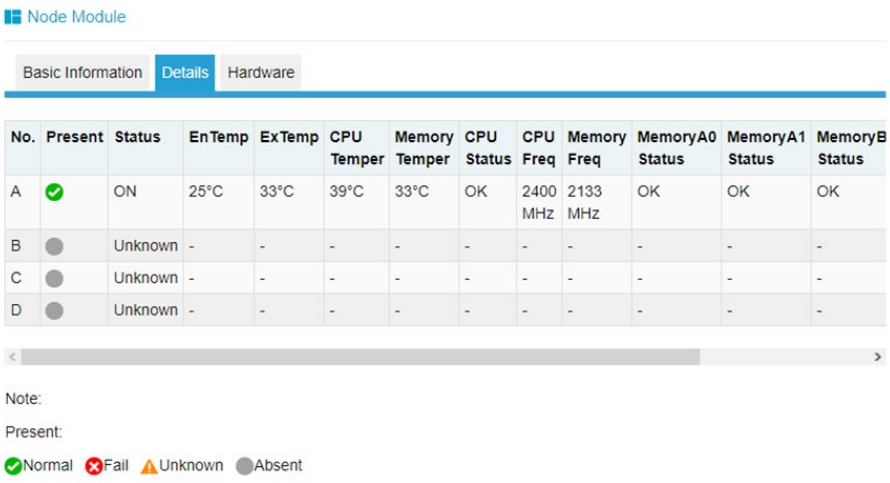


Figure 10-5

Hardware tab displays the CPU type and amount, memory type and amount, NIC MAC address and BMC&BIOS version information.

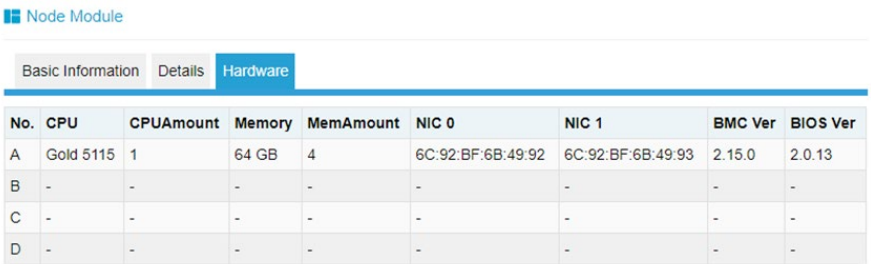


Figure 10-6

10.4.2 Fan Module

Users can view the status, current speed and duty ratio of each fan in the system.

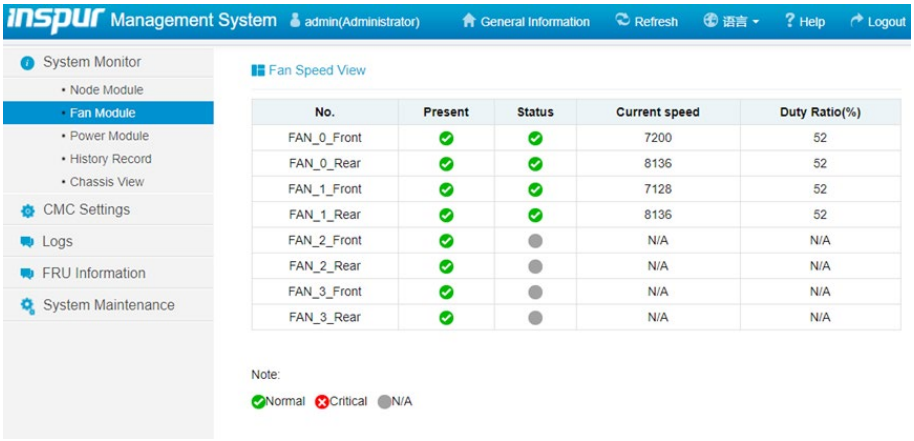


Figure 10-7

10.4.3 Power Module

Power module includes power supply unit monitor, power monitor and power capping information.

Power supply unit monitor displays the status of power supply on the host. You can get the following information for a single power supply unit:

- ID
- Present
- Alert: Alert Information
- Temp(°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
- FW Version: FW Version of power supply unit

Power monitor displays the fan power and rack power.

Power capping is used to configure the power capping limit and policy.

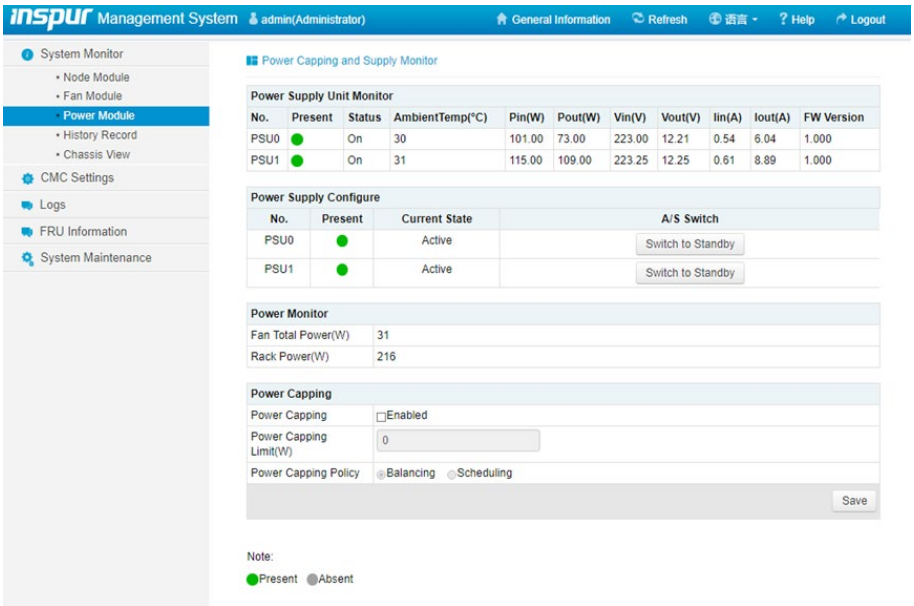


Figure 10-8

10.4.4 History Record

This page displays history information about inlet temperature and total power. It shows average and max inlet temperature and total power and displays as curves. You can see 3 types: Last Day, Last Month, and Last Year.

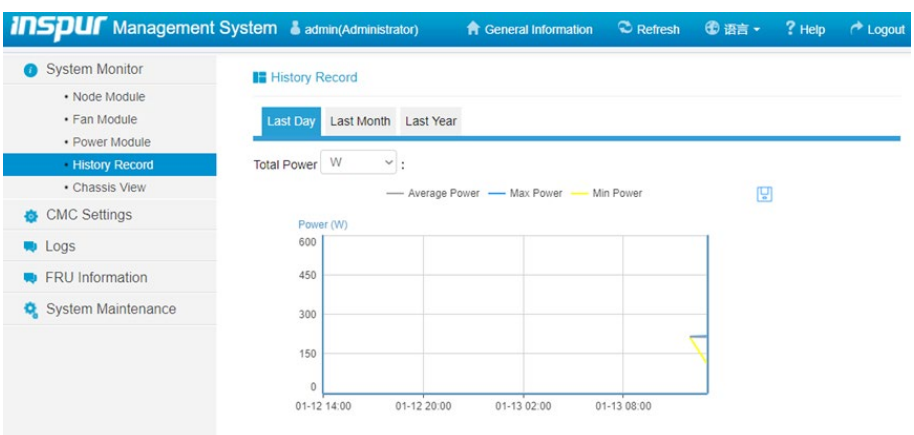


Figure 10-9

10.4.5 Chassis View

This page displays the front panel view, rear panel view and vertical view of the chassis.

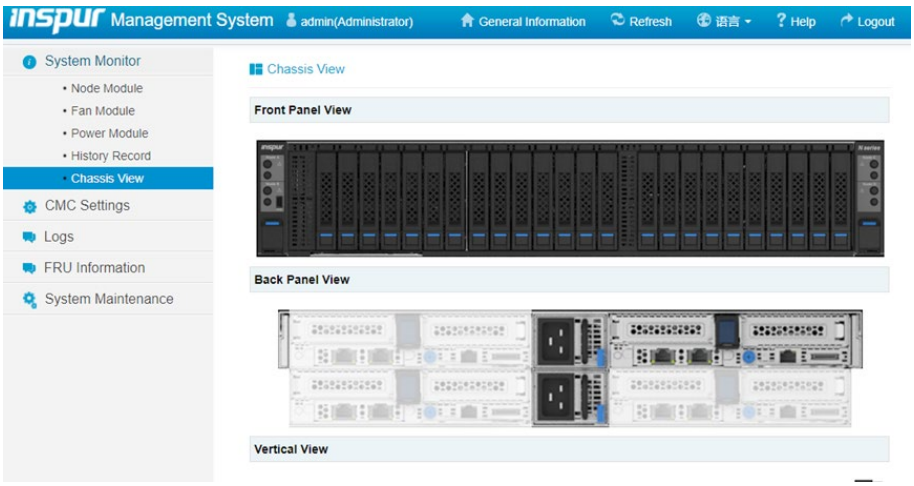


Figure 10-10

10.5 CMC Settings

Select “CMC Settings” on the navigation tree to open the CMC settings interface, which contains six interfaces of CMC network management, services, alerts, LDAP/E-Directory, users and access control, as shown in the following figures.

