



Inspur Server User Manual

ON5263M5

Revision History

Refer to the table below for the updates made to this user manual.

Date	Version	Chapter	Updates
August 24, 2020	V1.00		

Copyright

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

© Copyright Inspur 2020. All rights reserved.

Disclaimer

This document, including all images, illustrations and information related to Inspur product, is protected under international copyright laws. Reproduction of this manual, or the material contained herein, in any form or by any means without the written permission of Inspur is strictly forbidden.

The information in this manual is subject to change without notice. The latest manual or characterized errata are available on request. Images provided herein are for reference only and may contain information or features that do not apply to your purchased model. Inspur shall not be liable for technical or editorial errors or omissions contained in this manual.

Conventions

The following conventions are used in this manual:



WARNING indicates a potential for personal injury.



CAUTION indicates a potential loss of data or damage to equipment



NOTE indicates tips and additional information to aid in the proper completion of a procedure, choice of an option, or completing a task.

General Information

This manual introduces ON5263M5 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.

It is recommended that server installation, configuration, and maintenance is performed by experienced technicians only. This manual is intended for: Technical support engineers, Product maintenance engineers, and Technicians.

Safety Precautions

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.

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

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.

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.

Table of Contents

- 1. Safety Instructions..... 1**
- 2. Product Specification 5**
 - 2.1 Introduction.....5
 - 2.2 Specification6
- 3. Product Overview 7**
 - 3.1 Front View7
 - 3.2 Rear View.....8
 - 3.3 Motherboard View9
 - 3.4 Exploded Diagram.....10
- 4. Getting Started.....11**
 - 4.1 Package Contents11
 - 4.2 Power On/Off11
 - 4.3 Pre-disassembly Instructions.....11
 - 4.4 Disassembly/Reassembly Process12
 - 4.4.1 Air Baffle Replacement.....12
 - 4.4.2 Fan Module Replacement14
 - 4.4.3 DIMM Replacement.....14
 - 4.4.4 PCIe Riser-Card Assembly Replacement.....16
 - 4.4.5 M.2 SSD Replacement17
- 5. Setup19**
 - 5.1 Operational Requirements19
 - 5.1.1 Space and Airflow19
 - 5.1.2 Temperature.....20
 - 5.1.3 Power.....20
 - 5.1.4 Electrical Grounding20
 - 5.2 Downloading the Drivers21

6. BIOS Settings.....	22
6.1 Basic Operations	22
6.1.1 System Information	24
6.1.2 CPU Information	24
6.1.3 Memory Information	24
6.1.4 UEFI/Legacy Mode.....	25
6.1.5 RAID Volume Configuration.....	25
6.1.6 BMC Network Configuration	33
6.2 BIOS Setup Menu.....	37
6.2.1 Main.....	37
6.2.2 Advanced	38
6.2.2.1 Trusted Computing	39
6.2.2.2 Super IO Configuration	40
6.2.2.3 Serial Port Console Redirection	41
6.2.2.4 PCI Subsystem Settings.....	43
6.2.2.5 CSM Configuration.....	44
6.2.2.6 Onboard LAN Configuration	46
6.2.2.7 USB Devices Information	46
6.2.2.8 Network Stack Configuration	47
6.2.2.9 iSCSI Configuration	48
6.2.3 Chipset.....	51
6.2.3.1 PCH SATA/sATA Configuration	51
6.2.3.2 USB Configuration	52
6.2.3.3 Miscellaneous Configuration.....	53
6.2.3.4 Server ME Configuration	54
6.2.3.5 Runtime Error Logging.....	54
6.2.4 Processor	55
6.2.4.1 Processor Configuration	55
6.2.4.2 Common Configuration	57
6.2.4.3 UPI Configuration	58
6.2.4.4 Memory Configuration	59
6.2.4.5 IIO Configuration	63
6.2.4.6 Advanced Power Management Configuration	64
6.2.5 Server Mgmt.....	71
6.2.5.1 BMC Network Configuration	72
6.2.5.2 BMC User Settings	74
6.2.5.3 VLAN Configuration	77

- 6.2.5.4 View FRU information78
- 6.2.6 Security78
- 6.2.7 Boot79
- 6.2.8 Save & Exit80
- 6.3 Firmware Update.....81
 - 6.3.1 UEFI Shell81
 - 6.3.2 AMI Flash Utility82

7. BMC Settings.....84

- 7.1 Introduction.....84
- 7.2 Software Interfaces85
 - 7.2.1 IPMI 2.0.....85
 - 7.2.1.1 Channel ID Assignment for Each Interface85
 - 7.2.1.2 System Interfaces86
 - 7.2.1.3 IPMB Interfaces86
 - 7.2.1.4 LAN interfaces.....86
 - 7.2.1.5 IPMI Commands86
 - 7.2.2 Web GUI.....94
 - 7.2.2.1 Web GUI Login95
 - 7.2.2.2 Web GUI Introduction96
 - 7.2.2.3 Web GUI Features96
 - 7.2.3 SNMP99
 - 7.2.4 Smash-Lite CLI..... 100
 - 7.2.4.1 Command Line Login 100
 - 7.2.4.2 Command Line Features..... 100
- 7.3 System Overview 103
 - 7.3.1 System Running State..... 103
 - 7.3.2 Management Device (BMC) Information and Server information..... 105
 - 7.3.3 Quick Launch 105
 - 7.3.4 Online User Information..... 105
 - 7.3.5 Firmware Version Information 105
 - 7.3.6 Recent Event Logs..... 106
- 7.4 Information..... 106
 - 7.4.1 System Information 106

7.4.2	BIOS Setup Options.....	110
7.4.3	FRU Information	111
7.4.4	History Record	111
7.5	Remote Control	113
7.5.1	Console Redirection (KVM)	113
7.5.1.1	HTML5 KVM.....	113
7.5.1.2	Java KVM.....	114
7.5.2	Locate Server	114
7.5.3	Remote Session Settings	115
7.5.4	Virtual Media Settings	115
7.5.5	Mouse Mode Settings.....	117
7.6	Power and Fan.....	118
7.6.1	Server Power Control	118
7.6.2	Fan Speed Control	119
7.7	BMC Settings.....	120
7.7.1	BMC Network Management.....	120
7.7.2	Service Settings.....	121
7.7.3	NTP Settings.....	122
7.7.4	SMTP Settings	123
7.7.5	Alert Management	123
7.7.6	Access Control	125
7.7.7	BIOS Boot Options	125
7.8	Logs.....	125
7.8.1	System Event Log.....	126
7.8.2	BMC System Audit Log.....	127
7.8.3	Event Log Setting	128
7.8.4	System Audit Log Settings	128
7.8.5	One-key Collection Log.....	129
7.8.6	System Serial Log.....	129
7.9	Fault Diagnosis.....	130
7.9.1	BMC Self-inspection Result.....	130

- 7.9.2 BMC Recovery..... 130
- 7.9.3 Screen Capture 131
- 7.9.4 HOST POST Code..... 131
- 7.9.5 BMC Watchdog for System..... 131
- 7.10 Administration..... 132
 - 7.10.1 User Management..... 132
 - 7.10.1.1 User Privileges 134
 - 7.10.2 Security..... 136
 - 7.10.3 BMC Dual Image Configuration 137
 - 7.10.4 BMC Dual Firmware Update..... 137
 - 7.10.5 BIOS FW Update 139
 - 7.10.6 Restore Factory Defaults 141
- 7.11 Device State Monitor and Diagnostic..... 142
 - 7.11.1 Sensors..... 142
 - 7.11.1.1 Physical Sensors..... 142
 - 7.11.1.2 Virtual Sensors..... 143
 - 7.11.1.3 Event-Only sensors 143
 - 7.11.1.4 Sensor attribute..... 143
 - 7.11.2 CPU 144
 - 7.11.3 Memory 144
- 7.12 Event Alerts..... 144
 - 7.12.1 SMTP Email Alerts..... 144
 - 7.12.2 Syslog 146
- 7.13 BMC Self Recovery..... 146
 - 7.13.1 Hardware Watchdog 146
 - 7.13.2 Software Watchdog..... 146
- 7.14 LED 146
- 7.15 SOL and System Serial Log 147
- 8. Troubleshooting.....149**
- 9. Battery Replacement150**

- 10. Regulatory Information.....151**
 - 10.1 Regulatory Compliance Identification Numbers 151
 - 10.2 Federal Communications Commission Notice..... 151
 - 10.2.1 FCC Rating Label 151
 - 10.3 Battery Replacement Notice 152
- 11. Electrostatic Discharge.....153**
 - 11.1 Preventing Electrostatic Discharge..... 153
 - 11.2 Grounding Methods to Prevent Electrostatic Discharge..... 153
- 12. Warranty154**
 - 12.1 Warranty Service 154
 - 12.2 Inspur Service SLA..... 155
 - 12.3 Warranty Exclusions 156

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 so 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 dismantling the host cover or touching the internal components.
 - 3) During the dismantling process, avoid making large movement ranges to prevent damage to the components or scratching arms.
 - 4) Handle components and plug-in cards with care. Please do not touch the components or connection points on the plug-in cards. When handling the plug-in cards or components, firmly grab the edges of the plug-in cards and components, and/or their metal fixed supports.
8. During the process of rack installation and application, please pay attention to the followings:
- 1) After the rack installation is finished, please ensure that the stabilizers have been fixed to the rack and supported to ground, and the weight of the rack is firm on ground.
 - 2) When pulling out the components from the rack, apply slight force to keep the rack balanced.
 - 3) When pressing down the release latch and the rail of components is sliding, please be careful; as the sliding may hurt your fingers.
 - 4) 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.
 - 5) Ensure that components in the rack have good ventilation conditions.
 - 6) When repairing components in the rack, never step on any other components.

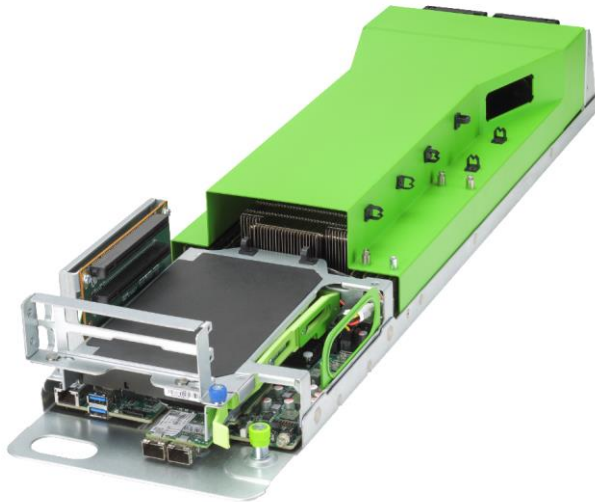
2. Product Specification

This chapter describes the basic information and specification of Inspur ON5263M5 server.

2.1 Introduction

Inspur ON5263M5 is an Open Compute Project v2 compatible multi-node compute system, supports dual Intel® Xeon Scalable Processors and 16 slots of DDR4 memory with a maximum capability of 512GB to handle versatile workloads among current datacenters.

ON5263M5 has one (1) SATA/PCIE M.2, two (2) PCIe expansion slots, and one (1) OCP 2.0 slot at the front side, providing the ultimate flexibility for scale-out solutions. With modularized design, users can swap the selected front I/O modules to fulfill hardware requirements according to the multiple applications. Following the principle of OCP, ON5263M5 can be installed in a uniform enclosure that is compliant with Open Rack v2 frame and get the necessary power through the singular bus bar located at the rear side.

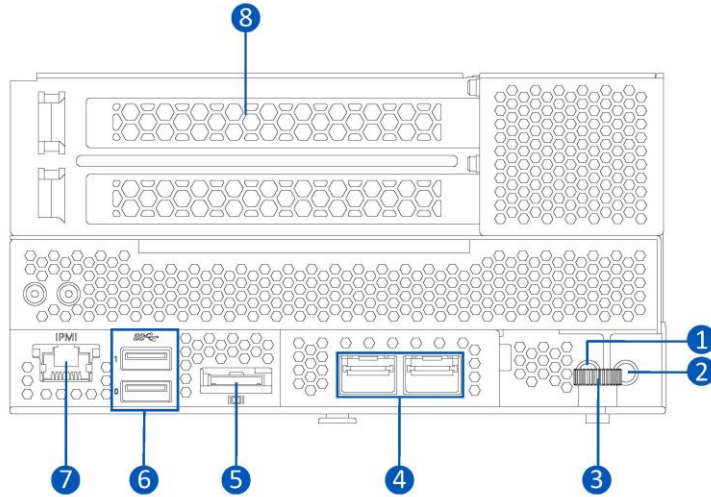


2.2 Specification

Processor	Intel® Xeon Scalable processor, TDP up to 165W
Chipset	Intel® C622
Memory	
Memory Type	DDR4 RDIMM/LRDIMM
Memory Slot Qty.	16
Total Memory Capacity	Supports up to 512GB (32GB per memory module)
Port and Connector	
USB	Two USB 3.0 ports (front side)
VGA	One VGA port (front side)
Mgmt	One RJ45 IPMI port (front side)
Expansion Slot	Option 1: Two PCIe Gen3 x16 FHFL Option 2: One PCIe Gen3 x16 HHHL + Two PCIe Gen3 x8 HHHL
OCP Slot	One OCP card, OCP2.0 x16 slot on the motherboard
Storage Drive	One SATA/PCIe x4 M.2 card on the motherboard
Power	Centralized OCP Power Shelf, compliant with Open Rack v2
Physical	
Dimension	830mm (L) × 537mm (W) × 95.2mm (H)
Product Weight	Full configuration: 7kg Cubby weight: 15kg (one cubby is available for 3 compute sleds)
Environmental	
Operating Temperature	5°C - 35°C (41°F - 95°F)
Storage & Transportation Temperature	-40°C - 60°C
Operating Humidity	20% - 80% relative humidity
Storage & Transportation Humidity	20% - 93% (40°C) relative humidity

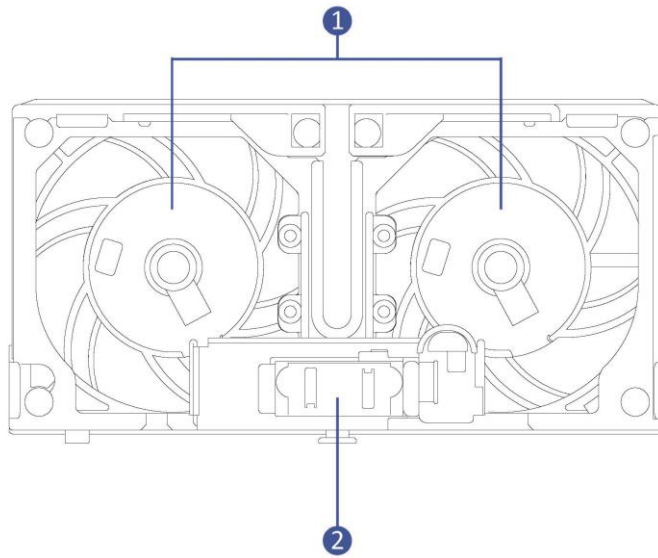
3. Product Overview

3.1 Front View



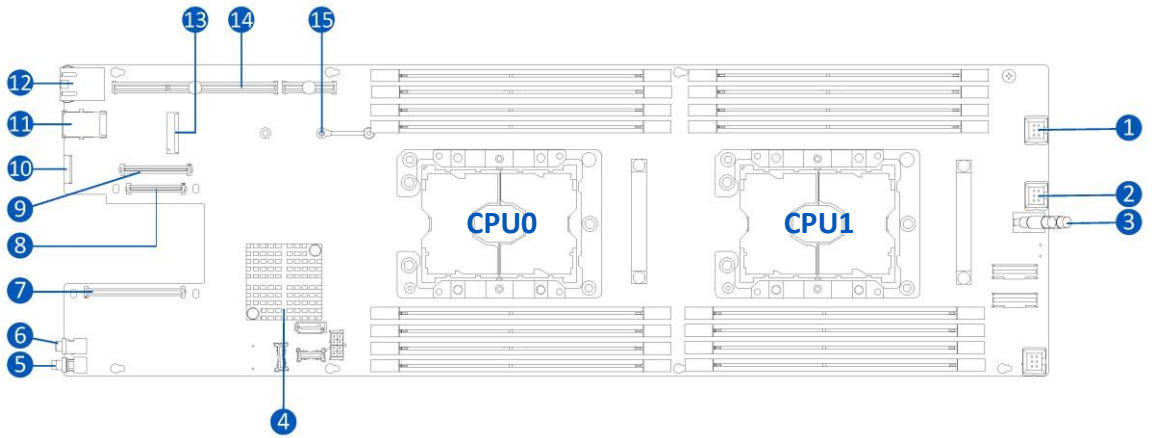
#	Item
1	UID Button with LED
2	Power Button
3	Thumb Screw (for Cubby)
4	OCP Connector (x2)
5	VGA Port
6	USB 3.0 Port (x2)
7	IPMI Port
8	PCIe Riser-Card Module

3.2 Rear View



#	Item
1	Fan Module (x2)
2	Power Connector

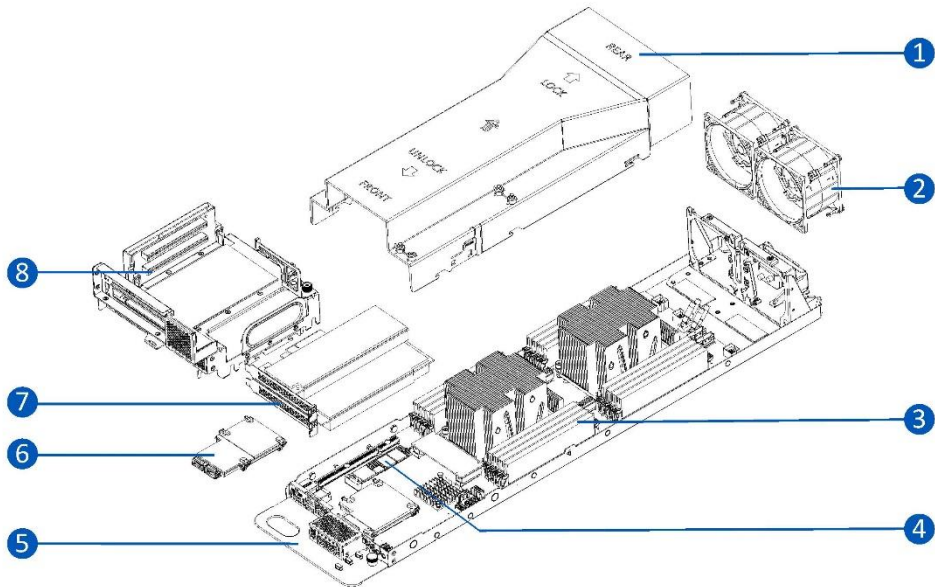
3.3 Motherboard View



#	Item	#	Item
1	Fan Connector	9	OCP Slot B
2	Fan Connector	10	VGA Port
3	Power Connector	11	USB 3.0 Port (x2)
4	PCH	12	IPMI Port
5	Power Button	13	M.2 Card Slot
6	UID Button	14	PCIe Riser Slot
7	OCP Slot A	15	M.2 Card Snap Clip
8	OCP Slot C		

3.4 Exploded Diagram

The following illustration shows the major components in the server.



#	Item
1	Air Baffle
2	8056 Fan Module (x2)
3	DIMM Module (x16)
4	M.2 Card
5	Base with Motherboard
6	OCP Card
7	PCIe Card
8	PCIe Riser Module

4. Getting Started

4.1 Package Contents

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


The contents of the server shipping carton include:

- Cubby
- Compute Sled (containing commodities)

4.2 Power On/Off


To power on and off the server, press the **Power** button.


To complete shut-down the server, press the **Power** button and disconnect the power cord from the server.

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

4.3 Pre-disassembly Instructions

Read the installation instructions for all the hardware operations before disassembling or re-assembling the components. All prerequisites must be completed prior to starting the installation or maintenance procedure.

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

Do the following prior to starting any the installation or maintenance procedure.

1. Shut-down the server.
2. Remove all cables from the system.
3. Remove the node server from the rack. For more information on removing the node server, see [Open Rack Server Installation Guide](#).

4.4 Disassembly/Reassembly Process

NOTE:

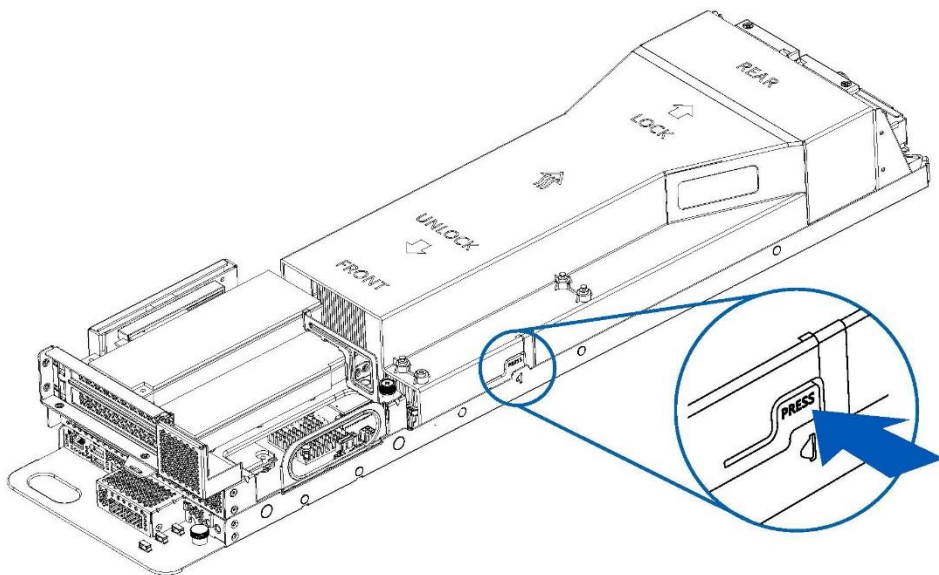
- During installation or removal of any hardware, always ensure all data is backed up properly.
- Disconnect any cables from the server.
- Disconnect the server and all attached devices from their electrical outlets.

Item appearance may be different on actual models.

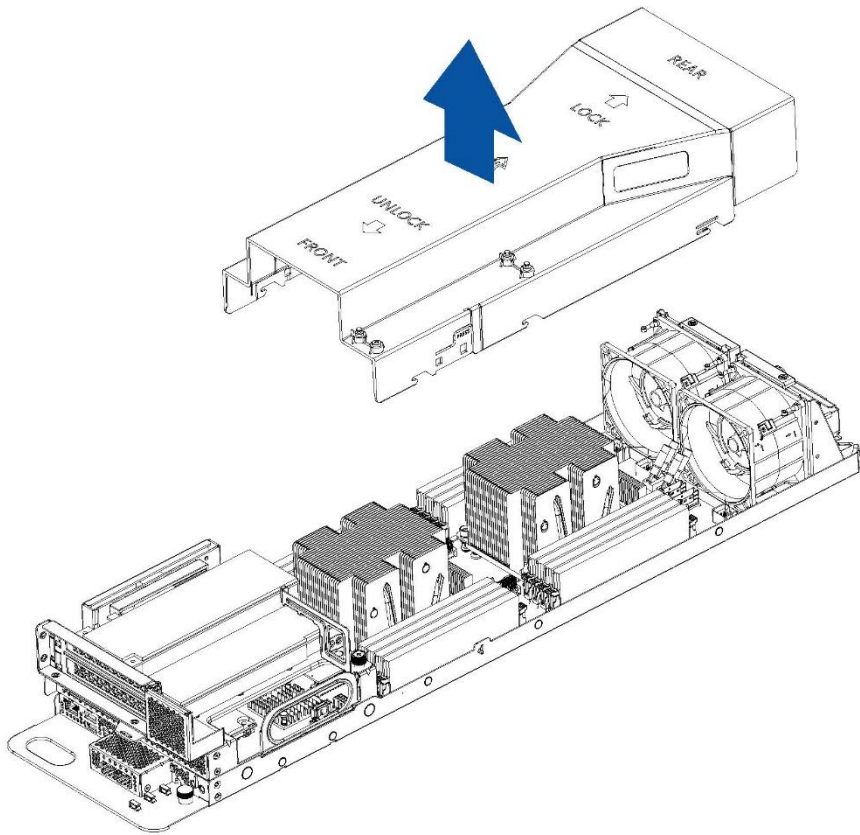
4.4.1 Air Baffle Replacement

CAUTION: For proper cooling, do not operate the server without the air baffle or fan installed.


1. Press the locking tab on both sides of the server simultaneously.



2. Once the locking tabs are released from the server, remove the air baffle.

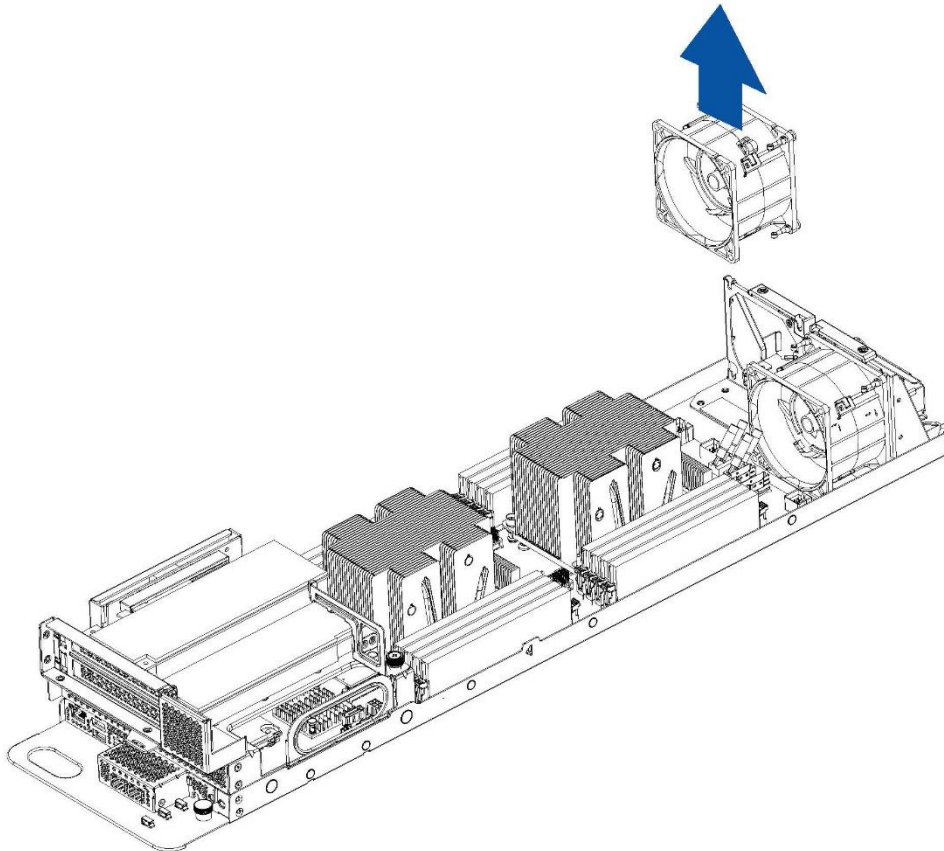


3. Follow the preceding steps to install the air baffle.

 **NOTE:** Make sure that both locking tabs are firmly secured on the server base when installing the air baffle.


4.4.2 Fan Module Replacement

1. Remove the air baffle (Refer to [Air Baffle Replacement](#)).
2. Disconnect the fan cable from the motherboard connector.
3. Lift up and remove the fan module.




4. Follow the preceding steps to install the fan module.

4.4.3 DIMM Replacement

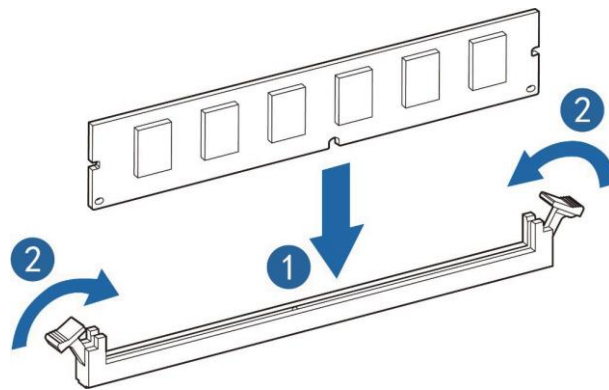
 **WARNING:** Always wear an electrostatic-discharge strap or gloves when removing or installing DIMM modules.

1. Remove the air baffle (Refer to [Air Baffle Replacement](#)).
2. Locate the DIMM slot (see the [DIMM slot layout](#)). Determine which DIMM you want to replace.
3. Carefully open the retaining clips on both end of the DIMM slot.

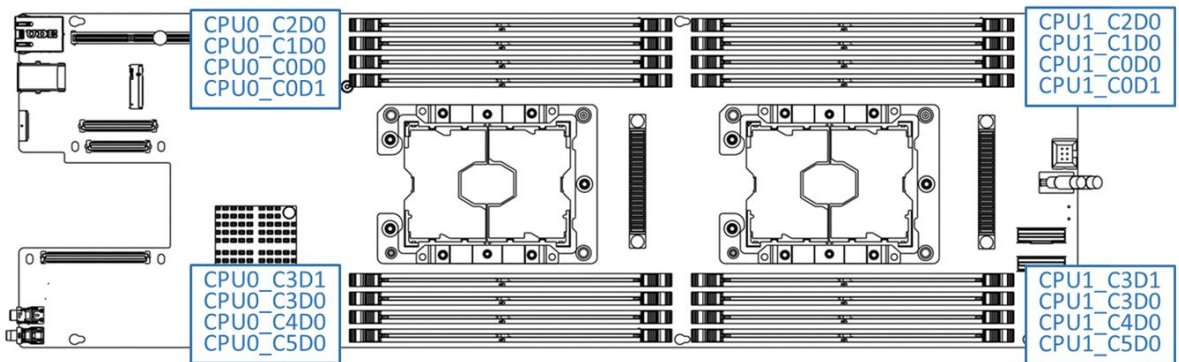
 **NOTE:** Make sure that both retaining clips on the DIMM slot are in the fully-open position.

4. Gently lift and remove the DIMM from the slot.
5. Install the DIMM in the order of DIMM population sequence (see the [DIMM population sequence](#)). Align the golden key of the DIMM with the receptive point on the slot.
6. Insert and gently press down the DIMM into the slot until the retaining clips snap into the locked position.

NOTE: Make sure that retaining clips engage the notches on the DIMM. If the retaining clips are not in the fully-closed position, the DIMM has not been correctly installed. Press the DIMM firmly into the slot again until the retaining clips are fully seated.



DIMM slot layout:



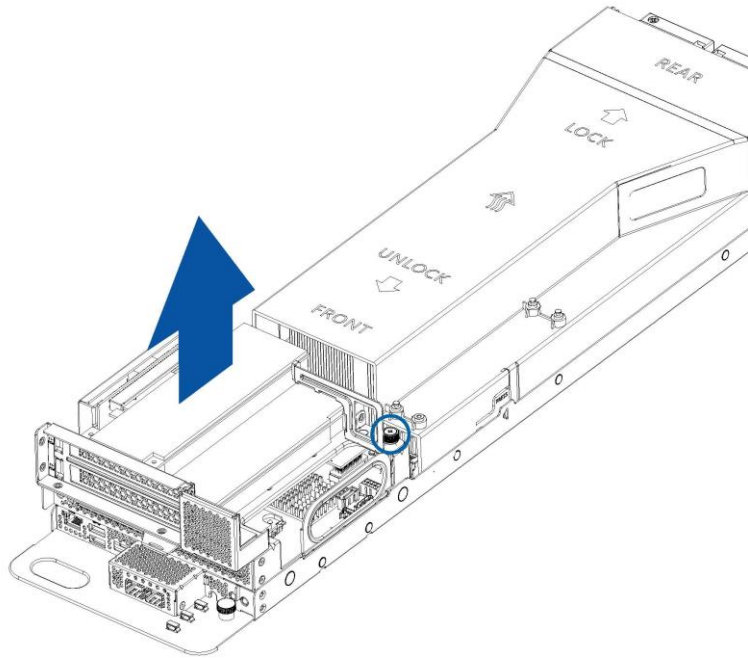
DIMM population sequence:

- The white slots take the priority, while CPU1 DIMM shall be symmetrically installed with CPU0 DIMM.
- For the single CPU, the DIMM population follows the screen printed sequence: CPU0_COD0, CPU0_C1D0, CPU0_C2D0, CPU0_C3D0, CPU0_C4D0, CPU0_C5D0; CPU0_COD1, CPU0_C3D1.

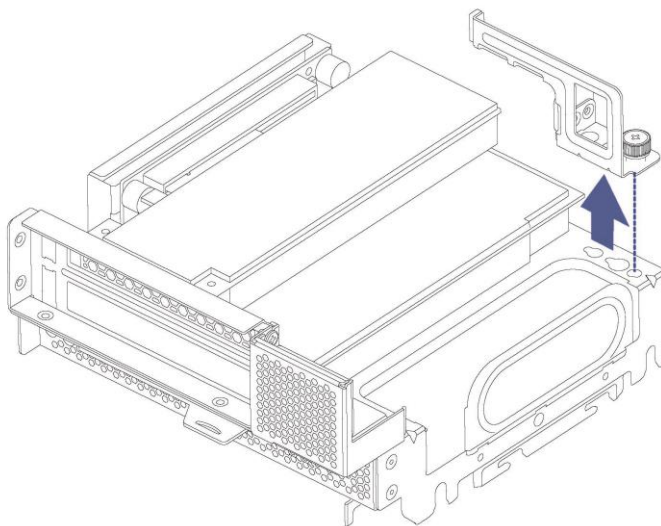
- For dual CPUs, CPU0 DIMM population follows the screen printed sequence: CPU0_C0D0, CPU0_C1D0, CPU0_C2D0...; CPU1 DIMM population follows the screen printed sequence: CPU1_C0D0, CPU1_C1D0, CPU1_C2D0.

4.4.4 PCIe Riser-Card Assembly Replacement

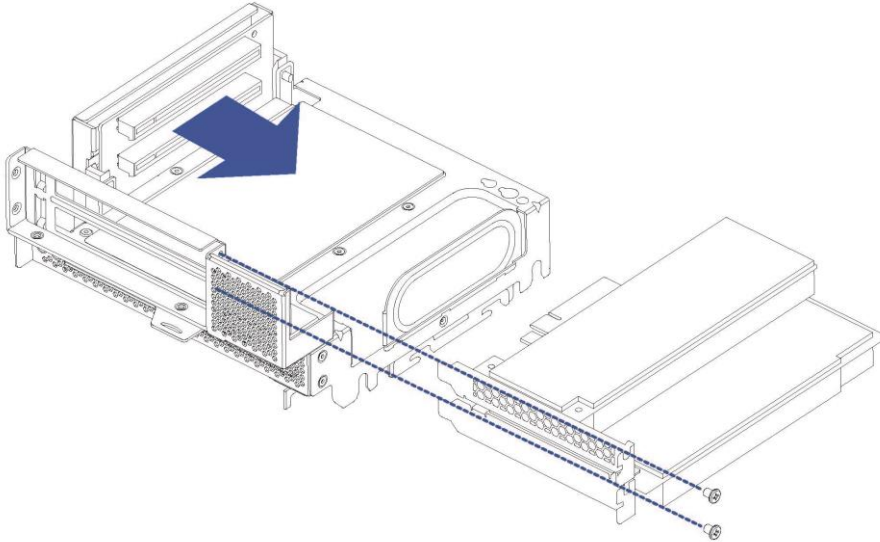
1. Loosen the screw securing the PCIe riser-card assembly to the motherboard.
2. Lift up and remove the PCIe riser-card assembly from the motherboard connector.




3. Remove the PCIe riser securing bracket from the PCIe riser module.



4. Remove the two screws securing the PCIe card in place.
5. Remove the PCIe card from the PCIe riser module.

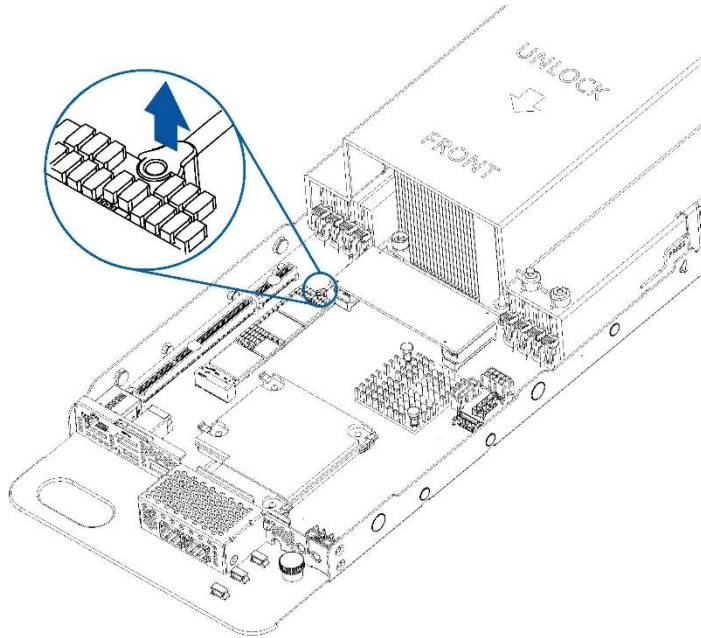


6. Follow the preceding steps to install the PCIe riser-card assembly.

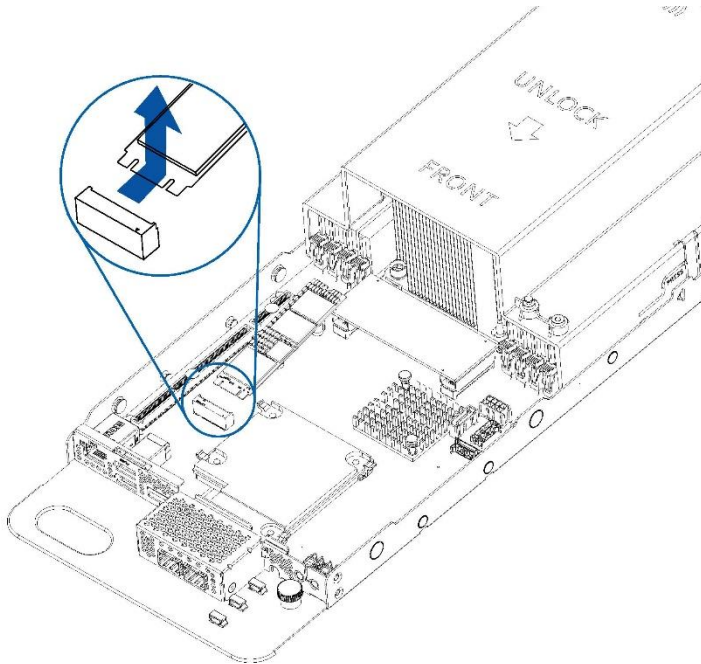
 **NOTE:** Make sure that the PCIe riser-card assembly is firmly connected to the motherboard connector before tightening the screw to secure the PCIe riser-card assembly in place.

