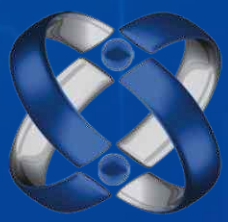


FusionStor®

Fusionstor i6427

Rack Server

User Manual

Document Version: V1.0

Document name	Version	Release date	Publisher	Reviewers	Changes
Fusionstor i6427 Server User Manual	Rack V1.0	2023/12/23			Initial release

Abstract

This manual describes the product specifications, unpacking and installation operations, fault diagnosis and handling suggestions, and product maintenance of the server.

Intended Audience

This manual is intended for engineers who:

Technical support engineer

An administrator responsible for server configuration

Product maintenance engineer

Contents

Chapter 1 Product introduction

1.1 Product Overview

Fusionstor i6427 is a 2U2P universal server developed for the current market demand. Based on the X86 architecture of Intel® Xeon fifth/fourth-generation processor Eagelstream platform, Fusionstor i6427 is suitable for core , business cloud computing, high performance computing, distributed storage and other fields. The Fusionstor i6427 has the advantages of strong scalability and easy management.

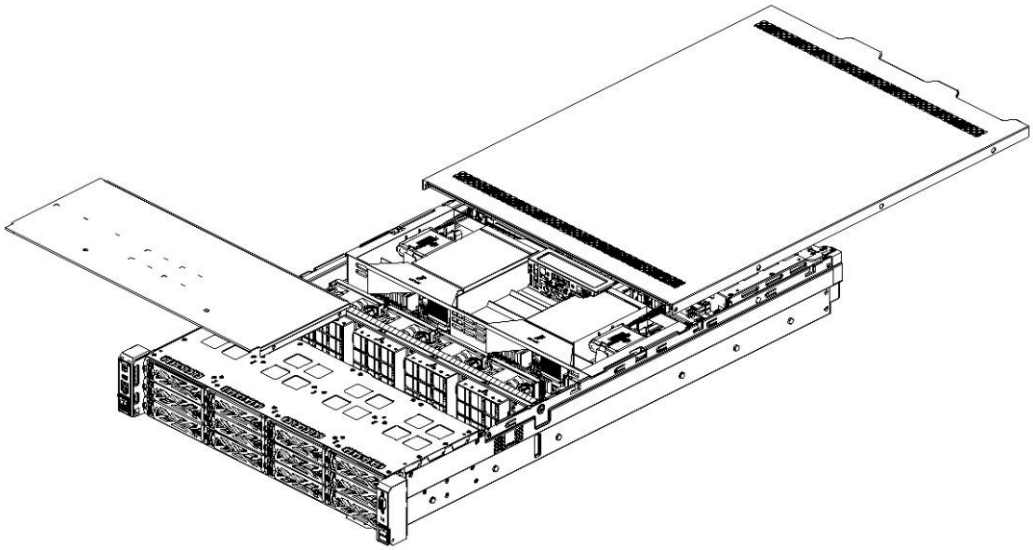


Figure 01.12HDD configuration Fusionstor i6427 system

1.2 Product Features

- High performance

Based on Intel Eagelstream platform, X86 architecture, support the highest specifications of 350W CPU, providing more powerful computing performance;

Support up to 32 DDR5 memory, each CPU supports 8 memory channels.

- Variety

Supports a variety of flexible hard disk configuration schemes, providing flexible and expandable storage capacity space to meet different storage capacity requirements and upgrade requirements;

Supports up to 12 3.5-inch hard disks or 28 2.5-inch hard disks, and

supports 2 M.2 SSDS;

Supports onboard NIC and flexible I/O card, providing a variety of network interfaces;

Supports up to 8 PCIe standard expansion slots;

- Manageability

The UID/HLY LED indicator on the BMC (BMC Integrated Management Module) Web management interface and panel guide technicians to quickly locate components that have failed (or are in the process of failing), simplifying maintenance, speeding up problem resolution, and improving system availability;

The onboard BMC integrated management module (BMC) can continuously monitor system parameters and trigger alarms.

It supports sideband management (NC-SI) and multiplexes management network ports and service network ports. The NC-SI feature is enabled by default.

- Low Power consumption

High efficiency single-board VRD power supply, reduce the loss of motherboard DC power conversion;

Comprehensively optimized system heat dissipation design, efficient and energy-saving system heat dissipation fan, reduce system heat dissipation energy consumption.

1.3 Product technical specifications

For technical specification details, please refer to the Fusionstor i6427 User Technical White paper.

Chapter 2 Product components

2.1 Front Panel components

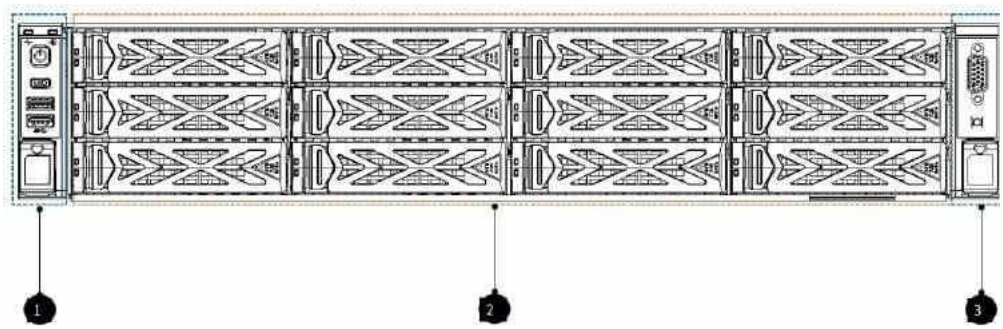


Figure 2-1 Appearance of the front panel

Table 2-11 describes the front panel

1	Left Ear (2*USB 3.0 port)
2	3.5 "LFF Carrier *12
3	Right Ear (VGA port)

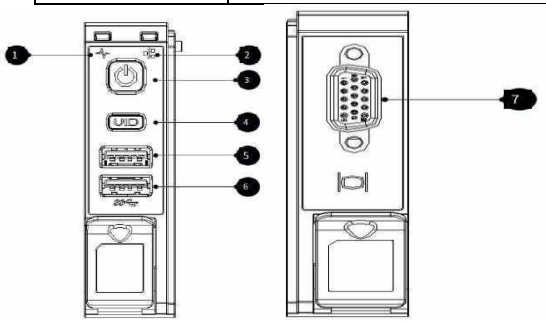


Figure 2-2 Indicators and ports on the front panel

Table 2-2 Describes the indicators and ports on the front panel

Serial Number	Keys	Symbols	Function description
1	System Status Indicator		Persistent green: The system is normal Blinking red (at 1Hz) : A major alarm is generated Blinking red (5Hz) : A critical alarm is generated Off: The system is shut down
2	Network link indicator		Persistent yellow: Any network port is properly connected Blinking (2.5Hz) : Any network port is connected
3	Power switch button/indicator light		Steady green: The device is powered on properly Off: The device is not powered on Persistent yellow: Power off Flash yellow: 1. If the single PSU is present and the PSU overtemperature is detected, the yellow indicator blinks at 4Hz. If the PSU overtemperature is detected, the system automatically powers off 2. If both power supplies are present and single power supply overtemperature is present, the yellow indicator blinks, indicating
4	UID button/indicator light		Persistent blue: System identifier activated Off: The system ID is not activated Blinking blue: Remote management
5	USB 3.0 port		Devices that can support USB3.0
6	USB 3.0 port		Devices that can support USB3.0

Serial Number	Keys	Symbols	Function description
7	VGA interface		Support VGA port display device

2.2 Rear Panel components

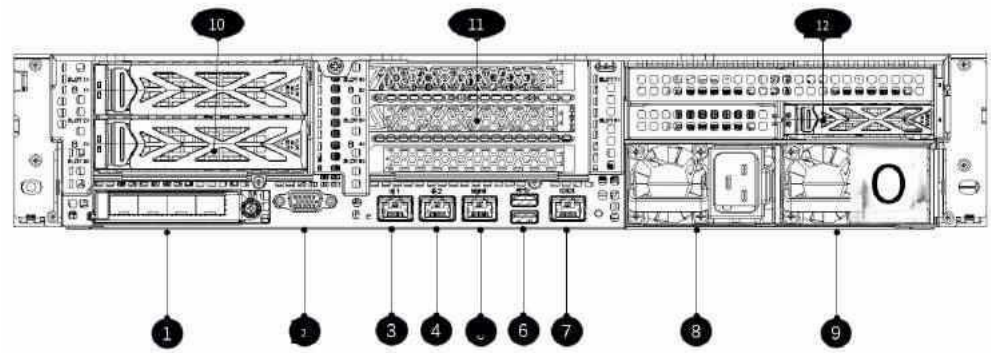


Figure 22-2panel appearance 1

Table 22-2panel

1	OCP module
2	VGA port
3	GE1 electrical port
4	GE2 electrical port
5	BMC Management network port
6	USB 3.0 port *2
7	RJ45 serial port
8	Power module interface
9	Power module interface
10	IO module 1
11	IO Module 2
12	IO module 3

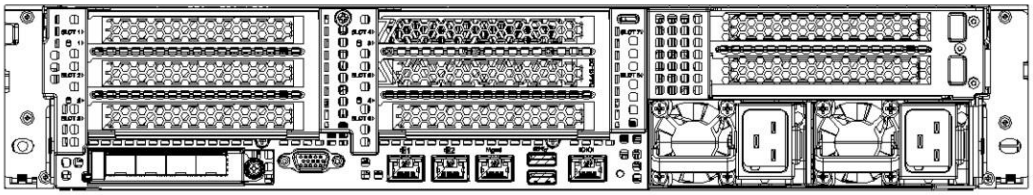


Figure 23-3panel appearance 2

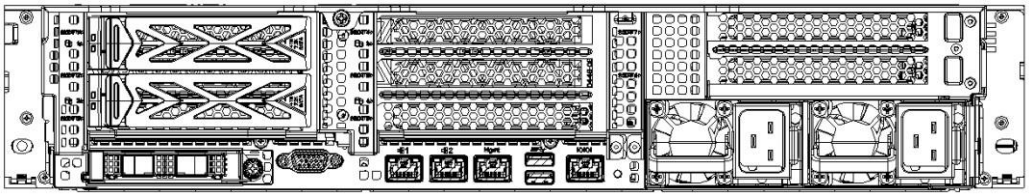


Figure 24-4panel appearance 3

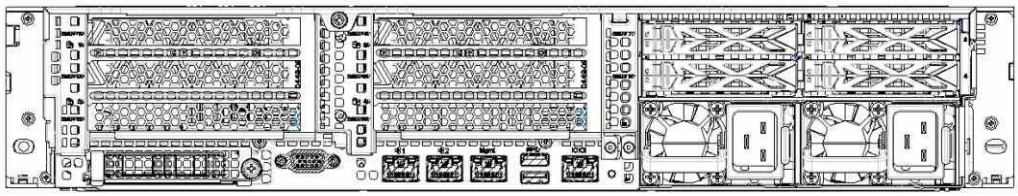


Figure 25-5panel appearance 4

2.3 Mainboard Components

The Fusionstor i6427 architecture block diagram is as follows:

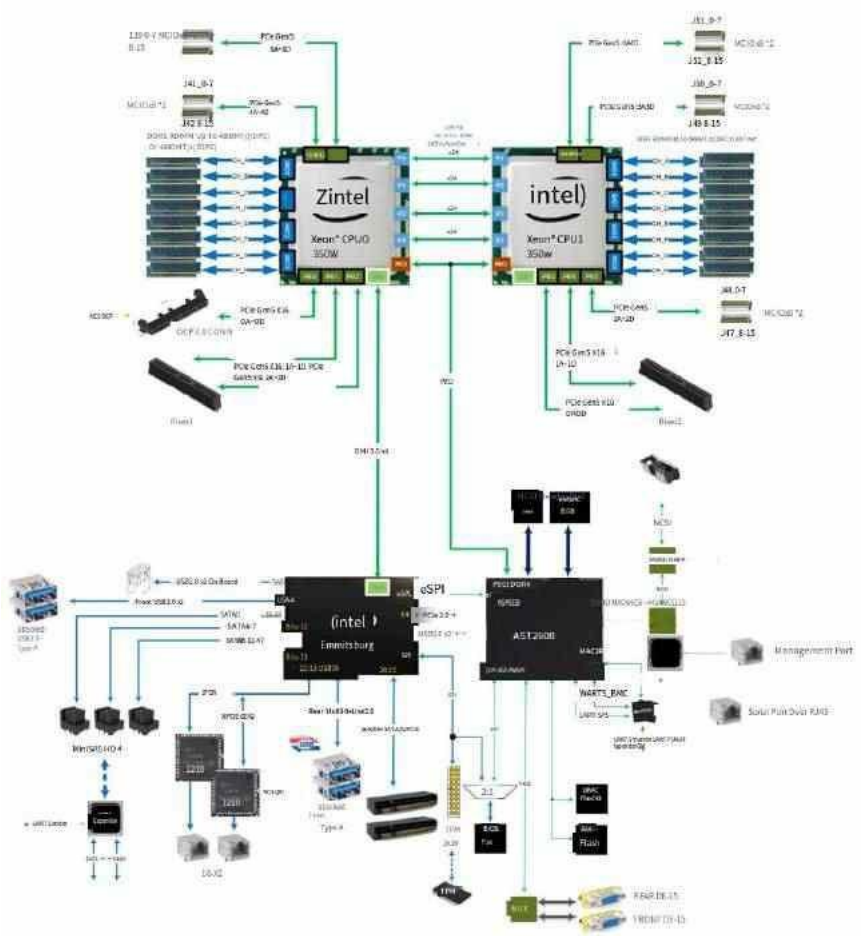


Figure 27 Motherboard architecture schematic diagram-

- Support 2 Intel Icelake processors.
- Support 32 RAM.
- The processor is connected to three PCIe Riser cards through the PCIe bus.
  Different PCIe Riser cards support different PCIe slots.
- The PCH comes out with 14 sets of SATA signals to support various local storage specifications through different hard drive backplanes.
- Using LBG-R PCH (Platform Controller Hub), through PCH: supports 2 onboard GE electrical ports.

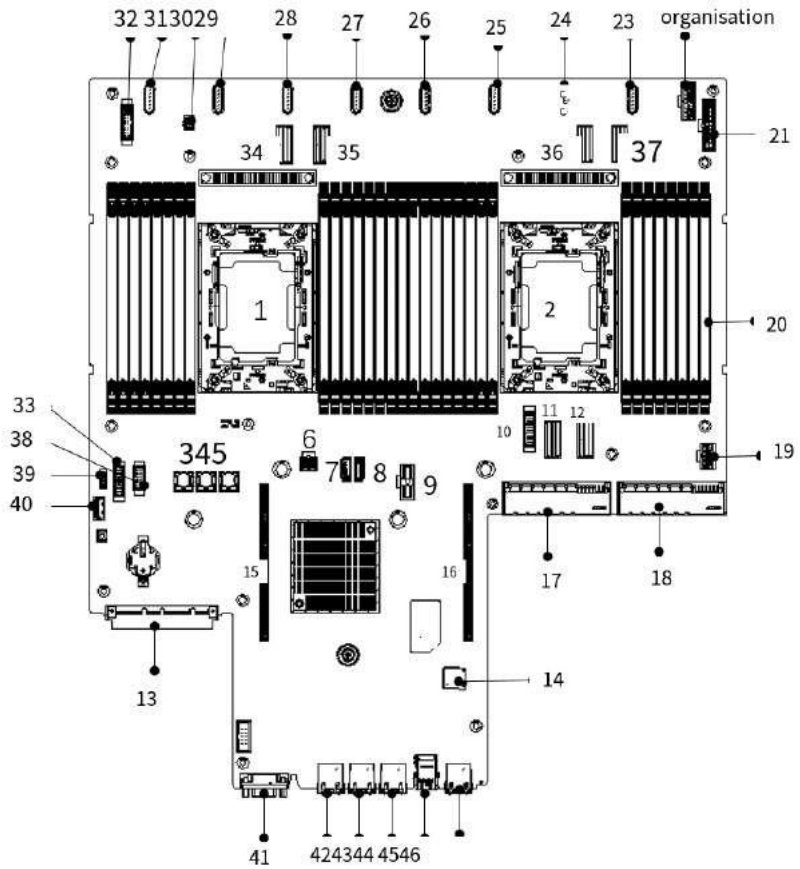


Figure 2-8 Schematic diagram of ports on the mainboard

Table 2-4 Description of ports on the Fusionstor i6427 mainboard

Serial Number	Instructions	Serial number	Instructions
1	CPU0(U1) socket	24	2U Fan1 interface (J201)

2	CPU1(U2) socket	25	1U Fan3 Interface (J202)[reserved]
3	MINIHD PORTC Interface (J171)	26	2U Fan2 interface (J203)
4	MINIHD PORTB Interface (J170)	27	1U Fan5 Interface (J204)[reserved]
5	MINIHD PORTA Interface (J172)	28	2U Fan3 interface (J205)
6	RBP_PWR2 interface (J198)	29	1U Fan7 Interface (J206)[reserved]
7	sSATA 0 interface (J193)	30	CHASSIS_OPEN interface (J235)[reserved]
8	sSATA 1 Interface (J194)	31	2U Fan4 interface (J207)
9	FBP_USB interface (J53)	32	FBP_MISC interface (J212)
10	RBP_MISC Interface (J209)	33	Front VGA port (J55)
11	SLIMLINE 6 Interface (J165)	34	SLIMLINE 1 Interface (J161)
12	SLIMLINE 7 Interface (J166)	35	SLIMLINE 2 Interface (J162)
13	OCP 3.0 Interface (J68)	36	SLIMLINE 3 Interface (J163)
14	SD1 interface (J79)[reserved]	37	SLIMLINE 4 Interface (J164)
15	RISER 1 port (J145)	38	NCSI Interface (J213)
16	RISER 2 port (J179)	39	RAID_Key interface (J4A1)
17	PSU1 interface (J75)	40	USB 2.0 port (J78)
18	PSU2 interface (J76)	41	REAR VGA port (J52)

19	RBP_PWR interface (J210)	42	LAN1 Electrical port (J176)
20	DIMM slot	43	LAN2 Electrical port (J177)
21	FBP_PWR1 interface (J168)	44	Mgmt Network Port (J150)
22	FBP_PWR2 interface (J167)	45	USB 3.0 port (J199)
23	1U Fan1 Interface (J200)[reserved]	46	COM1 Interface (J242)

2.4 DIMM slot

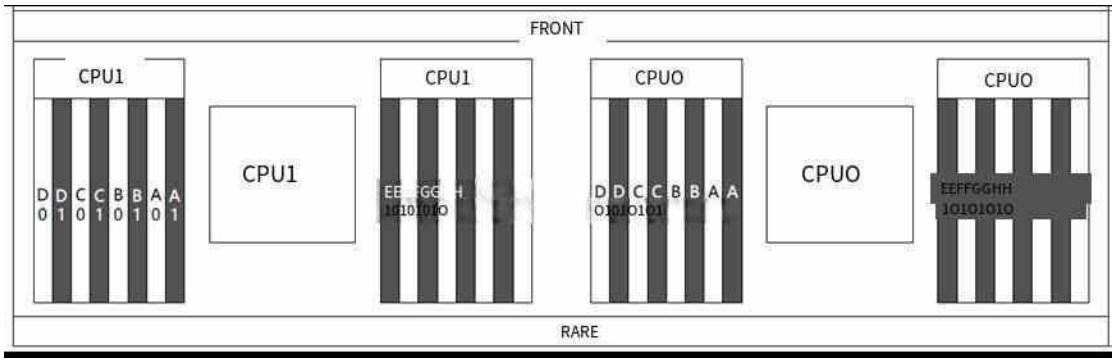


Figure 2-9 Location of memory slots

DDR5 installation rules:

Table 2-5 Memory installation rules for CPU0

Channels	Memory Location	Amount of memory (√ for recommended, O for not recommended)															
		√	√	O	√	O	√	O	√	O	O	O	√	O	O	O	√
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	CPU0_CH_A0	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU0_CH_A1									●	●	●	●	●	●	●	●
B	CPU0_CH_B0					●	●	●	●	●	●	●	●	●	●	●	●
	CPU0_CH_B1													●	●	●	●
C	CPU0_CH_C0			●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU0_CH_C1											●	●	●	●	●	●
D	CPU0_CH_D0							●	●	●	●	●	●	●	●	●	●
	CPU0_CH_D1															●	●
E	CPU0_CH_E0		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU0_CH_E1										●	●	●	●	●	●	●
F	CPU0_CH_F0						●	●	●	●	●	●	●	●	●	●	●
	CPU0_CH_F1														●	●	●
G	CPU0_CH_G0				●	●	●	●	●	●	●	●	●	●	●	●	●

	CPU0_CH_G1												●	●	●	●	●
H	CPU0_CH_H0								●	●	●	●	●	●	●	●	●
	CPU0_CH_H1																●

Table 2-6 CPU1 Memory installation rules

Channels	Memory Location	Amount of memory (√ for recommended, O for not recommended)															
		√	√	O	√	O	√	O	√	O	O	O	√	O	O	O	√
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	CPU1_CH_A0	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_A1									●	●	●	●	●	●	●	●
B	CPU1_CH_B0					●	●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_B1													●	●	●	●
C	CPU1_CH_C0			●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_C1											●	●	●	●	●	●
D	CPU1_CH_D0							●	●	●	●	●	●	●	●	●	●
	CPU1_CH_D1															●	●
E	CPU1_CH_E0		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_E1										●	●	●	●	●	●	●

F	CPU1_CH_F0						●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_F1														●	●	●
G	CPU1_CH_G0				●	●	●	●	●	●	●	●	●	●	●	●	●
	CPU1_CH_G1												●	●	●	●	●
H	CPU1_CH_H0								●	●	●	●	●	●	●	●	●
	CPU1_CH_H1																●

CPUs/DIMMs	DIMM Slots
2CPUs&2DIMMs (1+1)	CPU0: A0 CPU1: A0
2CPUs&4DIMMs (2+2)	CPU0: A0, E0 CPU1: A0, E0
2CPUs&6DIMMs (4+2)	CPU0: A0, C0, E0, G0 CPU1: A0, E0
2CPUs&8DIMMs (4+4)	CPU0: A0, C0, E0, G0 CPU1: A0, C0, E0, G0
2CPUs&12DIMMs (6+6)	CPU0: A0, B0, C0, E0, F0, G0 CPU1: A0, B0, C0, E0, F0, G0
2CPUs&16DIMMs (8+8)	CPU0: A0, B0, C0, D0, E0, F0, G0, H0 CPU1: A0, B0, C0, D0, E0, F0, G0, H0
2CPUs&24DIMMs (12+12)	CPU0: A0, A1, B0, C0, C1, D0, E0, E1, F0, G0, G1, H0 CPU1: A0, A1, B0, C0, C1, D0, E0, E1, F0, G0, G1, H0
2CPUs&32DIMMs (16+16)	CPU0: A0, A1, B0, B1, C0, C1, D0, D1, E0, E1, F0, F1, G0, G1, H0, H1 CPU1: A0, A1, B0, B1, C0, C1, D0, D1, E0, E1, F0, F1, G0, G1, H0, H1

Note: 1: x8 DIMMs and x4 DIMMs cannot be mixed in the same channel.

2: non-3DS and 3DS RDIMMs cannot be mixed in the same channel;

3:9X4 RDIMMS cannot be mixed with other DIMMs (10x4 CPS or non 9x4 RDIMMs).

2.5 Model explosion diagram

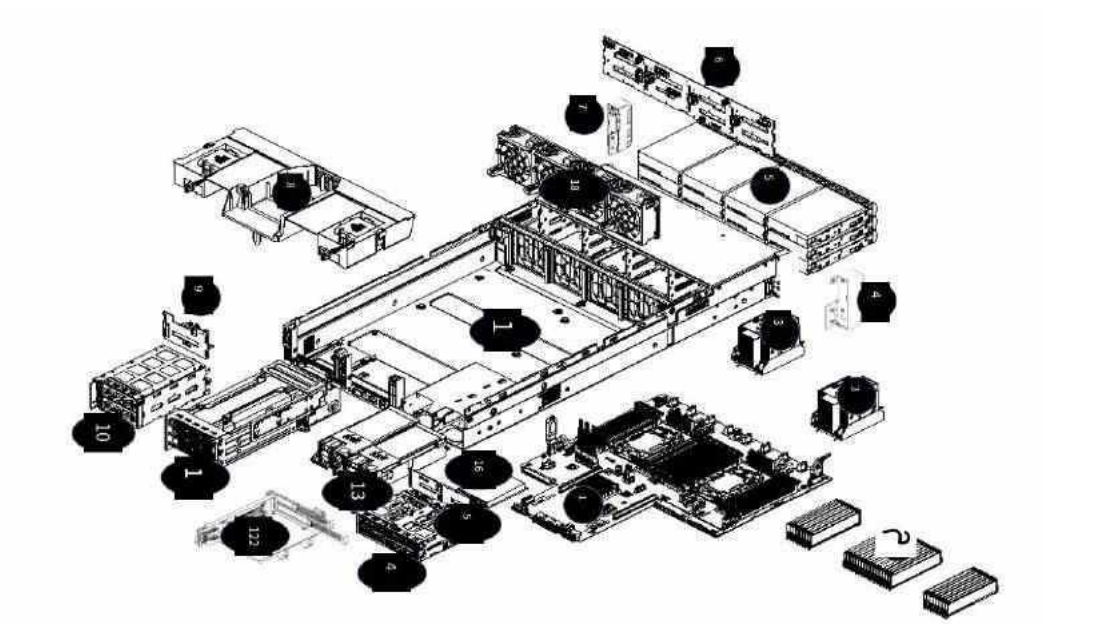


Figure 2-10 Product layout

Table 2-7 Product layout description

Serial Number	Instructions	Serial number	Instructions
1	Motherboard	10	Dual hard drive module
2	Memory	11	3PCIE modules
3	radiator	12	2PCIE module
4	Left ear	13	Power supply
5	Front hard drive module	14	4 Hard drive module
6	Front hard drive backplane	15	4 Hard drive backplane
7	A.d.	16	Flexible I/O card
8	Air deflector	17	Case
9	Dual hard drive backplane	18	Fan

Chapter 3 Product Installation and removal

3.1 Complete machine installation procedure

Step 1: Unpack the server

Before opening the packing case, check whether the packing case is damaged. If it is damaged, contact the delivery personnel to consult the situation, and record the documents for later processing.

Step 2: Place the server

The server should be placed in a clean environment, well ventilated, away from heat sources and strong electromagnetic areas, and provide enough space. Step 3: Connect the server

Connect the monitor, and gently insert the signal cable of the monitor according to the shape of the interface, and lock the screws on both sides;

Connect the network cable, the network cable is the standard RJ45 interface;

Connect the power cable, the power cable adopts the standard 220V input, and use the three-wire interface with safety grounding, make sure that the total power supply is off before inserting the power cable;

Finally confirm that each part of the connection is correct and firm, turn on the main power switch.

3.1.1 Packaging diagram

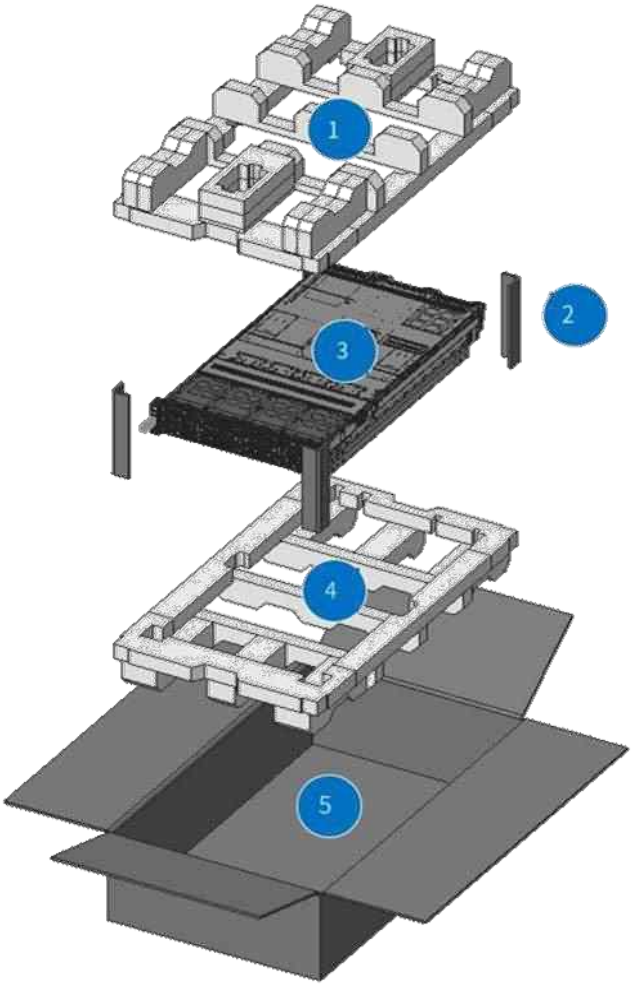


Figure 3-1 Packaging diagram

Table 3-1 Description of the packing parts

Serial Number	Instructions
1	Foam the upper part of the chassis
2	Paper fluting
3	Machine &PE bag
4	Foam the bottom of the chassis
5	Cartoon box

3.1.2 Machine out

Step 1: Open the outer package and remove the foam from the upper part of the chassis:

Step 2: Two people take out the machine, remove the PE bag, and place the machine horizontally on the table.

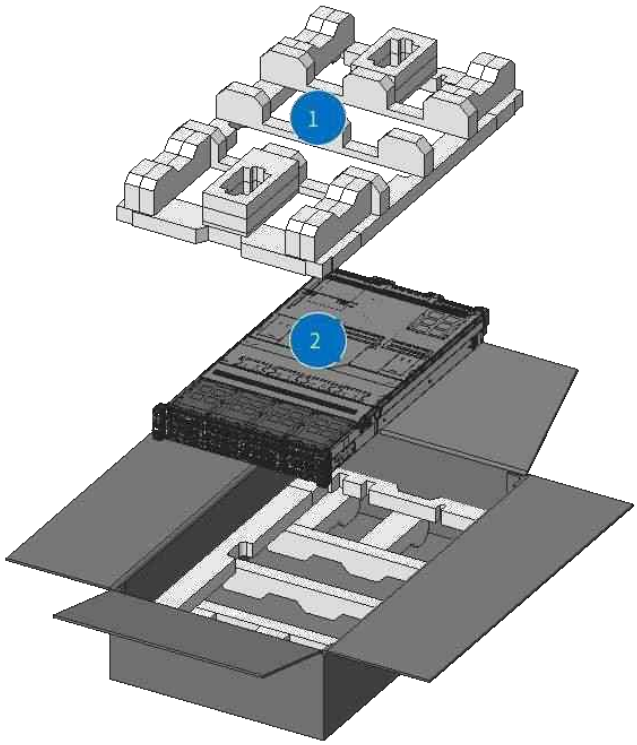


Figure 3-2 Packaging diagram

Before opening the packing case, check whether the packing case is damaged. If it is damaged, contact the delivery personnel to consult the situation, and record the documents for subsequent processing.

3.1.3 Connecting cables outside the chassis

Step 1 Connect cables in the I/O area of the mainboard. For details, see Figure 2-3 and Table 2-3.

Step 2: Connect the CRPS power cable in the red box.

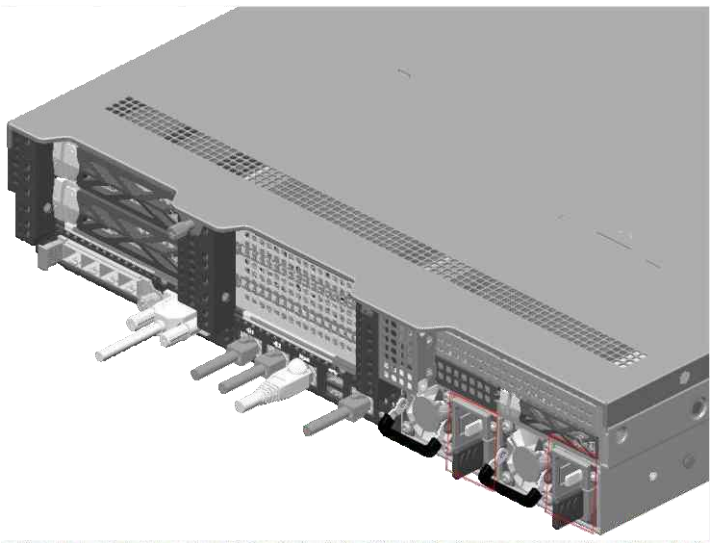


Figure 3-3 External chassis wiring diagram

3.2 Cover opening procedure

Step 1: Remove the two fixing screws on the side of the chassis;

Step 2: Unscrew the hand screw;

Step 3: Push back to remove the back cover;

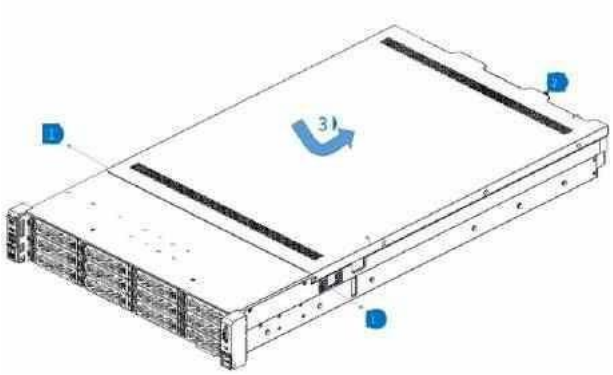


Figure 3-4 Schematic diagram of opening the chassis cover

Step 4: Remove the air hood as shown.

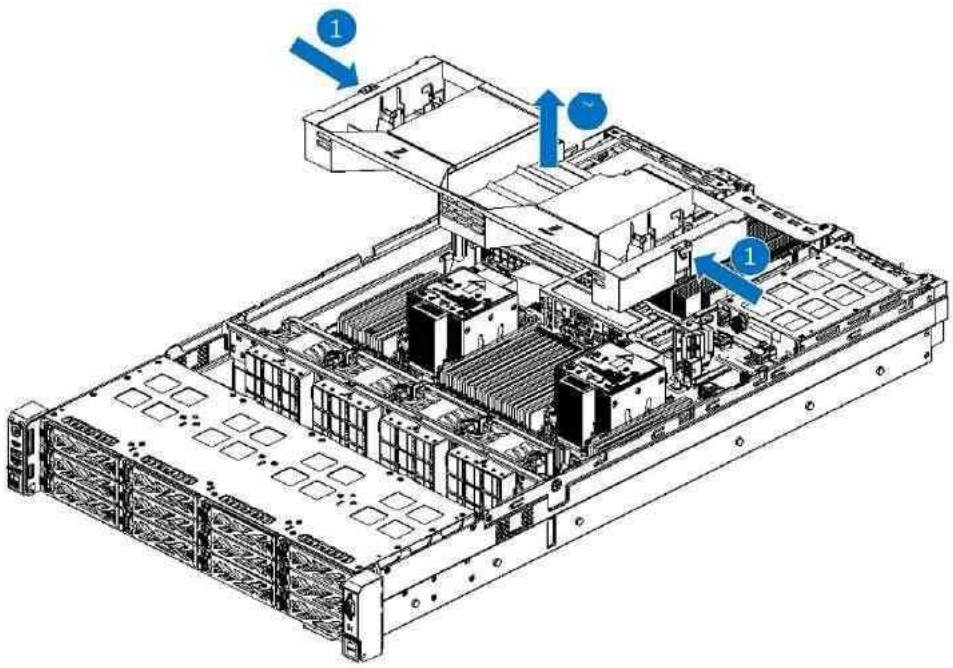
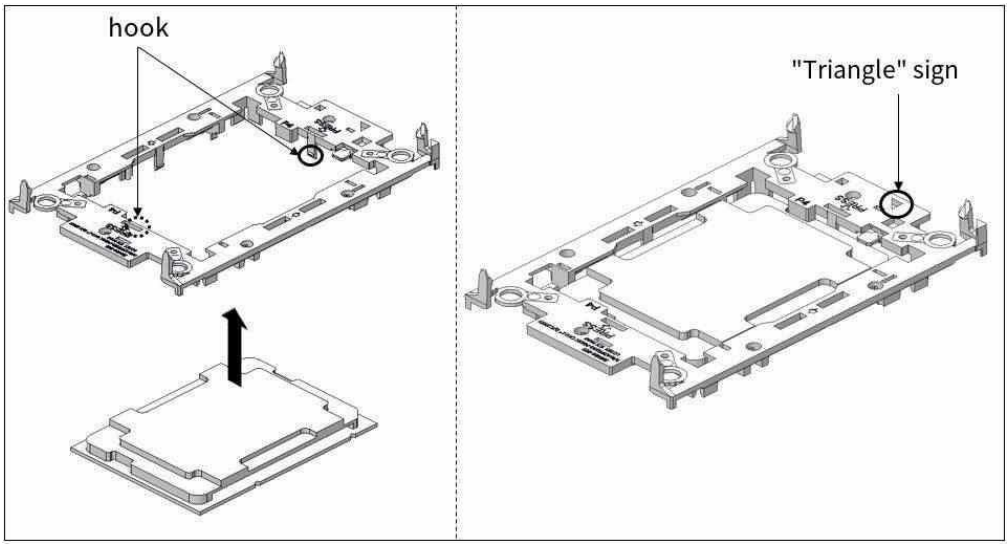


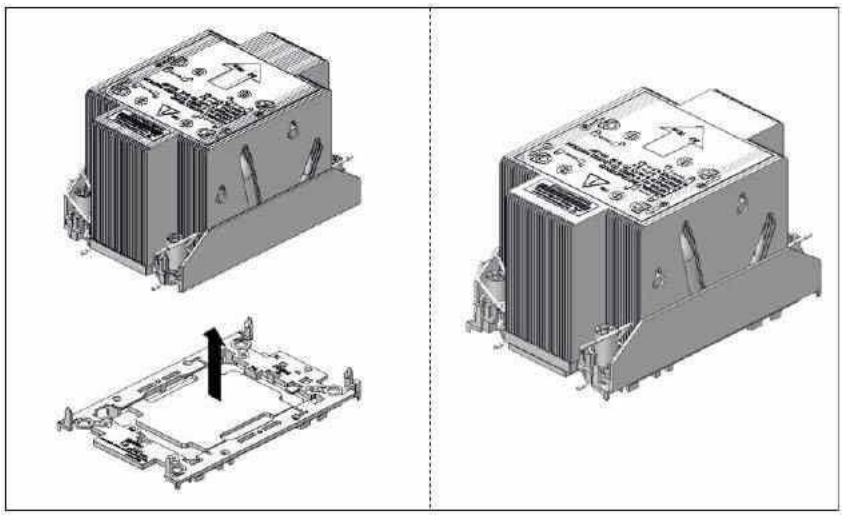
Figure 3-5 Removing the air hood

3.3 Steps for removing and installing a CPU

Step 1: Install the CPU to the Clip, pay attention to the CPU must be fixed by the Clip Clip, and the "triangle" on the CPU and the "triangle" on the clip must be in the same corner;



Step 2: Then install the Clip&CPU on the heat sink, and note that the "triangle" on the heat sink and the triangle on the Clip must be in the same corner;



Step 3: Align the module with the heat sink hole on the mainboard, and tighten the screws according to the indicating sticker on the heat sink.

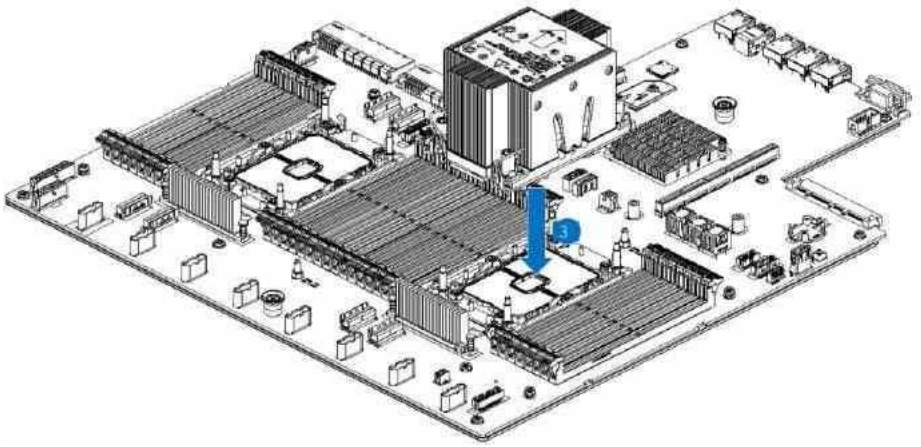


Figure 3-6 Installing the CPU

3.4 Steps for removing and installing the memory

● Assembly steps:

Step 1: Open the wrenches on either side of the memory slot;

Step 2: Put the memory into the slot with the anti-stay gap;

Step 3: Press the memory firmly into the memory slot until the memory latch is fully locked.

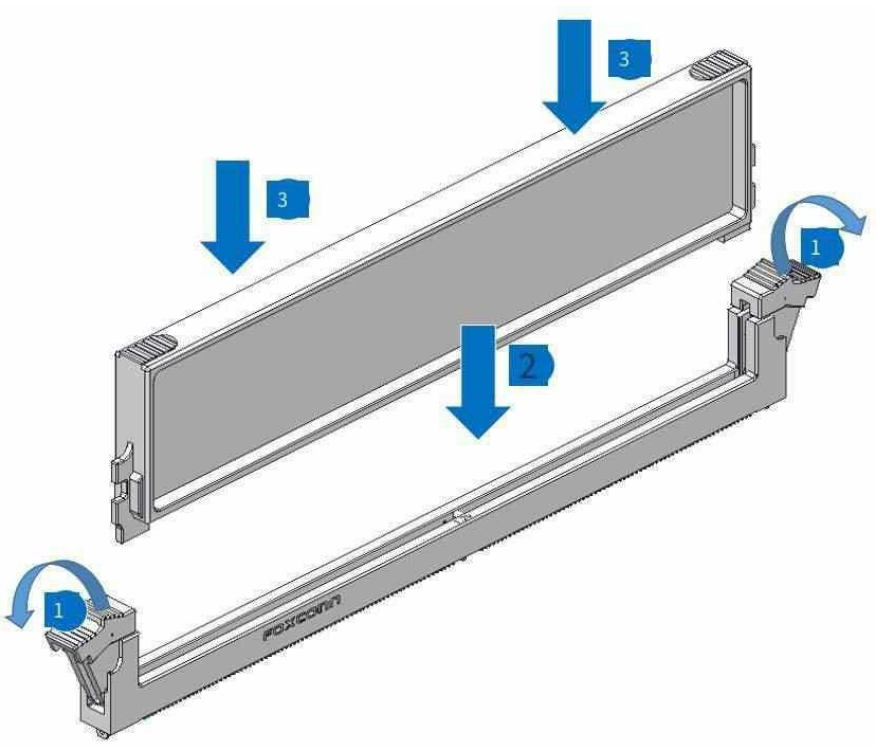


Figure 3-7 Memory installation diagram

- Dismantling steps:

Step 1: Open the wrenches on both sides of the memory slot to unlock it;

Step 2: Slowly pull out the memory module upward, that is, the removal is complete.

3.5 Steps for removing and installing a Hard disk

- Installation

Step 1: Push the hard drive into place; Step 2: Rotate the baffle to secure.

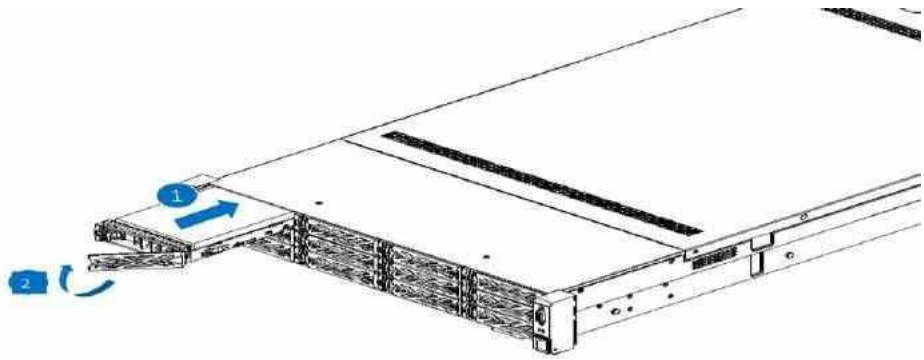


Figure 3-8 Installing the hard disk

- Remove

Step 1: Press the release mechanism;

Step 2: Open the panel;

Step 3: Pull out the hard drive module.

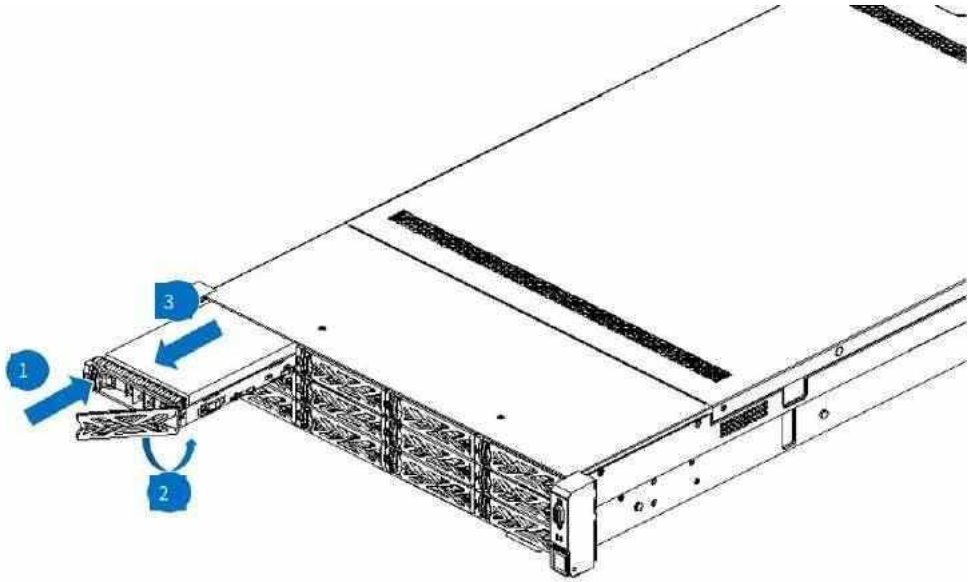


Figure 3-9 Removing the hard drive

3.6 Steps for removing and installing a power supply

- Installation

Step 1: Push power supply into fixed position; Step 2: Depress the pull ring.

Step 3: Insert the AC cable and straighten the Velcro

Step 4: Use Velcro to wrap and secure the AC cable

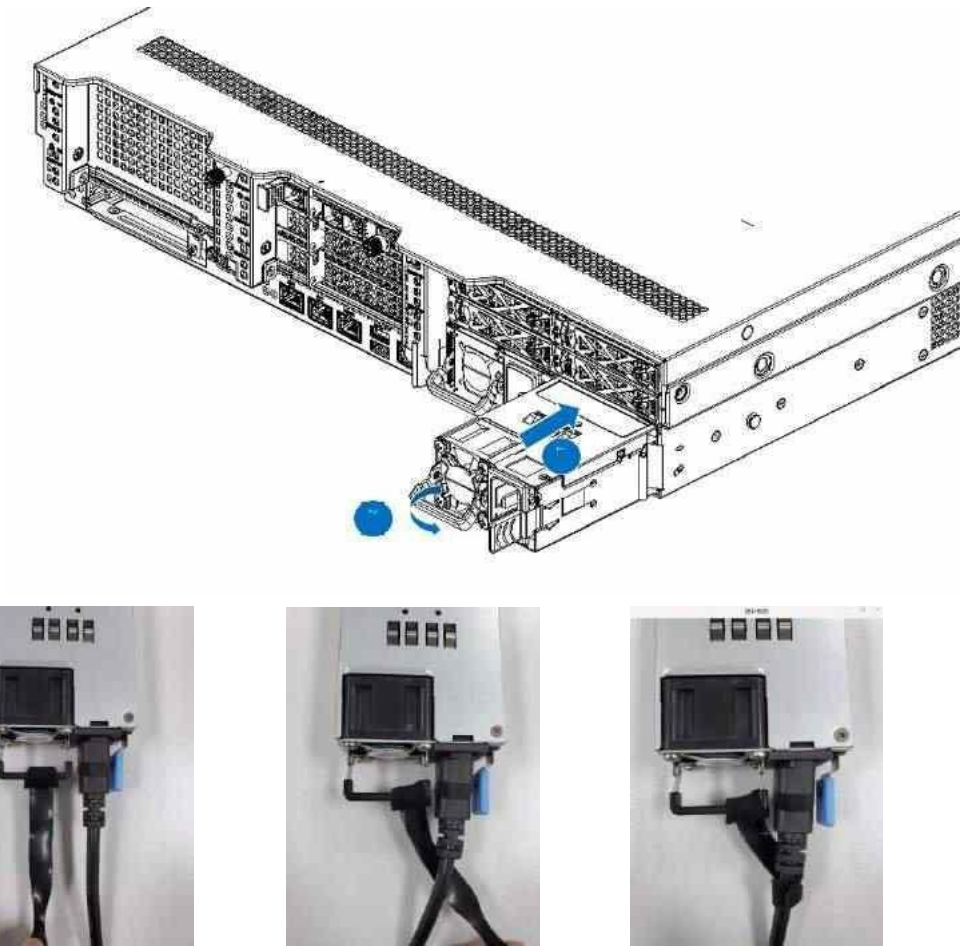


Figure 3-10 Power supply installation diagram

● Remove

Step 1: Press the release mechanism;

Step 2: Lift the pull ring;

Step 3: Pull out the power supply.

3.7 Steps for removing and installing an expansion card

Step 1: Open the clip and remove the baffle plate;

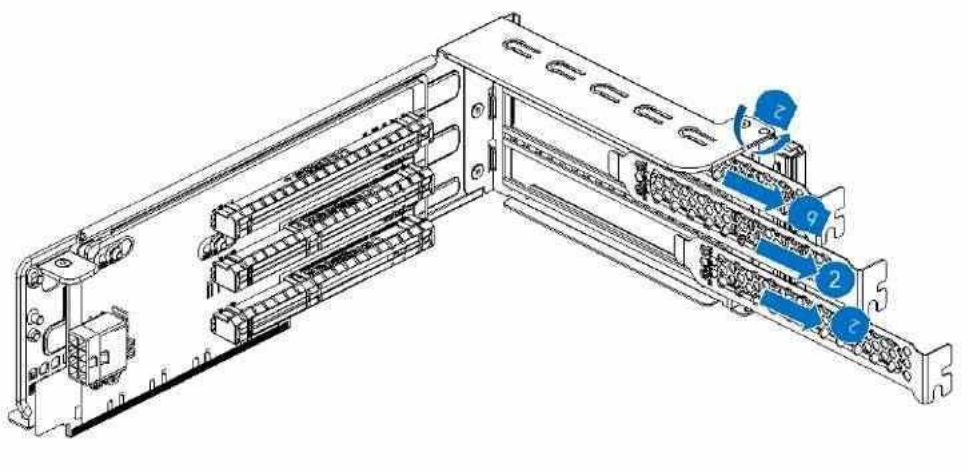


Figure 3-11 Removing the baffle from the expansion card support

Step 2: Install the expansion card into the slot and lock the structure of the compression card;

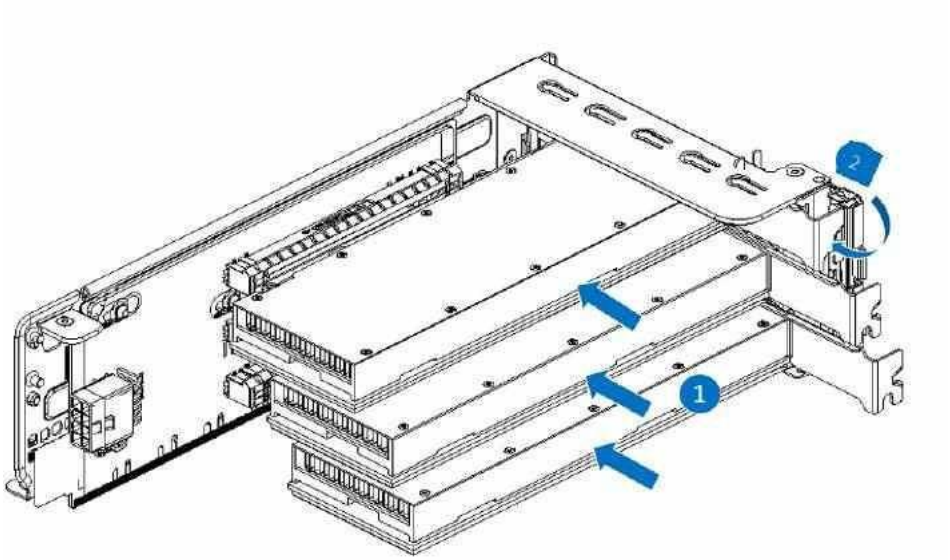


Figure 3-12 Installation diagram of the expansion card

Step 3: To install a full-height full-length video card, install a video card bracket.

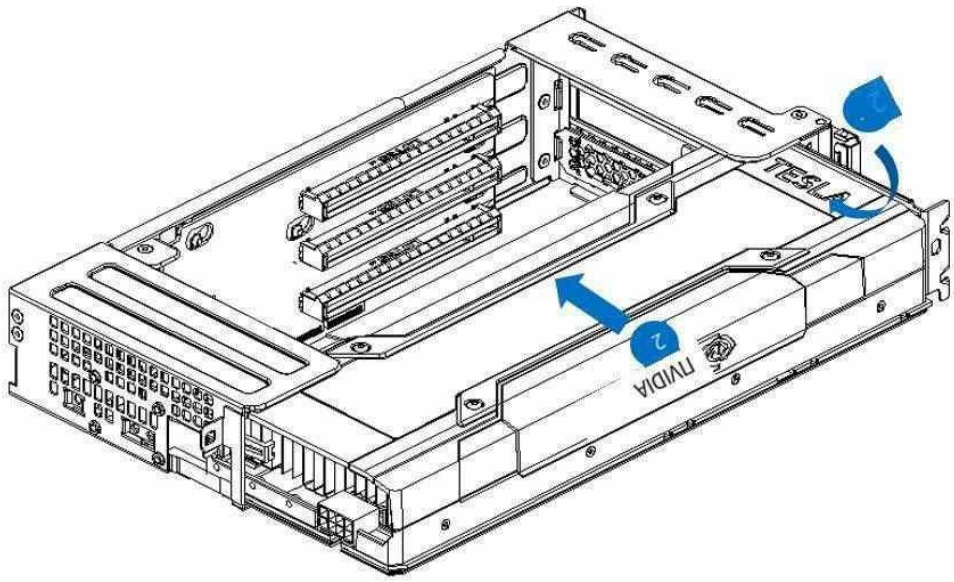


Figure 3-13 Installing the GPU card

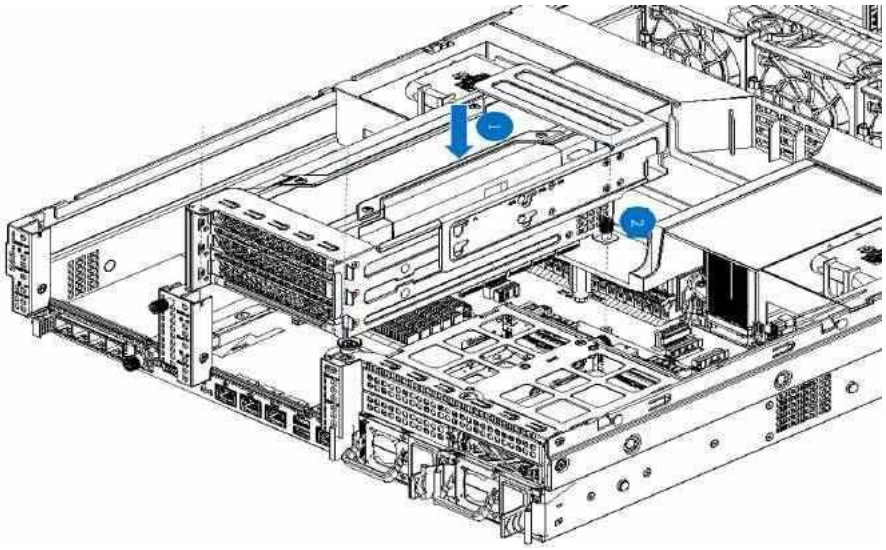


Figure 3-14 Installing the expansion card module

Note: The disassembly procedure is reversed.

3.8 Steps for removing and installing a Dual GPU module

Step 1: Open the clip and remove the block;

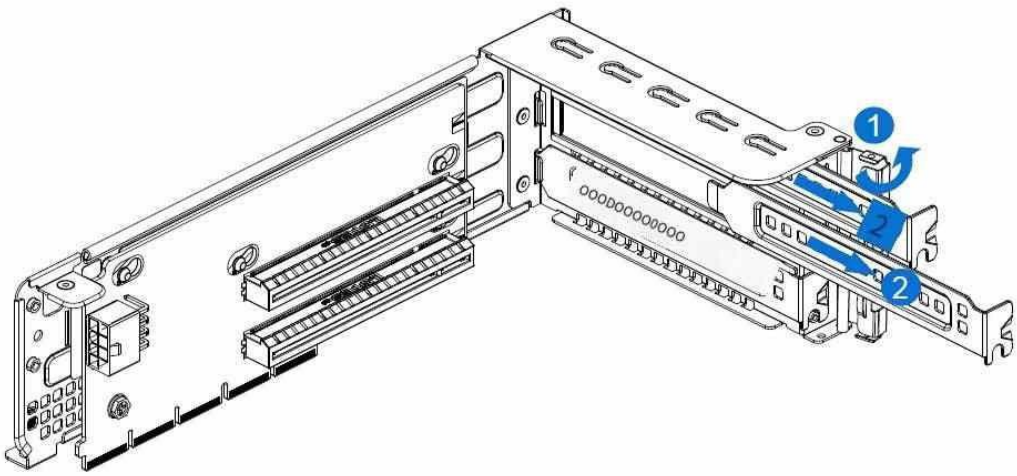


Figure 3-15 Removing the baffle from the expansion card support

Step 2: Install the GPU bracket.

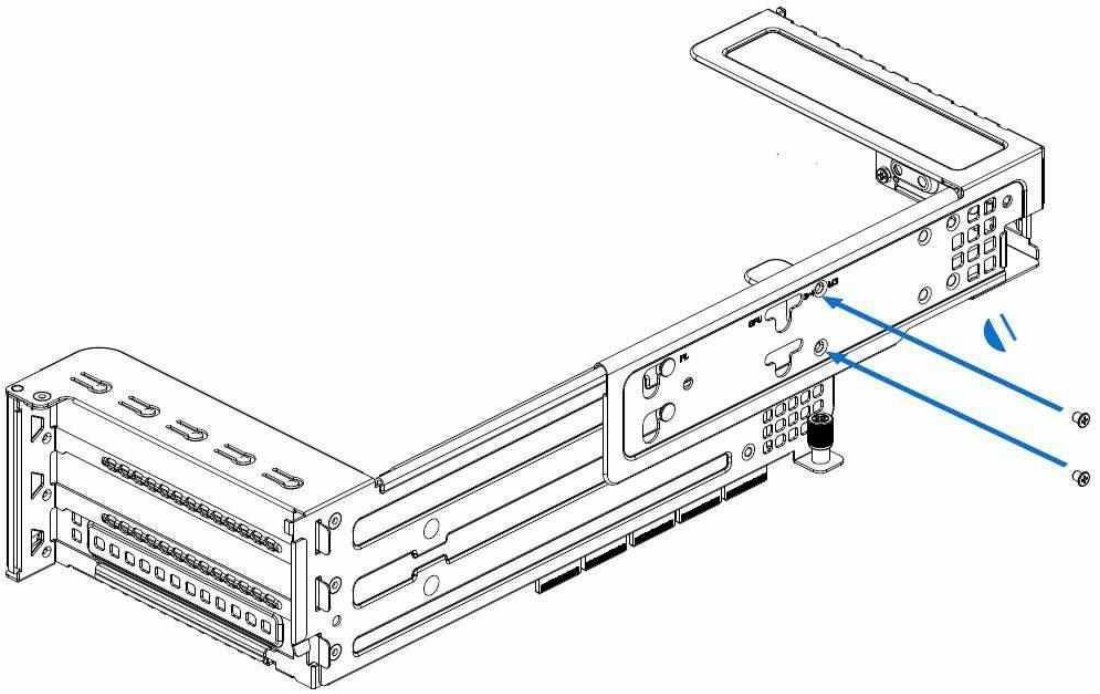


Figure 3-16 Installing the GPU bracket

Step 3: Load the full-height full-length GPU into the slot and lock the compression card structure;

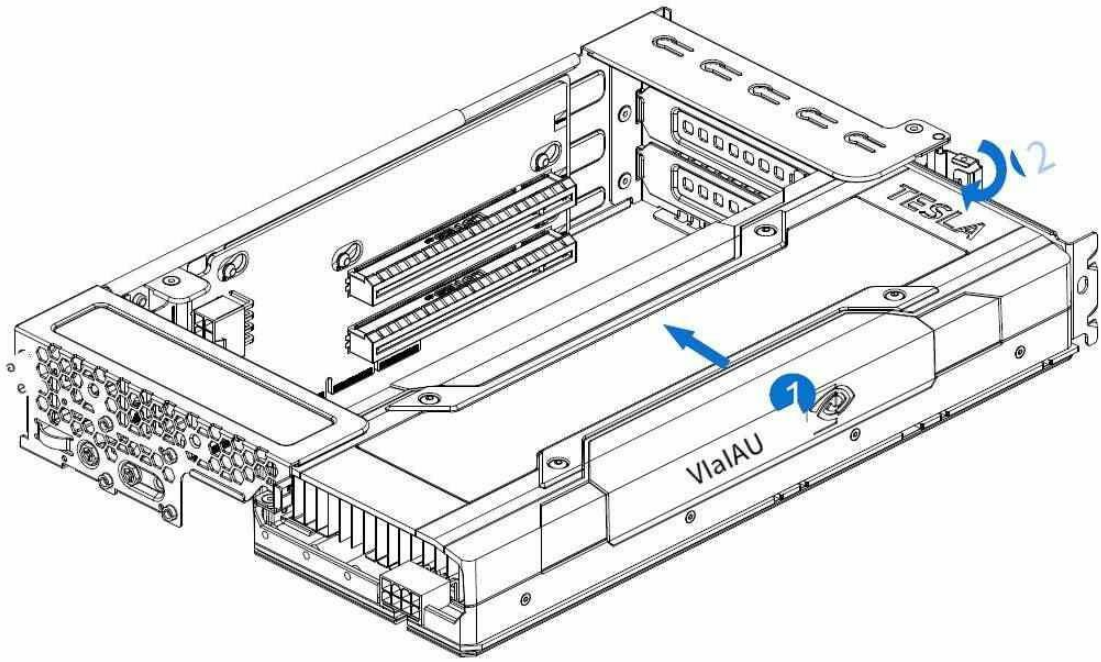


Figure 3-17 GPU installation diagram

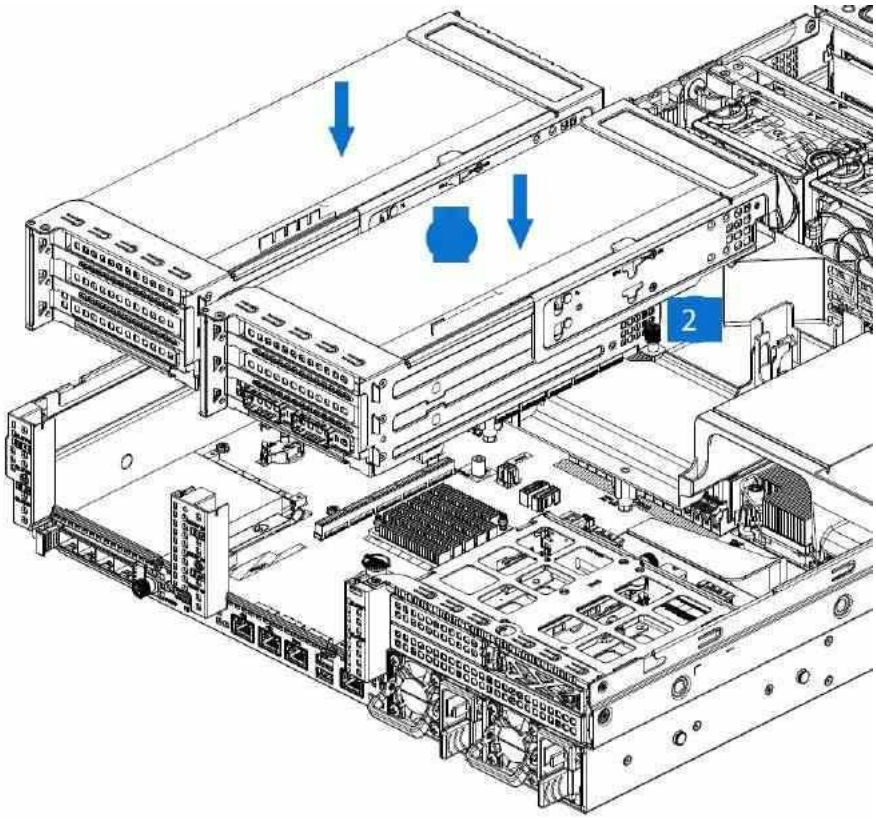


Figure 3-18 Installing a dual GPU module

Note: The removal steps are reversed.

3.9 Steps for removing and installing a fan card

● Installation

Step 1: Load the fan mold into the case as shown.

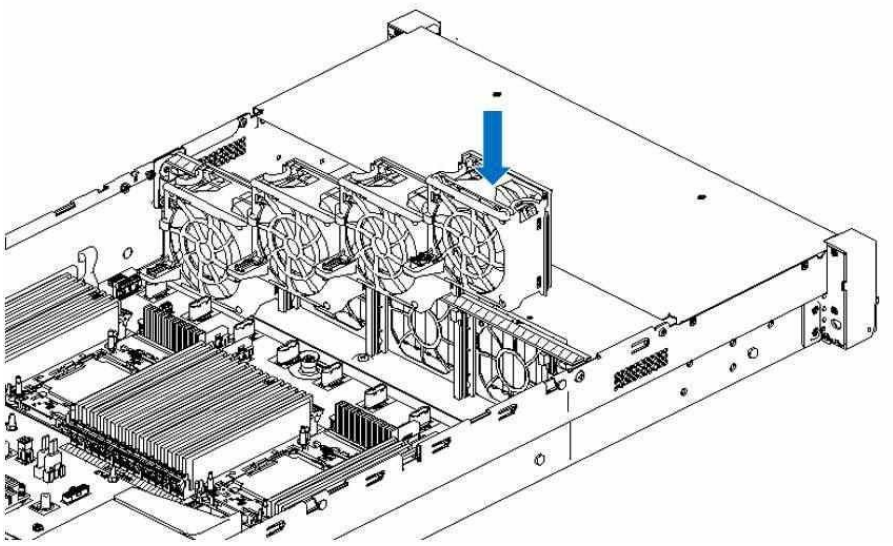


Figure 3-15 Schematic diagram of installing the fan

● Remove

Step 1: Press the bayonet on both sides; Step 2: Lift the fan module.

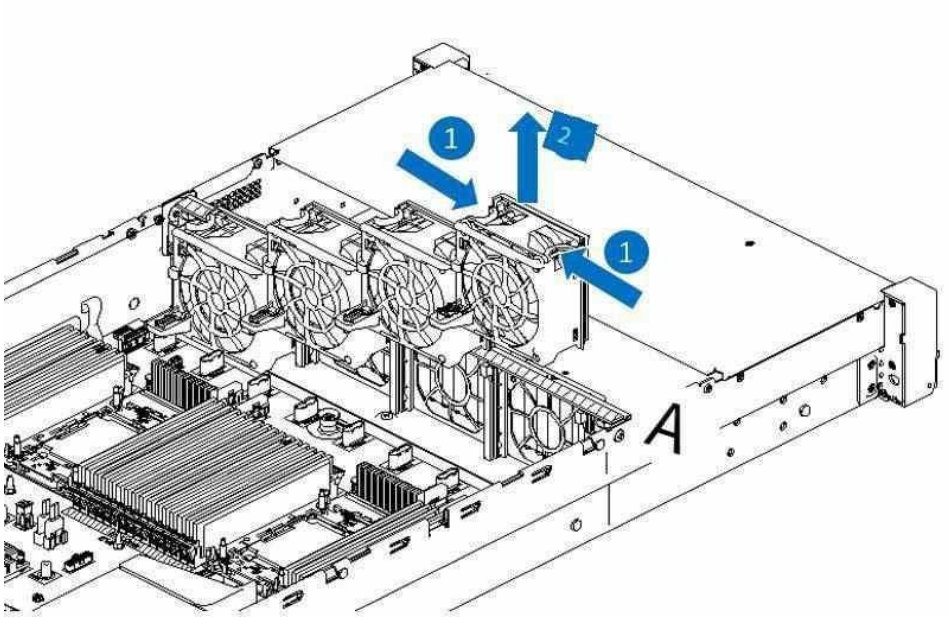


Figure 3-16 Pulling out the fan module

Note: To install, simply align the fan with the slot and insert it into the chassis.

3.10 OCP Card Installation Steps

- Install

Step 1: Push the OCP card into a fixed position; Step 2: Tighten the hand screw.

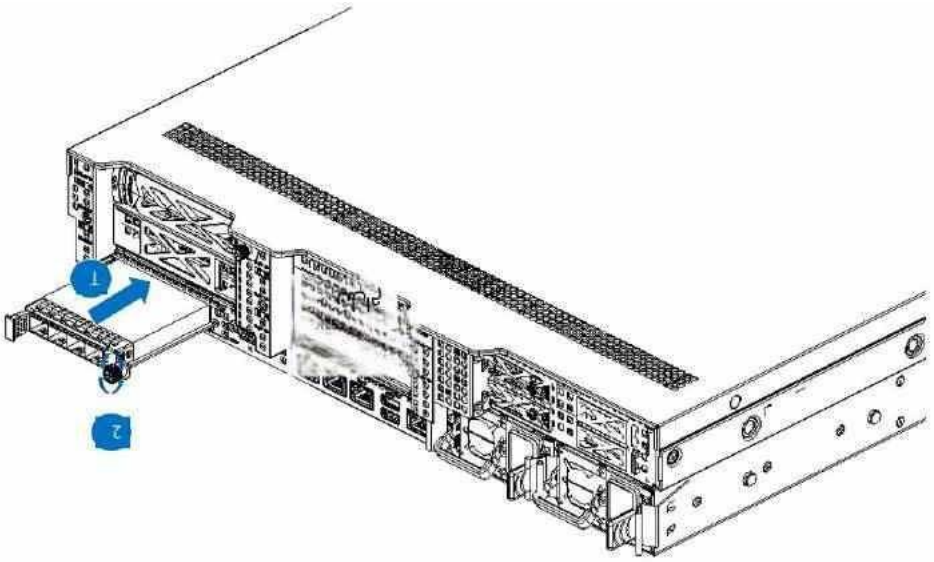


Figure 3-17 Installing the OCP card

- Remove

Step 1: Unscrew the secured hand screw;

Step 2: Press to unlock the structure;

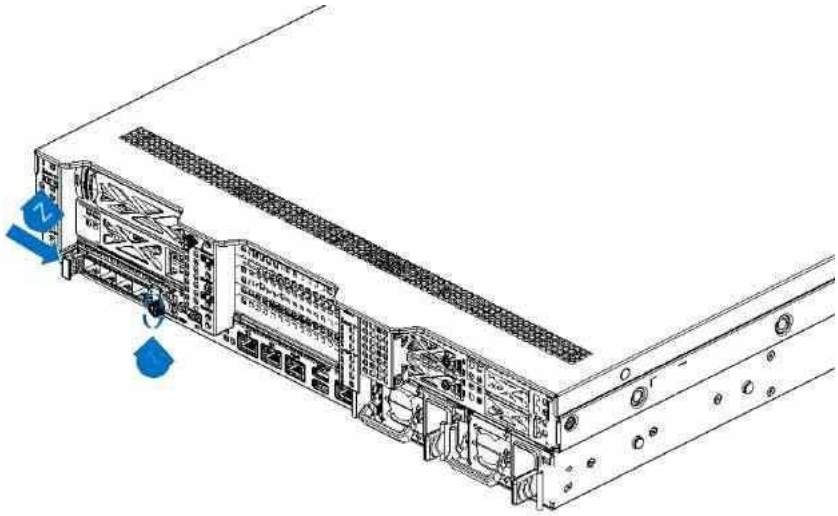


Figure 3-18 Unlocking the OCP card

Step 3: Pull out the OCP card.

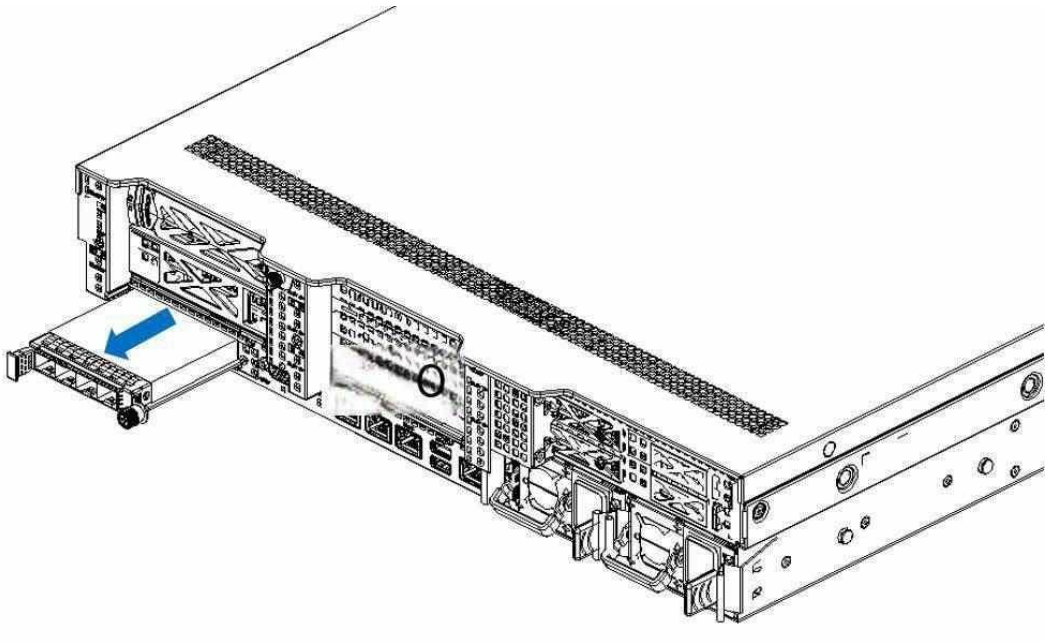


Figure 3-19 Pulling out the OCP card

3.11 Guide Rail installation

Remove the inner rail of the guide rail and fix it to the chassis by aligning the chassis hanging nails.

Figure 3-20 Installing the inner rails on the chassis

3.12 Installing the chassis into the Cabinet

Step 1: Two people in front and behind, the rear operator first guide rail rear spring latch aligned with the hole into the rack hole.

Step 2: The front operator aligns the hole of the outer rail of the guide rail to the frame hole, and locks two screws to fix the guide rail on the frame.

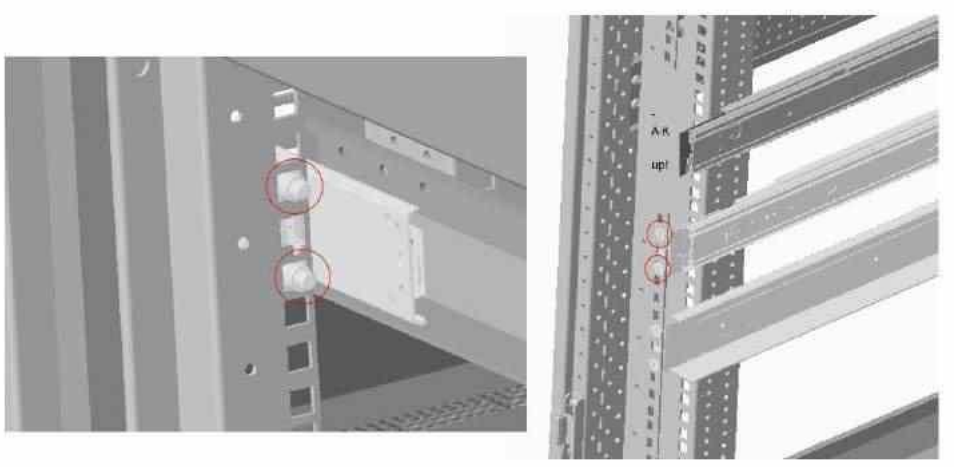


Figure 3-21 Installing the outer rail of the rack guide rail

Step 3: Lift the chassis, align the inner rail of the chassis with the outer rail of the rack, and push the machine into the cabinet

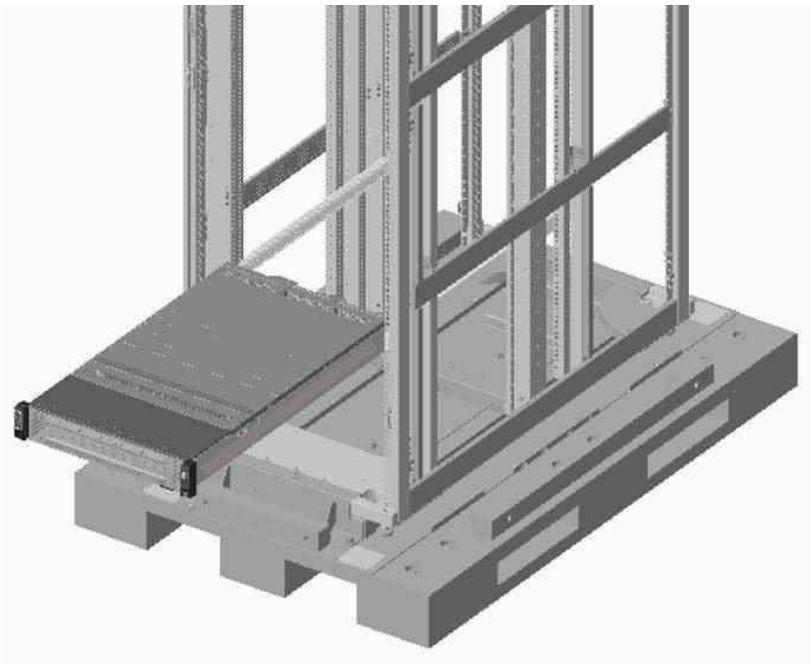


Figure 3-22 Installing the chassis into the cabinet

Step 4: Secure the two screws above the ears to the slide rail.

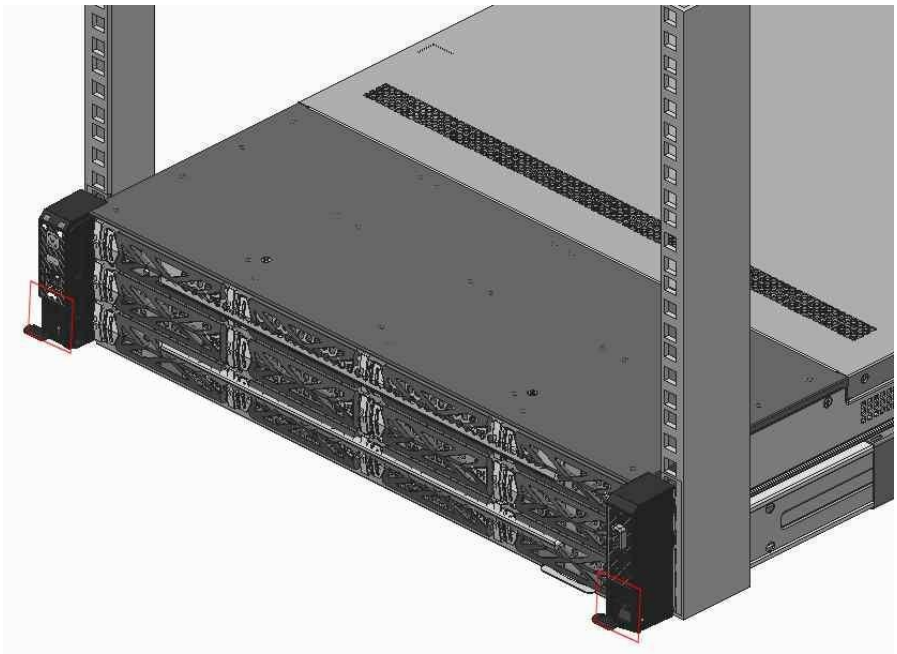


Figure 3-23 Securing the chassis

Chapter 4 Electrical operations

4.1 Power on the server

After placing the server according to the assembly instructions, connect at least one AC power cable to the server, and power on properly.

- Check the power LED indicator and the power LED indicator on the front control panel. The power LED light shows that the power is powered on and the system is in power standby.
- Start the Server
- Start the local server: Press the power button on the control board in front of the server to start the server;
- Start the BMC network interface: Log in to the BMC network interface and select Start from the power control action list box.

4.2 Powering off the Server

- Perform a normal shutdown: Before shutting down, store all open files and network services and close all applications.
- Stop or terminate all necessary system processes to shut down the operating system and compute nodes through a normal shutdown of the system.
- Press the power button on the front panel and the server will shut down immediately

Warning: An abnormal shutdown may result in file loss.

4.3 Power Requirements

When installing the equipment, you must comply with the local or regional electrical regulations for the installation of information technology equipment and must be performed by a certified electrical engineer. This equipment has been carefully designed to be installed in an environment that can refer to the following codes :NFPA 70, 1999 (National Electrical Code) and NFPA-75, 1992(Protection Code for Electronic Computers/Data Processing Equipment). Refer to the product rating label or the user documentation provided with this option for the required power rating of the option.

Note: Use an uninterruptible power supply (UPS) to protect your server from power fluctuations and temporary power outages. This device protects the hardware from the effects of surges and voltage spikes, and keeps the system up and running in the event of a power grid failure.

● Install multiple servers and use additional power distribution equipment if needed to safely power all devices. Follow these guidelines:

Balance the server power load between the AC power branch circuits;

Do not allow the total AC current load of the system to exceed 80% of the AC current rating of the branch circuit;

Please use a dedicated power patch board to connect the device; ➢ Power the server through a separate circuit.

4.4 Electrical grounding requirements

The server must be properly grounded in order for it to operate properly and ensure safety. This equipment must be installed in compliance with any regional or national electrical wiring regulations, such as International Electrotechnical Commission (I EC) Regulations 364 Parts 1 to 7. In addition, you must ensure that all power distribution equipment used in the installation process (such as branch connections and sockets) are listed or certified ground equipment, as multiple servers connected to the same power supply require a large amount of current to be channeled into the ground. It is therefore recommended that the PDUs used be either securely connected to the branch circuit of the building or fitted with a non-detachable wire to an industrial plug. NEMA lock plugs or those that comply with IEC 60309 standards are considered suitable plugs. It is recommended to use a dedicated power strip to connect to this server.

4.5 Prevent static electricity release

To avoid damage to the system, take necessary precautions when installing the system or removing and placing components. The static electricity emitted by fingers or other conductors may damage the motherboard or other electrostatic sensitive devices. Damage caused by static electricity can shorten the expected service life of the device.

To avoid static damage, pay attention to the following:

- Pack the product in anti-static packaging to avoid direct hand contact with the product during transportation and storage.
- Place the electrostatic sensitive parts in their respective anti-static packaging for safekeeping until they are transported to a work area that is protected from static electricity.

- Before installation, place the parts on a grounded surface for 2-3 seconds to release the static electricity from the packaging and the human body before removing them from their anti-static packaging.
- Take the parts out of the packaging, do not temporarily place them anywhere, and install them directly into the server. If you need to temporarily place it, put it back in the anti-static package. Do not place the part on the outer cover of the server or any metal surface.
- Do not touch pins, wires, solder point pins, or exposed circuits.
- Always take proper grounding measures when touching electrostatic sensitive components or devices.
- Use extreme caution when operating equipment in a dry environment. A dry environment is more likely to accumulate electrical charges and increase static electricity.

4.6 Grounding Method to prevent static electricity release

There are several methods of grounding. You can use one or more of the following grounding methods when taking and placing or installing electrostatic sensitive parts:

- You can use a wristband that connects to a grounded work area or computer case using a ground cable. The wristband must be able to flex and retract flexibly, and the grounding wire must have a resistance of at least 1 megohm
  (±10%). To achieve grounding, wear the wristband close to your skin;
- In vertical work areas, use heel straps, toe straps, or boot straps. Tie straps around your feet when standing on conductive floors or floor MATS that dissipate static;
- Use conductive on-site maintenance tools and wear antistatic gloves when handling electronic components;
- Use a foldable tool pad that dissipates static electricity and a portable field repair kit.

4.7 Space requirements and ventilation requirements

When placing racks, the maintenance and ventilation of the server should be fully considered. Improper rack layout may affect the maintenance and heat dissipation of the server, resulting in the normal use of the server. Specific requirements are as follows:

- Leave at least 635mm gap in front (direction of the server air inlet);
- Leave at least 762mm gap in the rear (server air inlet direction).
- At least 1220mm gap on the back of the two rows of racks;
- This server is designed for air intake from the front and air discharge from the back, so it is necessary to ensure that the front and rear channels of the rack are well ventilated, and the hot and cold channels are planned to ensure that the cold air is inhaled from the front of the server and the hot air is discharged from the back of the server.
- When the rack server is not fully placed, the panel should be used to block the vacant position to ensure that the hot air does not return from the server outlet to the intake vent.
- Ensure that the equipment room can provide sufficient cold air flow based on

the number and configuration of servers in the equipment room.

4.8 Temperature Requirements

To ensure the reliable and stable operation of the server, place the server in an environment with good ventilation and controlled temperature that meets its specifications.

It is recommended that the ambient temperature of the server not exceed 35 ° C (The ambient temperature in a single equipment room cannot be too high according to the model configuration. The lowest temperature of the server is supported). Do not run the server in an environment that exceeds the temperature specified by the server. Otherwise, system damage may occur.

Chapter 5 BIOS and BMC Functions

5.1 BIOS Overview

The Basic Input Output System (BIOS), also known as the basic input output system, is a solidified program code loaded on the ROM chip of the computer motherboard. It saves the most important basic input and output program of the computer, POST self-test program after boot and system self-start program, which can read and write the specific information of system Settings from the CMOS. Its main function is to provide the lowest level of the computer, the most direct hardware setting and control, to find the boot device, start the system or other boot environment. Note: 1. Usually the default Settings are the best property Settings recommended by the machine, and it is not recommended to make random changes without the guidance of professional personnel;

If the modification of BIOS Settings leads to some unexpected situations such as system abnormalities, you can restore the corresponding Settings according to the modification record. If the recovery option can not solve the problem or the modification option causes the problem of not starting up, you can try to recover by clearing CMOS operation;

The BIOS Settings and operations described in this manual are based on the official BIOS version pushed with the manual. With the iteration of the BIOS version, some operating interfaces may be different from the graphical representation.

