Inspur Server User Manual

NX5460M5

© Copyright Inspur 2018. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Inspur.
The information in this manual is subject to change without notice.
Inspur is the registered trademark of Inspur. All the other trademarks or registered trademarks mentioned in this manual are the property of their respective holders.

Edition: 1.0
Aug. 2018

Abstract

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

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

Target Audience

This manual is intended for:

- Technical support engineers
- Product maintenance engineers
- Technicians

Warnings:

This manual introduces the NX5460M5 server's technical features, system installation and setup, which will help the user to understand how best to utilize the server and all its functionalities.

1.For your safety, please do not disassemble the server's components arbitrarily. Please do not extend configuration or connect other peripheral devices arbitrarily. If needed, please contact Inspur for our support and guidance.

2.Before disassembling the server's components, please be sure to disconnect all the power cords connected to the server.

3.BIOS and BMC setup is a significant factor in correctly configuring your server. If there are no special requirements, it is suggested to use the Default Values and not alter the parameter settings arbitrarily. 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

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

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

not to block the air vents.

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

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

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

1) The power cables, extension cables or power plugs are damaged.

2) The products get wet.
3) The products have fallen or have been damaged.
4) Other objects have fallen into the products.
5) The products do not or are unable to function normally even when attempting to operate according to the instructions.

2. If the system becomes wet or damp, please follow these steps:

1) Power off the equipment, disconnect them with the power socket, wait for 10 to 20 seconds, and then open the host cover.
2) Move the equipment to a well-ventilated place to dry the system at least for 24 hours and make sure that the system is fully dried.
3) Close the host cover, reconnect the system to the power socket, and then power on.
4) In case of operation failure or other abnormal situations, please contact Inspur and get technical support.

3. Pay attention to the position of system cables and power cables-avoid placing wires in high foot traffic locations. Please do not place objects on the cables.
4. Before removing the host cover, and/or touching the internal components, please allow for the equipment to cool first. To avoid damaging the mainboard, please power off the system and wait for five seconds, and then remove the components from the mainboard and/or disconnect the peripheral device from the system. Please remember that only service technicians trained by Inspur are authorized to remove the cover of the host, and to remove and replace internal components.
5. If there is modem, telecom or LAN options installed in the equipment, please pay attention to the followings:

1) In the case of thunder and lightning, please do not connect or use the modem.
2) Never connect or use the modem in a damp environment.
3) Never insert the modem or telephone cables into the socket of network interface controller (NIC).
4) Before unpacking the product package, installing internal components, touching uninsulated cables or jacks of the modem, please disconnect the modem cables.

6. In order to prevent electrostatic discharge from damaging the electronic components in the equipment, please pay attention to the followings:

1) Please remove any static electricity on your body before dismounting or touching any electronic component in the equipment, to prevent the static electricity from

conducting itself to the sensitive components. You may remove the static electricity on the body by touching the metal earthing objects (such as the unpainted metal surface on the rack).

2) Please do not take electrostatic sensitive components that are not ready to be installed for application out of the antistatic package materials.

3) While working, please touch the earthing conductor or the unpainted metal surface on the cabinet regularly to remove any static electricity from the body that may damage the internal components.

7. Upon receiving the proper authorization from Inspur and dismounting the internal components, please pay attention to the following:

1) Switch the system power supply off and disconnect the cables, including all connections of the system. When disconnecting the cables, please hold the connector of the cables and slowly pull the plugs out. Never pull on the cables.

2) The products need to completely cool down before 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 Specification

2.1 Introduction

Inspur NX5460M5 is a half-width 2S blade server, which is designed on the basis of the new generation of Intel® Xeon® scalable processor. The product is optimized for cloud computing, virtualization, HPC and other requirements:

- **Ultra-high performance**: Supports a full range of CPUs (up to 205W) with a new generation of Intel® Xeon® scalable processors, up to 28 cores per CPU, and the industry's highest density of computing power. It supports 24 DIMMs, up to 3TB DDR4 memory, providing large memory expansion capability; and supports 2 SATA/SAS/NVME SSDs and 2 M.2 SSDs to meet users' high-speed read-write storage needs.
- **Flexible expansion:** Under the premise of maintaining the highest density among the blade servers, the unique IO BOX design can be combined with standard network cards to achieve the parallel of direct and exchange solutions to meet the customers' needs. At the same time, it can support the one front PCIe X16 slot, equipped with FPGA and IO accelerator card, further improving the performance of the blade server and meeting the different application needs of customers.
- **Intelligent management**: Intelligent management software developed by Inspur supports advanced functions such as stateless computing and multi-chassis management, greatly improving the product management efficiency and deployment speed. It also provides standardized interfaces, supports a range of industry-standard specifications, and provides seamless connectivity for third-party management.
- **Green energy saving:** N+N redundant centralized power supply design improves power conversion efficiency to 92%. At the same time, it adopts the most advanced Z-type heat dissipation architecture and centralized cooling fan to achieve optimal balance between heat dissipation and muting. With Inspur's unique intelligent management software and patented technology, the product achieves optimal green energy saving and reduces TCO.

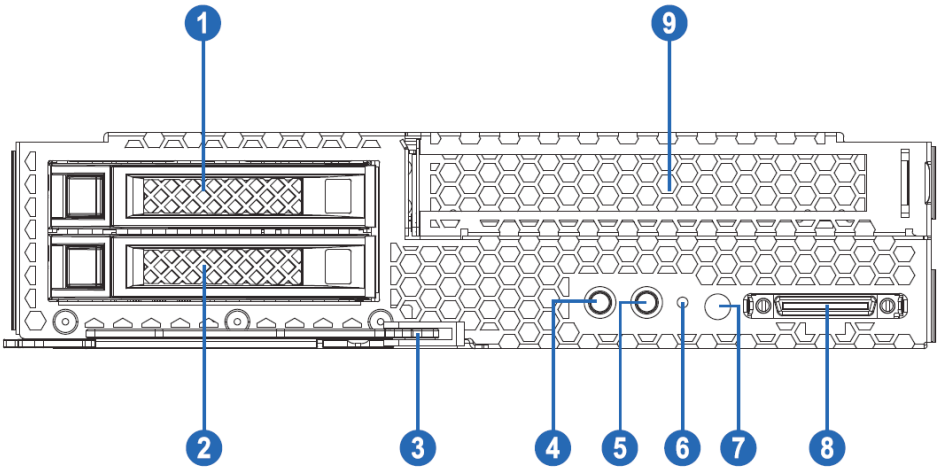
2.2 Features and Specifications

Processor	
Processor Type	Intel® Skylake series processors
Chipset	
Chipset Type	Intel® C62x Chipset Family
Memory	
Memory Type	ECC Registered DDR4, RDIMM, LRDIMM, NVDIMM
Memory Slot Qty.	24
Total Memory Capacity	Supports up to 3TB (128GB per memory)
I/O	
USB	Front: 2 USB2.0 ports + 1 USB3.0 port Internal: 1 USB3.0 port
VGA	Front: 1 VGA port
Display	
Controller Type	Integrated in the chip Aspeed2500, up to 1920×1080 resolution
SAS	
SAS3.0 Backplane	Supports hot-plug SAS/SATA/SSD/NVME disks
SATA3.0 Backplane	Supports hot-plug SATA/SSD disks
Hard Drive	
Hard Drive Type	SAS, SATA, SSD, NVME, SATA M.2 and PCIE M.2
Management	
Management Chip	AST2500 chip
NIC	
NIC controller	Onboard Gigabit NIC
PCIE	
PCI Expansion Slot	1 PCI Express 3.0 x16 slot
External Storage Drive	
Optical Drive	Supports external USB drive
Environmental	
Operating Temperature	10℃ -35℃
Storage & Transportation Temperature	-40℃ -60℃
Operating Humidity	20％ -80％ relative humidity
Storage & Transportation Humidity	20％ -93％ (40℃) relative humidity

3 Component Identification

3.1 Front Panel Components

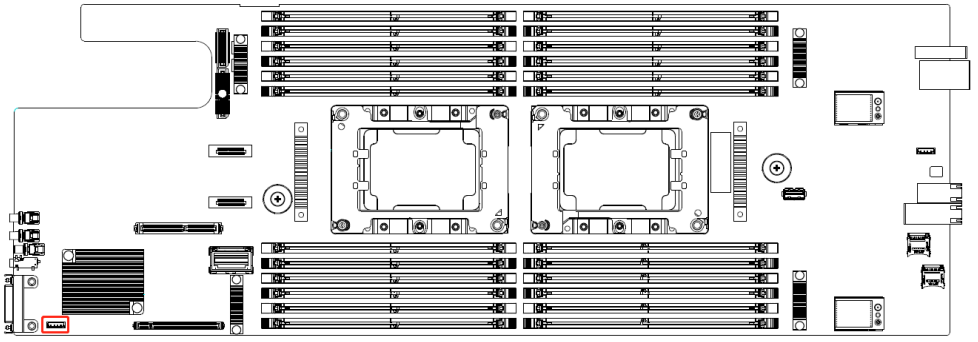
Front View



Item	Name & Function
1~2	HDD 1/0
3	Handle
4	UID button/LED Used to locate the compute node to be operated in the rack; turn on/off the light through manual pressing/ BMC remote control. Off: The compute node is not located. Steady blue: The compute node is located.
5	Power button/LED Off: No power Steady green: Powered on
6	Reset button & Status LED Off: Normal Steady red: Abnormal
7	BMC serial port
8	High-density interface (Extend 2 USB2.0 ports + 1 USB3.0 port + 1 VGA port + 1 serial port)
9	PCIE slot (×16)

3.2 CLR_CMOS Jumper Introduction

The jumper position is shown in the red box below.



Item	Description	Function
CLR_CMOS (J54)	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. Power off the server, and open the node handle.
2. Extend the server from the rack.

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

3. After performing the installation or maintenance procedure, slide the server back into the rack.

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

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. Press down the hood latch, and then push the access panel back to remove it.

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 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.

5.1.2 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.

5.1.3 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 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
- Documents checklist

In addition to the supplied items, you may need:

- Operating system or application software
- Hardware options

5.3 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”.

5.4 Installing the Operating System

To operate properly, the server must have a supported operating system installed. For the latest information on supported operating systems, refer to the Inspur website (http://www.inspur.com).

Installing an operating system on the server may require you to obtain additional drivers from the Inspur website (http://www.inspur.com).

6 Hardware Options Installation

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.

6.1 Processor Option

This server 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 configurations must contain processors with the same part number.

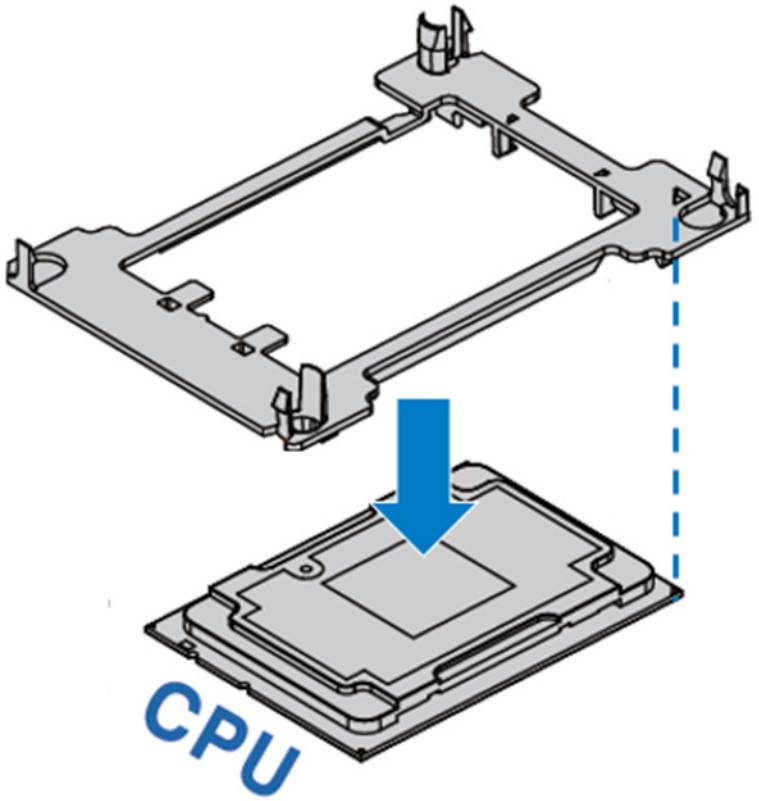
⚠ **CAUTION:** To install a faster processor, update the system ROM before installing the processor.

To install the component:

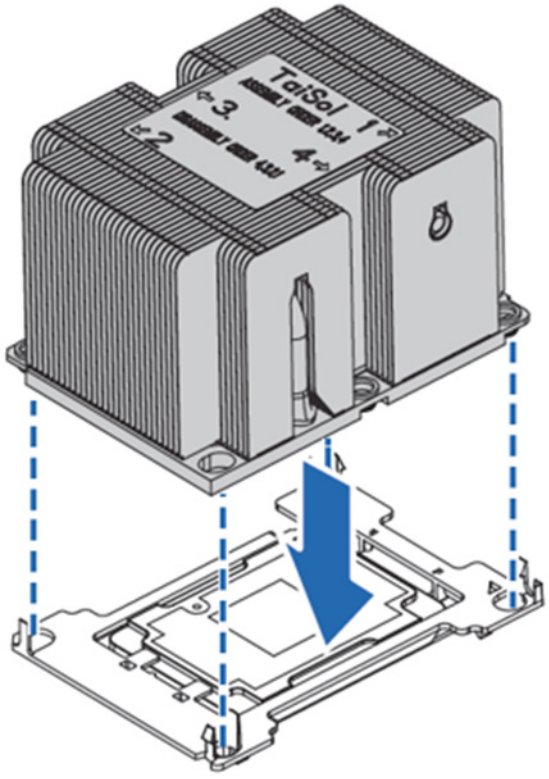
1. Power down the server.
2. Extend the server from the rack.
3. Remove the top cover.
4. Remove the air baffle.

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

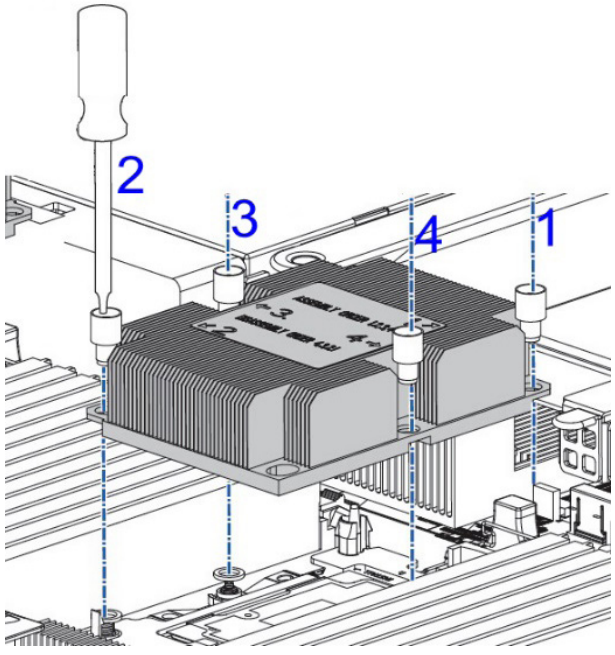
Step 1: Align the Clip's triangle mark with the CPU's corner mark, and then assemble the Clip and CPU together.



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



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



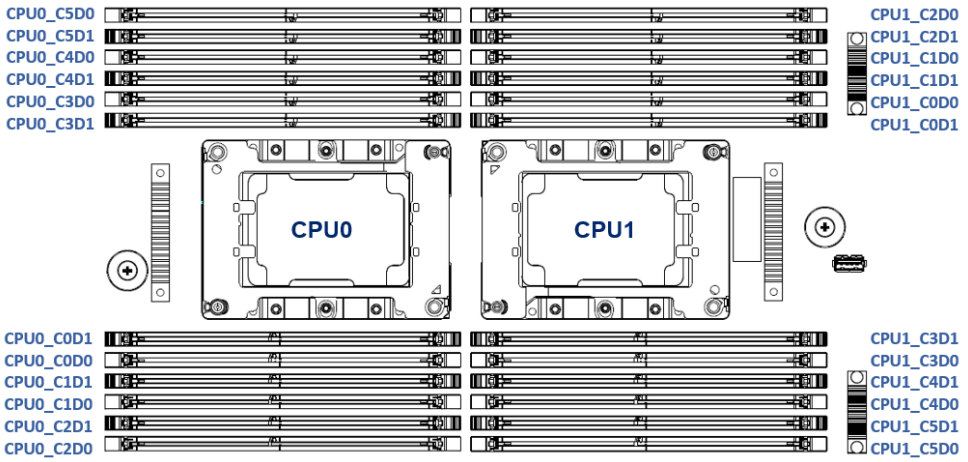
Notes:

● It is required to coat thermal grease evenly onto the contact position between CPU heatsink and CPU.

● During fixing CPU heatsink, it is required to fasten screws according to the sequence accordingly.

6.2 Memory Option

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



● DIMM population guidelines:

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

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

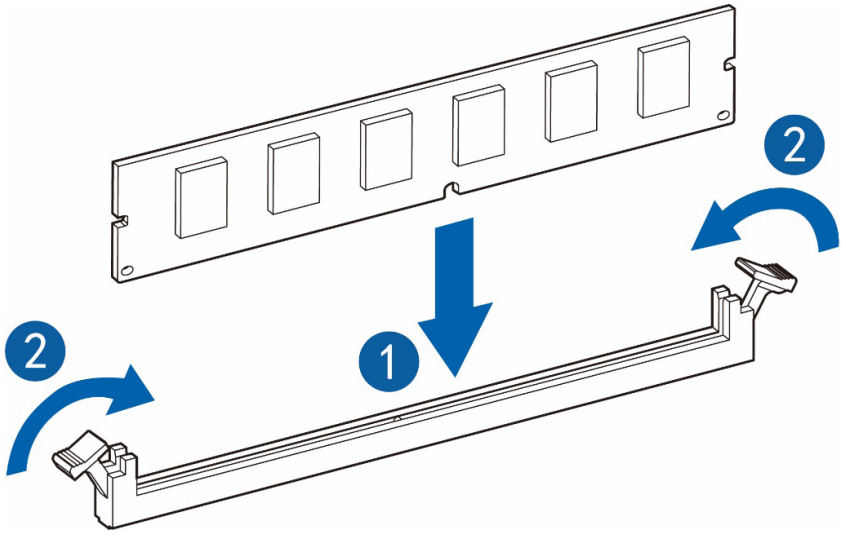
c. For dual CPUs, CPU0 DIMM population follows the screen printed sequence: CPU0_C0D0, CPU0_C1D0, CPU0_C2D0, CPU0_C3D0, CPU0_C4D0, CPU0_C5D0, CPU0_C0D1… ; CPU1 DIMM population follows the screen printed sequence: CPU1_C0D0, CPU1_C1D0, CPU1_ C2D0, CPU1_C3D0, CPU1_C4D0, CPU1_C5D0, CPU1_C0D1…

Installation steps:

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

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

automatically secure the DIMM, locking it into place.

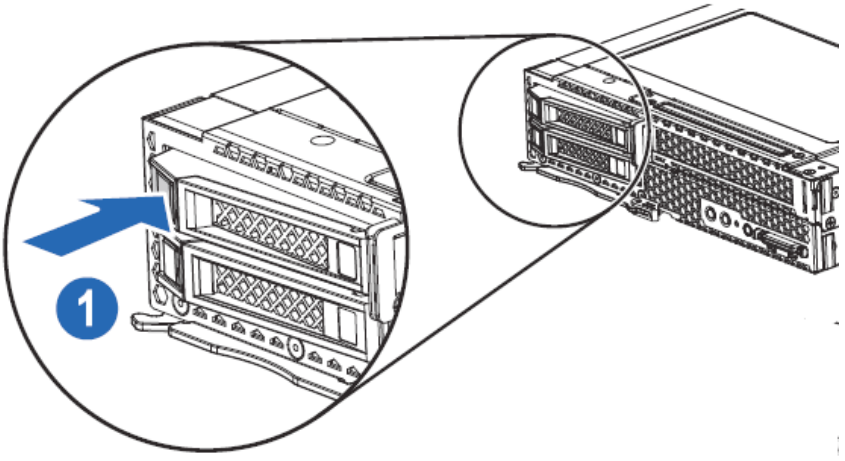


6.3 Hot-plug HDD Option

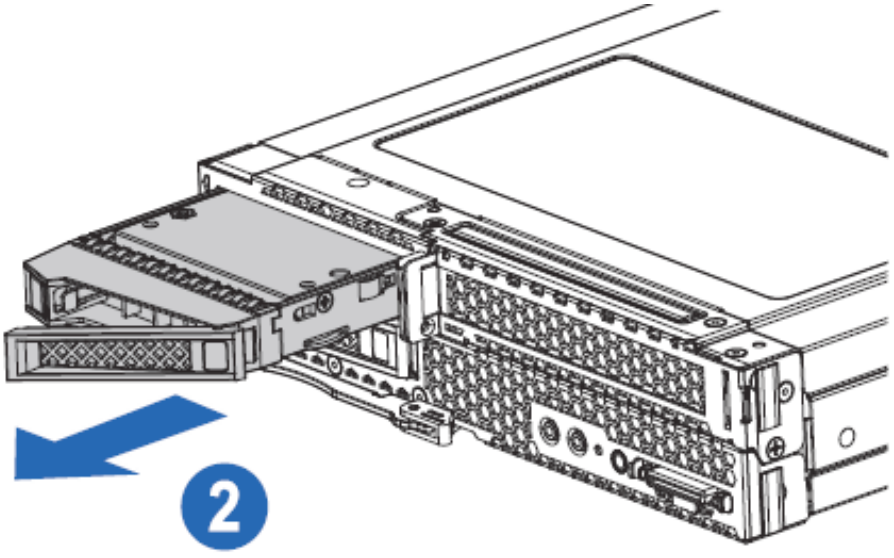
CAUTION: For proper cooling, do not operate the server without the access panel, baffles, expansion slot covers, or blanks installed. If the server supports hot-plug components, minimize the amount of time the access panel is open.

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.

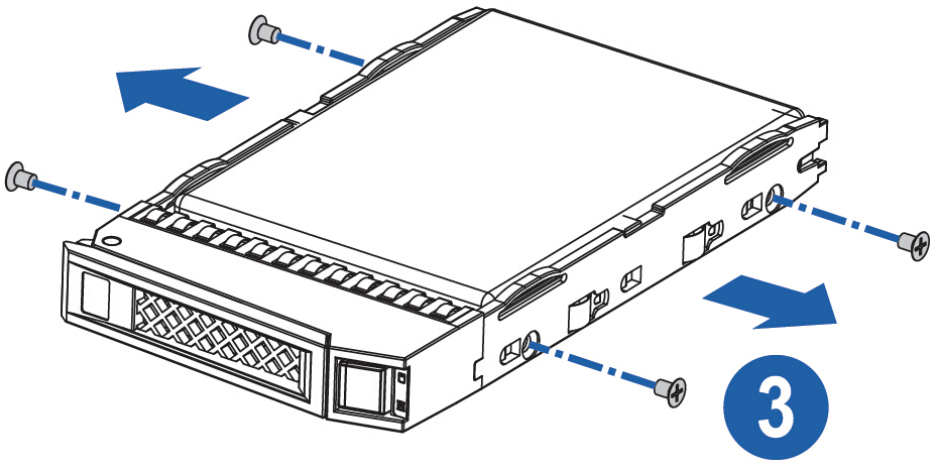
Step 1: Press the HDD panel button, the lever on HDD tray pops up automatically.



Step 2: Remove the HDD tray out of the chassis.



Step 3: Remove the four screws on the two sides of the tray, and remove the old hard drive.



Step 4: Install a new hard drive into the tray, and install it back into the server. Close the lever to fix the tray firmly.

7 BIOS Setup

This chapter introduces how to configure BIOS. All operations described in this section are limited to experienced operators or administrators with proper system maintenance qualifications.

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.

NX5460M5 server is developed on the basis of Insyde 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 different configurations of the products; hence the detailed introduction is elided.

7.1 Login to BIOS Interface

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

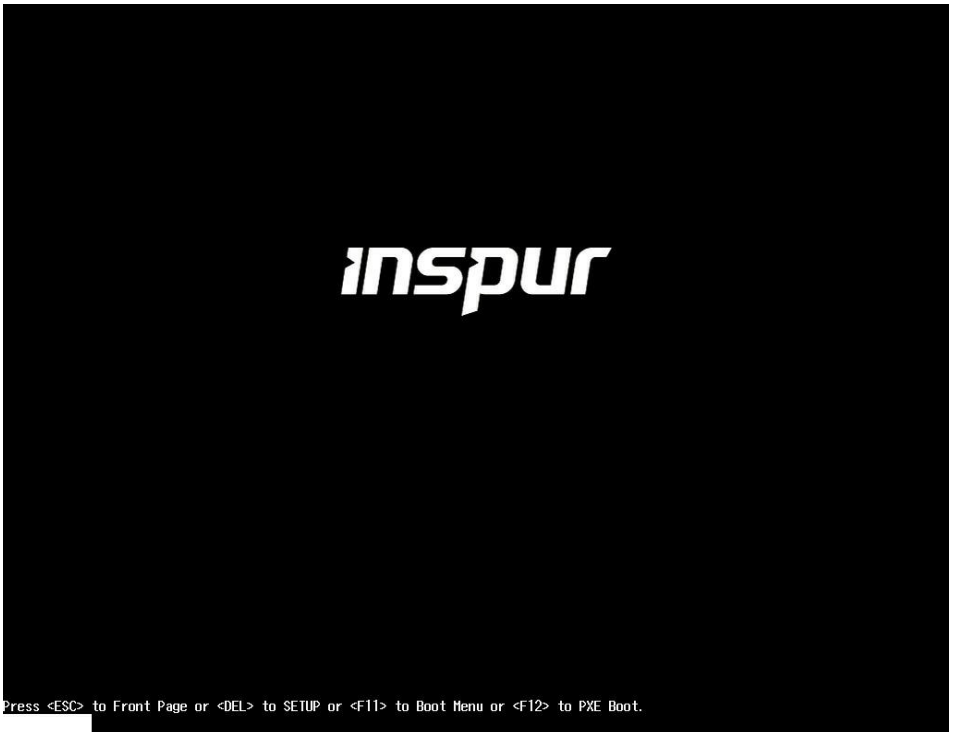
Other hotkeys function:

- ESC: Enter BIOS Front Page interface.
- DEL: Enter BIOS Setup interface.
- F11: Enter the BIOS Boot Manager interface, select the boot device.
- F12: Boot the PXE.

BIOS Setup Interface Control Key Instruction Table

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

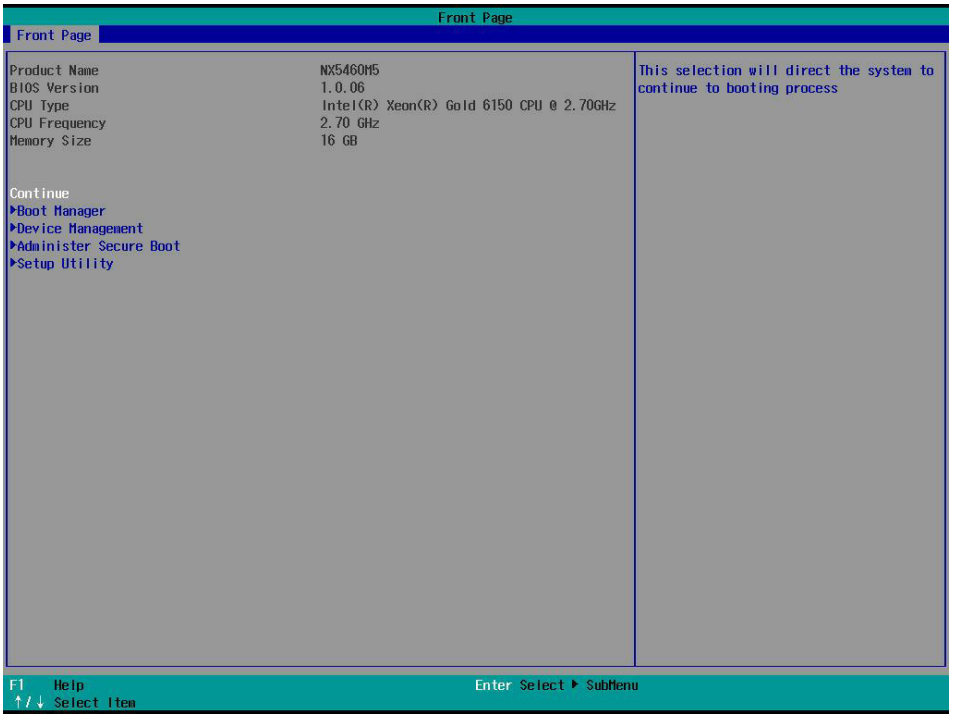
Note: Options in grey are not available. Options with symbol "▶" have a sub-menu.