- CMC network: Contains network and DNS settings.
- Services: To configure the service’s name, current state, interface, nonsecure port, secure port, timeout, maximum sessions and active sessions.
- Alerts: To configure SNMP Trap settings.
- LDAP/E-Directory: To configure LDAP/E-Directory settings.
- Users: User management function, including add user, modify user and delete user.
- Access control: Contains IP access control and other related information.

10.5.1 CMC Network

This page is used to configure the network settings for available LAN channels.

Note: Click ‘Save’ to save any changes made. You will be prompted to log out of current UI session and log back in at the new IP address.

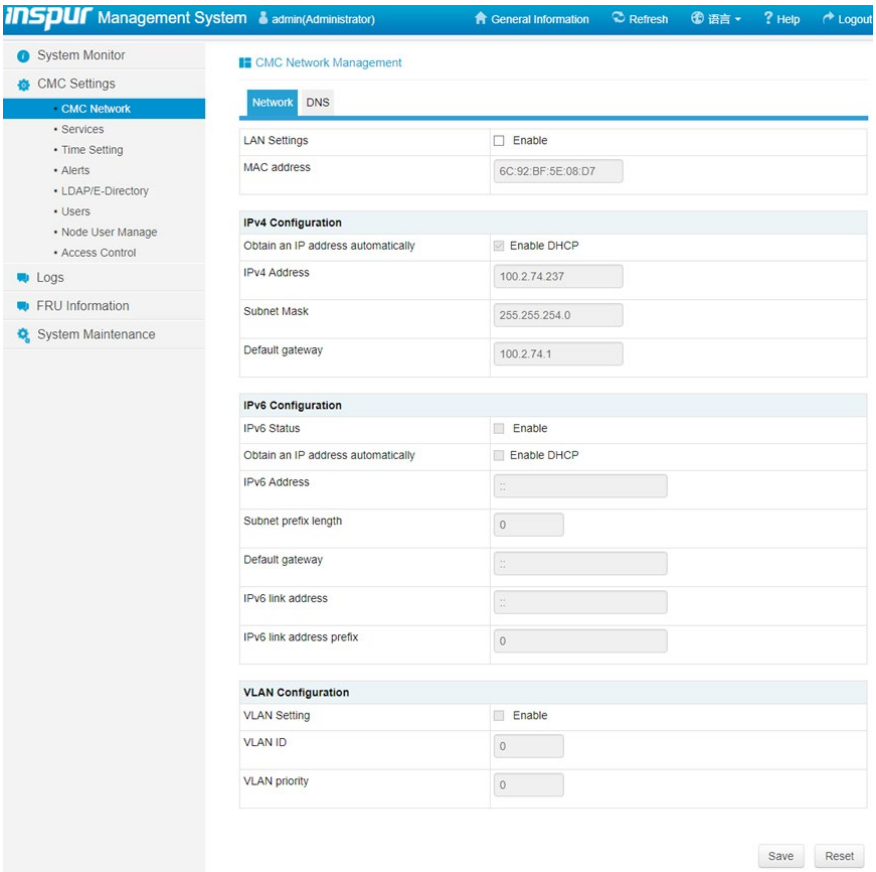


Figure 10-11

DNS page is used to configure the host name and domain name server of the device.

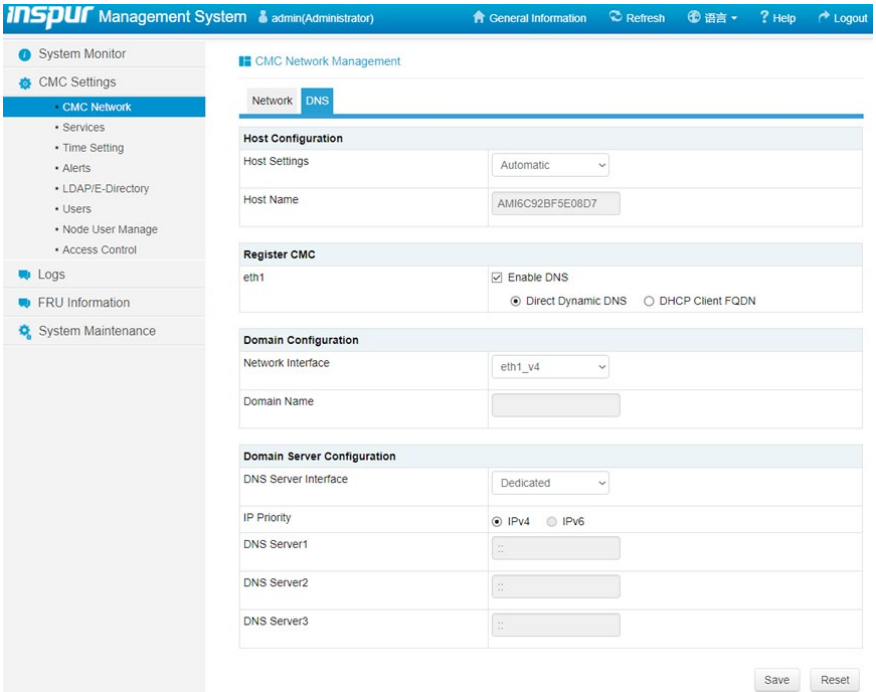
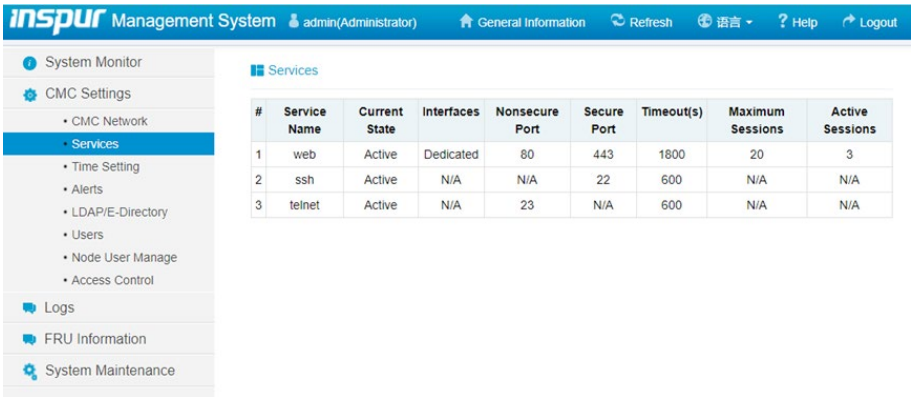


Figure 10-12

10.5.2 Services

This page displays the basic information about services running in the CMC. To modify a service, the user must be an Administrator.



#	Service Name	Current State	Interfaces	Nonsecure Port	Secure Port	Timeout(s)	Maximum Sessions	Active Sessions
1	web	Active	Dedicated	80	443	1800	20	3
2	ssh	Active	N/A	N/A	22	600	N/A	N/A
3	telnet	Active	N/A	23	N/A	600	N/A	N/A

Figure 10-13

Select a slot and click ‘Modify’ to modify the configuration of the service. Alternatively, double click on the slot. The pop-up interface as shown below:

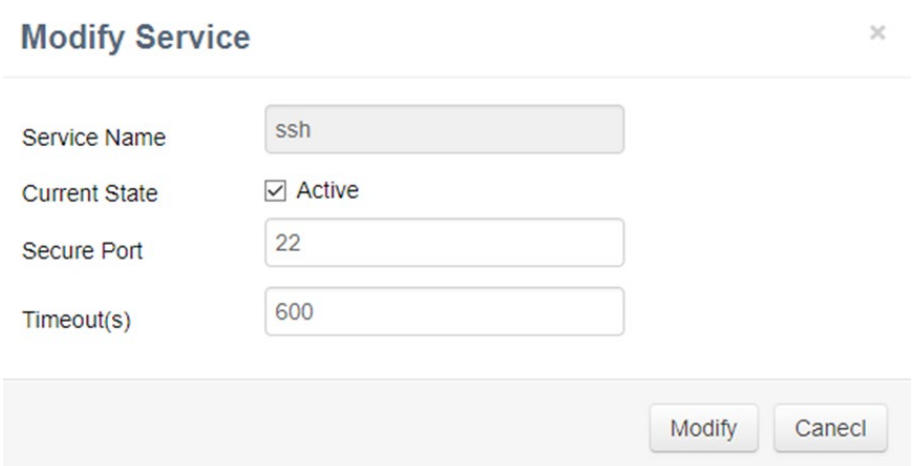


Figure 10-14

10.5.3 Time Setting

This page displays the device’s current Date & Time Settings. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

UTC TimeZone: This list contains the UTC TimeZone values for NTP server, which can be used to display the exact local time.

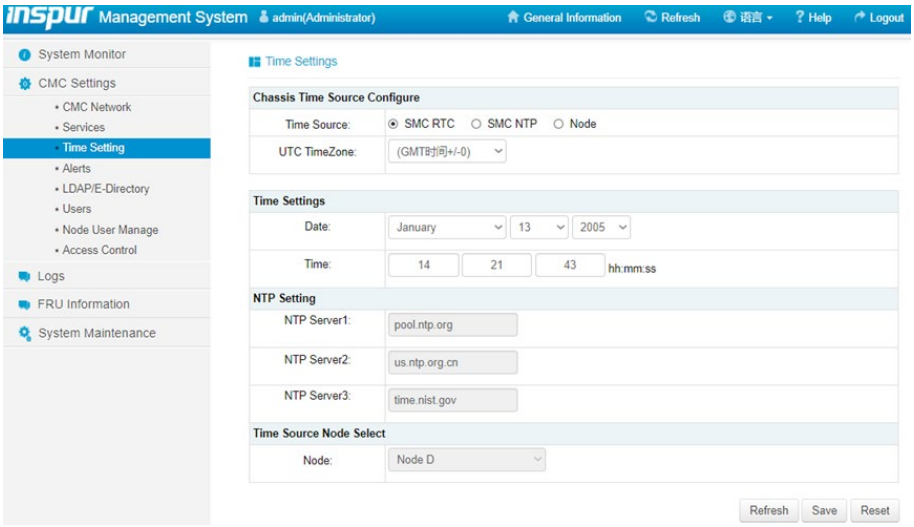


Figure 10-15

10.5.4 Alerts

You can configure SNMP Trap alert in this page.