5.2 Common BIOS Operations

This topic describes common operations and functions of the BIOS interface to help you configure functions of the BIOS. This topic describes how to log in to the BIOS Setup screen, switch between Legacy boot mode and UEFI, view system information, view CPU information, view memory information, view hard disk information, and view/set BMC network information.

5.2.1 Logging in to BIOS

Figure 5-1 BIOS startup screen

Power on and start the server. The system starts to boot. When the AMI Logo appears at the top of the screen and the following message is displayed at the bottom of the screen: Press <DEL> to enter SETUP.Press <F11> to enter Boot Menu.Press <F12> to enter PXE Boot. Press the [Del] key when the message "" Entering Setup..." appears in the lower right corner of the screen. ", you will enter BIOS Setup later, you can select the subitem through the arrow arrow keys and press Enter to enter the submenu.

Hot key introduction:

Press F7 to enter the BOOT option selection screen and select the system boot device.

Press F12 to select the PXE boot mode.

Table 5-1 Description of control keys

↑↓→←	Move
Enter	Enter
+ / —	Change
ESC	Exit

F1	General Tips
F2	Previous set value
F3	Optimize the presets
F4	Save & Exit
<K>	Scroll up the help area
<M>	Scroll down the help area

5.2.2 Switching between Legacy and UEFI mode

Log in to the BIOS Setup screen, navigate to the Boot screen, choose Boot->Boot mode select option to set the boot mode, configurable option (LEGACY/UEFI) (cannot be set by default, if you need to set, you need to right ctrl+f3 to open the hidden mode, Then set Advanced->CSM Configuration->CSM Support to enable as shown in the following picture:

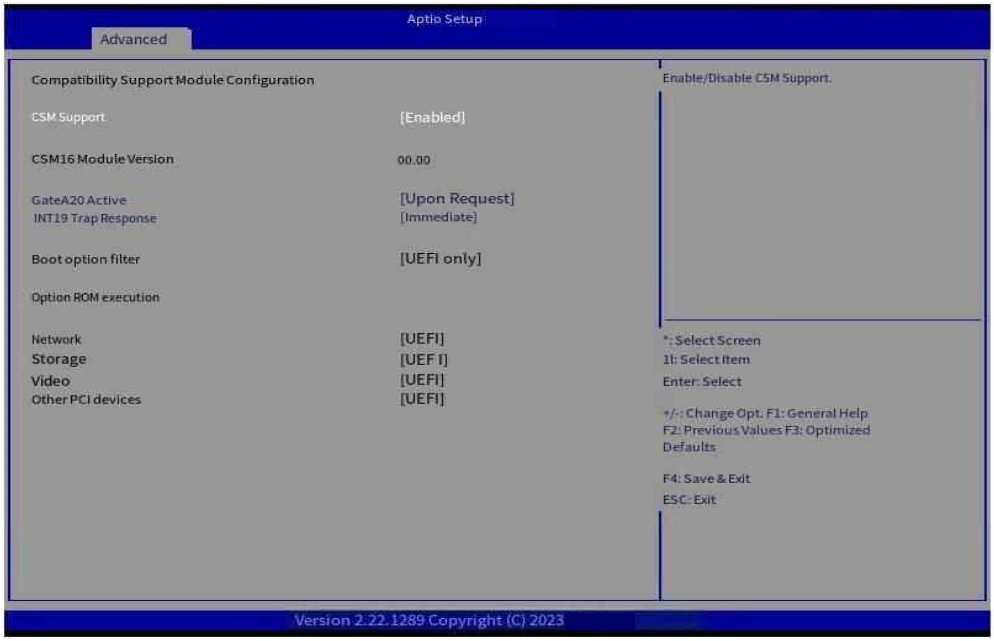


Figure 5-2 Setting boot mode

5.2.3 Viewing System Information

Log in to the BIOS Setup screen and navigate to the Main screen, which displays the summary of system information, including BIOS firmware, BMC firmware and ME version information, CPU, PCH, Microcode and memory information. As shown in the following picture:

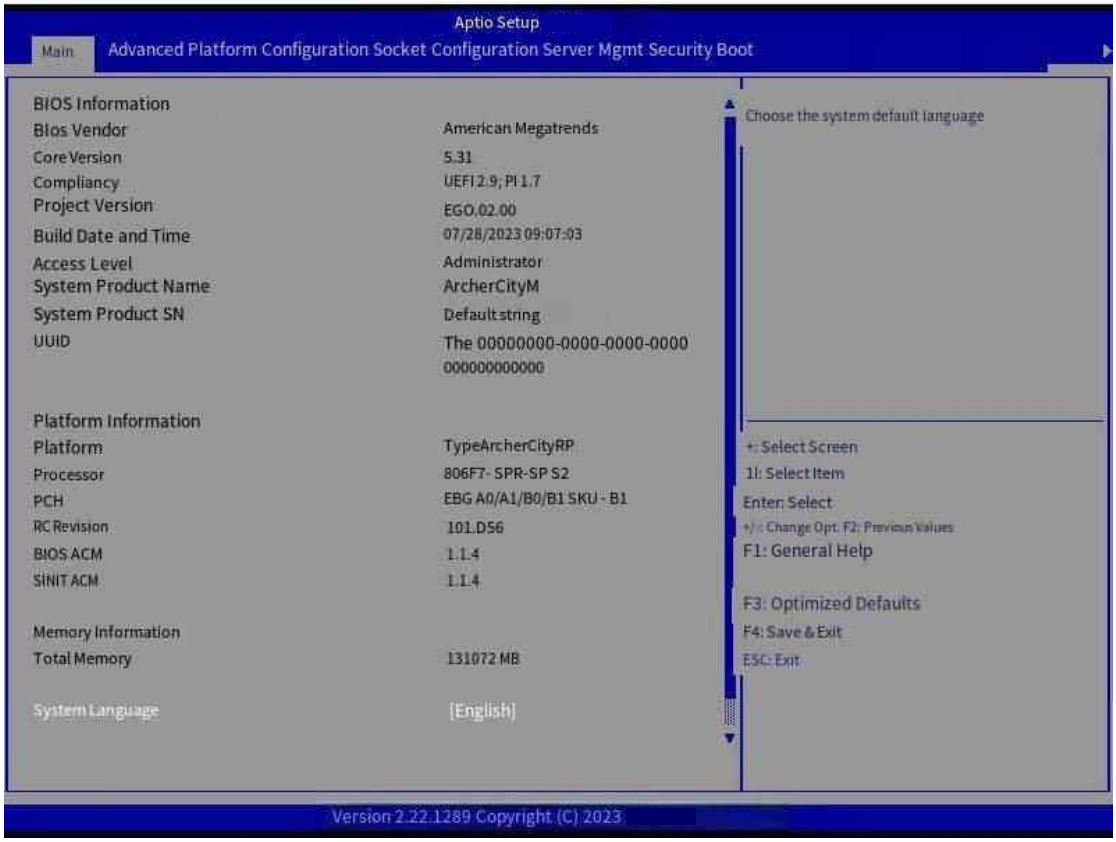


Figure 5-3 Firmware version information

5.2.4 Viewing CPU Details

Log in to the BIOS Setup screen, navigate to the Advanced screen, and enter Scoket Configuration -> Processor Configuration on this page to view the details and configurable options of the CPU, as shown in the following picture:

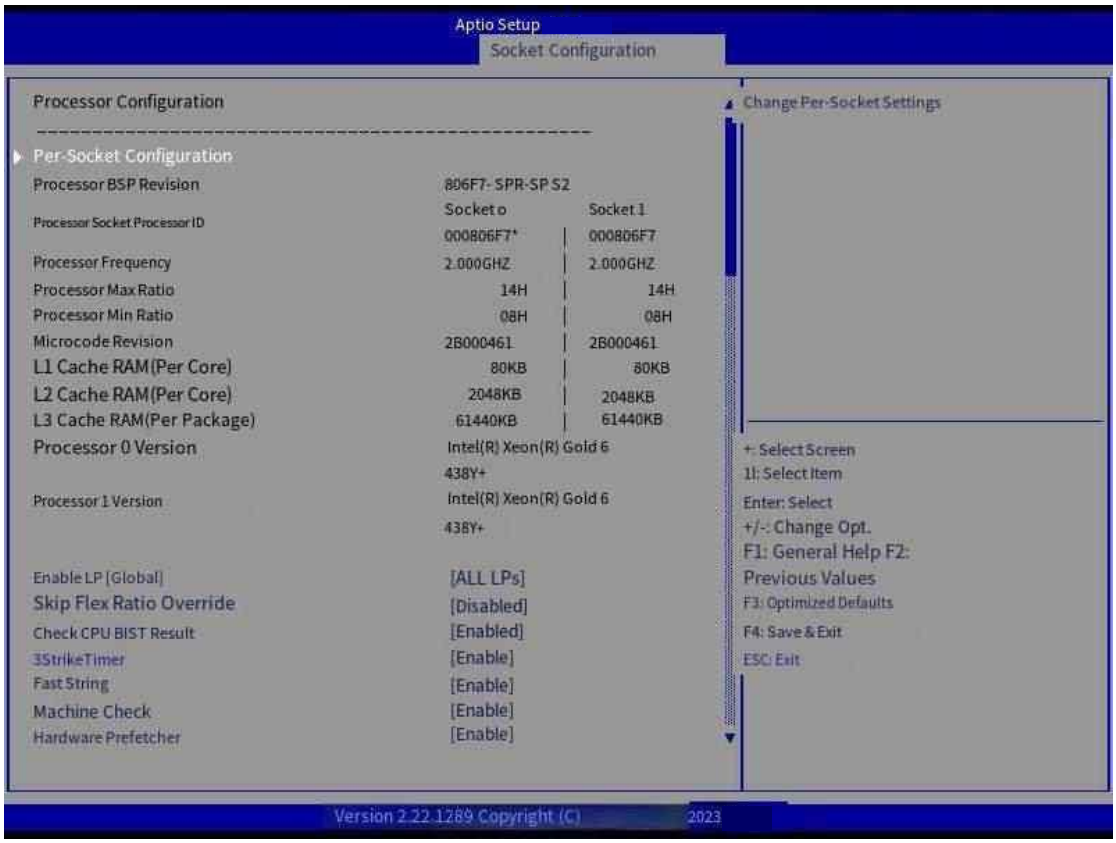


Figure 5-4 Processor information

5.2.5 Viewing Memory Information

Log in to the BIOS Setup screen, navigate to the Advanced screen, enter the page under Scoket Configuration -> Memory Configuration, you can view the memory details and configurable options, as shown in the following picture:

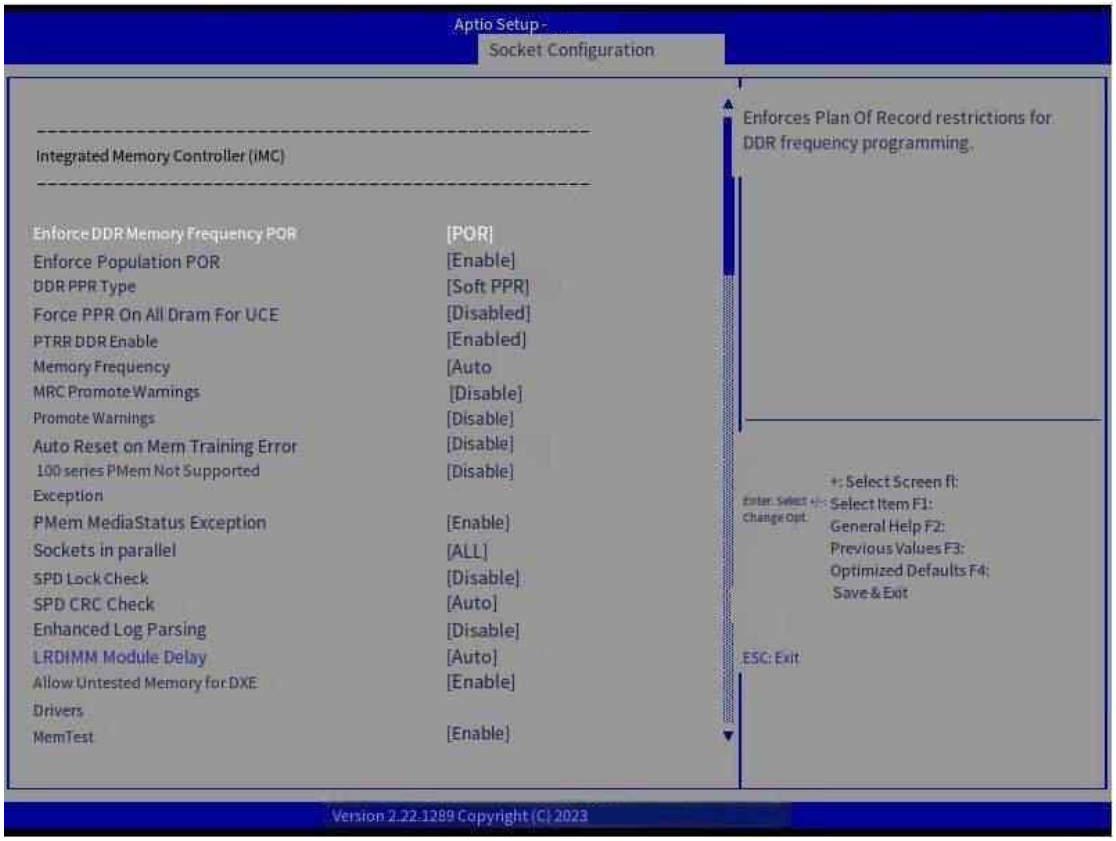


Figure 5-5 Memory information

5.2.6 Viewing Hard Drive Information

Log in to the BIOS Setup screen, navigate to the Advanced screen, Go to Platfrom Configuration -> PCH Configuration -> PCH SATA Configuration or Platfrom Configuration -> PCH Configuration -> PCH sSATA Configuration, you can view the hard disk information of the current SATA interface or sSATA interface, as shown in the following picture:

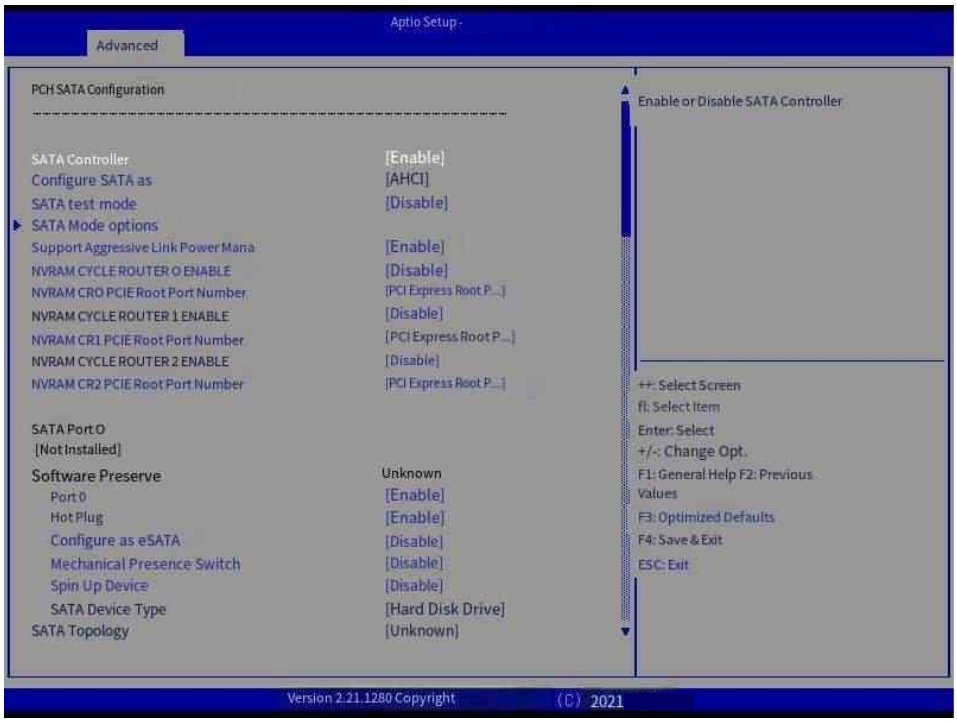


Figure 5-6 SATA hard drive information

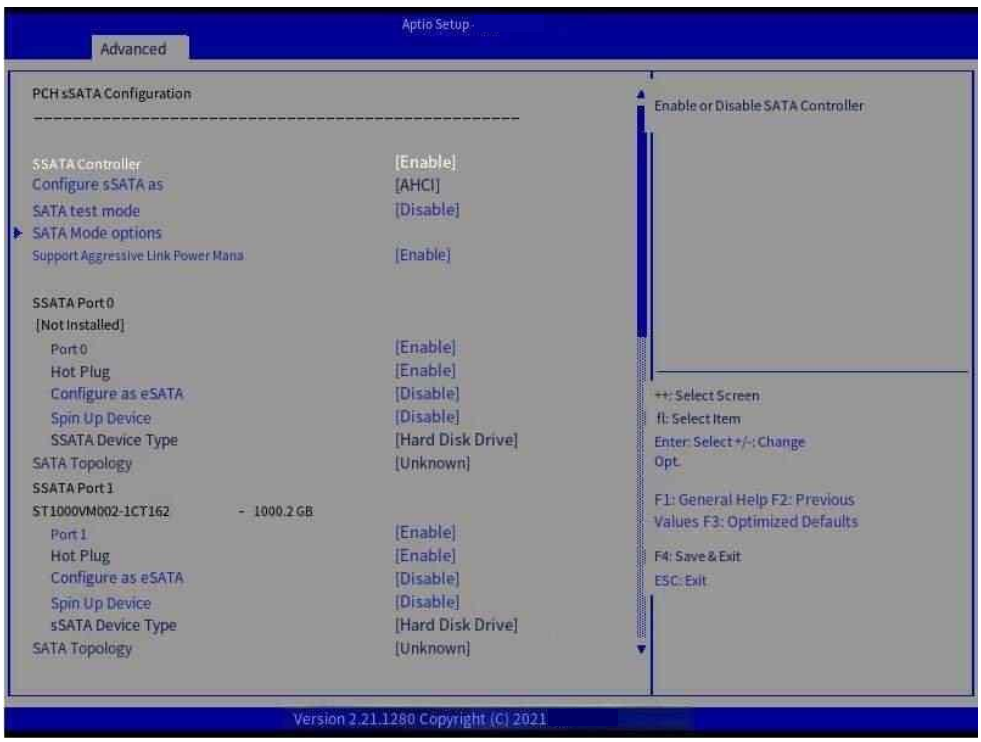


Figure 5-7 Disk information of the sSATA interface

5.2.7 Viewing/Setting BMC Network Information

Log in to the BIOS Setup screen, navigate to the Server Mgmt screen, and enter BMC network configuration to view the current BMC IPv4/IPv6 network parameters and configurable options, as shown in the following figure:

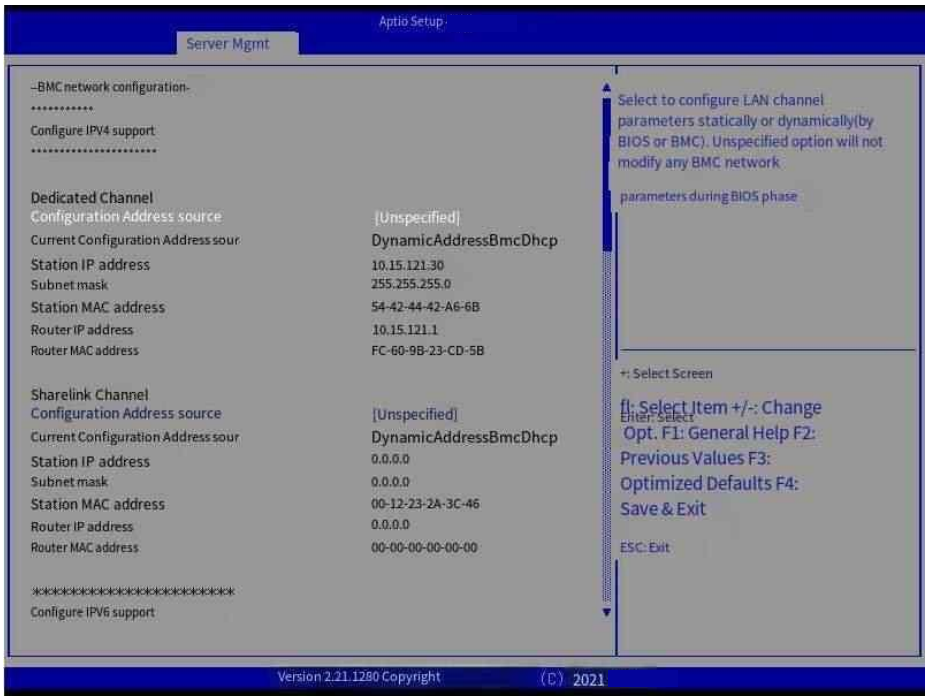


Figure 5-8 BMC IPv4 network Settings

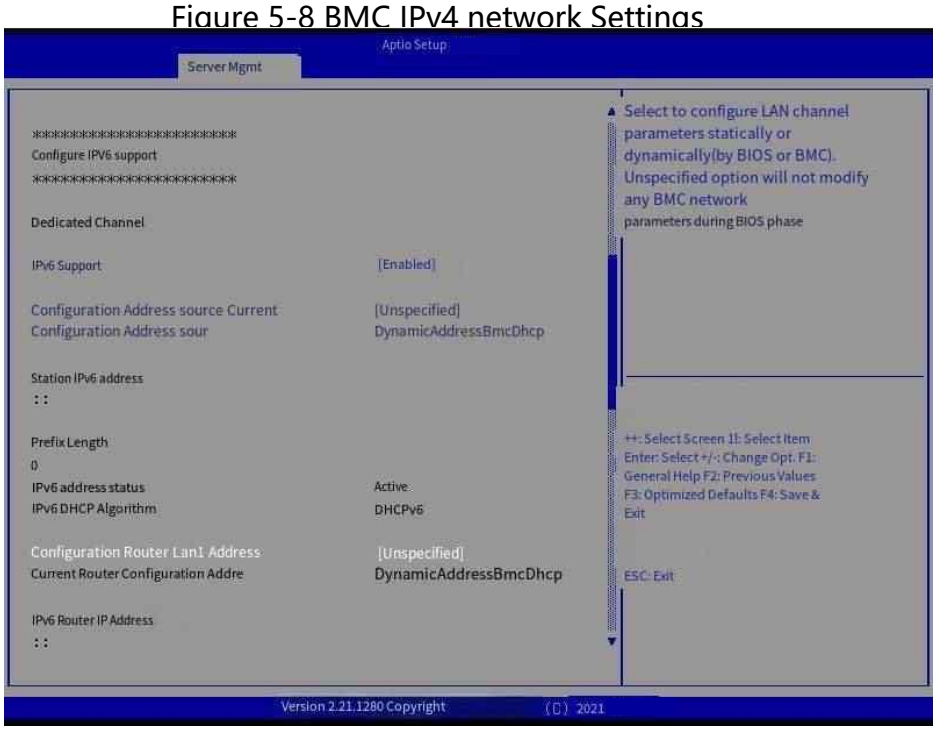


Figure 5-9 BMC IPv6 network Settings

5.3 BIOS Parameter Settings

The default Settings of the system are recommended parameters. You are not advised to modify them without the guidance of professional personnel. Because the modification of some options may cause the system to malfunction or fail to start up. In order to avoid this situation as much as possible, this chapter briefly describes the overall option configuration.

5.3.1 Main Menu

The Main menu is the first interface that appears after logging in to the BIOS Setup interface, which is used to display the basic information of the system, as well as provide the BIOS Setup language Settings and time Settings. When an option is selected on the left side of the screen, the item is highlighted, the description of the option is displayed in the upper right window, and the description of buttons is displayed in the lower right window.

Figure 5-10 Main screen information

Figure 5-11 Main screen

Table 5-2 Parameters on the Main screen

Parameters on the screen	**Function description**
Core Version	BIOS core version
Project Version	Motherboard version number
System Product Name	System Product Name
System Product SN	System product SN
Platform	Motherboard platform
processor	Processor number
RC Revision	RC Revision number
PCH	PCH Information
Total Memory	Total memory capacity
Memory Frequency	Memory frequency
Access Level	User level
System Language	System Default Language
System Date	System Date

System Time	System time

5.3.2 Advanced Menu

The Advanced menu allows the user to modify the Settings of the system CPU and other devices. The following is a description of the common parameters.

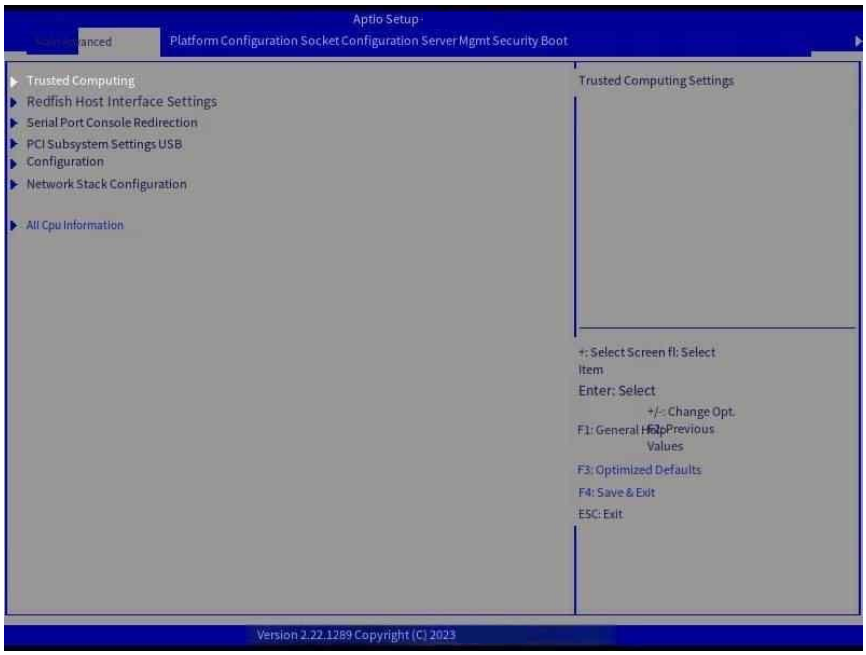


Figure 5-12 Advanced screen

Table 5-3 Parameters on the Advanced screen

Parameters on the screen	**Function description**
Trusted Computing	Trusted Computing
Redfish Host Interface Settings	Redfish Host Interface Settings
Serial Port Console Redirection	Serial Port Console redirection
PCI Subsystem Settings	PCI Subsystem Settings
USB Configuration	USB Configuration
Network Stack Configuration	Network Stack Configuration
All Cpu Information	CPU details

5.3.3 Platform Configuration screen

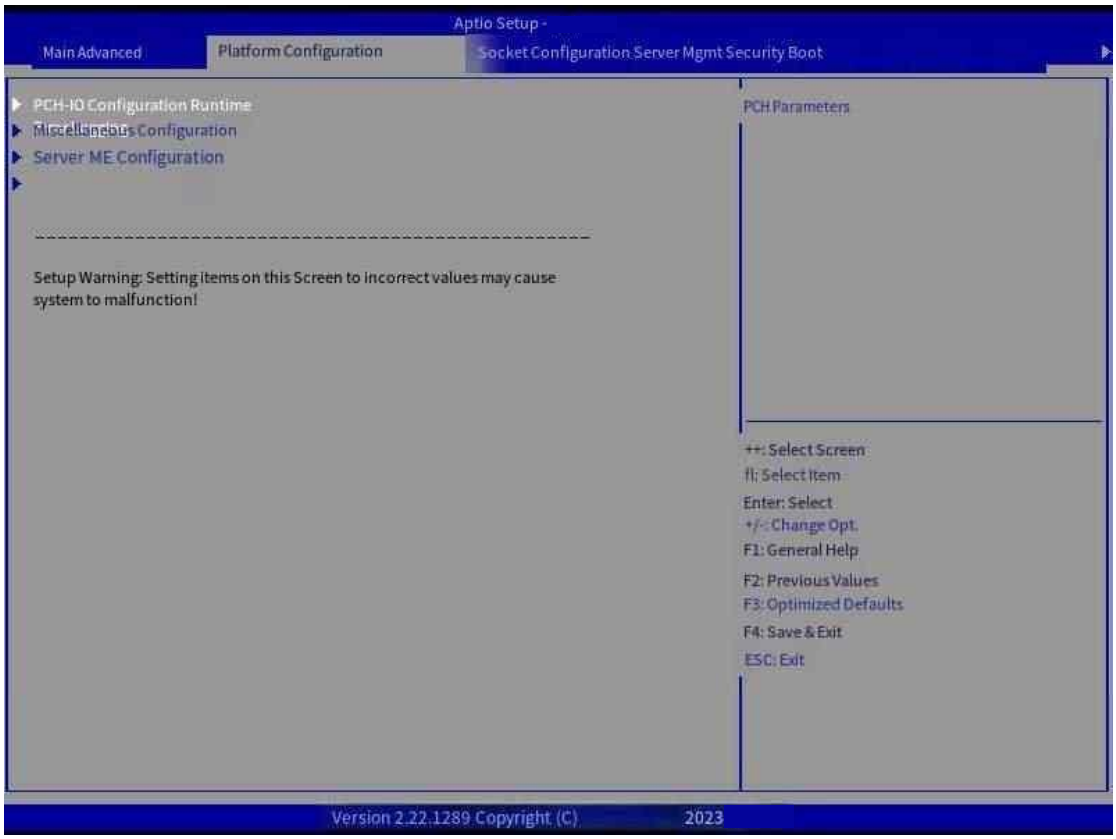


Figure 5-13 Platform Configuration screen

Table 5-4 Parameters on the Platform Configuration screen

Parameters on the screen	**Function description**
PCH Configuration	PCH Configuration
Miscellaneous Configuration	Miscellaneous Configuration
Server ME Configuration	ME Information
Runtime Error Logging	Runtime error logging

5.3.4 Socket Configuration menu

On the CPU configuration screen, you can view information about the CPU and memory, and set the working status of the CPU, including P-State and C-State.

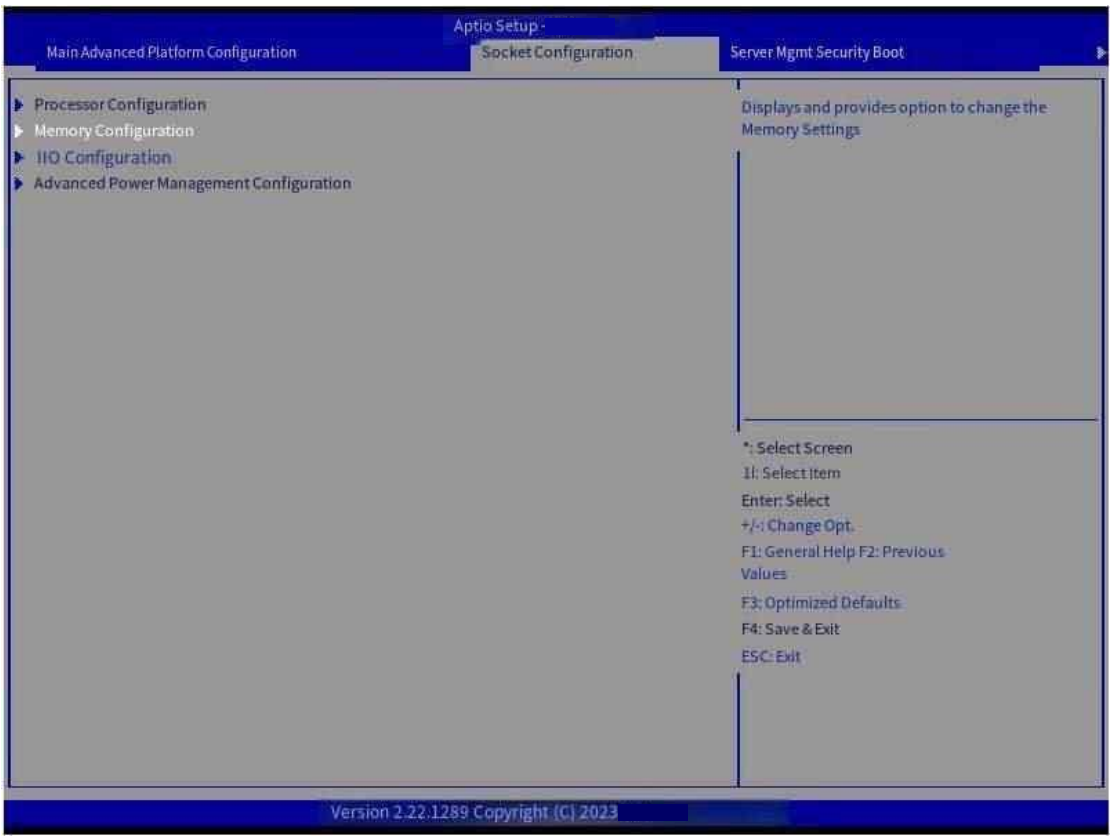


Figure 5-14 Socket Configuration screen

Table 5-5 Parameters on the Socket Configuration screen

Parameters on the screen	**Function description**
Processor Configuration	Processor Configuration
Memory Configuration	Memory Configuration
IIO Configuration	IIO Configuration
Advanced Power Management Configuration	Advanced Power Management Configuration

5.3.5 Server Mgmt Menu

The Server Mgmt screen allows you to set functional options related to BMC.

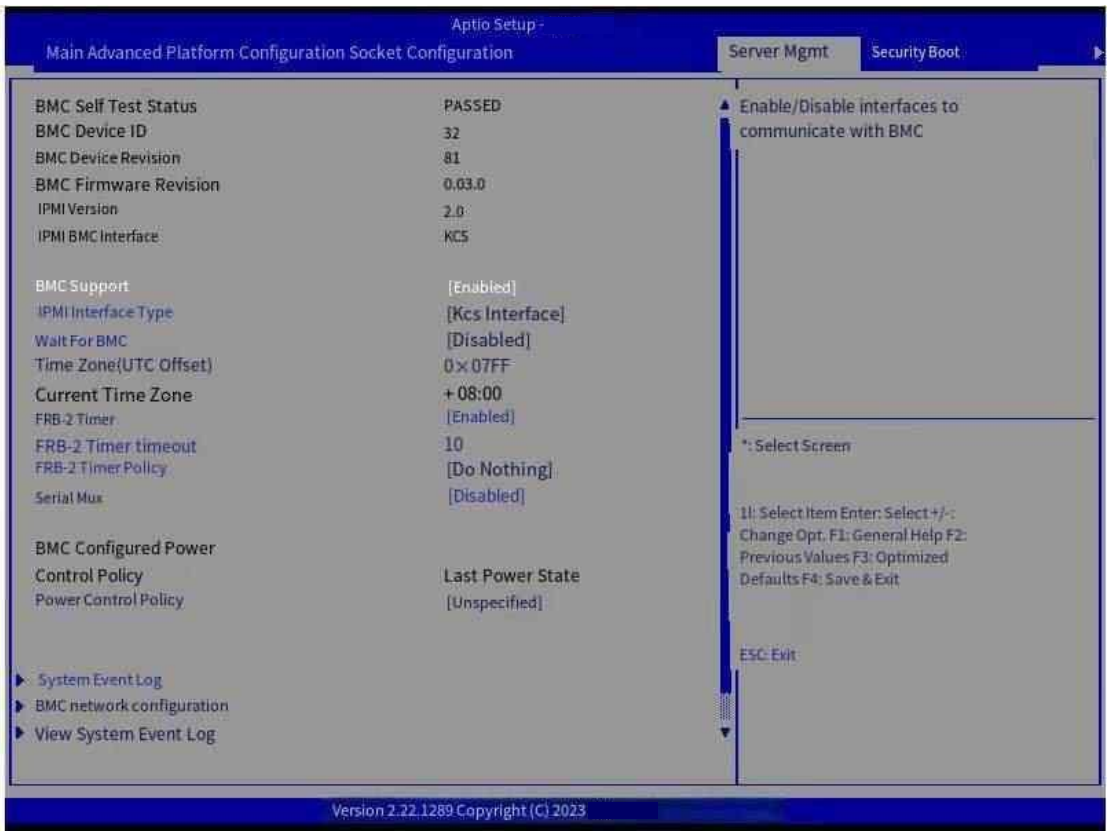


Figure 5-15 Server Mgmt screen

Table 5-6 Parameters on the Server Mgmt screen

Parameters on the screen	**Function description**
BMC Self Test Status	BMC self-check status
BMC Device ID	BMC Device ID
BMC Device Revision	BMC device Revision
BMC Firmware Revision	BMC Firmware Revision
IPMI Version	IPMI version
IPMI BMC Interface	IPMI BMC Interface
BMC Support	BMC Function Support
Wait For BMC	Wait for BMC time
Power Restore Policy	Power recovery strategy
FRB-2 Timer	FRB-2 Timer
FRB-2 Timer Timeout	FRB-2 timer timeout
FRB-2 Timer Policy	Load BMC presets

View FRU information	View FRU information
BMC network configuration	BMC Network Configuration
System Event Log	System Event log Settings
View System Event Log	View the system event log
BMC User Settings	BMC User Settings
BMC Reset	BMC reset

5.3.6 Security Menu

The Security page allows for security-related actions. For example, you can set passwords of BIOS users with different permission levels.

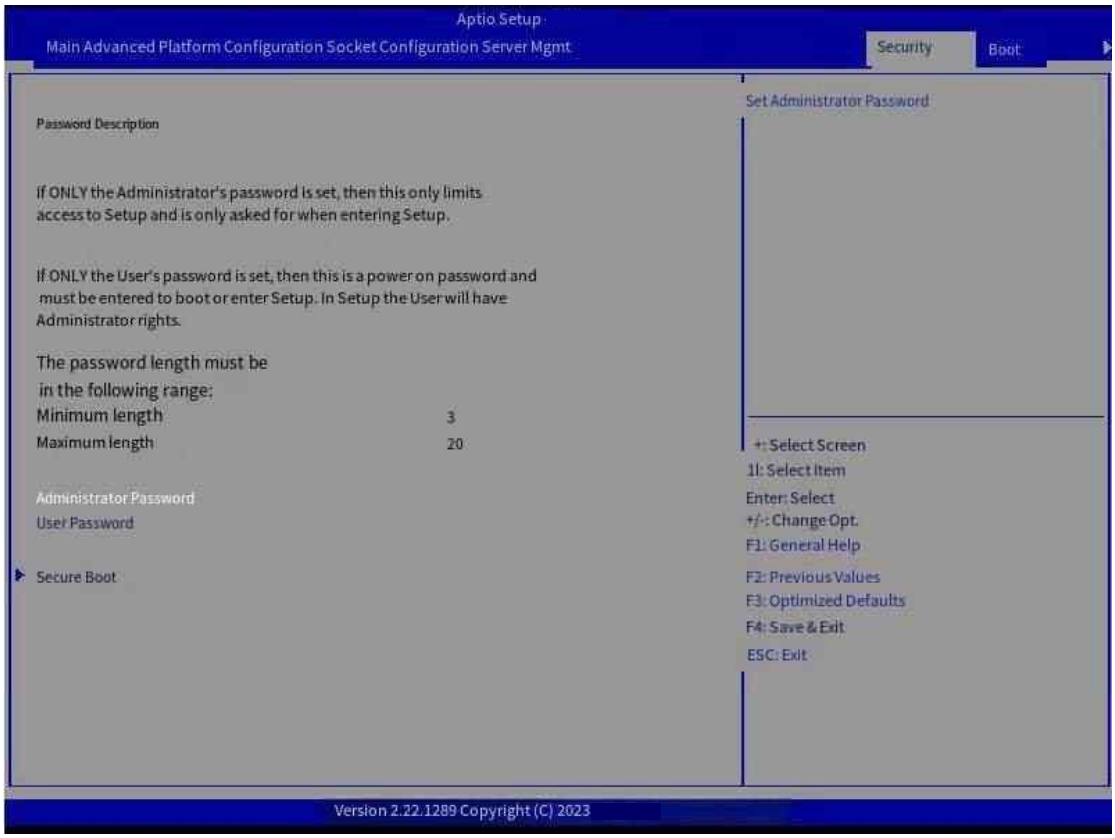


Figure 5-16 Security screen

Table 5-7 Parameters on the Security screen

Parameters Screen	**Function description**
Administrator Password	Administrator password
User Password	User password

Secure Boot	Secure Boot Settings

5.3.7 Boot Menu

On the Boot page, you can select and set the boot device.

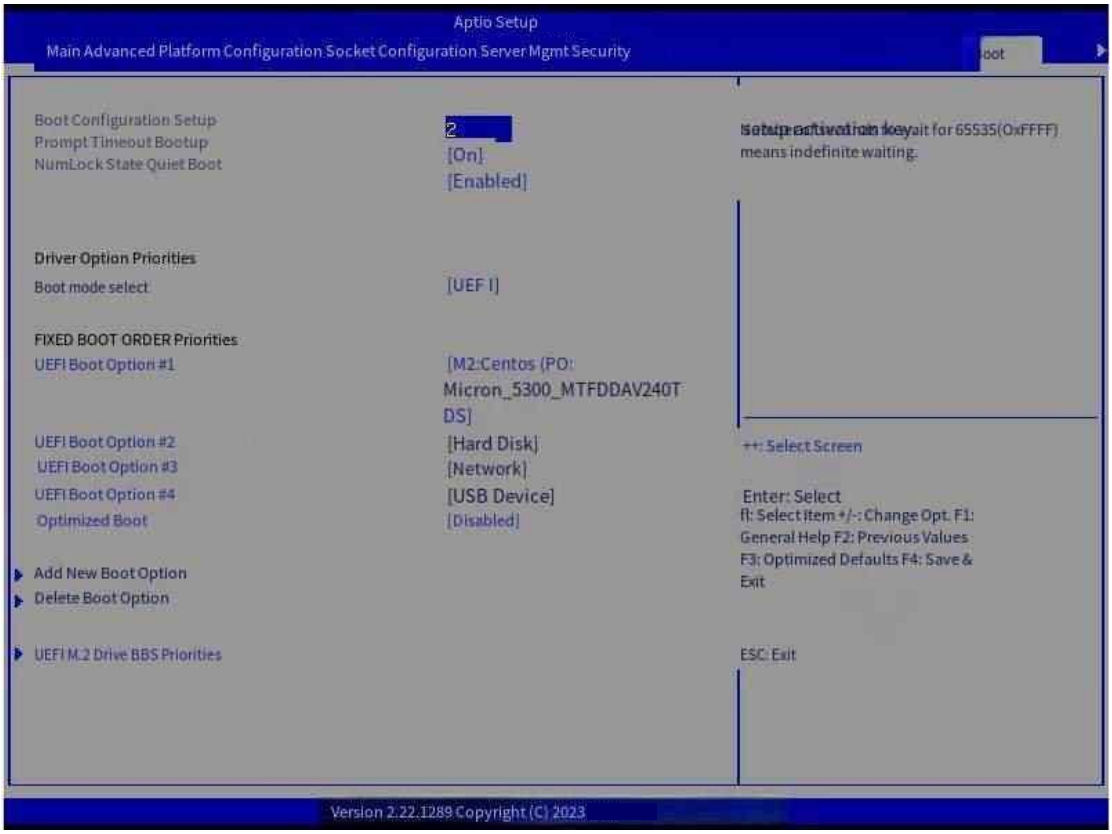


Figure 5-17 Boot screen

Table 5-8 Parameters on the Boot screen

Parameters Screen	**Function description**
Boot Configuration	Boot Configuration
Setup Prompt Timeout	Prompt timeout
Bootup Numlock State	Bootup Numlock State
Quiet Boot	Quiet Boot
Boot mode select	Boot Mode Select
FIXED BOOT ORDER Priorities	Fixed boot order priority
Add New Boot Option	Add new boot option
Delete Boot Option	Delete Boot option
UEFI M.2 Drive BBS Priorities	UEFI hard drive BBS priorities

5.3.8 Save & Exit menu

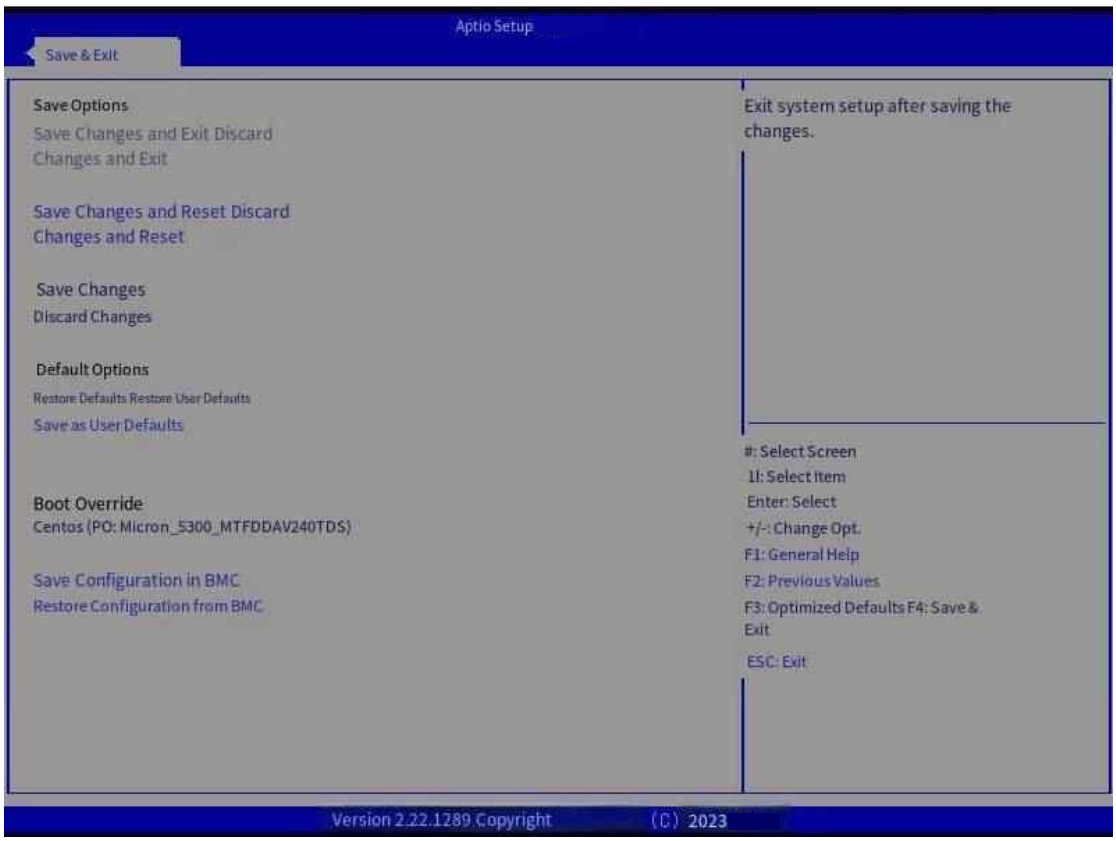


Figure 5-18 Save & Exit screen Table 5-9 Parameters on the Save & Exit screen

Parameter Description Screen	**Function description**
Save Options	Save configuration
Save & Exit	Save & exit
Discard changes & exit	Discard changes & exit
Save Changes and Reset	Save changes and reset
Discard Changes and Reset	Abandon changes and resets
Save Changes	Save changes
Discard Changes	Discard changes
Default Options	Default options
Restore Default Values	Restore default values
Save the User Default Values	Save the user default values

Restore the User Default Values	Restore the user default values
Boot Device Priority	Boot device priority

5.4 BIOS Firmware brushing

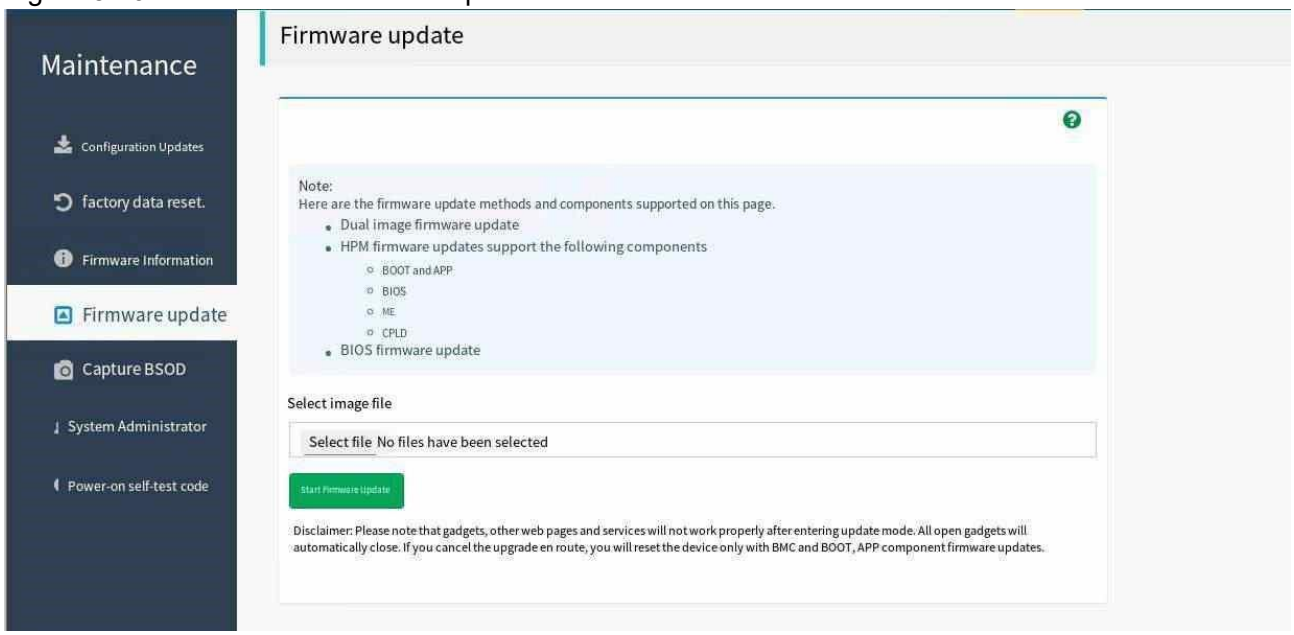
This product provides four BIOS upgrade modes: BMC WEB upgrade, UEFI Shell upgrade, operating system upgrade, and Redfish upgrade.

5.4.1 BMC WEB Refresh

Step 1: Log in to BMC remotely, default user name admin, password admin; Step 2: Click Maintenance -> Firmware Update option to enter the firmware update page, which is mainly used to update the firmware related to BMC

The BIOS firmware file is:.bin file

Figure 5-19 Maintenance-Firmware update



Step 3: BIOS firmware update

BIOS retain configurations: By default, all configurations are not retained

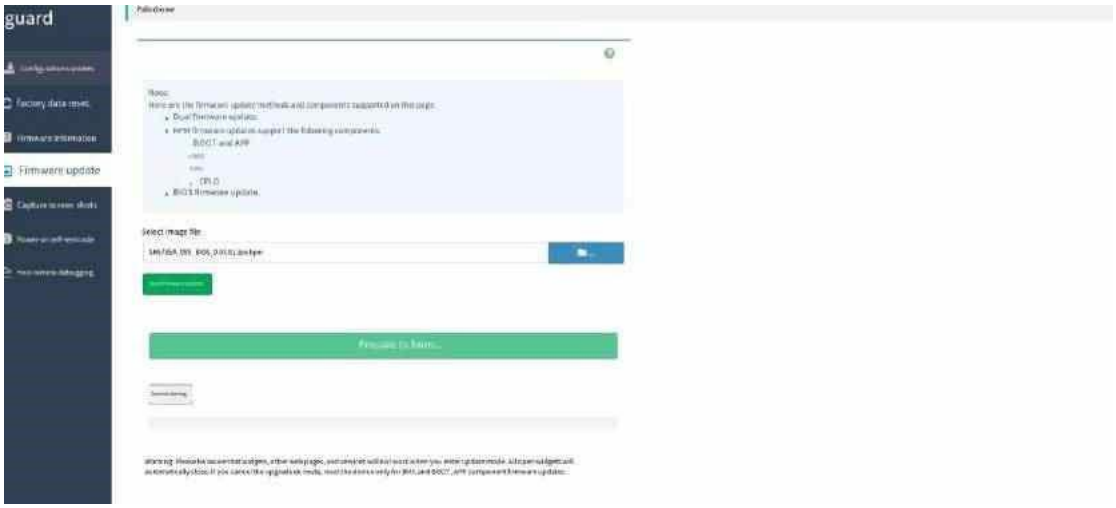


Figure 5-20 BMC does not save configuration updates

Step 4: After the file is uploaded, the updated version and the existing version are displayed. Select Update or Update All to continue updating the firmware.

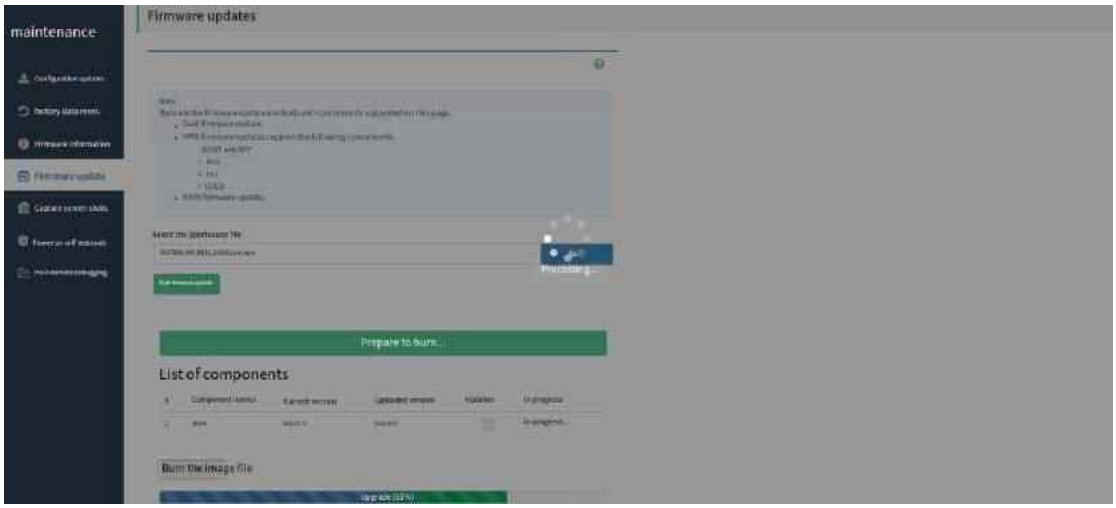


Figure 5-21 BIOS firmware update

Step 5: After the BIOS FW is updated, shut down the server and turn off the AC. After the server is powered on again, the new FW takes effect.

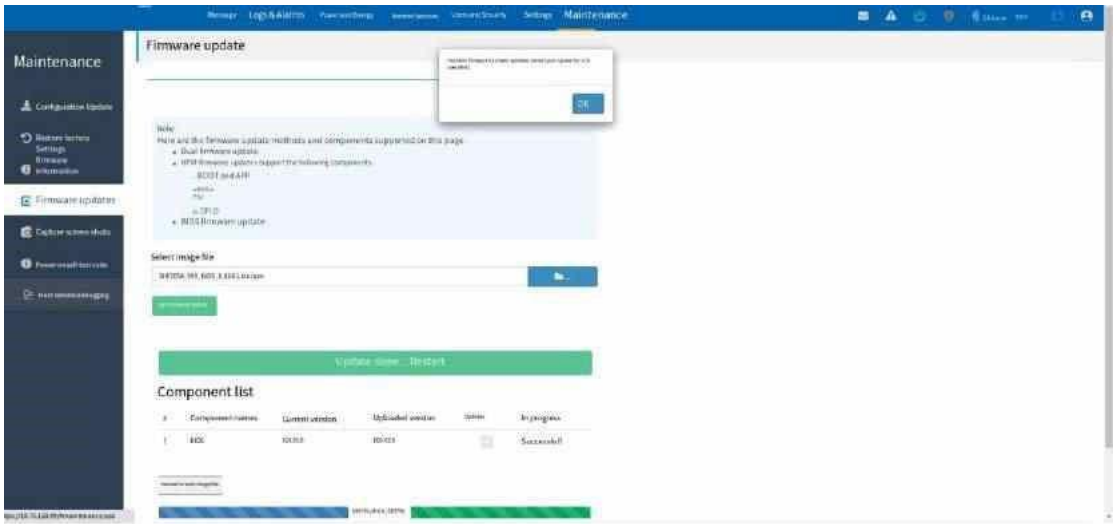


Figure 5-22 BMC configuration update completed

5.4.2 UEFI Shell Refresh

Step 1: Copy the BIOS FW update folder to the USB flash drive and plug the USB flash drive into the server;

Step 2: boot into UEFI Shell, enter "FS1:" to enter the USB flash drive directory (FS1 is the drive letter of the USB flash drive), and then enter the directory where the refresh script is located;

Note: FS1 is to demonstrate the location of the USB flash drive. In specific use, you need to find the location of the USB flash drive according to the file system directory in the Shell.

Figure 5-23 Shell BIOS firmware update

Step 3: Go to the Shell folder and execute Flash.nsh or FlashAll.nsh in the Shell folder to update the BIOS FW. Where, Flash.nsh indicates that the FW is updated on the premise of saving the current configuration; FlashAll.nsh indicates that the FW is updated without saving the current configuration. The execution result of FlashAll.nsh is used as an example.

Figure 5-24 Shell BIOS firmware update

Step 4 Wait until the BIOS FW refresh script is complete. Power off the server as prompted. After powering on the server again, the new FW takes effect.

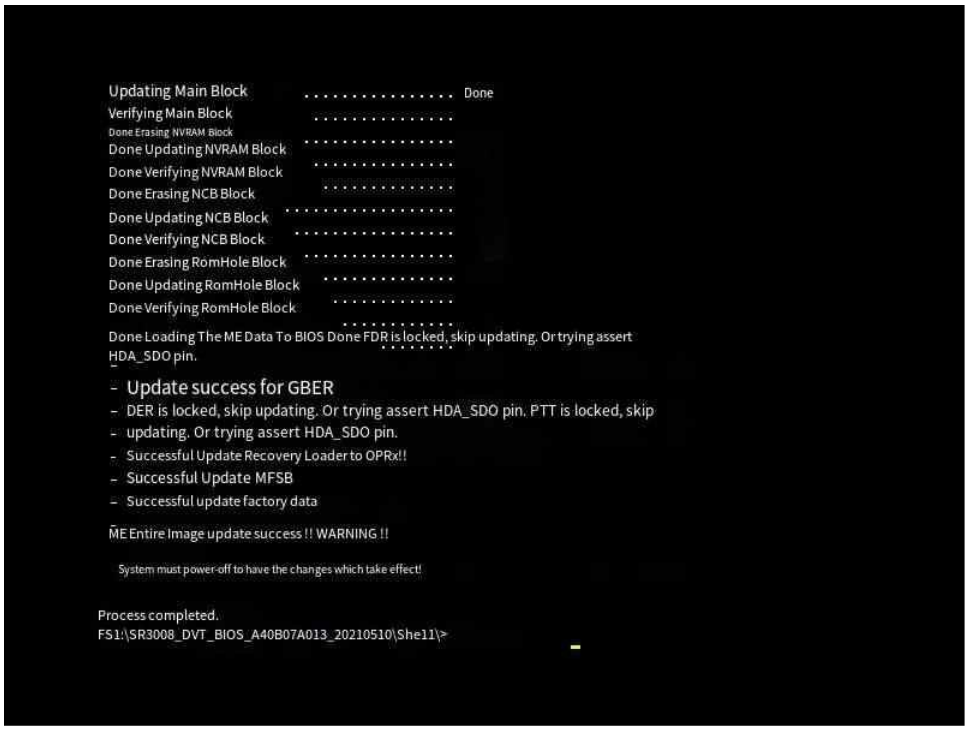


Figure 5-25 Shell BIOS firmware update

5.4.3 Operating System Refresh

● Linux System

Step 1: Copy the BIOS FW update folder from the USB flash drive to the server and add execute permissions.

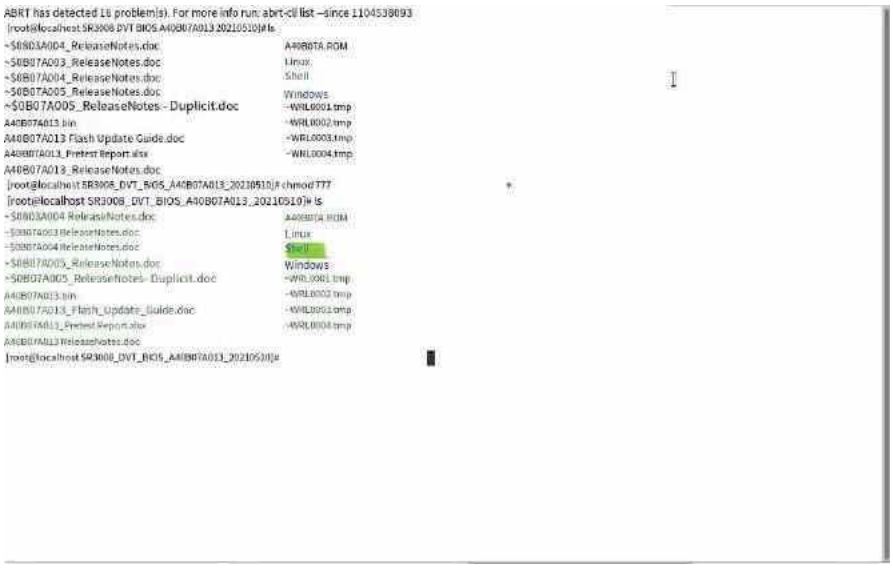


Figure 5-26 Linux BIOS firmware update

Step 2: Go to the Linux folder and select either 32-bit or 64-bit (using 64-bit as an example) depending on the system the server is installed on.

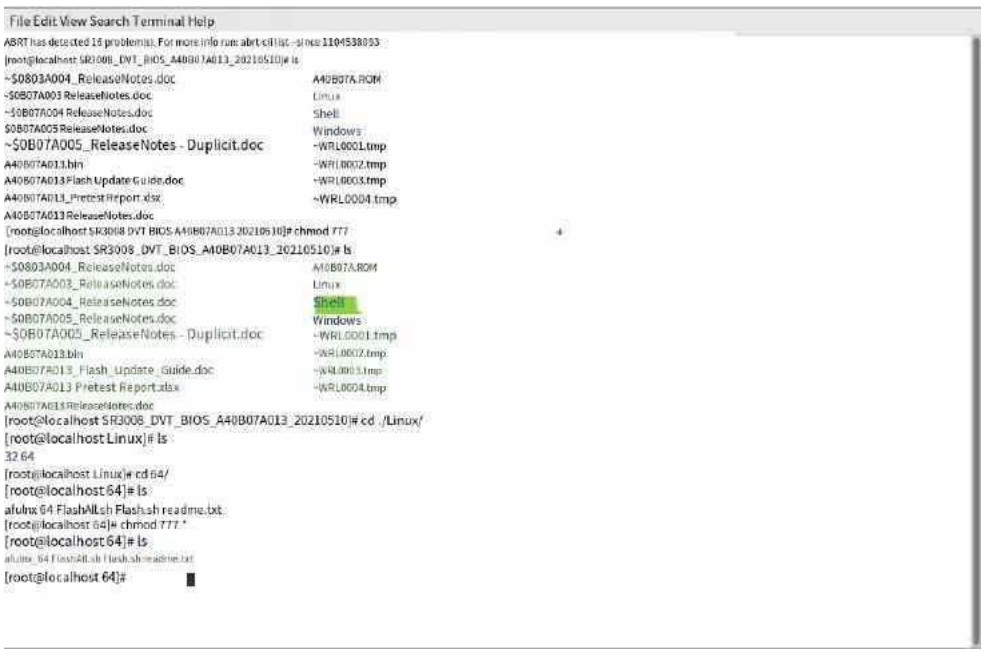


Figure 5-27 Linux BIOS firmware update

Step 3: Run Flash.nsh or FlashAll.nsh in the Linux folder to update the BIOS FW. Where, Flash.nsh indicates that the FW is updated on the premise that the current configuration is saved; FlashAll.nsh indicates that the FW is updated without saving the current configuration. The execution result of FlashAll.nsh is used as an example.

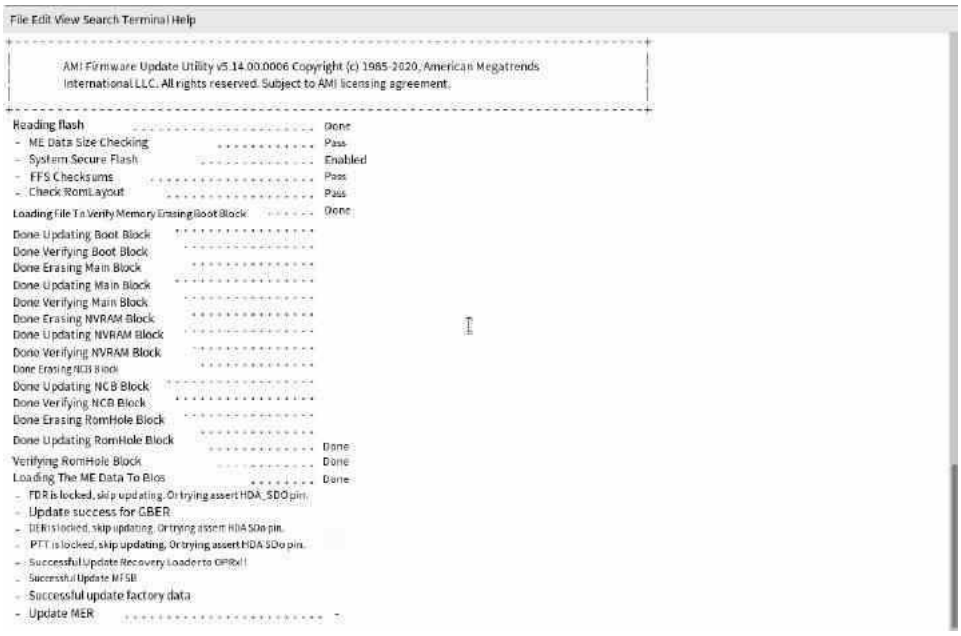


Figure 5-28 Linux BIOS firmware update

Step 4 Wait until the BIOS FW refresh script is complete. Power off the server as prompted. Power on the server again to make the new FW take effect.

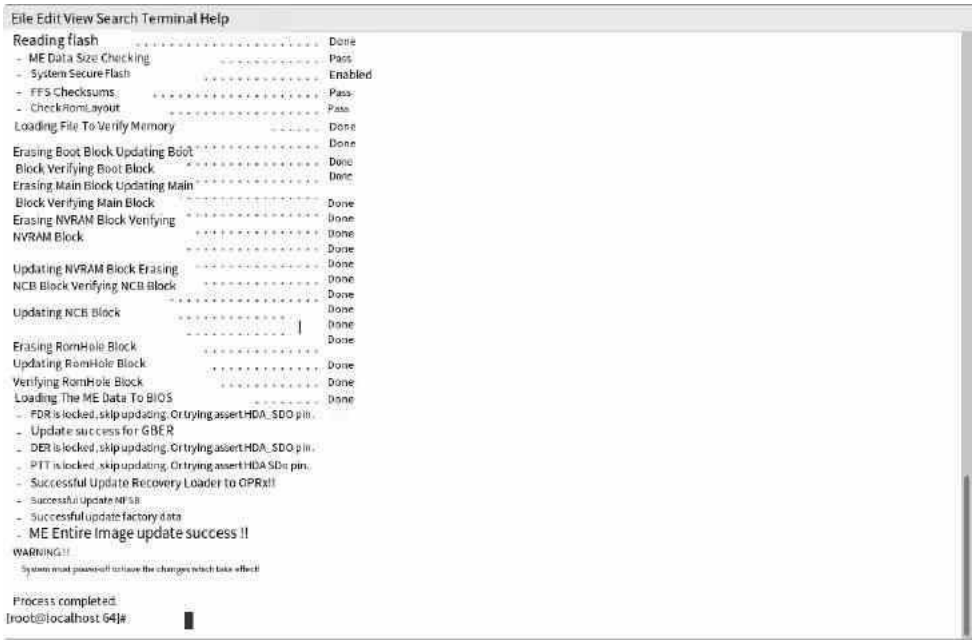


Figure 5-29 Linux BIOS firmware update

5.4.4 Redfish Write

Redfish requires the POSTMAN tool to upgrade the BIOS.

Step 1: Create a session and get the token value

Operation type: POST

URL: https://device_ip/redfish/v1/SessionService/Sessions

Fill in the request header under Headers

X-Auth-Token: auth_value

Content-Type: application/json

Select Body->raw, fill in the body of the request message, and enter the username and password that already exists:

Request body:

{

"UserName":"Administrator",

"Password":"Admin@9000"

}

Click Send to view the response code and response information with expected result A.

A, URL POST response code 201 Created; Can obtain X-Auth-Token information; The response information contains the user name, id, permission, login time, local ip address of the user, id of the created session, name, and description Operation example:

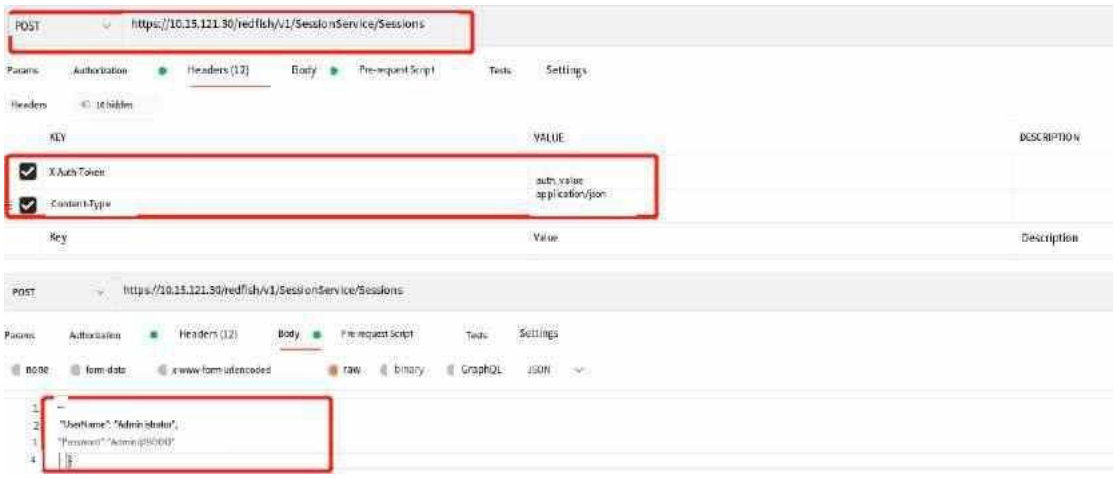


Figure 5-30 Redfish Upgrading BIOS firmware

Figure 5-31 Redfish upgrading BIOS firmware

View the created session token value (default timeout is 300s)

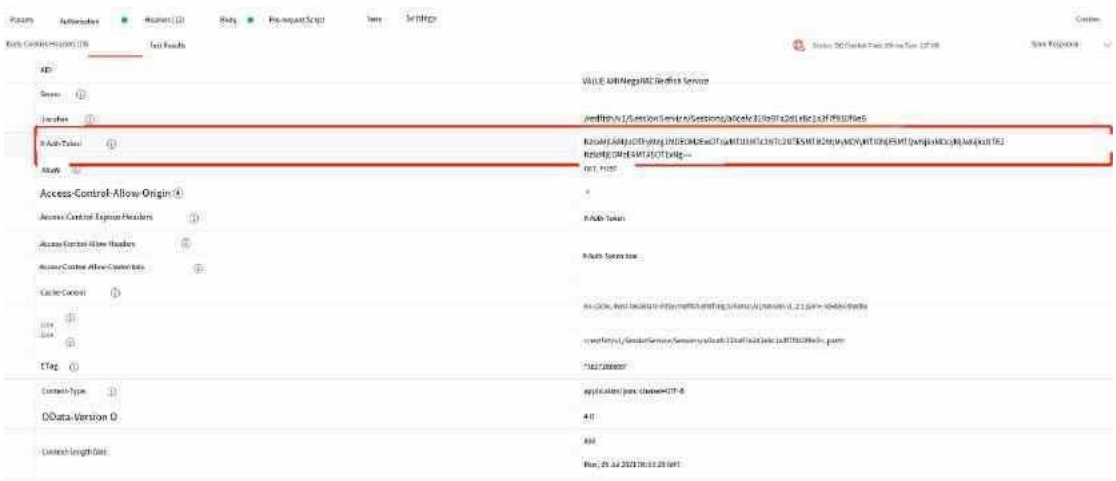


Figure 5-32 Redfish upgrade BIOS firmware

Step 2: Issue the command to upgrade the BIOS and view the upgrade task id in the response body

Operation type: POST

Input the correct request URL: https://device_ip/redfish/v1/UpdateService/upload;

Headers type the request header that is obtained under headers

X-Auth-Token: auth_value

Refer to the redfish interface documentation, click body->form-data,

Fill in the following information

Fill in the KEY field with UpdateParameters; In the corresponding VALUE field, click Text, select File, then click "Select File ", navigate to the refresh path, select parameters.json (the file name in the version package).

Enter OemParameters in the KEY field; In the corresponding VALUE field, click Text, select File, then click "Select File ", navigate to the refresh path, select oem_parameters.json (the file name in the version package)

In the KEY field, enter UpdateFile; In the corresponding VALUE field, click Text, select File, and then click "Select File" to navigate to the refresh path and select A40B07A00x.hpm (refresh file name in the version package).

Click Send to view the response code and task id in the response information. The expected result is A.

● URL POST Response code 202 Accepted, the response information is the information of the created task Parameter Description:

Parameters	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	Through https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - x - auth - token value

Operation Example:

Figure 5-33 Redfish Upgrading BIOS firmware

Figure 5-34 Redfish upgrading BIOS firmware

Figure 5-35 Redfish upgrade BIOS firmware

Step 3: Check the upgrade task status and wait for the task to complete

Operation type: GET

URL: https://device_ip/redfish/v1/TaskService/Tasks/id Request header:

X-Auth-Token: auth_value Request message body: None Parameter Description:

Parameters	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	pass https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - x - auth - token value
id	id of the task you created	Obtained from the body of the response returned by the POST upgrade operation

Example operation:

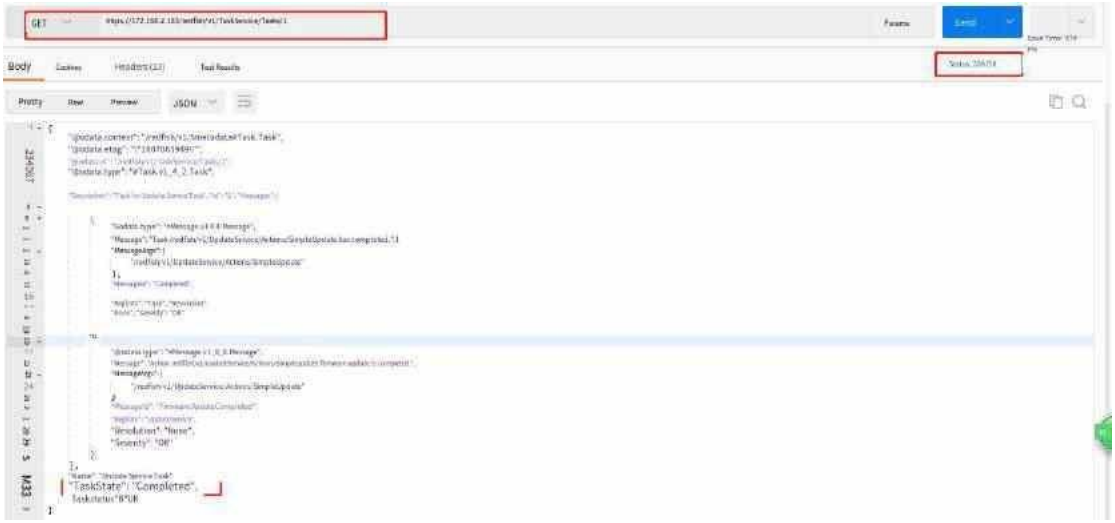


Figure 5-36 Redfish Upgrading BIOS firmware

Information description is displayed:

Return Information	Meaning	Return value
Response code	The response status of the request	200 OK
TaskState	Current state of the task	Specifies the state of the task resource. New Starting Running Suspended Interrupted Pending Stopping Completed Killed Exception Service

Step 4: The AC is powered off when the task status is "TaskState": "Completed".

Step 5: After the machine is powered on, check whether the BIOS version is upgraded to a higher version.

5.5 Introduction to BMC

The Baseboard Management Controller (BMC) remotely manages servers.

The BMC monitors the parameters of the CPU, memory, fan module, and power module, such as the temperature, voltage, current, and speed of the fan module, and adjusts the parameters accordingly to ensure a healthy system. In addition, the BMC records hardware information and logs, informing you of possible system operating risks and helping you locate future problems.

The BMC is an independent system. It does not depend on other hardware (such as the CPU and memory), nor on software (such as the BIOS and OS). It can upgrade the firmware of the machine, view the machine equipment, and other operations when the machine is not turned on. At the same time, the BMC can interact with the BIOS and OS, so that you can better manage the server.

BMC Default contents:

Categories	**Default**
BMC management network port parameters	Default DHCP
BMC login username and password	Default username: admin Default password: admin
BMC Time Zone	East 8
BMC MAC address	The MAC address is stored in the EEPROM
Date/time and NTP service	Sync with the NTP server
Service port	KVM service port: 443 IPMI Service port: 623 Https service port: 443
Serial port parameters	115200, 8, N, 1, None

BMC COM port	ttys5
Verify each message	Enable
User level authentication	Enable
Access mode	Always available
Privilege Level Limit	Privilege level Limit
Power recovery strategy	Always on
IPMB subaddress	0x20
KCS base address	0xCA2(SMS)
Power Management	Remote power restart in the standby state, support power on, power off, and reset operations, independent of system power on
BMC system event logs	Record memory ECC logs Record ambient temperature alerts Record system startup/shutdown logs Record the CPU temperature exception log Record CPU abnormal alerts Record power supply voltage alerts
Remote KVM	Enable

Firmware updates	Support for Web UI updates Supports local update under Linux Support for SSH updates Support for Redfish updates

Configure the IP address of the BMC management network port:

You can configure the IP address of the BMC management network port through the BIOS (Setup->Server Mgmt->BMC network configuration). You can configure the network as a dynamic IP address or a static IP address.

Note: The management network port must be in different network segments from the data network port. Otherwise, security risks may occur.

5.6 This topic describes the BMC function

The BMC home screen displays the following information:

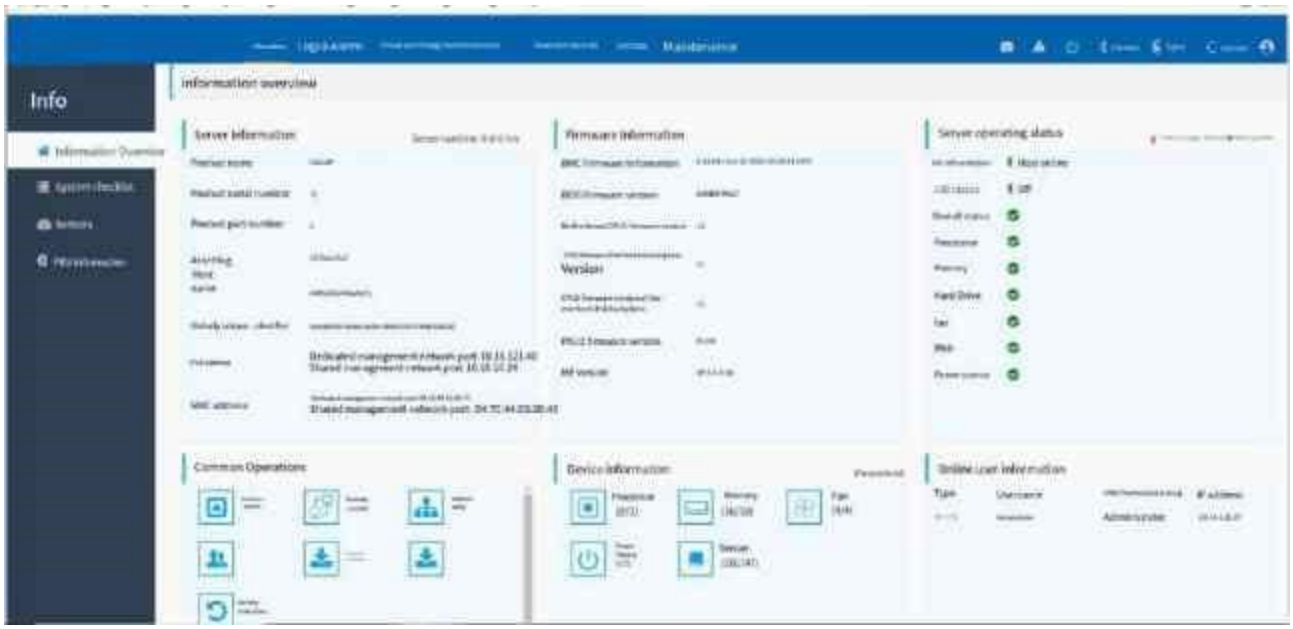


Figure 5-37 BMC home screen

Warnings:

Once the user is logged into the admin interface (as shown in Figure 5-37), remember not to do the following:

Refresh the browser button

Refresh the browser's menu

Browser forward and backward options

F5 on your keyboard

Backspace on the keyboard

Otherwise, the BMC will exit the management interface and you need to log in again

Options	Instructions
Information	This page mainly contains the following four points: Information overview System checklist Sensors FRU information

Options	Instructions
Logs and Alarms	This page mainly displays log and human alarm information, which has the following six categories: Current Alarms IPMI Event Log Log setting Audit log Historical alarm logs One-click collection
Power and Energy	This page displays information about power supplies and energy consumption. • Power Control Historical statistics Thermal management Power capping Power configuration

Remote Services	This page mainly displays remote services related information: Services Remote control Mirror redirection RAID management UID Settings
Users and Security	This page mainly displays information about users and security User Management User Group Management PAM Sequence Settings SSL Settings External User Services
Options	**Instructions**
Settings	This page is mostly about configuring BMC options Date & Time Network Settings Media redirection SMTP Settings Platform Event Filter Video recording IPMI interface System boot item HDD lighting Settings

Maintenance	This page contains the following features: Configuration updates factory data reset. Firmware information Firmware Updates Capture BSOD System Administrator Power-on self-test code

5.6.1 Logging in to BMC

Enter https://BMC IP in the address bar of the browser. The system displays the login page, prompting you to enter the user name and password. The following screenshot is shown. Click the language bar to change the language. Note: You need to change the default password for your first login.

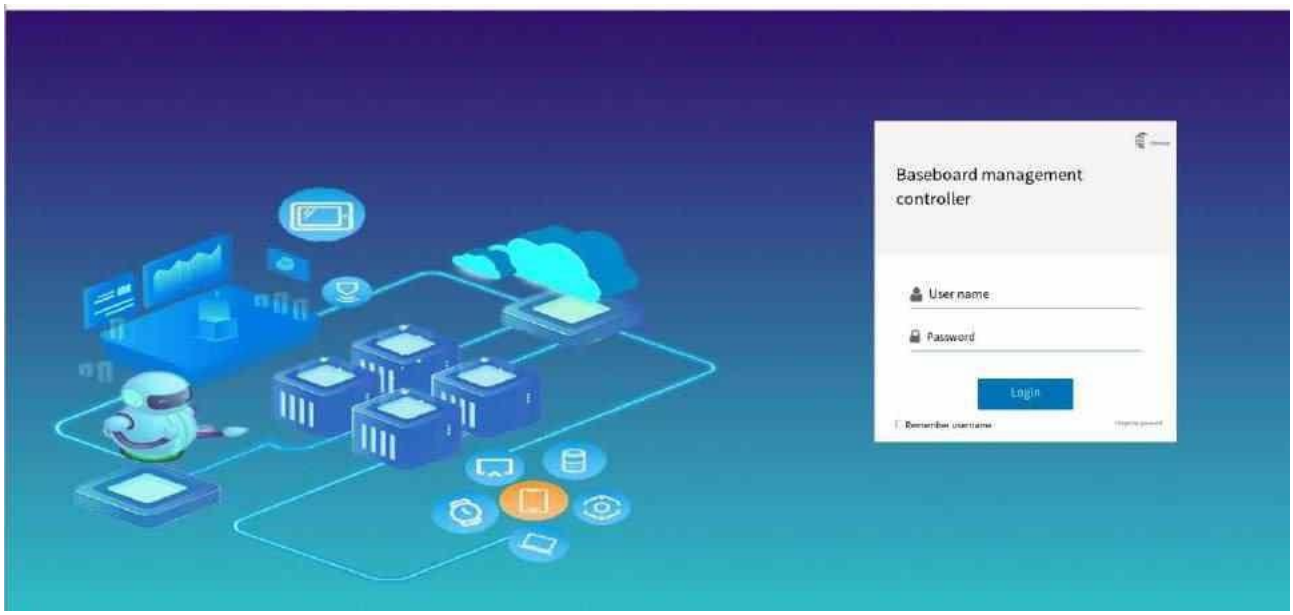


Figure 5-38 BMC login page

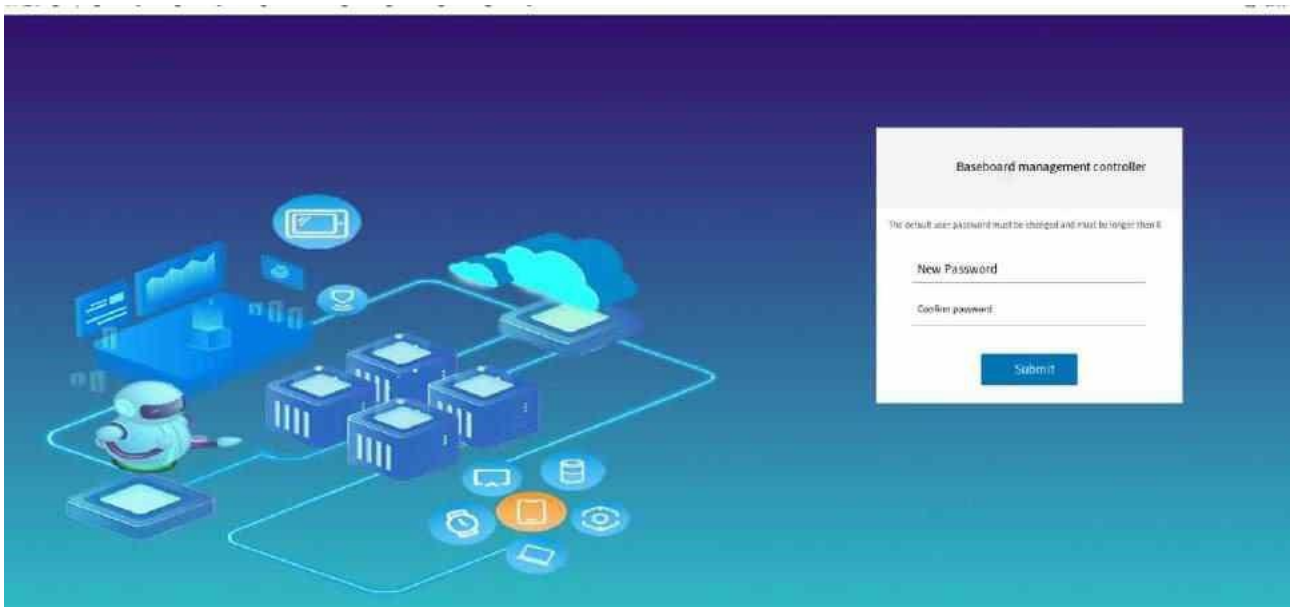


Figure 5-39 BMC password change screen

5.6.2 System Summary

The information summary includes server information, firmware information, server running status, common operations, equipment information, and online user information.