7.2 BIOS Parameter Description

7.2.1 Front Page

When Inspur Logo appears during system boot, press ESC to enter the BIOS Front Page interface, as shown in the following figure:



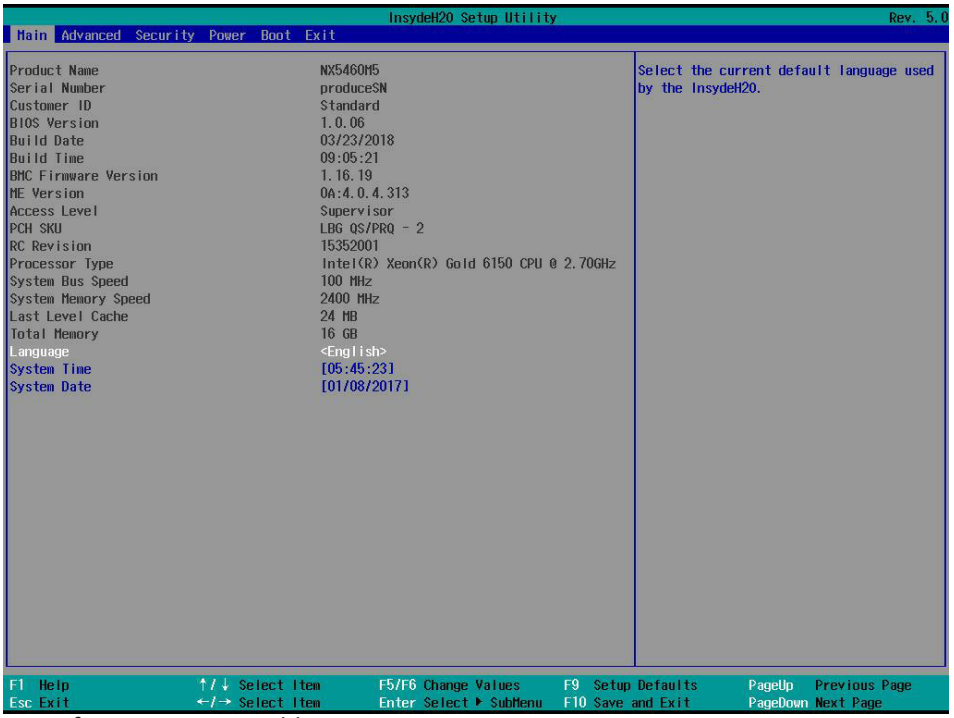
Front Page Interface Instruction Table

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

7.2.2 Main

When the logo appears, press DEL to enter the BIOS Setup Main interface, or select the

Setup Utility option on the Front Page interface to enter the BIOS Setup Main interface. BIOS Main interface contains the basic information of BIOS system, the version information of BIOS, BMC and ME, CPU model information, total memory capacity information and system time. The specific parameters are shown in the following table, and the Main interface is shown in the following figure.

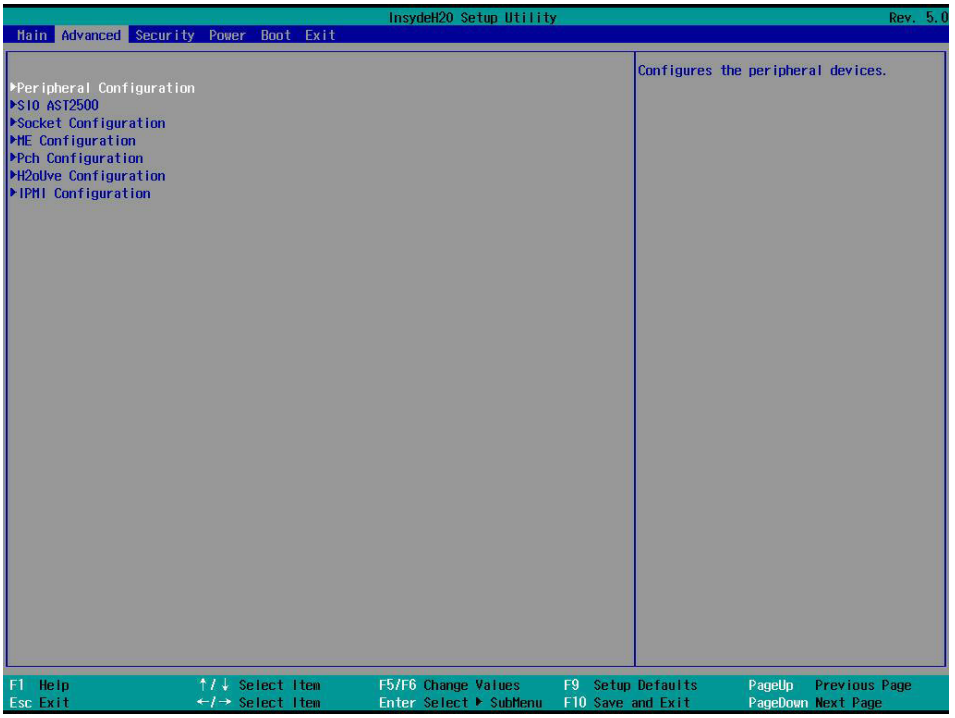


Main Interface Instruction Table

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

7.2.3 Advanced Menu

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

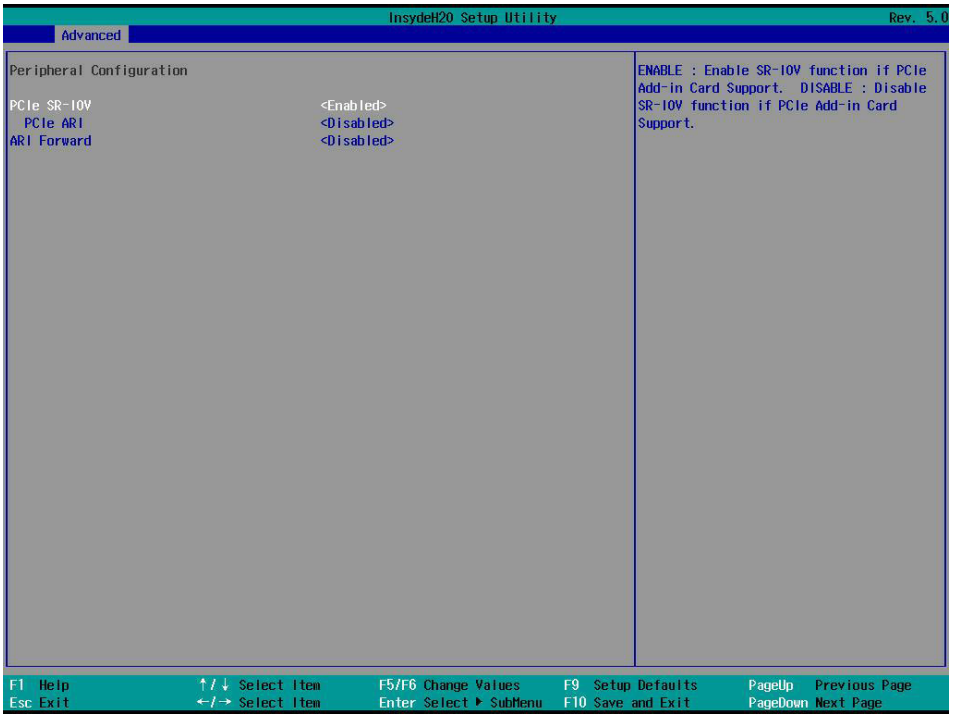


Advanced Interface Instruction Table

Interface Parameters	**Function Description**
Peripheral Configuration	Peripheral devices configuration options menu
SIO AST2500	SIO configuration options menu
Socket Configuration	Socket configuration options menu
ME Configuration	ME configuration options menu
PCH Configuration	PCH configuration options menu
H2oUve Configuration	H2oUve configuration options menu
IPMI Configuration	IPMI configuration options menu

7.2.3.1 Peripheral Configuration

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



Peripheral Configuration Interface Instruction Table

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

7.2.3.2 SIO AST2500

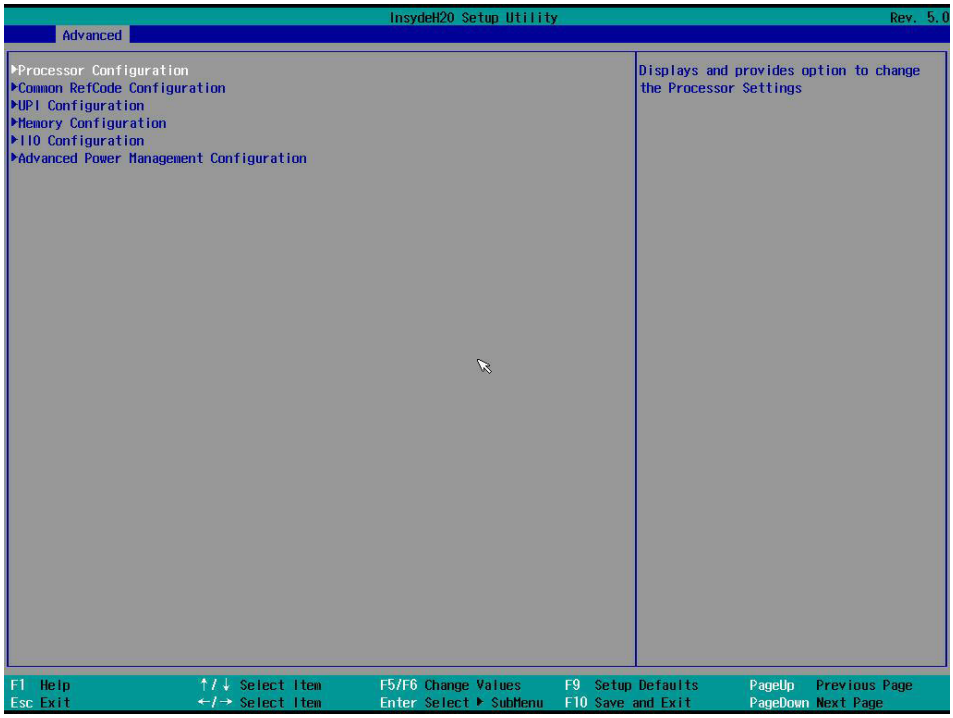
SIO AST2500 interface is used for serial port settings, as shown in the following figure and table.

SIO AST2500 Interface Instruction Table

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

7.2.3.3 Socket Configuration

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

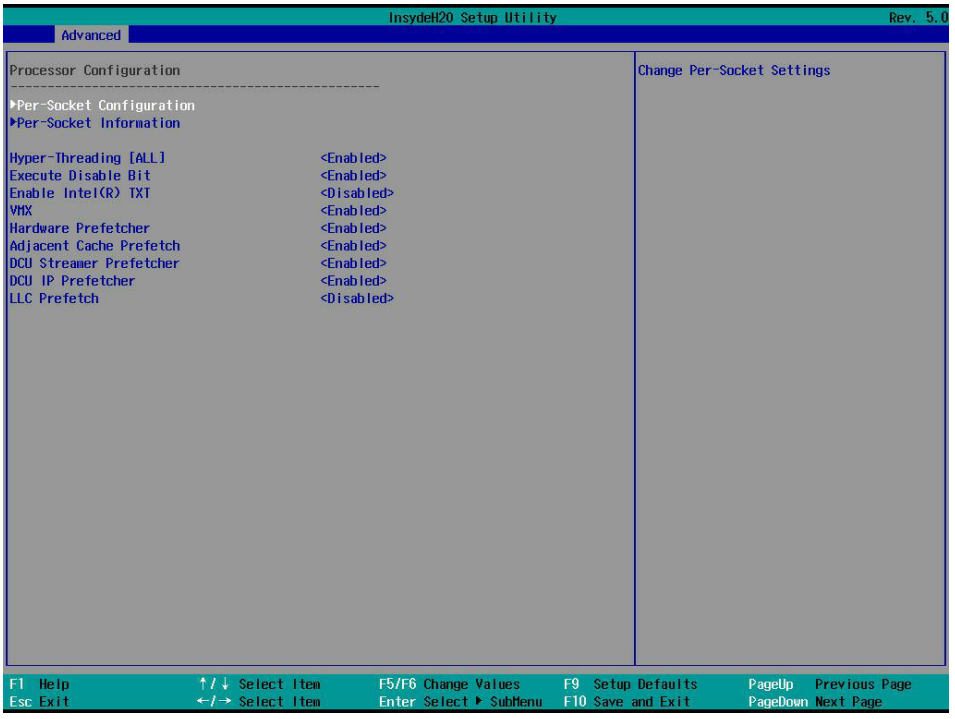


Socket Configuration Interface Instruction Table

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

7.2.3.3.1 Processor Configuration

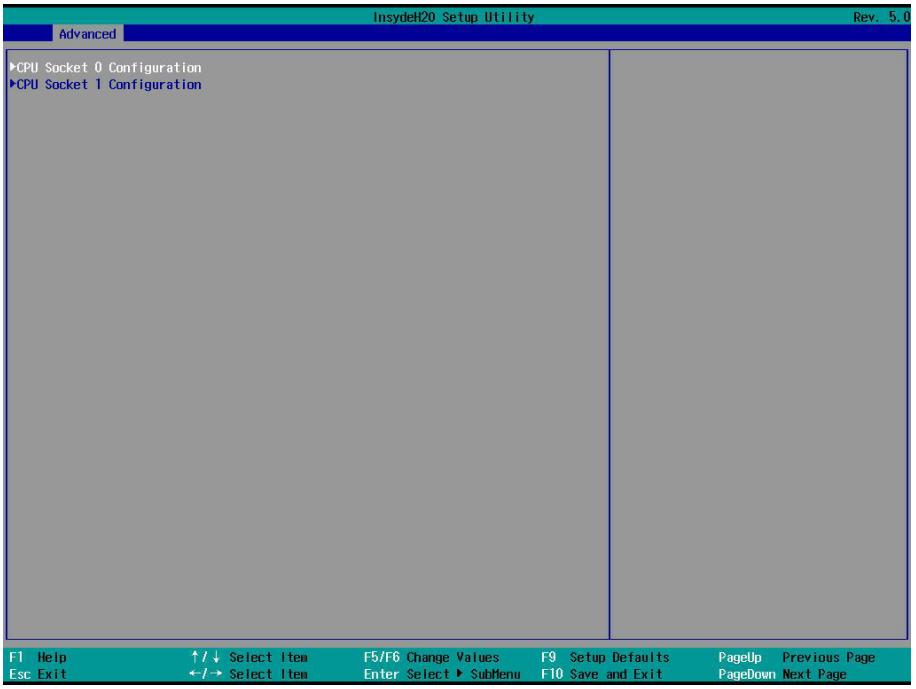
Processor Configuration interface is used for system processor related settings, as shown in the following figure and table.

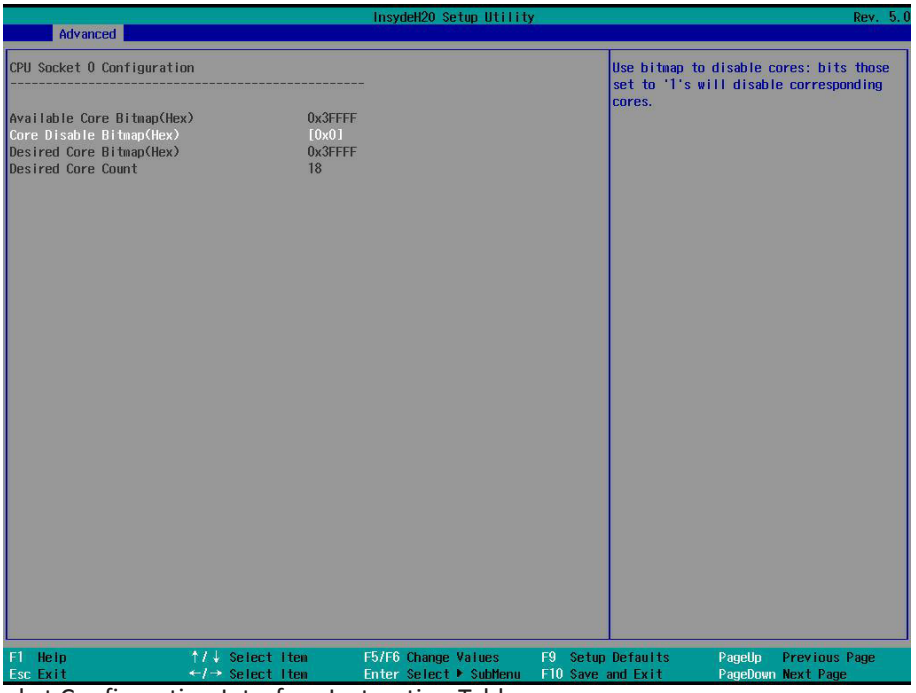


Processor Configuration Interface Instruction Table

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

(a) Select Per-Socket Configuration menu, Enable/Disable the corresponding core of each CPU, as shown in the following figures :

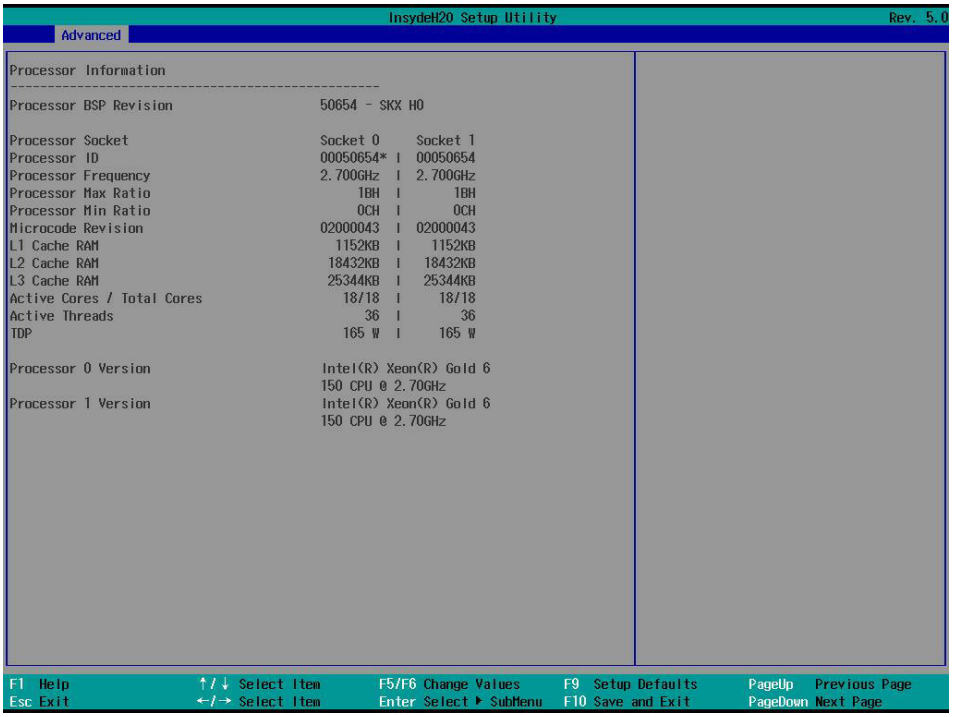




Per-Socket Configuration Interface Instruction Table

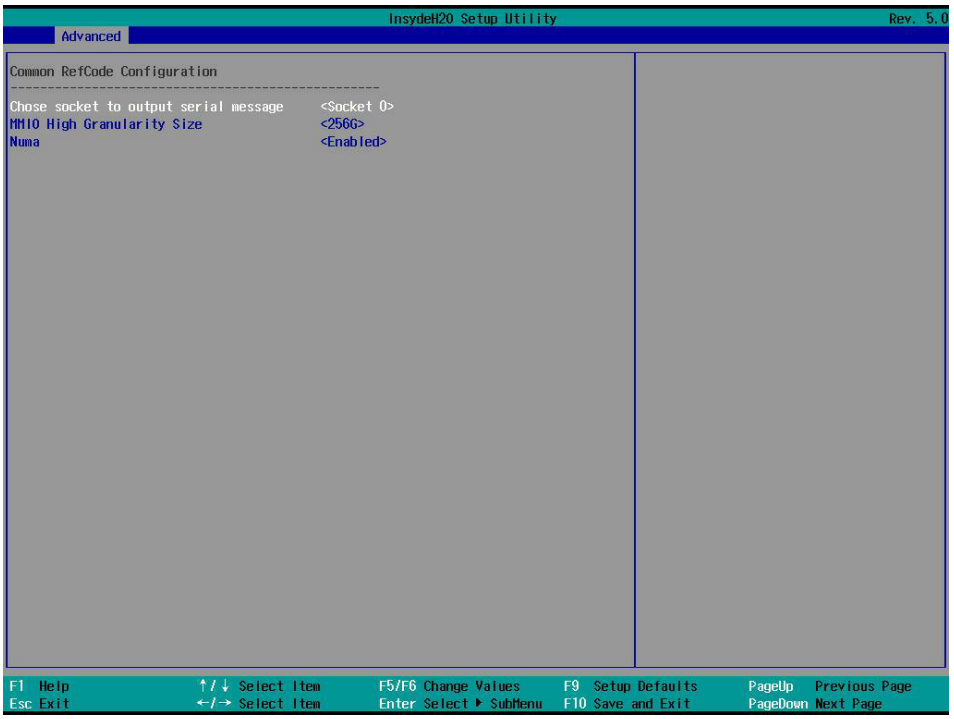
Interface Parameters	Function Description	Default Value
Available Core Bitmap (Hex)	Display the current available core Bitmap in hex	--
Core Disable Bitmap (Hex)	Disable CPU core settings	0x0
Enable Core Bitmap (Hex)	Display enabled CPU cores	--
Desired Core Count	Display enabled core count	--

(b) Per-Socket Information menu displays the current CPU information, as shown below :



7.2.3.3.2 Common RefCode Configuration

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

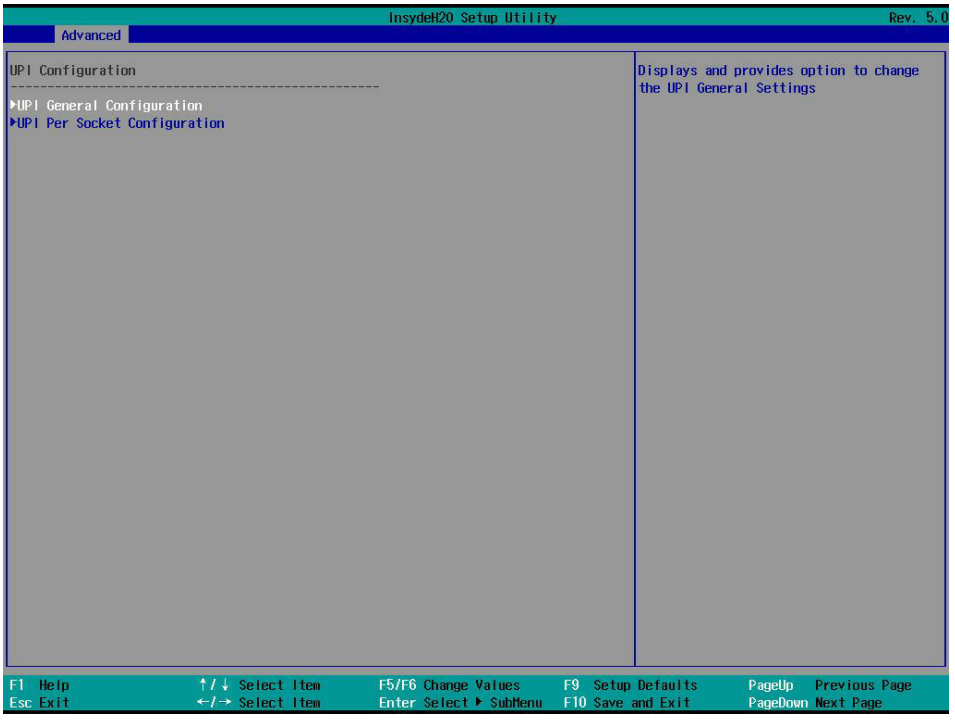


Common RefCode Configuration Interface Introduction

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

7.2.3.3.3 UPI Configuration

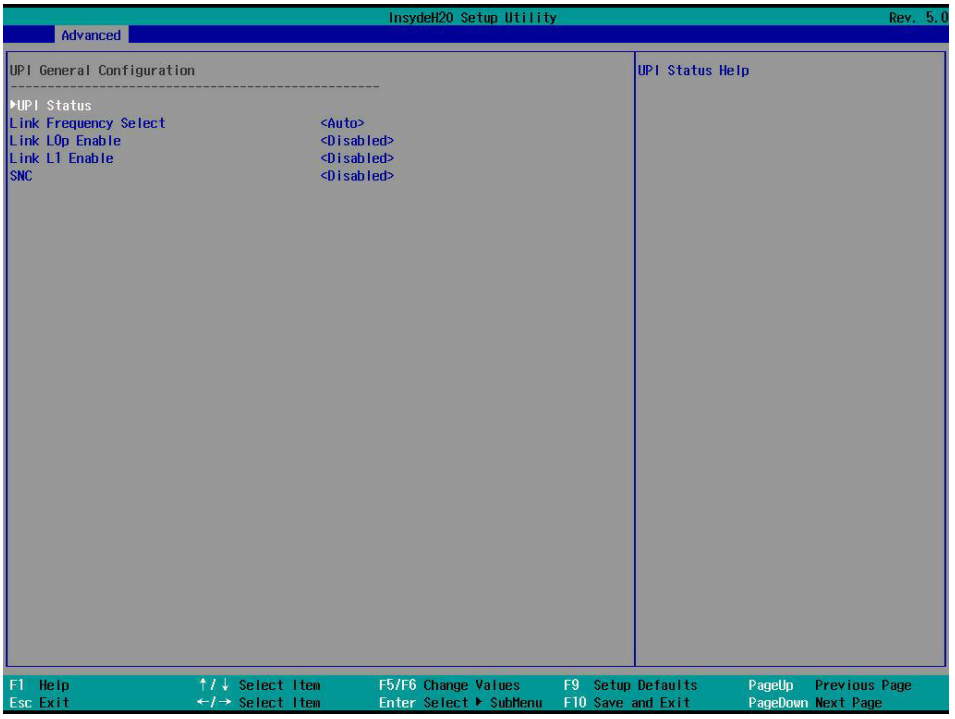
UPI Configuration interface is used for UPI related settings, as shown in the following figure and table.



UPI Configuration Interface Instruction Table

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

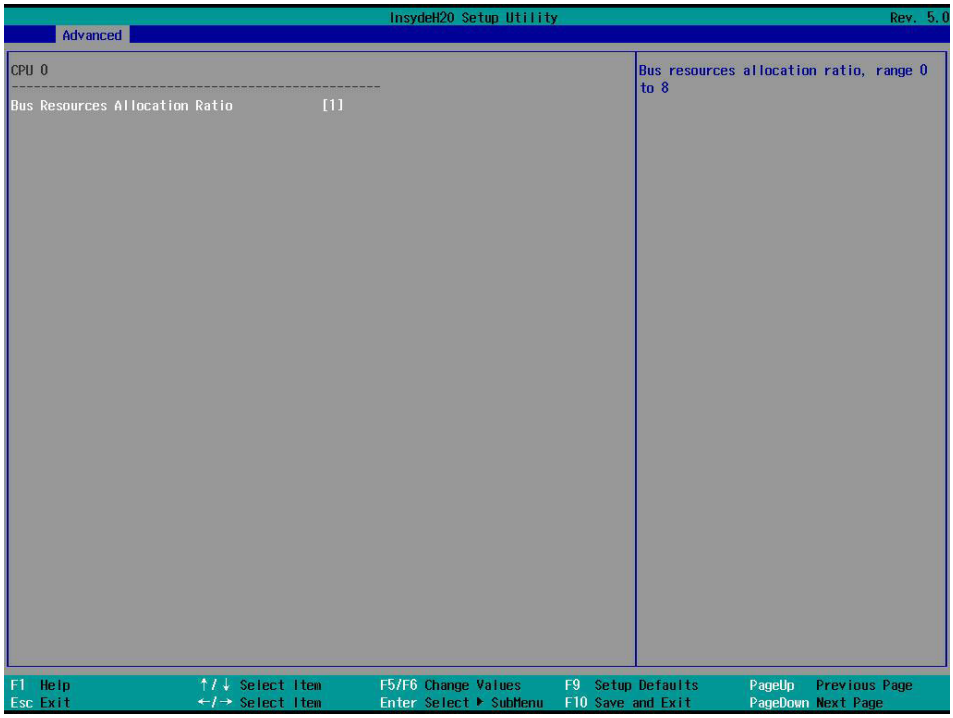
(a) Select UPI General Configuration menu, and it displays the UPI general configuration options, as shown below:



UPI General Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
UPI Status	UPI status display submenu	--
Link Frequency Select	UPI link frequency setting	Auto
Link L0p Enable	UPI link power saving mode settings	Auto
Link L1 Enable	In the case that system is extremely idle, turn off QPI Link.	Auto
SNC	SNC setting	Disabled

(b) Bus resources allocation ration can be configured by entering UPI Per Socket Configuration submenu, as show below:

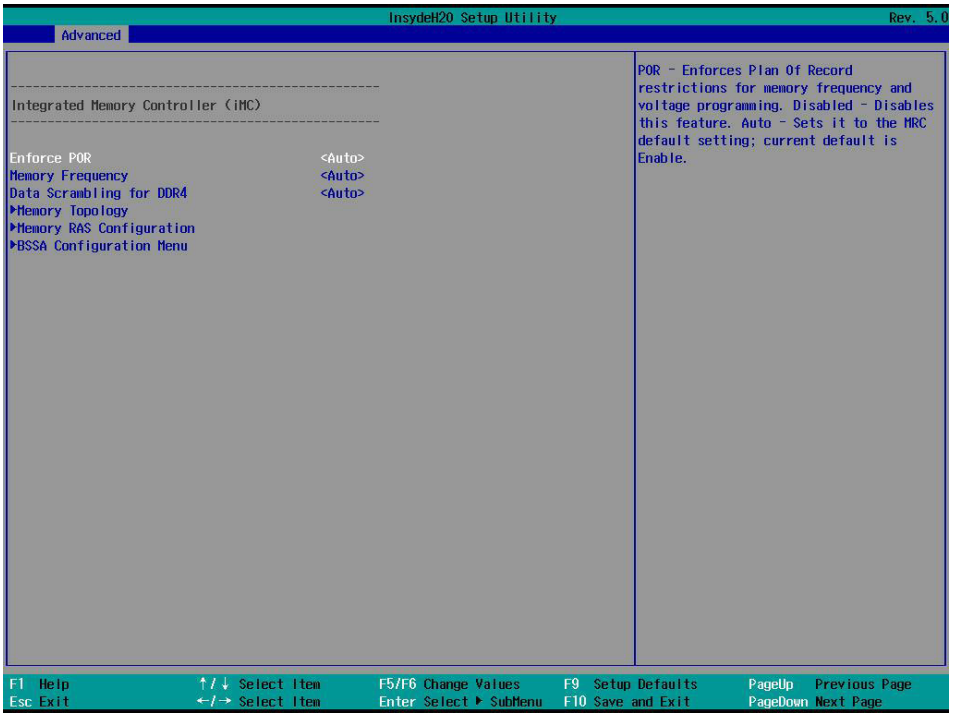


UPI Per Socket Configuration Interface Instruction Table

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

7.2.3.3.4 Memory Configuration

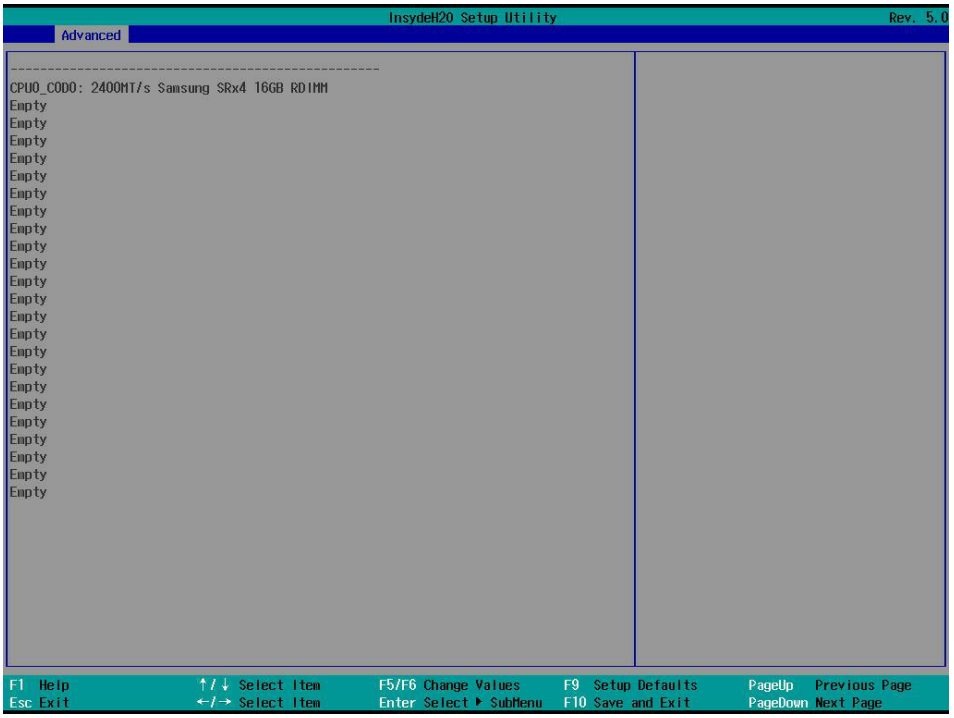
Memory Configuration interface is used for memory related settings, as shown in the following figure and table.