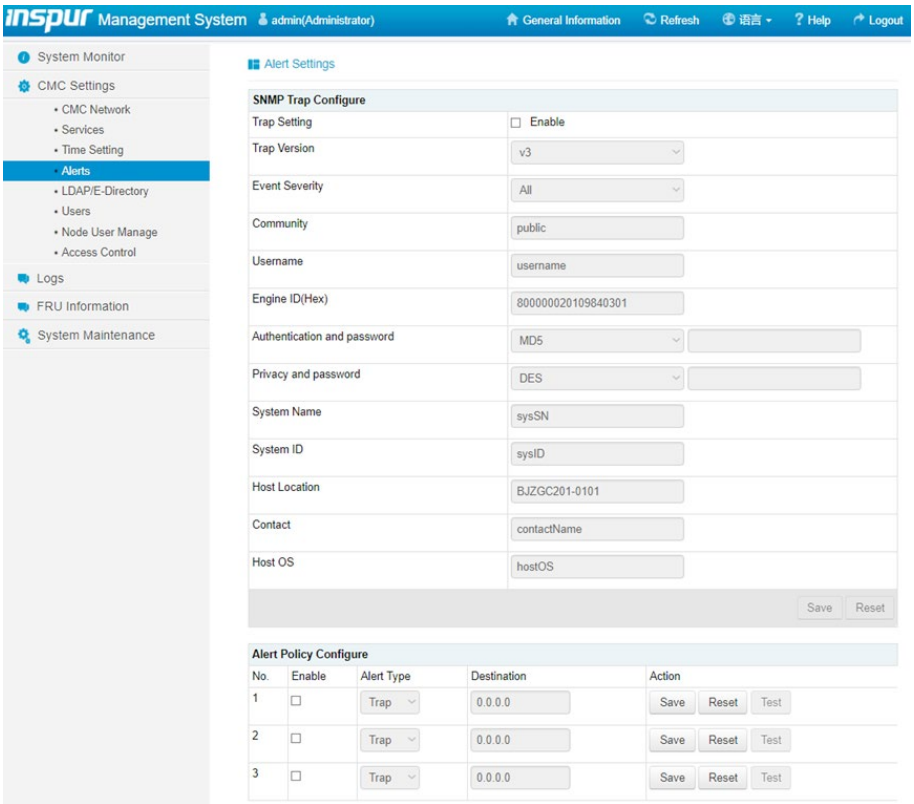


Figure 10-16

10.5.5 LDAP/E-Directory

The displayed table shows any configured Role Groups and available slots. You can modify or add/delete role groups from here. Group Search Base can be any path from where Group is located to Base DN. Group Name should correspond to the name of an actual LDAP/ E-Directory group. To view the page, the user must at least be a User. To modify or add a group, the user must be an Administrator.

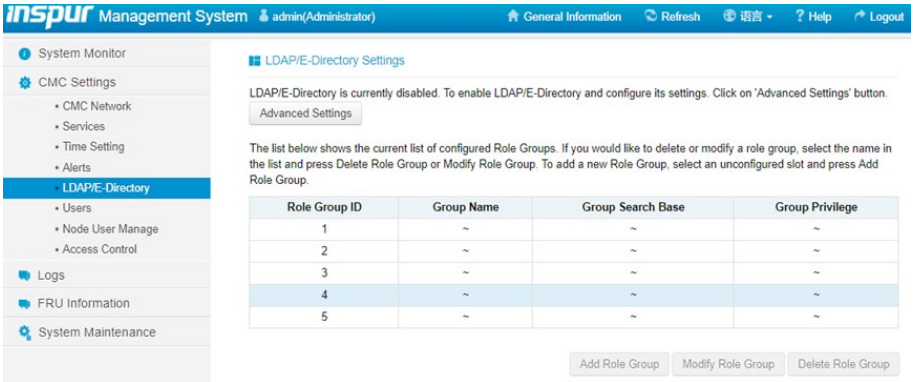


Figure 10-17

Advanced Settings interface:

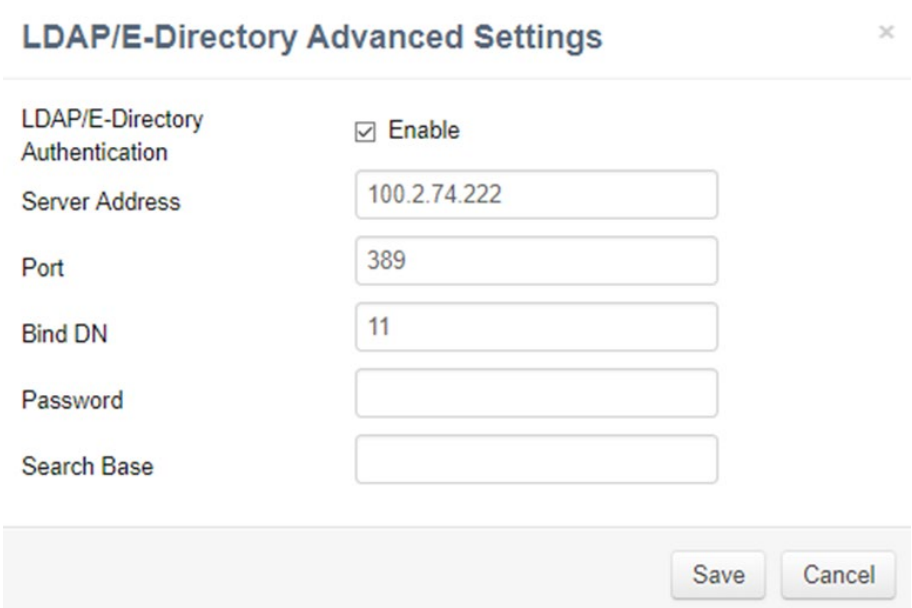


Figure 10-18

10.5.6 Users

The displayed table shows any configured Users. You can modify or add new users from here. A maximum of 10 users are available, including the default administrator. To view the

page, the user must at least be an Operator. To modify or add a user, the user must be an Administrator.

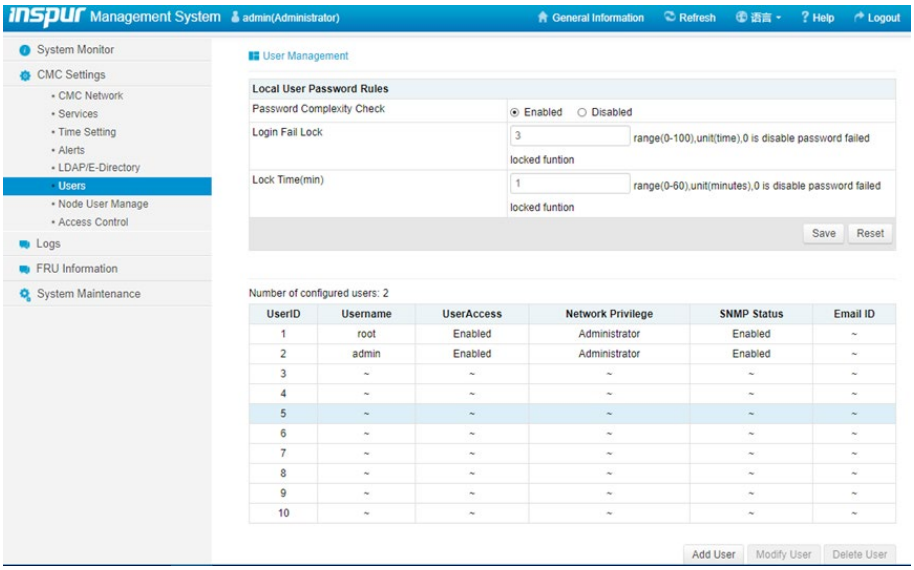


Figure 10-19

Add User interface:

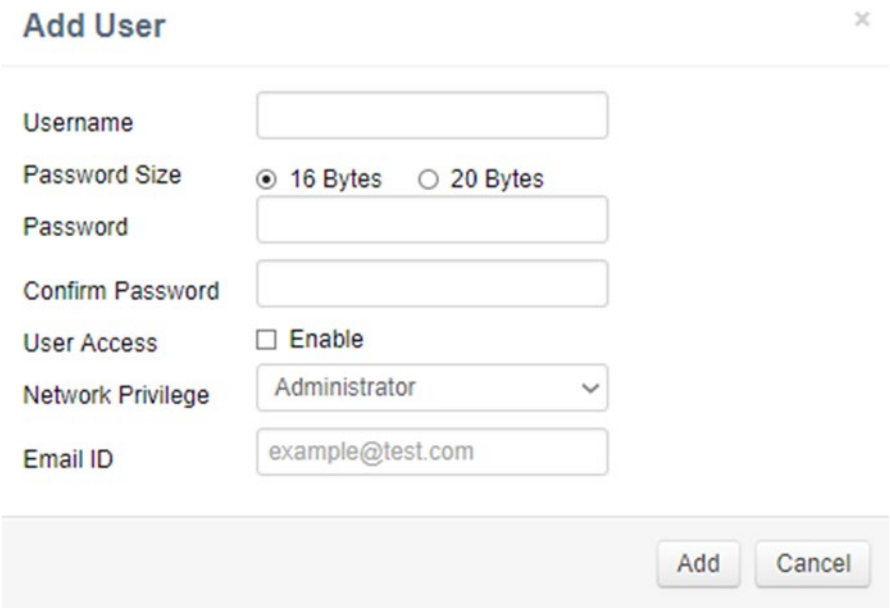


Figure 10-20

10.5.7 Node User Manage

This page is is used for batch addition, modification and deletion of node users. This operation will be synchronized to all present nodes.