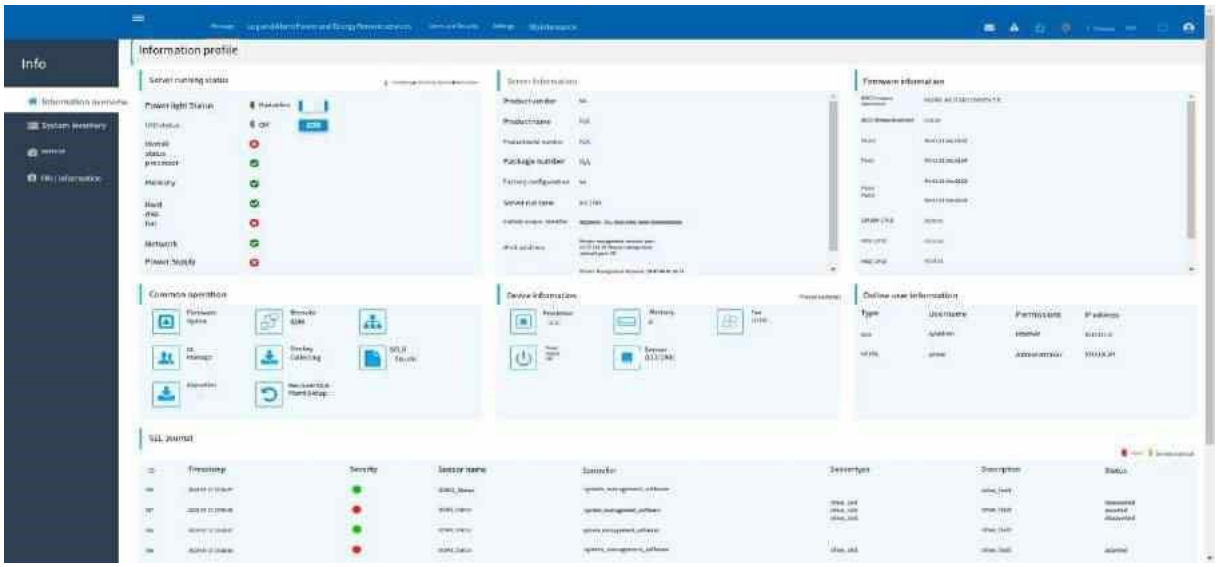


Figure 5-40 System list page

5.6.3 System List

This page displays information about the hardware layout of the system and details about the active PSU, DIMM, PCIE, CPU, and storage devices.

System: Displays current system information, including manufacturer, power status, serial number, BIOS version, UUID, etc.

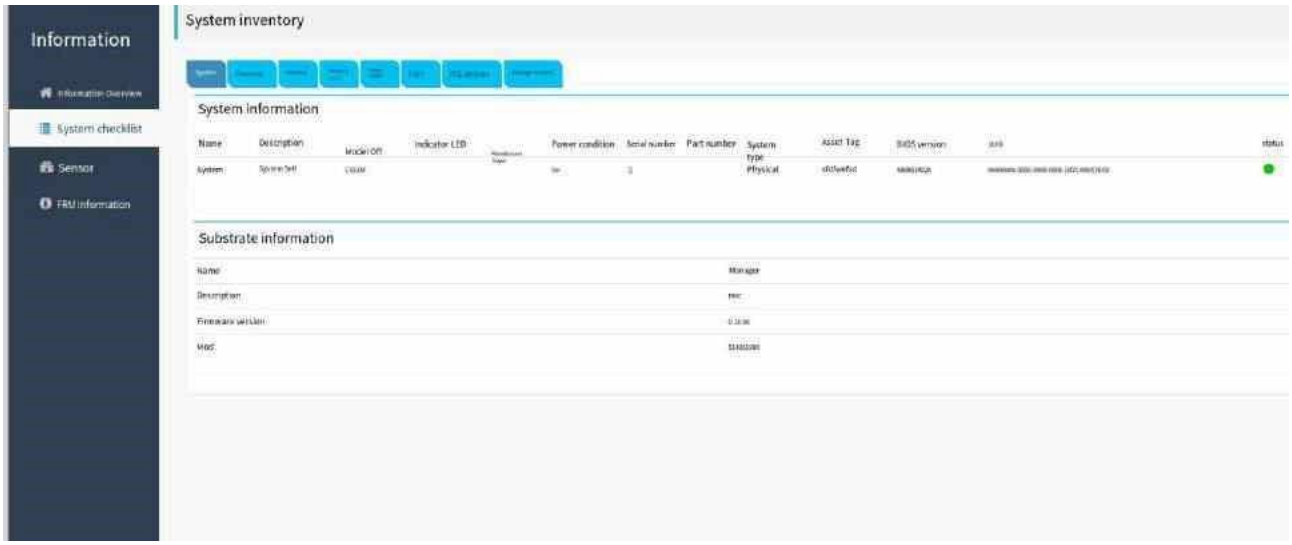


Figure 5-41 System list - System

Processor: Displays information about the processor used.

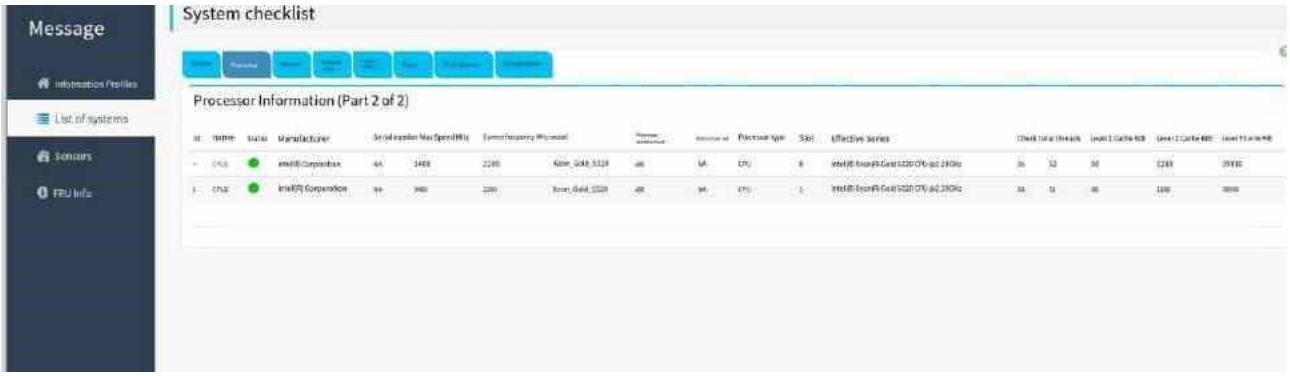


Figure 5-42 System listing - Processor

Memory controller: Provides basic memory information, including the manufacturer, capacity, status, and type of memory.

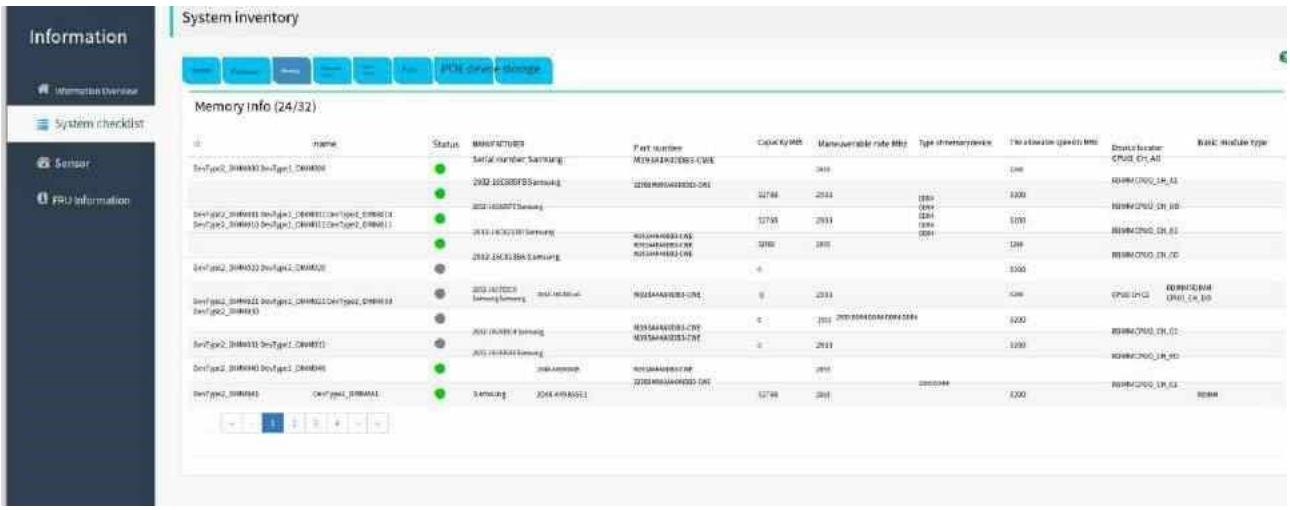


Figure 5-43 System checklist - Memory controller

Baseboard: Displays baseboard BMC information and network port information and status.

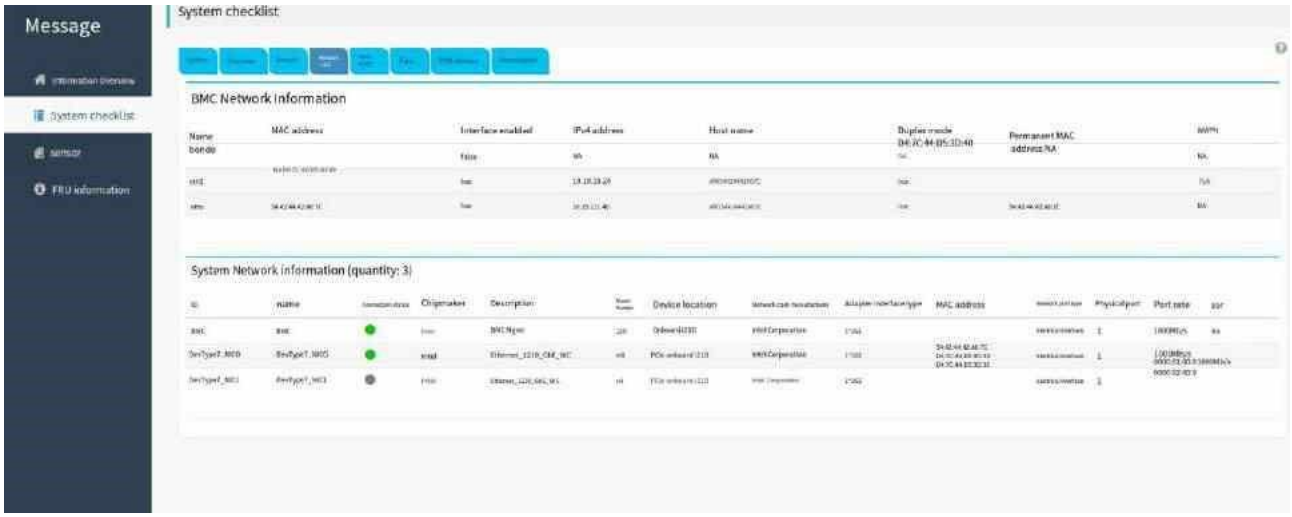


Figure 5 -44 System list - Baseboard information

Power supply: Displays power supply information and voltage sensor information.

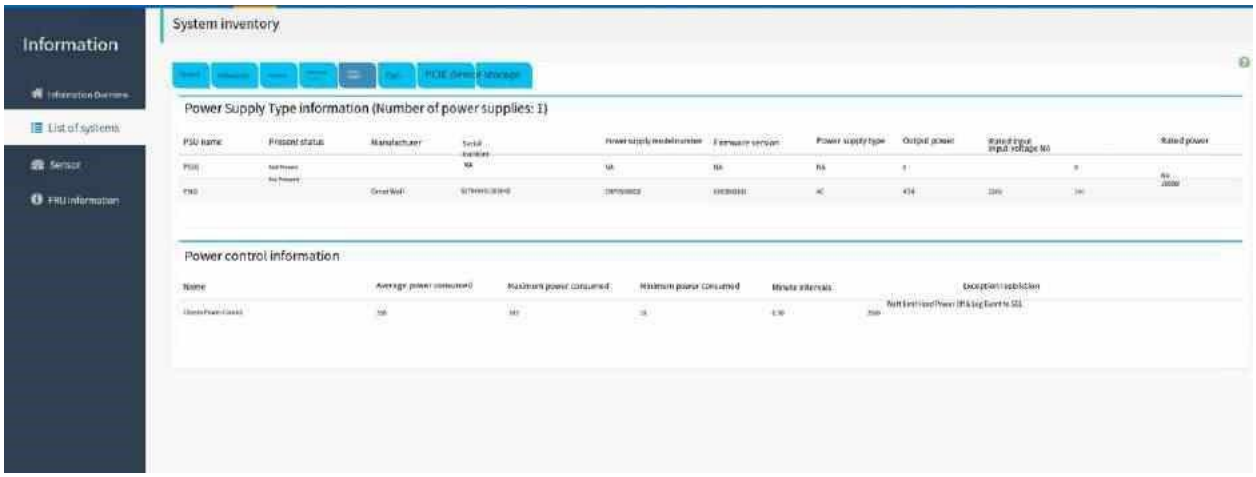


Figure 5-45 System list - Power supply information

Thermal: Displays the status and speed of the fan and the status and value of the temperature sensor.

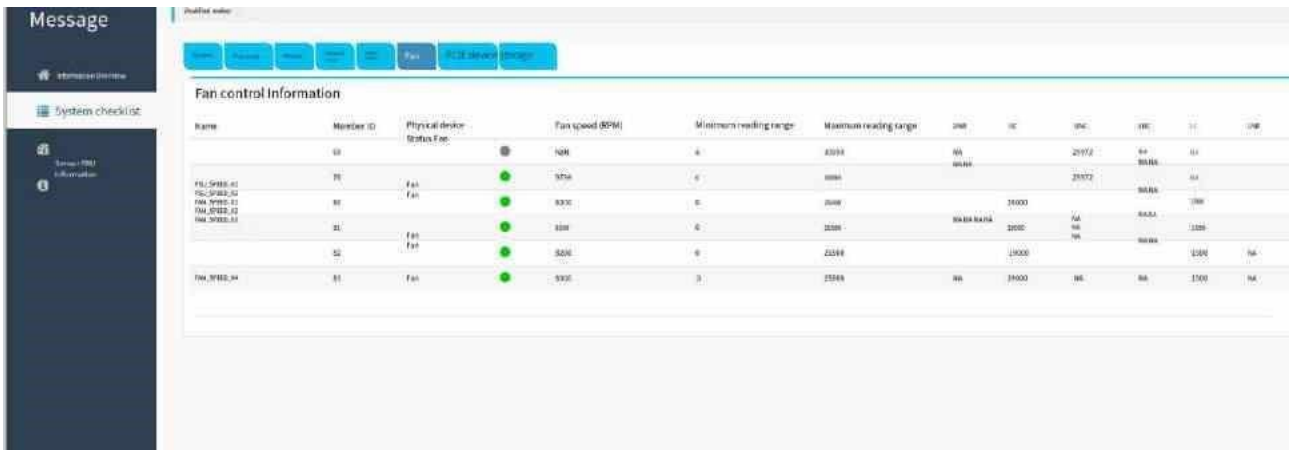


Figure 5-46 System list - Thermal information

PCIE Devices: Displays the current PCIE devices.

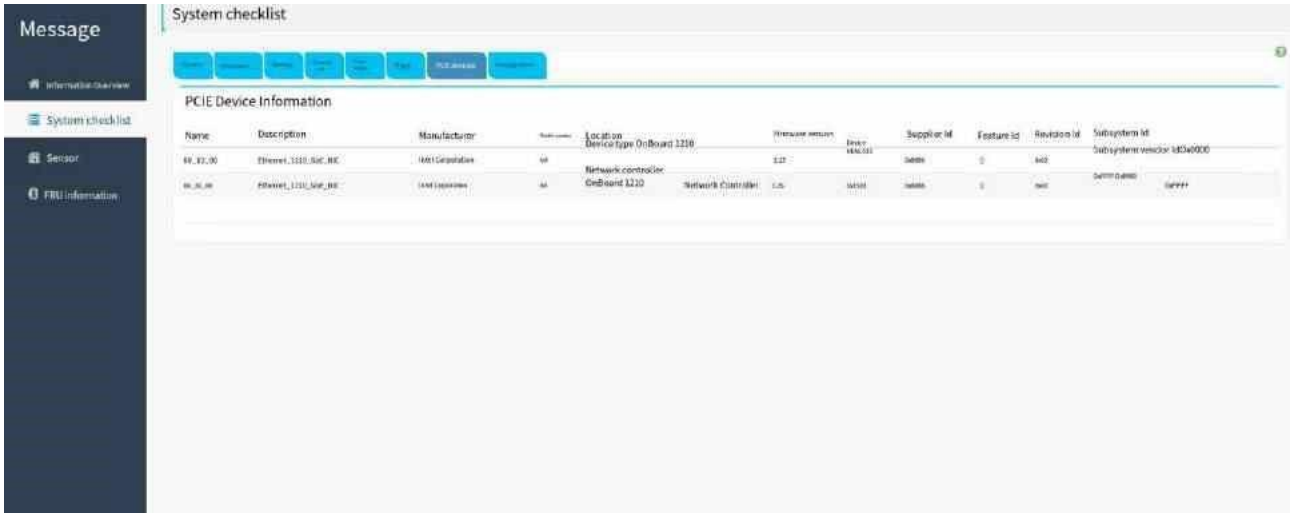


Figure 5-47 System list -PCIE devices

Storage device: Displays storage device driver information and storage device controller information.

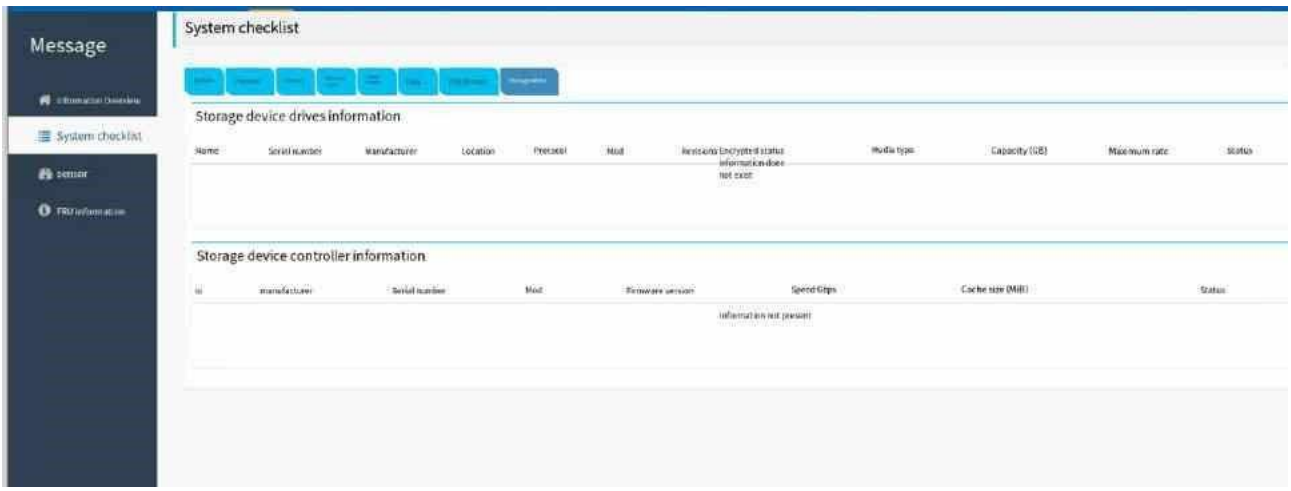


Figure 5-48 System list - Storage devices

5.6.4 Sensors

You can view all sensors supported by the server on this page. The Sensor Reading page displays all sensor information. On the Sensor readings page, real-time readings of all available sensors will be displayed with details such as sensor name, status, current reading and behavior. It is also possible to select the type of sensor you want to display from the list. Sensors include temperature sensors, fan sensors, watchdog sensors, and voltage sensors, among others. This page will refresh automatically with the data from the database. Note that there may be some delay in retrieving live data.

Sensor Types	Description
Alarm Sensor	Information about the sensor that generated an abnormal alarm
Temperature Sensor	Displays the real-time value of the current temperature sensor
Power sensor	Displays the real-time value of the current power sensor
Voltage sensor	Displays the real-time value of the current voltage sensor
Fan sensor	Displays the real-time value of the current fan sensor
Utilization sensor	Displays the real-time value of the current utilization sensor
Discrete sensor	Displays the real-time value of the current discrete sensor
Historical statistics	Display historical data of power consumption, ambient temperature, fan speed

Critical sensors (Describes information about the sensor that generated an abnormal alarm)

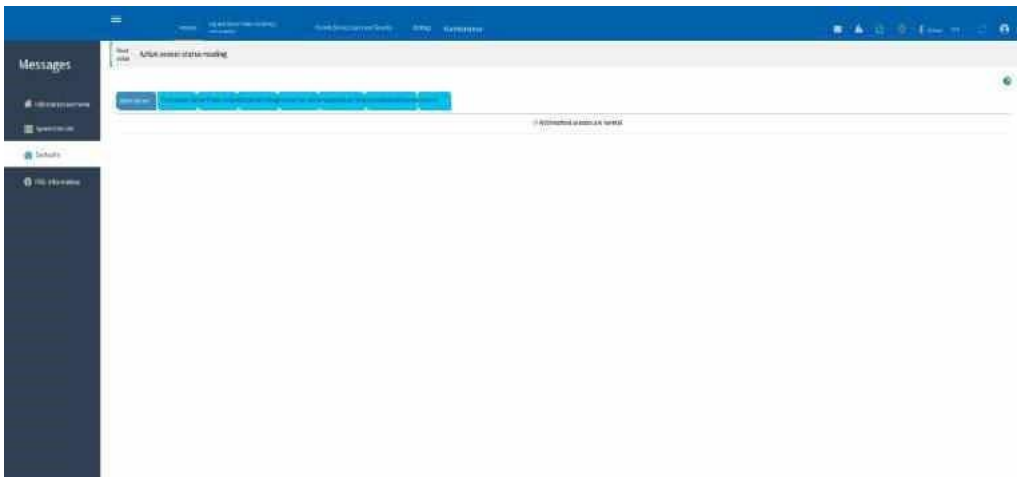


Figure 5-49 Key sensor

Temperature sensor (shows the real-time value of the current temperature sensor)

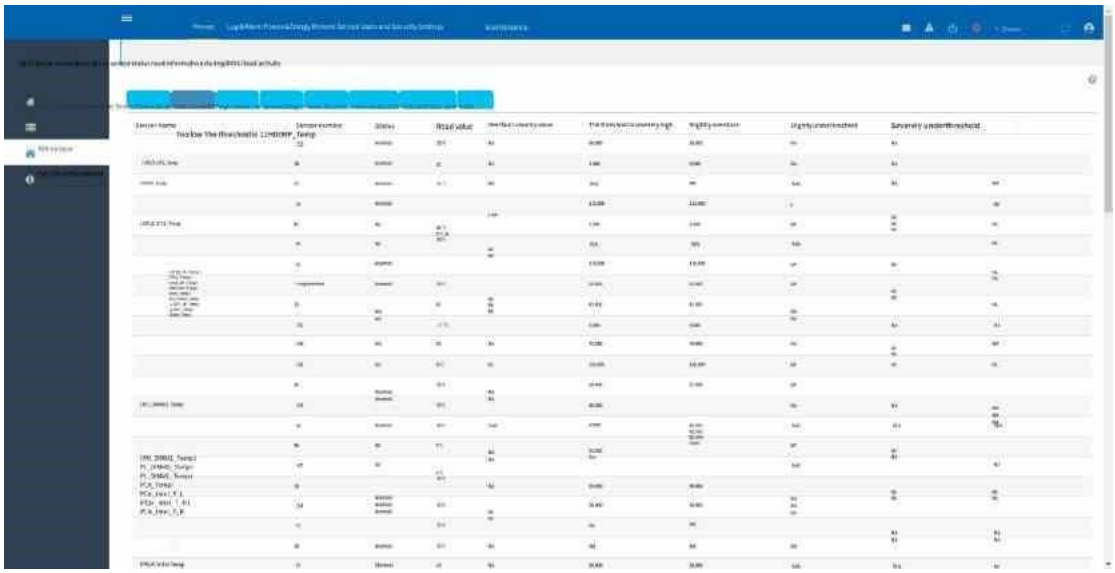


Figure 5-50 Diagram of the temperature sensor

Power sensor status (shows the real-time value of the current power sensor)

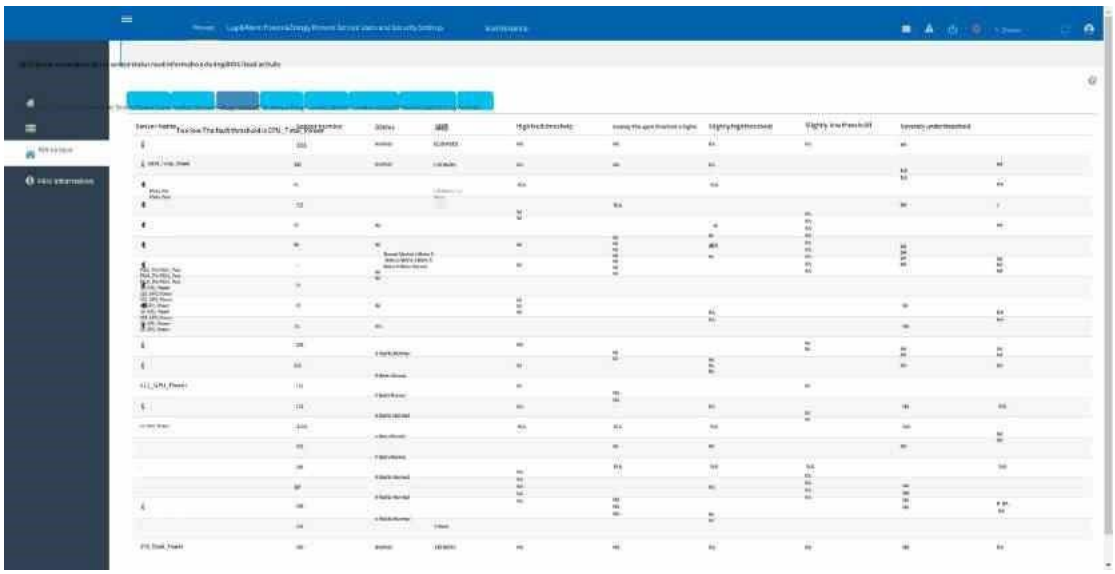


Figure 5-51 Power sensor

Voltage sensor status (shows the real-time value of the current voltage sensor)

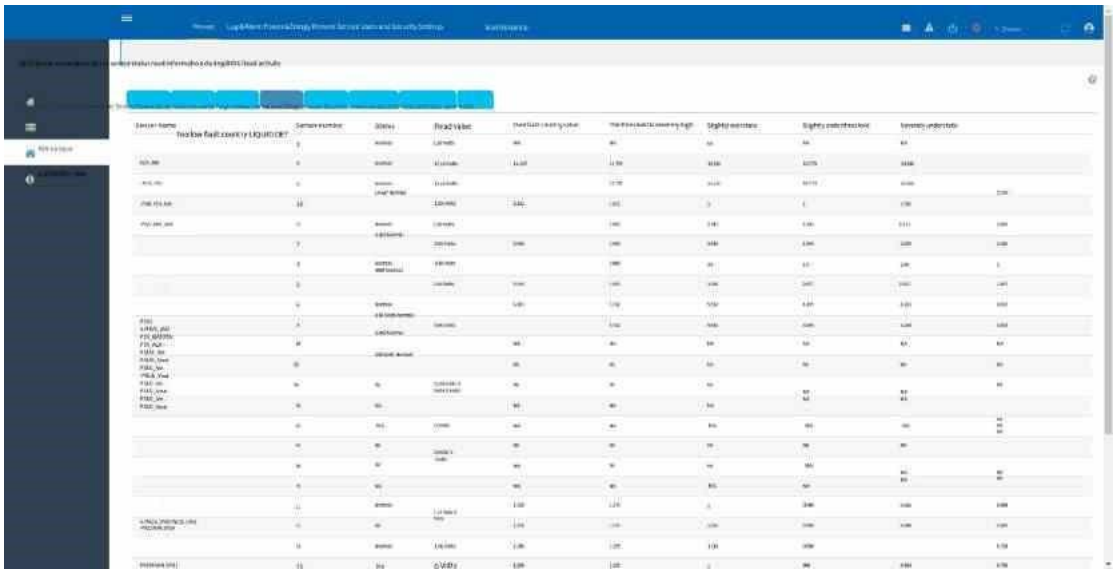


Figure 5-52 Voltage sensor diagram

Fan sensor status (Shows the current real-time value of the fan sensor)

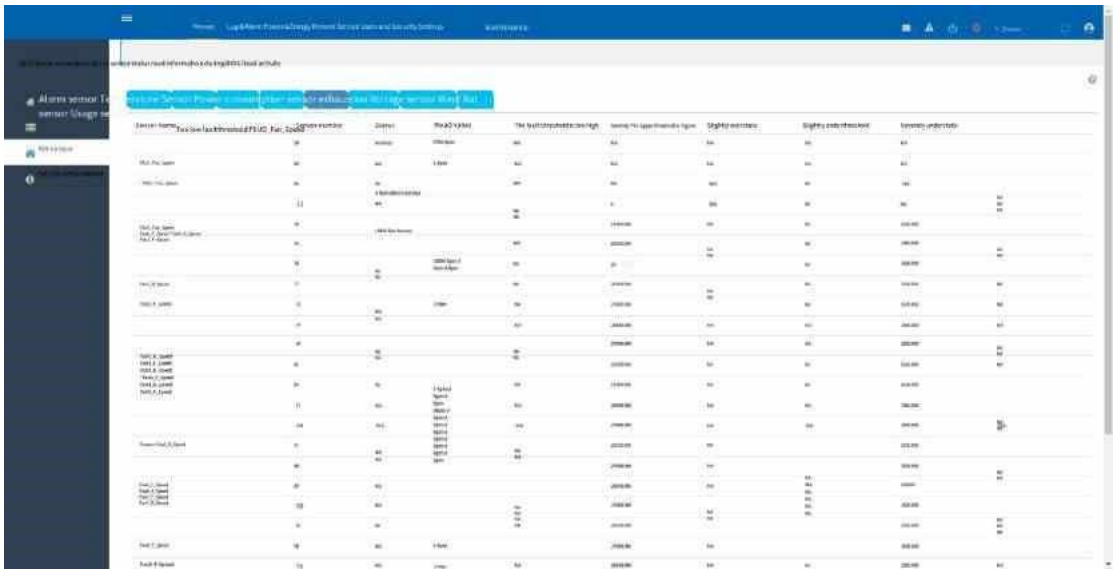


Figure 5-53 Fan sensor status

Utilization sensor (Shows the real-time value of the current utilization sensor)

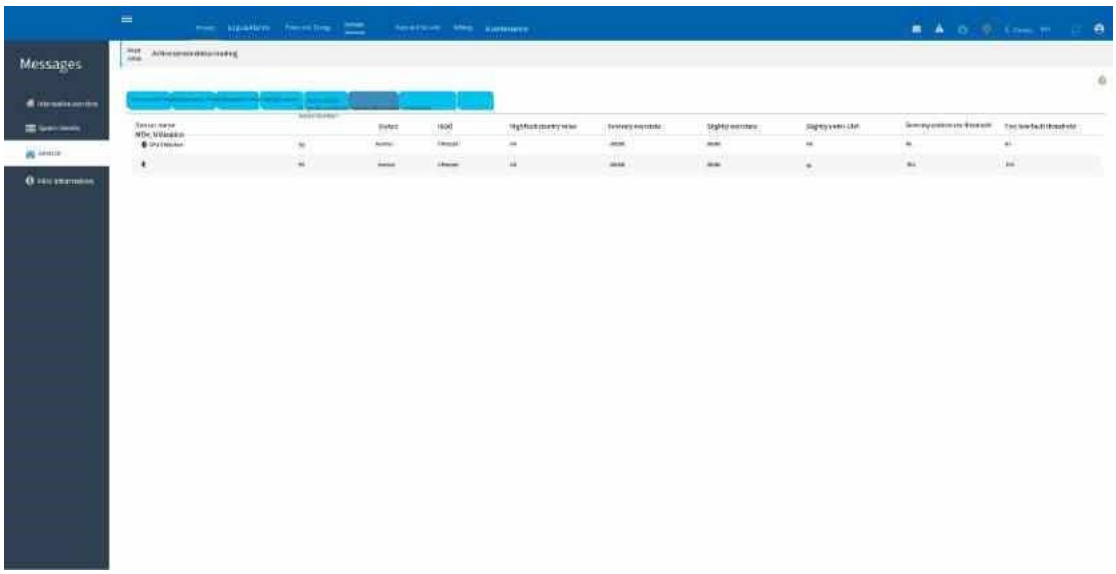


Figure 5-54 Diagram of the utilization sensor

Discrete sensor (Displays information about the current discrete sensor)

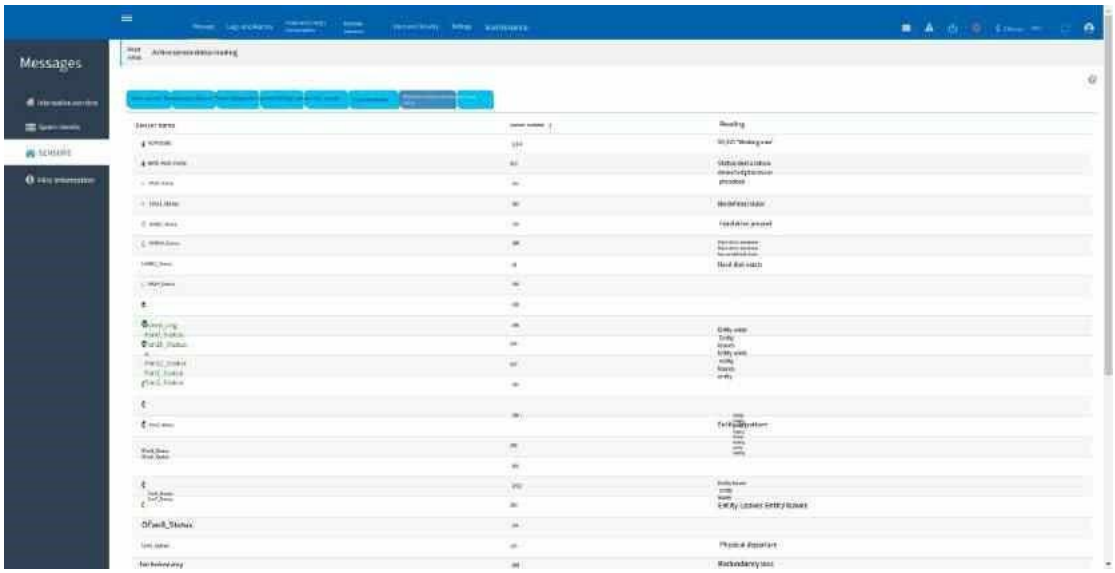


Figure 5-55 Discrete sensor diagram

Historical statistics (showing power consumption, ambient temperature, and the last month's historical data of the fan)

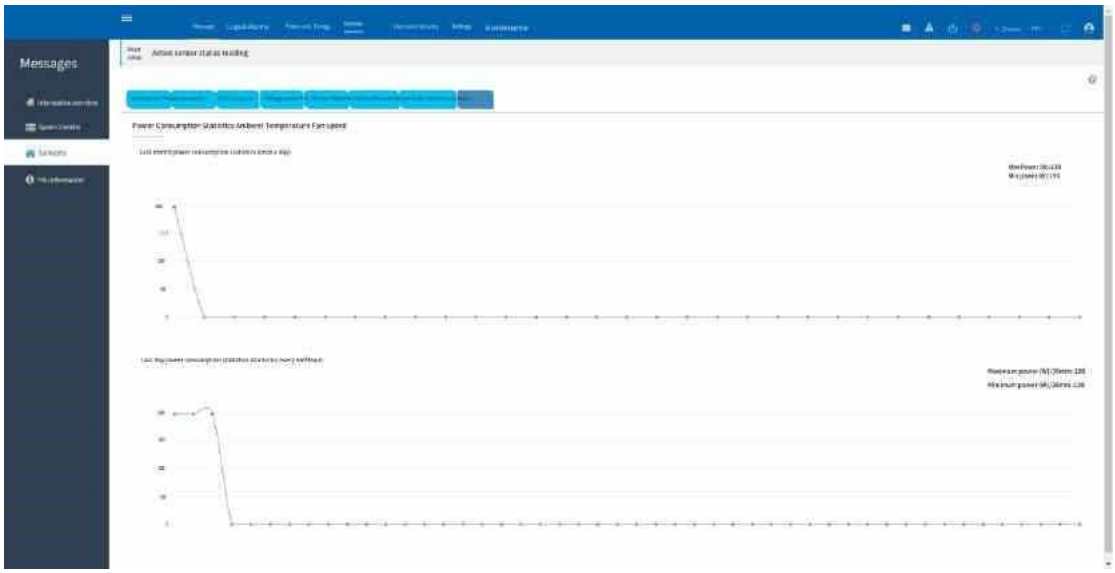


Figure 5-56 Historical statistics

5.6.5 FRU Information

This page displays BMC FRU device information. The FRU page displays basic information, chassis information, mainboard information, and product information about the FRU.

FRU Device ID: Select an FRU device ID from the drop-down list to view the details of the selected device.

FRU Device Name: The device name of the selected FRU device will be displayed.

Users can view different devices by selecting different FRU ids. A maximum of nine FRUs can be viewed on the page, which are as follows: Motherboard FRU, PSU1 FRU,

PSU2 FRU, Front 12 HDD BP FRU, Rear 4 HDD BP FRU, Riser1_FRU, Riser2_FRU, on the Motherboard FRU page.

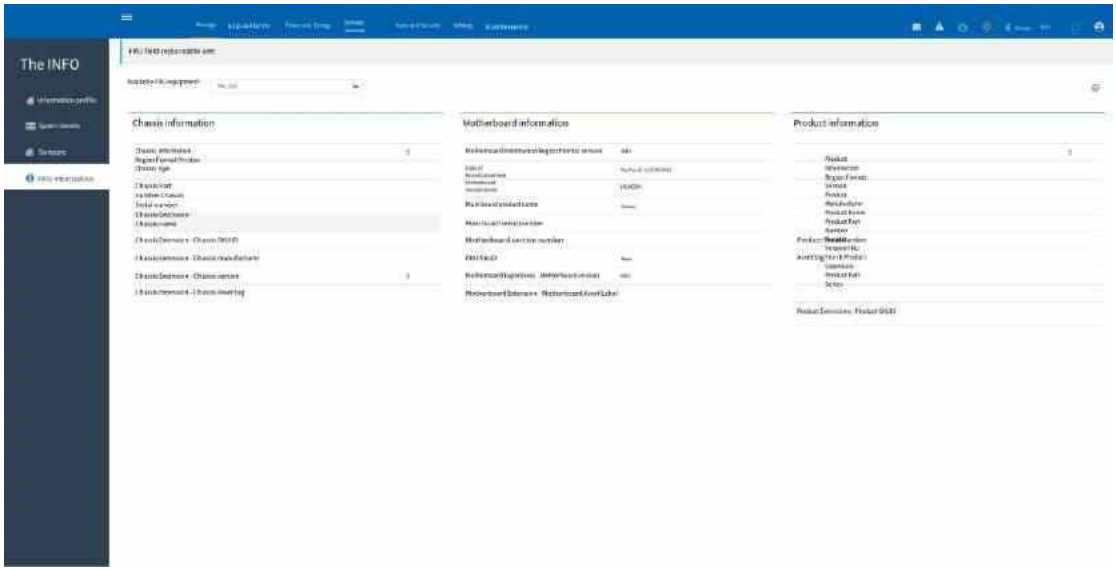


Figure 5-57 FRU information

5.6.6 Logs & Alarms

5.6.6.1 SEL Logs

This page displays all SEL log information.

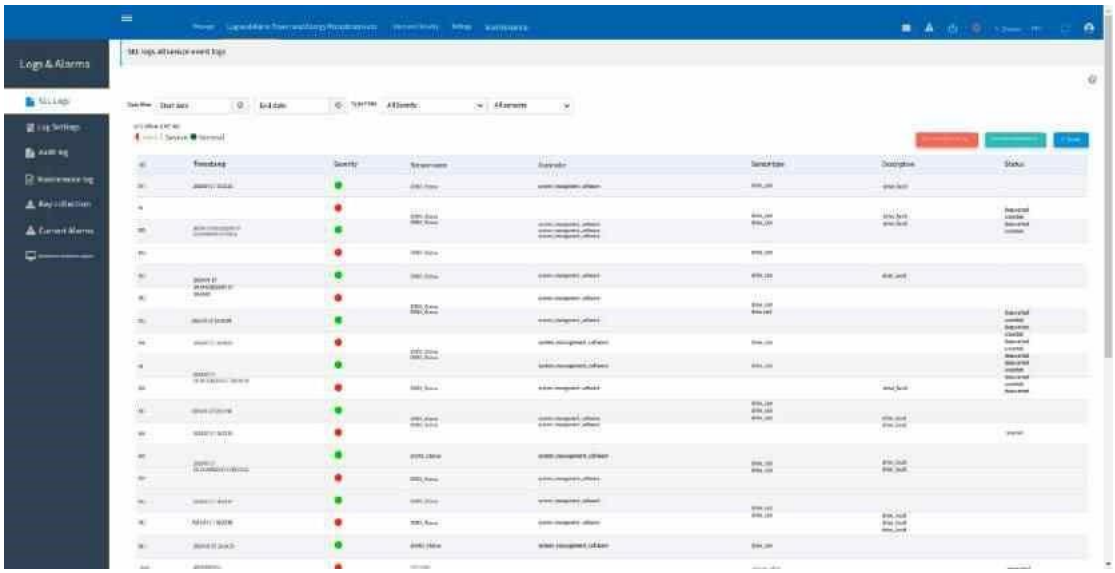


Figure 5-58 SEL logs

5.6.6.2, Log Settings

This page is used to configure the event log

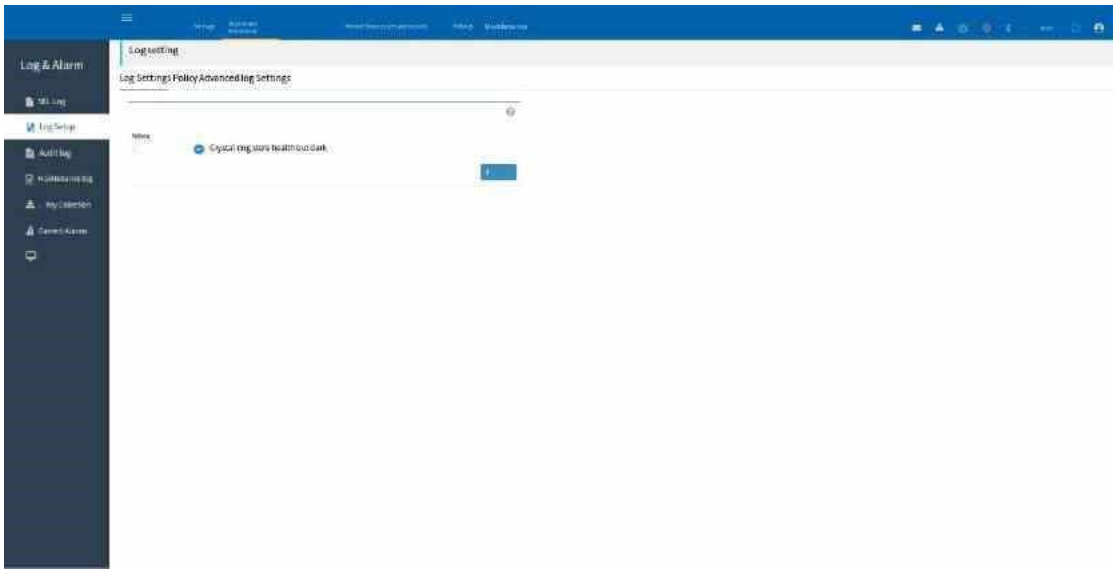


Figure 5-59 Log Settings

Log Setup Policy: This page is used to configure the log storage policy for event logs.

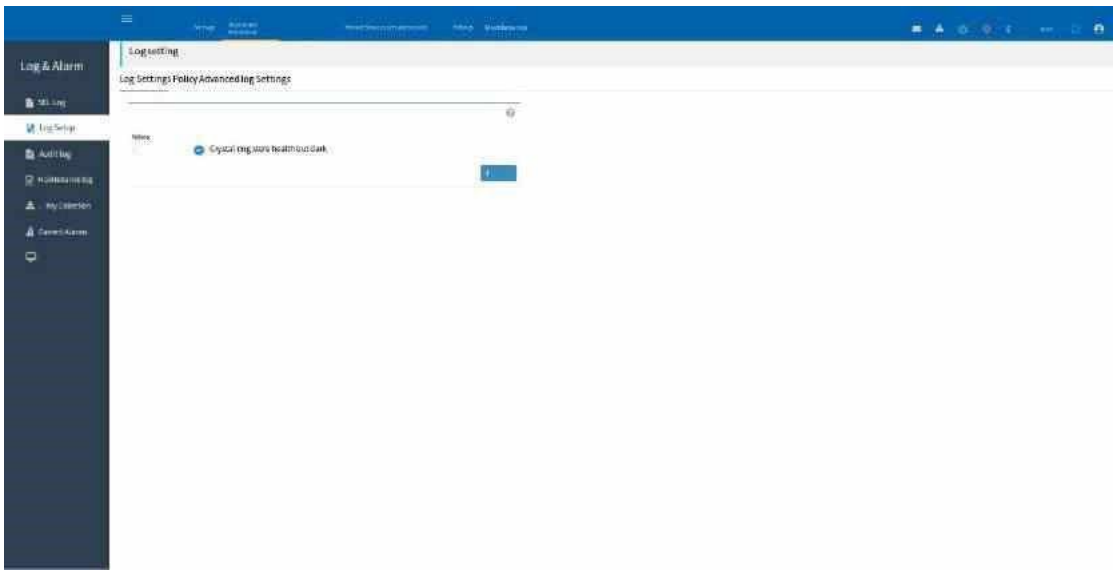


Figure 5-60 Log Setup Policy - Log Setup policy

Advanced Log Settings: This page is used to configure the enable/disable of the logging system and the configuration of local/remote storage log policies

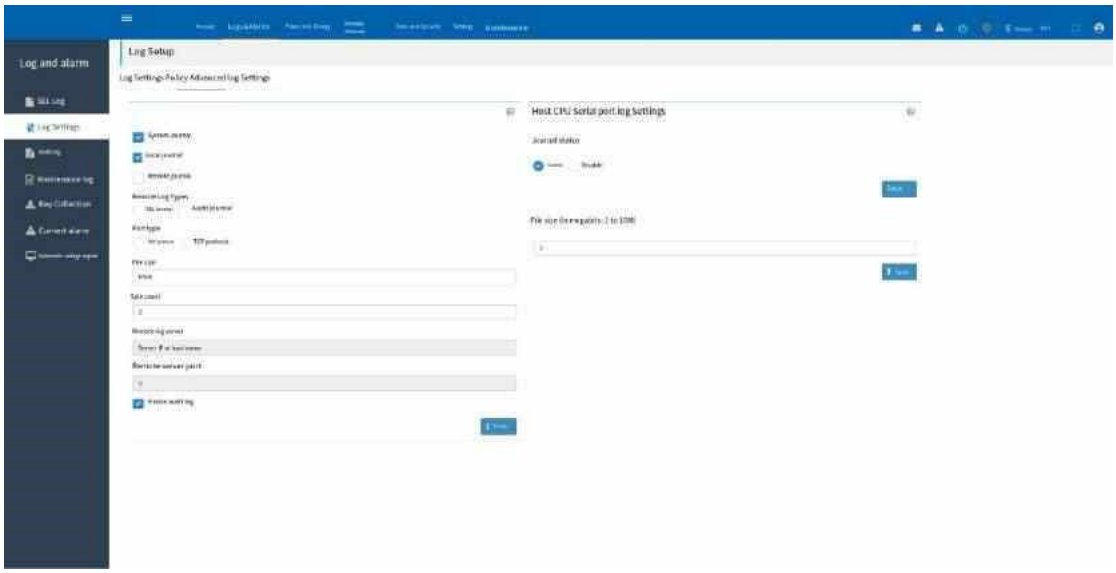


Figure 5-61 Log Settings - Advanced Log Settings

5.6.6.3, Audit log

This page is used to display audit logs.

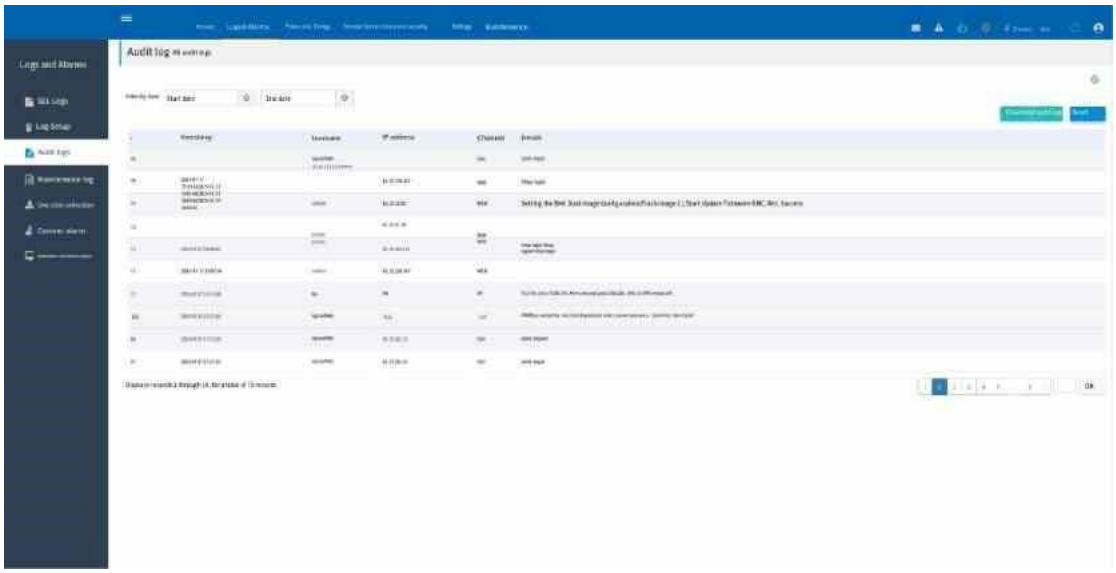


Figure 5-62 Audit logs

5.6.6.4 Maintenance Logs

This page is used to display maintenance logs

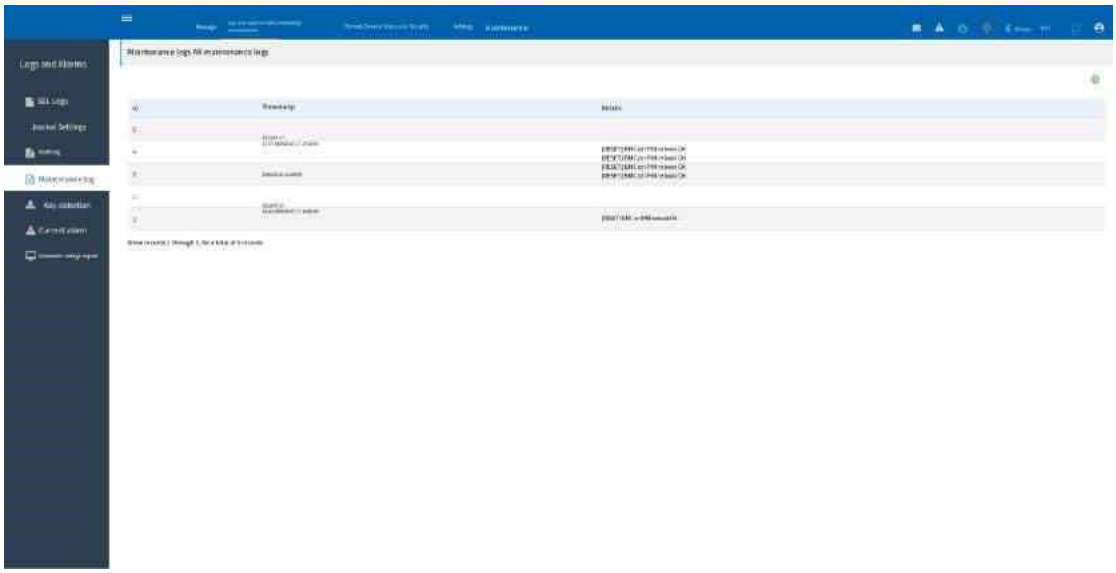


Figure 5-63 Maintenance logs

5.6.6.5. One-click Collection

This page supports one-click collection of logs, server configuration, asset information and other data.

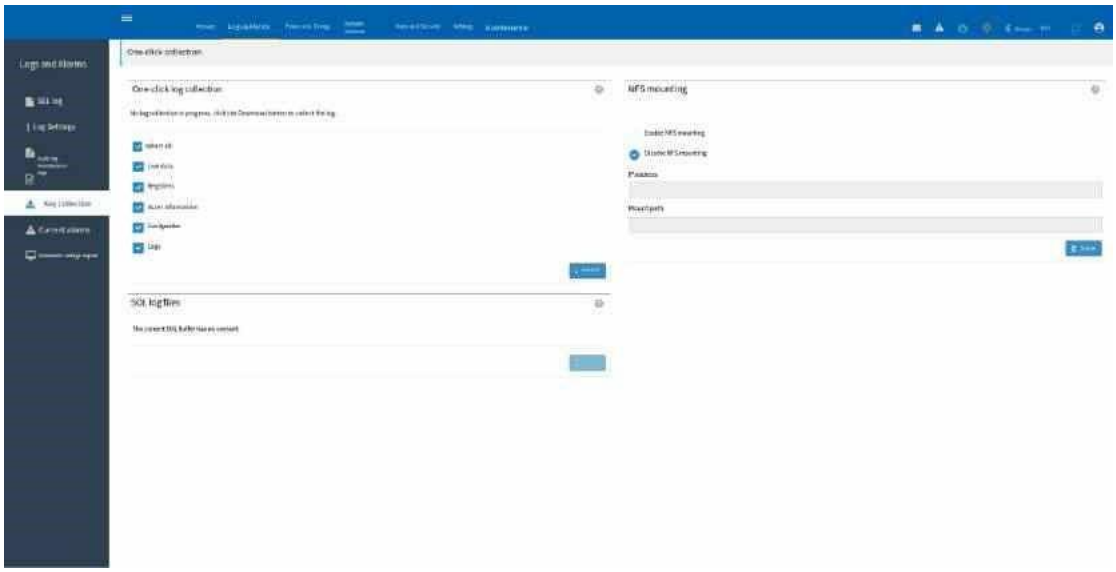


Figure 5-64 One-click collection

5.6.6.6. Current Alarms

This page displays current alarms

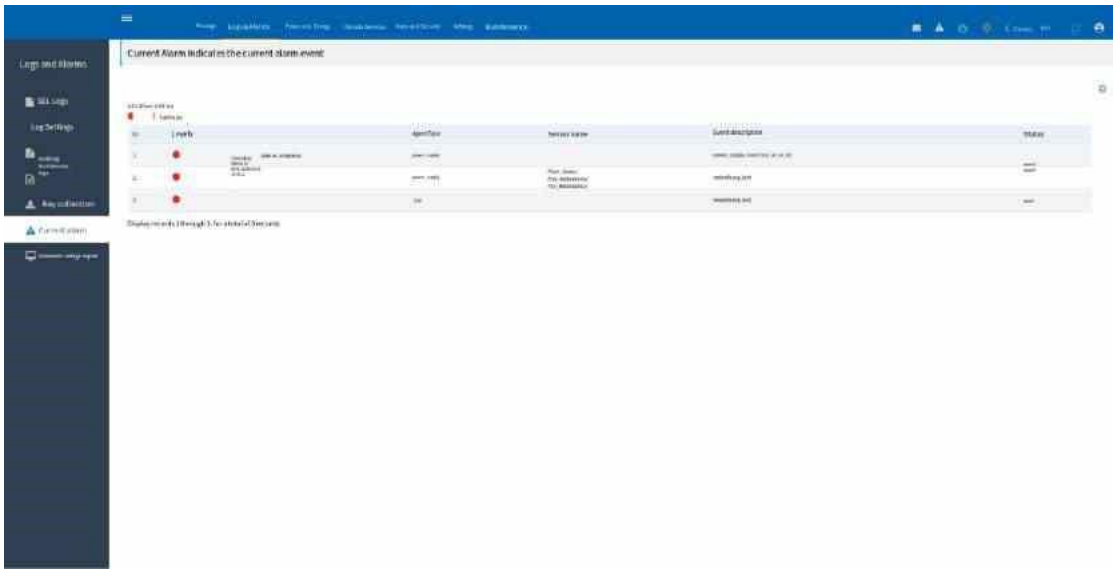


Figure 5-65 Current alarms

5.6.6.7 Automatic Outage Export

This page shows the outage export Settings.

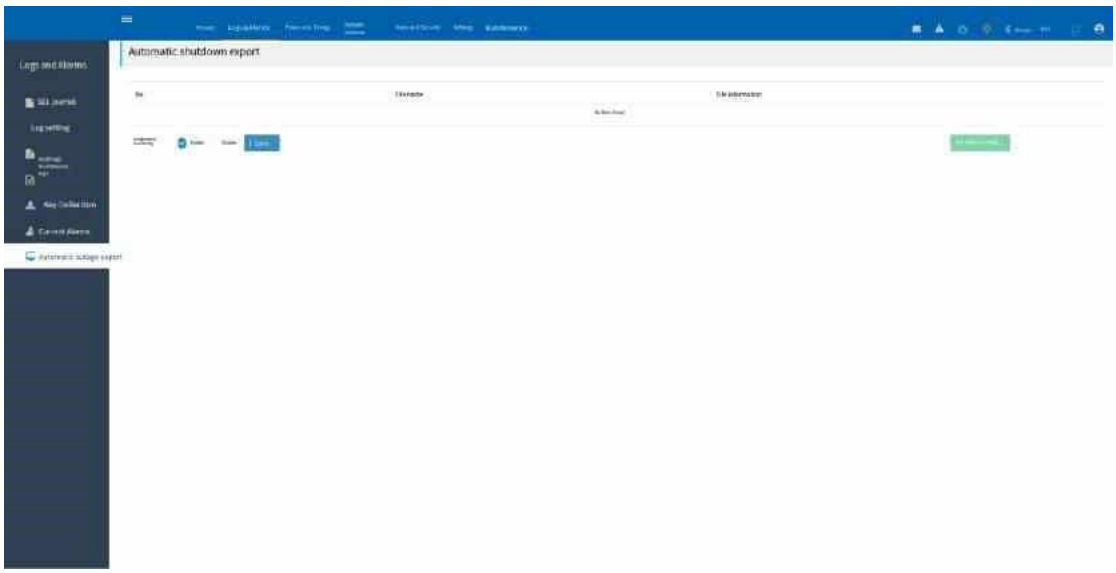


Figure 5-66 Automatic outage Export

5.6.7 Power and Energy

5.6.7.1 Power Control

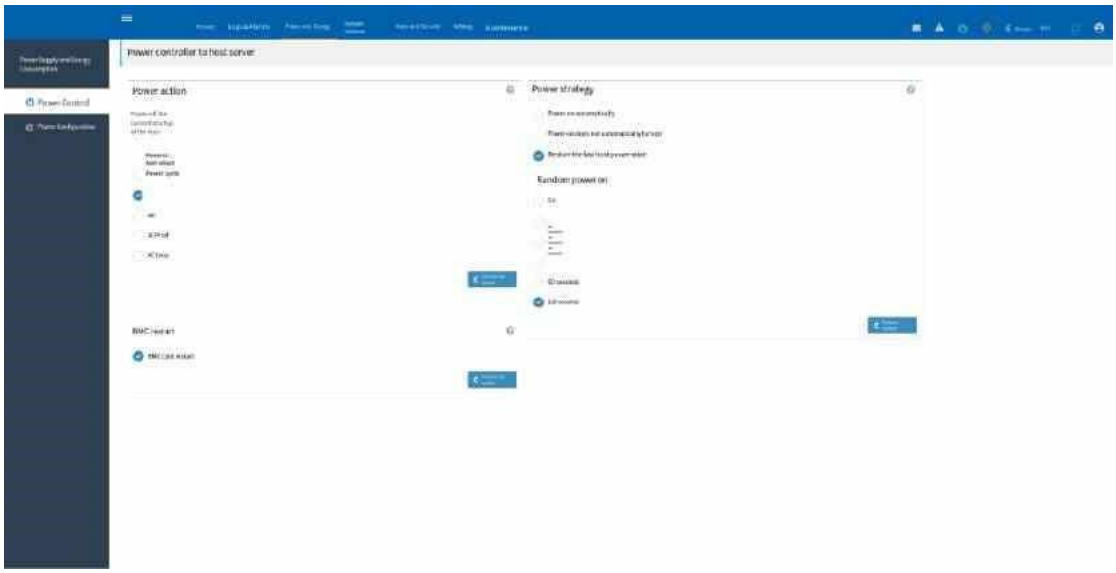


Figure 5-67 Power control

Power off: Selecting this option will immediately power off the server.

Power on: Selecting this option will power on the server.

Power Cycle: Selecting this option will first turn off power and then restart the system (cold boot).

Hard Reboot: Selecting this option will restart the system without shutting it down (hot boot).

NMI: Triggers to produce a non-maskable interrupt. It is recommended to use this feature when you can no longer use the operating system.

ACPI Shutdown: Select this option to start the operating system shutdown before shutdown.

AC Loop: Select this option to perform an AC loop.

BMC Cold Restart: Select this option to restart the BMC directly.

Power-on Auto power on: Automatically power on after the power is connected Power-on does not automatically turn on: After the power is connected, wait for the power to turn on

Restore the status of the last host power supply: After the host power supply is connected, the host power supply is restored to the status before power failure Random power-on: After you select a time, the BMC randomly generates a delay within the selected time and then powers on the host. If you select 0 seconds, the delayed power-on function is disabled

5.6.7.2 Power Supply Configuration

This page describes the configuration of the power supply working mode

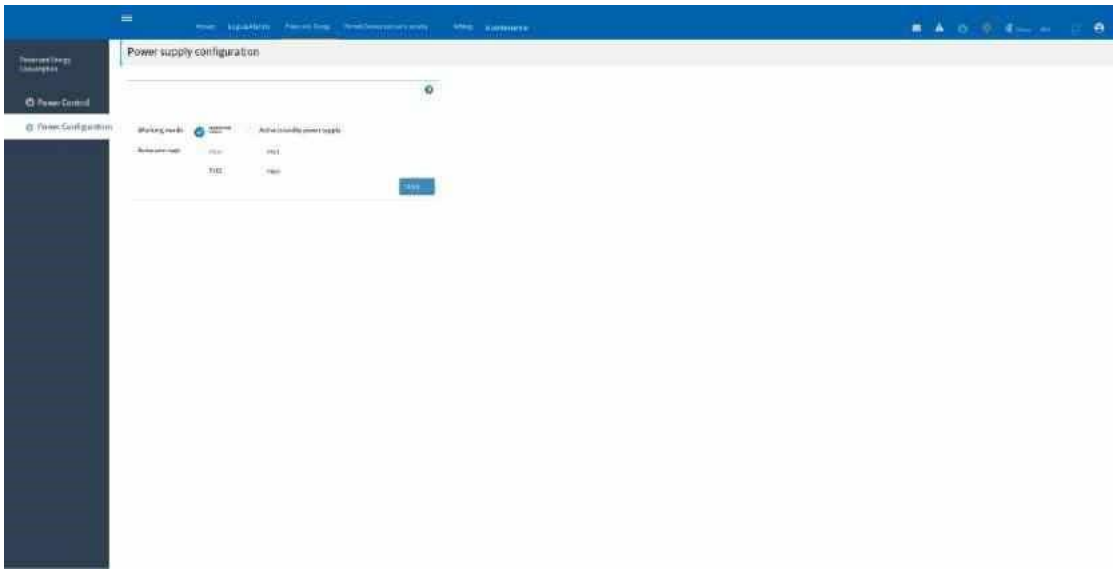


Figure 5-68 PSU configuration

5.6.8 Remote Services

5.6.8.1, Service

This page lists the services performed on BMC. Displays the current status and other basic information for each service.

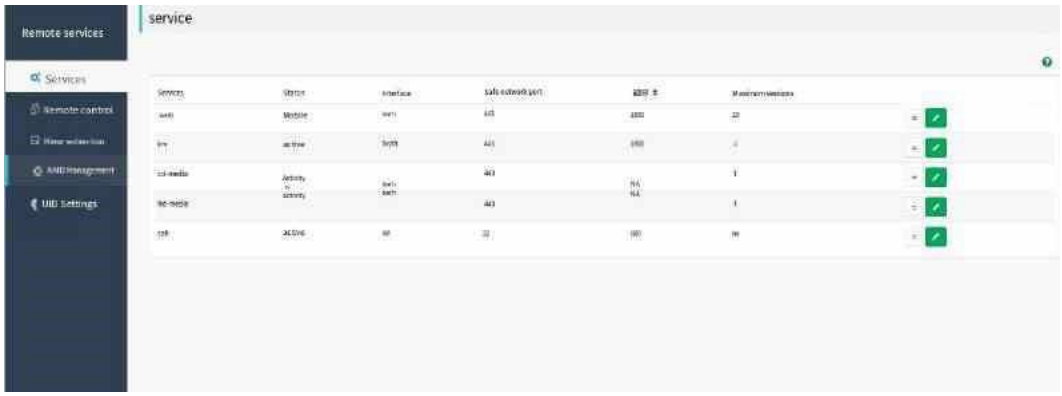


Figure 5-69 Services

5.6.8.2, Remote Control

This page provides an interface to enable HTML5 KVM.

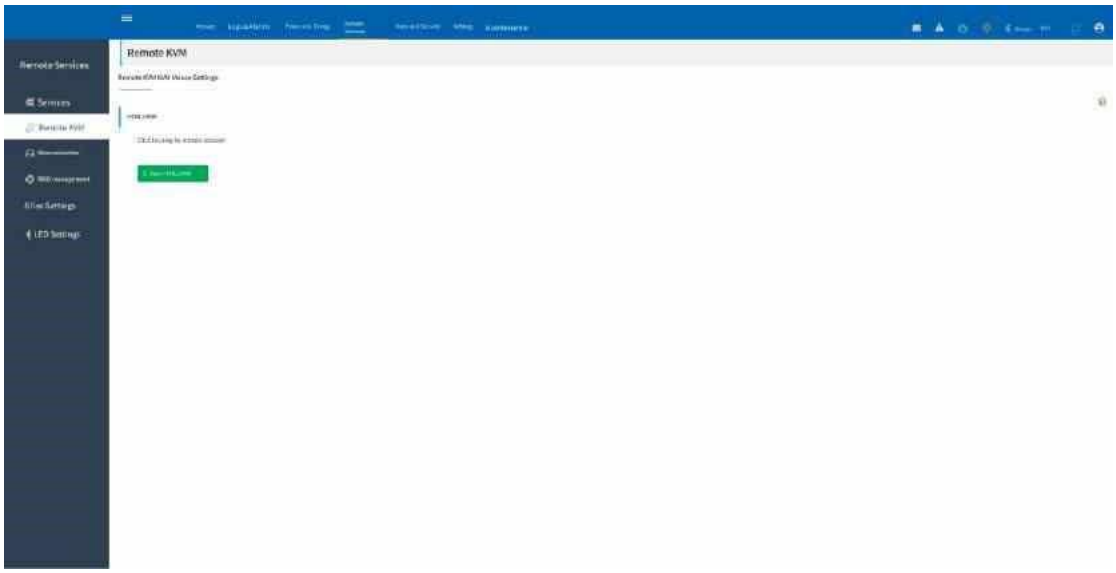


Figure 5-70 Remote KVM

KVM

After clicking "Enable HTML5 KVM", the browser will display a new page. The left side of the page mainly provides other functions such as video recording Settings, power management, and shortcut key sending.

The right side of the KVM page provides shortcut keys for mounting media image, and powering on or off the power supply.

The lower right corner of the page provides control keys that you need to use the KVM. The green color of the control key indicates enable, and the gray color indicates disable. You can press the control key to change its status to the opposite of the current one.

Figure 5-71 Remote control -H5 KVM Note:

If the user wants to use a key combination, for example "Ctrl C". Press CTRL enable on the KVM and then type C. Then the KVM sends Ctrl C to the operating system. If you do not set the CTRL key to enable and type Ctrl C directly on the keyboard, the KVM will send a letter C to the operating system (the local control key is blocked by the local operating system and cannot be recognized by the KVM). When you do not need to send a key combination, set the KVM control key to the default state (NUM is "enable", all others are "disable").

KVM Mouse Settings

This page allows you to configure mouse mode in KVM. Only "Administrator" has permission to configure this option.

Relative Mouse mode: Relative mode calculates the amount of relative mouse displacement and transmits it to the server

Absolute Mouse mode: Absolute mode transmits the absolute position of the local mouse to the server. It is recommended that the server run Windows or a newer version of Linux

Other mouse modes: Other modes calculate the displacement of the local mouse in the central position and send it to the server

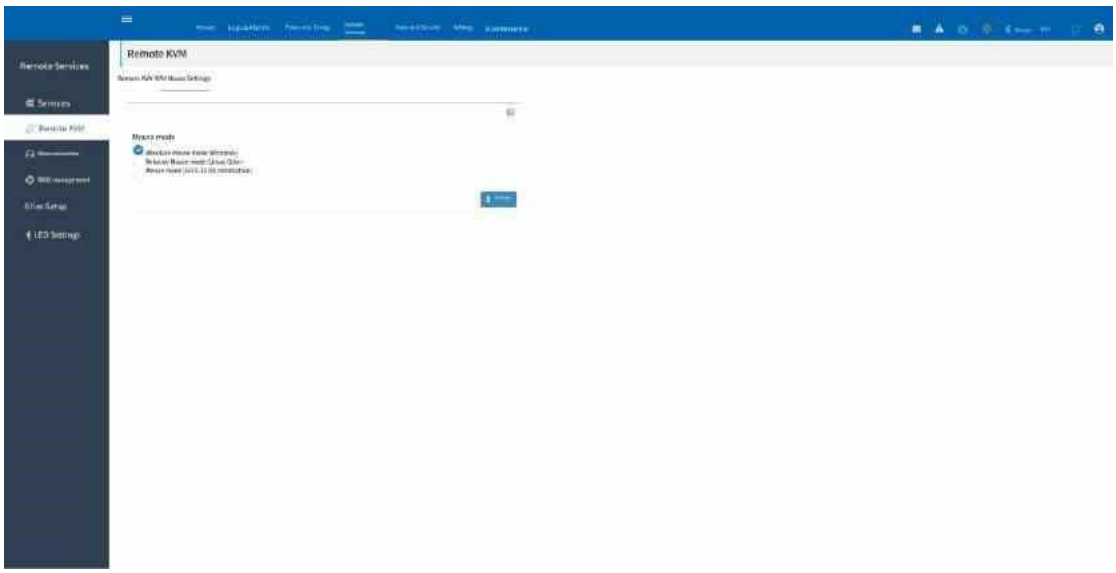


Figure 5-72 Remote Control -KVM Mouse Settings

5.6.8.3. Image redirection

Local Mirror

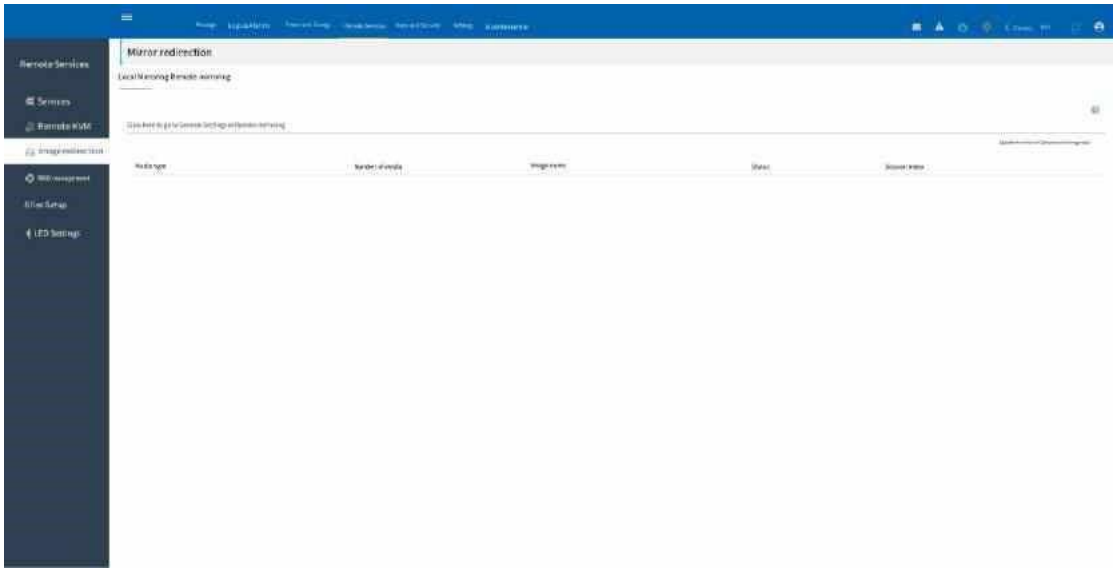


Figure 5-73 Mirror redirection - Local mirror

Remote Image: Emulates CD/DVD/floppy/hard disk images in the network through BMC for media hosting.

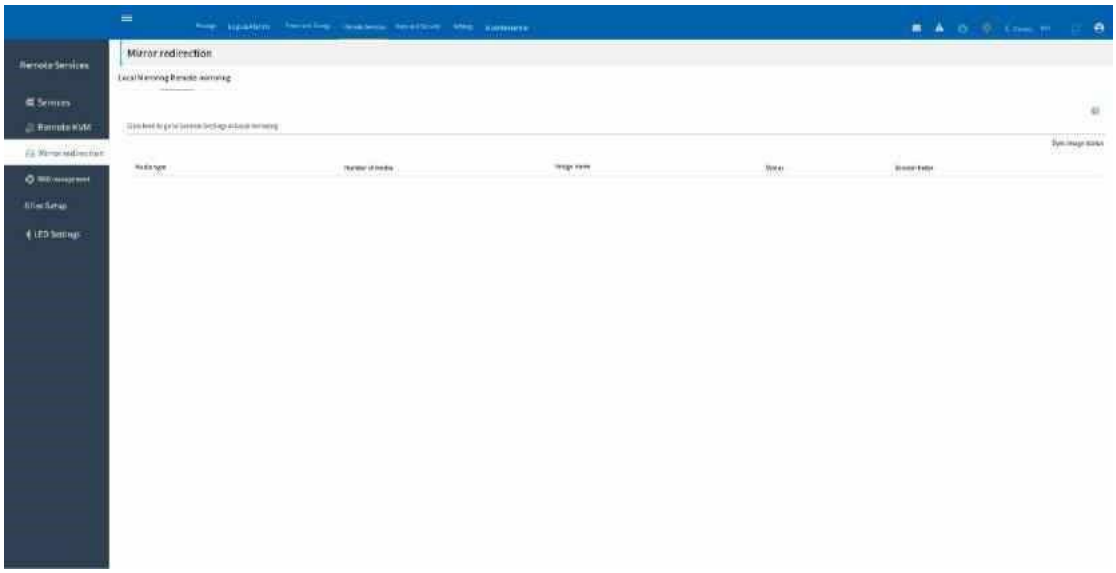


Figure 5-74 Image redirection - Remote mirroring

5.6.8.4. RAID Management

RAID management includes RAID controller information, storage summary, physical disk information, logical disk information, backup power supply information, event logs, and chassis information.

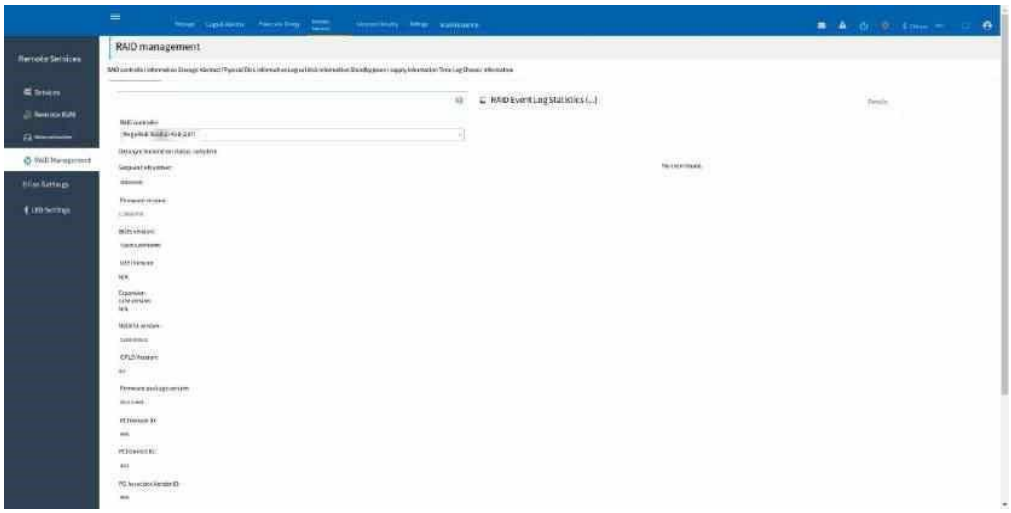
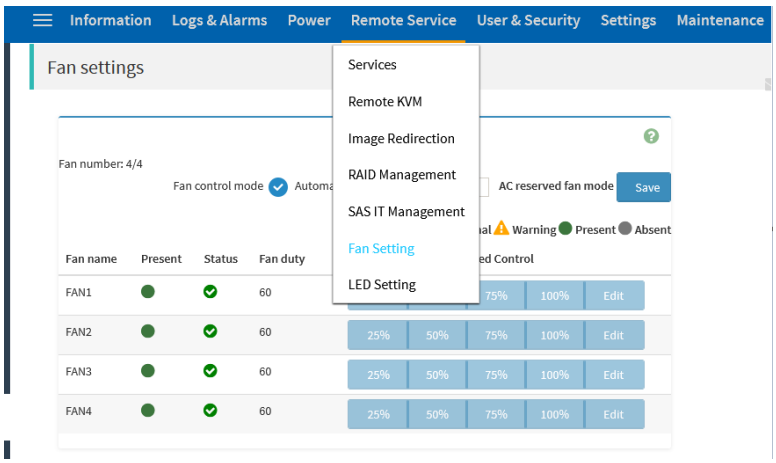


Figure 5-75 RAID management

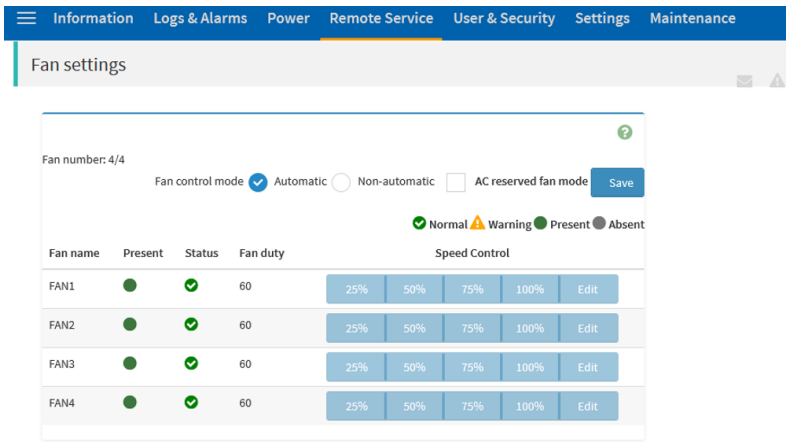
5.6.8.5. Fan Settings

This page allows you to view and set the duty cycle of the fan.

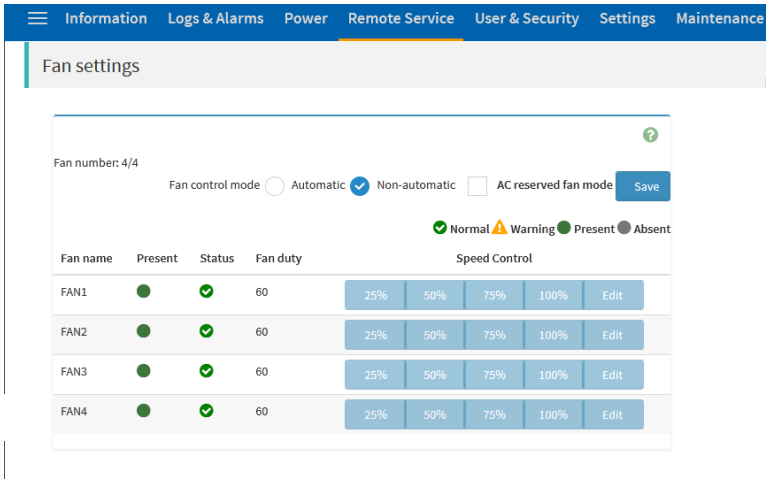
Go to “Fan Setting”



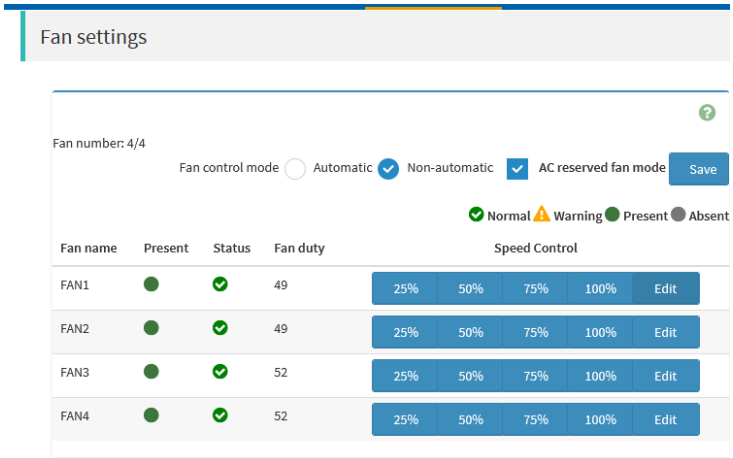
Default setting would be Automatic



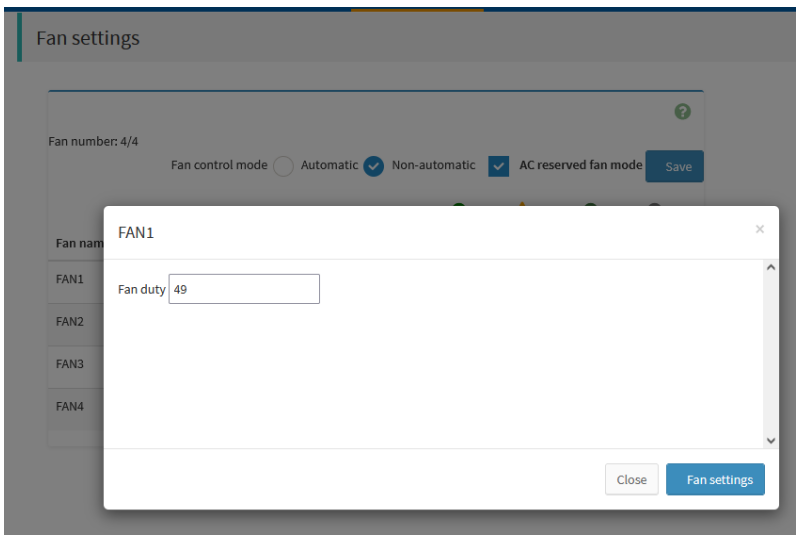
To change the speed of Fans check Non-automatic and click on Save button



Now the options will be available to change the speed of fans



Ent the Fan duty speed accordingly or can click on the available fan duty speed in the range of 25%, 50%, 75%, 100%



Now click on Save button for setting done

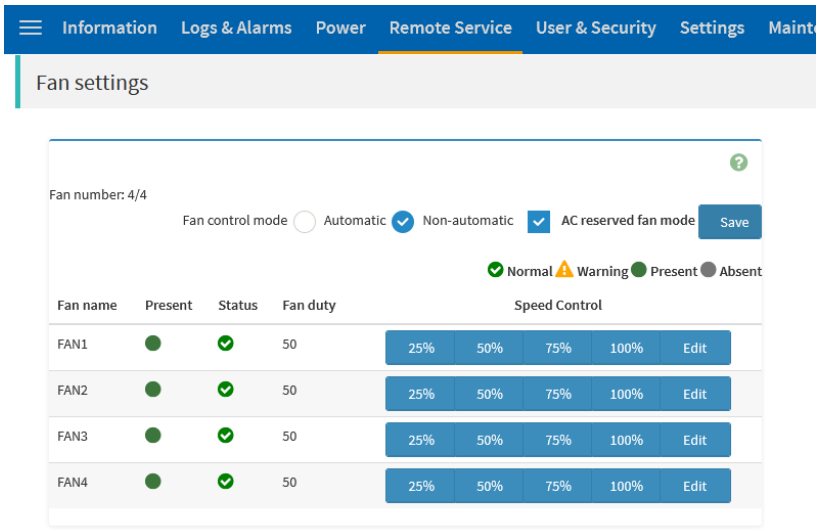


Figure 5-76 Fan Settings

Note: On each system boot activity, the fan speed will reset to Automatic.

5.6.8.6. LED Settings

This page displays and sets the status of UID light, health light, NVME light, HDD light.