4.4.5 M.2 SSD Replacement


1. Remove the PCIe riser-card assembly (Refer to [PCIe Riser-Card Assembly Replacement](#)).
2. Using your fingers, gently pull up the snap clip.



3. Remove the M.2 SSD from the motherboard connector.



4. Follow the preceding steps to install the M.2 SSD.

 **NOTE:** Make sure that the snap clip is fully engage with the notch on the SSD. If the snap clip is not in the fully-closed position, the SSD has not been correctly installed. Press the snap clip firmly into the notch again until the SDD is fully secured in place.

5. Setup

This chapter describes the information on the operational requirements and additional driver information of Inspur ON5263M5 server.

5.1 Operational Requirements

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

5.1.1 Space and Airflow

To allow for servicing and adequate airflow, it is recommended to use the following space and airflow suggestions when deciding where to install a rack:

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

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

CAUTION:


- To prevent improper cooling and damage to the equipment, do not block the ventilation openings.
 - Always use blanking panels to fill empty vertical spaces in the rack. When the rack is not filled by a server or rack component, the gaps between the components cause changes in airflow through the rack and across the servers. Cover all gaps with blanking panels to maintain proper airflow.
-

If a third-party rack is used, it is recommended to use the following additional requirements to ensure adequate airflow and to prevent thermal damage to the server and rack component:

- Front and rear doors—If the rack includes the closed front and rear doors, you must allow 5,350 square centimeters (830 square inches) of holes evenly distributed from top to bottom to permit adequate airflow (about 64% open area for ventilation).
- Side—The clearance between the installed rack component and the side panels of the rack must be a minimum of 7 cm (2.75 in).

5.1.2 Temperature


It is recommended that the ambient operating temperature is 5°C-35°C (41°F -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 the third-party racks, do not permit optional equipment to impede airflow around the server or to increase the internal rack temperature beyond the maximum allowable limits.

5.1.3 Power

Any installation procedures must comply with local and regional electrical regulations governing the installation of information technology equipment by licensed electricians.

Inspur Servers are 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 provided 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 into the rack, you may need to use additional power distribution devices to provide power to all devices. Observe the following guidelines:

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

5.1.4 Electrical Grounding

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 non-detachable 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 Downloading the Drivers

For the information on downloading the latest drivers, firmware, documentations, go to Inspur website: <https://en.inspur.com/eportal/ui?pagelId=2490734>.

6. BIOS Settings

Inspur ON5263M5 server is UEFI BIOS. UEFI (Unified Extensible Firmware Interface) defines the interface between the operating system and firmware during the boot or startup process. The UEFI BIOS program is integrated into the motherboard chip. Its main functions include power-on, self-test, CPU/memory initialization, detection of input and output devices and bootable devices to finally boot the operating system.

The BIOS development of Inspur ON5263M5 is based on AMI Codebase, supporting Legacy and UEFI operating environments with in-band and out-of-band configurations and its flexibility and scalability is to meet various customized needs.

The main features are:

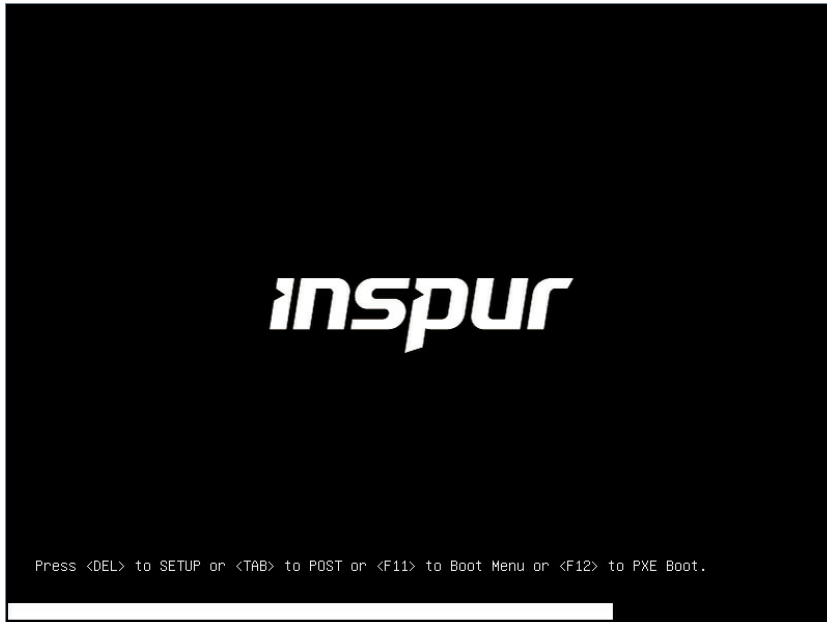
- Supports BIOS configuration utilities in Chinese and English
- Supports high-capacity hard drives, and boot partitions are larger than 2.2 TB.
- Supports UEFI Shell, providing a pre-boot environment for running scripts and tools.
- Supports UEFI Secure Boot, Intel TXT, Boot Guard and other security technologies, with a stronger security performance.

NOTE:

- Before changing the BIOS settings, please backup all the original settings. When the system works abnormally due to the modifications, you can restore it with the backups.
 - The default settings of the system are usually the optimal settings. Please do not attempt to make changes without the understandings of the BIOS parameters.
 - This chapter describes the common settings in general. The options that are rarely used in BIOS setting will be given a brief introduction.
 - The content of the BIOS will vary depending on the actual configuration of products.
-

6.1 Basic Operations

To enter the BIOS Setup, press the key to SETUP or the <TAB> key to POST or the <F11> key to Boot Menu or the <F12> key to PXE Boot during boot time when the OEM or Inspur Logo Screen is displayed.



When “Entering Setup ...” appears in the lower right corner of the screen, the system enters to the BIOS Main Menu. In the BIOS Setup Menu, you can use the arrow keys to navigate through the BIOS menu and item, press the **Enter** key to enter the submenus.

Other hotkeys function :

1. Press **F2** to enter BIOS Setup Menu.
2. Press **TAB** to display the system information during POST.
3. Press **F11** to enter the boot management menu.
4. Press **F12** to enter the Preboot eXecution Environment (PXE).

Table 6-1 BIOS Setup Control Key Instruction Table

Key	Function
<Esc>	Exit or return from submenu to main menu
<<-> or <->>	Select a menu
<↑> or <↓>	Move the cursor up or down
<Home> or <End>	Move the cursor to the top or bottom of the screen
<+> or <->	Select the previous or next numerical value or setting of the current one
<F1>	Help
<F2>	Restore to the last configuration
<F9>	Restore to the default configuration
<F10>	Save and exit
<Enter>	Execute commands or select a submenu
<K> or <M>	Scroll up/down the help information area

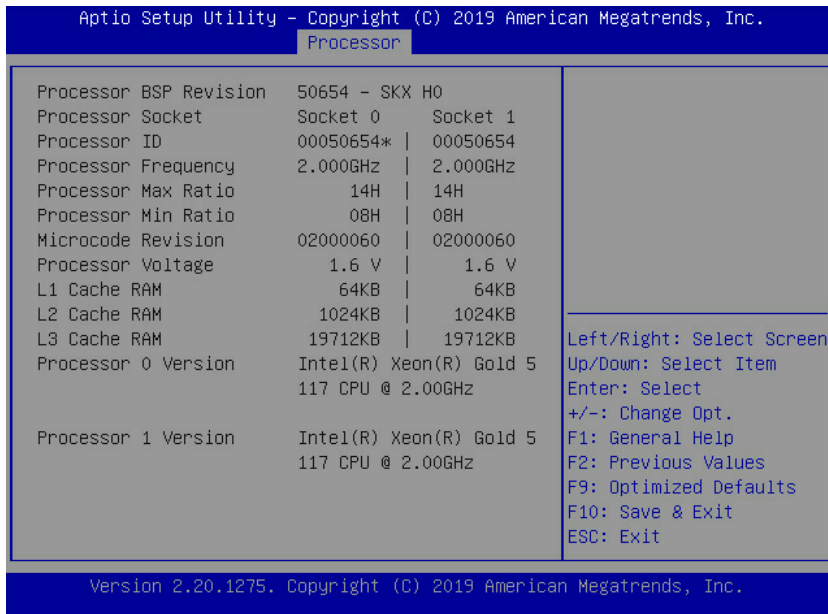
NOTE: Options grayed-out are not available. Options with symbol “▶” have a sub-menu.

6.1.1 System Information

To view the system information, login to the BIOS Setup Menu and select “**Main**”. The Main menu displays the current system information, including BIOS/BMC/ME version, CPU/PCH SKU/RC version, memory and other information. For more information on Main menu, see [6.2.1 Main](#).

6.1.2 CPU Information

To view the CPU information, login to the BIOS Setup Menu and select “**Processor** → **Processor Configuration** → **Processor Information**”. For more information on CPU, see [6.2.4.1 Processor Configuration](#).



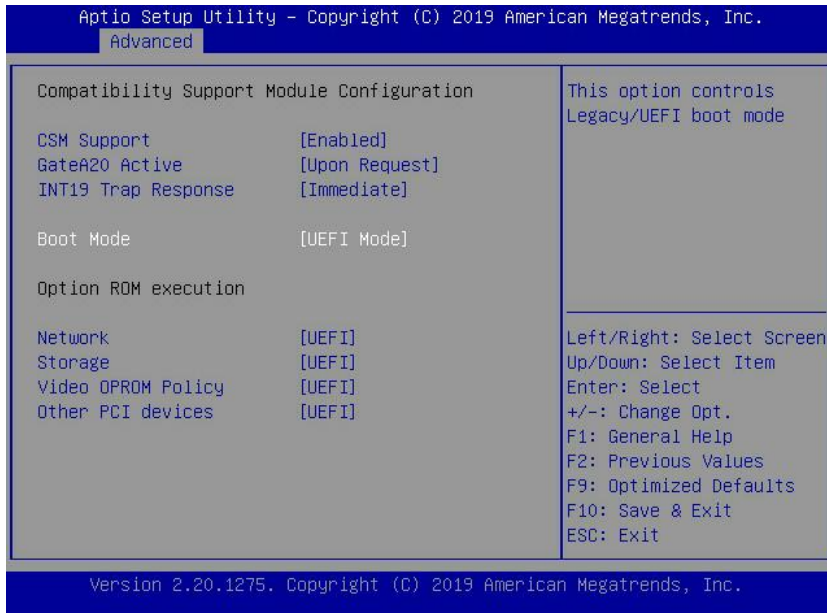
6.1.3 Memory Information

To view the memory information, login to the BIOS Setup Menu and select “**Processor** → **Memory Configuration** → **Memory Topology**”. For more information on memory, see [6.2.4.4 Memory Configuration](#).

6.1.4 UEFI/Legacy Mode

To set the Boot Mode (UEFI Mode/Legacy Mode):

1. Login to the BIOS Setup Menu, select “**Advanced** → **CSM Configuration**” and press **Enter**.
2. Press <+> or <-> to change the Boot Mode to [UEFI Mode] or [Legacy Mode]. The options under the *Option ROM execution* also need to set to [UEFI Mode] or [Legacy Mode].



The default setting of Boot Mode for Inspur ON5263M5 server is [UEFI Mode]. The advantages of UEFI mode are, it supports boot from the GPT disk, supports IPv6/IPv4 PXE boot, and provides UEFI Shell environment.

If the Boot Mode is set to [Legacy Mode], the options under the *Option ROM execution* (Network, Storage, Video OPROM Policy and Other PCI devices) must set to [Legacy Mode] as well.

If the Boot Mode is set to [UEFI Mode], the options under the *Option ROM execution* (Network, Storage, Video OPROM Policy and Other PCI devices) are suggested to set to [UEFI Mode]. If there are special requirements, it can be set to [Legacy Mode].

6.1.5 RAID Volume Configuration

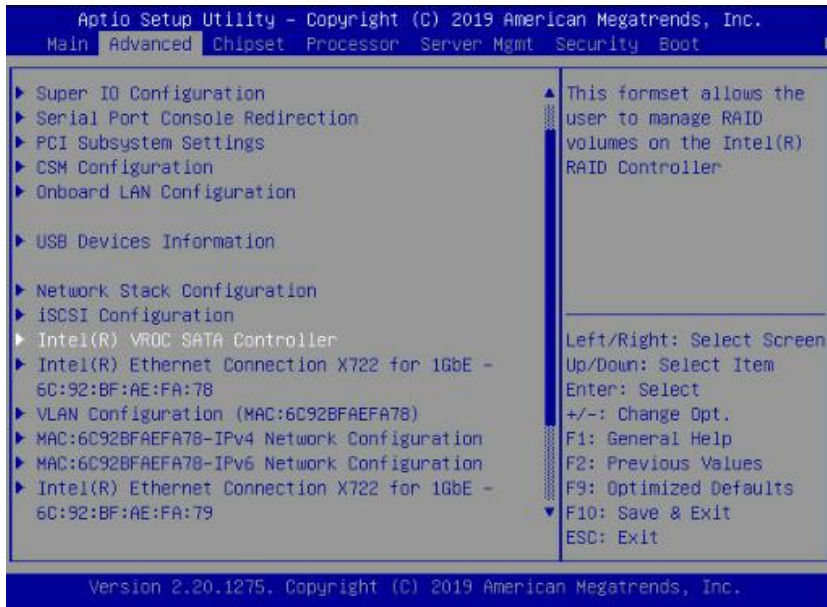
To view the HDD information, login to the BIOS Setup Menu and select “**Chipset** → **PCH SATA Configuration (PCH sSATA Configuration)**”. For more information on HDD, see [6.2.3.1 PCH SATA/sSATA Configuration](#).

The default setting for *SATA Mode Options* is [AHCI], the SATA controller enables its AHCI functionality. The RAID functions are disable and the RAID setup utility cannot be accessed at boot time.

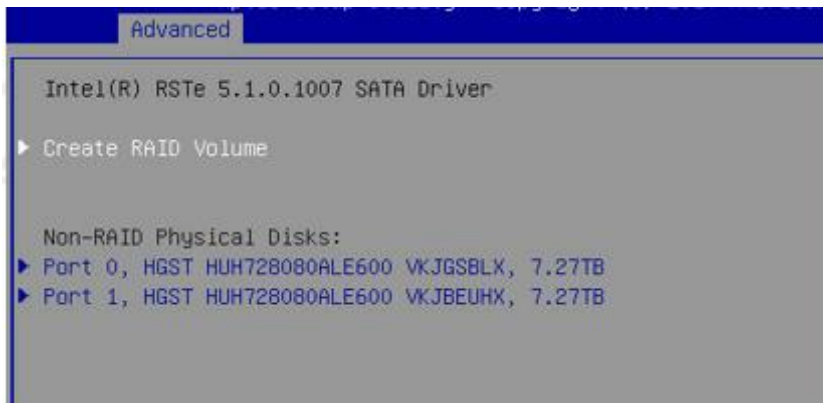
To create a RAID volume under UEFI Mode:

NOTE: This action is available when *SATA Controller* is set to [Enabled] and *SATA Mode Options* is set to [RAID].

1. Login to the BIOS Setup Menu.
2. Select “**Chipset → PCH SATA Configuration/PCH sSATA Configuration → SATA Mode Options**” and press +/- to change the item to [RAID].
3. Press F10 to save & exit the BIOS Setup. The system will reboot automatically.
4. Login to the BIOS Setup Menu, select “**Advanced → CSM Configuration → Boot Mode**”, and press +/- to change the item to [UEFI].
5. When the *Boot Mode* is set to [UEFI], the Intel(R) VROC SATA Controller menu appears on the Advanced menu. Press **Enter** to show the HDD information.



6. Press **Enter** to create a RAID volume.



7. Using the following instructions in Table 6-2 to create the RAID Volume.

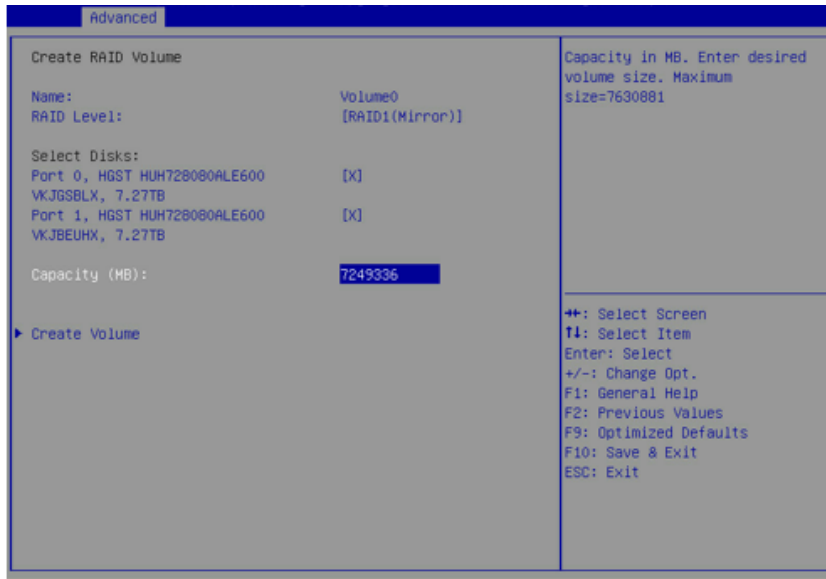


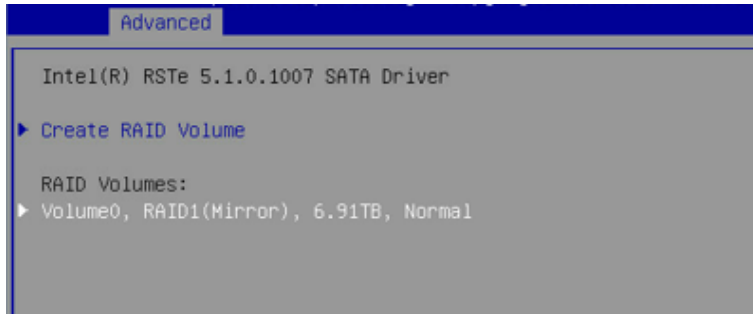
Table 6-2 Creating a RAID Volume in UEFI Mode

Parameter	Description
Name	Enter a volume name less than 16 characters without containing any special characters.
RAID Level	Select the RAID volume level. Options: <ul style="list-style-type: none"> RAID0 (Stripe): This RAID volume is allowed to be made on 2 or more than 2 HDDs. RAID1 (Mirror): This RAID volume is allowed to be made on 2 HDDs. RAID10 (RAID0+1): 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 more than 3 HDDs.
Select Disks	Select which HDDs to make the RAID volume.
Capacity	Set the volume capacity. When highlight this item, the maximum capacity is shown in the Help area on the right side.
Create Volume	After finishing the above settings, select this item to create RAID volume.

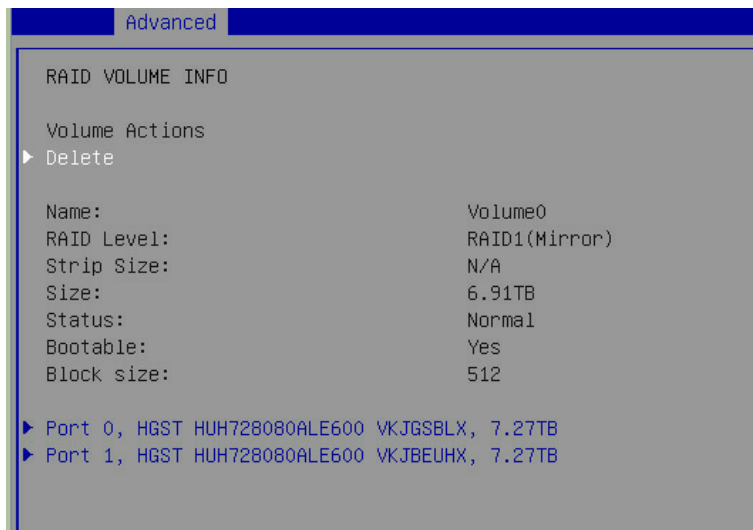
If a RAID Volume has not previously been created, it will be necessary to press <F10> to Save & Exit and reboot after creating a RAID Volume in BIOS Setup.

To delete a RAID Volume under UEFI Mode:

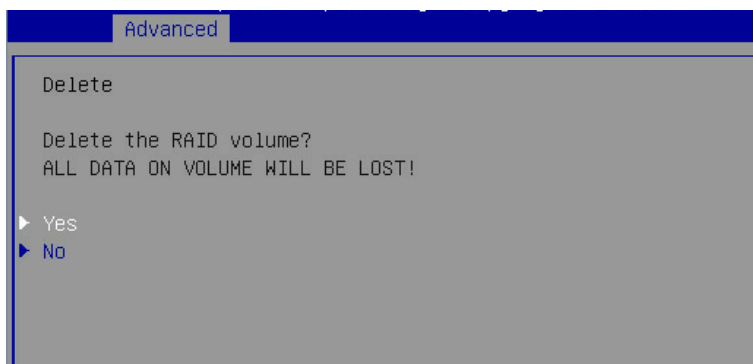
1. After creating a RAID Volume successfully, the RAID Volume information will appear on “**Advanced** → **Intel(R) VROC SATA Controller**” menu. Press **Enter** to show the detailed information



2. Press **Enter** to delete the RAID Volume.



3. Confirm the deletion action.



To Create a RAID Volume under Legacy Mode:

1. Login to the BIOS Setup Menu, select “**Advanced** → **CSM Configuration** → **Boot Mode**”, and press +/- to change the item to [Legacy].
2. Press **F10** to save & exit the BIOS Setup. The system will reboot automatically.
3. Press the <CTRL> + <I> keys to enter the SATA RAID configuration when “Press <CTRL>-> I to enter Configuration Utility...” message appears.

```

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

RAID Volumes:
None defined.

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

4. The SATA RAID configuration interface shows 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).

```

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

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

[ DISK/VOLUME INFORMATION ]

RAID Volumes:
None defined.