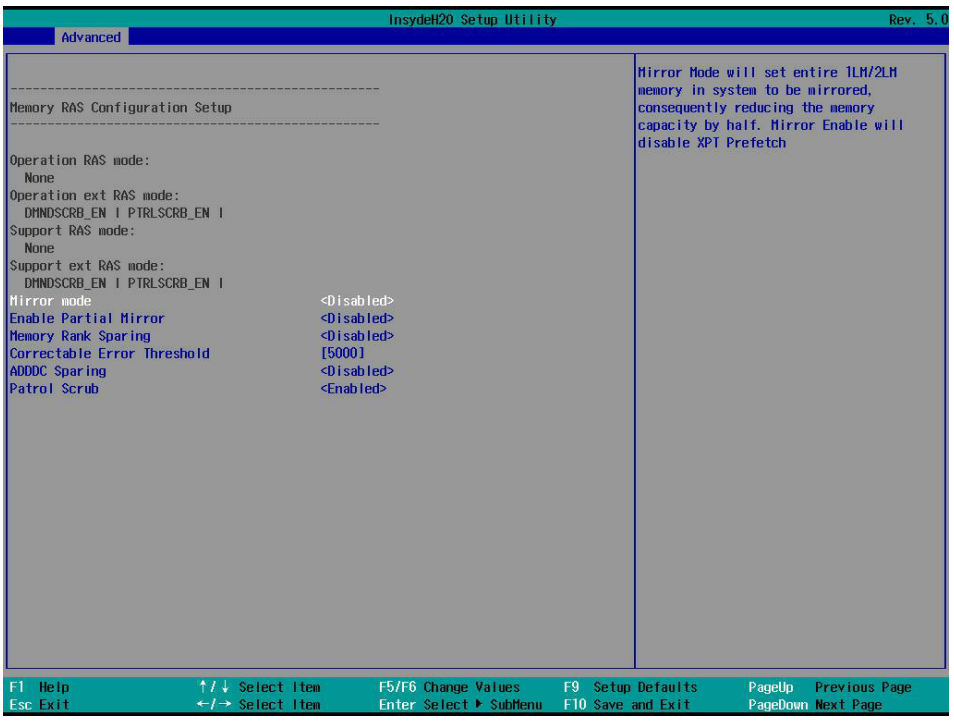
Memory Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Enforce POR	Enforce POR settings	Auto
Memory Frequency	Memory frequency selection	Auto
Data Scrambling for DDR4	Data scrambling setting	Auto
Memory Topology	Memory topology submenu	--
Memory RAS Configuration	Memory RAS setting submenu	--
BSSA Configuration Menu	BSSA configuration menu	--

(a) Select Memory Topology menu, and it will display the memory topology information, as shown below:



(b) Select Memory RAS Configuration menu, and it will display the memory RAS configuration options, as shown below:



Memory RAS Configuration Interface Instruction Table

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

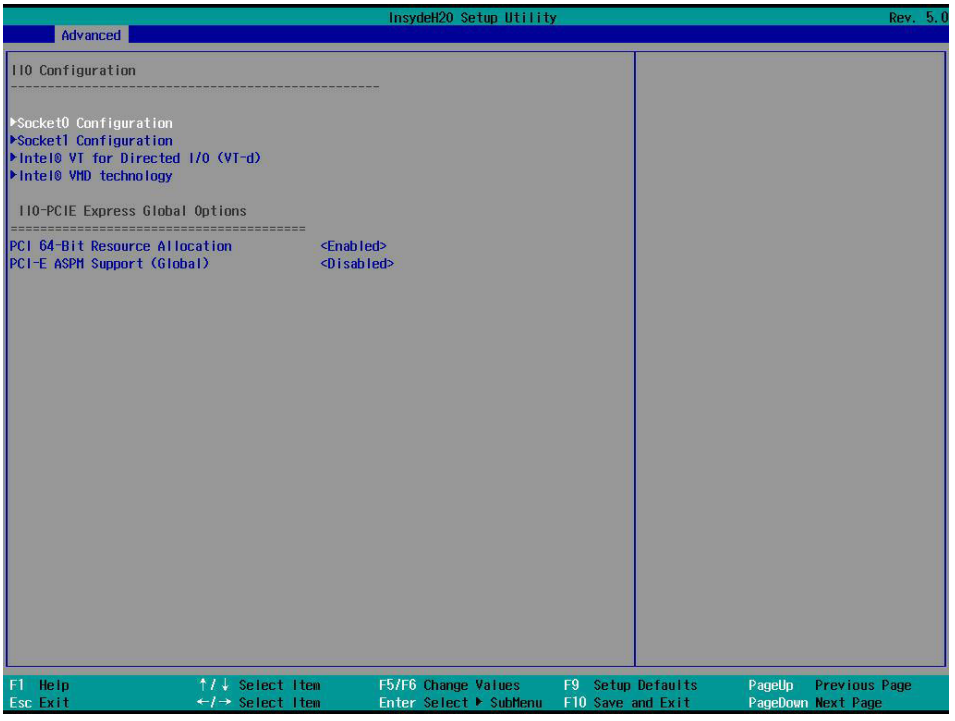
(c) Select BSSA Configuration Menu to enter the BSSA configuration menu options, as shown below:

BSSA Configuration Menu Interface Instruction Table

Interface Parameters	Function Description	Default Value
BSSA Rank Margin Tool	BSSA Rank Margin Tool on/off settings	Disabled

7.2.3.3.5 IIO Configuration

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

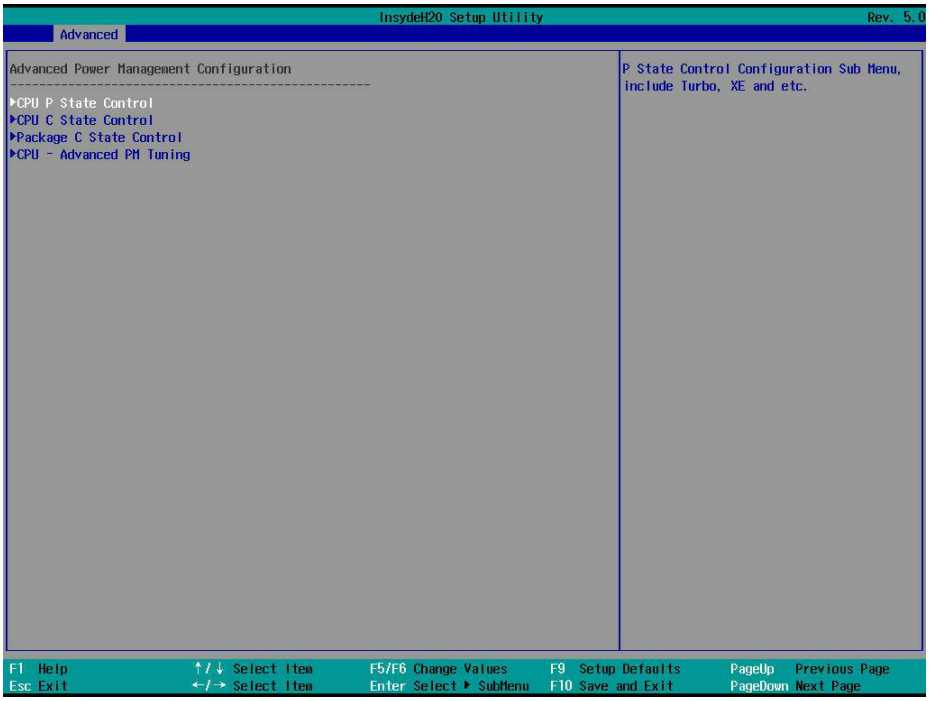


IIO Configuration Interface Instruction Table

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

7.2.3.3.6 Advanced Power Management Configuration

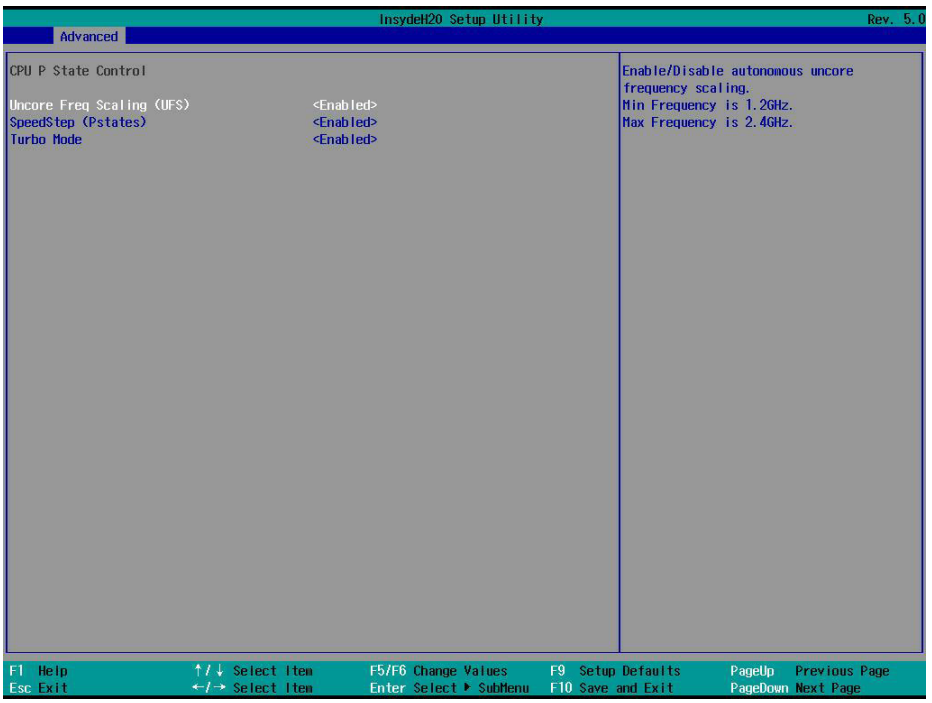
Advanced Power Management Configuration interface is used for CPU power management settings, as shown in the following figure and table.



Advanced Power Management Configuration Interface Instruction Table

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

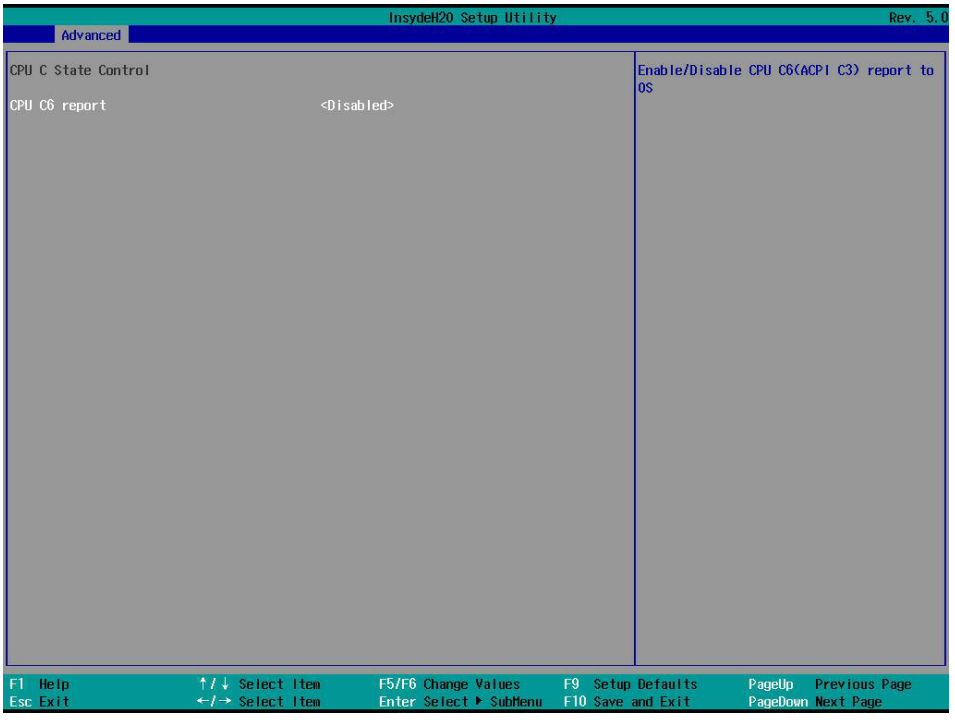
(a) Select CPU P State Control menu to set the related options of CPU P state, as shown below:



CPU P State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
Uncore Fre Scaling (UFS)	Uncore frequency limit setting	Enabled
SpeedStep (Pstates)	SpeedStep on/off setting	Enabled
Turbo Mode	Turbo mode setting	Enabled

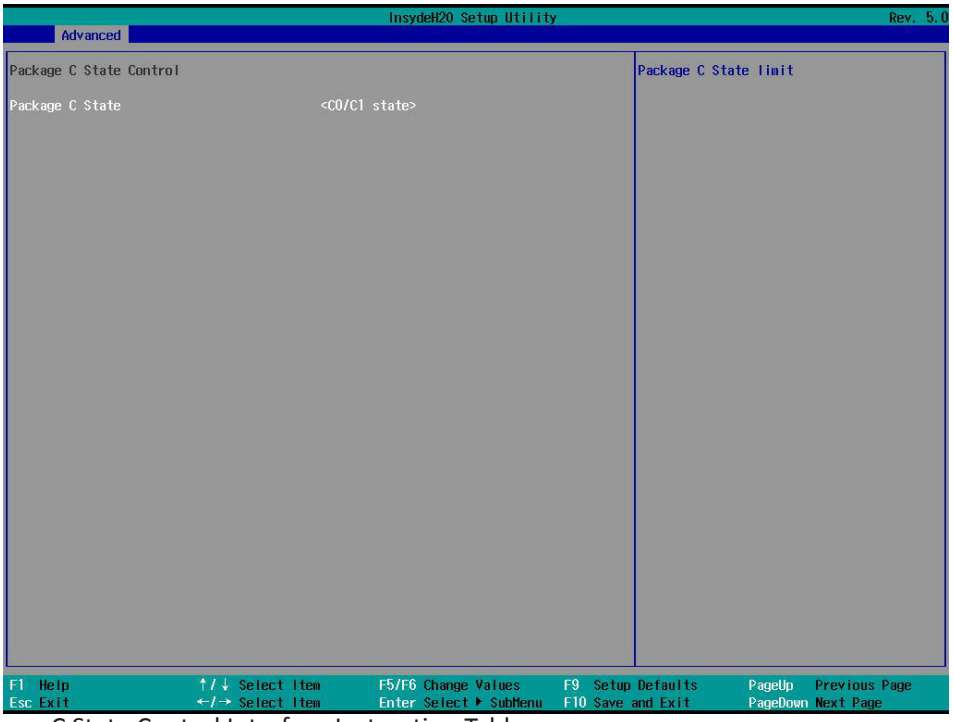
(b) Select CPU C State Control menu to set the related options of CPU C state, as shown below:



CPU C State Control Interface Instruction Table

Interface Parameters	Function Description	Default Value
CPU C6 report	CPU C6 state on/off settings	Disabled

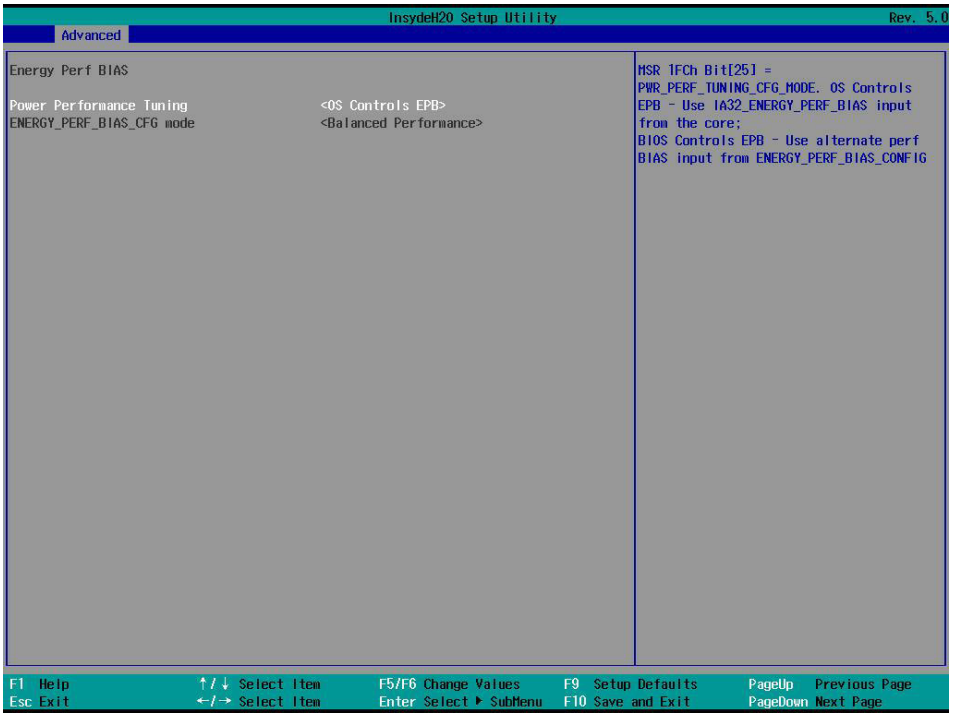
(c) Select Package C State Control menu to set the package C state, as shown below:



Package C State Control Interface Instruction Table

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

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

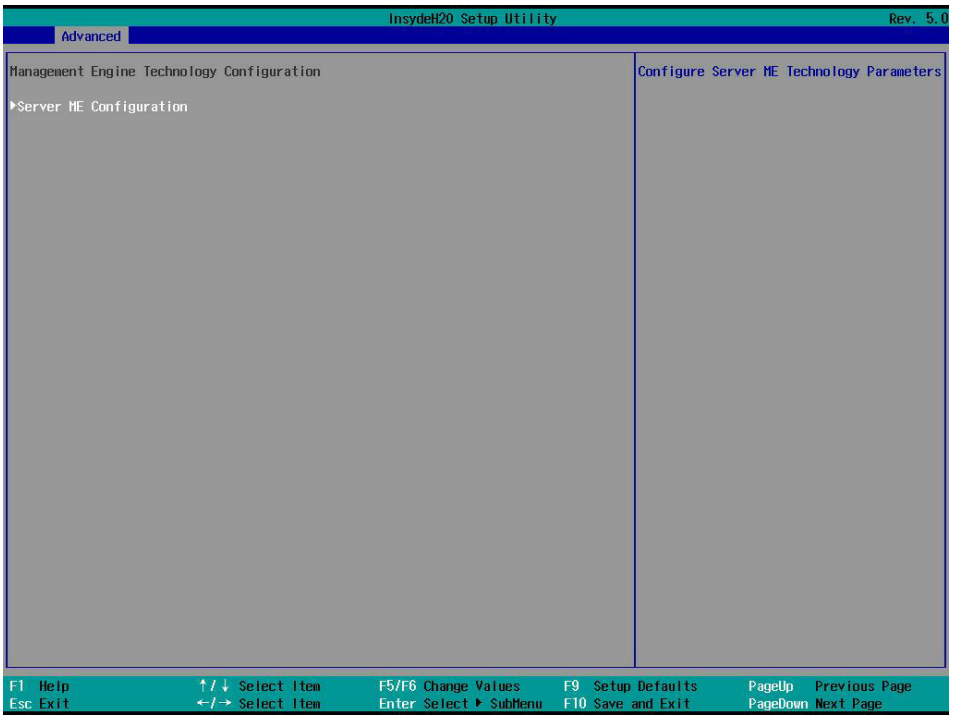


Energy Perf BIAS Interface Instruction Table

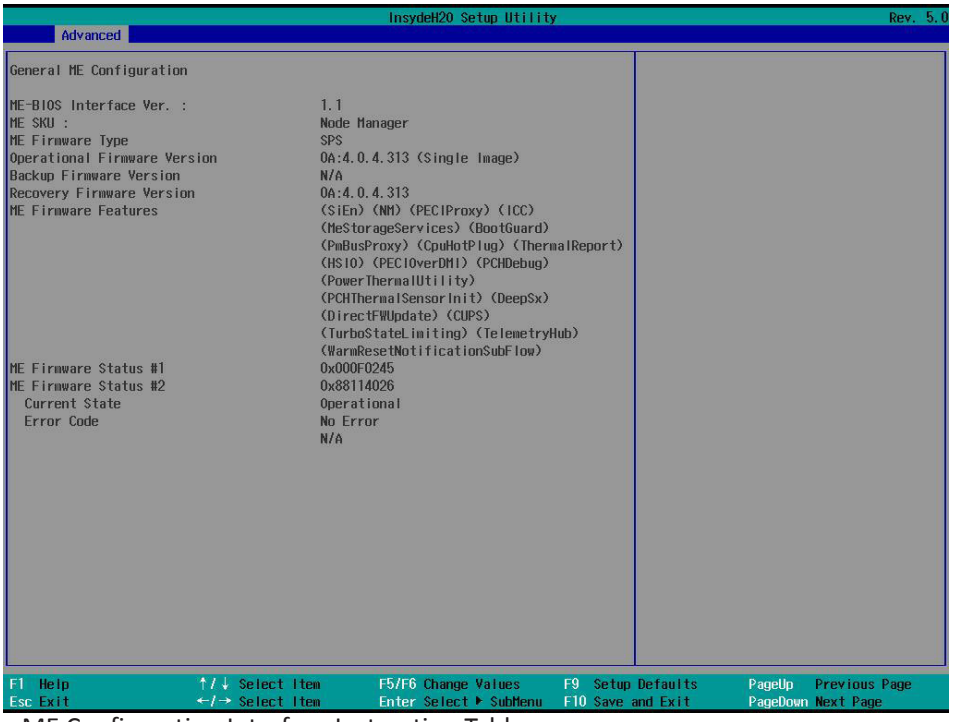
Interface Parameters	**Function Description**	**Default Value**
Power Performance Tuning	Power performance tuning setting	OS Controls EPB
ENERGY_PERF_BIAS_CFG mode	Performance setting	Balanced Performance

7.2.3.4 ME Configuration

ME Configuration interface displays the information related with ME configuration.



The general information of ME configuration will be displayed by entering Server ME Configuration submenu, as shown below:

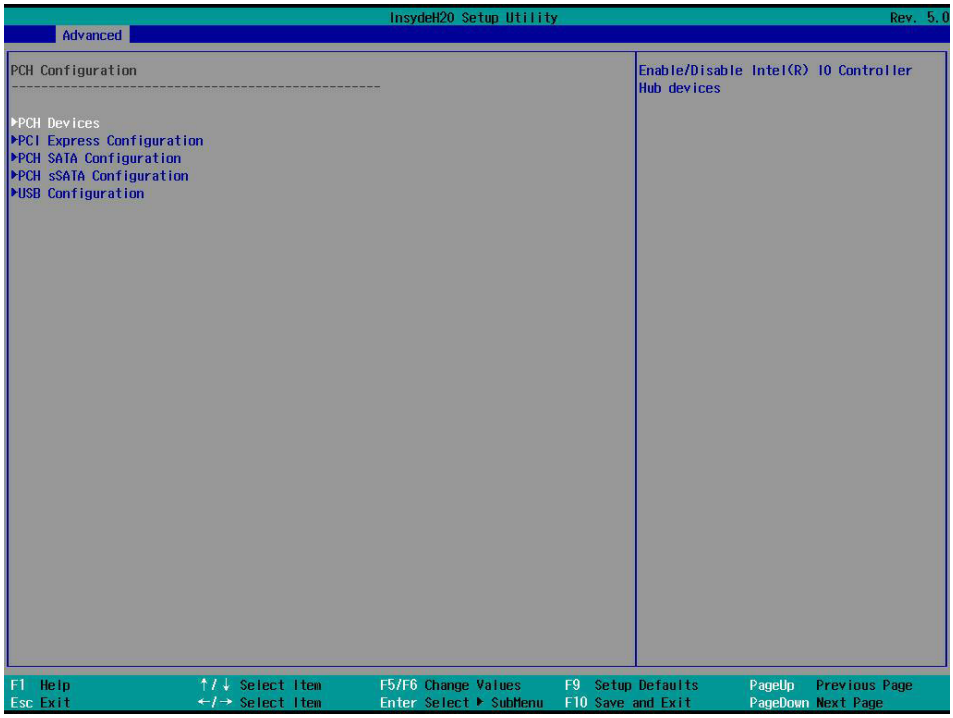


Sever ME Configuration Interface Instruction Table

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

7.2.3.5 PCH Configuration

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

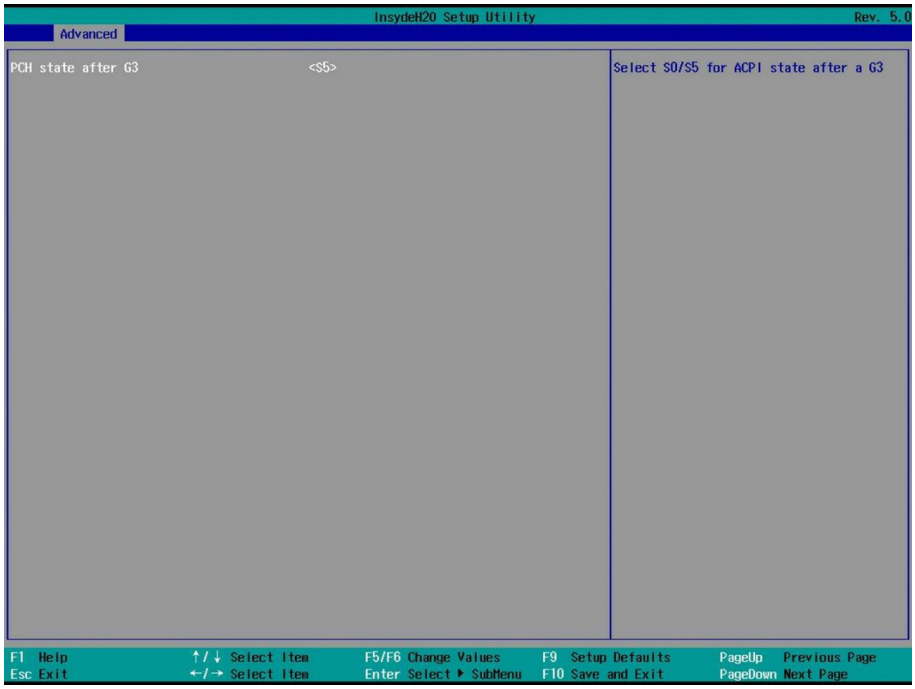


PCH Configuration Interface Instruction Table

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

7.2.3.5.1 PCH Devices

PCH Devices interface is used to set the IO controller, as shown in the following figure and table.