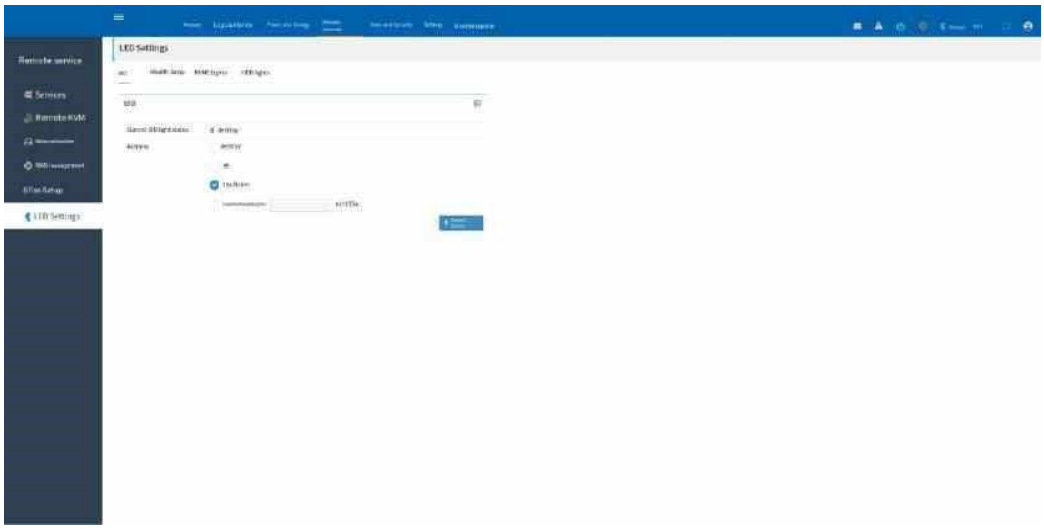


Figure 5-77 UID Settings

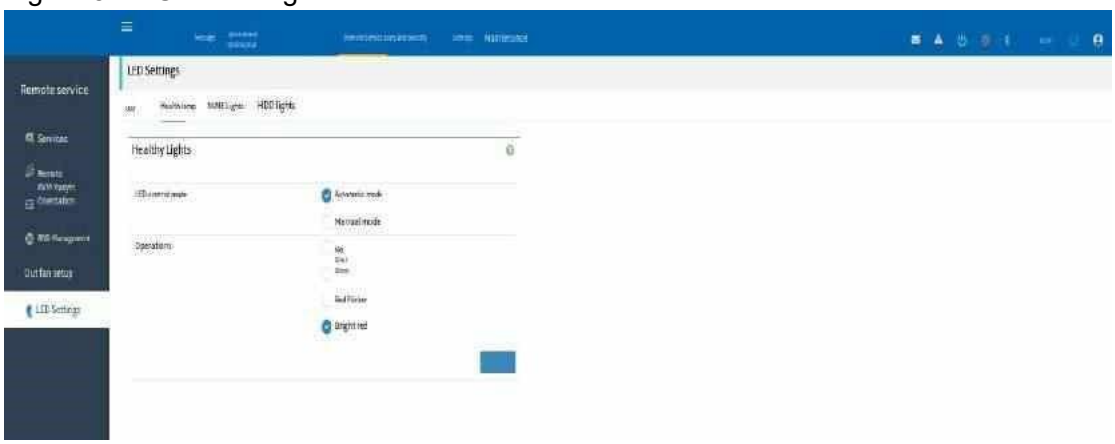


Figure 5-78 Setting health indicator

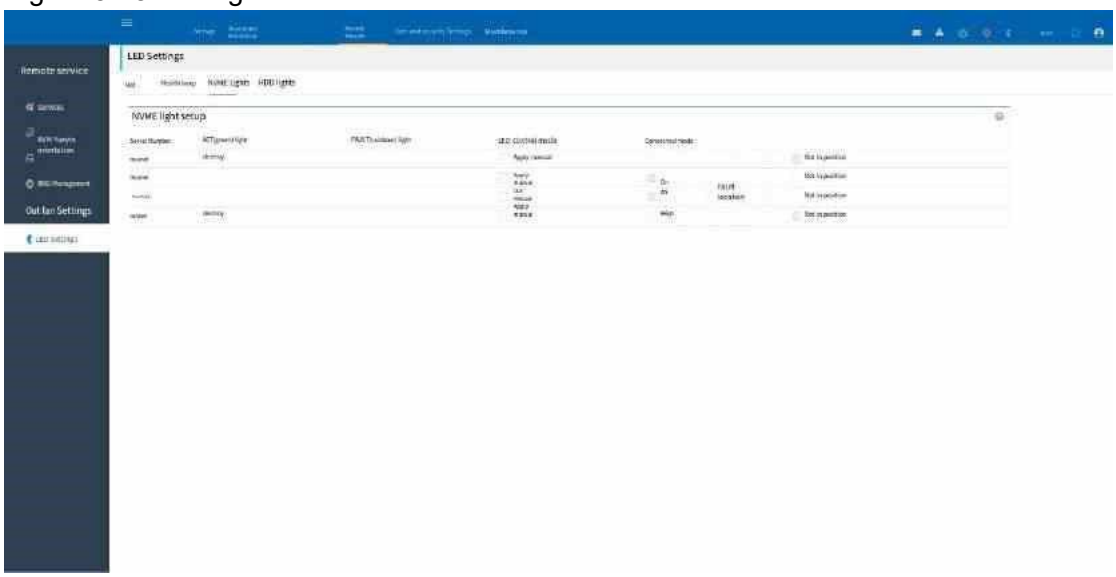


Figure 5-79 Setting an NVMe indicator

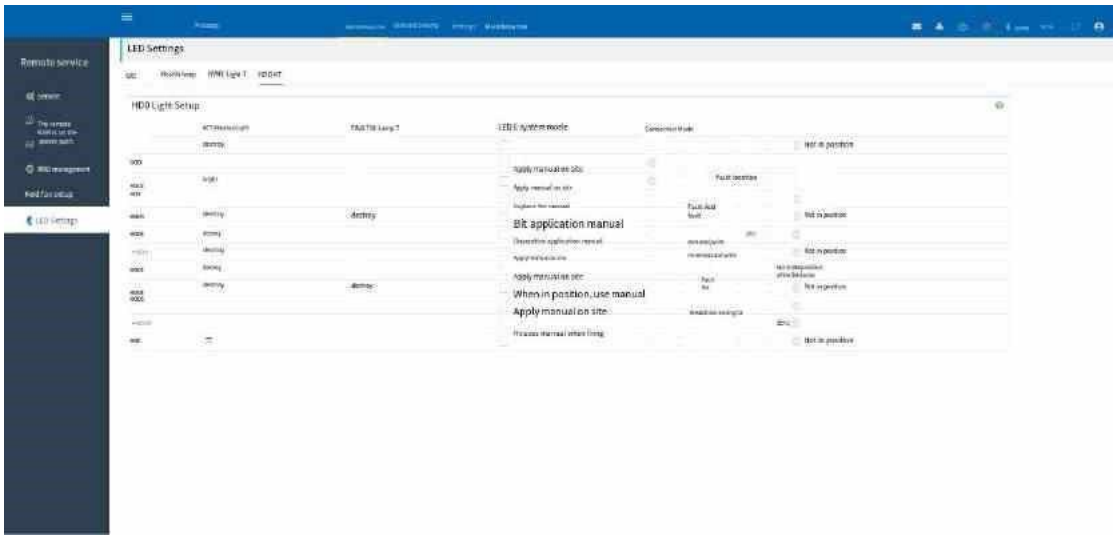


Figure 5-80 HDD indicator Settings

5.6.9 Users and Security

5.6.9.1 User Management

This page will list the permissions of all existing users and users as well as the number of failed attempts to set a password.

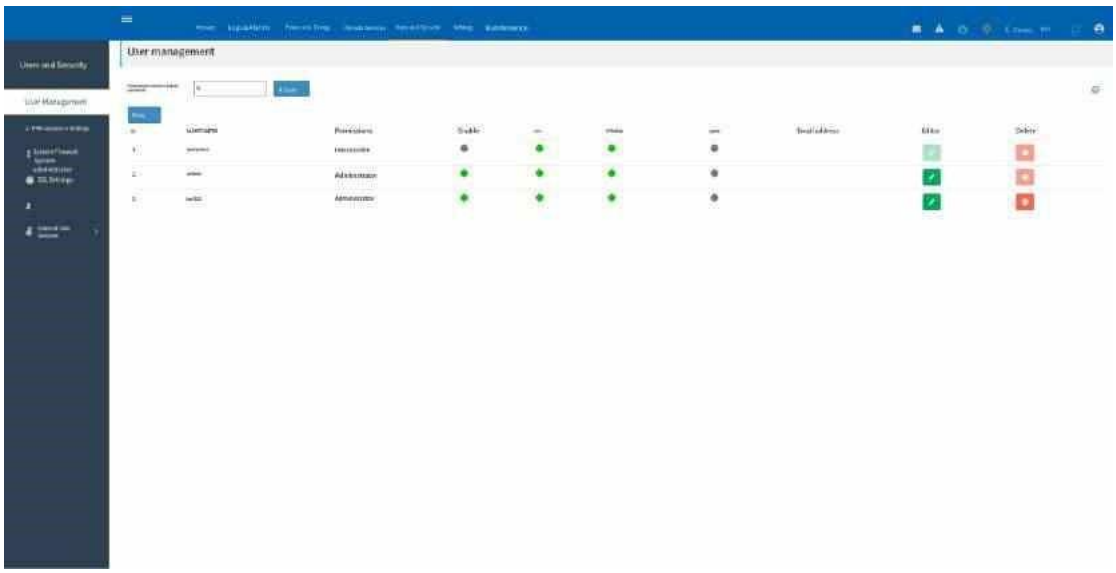


Figure 5-81 User Management

5.6.9.2 PAM Sequence Settings

This page is used to configure the PAM user authentication order to BMC. Shows the available PAM modules in the BMC support list. Click and drag and drop the PAM modules to change the order in which they are needed.

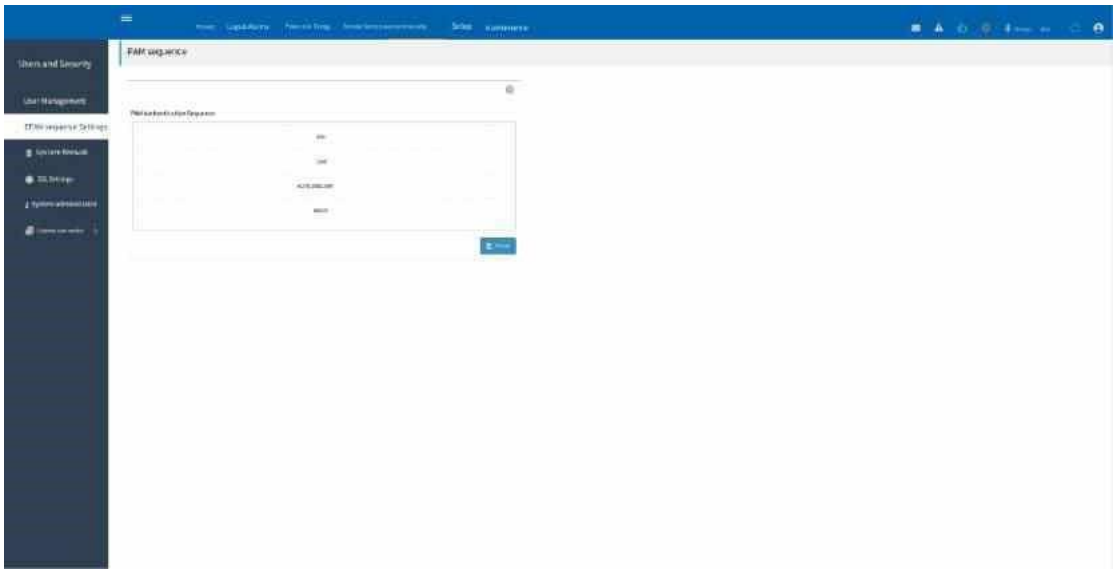


Figure 5-82 PAM sequence Settings

5.6.9.3 System Firewall

This page can be used to set the system firewall

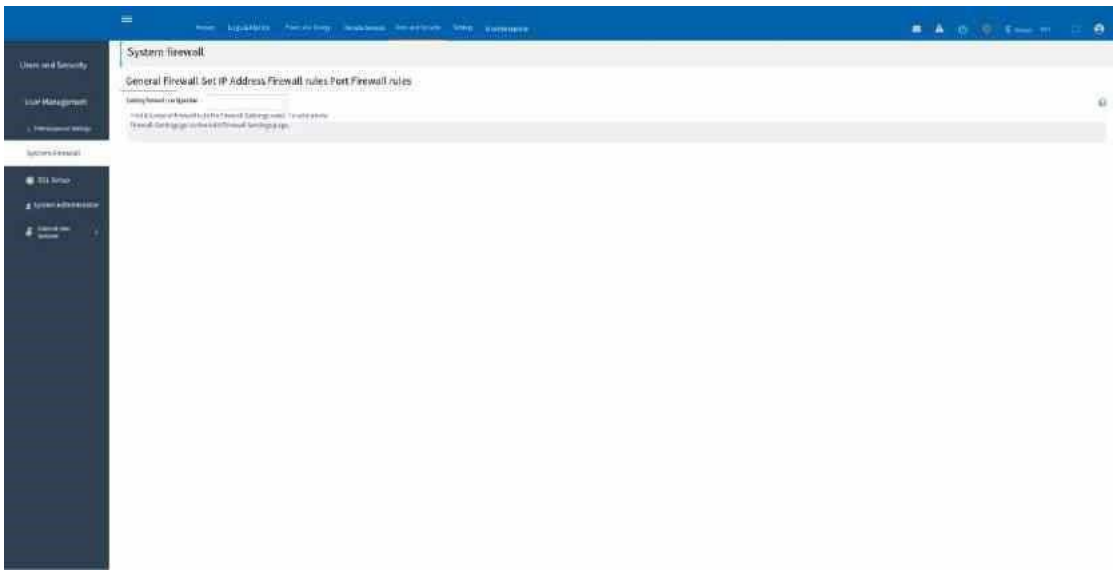


Figure 5-83 System firewall

General firewall: You can configure a general firewall to view existing firewalls and add firewall rules.

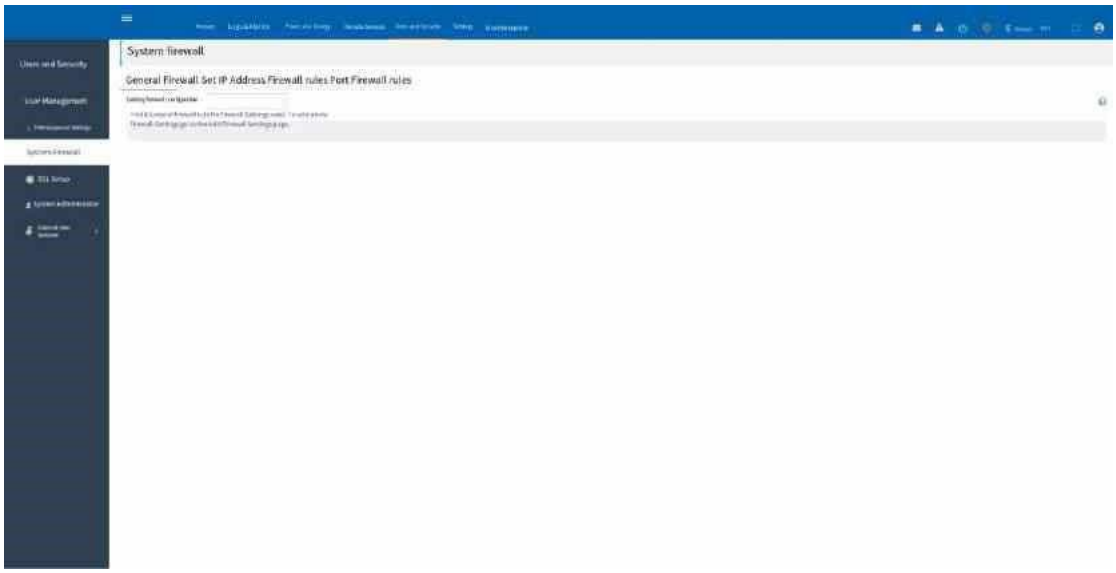


Figure 5-84 General Firewall Settings

Add Firewall Settings: Add a new general firewall setting

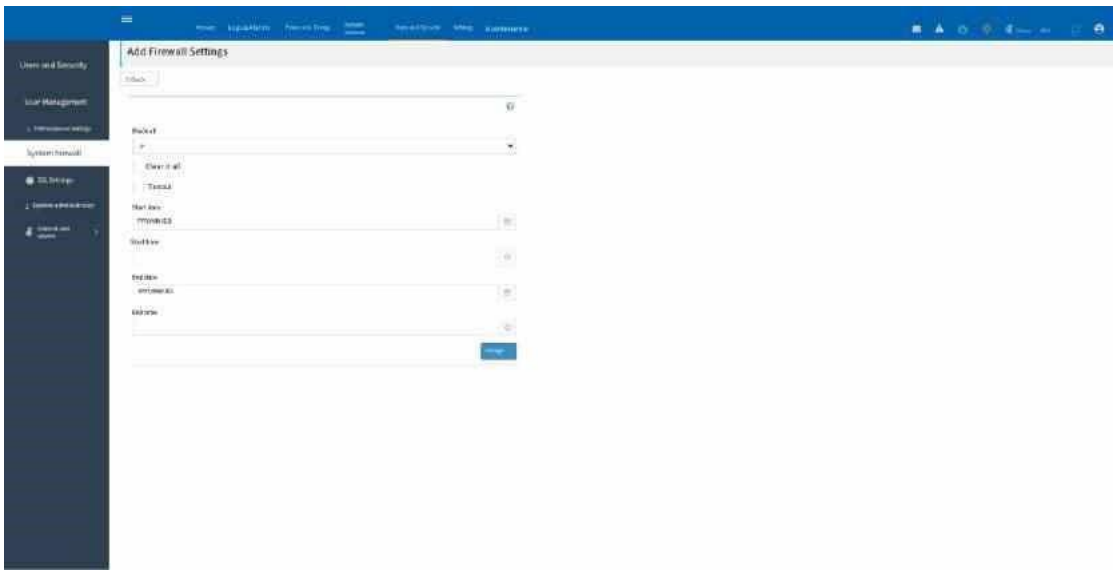


Figure 5-85 Add firewall Settings

IP Firewall Rules: Existing IP rules can be viewed, and buttons are provided to allow users to add IP rules.

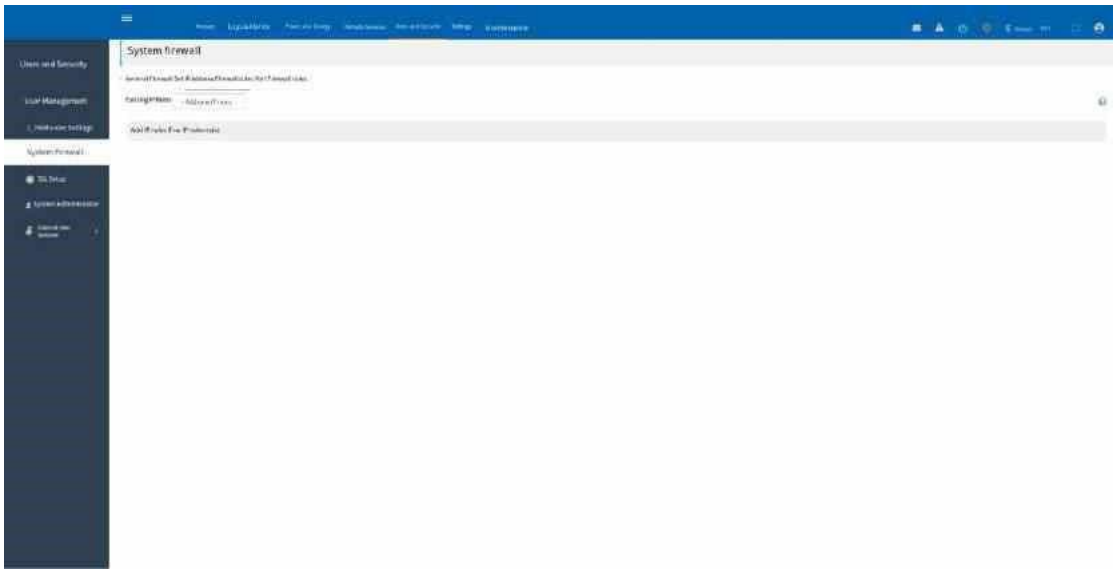


Figure 5-86IP firewall rule

Add IP Rule: Add a new IP firewall rule

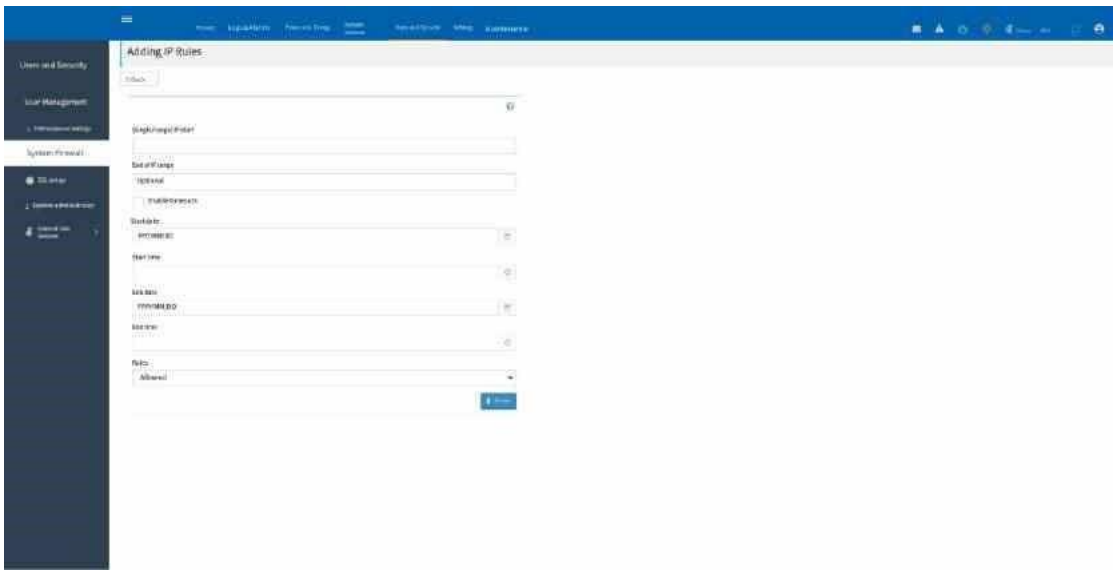


Figure 5-87 Add IP rule

Port firewall rule: You can view the current port rule and add a button to add a port rule.

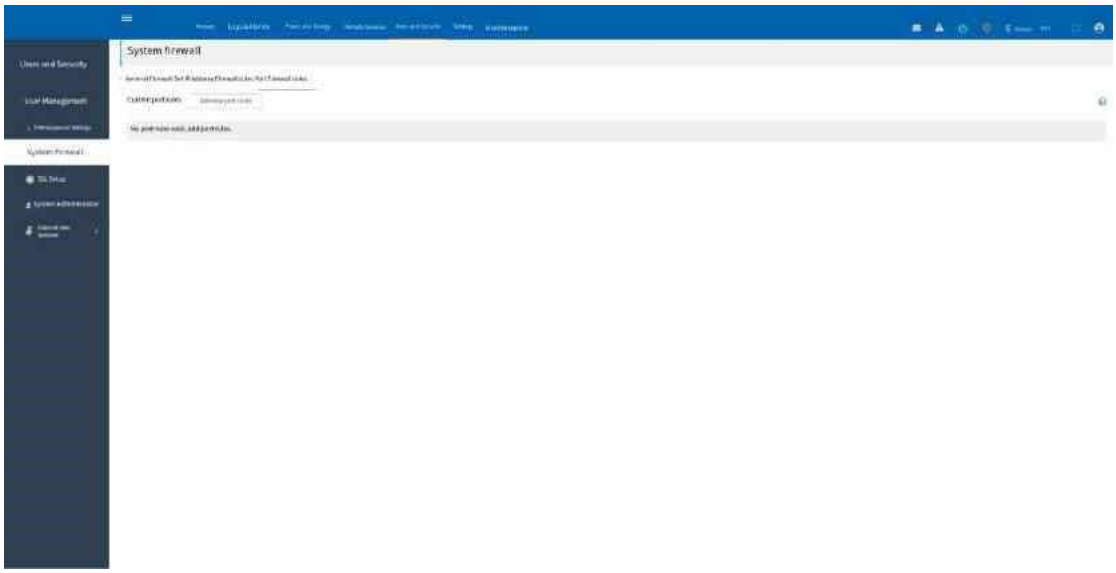


Figure 5-88 Port firewall rules

Add Port Rule: Add a new port firewall rule

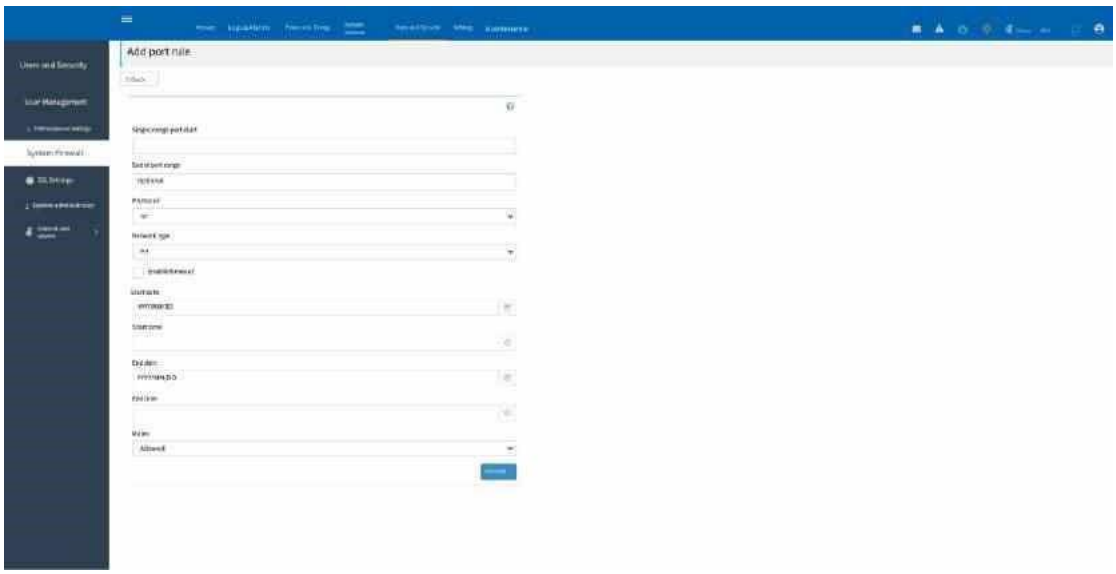


Figure 5-89 Add Port Rule

5.6.9.4 SSL Settings

SLL Settings can be made on this page. This includes viewing SSL certificates, generating SSL certificates, and uploading SSL certificates.

Viewing SSL Certificates: Displays basic information about uploading SSL certificates. It contains the version serial number, signature mechanism, and public key.

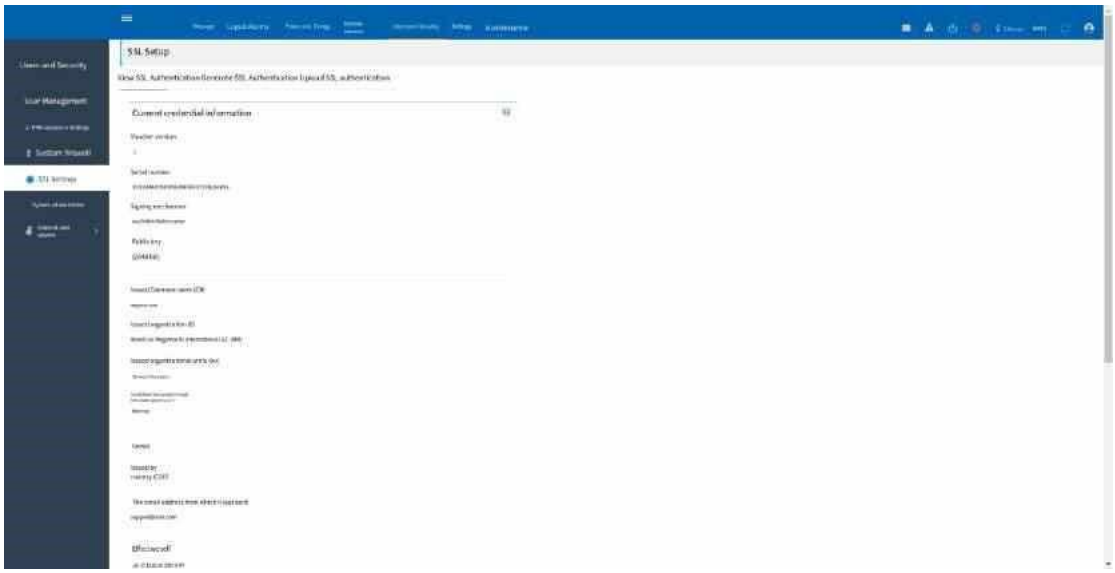


Figure 5-90SLL Settings - View SSL credentials

Generate SSL Certificate: Enter the information required for SSL to generate the SSL certificate.

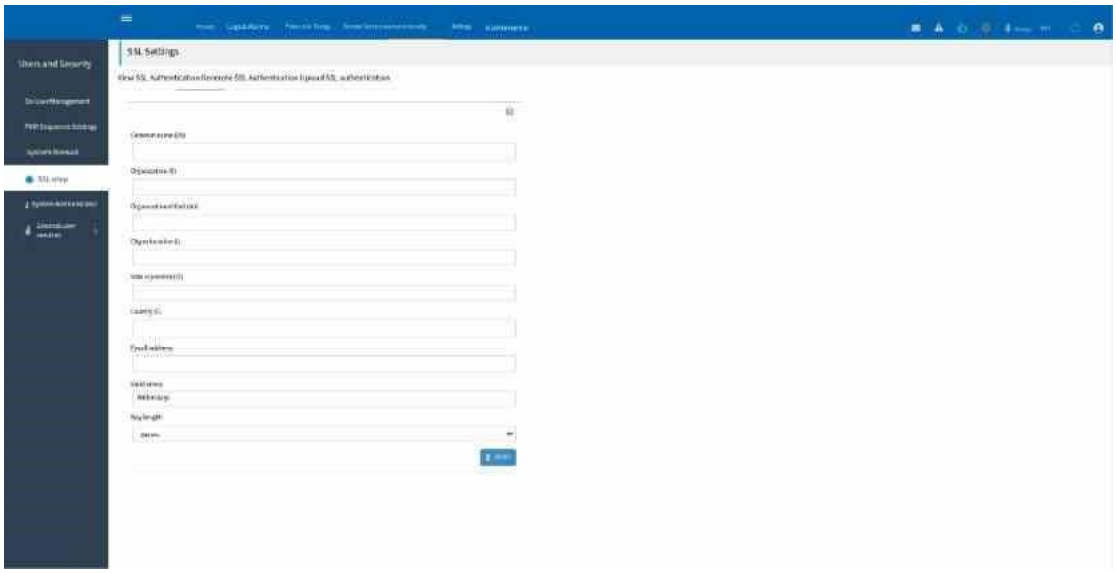


Figure 5-91 Generating an SSL certificate

Upload SSL authentication: Displays the current certificate and private key, and can upload a new certificate and private key.

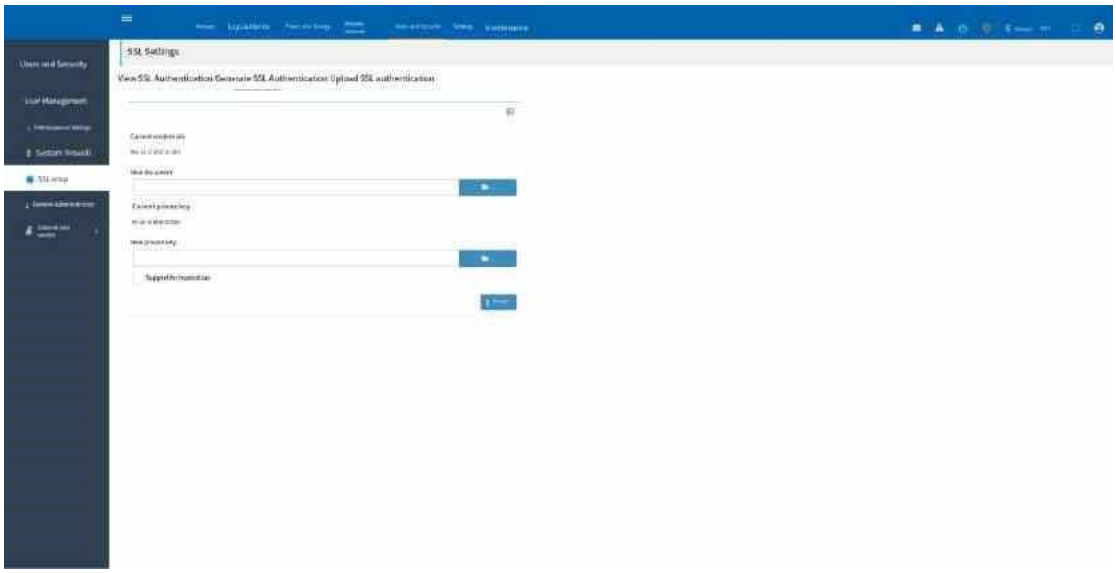


Figure 5 -92 Uploading SSL authentication

5.6.9.5. System Administrator

This page displays the information of the system administrator and supports changing the password of the system administrator.

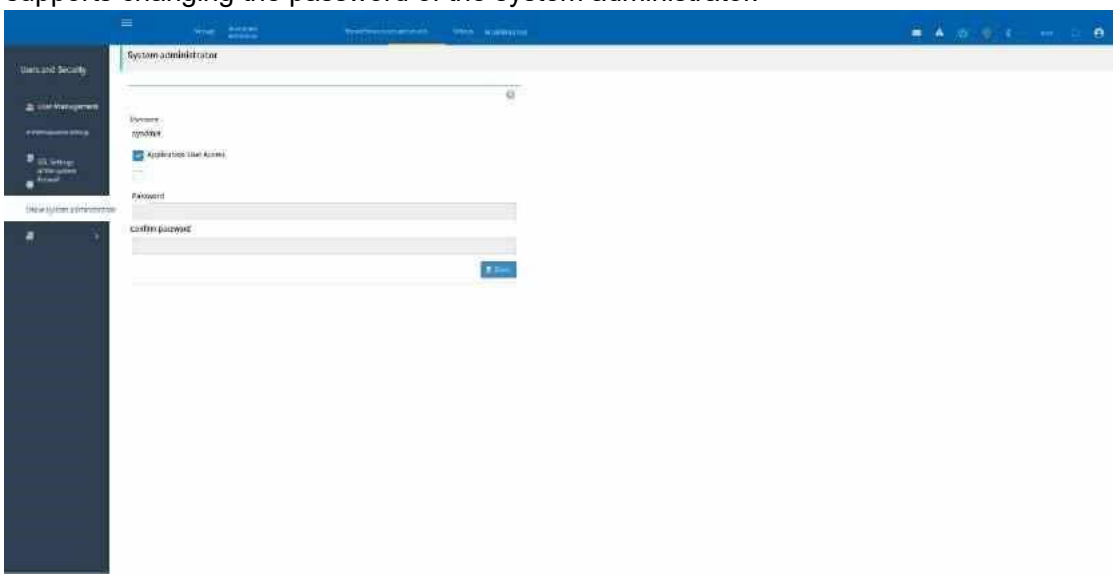


Figure 5-93 System administrators

Figure 5.6.9.6. External User Services

This page supports Settings for LDAP/E-directory, Active Directory and Radius

LDAP/E-Directory Settings: General LDAP Settings

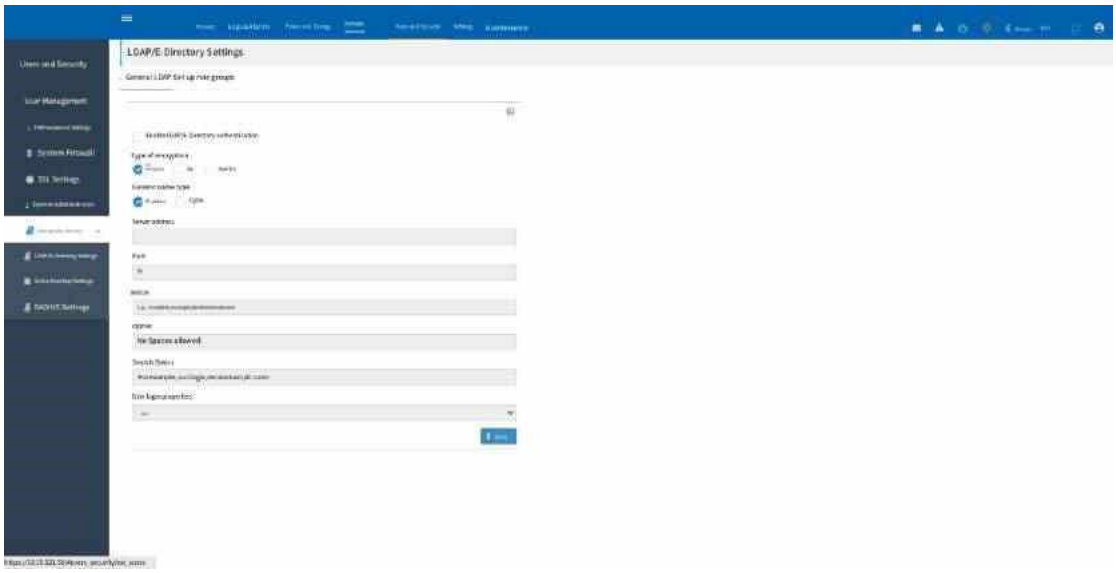


Figure 5-94 External User Services - LDAP/E-Directory Settings - General LDAP Settings

Role Groups:

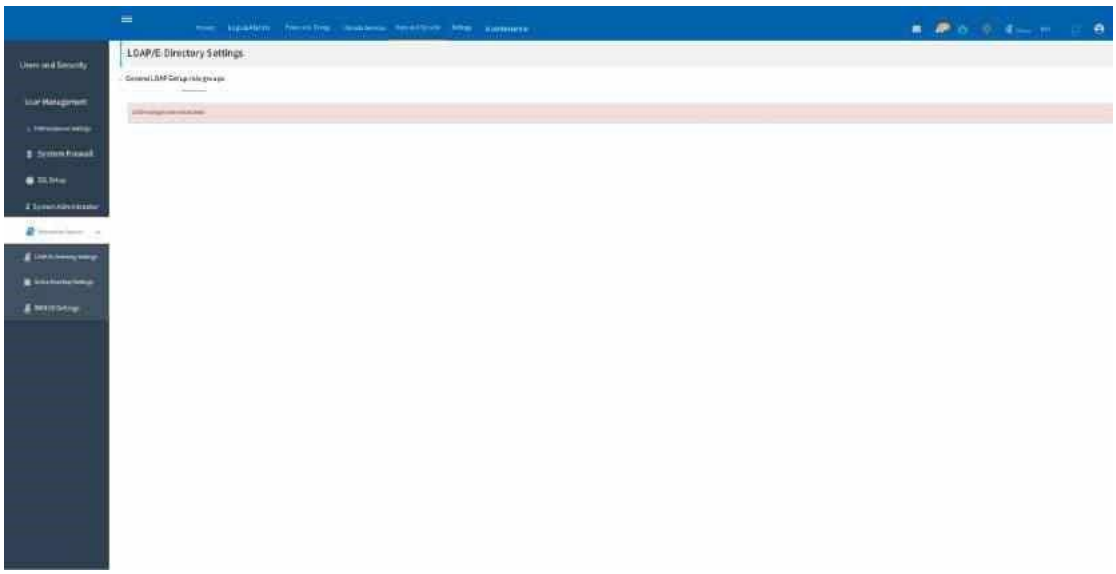


Figure 5-95 External User Services - LDAP/E-Directory Settings - Role groups

Active directory Settings: General Active directory Settings

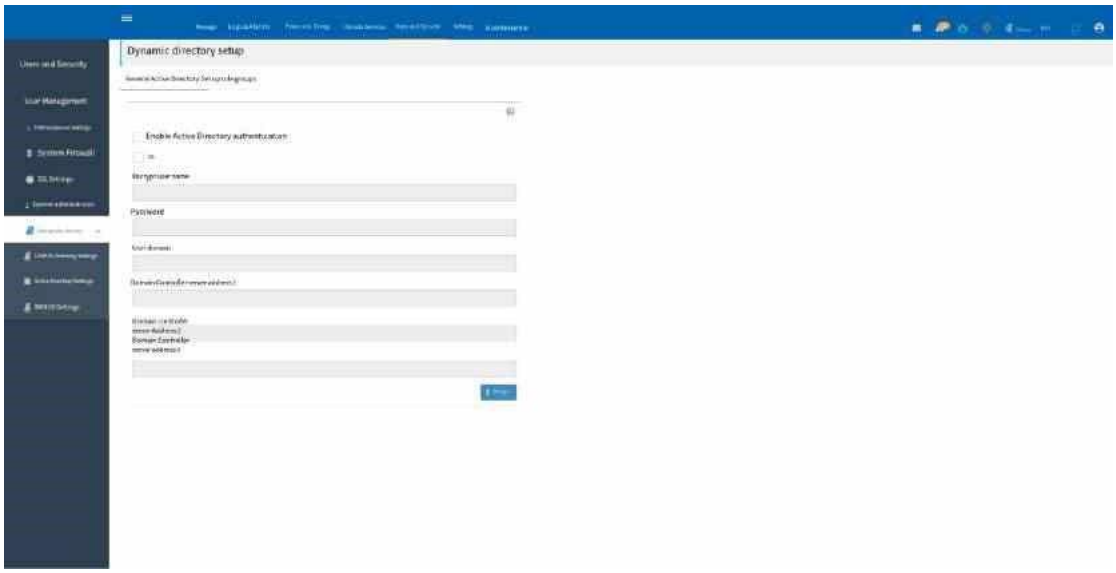


Figure 5-96 External User Services -Active Directory Settings - General Active Directory Settings Role Groups:

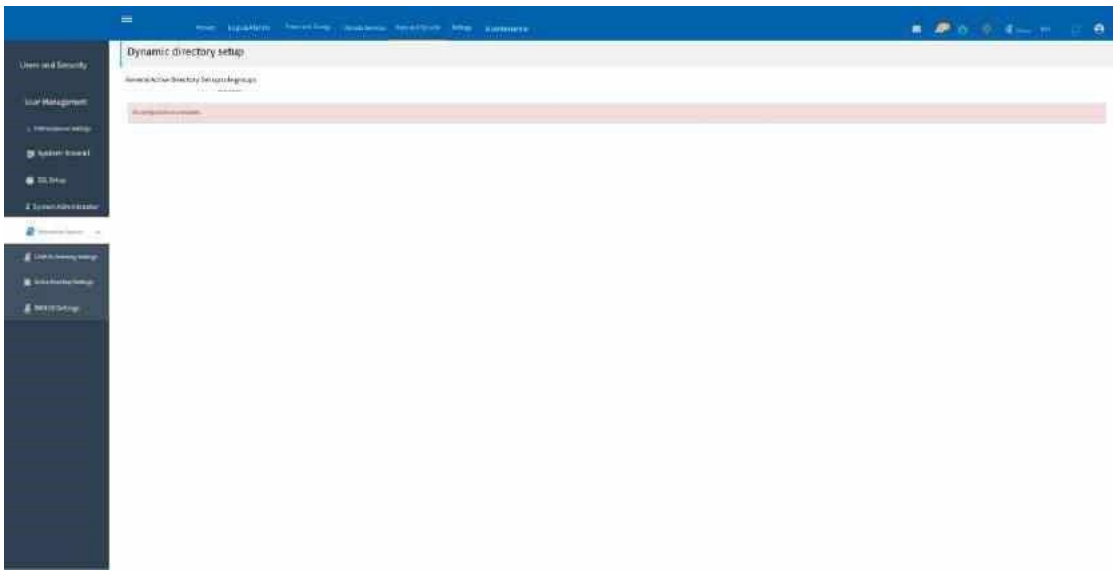


Figure 5-97 External User Services -Active Directory Settings - Role groups

RADIUS Settings: General RADIUS Settings

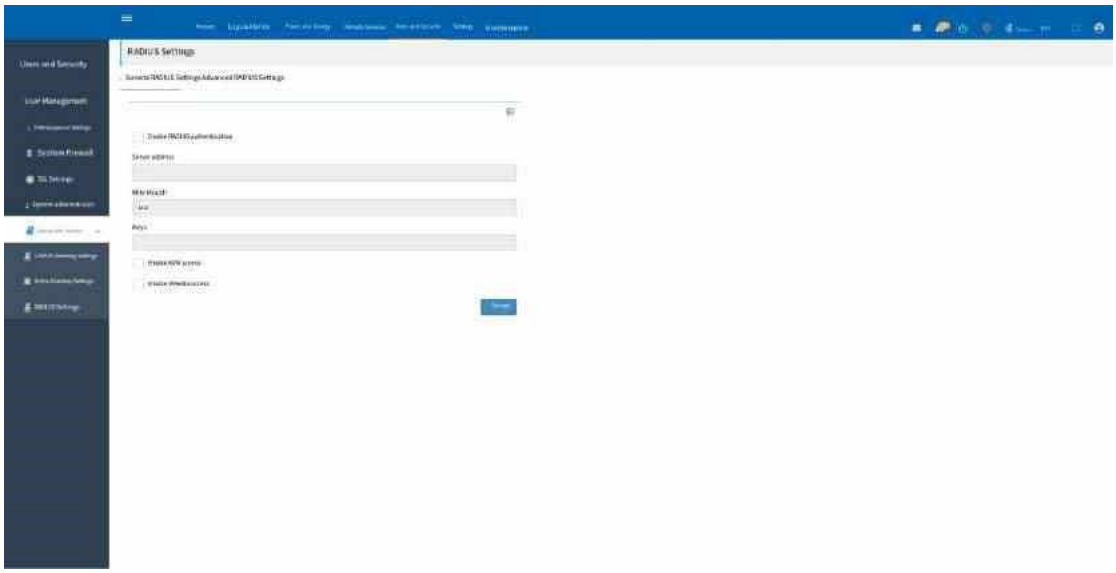


Figure 5-98 External User Services -RADIUS Settings - General RADIUS Settings Advanced RADIUS Settings:

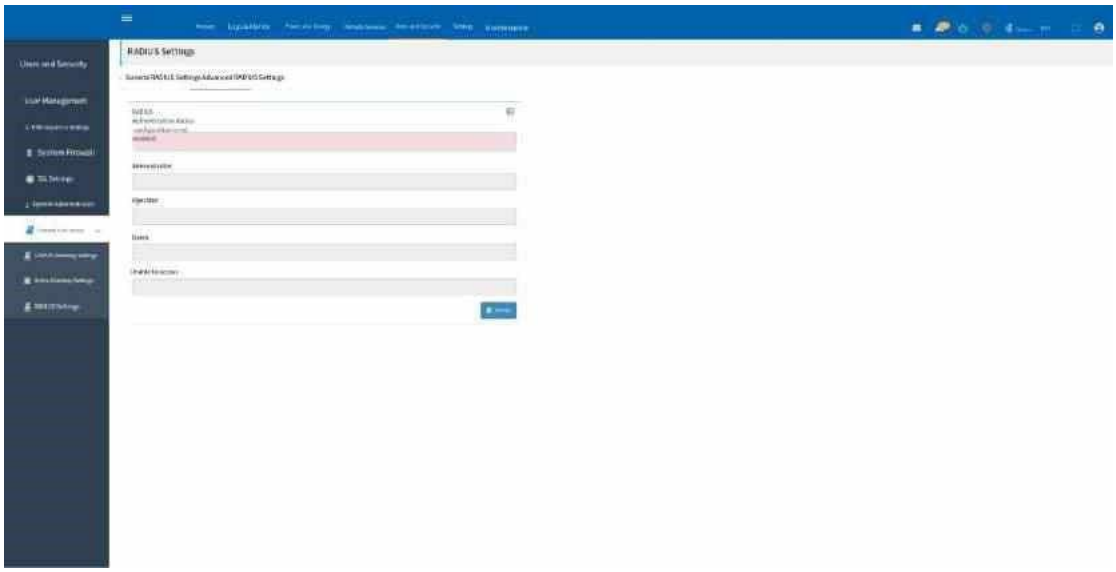


Figure 5-99 External User Services -RADIUS Settings - Advanced RADIUS Settings

5.6.10 Settings

5.6.10.1, Date & Time

This page is used to set the date & time on BMC. You can select a point on the map to configure the time zone. In other boxes, you can configure the time, NTP server, and time synchronization method.

Points to note:

When the NTP service is enabled but the BMC fails to synchronize time from the NTP server, the BMC synchronizes time from the BIOS during the BIOS restart.

When the NTP service is disabled, the BMC synchronizes time from the BIOS during the BIOS restart.

In the preceding two scenarios, if the BIOS time is longer than the BMC time and the time difference exceeds the remaining valid session time, the BMC sessions will be logged out after the time is synchronized from the BIOS. The current Web session, KVM session, and ssh session will be logged out. If the time difference is smaller than the remaining valid session time, the session is not logged out.

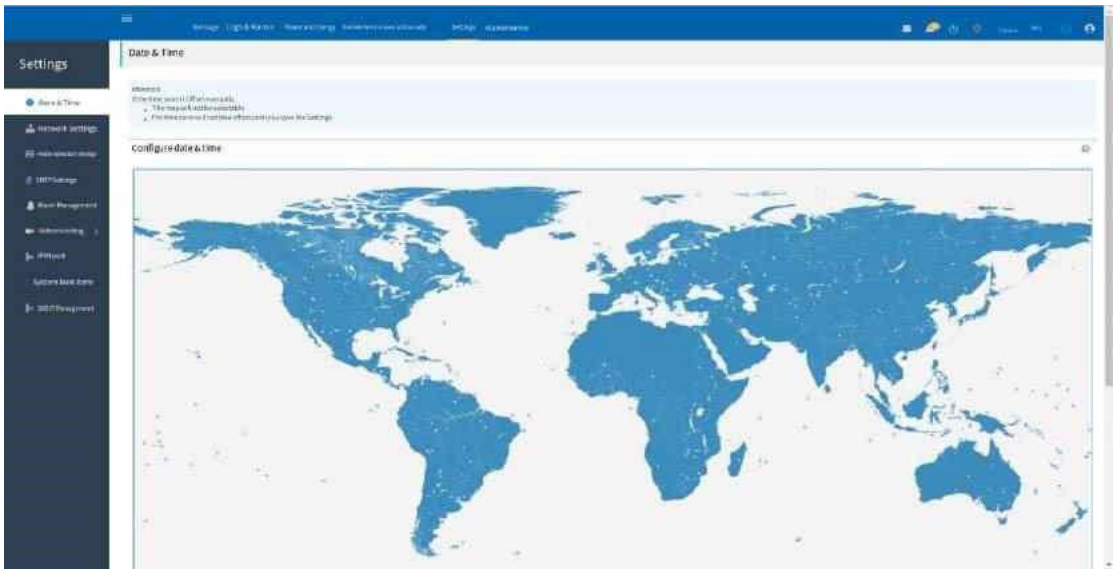


Figure 5-100 Settings - Date & Time

5.6.10.2, Network Settings

This page includes network IP Settings, network binding configuration, network link configuration, DNS configuration and NC-SI configuration.

Network IP Settings: This page allows you to configure the network parameters of BMC

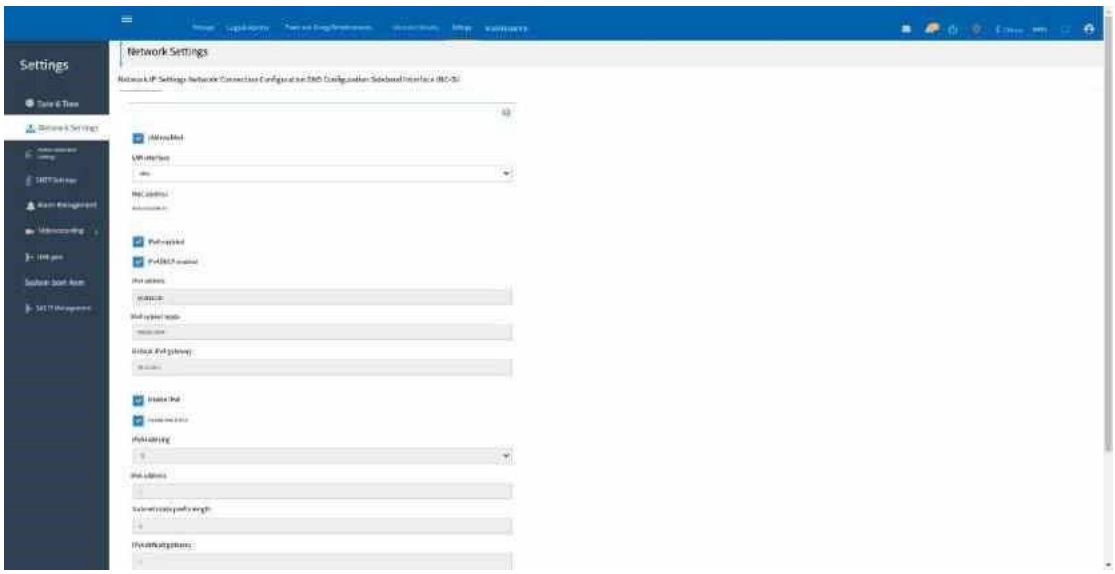


Figure 5-101 Network Settings - Set the network IP address

Network Connection Configuration: This page allows you to configure the working mode of the network port

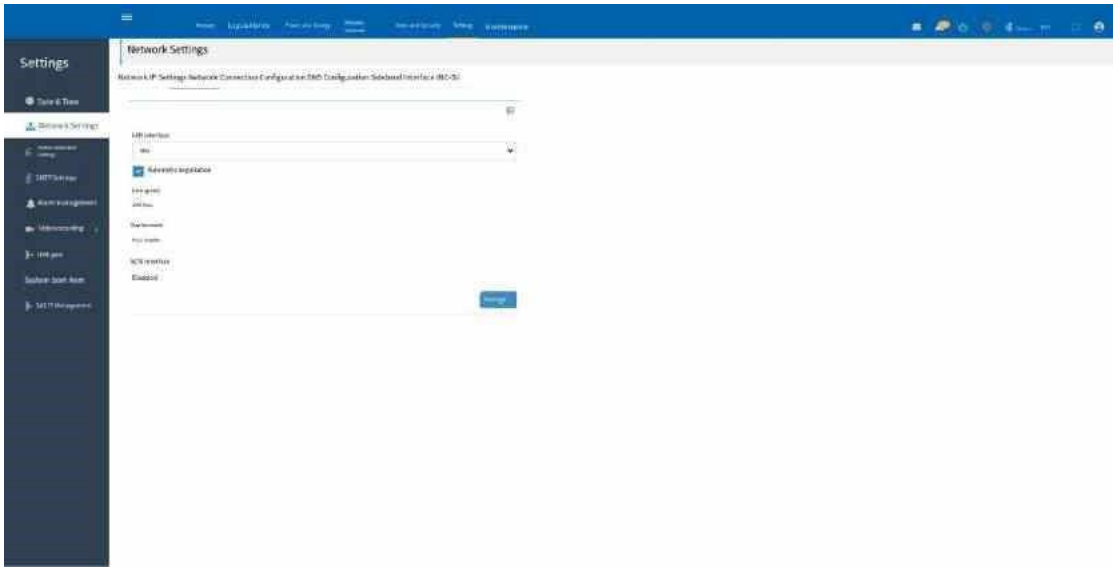


Figure 5-102 Network Settings - Network Connection Settings

DNS Configuration: This page allows you to configure the server DNS

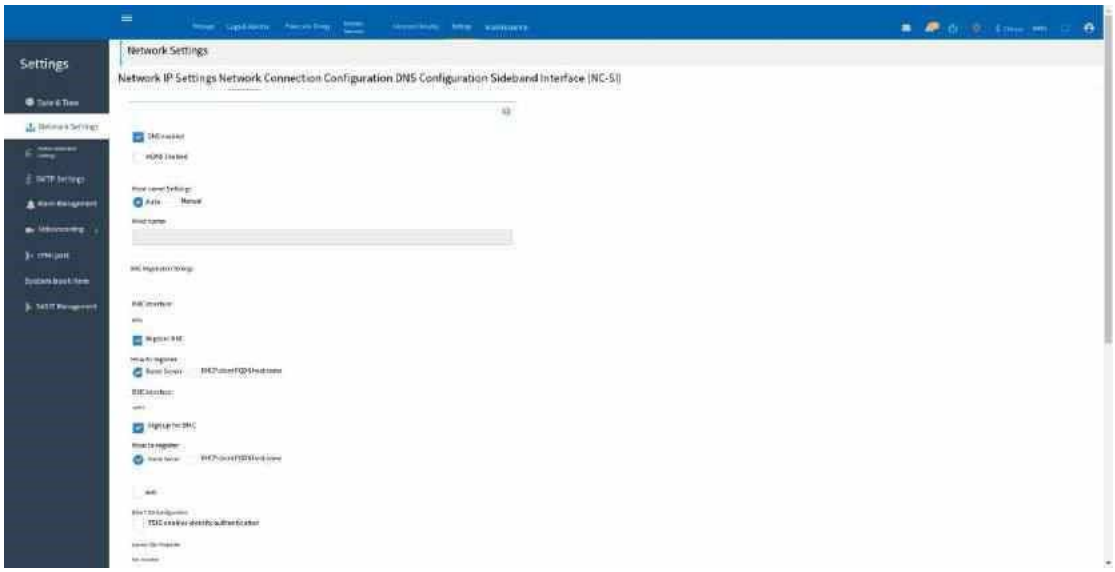


Figure 5-103 Network Settings -DNS configuration

Sideband Interface: This page can select the mode configuration of NCSI

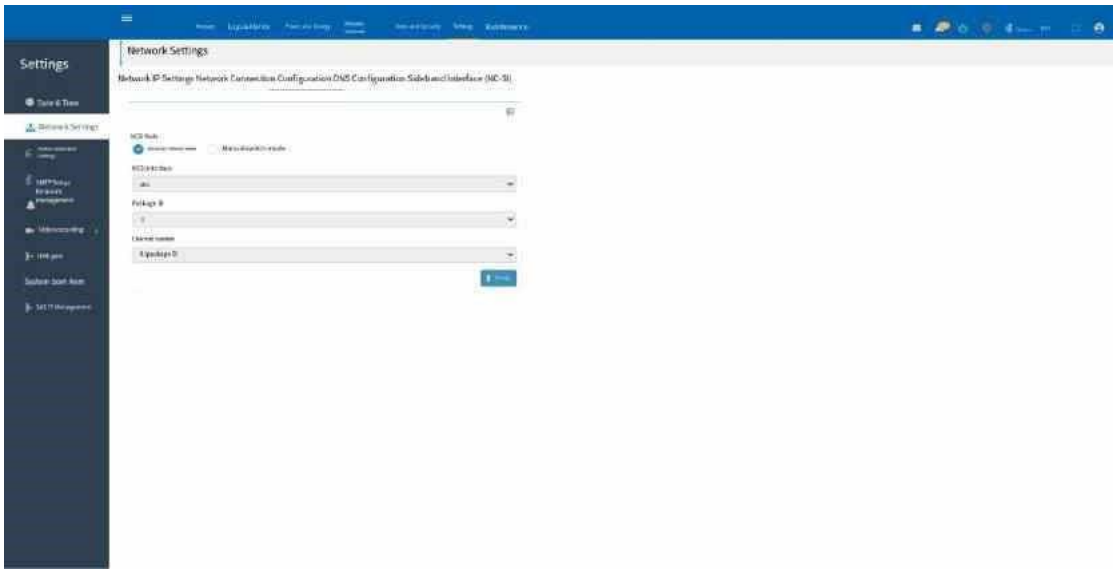


Figure 5-104 Network Settings -NCSI configuration

5.6.10.3. Media Redirection Settings

This page can configure server remote mirroring.

General Settings: Remote Media support and local media support can be enabled/disabled on the page by selecting/unselecting. If selected, the corresponding remote media type will be displayed (CD/DVD, hard disk). When selecting a different media type, its corresponding configuration will be displayed.

Users can configure different Settings for different remote media types.

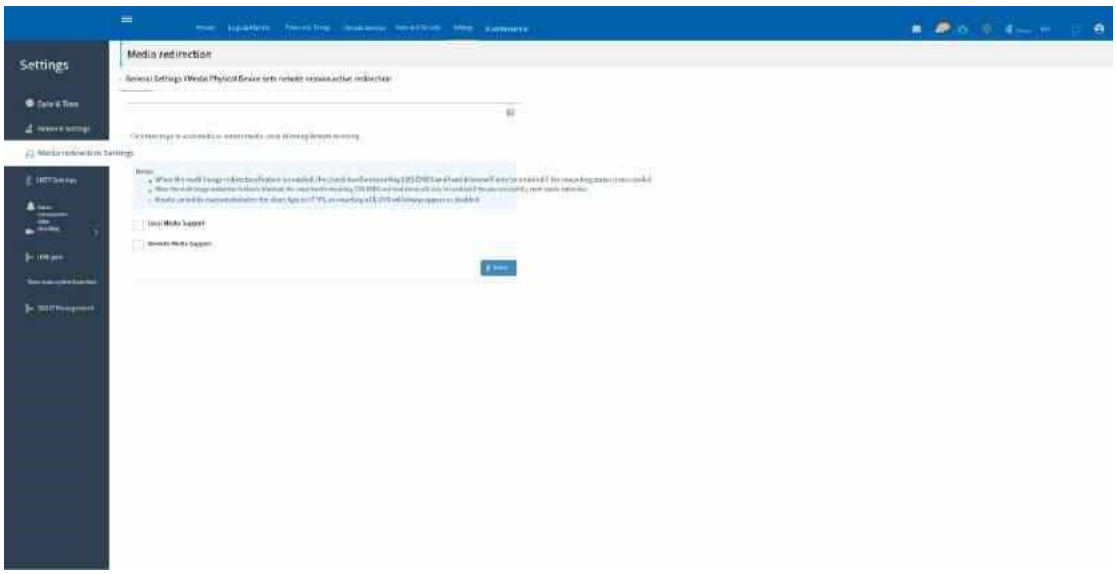


Figure 5-105 Media Redirection Settings - General Settings

VMedia Physical Device Settings: This page configures Flobby, CD/DVD, number of devices supported by virtual media redirection, and the physical device corresponding to remote KVM HD.

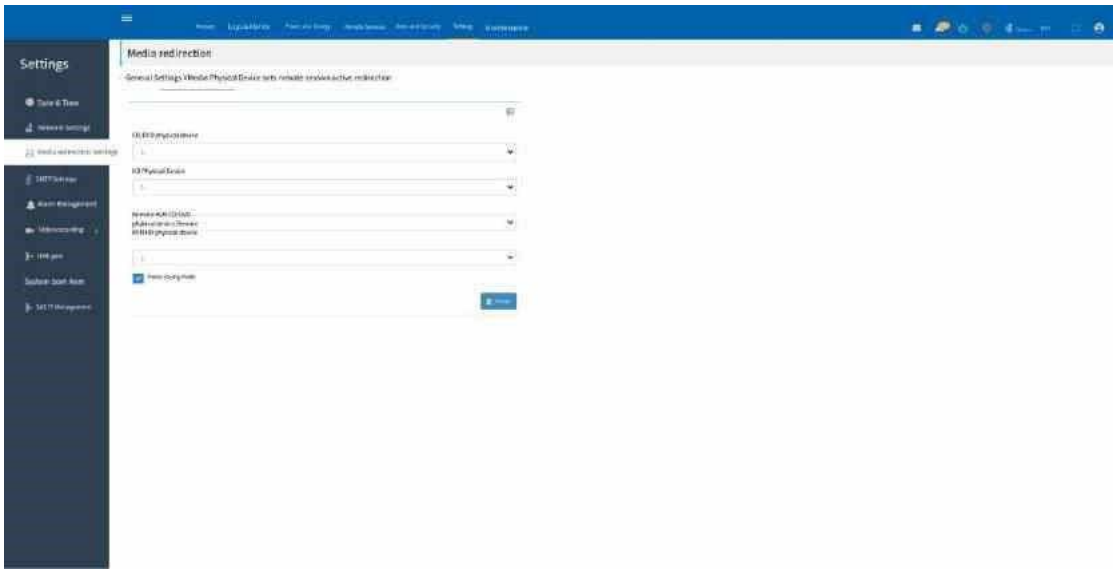


Figure 5-106 Media Redirection Settings -VMedia physical Device Settings Remote Session:

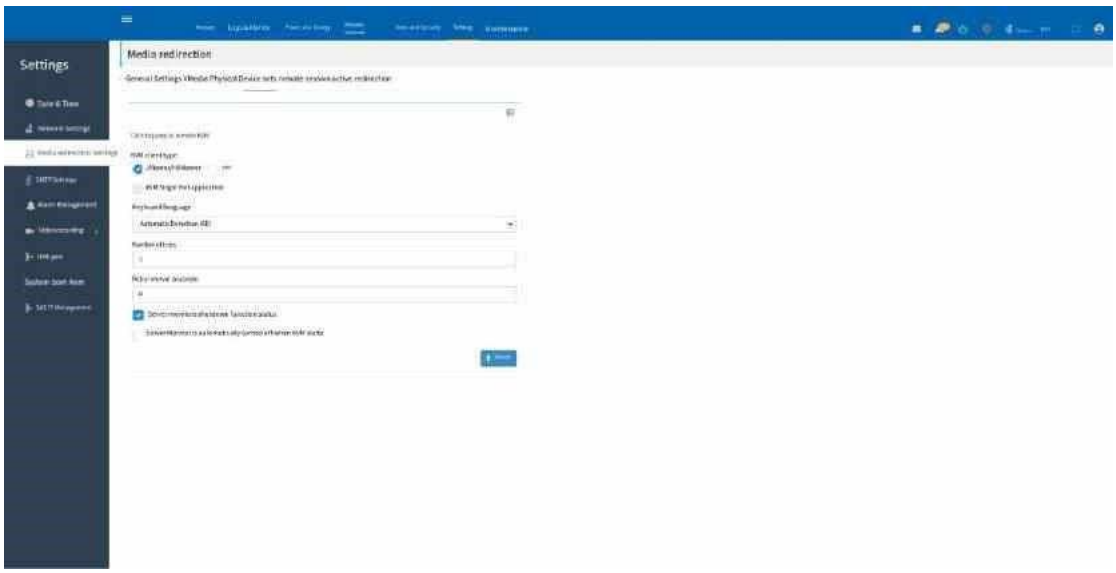


Figure 5-107 Media Redirection Settings - Remote session Active redirection:

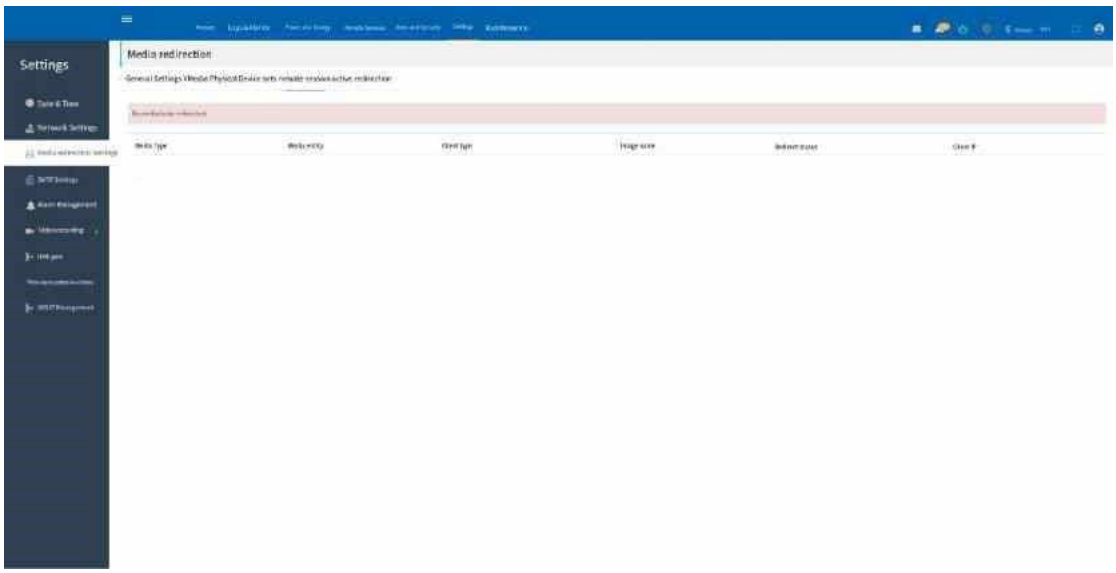


Figure 5-108 Media redirection Setti ngs - Active redirection

5.6.10.4. SMTP Settings

This page is used to set SMTP. If you have any questions about the specific setting, please refer to the help information.

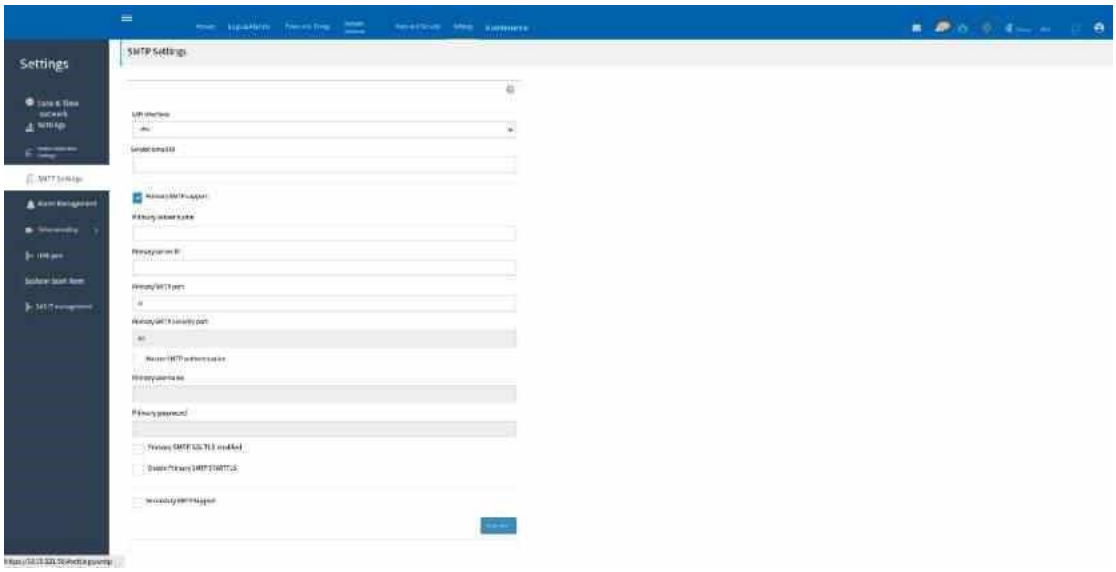


Figure 5-109 Settings -SMTP

5.6.10.5. Alarm Management

This page contains Trap message notifications, SNMP Settings and event filters.

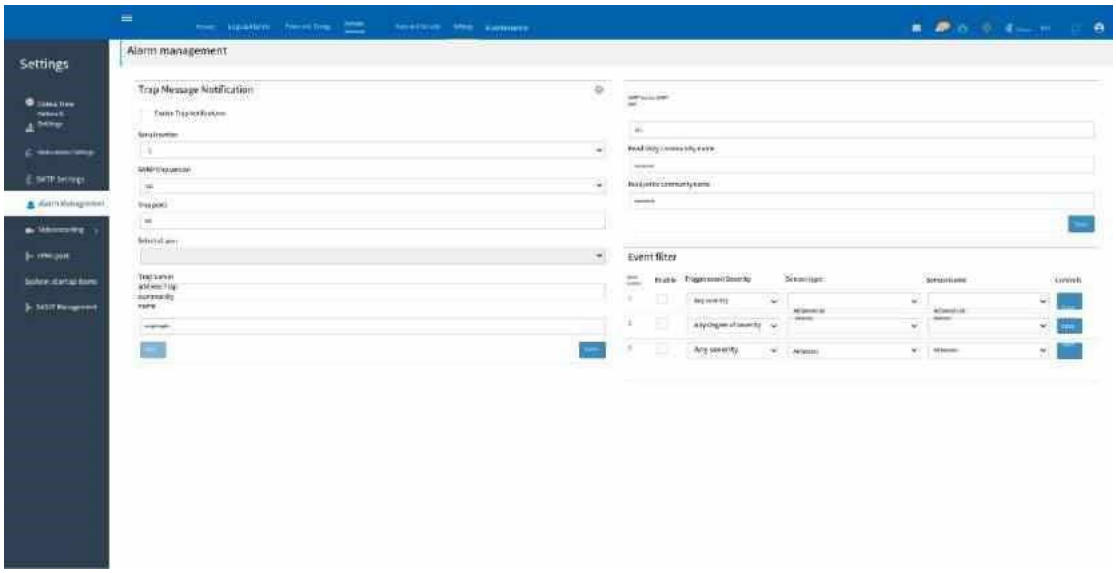


Figure 5-110 Alarm Management **5.6.10.6. Video Recording**

Video log: This page displays the available recorded video files

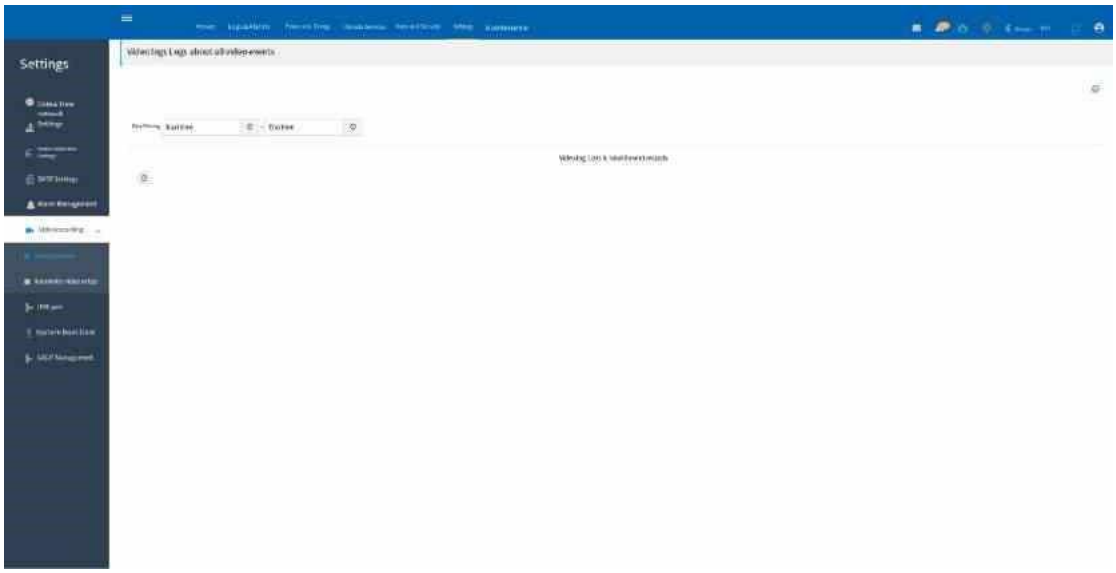


Figure 5-111 Video log

Automatic Video Settings: This page can be used to make automatic video Settings.

Video Trigger Settings: Can be selected/unselected to add or remove triggers for your system.

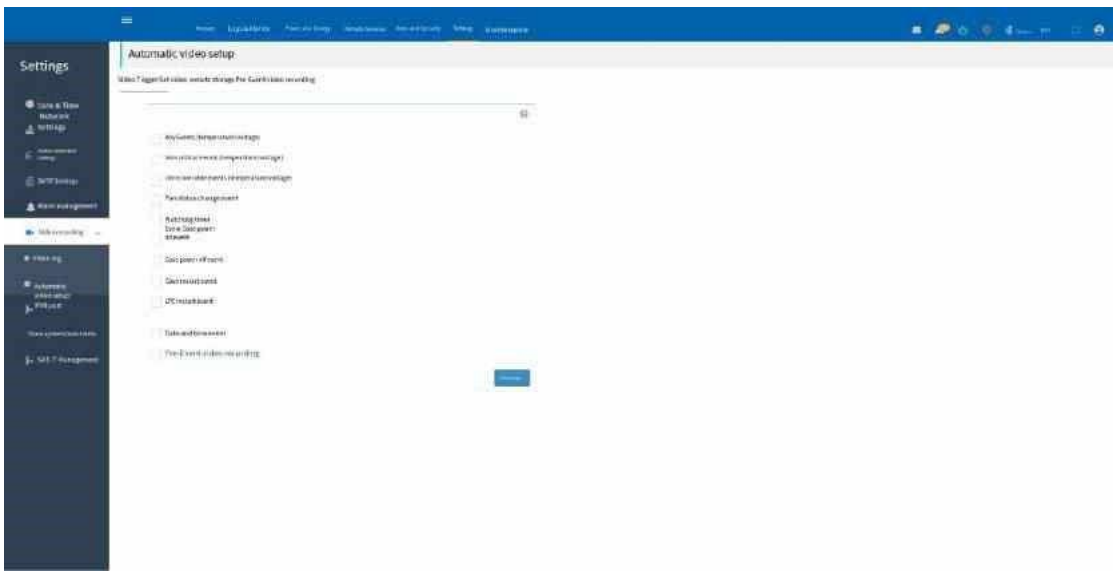


Figure 5-112 Automatic Video Settings - Video trigger Settings

Video Remote Storage: Enable/disable remote video support by selecting/not selecting.

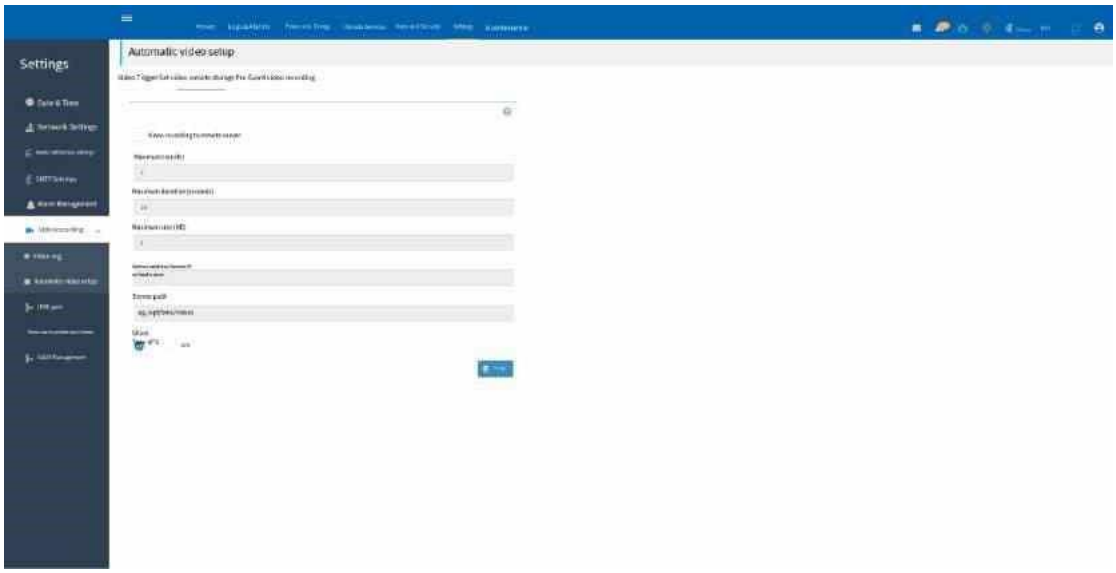


Figure 5-113 Automatic Video Settings - Video Remote Storage Pre-Event Video recording: This page is used to set Pre-Event video recording configurations. Pre-Event video recording is disabled by default. To enable PreEvent video recording, set Trigger video recording on the Trigger Configuration page.

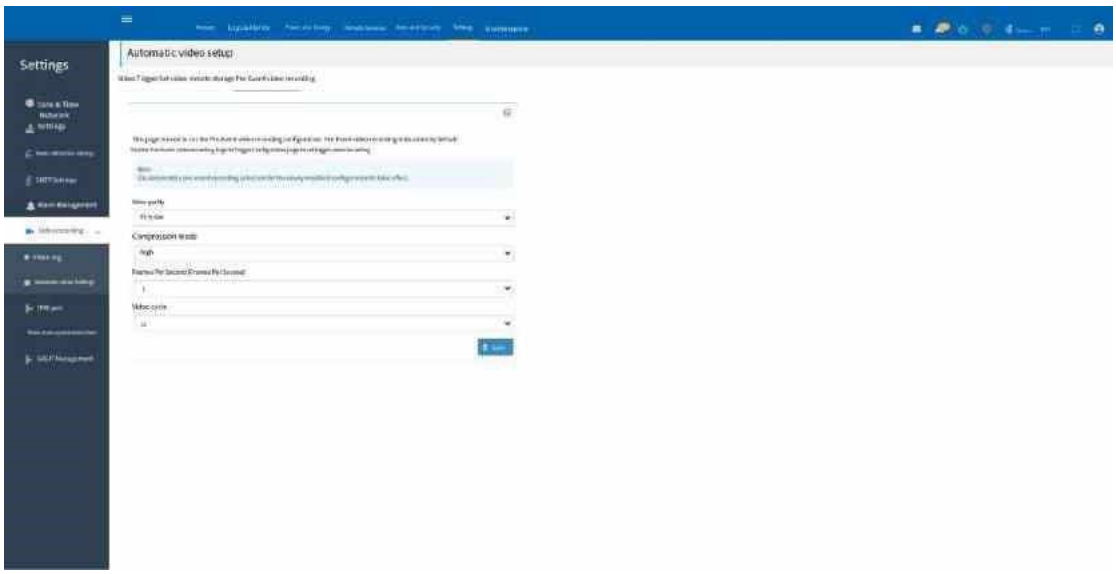


Figure 5-114 Automatic video Settings -Pre-Event Video record

5.6.10.7 IPMI interface

This page is used to configure the IPMI interface

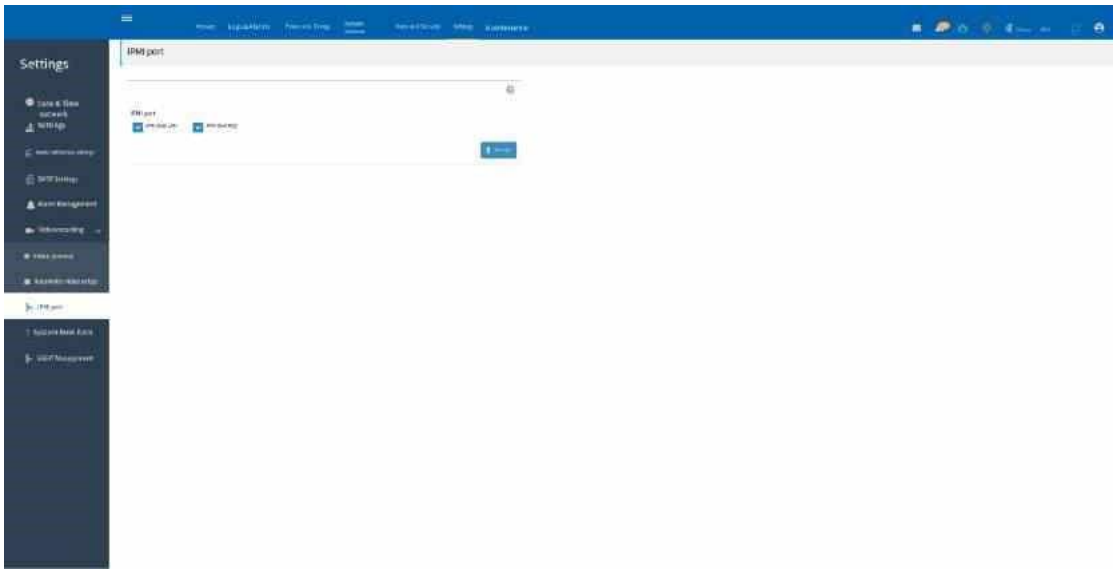


Figure 5-115 IPMI interface 5.6.10.8 System Boot Option

This page shows and configures the system boot sequence

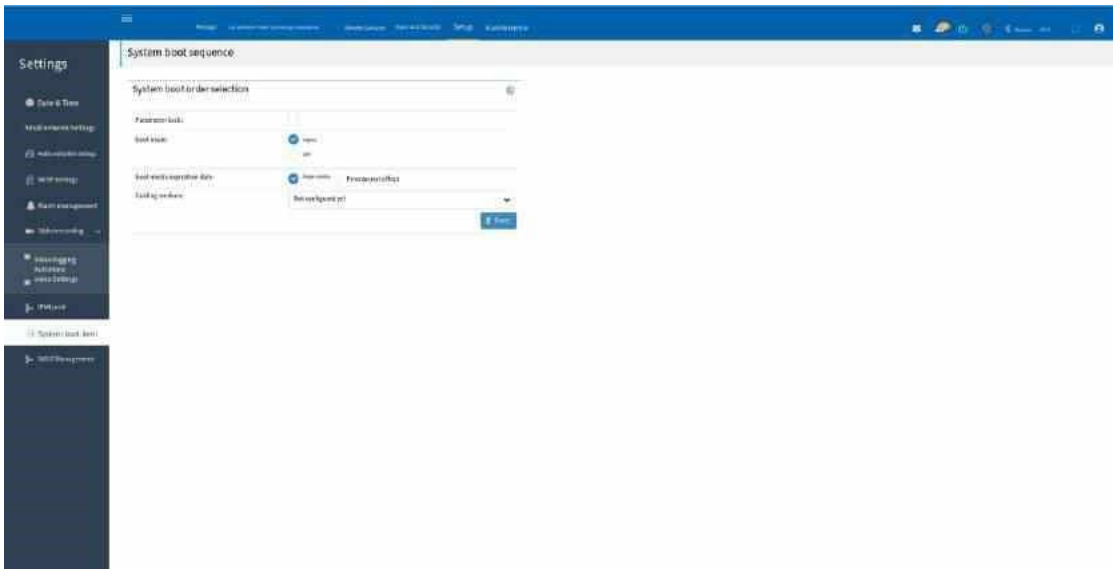


Figure 5-116 System boot options

5.6.10.9 SAS IT Management

The SAS IT control management page contains SAS IT controller information, physical device information, topology information, event logs, and SAS IT chassis information.