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

[↑↓]-Select [ESC]-Exit [ENTER]-Select Menu
    
```

Table 6-3 SATA RAID Configuration Interface

Parameter	Description
Create RAID Volume	Create an RAID volume.
Delete RAID Volume	Delete an existed RAID volume.
Reset Disks to Non-RAID	Reset the HDDs in RAID volume, and restore them to non-RAID status.
Mark Disk as Spare	Mark the HDDs as spare disks. The data will be cleared, and those HDDs cannot be selected during RAID setting.
Exit	Exit SATA HostRAID configuration interface.

5. Using the following instructions in Table 6-4 to create a RAID Volume, and press **Create Volume**.

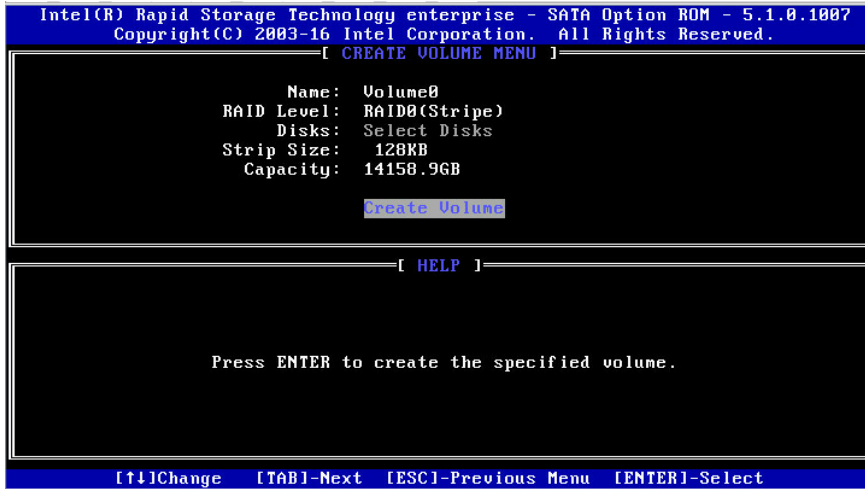
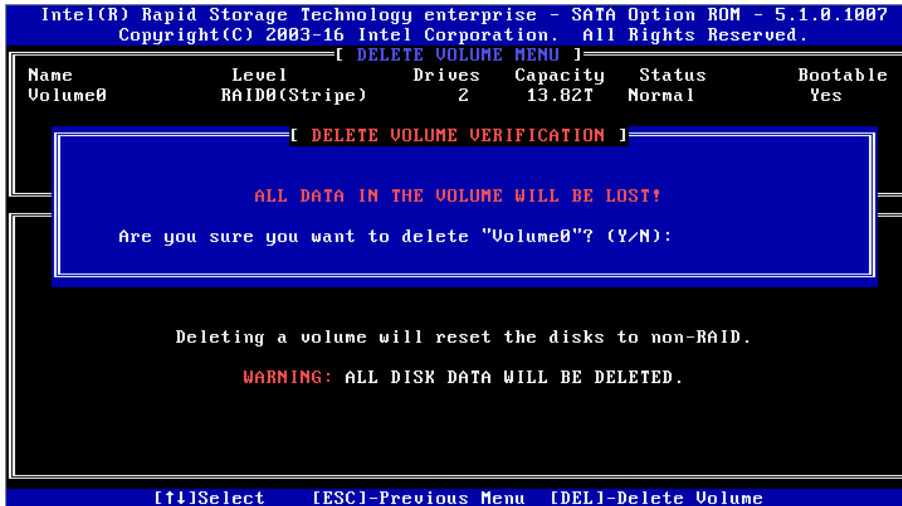


Table 6-4 Creating a RAID Volume in Legacy Mode

Parameter	Description
Name	Enter a volume name less than 16 characters without containing any special characters.
RAID Level	Select the RAID volume level. Options: <ul style="list-style-type: none"> RAID0 (Stripe): This RAID volume is allowed to be made on 2 or more than 2 HDDs. RAID1 (Mirror): This RAID volume is allowed to be made on 2 HDDs. RAID10 (RAID0+1): 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 more than 3 HDDs.
Select Disks	Select which HDDs to make the RAID volume.
Strip Size	Select the strip size. Only RAID0 and RAID5 volumes could enable this item.
Capacity	Set the volume capacity.

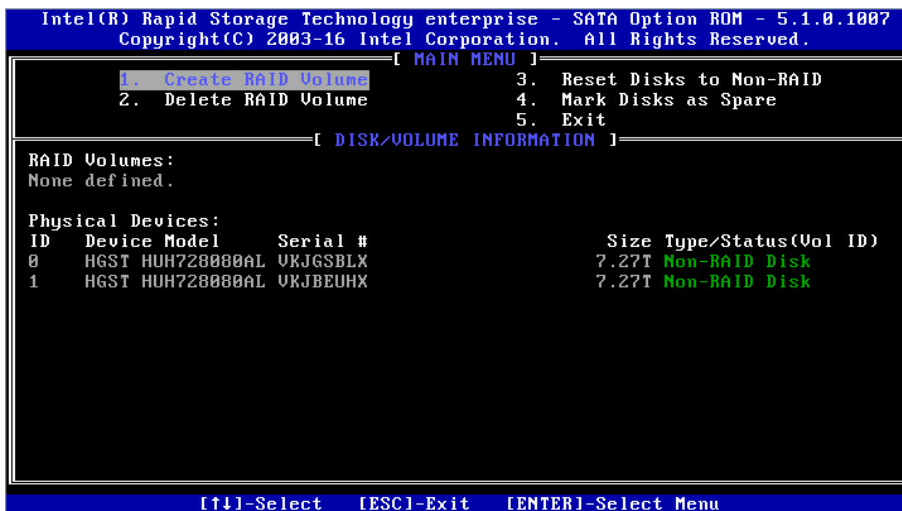
To delete a RAID Volume under Legacy Mode:

1. After creating a RAID Volume successfully, the RAID Volume information will appear on SATA RAID configuration interface. Select **Delete RAID Volume** and press **Enter**.
2. Press **Del** to delete the selected RAID Volume.
3. Confirm the deletion action.

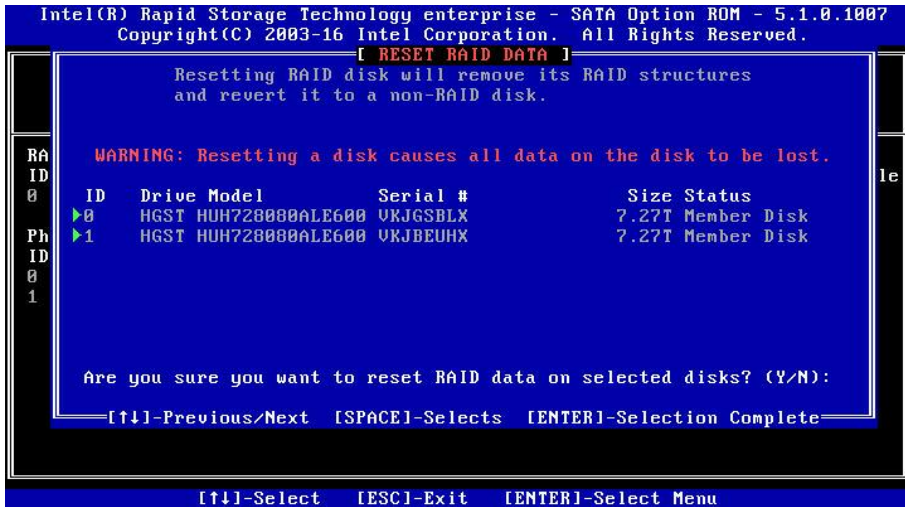


To reset the HDD Disks to Non-RAID Volumes under Legacy Mode:

1. Use the <↑> or <↓> keys to select **Reset Disks to Non-RAID** and press **Enter**.




2. Use the space key to select the HDD to be reset, and press **Enter** to reset the selected HDD.
3. Confirm the deletion action.

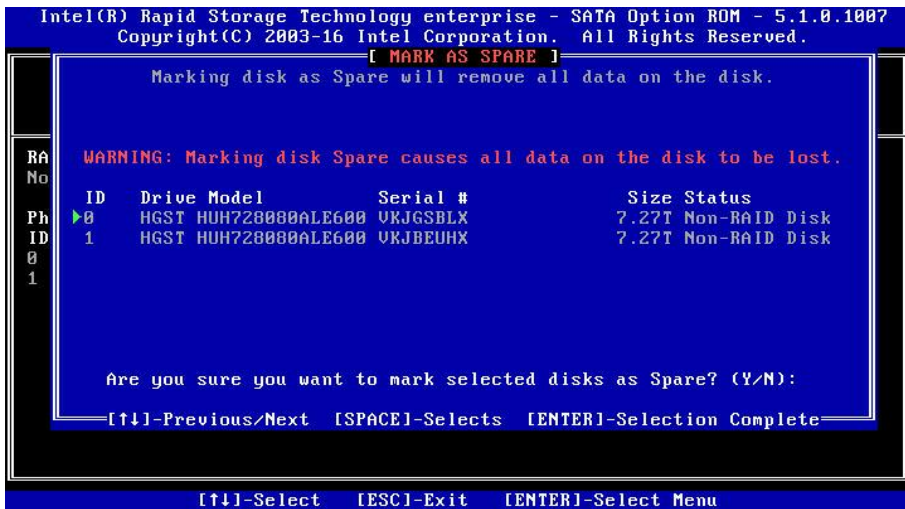


To mark the HDD Disks to spare HDDs under Legacy Mode:

1. Use the <↑> or <↓> keys to select **Mark Disks as Spare** and press **Enter**.
2. The non-RAID HDDs will be displayed on the screen. Use the space key to select the HDD to be marked as spare, and press **Enter**.

 **NOTE:** All data on the marked disk will be lost as the spare disk.

3. Confirm the mark action.



6.1.6 Configuring the BMC Network

To view the current configuration of BMC IPv4 or BMC IPv6 network:

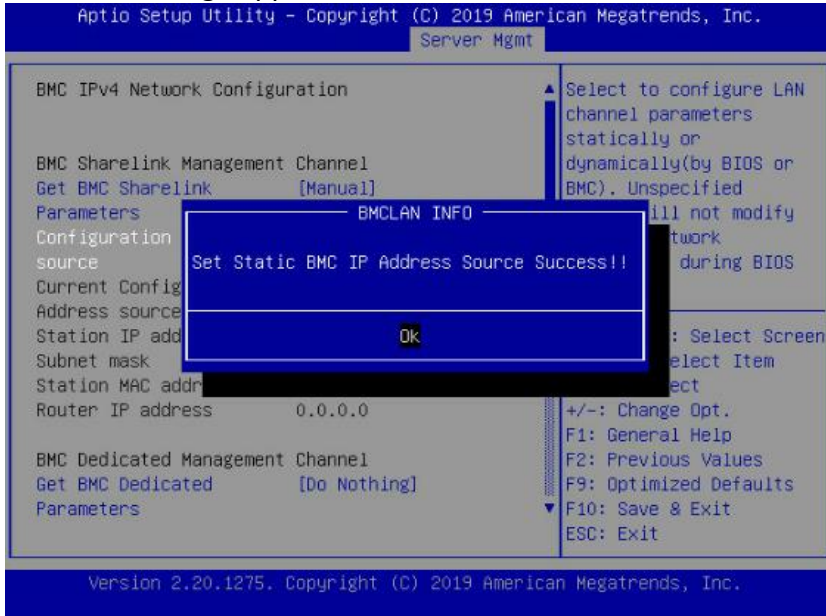
1. Login to the BIOS Setup Menu.
2. Select “**Server Mgmt → BMC Network Configuration BMC → IPv4 Network Configuration/BMC IPv6 Network Configuration**”.

Table 6-5 BMC Network Configuration

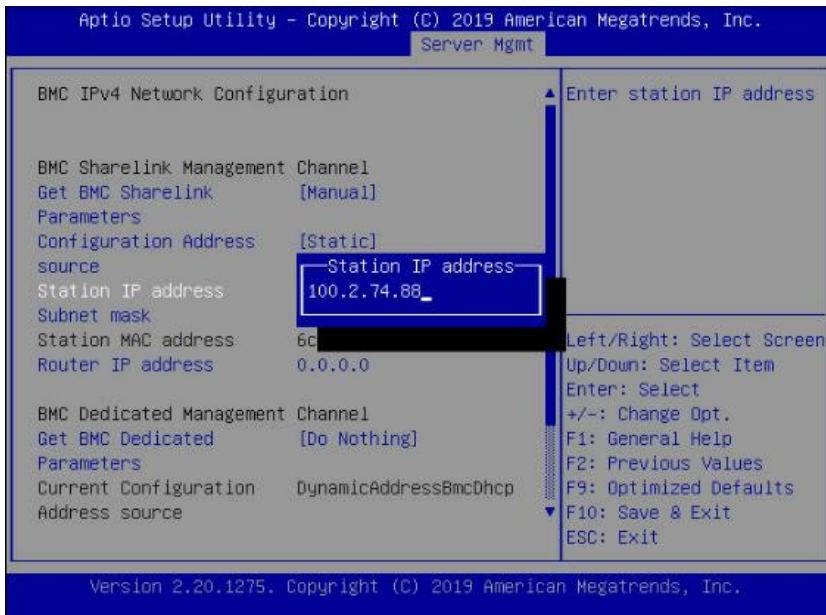
Parameter	Description	Default Setting / Format
Get BMC Sharelink Parameters / Get BMC Dedicated Parameters	<p>Set a method to get the BMC Sharelink / Dedicated Management Channel</p> <p>Options:</p> <ul style="list-style-type: none"> • Do Nothing • Auto: Automatically get the current BMC network Settings • Manual: Manually set the BMC network 	Do Nothing
Configuration Address Source	<p>Display the current BMC network parameters</p> <p> NOTE: This item is only available when <i>Get BMC Dedicated Parameters</i> is set to [Manual].</p> <p>Options:</p> <ul style="list-style-type: none"> • Unspecified: Unspecified option will not modify any BMC network parameters during BIOS phase. • Static: Statically obtain BMC network information • DynamicBmcDhcp: Dynamically obtain BMC network information <p> NOTE: Static and dynamic network parameter Settings take effect immediately.</p>	Unspecified
Station IP address	Display IP Address information	0.0.0.0
Subnet mask	<p>Display Subnet Mask information</p> <p> NOTE: The IP address must be in Hex format, for example, 6c-92-bf-a2-b8-c6.</p>	xx-xx-xx-xx-xx-xx
Station MAC address	Display the MAC Address information	0.0.0.0
Router IP address	Display the Router IP Address information	0.0.0.0

To configure the BMC Static network parameters:

1. Set the *Get BMC Sharelink Parameters* or *Get BMC Dedicated Parameters* to [Manual].
2. Set the *Configuration Address Source* to [Static]. The “Set Static BMC IP Address Source Success!!” message appears. Press **Enter** to continue.

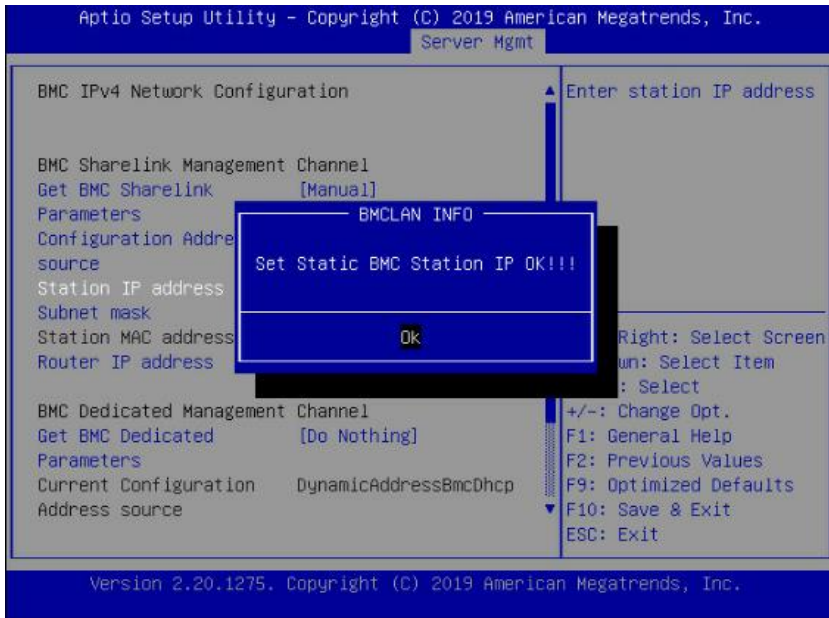


3. At the Station IP address prompt, type the station IP address, and then press **Enter**.

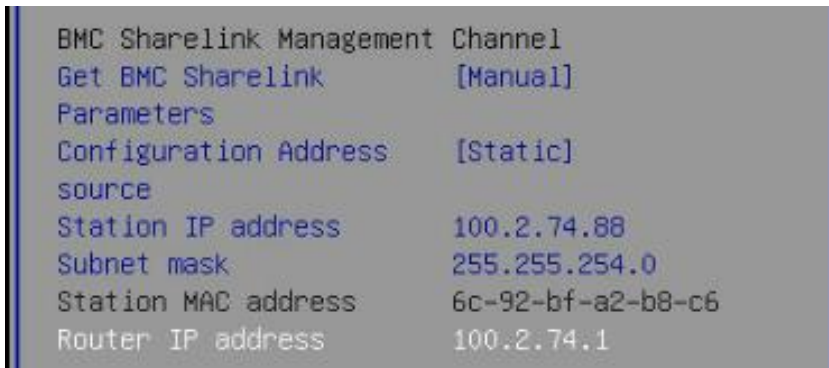


4. If the setting was successful, the “Set Static BMC Station IP OK!!!” appears. If the setting was failed, the “Set Static BMC Station IP Fail!!!” appears. If the IP address was the same, the “Static BMC Station IP Not Change!!!” appears. If the IP address was invalid, the “Invalid Station IP Entered!!!” appears, and the system will assign 0.0.0.0

to the Station IP address. This setting only changes the IP address in BIOS Setup interface, and does not notify BMC to change the IP settings.

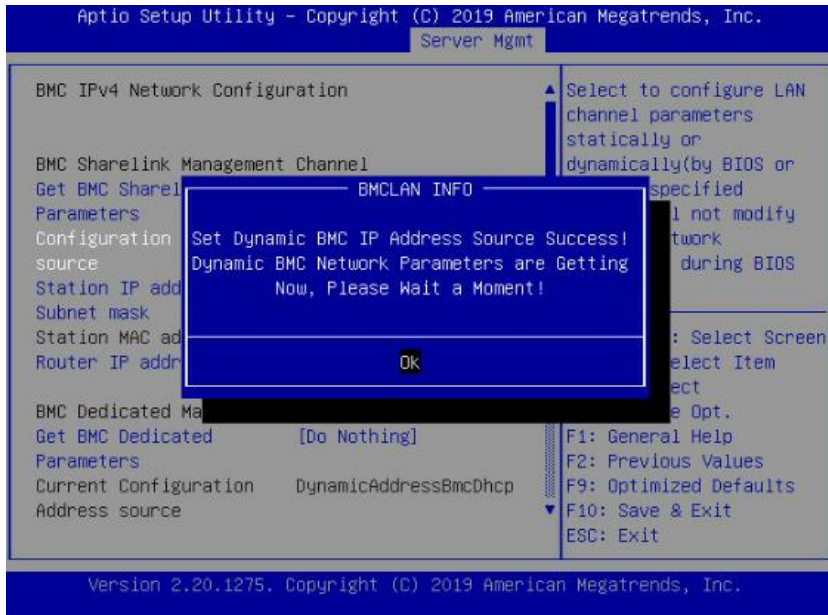


- Repeat step 3 and step 4 (on how to change the setting for Station IP address) to change the settings for Subnet mask, Station MAC address and Router IP address.

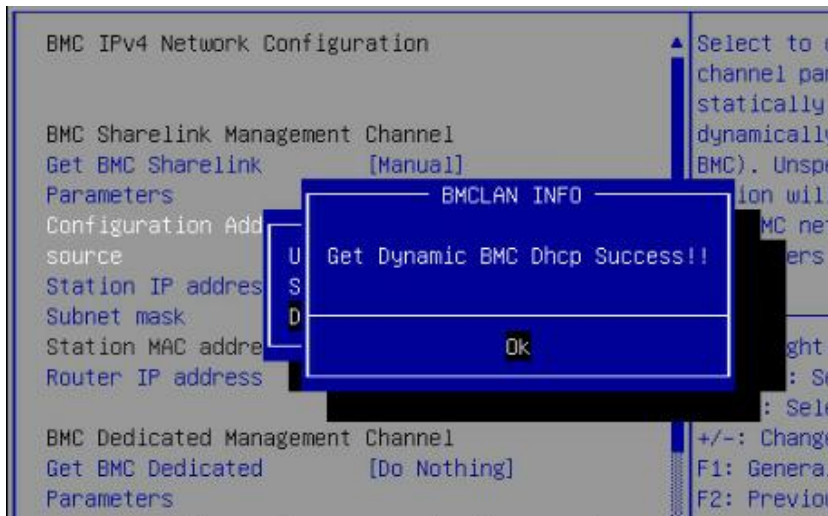


To configure the BMC Dynamic network parameters:

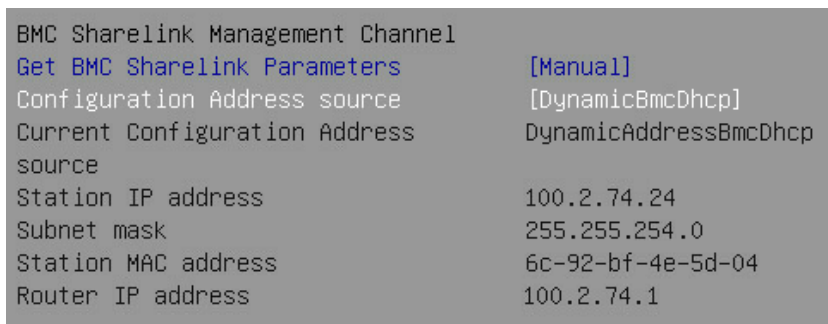
- Set the *Get BMC Sharelink Parameters* or *Get BMC Dedicated Parameters* to [Manual].
- Set the *Configuration Address Source* to [DynamicBmcDhcp]. The "Set Dynamic BMC IP Address Source Success!" message appears. Press **Enter** to continue.



3. Wait for 30 seconds, press **Enter** when the “Get Dynamic BMC Dhcp Success!!” appears.



4. The BMC network parameters (Station IP address, Subnet mask, Station MAC address, and Router IP address) will be set dynamically.



NOTE:

- Make sure that the BMC management port is connected to the network when configuring to the [Manual] options.
- The options that take effect immediately are implemented by the Callback function. Callback function is only activated when the options in the BIOS Setup are changed. For example, if you want to automatically get the BMC parameters again, the *Get BMC Sharelink Parameters* needs to be set to [Do nothing] or [Manual], then set to [Auto], the function will take effect. .

6.2 BIOS Setup Menu

To access the BIOS Setup Menu, press the key during the POST when the power is turned on. The following sections describe the eight BIOS Setup menu options: Main, Advanced, Chipset, Processor, Server Management, Security, Boot, and Save & Exit, respectively.

6.2.1 Main

The Main menu shows a summary of basic hardware information.



Table 6-6 BIOS Main Menu Option

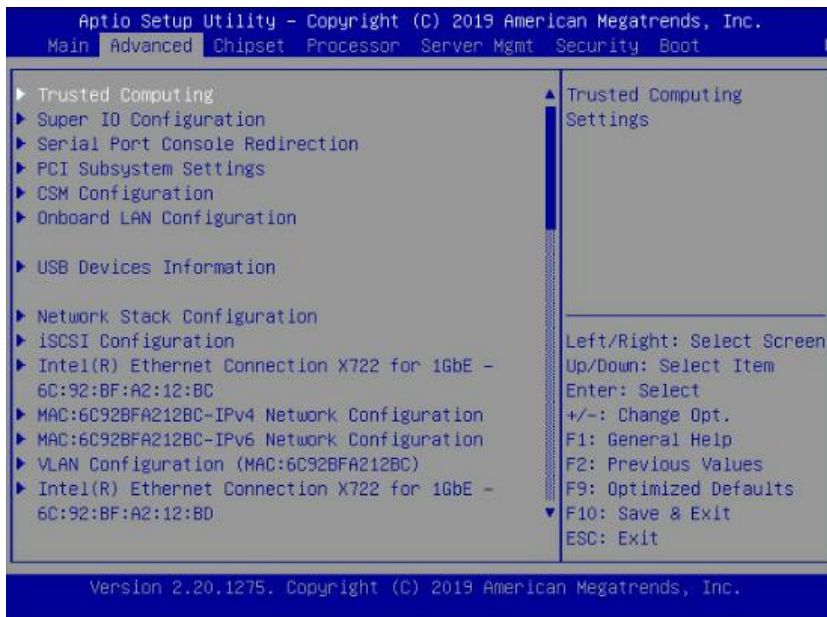
Parameter	Description
Product Name	Product name
Serial Number	Serial number
Customer ID	Customer ID
BIOS Version	System BIOS version

Parameter	Description
Build Date	The date and time when the BIOS Setup was created
BMC Firmware Version	BMC FW version information
ME Firmware Version	ME FW version information
Access Level	Current access level
CPU Type	Current CPU type
CPU Current Speed	Current CPU speed
PCH SKU	Current PCH SKU version
RC Revision	Current RC version information
DRAM Total Memory	The installed DRAM memory size
AEP Total Memory	The installed AEP memory size
System Memory Speed	The installed memory speed
System Language	Display and set the system language.
System Date (mm/dd/yyyy)	Display and set the system date.
System Time (hh/mm/ss)	Display and set the system time.

NOTE: Use **[Tab]** or **[Enter]** key to switch between system date and time, directly input the value or use +/- keys to change the value (Press + key, the value increases by 1, and press – key, the value decreases by 1).

6.2.2 Advanced

The Advanced menu allows the user to set BIOS system parameters and related function settings, such as ACPI, serial port, PCI subsystem, CSM, USB, or onboard NIC. To access the submenu item, press the **Enter** key



6.2.2.1 Trusted Computing

Enable or disable BIOS support for security device.

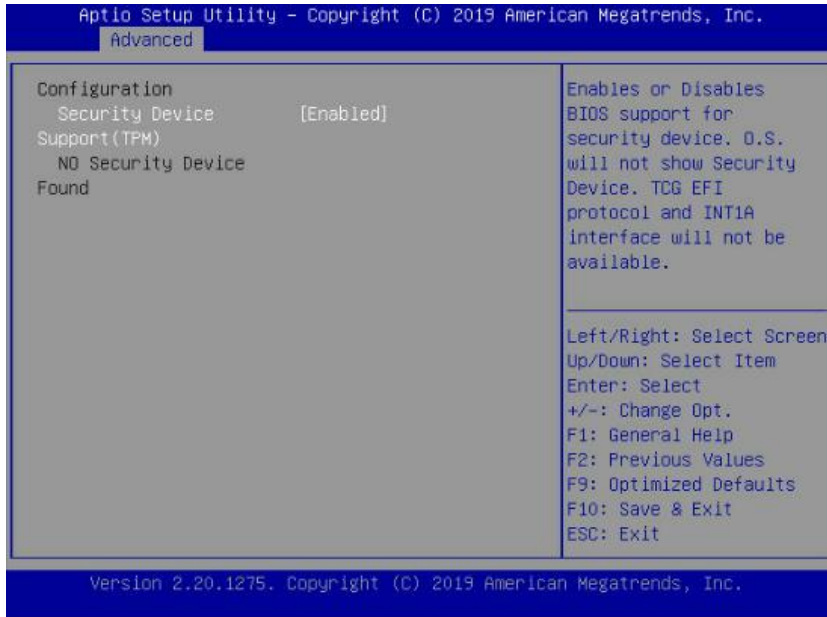


Table 6-7 Advanced > Trusted Computing

Parameter	Description	Default Setting / Format
Security Device Support (TPM)	Security device support settings. Options: Enabled/Disabled. NOTE: BIOS supports TPM TCG version 1.2/2.0. BIOS supports TPM module through TPM software binding, when the verification of software binding fails, BIOS will record the error to SEL.	Enabled
No Security Device Found	Display the status of security device. NOTE: This item is only available when the TPM chip is installed.	

6.2.2.2 Super IO Configuration

Set the super I/O chip information.

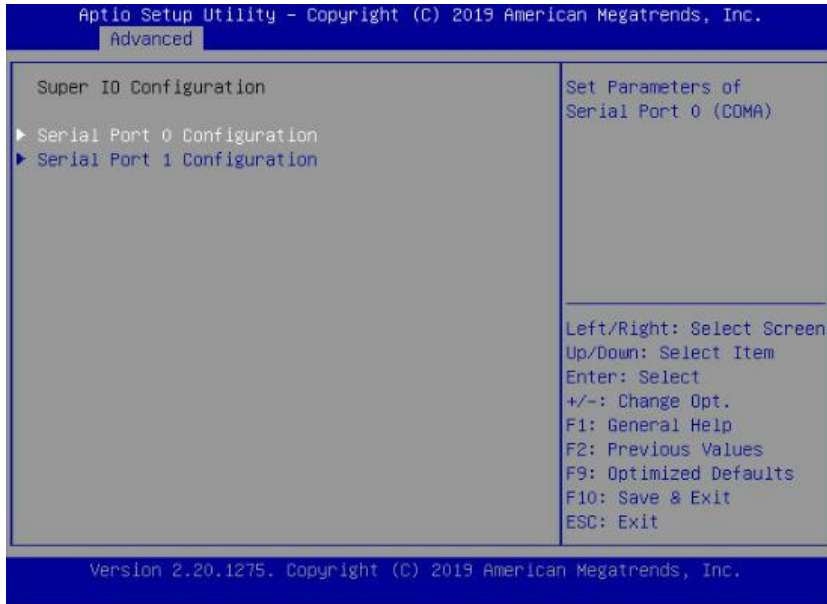


Table 6-8 Advanced > Super IO Configuration

Parameter	Description
Serial Port 0 Configuration	Press <Enter> for configuration of advanced items.
Serial Port 1 Configuration	Press <Enter> for configuration of advanced items.

Serial Port 0/1 Configuration enables/disables the Serial Port (COM). When set to [Enabled], allows the user to configure the Serial Port 0/1 settings. When set to [Disabled], displays no configuration for the Serial Port.

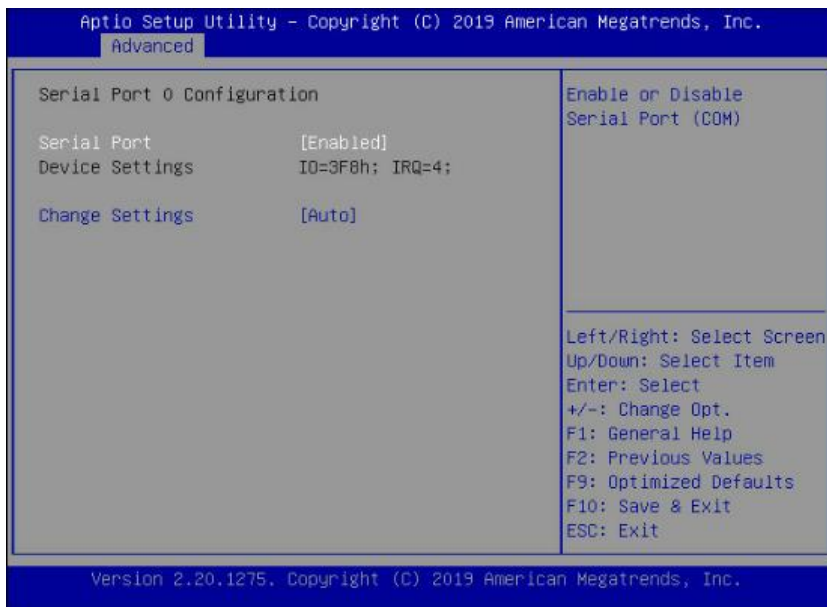


Table 6-9 **Advanced > Super IO Configuration > Serial Port 0/1 Configuration**

Parameter	Description	Default Setting / Format
Serial Port	Enable/disable the Serial Port (COM). Options: Enabled/Disabled	Enabled
Device Settings	Display the Serial Port 1/2 device settings	
Change Settings	Select an optimal setting for super IO device. Options: <ul style="list-style-type: none"> • Auto • IO=3F8h; IRQ=4; • IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; • IO=2F8h; IRO=3,4,5,6,7,9,10,11,12; • IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; • IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; 	Auto

6.2.2.3 Serial Port Console Redirection

Set the Serial Port console redirection.

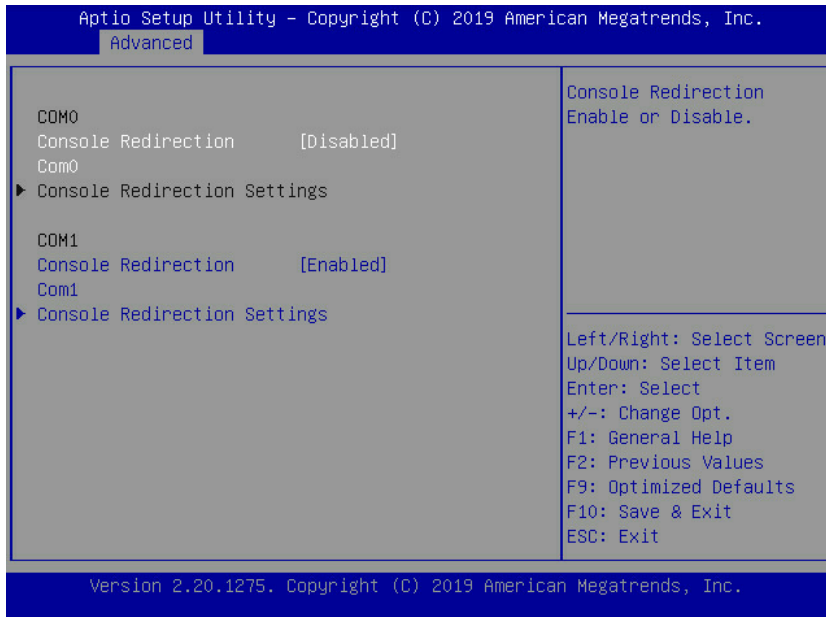


Table 6-10 **Advanced > Serial Port Console Redirection**

Parameter	Description	Default Setting / Format
Console Redirection Com0/Com1	Select whether to enable console redirection for the specified device. Options: Enabled/Disabled	Disabled
Console Redirection Settings	Press <Enter> for configuration of advanced items.	

Parameter	Description	Default Setting / Format
	NOTE: This item is only available when <i>Console Redirection Com0/Console Redirection Com1</i> is set to [Enabled].	

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



Table 6-11 **Advanced > Serial Port Console Redirection > Console Redirection Settings**

Parameter	Description	Default Setting / Format
Terminal Type	Select a terminal type to be used for console redirection. Options: VT100/VT100+/VT-UTF8/ANSI	ANSI
Bits per second	Select the transfer rate. Options: 9600/19200/38400/57600/115200	115200
Data Bits	Select the number of data. Options: 7/8	8
Parity	A parity bit can be sent with the data bits to detect some transmission errors. Options: None/Even/Odd/Mark/Space	None
Stop Bits	Indicate the end of a serial data packet. Options: 1/2	1

Parameter	Description	Default Setting / Format
Flow Control	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals Options: None and Hardware RTS/CTS	None
VT-UTF8 Combo Key Support	Enable/Disable the VT-UTF8 Combo Key Support. Options: Enabled/Disabled	Enabled
Recorder Mode	When this mode enabled, only texts will be send. This is to capture Terminal data. Options: Enabled/Disabled	Disabled
Redirection 100×31	Enable/Disable extended terminal resolution. Options: Enabled/Disabled	Disabled
Putty KeyPad	Selects FunctionKey and KeyPad on Putty. Options: VT100/LINUX/XTERMR6/SCO/ESCN/VT400	VT100

6.2.2.4 PCI Subsystem Settings

Set the PCI subsystem information.

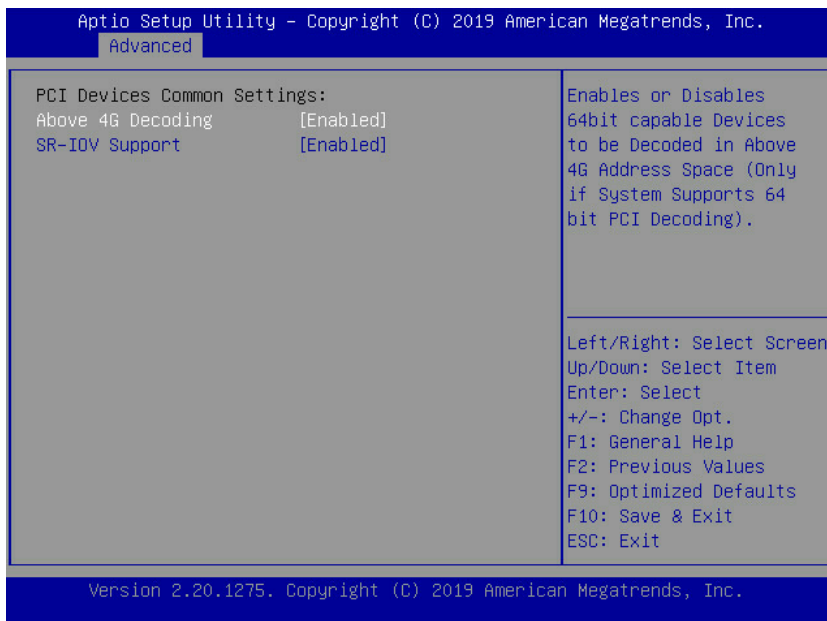


Table 6-12 Advanced > PCI Subsystem Settings

Parameter	Description	Default Setting / Format
Above 4G Decoding	Enable/Disable 64-bit capable Devices to be decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding) Options: Enabled/Disabled	Enabled
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options: Enabled/Disabled	Enabled

6.2.2.5 CSM Configuration

Set the compatibility support module (CSM) configuration.

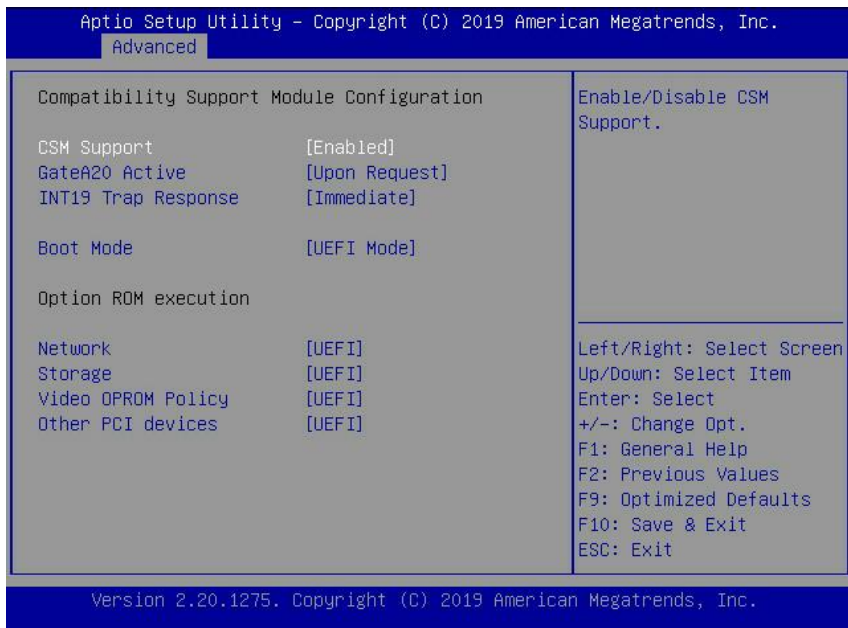




Table 6-13 Advanced > CSM Configuration

Parameter	Description	Default Setting / Format
CSM Support	Enable/Disable the Compatibility Support Module (CSM) support Options: Enabled/Disabled	Enabled
GateA20 Active	When set to Upon Request, GA20 can be disabled. When set to Always, GA20 cannot be disabled; this option is useful when any RT code is executed above 1MB.	Upon Request

Parameter	Description	Default Setting / Format
	<p>Options: Upon Request/Always</p> <p> NOTE: This item is only available when <i>CSM Support</i> is set to [Enabled].</p>	
INT19 Trap Response	<p>Configure BIOS reaction on INT19 trapping by Option ROM. When set to Immediate, the system executes the trap right away. When set to Postponed, the system executes the trap during legacy boot.</p> <p>Options: Immediate/Postponed</p> <p> NOTE: This item is only available when <i>CSM Support</i> is set to [Enabled].</p>	Immediate
Boot Mode	<p>Set the Boot mode.</p> <p>Options: Legacy Mode/UEFI Mode</p> <p>For more information, refer to 6.1.4 UEFI/Legacy Mode.</p>	UEFI Mode
Network	<p>Control the execution of UEFI and Legacy PXE Option ROM.</p> <p>Options: Do not launch/Legacy/UEFI</p>	UEFI
Storage	<p>Control the execution of UEFI and Legacy Option ROM.</p> <p>Options: Do not launch/Legacy/UEFI</p>	UEFI
Video OPROM Policy	<p>Control the execution of UEFI and Legacy Video Option ROM.</p> <p>Options: Do not launch/Legacy/UEFI</p>	UEFI
Other PCI devices	<p>Determine Option ROM execution policy for devices other than Network, Storage, or Video.</p> <p>Options: Do not launch/Legacy/UEFI</p>	UEFI

6.2.2.6 Onboard LAN Configuration

Set the Onboard network card Configuration