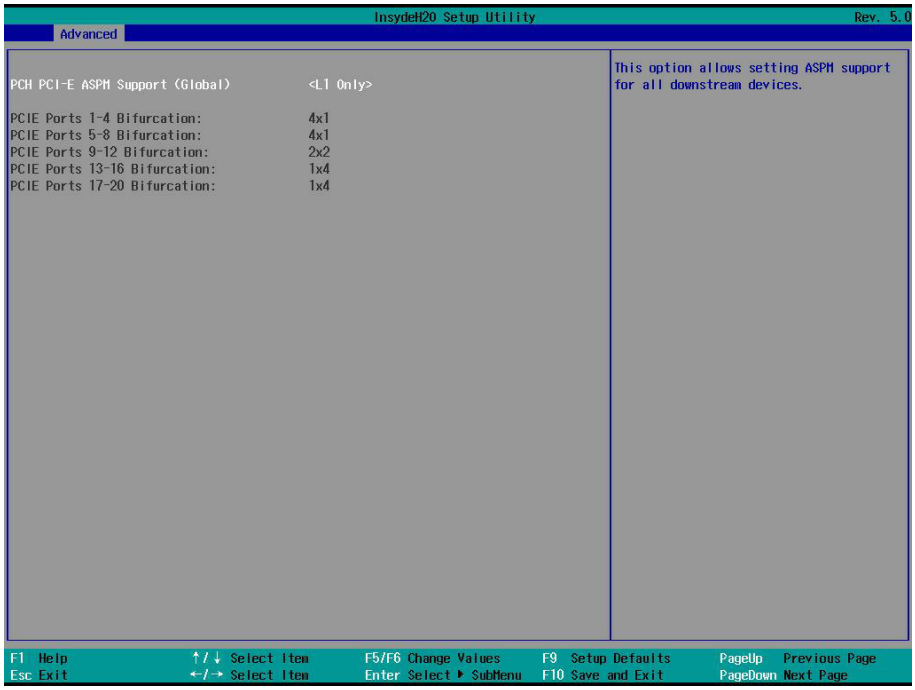


PCH Devices Interface Instruction Table

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

7.2.3.5.2 PCI Express Configuration

PCH Express Configuration interface is used to set the options related with PCH PCIe, as shown in the following figure and table.

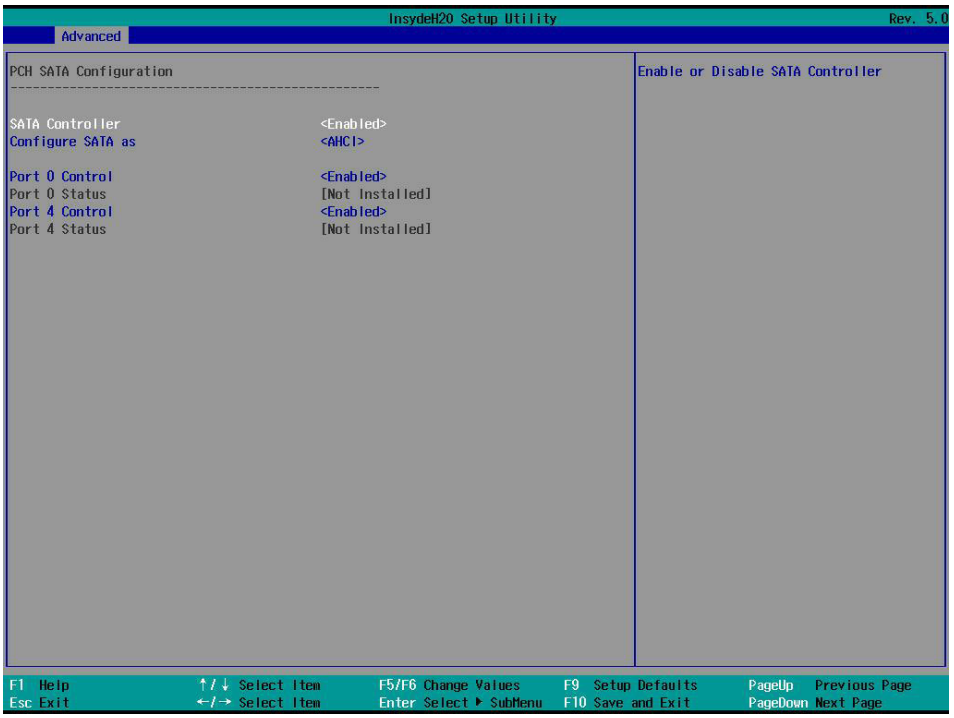


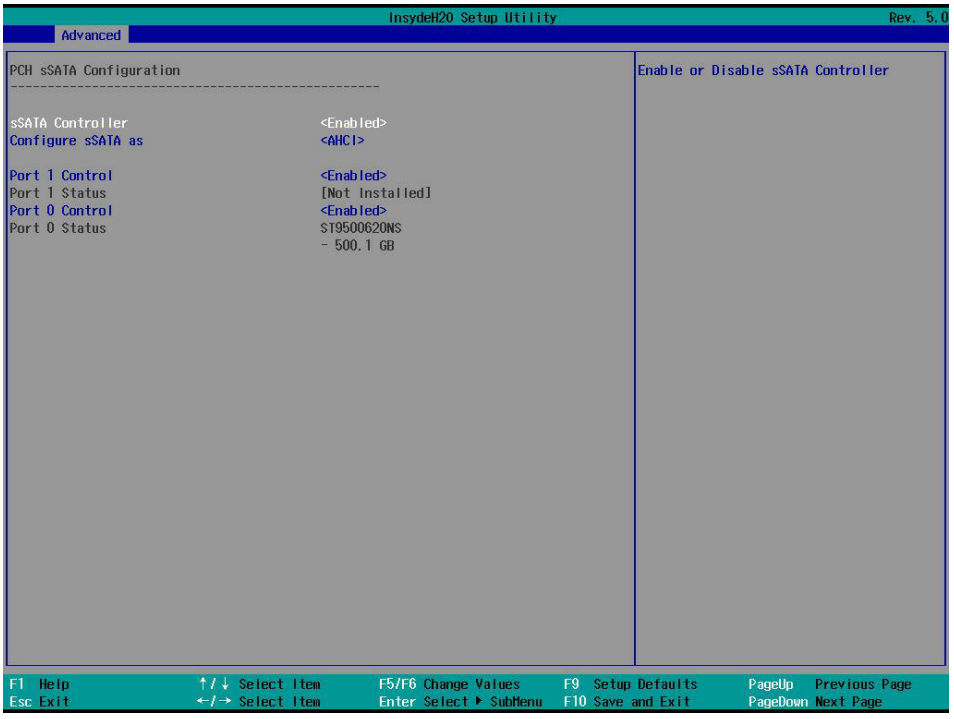
PCI Express Configuration Menu Interface Instruction Table

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

7.2.3.5.3 PCH SATA Configuration/PCH sSATA Configuration

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





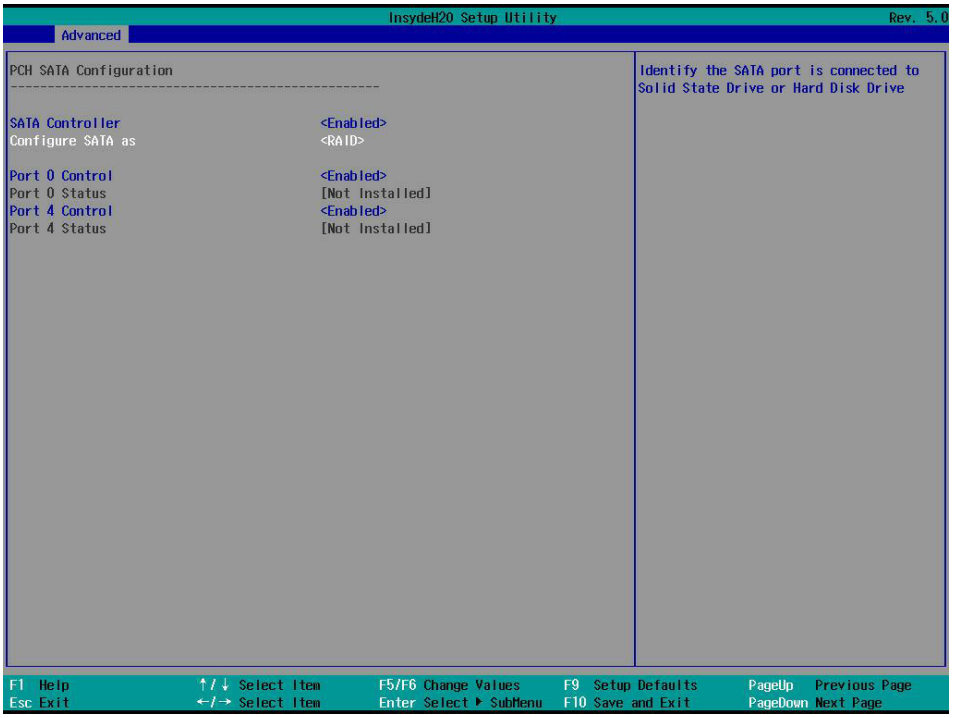
PCH SATA Configuration Menu Interface Instruction Table

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

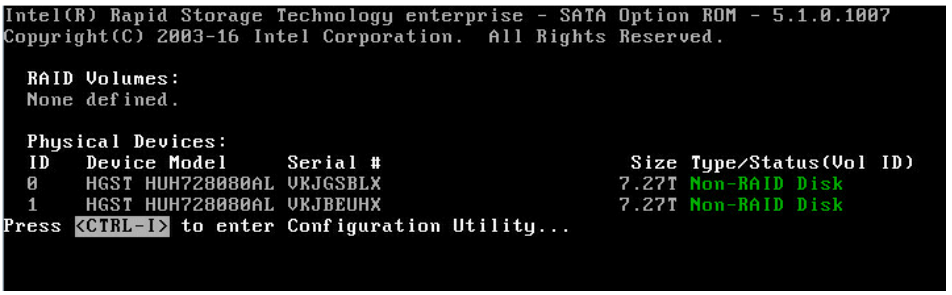
PCH SATA/sSATA RAID mode setting

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

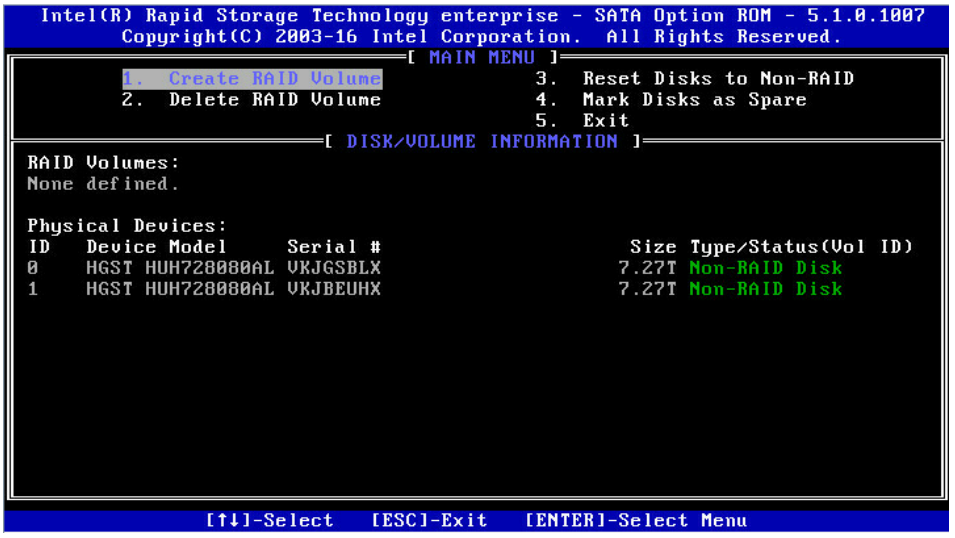
1. Set the Configure SATA/sSATA as option to [RAID], press F10 to save the setting, and the system reboots.



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



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



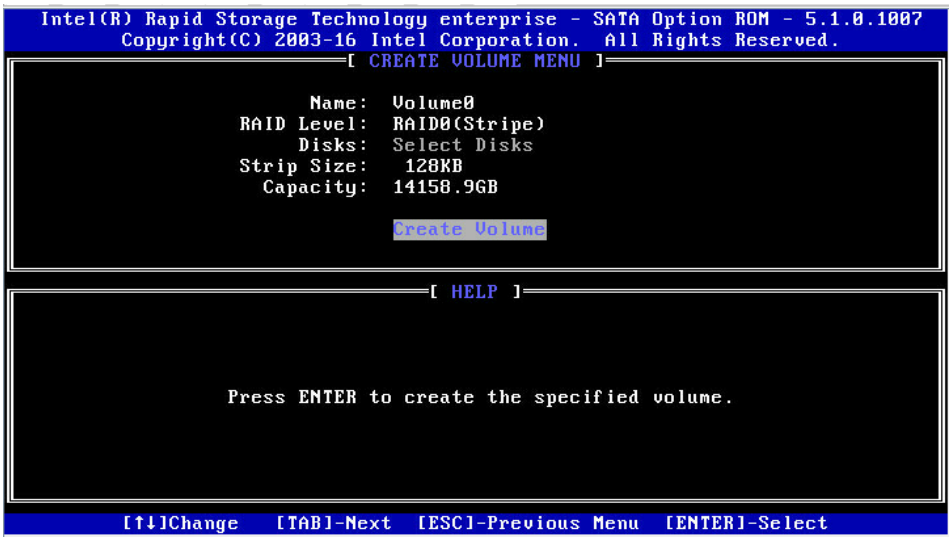
Key Instruction Table

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

Menu Instruction Table

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

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



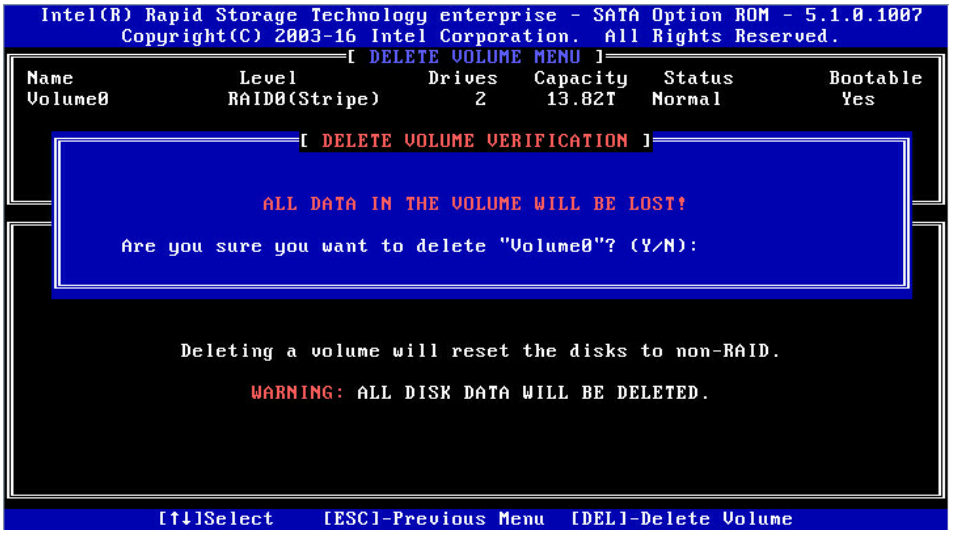
Create RAID Menu Instruction Table

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

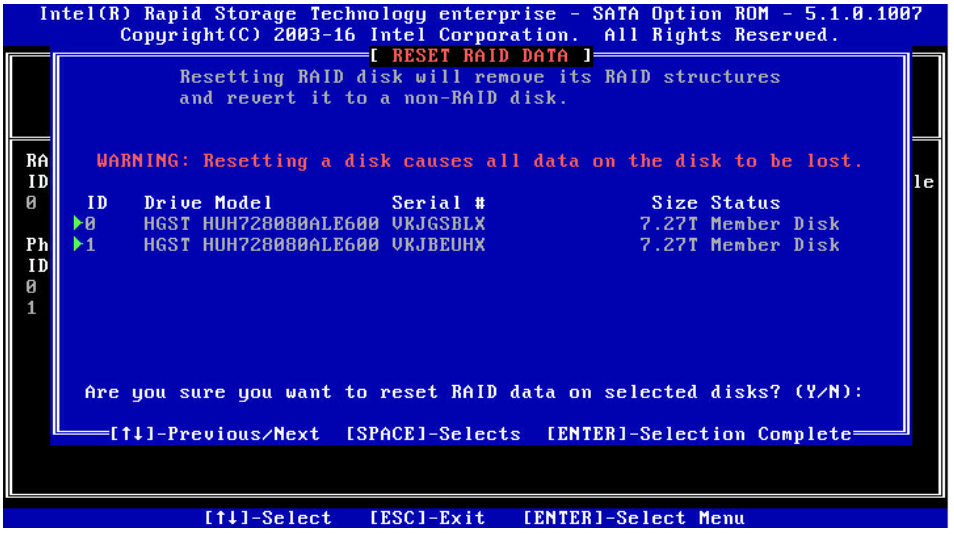
After completing the above settings, please select [Create Volume], and press Enter. The system will prompt “WARNING: ALL DATA ON THE SELECTED DISKS WILL BE LOST. Are you sure you want to create this volume? (Y/N)”. To create an RAID volume, please enter “Y”. A volume will be created, and all data on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

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

volume, please enter “Y”, to cancel the deletion, please enter “N”.

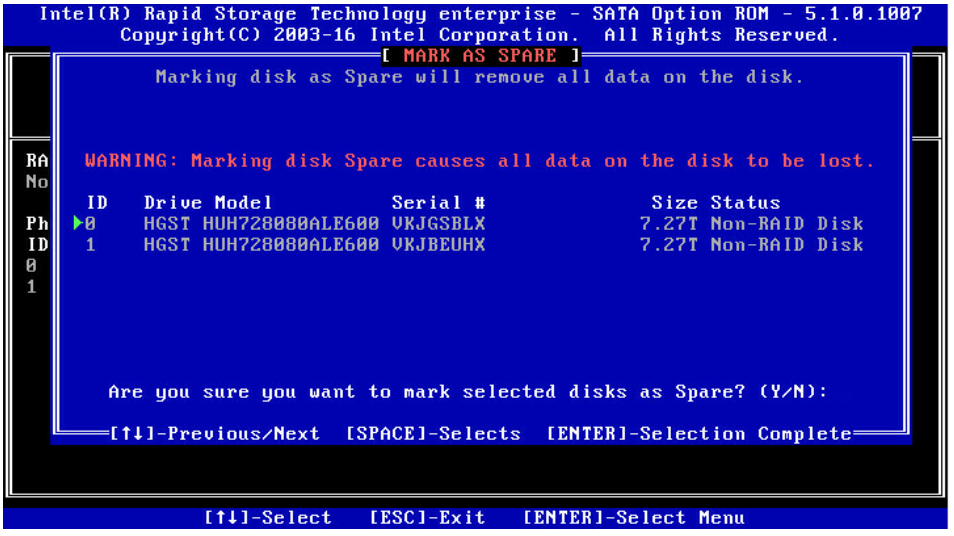


2.4 Reset Disks to Non-RAID menu. After entering Reset Disks to Non-RAID menu, system will display all HDDs in RAID volume. Please use the space key to select the HDD to reset according to the actual demand, and then press Enter to reset the HDD. The system will prompt “Are you sure you want to reset RAID data on selected disks? (Y/N)” again, enter “Y” or “N” according to the prompt. It is to be noted that all data on this disk will be lost after reset. Meanwhile, this disk will not belong to RAID volume any more.

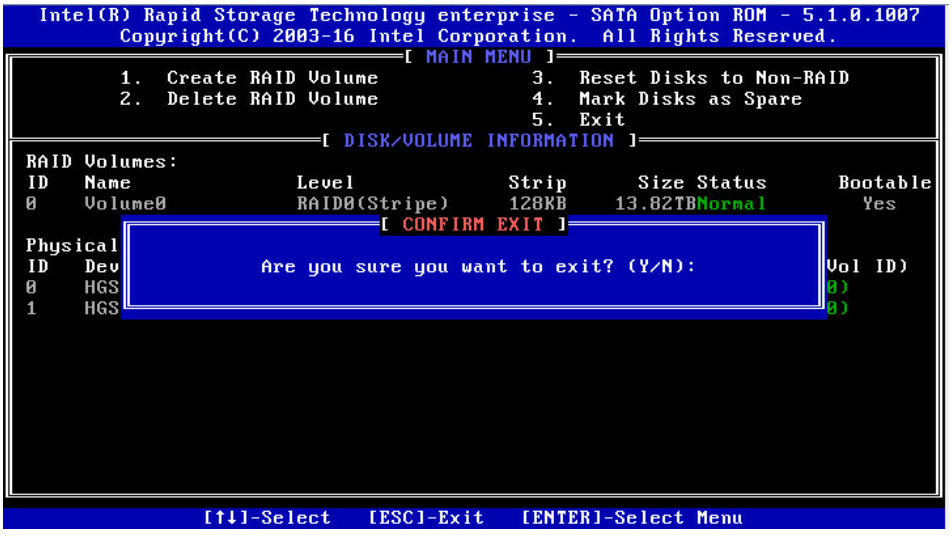


2.5 Mark Disk as Spare menu. After entering Mark Disk as Spare menu, system will display the HDDs not in RAID volume. Please use the space key to select the HDDs according to the actual demand, and then press Enter. The system will prompt “Are you sure you want to mark selected disks as Spare? (Y/N)”,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

noted that all data on this disk will be lost as the spare disk.

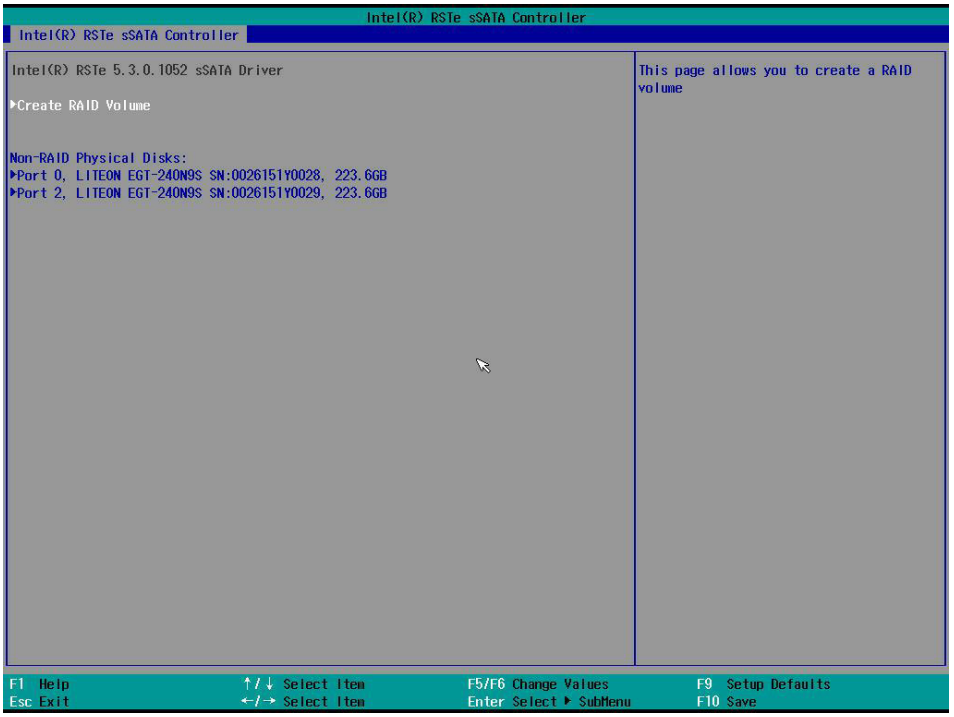


2.6 Exit menu. Use the up and down keys to move to the Exit menu or press the ESC key to exit the SATA RAID configuration interface, as shown below. The system prompts: “Are you sure you want to exit? (Y/N):”, enter “Y” to exit, enter “N” to cancel the exit operation.

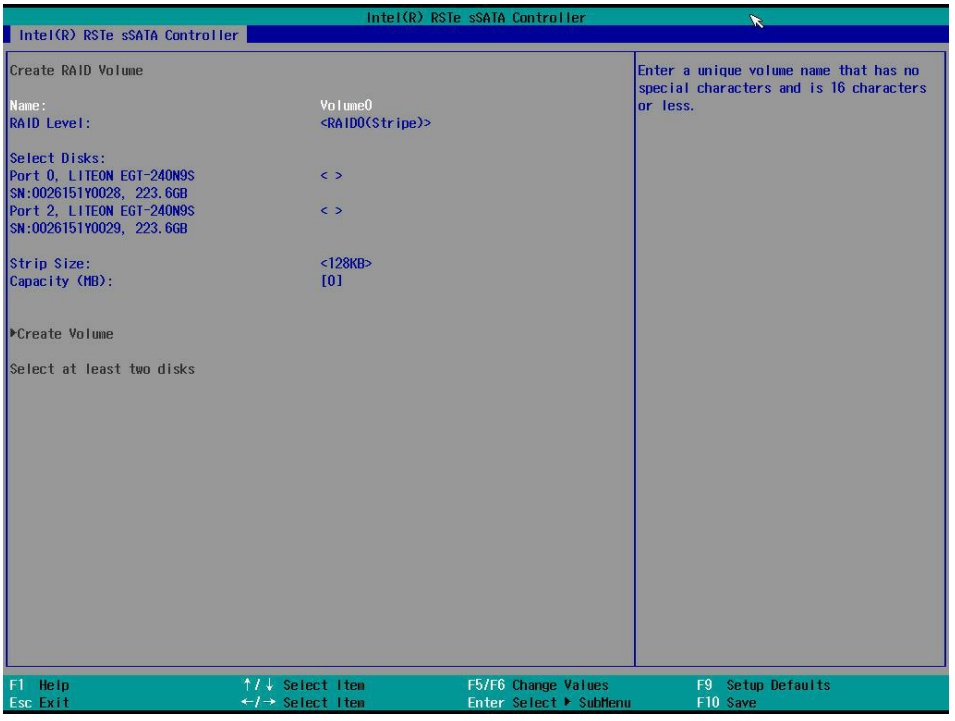


3. Take sSATA RAID configuration in Legacy Mode as an example to introduce the sSATA RAID configuration. When the logo appears during system startup, press ESC to enter the Front Page interface, enter the Device Management configuration interface, and select Intel RSTe sSATA Controller to configure RAID.

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



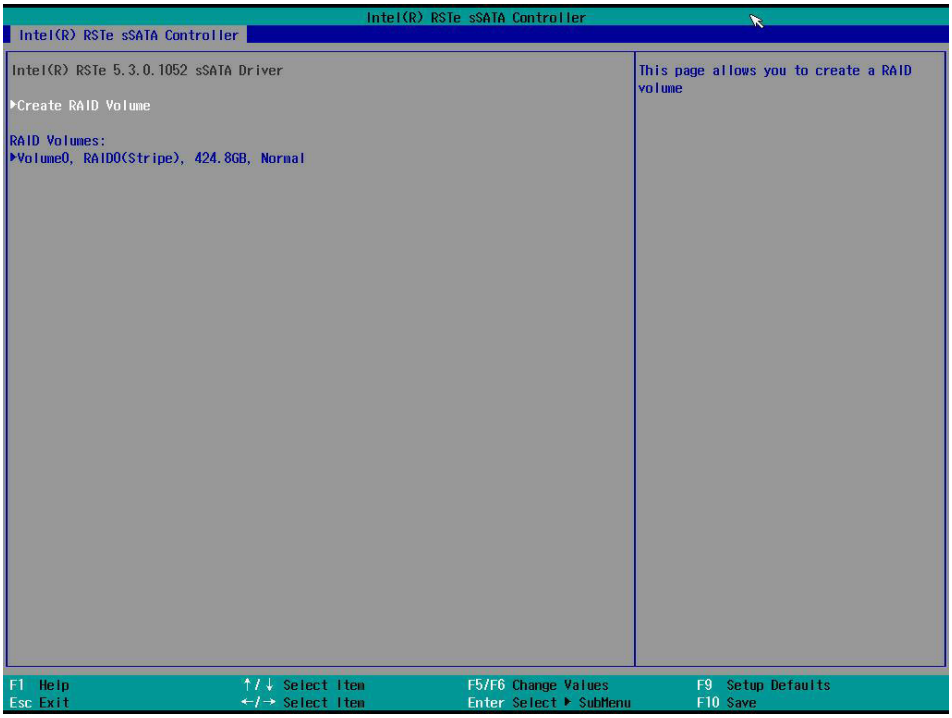
3.2 Create RAID Volume. Enter this menu interface, as shown below.



Create RAID Menu Instruction Table

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

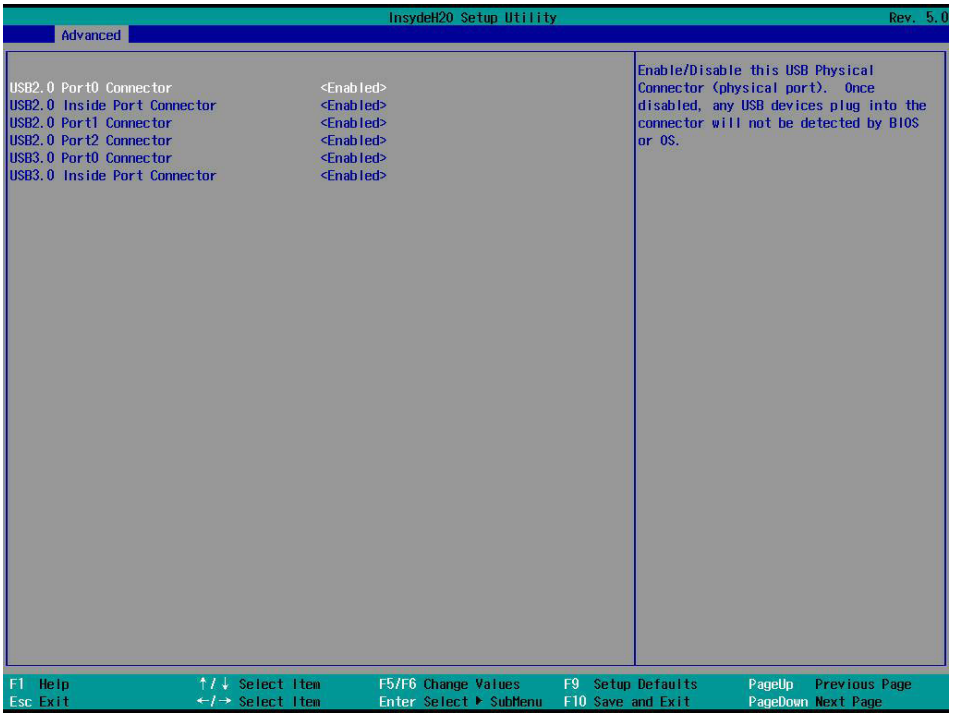
After completing the above settings, please select [Create Volume], and press Enter. After the creation is completed, it will return to RAID configuration interface, the created RAID volume will be displayed.