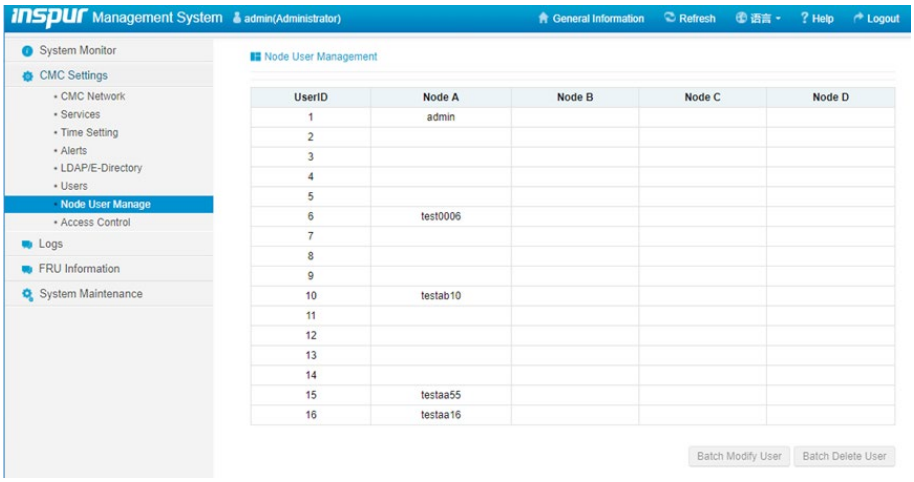


Figure 10-21

Batch Add User interface is shown below. To modify users or add users, it needs to reset the password.

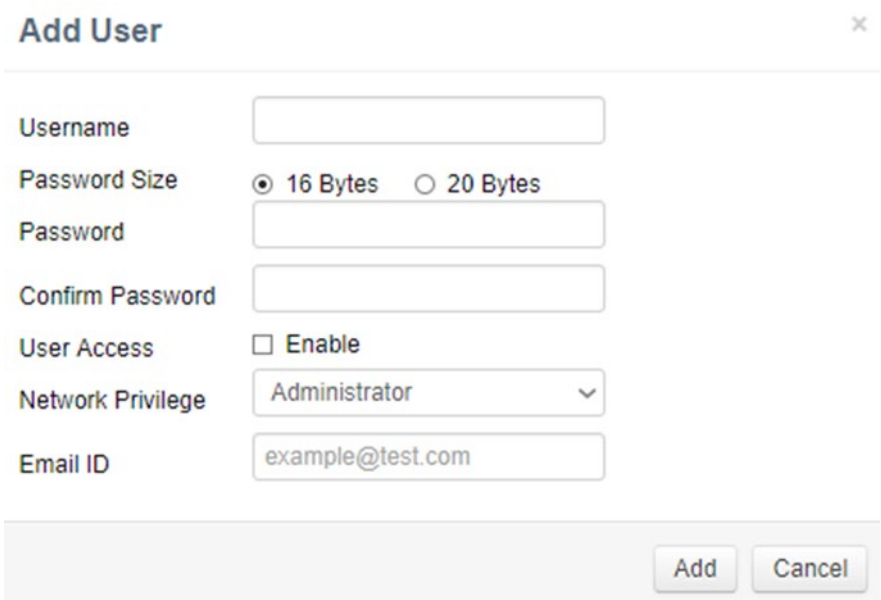


Figure 10-22

10.5.8 Access Control

This page is used to configure IP range entries which will be allowed to access CMC. You can add new IP range entry or delete the enabled ones in this page.

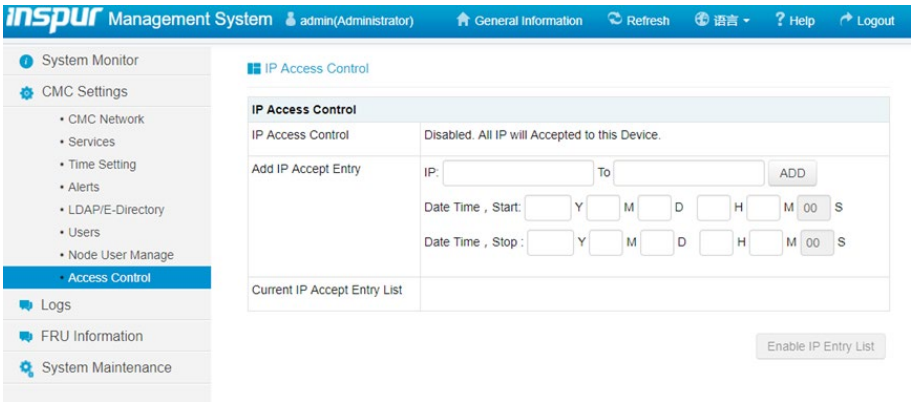


Figure 10-23

10.6 Logs

Select “Logs” on the navigation tree to open the logs interface, which contains five interfaces of system event log, CMC syslog, CMC audit log, event log setting and CMC system log setting, as shown in the following figures.

- System event log: Displays various event logs generated by server.
- CMC syslog: Displays CMC system logs.
- CMC audit log: Displays CMC audit logs.
- Event log setting: To set the current event log policy.
- CMC system log setting: To configure the CMC system log settings.

10.6.1 System Event Log

This page displays the list of events incurred by different sensors on this device. You can export and clear logs. The exported event log is in TXT format, and the log will be displayed on a new web page.

Note: The exported Chinese logs may be garbled in some browsers. This is caused by the differences in browser decoding modes. Please set the appropriate browser character encoding. The recommended character encoding is Unicode (UTF-8). Take IE as an example: Toolbar -> View -> Coding -> Auto Selection.

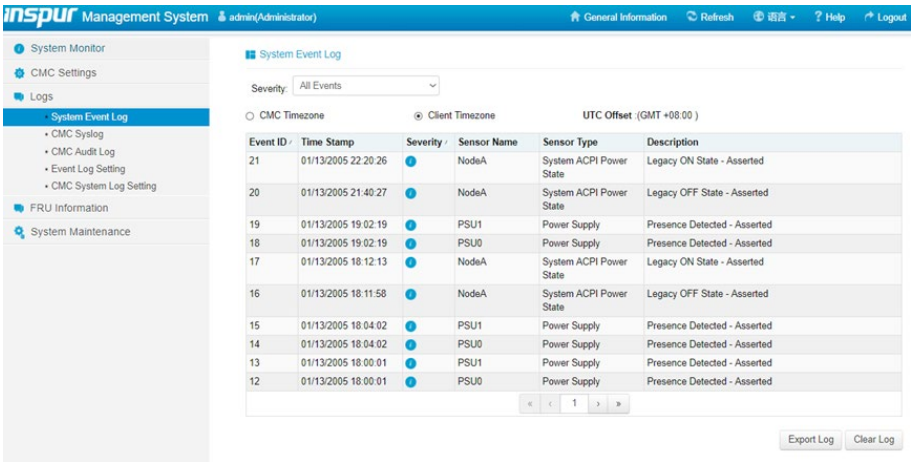


Figure 10-24

10.6.2 CMC Syslog

This page displays the list of CMC system logs on this device. You can export and clear logs. The exported event log is in TXT format, and the log will be displayed on a new web page.

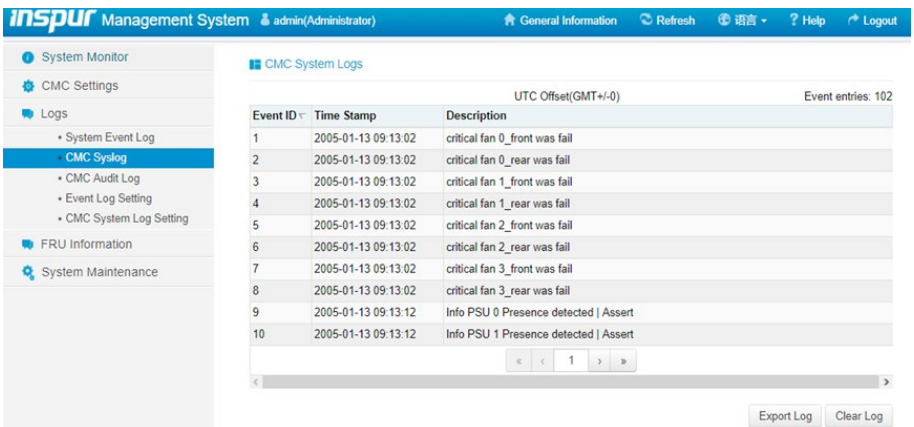


Figure 10-25

10.6.3 CMC Audit Log

This page displays the list of CMC audit logs on this device. You can export and clear logs. The exported event log is in TXT format, and the log will be displayed on a new web page.