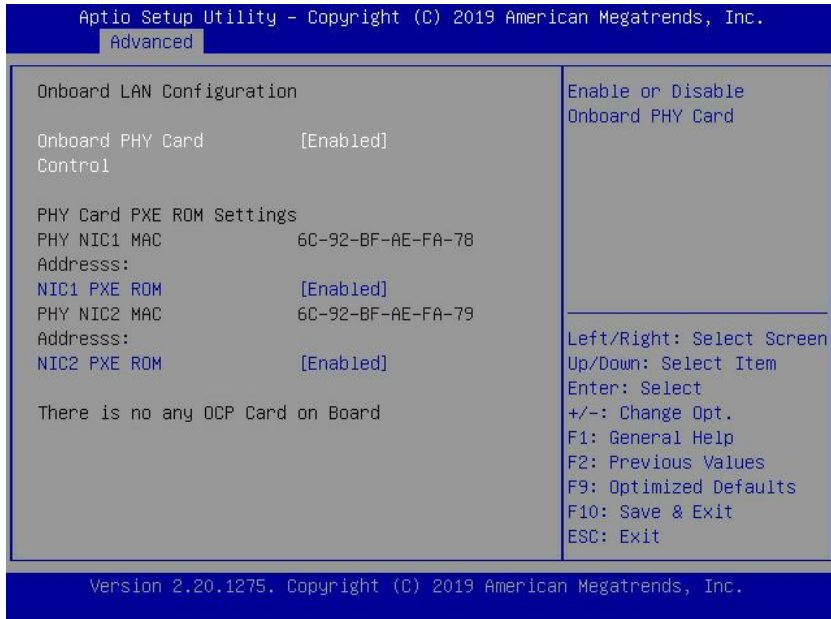


Table 6-14 Advanced > Onboard LAN Configuration

Parameter	Description	Default Setting / Format
Onboard PHY Card Control	Enable/disable the Onboard PHY card. Options: Enabled/Disabled	Enabled
PHY NIC MAC Address	Display the PHY NIC1/NIC2 MAC address	
NIC PXE ROM	Enable/disable the NIC PXE ROM feature. Options: Enabled/Disabled	Enabled

6.2.2.7 USB Devices Information

Display the USB devices connected to the system.

6.2.2.8 Network Stack Configuration

Set the UEFI Network stack configuration.

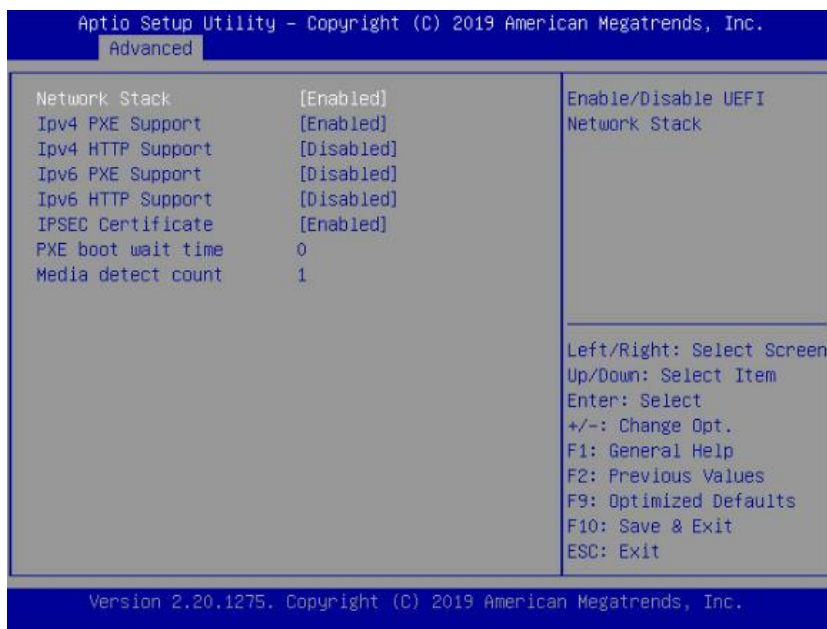


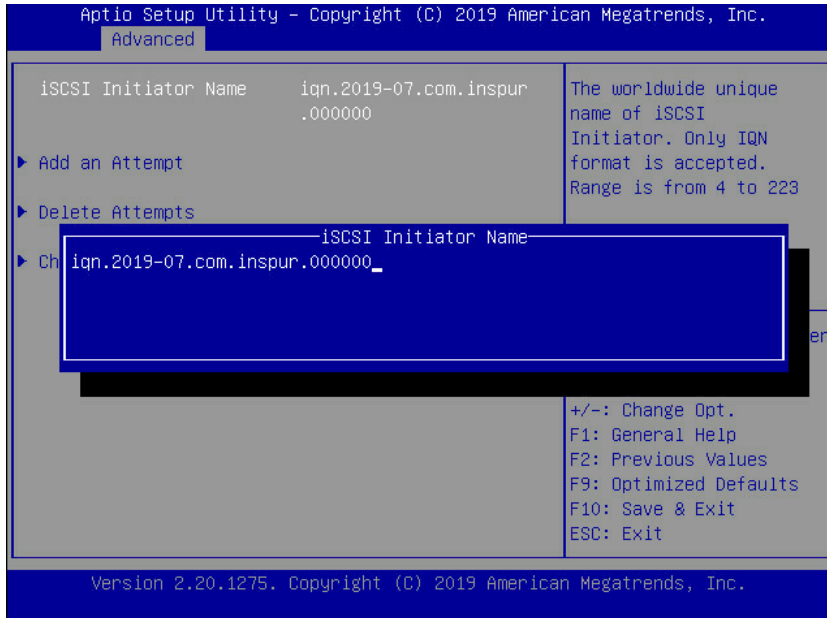
Table 6-15 Advanced > Network Stack Configuration

Parameter	Description	Default Setting / Format
Network Stack	Enable/Disable the UEFI network stack. Options: Enabled/Disabled NOTE: When set to [Enabled], the following items are configurable.	Enabled
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options: Enabled/Disabled	Enabled
Ipv4 HTTP Support	Enable/Disable the Ipv4 HTTP feature. Options: Enabled/Disabled	Disabled
Ipv6 PXE Support	Enable/Disable the Ipv6 PXE feature. Options: Enabled/Disabled	Disabled
Ipv6 HTTP Support	Enable/Disable the Ipv6 HTTP feature. Options: Enabled/Disabled	Disabled
IPSEC Certificate	Enable/Disable the IPSEC certificate feature. Options: Enabled/Disabled	Enabled
PXE boot wait time	Set the wait time to cancel PXE boot after pressing ESC key, the setting range is 0-5.	0
Media detect Count	Set the detected device count, the setting range is 1-50.	1

6.2.2.9 iSCSI Configuration

Set the Internet Small Computer System Interface (iSCSI) information. The iSCSI virtual drive is mainly used to run a supported operating system residing on an external server and a supported operating system used as a local server host operating system.

Press **Enter** to specify the iSCSI initiator name in iSCSI Qualified Name (iqn) format, for example: iqn.2019-07.com.inspur.000000.



Add an Attempt Submenu

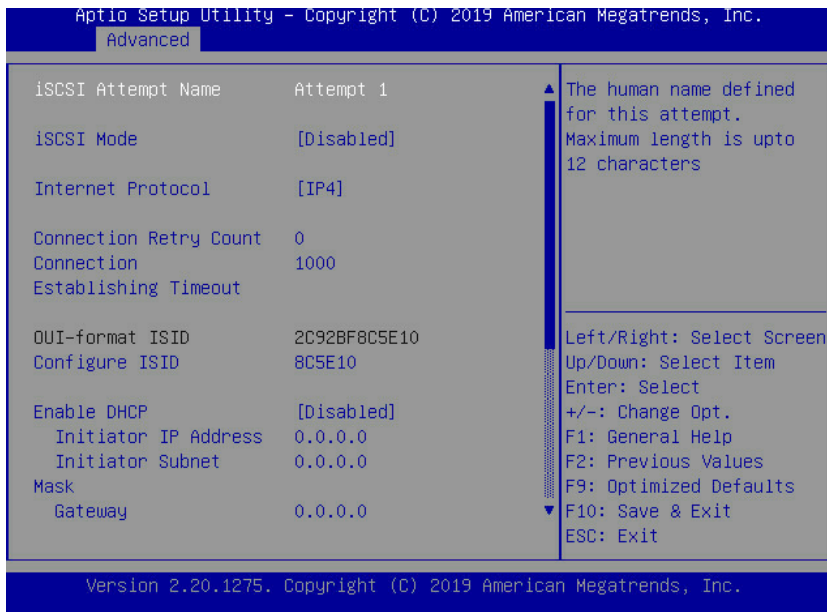
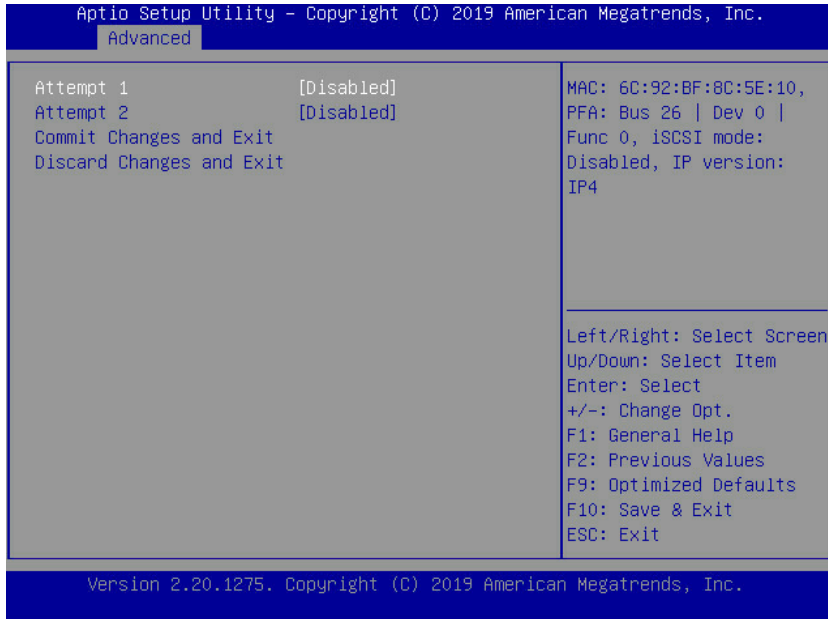


Table 6-16 Advanced > Network Stack Configuration > iSCSI Configuration > Add an Attempt

Parameter	Description	Default Setting / Format
iSCSI Mode	Enabled for MPIO. Options: Enabled/Disabled	Disabled
Internet Protocol	This item is specific to IPv6. Options: IP4/IP6/Autoconfigure	IP4
Connection Retry Count	The minimum value is 0 and the maximum is 16. 0 means no retry.	0
Connection Establishing Timeout	The minimum value is 100 milliseconds and maximum is 20 seconds.	1000
OUT-format ISID	OUT-format ISID in 6 bytes, default value is derived from the MAC address. Only last 3 bytes are configurable.	
Configure ISID	Configure the out-format ISID	
Enable DHCP	Enable/disable DHCP. Options: Enabled/Disabled	Disabled
Initiator IP Address	Enter IP address in dotted-decimal notation.	0.0.0.0
Initiator Subnet Mask	Enter IP address in dotted-decimal notation.	0.0.0.0
Gateway	Enter IP address in dotted-decimal notation.	0.0.0.0
Target Name	The worldwide unique name of the target. Only iqn. Format is accepted.	----
Target Address	Enter Target address in IPV4, IPV6 or URL format. You need to configure the DNS server address in advance if it's a URL string.	----
Target Port	Target Port	3260
Boot LUN	Hexadecimal representation of the LU number.	0
Authentication Type	Options: CHAP/Kerberos/None	None
Save Changes	System must be rebooted in order for changes to take effect..	----
Back to Previous Page	Back to Previous Page	----

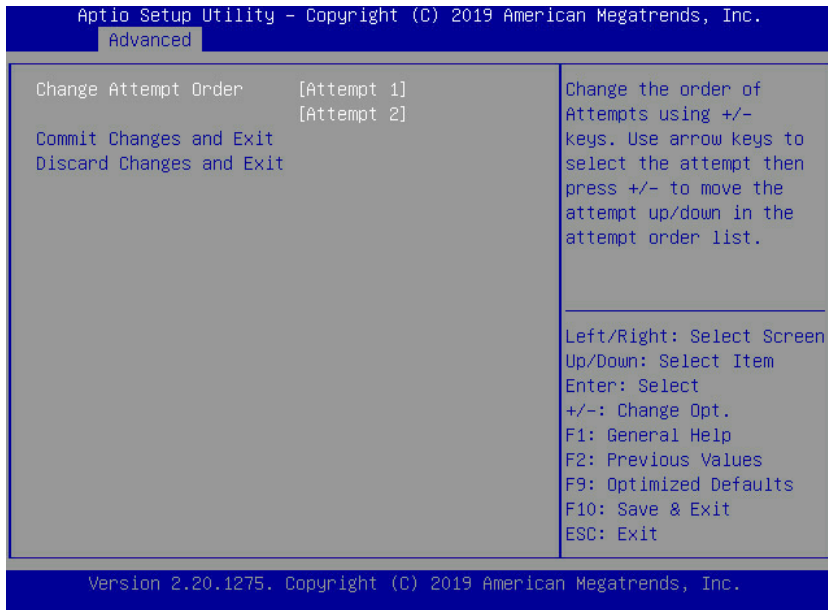
Delete Attempts Submenu

Delete one or more attempts by setting the item to [Enabled].




Change Attempt Order Submenu

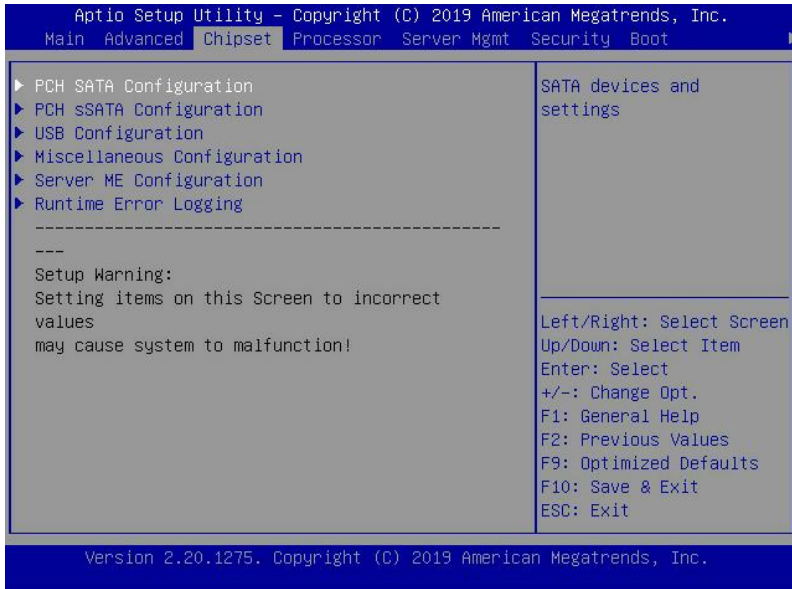
Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the attempt order list.



6.2.3 Chipset

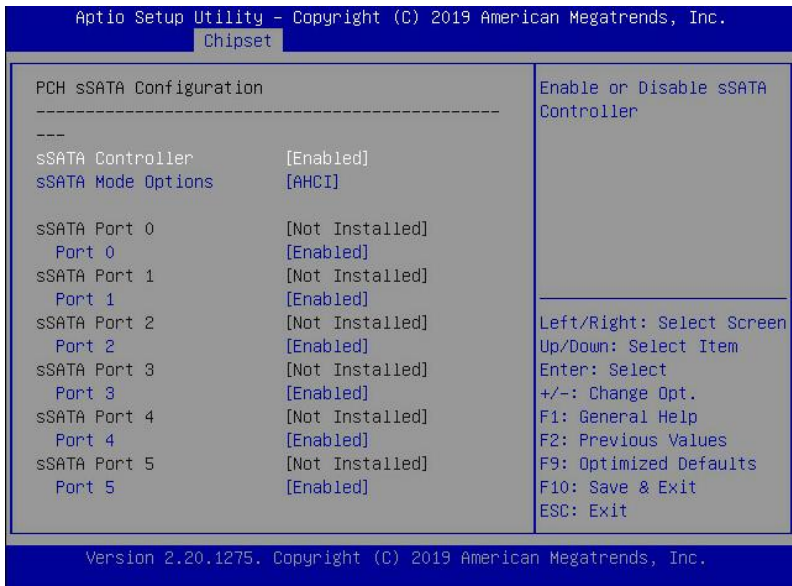
 **WARNING:** Setting items on this menu to incorrect values may cause system to malfunction.

The Chipset menu allows the user to configure the function and runtime error logging settings of PCH SATA/sSATA USB, and ME devices. To access the submenu item, press the **Enter** key.



6.2.3.1 PCH SATA/sSATA Configuration

Display and set the HDD information of onboard SATA ports/sSATA ports.



NOTE: The SATA/sSATA port number displayed on the BIOS Chipset menu may vary depending on the actual product.

Table 6-16 Chipset > PCH SATA/sSATA Configuration

Parameter	Description	Default Setting / Format
SATA Controller	Enable/disable the SATA controller. Options: Enabled/Disabled	Enabled
SATA Mode Options	When set to [AHCI], the RAID functions will be disabled and the RAID setup utility cannot be accessed at boot time. When set to [RAID], the SATA controller enables both its RAID and AHCI functions. The RAID setup utility is allowed to access at boot time. Options: AHCI/RAID NOTE: This item is only available when <i>SATA Controller</i> is set to [Enabled].	AHCI
SATA Port *	Display the SATA port * HDD information.	
Port *	Enable/disable the SATA port * Options: Enabled/Disabled	Enabled

6.2.3.2 USB Configuration

Display and set the onboard USB ports. The specific contents are displayed according to the actual project.

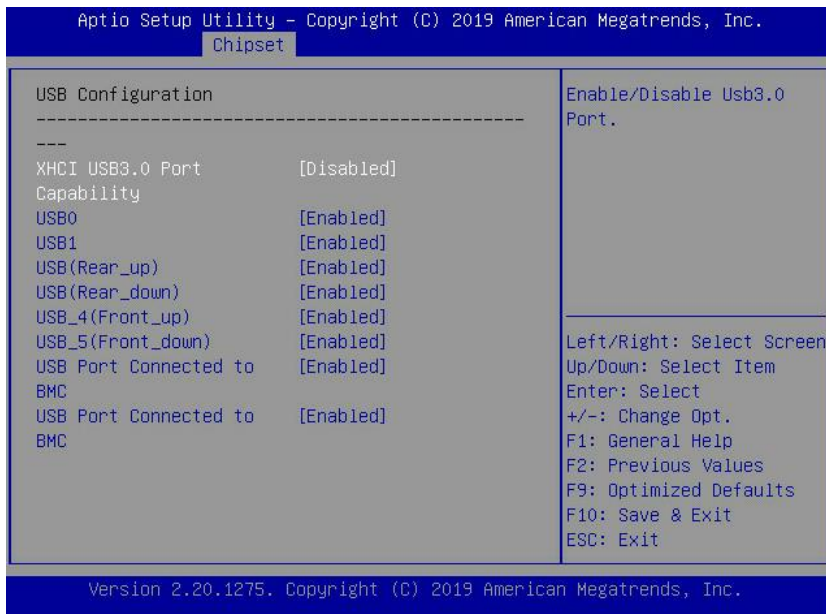


Table 6-17 Chipset > USB Configuration

Parameter	Description	Default Setting / Format
XHCI USB3.0 Port Capability	Enable/disable the XHCI USB3.0 port capability. Options: Enabled/Disabled	Disabled
USB *	Enable/disable the onboard USB ports. Options: Enabled/Disabled	Enabled
USB Port Connected to SD Card	Enable/disable the USB port connected to SD card. Options: Enabled/Disabled	Disabled
USB Port Connected to BMC	Enable/disable the USB port connected to BMC. Options: Enabled/Disabled	Enabled

6.2.3.3 Miscellaneous Configuration

Display and set the other common options.

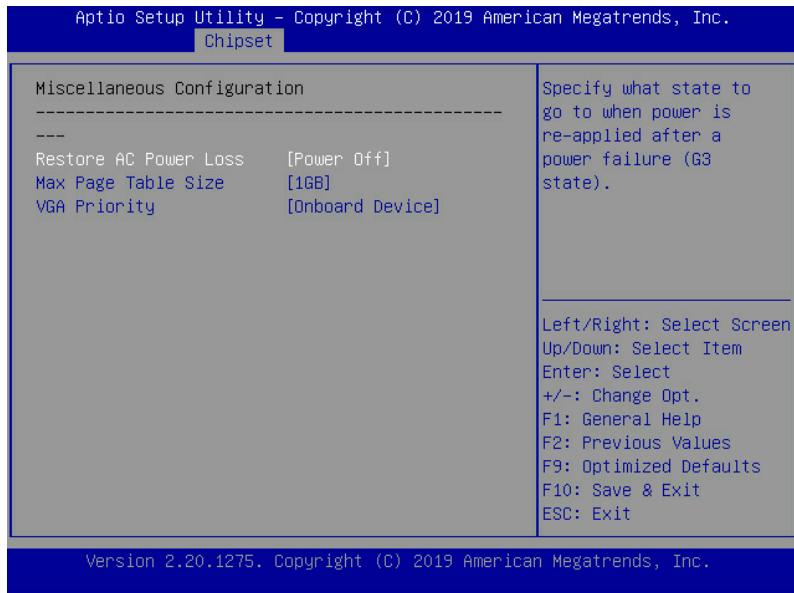


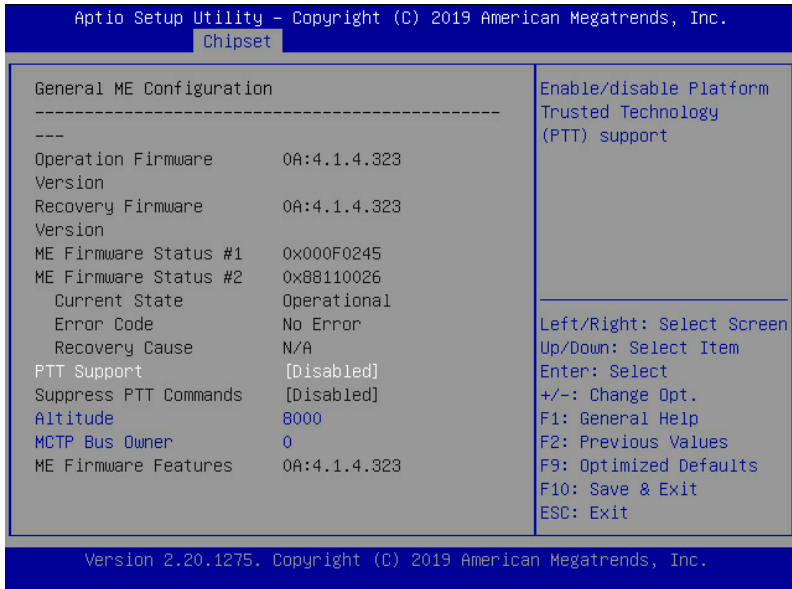
Table 6-18 Chipset > Miscellaneous Configuration

Parameter	Description	Default Setting / Format
Restore AC Power Loss	Specify what state to go to when a power failure (G3 State). Options: Power OFF/Last State/Power ON	Power off
Max Page Table Size	Set the maximum page table sizes. For an older OS, it is suggested to select 2MB	1GB

Parameter	Description	Default Setting / Format
	Options: 1GB/2MB	
VGA Priority	Set the VGA device priority. Options: Onboard Device/Offboard Device	Onboard Device

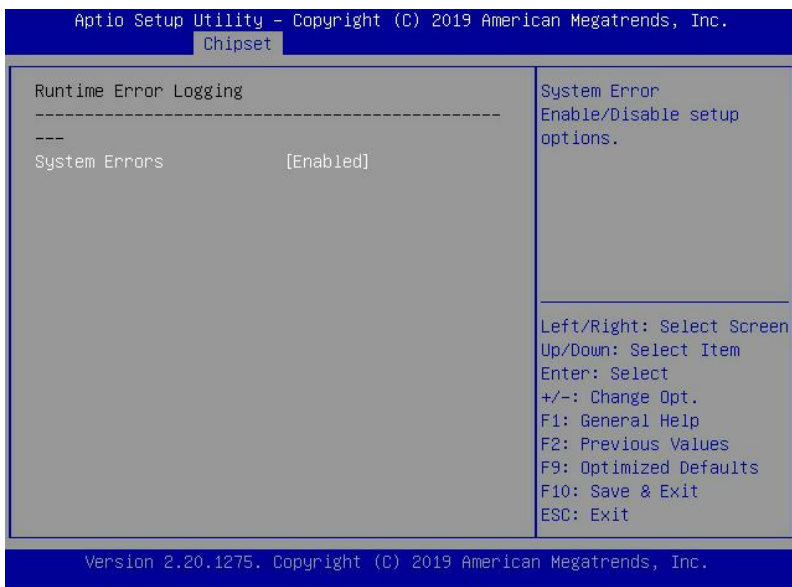
6.2.3.4 Server ME Configuration

Display and set the server ME information.



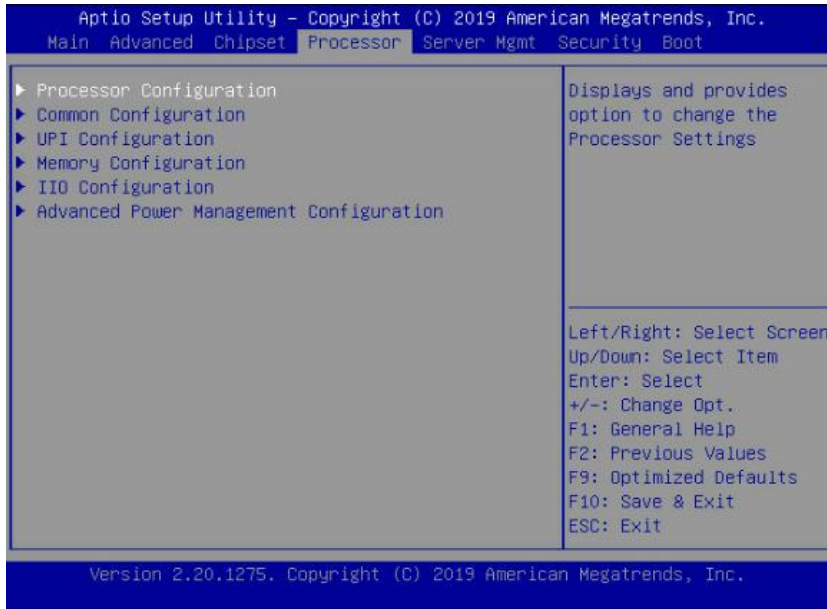
6.2.3.5 Runtime Error Logging

Set the system error logs.



6.2.4 Processor

The Processor menu allows the user to configure the processor and memory information. To access the submenu item, press the **Enter** key.



6.2.4.1 Processor Configuration

Configure the system processor settings.

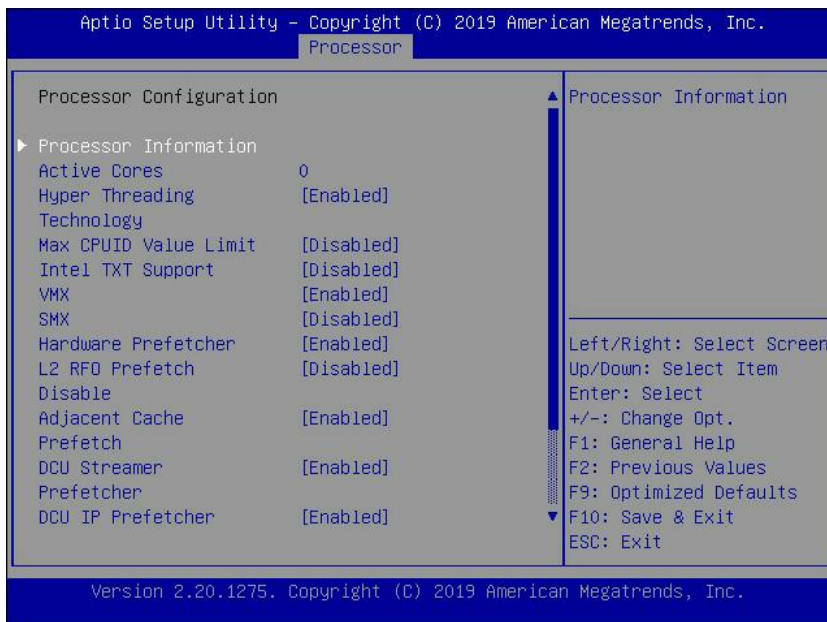



Table 6-19 Processor > Processor Configuration

Parameter	Description	Default Setting / Format
Active Cores	Input the number of CPU cores you want to enable. In the Help information area, it will display the effective values you can set and the maximum number of physical cores according to the current CPU usage. The default value is 0, all cores enabled.	0
Hyper Threading Technology	Enable/disable the hyper threading technology Options: Enabled/Disabled	Enabled
Max CPUID Value Limit	Enable/disable the max CPUID value limit. Options: Enabled/Disabled  NOTE: When the legacy OS boot does not support CPUID function, this item needs to set to [Enabled].	Disabled
Intel TXT Support	Enable/disable the Intel Trusted Execution Technology function. Options: Enabled/Disabled	Disabled
VMX	Enable/disable the Intel virtual machine extensions function. Options: Enabled/Disabled	Enabled
SMX	Enable/disable the safe mode extension function. Options: Enabled/Disabled	Disabled
Hardware Prefetcher	Prefetch the instructions or data from memory to L2 cache before CPU processing these instructions or data, to shorten the memory reading time, in order to eliminate potential bottlenecks and to improve system performance. Options: Enabled/Disabled	Enabled
L2 RFO Prefetch Disable	Enable/disable the L2 RFO prefetch. Options: Enabled/Disabled	Disabled
Adjacent Cache Prefetch	If this item set to [Enabled], when computer is reading data, it will intelligently consider the adjacent data is needed as well, and it will prefetch these data during data processing, to speed up the reading process. Options: Enabled/Disabled	Enabled

Parameter	Description	Default Setting / Format
DCU Streamer Prefetcher	Prefetcher the CPU data to shorten the data reading time Options: Enabled/Disabled.	Enabled
DCU IP Prefetcher	Judge whether there is data to prefetch in order to shorten the data reading time. Options: Enabled/Disabled	Enabled
LLC Prefetcher	Enable/disable all threads LLC. Options: Enabled/Disabled	Disabled
DCU Mode	Set the DCU mode Options: 32KB 8Way Without ECC/16KB 4Way With ECC	32KB 8Way Without ECC
Extended APIC	Enable/disable the extended APIC. Options: Enabled/Disabled	Enabled
AES-NI	Control whether the CPU supports AES instruction. Options: Enabled/Disabled	Enabled

6.2.4.2 Common Configuration

Configure the system common options for processor.

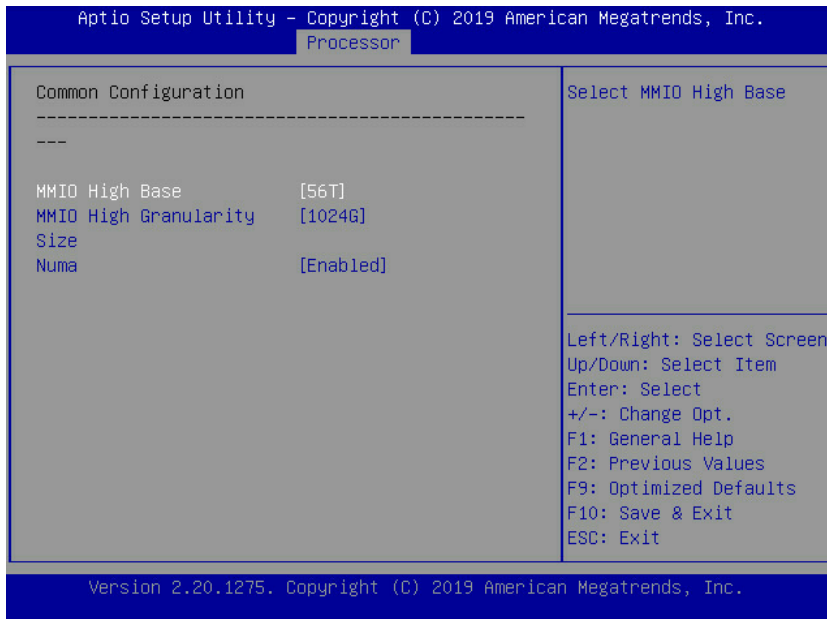


Table 6-20 Processor > Common Configuration

Parameter	Description	Default Setting / Format
MMIO High Base	MMIO high base settings.	56T

Parameter	Description	Default Setting / Format
	Options: 56T/40T/24T/16T/4T/1T	
MMIO High Granularity Size	MMIO high granularity size settings. Options: 1G/4G/16G/64G/256G/1024G	1024G
Numa	Allow a “NUMA Aware” OS to optimize which processor threads are used by processes can benefit by having the best access to those resources. Options: Enabled/Disabled	Enabled

6.2.4.3 UPI Configuration

Configure the system UPI settings.

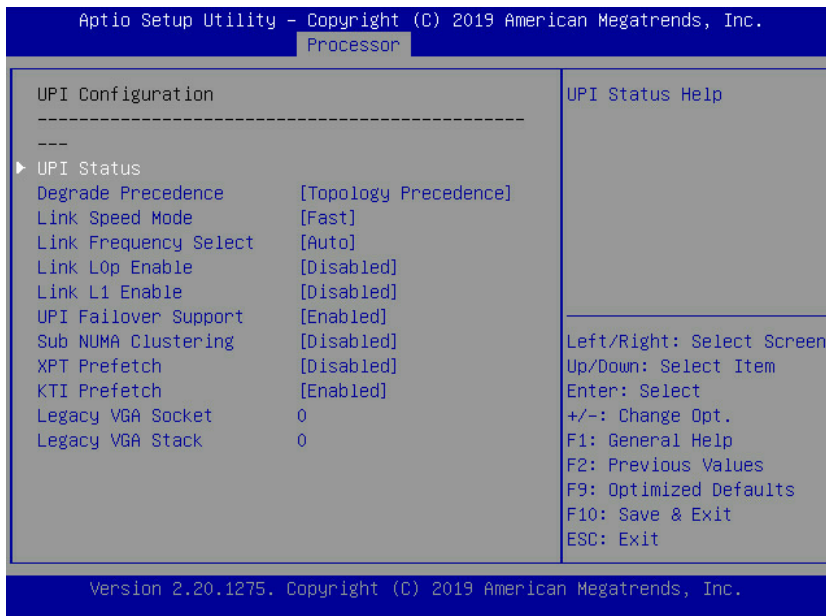


Table 6-20 Processor > UPI Configuration

Parameter	Description	Default Setting / Format
Degradate Precedence	When the system settings conflict, set this item to reduce Feature or to reduce Topology. Options: Topology Precedence/Feature Precedence	Topology Precedence
Link Speed Mode	Link speed mode settings. Options: Fast/Slow	Fast
Link Frequency Select	Link frequency select settings. Options: Auto/9.6 GT/s/10.4GT/s/Use Per Link Setting	Auto

Parameter	Description	Default Setting / Format
Link L0p Enable	Link power-saving mode setting. Options: Enabled/Disabled	Disabled
Link L1 Enable	In the case where the system is extremely idle, turn off the QPI Link. Options: Enabled/Disabled	Disabled
UPI Failover Support	Enable/disable the UPI failover support. Options: Enabled/Disabled	Enabled
Sub NUMA Clustering	Sub NUMA cluster settings Options: <ul style="list-style-type: none"> Auto: Support 1-cluster or 2-clusters according to IMC interleave. Enabled: Support all SNC clusters (2-clusters) and 1-way IMC interleave. Disabled: SNC function not supported. 	Disabled
XPT Prefetch	Enable/disable the XPT Prefetch. Options: Enabled/Disabled	Disabled
KTI Prefetch	Enable/disable the KTI Prefetch. Options: Enabled/Disabled	Enabled
Legacy VGA Socket	Set the Legacy VGA number, the range is 0-1.	0
Legacy VGA Stack	Set the Legacy VGA stack number, the range is 0-6.	0

6.2.4.4 Memory Configuration

Configure the system memory settings.

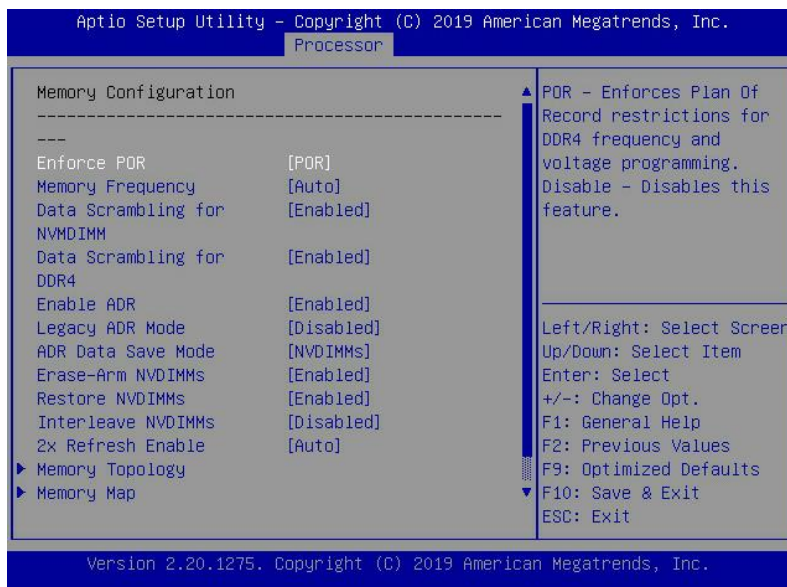


Table 6-21 Processor > Memory Configuration

Parameter	Description	Default Setting / Format
Enforce POR	Configure the enforce POR. Options: POR/Disabled	POR
Memory Frequency	Set the Memory frequency. Options: Auto/1866/2133/2400/2666/2933	Auto
Data Scrambling for NVMDIMM	Enable/disable the NVMDIMM (DCPMM) data scrambling. Options: Enabled/Disabled	Enabled
Data Scrambling for DDR4	Enable/disable the DDR4 data scrambling. Options: Auto/Enabled/Disabled	Enabled
Enable ADR	Enable/disable the ADR. Options: Enabled/Disabled	Enabled
Legacy ADR Mode	Enable/disable the Legacy ADR. Options: Enabled/Disabled	Disabled
ADR Data Save Mode	Set the ADR data save mode Options: Disabled/Batterybacked DIMMs/NVDIMMs	NVDIMMs
Erase-Arm NVDIMMs	Erase-Arm NVDIMMs settings. Options: Enabled/Disabled	Enabled
Restore NVDIMMs	Restore NVDIMMs settings. Options: Enabled/Disabled	Enabled
Interleave NVDIMMs	Interleave NVDIMMs settings. Options: Enabled/Disabled	Disabled
2x Refresh Enable	2x Refresh Enable settings. Options: Enabled/Disabled	Auto
Memory Topology	Press <Enter> to display the detailed system memory information.	
Memory Map	Press <Enter> for configuration of advanced items	
Memory RAS Configuration	Press <Enter> for configuration of advanced items	

Memory Map Submenu

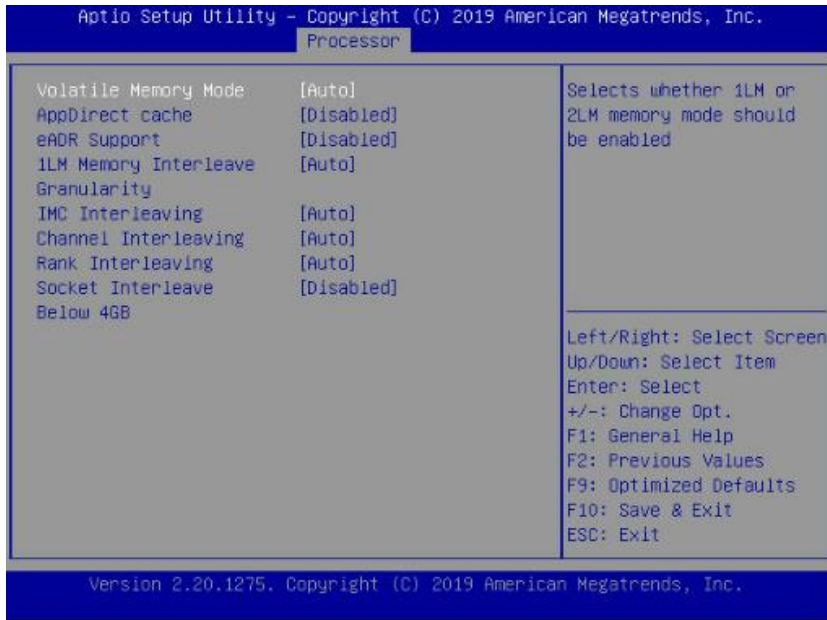


Table 6-21 Processor > Memory Configuration > Memory Map

Parameter	Description	Default Setting / Format
Volatile Memory Mode	Volatile memory mode settings. Options: 1LM/2LM/Auto	Auto
AppDirect cache	Enable caching for memory areas. Options: Auto/Enabled/Disabled	Disabled
eADR Support	eADR support settings. Options: Auto/Enabled/Disabled	Disabled
1LM Memory Interleave Granularity	1LM memory interleave granularity settings. Options: Auto/256B Target, 256B Channel/64B Target, 64B Channel	Auto
IMC Interleaving	IMC interleaving settings. Options: Auto/1-way Interleavel/2-way Interleavel	Auto
Channel Interleaving	Channel interleaving settings. Options: Auto/1-way Interleavel/2-way Interleavel/3-way Interleavel	Auto
Rank Interleaving	Rank interleaving settings. Options: Auto/1-way Interleavel/2-way Interleavel/4-way Interleavel/8-way Interleavel	Auto
Socket Interleave	Enable/disable the 4GB or less address space	Disabled

Parameter	Description	Default Setting / Format
Below 4GB	processor interleave. Options: Enabled/Disabled	

Memory RAS Configuration Submenu

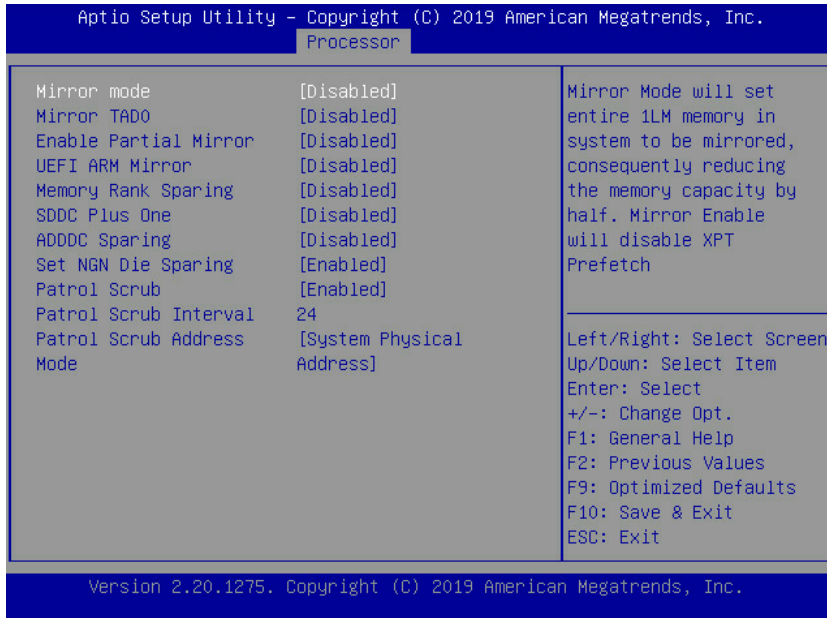


Table 6-22 Processor > Memory Configuration > Memory RAS Configuration

Parameter	Description	Default Setting / Format
Mirror Mode	Mirror mode settings. Options: Disabled/Mirror Mode (1LM)	Disabled
Mirror TAD0	Mirror TAD0 mode settings. Options: Enabled/Disabled	Disabled