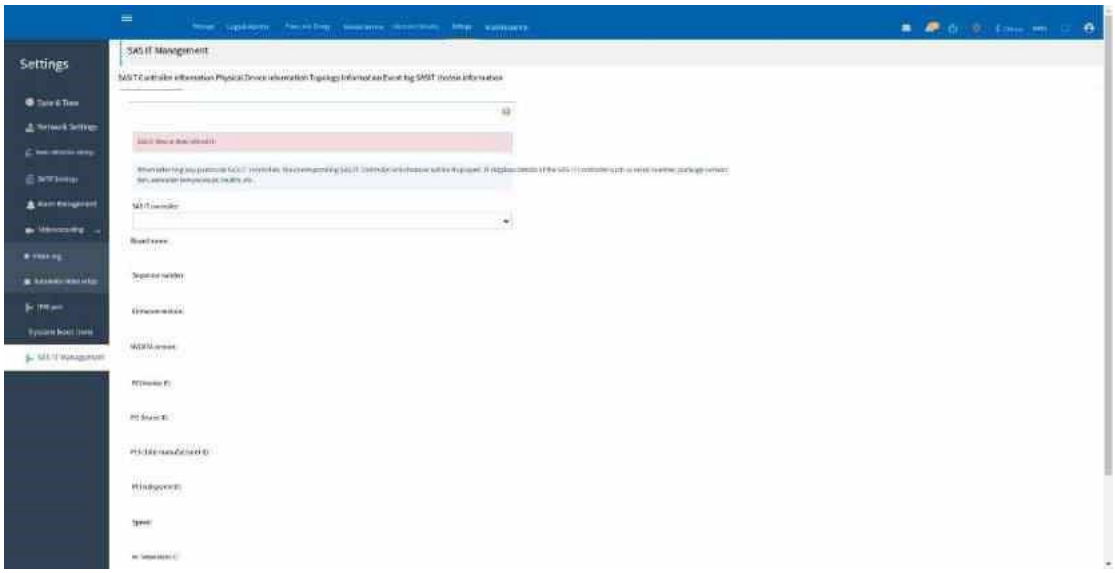


Figure 5-117 SAS IT management page

5.6.11 Maintenance

5.6.11.1 Configuration Update

Configuration Update: This page includes backing up configuration, restoring configuration, and saving configuration.

Backup configuration: Save the BMC configuration in a file by clicking on the corresponding module and clicking on Download Configuration (the file is used to restore the configuration).

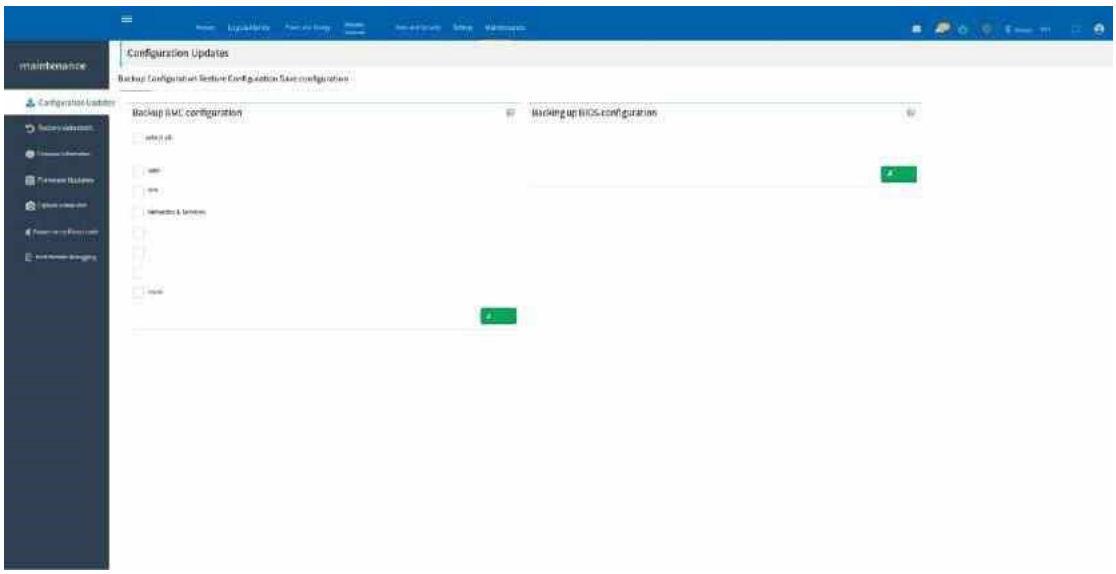


Figure 5-118 Configuration Update - Back up configuration

Restore configuration: You can use the previously saved configuration file to change the BMC configuration. Use the search button to select the profile you want to restore.

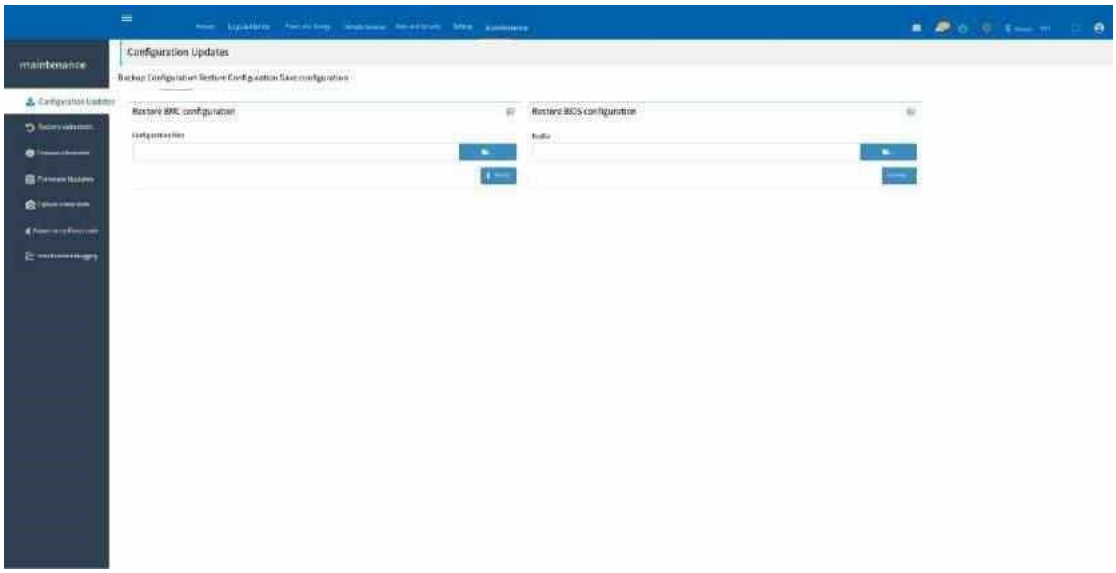


Figure 5-119 Configuration Update - Restore configuration

Save the configuration: Check the configuration that you want to save when restoring the configuration. The checked content in this section will be reserved by the BMC when performing operations such as updating the firmware or restoring factory Settings.

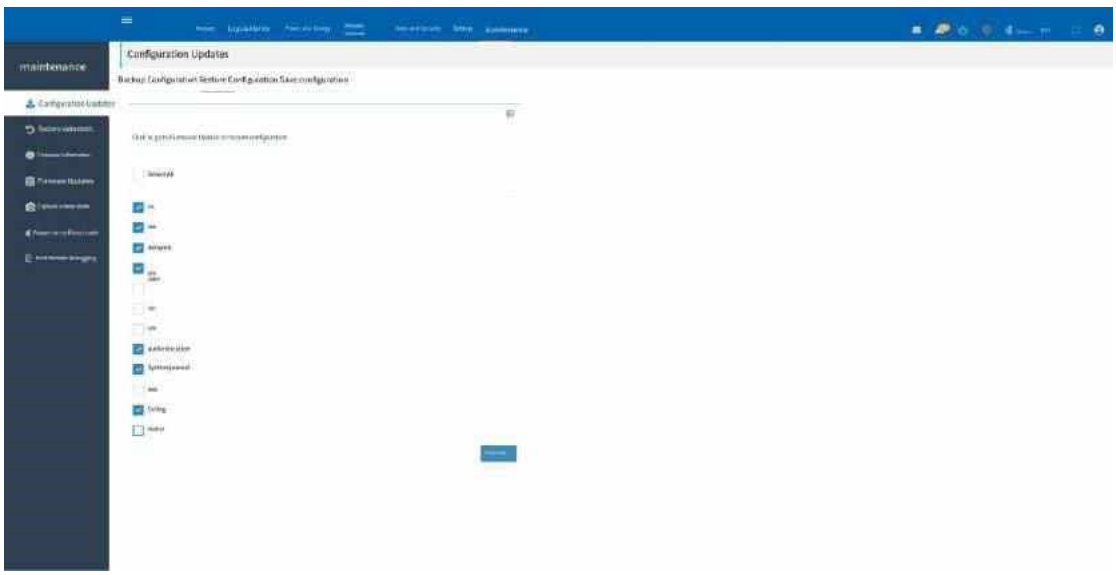


Figure 5-120 Configuration Update - Save the configuration

5.6.11.2 restore factory Settings

Change all BMC Settings to factory default Settings (If you need to retain some functions, please go to the Save configuration page and select the configuration items that need to be retained. This part will not be processed when the BMC is

restored to factory Settings.) Restoring the configuration will restart the device.

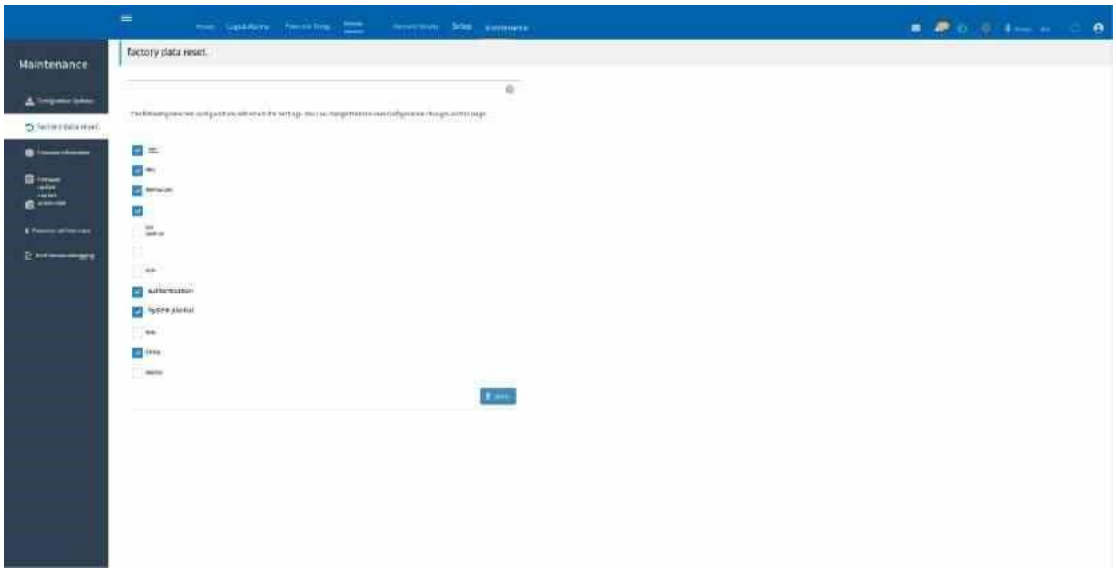


Figure 5-121 Restoring factory Settings

5.6.11.3. Firmware Info

Firmware Information: This page displays firmware information in action, including BMC build date compile time and firmware version.

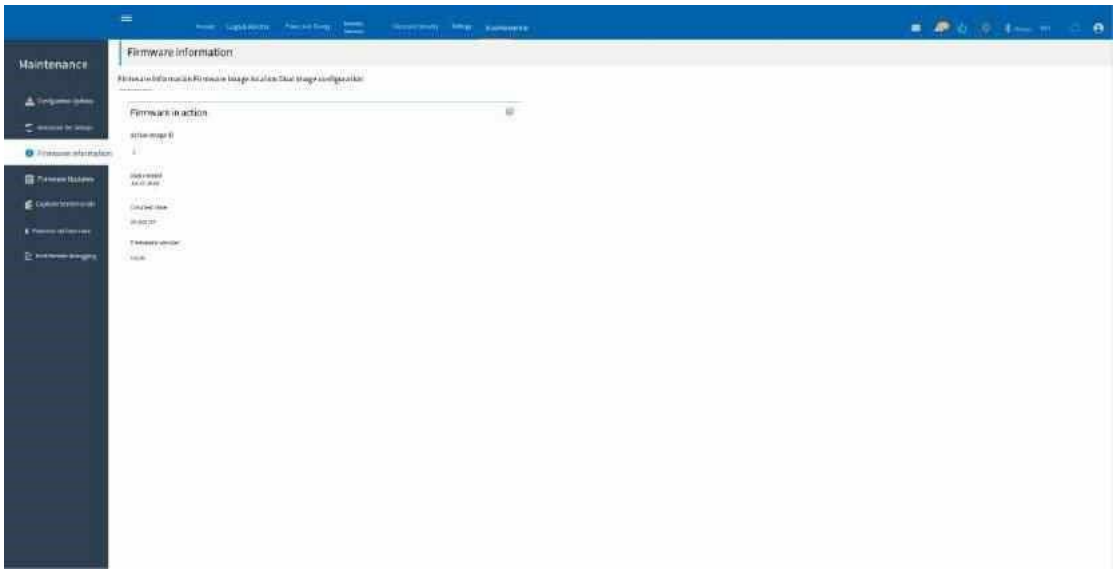


Figure 5-122 Firmware information

Firmware image Location: Protocol for transferring the firmware image to the BMC in use.

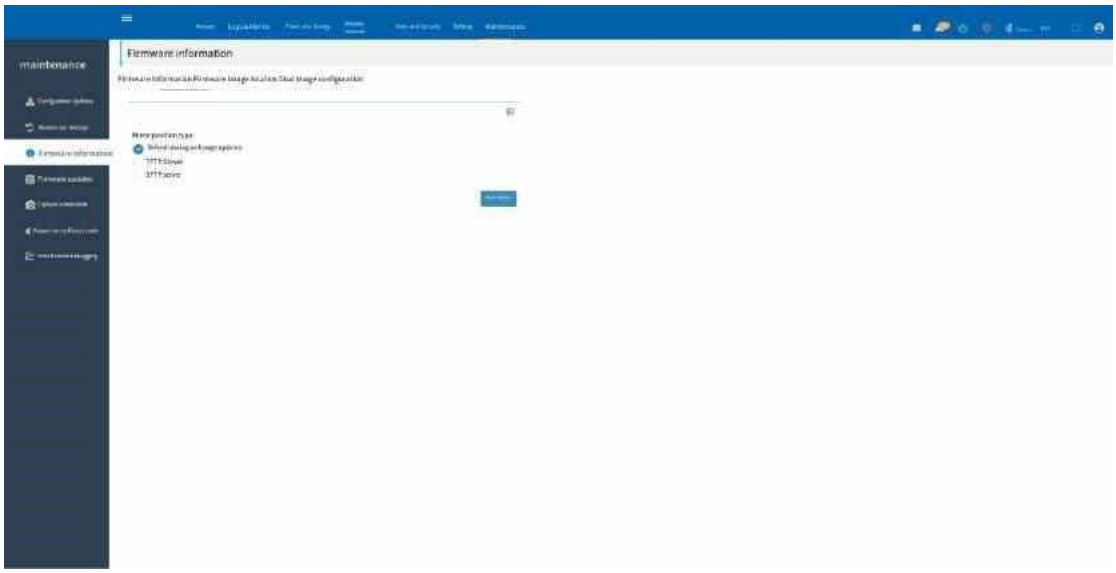


Figure 5-123 Firmware image location

Dual image configuration: Displays basic information about the two BMC images and can also set which image to boot from next time.

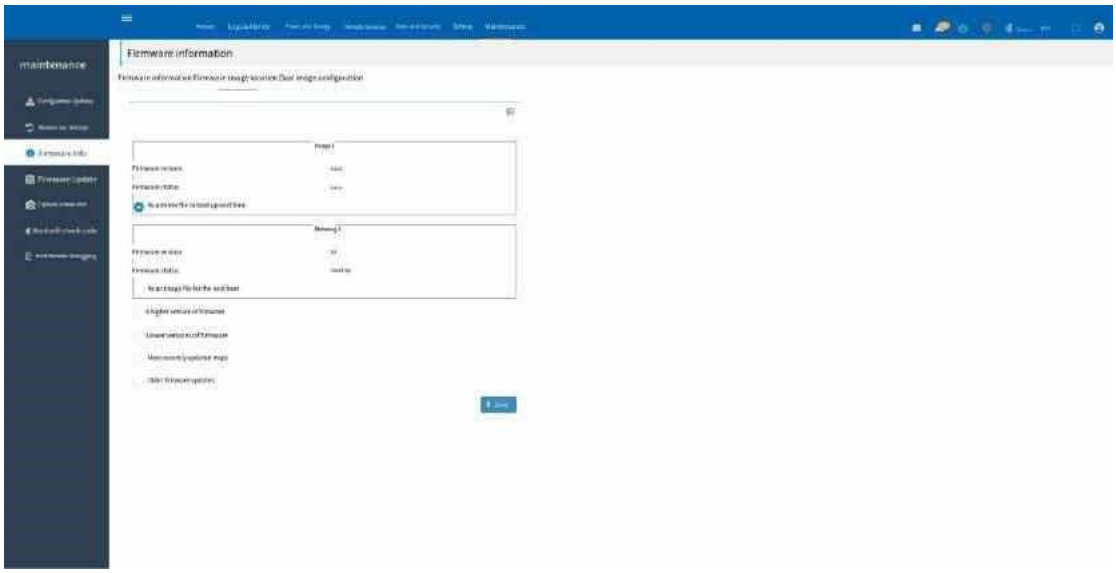


Figure 5-124 Dual mirroring configuration

5.6.11.4, Firmware update

This page is mainly used to update the firmware related to BMC

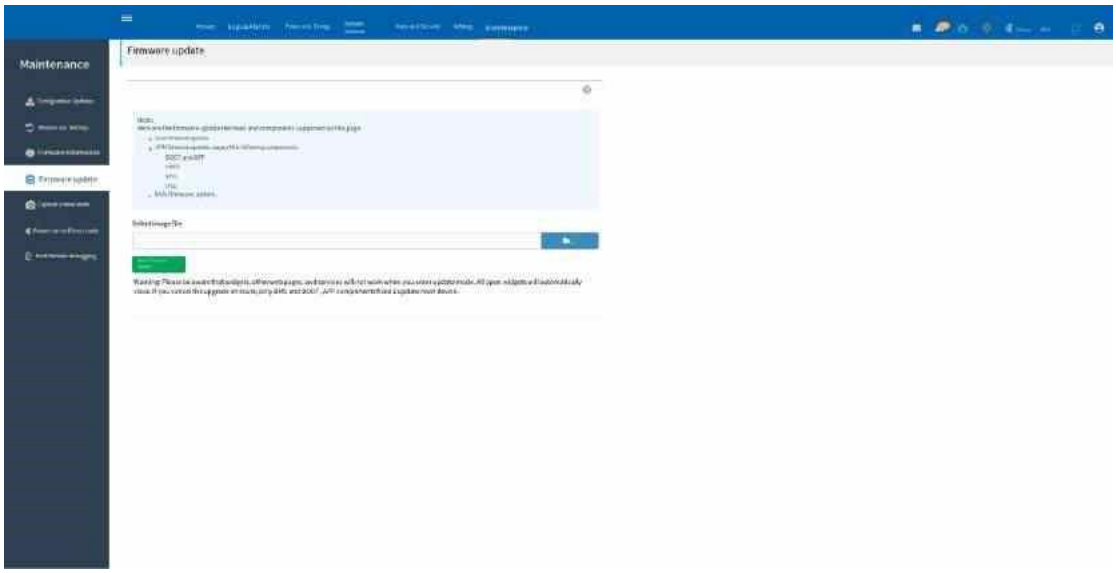


Figure 5-125 Maintenance-Firmware update

I.mb firmware update

BMC Reserved configuration: Some configuration information (SEL, IPMI, network, authentication, NTP, system log, Extlog, etc.) is reserved by default. To modify the save configuration options, click Edit Save configuration options or click Maintenance -> Config Update -> Save Configuration page.

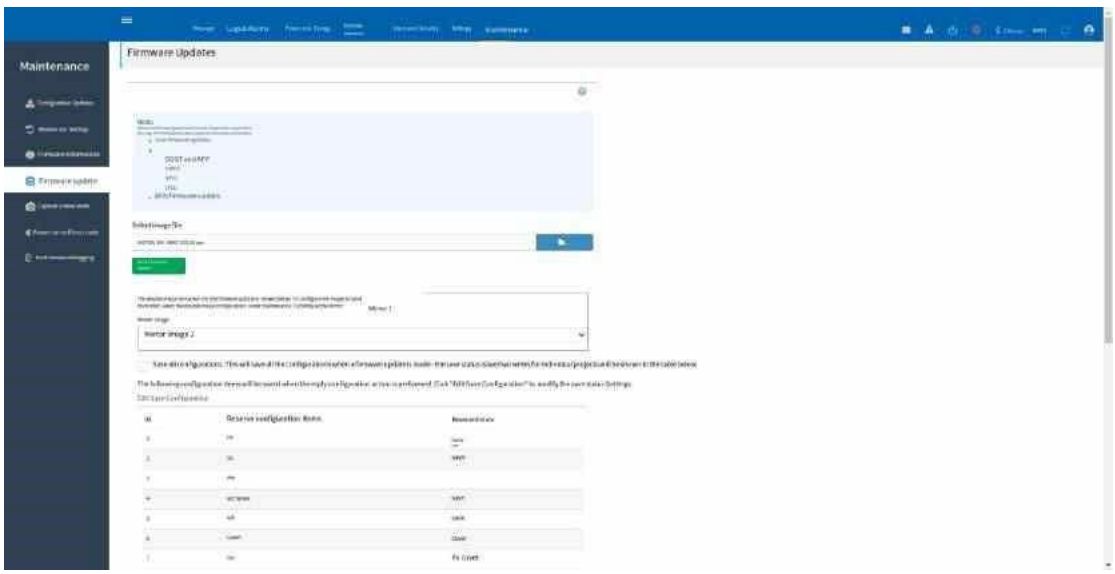


Figure 5-126 BMC Firmware update

When the update is complete, you are prompted that the BMC will restart.

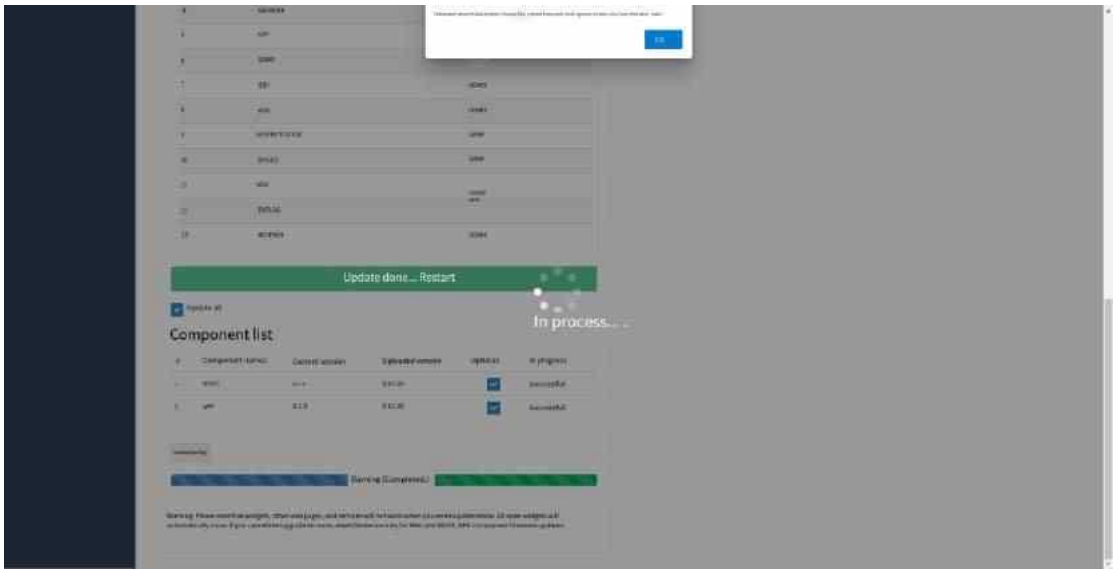


Figure 5-127 BMC update complete

5.6.11.5. Capture the screenshot

This page will capture the blue screen of death when the system went down the last time you booted it up.

Note: The KVM service must be enabled before the BSOD screen can be displayed. The KVM service can be set in 'Remote Service -> Service ->KVM'.

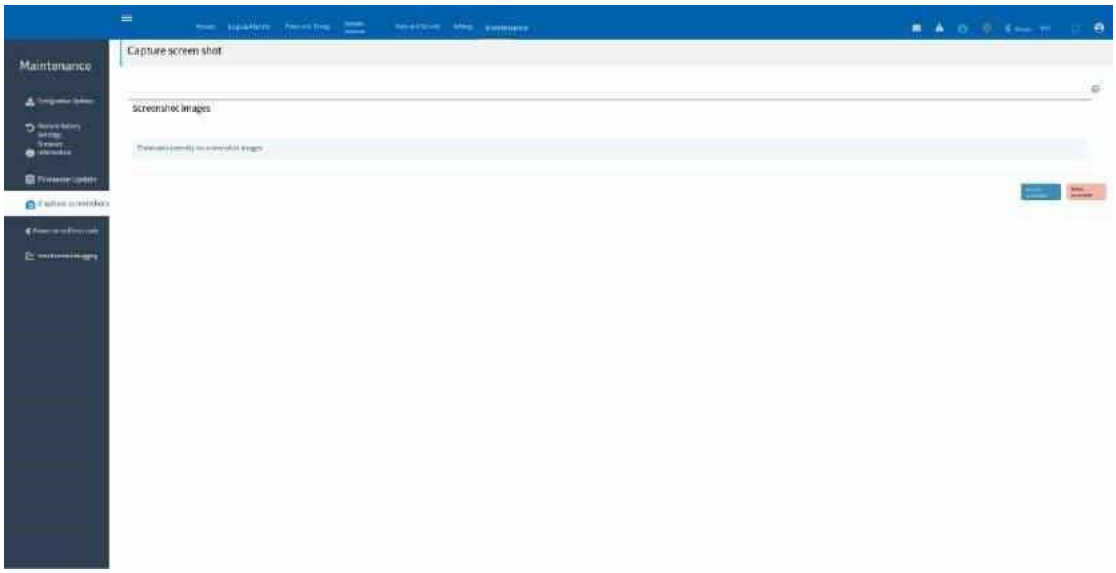


Figure 5-128 Capturing a screen grab

5.6.11.6, power-on self-test code

You can click the download button to download the current power-on self-test code and the last power-on self-test code. The display of the current power-on self-test code is related to the specific configuration of the machine (the startup timeout time is 5 minutes, the latest display after 5 minutes).

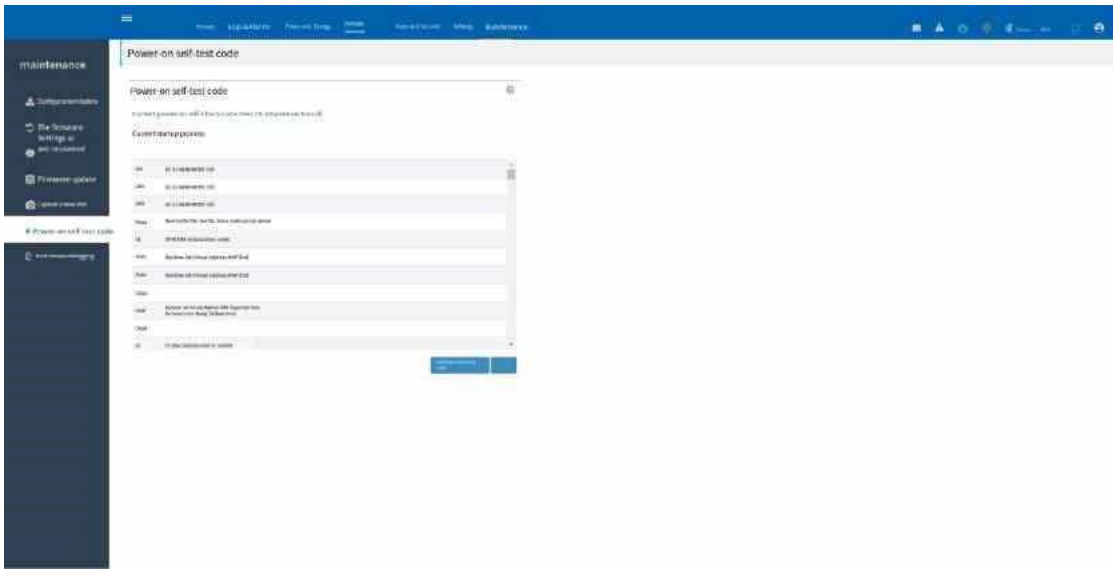


Figure 5-129 Power-on self -test code

5.6.11.7, host remote debugging

This interface is used to enable/disable/restart the remote debugging function.

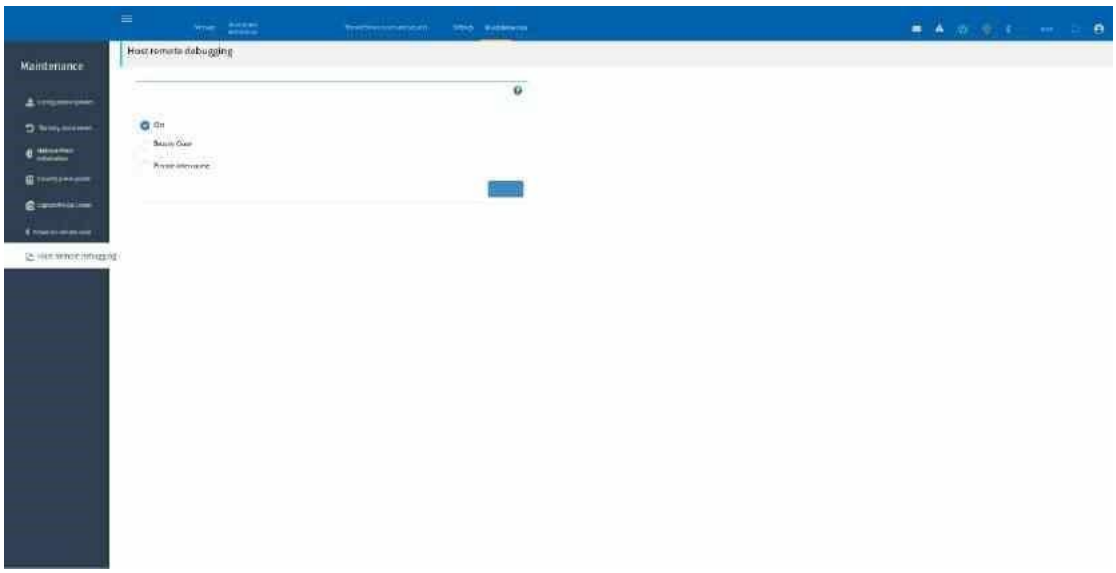


Figure 5-130 Remote debugging screen

5.7 Brushing BMC Firmware

5.7.1 BMC WEB Write

Click Maintenance -> Firmware Update option to enter the Firmware update page, which is mainly used to update the firmware related to BMC

The BMC firmware file is.ima, and the BIOS firmware file is.bin

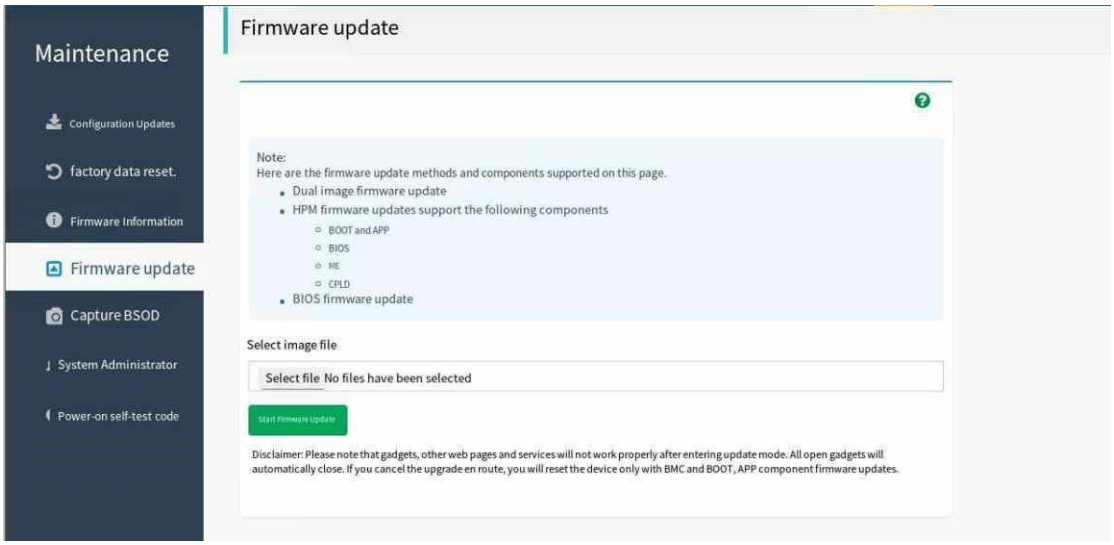


Figure 5-131 Maintenance-Update firmware

I.mc firmware update

BMC Reserved configuration: All configurations are not reserved by default If some of the configurations are reserved, go to the Reserved configuration page and select the configuration items you want to reserve.

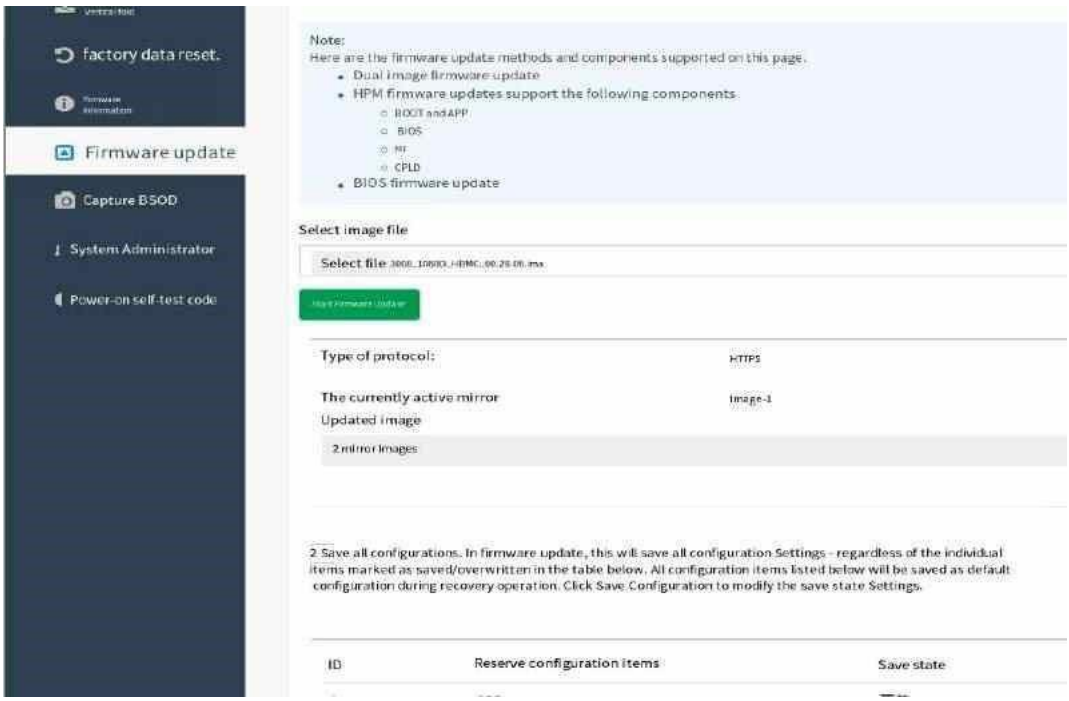


Figure 5-132 BMC does not save configuration updates

After the file is uploaded, the updated version and the existing version are displayed. Select Version Compare Update or Update All to continue updating the firmware.

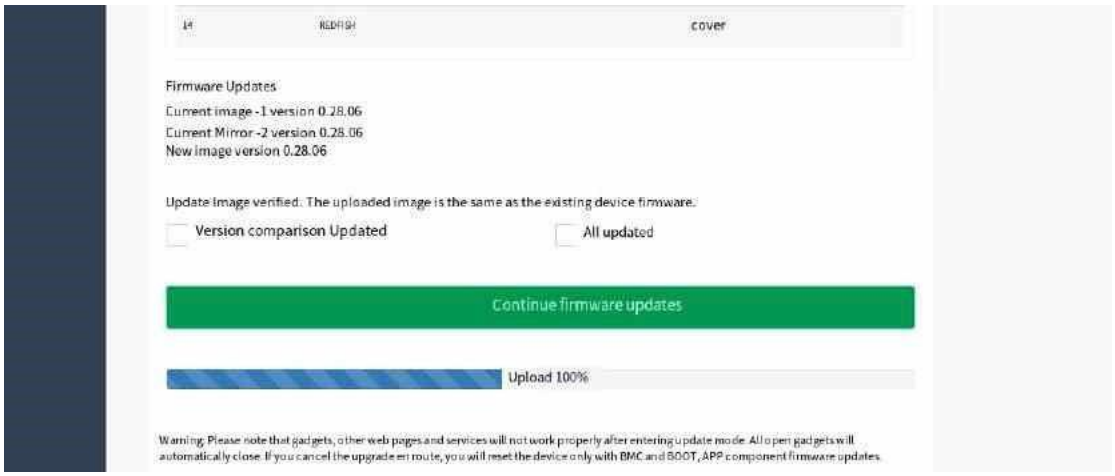


Figure 5-133 BMC Update

When you finish updating, you are prompted that the BMC will restart.

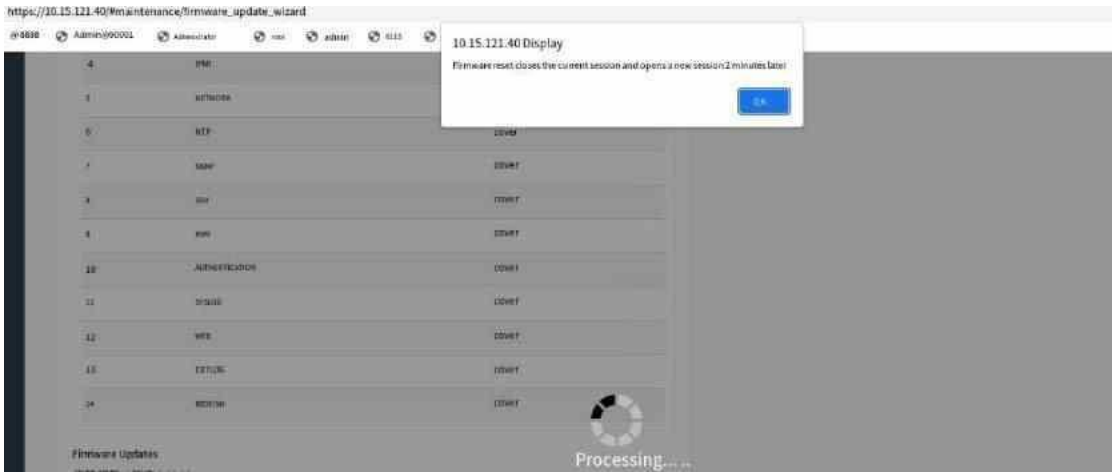


Figure 5-134 BMC configuration update completed

5.7.2 UEFI Shell Refresh

Step 1: copy the BMC version package to be refreshed to the root directory of the USB flash drive.

Step 2: Connect the USB flash drive to the USB port of the machine;

Step 3: Restart the machine and select "UEFI: Build-in EFI Shell" in the SETUP interface;

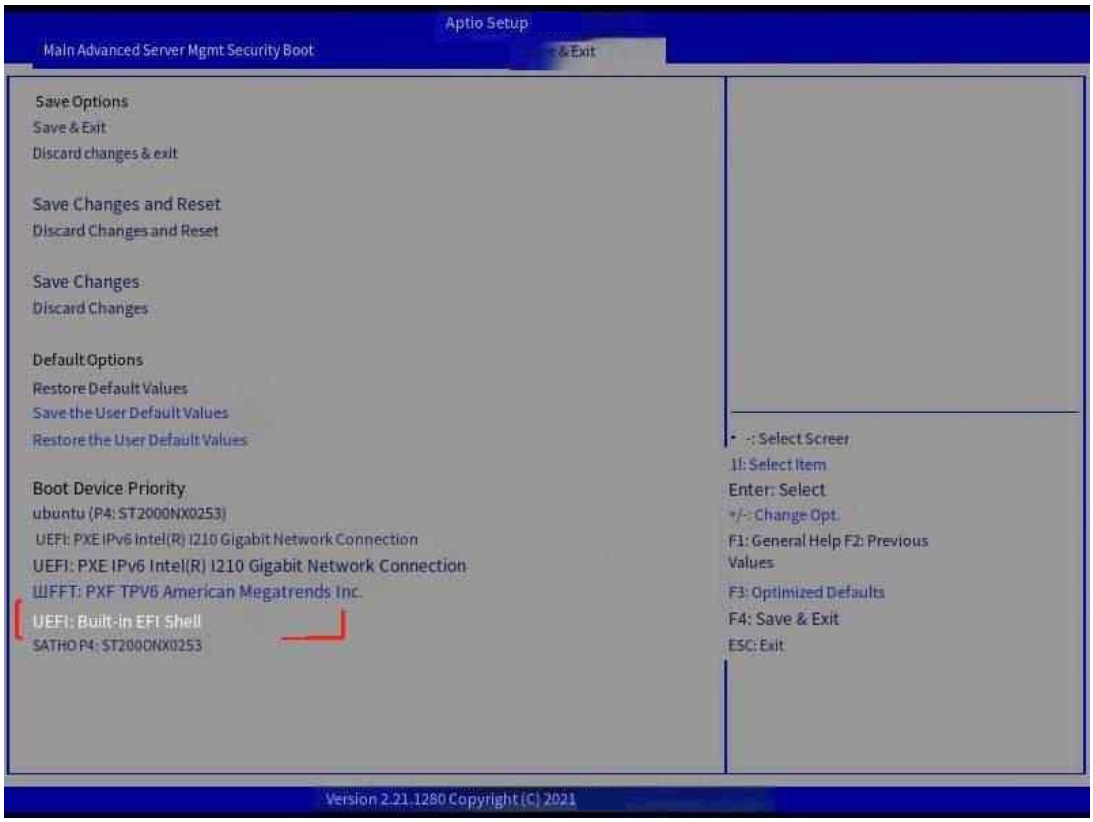


Figure 5-135 UEFI upgrade BMC firmware

Step 4: Run the following command to switch to the BMC version package directory on the USB flash drive and find fwupdate_bmc_shell.nsh to be refreshed.

Figure 5-136 UEFI upgrade BMC firmware

Step 5: On the command line, type fwupdate_bmc_shell.nsh and press Enter to start refreshing;

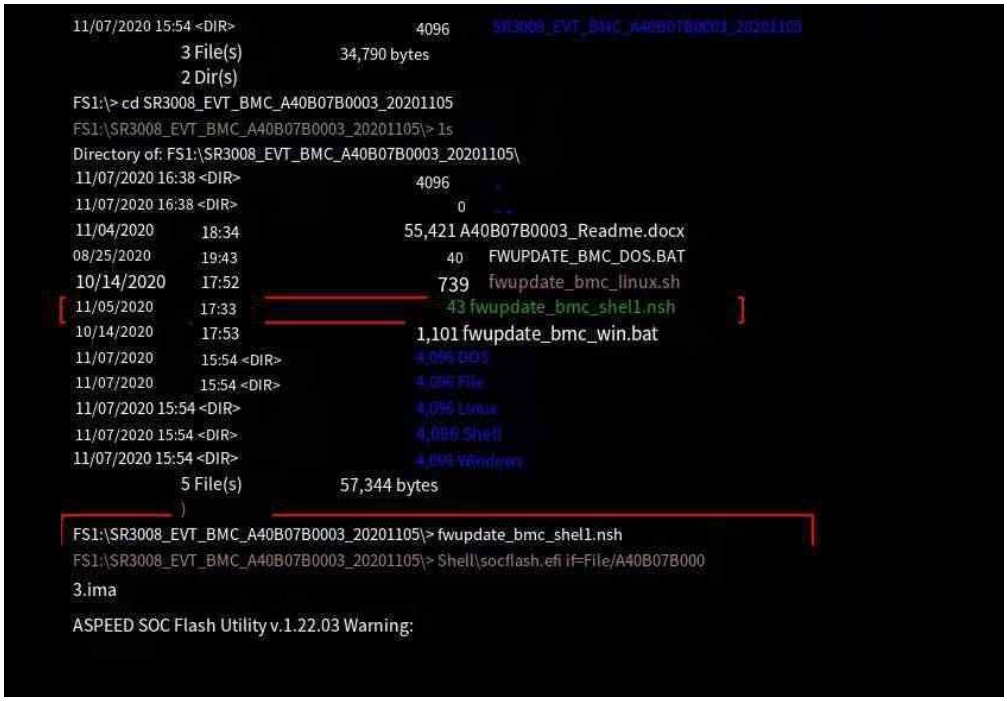


Figure 5-137 UEFI upgrade BMC firmware

Step 6: Wait until the refresh is complete. The following message is displayed: Do not AC or restart the BMC during the refresh process.

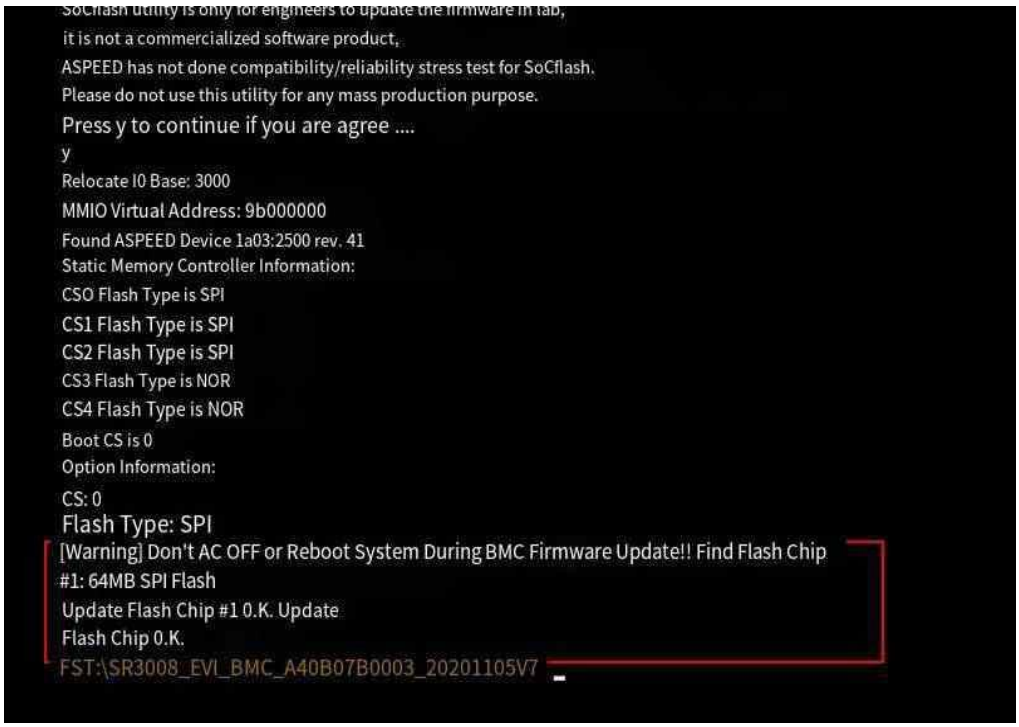


Figure 5-138 UEFI upgrade BMC firmware

Step 7: After the BMC restarts automatically, check whether the firmware is the target version on the Maintenance-Firmware Info page.

5.7.3 Operating System refresh

Step 1: Copy the BMC update package to any directory in the system (here, copy the BMC update package to the system desktop).

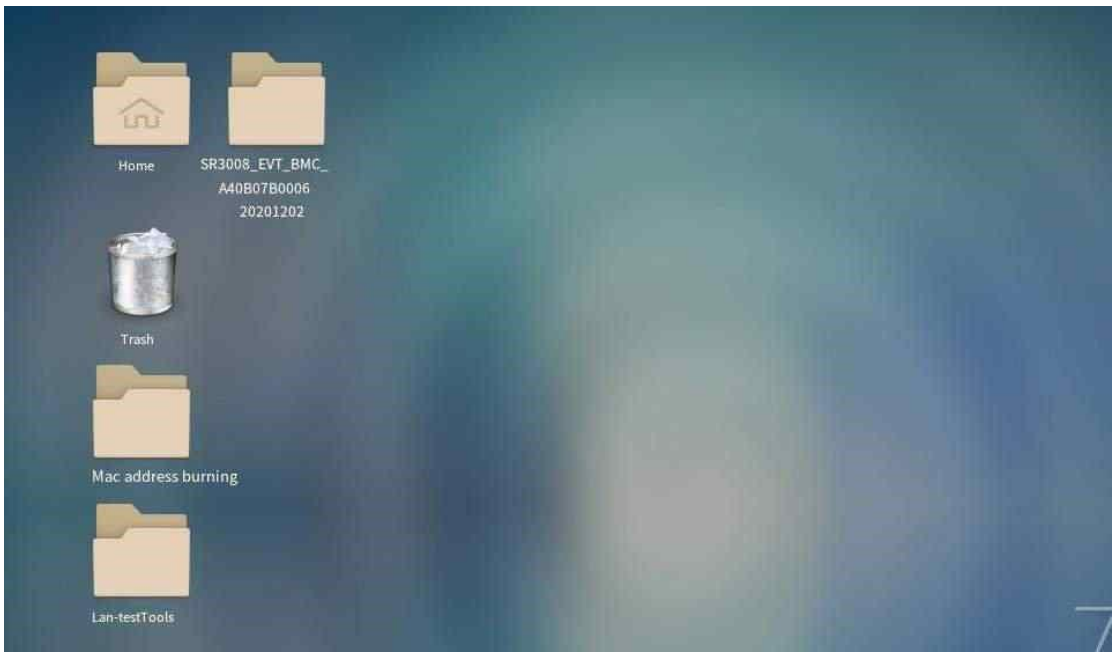


Figure 5-139 Upgrading the BMC firmware for the operating system

Step 2: Open the terminal and go to the installation package directory.

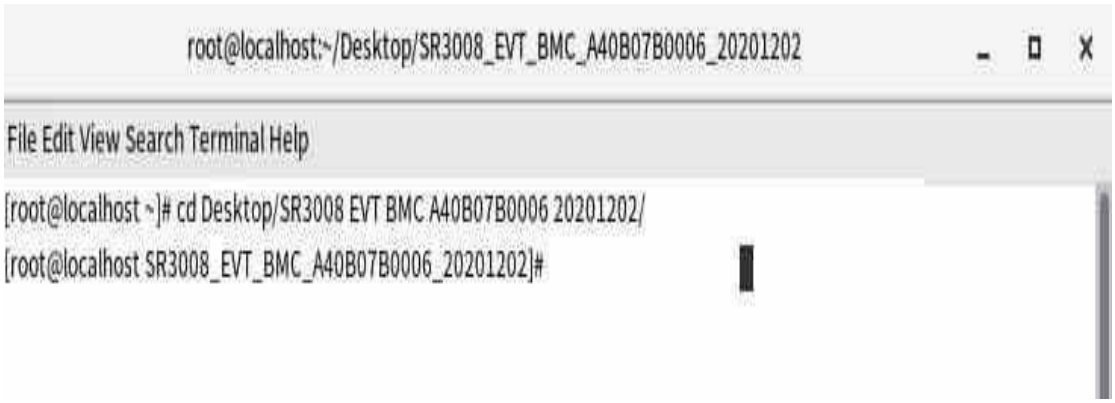


Figure 5-140 Operating system upgrade BMC firmware

Step 3: Chmod gives executable permissions to all files;

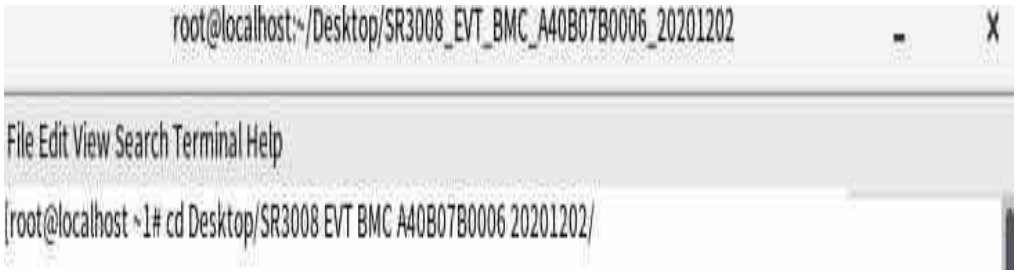


Figure 5-141 Operating system upgrade BMC firmware

Step 4: Run./fwupdate_bmc_linux.sh.

Type "y" to continue and start updating the bmc

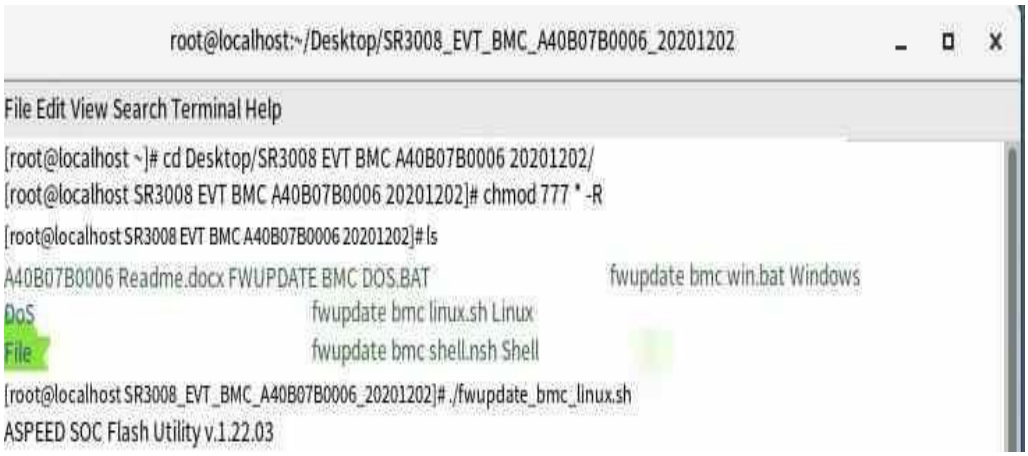


Figure 5-142 Operating system Upgrade BMC firmware

Do not AC during the operation. Shut down or restart the machine. After the update is complete, the BMC will automatically restart

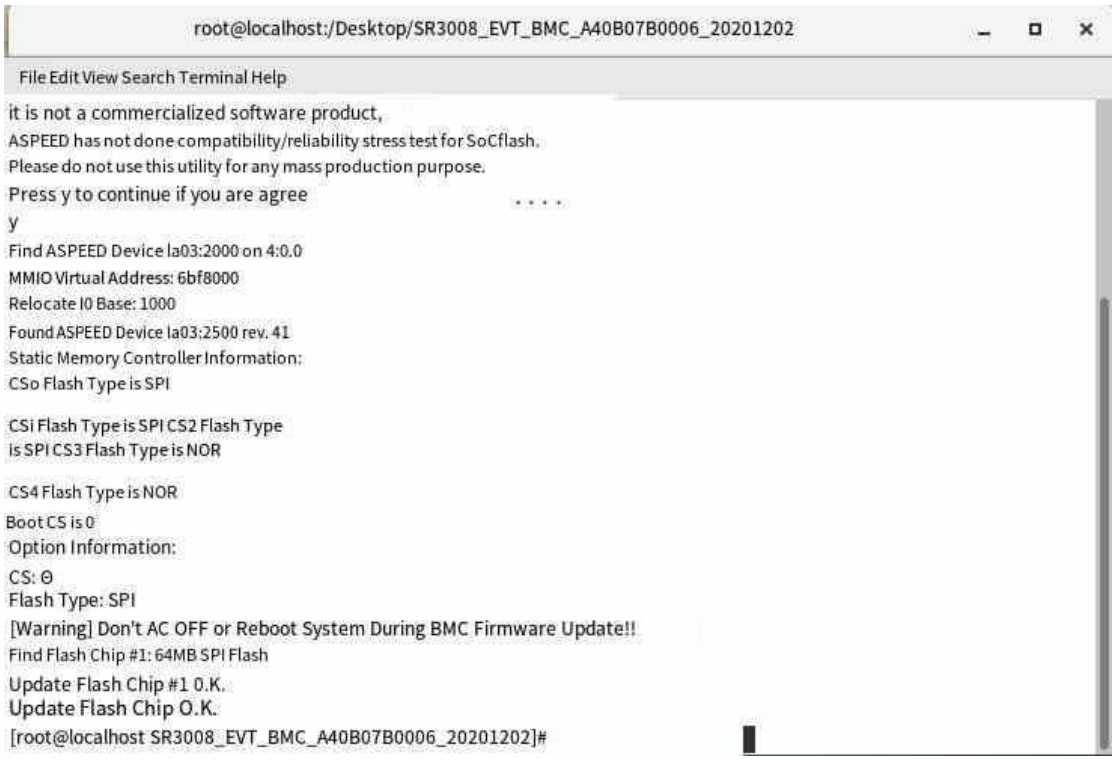


Figure 5-143 Operating system Upgrade BMC firmware

Step 5: Check the BMC version in the system

Figure 5-144 Operating system upgrade BMC firmware

5.7.4 Redfish Write

The following is a brief introduction to common Redfish operations without detailed description. The images are for reference only and are subject to actual conditions. **5.6.4.1. Common Parameters**

Parameters	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
header_type	Format of the request message	application/json
Username	Server username	Only administrators and operators have upgrade permissions. Therefore, use the existing administrator and operator usernames
Password	Password of the server user	Only the administrator and operator have the upgrade permission. Therefore, use the password of the existing administrator and operator
auth_value	Authentication parameters for the request message	Via https://device_ip/redfish/v1/SessionService/Session The X-Auth-Token value of Headers in the body of the response returned when the session is created
ifmatch_value	Usually a message digest	This parameter is obtained when the corresponding URL is obtained through the Redfish interface. The value is the etag value in Headers in the response body. The detailed URL is subject to the actual test.

5.7.4.2, operation build meeting

Operation types: POST URL: https://device_ip/redfish/v1/SessionService/Sessions

Request header: Content-Type: header_type Request message body:

{

"User":username

"Password":password

}

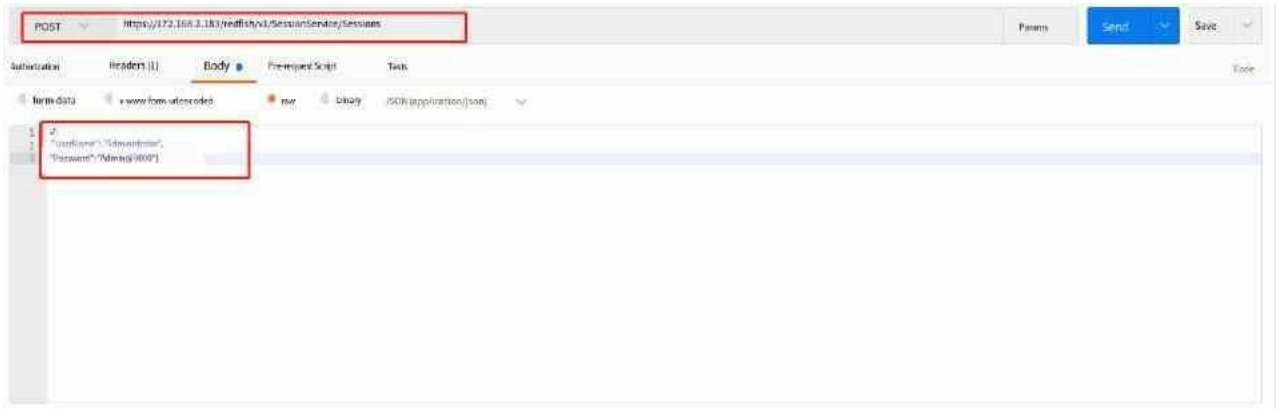


Figure 5-145 Creating a session

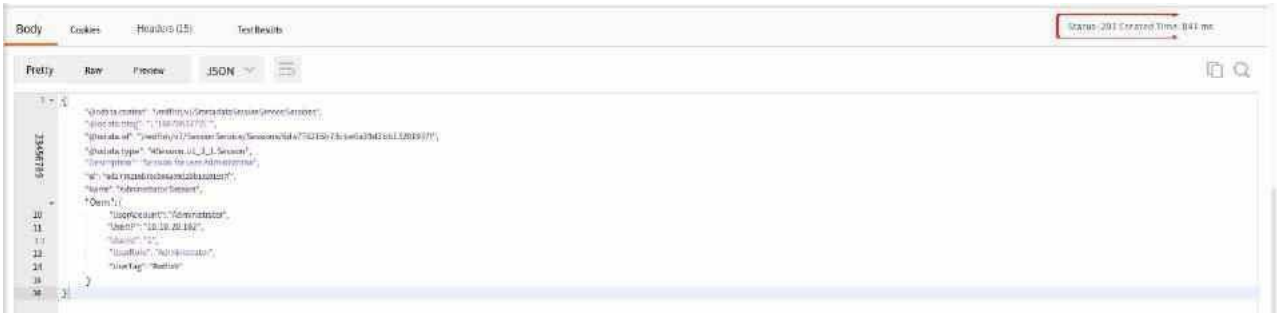


Figure 5-146 Creating a session

View the value of the created session token (default timeout is 300s)

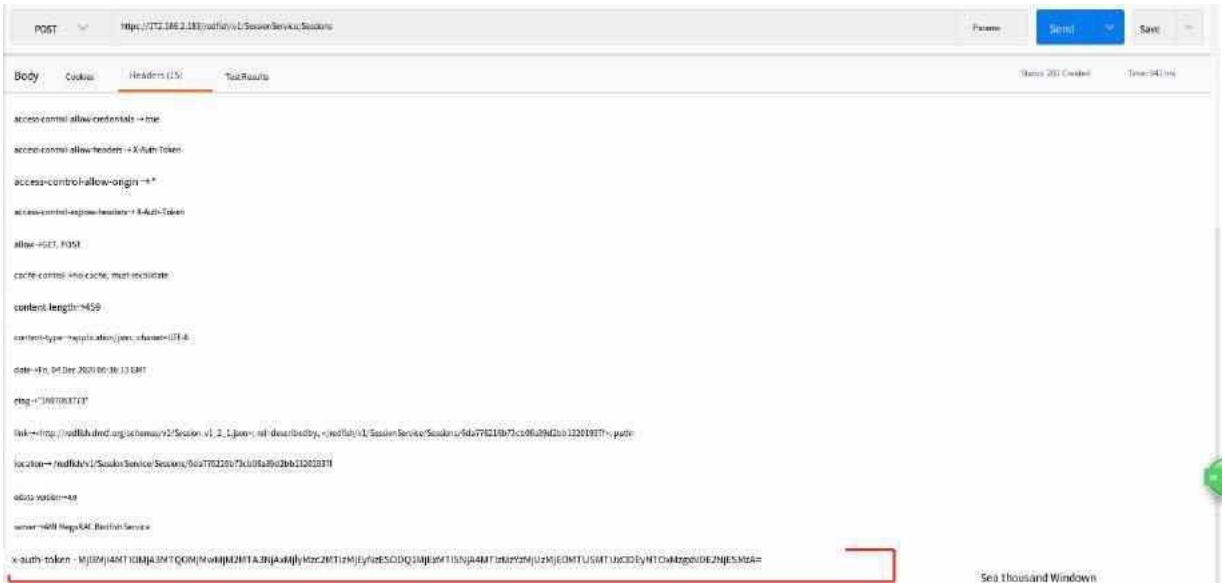


Figure 5-147 Obtaining the token value

Before performing GET, POST, PATCH, and DELETE operations, you need to create a session to obtain the token value. This step will be omitted in the following introduction.

5.7.4.3. User Management

- View users: View existing users

Operation type: the GET URL: https://device_ip/redfish/v1/AccountService/Account Request header: X-Auth-Token: auth_value

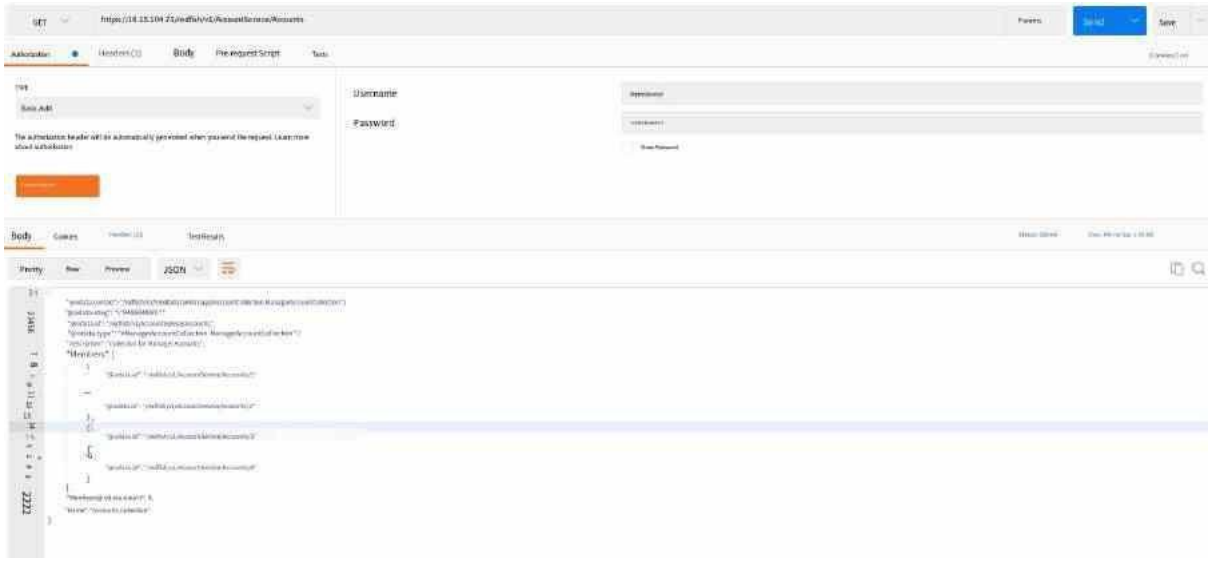


Figure 5-148 Viewing the user

● Create a BMC user: Create a BMC user using Redfish.

Operation types: POST URL: https://device_ip/redfish/v1/AccountService/Accounts

Request header: X-Auth-Token: auth_value

Message request body

{

"Enabled": true,

"Password": "superuser",

"UserName": "user_account",

"RoleId": " Value ",

}

Parameter description:

Parameters	Meaning	Value
Enabled	User enabled permissions	ture: Enables flase : disables
Password	User password	A string of 1 to 16 alphanumeric characters
UserName	Username	A string of 8 to 20 alphanumeric characters
RoleId	Permissions available to the user	"Administrator"/"Operator"/"ReadOnly"

UserName and Password must follow the following rules:

- UserName only allows the special characters '-' (hyphen), '_' (underscore), and '@' (symbol).
- UserName must be a string of 1 to 16 alphanumeric characters.
- UserName must begin with an alphanumeric character.
- The Password must be a string of 8 to 20 characters.
- UserName and Password cannot be the same

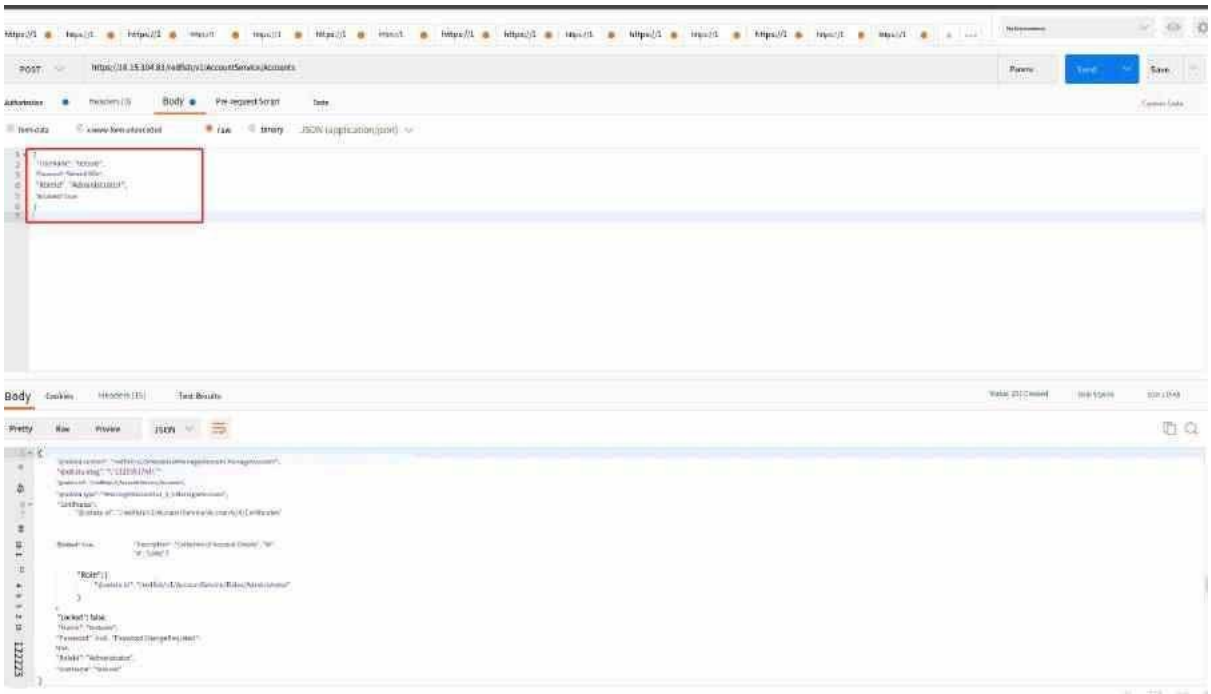


Figure 5-149 New user

- Delete user: Deletes an existing user Operation type: DELETE URL: https://device_ip/redfish/v1/AccountService/Accounts/{userid}

Request header: Content-Type: header_type

X-Auth-Token: auth_value

Note: HostAutoFW, HostAutoOS can't be deleted or modified.

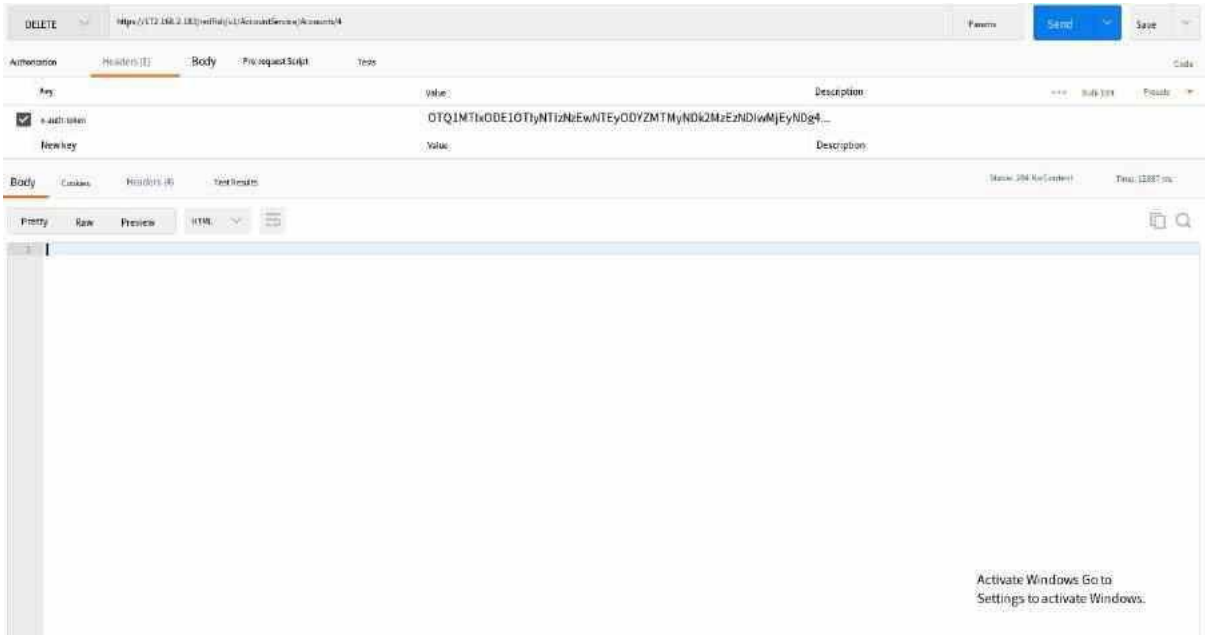


Figure 5-150 Deleting a user

5.7.4.4. Network Settings

● Network switching: dynamic switching static. (Static switching dynamic network similar, do not do detailed description)

Type of operation: PATCH

URL: https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/eth0 (eth1)

Request header: Content-Type: header_type

X-Auth-Token: auth_value

If-Match: ifmatch_value

Request message body:

To disable dhcp for IPv4Address

```
{
"DHCPv4": {
"DHCPEnabled": false
},
"IPv4Addresses": [
{
"Address": "10.0.124.86",
"Gateway": "10.0.120.1",
"SubnetMask": "255.255.248.0"
}
]
}
```

To modify IPv4StaticAddress details

{

"IPv4StaticAddresses": [

{

"Address": "10.0.124.86",

"Gateway": "10.0.120.1",

"SubnetMask": "255.255.248.0"

}

]

}

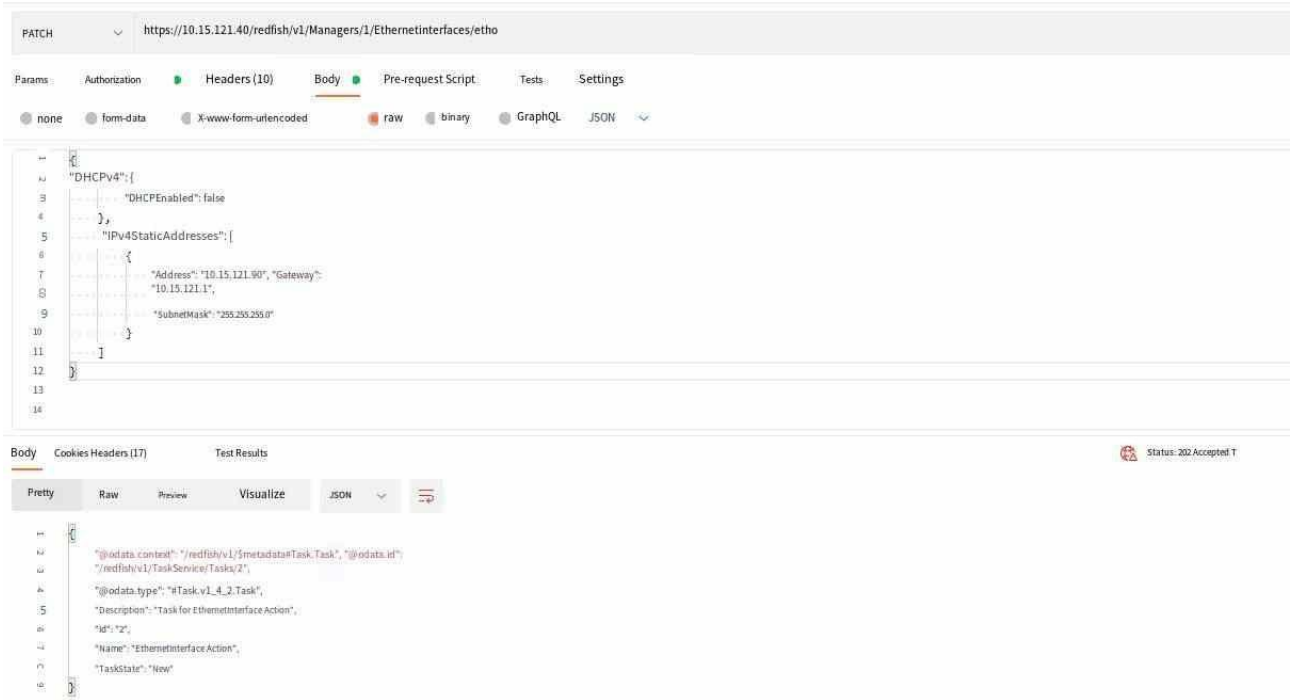


Figure 5-151 Dynamic switching static

● Network switching: Static switching dynamic

Operation type: PATCH

URL: https://device_ip/redfish/v1/Managers/1/EthernetInterfaces/eth0 (eth1)

Request header: Content-Type: header_type

X-Auth-Token: auth_value

If-Match: ifmatch_value

Request message body:

{"DHCPv4":

{

"DHCPEnabled": true

}

}

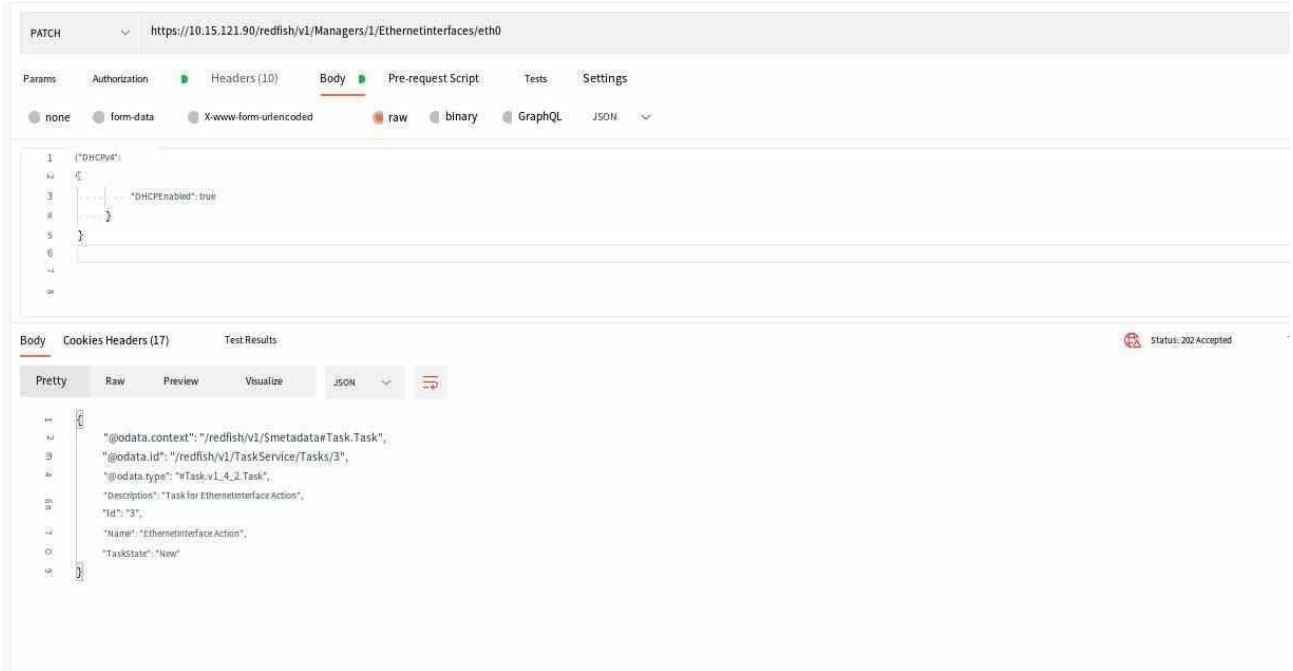


Figure 5-152 Static switching dynamic

5.7.4.5. UID Indicator Settings

● View UID status

Operation type: GET URL: https://device_ip/redfish/v1/Chassis/1

Request header: X-Auth-Token: auth_value

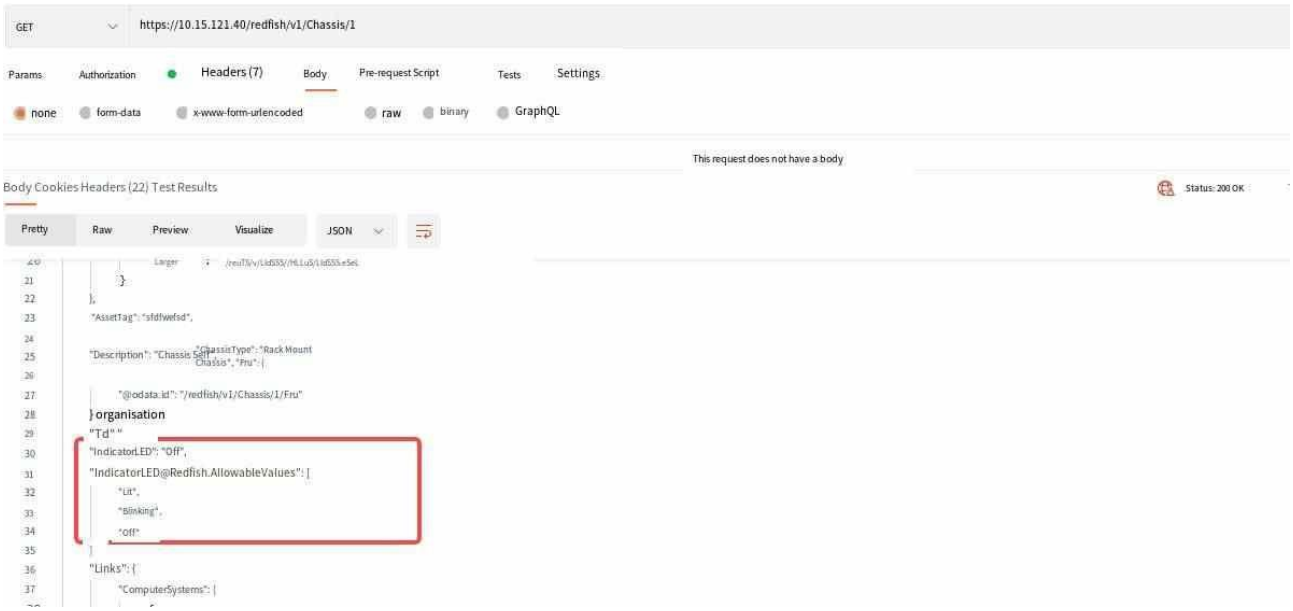


Figure 5-153 UID indicator Settings

● Setting the UID

Operation type: PATCH URL: https://device_ip/redfish/v1/Chassis/1

Request header: Content-Type: header_type

X-Auth-Token: auth_value

If-Match: ifmatch_value

Request message body:

{

"IndicatorLED": Value

}

Value The values are "Lit", "Off" and "Blinking".

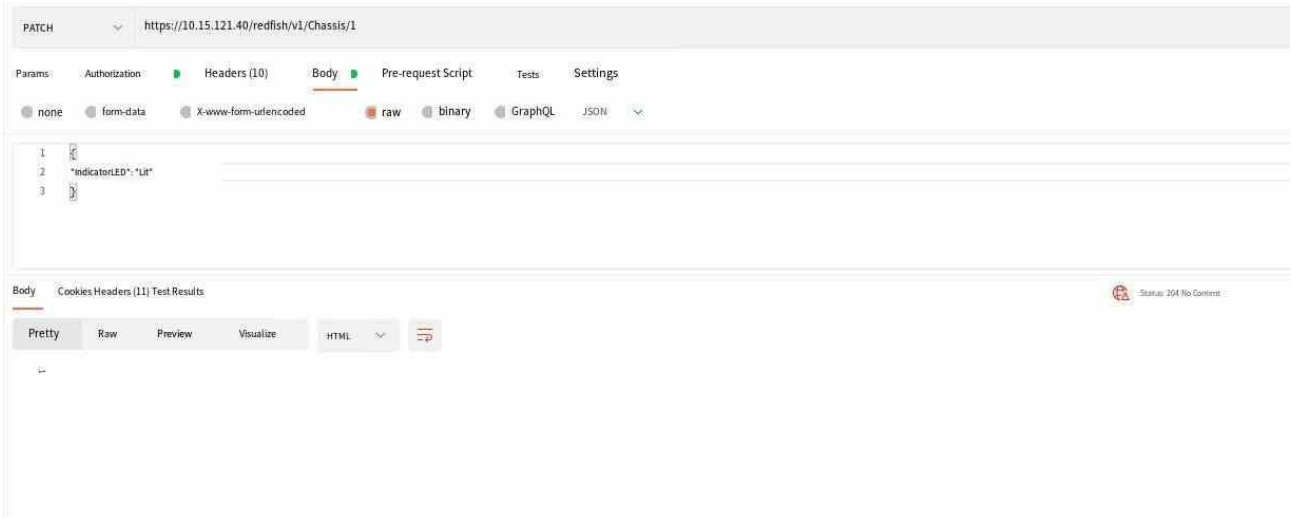


Figure 5-154 Setting the UID

5.7.4.6. Power Control

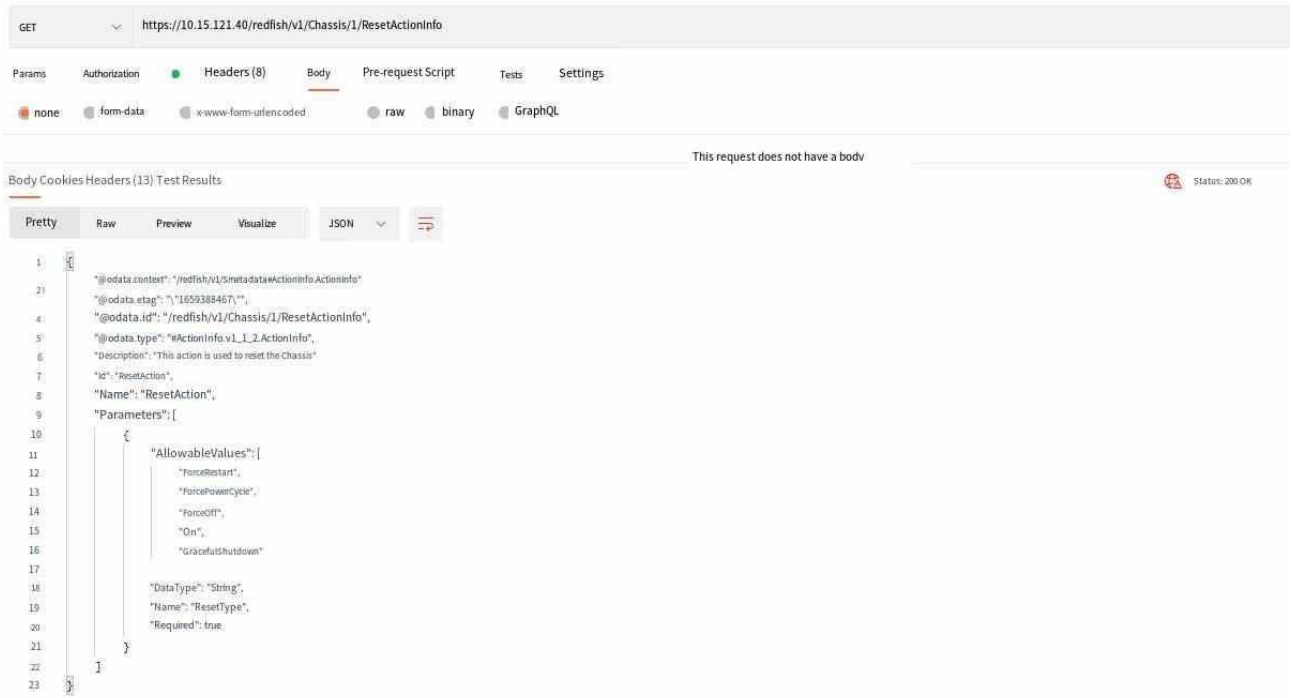
● View power-on and power-off operations

Operation type: the GET URL:

https://device_ip/redfish/v1/Chassis/1/ResetActionInfo

Request header: X-Auth-Token: auth_value

Figure 5-155 Power-on and power-off operation type



● Power-on and power-off Operations

Type of operation: POST

URL: https://device_ip/redfish/v1/Systems/1/Actions/ComputerSystem.Reset;

Request header: Content-Type: header_type

X-Auth-Token: auth_value

Request message body:

{

" ResetType": Value

}

Value can be "GracefulShutdown", "On", "ForceRestart", "ForceOff", and "ForcePowerCycle".