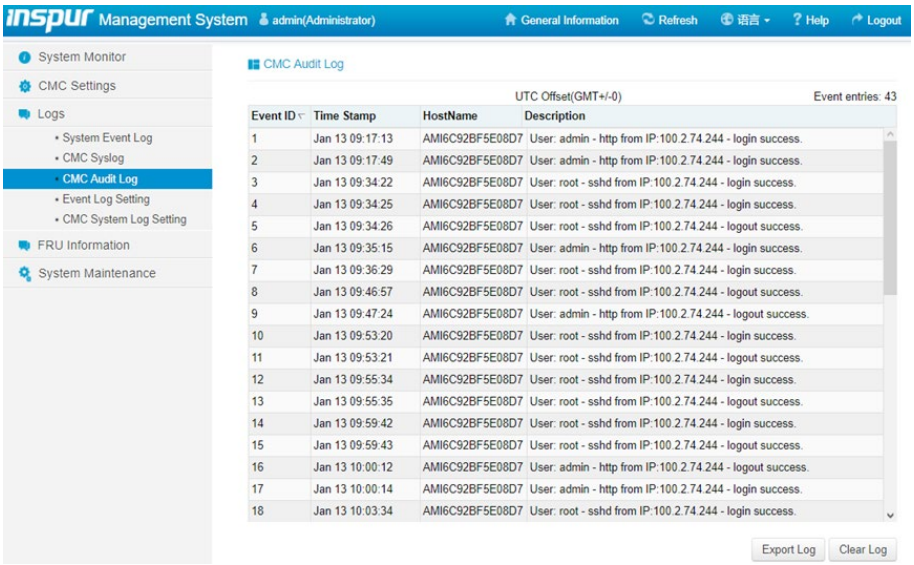


Figure 10-26

10.6.4 Event Log Setting

This page is used to configure the System Event log information.

System Event Log Policy Options

Linear Policy: Check this option to enable the Linear System Event Log Policy for Event Log.

Circular Policy: Check this option to enable the Circular System Event Log Policy for Event Log.

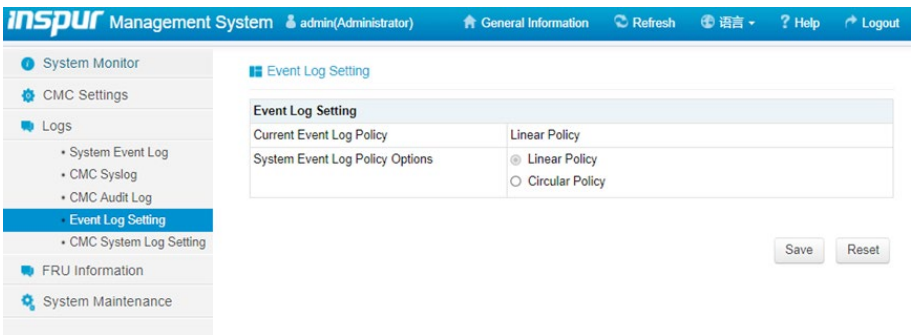


Figure 10-27

10.6.5 CMC System Log Setting

This page is used to configure the System and Audit log settings. Select the log type for system logs, whether it should be preserved in a local file or on a remote server. Local file resides at /var/log/.

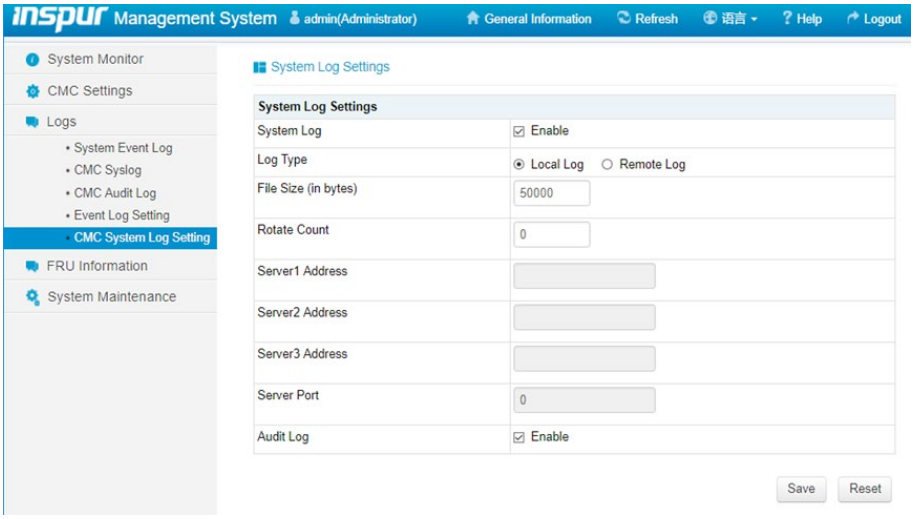


Figure 10-28

10.7 FRU Information

Select “FRU Information” on the navigation tree to open the FRU information interface, which contains three interfaces of CMC information, node information and power information, as shown in the following figures.

- CMC information: Displays the CMC’s basic information and attribute values.
- Node information: Displays the node’s No., product name, serial number, chassis extra and other basic information.
- Power information: Displays the PSU’s basic information.

10.7.1 CMC Information

This page shows FRU information of CMC module: device name and device information.

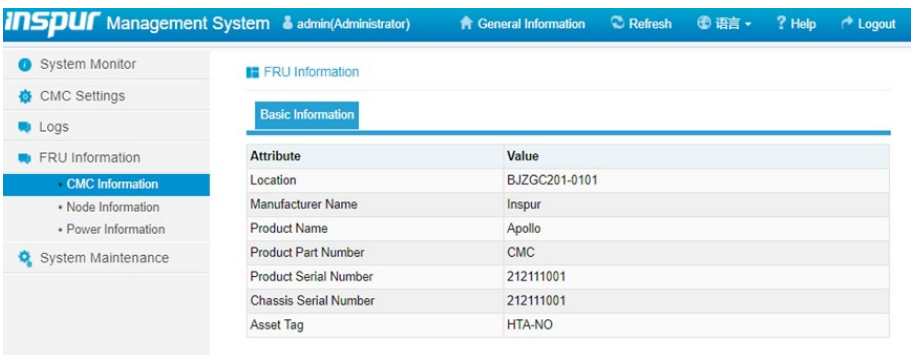


Figure 10-29

10.7.2 Node Information

This page displays FRU information of each node.

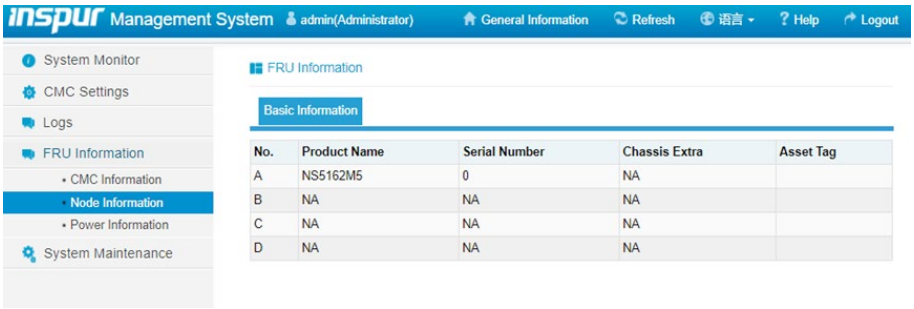


Figure 10-30

10.7.3 Power Information

This page shows the information of power supply module and switch module.

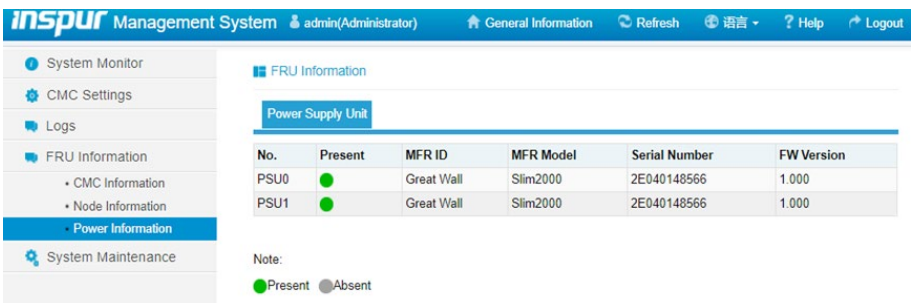


Figure 10-31

10.8 System Maintenance

Select “System Maintenance” on the navigation tree to open the system maintenance interface, which contains four interfaces of CMC FW update, restore factory defaults, system administrator and CMC reboot, as shown in the following figures.

- CMC FW update: Displays the related configuration information about CMC FW update.
- Restore factory defaults: Displays the configuration items about restore factory defaults.
- System administrator: To set the administrator’s username, user access and password.
- CMC reboot: CMC reboot button.

10.8.1 CMC FW Update

This wizard takes you through the process of firmware upgradation.