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

7.2.3.5.4 USB Configuration

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

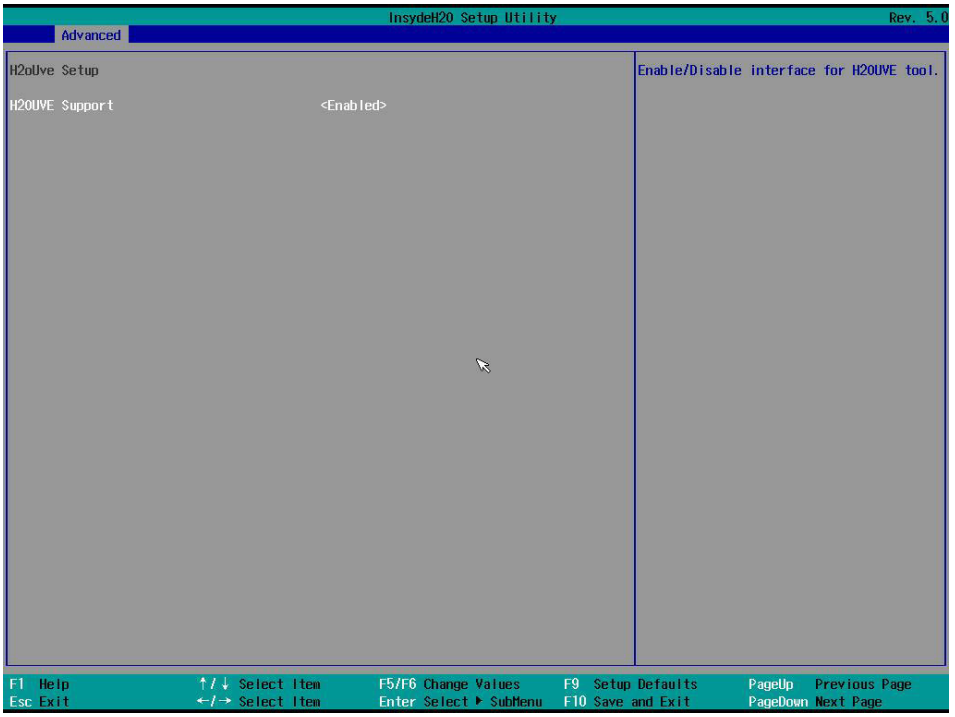


USB Configuration Interface Instruction Table

Interface Parameters	Function Description	Default value
USB2.0 Port0 Connector	High-density blue port USB2.0 setting	Enabled
USB2.0 Insyde Port Connector	Chassis internal USB2.0 setting	Enabled
USB2.0 Port1 Connector	High-density white port USB2.0 setting	Enabled
USB2.0 Port2 Connector	High-density white port USB2.0 setting	Enabled
USB3.0 Port0 Connector	High-density blue port USB3.0 setting	Enabled
USB3.0 Insyde Port Connector	Chassis internal USB3.0 setting	Enabled

7.2.3.5.5 H2oUve Configuration

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

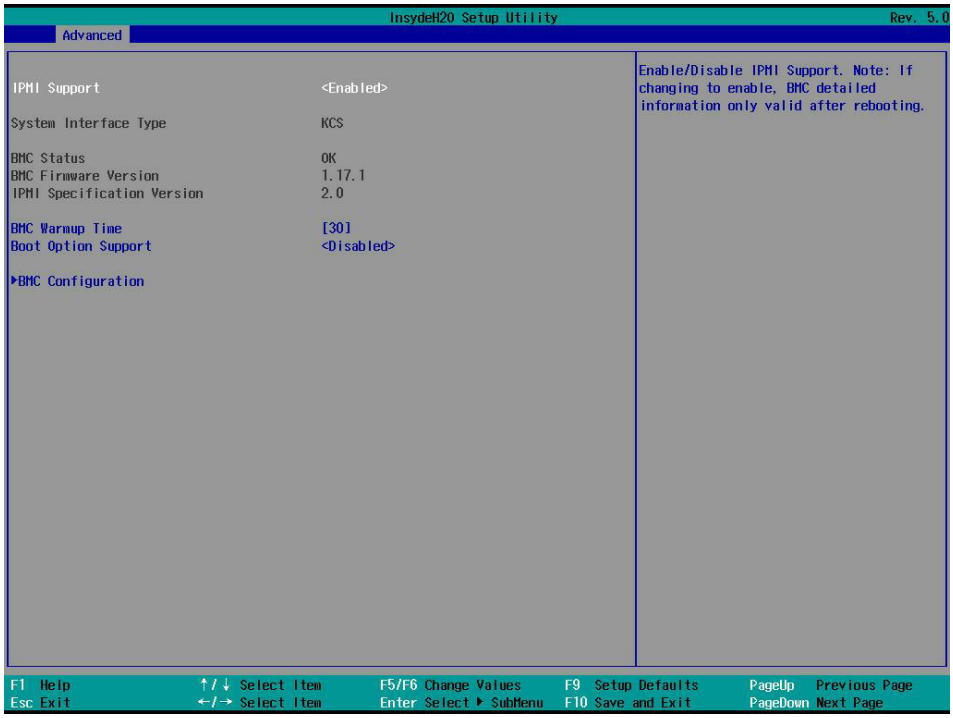


H2oUve Configuration Interface Instruction Table

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

7.2.3.5.6 IPMI Configuration

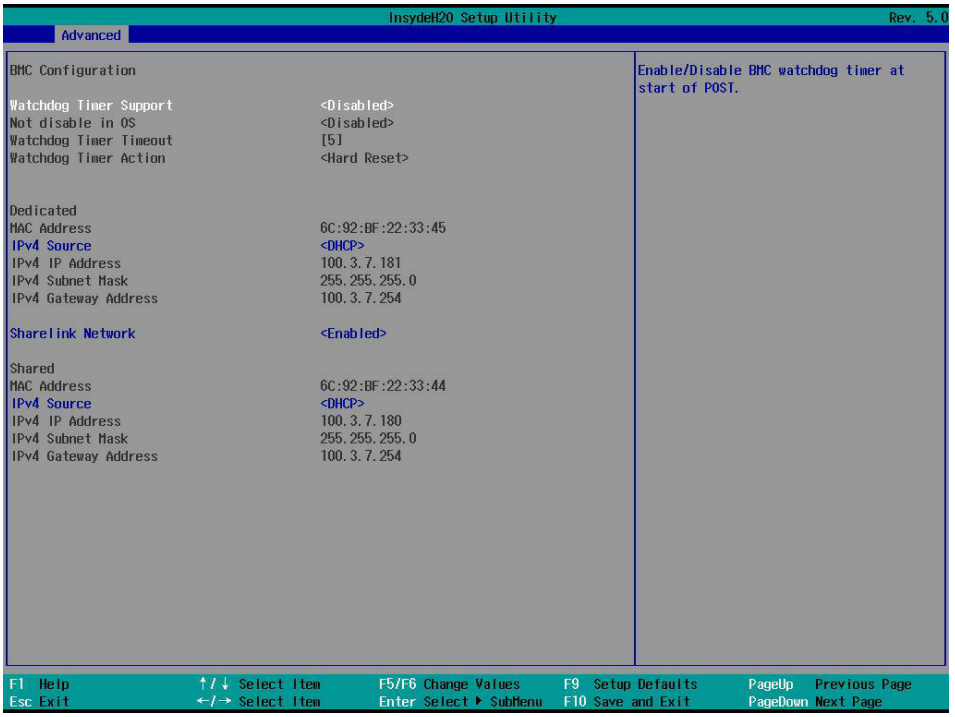
IPMI Configuration interface is used to set IPMI related options, as shown in the following figure and table.



IPMI Configuration Interface Instruction Table

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

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



BMC Configuration Menu Interface Instruction Table

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

(a) BMC dynamic IP setting method:

(1) Select Dedicated or Share BMC port.

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

(3) Select Exit -> Save Change Without Exit option to save, it takes effect immediately.

(b) BMC static IP setting method:

(1) Select Dedicated or Share BMC port.

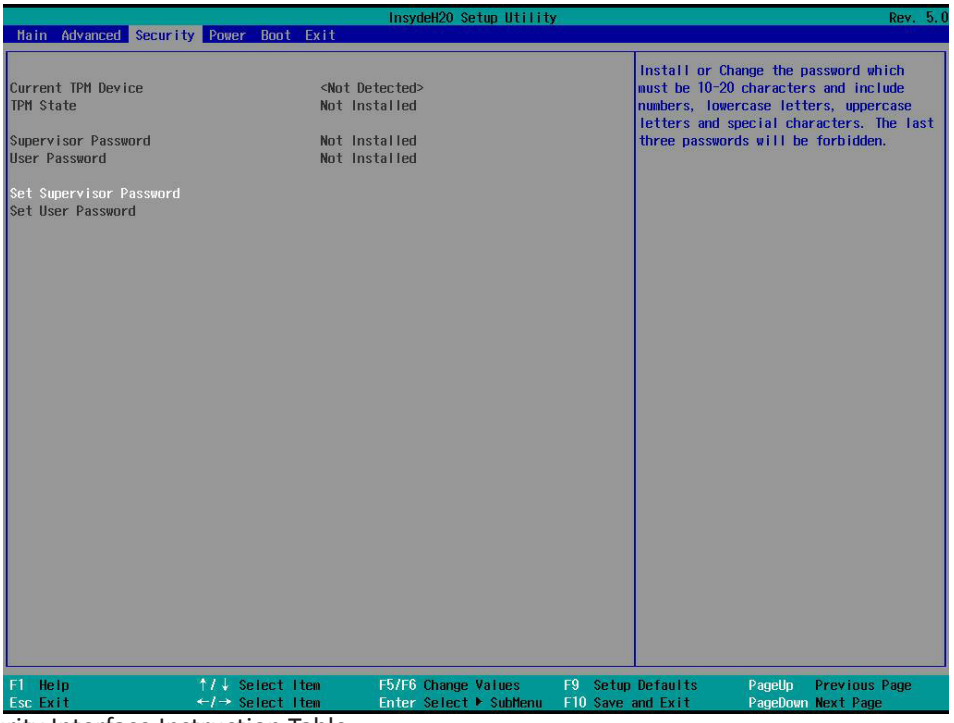
(2) Modify the IP address acquisition mode of this port to Static through IPV4 source.

(3) Select IPV4 IP Address, press Enter, input IP, and press Enter to confirm; then set IPV4 Subnet Mask and IPV4 Gateway Address in the same way.

(4) Select Exit -> Save Change Without Exit option to save, it takes effect immediately.

7.2.4 Security

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

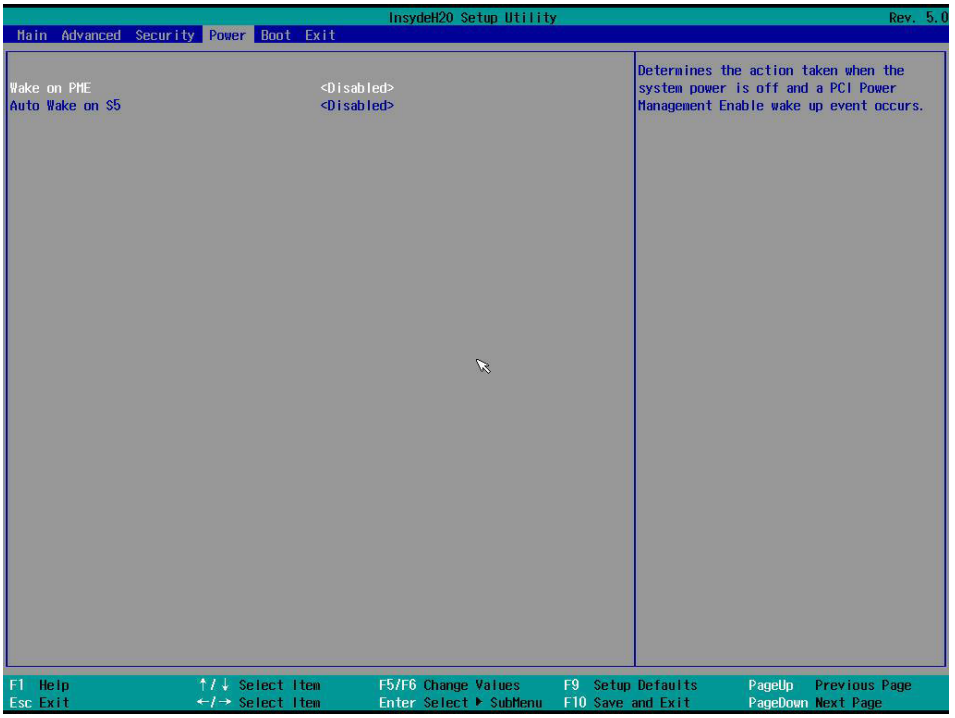


Security Interface Instruction Table

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

7.2.5 Power

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

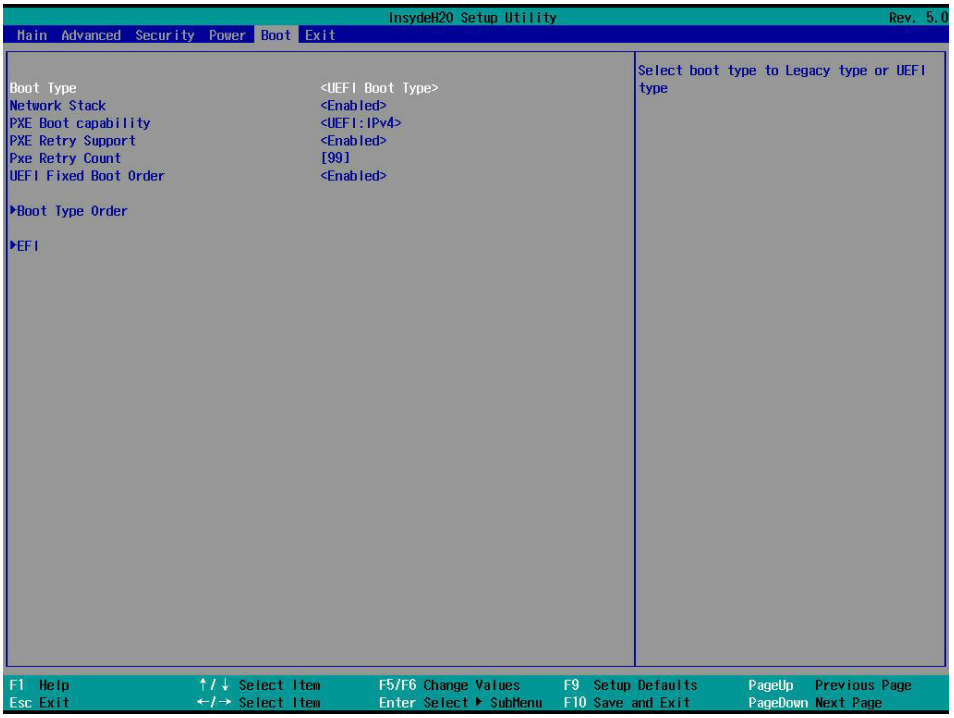


Power Interface Instruction Table

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

7.2.6 Boot

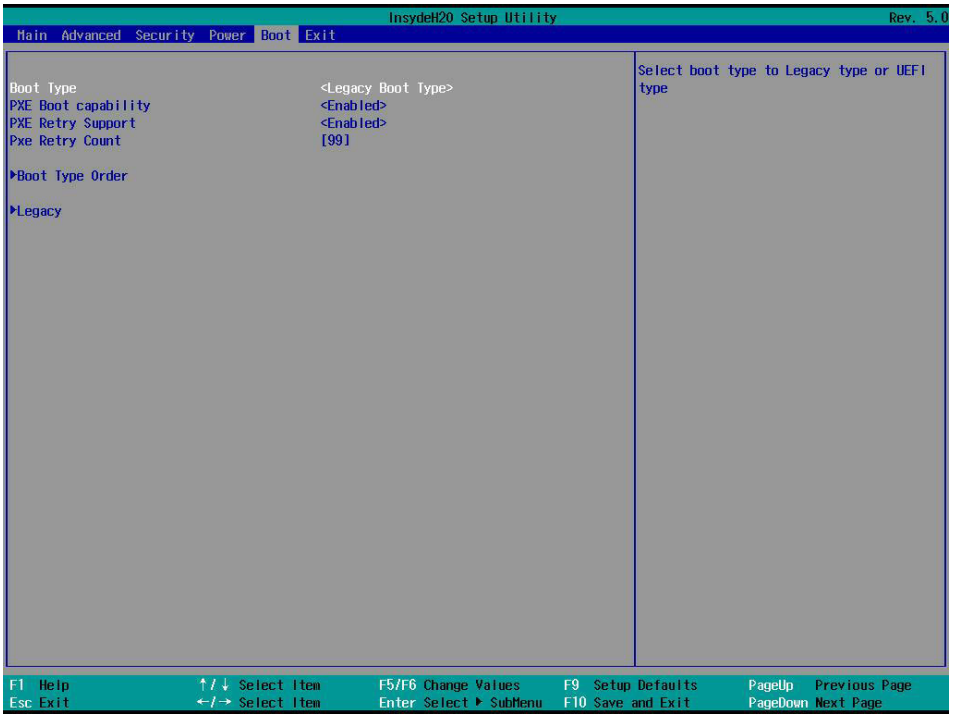
Boot interface is used to set system boot options, including boot type, boot priority, etc. The BIOS boot type defaults to UEFI mode, as shown in the following figure and table.



Boot Interface Instruction Table

Interface Parameters	Function Description	Default Value
Boot Type	Select boot type	UEFI Boot Type
Network Stack	Network stack support setting	Enabled
PXE Boot capability	PXE boot setting	UEFI:IPv4
PXE Retry Support	PXE retry support setting	Enabled
PXE Retry Count	PXE retry count setting	99
UEFI Fixed Boot Order	UEFI fixed boot order setting	Enabled
Boot Type Order	Boot type order setting	--
EFI	EFI boot option setting submenu, the boot priority can be adjusted and set	--

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

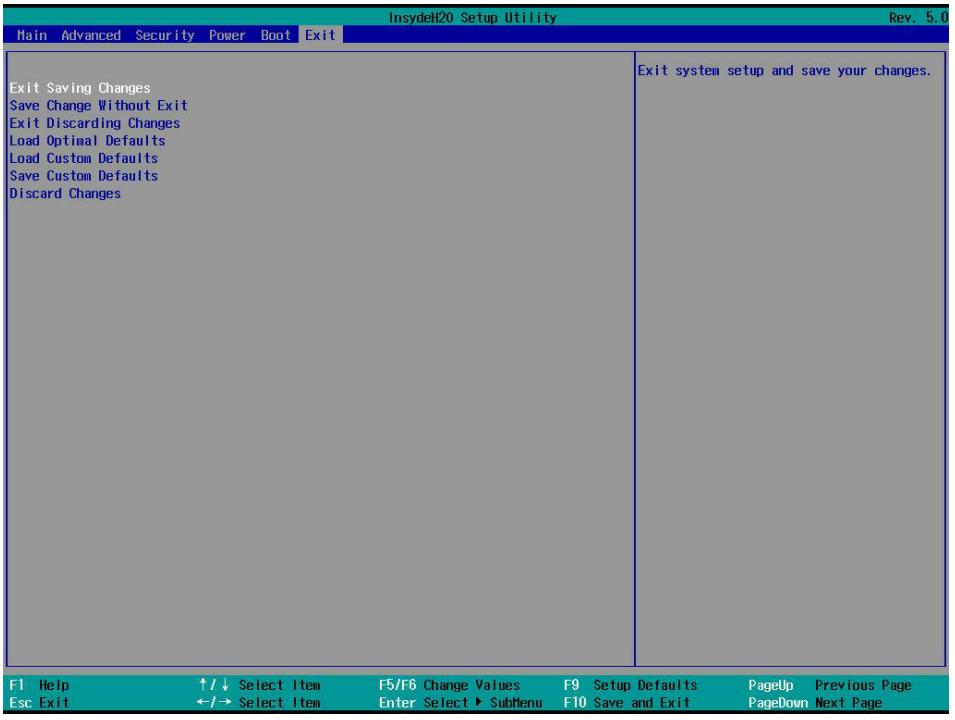


Legacy Boot Configuration Interface Instruction Table

Interface Parameters	Function Description	Default Value
Boot Type	Select boot type	Legacy Boot Type
PXE Boot capability	PXE boot setting	Enabled
PXE Retry Support	PXE retry support setting	Enabled
PXE Retry Count	PXE retry count setting	99
Boot Type Order	Boot type order setting	--
Legacy	Legacy boot option setting submenu, the boot priority can be adjusted and set	---

7.2.7 Exit

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



Exit Menu Interface Instruction Table

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

7.3 Firmware Update

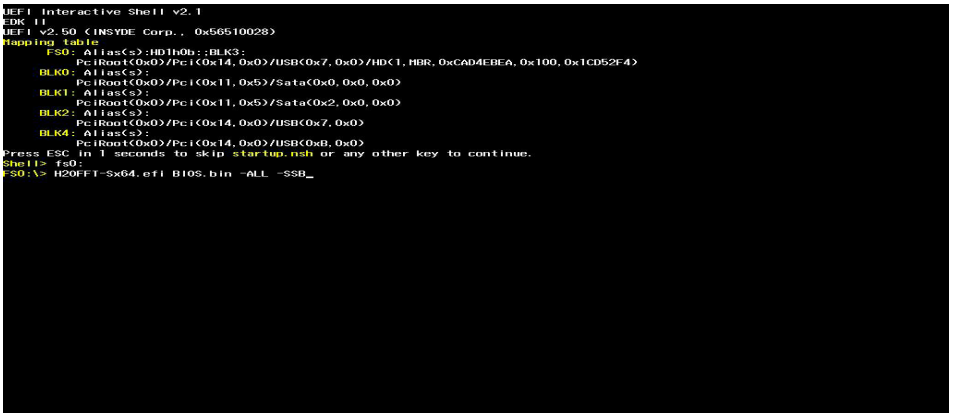
For BIOS update, you could select to update in UEFI Shell or OS.

7.3.1 Update BIOS in UEFI Shell

1) When Inspur Logo appears during system startup, there is a prompt “Press <ESC> to Front Page or <DEL> to Setup or <F11> to Boot Menu or <F12> to PXE Boot.” on the bottom of the screen. Press F11 to start the Boot Menu, and enter EFI shell.

2) Enter the disk in which the BIOS flash toolkit H2OFFT-Sx64.efi resides, enter the flash toolkit folder, and BIOS.bin is the 32M BIOS+ME file to be updated. Execute the command **H20FFT-Sx64.efi XXXX.bin -ALL –SSB** to flash BIOS+ME, and execute **H20FFT-Sx64.efi XXXX.**

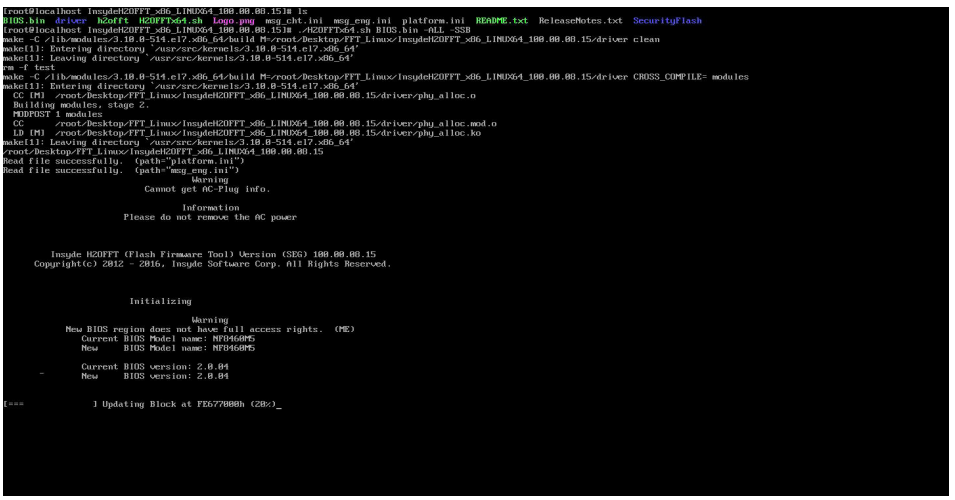
bin -ALL -BIOS –SSB to flash BIOS only, as shown in the following figure.



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

7.3.2 Update BIOS in Linux

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



Notes:

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

8 BMC Settings

8.1 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 management 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. The IPMITool is downloadable: **http://ipmitool.sourceforge.net/manpage.html**

- 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

Store accounts in the Active Directory server, direct the authentication process to server, and achieve management system login with domain accounts.

8.2 Functional Modules

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

8.2.1 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.

8.2.2 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.

8.2.3 Command Line Function Introduction

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

8.2.4 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.

Note:

If the Java runtime environment does not meet the requirements, you can download it at http://www.oracle.com/technetwork/java/javase/downloads/index.html.

8.3 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.

8.3.1 Login Web Interface

This guide introduces the operation steps to login to the Web management interface, taking the Windows Operating System and the 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.

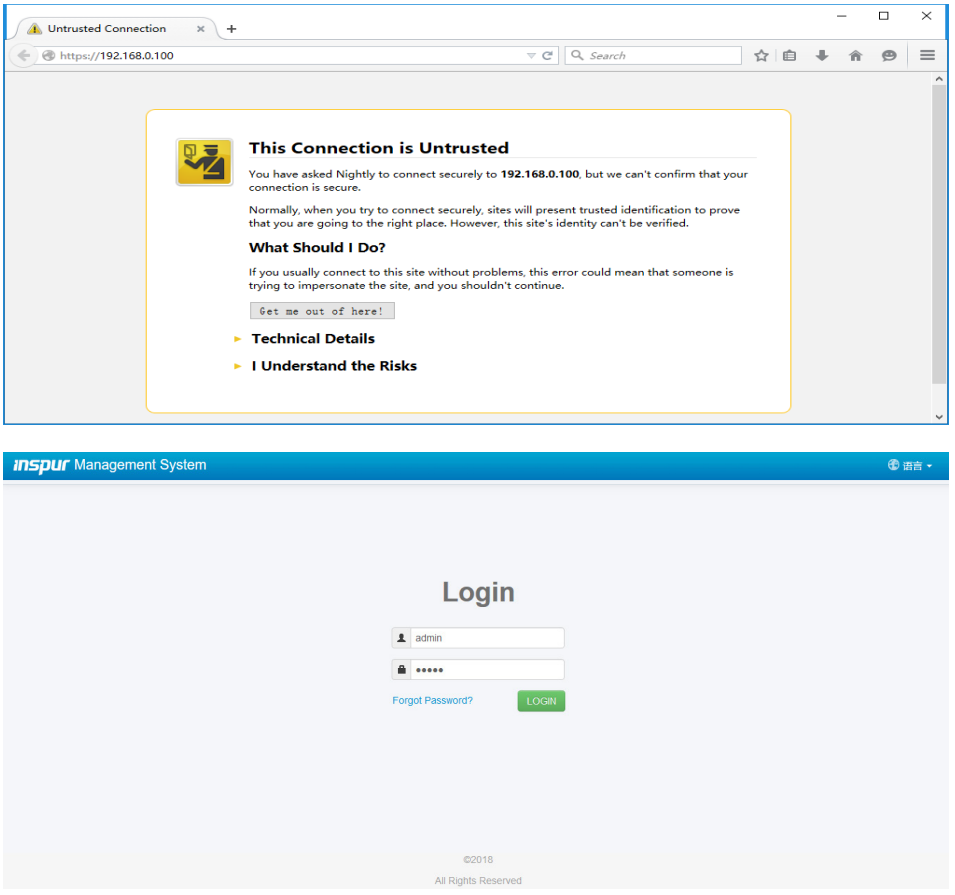
Step 2: Open the browser, and enter “http://ipaddress” in the address bar (ipaddress is the IP address of the management network port, which can be obtained from the CMC management interface of I9000 server. The default login mode is https, and safe operation configuration is needed).

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.

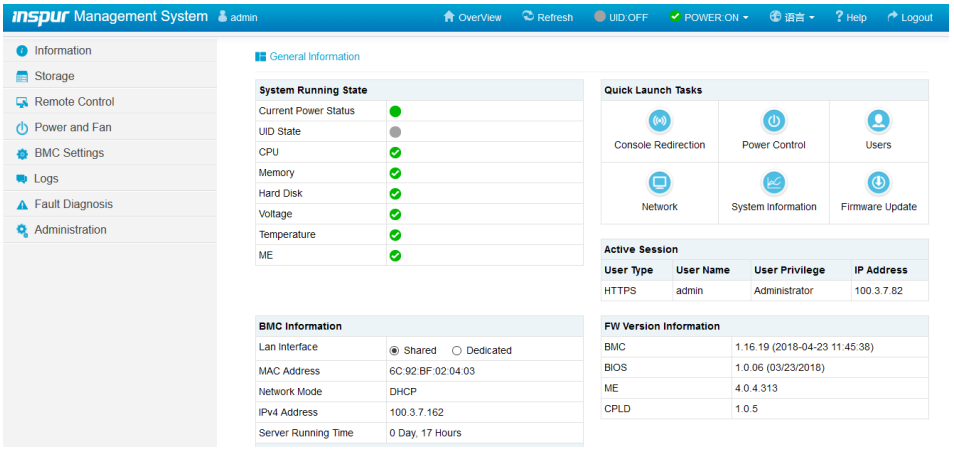


8.3.2 Web Interface Introduction

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.



- 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.

✧ 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.