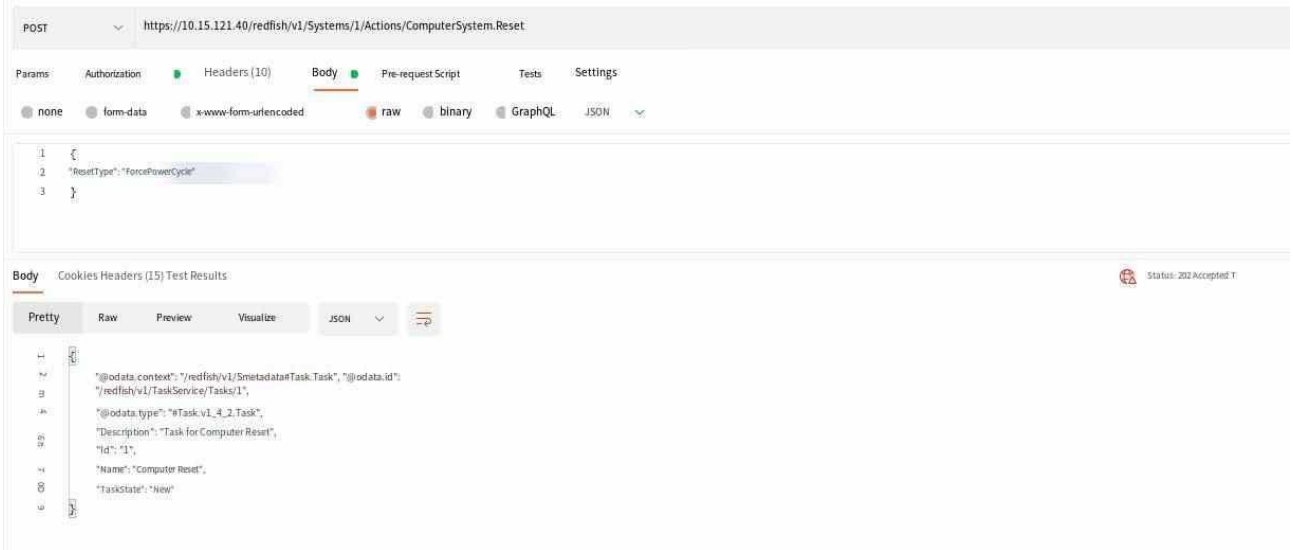


Figure 5-156 Power-on and power-off operations

5.7.4.7 Firmware upgrade

● BMC update

Action type: POST

URL: https://device_ip/redfish/v1/UpdateService/Actions/SimpleUpdate

Request header: X-Auth-Token: auth_value

Content-Type: header_type Request message body:

```
{
"TransferProtocol": protocol,
  "ImageURI": filepath,
  "User":username,
"Password":password
}
```

Parameter description:

PARAMETERS	Meaning	Value
filepath	Filepath 3 Path where the upgrade file is located	Such as: "http://172.168.0.49/httpsshare/A40B07B0001.ima" "Ftp://172.168.0.46/pub/A40B07B000.ima"
protocol	Download the protocol required for the upgrade package	“HTTPS”/“HTTP”/“FTP”
username	Username for sharing the file with the FTP service	Note: This parameter is required only when you use FTP to download the upgrade package
password	Password for sharing the file with the FTP service	Note: This field is only required when you download the upgrade package using FTP

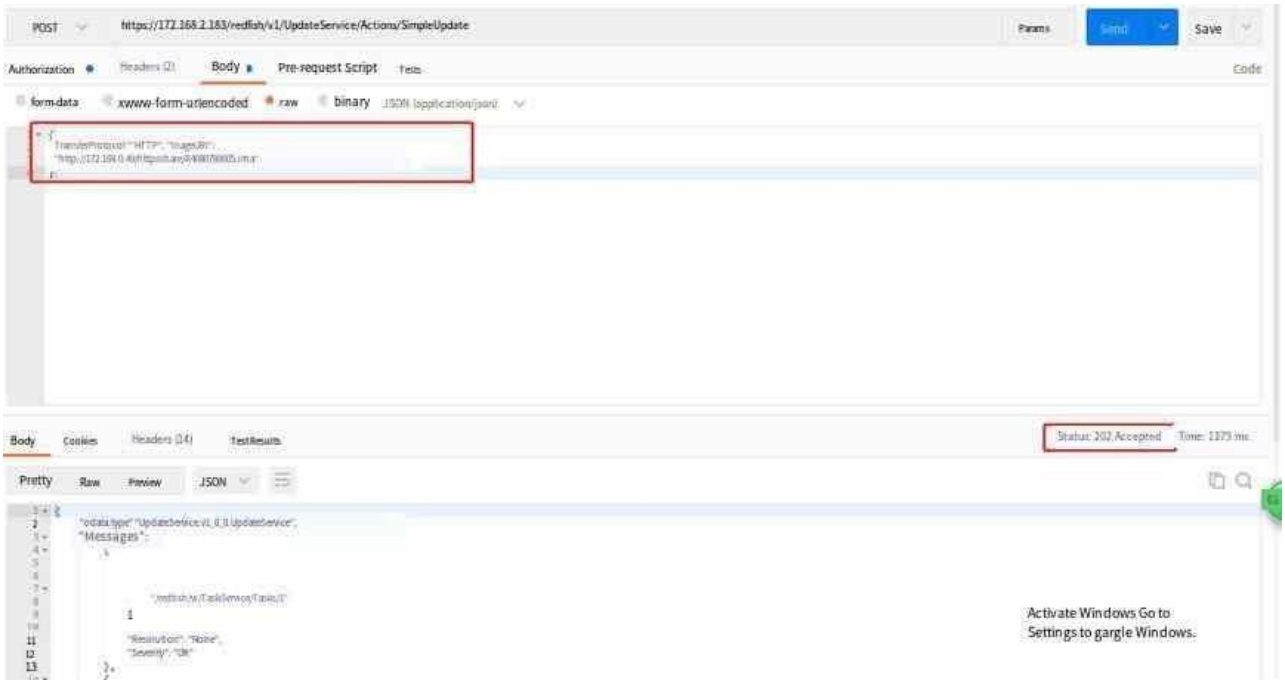


Figure 5-157 BMC Update

● Obtain BMC version information Type of action: GET URL: https://device_ip/redfish/v1/UpdateService/FirmwareInventory/BMC

Request header: X-Auth-Token: auth_value

Figure 5-158 BMC version information

● BIOS firmware Update

Operation types: POST URL: https://device_ip/redfish/v1/UpdateService/upload

Request header: X-Auth-Token: auth_value

Content-Type: multipart/form-data; Request message body:

KEY: UpdateParameters VALUE: parameters.json (file name in the version package)

KEY: OemParameters VALUE: oem_parameters.json (file name in version package)

KEY: UpdateFile VALUE: A40B07A00x.hpm (refresh file name in version package) Parameter Description:

Parameters	Meaning	Value

parameters.json	Request header parameters	parameters.json (file name in the version package)
oem_parameters.json	Customize request header parameters	oem_parameters.json (file name in the version package)
A40B07A00x.hpm	Upgrade pack name	bios upgrade file (.hpm)

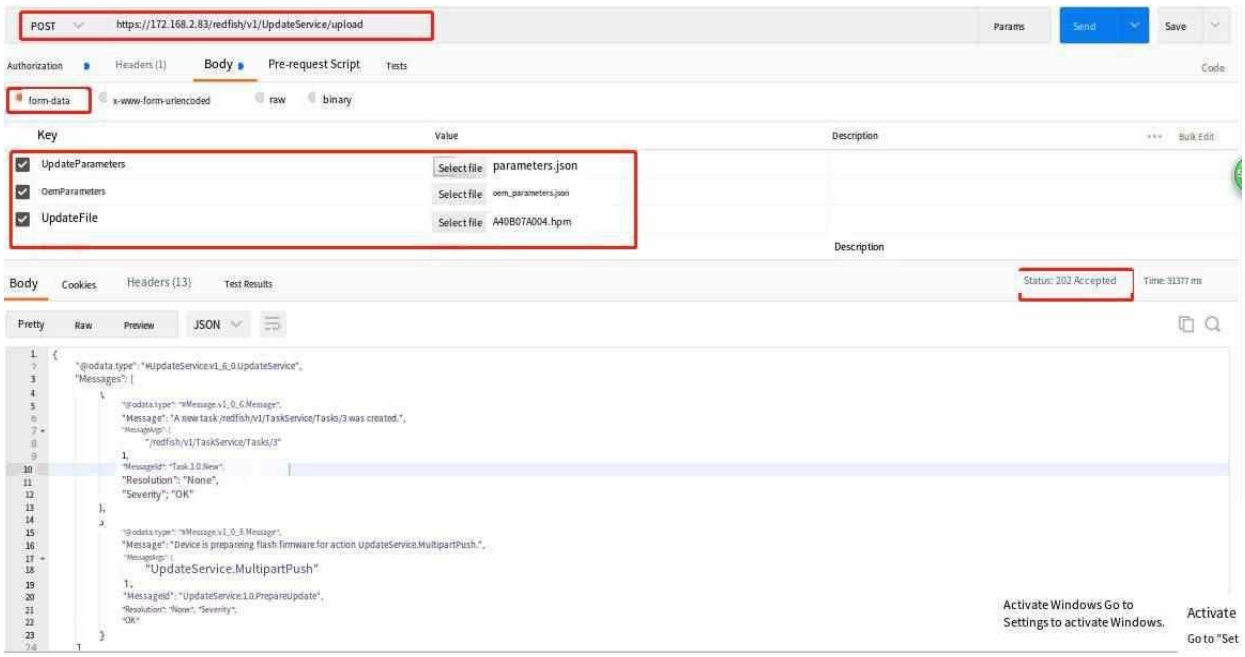


Figure 5-159 BIOS firmware update

Chapter 6 Operating System Installation Guide

6.1 KVM Mounting and Installation

6.1.1 Introduction

The Keyboard Video Mouse (KVM) allows users to easily and directly access servers and devices in multiple remote locations from the KVM client management software by directly connecting the keyboard, video, and mouse (KVM) ports. KVM provides true motherboard-level access and supports multi-platform servers. Current machines support both H5 KVM and JViewer KVM. The H5 KVM starts the H5viewer window. For the JViewer KVM, download the jviewer(.jnlp) file and start the jviewer file to open the KVM.

6.1.2 CentOS 7.8

Step 1 Log in to the BMC of the server where the OS is to be installed. The default user name is Administrator and password is Admin@9000.

Figure 6-1 BMC control page

Step 2: Click Remote Control -> Console Redirection KVM to enter the KVM mounting screen.

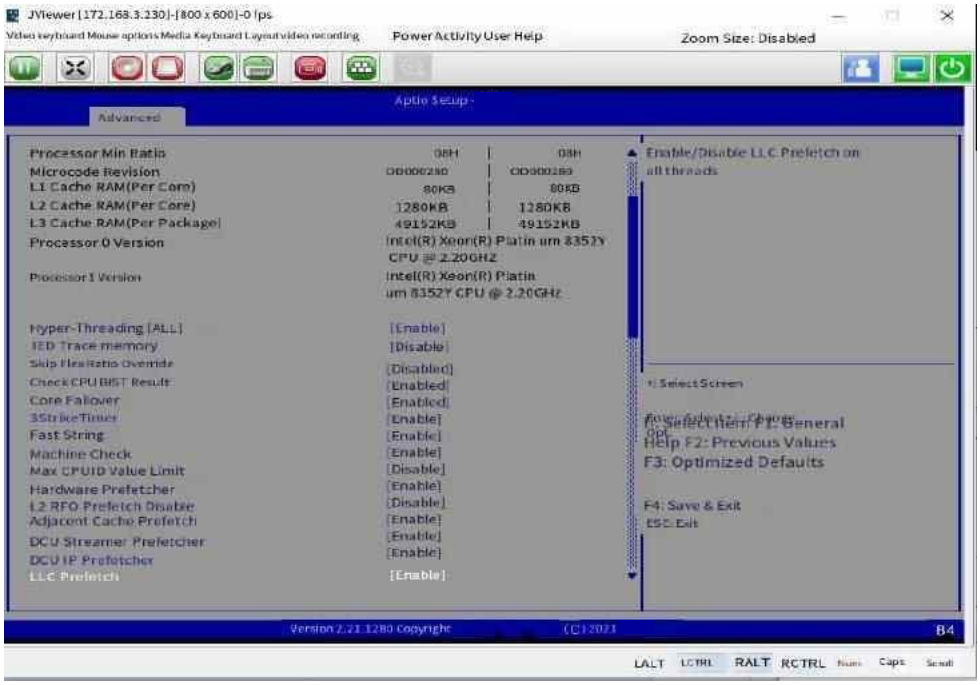


Figure 6-2 JAVA control screen

Step 3: Click Media > Virtual Media Wizard to enter the CD/DVD image mount screen.

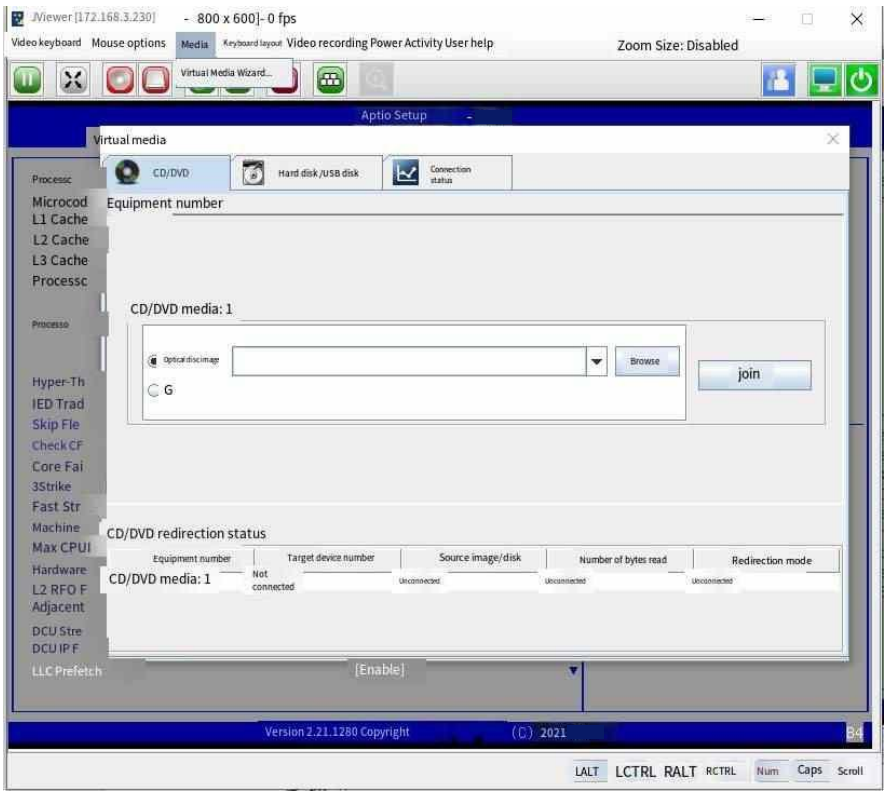


Figure 6-3 Virtual image mount screen

Step 4: Click Browse, select the system image you want to install, click Connect, the

image is mounted successfully;

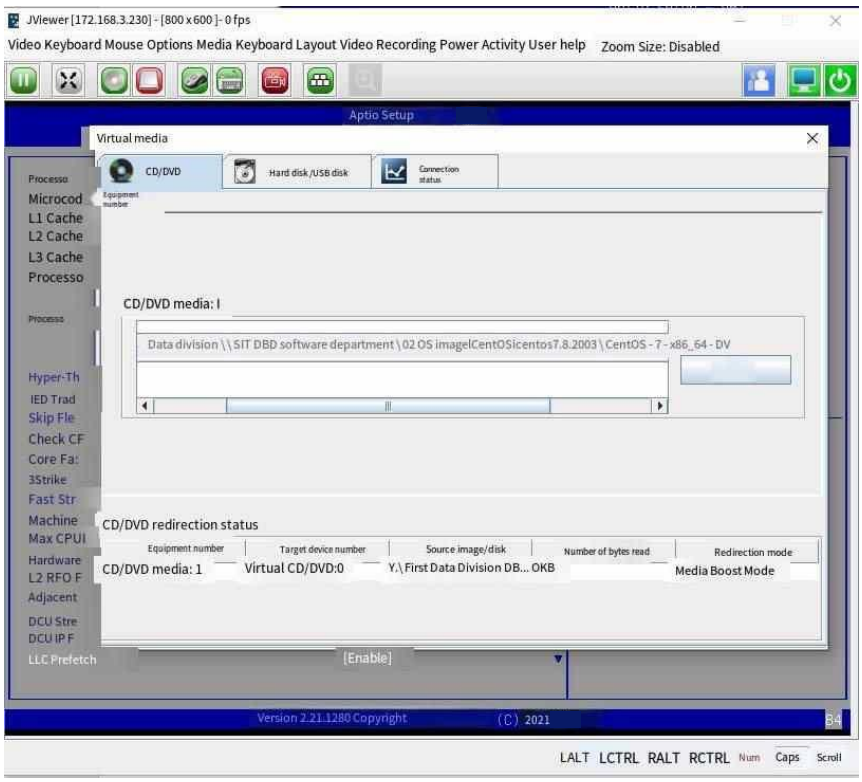


Figure 6-4 Mounting the virtual image

Step 5: Restart the server. When "Please <F11> to enter Boot Menu" is displayed, press F11 to enter the boot item boot screen.

Figure 6-5 Press F11 to enter the boot menu screen

Step 6: Select the AMI Virtual CDROM option to mount the OS image to boot up;

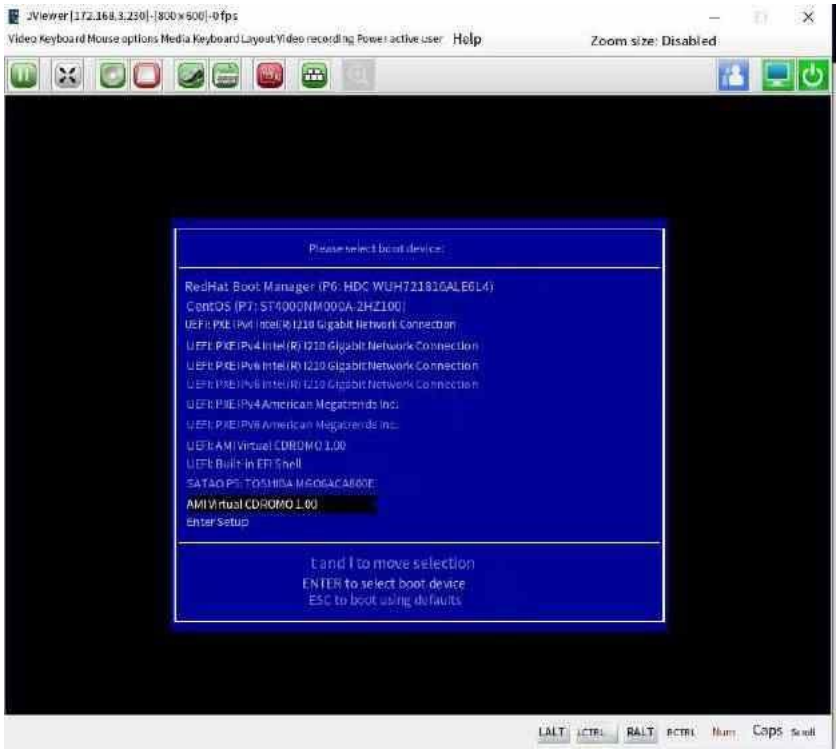


Figure 6-6 Select the CDROM image boot option

Step 7: Enter the image installation screen, select "Install CentOS7", and press Enter to install the system;

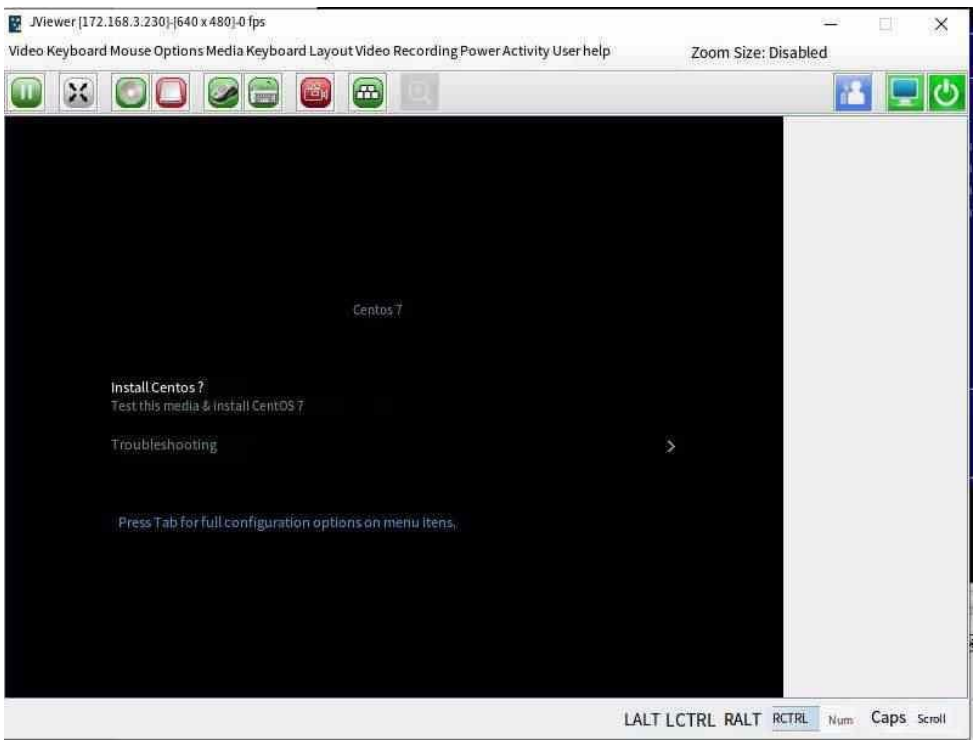


Figure 6-7 System installation screen

Step 8: Select the language to install the system and click Continue to proceed to the next step;

Figure 6-8 System language Settings

Step 9: Go to the installation system configuration preview screen, as shown in the following picture;

Figure 6-9 System configuration screen

Step 10: Click "Date&Time, set the system time, click Done to save the Settings;

Figure 6-10 Setting the system time

Step 11: Set the KEYBOARD and click Done to save the configuration.

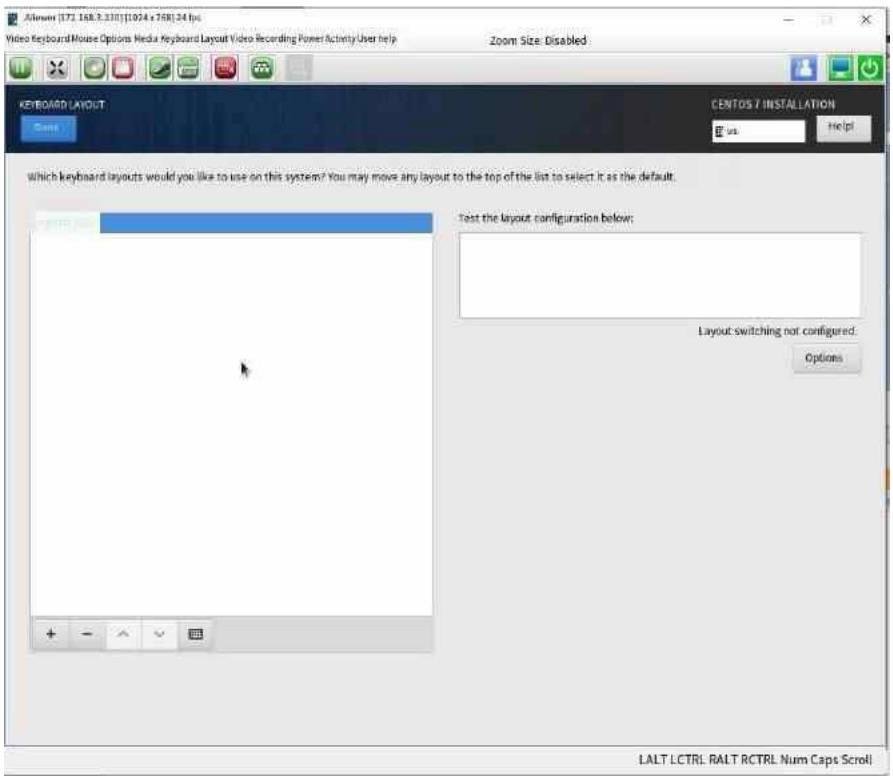


Figure 6-11 KEYBOARD Settings

Step 12: Configure the installation source, select the default configuration and click Done to save the configuration;

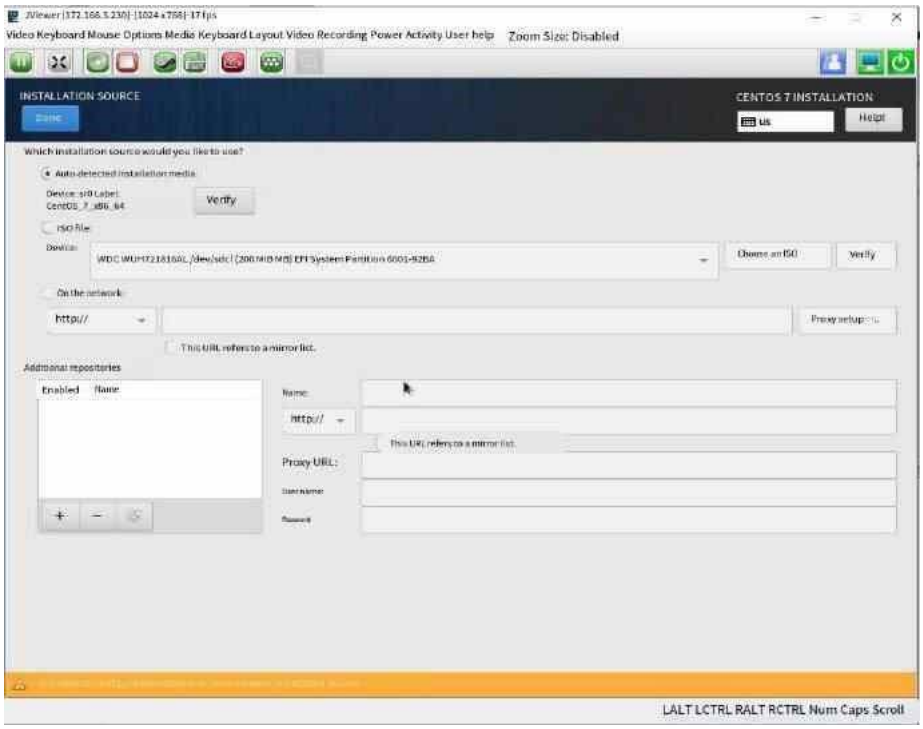


Figure 6-12 Install source Settings

Step 13: Configure Software Selection. Select the system installation package as required. After the selection is complete, click Done to save the configuration.

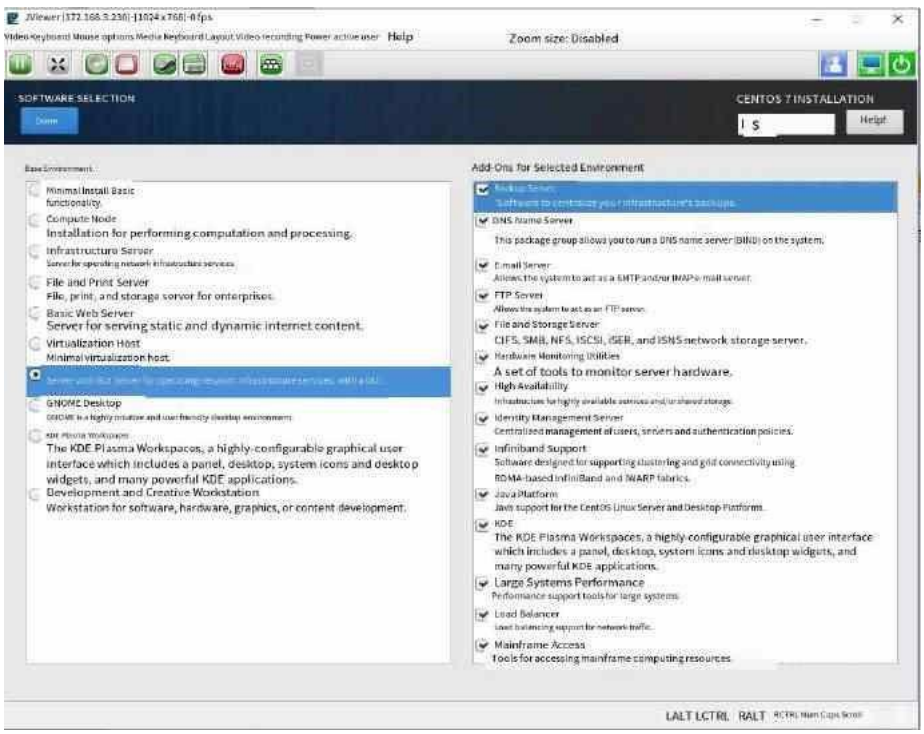


Figure 6-13 Software Selection configuration

Step 14: Select the hard drive on which you want to install the system and click Done to save the configuration;

Figure 6-14 Installing System Hard drive Select Automatic partition

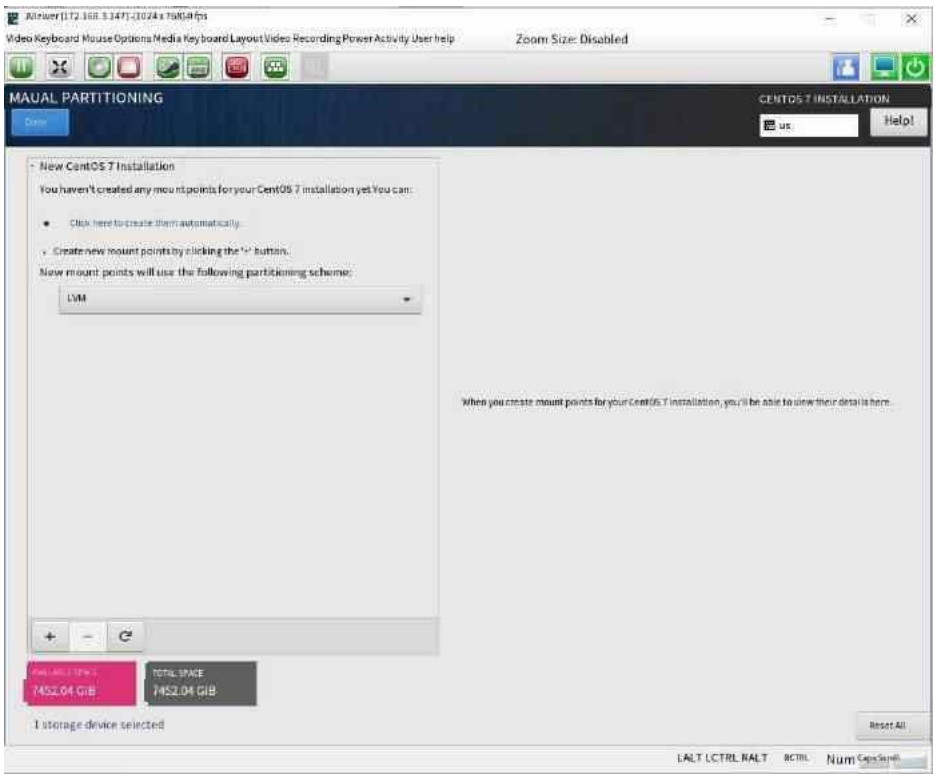


Figure 6-15 Installing a system hard disk select manual partitioning

Note: When automatic partitioning is selected, the base partition required by the system is created and formatted as an XFS file system; When manual partitioning is selected, create your own partitions ((/boot, /swap, etc.).

Step 15: Configure KDUMP and click Done to save the configuration

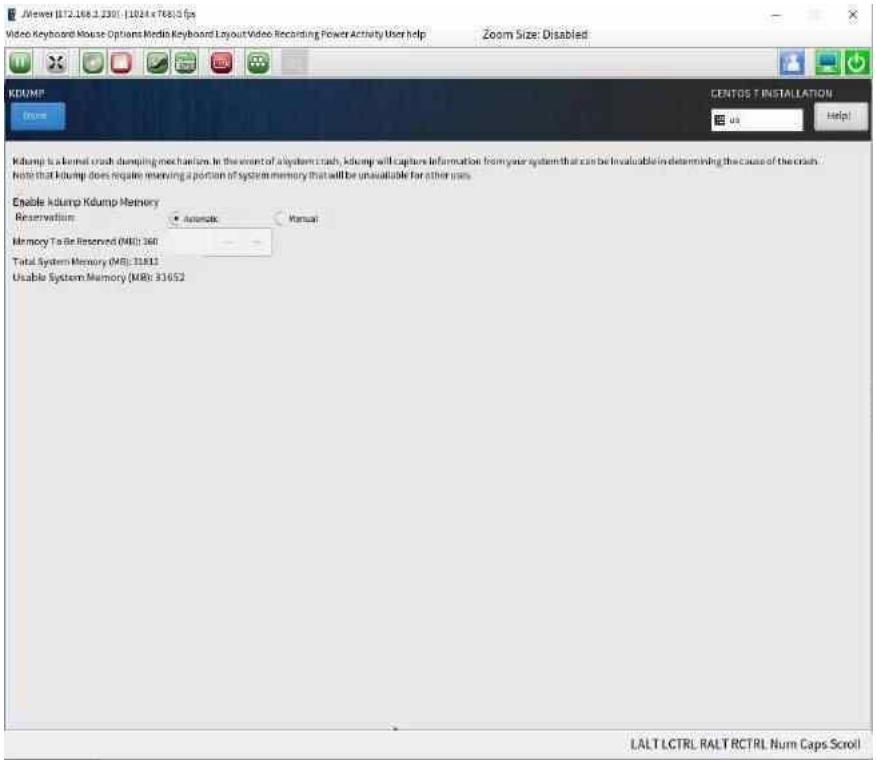


Figure 6-16 KDUMP configuration

Step 16: Click "Network & Hostname" to configure the network information and click Done to save the configuration. (This step can also be configured under the system after the installation of the system is completed);

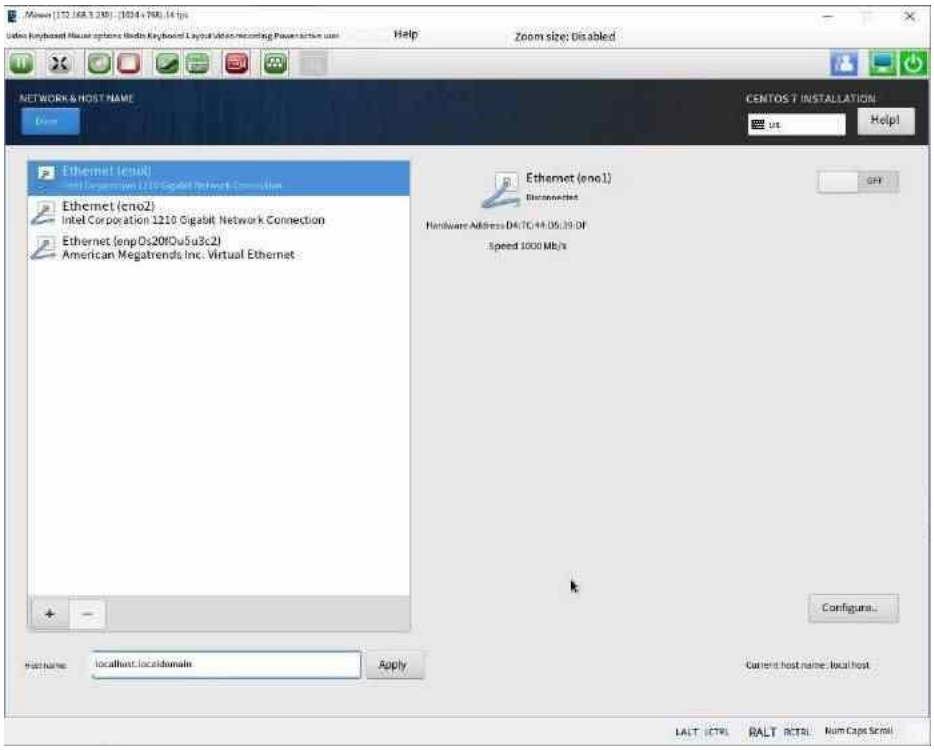


Figure 6-17 Configuring network information

Step 17: Click "SECURTY POLICY" for security configuration and select the default configuration.

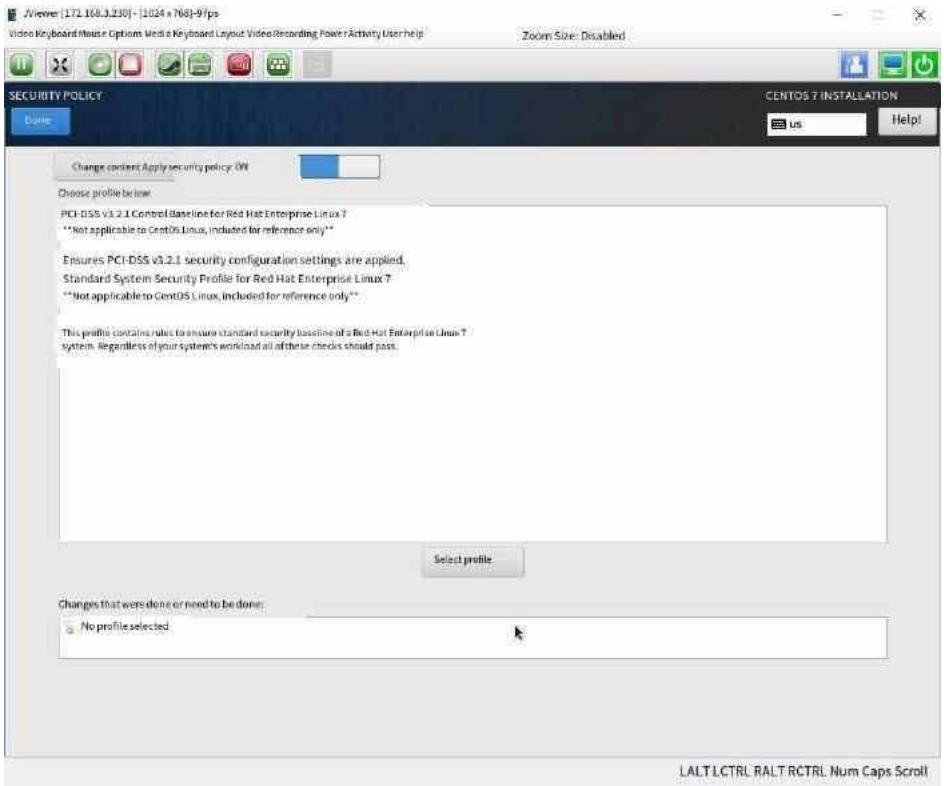


Figure 6-18 Security Policy configuration

Step 18: After the above configuration is complete, click "Begin Installation" to install the system.

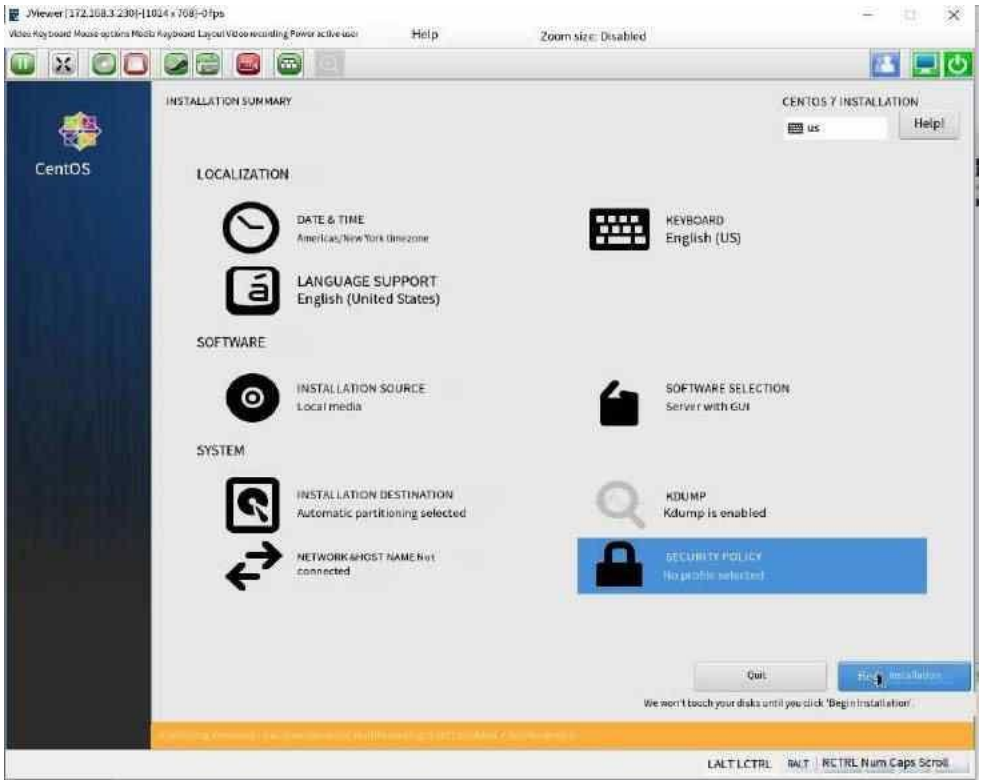


Figure 6-19 System installation

Step 19: Enter the installation screen, click "ROOT PASSWORD" to set the password of the root user according to the password requirements, after the setting, click

Done to save the configuration;

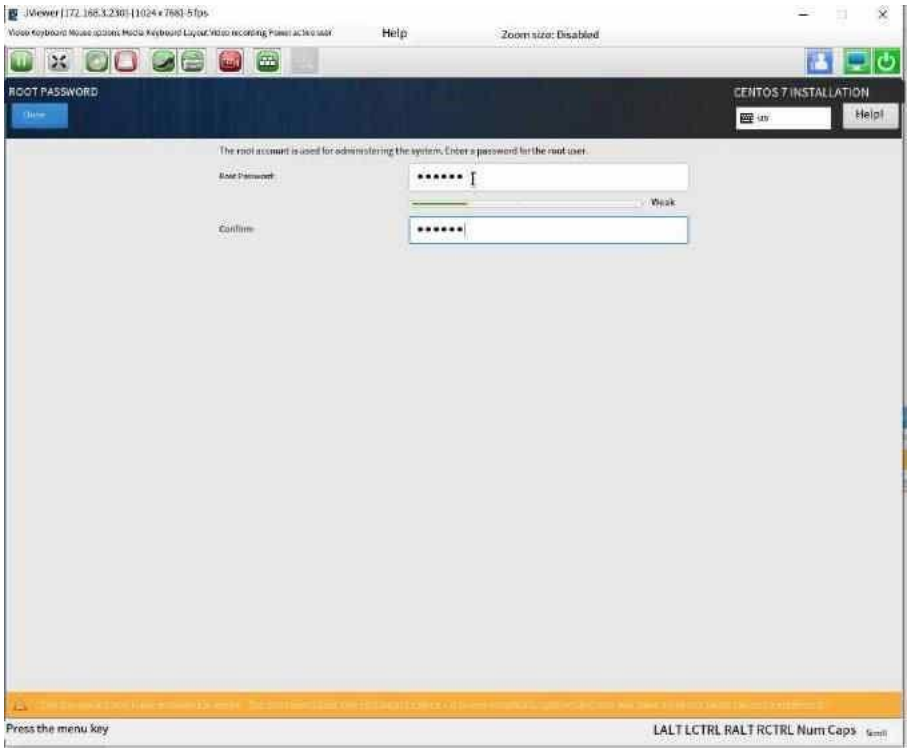


Figure 6-20 Setting the root password

Step 20: Click "USER CREATION" to create a user, enter the user name and password, and click Done to save the configuration;

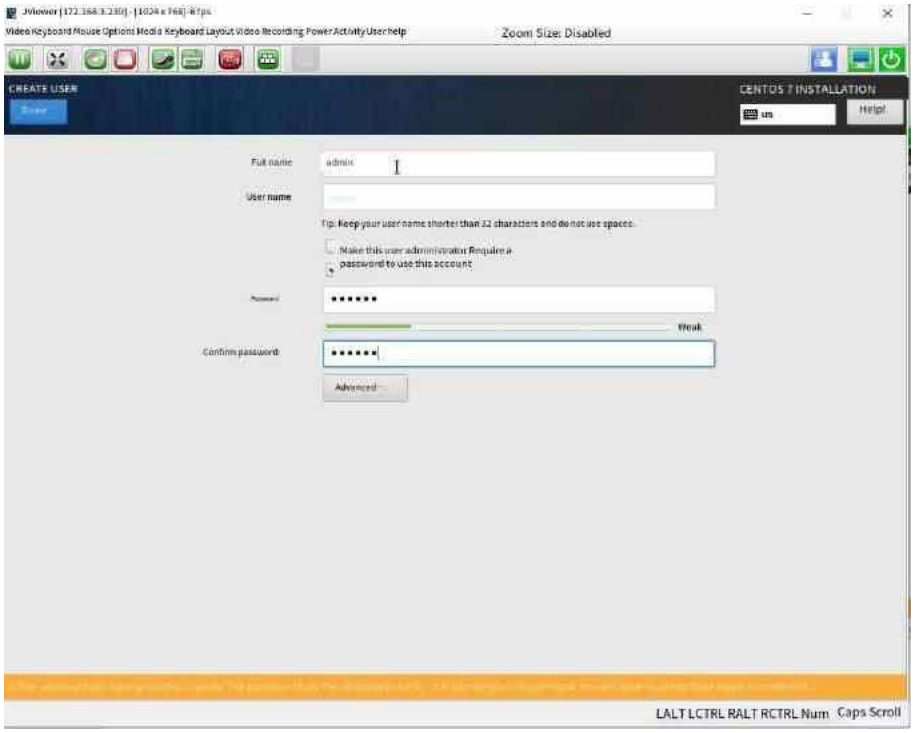


Figure 6-21 Creating a user

Step 21: After the system is installed, click reboot to restart the server.

Figure 6-22 After the OS is installed, run reboot

Step 22 On the boot device screen, select the boot device to be installed. The boot device screen is displayed.

Figure 6-23 System boot screen

6.2 DVD Install OS

6.2.1 Introduction

When installing a DVD system, you need to burn the image to the disc. This section uses the CD-ROM as an example to describe how to install the operating system. Compared with KVM, CD-ROM installation is faster, but less convenient than virtual image mounting.

6.2.2 Making a DVD Boot Disk

Step 1: Open the burning software UltraISO, click File -> Open and select the location of the image file you want to burn;

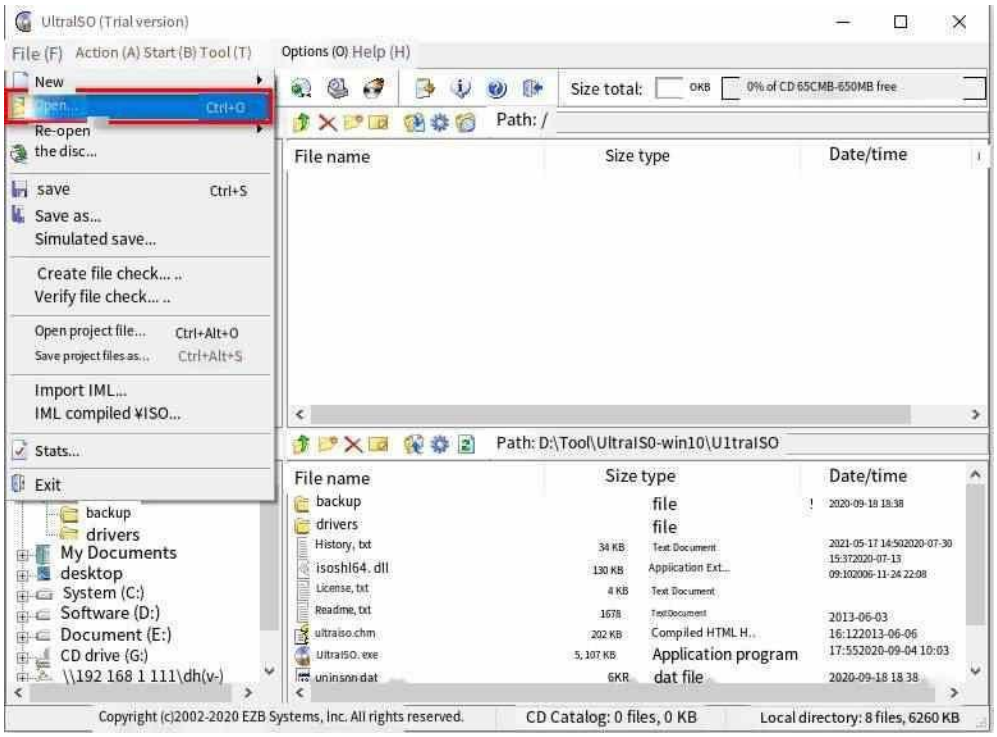


Figure 6-24 Select the image file to burn

Step 2: Click Tools -> Burn CD image to make CD image;

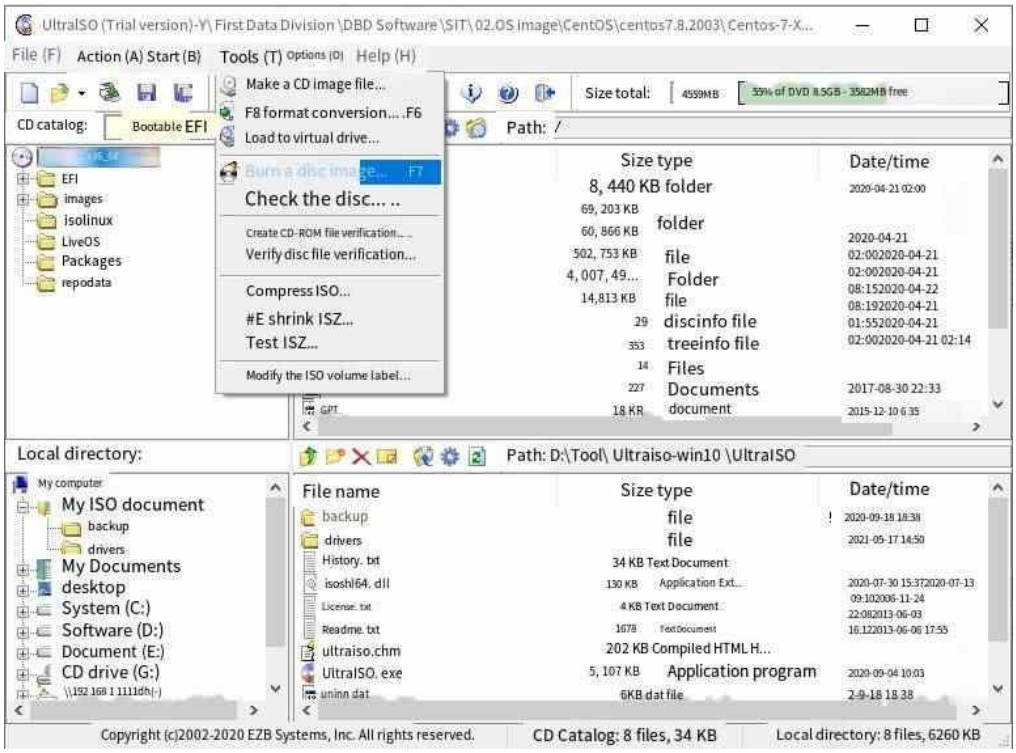


Figure 6-25 Burning a disc image

Step 3: At the burner, select the optical drive you want to burn and click Burn to burn the image of the disc;

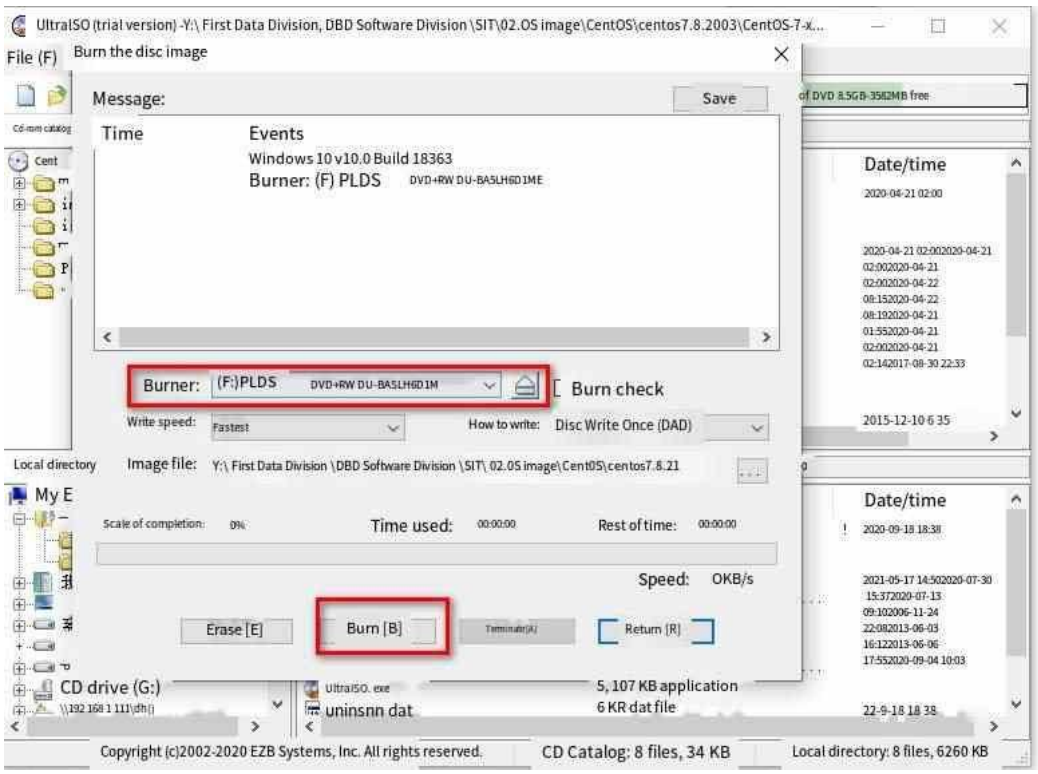


Figure 6-26 Performing the burn operation

Step 4: After burning, close UltraISO and install the CD/DVD-ROM drive to the server;

Step 5: After the server is powered on, press F11 to enter the boot device screen and select the move CD/DVD-ROM drive as the boot device.

Figure 6-27 Select the CD/DVD-ROM drive as the boot device

Step 6: After the boot device is selected, the system installation screen is displayed as follows. For other installation steps, repeat Step 8 to Step 22 in 6.1.3.

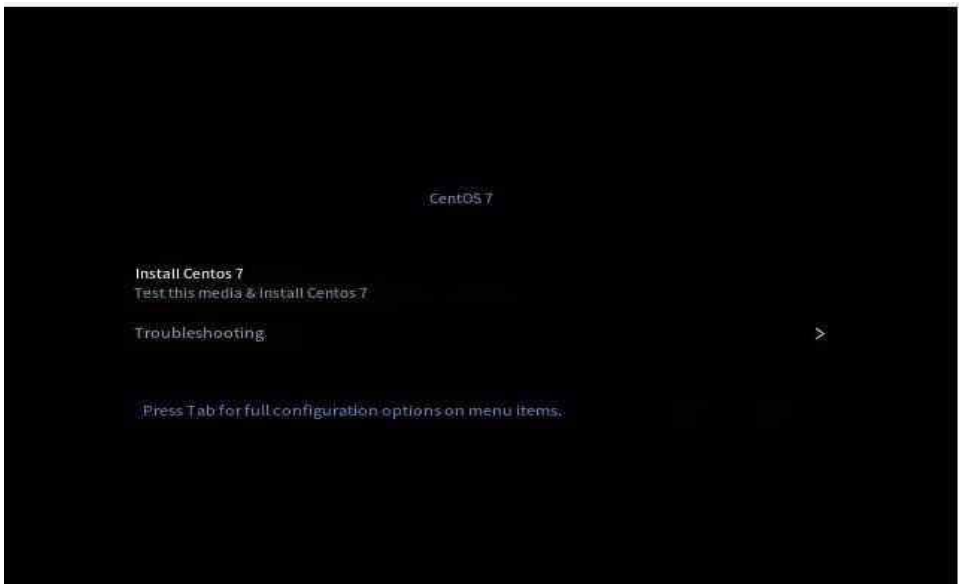


Figure 6-28 System installation screen

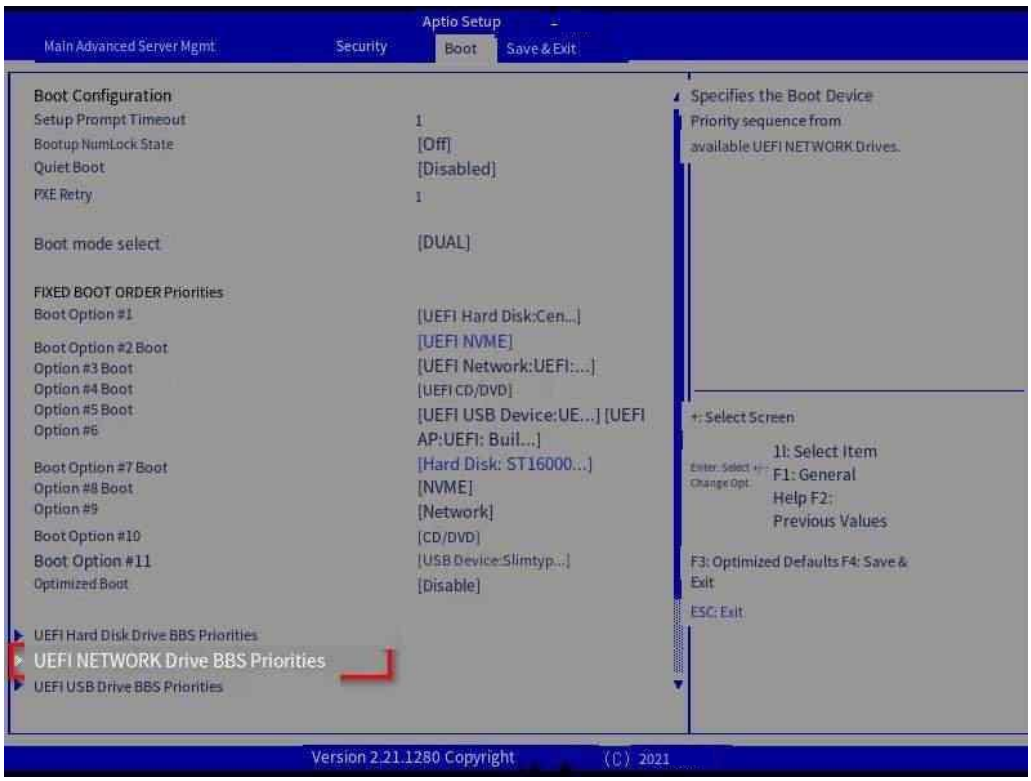
6.3 Installing an OS on PXE

6.3.1 Introduction

PXE(Pre-boot Execution Environment) is a protocol designed by Intel that enables computers to boot over a network. The protocol is divided into client and server. The PXE client is in the ROM of the network adapter. When the computer starts, the BIOS transfers the PXE client to the memory for execution and displays the command menu. After the user selects the PXE client, the PXE Client downloads the remote operating system to run on the local computer through the network. Therefore, you need to set up your own PXE environment, and the system source to be installed has been deployed in the PXE environment.

6.3.2 Boot from PXE

Step 1: When the server is powered on, go to BIOS setup->Boot->UEFI NETWORK Drive BBS Priorities. On this screen, you can change the boot sequence of the PXE boot network adapter.



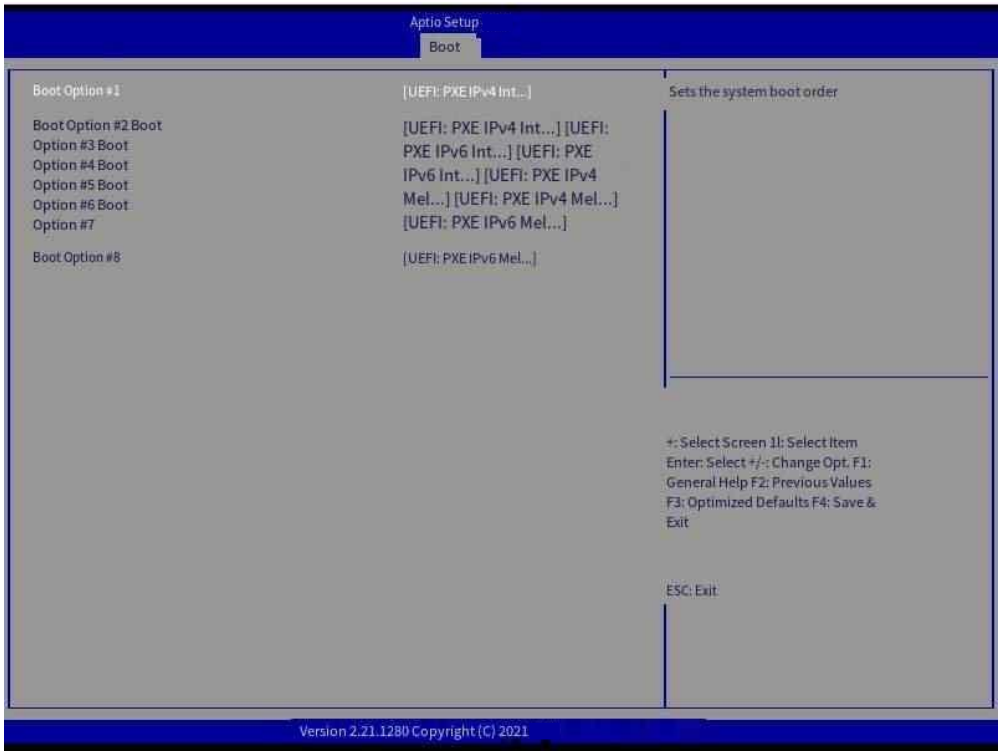


Figure 6-29 UEFI NETWORK Drive BBS Priorities screen

Note: You can also press the F12 shortcut key to go to the PXE boot screen when Please <F12> to enter PXE boot is displayed after the server is powered on and p owered on.

Figure 6-30 F12 The PXE boot option screen is displayed

Step 2: The PXE environment is automatically displayed. Select a network port to enter the PXE environment.

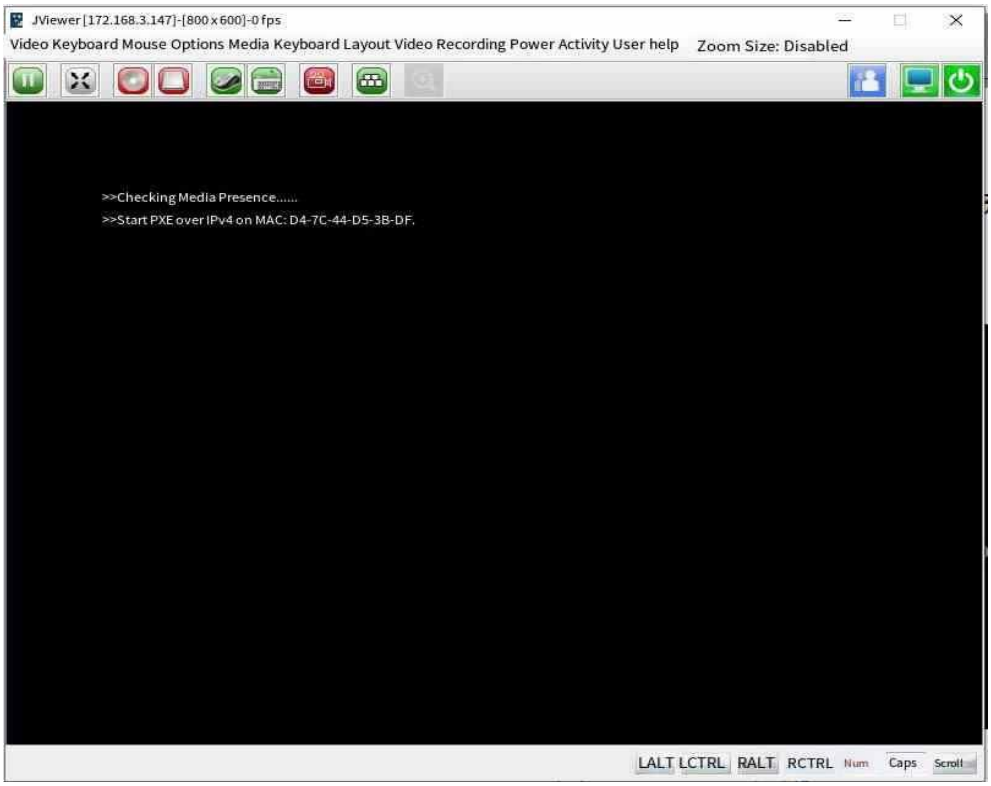


Figure 6-31 Selecting a network port to enter the PXE environment

Step 3: Enter the PXE environment and select the system source to be installed (Cent OS 7.8 is used as an example).

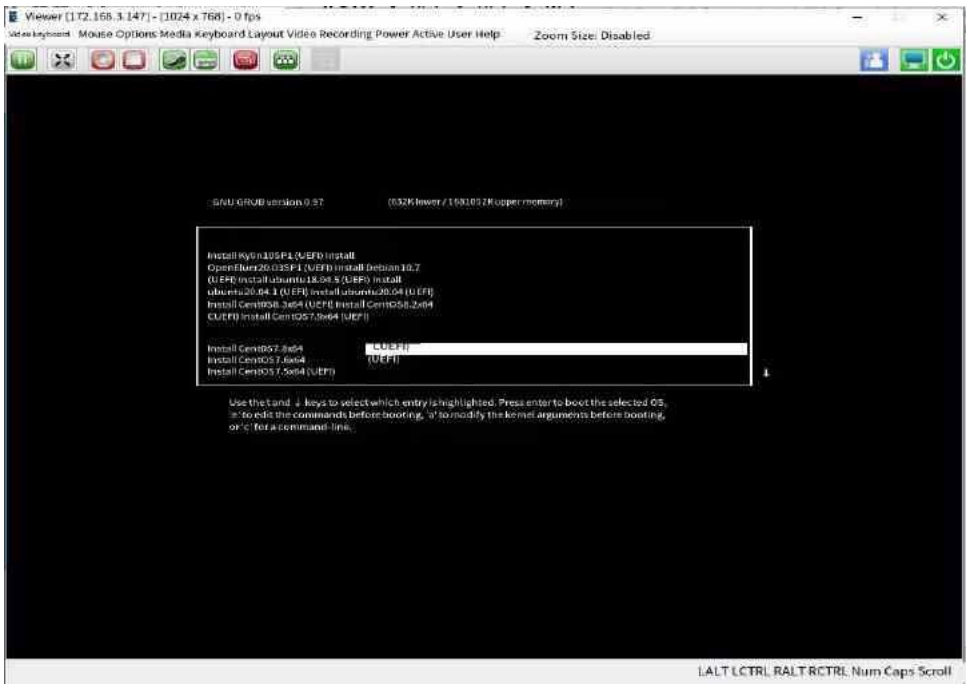


Figure 6-32 Selecting a system installation source

Step 4: After selecting the system installation source, go to the system installation page as shown below. For other installation steps, repeat Step 8 to Step 22 in 6.1.3.

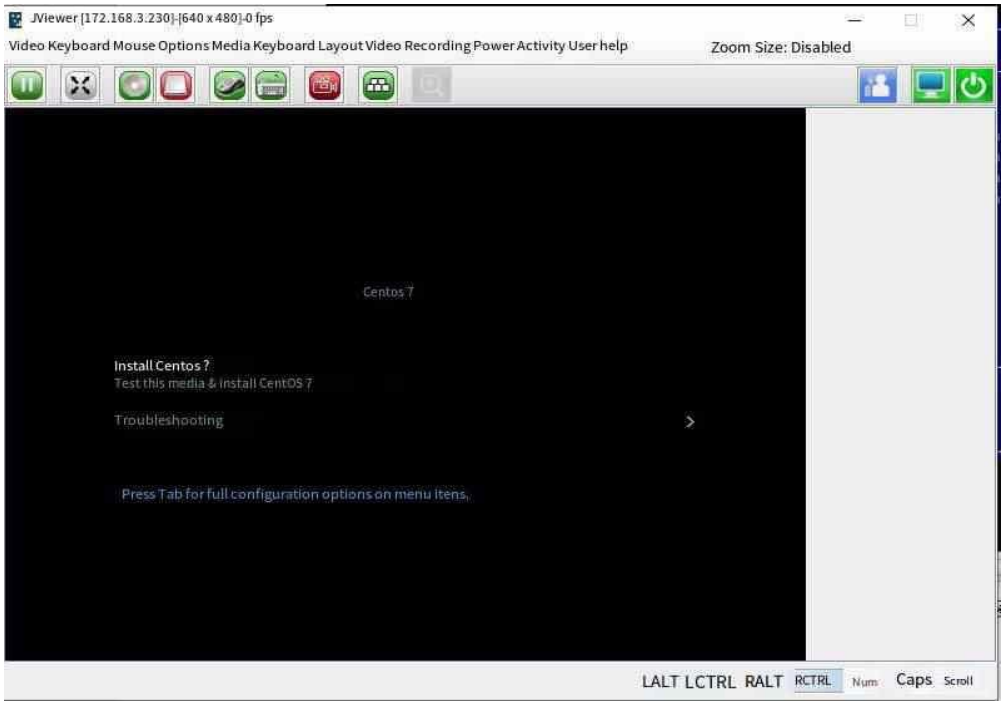


Figure 6-33 System installation screen

Chapter 7 RAID Card Operation Guide

7.1 94060-8i RAID Controller Card

This chapter describes how to operate the 9460-8i controller.

The Avago MegaRAID SAS 940-8I RAID card (hereinafter referred to as 940-8I) is an 8-port 12Gbit/s SAS controller based on the MegaRAID architecture, and uses the PCIe3.0x8 interface to provide a powerful I/O storage engine. Performs all data protection, verification, and recovery tasks transparently.

The 9460-8i improves system performance, provides fault-tolerant data storage, supports data storage in multiple hard disk partitions, and supports multiple hard disk read/write access at the same time, effectively reducing hard disk data access delay.

The 9406-8I supports the use of hard drives in passthrough mode and RAID group creation.

7.1.1 RAID Levels and Parameters

The following table lists the RAID types supported by the 9460-8i and the number of hard drives.

Table 7-1 RAID-hard drive parameters

RAID level	Number of supported hard drives	Number of supported subgroups	Number of hard drives supported by subgroups	Number of bad drives allowed
RAID 0	1 ~ 32	Not involved	Not involved	0
RAID 1	2 to 32 (even numbers)			Number of hard drives ÷ 2
RAID 5	3 ~ 32			1
RAID 6	3 ~ 32			2
RAID 10	4~240 (even numbers)	2 to 8 RAID 1	2 to 32(even number)	Number of subgroups
RAID 50	6-240	2 to 8 RAID 5	3 ~ 32	Number of subgroups
RAID 60	6-240	2 to 8 RAID 6	3 ~ 32	Number of subgroups x2

NOTE

RAID 00 level is not supported;

The damaged hard drive cannot be continuous;

Number of sub-groups: The number of sub-RAID groups, for example, RAID 50 consists of two RAID 5s, then the number of sub-groups is 2;

Each subgroup of RAID 10 and RAID 50 allows a maximum of one failed drive.

A maximum of two failed drives are allowed in each subgroup of RAID 60. ● The total number of hard drives in RAID10, 50, and 60 is determined by the number of subgroups and the number of hard drives supported by the subgroup.

7.1.2 Log in to the management page of the 94060-8I card

The 940-8I does not support Legacy configuration, but UEFI configuration. Both Legacy and UEFI boot are supported.

To do so:

Step 1: When the following information is displayed on the screen during POST startup, press Delete to enter the BIOS interface.

Figure 7-1 BIOS startup screen

Step 2: Select Advanced->Dunamic UEFI Oprom Select AVAGO<AVAGO MegaRAID SAS 9460-8i> Configuration Utility (Figure 7-2), Press enter to go to the RAID card management screen (Figure 7-3).

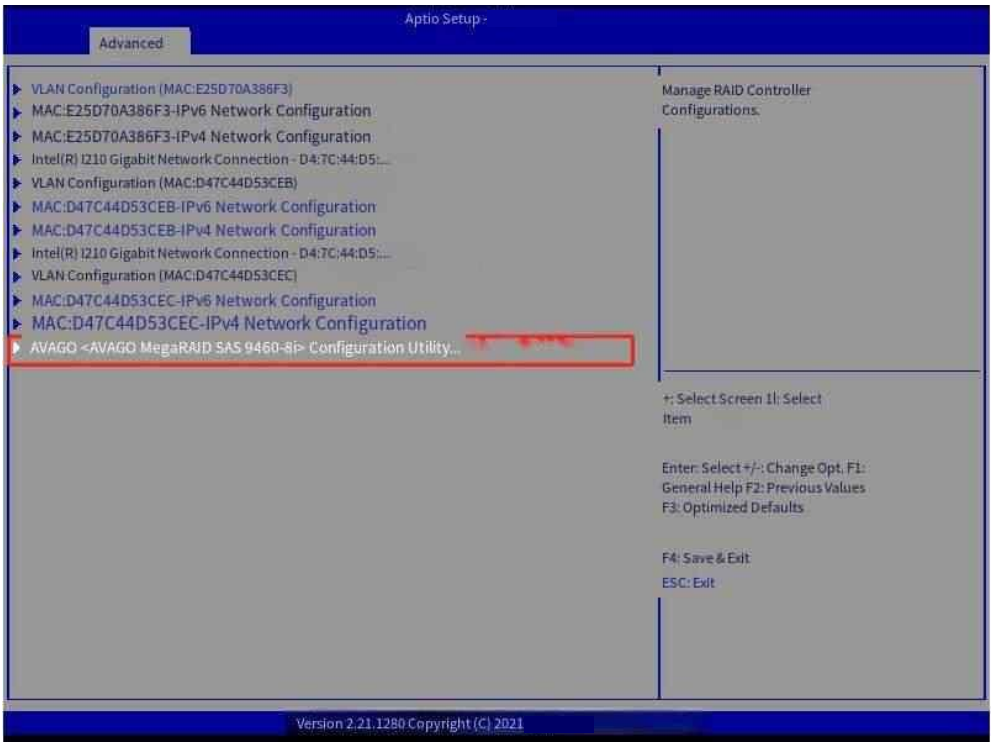


Figure 7-2 Information about the RAID card in Dunamic UEFI Oprom

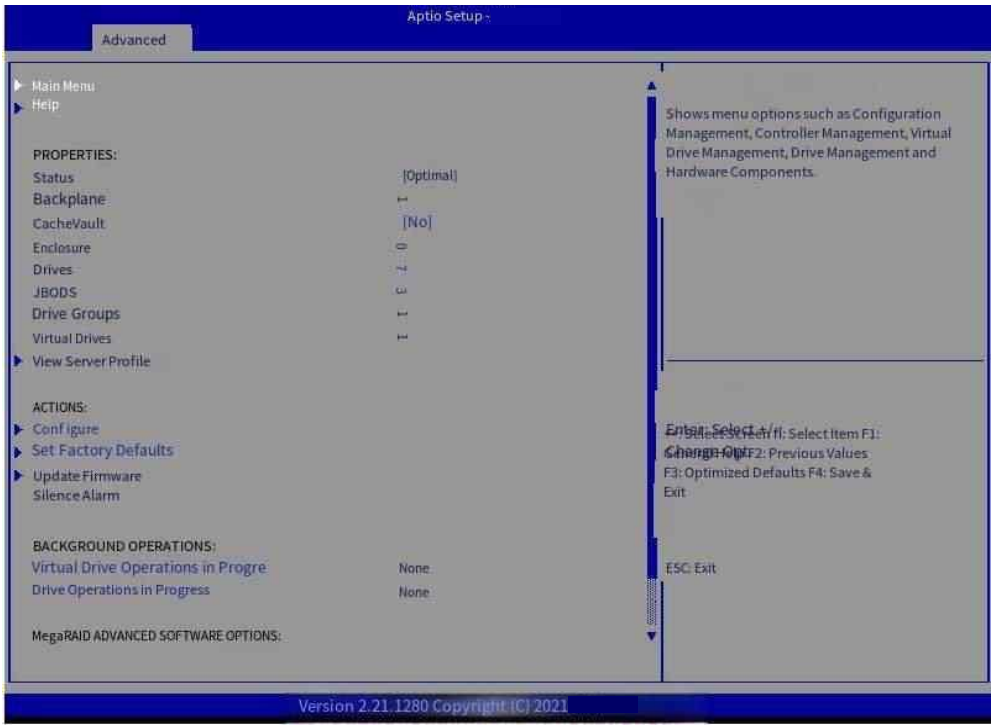


Figure 7-3 RAID card management page

Table 7-2 Parameter description

argument	Instructions
Main Menu	The main menu of the RAID controller card contains all operations of the RAID controller card.
Help	Get help information.
Status	Current operating status of the RAID controller card.
Backplane	Number of backplanes.
Enclosure	Number of components.
Drives	Number of mounted hard disks.
Drive Groups	Number of existing disk groups.
Virtual Drives	Number of existing virtual disks.
View Server Profile	View and manage RAID card features.
View Foreign Configuration	View and manage external configurations.
Configure	Provides interfaces for creating RAID arrays, quickly creating RAID arrays, viewing disk group properties, clearing all current RAID configurations, and managing external configurations.
Set Factory Default	factory data reset.
Update Firmware	Upgrade the firmware.
Silence Alarm	Enable status of the onboard buzzer.
Virtual Drive Operations in Progress	Whether a vdisk operation is being processed in the background.
Drive Operations in Progress	Check whether a disk operation is being processed in the background.
MegaRAID xxx	Enable status of advanced features.
Manage MegaRAID Advanced Software	Manage advanced features.

Step 3: Move the cursor to the Main Menu and type Enter to go to the main menu of the RAID controller card (Figure 7-4).

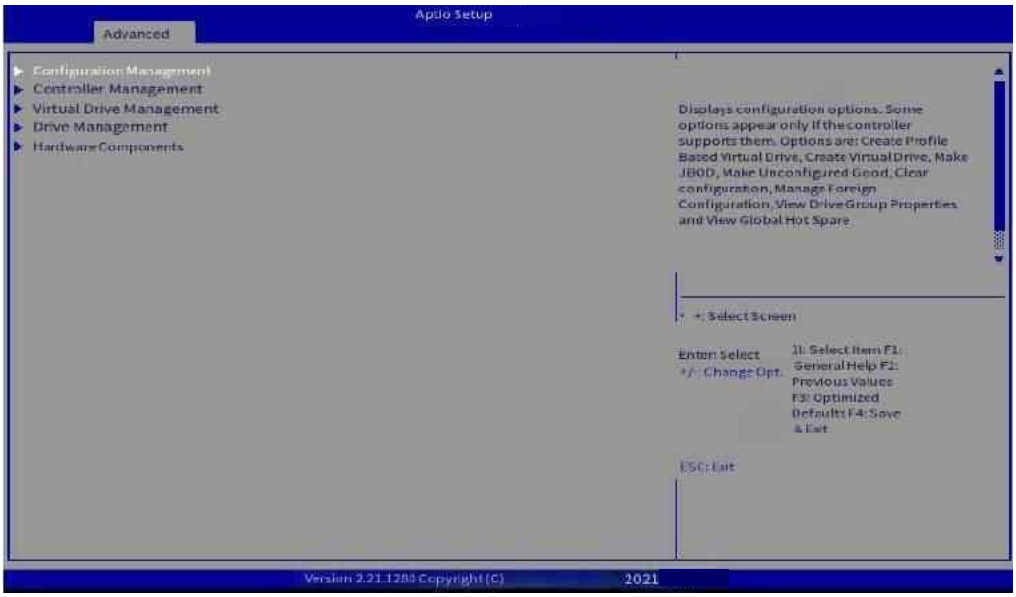


Figure 7-4 Moving the cursor to Main Menu type Enter

The parameters are described as follows:

Table 7-3 Parameters on the main menu

argument	Subarguments
Configuration Management	Displays configuration options. Some options will only appear if the controller supports them. Options include :create Profile Based virtua,create virtual Drive Make JBOD, Make Unconf igured Good, Clear configuration,Manage Foreign Configuration,View Drive Group Properties和View Global Hot spare
Controller Management	Query the status and basic attributes of the controller, such as the product name, serial number, PCID, irmuare version, and NVDATA version. You can also use the Advanced link to view other properties and perform other tasks such as changing the security key, saving the TTY log, etc.
Virtual Drive Management	You can manage virtual drive properties, view basic virtual drive properties, and perform background initialization and consistency check. You can also use the Advanced link to view other properties.
Drive Managemant	Displays the basic properties of a disk, and performs operations such as assigning or canceling a hot spare disk, locating a disk, taking a disk offline/online, and rebuilding a disk. You can also use the Advanced link to view other properties.
Hardware Components	Displays battery and enclosure status if applicable. You can also use the Advanced link to view other properties and perform other actions. Some options will only appear if the controller supports them

7.1.3 Creating RAID Group Columns

The 940-8I supports RAID0/1/5/6/10/50/60 on the Fusionstor i6427 rack server.

Note:

Data on the hard drives added to the RAID group will be deleted. Before creating the RAID group, ensure that there is no data on the hard drives or data does not need to be retained.

The 9460-8i supports SAS/SATA HDD and SAS/SATA SSD. The same RAID group must use the same type of hard drives, but can use hard drives with different capacities or from different manufacturers.