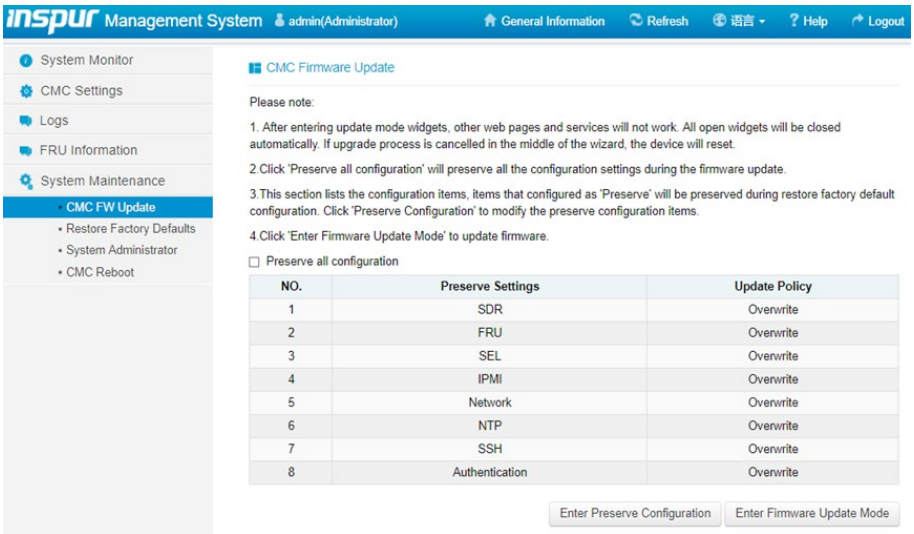


Figure 10-32

Config Panel interface:

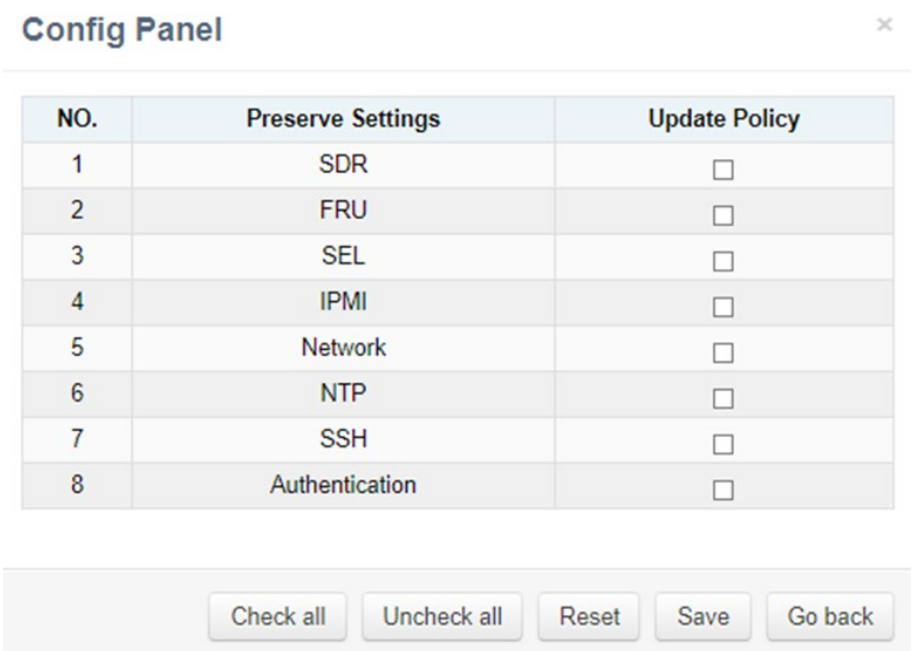


Figure 10-33

10.8.2 Restore Factory Defaults

This page helps to restore the factory defaults of the device.

Note: After entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

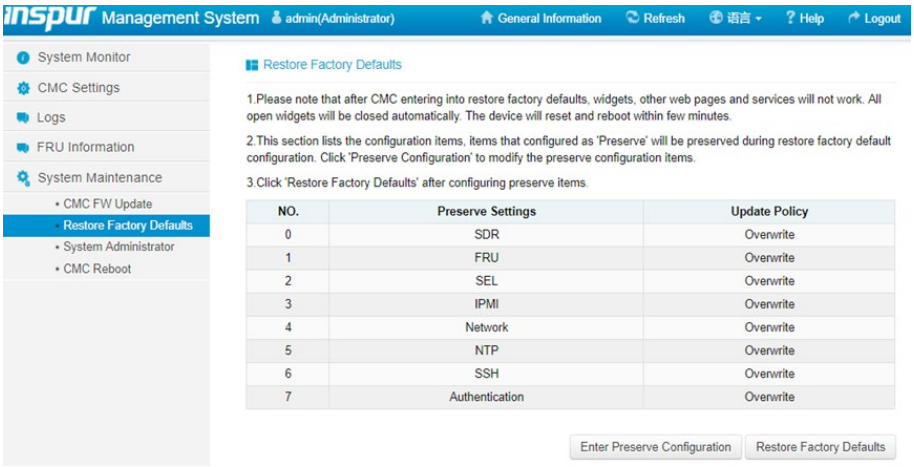


Figure 10-34

Config Panel interface:

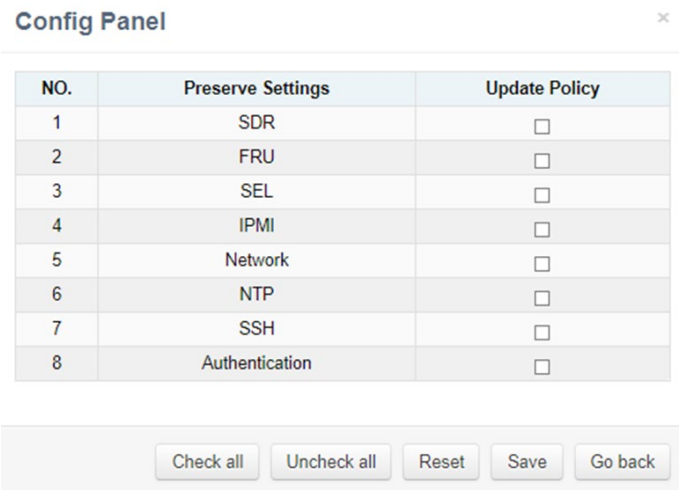


Figure 10-35

10.8.3 System Administrator

This page is used to configure the System Administrator configuration.

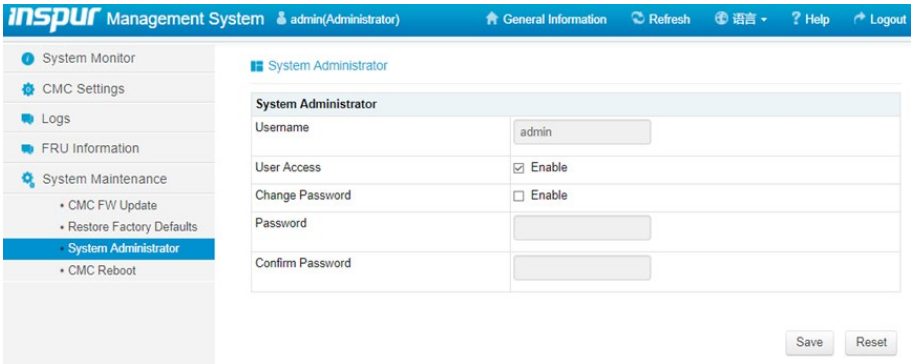


Figure 10-36

10.8.4 CMC Reboot

This page is used to reboot the CMC System.

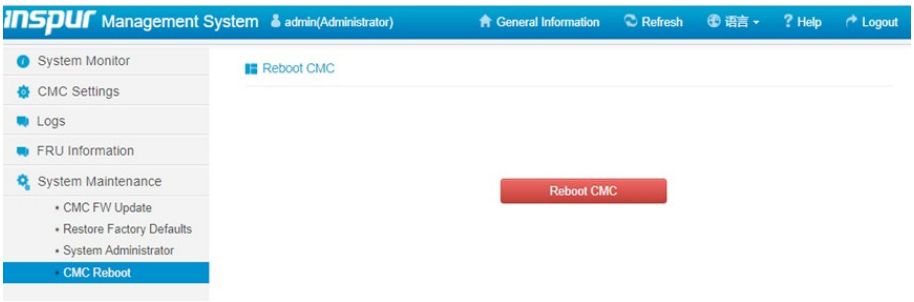


Figure 10-37

10.9 Command Line Function Introduction

This chapter introduces Web interface of the management system, as well as operation steps to login the Web interface.

● Login command line

Introduces methods of login command line.

● Command line function introduction

Introduces command line functions.

10.9.1 Command Line Login

Login to CMC Command line through ssh. After login, enter the command line interface:

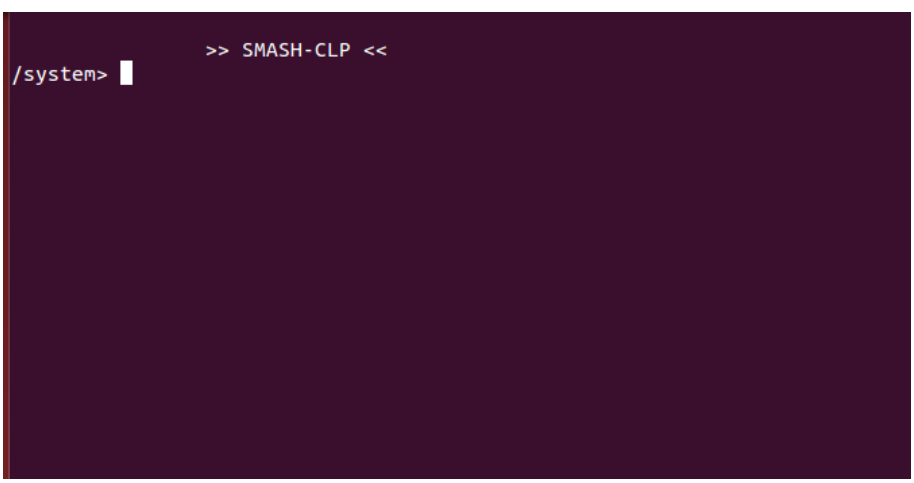


Figure 10-38

Enter help to view the online help information:

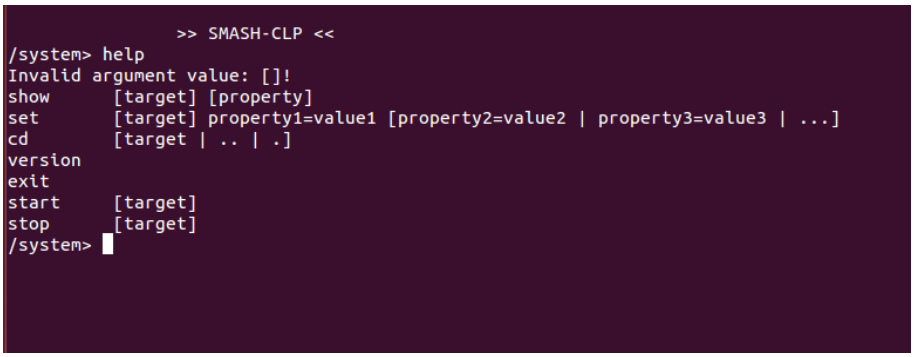


Figure 10-39

10.9.2 Command Line Function Introduction

Via show command, users can view the command line function introduction.