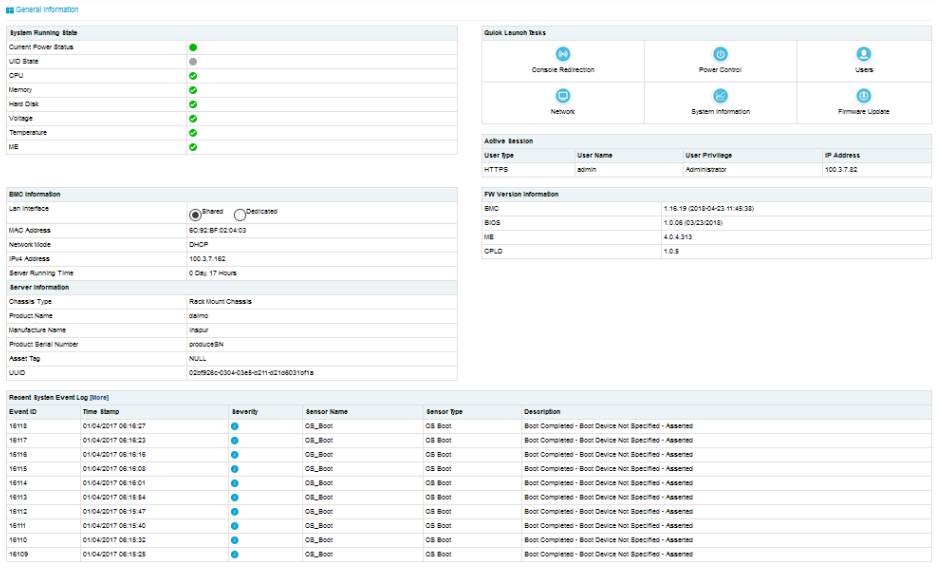
- The navigation tree is on the left. Via the nodes on the tree, you can select different functional interfaces. The following functions are included:
- Information
- Storage
- Remote control
- Power and fan
- BMC settings
- Logs
- Fault diagnosis
- Administration

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

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

8.3.3 Overview

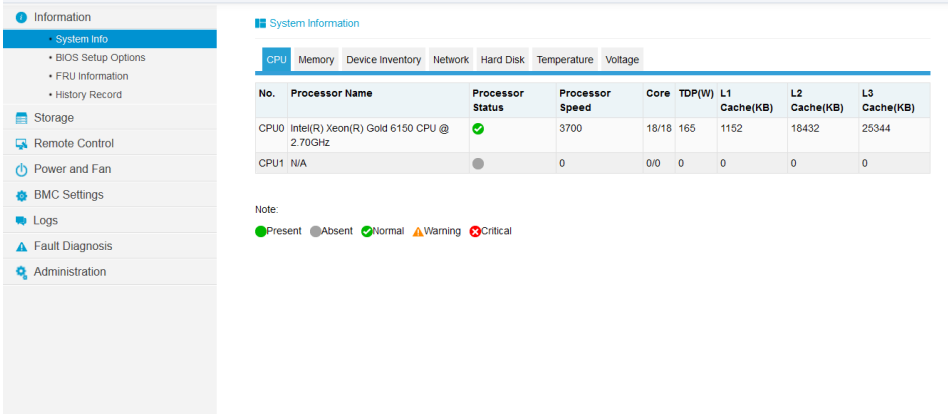
Click on Overview to open the “General Information” interface, as shown below.

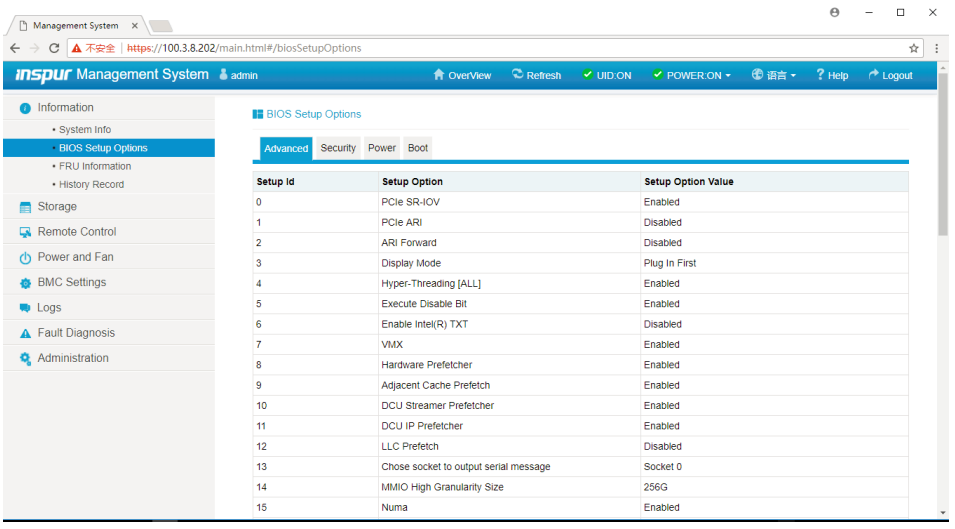


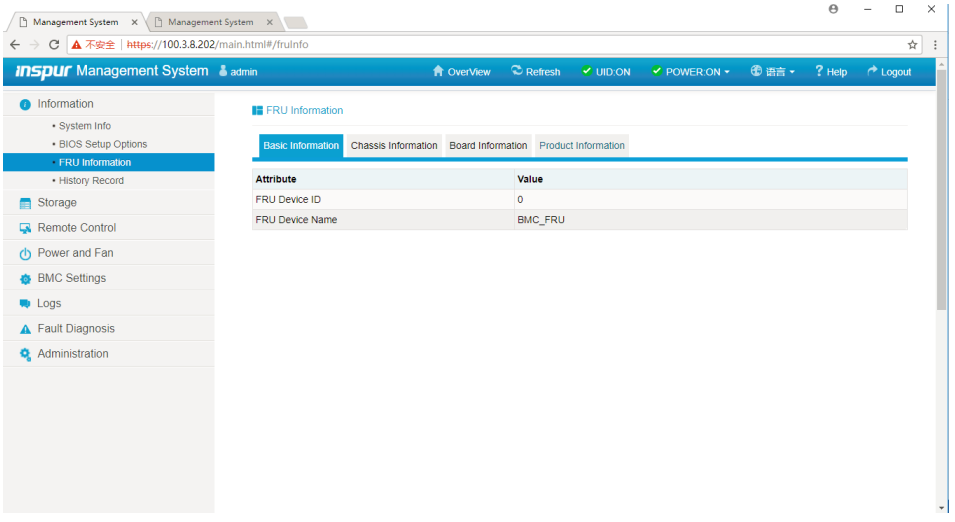
8.3.4 Information

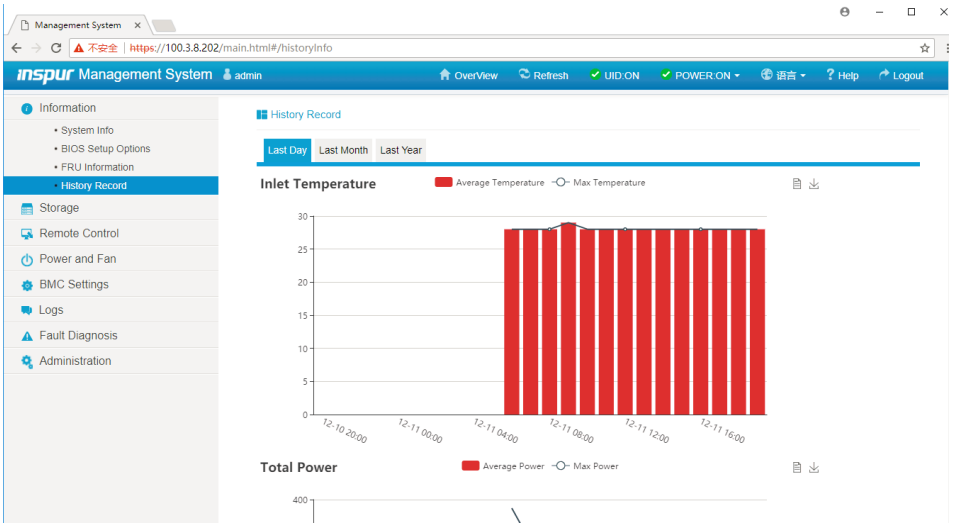
Select “Information” on the navigation tree. It contains the interfaces of system information, BIOS setup options, FRU information and history record, as shown in the following figures below.

- System information: Displays system configuration information, including CPU, memory, PCIE device, NIC, HDD, power supply unit, fan, temperature and voltage information.
- BIOS setup options: Displays the key BIOS setup options information.
- FRU information: Displays the FRU information.
- History record: Displays the history information of inlet air temperature and total power.



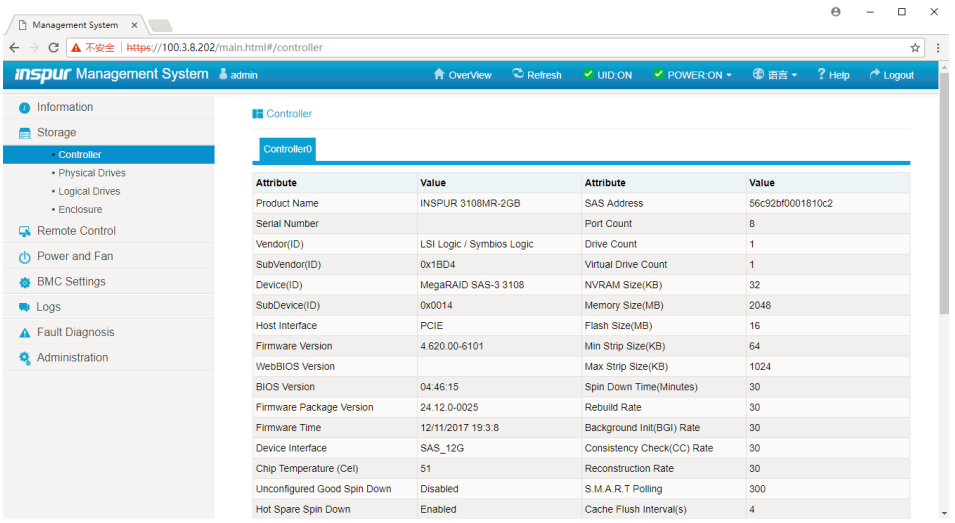

Management System
不安全 | https://100.3.8.202/main.html#/biosSetupOptions
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
语言
Help
Logout
Information
System Info
BIOS Setup Options
FRU Information
History Record
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
BIOS Setup Options
Advanced
Security
Power
Boot
Setup Id
Setup Option
Setup Option Value
0 PCIe SR-IOV Enabled
1 PCIe ARI Disabled
2 ARI Forward Disabled
3 Display Mode Plug In First
4 Hyper-Threading [ALL] Enabled
5 Execute Disable Bit Enabled
6 Enable Intel(R) TXT Disabled
7 VMX Enabled
8 Hardware Prefetcher Enabled
9 Adjacent Cache Prefetch Enabled
10 DCU Streamer Prefetcher Enabled
11 DCU IP Prefetcher Enabled
12 LLC Prefetch Disabled
13 Chose socket to output serial message Socket 0
14 MMIO High Granularity Size 256G
15 Numa Enabled


Management System
Management System
不安全 | https://100.3.8.202/main.html#/fruInfo
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
语言
Help
Logout
Information
System Info
BIOS Setup Options
FRU Information
History Record
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
FRU Information
Basic Information
Chassis Information
Board Information
Product Information
Attribute
Value
FRU Device ID 0
FRU Device Name BMC_FRU


Management System
不安全 | https://100.3.8.202/main.html#/historyInfo
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
语言
Help
Logout
Information
System Info
BIOS Setup Options
FRU Information
History Record
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
History Record
Last Day
Last Month
Last Year
Inlet Temperature
Average Temperature
Max Temperature
30
25
20
15
10
5
0
12-10 20:00
12-11 00:00
12-11 04:00
12-11 08:00
12-11 12:00
12-11 16:00
Total Power
Average Power
Max Power
400

8.4 Storage

Select “Storage” on the navigation tree to open the storage interface. At present, the storage information control only supports LSI RAID card. This interface contains controller, physical drives, and logical drives information, as shown in the following figures.

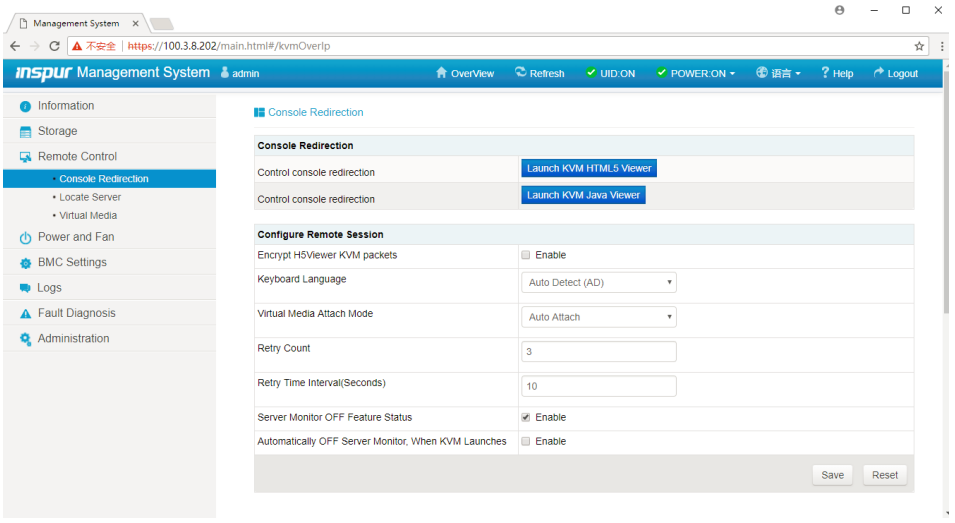


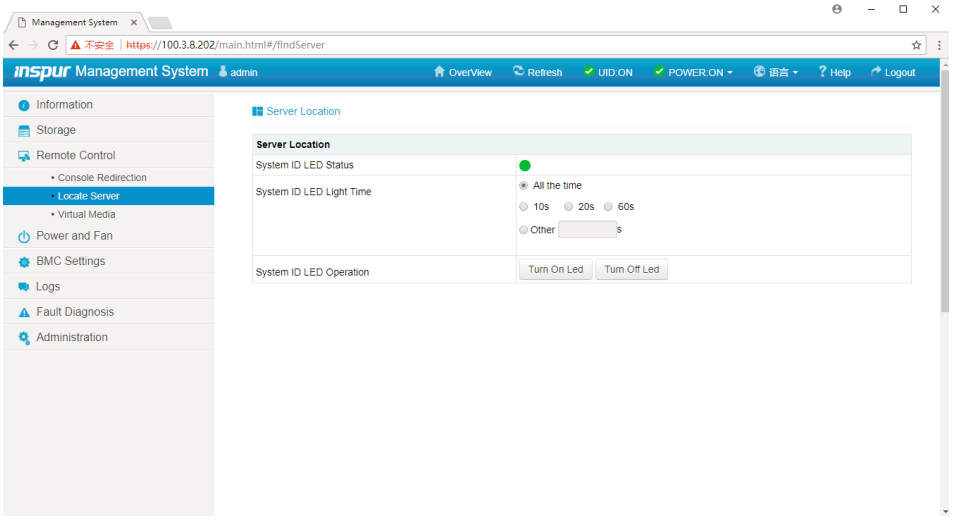
Attribute	Value	Attribute	Value
Product Name	INSPUR 3108MR-2GB	SAS Address	56c92bf0001810c2
Serial Number		Port Count	8
Vendor(ID)	LSI Logic / Symbios Logic	Drive Count	1
SubVendor(ID)	0x1BD4	Virtual Drive Count	1
Device(ID)	MegaRAID SAS-3 3108	NVRAM Size(KB)	32
SubDevice(ID)	0x0014	Memory Size(MB)	2048
Host Interface	PCIE	Flash Size(MB)	16
Firmware Version	4.620.00-6101	Min Strip Size(KB)	64
WebBIOS Version		Max Strip Size(KB)	1024
BIOS Version	04.46.15	Spin Down Time(Minutes)	30
Firmware Package Version	24.12.0-0025	Rebuild Rate	30
Firmware Time	12/11/2017 19:3:8	Background Init(BGI) Rate	30
Device Interface	SAS_12G	Consistency Check(CC) Rate	30
Chip Temperature (Cel)	51	Reconstruction Rate	30
Unconfigured Good Spin Down	Disabled	S.M.A.R.T Polling	300
Hot Spare Spin Down	Enabled	Cache Flush Interval(s)	4

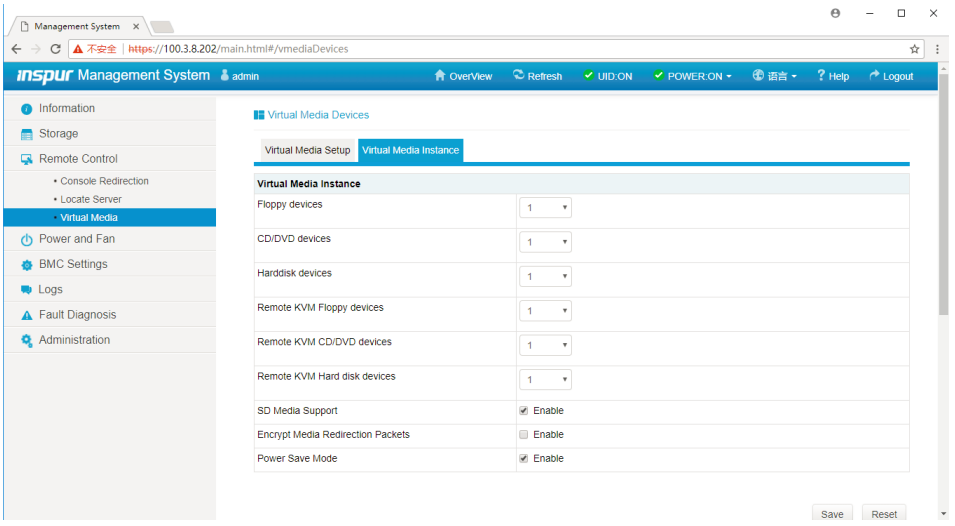
8.5 Remote Control

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

- Console redirection (KVM): The KVM console window will pop up, supporting Java KVM and HTML5 KVM.
- Server location: To turn on/off the system ID LED.
- Virtual media devices: To set the quantity of virtual media (floppy devices, CD/DVD devices and hard disk drives, etc.).


Management System
不安全 | https://100.3.8.202/main.html#/kvmOverIp
inspur Management System admin
OverView Refresh UID:ON POWER:ON 语言 Help Logout
Information
Storage
Remote Control
• Console Redirection
• Locate Server
• Virtual Media
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
Console Redirection
Console Redirection
Control console redirection
Launch KVM HTML5 Viewer
Control console redirection
Launch KVM Java Viewer
Configure Remote Session
Encrypt H5Viewer KVM packets
Enable
Keyboard Language
Auto Detect (AD)
Virtual Media Attach Mode
Auto Attach
Retry Count
3
Retry Time Interval(Seconds)
10
Server Monitor OFF Feature Status
Enable
Automatically OFF Server Monitor, When KVM Launches
Enable
Save
Reset

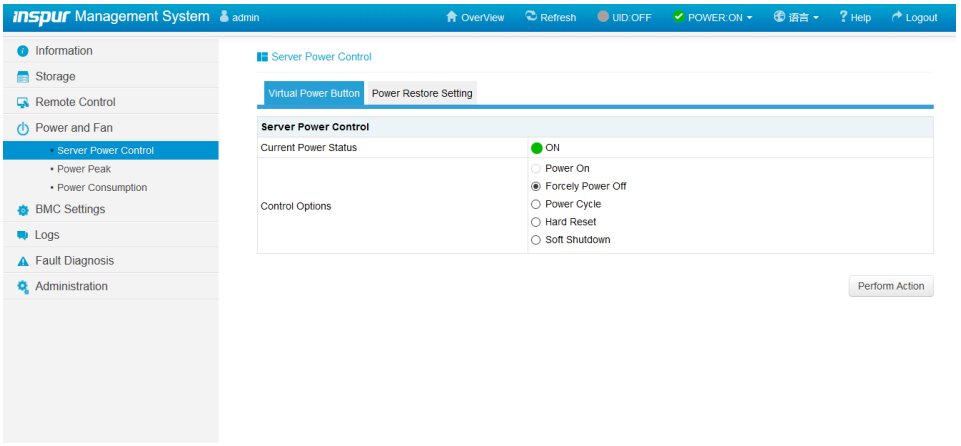

Management System
不安全 | https://100.3.8.202/main.html#/findServer
inspur Management System admin
OverView Refresh UID:ON POWER:ON 语言 Help Logout
Information
Storage
Remote Control
• Console Redirection
• Locate Server
• Virtual Media
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
Server Location
Server Location
System ID LED Status
System ID LED Light Time
All the time
10s 20s 60s
Other
s
System ID LED Operation
Turn On Led
Turn Off Led

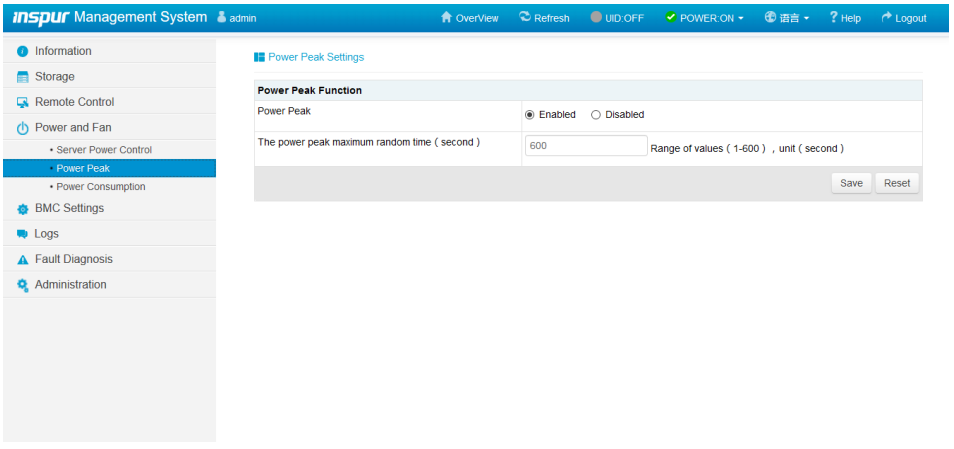

Management System
不安全 | https://100.3.8.202/main.html#/vmediaDevices
inspur Management System admin
OverView Refresh UID:ON POWER:ON 语言 Help Logout
Information
Storage
Remote Control
• Console Redirection
• Locate Server
• Virtual Media
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
Virtual Media Devices
Virtual Media Setup
Virtual Media Instance
Virtual Media Instance
Floppy devices
CD/DVD devices
Harddisk devices
Remote KVM Floppy devices
Remote KVM CD/DVD devices
Remote KVM Hard disk devices
SD Media Support
Enable
Encrypt Media Redirection Packets
Enable
Power Save Mode
Enable
Save
Reset

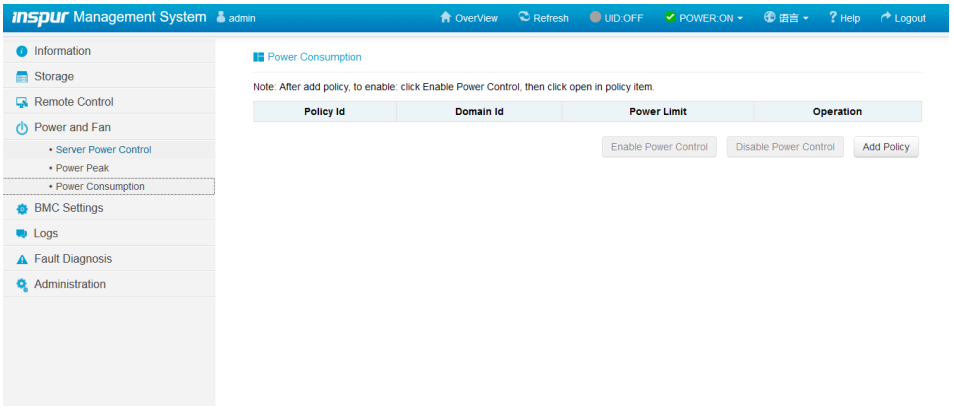
8.6 Power and Fan

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

- 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: Dynamic management of power consumption.



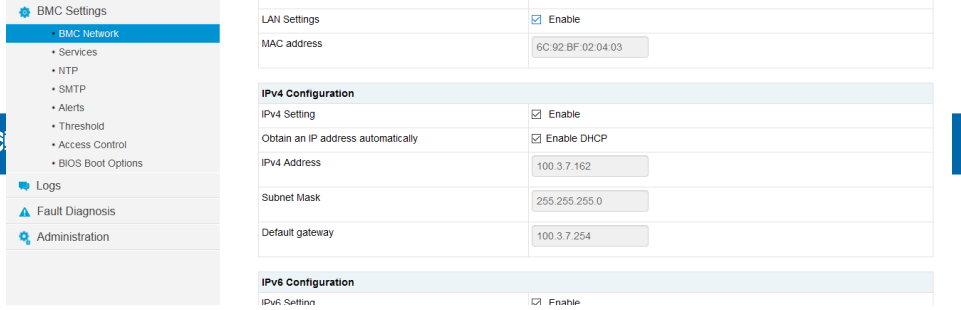


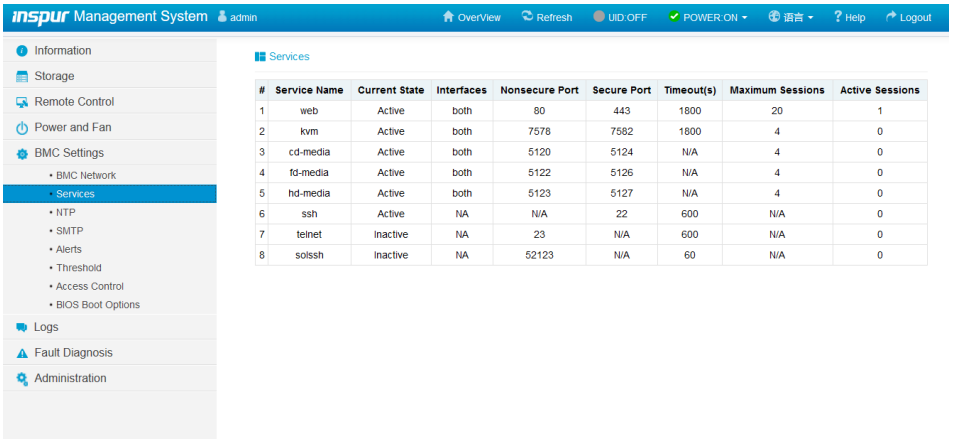


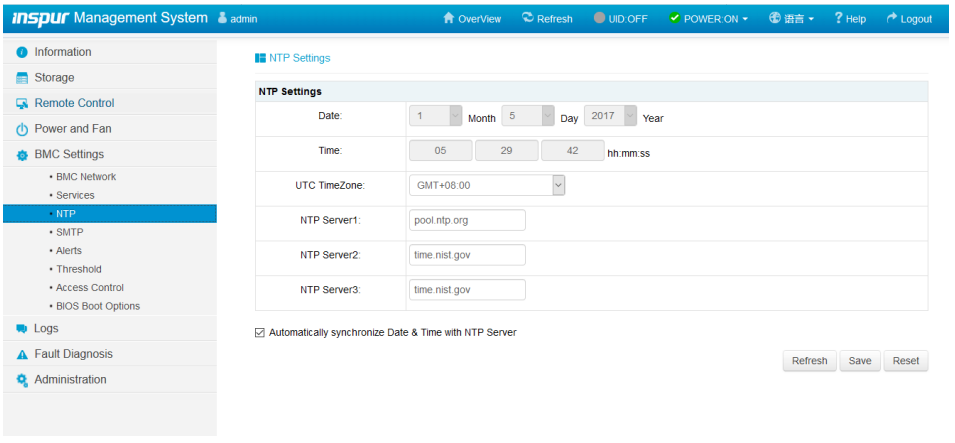
8.7 BMC Settings

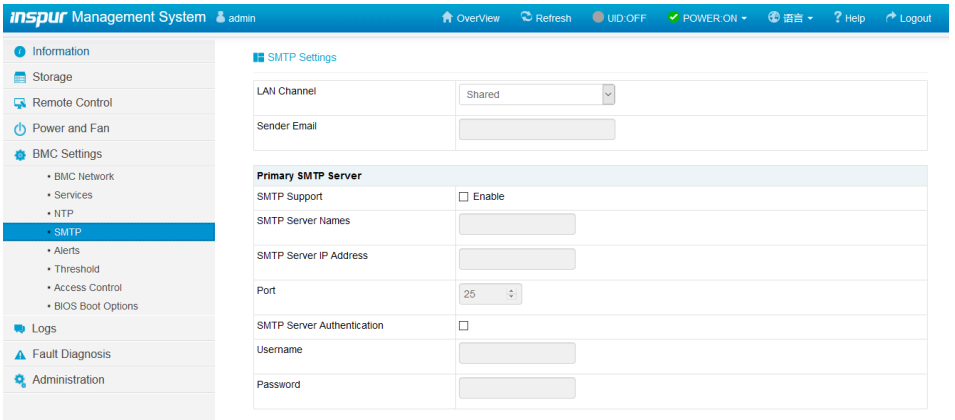
Select “BMC Settings” on the navigation tree to open the BMC Settings interface. It contains the interfaces of BMC network, services, NTP, SMTP, alerts, access control and BIOS boot options, as shown in the following figures.