Enable Partial Mirror	Enable partial mirror mode settings. Options: Disabled/Partial Mirror mode (1LM)	Disabled
UEFI ARM Mirror	UEFI ARM mirror mode settings. Options: Enabled/Disabled	Disabled
Memory Rank Sparing	Memory Rank sparing settings. Options: Enabled/Disabled When set to Enabled, user can select the memory sparing mode. The total memory capacity varies with the sparing mode, and it supports at most half of the memory capacity to be used for sparing.	Disabled

Parameter	Description	Default Setting / Format
SDDC Plus One	SDDC+1 settings. Options: Enabled/Disabled	Disabled
ADDDC Sparing	ADDDC sparing settings. Options: Enabled/Disabled	Disabled
Set NGN Die Sparing	NGN Die sparing settings. Options: Enabled/Disabled	Enabled
Patrol Scrub	Patrol Scrub settings. Options: Enabled/Disabled	Enabled
Patrol Scrub Interval	Patrol Scrub interval settings, the unit is hour and the range is 0-24. When set to 0, it means auto.	24
Patrol Scrub Address Mode	Patrol Scrub address mode settings. Options: System Physical Address/Reverse Address	System Physical Address

6.2.4.5 IIO Configuration

Configure the system PCIe slot settings.

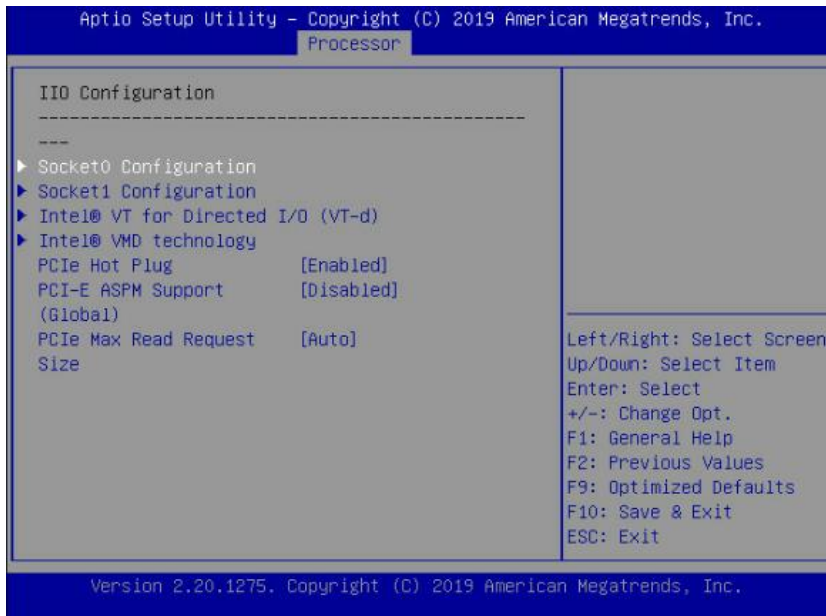


Table 6-23 Processor > IIO Configuration

Parameter	Description	Default Setting / Format
Socket Configuration	Press <Enter> for configuration of advanced items, such as the Link speed, Max Payload Size and ASPM of the CPUO's PCIE device.	

Parameter	Description	Default Setting / Format
Intel VT for Directed I/O (VT-d)	Press <Enter> for configuration of advanced items.	
Intel VMD Technology	Press <Enter> for configuration of advanced items.	
PCIe Hot Plug	PCIe hot plug settings. Options: Enabled/Disabled	Enabled
PCI-E ASPM Support (Global)	PCIE ASPM support settings. Options: Disabled/Per-Port/L1 Only	Disabled
PCIe Max Read Request Size	PCIe max read request size settings. Options: Auto/128B/256B/512B/1024B/2048B/4096B	Auto

6.2.4.6 Advanced Power Management Configuration

Configure the CPU power management.

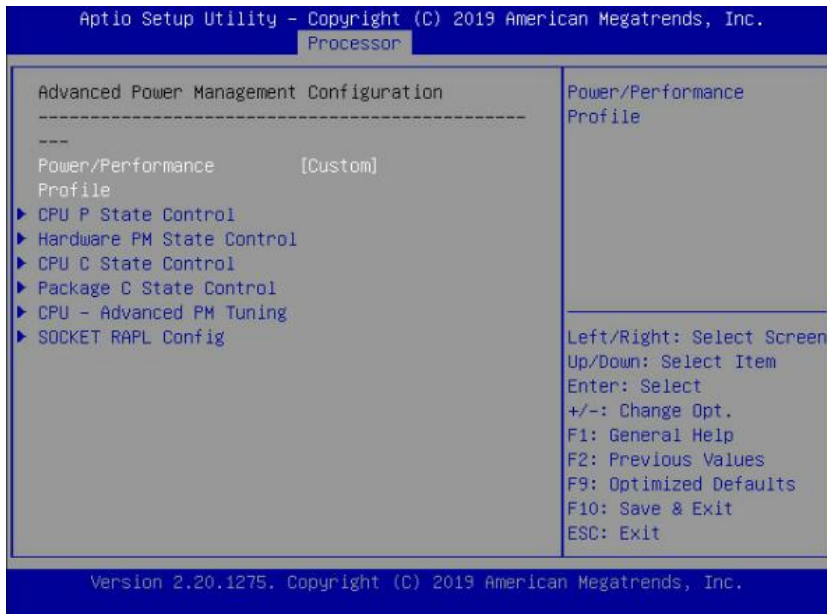


Table 6-24 Processor > Advanced Power Management Configuration

Parameter	Description	Default Setting / Format
Power/Performance Profile	Power/Performance profile settings. Options: Maximum Performance/Minimum Power/Custom	Custom
CPU P State Control	Press <Enter> for configuration of advanced items.	
Hardware PM State	Press <Enter> for configuration of advanced	

Parameter	Description	Default Setting / Format
Control	items.	
CPU C State Control	Press <Enter> for configuration of advanced items.	
Package C State Control	Press <Enter> for configuration of advanced items.	
CPU-Advanced PM Tuning	Press <Enter> for configuration of advanced items.	
SOCKET RAPL Config	Press <Enter> for configuration of advanced items.	

CPU P State Control Submenu

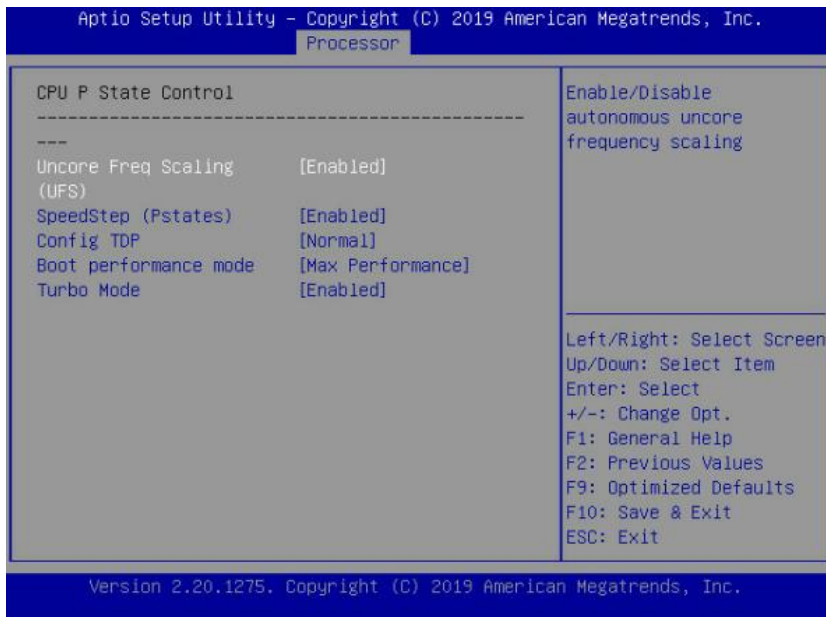


Table 6-25 Processor > Advanced Power Management Configuration > CPU P State Control

Parameter	Description	Default Setting / Format
Uncore Freq Scaling (UFS)	Enable/disable the autonomous uncore frequency scaling. Options: Enabled/Disabled(Min Frequency)/Disabled(MAX Frequency)/Custom	Enabled
SpeedStep (Pstates)	Enable/disable the Intel(R) SpeedStep Technology. Options: Enabled/Disabled	Enabled

Parameter	Description	Default Setting / Format
Config TDP	TDP level settings. Options: Normal/Level 1/Level 2	Normal
Boot performance mode	BIOS boot performance mode settings. Options: Max Performance/Max Efficient/Set by Intel Node Manager	Max Performance
Turbo Mode	Enable/disable the Intel(R) Turbo Boost Technology. Options: Enabled/Disabled	Enabled

Hardware PM State Control Submenu

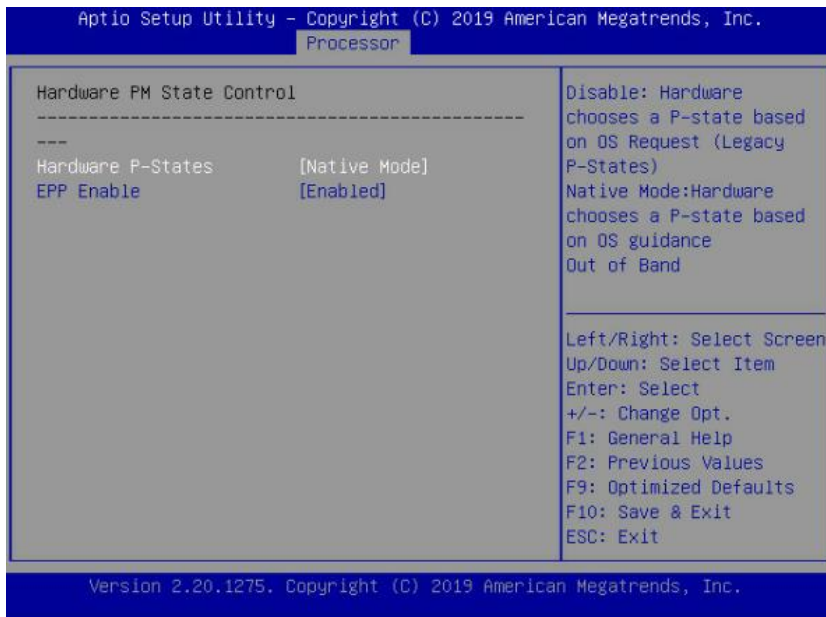


Table 6-26 Processor > Advanced Power Management Configuration > Hardware PM State Control

Parameter	Description	Default Setting / Format
Hardware P-States	Set the hardware P-States. Options: <ul style="list-style-type: none"> Disabled: based on legacy OS request Native Mode: based on legacy OS boot Out of Band Mode: hardware auto select, no OS boot Native Mode with No Legacy Support 	Native Mode
EPP Enable	Enable/disable the EPP feature. Options: Enabled/Disabled	Enabled

CPU C State Control Submenu

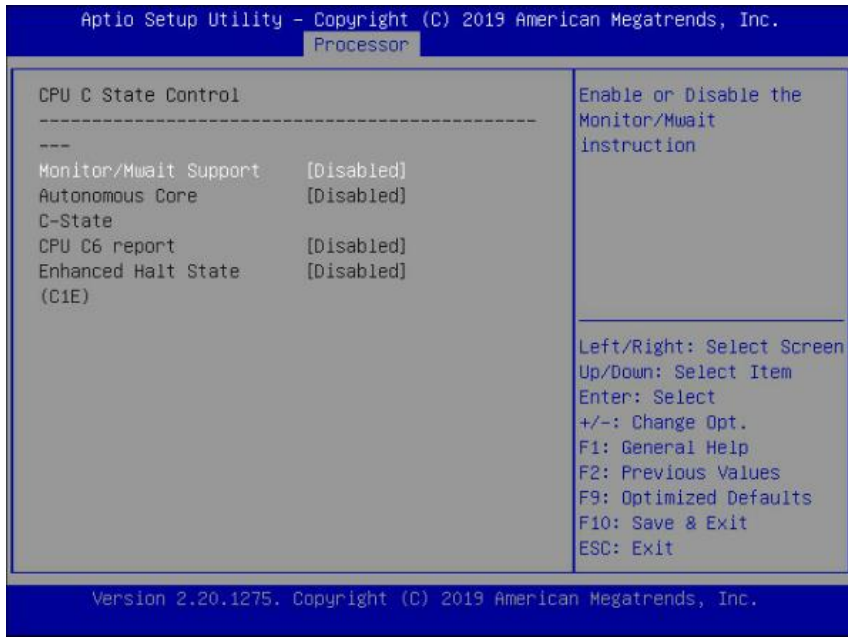


Table 6-27 Processor > Advanced Power Management Configuration > CPU C State Control

Parameter	Description	Default Setting / Format
Monitor/Mwait Support	Enable/disable the Monitor/Mwait instruction. Options: Enabled (two-way)/Disabled (four-way)	Disabled
Autonomous Core C-State	Enable/disable the autonomous core C-state. Options: Enabled/Disabled	Disabled
CPU C6 report	Enable/disable the C6 state to OS reports. Options: Enabled/Disabled	Disabled
Enhanced Halt State (C1E)	Enable/disable the C1E feature. Options: Enabled/Disabled	Disabled

Package C State Control Submenu

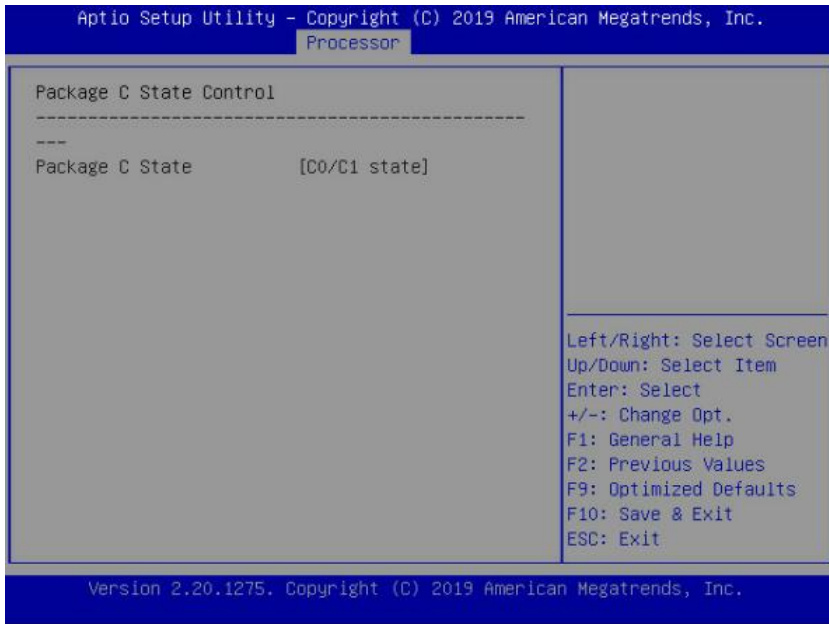


Table 6-28 Processor > Advanced Power Management Configuration > Package C State Control

Parameter	Description	Default Setting / Format
Package C State	Package C state settings. Options: <ul style="list-style-type: none"> • C0/C1 state • C2 state • C6 (non Retention) state • C6 (Retention) state • No Limit 	C0/C1 state

CPU-Advanced PM Tuning Submenu

Set the CPU power-saving performance, with an Energy Perf BIAS submenu.

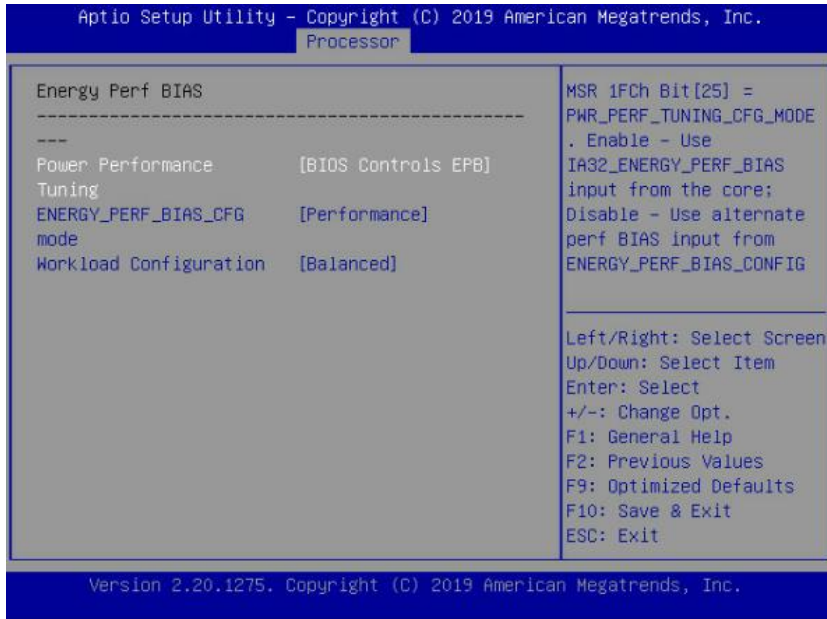


Table 6-29 Processor > Advanced Power Management Configuration > CPU-Advanced PM Tuning > Energy Perf BIAS

Parameter	Description	Default Setting / Format
Power Performance Tuning	Power performance tuning settings. Options: OS Controls EPB/BIOS Controls EPB	BIOS Controls EPB
ENERGY_PERF_BIAS_CFG Mode	Power performance management settings. Options: Performance/Balanced Performance/Balanced Power/Power NOTE: This item is only available when <i>Power Performance Tuning</i> is set to [BIOS Controls EPB].	Performance
Workload Configuration	Workload optimization settings. Options: Balanced / I/O Sensitive	Balanced

SOCKET RAPL Config Submenu

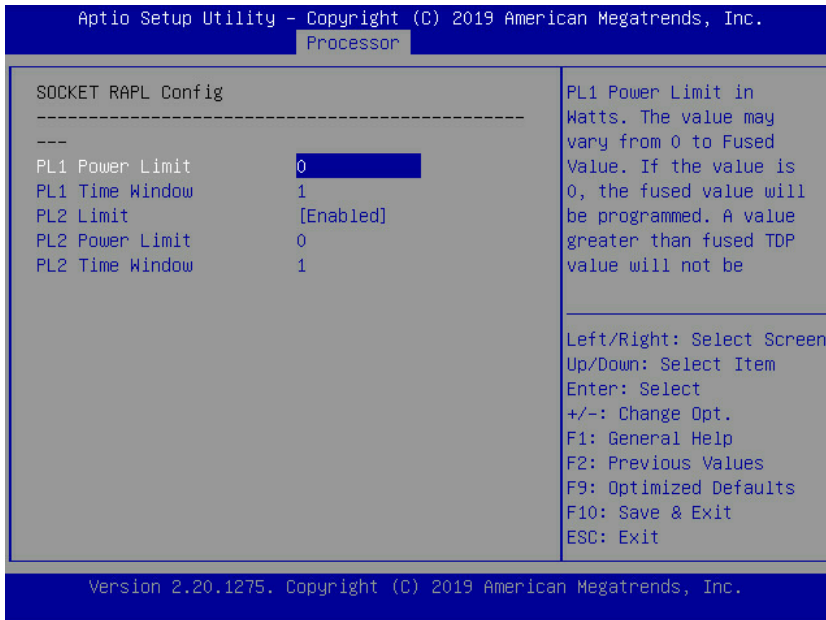


Table 6-30 Processor > Advanced Power Management Configuration > Socket RAPL Config

Parameter	Description	Default Setting / Format
PL1 Power Limit	PL1 power limit settings	0
PL1 Time Window	PL1 time window settings, the range is 0-56.	1
PL2 Limit	Enable/disable the PL2 limit function. Options: Enabled/Disabled	Enabled
PL2 Power Limit	PL2 power limit settings	0
PL2 Time Window	PL2 time window settings, the range is 0-56.	1

6.2.5 Server Mgmt

The Server Mgmt menu allows the user to configure the server additional features, including watchdog, BMC network configuration, BMC user settings, and system health information.

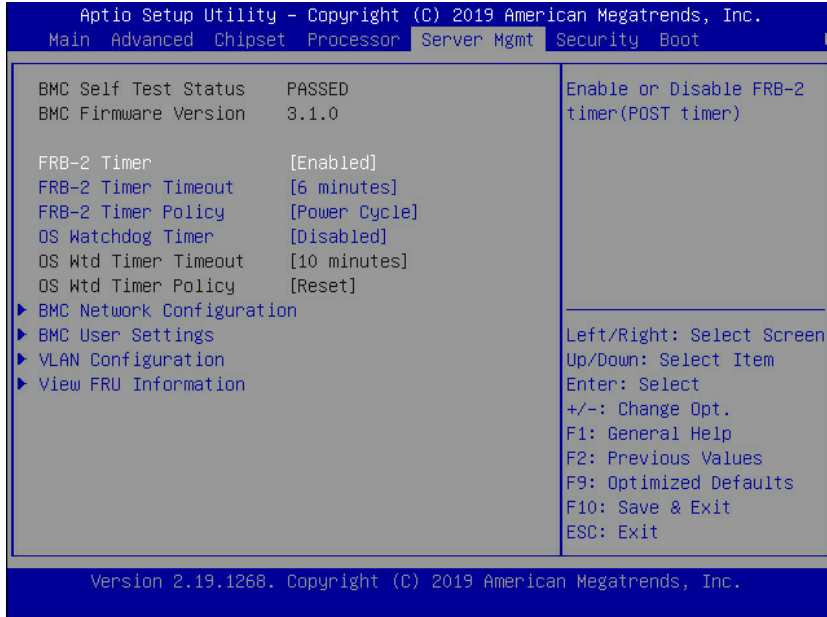




Table 6-31 Server Mgmt Menu

Parameter	Description	Default Setting / Format
BMC Self Test Status	BMC self-test status	PASSED
BMC Firmware Version	Display BMC firmware version information	
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer) Options: Enabled/Disabled	Enabled
FRB-2 Timer Timeout	Configure the FRB2 Timer timeout. Options: 3 minutes/4 minutes/5 minutes/6 minutes  NOTE: This item is only available when <i>FRB-2 Timer</i> is set to [Enabled].	6 minutes
FRB-2 Timer policy	Configure the FRB2 Timer policy. Options: Do Nothing/Reset/Power Down/Power Cycle  NOTE: This item is only available when <i>FRB-2 Timer</i> is set to [Enabled].	Power Cycle
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function Options: Enabled/Disabled	Disabled

Parameter	Description	Default Setting / Format
OS Wtd Timer Timeout	Configure OS Watchdog Timer Options: 5 minutes/10 minutes/15 minutes/20 minutes NOTE: This item is only available when <i>OS Watchdog Timer</i> is set to [Enabled].	10 minutes
OS Wtd Timer policy	Configure OS Watchdog Timer Policy. Options: Do Nothing/Reset/Power Down/Power Cycle NOTE: This item is only available when <i>OS Watchdog Timer</i> is set to [Enabled].	Reset
BMC Network Configuration	Press <Enter> for configuration of advanced items	----
BMC User Settings	Press <Enter> for configuration of advanced items	----
VLAN Configuration	Press <Enter> for configuration of advanced items	----
View FRU information	Press <Enter> for configuration of advanced items	----

6.2.5.1 BMC Network Configuration

Configure the BMC network through BIOS.

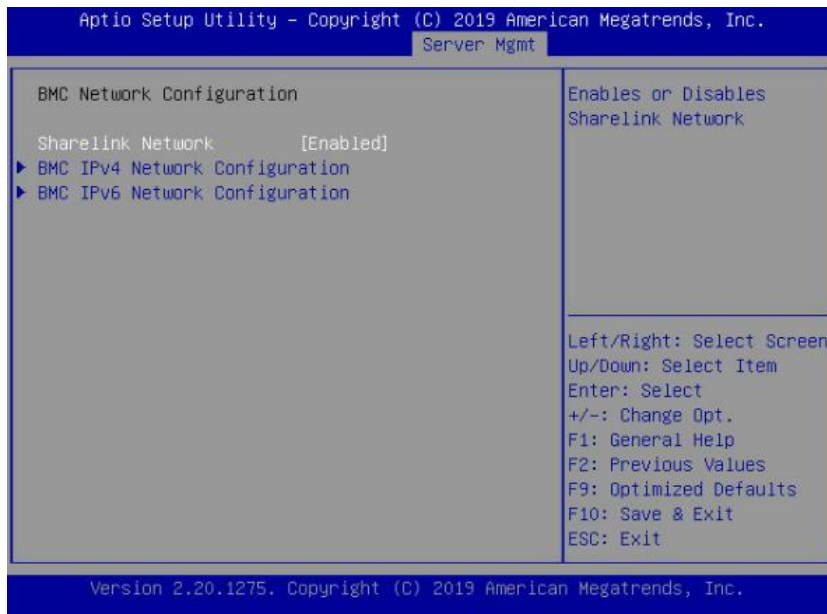
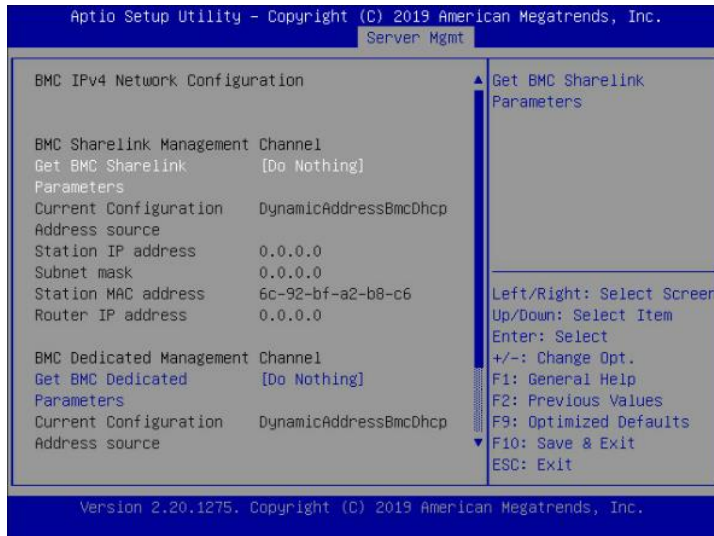


Table 6-32 Server Mgmt > BMC Network Configuration

Parameter	Description	Default Setting / Format
Sharelink Network	Enable/disable the Sharelink network function. Options: Enabled/Disabled	Enabled
BMC IPv4 Network Configuration	Press <Enter> for configuration of advanced items	
BMC IPv6 Network Configuration	Press <Enter> for configuration of advanced items	

BMC IPv4 Network Configuration Submenu



BMC IPv6 Network Configuration Submenu

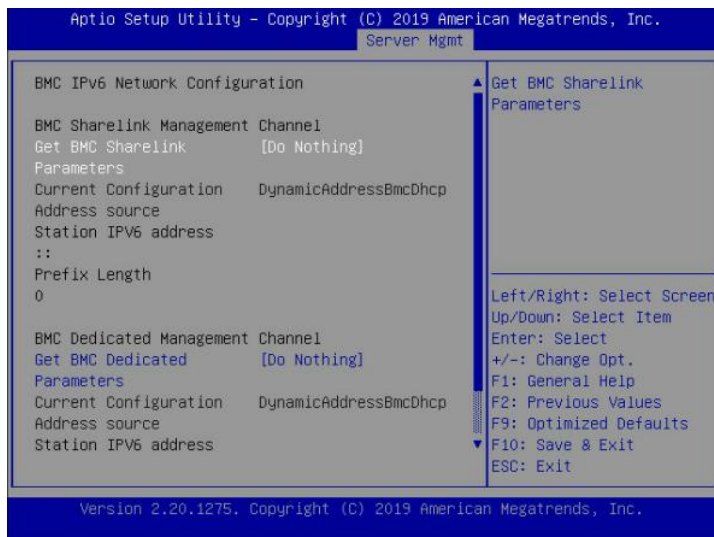


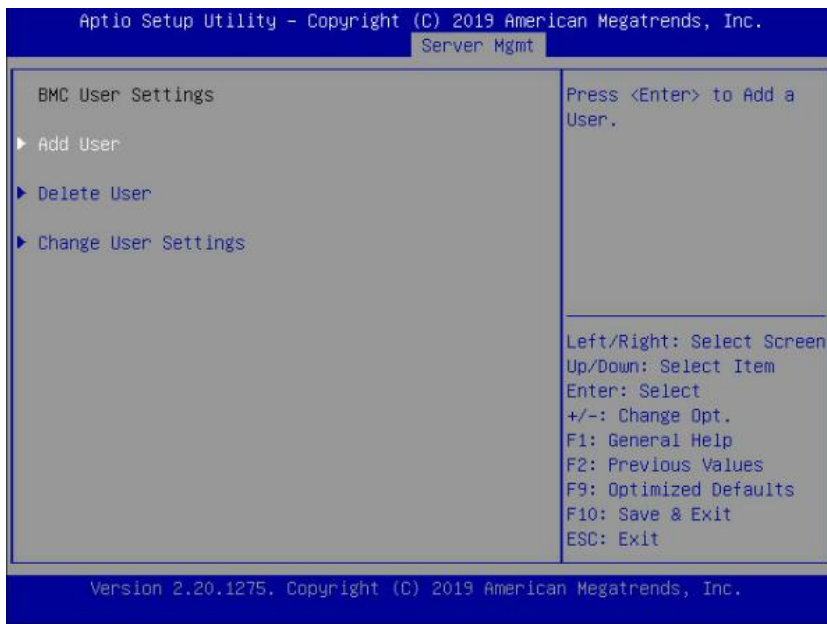
Table 6-33 Server Mgmt > BMC Network Configuration > BMC IPv4/IPv6 Network Configuration

Parameter	Description	Default Setting / Format
Get BMC Sharelink Parameters	Set the method to get the BMC sharelink parameters. Options: Do Nothing/Auto/Manual	Do Nothing
Get BMC Dedicated Parameters	Set the method to get the BMC dedicated parameters. Options: Do Nothing/Auto/Manual	Do Nothing

For more information, see [6.1.6 Configuring the BMC Network](#).

6.2.5.2 BMC User Settings

Configure the BMC users. Press **Enter** for configuration of advanced items.



Add User Submenu

Add a BMC user to the BMC user list. This action takes effect immediately.

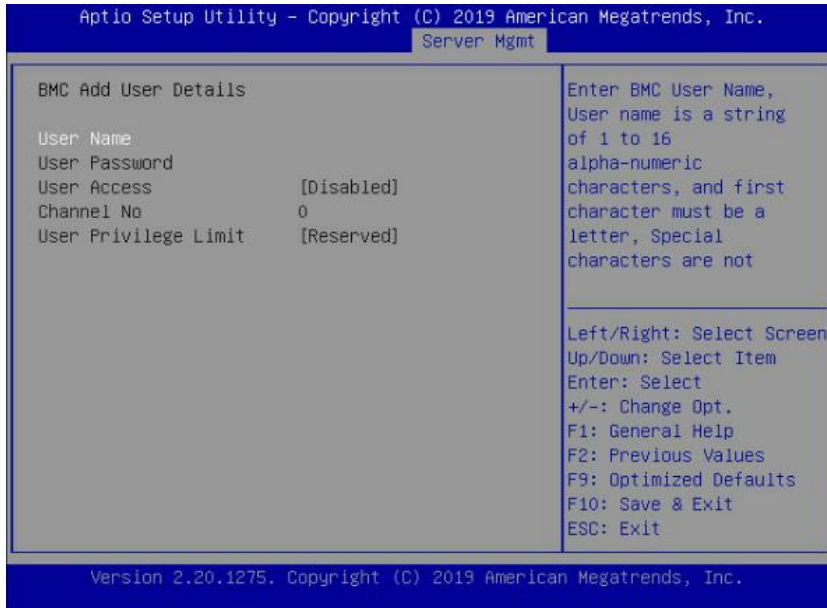


Table 6-34 Server Mgmt > BMC User Settings > Add User

Parameter	Description	Default Setting / Format
User Name	Set the user name, up to 16 characters.	----
User Password	Set the user password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.	----
User Access	Enable/disable the user access settings. Options: Enabled/Disabled	Disabled
Channel No	Set the BMC channel, input 1 or 8.	0
User Privilege Limit	User privilege settings. Options: <ul style="list-style-type: none"> Reserved Callback User Operator Administrator 	Reserved

If the setting succeeds, it will prompt “Set User Access Command Passed”, and take effect immediately.

 **NOTE:** To allow the new user to operate the BMC, *User Access* must set to

[Enabled].

Delete User Submenu

Delete a BMC user from the BMC user list. This action takes effect immediately.

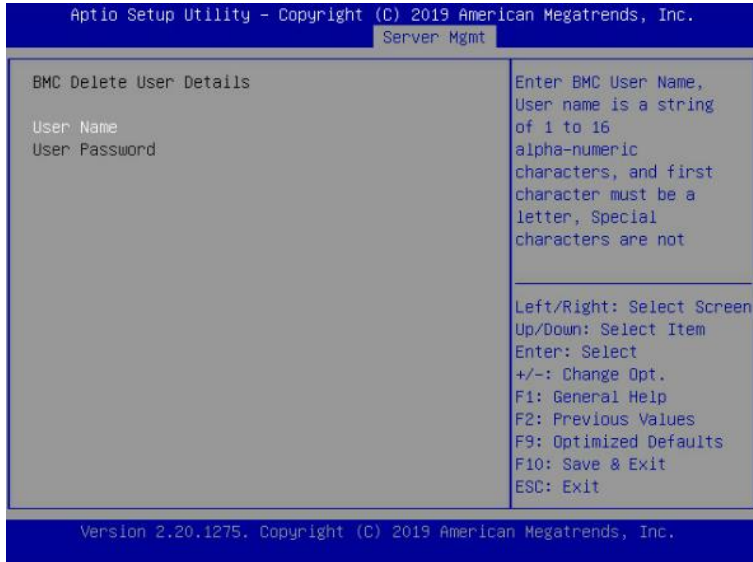


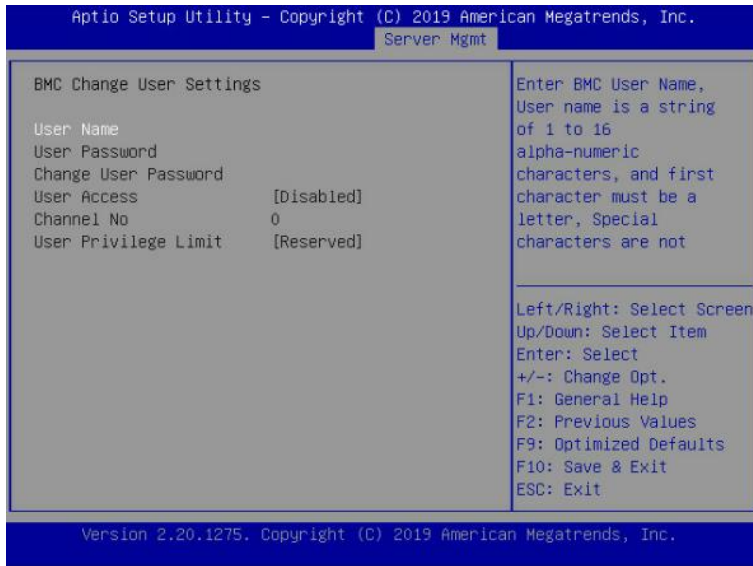
Table 6-35 Server Mgmt > BMC User Settings > Delete User

Parameter	Description	Default Setting / Format
User Name	Enter the user name you want to delete.	----
User Password	Enter the password to confirm the deletion.	----

If the setting succeeds, it will prompt “User Deleted!!!”, and take effect immediately.

Change User Settings Submenu

Modify the BMC user settings. See [Table 6-34](#) for the operation.



6.2.5.3 VLAN Configuration

Configure the Virtual LAN (VLAN).

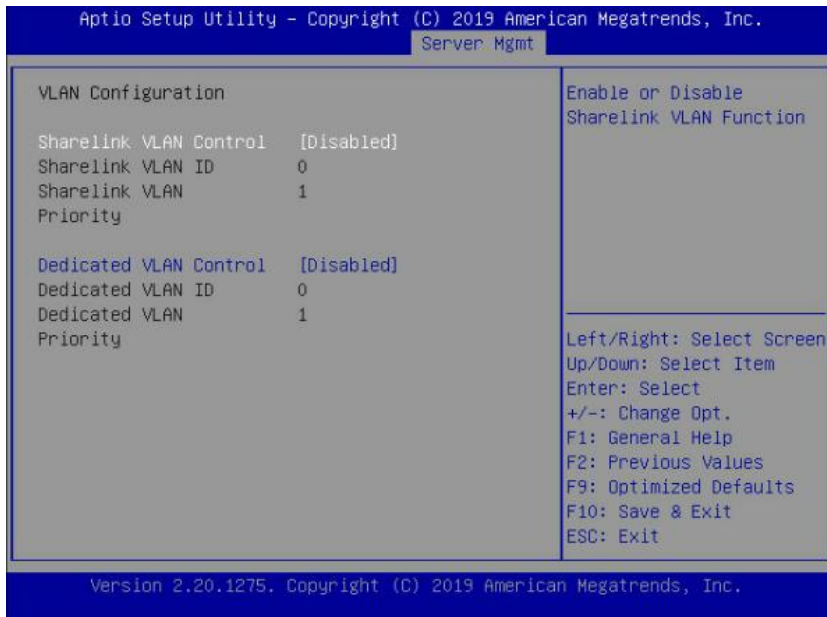



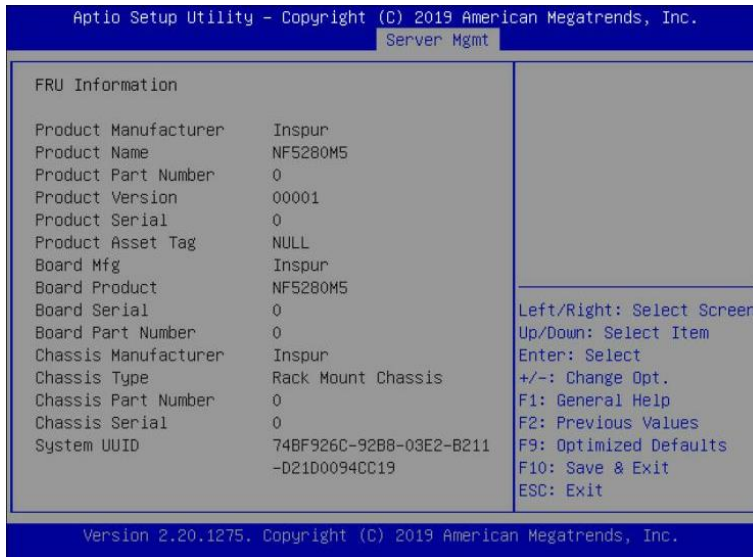
Table 6-36 Server Mgmt > VLAN Configuration

Parameter	Description	Default Setting / Format
Sharelink/Dedicated VLAN Control	Enable/disable BMC sharelink/dedicated VLAN function Options: Enabled/Disabled  NOTE: To enable VLAN, it needs to set the	Disabled

Parameter	Description	Default Setting / Format
	VLAN ID first.	
Sharelink/Dedicated VLAN ID	Set the BMC sharelink/dedicated VLAN ID, the range is 2-4094. NOTE: The setting takes effect immediately.	0
Sharelink/Dedicated VLAN Priority	Set the BMC sharelink/dedicated VLAN priority, the range is 1-7. NOTE: The setting takes effect immediately.	1

6.2.5.4 View FRU information

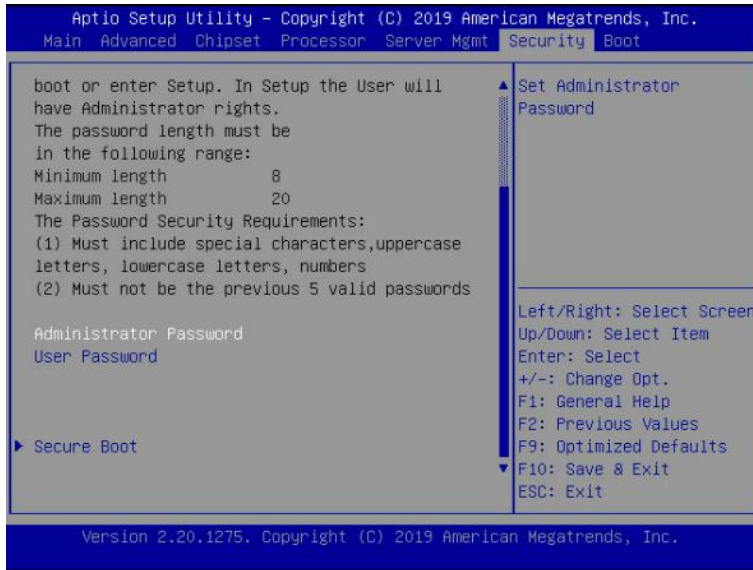
Display the basic system ID information, as well as System product information. Items on this window are non-configurable



NOTE: The model name will vary depends on the product you purchased.

6.2.6 Security

The Security menu allows the user to configure the system security.



The *Administrator Password* and *User Password* are null by default, press **Enter** to set a new password. It must contain uppercase and lowercase letters, special characters and numbers, within 8-20 characters.

6.2.7 Boot

The Boot menu allows the user to configure the boot mode, boot priority and boot procedure.

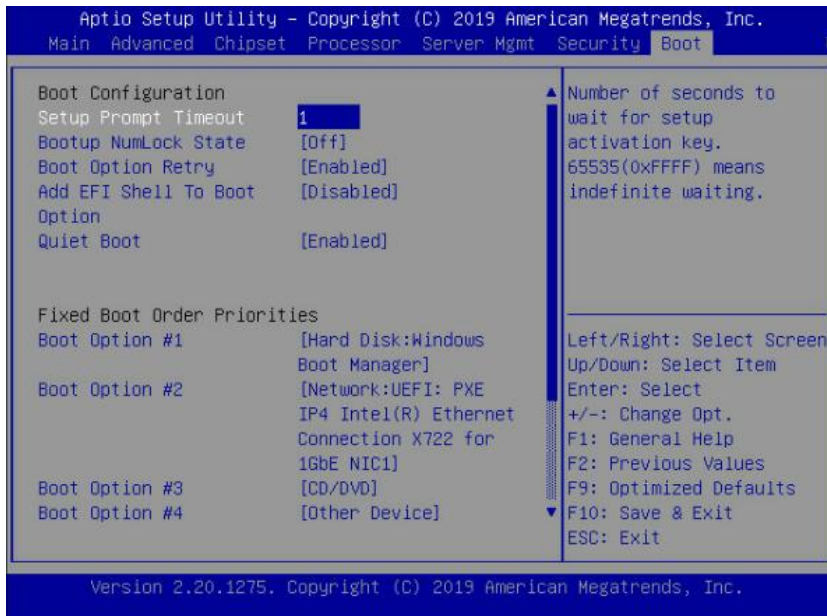


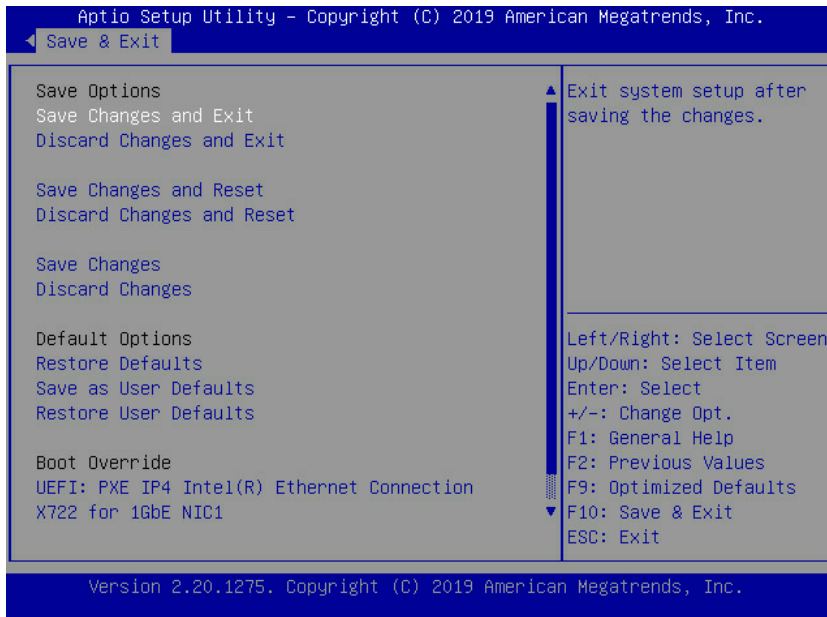
Table 6-37 Boot Menu

Parameter	Description	Default Setting / Format
-----------	-------------	--------------------------

Parameter	Description	Default Setting / Format
Setup Prompt Timeout	Set the time to wait for the Setup activate key. The maximum value is 65535 seconds.	1
Bootup NumLock State	Enable/disable the Bootup Numlock. Options: On/Off	Off
Boot Options Retry	Enable/disable the Boot option retry feature. Options: Enabled/Disabled	Enabled
Add EFI Shell To Boot Option	Add the EFI Shell to the Boot Option. Options: Enabled/Disabled	Disabled
Quiet Boot	Enable/disable the quite boot feature. Options: Enabled/Disabled If set to [Enabled], the boot logo displays during POST. If set to [Disabled], a text-mode boot screen displays.	Enabled
Boot Order Priorities	Press <Enter> on Boot Option to change the priority.	
Driver BBS Priorities	Press <Enter> on Driver BBS Option to change the priority	

6.2.8 Save & Exit

The Save & Exit menu allows the user to save the BIOS parameters and exit the BIOS Setup menu.



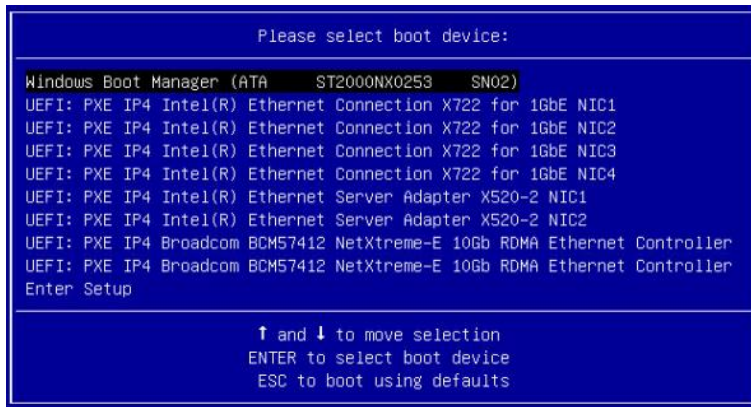
6.3 Firmware Update

There are two methods to update the firmware: UEFI Shell or under OS environment.

6.3.1 UEFI Shell

To update the firmware with UEFI Shell:

1. When Inspur Logo appears on the screen during system booting, press **F11** key to enter the Boot Menu.
2. Highlight **UEFI: Built-in EFI Shell**, and press **Enter**.



3. Type `'cd afuefi64'` (the location where the disk stores the AfuEfi64 package), and type `'dir'` to enter the aafuefi64 folder. The BIOS.bin file contains the 32M BIOS and ME file.