7.1.3.1 Creating RAID0 Group columns

To do so:

Step 1: Go to the Create Virtual Drive screen, select Main Menu->Configuration Management->Create Virtual Drive and press Enter;

Step 2: Open the RAID configuration screen, Select a RAID Level, use ↑ and ↓ to select Select RAID Level and press Enter, select RAID 0 from the displayed list, and press Enter (Figure 7-5) :

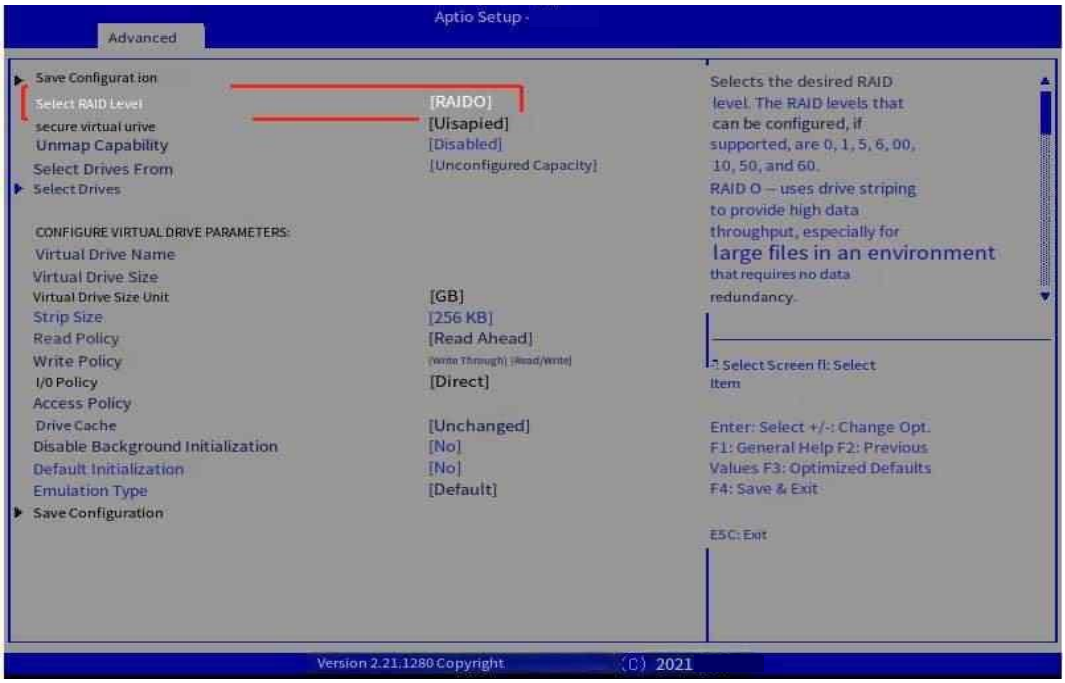


Figure 7-5 Select a RAID level screen

Step 3: Use ↑ and ↓ to Select Select Drives and press Enter, after selecting the member drives you want to create RAID0, Click "Apply Changes->OK->Save Configuration" to create RAID (Figure 7-6, Figure 7-7, Figure 7-8, Figure 7-9);

Figure 7-6 Select two disks to create RAID0

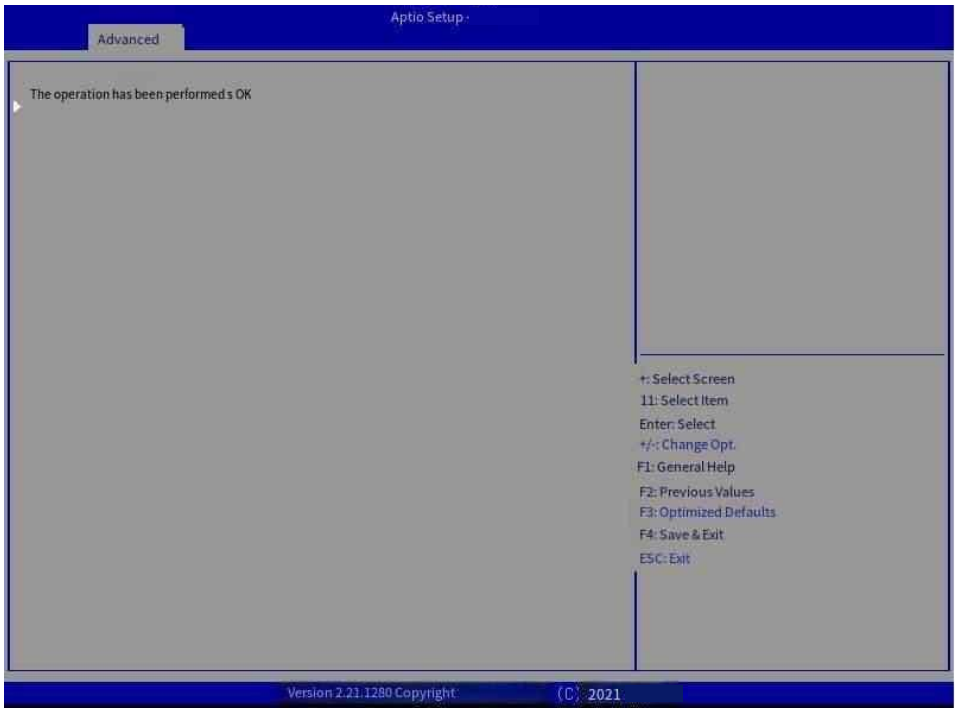


Figure 7-7 Click OK

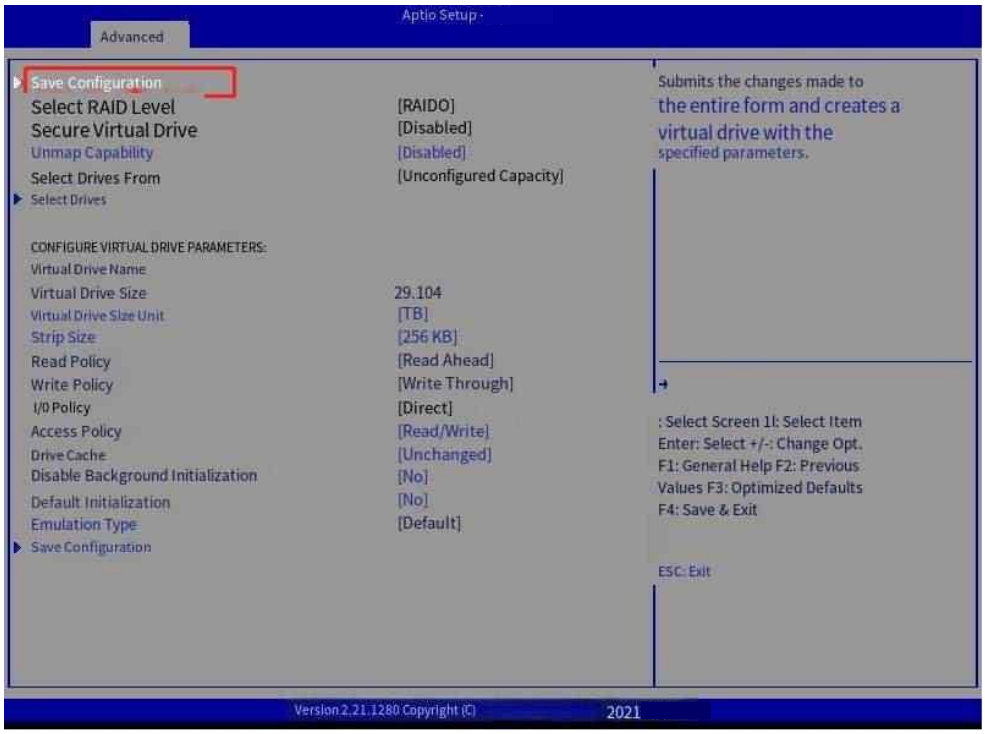


Figure 7-8 Press enter to select Save Configuration

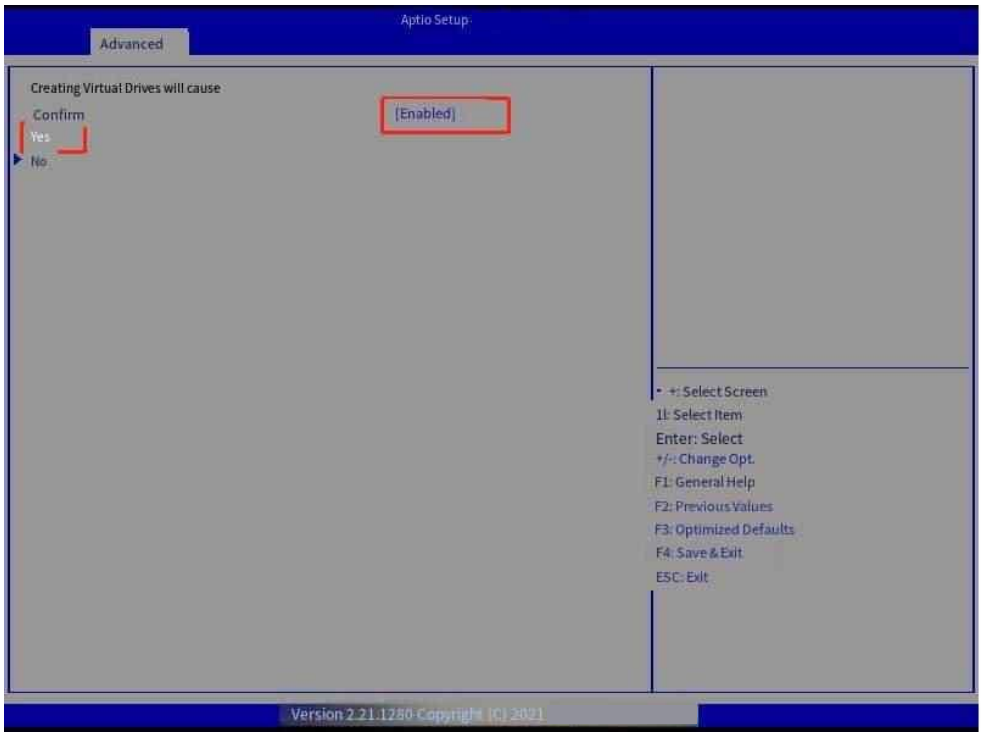


Figure 7-9 confirm Click Yes after selecting Enabled

Step 4: Press ESC to return to the upper screen, select Virtual Drive Management and press Enter (Figure 7-10);

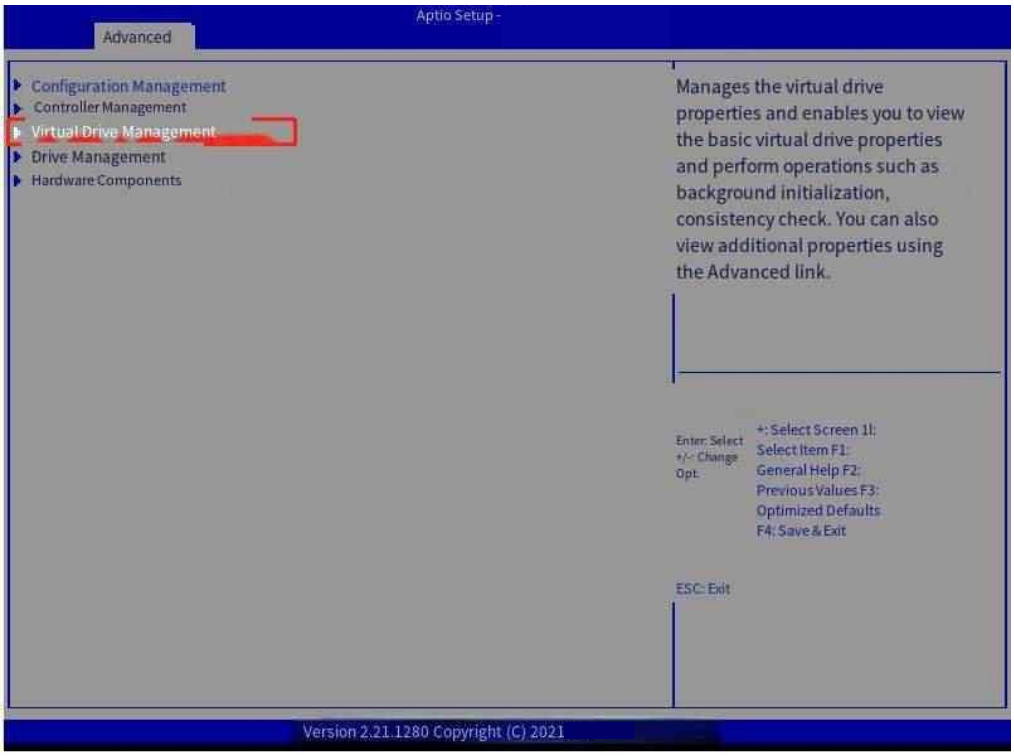


Figure 7-10 RAID home screen

Step 5 On the Virtual Drive Management screen, you can view the RAID array created under the controller, as shown in Figure 7-11.

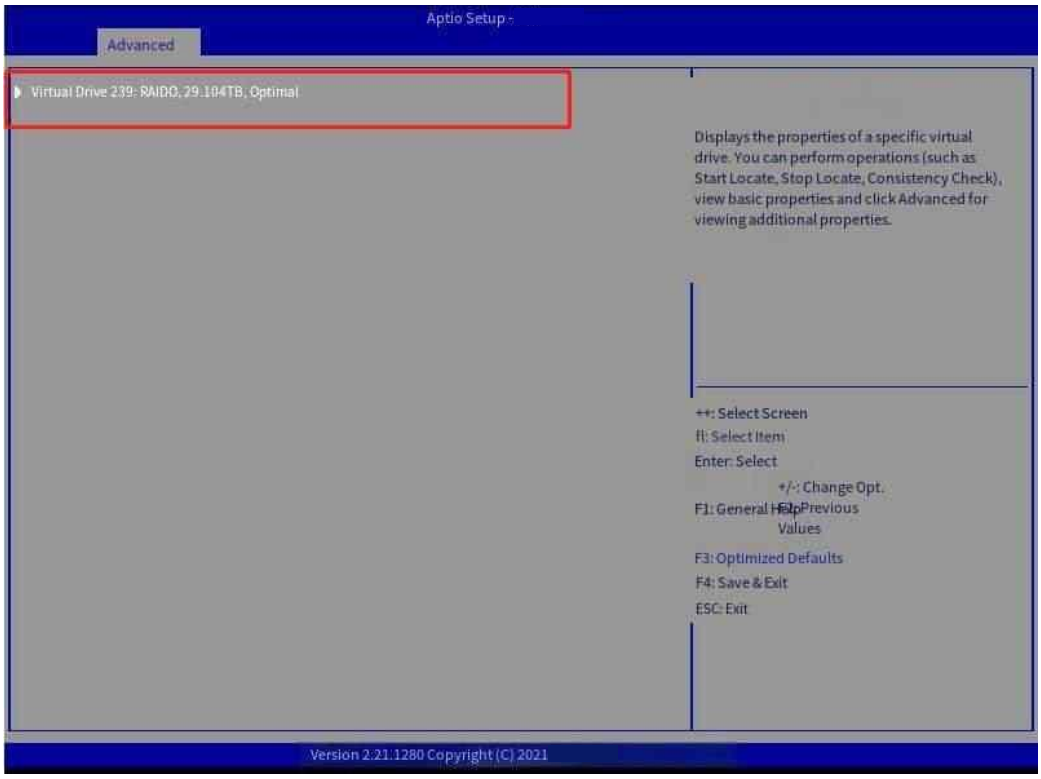


Figure 7-11 Viewing RAID information

7.1.3.2 Creating RAID1 Group Columns

To do so:

Step 1: Go to the Create Virtual Drive screen, select Main Menu->Configuration Management->Create Virtual Drive and press Enter;

Step 2: On the RAID configuration screen, Select a RAID Level and use ↑ and ↓ to select Select RAID Level and press Enter. On the displayed list, select RAID 1 and press Enter (Figure 7-12).

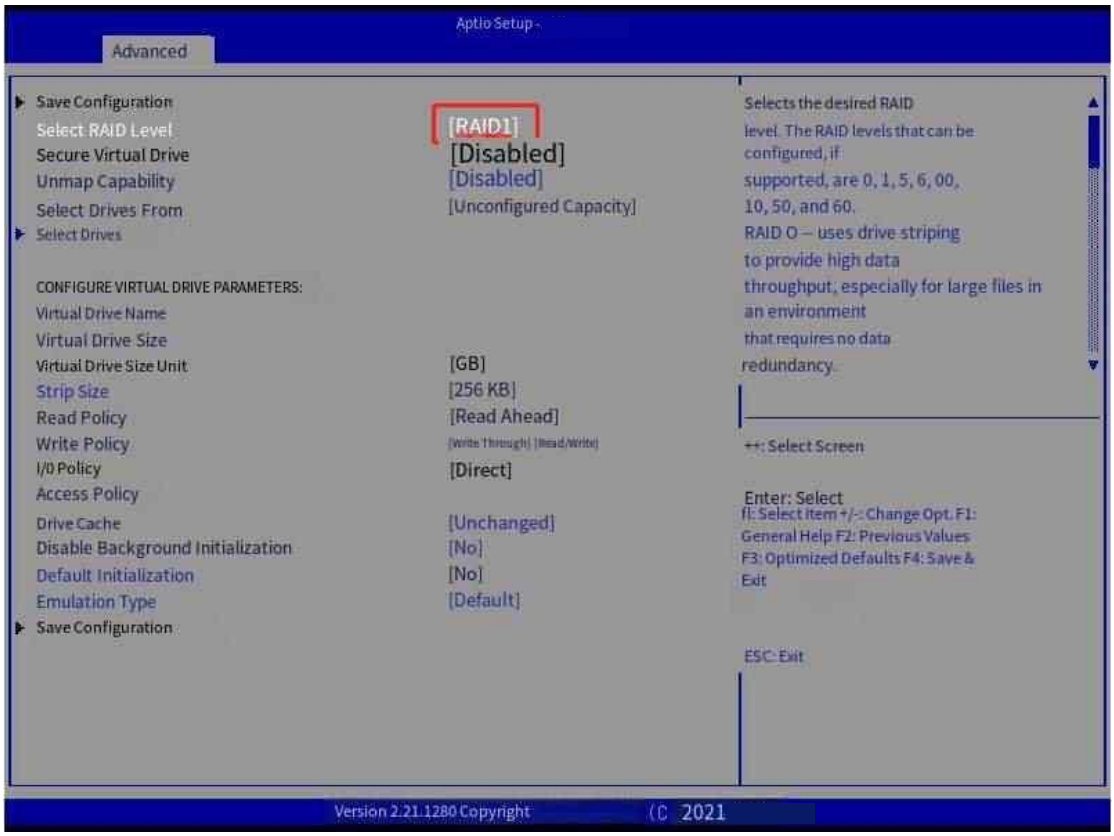


Figure 7-12 Select a RAID level screen

Step 3: Use ↑ and ↓ to Select Select Drives and press Enter. Select member drives to create RAID0 and click Apply Changes->OK->Save Configuration to create a RAID

(Figure 7-13, Figure 7-14, Figure 7-15, Figure 7-16, Figure 7-17);

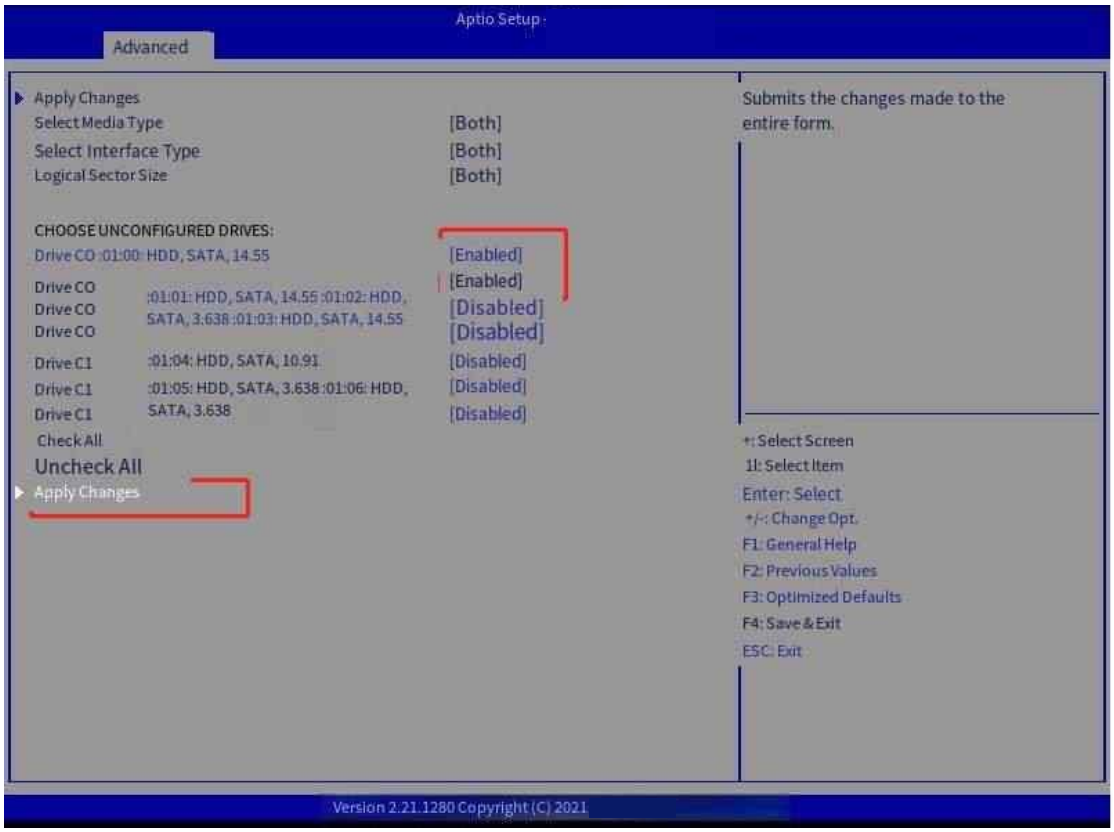


Figure 7- 13 Select two disks to create RAID 1

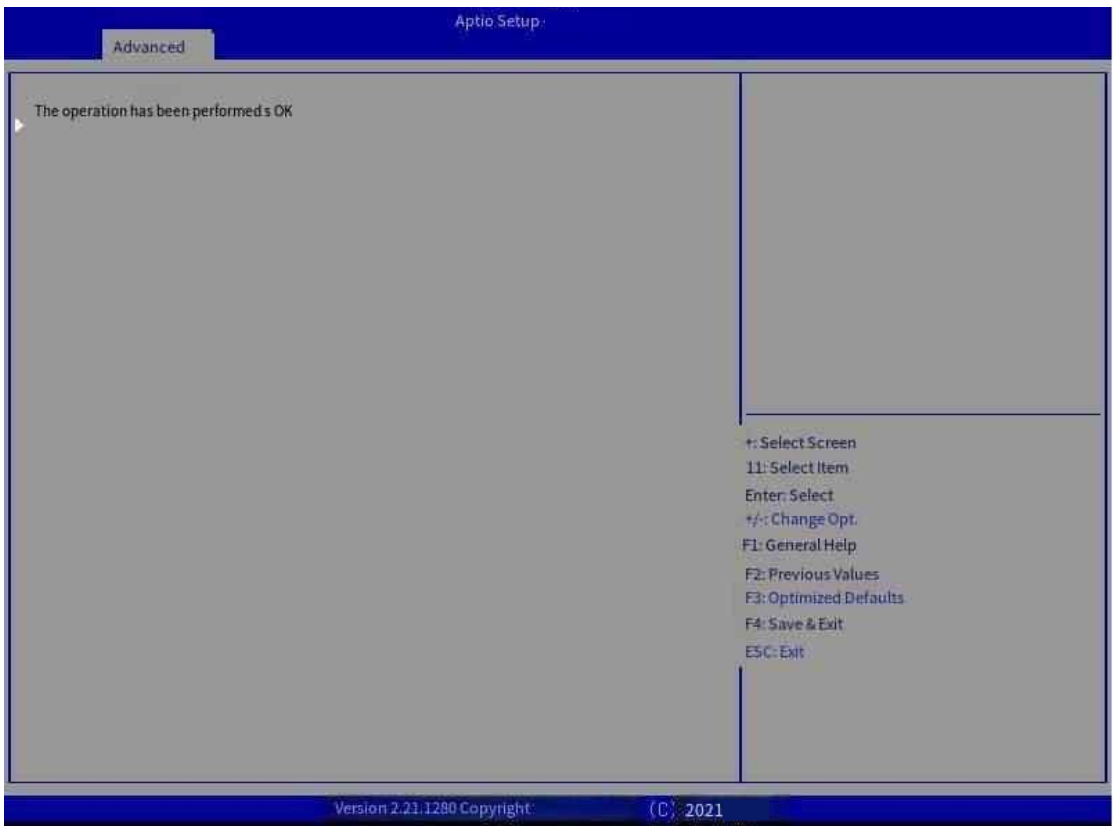


Figure 7-14 Click OK

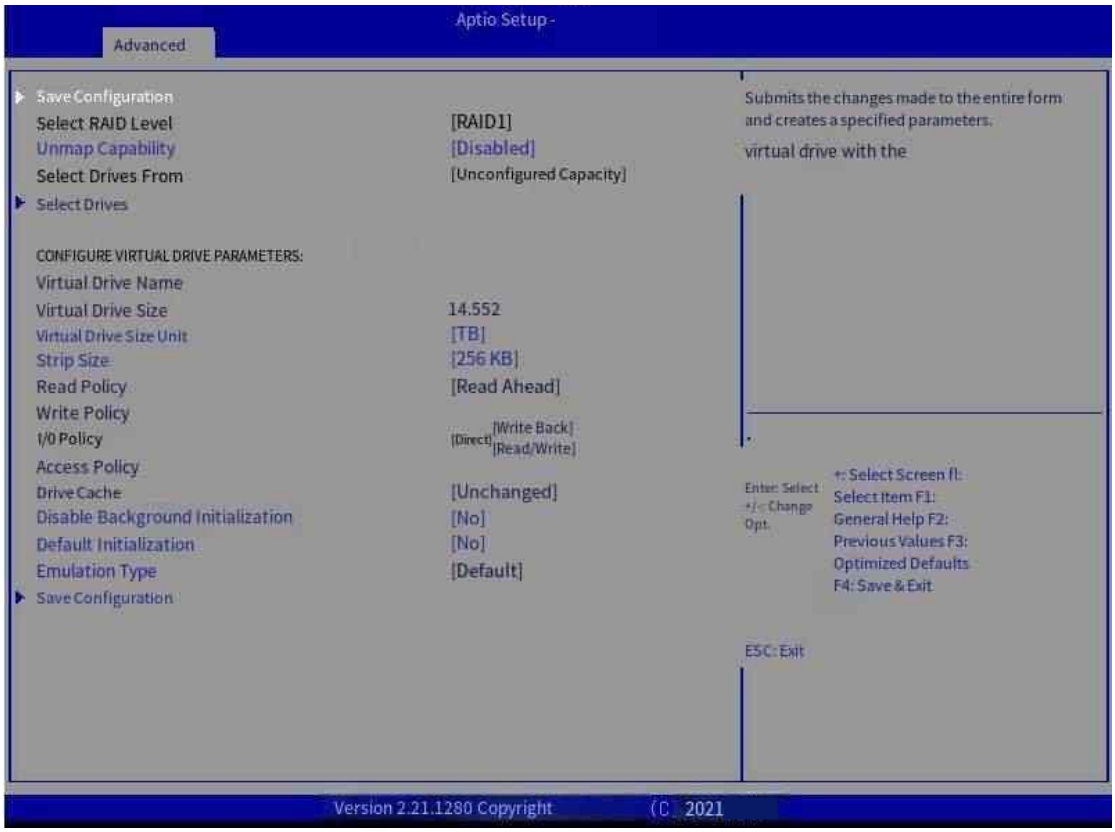


Figure 7-15 Press enter to select Save Configuration

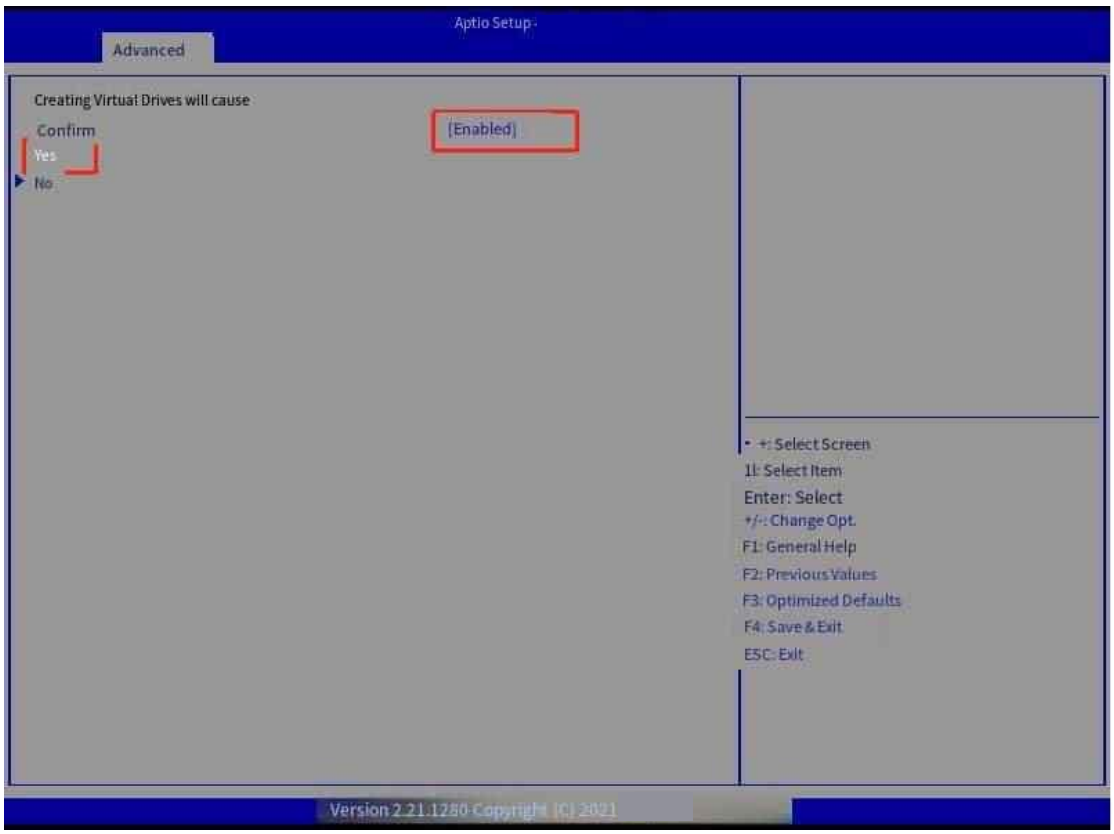


Figure 7-16 confirm Click Yes after selecting Enabled

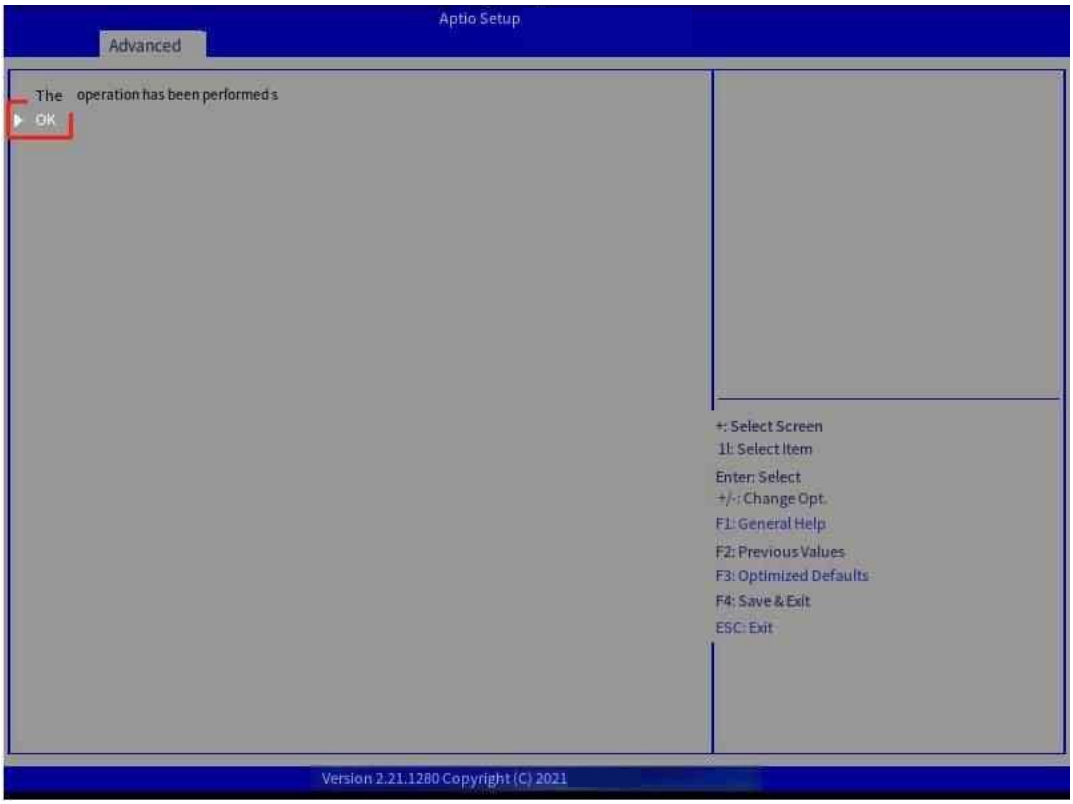


Figure 7-17 Click ok

Step 4: Press ESC to go back to the upper screen, select Virtual Drive Management and press Enter (Figure 7-18);

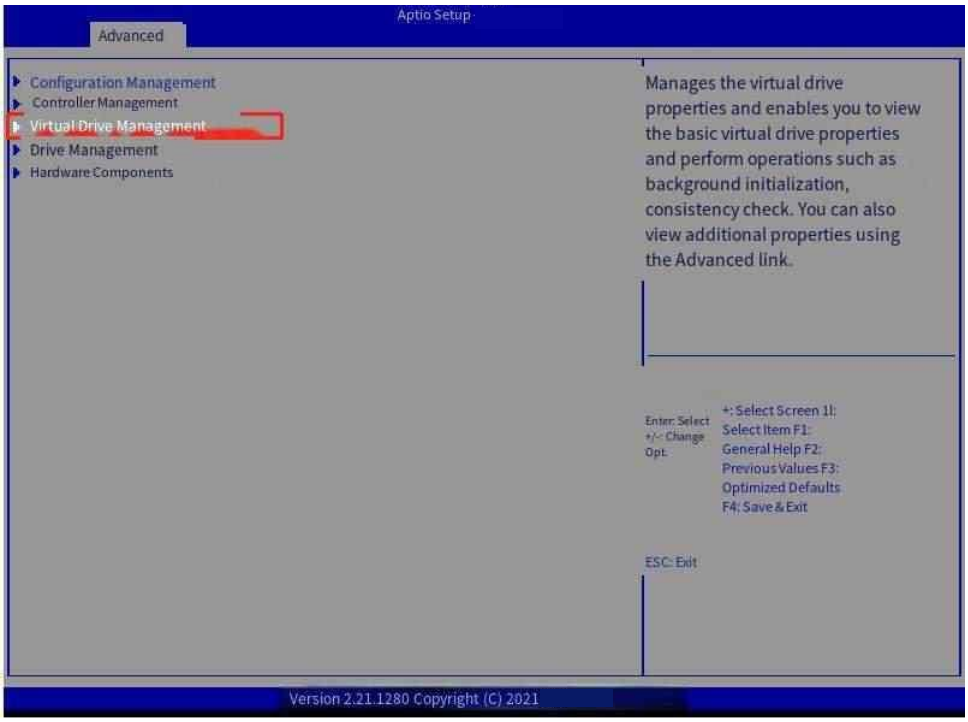


Figure 7-18 RAID home screen

Step 5 The Virtual Drive Management screen is displayed. On the screen, you can view the RAID array created under the controller, as shown in Figure 7-19.

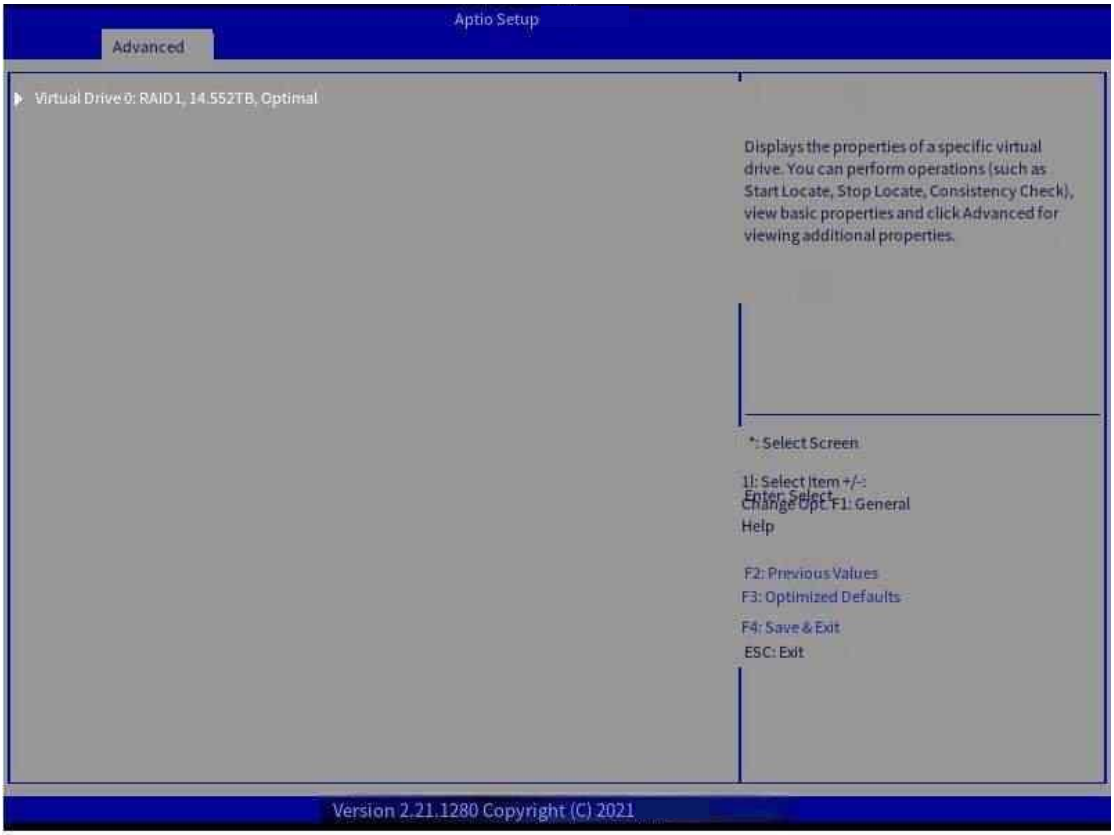


Figure 7-19 Viewing RAID properties

7.1.3.3 Creating RAID5/6 Group columns

Create RAID5/6 using the same method as RAID0 and RAID1. After accessing the Main Menu of RAID group, Choose Configuration Management >Creat Virtual Drive >Select RAID Level >RAID5/6 to create a RAID5/6 column (see Figure 7-20 and Figure 7-21). The following steps are the same as those for RAID0/RAID1. Note: To form RAID5/6, the number of hard disks must be greater than 3

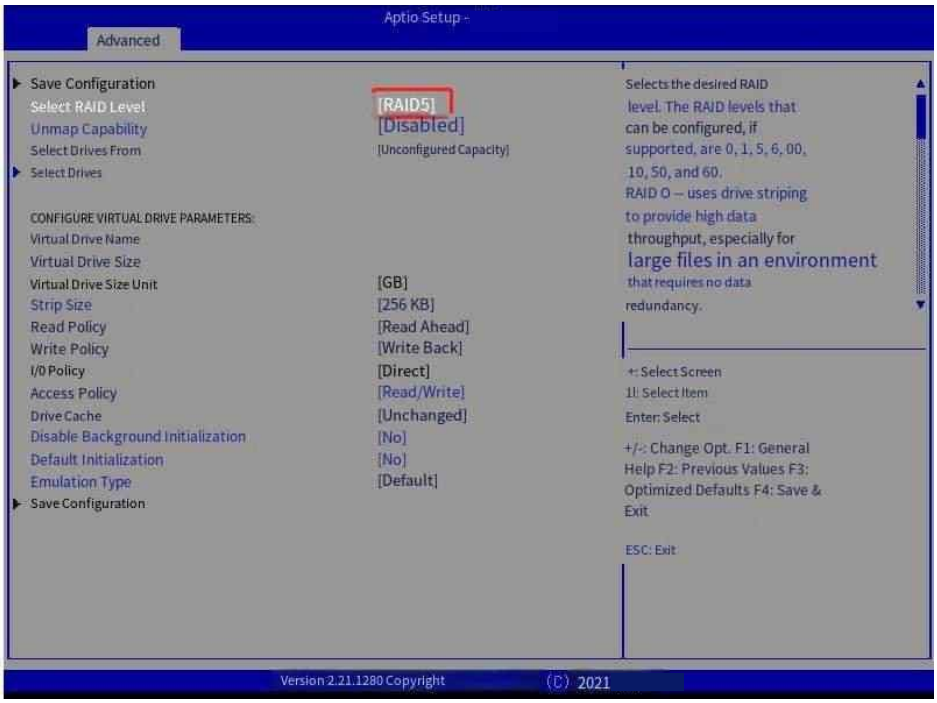


Figure 7-20 Select RAID level screen Select RAID5

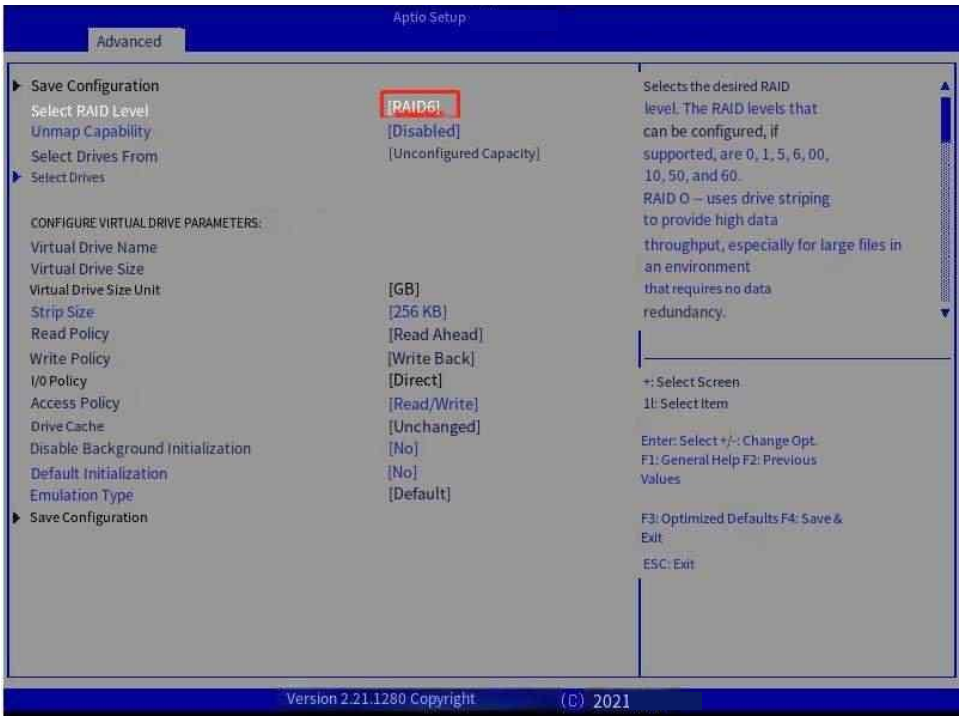


Figure 7-21 Select a RAID level screen, select RAID6

7.1.3.4 Creating RAID10 Group Columns

Step 1: Go to the Create Virtual Drive screen, select Main Menu->Configuration Management->Create Virtual Drive from the main screen and press Enter;

Step 2: Open the RAID configuration screen, Select a RAID Level, use ↑ and ↓ to select Select RAID Level and press Enter, select RAID 10 from the displayed list, and press Enter (Figure 7-22) :

Figure 7-22 Select a RAID level screen

Step 3: Use ↑ and ↓ to Select Select Drives From and press Enter. Select member drives to create Span 0 and click Apply Changes->OK to create Span 0 (Figure 7-23, Figure 7-24).

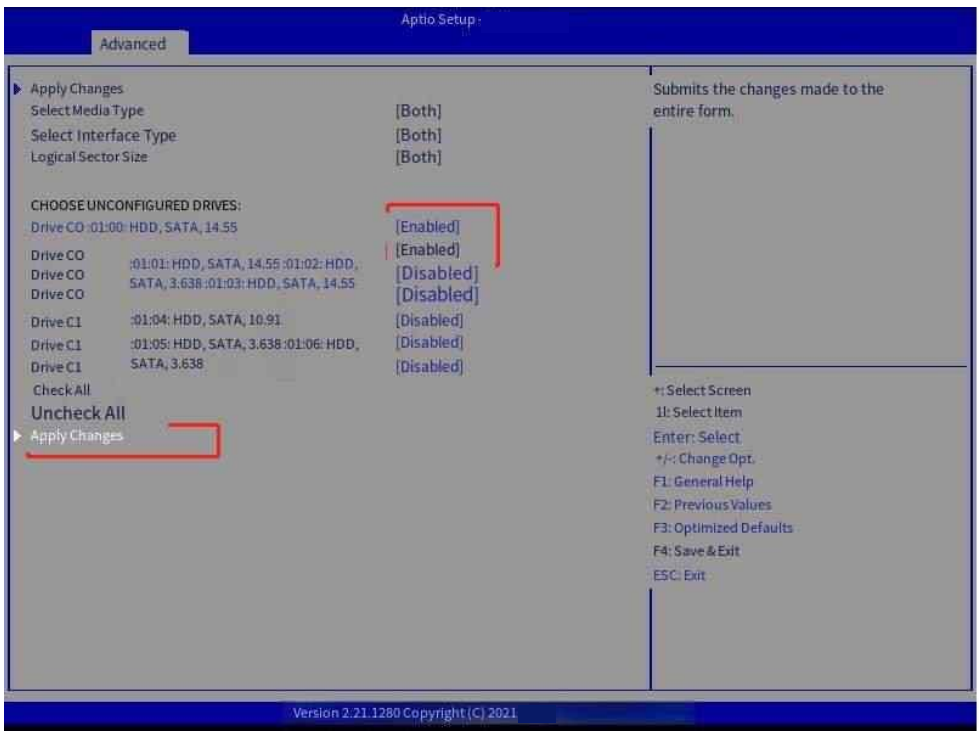


Figure 7-23 Select two drives to create Span0

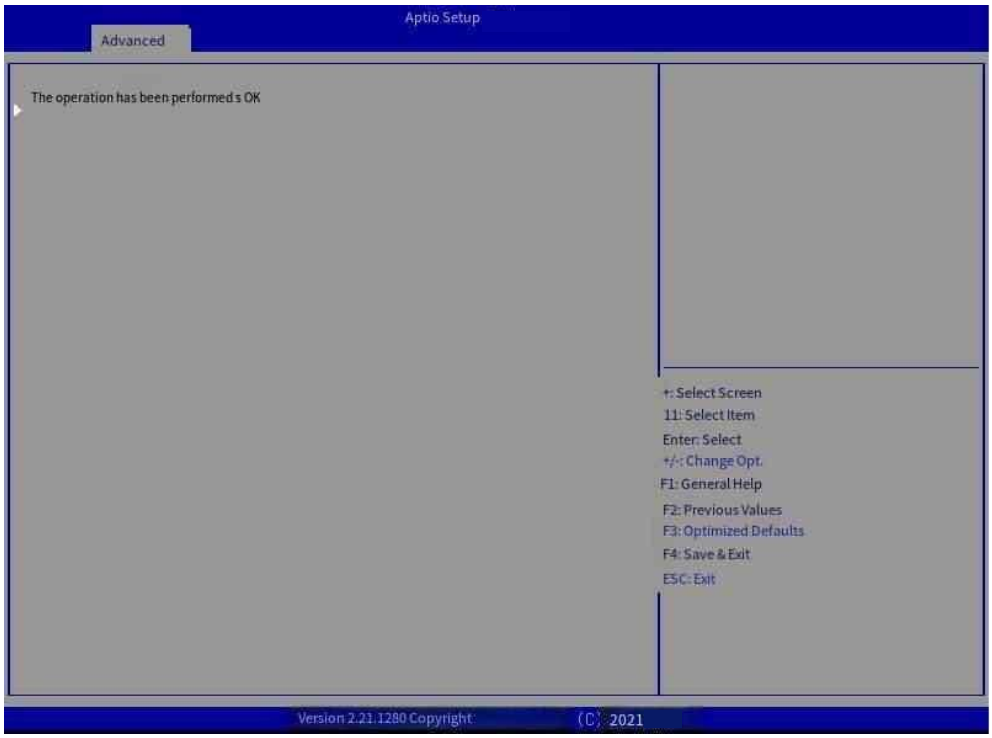


Figure 7-24 Click OK

Step 4: Select "Add More Spans", press Enter, select Span1->Select Drives, select the member drive to create Span1, click "Apply Changes" to create Span1 (Figure 7-25,

7-26, Figure 7-27, Figure 7-28);

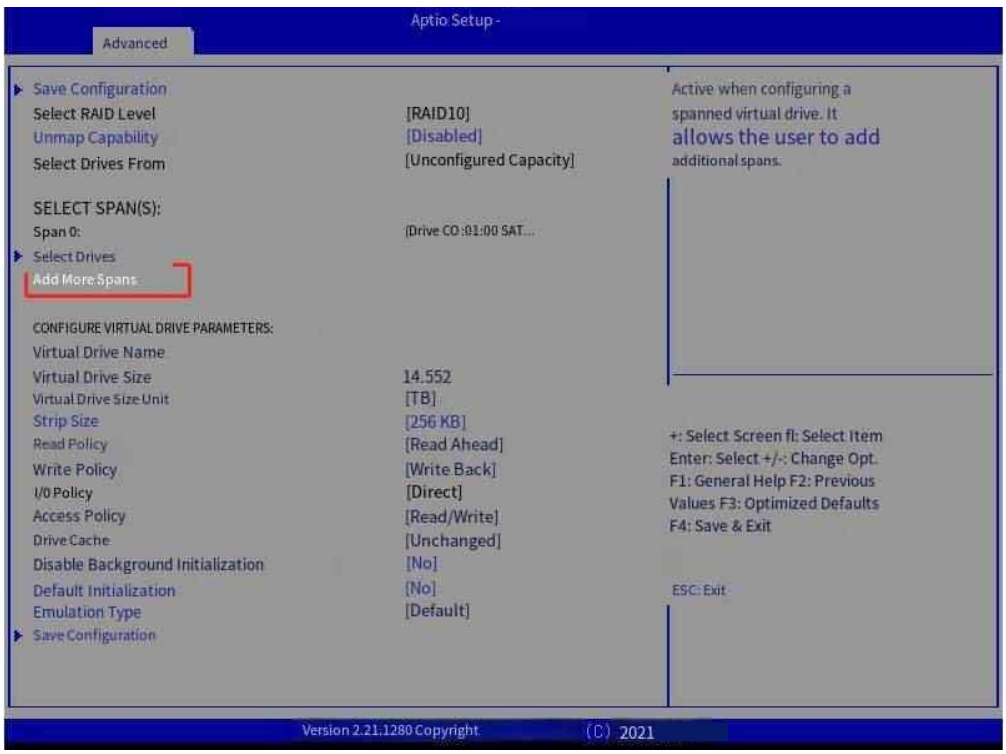


Figure 7-25 Select "Add More Spans" and press Enter

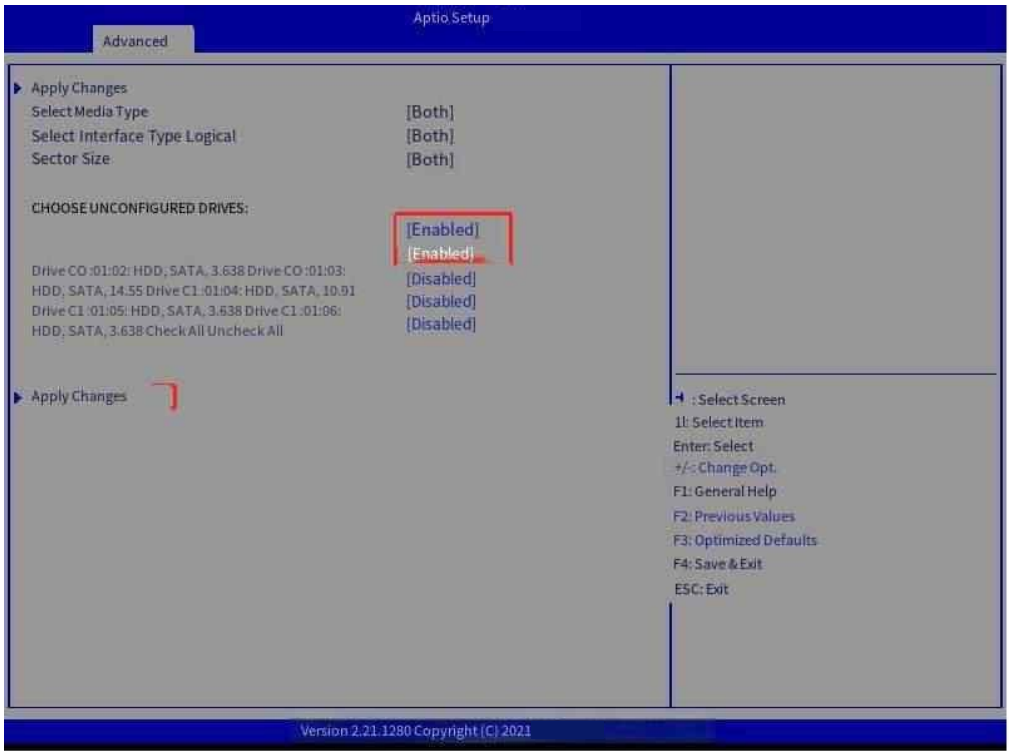


Figure 7-26 Select the hard drive you want to build Span1

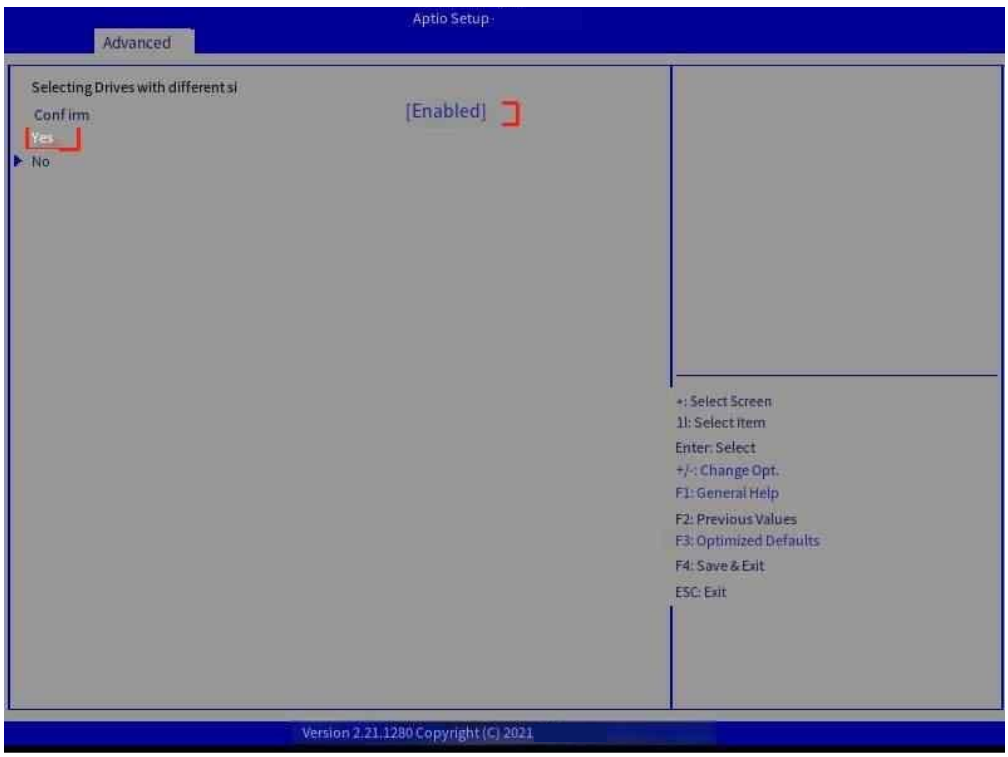


Figure 7-27 Set Confirm to enabled and click Yes

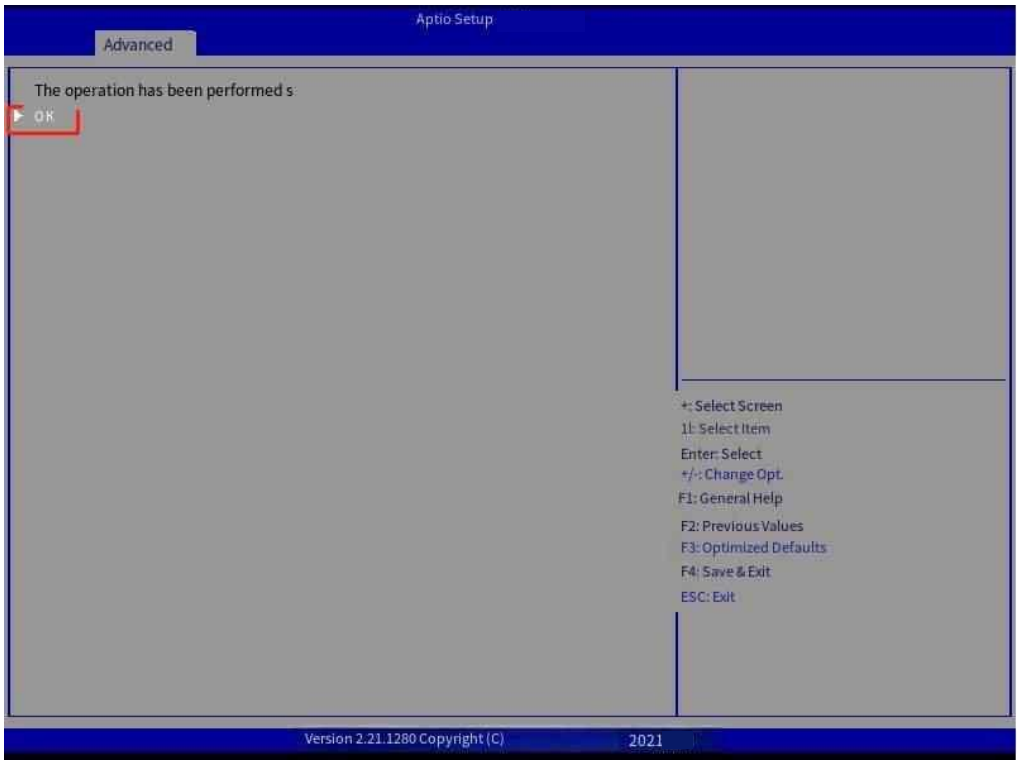


Figure 7-28 Click OK

Step 5: Select Save Configuration and press enter to create RAID10 (Figure 7-29 Figure 7-30, Figure 7-31)

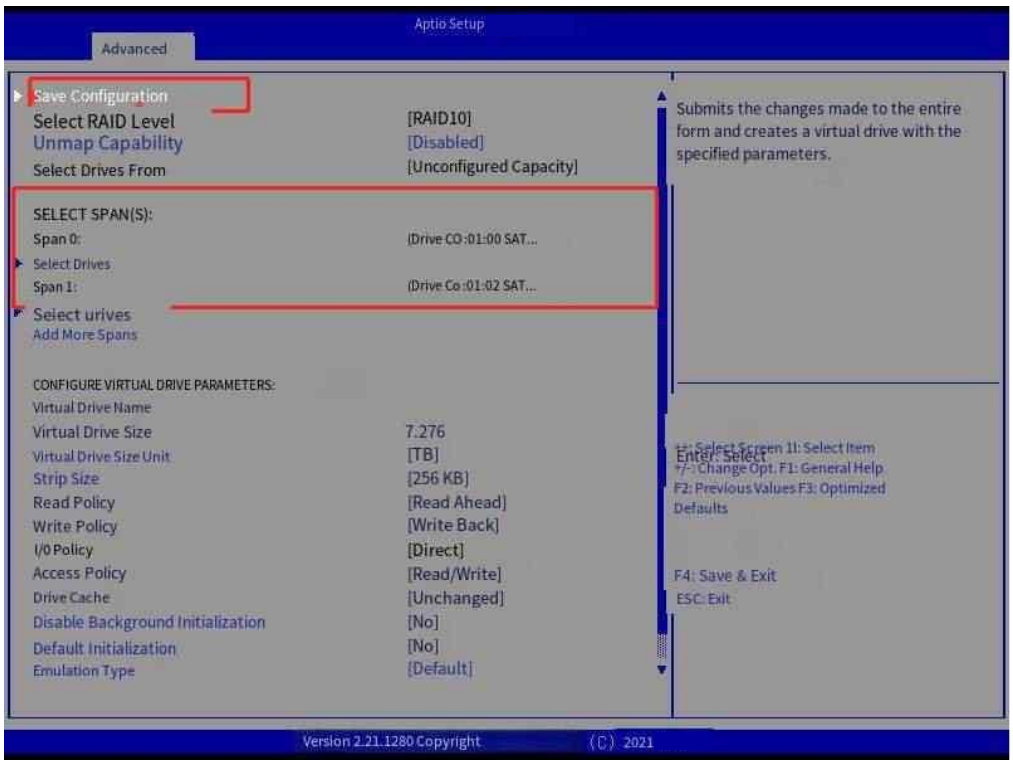


Figure 7-29 Press enter to select Save Configuration

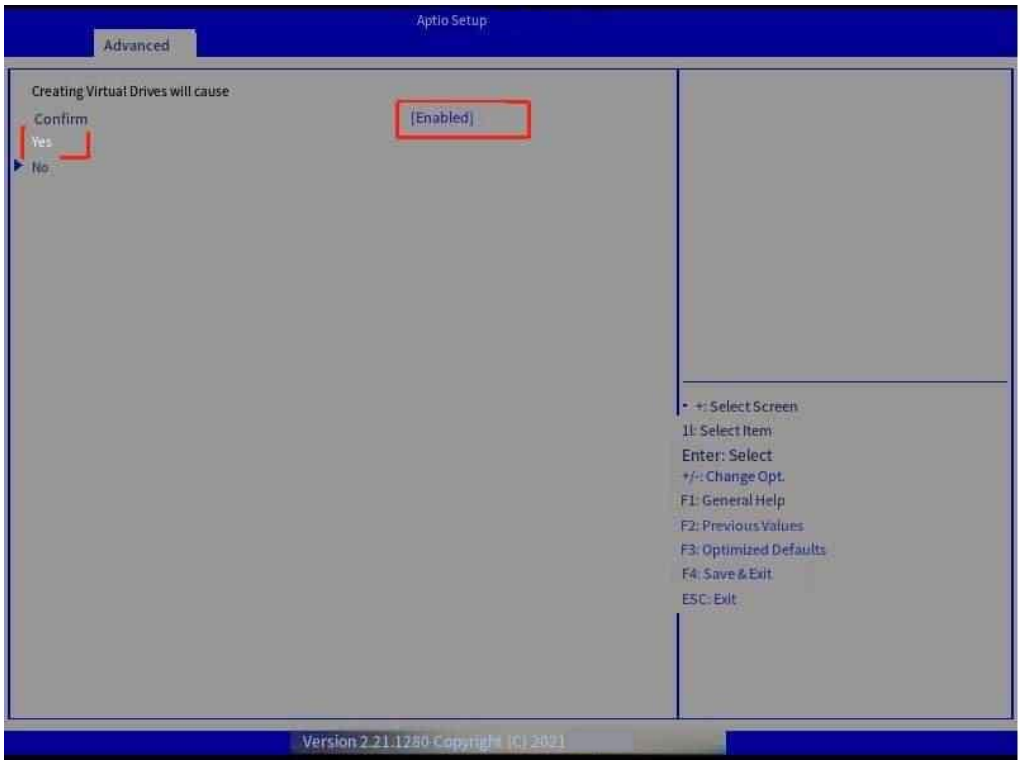


Figure 7-30 confirm Click Yes after selecting Enabled

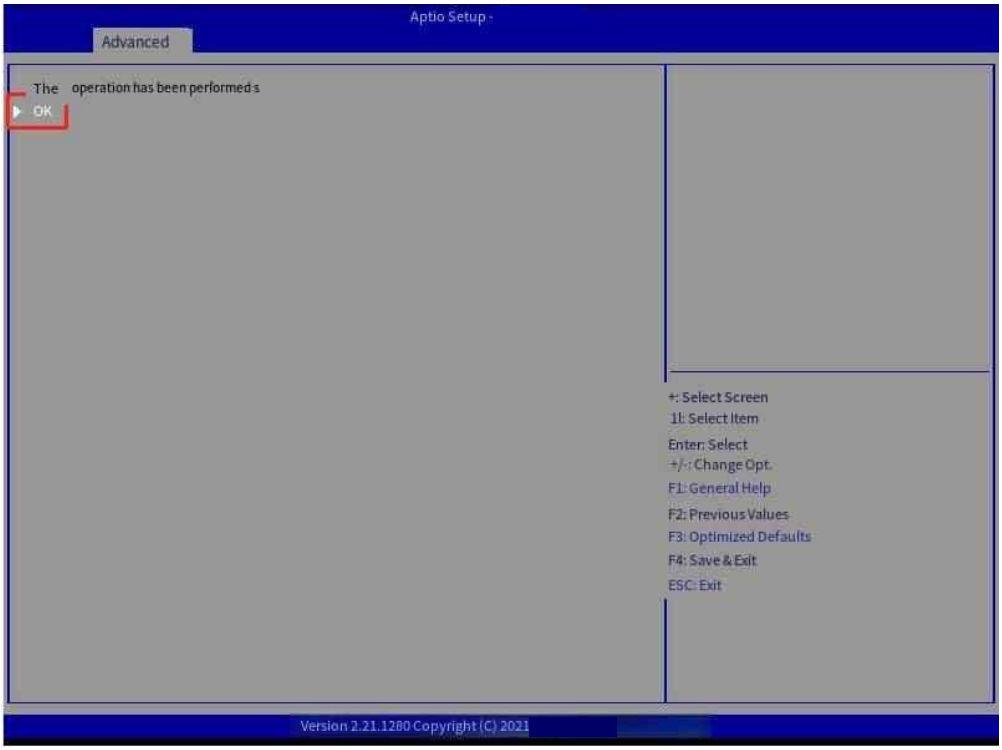


Figure 7-31 Click ok

Step 6: Press ESC to return to the upper screen, select Virtual Drive Management and press Enter (Figure 7-32);

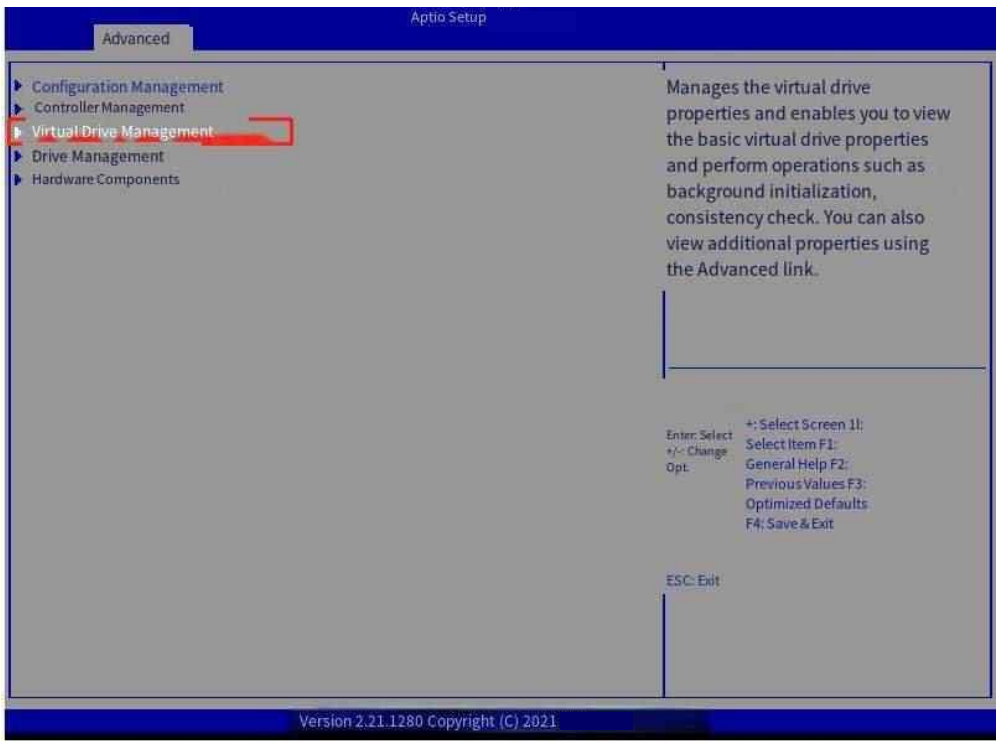


Figure 7-32 RAID home screen

Step 7 On the Virtual Drive Management screen, you can view the RAID array created under the controller, as shown in Figure 7-33.

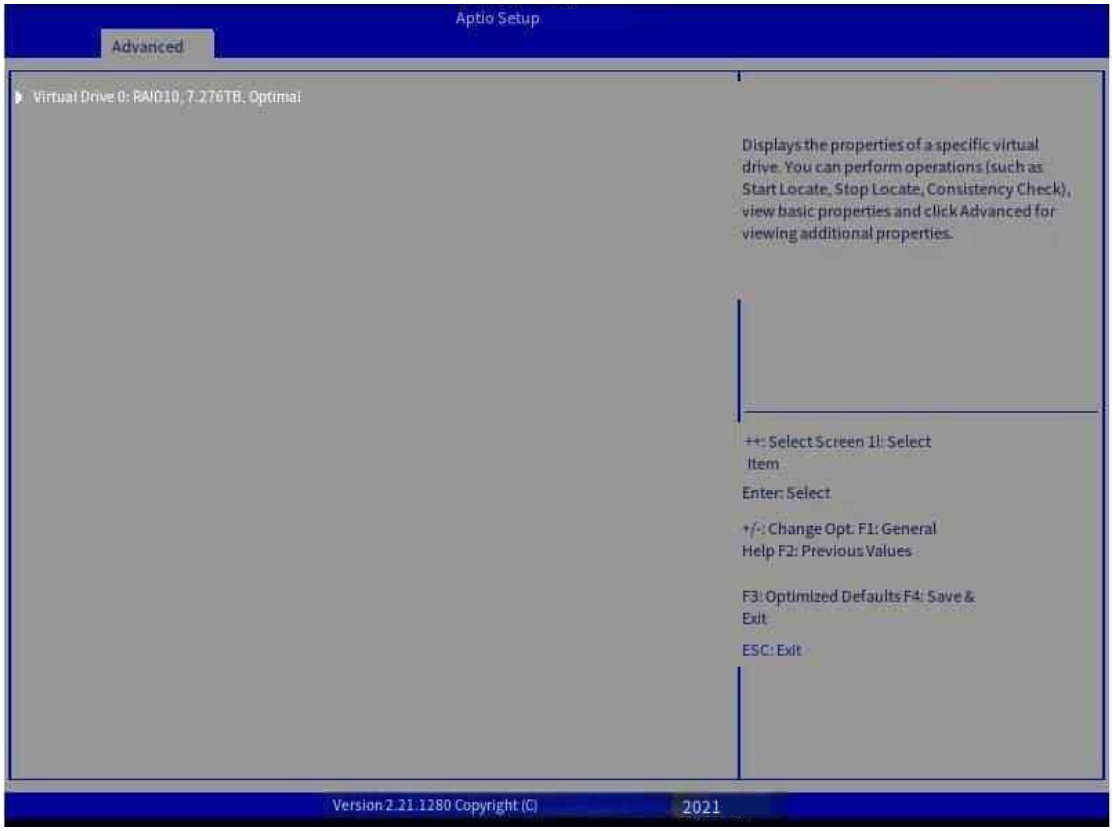


Figure 7-33 Viewing RAID information

7.1.3.5 Creating RAID50/60 Group Columns

The method for creating RAID50/60 is the same as that for RAID10. After entering the Main Menu of RAID group, Select Configuration Management->Creat Virtual Drive->Select RAID Level->RAID50/60 (select the corresponding RAID type during creation). Create a RAID50/60 group (as shown in Figure 7-34 and Figure 7-35). The following steps are the same as those for RAID10.

Note: Build RAID10/50/60 with at least 2 spans, RAID10 with at least 2 disks per Span (i.e., use at least 4 hard drives), and RAID50/60 with at least 3 disks per Span (i.e., use at least 6 hard drives).

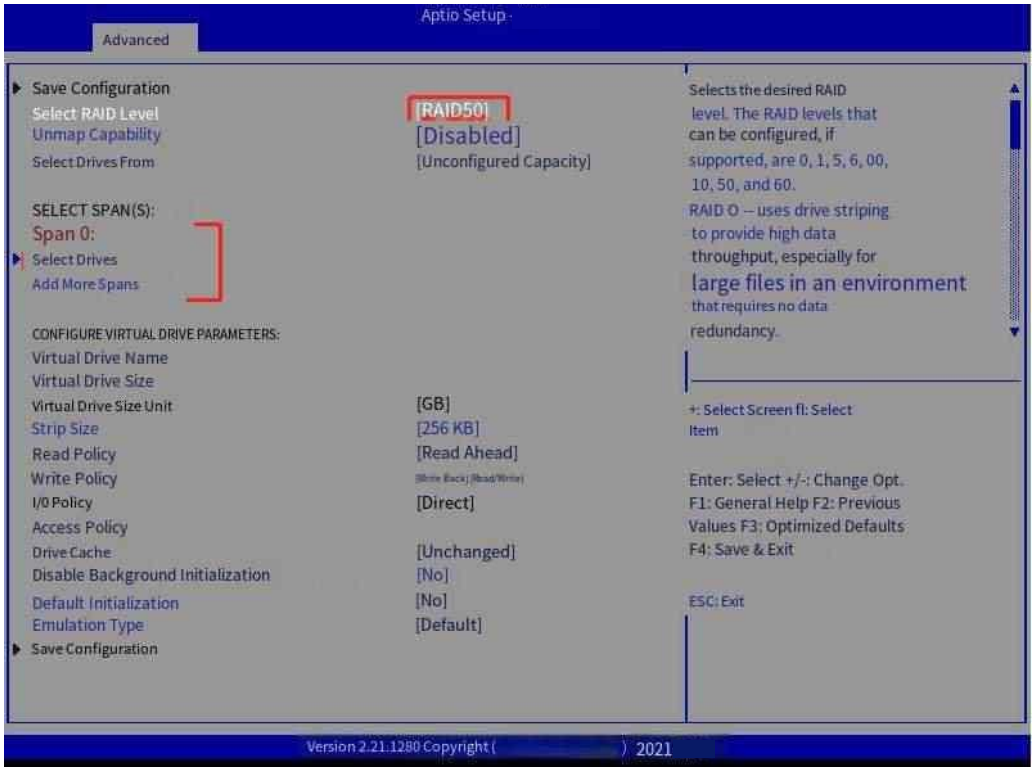


Figure 7-34 Selecting a RAID type for RAID50

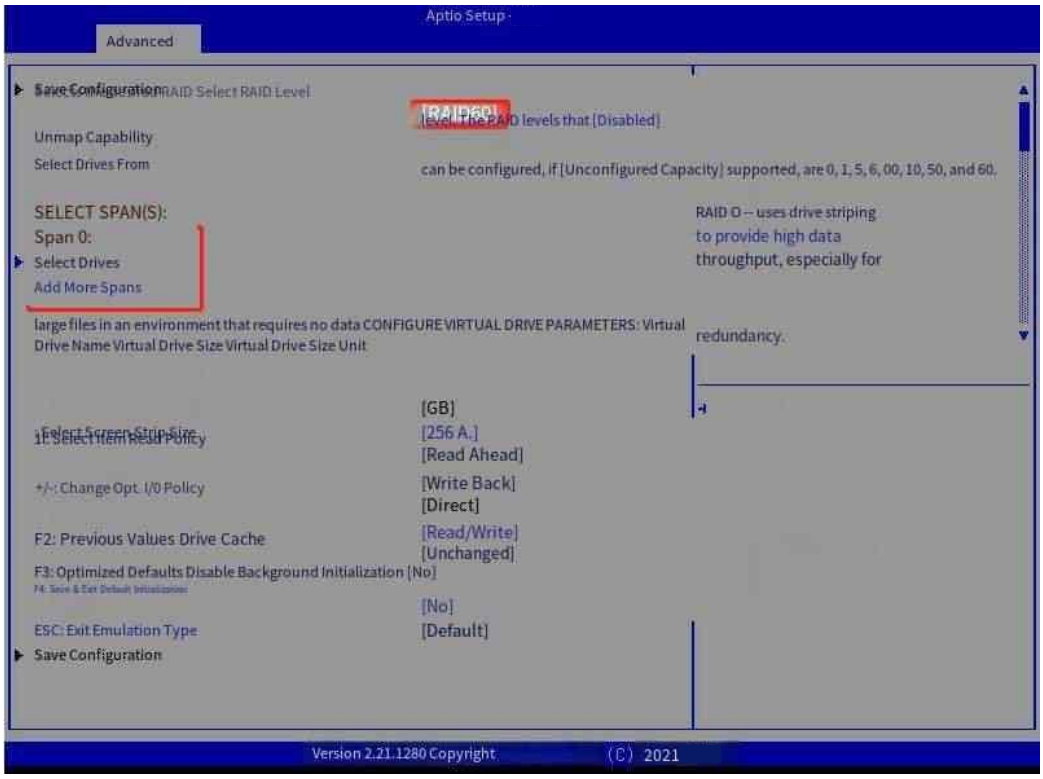


Figure 7-35 Selecting RAID type RAID60

7.1.4 Hot Spare Drive Settings

- Hot Spare Drive:

After hard drives of a server are configured with RAID properties, hot spare drives can be configured to improve security and reduce the impact on services caused by hard drive failures.

Global HSP: Global hot spare drive. It is shared by all configured RAID arrays. Each RAID controller card can be configured with one or more global hot spare drives. If a hard drive of the same type fails in any RAID array, the global hot spare drive automatically replaces it.

Dedicated HSP: A dedicated hot spare drive is dedicated to a specified RAID array. Each RAID array can be configured with one or more dedicated hot spare drives. A dedicated hot spare drive automatically replaces a hard drive of the same type in a specified RAID array if it fails.

● The capacity of a hot spare drive must be no smaller than that of a member drive.

Description:

Mechanical disk and solid state disk can not be used as hot spare disk;

A mechanical drive can be configured with SAS or SATA interfaces. When a member drive of a RAID group is a SAS disk, a SATA disk can be used as a local hot spare disk. When a member drive is a SATA disk, a SAS disk cannot be used as a local hot spare disk.

An idle hard drive can be configured as a hot spare drive. A hard drive that has been added to a RAID array cannot be configured as a hot spare drive.

A hot spare drive must be of the same type as a member drive in a RAID group, and its capacity must be no smaller than the maximum capacity of a member drive.

All RAID types except RAID 0 support hot spare drives.

A global hot spare drive cannot be directly converted to a local hot spare drive. You need to restore the drive to the idle state, and then set the drive to the global or local hot spare drive as required.

Data on the hard drive used as a hot spare drive will be lost.

● To set up a hot spare drive, do as follows:

Step 1: On the home screen, select Main Menu and press Enter, select Drive Management, and select a hard drive for hot spare drive Settings (Figure 7-36, Figure 7-37).

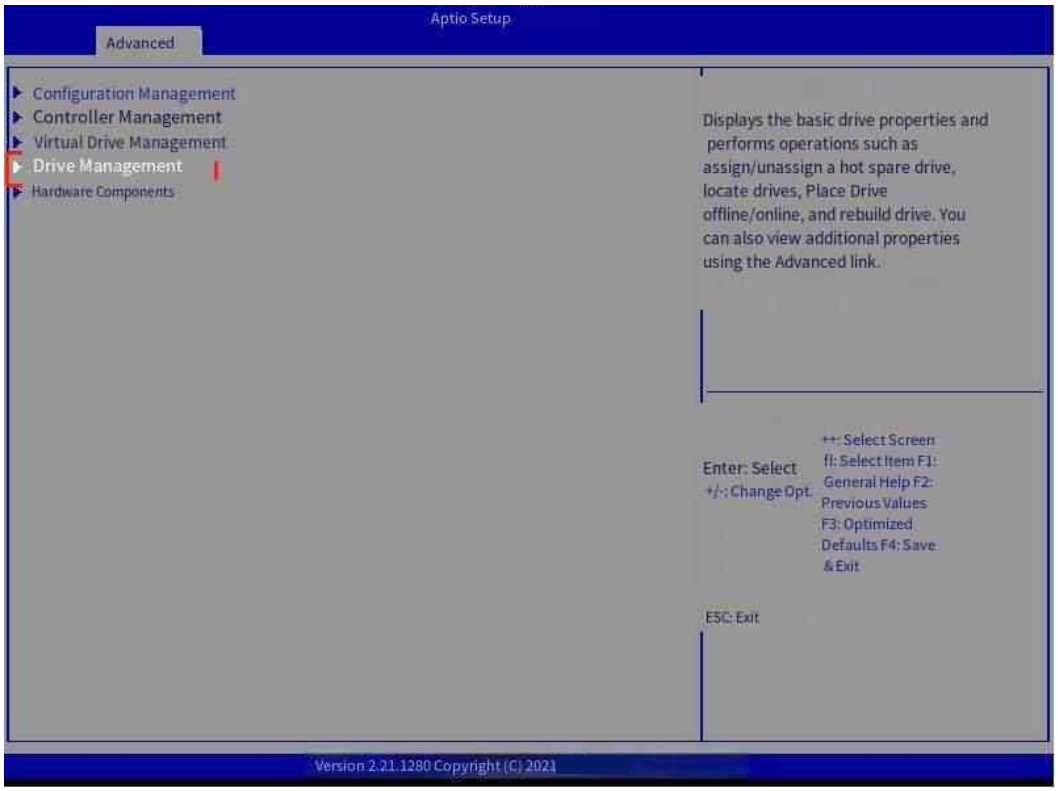


Figure 7-36 Select Drive Management and press Enter

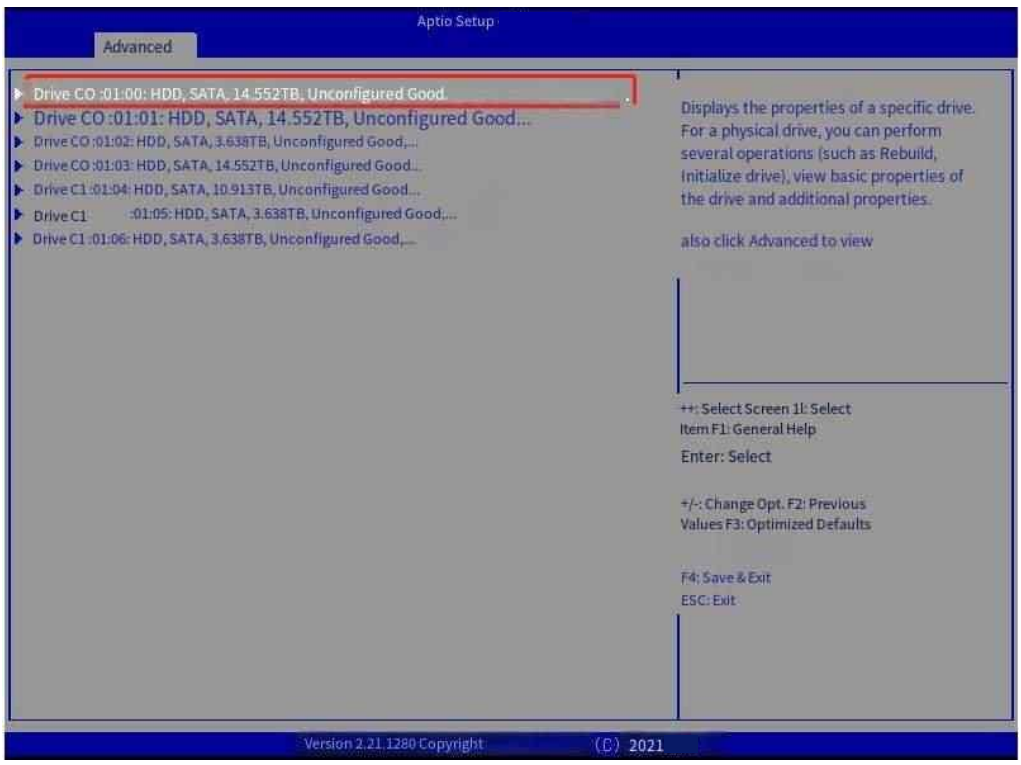


Figure 7-37 Selecting a hard drive Press Enter to set hot spare

Step 2: Click Select operation, use ↑ and ↓ to select Assign Global Hot Spare Drive (Figure 7-38), and click Go->Ok (Figure 7-40).

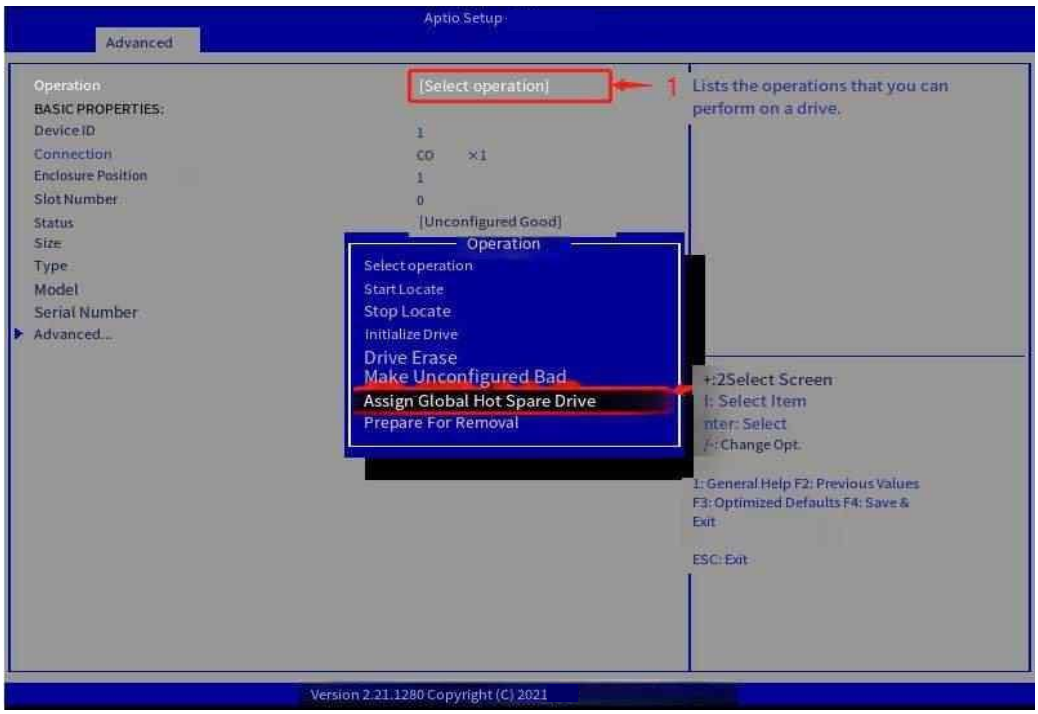


Figure 7-38 Select Assign Global Hot Spare Drive

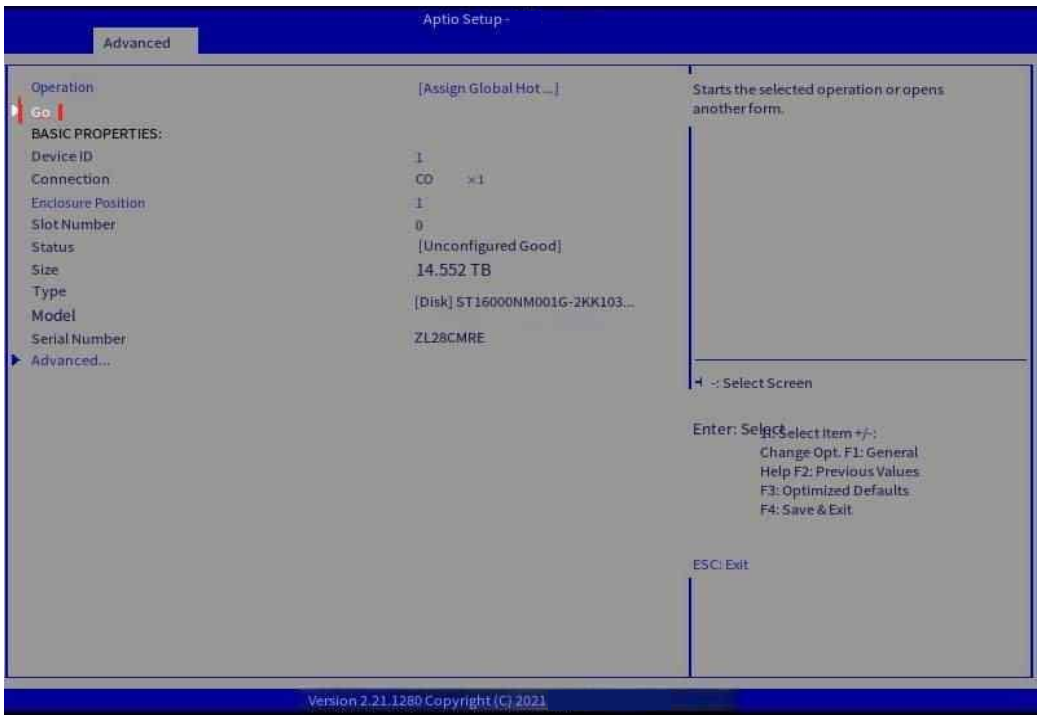


Figure 7-39 Click Go

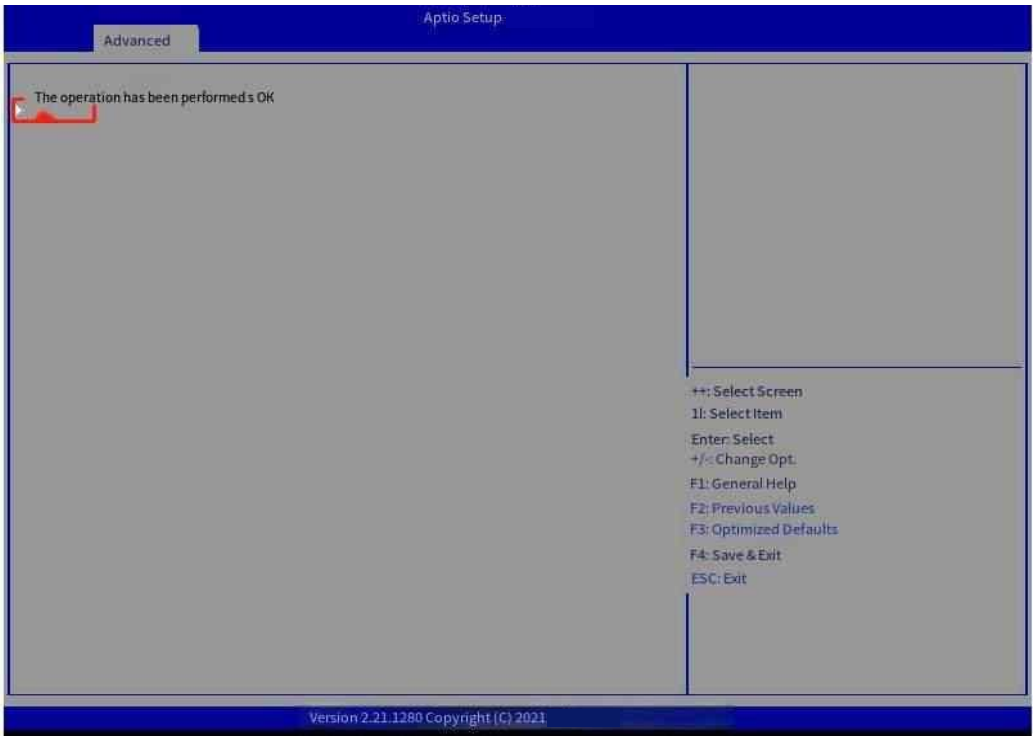


Figure 7-40 Click Ok

Step 3: Click Ok and return to the hard drive information screen. Check the Status of the hard drive, which is Hot Spare (Figure 7-41).