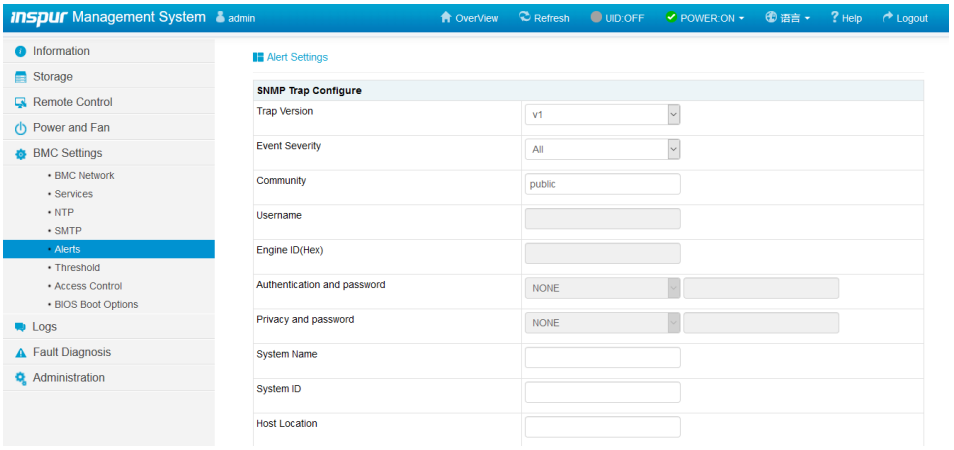
- BMC network management: Contains BMC network (static IP and DHCP), DNS settings and network interface bonding and network link information.
- Services: To configure the BMC’s Web service, KVM service, ssh service, telnet service, etc.
- NTP settings: To set the BMC time, which has two methods:
  - 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.
- Access control: To set IP address fields accessible to BMC.
- BIOS boot options: To set the boot option after BIOS reset.

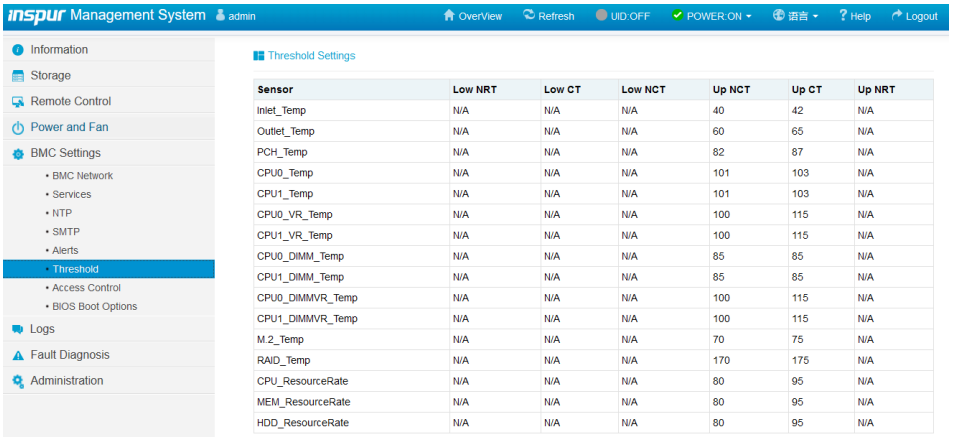

BMC Settings
BMC Network
Services
NTP
SMTP
Alerts
Threshold
Access Control
BIOS Boot Options
Logs
Fault Diagnosis
Administration
LAN Settings
Enable
MAC address
6C:92:BF:02:04:03
IPv4 Configuration
IPv4 Setting
Enable
Obtain an IP address automatically
Enable DHCP
IPv4 Address
100.3.7.162
Subnet Mask
255.255.255.0
Default gateway
100.3.7.254
IPv6 Configuration

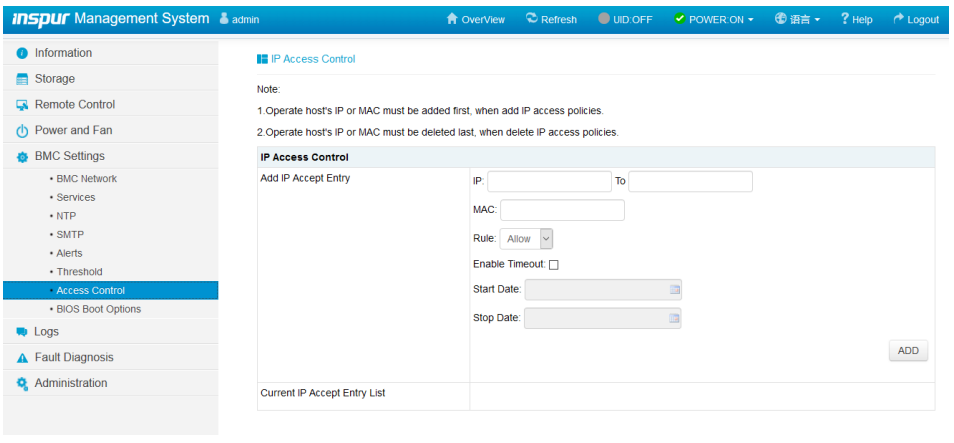

inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
BMC Network
Services
NTP
SMTP
Alerts
Threshold
Access Control
BIOS Boot Options
Logs
Fault Diagnosis
Administration
Services
Service Name Current State Interfaces Nonsecure Port Secure Port Timeout(s) Maximum Sessions Active Sessions
1 web Active both 80 443 1800 20 1
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 NA N/A 22 600 N/A 0
7 telnet Inactive NA 23 N/A 600 N/A 0
8 solssh Inactive NA 52123 N/A 60 N/A 0

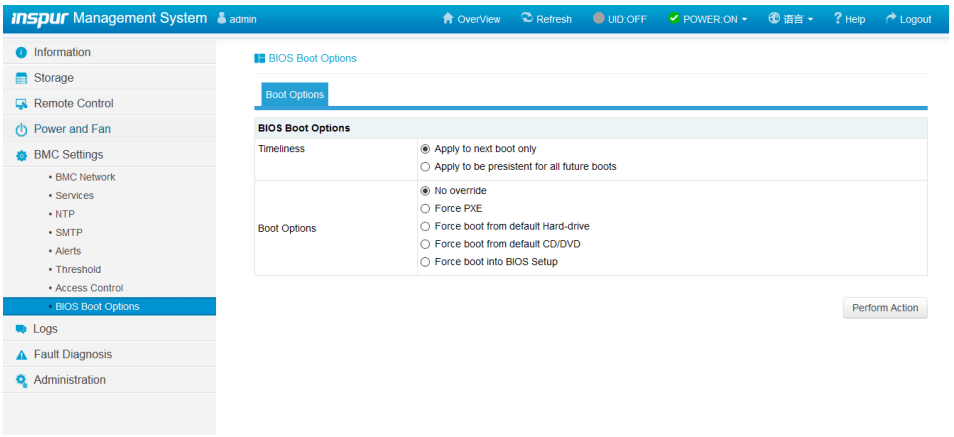

inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
BMC Network
Services
NTP
SMTP
Alerts
Threshold
Access Control
BIOS Boot Options
Logs
Fault Diagnosis
Administration
NTP Settings
NTP Settings
Date:
1
Month
5
Day
2017
Year
Time:
05
29
42
hh:mm:ss
UTC TimeZone:
GMT+08:00
NTP Server1:
pool.ntp.org
NTP Server2:
time.nist.gov
NTP Server3:
time.nist.gov
Automatically synchronize Date & Time with NTP Server
Refresh
Save
Reset


inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
BMC Network
Services
NTP
SMTP
Alerts
Threshold
Access Control
BIOS Boot Options
Logs
Fault Diagnosis
Administration
SMTP Settings
LAN Channel
Shared
Sender Email
Primary SMTP Server
SMTP Support
Enable
SMTP Server Names
SMTP Server IP Address
Port
25
SMTP Server Authentication
Username
Password


inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
• BMC Network
• Services
• NTP
• SMTP
• Alerts
• Threshold
• Access Control
• BIOS Boot Options
Logs
Fault Diagnosis
Administration
Alert Settings
SNMP Trap Configure
Trap Version
v1
Event Severity
All
Community
public
Username
Engine ID(Hex)
Authentication and password
NONE
Privacy and password
NONE
System Name
System ID
Host Location


inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
• BMC Network
• Services
• NTP
• SMTP
• Alerts
• Threshold
• Access Control
• BIOS Boot Options
Logs
Fault Diagnosis
Administration
Threshold Settings
Sensor | Low NRT | Low CT | Low NCT | Up NCT | Up CT | Up NRT
Inlet_Temp | N/A | N/A | N/A | 40 | 42 | N/A
Outlet_Temp | N/A | N/A | N/A | 60 | 65 | N/A
PCH_Temp | N/A | N/A | N/A | 82 | 87 | N/A
CPU0_Temp | N/A | N/A | N/A | 101 | 103 | N/A
CPU1_Temp | N/A | N/A | N/A | 101 | 103 | N/A
CPU0_VR_Temp | N/A | N/A | N/A | 100 | 115 | N/A
CPU1_VR_Temp | N/A | N/A | N/A | 100 | 115 | N/A
CPU0_DIMM_Temp | N/A | N/A | N/A | 85 | 85 | N/A
CPU1_DIMM_Temp | N/A | N/A | N/A | 85 | 85 | N/A
CPU0_DIMMVR_Temp | N/A | N/A | N/A | 100 | 115 | N/A
CPU1_DIMMVR_Temp | N/A | N/A | N/A | 100 | 115 | N/A
M.2_Temp | N/A | N/A | N/A | 70 | 75 | N/A
RAID_Temp | N/A | N/A | N/A | 170 | 175 | N/A
CPU_ResourceRate | N/A | N/A | N/A | 80 | 95 | N/A
MEM_ResourceRate | N/A | N/A | N/A | 80 | 95 | N/A
HDD_ResourceRate | N/A | N/A | N/A | 80 | 95 | N/A

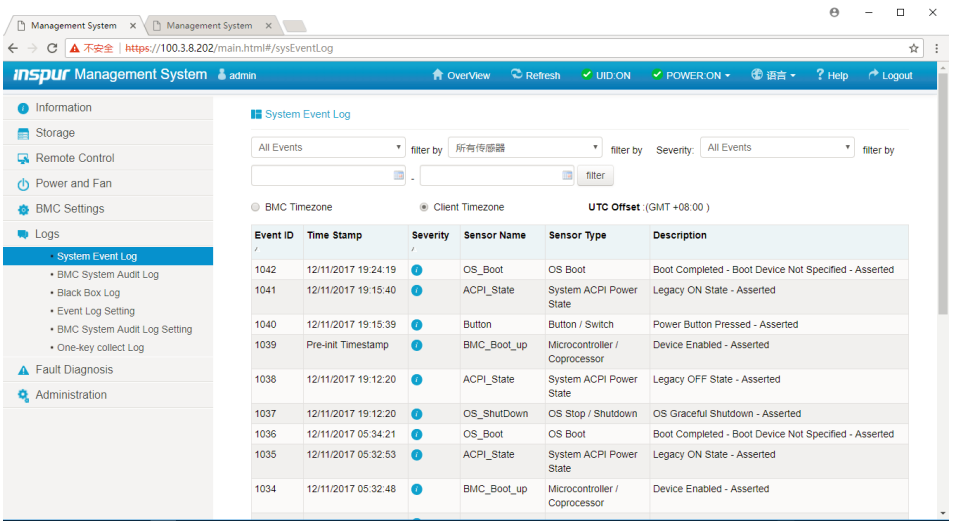

inspur Management System
admin
OverView
Refresh
UID:OFF
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
• BMC Network
• Services
• NTP
• SMTP
• Alerts
• Threshold
• Access Control
• BIOS Boot Options
Logs
Fault Diagnosis
Administration
IP Access Control
Note:
1.Operate host's IP or MAC must be added first, when add IP access policies.
2.Operate host's IP or MAC must be deleted last, when delete IP access policies.
IP Access Control
Add IP Accept Entry
IP:
To
MAC:
Rule:
Allow
Enable Timeout:
Start Date:
Stop Date:
ADD
Current IP Accept Entry List

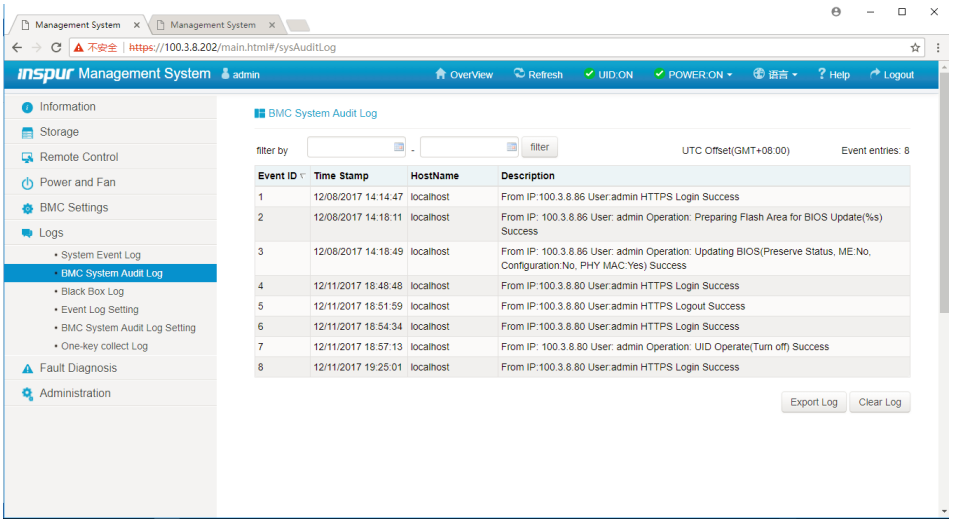


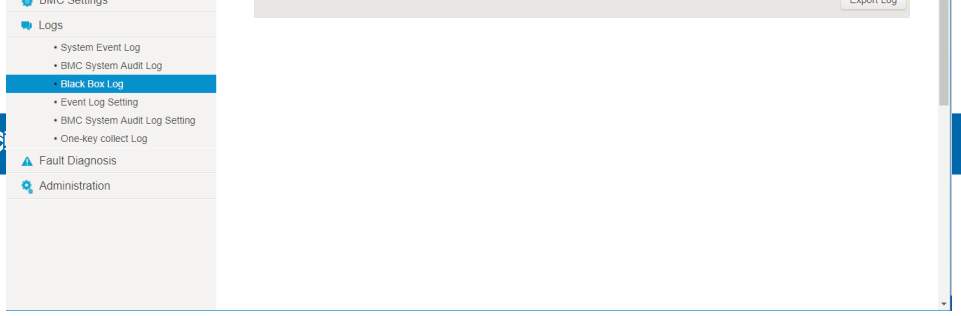
8.8 Logs

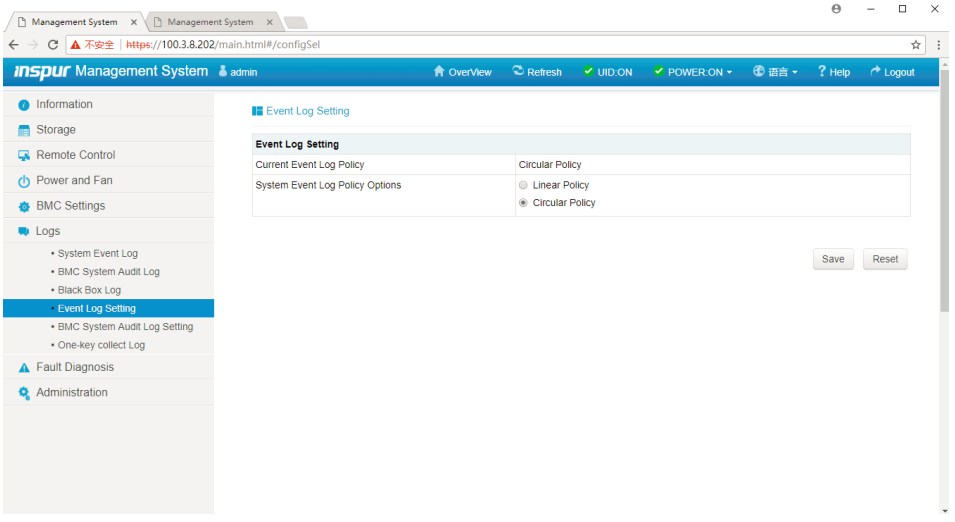
Select “Logs” on the navigation tree to open the related log interface. It contains the interfaces of system event log, BMC system audit log, black box log, event log setting, BMC system audit log setting and one-key collect log, as shown in the following figures.

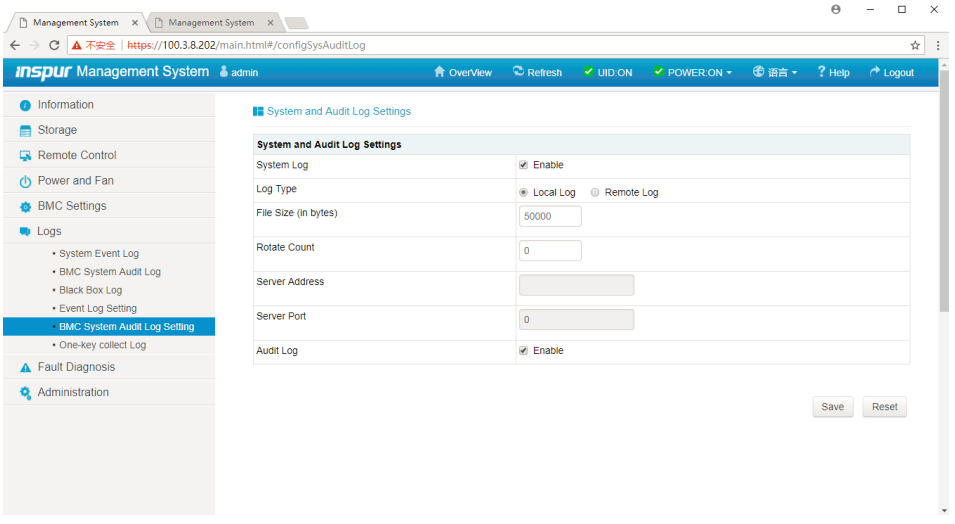
- System event log: Displays various event logs generated by the server.
- BMC system audit log: Displays system logs and audit logs of BMC.
- Black box log: Used to import fault logs.
- Event log setting: To set the BMC log storage policy:
  - Linear strategy: To clear all logs after log storage is 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.
- One-key collect log: Collect the logs via one key.


Management System
Management System
不安全 | https://100.3.8.202/main.html#/sysEventLog
inspur Management System admin
OverView
Refresh
UID:ON
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
System Event Log
BMC System Audit Log
Black Box Log
Event Log Setting
BMC System Audit Log Setting
One-key collect Log
Fault Diagnosis
Administration
System Event Log
All Events
filter by
所有传感器
filter by
Severity:
All Events
filter by
filter
BMC Timezone
Client Timezone
UTC Offset :(GMT +08:00)
Event ID
Time Stamp
Severity
Sensor Name
Sensor Type
Description
1042 12/11/2017 19:24:19 OS_Boot OS Boot Boot Completed - Boot Device Not Specified - Asserted
1041 12/11/2017 19:15:40 ACPI_State System ACPI Power State Legacy ON State - Asserted
1040 12/11/2017 19:15:39 Button Button / Switch Power Button Pressed - Asserted
1039 Pre-init Timestamp BMC_Boot_up Microcontroller / Coprocessor Device Enabled - Asserted
1038 12/11/2017 19:12:20 ACPI_State System ACPI Power State Legacy OFF State - Asserted
1037 12/11/2017 19:12:20 OS_ShutDown OS Stop / Shutdown OS Graceful Shutdown - Asserted
1036 12/11/2017 05:34:21 OS_Boot OS Boot Boot Completed - Boot Device Not Specified - Asserted
1035 12/11/2017 05:32:53 ACPI_State System ACPI Power State Legacy ON State - Asserted
1034 12/11/2017 05:32:48 BMC_Boot_up Microcontroller / Coprocessor Device Enabled - Asserted


Management System
Management System
不安全 | https://100.3.8.202/main.html#/sysAuditLog
inspur Management System admin
OverView
Refresh
UID:ON
POWER:ON
语言
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
System Event Log
BMC System Audit Log
Black Box Log
Event Log Setting
BMC System Audit Log Setting
One-key collect Log
Fault Diagnosis
Administration
BMC System Audit Log
filter by
filter
UTC Offset(GMT+08:00)
Event entries: 8
Event ID
Time Stamp
HostName
Description
1 12/08/2017 14:14:47 localhost From IP:100.3.8.86 User:admin HTTPS Login Success
2 12/08/2017 14:18:11 localhost From IP: 100.3.8.86 User: admin Operation: Preparing Flash Area for BIOS Update(%s) Success
3 12/08/2017 14:18:49 localhost From IP: 100.3.8.86 User: admin Operation: Updating BIOS(Preserve Status, ME:No, Configuration:No, PHY MAC:Yes) Success
4 12/11/2017 18:48:48 localhost From IP:100.3.8.80 User:admin HTTPS Login Success
5 12/11/2017 18:51:59 localhost From IP:100.3.8.80 User:admin HTTPS Logout Success
6 12/11/2017 18:54:34 localhost From IP:100.3.8.80 User:admin HTTPS Login Success
7 12/11/2017 18:57:13 localhost From IP: 100.3.8.80 User: admin Operation: UID Operate(Turn off) Success
8 12/11/2017 19:25:01 localhost From IP:100.3.8.80 User:admin HTTPS Login Success
Export Log
Clear Log


Logs
• System Event Log
• BMC System Audit Log
• Black Box Log
• Event Log Setting
• BMC System Audit Log Setting
• One-key collect Log
Fault Diagnosis
Administration


Management System
https://100.3.8.202/main.html#/configSel
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
• System Event Log
• BMC System Audit Log
• Black Box Log
• Event Log Setting
• BMC System Audit Log Setting
• One-key collect Log
Fault Diagnosis
Administration
Event Log Setting
Event Log Setting
Current Event Log Policy
Circular Policy
System Event Log Policy Options
Linear Policy
Circular Policy
Save
Reset


Management System
https://100.3.8.202/main.html#/configSysAuditLog
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
• System Event Log
• BMC System Audit Log
• Black Box Log
• Event Log Setting
• BMC System Audit Log Setting
• One-key collect Log
Fault Diagnosis
Administration
System and Audit Log Settings
System and Audit Log Settings
System Log
Enable
Log Type
Local Log
Remote Log
File Size (in bytes)
50000
Rotate Count
0
Server Address
Server Port
0
Audit Log
Enable
Save
Reset

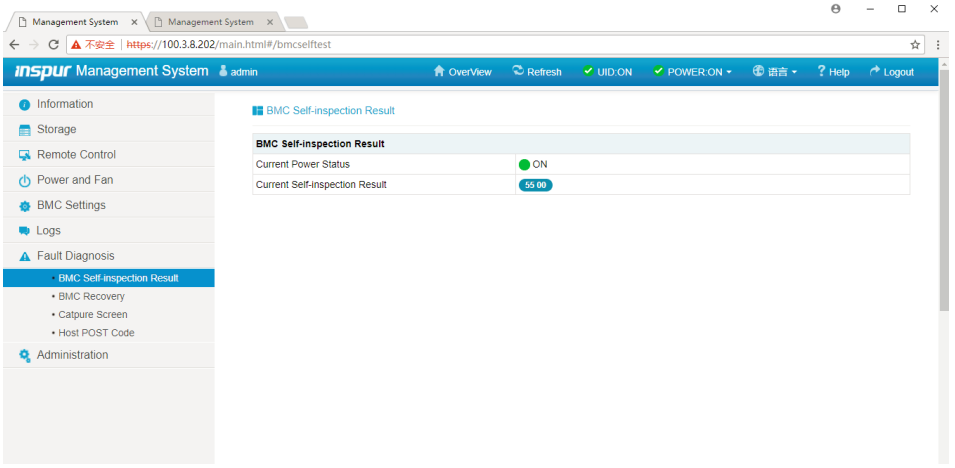
8.9 Fault Diagnosis

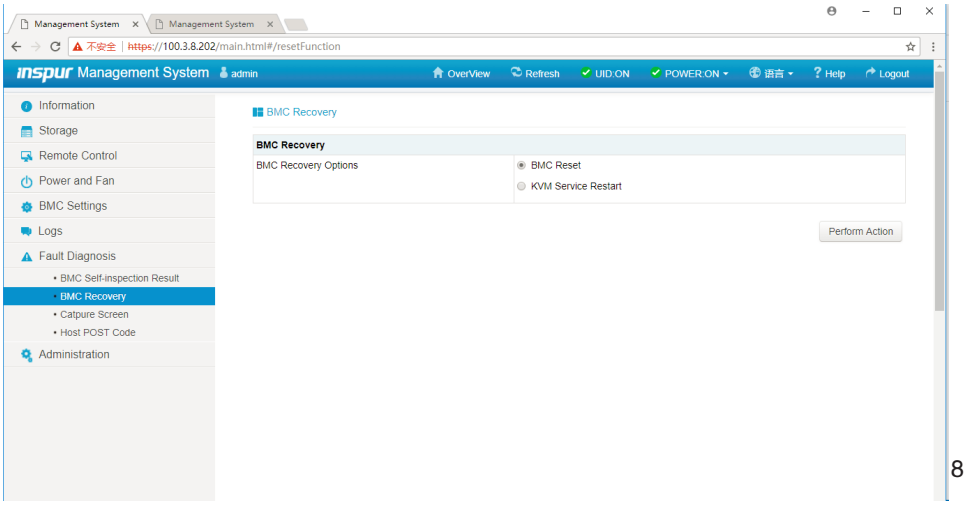
Select “Fault Diagnosis” on the navigation tree to open the fault diagnosis interface. It contains the interfaces of BMC self-inspection result, BMC recovery, capture screen and host POST code, as shown in the following figures.

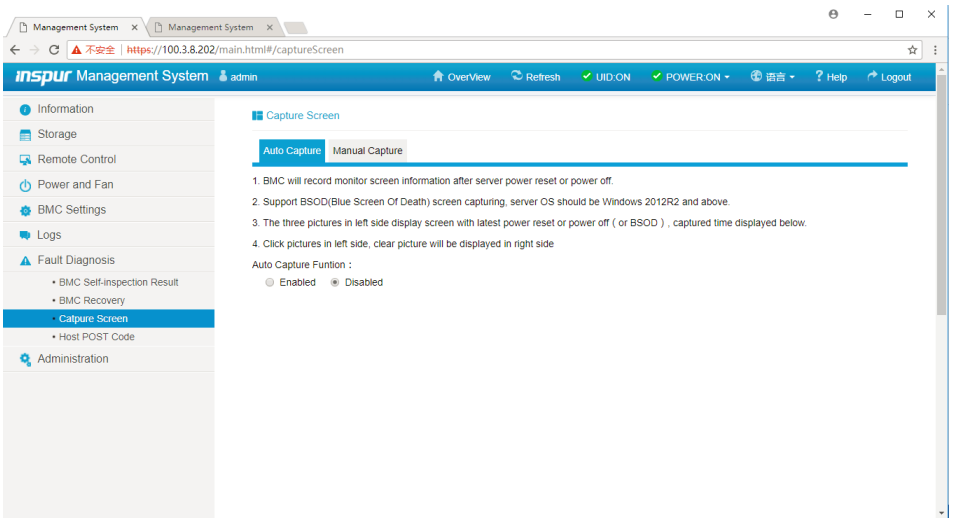
- BMC self-inspection result: To view the BMC self-inspection result.
- BMC recovery: Contains two functions of BMC warm reset and KVM service restart.
- Capture screen: Used to record the information on the last screen at system crash.

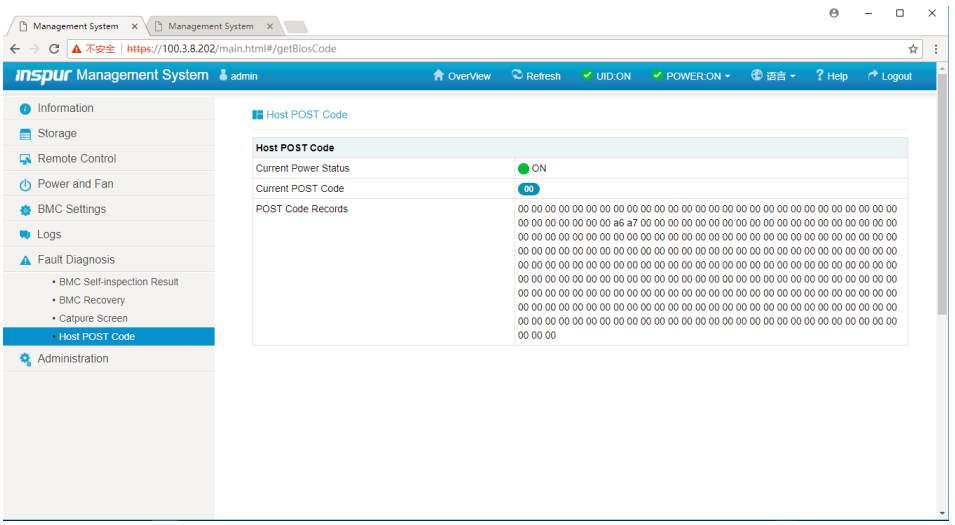
Note: Support BSOD (Blue Screen Of Death) screen capturing, server OS should be Windows 2008R2 and Windows 2012.