```
fs0:\> cd afuefi64

fs0:\afuefi64> dir
Directory of: fs0:\afuefi64


10/24/14 09:34a <DIR>          4,096 .
10/24/14 09:34a <DIR>           0 ..
04/14/15 09:56a              16,777,216 BIOS.bin
02/02/15 02:58p              405,104 AfuEfix64.efi
2 File(s) 17,182,320 bytes
2 Dir(s)
```

4. Execute the command to update the 16M BIOS.

```
FS0:\AfuEfi64\> AfuEfix64.efi BIOS.bin /b /p /n /x /k /l
+-----+
|          AMI Firmware Update Utility v5.12.02.2028          |
| Copyright (c) 1985-2019, American Megatrends International LLC. |
| All rights reserved. Subject to AMI licensing agreement.      |
+-----+
Reading flash ..... done
- ME Data Size checking . ok
- Secure Flash enabled, recalculate ROM size with signature... Enable.
- FFS checksums ..... ok
- Check RomLayout ..... ok.
Loading capsule to secure memory buffer ... done
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
_Erasing Main Block ..... 0x0028F000 (13%)
```

5. Execute the command to update the 32M ME+BIOS.

```
FS1:\afuefi64\> AfuEfix64.efi BIOS.bin /b /p /n /x /k /l /me
+-----+
|          AMI Firmware Update Utility v5.12.02.2028          |
| Copyright (c) 1985-2019, American Megatrends International LLC. |
| All rights reserved. Subject to AMI licensing agreement.      |
+-----+
Reading flash ..... done
- ME Data Size checking . ok
- Secure Flash enabled, recalculate ROM size with signature... Enable.
- FFS checksums ..... ok
- Check RomLayout ..... ok.
Loading capsule to secure memory buffer ... done
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
Erasing Main Block ..... done
Updating Main Block ..... done
Verifying Main Block ..... done
Erasing NVRAM Block ..... done
_Updating NVRAM Block ..... 0x00074000 (38%)
```

 **NOTE:** After the update is complete, power off the server, confirm that there is no residual electricity on the motherboard, and then power it on.

6.3.2 AMI Flash Utility

To update the firmware in Linux:

1. Boot the system to Linux OS.
2. Enter the directory containing the `afulnx_64` tool (for Linux 64bit OS) or `afulnx_32` tool (for Linux 32bit OS)
3. Copy the BIOS bin file into this folder.
4. Execute the command to update BIOS: `./afulnx_64 BIOS.bin /b /p /n /x /k /l`.

```

[root@localhost afulnx]# ./afulnx_64 BIOS.bin /b /p /n /x /k /l
-----
|          AMI Firmware Update Utility v5.12.02.2028          |
| Copyright (c) 1985-2019, American Megatrends International LLC. |
| All rights reserved. Subject to AMI licensing agreement.    |
|-----|
| Reading flash ..... done                                   |
| - ME Data Size checking . ok                               |
| - Secure Flash enabled, recalculate ROM size with signature... Enable. |
| - FFS checksums ..... ok                                  |
| - Check RomLayout ..... ok.                               |
| Loading capsule to secure memory buffer ... done          |
| Erasing Boot Block ..... done                             |
| Updating Boot Block ..... done                            |
| Verifying Boot Block ..... done                           |
| Erasing Main Block ..... done                             |
| Updating Main Block ..... done                            |
| Verifying Main Block ..... done                           |
| Erasing NVRAM Block ..... done                            |
| Updating NVRAM Block ..... done                           |

```

- Execute the command to update both BIOS and ME: `./afulnx_64 BIOS.bin /b /p /n /x /k /l /me.`


```

[root@localhost afulnx]# ./afulnx_64 BIOS.bin /b /p /n /x /k /l /me
-----
|          AMI Firmware Update Utility v5.12.02.2028          |
| Copyright (c) 1985-2019, American Megatrends International LLC. |
| All rights reserved. Subject to AMI licensing agreement.    |
|-----|
| Reading flash ..... done                                   |
| - ME Data Size checking . ok                               |
| - Secure Flash enabled, recalculate ROM size with signature... Enable. |
| - FFS checksums ..... ok                                  |
| - Check RomLayout ..... ok.                               |
| Loading capsule to secure memory buffer ... done          |
| Erasing Boot Block ..... done                             |
| Updating Boot Block ..... done                            |
| Verifying Boot Block ..... done                           |
| Erasing Main Block ..... done                             |
| Updating Main Block ..... done                            |
| Verifying Main Block ..... done                           |
| Erasing NVRAM Block ..... done                            |
| Updating NVRAM Block ..... done                           |
| Verifying NVRAM Block ..... done                          |
| Erasing NCB Block ..... done                             |
| Updating NCB Block ..... done                             |

```

 **NOTE:**

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

 **NOTE:** Parameter Instruction:

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

7. BMC Settings

This chapter describes the functional specifications of Inspur baseboard management controller (BMC) and its detailed information.

7.1 Introduction

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

The main functions of the Inspur Server Management System are:

- 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.
- IPMITool management
Supports the command operation sent by IPMITool. The IPMITool is downloadable: <http://ipmitool.sourceforge.net/manpage.html>.
- 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.
- Account centralized management
Store accounts in the Active Directory server, direct the authentication process to server, and achieve management system login with domain accounts.

7.2 Software Interfaces

The Baseboard Management Controller (BMC) offers remote management control for server system status monitoring. It is an embedded system running independently of host operation system which is able to perform a series of operations such as firmware upgrade, management control, and device status checking even when the host is shut down.

The BMC has the following features:

- Support IPMI 2.0, IPMI interfaces including KCS, Lan and IPMB
- Management Protocol: IPMI2.0, HTTPS, SNMP, Smash CLI
- Web GUI
- Redfish
- Management Network Interface, Dedicated/NCSI
- Console Redirection (KVM) and Virtual Media
- Serial Over Lan (SOL)
- Diagnostic Log, System Event Log (SEL), Inspur Diagnostic Logs and One-key collection log
- BMC hardware watchdog timer, if the BMC does not respond within four minutes, the fan will reach full speed.
- Support Intel® Intelligent Power Node Manager 4.0
- Event Alert: SNMP Trap (v1/v2c/v3), Email Alert and Syslog
- Dual BMC firmware image
- Firmware upgrade, BMC/BIOS/CPLD
- Device State Monitor and Diagnostic

7.2.1 IPMI 2.0

7.2.1.1 Channel ID Assignment for Each Interface

Table 7-1 Channel ID Assignment for Each Interface

Channel ID	Interface	Purpose	Support Sessions
0x00	Primary IPMB	Unused	No
0x06	Secondary IPMB	Access ME	No
0x0A	Third IPMB	Unused	No
0x01	Primary LAN	Dedicated management interface	Yes
0x08	Secondary LAN	Shared management interface	Yes
0x0F	KCS / SMS	In-band IPMI communication	No

7.2.1.2 System Interfaces

LPC interface is supported, and LPC provides hardware path for KCS messaging.

7.2.1.3 IPMB Interfaces

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

7.2.1.4 LAN interfaces

- Supports IPMI V2.0, compatible with V1.5
- Supports receiving and sending IPMI messages based on RMCP or RMCP+ format.
- Supports up to 2 LAN Interfaces (Dedicated NIC and Shared NIC).
- Supports cipher suites in IPMI, the supported cipher suites as lists below.

Table 7-2 Supported Cipher Suites in IPMI

ID	Authentication algorithm	Integrity algorithm	Confidentiality algorithm
1	RAKP-HMAC-SHA1	NONE	NONE
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC-MD5	NONE	NONE
7	RAKP-HMAC-MD5	HMAC-MD5-128	NONE
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	NONE
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_SHA256	NONE	NONE
16	RAKP_HMAC_SHA256	HMAC-SHA256-128	NONE
17	RAKP_HMAC_SHA256	HMAC-SHA256-128	AES-CBC-128

7.2.1.5 IPMI Commands

Tables below define the IPMI commands supported by the BMC.

Table 7-3 IPMI NetFn

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

Table 7-4 IPMI Spec Standard Commands

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Get Device ID	App	0x01	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Broadcast ‘Get Device ID’ [1]	App	0x02	YES
Cold Reset	App	0x03	YES
Warm Reset	App	0x04	YES
Get Self Test Results	App	0x05	YES
Manufacturing Test On	App	0x06	YES
Set ACPI Power State	App	0x07	YES
Get ACPI Power State	App	0x08	YES
Get Device GUID	App	0x09	YES
Get NetFn Support	App	0x10	YES
Get Command Support	App	0x0A	YES
Get Command Sub-function Support	App	0x0B	YES
Get Configurable Commands	App	0x0C	YES
Get Configurable Command Sub-functions	App	0x0D	YES
Set Command Enables	App	0x60	YES
Get Command Enables	App	0x61	YES
Set Command Sub-function Enables	App	0x62	YES
Get Command Sub-function Enables	App	0x63	YES
Get OEM NetFn IANA Support	App	0x64	YES
BMC Watchdog Timer Commands			
Reset Watchdog Timer	App	0x22	YES
Set Watchdog Timer	App	0x24	YES
Get Watchdog Timer	App	0x25	YES
BMC Device and Messaging Commands			
Set BMC Global Enables	App	0x2E	YES
Get BMC Global Enables	App	0x2F	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Clear Message Flags	App	0x30	YES
Get Message Flags	App	0x31	YES
Enable Message Channel Receive	App	0x32	YES
Get Message	App	0x33	YES
Send Message	App	0x34	YES
Read Event Message Buffer	App	0x35	YES
Get BT Interface Capabilities	App	0x36	YES
Get System GUID	App	0x37	YES
Set System Info Parameters	App	0x58	YES
Get System Info Parameters	App	0x59	YES
Get Channel Authentication Capabilities	App	0x38	YES
Get Session Challenge	App	0x39	YES
Activate Session	App	0x3A	YES
Set Session Privilege Level	App	0x3B	YES
Close Session	App	0x3C	YES
Get Session Info	App	0x3D	YES
Get AuthCode	App	0x3F	YES
Set Channel Access	App	0x40	YES
Get Channel Access	App	0x41	YES
Get Channel Info Command	App	0x42	YES
Set User Access Command	App	0x43	YES
Get User Access Command	App	0x44	YES
Set User Name	App	0x45	YES
Get User Name Command	App	0x46	YES
Set User Password Command	App	0x47	YES
Activate Payload	App	0x48	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Deactivate Payload	App	0x49	YES
Get Payload Activation Status	App	0x4A	YES
Get Payload Instance Info	App	0x4B	YES
Set User Payload Access	App	0x4C	YES
Get User Payload Access	App	0x4D	YES
Get Channel Payload Support	App	0x4E	YES
Get Channel Payload Version	App	0x4F	YES
Get Channel OEM Payload Info	App	0x50	YES
Master Write-Read	App	0x52	YES
Get Channel Cipher Suites	App	0x54	YES
Suspend/Resume Payload Encryption	App	0x55	YES
Set Channel Security Keys	App	0x56	YES
Get System Interface Capabilities	App	0x57	YES
Firmware Firewall Configuration	App	0x60-0x64	NO
Chassis Device Commands			
Get Chassis Capabilities	Chassis	0x00	YES
Get Chassis Status	Chassis	0x01	YES
Chassis Control	Chassis	0x02	YES
Chassis Reset	Chassis	0x03	YES
Chassis Identify	Chassis	0x04	YES
Set Front Panel Button Enables	Chassis	0x0A	YES
Set Chassis Capabilities	Chassis	0x05	YES
Set Power Restore Policy	Chassis	0x06	YES
Set Power Cycle Interval	Chassis	0x0B	YES
Get System Restart Cause	Chassis	0x07	YES
Set System Boot Options	Chassis	0x08	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Get System Boot Options	Chassis	0x09	YES
Get POH Counter	Chassis	0x0F	YES
Event Commands			
Set Event Receiver	S/E	0x00	YES
Get Event Receiver	S/E	0x01	YES
Platform Event (a.k.a. “Event Message”)	S/E	0x02	YES
PEF and Alerting Commands			
Get PEF Capabilities	S/E	0x10	YES
Arm PEF Postpone Timer	S/E	0x11	YES
Set PEF Configuration Parameters	S/E	0x12	YES
Get PEF Configuration Parameters	S/E	0x13	YES
Set Last Processed Event ID	S/E	0x14	YES
Get Last Processed Event ID	S/E	0x15	YES
Alert Immediate	S/E	0x16	YES
PET Acknowledge	S/E	0x17	YES
Sensor Device Commands			
Get Device SDR Info	S/E	0x20	YES
Get Device SDR	S/E	0x21	YES
Reserve Device SDR Repository	S/E	0x22	YES
Get Sensor Reading Factors	S/E	0x23	YES
Set Sensor Hysteresis	S/E	0x24	YES
Get Sensor Hysteresis	S/E	0x25	YES
Set Sensor Threshold	S/E	0x26	YES
Get Sensor Threshold	S/E	0x27	YES
Set Sensor Event Enable	S/E	0x28	YES
Get Sensor Event Enable	S/E	0x29	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Re-arm Sensor Events	S/E	0x2A	YES
Get Sensor Event Status	S/E	0x2B	YES
Get Sensor Reading	S/E	0x2D	YES
Set Sensor Type	S/E	0x2E	YES
Get Sensor Type	S/E	0x2F	YES
Set Sensor Reading And Event Status	S/E	0x30	YES
FRU Device Commands			
Get FRU Inventory Area Info	Storage	0x10	YES
Read FRU Data	Storage	0x11	YES
Write FRU Data	Storage	0x12	YES
SDR Device Commands			
Get SDR Repository Info	Storage	0x20	YES
Get SDR Repository Allocation Info	Storage	0x21	YES
Reserve SDR Repository	Storage	0x22	YES
Get SDR	Storage	0x23	YES
Add SDR	Storage	0x24	YES
Partial Add SDR	Storage	0x25	YES
Delete SDR	Storage	0x26	YES
Clear SDR Repository	Storage	0x27	YES
Get SDR Repository Time	Storage	0x28	YES
Set SDR Repository Time	Storage	0x29	YES
Enter SDR Repository Update Mode	Storage	0x2A	YES
Exit SDR Repository Update Mode	Storage	0x2B	YES
Run Initialization Agent	Storage	0x2C	YES
SEL Device Commands			
Get SEL Info	Storage	0x40	YES
Get SEL Allocation Info	Storage	0x41	YES

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Reserve SEL	Storage	0x42	YES
Get SEL Entry	Storage	0x43	YES
Add SEL Entry	Storage	0x44	YES
Partial Add SEL Entry	Storage	0x45	YES
Delete SEL Entry	Storage	0x46	YES
Clear SEL	Storage	0x47	YES
Get SEL Time	Storage	0x48	YES
Set SEL Time	Storage	0x49	YES
Get Auxiliary Log Status	Storage	0x5A	YES
Set Auxiliary Log Status	Storage	0x5B	YES
Get SEL Time UTC Offset	Storage	0x5C	YES
Set SEL Time UTC Offset	Storage	0x5D	YES
LAN Device Commands			
Set LAN Configuration Parameters	Transport	0x01	YES
Get LAN Configuration Parameters	Transport	0x02	YES
Suspend BMC ARPs	Transport	0x03	YES
Get IP/UDP/RMCP Statistics	Transport	0x04	NO
Serial/Modem Device Commands			
Set Serial/Modem Configuration	Transport	0x10	YES
Get Serial/Modem Configuration	Transport	0x11	YES
Set Serial/Modem Mux	Transport	0x12	YES
Get TAP Response Codes	Transport	0x13	NO
Set PPP UDP Proxy Transmit Data	Transport	0x14	NO
Get PPP UDP Proxy Transmit Data	Transport	0x15	NO
Send PPP UDP Proxy Packet	Transport	0x16	NO

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Get PPP UDP Proxy Receive Data	Transport	0x17	NO
Serial/Modem Connection Active	Transport	0x18	NO
Callback	Transport	0x19	YES
Set User Callback Options	Transport	0x1A	YES
Get User Callback Options	Transport	0x1B	YES
Set Serial Routing Mux	Transport	0x1C	NO
SOL Activating	Transport	0x20	NO
Set SOL Configuration Parameters	Transport	0x21	YES
Get SOL Configuration Parameters	Transport	0x22	YES
Command Forwarding Commands			
Forwarded Command	Bridge	0x30	NO
Set Forwarded Commands	Bridge	0x31	NO
Get Forwarded Commands	Bridge	0x32	NO
Enable Forwarded Commands	Bridge	0x33	NO
Bridge Management Commands (ICMB)			
Get Bridge State	Bridge	0x00	NO
Set Bridge State	Bridge	0x01	NO
Get ICMB Address	Bridge	0x02	NO
Set ICMB Address	Bridge	0x03	NO
Set Bridge ProxyAddress	Bridge	0x04	NO
Get Bridge Statistics	Bridge	0x05	NO
Get ICMB Capabilities	Bridge	0x06	NO
Clear Bridge Statistics	Bridge	0x08	NO
Get Bridge Proxy Address	Bridge	0x09	NO
Get ICMB Connector Info	Bridge	0x0A	NO
Get ICMB Connection ID	Bridge	0x0B	NO

IPMI Device “Global” Command	NetFn	CMD	SUPPORT
Send ICMB Connection ID	Bridge	0x0C	NO
Discovery Commands (ICMB)			
PrepareForDiscovery	Bridge	0x10	NO
GetAddresses	Bridge	0x11	NO
SetDiscovered	Bridge	0x12	NO
GetChassisDeviceId	Bridge	0x13	NO
SetChassisDeviceId	Bridge	0x14	NO
Bridging Commands (ICMB)			
BridgeRequest	Bridge	0x20	NO
BridgeMessage	Bridge	0x21	NO
Event Commands (ICMB)			
GetEventCount	Bridge	0x30	NO
SetEventDestination	Bridge	0x31	NO
SetEventReceptionState	Bridge	0x32	NO
SendICMBEventMessage	Bridge	0x33	NO
GetEventDestination (optional)	Bridge	0x34	NO
GetEventReceptionState (optional)	Bridge	0x35	NO

7.2.2 Web GUI

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

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

The Web GUI is supported by following browsers:

Table 7-1 Supported Browsers

Client OS	Browser Versions
Windows 7.1 x64	On Windows Clients: Edge ,Firefox 43, Chrome 47+, IE 11+
Windows 8 x64	
Windows 10 x64	


Ubuntu 14.04.03 LTS x64 MAC OS X
Fedora 23 x64
CentOS 7 x64

Firefox 43, Chrome 47+
On MAC Client: Safari

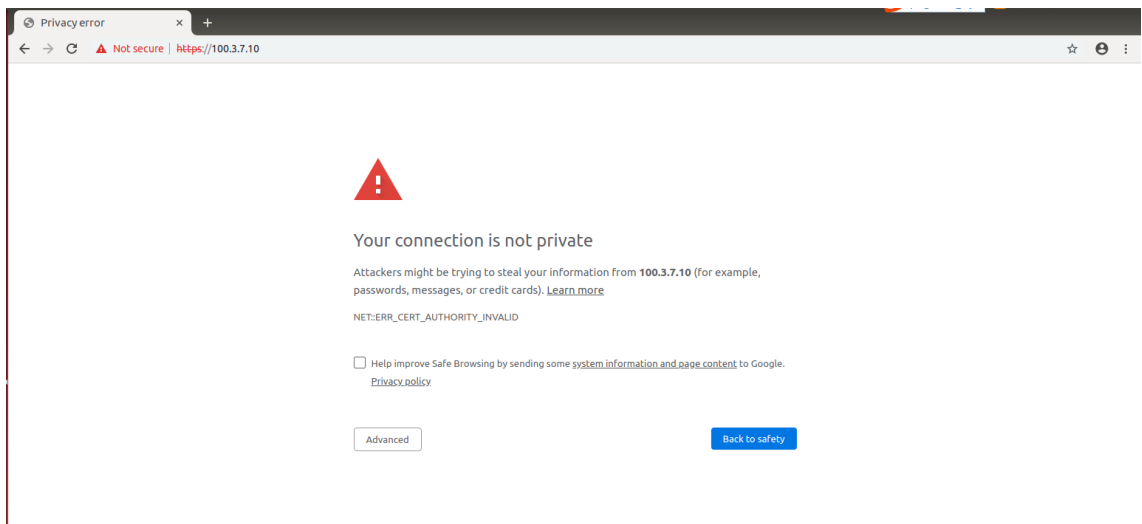
7.2.2.1 Web GUI Login

Step 1

Type "https://BMC_IP" in the browser address bar.

 **NOTE:** The port number is modifiable (For more information, see [7.7.2 Service Settings](#)). The http port number is 80 (disabled by default), and the https port number is 443. If the port number is modified, the user need to specify the port number when log-in, for example https://BMC_IP: sslport.

When log-in the BMC WEB for the first time, it will pop up a security warning message. For Chrome or Firefox browser, click the "Advanced" button and then click **Proceed to BMC_IP** to continue.

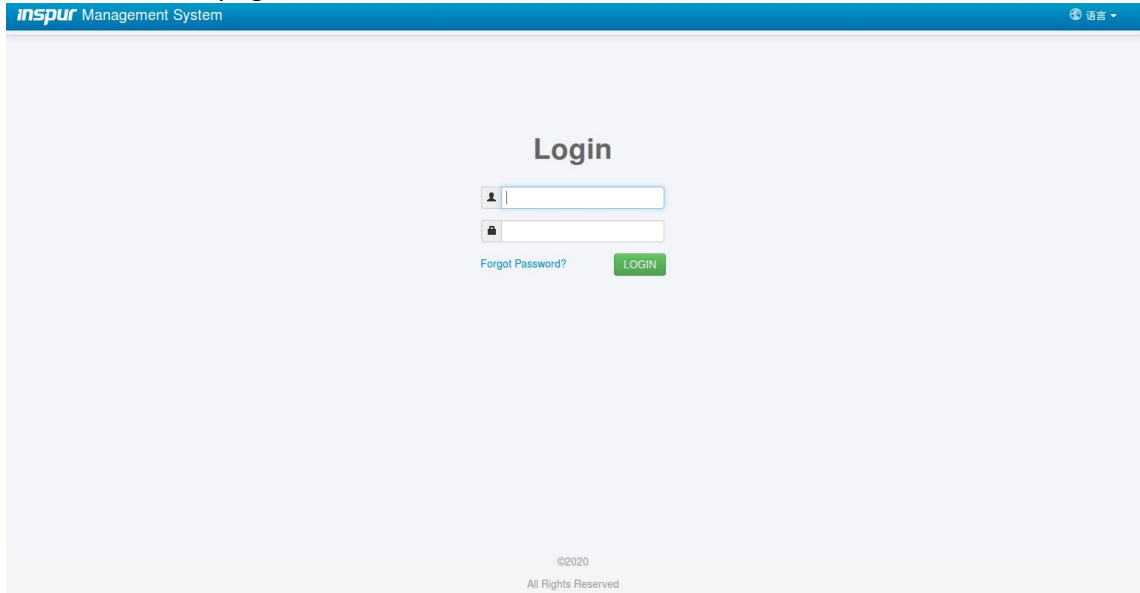


For Internet Explorer, click "**Continue to this website (not recommended)**" to continue.



Step 2

In the WEB login page, enter the user name and password, click the “**Login**” button to enter the home page.



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

7.2.2.2 Web GUI Introduction

The Web interface helps the users to accomplish server management. User can click the “help” button to launch the help function.

The name of the Web interface is displayed on the upper left corner.

The operating buttons are displayed on the upper right corner:

- Overview: click to return to the overview page.
- Refresh: click to refresh the current page.
- Language: click to change the language (Chinese or English).
- Help: click to query on the related corresponding question.
- Logout: click to return to the login page.

To access the functional interfaces, click the navigation tree on the left side. The functions include: Information, Remote Control, Power and Fan, BMC settings, Logs, Fault Diagnosis and System maintenance. For detailed information, please refer to the following chapters.

The specific operation interface is on the right side.

7.2.2.3 Web GUI Features

The following table lists the main features supported in Web GUI.

Table 7-2 Features supported in Web GUI

Menu	Subdirectory	Auto Refresh Support	Main content
Overview	General Information	YES	System Running State
			BMC information and server information
			Quick Launch Tasks
			Active Session
			FW Version Information
			Recent System Event Logs
Information	System Info	YES	Device asset info and health state, include: CPU Memory Device Inventory Network Fan Temperature Voltage
	BIOS Setup Options	NO	Display main setup options
	FRU Information	NO	Display BMC field replaceable unit information
	History Record	YES	Last Day/Last Month/Last Year - Inlet history curve, and total power history curve, Current Power, Minimum Power, Maximum Power, Average Power
Remote Control	Console Redirection	NO	HTML5 KVM Java KVM
	Locate Server	YES	Display UID status Turn on/off UID
	Remote Session	NO	Virtual media settings for redirected sessions
	Virtual Media	NO	Virtual media settings
	Mouse Mode	NO	Settings for mouse mode for redirecting the console
Power and Fan	Server Power Control	YES	Power on/off/reset/cycle Power Restore Setting

Menu	Subdirectory	Auto Refresh Support	Main content
	Fan Speed Control	YES	Display fan speed and state; Switch to manually fan control
BMC Settings	BMC Network	NO	BMC Network Setting BMC DNS Setting Network Interface Bonding Network Link
	Services	NO	Supported service or protocol setting
	NTP	NO	BMC time setting
	SMTP	NO	SMTP setting for email alert
	Alerts	NO	SNMP Trap and email alert setting
	Access Control	NO	IP/MAC access restrictions policy
	BIOS Boot Options	NO	BIOS Boot Options setting
Logs	System Event Log	NO	Display system event log (SEL)
	BMC System Audit Log	NO	Display audit Log
	Event Log Setting	NO	System event log storage strategy
	BMC System Audit Log Setting	NO	BMC Syslog setting
	One-key Collection Log	NO	Collect logs with one click
Fault Diagnosis	BMC Self-inspection Result	YES	Display BMC self-inspection result
	BMC Recovery	NO	Manually reset BMC or KVM
	Capture Screen	NO	Auto Capture and Manual Capture
	Host POST Code	YES	Display current and history POST code
Administration	User Administration	NO	Local Users setting BMC System Administrator Directory Group setting
	Security	NO	LDAP setting AD setting
	Dual Image Configuration	Dual Image	Dual Image
	Dual Firmware	NO	Upgrade BMC firmware

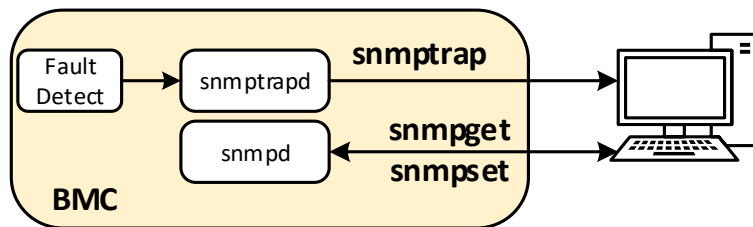
Menu	Subdirectory	Auto Refresh Support	Main content
	Update		
	BIOS FW Update	NO	Upgrade BIOS firmware
	Restore Factory Defaults	NO	Restore BMC settings to factory defaults

7.2.3 SNMP

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

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

- Support SNMP Get/Set/Trap.
- Support V1/V2C/V3 version.
- SNMPv3 supports authentication algorithm MD5 or SHA, and encryption algorithm to DES or AES.
- SNMP Get supports querying system health status, sensor status, hardware status, device asset information, etc.
- SNMP Set supports local users or network users to power on/off machine and perform other operations.
- SNMP Trap supports IPMI-based Trap messages



7.2.4 Smash-Lite CLI

7.2.4.1 Command Line Login

BMC supports Smash-Lite CLI, users can login to BMC via SSH and enter Smash-Lite CLI. After logging in, you can enter the command line interface.

```

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

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

```

7.2.4.2 Command Line Features

Smash-Lite CLI supports ipconfig, sensor, fru, chassis, user, mc, fan, cpld, id, and diagnose commands. See the description below for the usage of each command.

1. Get and Set Network Information

You can get and set the BMC network information using `ipconfig` commands.

```

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

```

2. Get Sensor Information

You can get a list of all sensor information using `sensor` commands.

```
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]
```

3. Get and Set FRU Information

You can get and set the FRU information using `fru` commands.

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

4. Get and Control Chassis Status

You can get and control the system power status using `chassis` commands.

```
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
```

5. Get, Add, and Delete Users

You can access and edit (add or delete) the user list using `user` commands.

```

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

```

6. Get BMC Versions and Reboot BMC

You can get the BMC version information and reboot the BMC using `mc` commands

```

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

```

7. Get and Set Fan Information

You can get the fan information and setup the fan mode and fan level using `fan` commands.

```

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

```

8. CPLD

You can operate CPLD using `cp1d` commands.

```

cp1d commands:
cp1d <host_ip> <tftp_port> <cpld_image_file>
for example : cp1d <host_ip> <tftp_port> <cpld_image_file>

```

9. Get ID

You can get the UUID and SN information using `id` commands.

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

10. Fault Diagnosis

You can execute the common tools and commands to check the BMC operating status using `diagnostic` commands.