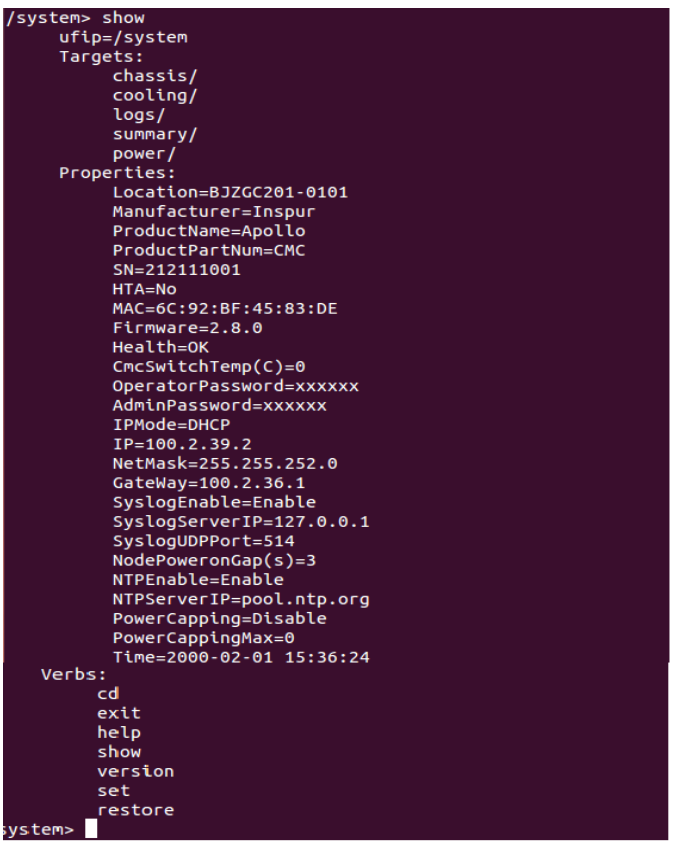


Figure 10-40

10.10 Time Zone Table

Table 10-1

Name of Time Zone	Time
Dateline Standard Time	(GMT-12:00) International Date Line West
Samoa Standard Time	(GMT-11:00) Midway Island, Samoa
Hawaiian Standard Time	(GMT-10:00) Hawaii
Alaskan Standard Time	(GMT-09:00) Alaska
Pacific Standard Time	(GMT-08:00) Pacific Time (US and Canada); Tijuana
Mountain Standard Time	(GMT-07:00) Mountain Time (US and Canada)
Mexico Standard Time 2	(GMT-07:00) Chihuahua, La Paz, Mazatlan
U.S. Mountain Standard Time	(GMT-07:00) Arizona
Central Standard Time	(GMT-06:00) Central Time (US and Canada
Canada Central Standard Time	(GMT-06:00) Saskatchewan
Mexico Standard Time	(GMT-06:00) Guadalajara, Mexico City, Monterrey
Central America Standard Time	(GMT-06:00) Central America
Eastern Standard Time	(GMT-05:00) Eastern Time (US and Canada)
U.S. Eastern Standard Time	(GMT-05:00) Indiana (East)
S.A. Pacific Standard Time	(GMT-05:00) Bogota, Lima, Quito
Atlantic Standard Time	(GMT-04:00) Atlantic Time (Canada)
S.A. Western Standard Time	(GMT-04:00) Caracas, La Paz
Pacific S.A. Standard Time	(GMT-04:00) Santiago
Newfoundland and Labrador Standard Time	(GMT-03:30) Newfoundland and Labrador
E. South America Standard Time	(GMT-03:00) Brasilia
S.A. Eastern Standard Time	(GMT-03:00) Buenos Aires, Georgetown
Greenland Standard Time	(GMT-03:00) Greenland
Mid-Atlantic Standard Time	(GMT-02:00) Mid-Atlantic
Azores Standard Time	(GMT-01:00) Azores
Cape Verde Standard Time	(GMT-01:00) Cape Verde Islands
GMT Standard Time	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Greenwich Standard Time	(GMT) Casablanca, Monrovia
Central Europe Standard Time	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Central European Standard Time	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Romance Standard Time	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
W. Europe Standard Time	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

W. Central Africa Standard Time	(GMT+01:00) West Central Africa
E. Europe Standard Time	(GMT+02:00) Bucharest
Egypt Standard Time	(GMT+02:00) Cairo
FLE Standard Time	(GMT+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
GTB Standard Time	(GMT+02:00) Athens, Istanbul, Minsk
Israel Standard Time	(GMT+02:00) Jerusalem
South Africa Standard Time	(GMT+02:00) Harare, Pretoria
Russian Standard Time	(GMT+03:00) Moscow, St. Petersburg, Volgograd
Arab Standard Time	(GMT+03:00) Kuwait, Riyadh
E. Africa Standard Time	(GMT+03:00) Nairobi
Arabic Standard Time	(GMT+03:00) Baghdad
Iran Standard Time	(GMT+03:30) Tehran
Arabian Standard Time	(GMT+04:00) Abu Dhabi, Muscat
Caucasus Standard Time	(GMT+04:00) Baku, Tbilisi, Yerevan
Transitional Islamic State of Afghanistan Standard Time	(GMT+04:30) Kabul
Ekaterinburg Standard Time	(GMT+05:00) Ekaterinburg
West Asia Standard Time	(GMT+05:00) Islamabad, Karachi, Tashkent
India Standard Time	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
Nepal Standard Time	(GMT+05:45) Kathmandu
Central Asia Standard Time	(GMT+06:00) Astana, Dhaka
Sri Lanka Standard Time	(GMT+06:00) Sri Jayawardenepura
N. Central Asia Standard Time	(GMT+06:00) Almaty, Novosibirsk
Myanmar Standard Time	(GMT+06:30) Yangon Rangoon
S.E. Asia Standard Time	(GMT+07:00) Bangkok, Hanoi, Jakarta
North Asia Standard Time	(GMT+07:00) Krasnoyarsk
China Standard Time	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi
Singapore Standard Time	(GMT+08:00) Kuala Lumpur, Singapore
Taipei Standard Time	(GMT+08:00) Taipei
W. Australia Standard Time	(GMT+08:00) Perth
North Asia East Standard Time	(GMT+08:00) Irkutsk, Ulaanbaatar
Korea Standard Time	(GMT+09:00) Seoul
Tokyo Standard Time	(GMT+09:00) Osaka, Sapporo, Tokyo
Yakutsk Standard Time	(GMT+09:00) Yakutsk
A.U.S. Central Standard Time	(GMT+09:30) Darwin
Cen. Australia Standard Time	(GMT+09:30) Adelaide

A.U.S. Eastern Standard Time	(GMT+10:00) Canberra, Melbourne, Sydney
E. Australia Standard Time	(GMT+10:00) Brisbane
Tasmania Standard Time	(GMT+10:00) Hobart
Vladivostok Standard Time	(GMT+10:00) Vladivostok
West Pacific Standard Time	(GMT+10:00) Guam, Port Moresby
Central Pacific Standard Time	(GMT+11:00) Magadan, Solomon Islands, New Caledonia
Fiji Islands Standard Time	(GMT+12:00) Fiji Islands, Kamchatka, Marshall Islands
New Zealand Standard Time	(GMT+12:00) Auckland, Wellington
Tonga Standard Time	(GMT+13:00) Nuku'alofa

10.11 Service & Protocol

The services or protocols supported by BMC include RCMP+, Http/Https, ssh and telnet. Users can choose to enable or disable these services, as well as configure the port number, session timeout and the maximum sessions.

Table 10-2

Service	Use	Default State	Non-secure Port Number	Secure Port Number	Default Port Number	Timeout(s)	Max. Sessions
RMCP+	IPMI	Enable	623	N/A	N/A	1800	20
Http/Https	WEB interface	Enable	80(Http)	443(Https)	443(Https)	1800	20
ssh	ssh	Disable	N/A	22	22	600	N/A
telnet	telnet	Disable	23	N/A	23	600	N/A

Notes:

1. Http/Https timeout, if there is no page request within the timeout period, the page session will be deleted and the new page request will not be responded. If the page does not update automatically, the page will be logged out when you switch the page or refresh the page.
2. Telnet is a non-secure protocol, if you do not use it, it is recommended to disable it.