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







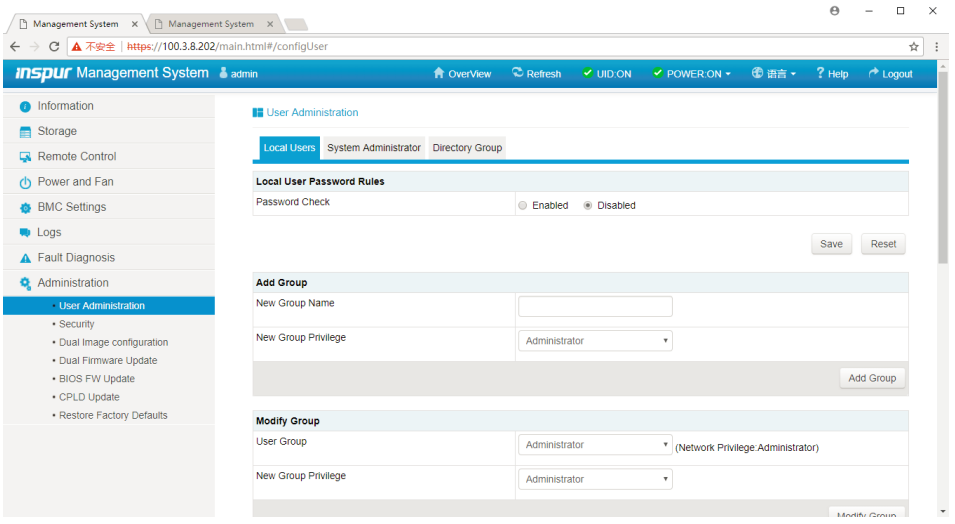


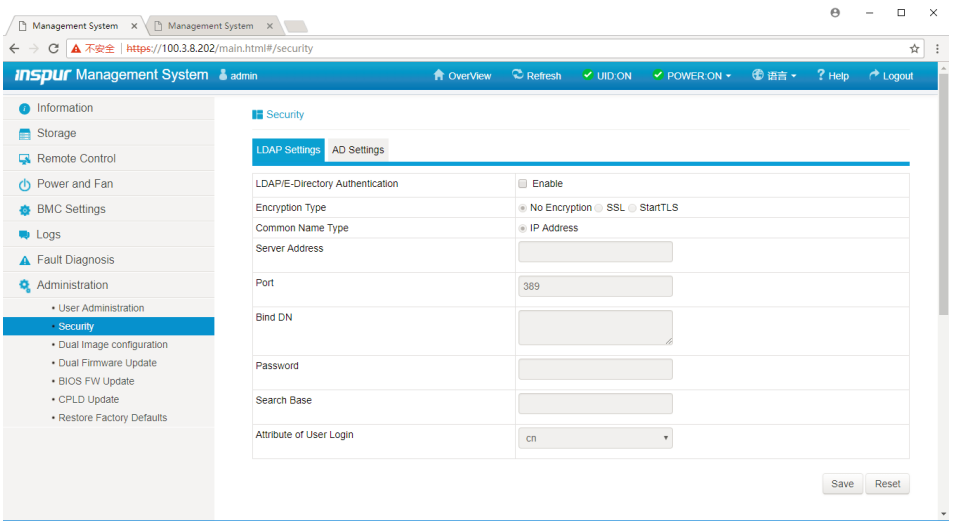
8.10 Administration

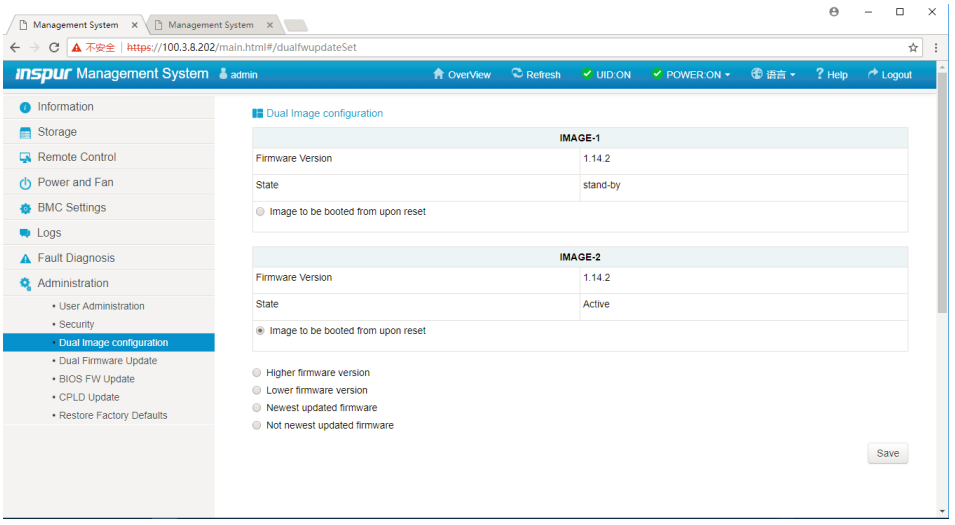
Select “Administration” on the navigation tree to open the administration interface. It contains the interfaces of user administration, security, dual image configuration, dual firmware update, BIOS firmware update, CPLD update and restore factory defaults, as shown in the following figures.

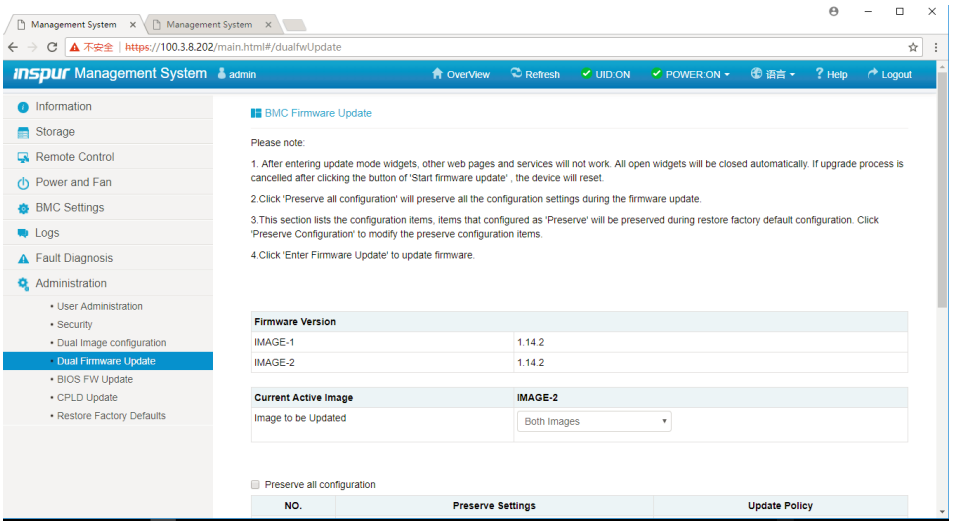
- User administration: To add, delete or modify users via BMC Web interface.
- Security: To configure LDAP and AD servers via BMC Web interface.

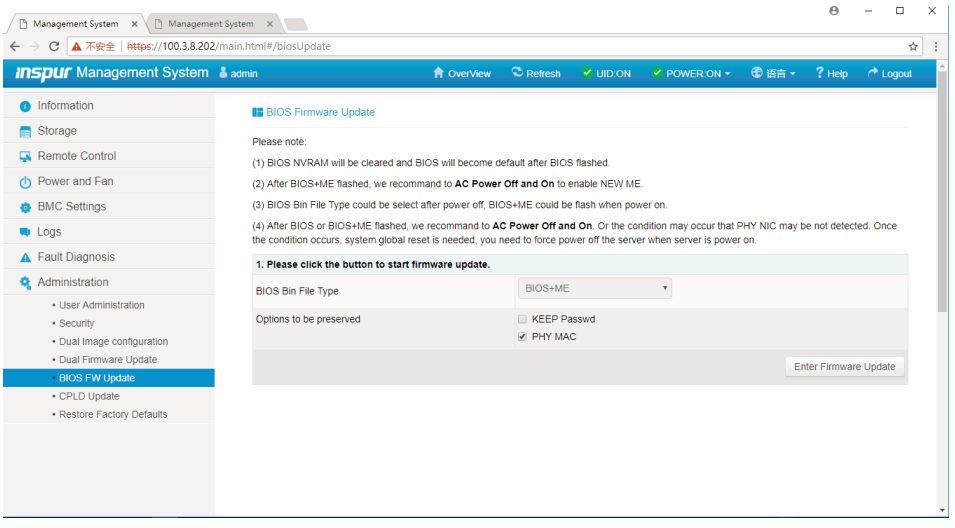
- Dual image configuration: To configure the boot options in dual image mode via BMC Web interface.
- Dual firmware update: To update BMC FW via BMC Web interface.
- BIOS firmware update: To update BIOS FW via BMC Web interface.
- CPLD update: To update CPLD via BMC Web interface.
- Restore factory defaults: To restore BMC's configuration to factory state.

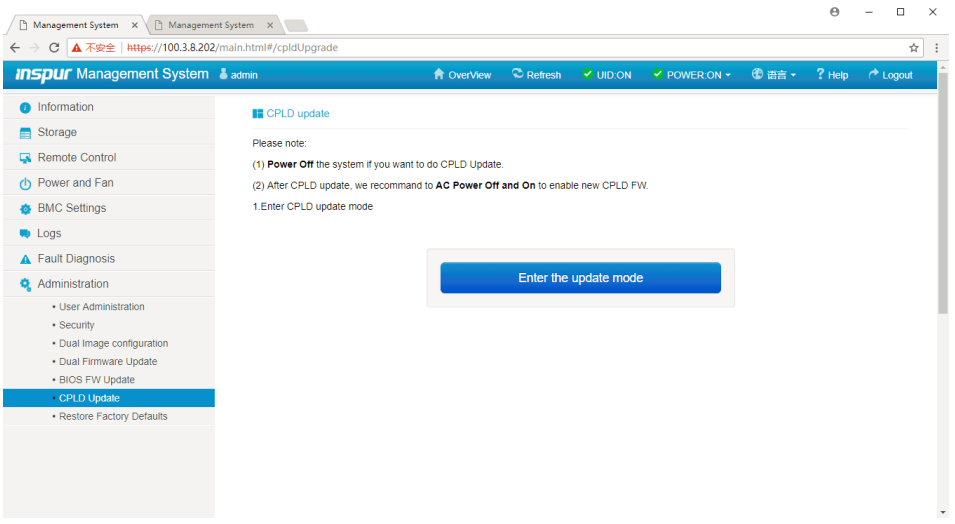


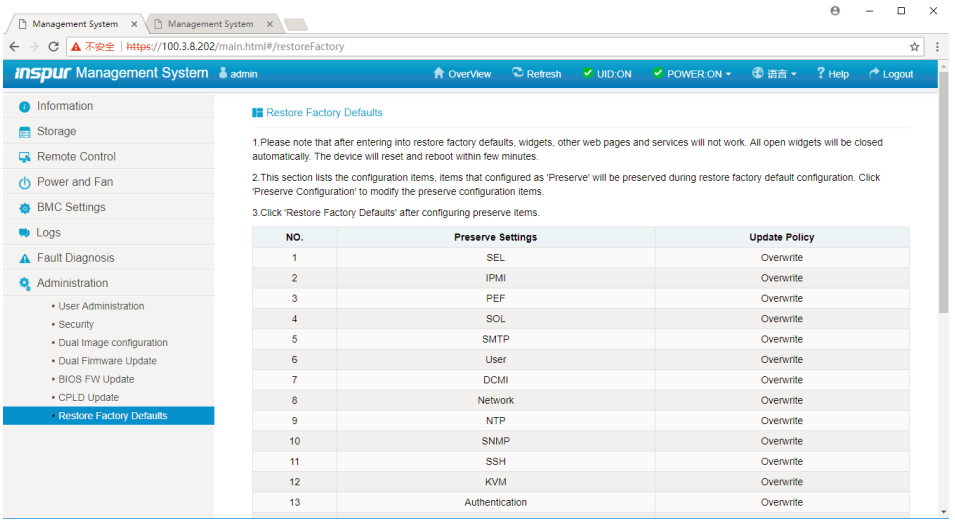



Management System
https://100.3.8.202/main.html#/dualfwupdateSet
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
User Administration
Security
Dual Image configuration
Dual Firmware Update
BIOS FW Update
CPLD Update
Restore Factory Defaults
Dual Image configuration
IMAGE-1
Firmware Version
1.14.2
State
stand-by
Image to be booted from upon reset
IMAGE-2
Firmware Version
1.14.2
State
Active
Image to be booted from upon reset
Higher firmware version
Lower firmware version
Newest updated firmware
Not newest updated firmware
Save


Management System
https://100.3.8.202/main.html#/dualfwUpdate
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
User Administration
Security
Dual Image configuration
Dual Firmware Update
BIOS FW Update
CPLD Update
Restore Factory Defaults
BMC Firmware Update
Please note:
1. After entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled after clicking the button of 'Start firmware update' , the device will reset.
2.Click 'Preserve all configuration' will preserve all the configuration settings during the firmware update.
3.This section lists the configuration items, items that configured as 'Preserve' will be preserved during restore factory default configuration. Click 'Preserve Configuration' to modify the preserve configuration items.
4.Click 'Enter Firmware Update' to update firmware.
Firmware Version
IMAGE-1
1.14.2
IMAGE-2
1.14.2
Current Active Image
IMAGE-2
Image to be Updated
Both Images
Preserve all configuration
NO.
Preserve Settings
Update Policy


Management System
https://100.3.8.202/main.html#/biosUpdate
inspur Management System
admin
OverView
Refresh
UID:ON
POWER:ON
Help
Logout
Information
Storage
Remote Control
Power and Fan
BMC Settings
Logs
Fault Diagnosis
Administration
User Administration
Security
Dual Image configuration
Dual Firmware Update
BIOS FW Update
CPLD Update
Restore Factory Defaults
BIOS Firmware Update
Please note:
(1) BIOS NVRAM will be cleared and BIOS will become default after BIOS flashed.
(2) After BIOS+ME flashed, we recommand to AC Power Off and On to enable NEW ME.
(3) BIOS Bin File Type could be select after power off, BIOS+ME could be flash when power on.
(4) After BIOS or BIOS+ME flashed, we recommand to AC Power Off and On. Or the condition may occur that PHY NIC may be not detected. Once the condition occurs, system global reset is needed, you need to force power off the server when server is power on.
1. Please click the button to start firmware update.
BIOS Bin File Type
BIOS+ME
Options to be preserved
KEEP Passwd
PHY MAC
Enter Firmware Update





8.11 Service & Protocol

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

Service	Usage	Default State	Non-Security Port	Security Port	Default Port	Timeout(s)	Max Session
RMCP+	IPMI	Enable	623	N/A	N/A	1800	20
Http/Https	WEBGUI	Enable	80(Http)	443(Https)	443(Https)	1800	20
KVM	Console Redirection	Enable	7578	7582	7578	1800	4
cd-media	Virtual Media	Enable	5120	5124	5120	N/A	4
fd-media	Virtual Media	Enable	5122	5126	5122	N/A	4
hd-media	Virtual Media	Enable	5123	5127	5123	N/A	4
ssh	ssh	Disable	N/A	22	22	600	N/A
telnet	telnet	Disable	23	N/A	23	600	N/A
solssh	sol by ssh	Enable	52123	N/A	N/A	60	N/A

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

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

Fixed Protocols could not be configured.

Service	Usage	State	Port
SNMP	SNMP Get/Set	Enable	161
syslog	syslog	Enable	514
Websockify	KVM on HTML5	Enable	9666
Websockify	Virtual Media on HTML5	Enable	9999

8.12 Users

8.12.1 IPMI User

BMC supports the IPMI 2.0 user model. 16 user IDs are supported. These 16 users can be assigned to any channel. All of them can login simultaneously. The available user privilege levels are Administrator, Operator, User, OEM Proprietary and No Access.

Users	User Name	Password	Status	Default Privilege

User 1	admin	admin	Enabled	Administrator
User 2- 16	undefined	undefined	Disabled	Administrator

User Privilege for IPMI, please refer to IPMI 2.0 Spec.

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

Username

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

Password

- At password complexity check disabled, Password must be at least 1 character long.
- At password complexity check enabled, Password must include special, uppercase, lowercase character and number, at least 8 characters long.
- Not allow more than 16 characters.
- Default disable complexity check, we strongly suggest you enable this function for security.
- Password Expiration, the range of the expiration is 0~90 days, and 0 presents forever. Default disable, we strongly suggest you enable this function for security. If enable, you need change password in expiration time. If password expired, you need disable this function in OS by OEM IPMI CMD.

-Login Fail Retry Count: the retry count should be a number between 0 and 5. Lock Time: the range of the time is 5 ~ 60 minutes. Default disable, we strongly suggest you enable this function for security.

-Password History Records: the range is 0 ~ 5. Default disable. If enable, you could not set password same to Password History Records (last N password).

8.12.2 System User

System user is root user in BMC Linux OS, user can use this user to access smash cli by ssh/ telnet.

User name: sysadmin (Fixed, cannot be changed)

Default password: superuser

Username and Password Security

- Username is fixed, cannot be changed.
- Password must be at least 8 characters long.
- Password must be include special, uppercase, lowercase characters and numbers.
- White space is not allowed.
- Not allow more than 64 characters.

8.13 BMC Firmware Update

8.13.1 Firmware Integrity Checking

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

8.13.2 WEB Update

BMC firmware update is supported via the Management Web GUI. BMC firmware update is configured with Watchdog. The watchdog time is 20 min. When entering the flash mode, the watchdog will be active, 20min timeout will reset the BMC automatically. When flashing the image, the watchdog will be active, 20 min timeout will reset the BMC automatically.

Dual BMC firmware image is supported.

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

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

Note:

The firmware upgrade 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 flash page.
- Select image file, click Upload button to upload file, BMC will go to flash mode after upload file, IPMI service will stop, and then BMC will verify image. Verify:

Size should be 32M.

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

If verify failed, BMC will stop flash and restart.

- Check image version and current image version, then click Update button to flash.

8.13.3 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.

8.14 Redfish

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

The client can access the Redfish service through the HTTP client. The following is the use of curl in Linux to send the request that can operate on redfish. The usual request operations have “GET”, “PUT”, “POST”, “PATCH” and “DELETE”, and the data sent and returned both are in json format.

The username and password below refer to those of BMC users with administrator privileges.

8.14.1 GET Basic Format

The client can get the data under the specified URL via HTTP GET. The basic format of access is as follows:

curl -k -u username:password https://BMC_IP:8080/redfish/v1/Chassis/1

8.14.2 POST Basic Format

The client can send data to the specified URL via HTTP POST, so that the server can configure accordingly. The basic format of POST access is as follows:

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

Notes:

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

The parameters behind –H is the format of the requested data.

The parameters behind –d is the requested data.

8.14.3 DELETE Basic Format

The client can delete the data under the specified URL via HTTP DELETE, so that the server can delete the specified configuration according to the URL. The basic format of DELETE access is as follows:

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

Note:

https://BMC_IP:8080/redfish/v1/SessionService/Sessions/1 is the address you want to delete.

8.14.4 Access Steps

1. Get the resources provided by Redfish. It needs no authorization to access the root directory of Redfish. Through the access, users can know the resource-accessible URLs that Redfish can provide.

Request:

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

Response


```
{
  “@Redfish.Copyright”: “Copyright 2014-2016 Distributed Management Task Force, Inc. (DMTF). For the full DMTF copyright policy, see http://www.dmtf.org/about/policies/copyright.”,
  “@odata.context”: “/redfish/v1/$metadata#ServiceRoot.ServiceRoot”,
  “@odata.id”: “/redfish/v1/”,
  “@odata.type”: “#ServiceRoot.v1_1_0.ServiceRoot”,
  “AccountService”: {
    “@odata.id”: “/redfish/v1/AccountService”
  },
  “Chassis”: {
    “@odata.id”: “/redfish/v1/Chassis”
  },
  “EventService”: {
    “@odata.id”: “/redfish/v1/EventService”
  },
  “Id”: “RootService”,
  “Links”: {
    “Sessions”: {
      “@odata.id”: “/redfish/v1/SessionService/Sessions”
    }
  },
  “Managers”: {
    “@odata.id”: “/redfish/v1/Managers”
  },
  “Name”: “Root Service”,
  “Oem”: {},
  “RedfishVersion”: “1.1.0”,
  “SessionService”: {
    “@odata.id”: “/redfish/v1/SessionService”
  },
  “Systems”: {
    “@odata.id”: “/redfish/v1/Systems”
  },
  “Tasks”: {
    “@odata.id”: “/redfish/v1/TaskService”
  },
  “UUID”: “92384634-2938-2342-8820-489239905423”
}
```

2. The URL of the device type to be accessed can be obtained based on the acquired resource above.

e.g. The URL to get the Chassis type is */redfish/v1/Chassis:*

Request:

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

Response:


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


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

e.g. The URL to get the Chassis detailed information is */redfish/v1/Chassis/Chassis1:*

Request:

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

Response:

```
{
  “@odata.type”: “#Chassis.v1_2_0.Chassis”,
  “Id”: “1”,
  “Name”: “Computer System Chassis”,
  “ChassisType”: “RackMount”,
  “AssetTag”: “5180”,
  “Manufacturer”: “Inspur”,
  “Model”: “5180”,
  “SKU”: “8675309”,
  “SerialNumber”: “5180”,
  “PartNumber”: “224071-J23”,
  “PowerState”: “On”,
  “IndicatorLED”: “Lit”,
  “Status”: {
  “State”: “Enabled”,
    “Health”: “OK”
  },
  “Thermal”: {
    “@odata.id”: “/redfish/v1/Chassis/1/Thermal”
  },
  “Power”: {
    “@odata.id”: “/redfish/v1/Chassis/1/Power”
  },
  “Links”: {
    “ComputerSystems”: [
      {
        “@odata.id”: “/redfish/v1/Systems/5180”
      }
    ],
    “ManagedBy”: [
      {
        “@odata.id”: “/redfish/v1/Managers/BMC”
      }
    ],
    “ManagersInChassis”: [
      {
        “@odata.id”: “/redfish/v1/Managers/BMC”
      }
    ]
  },
  “@odata.context”: “/redfish/v1/$metadata#Chassis.Chassis”,
  “@odata.id”: “/redfish/v1/Chassis/1”,
  “@Redfish.Copyright”: “Copyright 2014-2016 Distributed Management Task Force, Inc. (DMTF). For the full DMTF copyright policy, see http://www.dmtf.org/about/policies/copyright.”
}
```


Note: The response values vary with server models, please refer to the return values of the

actual model you purchased.

8.15 Command Line Function Introduction

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

- Login command line

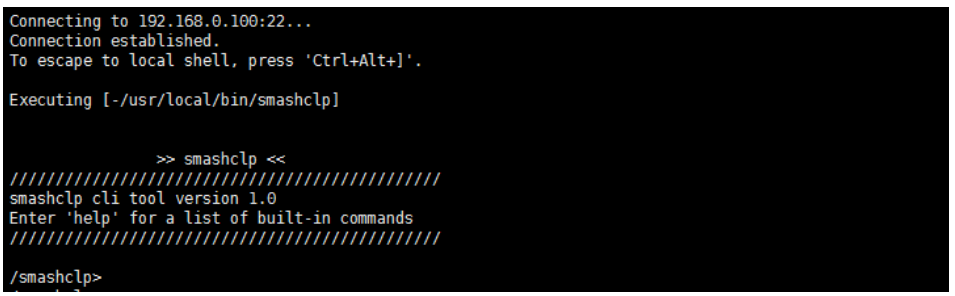
Introduces methods of login command line.

- Command line function introduction

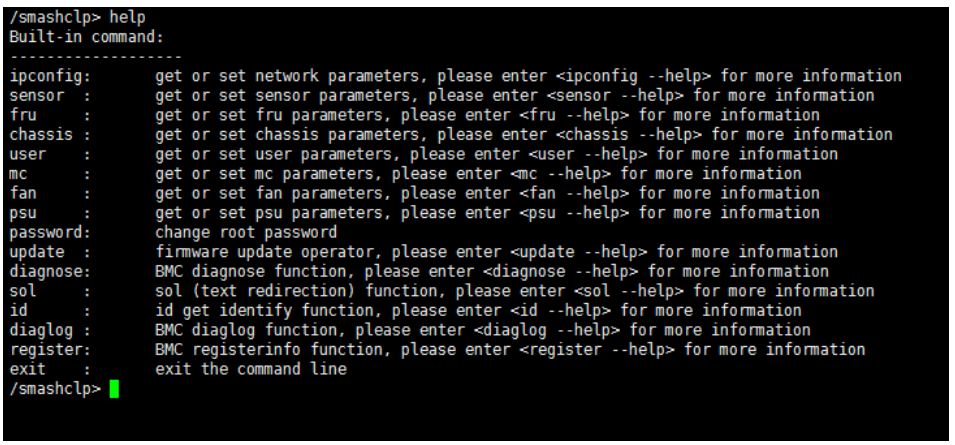
Introduces command line functions.

8.15.1 Command Line Login

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



Enter help to view online help:



8.15.2 Command Line Function Introduction

8.15.2.1 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>
```

8.15.2.2 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
```

8.15.2.3 Get and Set FRU Information

Via FRU command, get the FRU configuration information:

```
      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>
```

8.15.2.4 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>
```

8.15.2.5 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
```

8.15.2.6 Get BMC Version and Reset BMC

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

```
    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>
```

8.15.2.7 Change Root Password

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

```
/smashclp> password
New password:
```

8.15.2.8 Fault Diagnosis

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

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

8.15.2.9 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.

```
/smashclp> diaglog --help
diaglog commands:
     diaglog <option1>
     option1:
       --help    show help information
       ?         show help information
       --get     trigger one key log
       for example : diaglog --get
/smashclp>
```

8.15.2.10 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: ~.
```

8.16 Time Zone Table

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

9 Common Faults, Diagnosis and Troubleshooting

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

9.1 Hardware Problems

1) Power-on failure at startup

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

Suggestions:

a. Check the power supply situation: If the power module LED is on, it indicates normal power supply. If the power module LED is off or red, please check whether the power supply is normal, and whether the power cord is connected well.

b. If the power supply is normal, insert the power module again, and then power on for verification.

c. If there is a machine and a power module of the same type, you could change the power module to test whether there is a power module fault.

d. If the instructions above do not resolve the problem, please contact Inspur customer service.

2) No display after power on

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

Suggestions:

a. Firstly check whether the monitor is powered up normally.

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

c. Test on another monitor.

d. If there is no output on the new monitor, login to the BMC Web interface. Open BMC remote KVM to check whether there is output on the monitor. If there is normal output, it indicates the VGA port may be abnormal, please contact Inspur customer service.

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

3) Status LED on front panel is abnormal

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

Suggestions:

a. Firstly confirm which LED is abnormal according to the previous chapter about the LEDs on the front panel.

b. If the system failure LED is abnormal, check whether the system runs normally; if the system runs normally, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.

c. If the power failure LED is abnormal, check whether the power module LED is normal; if the power module LED is normal, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.

d. If other LEDs are abnormal, you can login to the BMC Web interface to view the BMC logs, to check whether there are errors reported.

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

4) Power module LED is off or red

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

Suggestions:

a. Firstly check whether all power cables are normal, and plug in the power cables again.

b. If the fault still exists, insert the power module again.

c. If shutdown is allowed, you could exchange the two power modules to judge whether it is a power module fault.

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

5) HDD status LED is abnormal

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

Suggestions:

a. If it is caused by manual operations, restore the array through RAID configuration.

b. If there is no manual operations, check whether the HDDs are identified normally. If the server is configured with an RAID card, login to the RAID management interface to check whether there is an HDD failure.

c. If there is an HDD failure, or the above operations could not resolve the problem, please

contact Inspur customer service.

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

6) Chassis fans make excessive noise

Suggestions:

a. Firstly check whether the chassis fans operate at a high speed caused by the over-temperature chassis.

b. If the chassis has a high temperature, check the temperature of server room, if it is excessively high, open the air conditioner to cool the room.

c. If the server room's temperature is normal, check whether the front panel or chassis interior is jammed with dust, or the air inlet is blocked. It needs to improve the server room's environment, to avoid server over-temperature running because of too much dust.

d. Check whether the server runs under high load.

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

7) There is alarm sound during startup

Suggestions:

Firstly identify the source of alarm sound:

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

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

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

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

8) Keyboard and mouse are not available

Description: Neither keyboard nor mouse could be operated normally.

Suggestions:

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

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

c. Power cycle the server and retest.

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

9) USB interface problem

Description: Unable to use devices with a USB interface.

Suggestions:

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

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

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

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

e. If the USB device is normal when connected to other hosts, the server may be abnormal: please contact Inspur customer service.

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

9.2 Software Problems

1) System installation problems

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

Suggestions:

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

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

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

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

2) The memory capacity is abnormal

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

Suggestions:

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

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

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

3) Abnormal network

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

Suggestions:

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

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

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

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

10 Battery Replacement

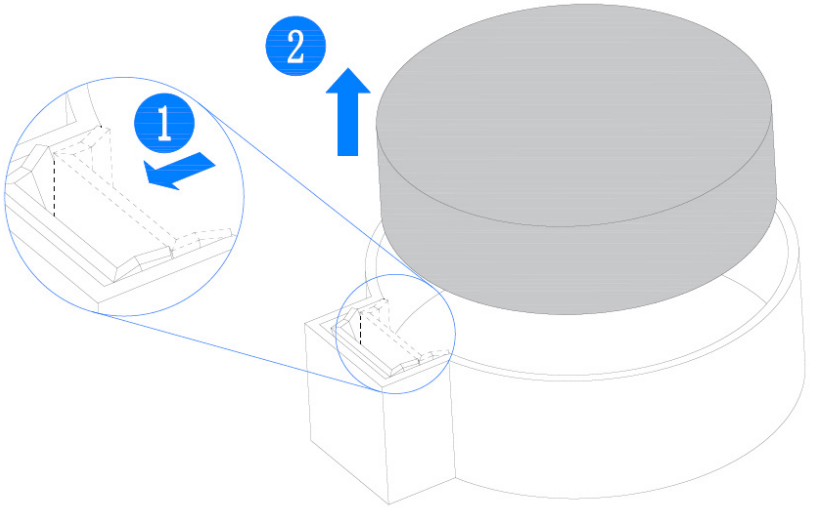
If the server no longer automatically displays the correct date and time, you may need to replace the battery that provides power to the real-time clock.

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 interconnection module.
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.



11 Regulatory Compliance Notices

11.1 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.

11.2 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.

11.2.1 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.

11.3 Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

11.4 European Union Regulatory Notice

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

- Low Voltage Directive 2006/95/EC
- EMC Directive 2004/108/EC
- Eco-design Directive 2009/125/EC, where applicable

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.

11.5 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.

11.6 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.

11.7 Chinese Notice

Class A Equipment

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

11.8 Battery Replacement Notice

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

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

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

12 Electrostatic Discharge

12.1 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.

12.2 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.

13 Warranty

13.1 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.

13.2 Warranty Service

13.2.1 Service Overview

Type	**uration**
Remote Services	3 years
RMA Services	3 years

13.2.2 Warranty Service Terms & Conditions

i. Remote Services

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

Below is how to obtain our remote service:

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

ii. RMA Services

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

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

13.3 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.