```
diagnose commands:
  diagnose <option> [<parameter1>] [<parameter2>...]
  option:
    --help      show help information
    ?          show help information
  bmc diagnose support command:
    ls          show log file profile, only support parameter1 select log file
    cat        show log file content, only support parameter1 select log file
    last       show listing of last logged in users
    ifconfig   show and configure network info
    ethtool    show and configure phy configuration
    ps         report a snapshot of the current processes
    top        display Linux tasks
    dmesg      print or control the kernel ring buffer
    netstat    Print network connections and routing tables etc.
    gpiotool   bmc gpio test tool
    i2c-test   bmc i2c test tool
    pwmtachtool bmc fan test tool
    ipmitool   bmc ipmitool tool
    df         bmc df info
    uptime     bmc running time
  parameter1:
    only support for option ls and cat command
    ncm1       bmc service configuration
    log        bmc system log   cat log in ROOT user
    cpuinfo    bmc cpu info
    meminfo    bmc memory info
    versioninfo bmc version info
    crontab    bmc crontab file
  for example : diagnose ls ncm1
  for example : diagnose cat log debug.log
```

7.3 System Overview

When log-in to the WEB GUI, the system overview page is displayed. It contains the server health information, management device information, server information, online user information, firmware version information, and a list of recent event logs.

7.3.1 System Running State

The general information shows the operating status of the device.

■ General Information

System Running State	
Current Power Status	
UID State	
CPU	
Fan	
Fan redundancy	
Voltage	
Temperature	
ME	

Item	Description
Current Power Status	Power On Power Off
UID Status	UID LED On UID LED Off
CPU	CPU Healthy state: <ul style="list-style-type: none"> ✔ Normal – All CPUs Normal ⚠ Warning – One or more CPUx_Status warning ✖ Critical – One or more CPUx_Status critical ● Power Off
Fan	Fan Healthy state: <ul style="list-style-type: none"> ✔ Normal – All Fans Normal ✖ Critical – One or more fans fail ● Power Off
Fan Redundancy	Fan Redundant state: <ul style="list-style-type: none"> ✔ Normal – All Fans Normal ✖ Critical – One or more fans absent or cannot be read ● Power Off
Voltage	Voltage Sensor state: <ul style="list-style-type: none"> ✔ Normal ⚠ Warning – One or more Voltage Sensors warning ✖ Critical – One or more Voltage Sensors critical ● Power Off
Temperature	Temperature Sensor state: <ul style="list-style-type: none"> ✔ Normal ⚠ Warning – One or more Temperature Sensors warning ✖ Critical – One or more Temperature Sensors critical ● Power Off
ME	ME state: <ul style="list-style-type: none"> ✔ Normal ⚠ Warning – ME_FW_Status Sensor warning ✖ Critical – ME_FW_Status Sensor critical ● State unavailable or current power is off

7.3.2 Management Device (BMC) Information and Server information

The general information also shows the BMC information and server information.

BMC Information	
Lan Interface	eth0
MAC Address	B4:05:5D:34:30:0D
Network Mode	DHCP
IPv4 Address	100.2.76.110
Server Running Time	0 Day, 0 Hour
Server Information	
Chassis Type	RAID Chassis
Product Name	ON5263M5
Manufacture Name	Inspur
Product Serial Number	P10020783800
Asset Tag	YAHOO
UUID	345d05b4-0d30-03db-b211-d21dc051bd19

7.3.3 Quick Launch

The quick launch tasks allows you to perform the shortcut operations.

Quick Launch Tasks		
Console Redirection	Power Control	Users
Network	Hardware Monitor	Firmware Update

7.3.4 Online User Information

The active session shows the on-line user information about the information of the current-user logged in on the BMC WEB, including the user type, user name, user privilege, and IP address.

Active Session			
User Type	User Name	User Privilege	IP Address
HTTPS	admin	Administrator	100.3.2.1

7.3.5 Firmware Version Information

The FW version information shows the latest version of the firmware in the platform, including BMC, BIOS, ME and CPLD.

FW Version Information	
BMC	3.1.0 (2020-05-20 20:53:48)
BIOS	3.0.0 (2020/04/23 13:52:12)
ME	0A:4.1.4.339
CPLD	1.0

Firmware Item	Description
BMC	Revision and Build Time
BIOS	Revision and Build Time
ME	Revision
CPLD	Revision

7.3.6 Recent Event Logs

The recent system event log shows the recent event log information. Click "**More**" for more event logs.

Recent System Event Log [More]					
Event ID	Time Stamp	Severity	Sensor Name	Sensor Type	Description
4	05/21/2020 08:19:10		CPU0_Status	Processor	Processor Presence Detected - Asserted
3	05/21/2020 08:19:08		ACPI_State	System ACPI Power State	Legacy ON State - Asserted
2	Pre-init Timestamp		BMC_Boot_up	Microcontroller / Coprocessor	Invalid Offset for this SensorType - Asserted
1	Pre-init Timestamp		BMC_FW	Version Change	Firmware / Software Change Detected - Asserted

7.4 Information

7.4.1 System Information

On the WEB GUI, go to the **Information** → **System Information**. The system information page shows the information and health status of main components of platform, including CPU, memory, device inventory, network, fan, temperature and voltage.

System Information

- CPU**
- Memory
- Device Inventory
- Network
- FAN
- Temperature
- Voltage

Click on the **CPU** tab to see the CPU information.

System Information									
CPU Memory Device Inventory Network FAN Temperature Voltage									
No.	Processor Name	Processor Status	Processor Speed	Core	TDP(W)	L1 Cache(KB)	L2 Cache(KB)	L3 Cache(KB)	
CPU0	Intel(R) Xeon(R) Platinum 8256 CPU @ 3.80GHz		3800	4/4	105	64	1024	16896	
CPU1	N/A		N/A	N/A	N/A	N/A	N/A	N/A	

Note:

- Present
- Absent
- Normal
- Warning
- Critical

Item	Description
No.	x, x denotes the number of CPU
Processor Name	Processor name
Processor Status	Normal Warning

Item	Description
	✘ Critical ● Absent or PowerOff
Processor Speed	Processor speed
Core	Core number
TDP(W)	TDP
L1 Cache (KB)	L1 Cache
L2 Cache (KB)	L2 Cache
L3 Cache (KB)	L3 Cache

Click on the **Memory** tab to see the memory information.

■ System Information

CPU Memory Device Inventory Network FAN Temperature Voltage										
No.	Location	Present	Size(GB)	Type	Maximum Frequency(MHz)	Manufacturer	Part Number	Serial Number	Minimum Voltage(mV)	Ranks
0	CPU0_C0D0	●	32	DDR4	2133	Samsung	M393A4K40BB0-CPB	40CAD562	1200	2
1	CPU0_C0D1	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	CPU0_C1D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	CPU0_C2D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	CPU0_C3D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	CPU0_C3D1	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	CPU0_C4D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	CPU0_C5D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	CPU1_C0D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	CPU1_C0D1	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	CPU1_C1D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	CPU1_C2D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	CPU1_C3D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	CPU1_C3D1	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	CPU1_C4D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	CPU1_C5D0	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note:

● Present ● Absent ● Normal ▲ Warning ✘ Critical

Click on the **Device Inventory** tab to see the device inventory information.

■ System Information

CPU Memory Device Inventory Network FAN Temperature Voltage											
No.	Slot on Board	Slot on Riser	Connection Type	Present	Device Type	Device(ID)	Vender(ID)	Rated Width	Rated Speed	Current Width	Current Speed
0	OCPA+B_CPU0	None	No Riser	●	Network Controller	MT27710 Family [ConnectX-4 Lx]	Mellanox Technologies	X8	GEN3	X8	GEN3
1	PCIE0_CPU0	Down	RiserType2-X8+X16	●	Mass Storage Controller	Toshiba KXG6 PCIE M.2	Toshiba	X4	GEN3	X4	GEN3

Note:

● Present ● Absent ● Normal ▲ Warning ✘ Critical

Click on the **Network** tab to see the BMC and System adapter information.

System Information

CPU Memory Device Inventory **Network** FAN Temperature Voltage

BMC Adapter

No.	Name	MAC Address	IP Address
0	eth0	B4:05:5D:34:30:0D	100.2.76.110

System Adapter

No.	Present	Location	Port Number	MAC Address
0		OCPA+B_CPU0	1	24:8A:07:B2:75:8E 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00

Note:

Present Absent Normal Warning Critical

Click on the **FAN** tab to see the fan information.

System Information

CPU Memory Device Inventory Network **FAN** Temperature Voltage

No.	Present	Status	Speed(rpm)	Duty Ratio(%)
FAN_0_Front			3750	19
FAN_0_Rear			3450	19
FAN_1_Front			4050	19
FAN_1_Rear			3600	19

Note:

Present Absent Normal Warning Critical

Item	Description
No.	FANx_y, x denotes FAN or FAN group number, y denotes the FAN number in group.
Present	Present Absent
Status	Normal Warning Critical State unavailable or current power is off
Speed (rpm)	Speed in rpm
Duty Ratio (%)	Speed in duty

Click on the **Temperature** tab to see the temperature information.

System Information

System Information								
CPU	Memory	Device Inventory	Network	FAN	Temperature	Voltage		
Sensor	Status	Reading(°C)	Low NRT(°C)	Low CT(°C)	Low NCT(°C)	Up NCT(°C)	Up CT(°C)	Up NRT(°C)
Inlet_Temp	✔	37	N/A	N/A	N/A	40	42	N/A
Outlet_Temp	✔	31	N/A	N/A	N/A	N/A	N/A	N/A
CPU0_Temp	✔	42	N/A	N/A	N/A	98	100	N/A
CPU1_Temp	●	N/A	N/A	N/A	N/A	110	112	N/A
CPU0_DTS	✔	58	N/A	N/A	N/A	N/A	N/A	N/A
CPU1_DTS	●	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CPU0_DIMM_Temp	✔	34	N/A	N/A	N/A	83	85	N/A
CPU1_DIMM_Temp	●	N/A	N/A	N/A	N/A	83	85	N/A
PCH_Temp	✔	43	N/A	N/A	N/A	95	100	N/A
OCP_Temp	✔	77	N/A	N/A	N/A	100	105	N/A

Note:

● Present ● Absent ✔ Normal ⚠ Warning ❌ Critical

Item	Description
Sensor	Sensor name
Status	<ul style="list-style-type: none"> ✔ Normal ⚠ Warning ❌ Critical ● State unavailable or current power is off
Reading (°C)	Temperature reading
Low NRT (°C)	Low Non Recoverable Threshold
Low CT (°C)	Low Critical Threshold
Low NCT (°C)	Low Non Critical Threshold
Up NCT (°C)	Up Non Critical Threshold
Up CT (°C)	Up Critical Threshold
Up NRT (°C)	Up Non Recoverable Threshold

Click on the **Voltage** tab to see the voltage information.

System Information

System Information								
CPU	Memory	Device Inventory	Network	FAN	Temperature	Voltage		
Sensor	Status	Reading(V)	Low NRT(V)	Low CT(V)	Low NCT(V)	Up NCT(V)	Up CT(V)	Up NRT(V)
P3V3	✔	3.27	2.87	2.97	3.07	3.53	3.63	3.73
P5V	✔	5.08	4.34	4.5	4.64	5.34	5.5	5.64
P12V	✔	12.42	10.86	11.22	11.4	13.56	13.74	14.1
PCH_P1V05	✔	1.06	0.91	0.95	0.98	1.13	1.16	1.19
PCH_VNN	✔	1.01	0.74	0.77	0.79	1.07	1.1	1.13

Note:

● Present ● Absent ✔ Normal ⚠ Warning ❌ Critical

Item	Description
Sensor	Sensor name

Item	Description
Status	✔ Normal
	⚠ Warning
	✖ Critical
	● State unavailable or current power is off
Reading (V)	Voltage reading
Low NRT (V)	Low Non Recoverable Threshold
Low CT (V)	Low Critical Threshold
Low NCT (V)	Low Non Critical Threshold
Up NCT (V)	Up Non Critical Threshold
Up CT (V)	Up Critical Threshold
Up NRT (V)	Up Non Recoverable Threshold

NOTE: If the threshold value is N/A, it means the sensor is not configured.

7.4.2 BIOS Setup Options

On the WEB GUI, go to the **Information** → **BIOS Setup Options**.

Users can modify the option value using IPMI OEM CMD, and the BIOS will update the setup options after the system reboot. The BIOS sends the BIOS setup options to the BMC when the BIOS POST is completed.

■ BIOS Setup Options

Advanced | Chipset | Processor | Server Mgmt | Boot

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

Save

7.4.3 FRU Information

On the WEB GUI, go to the **Information** → **FRU Information**. The FRU information page shows the basic information, chassis information, motherboard information, and product information.

FRU Information

Attribute	Value
FRU Device ID	0
FRU Device Name	BMC_FRU

The FRU information is stored in EEPROM. BMC will read the FRU information from EEPROM when BMC boots, the FRU information will not lose after BMC firmware is upgraded.

Item	Description
Basic Information	FRU device ID: 0
	FRU device name: BMC_FRU
Chassis Information	Chassis information area format version: *
	Chassis type: *
	Chassis part number: ** Chassis serial number: **
Board Information	Board information area format version: *
	Manufacture date time: weekday/month/day/year
	Board manufacturer: Inspur
	Board product name: *****
	Board serial number: ** Board part number: **
Product Information	Product information area format version: *
	Manufacture name: Inspur
	Product name: *****
	Product part number: ** Product version: **
	Product serial number: ** Asset Tag: **

7.4.4 History Record

BMC provides the curve-based inlet temperature and power monitoring statistics. Administrators can know the actual use of electricity and cooling resources through energy monitoring devices. Users can optimize the server's energy savings based on the historical data.

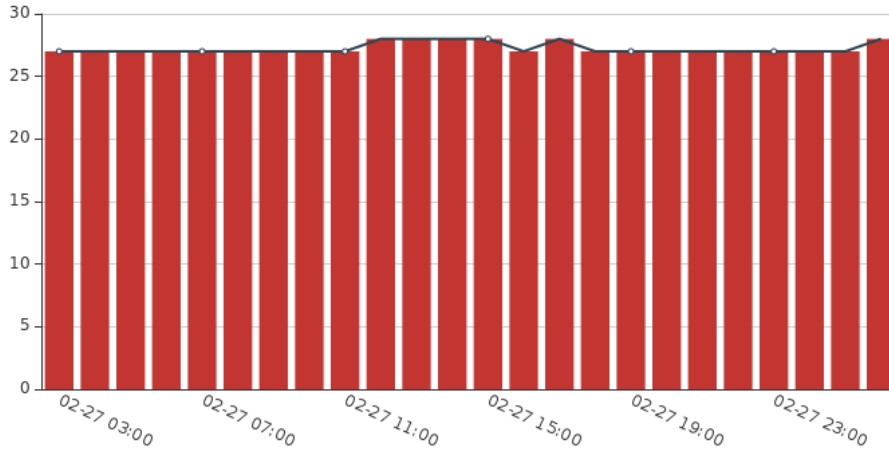
On the WEB GUI, go to the **Information** → **History Record**. The history record page shows the system current power, CPU total power, total memory power and a specific period of peak power, average power, and cumulative power consumption.

History Record

Last Day Last Month Last Year

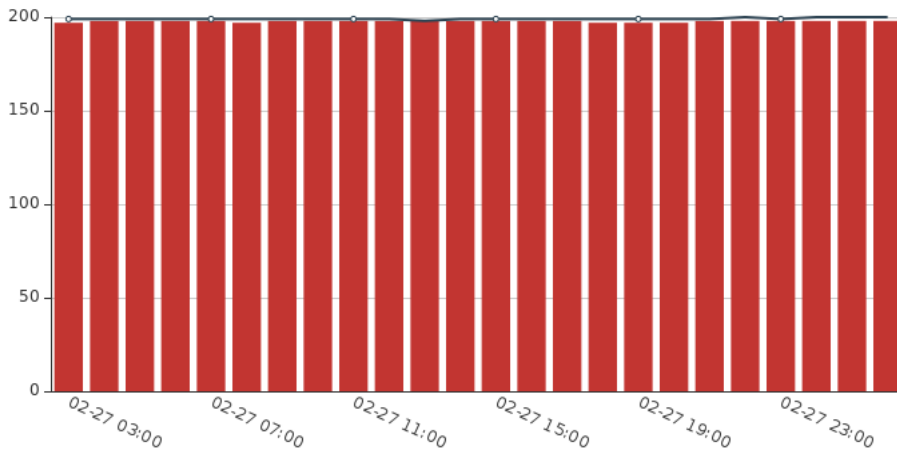
Inlet Temperature

Average Temperature Max Temperature



Total Power

Average Power Max Power

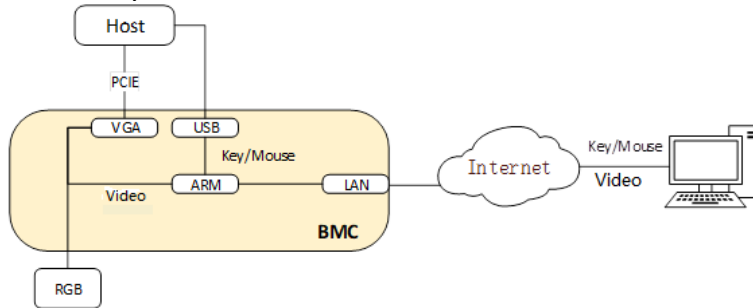


Current Power	198
Minimum Power	10
Maximum Power	251
Average Power	200

7.5 Remote Control

7.5.1 Console Redirection (KVM)

Remote KVM redirects the host system’s console to user’s PC by BMC. When the user logs in to BMC and open KVM, then host’s screen will be displayed in KVM application. User then can use PC’s keyboard and mouse to control the server.

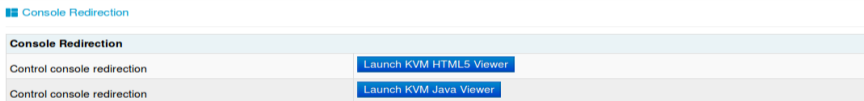


7.5.1.1 HTML5 KVM

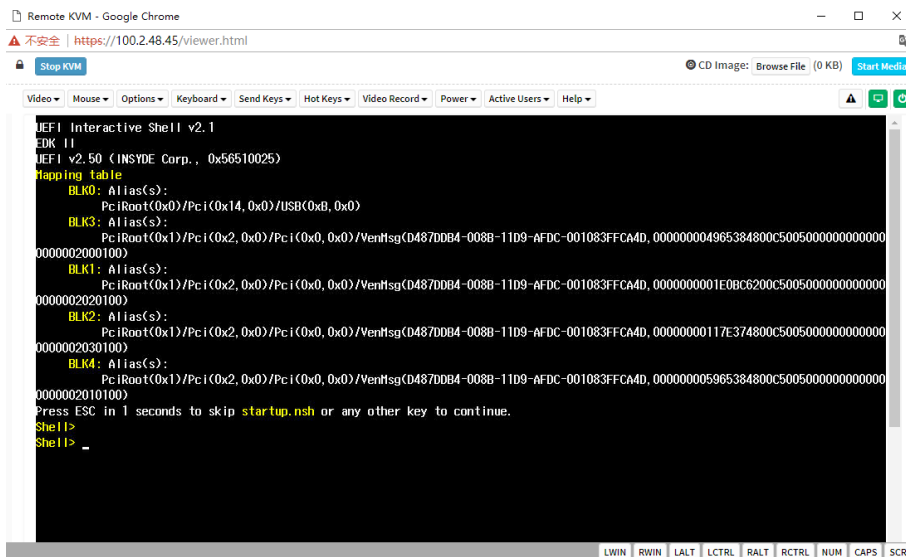
BMC supports HTML5 KVM (for Google Chrome 58 and above, and Internet Explorer 11 and above). Not depend on JAVA, .NET.

On the WEB GUI, go to the **Remote Control** → **Console Redirection**, and then click

Launch KVM HTML5 Viewer.



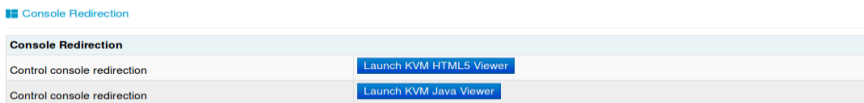
The HTML5 KVM is displayed.



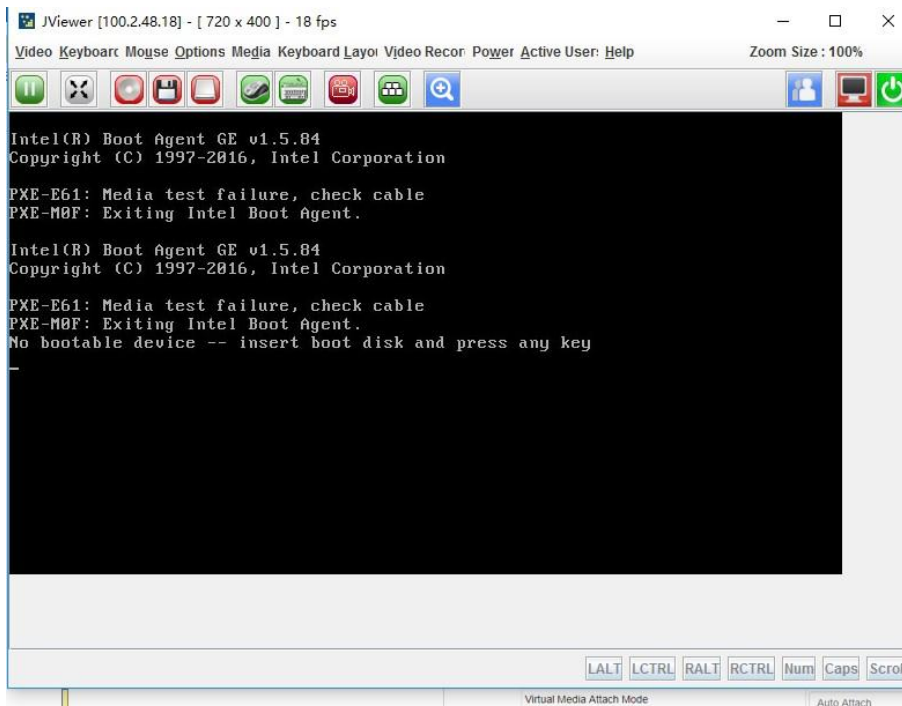
7.5.1.2 Java KVM

BMC supports Java KVM. To enter the JRE environment , users should download and open JNLP (Java Application). The supported JRE version: jre-7u40 and above; and jre-8u45 and above.

On the WEB GUI, go to the **Remote Control** → **Console Redirection**, and then click **Launch KVM Java Viewer**.



The Java KVM is displayed.



7.5.2 Locate Server

User can locate the managed server with the UID LED which is controlled by BMC or UID button. You can turn on/off the UID by pressing the UID button even BMC is not connected.

On the WEB GUI, go to the **Remote Control** → **Server Location** to configure the UID.

To turn on the UID for a specified time, select the time period in the “**System ID LED Light Time**” and click on “**Turn On Led**” button. To turn off the UID, click on “**Turn Off Led**” button.

Server Location

Server Location	
System ID LED Status	<input type="radio"/>
System ID LED Light Time	<input checked="" type="radio"/> All the time <input type="radio"/> 10s <input type="radio"/> 20s <input type="radio"/> 60s <input type="radio"/> Other <input type="text"/> s
System ID LED Operation	<input type="button" value="Turn On Led"/> <input type="button" value="Turn Off Led"/>

7.5.3 Remote Session Settings

On the WEB GUI, go to the **Remote Control** → **Configure Remote Session** to configure the remote session settings. KVM can be reconnected after network is disconnection.

The retry count range is 1-20 (12 by default), and the retry time interval is 5-30 (10 second by default).

Configure Remote Session

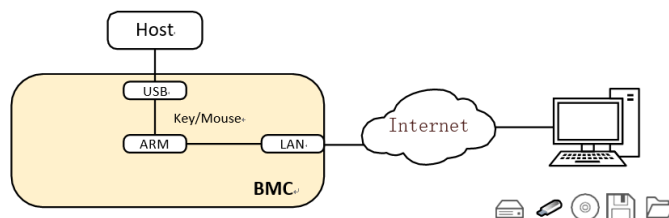
Configure Remote Session	
Encrypt KVM packets	<input type="checkbox"/> Enable
Keyboard Language	Auto Detect (AD) ▾
Virtual Media Attach Mode	Auto Attach ▾
Retry Count	3 ▾
Retry Time Interval(Seconds)	10 ▾
Server Monitor OFF Feature Status	<input checked="" type="checkbox"/> Enable
Automatically OFF Server Monitor, When KVM Launches	<input type="checkbox"/> Enable

7.5.4 Virtual Media Settings

The media redirection function allows the user to use various media devices and images on the client side (Local Media Support) or remote side (Remote Media Support), and attach them as virtual USB on the server side in which the BMC is present.

The virtual media supports:

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



On the WEB GUI, go to the **Remote Control** → **Virtual Media Devices** to configure the virtual media, including Virtual Media Setup and Virtual Media Instance.

To enable/disable the local media support or remote media support, click the checkbox in the **Virtual Media Setup** tab.

Virtual Media Devices

Virtual Media Setup | Virtual Media Instance

Virtual Media Setup	
Local Media Support	<input type="checkbox"/> Enable
Remote Media Support	<input type="checkbox"/> Enable

To emulate a SD Media on BMC as a USB device to the Host Server, click the SD Media Support checkbox in the **Virtual Media Instance** tab

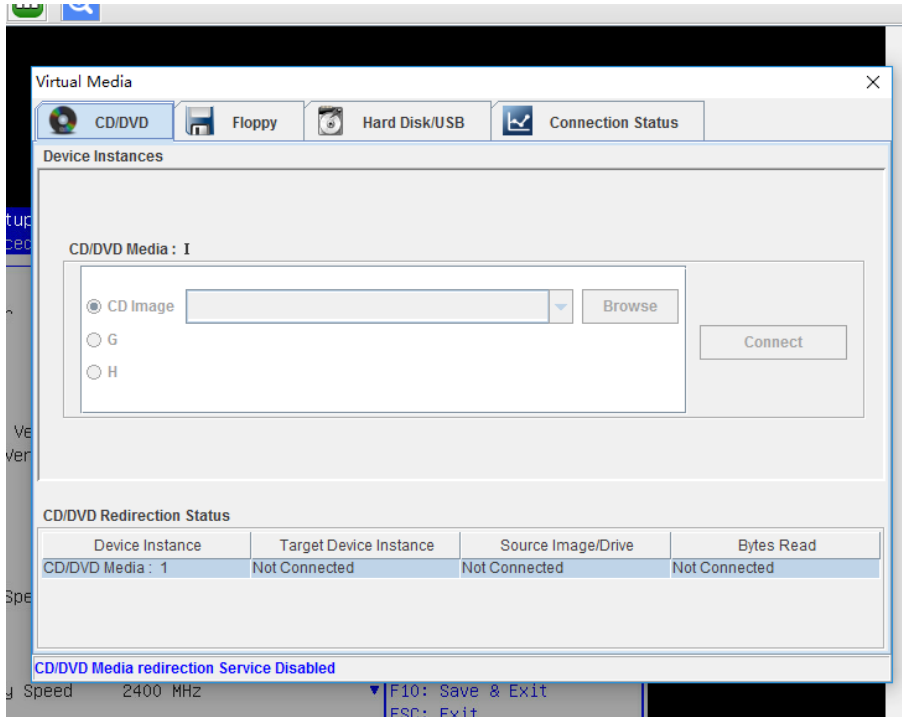
To enable/ disable the virtual USB devices visibility in the host server, click the Power Save Mode checkbox in the **Virtual Media Instance** tab. If this option is enabled, Virtual media devices will be connected to the Host machine only at the instance launching KVM session. If this option is disabled, Virtual media devices will remain connected to the host machine all the time irrespective of KVM session status.

Virtual Media Devices

Virtual Media Setup | Virtual Media Instance

Virtual Media Instance	
Floppy devices	1
CD/DVD devices	1
Harddisk devices	1
Remote KVM Floppy devices	1
Remote KVM CD/DVD devices	1
Remote KVM Hard disk devices	1
SD Media Support	<input type="checkbox"/> Enable
Encrypt Media Redirection Packets	<input type="checkbox"/> Enable
Power Save Mode	<input checked="" type="checkbox"/> Enable

User can also install the virtual media in KVM as shown below.



7.5.5 Mouse Mode Settings

On the WEB GUI, go to the **Remote Control** → **Mouse Mode Settings** to configure the mouse mode.

[Mouse Mode Settings](#)

Mouse Mode Settings	
Current Mouse Mode	Absolute
Mouse Mode Options	<input type="radio"/> Relative (Recommended for Linux(Except Redhat) running on Host) <input checked="" type="radio"/> Absolute (Recommended for Windows and Redhat running on Host) <input type="radio"/> Other (Try this, when relative and absolute mode can't work properly)

Host OS	Client OS			
	Windows 8	Windows 7	Windows Server 2012	Windows Server 2008 R2
RHEL 5.2	Relative	Relative	Relative	Relative
RHEL 5.4	Relative	Relative	Relative	Relative
RHEL 5.6	Relative	Relative	Relative	Relative
RHEL 6.0	Absolute	Absolute	Absolute	Absolute

Host OS	Client OS			
	Windows 8	Windows 7	Windows Server 2012	Windows Server 2008 R2
RHEL 6.4	Absolute	Absolute	Absolute	Absolute
RHEL 7.0	Absolute	Absolute	Absolute	Absolute
Fedora10	Relative	Relative	Relative	Relative
Fedora11	Absolute	Absolute	Absolute	Absolute
Fedora12	Absolute	Absolute	Absolute	Absolute
Fedora14	Absolute	Absolute	Absolute	Absolute
Fedora15	Absolute	Absolute	Absolute	Absolute
Fedora18	Absolute	Absolute	Absolute	Absolute
Fedora19	Absolute	Absolute	Absolute	Absolute
Fedora 20	Absolute	Absolute	Absolute	Absolute
Cent OS 5.4	Absolute	Absolute	Absolute	Absolute
Cent OS 6.0	Relative	Relative	Relative	Relative
Cent OS 6.1	Absolute	Absolute	Absolute	Absolute
Cent OS 6.2	Absolute	Absolute	Absolute	Absolute
Ubuntu 8.10	Absolute	Absolute	Absolute	Absolute
Ubuntu 9.10	Absolute	Absolute	Absolute	Absolute
Ubuntu 11.04	Absolute	Absolute	Absolute	Absolute
Ubuntu 12.04	Absolute	Absolute	Absolute	Absolute
Ubuntu 14.04	Absolute	Absolute	Absolute	Absolute
OpenSuse 11.1	Absolute	Absolute	Absolute	Absolute
OpenSuse 12.1	Relative	Relative	Relative	Relative
Windows 2008	Absolute	Absolute	Absolute	Absolute
Windows server 2012	Absolute	Absolute	Absolute	Absolute

7.6 Power and Fan

7.6.1 Server Power Control

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

On the WEB GUI, go to the **Power and Fan** → **Server Power Control** to configure the power button control options and power restore settings.

Virtual Power Button:

Server Power Control

Virtual Power Button | Power Restore Setting

Server Power Control

Current Power Status ● ON

Control Options

- Power On
- Force Power Off
- Power Cycle
- Hard Reset
- Soft Shutdown

Power Restore Setting:

Server Power Control

Virtual Power Button | Power Restore Setting

Power Policy

Current Power Status ● ON

Power Policy Options

- Always Power On
- Always Power Off
- Restore Last Power State

7.6.2 Fan Speed Control

BMC supports the Manual Fan Control / Auto Fan Control function, and the fan module speed is controlled by the thermal algorithm.

On the WEB GUI, go to the **Power and Fan** → **Fan Speed Control** to show the fan status. The **Auto Fan Control** is the default setting. If the user switches to **Manual Fan Control**, you need to setup the fan speed: Low (20%), Medium (50%), High (75%) or Full (100%).

Fan Speed Control

Manual Fan Control Auto Fan Control

No.	Present	Status	Current speed(rpm)	Duty Ratio(%)	Speed control
FAN_0_Front	✔	✔	3750	21	<input type="button" value="Low(20%)"/> <input type="button" value="Medium(50%)"/> <input type="button" value="High(75%)"/> <input type="button" value="Full(100%)"/>
FAN_0_Rear	✔	✔	3450	21	<input type="button" value="Low(20%)"/> <input type="button" value="Medium(50%)"/> <input type="button" value="High(75%)"/> <input type="button" value="Full(100%)"/>
FAN_1_Front	✔	✔	4200	21	<input type="button" value="Low(20%)"/> <input type="button" value="Medium(50%)"/> <input type="button" value="High(75%)"/> <input type="button" value="Full(100%)"/>
FAN_1_Rear	✔	✔	3600	21	<input type="button" value="Low(20%)"/> <input type="button" value="Medium(50%)"/> <input type="button" value="High(75%)"/> <input type="button" value="Full(100%)"/>

Note:
✔ Normal ✘ Critical ● N/A

MCU or CPLD will monitor the BMC fan control tasks by receiving a BMC watchdog signal. If MCU or CPLD cannot receive the watchdog signal in 4 minutes, all fans will set to full speed automatically to avoid the system overheating.

7.7 BMC Settings

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

- Maximum bandwidth: Dedicated NIC – 1000M, Shared NIC – 100M.
- BMC network interface compatibly supports IPV4 and IPV6, supports DHCP or IP address setting by manual.
- MAC address is stored in the EEPROM.
- Support VLAN.
- By default, IPMI LAN channels are assigned as below:

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

- BMC network interface supports enable/disable, enabled by default.

7.7.1 BMC Network Management

1. Network

On the WEB GUI, go to the **BMC Settings** → **BMC Network** → **Network** to configure the LAN interface settings, IPv4 configuration and IPv6 configuration.

BMC Network Management

Network | DNS | Network Link

LAN Interface: eth0

LAN Settings: Enable

MAC address: B4:05:5D:34:30:0D

IPv4 Configuration

IPv4 Setting: Enable

Obtain an IP address automatically: Enable DHCP

IPv4 Address: 100.2.76.110

Subnet Mask: 255.255.255.0

Default gateway: 100.2.76.1

IPv6 Configuration

IPv6 Setting: Enable

Obtain an IP address automatically: Enable DHCP

IPv6 Address: ::

Subnet prefix length: 0

VLAN Configuration

VLAN Setting: Enable

Save Reset

2. DNS

On the WEB GUI, go to the **BMC Settings** → **BMC Network** → **DNS** to configure the host, domain name and DNS.

BMC Network Management

Network **DNS** Network Link

DNS Enable

DNS Enable DNS Enable

Host Configuration

Host Settings

Host Name

Domain Configuration

Domain Settings

Network Interface

Domain Name Server Configuration

Domain Name Server Settings

DNS Server Interface

IP Priority IPv4 IPv6

3. Network Link

On the WEB GUI, go to the **BMC Settings** → **BMC Network** → **Network Link** to configure the network connection for the available networks.

BMC Network Management

Network DNS **Network Link**

LAN Interfaces

Auto Negotiation Enable

Link Speed

Duplex Mode

7.7.2 Service Settings

BMC supports the network connection manager library to configure the networking services in run-time system. User can enable/disable the WEB, KVM, CD-MEDIA, FD-MEDIA, HD-MEDIA, SSH services and configure the communication port, session timeout value of the service and the maximum number of allowed sessions for the services.

On the WEB GUI, go to the **BMC Settings** → **Services** to display the protocols and ports information.

■ Services

#	Service Name	Current State	Interfaces	Nonsecure Port	Secure Port	Timeout(s)	Maximum Sessions	Active Sessions
1	web	Active	eth0	80	443	1800	20	1
2	kvm	Active	eth0	7578	7582	1800	4	0
3	cd-media	Inactive	eth0	5120	5124	N/A	4	0
4	fd-media	Inactive	eth0	5122	5126	N/A	4	0
5	hd-media	Inactive	eth0	5123	5127	N/A	4	0
6	ssh	Inactive	N/A	N/A	22	600	N/A	0

NOTE: Http/Https (WEB) Timeout: if there is no web request in Timeout, web session will be deleted, and new web request will not respond. If the web page has no auto update, it will be logged out when you switch pages or refresh the page after timeout.

The fixed protocols cannot be configured, as shown below.

Service	Usage	State	Port	TCP/UDP
smux	SNMP Multiplexer	Enable	199	TCP
srvloc	Sever location	Enable	427	TCP, UDP
DHCP V6 Client	DHCP V6 Client	Enable	546	UDP
Websockify	KVM on HTML5	Enable	9666	TCP
Websockify	Virtual Media on HTML5	Enable	9999	TCP

7.7.3 NTP Settings

The real-time is defined as the number of seconds that have elapsed since 00:00:00 1970/01/01 and the time can be referenced as timestamp for other BMC application. By interface such as WEB UI, users are able to get current system date and time information, or configure date and time, or synchronize date and time through NTP.

Mode	State	UTC Timezone	NTP Server 1	NTP Server 2	NTP Server 3
Manual	Disable	N/A	N/A	N/A	N/A
NTP	Enable	GMT+/-0	pool.ntp.org	time.nist.gov	time.nist.gov

BIOS will synchronize time to BMC at the beginning of BIOS POST and synchronize time with ME after BMC running. If NTP is enabled and NTP servers are accessible, BMC will synchronize time with NTP servers per hour.

On the WEB GUI, go to the **BMC Settings** → **NTP Settings** to display and set the current BMC time and NTP settings.

■ NTP Settings

NTP Settings	
Date:	5 Month 21 Day 2020 Year
Time:	09 55 34 hh:mm:ss
UTC TimeZone:	(GMT+08:00)Beijing,Chongqir
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

7.7.4 SMTP Settings

On the WEB GUI, go to the **BMC Settings** → **SMPT Settings** to configure the SMTP settings.

■ SMTP Settings

LAN Channel	eth0
Sender Email	
Primary SMTP Server	
SMTP Support	<input checked="" type="checkbox"/> Enable
SMTP Server Names	
SMTP Server IP Address	
Port	25
SMTP Server Authentication	<input type="checkbox"/>
Username	
Password	
Secondary SMTP Server	
SMTP Support	<input type="checkbox"/> Enable
SMTP Server Names	
SMTP Server IP Address	
Port	25
SMTP Server Authentication	<input type="checkbox"/>
Username	
Password	

Save Reset

7.7.5 Alert Management

BMC supports the SNMP Trap configuration. User can open trap receiver and set trap destination IP in BMC Web GUI. When BMC detects an event, BMC will send the event to the trap receiver.

- BMC supports SNMP v1, v2, v3 traps (Default Trap v1).
- A Modular Information Block (MIB) file associated with the traps should be provided with the BMC firmware to help SNMP Trap receiver to interpret the trap.

Step 1

On the WEB GUI, go to the **BMC Settings** → **Alert Settings** to setup the SNMP Trap protocol.

[Alert Settings](#)

SNMP Trap Configure	
Trap Version	v1
Event Severity	All
Community	
Username	
Engine ID(Hex)	
Authentication and password	NONE
Privacy and password	NONE
System Name	
System ID	
Host Location	
Contact	
Host OS	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Step 2

Select the sensor type or sensor name to setup the event filter.

Event Filter	
Sensor Type	All Sensors
Sensor Name	All Sensors
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

Step 3

Setup the alert type and destination.

If SNMP is selected, the destination IP address should be set as well. If Email is selected, the LAN Channel should be set to dedicated or shared network, then set the destination to a user configured email.

Alert Policy Configure					
No.	Enable	LAN Channel	Alert Type	Destination	Action
1	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Test"/>
2	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Test"/>
3	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Test"/>

7.7.6 Access Control

On the WEB GUI, go to the **BMC Settings** → **Access Control** to manage the entries for the IP address range and MAC address that run or block access to the BMC. User can add new entries or delete existing entries.

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.

Access Control	
Add Accept Entry	IP: <input type="text"/> To <input type="text"/> MAC: <input type="text"/> Rule: <input type="text" value="Allow"/> Enable Timeout: <input type="checkbox"/> Start Date: <input type="text"/> Stop Date: <input type="text"/>
<input type="button" value="ADD"/>	
Current Accept Entry List	

7.7.7 BIOS Boot Options

BMC supports the BIOS boot options.

On the WEB GUI, go to the **BMC Settings** → **BIOS Boot Options** to modify the boot options.

BIOS Boot Options

BIOS Boot Options	
Timeliness	<input checked="" type="radio"/> Apply to next boot only <input type="radio"/> Apply to be persistent for all future boots
Boot Options	<input checked="" type="radio"/> No override <input type="radio"/> Force PXE <input type="radio"/> Force boot from default Hard-drive <input type="radio"/> Force boot from default CD/DVD <input type="radio"/> Force boot into BIOS Setup
<input type="button" value="Perform Action"/>	

7.8 Logs

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

7.8.1 System Event Log

BMC provides the system event log function, to record the IPMI sensors based on the event history. System event log outputs the following items and user can get the sensor event information by WEB or IPMI CMD.

- Support up to 3639 items.
- Support linear mode. When SEL is full, new log will be discarded.
- Support cycle mode, default mode. When SEL is full, oldest log will be discarded.
- When SEL is almost full (75%), then almost full log will be recorded in SEL.
- When SEL is full in linear mode, Full log will be recorded in SEL.
- When SEL is clear, Clear log will be recorded in SEL.
- Support exporting SEL by WEB or IPMI CMD.
- Support informing event to remote client by SNMP Trap, Email Alert, Syslog.

On the WEB GUI, go to the **Logs** → **System Event Log** to display all sensors. User can configure the event types, sensor types, event severity, and event occurrence time period parameters to filter system event logs. At the same time, the system provides the user with a time zone configuration option for the logs. System event log can be displayed in the desired time zone according to the time zone selected by users.

System Event Log

All Events filter by All Sensors filter by Severity: All Events filter by

BMC Timezone Client Timezone UTC Offset :(GMT)

Event ID /	Time Stamp /	Severity /	Sensor Name	Sensor Type	Description
93	02/28/2020 02:14:58	i	OS_Boot	OS Boot	Boot Completed - Boot Device Not Specified - Asserted
92	02/28/2020 02:14:13	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
91	02/28/2020 02:14:12	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
90	02/28/2020 02:14:11	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
89	02/28/2020 02:14:10	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
88	02/28/2020 02:14:09	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
87	02/28/2020 02:14:08	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
86	02/28/2020 02:14:07	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
85	02/28/2020 02:14:06	i	SYS_FW_Progress	BIOS POST Progress	Progress-PCI resource configuration. - Asserted
84	02/28/2020 02:13:35	i	SYS_Restart	System Boot / Restart Initiated	Initiated By Hard Reset - Asserted

Export Log Clear Log

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

The specific configuration parameters of the system event log are shown in the following table:

Parameter	Description
Filter	Select event types, sensors, severity, and start and end dates for a filtered search. Action: You can use the filter options (event types, sensor types, sensor names, event severity levels, and time) to view specific events logged in the device.
BMC timezone	Use this option to display event log entries based on the corresponding BMC timezone.
Client timezone	Use this option to display event log entries based on the client timezone (the user's time zone).
UTC offset	Display the current UTC offset based on the event time stamp.
Export logs	Export event logs locally.
Delete logs	Delete all existing sensor logs.

7.8.2 BMC System Audit Log

BMC provides the BMC system audit log function.

- All Web setting operating actions will be recorded.
- Web/SSH login and logout will be recorded.
- Audit log supported size is 50K, if more than 50K, log will be cleared.
- Support exporting log by Web.

On the WEB GUI, go to the **Logs** → **BMC System Audit Log** → **BMC Audit Log** to display the BMC audit log. User can filter the audit logs by choosing the start and end time, and click the "**Export Log**" button and "**Clear Log**" button to perform log exporting and deleting.

BMC System Audit Log

BMC Audit Log | BMC System Logs

filter by [] - [] filter UTC Offset(GMT+08:00) Event entries: 44

Event ID	Time Stamp	HostName	Description
44	02/28/2020 08:36:49	localhost	From IP:100.3.2.1 User:admin HTTPS Login Success
43	02/28/2020 08:36:43	localhost	From IP:100.3.2.1 User:admin HTTPS Logout Success
42	02/28/2020 07:35:25	localhost	From IP: 100.3.2.1 User: admin Operation: Preparing Flash Area for BIOS Update(Preserve Configuration: No) Success
41	02/28/2020 07:34:02	localhost	From IP: 100.3.2.1 User: admin Operation: Preparing Flash Area for BIOS Update(Preserve Configuration: No) Success
40	02/28/2020 07:30:27	localhost	From IP: 100.3.2.1 User: admin Operation: Preparing Flash Area for BIOS Update(Preserve Configuration: No) Success
39	02/28/2020 07:07:19	localhost	From IP:100.3.2.1 User:admin HTTPS Login Success
38	02/28/2020 07:03:35	localhost	From IP:100.3.7.205 User:admin HTTPS Logout Success
37	02/28/2020 07:03:14	localhost	From IP:100.3.7.205 User:admin HTTPS Login Success
36	02/21/2020 07:44:56	localhost	From IP:100.2.48.209 User:admin HTTPS Logout Success
35	02/21/2020 07:30:56	localhost	From IP:100.2.48.209 User:admin HTTPS Logout Success
34	02/21/2020 07:12:50	localhost	From IP:100.2.48.209 User:admin HTTPS Login Success
33	02/21/2020 07:00:49	localhost	From IP:100.2.48.209 User:admin HTTPS Login Success
32	02/21/2020 05:07:03	localhost	From IP:100.3.2.1 User:admin HTTPS Logout Success
31	02/21/2020 03:28:55	localhost	From IP:100.3.2.1 User:admin HTTPS Login Success
30	02/21/2020 03:25:53	localhost	From IP:100.3.2.1 User:admin HTTPS Logout Success
29	02/21/2020 03:03:05	localhost	From IP:100.3.2.1 User:admin HTTPS Login Success
28	02/21/2020 02:56:25	localhost	From IP:100.3.7.52 User:admin HTTPS Login Success

Export Log Clear Log

On the WEB GUI, go to the **Logs** → **BMC System Audit Log** → **BMC System Log** to display the BMC system log. User can filter the audit logs by choosing the types (alarm, criticality, fault, notification, warning, debug, emergency, and information), start time and end time, and click the "**Export Log**" button and "**Clear Log**" button to perform log exporting and deleting.