Non-configurable protocols:

Table 10-3

Service	Use	State	Port Number
SNMP	SNMP Get/Set	Enable	161
syslog	syslog	Enable	514

10.12 User Management

10.12.1 IPMI User

BMC supports IPMI2.0 user models, and supports up to 10 users. Multiple users can login simultaneously. User permissions include administrator, operator, user, OEM exclusive and no access.

User list:

Table 10-4

User ID	User Name	Password	State	Default Permission
User 1	admin	admin	Enable	Administrator
User 2 - 16	Undefined	Undefined	Disable	Administrator

IPMI user permissions, please refer to the IPMI2.0 specification.

Table 10-5

User Permission	Supported Operations
Administrator	Read/Write
Operator	Read
User	Read
No access	None

User name

- The user name is a string of 1 to 16 letters and numbers, including '-', '_', '@'.
- Must begin with a letter.
- Case sensitive.
- Special characters are not allowed, such as ',', '.', ':', ';', ' '(space), '/', '\\', '(', ')', etc.

Password

- When the password complexity check is disabled, the password must be at least 1 character long.
- When the password complexity check is enabled, the password must contain special characters, upper and lower letters and numbers, at least 8 characters long.
- The maximum length of the password is 16 characters.
- By default, the password complexity check is disabled. For security reasons, we strongly recommend that you enable this function.
- The password expiration can be set to a range of 0 to 90 days, and 0 means permanent. This function is disabled by default, and we strongly recommend that you enable this function for security reasons. If this function is enabled, the password needs to be changed

before expiration. If the password expires, you will need to disable this function in the operating system via the OEM's IPMI command.

- Login failed retry count: Retry count can be set to a number between 0 and 5. Lock time: The time setting range is 5 ~ 60 minutes. This function is disabled by default, and we strongly recommend that you enable this function for security reasons.
- Password history: It can be set to a range of 0 ~ 5. This function is disabled by default. If this function is enabled, the password can not be set to the used password (the last N passwords).

10.12.2 System User

System user refers to the BMC root user in Linux operating system. Users can login to BMC via ssh/telnet.

User name: sysadmin (unchangeable)

Default password: superuser

User name and password security

- The user name is fixed and can not be modified.
- The password must contain 8 characters at least.
- The password must contain special characters, upper and lower letters, and numbers.
- No space is allowed.
- At most 64 characters are allowed.

10.13 BMC Firmware Update

10.13.1 Firmware Integrity Check

Each firmware image can generate MD5 check code (Hash.exe) through the MD5 tool. Before updating the firmware, MD5 tool must be used to check the image's integrity to ensure that the firmware image file is correct.

10.13.2 WEB Update

CMC firmware can be updated through the management interface in the web interface.

Note:

The firmware upgrade process is a critical operation, once you enter the update mode and choose to cancel the firmware update operation, the CMC must reboot, which means that you must close the browser and login to the CMC again before any other action can be performed.

Firmware update steps:

- Go to the update page.
- Click “Enter FW update mode” button to enter the update mode.
- Choose the image file, and click Upload button to upload the file. CMC will enter the update mode after the file is uploaded. IPMI service will stop, and CMC will check the image’s size, which should be 32M, and check the image’s integrity to ensure it is the CMC image.

If the check fails, CMC will stop the update and reboot.

- Check the image version and the existed image version, after confirmation, click Update button to start the update.

11 Common Faults, Diagnosis and Troubleshooting

This chapter introduces the common server faults, as well as corresponding diagnosis and troubleshooting suggestions. If you are not sure about the cause of a failure and its removal method, please contact our customer service center for solutions.

When replacing or installing hardware devices, you should disconnect the power cable from the server completely. It is recommended to use the antistatic wrist strap with the other end grounded, to provide electrostatic protection when dismounting the server.

Note:

If your system goes wrong, you can handle it according to different phenomena. Some common system function problems are caused by using outdated Firmware, therefore, before fault definition, please make sure that all units (such as management module, IO module, blade unit, power module, etc.) installed in the server are using the latest Firmware. And please make sure that all of the installed blade units are using the latest FW (BIOS & BMC) and drivers.

Please check the following items first when system fails:

1. Whether the power indicators of each module are on;
2. Whether the chassis power has been connected to AC power interface;
3. Whether the chassis has been installed with the following modules: power module, management module and blade unit.

11.1 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.

---

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.

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 motherboard 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.

11.2 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://en.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://en.inspur.com/) to download the latest NIC driver.

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

12 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.

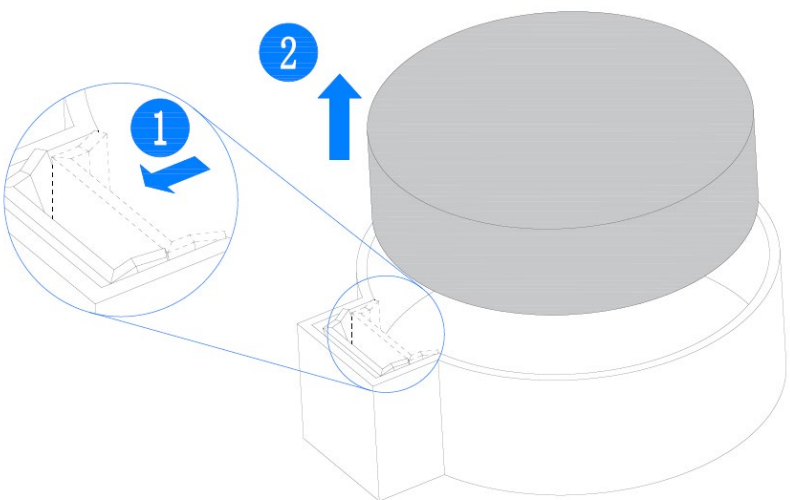


Figure 12-1

13 Regulatory Compliance Notices

13.1 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.

13.2 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.

13.2.1 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.

13.3 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.

13.4 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.

13.5 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.

13.6 Chinese Notice

Class A Equipment

本产品为 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，需要用户对其干扰采取切实可行的防护措施。

13.7 Battery Replacement Notice

⚠ **CAUTION:** Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instruct ions.

⚠ **ATTENTION:** Risque d’explosion si la batterie est remplacée par un type incorrect. Mettre au rebus les batteries usagées selon les instructions.

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

13.8 Battery Caution

13.8.1 Battery use caution

When battery is used, avoid:

- High or low extreme temperatures during use, storage and transportation.
- Extremely low air pressure, or low air pressure at high altitude.
- Battery replacement.

Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.

- Replace battery with an incorrect type;
- Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;

Dispose the used battery according to your local regulations or the battery manufacturer's instructions.

13.8.2 Avertis sement de l’utilisation de la batterie

Lorsque utiliser la batterie, évitez:

- Températures extrêmement élevées ou basses pendant l’utilisation, le stockage et le transport;
- Pression d’air extrêmement basse, ou pression d’air basse à haute altitude.
- Remplacement de la batterie.

Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d’incendie, d’explosion ou de fuite liquide de gaz inflammables.

- Remplacer la batterie par un type incorrect;

- Disposer d'une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;

Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.

13.8.3 Personal safety warnings

- Chemical Burn Hazard. This product contains a coin cell battery. Do not ingest battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

13.8.4 Avertissements de sécurité personnelle:

- Risque de brûlure chimique. Ce produit contient une batterie de

cellules. N'ingérer pas la batterie. Si la batterie de cellule est avalée, elle peut causer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.

- Gardez les batteries nouvelles ou utilisées à l'écart des enfants.
- Si le compartiment de la batterie ne se ferme pas en toute sécurité, cessez d'utiliser le produit et gardez-le à l'écart des enfants.
- Si vous pensez que des piles ont pu être avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.

13.9 Restricted Access Area

Equipment is intended for installation in Restricted Access Area.

Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT.

14 Electrostatic Discharge

14.1 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.

14.2 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.

15 Warranty

15.1 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.

15.2 Warranty Service

15.2.1 Service Overview

Table 15-1

Type	Duration
Remote Services	3 years
RMA Services	3 years

15.2.2 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:

Table 15-2

Type	Description	Response time
Hotline	1-844-860-0011(English) 1-760-769-1847(English) 86-400-860-0011(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.

15.3 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.

16 Appendix

16.1 Drive Neodymium Content Reference

Seagate drive neodymium content reference range:

Table 16-1

Product Series Name	Neodymium Content Range		
	＜ 5g	5g - 25g	＞ 25g
Cimarron（2T/4T）	√		
Cimarron（6T/8T）		√	
Evans		√	
Kestrel	√		
MakaraBP		√	
MakaraPLUS		√	
Mobula		√	
MobulaBP		√	
Skybolt	√		
Tatsu		√	

WD drive neodymium content reference range:

Table 16-2

Product Series Name	Neodymium Content Range		
	＜ 5g	5g - 25g	＞ 25g
Rainier	√		
Libra He10		√	
Leo A		√	
Vela-A		√	
Vela-AX		√	
Vela-AP		√	
Hs14		√	
Leo-B		√	

Toshiba drive neodymium content reference range:

Table 16-3

Product Series Name	Neodymium Content Range		
	＜ 5g	5g - 25g	＞ 25g
AL14SE-Lite	√		
AL15SE	√		
AL14SX	√		
MG04 Tomcat-R SAS		√	
MG04 Tomcat-R SATA		√	
MG04 Tomcat SATA		√	
MG06 SAS		√	
MG06 SATA		√	
MG07 SAS		√	
MG07 SATA		√	