The screenshot shows the BMC System Log interface. At the top, there are tabs for 'BMC Audit Log' and 'BMC System Logs'. Below the tabs, there is a search bar with 'Alert' selected, a 'filter by' section with two empty input fields and a 'filter' button, and a 'UTC Offset(GMT+08:00)' label. The main area contains a table with the following data:

Event ID	Time Stamp	HostName	Description
12	02/28/2020 06:58:33	localhost	kernel: Copyright (c) 2009-2015 American Megatrends Inc.
11	02/28/2020 06:58:33	localhost	kernel: Helper Module Driver Version 1.2
10	02/28/2020 06:55:48	localhost	kernel: Copyright (c) 2009-2015 American Megatrends Inc.
9	02/28/2020 06:55:48	localhost	kernel: Helper Module Driver Version 1.2
8	02/21/2020 02:53:20	localhost	kernel: Copyright (c) 2009-2015 American Megatrends Inc.
7	02/21/2020 02:53:20	localhost	kernel: Helper Module Driver Version 1.2
6	02/21/2020 02:51:10	localhost	kernel: Copyright (c) 2009-2015 American Megatrends Inc.
5	02/21/2020 02:51:10	localhost	kernel: Helper Module Driver Version 1.2
4	02/21/2020 02:35:40	localhost	kernel: Copyright (c) 2009-2015 American Megatrends Inc.
3	02/21/2020 02:35:40	localhost	kernel: Helper Module Driver Version 1.2

At the bottom right of the table area, there are two buttons: 'Export Log' and 'Clear Log'.

7.8.3 Event Log Setting

On the WEB GUI, go to the **Logs** → **Event Log Setting** to display system event log information and configuration.

■ Event Log Setting

The screenshot shows the 'Event Log Setting' configuration page. It has a title 'Event Log Setting' and two main sections:

- Current Event Log Policy:** Linear Policy
- System Event Log Policy Options:**
 - Linear Policy
 - Circular Policy

At the bottom right, there are two buttons: 'Save' and 'Reset'.

7.8.4 System Audit Log Settings

On the WEB GUI, go to the **Logs** → **System and Audit Log Settings** to configure SEL log system records.

When **Remote Log** is enabled, the Server Address (IPv4 address or FQDN) and Server Port (the default setting is 514) needs to be configured. Local files are stored in BMC DDR.

System and Audit Log Settings

System and Audit Log Settings	
System Log	<input checked="" type="checkbox"/> Enable
Log Type	<input checked="" type="radio"/> Local Log <input type="radio"/> Remote Log
File Size (in bytes)	50000
Rotate Count	0
Server Address	
Server Port	0
Audit Log	<input checked="" type="checkbox"/> Enable

Save Reset

7.8.5 One-key Collection Log

BMC supports the one-key log collection.

On the WEB GUI, go to the **Logs** → **One-Key Collect Log**. Click on the **One-Key Collect Log** button to collect logs, it takes about 4-5 minutes.

One-Key Collect Log

One-Key Collect Log(it will spend about 4-5 minutes,please be patiently.)

One-Key Collect Log Export Log

After the logs are collected, click on the **Export Log** button to export the logs, including the black box logs, alarm logs, audit logs, debug logs, etc.

alert.log	228 bytes	Text	11:03
audit.log	274 bytes	Text	11:03
bios_setup.conf	82.3 kB	Text	11:03
crit.log	1.2 kB	Text	11:03
debug.log	1.3 kB	Text	11:03
dhcp6c.conf	348 bytes	Text	11:03
dns.conf	541 bytes	Program	11:03
epromdata.log	32.8 kB	Text	11:03
emerg.log	0 bytes	Text	11:03
err.log	1.3 kB	Text	11:03
FRU.bin	255 bytes	Binary	11:03
interfaces	352 bytes	Text	11:03
IPMI.conf	3.1 kB	Text	11:03
lighttpd.conf	4.4 kB	Text	11:03
SDR.dat	4.0 kB	Binary	11:03
SEL.dat	92 bytes	Program	11:03
snmpcfg.conf	68 bytes	Text	11:03
syslog.conf	624 bytes	Text	11:03
sysmonitor.log	41.8 kB	Text	11:03
warning.log	5.7 kB	Text	11:03

7.8.6 System Serial Log

See [7.15 SOL and System Serial Log Recording](#) for more information.

7.9 Fault Diagnosis

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

7.9.1 BMC Self-inspection Result

On the WEB GUI, go to the **Fault Diagnosis** → **BMC Self-inspection Result** to displays the BMC self-inspection codes.

BMC Self-inspection Result

BMC Self-inspection Result	
Current Self-inspection Result	55 00

The following table shows the BMC self-inspection code.

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

7.9.2 BMC Recovery

Users can reset BMC through WEB or IPMI CMD in case of an abnormal situation occurs.

On the WEB GUI, go to the **Fault Diagnosis** → **BMC Recovery** to reset BMC or KVM.

To reset BMC, select the **BMC Warm Reset** (it uses WEB or IPMI CMD “ipmitool mc reset” to reset BMC). To reset KVM, select the **KVM Service Restart** (KVM server will be reset).

BMC Recovery

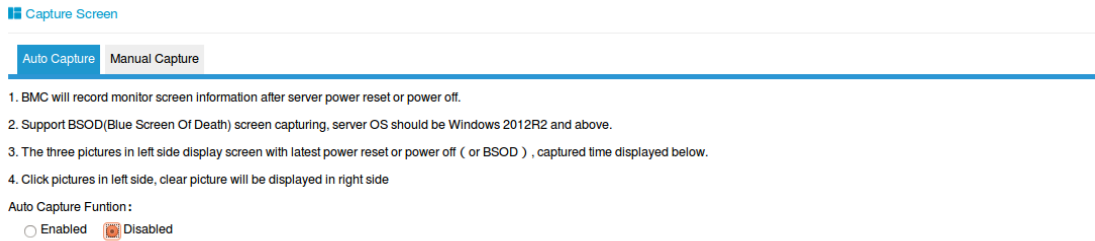
BMC Recovery	
BMC Recovery Options	<input checked="" type="radio"/> BMC Warm Reset <input type="radio"/> KVM Service Restart

Perform Action

7.9.3 Screen Capture

BMC will record the screen when a server restarts or is shut down, and supports BSOD (Blue Screen of Death) screen capturing, server OS should be Windows 2012R2 and above.

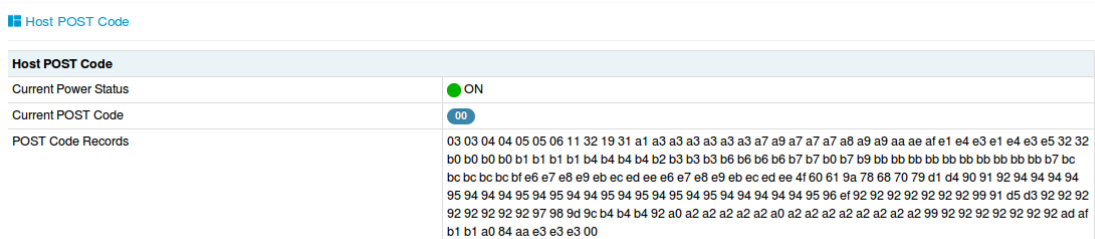
On the WEB GUI, go to the **Fault Diagnosis** → **Capture Screen** to to enable/disable the auto capture function.



7.9.4 HOST POST Code

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

On the WEB GUI, go to the **Fault Diagnosis** → **HOST POST Code** to display the host post codes.



7.9.5 BMC Watchdog for System

Software watchdog can be used for a number of system timeout functions by system management or by BIOS. For example, the common BIOS restarts the system after a timeout to avoid bringing the whole system to a standstill. If software watchdog is triggered, the following actions are available:

- System reset
- System power off
- System power cycle
- BMC will record SEL, when BMC watchdog works.

7.10 Administration


7.10.1 User Management

BMC supports IPMI, WEB, SSH, and SNMP users.

- BMC supports unified user management mechanism to manage IPMI, WEB and SSH users. Users created by IPMI or WEB will have IPMI, WEB as well as SSH user privileges, and can access Smash-Lit CLI via SSH.
- Sysadmin is used for access BMC diagnose serial consoles, and **cannot** access IPMI, WEB or SSH by LAN.
- SNMP users are used for SNMP Get/Set.

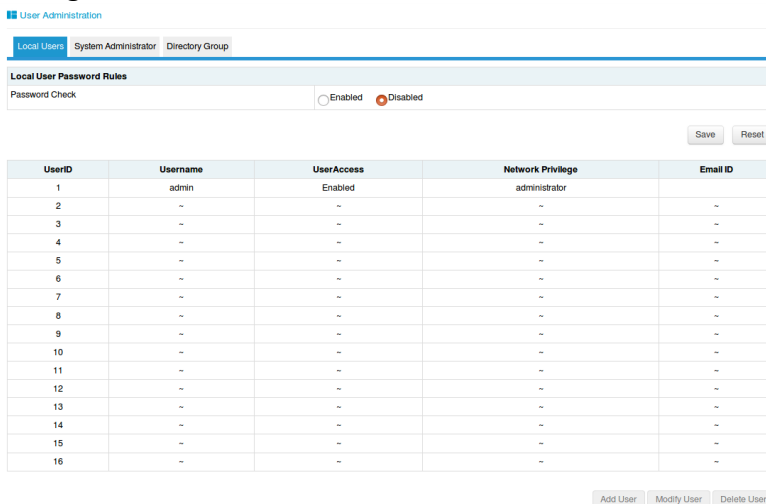
For Local Users (IPMI/WEB/SSH Unified Users):

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

 **NOTE:** For security reasons, please change the default password after first login, and update the password periodically.

User ID	User Name	Password	Status	Default privilege	Feature
1	admin	admin	Enabled	Administrator	User Name/Password can be changed
2- 16	undefined	undefined	Disabled	Administrator	User Name/Password can be changed

On the WEB GUI, go to the **Administration** → **User Administration** → **Local Users** to manage the user accounts



The screenshot shows the 'User Administration' page with a breadcrumb trail: Local Users > System Administrator > Directory Group. Under 'Local User Password Rules', there is a 'Password Check' section with radio buttons for 'Enabled' and 'Disabled' (selected). Below this is a table of users:

UserID	Username	UserAccess	Network Privilege	Email ID
1	admin	Enabled	administrator	
2	~	~	~	~
3	~	~	~	~
4	~	~	~	~
5	~	~	~	~
6	~	~	~	~
7	~	~	~	~
8	~	~	~	~
9	~	~	~	~
10	~	~	~	~
11	~	~	~	~
12	~	~	~	~
13	~	~	~	~
14	~	~	~	~
15	~	~	~	~
16	~	~	~	~

Buttons for 'Save' and 'Reset' are located above the table. At the bottom of the interface, there are buttons for 'Add User', 'Modify User', and 'Delete User'.

For BMC System Administrator:

On the WEB GUI, go to the **Administration** → **User Administration** → **System Administrator** to manage the system administrator account.

■ User Administration

Local Users **System Administrator** Directory Group

System Administrator

Username	sysadmin
User Access	<input checked="" type="checkbox"/> Enable
Change Password	<input type="checkbox"/> Enable
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Save Reset

The system administrator can access BMC diagnose serial consoles, users can change passwords by IPMI CMD or WEB GUI.

User name: **sysadmin** (Fixed, cannot be changed)

Default password: **superuser**

NOTE:

- For security reasons, please change the default password after first login, and update the password periodically.
- The username cannot be changed.
- A password must contain at least 8 characters, and must contain special characters, uppercase/lowercase letters and numbers.
- No blanks are allowed
- No more than 64 characters

For Directory Groups:

On the WEB GUI, go to the **Administration** → **User Administration** → **Directory Group**, and then click on the **Advanced Settings** button to enable and configure Active Directory or LDAP/E-Directory. For the detailed information, see [7.10.2 Security](#).

■ User Administration

Local Users System Administrator **Directory Group**

To enable Active Directory or LDAP/E-Directory, and configure its settings. Click on 'Advanced Settings' button. Advanced Settings

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name in the list and press Delete Role Group or Modify Role Group.

LDAP/E-Directory Settings			
Role Group ID	Group Name	Group Search Base	Group Privilege
Modify Role Group Delete Role Group			

Active Directory Settings			
Role Group ID	Group Name	Group Domain	Group Privilege
Modify Role Group Delete Role Group			

7.10.1.1 User Privileges

User privileges includes 3 types: IMPI user privilege, WEB GUI user privilege, and Smash-Lite CLI user privilege.

IPMI User Privileges

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

- **Out-band** mode means sending IPMI CMD to BMC by LAN, BMC will authenticate the username and password.
- **In-band** mode means sending IPMI CMD in HOST OS. In this mode, IPMI CMD does not need to authenticate the username and password, because users will get the highest privilege when accessing the HOST OS. So if users forgets their passwords or passwords expire, they can send IPMI CMD under HOST OS to disable the password security rule.

Please refer to IPMI 2.0 Spec, Appendix G - CMD assignments. Common privileges are as shown below:

User privilege	Supported operation
Administrator	Read/Write
Operator	Read Only
User	Read Only
No Access	Non

WEB GUI user privileges

Only IPMI/WEB/SSH unified users support the WEB GUI.

Menu	Subdirectory	User	Operator	Administrator
Information	System Information	Read Only	Read Only	Read/Write
	BIOS Setup Options	Read Only	Read Only	Read/Write
	FRU Information	Read Only	Read Only	Read/Write
	History Records	Read Only	Read Only	Read/Write
Remote Control	Console Redirection	NA	NA	Read/Write
	Locate Server	NA	NA	Read/Write
	Remote Session	Read Only	Read Only	Read/Write
	Virtual Media	Read Only	Read Only	Read/Write
	Mouse Mode	Read Only	Read Only	Read/Write
Power and Fan	Server Power Control	Read Only	Read Only	Read/Write
	Fan Speed Control	Read Only	Read Only	Read/Write
BMC Settings	BMC Network	NA	Read Only	Read/Write
	Service	Read Only	Read Only	Read/Write
	NTP	Read Only	Read Only	Read/Write
	SMTP	NA	NA	Read/Write
	Alerts	NA	Read Only	Read/Write

Menu	Subdirectory	User	Operator	Administrator
	Access Control	Read Only	Read Only	Read/Write
	BIOS Boot Options	Read Only	Read Only	Read/Write
Logs	System Event Log	Read Only	Read Only	Read/Write
	BMC System Audit Log	Read Only	Read Only	Read/Write
	Event Log Setting	Read Only	Read Only	Read/Write
	BMC System Audit Log Setting	Read Only	Read Only	Read/Write
	One-key collection Log	Read Only	Read Only	Read/Write
Fault Diagnosis	BMC Self-Inspection Result	Read Only	Read Only	Read/Write
	BMC Recovery	Read Only	Read Only	Read/Write
	Capture Screen	NA	NA	Read/Write
	Host POST Code	Read Only	Read Only	Read/Write
Administration	User Administration	NA	Read Only	Read/Write
	Security	Read Only	Read Only	Read/Write
	Dual Image Configuration	NA	NA	Read/Write
	Dual Firmware Update	NA	NA	Read/Write
	BIOS Firmware Update	NA	NA	Read/Write
	Restore Factory Defaults	NA	NA	Read/Write

For “Operator” and “User” privileges, if with Read Only attribute, the settings are visible, but the input fields and buttons are disabled, so users cannot modify the settings; if with NA attribute, the settings are invisible and no operation can be taken. Users with a “No Access” privilege cannot login WEB GUI.

Smash-Lite CLI user privileges (access via SSH)

CMD	Sub CMD	User	Operator	Administrator
ipconfig	get	YES	YES	YES
	set	NO	NO	YES
sensor	get	YES	YES	YES
fru	get	YES	YES	YES
	set	NO	NO	YES
chassis	get	YES	YES	YES
	set	NO	NO	YES
user	get	YES	YES	YES
	set	NO	NO	YES
mc	get	YES	YES	YES
	set	NO	NO	YES
fan	get	YES	YES	YES

	set	NO	NO	YES
id	set	YES	YES	YES
diagnose	get	NO	NO	YES

7.10.2 Security

LDAP Settings

On the WEB GUI, go to the **Administration** → **Security** → **LDAP Settings** to enable and configure LDAP/E-Directory.

■ Security

LDAP Settings | AD Settings

LDAP/E-Directory Authentication	<input type="checkbox"/> Enable
Encryption Type	<input checked="" type="radio"/> No Encryption <input type="radio"/> SSL <input type="radio"/> StartTLS
Common Name Type	<input checked="" type="radio"/> IP Address
Server Address	<input type="text"/>
Port	<input type="text" value="389"/>
Bind DN	<input type="text"/>
Password	<input type="password"/>
Search Base	<input type="text"/>
Attribute of User Login	<input type="text" value="cn"/>

AD Settings

On the WEB GUI, go to the **Administration** → **Security** → **AD Settings** to enable and configure Active Directory.

■ Security

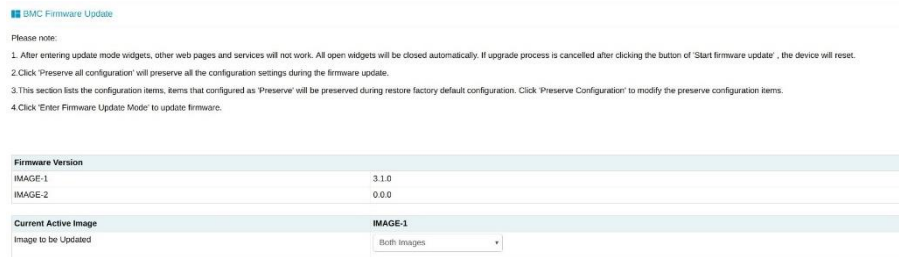
LDAP Settings | AD Settings

Active Directory Authentication	<input type="checkbox"/> Enable
Encryption Type	<input type="checkbox"/> SSL Enable
Secret Username	<input type="password"/>
Secret Password	<input type="password"/>
Time Out	<input type="text"/>
User Domain Name	<input type="text"/>
Domain Controller Server Address1	<input type="text"/>
Domain Controller Server Address2	<input type="text"/>
Domain Controller Server Address3	<input type="text"/>

7.10.3 BMC Dual Image Configuration

Dual image means that BMC supports dual image in flash memory. When the main image fails to start, BMC will try to boot with another image.

On the WEB GUI, go to the **Administration** → **Dual Image configuration** to display or modify the dual-image configuration.



7.10.4 BMC Dual Firmware Update

BMC supports dual BMC firmware update. The BMC flash contains two images: BMC flash image (size: 64M) and BMC firmware image (size: 32M).

On the WEB GUI, go to the **Administration** → **BMC Firmware Update** to update the firmware. This is a sideband mode, supporting firmware integrity checks and preserving configuration.

Firmware Integrity Checks

Before updating the firmware, MD5 tool must be used to check the image integrity to ensure that the firmware image file is correct.

WEB Update

User can update the BMC firmware via WEB GUI. It supports the hardware watchdog. For more information on watchdog, refer to [7.13.1 Hardware Watchdog](#).

When updating the BMC firmware, user can specify which image to update: Image-1, Image-2 or Both images (Default). Configuration can be preserved separately. Please refer to the [7.10.6 Restore Factory Defaults](#).

NOTE: The firmware upgrade process is a crucial operation. Make sure that the power or connectivity loss are minimal when performing this operation.

Once you enter into the update mode and choose to cancel the firmware flash operation, BMC must be reset. This means that you must close the Internet browser and log back onto the BMC before performing any operations.

After rebooting, BMC will boot to the higher version of the two images. You can change the value from WEB GUI.

Step 1

On the WEB GUI, go to the **Administration** → **BMC Firmware Update** to change the image to be updated. The default setting is **Both Images**, meaning both images will be updated.

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 Mode" to update firmware.

Firmware Version	
IMAGE-1	3.0.0
IMAGE-2	0.0.0

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

Check the **Preserve all configuration** box to preserve the configuration, click on the **Enter Preserve Configuration** button to select items needed to be preserved, and click on the **Enter Firmware Update Mode** button to start the update process.

Firmware Version	
IMAGE-1	3.1.0
IMAGE-2	0.0.0

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

Preserve all configuration

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

Step 2

Click on the **Browse** button to select an image file, and then click on the **Start firmware update** button to upload the file. BMC will enter into the flash mode, IPMI service will stop, and then BMC will verify the image (verify size should be 32M). Verify the image integrity to ensure that this is a BMC image. If the verification fails, BMC will stop the flash process and restart.

BMC Firmware Update

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

Abort Firmware Update

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

Enter Firmware Update Mode

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

Choose File ONS263M5_..._20200706

Start firmware update

Step 3

Check the image uploaded version and current version, then click on the **Proceed to update** button to start the update process. Wait for about 15 minutes (both images), then the BMC flash is complete.

BMC Firmware Update

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

Abort Firmware Update

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

Enter Firmware Update Mode

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

Choose File ONS263M5_..._20200706

The file has been uploaded and is being verified, please be patient


Name	Existing version	Uploaded version
IMAGE-1	3.1.0	3.1.0
IMAGE-2	0.0.0	3.1.0

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

Proceed to update

7.10.5 BIOS FW Update

BMC supports BIOS firmware update via WEB GUI. Intel ME firmware is packaged with BIOS firmware as a single firmware image.

 **NOTE:** Power off the system before updating the BIOS firmware.

After BIOS firmware update is finished, BIOS NVRAM will be cleared, all BIOS configuration will be reset to defaults. If BIOS and ME images are updated simultaneously, it is recommended that to power off the server completely.

Step 1

On the WEB GUI, go to the **Administration** → **BIOS Firmware Update**, and then click **Enter Firmware Update Mode** to enter the update mode.

BIOS Bin file Type has two selections: **BIOS+ME** or **BIOS Only**. Check the **BIOS Setup Options** checkbox if you want to preserve BIOS setup options.

BIOS Firmware Update

Please note:

- (1) You'd better **Power Off** the system if you want to do BIOS Update.
- (2) BIOS NVRAM will be cleared and BIOS will become default after BIOS flashed, when updating BIOS without preserve configuration.
- (3) After BIOS+ME flashed, we recommend to **AC Power Off and On** to enable NEW ME.
- (4) After BIOS or BIOS+ME flashed, we recommend to **AC Power Off and On**. Or the condition may occur that PHY NIC may be not detected. Once the condition occurs, system global reset is needed, you need to force power off the server when server is power on.

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

BIOS Bin File Type:

Options to be preserved: BIOS Setup Options

Step 2

Click **Browse** to select an image file, and then click **Upload** to upload and verify the file. ME will enter the recovery mode, and then BMC will verify the image (verify size should be 32M). Verify the image integrity to ensure that this is a BIOS image. If the verification fails, BMC will stop the flash process and force ME to enter to the normal mode. If the verification succeeds, click on the **Proceed to update** button to start the update. Wait for about 3 minutes, then the flash process is complete, and ME will enter the normal mode.

BIOS Firmware Update

Please note:

- (1) You'd better **Power Off** the system if you want to do BIOS Update.
- (2) BIOS NVRAM will be cleared and BIOS will become default after BIOS flashed, when updating BIOS without preserve configuration.
- (3) After BIOS+ME flashed, we recommend to **AC Power Off and On** to enable NEW ME.
- (4) After BIOS or BIOS+ME flashed, we recommend to **AC Power Off and On**. Or the condition may occur that PHY NIC may be not detected. Once the condition occurs, system global reset is needed, you need to force power off the server when server is power on.

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

BIOS Bin File Type:

Options to be preserved: BIOS Setup Options

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

Select Bin File: ONS263M5_B...00604.bin

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

7.10.6 Restore Factory Defaults

BMC supports the restore factory defaults via WEB GUI.

On the WEB GUI, go to the **Administration** → **Restore Factory Defaults** to restore to the factory defaults.

Restore Factory Defaults

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

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

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

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

NOTE: The Update Policy Overwrite means the selected items will be overwritten to the default settings after clicking on the **Restore Factory Defaults** button or after upgrading BMC; The Update Policy Preserve means the selected items will be restored clicking on the **Restore Factory Defaults** button or after upgrading BMC.

The following table shows the preserved configuration.

Item	Preserved configuration	Note
SDR	SDR	
SEL	SEL log	
IPMI	IPMI, including PEF data, SOL data, IPMI user information, SMTP, DCMI data, etc.	
PEF	PEF	Select IPMI option when this configuration is included.
SOL	SOL	Select IPMI option when this configuration is included.
SMTP	SMTP	Select IPMI option when this configuration is

Item	Preserved configuration	Note
		included.
User	IPMI user	Select IPMI option when this configuration is included.
DCMI	DCMI	Select IPMI option when this configuration is included.
Network	BMC network	
NTP	NTP	
SNMP	SNMP	
SSH	SSH	
KVM	KVM and Virtual Media Devices	
Authentication	Authentication, including LADP and superuser	
Syslog	Syslog	
Hostname	Hostname	

7.11 Device State Monitor and Diagnostic

7.11.1 Sensors

7.11.1.1 Physical Sensors

Physical sensors monitors the state change of main devices. The information gathered from the physical sensors is transmitted to IPMI sensors.

- Device state sensors: BMC monitors CPU/DIMM/PSU/HDD error state based on IPMI sensor type.
- Temperature: BMC monitors temperature of system components, including CPU, PCH, DIMM and HSBP, and Inlet/Outlet temperature.
- Voltage: System P12V, P5V, P3V3, PVNN, PVDDQ, PVCCIO, PVCCIN.
- Fan Speed: System fan.
- Power consumption: BMC monitors total power, CPU power, memory power, PSU input power. Fan Power and HDD Power are platform-specific.
- System main component health: BMC monitors system component's health, including CPU status, PCH status, MEM Hot, HDD status, ME FW status.
- Intrusion: Optional - An assertion event will be logged, when chassis cover is opened.

- Button: An assertion event will be logged, when power button or reset button is pressed.

7.11.1.2 Virtual Sensors

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

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

7.11.1.3 Event-Only sensors

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

7.11.1.4 Sensor attribute

- Sensor type: Please refer to *Sensor Type Codes* table in IPMI specification, version 2.0.
- Event type: Please refer to *Event/reading Type Code Ranges* table in IPMI specification, version 2.0.
- Event offset :
- If sensor event type is generic, please refer to *Generic Event/Reading Type Code* table in IPMI specification, version 2.0.
- If sensor event type is sensor-specific, please refer to *Sensor Type Code* tables in IPMI specification, version 2.0.
- Assertion/De-assertion: Assertion and de-assertion indicators reveal the type of events this sensor generates.

7.11.2 CPU

The following table shows the CPU health state.

State	Level	Related model
Present	Info	SDR/SEL
Thermal Trip	Critical	SDR/SEL
Processor Hot	Critical	SDR/SEL
Error0	Warning	Blackbox
Error1	Warning	Blackbox
Error2	Critical	Blackbox
CPU VR Hot	Critical	Blackbox
PCHThermal Trip	Critical	Blackbox

7.11.3 Memory

The following table shows the memory health state.

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

7.12 Event Alerts

BMC supports SNMP Trap and SMTP email alerts.

7.12.1 SMTP Email Alerts

When BMC detects an event , an SMTP (Simple Mail Transport Protocol, defined in RFC821) email alert will be sent to the specified mailbox.

Step 1

On the WEB GUI, go to the **BMC Settings** → **SMTP Settings** to configure SMTP settings. User should set a SMTP server for the LAN channels. If an event occurs, the sender will send an email to the specified mailbox.

SMTP Settings

LAN Channel: eth0

Sender Email: []

Primary SMTP Server

SMTP Support: Enable

SMTP Server Names: []

SMTP Server IP Address: []

Port: 25

SMTP Server Authentication:

Username: []

Password: []

Secondary SMTP Server

SMTP Support: Enable

SMTP Server Names: []

SMTP Server IP Address: []

Port: 25

SMTP Server Authentication:

Username: []

Password: []

Save Reset

Step 2

On the WEB GUI, go to the **Administration** → **User Administration** configure email address for the related users.

Modify User

Old Password: []

New Password: []

Confirm Password: []

User Access: Enable

Network Privilege: Administrator

Serial Privilege: Administrator

Email ID: example@test.com

Email Format: AMI-Format

Existing SSH Key: Not Available

New SSH Key: [] [open file](#)

Modify Cancel

Step 3

Setup the alert type and destination.

If SNMP is selected, the destination IP address should be set as well. If Email is selected, the LAN Channel should be set to dedicated or shared network, then set the destination to a user configured email.

Alert Policy Configure					Action		
No.	Enable	LAN Channel	Alert Type	Destination	Save	Reset	Test
1	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	Save	Reset	Test
2	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	Save	Reset	Test
3	<input type="checkbox"/>	eth0	Snmp	0.0.0.0	Save	Reset	Test

7.12.2 Syslog

Syslog is used for sending the alarm events to remote sites.

7.13 BMC Self Recovery

BMC self recovery provides the ability of automatic repair operations if necessary.

7.13.1 Hardware Watchdog

Known fault scenarios:

- Kernel panic
- System resources exhausted or error, system can't create a new task, but the original task can continue to run.
- Hardware watchdog :
- Watchdog starts when uboot loads kernel, and the timeout is 5 minutes. If BMC boot timeout occurs, BMC will reset.
- After the BMC system starts, the main process resets the Watchdog every minute. If the timeout is more than 1 minute, BMC will reset.
- When entering the flash mode, set watchdog time to 20 mins, if timeout BMC will reset automatically. When flashing image starts, the watchdog will update to 20 mins, if timeout BMC will reset automatically.

7.13.2 Software Watchdog

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

- IPMI server
- KVM server
- Virtual media server

7.14 LED

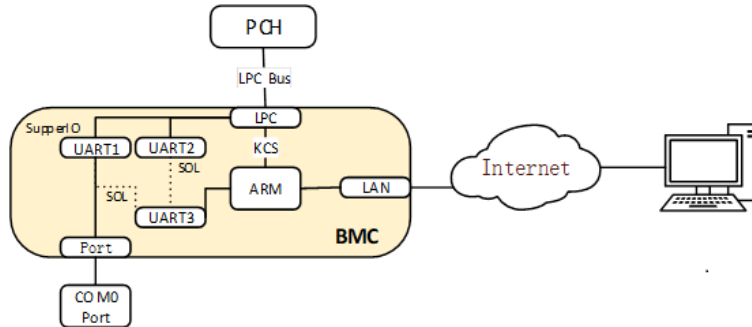
The system provides LEDs to indicate the health of the system

LED name	Color	Status	Description
UID Button LED	Blue	OFF	UID button is not pressed
		ON	UID button is pressed
BMC Fault LED	Red	OFF	BMC workable
		ON	BMC error
BMC Heatbeat LED	Green	OFF	BMC off
		ON	BMC active

7.15 SOL and System Serial Log

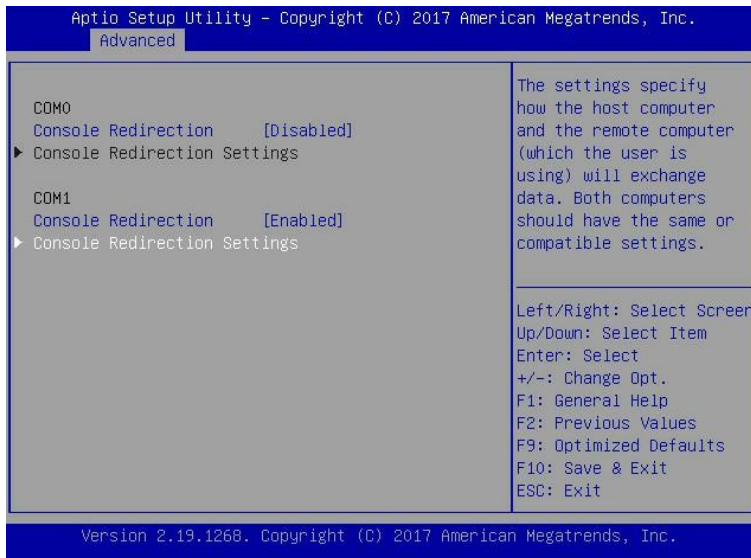
Serial Over LAN (SOL)

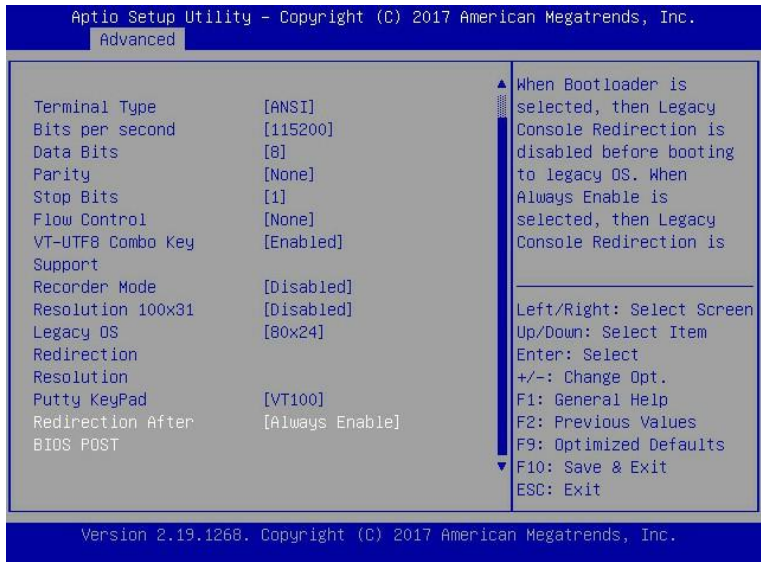
Serial Over LAN (SOL) redirects the system serial port to the remote network client. Users connect to the BMC on the local PC, open the serial port redirection function with the standard IPMI command (sol activate), view the system serial output, and enter the system serial port.



Both COM0 and COM1 support SOL. COM0 port has a connector on the motherboard. The COM1 port is dedicated for SOL function.

SOL is enabled on COM0 (in some projects on COM1) by default, users should configure SOL in BIOS setups (Serial port console redirection), if needed.





System Serial Log


BMC can record system serial information. The logs BIOS or OS sends to the serial port will be recorded to the BMC’s DDR, and keep up to 2M bytes of system serial logs. When more than 2M, log will loop to store, and the old log content will be deleted. When the system crashes or restarts, system serial log can be exported, and fault information can be used for fault diagnosis.

8. Troubleshooting

To access the troubleshooting resources, see the Inspur Information Library
<https://en.inspur.com/en/2494815/2498880/index.html> .

9. Battery Replacement


If the server does not show the date and time correctly, you may need to replace the battery that provides power to the real-time clock.

 **WARNING:** The server 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 recharge the battery.
 - DO NOT expose the battery to temperatures higher than 60°C (140°F).
 - DO NOT throw, immerse or dispose the battery into fire or water.
-

To replace the battery:

1. Remove the PCIe riser-card assembly (Refer to [PCIe Riser-Card Assembly Replacement](#)).
 2. Using fingers, gently push the battery away from the holder, and lift it out of the holder.
-

 **WARNING:** DO NOT push the battery using excessive force. Failing to remove the battery properly might damage the socket on the motherboard. Any damage to the socket might require replacing the entire base with the motherboard.

3. Put the battery into the holder, and gently press the battery outward to secure the battery into the holder
 4. Dispose of the battery as required by local ordinances or regulations
-

 **NOTE:** After replacing the battery, you must reconfigure the server and reset the system date and time.

10. Regulatory Information

10.1 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.

10.2 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.


10.2.1 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.

10.3 Battery Replacement Notice

-  **WARNING:** The equipment 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.



11. Electrostatic Discharge

11.1 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.

11.2 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.

12. Warranty

Inspur warrants that all Inspur-branded hardware products shall be free from material malfunctioning and material defects under conditions of normal use for a period of three (3) years from the Date of Invoice.

Service offerings may vary by geographic region. Please contact your Inspur representative to identify service levels and needs for your regions.

12.1 Warranty Service

i. Remote Technical Support

Inspur warranty service includes 24/7 remote technical support and 3 years parts replacement throughout the warranty period. Warranty Service are Advance Replacement Service in the first year and Standard Replacement Service in the second and third years.

Type	Duration
Remote Technical Support	3 years
RMA Services	3 years

The 24/7 remote technical support can through hotline, e-mail, and Service Portal*¹. Through hotline and e-mail support, Inspur engineers help customers diagnose the cause of malfunction and provide solution. Service Portal*¹ provides access to firmware, customized update files, and related manuals for Inspur products. Customer may also access the Service Portal*¹ to submit Return Material Authorization (RMA) for parts replacement or repair.

Information needed when requesting for support:

- Contact name, phone number, e-mail address
- System Serial Number, Part Number, Model and location (address) of the product needing service
- Detailed description of problem, logs (sel and blackbox, and any other related logs from OS), screenshot of issue, pictures of damaged/questions parts, etc.

Support Contact Information:

Type	Description	Support Window
Global Hotline	Global: 1-844-860-0011 (English) China: 800-860-0011/ 400-860-0011 (Chinese)	24 x 7 x 365
Email	Global: serversupport@inspur.com China: lckf@inspur.com	24 x 7 x 365
	US**: serversupportusa@inspur.com	Local business hours

Type	Description	Support Window
	Korea: serversupport_kr@inspur.com Japan: serversupport_jp@inspur.com	9AM to 6PM Monday to Friday **US: PST (GMT -8)
Service Portal* ¹	US**: http://service.inspursystems.com/login.htm EU: http://eurportal.inspur.com/	Local business hours 9AM to 6PM Monday to Friday **US: PST (GMT -8)

ii. RMA Services

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. Repaired or replaced 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.

Advance Replacement: Under the terms of Advance Replacement Service, if a problem with customer product cannot be resolved via hotline and e-mail support and a replacement part is required, Inspur will ship out replacement part(s) in advance within one (1) business day. Customer should return defective part(s) within five (5) business days after receiving the replacement(s). Inspur will cover one-way shipment via ground.

Standard Replacement: When a hardware failure happens, customer may submit RMA request to Inspur via e-mail or Service Portal*¹. Inspur will review and approve RMA submission, and provide an RMA number and return information that customer may use to return for RMA service. Inspur will ship out replacement part(s) within one (1) business day after receiving the defective part(s) and cover one-way shipment via ground.

12.2 Inspur Service SLA

Inspur offers a variety of Service Level Agreements (SLA)*² to meet customer requirements with different service components and service level targets.

- Base Warranty Services
- Advance Replacement
- 9x5 NBD Onsite Service
- 24x7x4 Onsite Service
- Onsite Deployment Service
- Data Media Retention
- Global Service
- Customized Service

12.3 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 Terms & Conditions do not apply to consumable parts, as well as any products that the serial number missed, damaged or obscured 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 staging, usage, or maintenance
- Virus infection
- Loss or damage in transit which is not arranged by Inspur
- The product has been modified or serviced by non-authorized personnel
- Any damage to or loss of any personal data, programs, or removable storage media
- The restoration or reinstallation of any data or programs except the software installed by Inspur when the product is manufactured
- Any consumable parts, such as, but not limited to, battery or protective coating that is diminished over time, unless the failure has occurred during DOA period, such failure caused by Inspur's material or workmanship
- Any cosmetic damage, such as, but not limited to, scratches, dents, broken plastics, metal corrosion, or mechanical damage, unless the failure has occurred during DOA period due to defect in Inspur's material or workmanship
- Any engineering sample, evaluation unit, or non-mass production product is not covered under warranty service
- Any solid-state drive (SSD) with the usages of which has reached its write endurance limit

In no event will Inspur be liable for any direct loss of use, interruption of business, lost profits, lost data, or indirect, special, incidental or consequential damages of any kind regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise, even if Inspur has been advised of the possibility of such damage, and whether or not any remedy provided should fail of its essential purpose.

*1 Service Portal availability is subject to customer type and customer location. Please contact your Inspur representative to learn more.

*2 Not all SLA offerings are available at all customer locations. Some SLA offerings may be limited to geolocation and/or customer type. Please contact your Inspur representative to learn more.