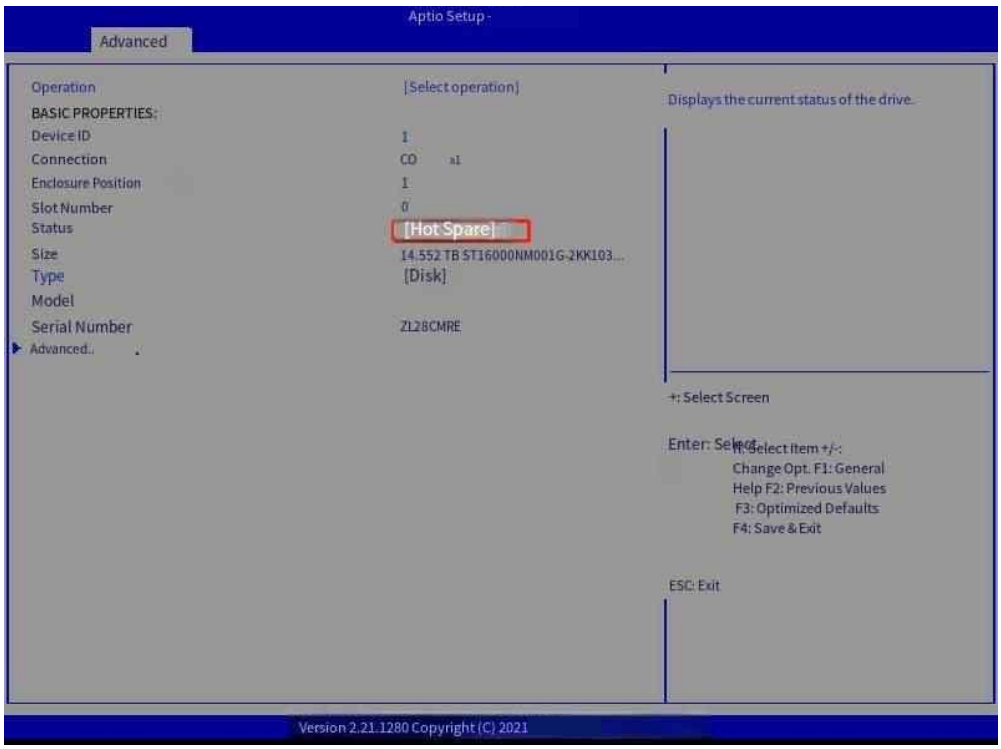


Figure 7-41 Check the hard drive status

7.1.5 Deleting a RAID Group Column

To do so:

Step 1: On the home screen, select Main Menu and press Enter, select Virtual Drive Management (Figure 7-42) :

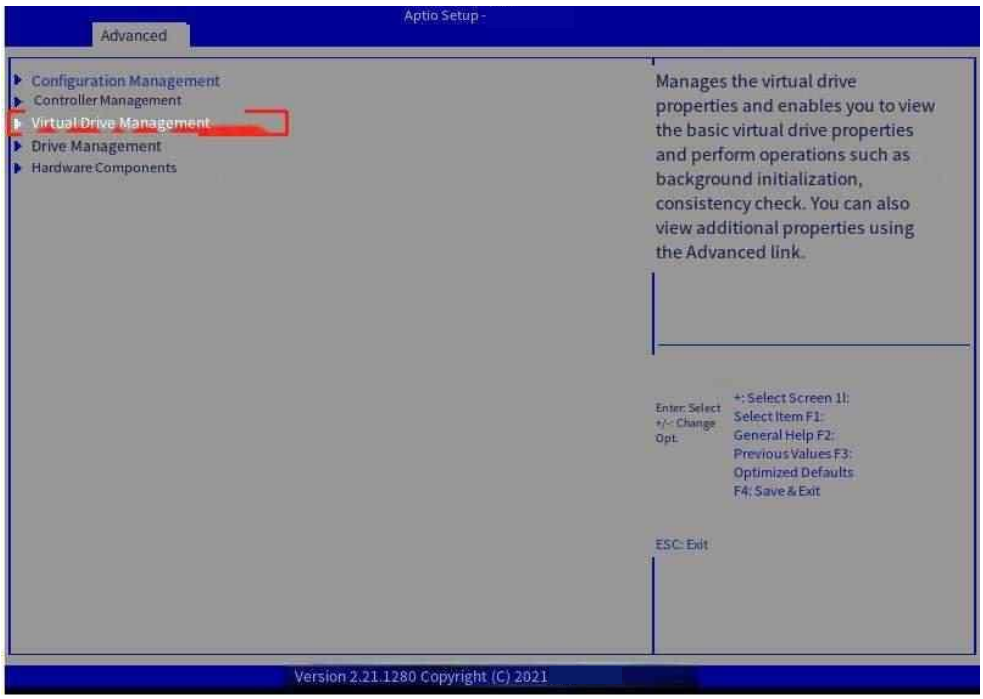


Figure 7-42 Main RAID screen

Step 2 Press Enter to go to the Virtual Drive Management screen. On the screen, you can view the RAID array created under the controller (Figure 7-43).

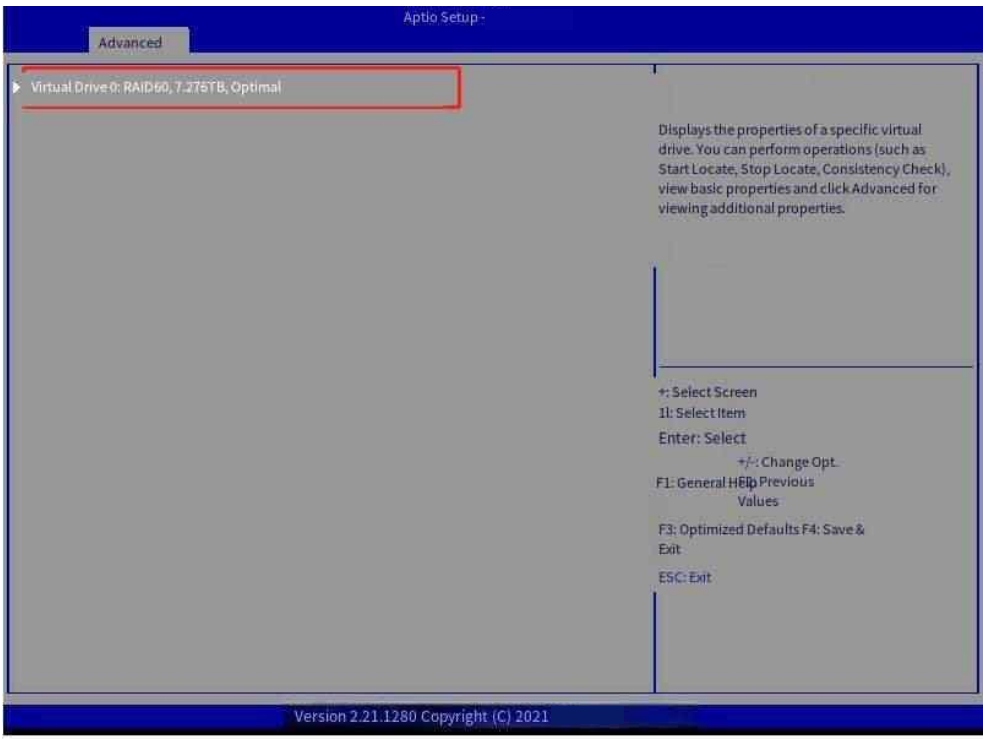


Figure 7-43 View the RAID properties

Step 3: Click "Select operation", select "Delete Virtual Drive" (Figure 7-43), click "Go",

Confirm setting to Enabled, click Yes->Ok(Figure 7-44, Figure 7-45, Figure 7-46)

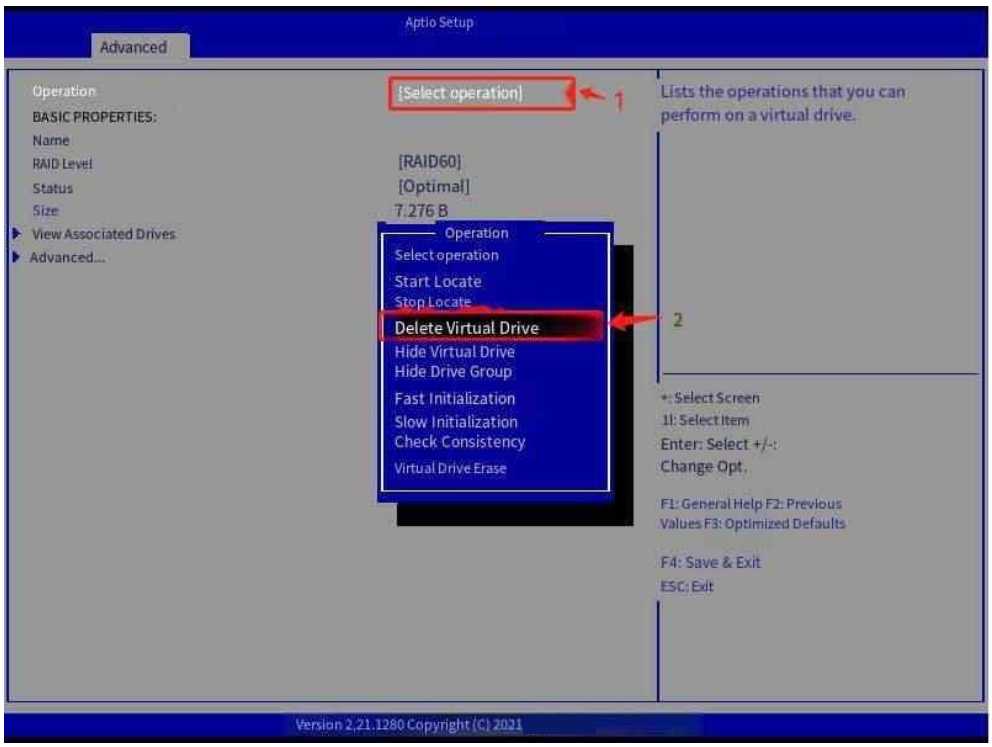


Figure 7-44 Select "Delete Virtual Drive"

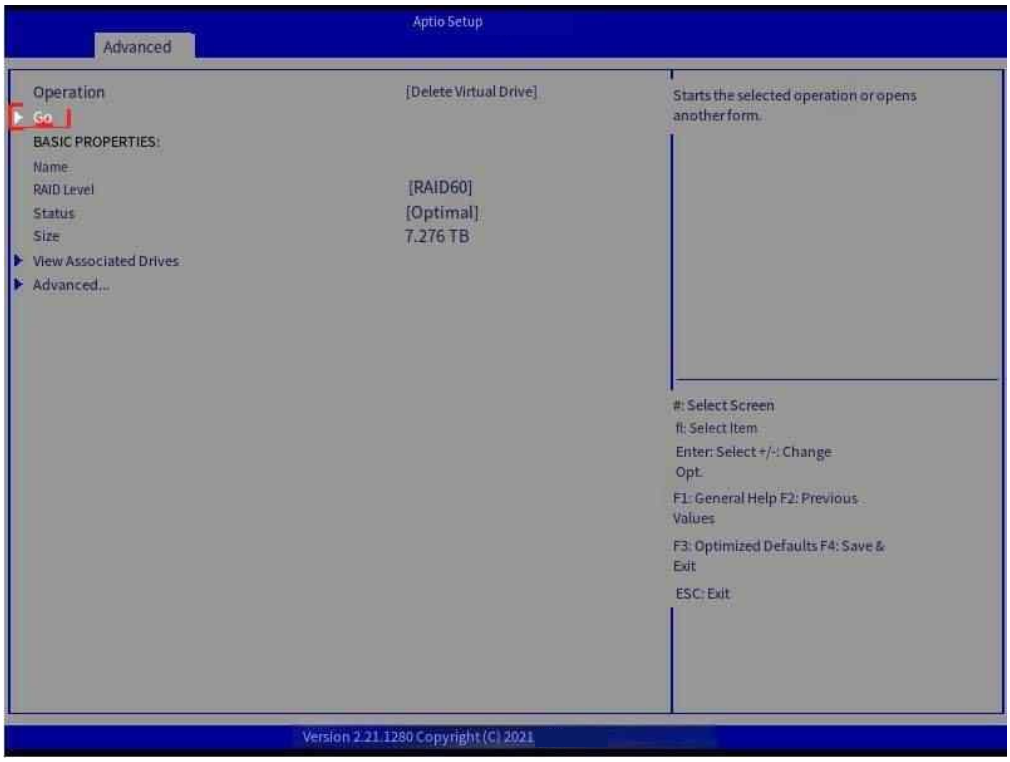


Figure 7-45 Click Go

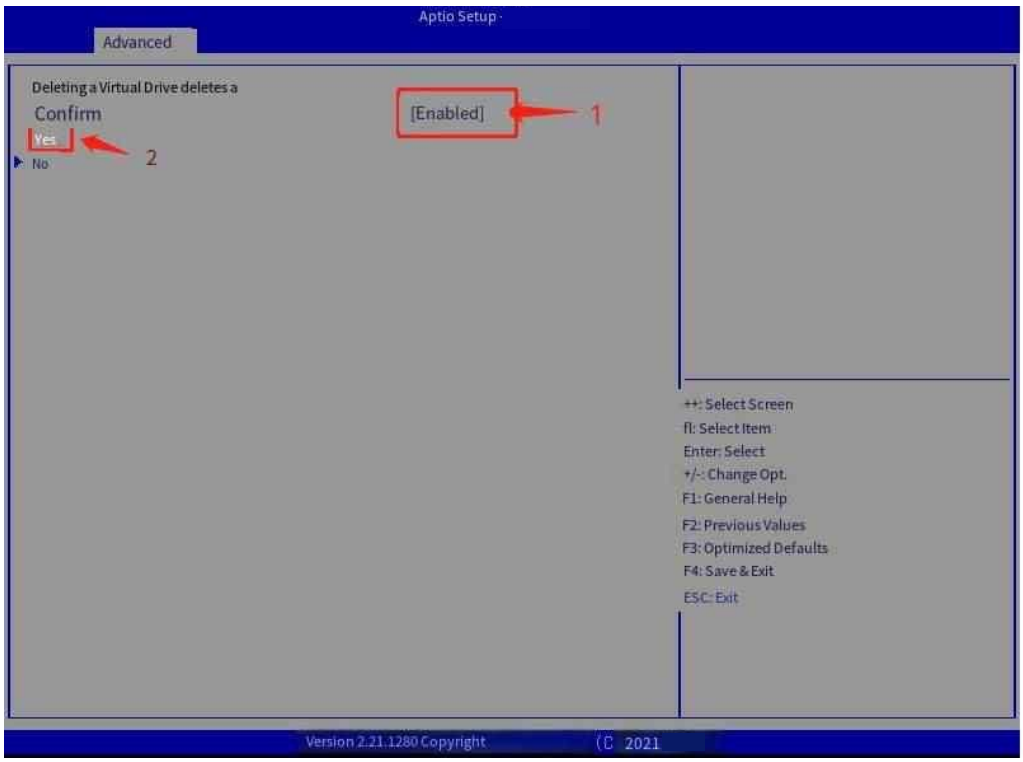


Figure 7-46 Confirm Click Yes after setting it to Enabled

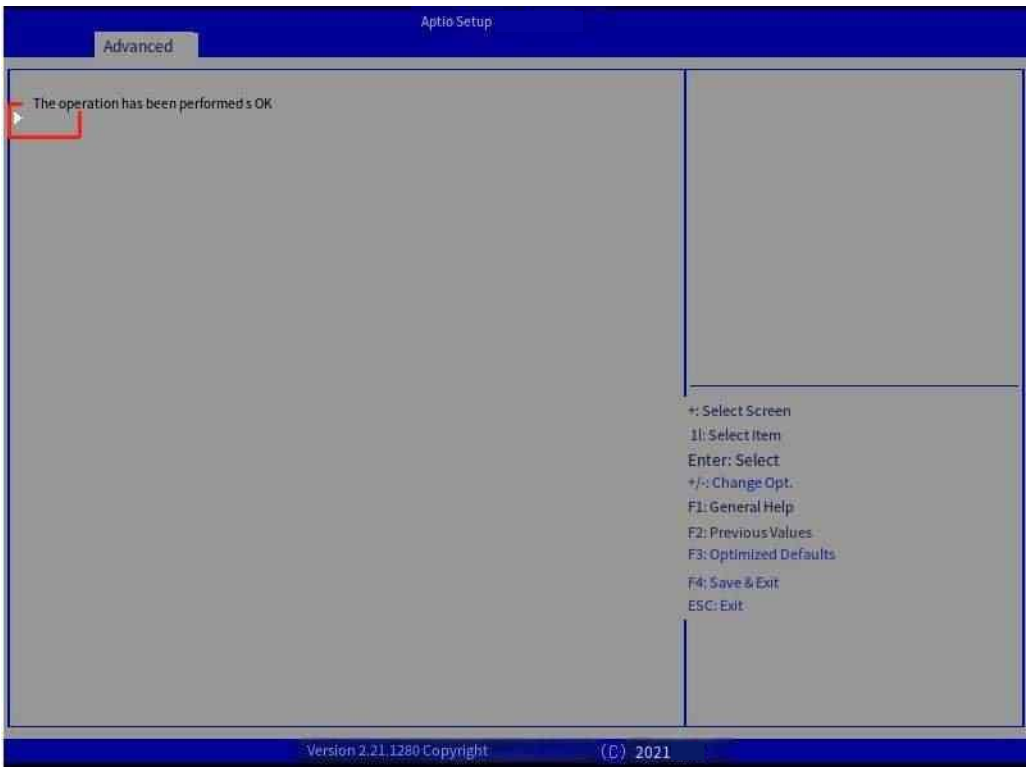


Figure 7-47 Click Ok

Step 4: On the home screen, select Main Menu and press Enter, select Virtual Drive Management, and press enter. After entering, check that the original RAID array has been deleted (Figure 7-48).

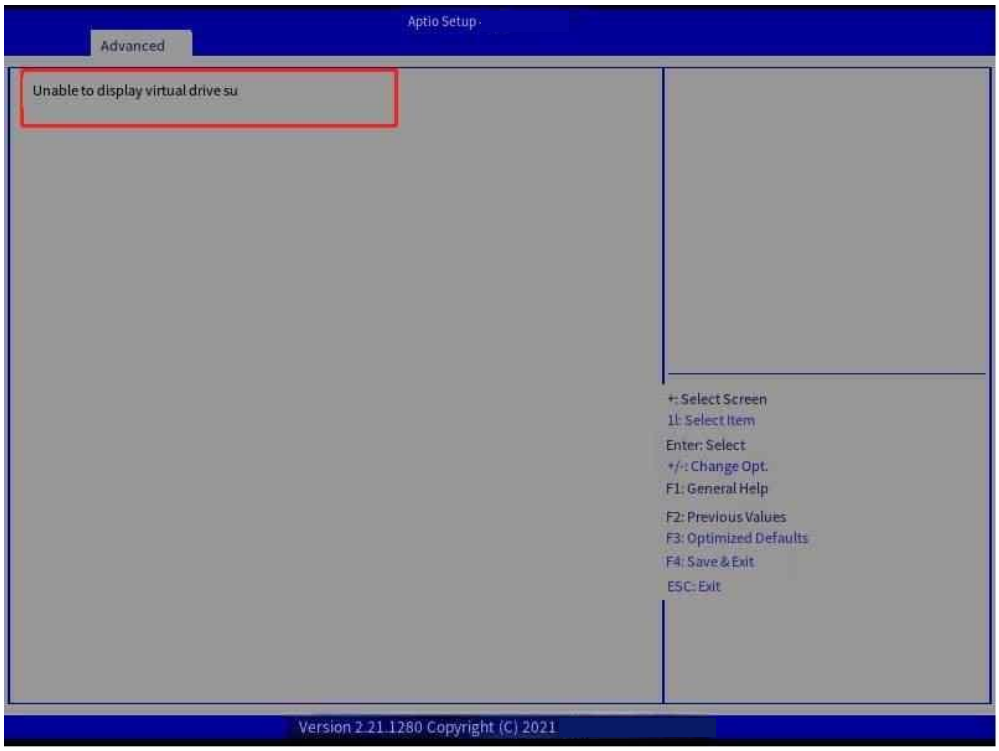


Figure 7-48 Checking the RAID

7.1.6 Viewing Hard Drive Information

Procedure:

Step 1: On the home screen, select Main Menu and press Enter. Select Drive Management (Figure 7-49).

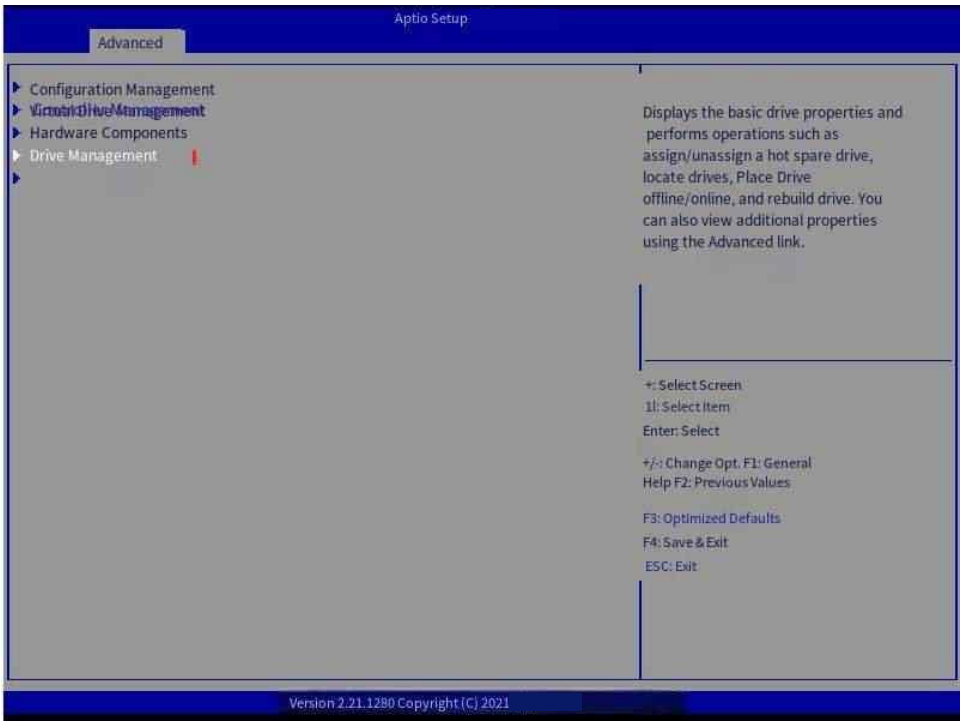


Figure 7-49 Main RAID screen

Step 2 Press Enter to go to Drive Management, where you can view hard drive information (Figure 7-50).

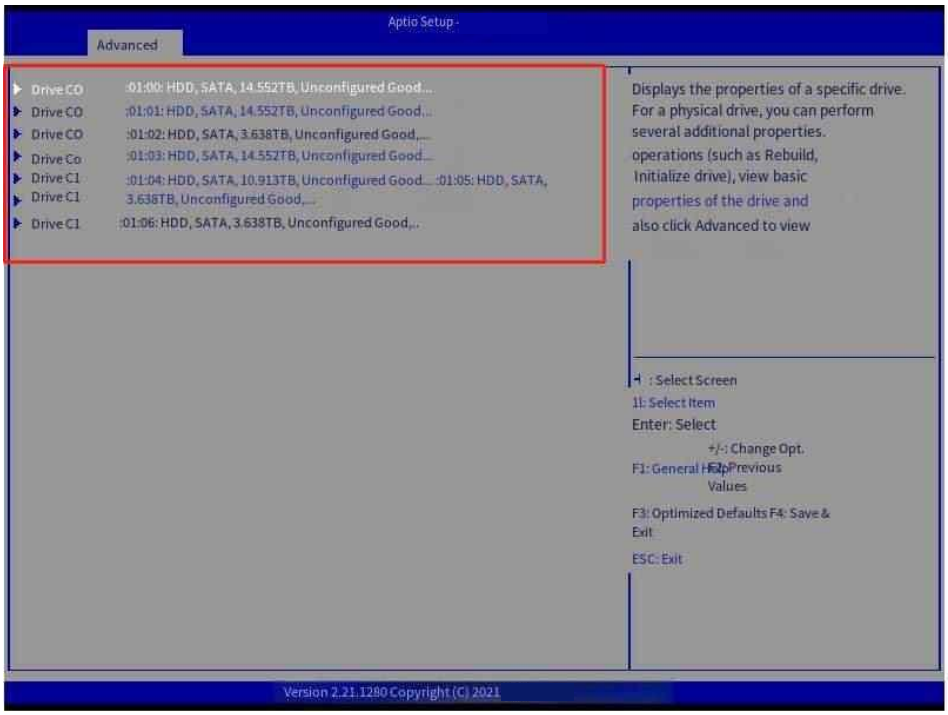


Figure 7-50 Viewing hard drive information

Step 3: Select a hard drive and press enter to view the details of a single hard drive (Figure 7-51);

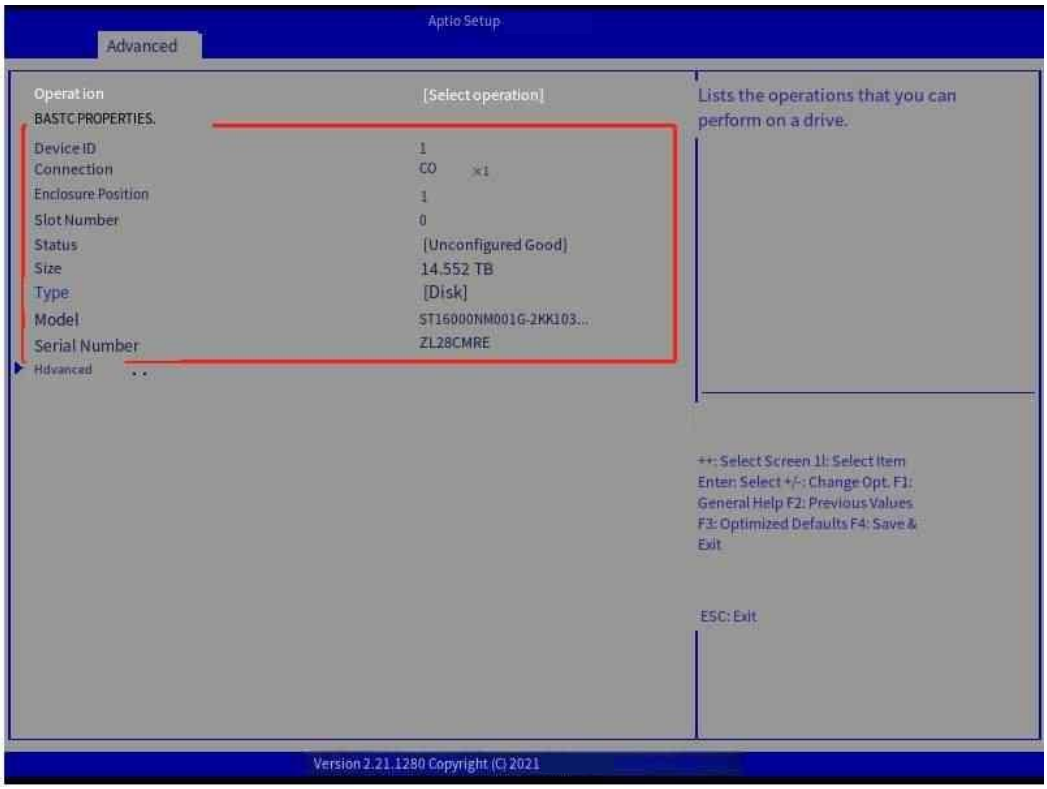


Figure 7-51 Viewing the details of a single hard drive

7.1.7 Setting the Boot Drive

To do so:

Step 1: On the home screen, select Main menu and press Enter. Select Controller Management (Figure 7-52).

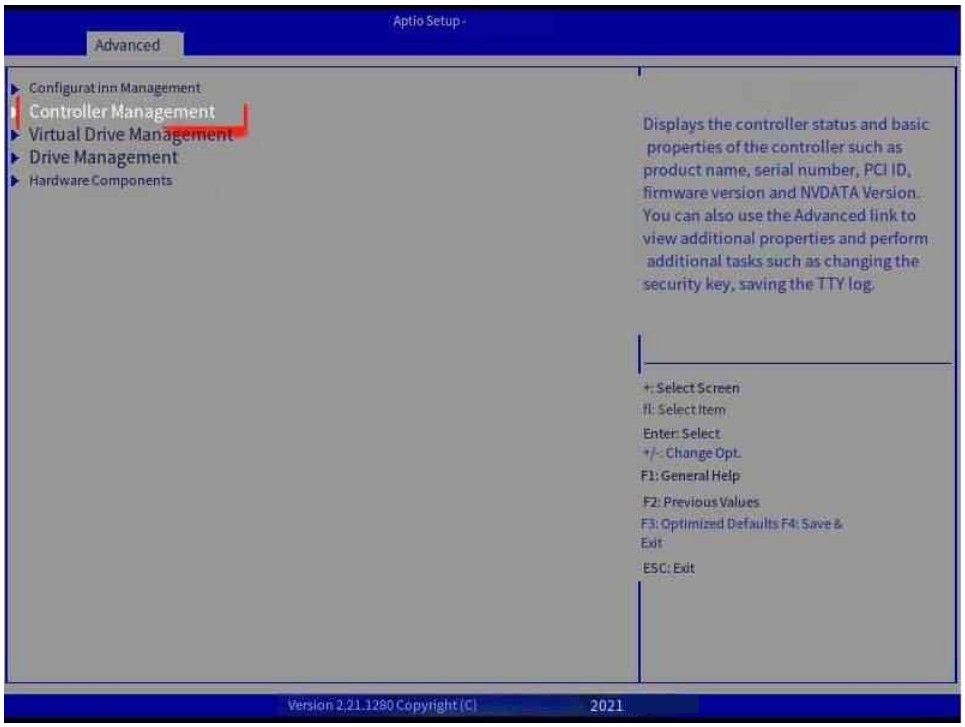


Figure 7-52 RAID main menu

Step 2: Press Enter to go to Controller Management and Select Select Boot Device. The default boot option is None(Figure 7-53).

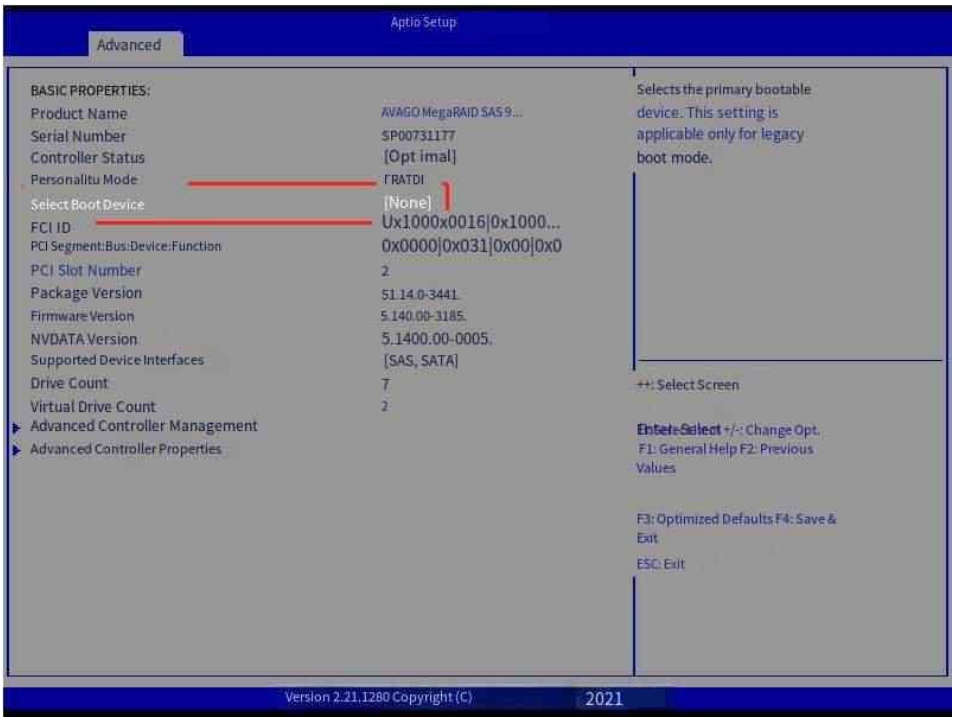


Figure 7-53 Controller Management

Step 3: Press Enter and select the desired raid or JBOD drive as the Boot Device in the pop-up window (Figure 7-54).

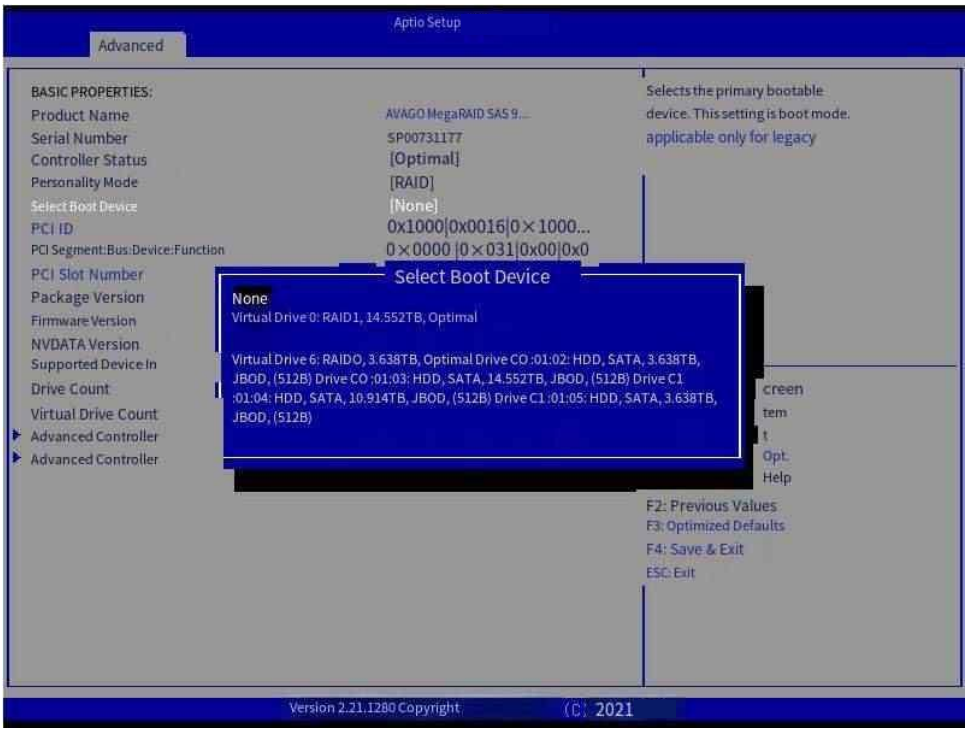


Figure 7-54 Select Boot Device

7.1.8 Locating the Hard Drive

Procedure:

Step 1: On the home screen, select Main Menu and press Enter, and select Drive Management (Figure 7-55).

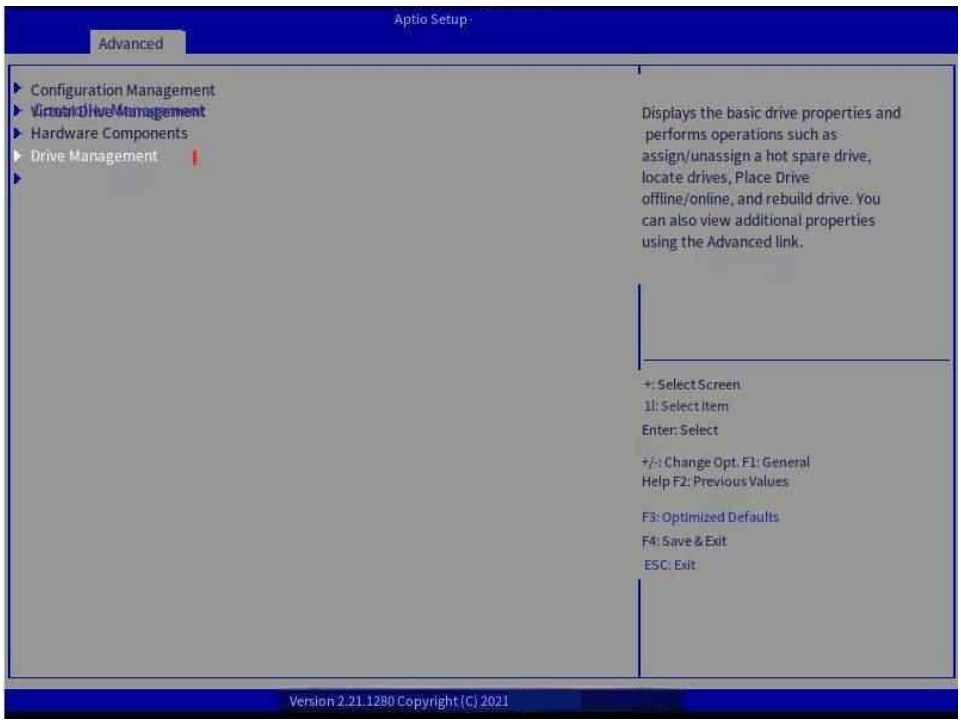


Figure 7-55 Main RAID menu

Step 2: Press Enter to go to Drive Management, where you can view hard drive information (Figure 7-56).

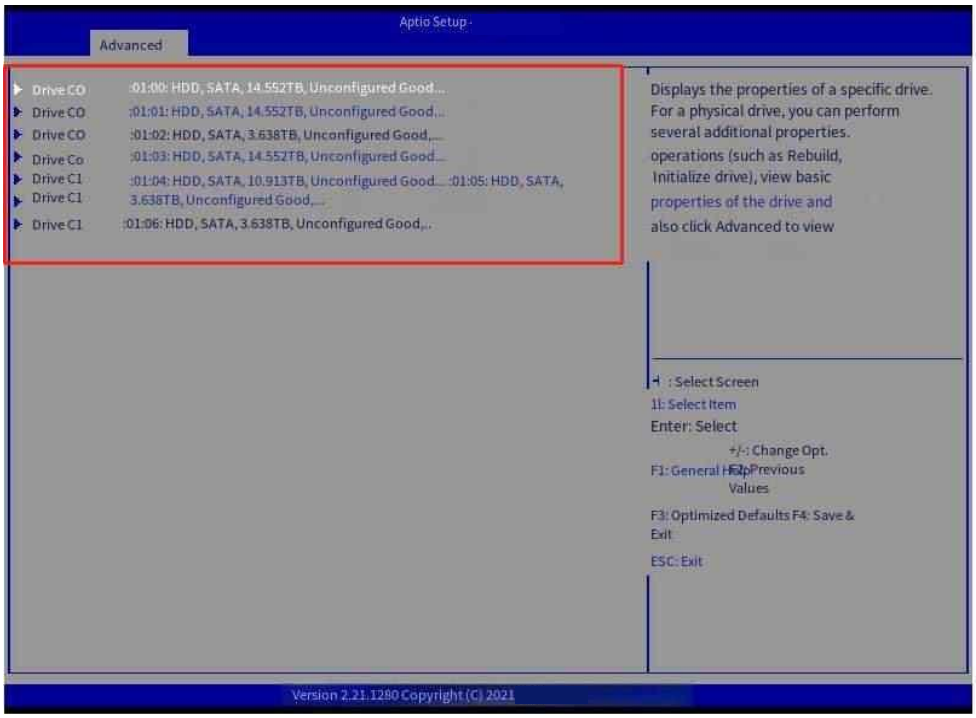


Figure 7-56 Viewing hard drive information

Step 3: Select a hard drive, press enter and click Select operation "Select" Start

Locate (Figure 7-57);

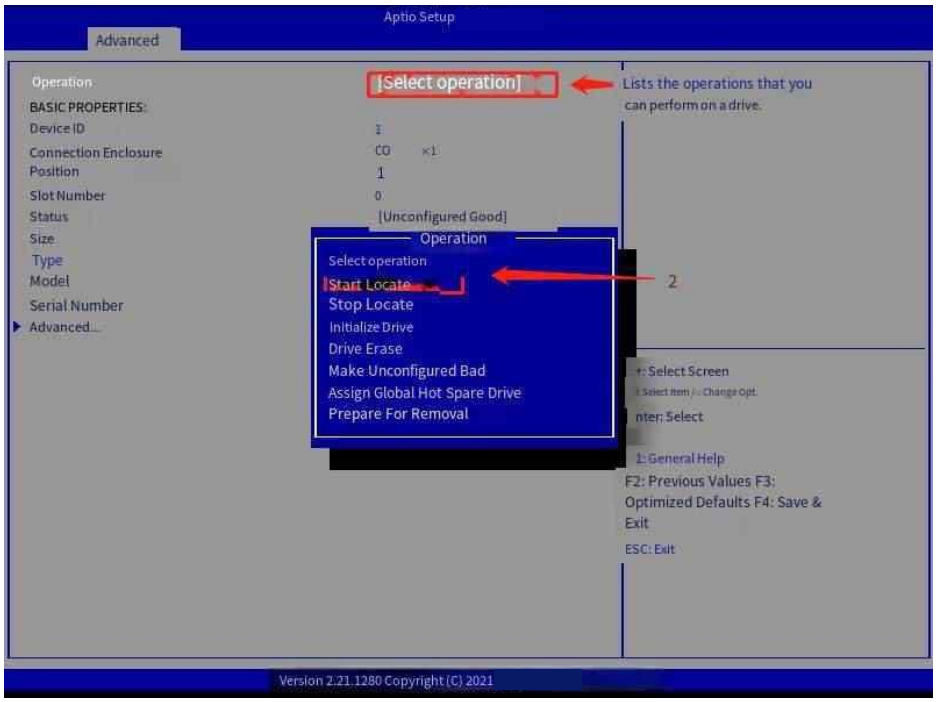
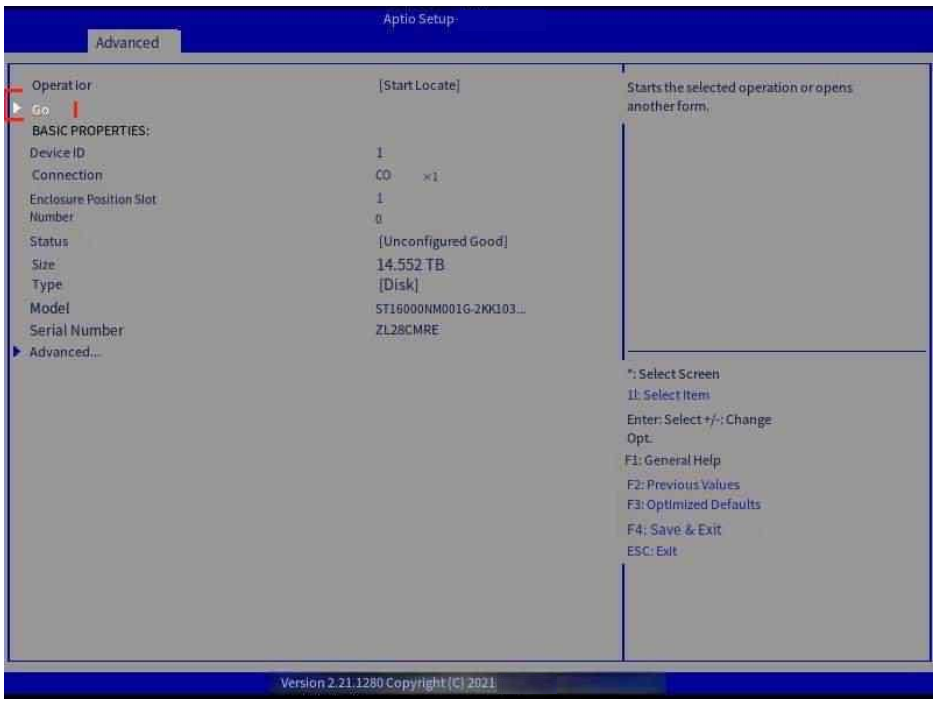


Figure 7-57 Select Start Locate

Step 4: Click Go->Ok to begin locating the hard drive (Figure 7-58, Figure 7-59);



Click Go for Figure 7-58

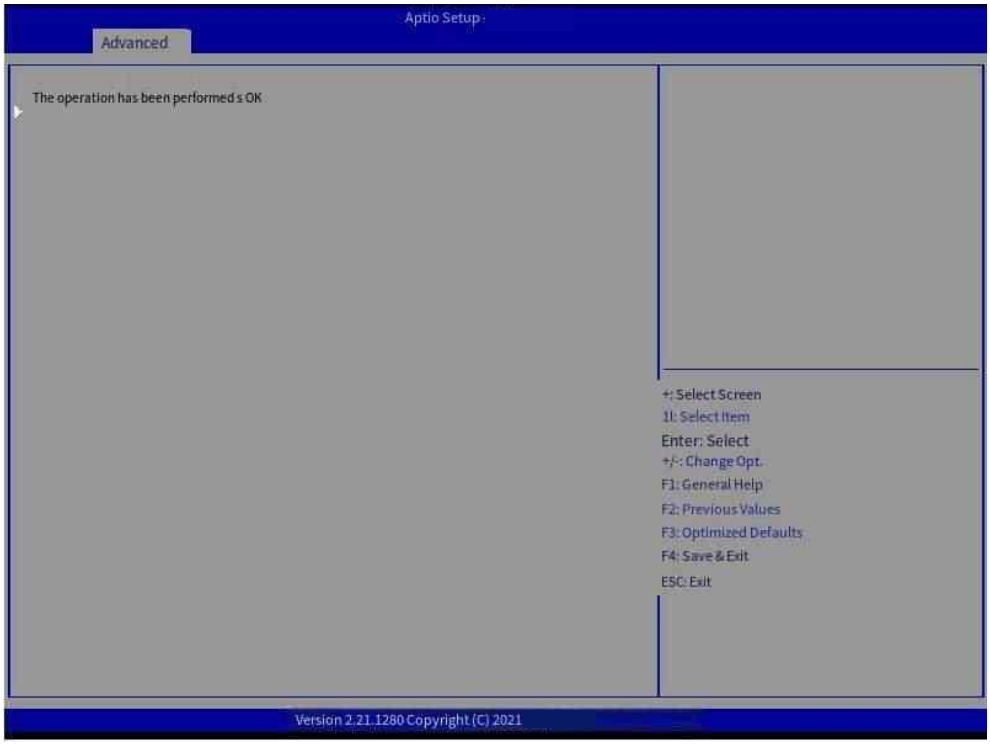


Figure 7-59 Click Ok

Step 5: Repeat the preceding method, click Select operation Select Stop Locate to stop locating the hard disk.

Chapter 8 Upgrade the PSU/CPLD firmware

8.1 CPLD FW Update

8.1.1 SSH Updates the CPLD FW

8.1.1.1 Update the CPLD of the mainboard

How to take immediate effect:

Step 1: Place the CPLD FW (xxx.vme) file on the mainboard in the shared folder of the tftp server

Using tftp32 software in Windows, double click tftpd32.exe program;

Step 2: Use SSH to log in to BMC with the login account name sysadmin and password superuser

ssh sysadmin@<$BMCIP>;

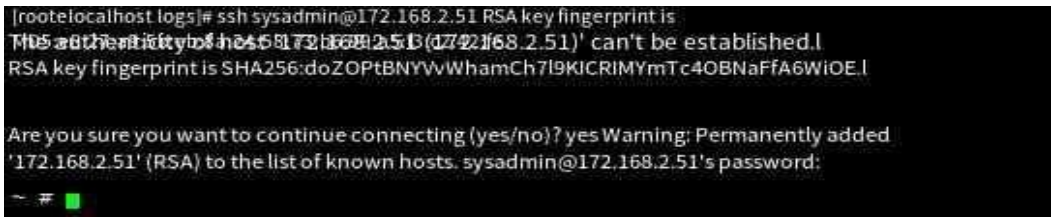


Figure 8-1 Refreshing the CPLD on the mainboard

Step 3: On the BMC, use the TFTP tool to save the CPLD FW file to the /var path of the BMC

tftp ClientIP -g -r xxx.vme -l /var/cpld.vme;

Step 4: Run the refresh command, # ispvmapp -- x -- i /var/cpld.vme;

Figure 8-2 Refreshing the CPLD on the mainboard

Step 5: After the refresh is complete, check whether the CPLD is updated successfully. The return value is the CPLD version

ipmitool raw 0x34 0x32 0x01

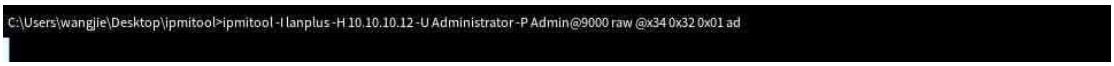


Figure 8-3 Refresh the CPLD on the mainboard

Note: You can select the Silent mode or Take Effect Immediately mode when upgrading the CPLD online.

Silent mode: The upgrade does not take effect immediately after the upgrade. The upgrade takes effect only after the AC is powered off and restarted. Upgrade package: xxx.vme

Immediate effect: The upgrade takes effect immediately and does not require AC power-off. The corresponding upgrade package is xxx_Refresh.vme

8.1.1.2 12HDD BP CPLD Update

Step 1: Put the 12HDD BP CPLD FW (xxx.aje) file into the shared folder of tftp server, use tftp32 software in Windows, double-click tftpd32.exe program;

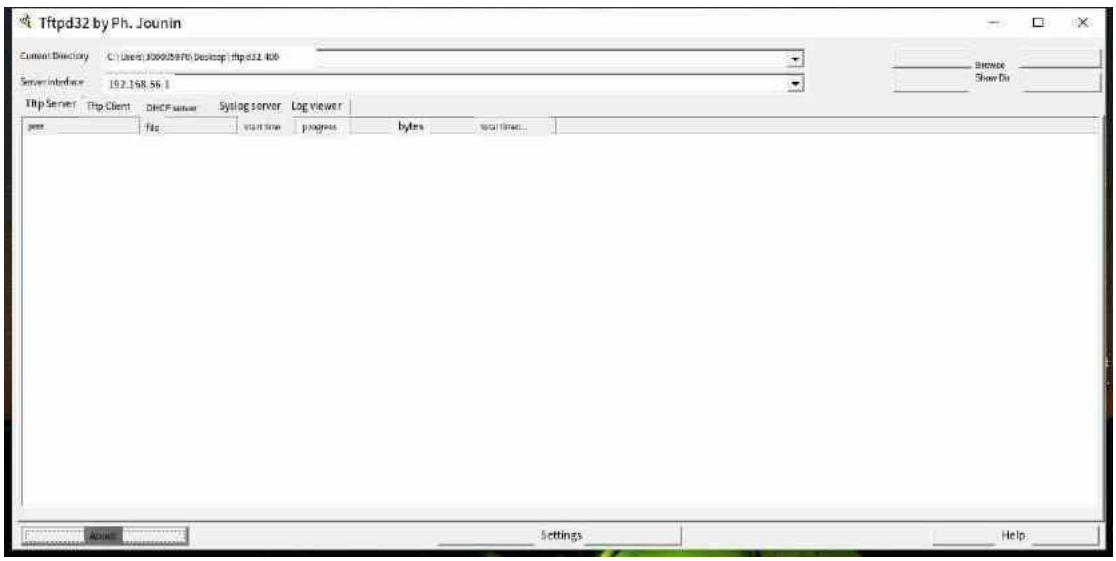


Figure 8-4 Refresh 12HDD BP CPLD

Note: current directory: indicates the file saving path. service interface: indicates the server ip address.

Step 2: Use SSH to log in to the BMC with the username sysadmin and password superuser

ssh sysadmin@<$BMCIP>

Step 3: Use TFTP tool under BMC to store CPLD FW file to /var path of BMC

tftp ClientIP -g -r file.aje -l /var/test.aje

Step 4: Run the refresh command, /usr/local/bin/Aje_Compress.elf12HDD /var/test.aje

/usr/local/bin/Aje_Compress.elf 12HDD /var/test.aje

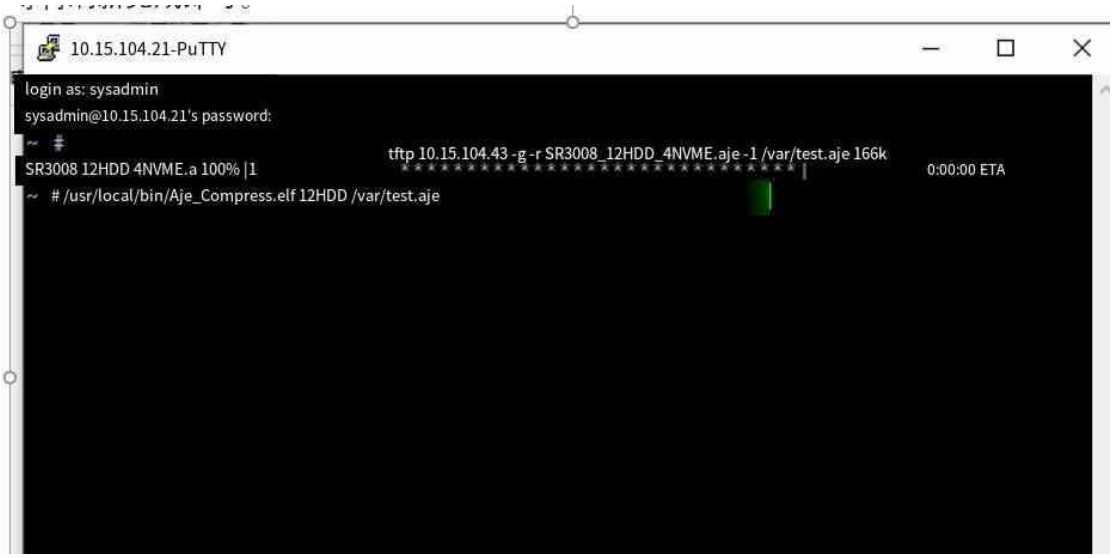


Figure 8-5 12HDD BP CPLD refresh

Step 5: After the refresh is complete, check whether the CPLD is updated successfully. The returned value is the CPLD version

ipmitool raw 0x34 0x32 0x02

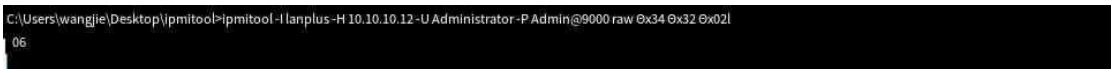


Figure 8-6 Refresh of 12HDD BP CPLD

8.1.1.3 Updated 4HDD BP CPLD

Step 1: Place the 4HDD BP CPLD FW (xxx.aje) file under the shared folder of the tftp server

Using tftp32 software in Windows, double click the tftpd32.exe program Step 2: Use SSH to log in to BMC with the login account name sysadmin and password superuser

ssh sysadmin@<$BMCIP>

Step 3: Use TFTP tool under BMC to store CPLD FW file to /var path of BMC

tftp ClientIP -g -r file.aje -l /var/test.aje

Step 4: Run the refresh command, /usr/local/bin/Aje_Compress.elf 4HDD /var/test.aje

/usr/local/bin/Aje_Compress.elf 4HDD /var/test.aje

Step 5: After the refresh is complete, check whether the CPLD is updated successfully. The returned value is the CPLD version information

ipmitool raw 0x34 0x32 0x03

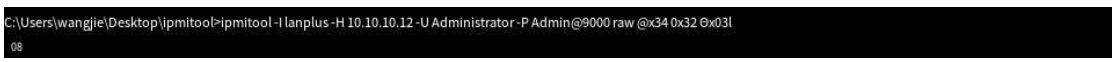


Figure 8-7 Refresh of 4HDD BP CPLD

8.1.2 Redfish updates the CPLD FW

Step 1: Create a session and obtain the token value

Operation type: POST

URL: https://device_ip/redfish/v1/SessionService/Sessions Request header:

Content-Type: header_type Request message body:

{

"UserName":username

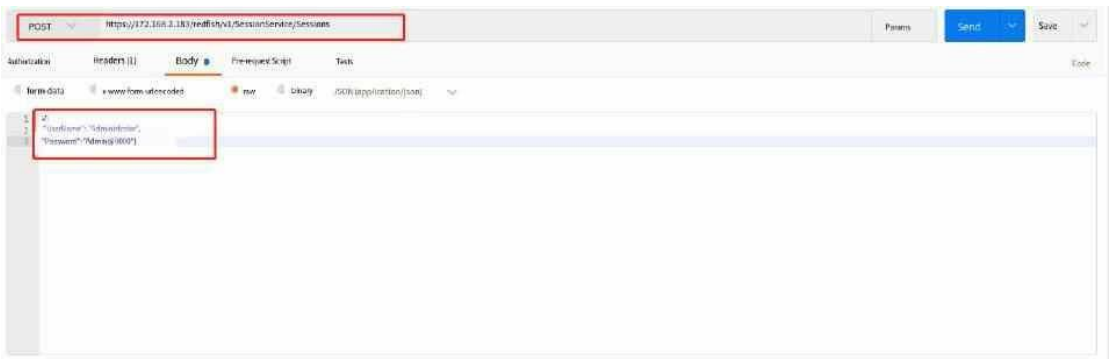
"Password":password

}

Parameter description:

Parameters	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
header_type	Format of the request message	application/json
username	Server username	Only administrators and operators have upgrade permissions. Therefore, use the existing administrator and operator usernames
password	Password of the server user	Only the administrator and operator have the upgrade permission. Therefore, use the password of the existing administrator and operator

Example screenshot:



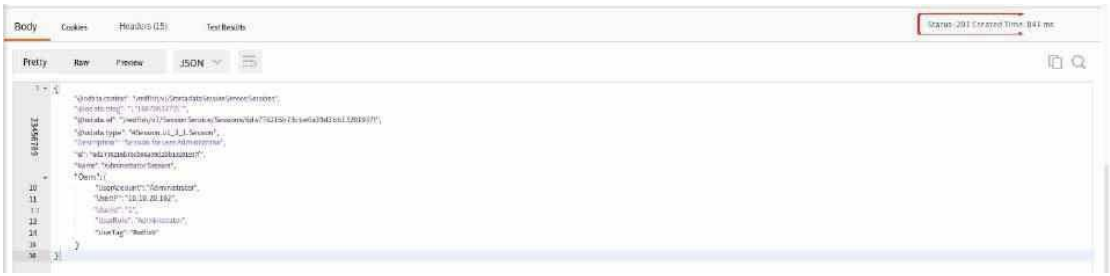


Figure 8-8 Creating a session

View the created session token value (default timeout is 300s)

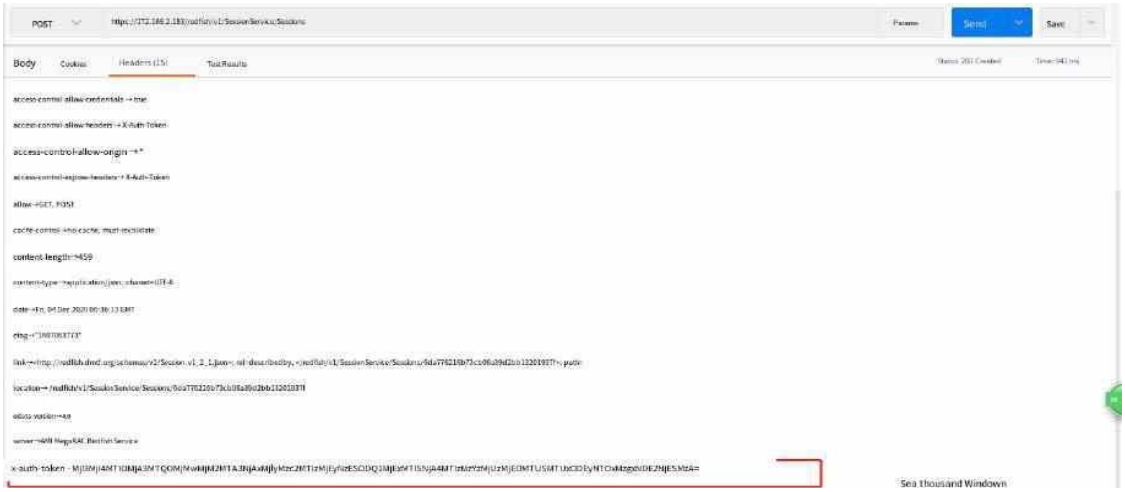


Figure 8-9 Viewing the created session token value

Step 2: Issue the command to upgrade CPLD and view the id of the upgrade task in the response body

Operation type: POST

URL: https://device_ip/redfish/v1/UpdateService/Actions/SimpleUpdate

When upgrading the firmware, note the following parameters: (

1) The user name and password are not required when upgrading the firmware through HTTP or HTTPS. BoardType and ImageType need to

be added. The optional value range of ImageType is PSU, CPLD, and BMC. The optional value range of BoardType is (MainBoard, 12NVME, 12HDD, 4HDD), other values are invalid; MainBoard CPLD firmware type is.vME suffix, 12NVME, 12HDD, and 4HDD CPLD firmware type is.aje suffix.

A sample is as follows:

Request header:

X-Auth-Token: auth_value

Content-Type: header_type Request message body:

{

"ImageURI": filepath,

"TransferProtocol": “FTP”,

"ImageType": "CPLD",

"BoardType": " MainBoard ",

"User":username

"Password":password

}

Parameter description:

Parameters	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	Through https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - x - auth - token value
header_type	Format of the request message	application/json
filepath	Path of the upgrade file	Such as: "Http://172.168.0.49/httpsshare/bpcpld.aje" "ftp://172.168.0.46/pub/cpld.jed"
protocol	Download the protocol required for the upgrade package	“HTTPS” “HTTP” “FTP”
BoardType	Type of CPLD to upgrade	"MainBoard", "12HDD", "4HDD"
username	Username for sharing the file with the FTP service	Note: This parameter is required only when you use FTP to download the upgrade package

password	Password for sharing the file with the FTP service	Note: This field is only required when you download the upgrade package using FTP

For example:

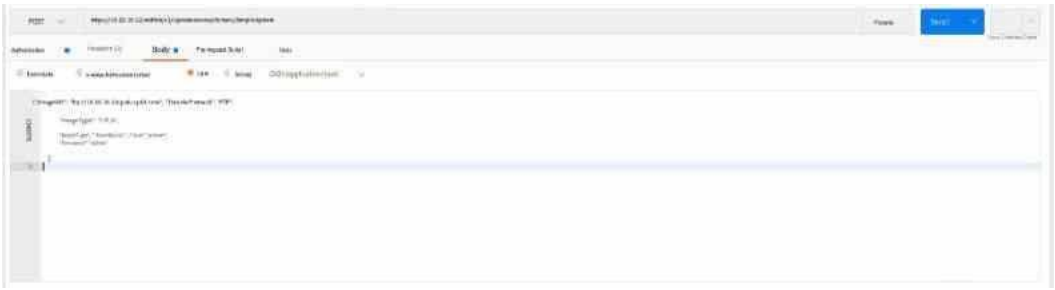


Figure 8-10 Refreshing the CPLD

Step 3: Check the upgrade task status and wait for the task to complete

Operation type: GET

URL: https://device_ip/redfish/v1/TaskService/Tasks/id Request header:

X-Auth-Token: auth_value Request message body: None Parameter Description:

Parameters	**Meaning**	**Value**
device_ip	ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	Through https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - x - auth - token value
id	id of the task you created	Obtained from the body of the response returned by the POST upgrade operation

Example operation:

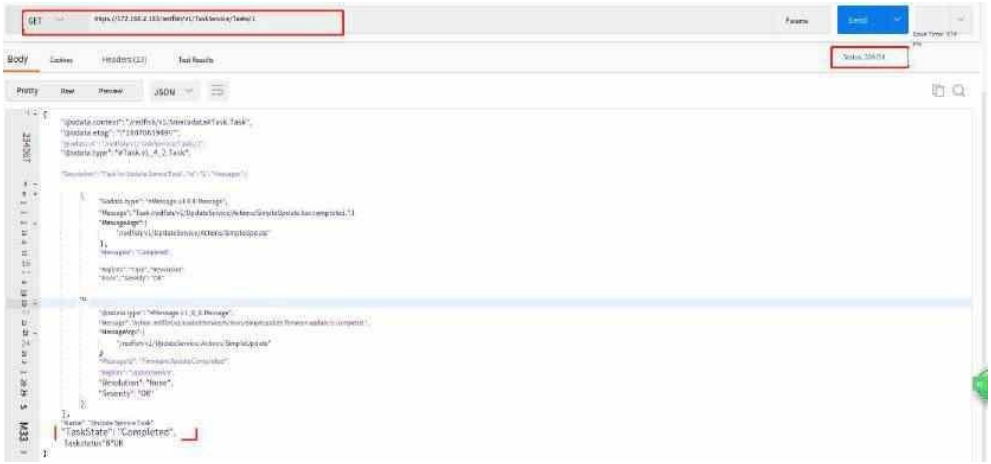


Figure 8-11 Upgrade task status

Information description is returned:

Return Information	Meaning	Return value
Response code	The response status of the request	200 OK
TaskState	Current state of the task	Specify the state of the task resource. New Starting Running Suspended Interrupted Pending Stopping Completed Killed Exception Service

8.2 Updating the PSU FW

8.2.1 SSH Updates the PSU FW

Step 1: Place the file (XXX.bin) used for the PSU upgrade under the shared folder of the tftp server

Using the tftp32 software in Windows, double-click the tftpd32.exe program Step 2: Use SSH to log in to BMC with the login account name sysadmin and password superuser

ssh sysadmin@<$BMCIP>

Step 3: Under BMC use TFTP tool to save PSU FW file to /var path of BMC

tftp ClientIP -g -r xxx.bin -l /var/psu.bin

Figure 8-12 Upgrade task status

Step 4: Run the refresh command: psuupdate A/B,

psuupdate A refreshes PSU0

psuupdate B refreshes PSU1

Step 5: When the refresh is complete, check whether the PSU has been updated successfully

The command to query PSU1 is as follows, to query PSU0, just replace 0x59 with 0x58.

i2c-test -b 1 -s 0x59 -m 1 -rc 40 -d 0x9B

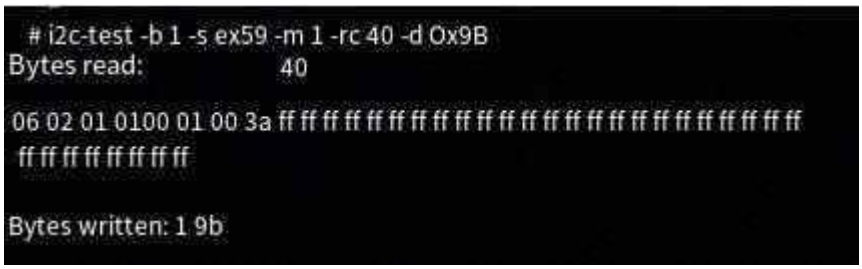


Figure 8-13 Check the PSU version

8.2.2 Redfish Updates the PSU FW

Step 1: Create a session and get the token value

Operation type: POST

URL: https://device_ip/redfish/v1/SessionService/Sessions Request header: Content-Type: header_type Request message body:

{

"UserName":username1.

"Password":password

}

Parameter description:

Parameters	Meaning	Value

device_ip	ip address of the server	Ipv4\ipv6\ domain name
header_type	Format of the request message	application/json
username1	Server username	Only administrators and operators have
		upgrade permissions. Therefore, use the existing administrator and operator usernames
password	Password of the server user	Only the administrator and operator have the upgrade permission. Therefore, use the password of the existing administrator and operator

For example:

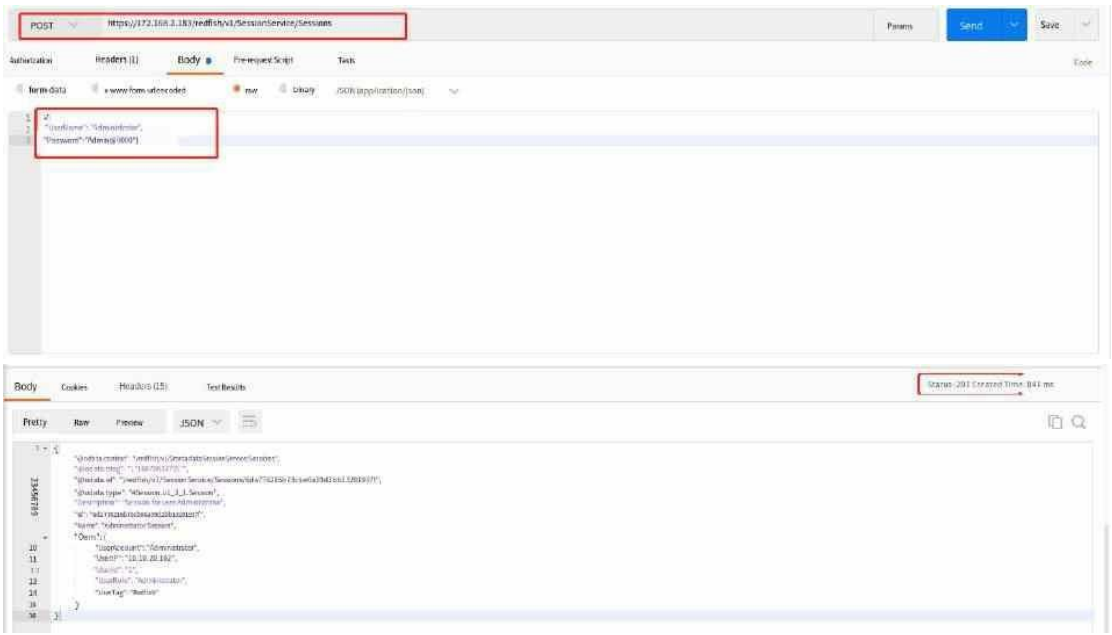


Figure 8-14 Creating a session

View the created session token value (default timeout is 300s)

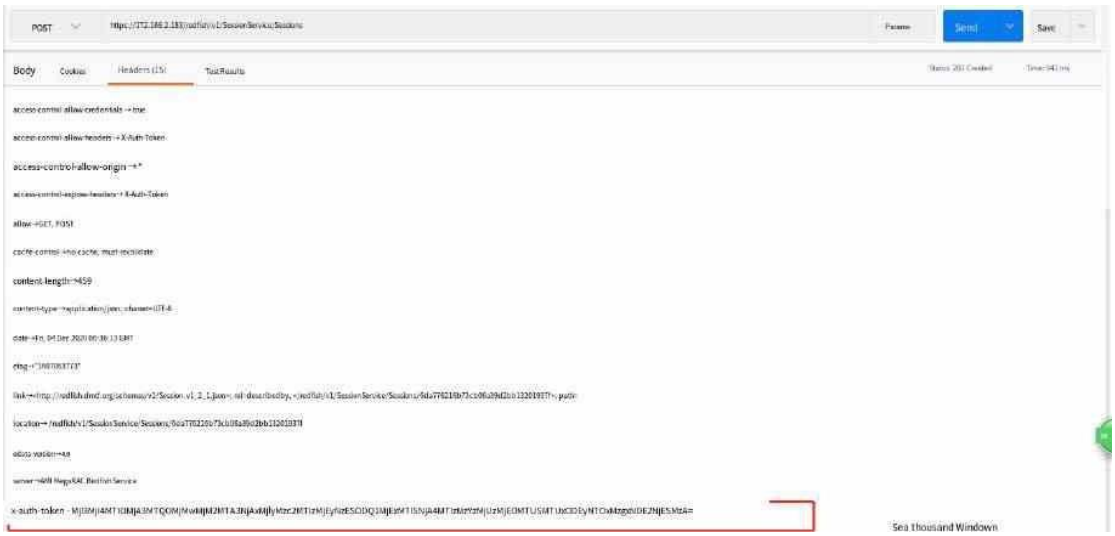


Figure 8-15 Viewing the created session token value

Step 2: Issue the upgrade PSU command to view the upgrade task id in the response body

Operation type: POST

URL: https://device_ip/redfish/v1/UpdateService/Actions/SimpleUpdate

Parameters for upgrading the firmware

To upgrade the PSU firmware

, you need to add the PsuId property, 1 for upgrading the power supply and 1 for upgrading the power supply 2. Other values are invalid The firmware type of the psu is the.bin suffix Examples are as follows:

Request header:

X-Auth-Token: auth_value

Content-Type: header_type Request message body:

{

"ImageURI" : "ftp://10.10.10.10/psu/psu31.bin"

, "TransferProtocol" : "FTP"

, "ImageType" : "PSU"

, "PsuId" : 1

, "User" : "admin"

, "Pass word":"admin"

}

Parameter description:

Table 8-6 Parameter description

Parameters	**Meaning**	**Value**

device_ip	The ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	Through https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - > x - auth - token value
header_type	Format of the	application/json
	request message	
filepath	Filepath 3 Path where the upgrade file is located	Such as: "Http://172.168.0.49/httpsshare/PSU1.bin" "ftp://172.168.0.46/pub/ PSU1. Bin"
protocol	Download the protocol required for the upgrade package	“HTTPS” “HTTP” “FTP”
username	Username for sharing the file with the FTP service	Note: This parameter is required only when you use FTP to download the upgrade package
password	Password for sharing the file with the FTP service	Note: This field is only required when you download the upgrade package using FTP

For example:

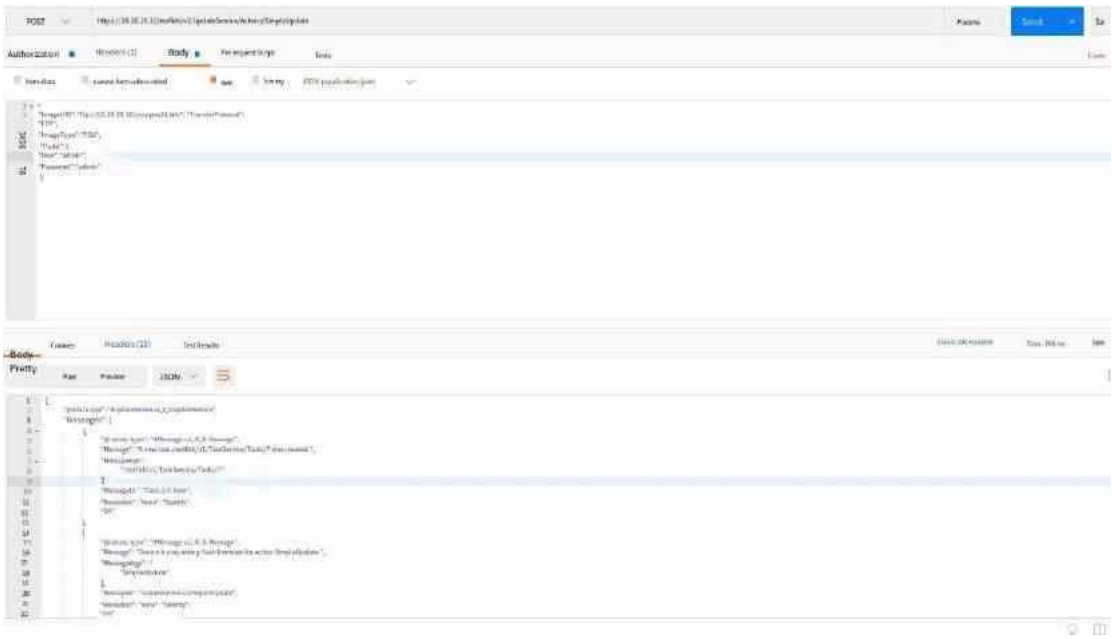


Figure 8-16 Refreshing the SPU

Step 3: Check the upgrade task status and wait for the task to complete

Operation type: GET

URL: https://device_ip/redfish/v1/TaskService/Tasks/id Request header:

X-Auth-Token: auth_value Request message body: none Parameter Description:

PARAMETERS	Meaning	Value
device_ip	The ip address of the server	Ipv4\ipv6\ domain name
auth_value	Authentication parameters for the request message	Through https://device_ip/redfish/v1/SessionService/Sessions create a session, when in the returned response Headers in the body - > x - auth - token value
id	id of the task you created	Obtained from the body of the response returned by the POST upgrade operation

Example operation:

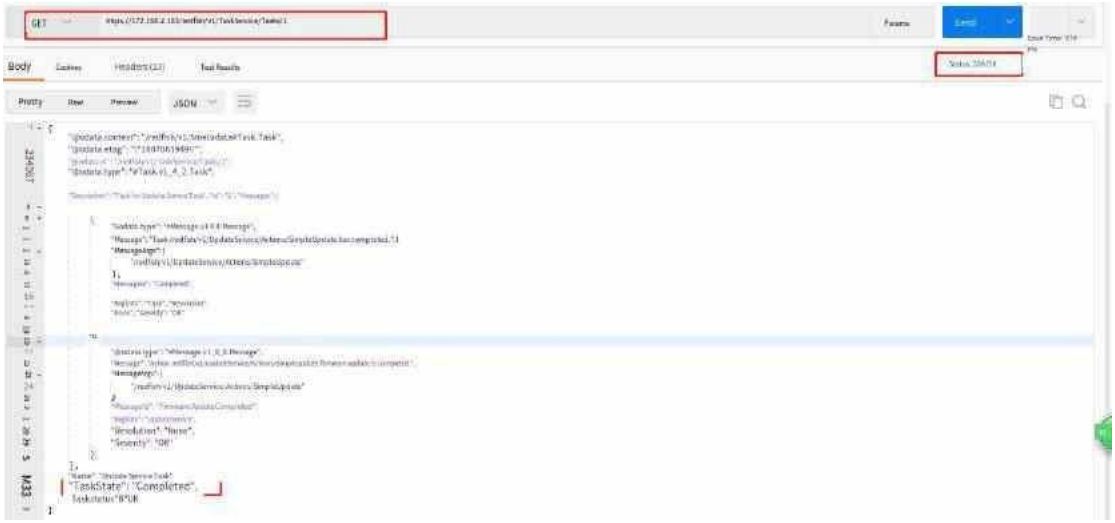


Figure 8-17 Upgrade task status Information description is returned:

Return Information	Meaning	Return value
Response code	The response status of the request	200 OK

Chapter 9 Hazard Instructions

9.1 Safety Precautions

- To protect your safety, read the following safety precautions in detail when installing the device:
- Follow the precautions and instructions marked on the device.
- Ensure that the voltage and frequency grading of the power supply conforms to the voltage and frequency indicated on the electrical specification label on the device.
- Do not insert any object into the opening of the device. Dangerous voltages may be present.
- Conductive objects may cause a short circuit, resulting in fire, electric shock, or damage.
- Do not install, use, or operate outdoor equipment (including but not limited to handling equipment, installing cabinets, installing power cables, etc.) or cables that are connected to the outdoors in bad weather such as lightning, rain, snow, and strong winds.
- Do not wear conductive objects such as watches, bracelets, bracelets, rings, and necklaces during installation, operation, and maintenance.
- Special insulation tools must be used during installation, operation and maintenance, such as wearing insulation gloves, safety clothing, safety helmet and safety shoes.
- Ensure that boards or filler panels are installed in all slots. Ensure that hazardous voltages and energy on boards are exposed, air ducts are normal, electromagnetic interference is controlled, and dust and other foreign bodies are protected from the backplane, baseboard, and boards.

9.2 Electrical Safety

- Electrical currents in power supplies, telephone and communication cables are dangerous. To avoid the danger of electric shock:
- Never connect or unplug any cables, or perform the installation, maintenance, or reconfiguration of this product during a thunderstorm.
- Connect all power cables to properly wired and grounded power outlets.
- Connect any device attached to this product to a properly wired outlet.
- When possible, use only one hand to connect or unplug the signal cable.

- Never turn on any device when there are signs of fire, flood, or house collapse.
- Unless otherwise instructed by the installation and configuration program, unplug connected power cables, telecommunications systems, networks, and modems before opening the cover of the device.
- Follow the instructions in the table below to connect and unplug cables when

installing, moving, or opening the cover or connecting device of this product.

To connect, follow these steps	To sever the connection, perform the following steps
Turn off all devices. First, connect all cables to the unit. 3. Connect the signal cable to the connector. Connect the power cord to the outlet. Turn on the power to the device.	Step 1 Turn everything off. First, unplug the power cord from the outlet. Unplug the signal cable from the connector. Unplug all cables from the device.

9.3 Battery Safety

When replacing a lithium battery, only replace it with the same type of battery recommended by the manufacturer. If the system has modules that contain lithium batteries, they can only be replaced with modules of the same type made by the same manufacturer. Lithium batteries may cause an explosion if improperly used, handled or discarded.

The following actions are prohibited:

- Plunge or submerge the battery in water
- Heat the battery to over 100°C (212°F)
- Repair or remove the battery
- Dispose of the battery as required by your local ordinances and regulations.

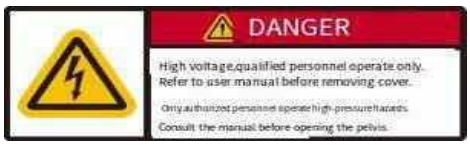
9.4 Laser component safety

When installing laser products, please note the following:

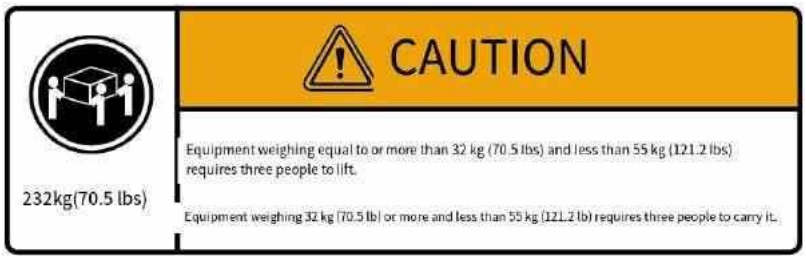
Do not remove the cover plate. Removing the cover of a laser product can result in exposure to dangerous laser radiation. There are no repairable parts in the unit. Failure to control, adjust, or perform the procedures specified here may result in exposure to dangerous radiation.

9.5 9.5 General Safety Symbol Instructions

	Warning Sign: This sign indicates that improper operation of the device may result in personal injury or damage to the device. Please follow the instructions.
	Protective grounding label: This label is affixed near the protective grounding terminal and is used next to the terminal where the device is connected to the external grounding network.
	Equipotential connection identifier, this identifier is used for equipotential connection terminals, that is, next to each equipotential terminal inside the device.
	Electrostatic sign: Use this sign in any electrostatic sensitive area. When you see this label, wear ESD gloves or a wristband before operating the device.
	Overheat warning label: This label is affixed to the surface of the device that may be scalded by high temperature. It warns the user not to touch the device casually during operation and maintenance. Please wear anti-hot gloves to avoid scalding.

	Non-tropical climate label: Only suitable for safe use in non-tropical climate conditions.
	Altitude instruction mark: Only for safe use in areas with an altitude of 2000 meters.
	High pressure hazards are operated by authorized personnel only. Consult the manual before opening the lid.
	Never touch the fan blades while the fan is rotating!
	Do not stack the devices after unpacking them. Device damage may occur.
	Do not place any objects on top of the rack-mounted device.
	Electric shock hazard! All power inputs must be disconnected when the device is powered off!

Equipment weighing less than 18 kg (39.7 lb) can be carried by one person. Equipment weighing 18 kg (39.7 lb) or more and less than 32 kg (70.5 lb) requires two people to carry it.



Equipment weighing 32 kg (70.5 lb) or more and less than 55 kg (121.2 lb) requires three people to carry it.

Equipment weighing 55 kg (121.2 lb) and less than 72 kg (157.8 lb) requires four people to carry it.

Equipment weighing 72 kg (158.7 lb) or greater requires the use of lifting equipment.

Check the relevant sections of the user manual before operating the product.

Chapter 10 Troubleshooting Guide

10.1 The startup process fails

The server needs to load all hardware on the mainboard during startup. Resources are allocated to some important components in phases during startup. In order to facilitate the handling of problems that may occur in each stage, the error codes corresponding to SEC, PEI and DXE in the POST process are described as follows.

10.1.1 Querying the POST process code

During the startup process of the server, according to the hardware self-check, the

BIOS will use the code to represent the current POST corresponding phase.

Table 10-1 Boot process code scope and description

Status Code Range	Description
0x01 – 0x0B	SEC enforcement
0x0C – 0x0F	SEC error
0x10 – 0x2F	PEI performs to memory initialization
0x30 – 0x4F	PEI executes after memory initialization
0x50 – 0x5F	PEI error
0x60 – 0x8F	DXE executes to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE error
0xE0 – 0xE8	S3 Restart (PEI)
0xE9 – 0xEF	S3 Restart error (PEI)
0xF0 – 0xF8	Restore (PEI)
0xF9 – 0xFF	Recovered Error (PEI)

SEC and PEI stage startup codes are examples in the red box in Figure 10-1, and DXE and BDS stage startup codes are examples in the red box in Figure 10-2.

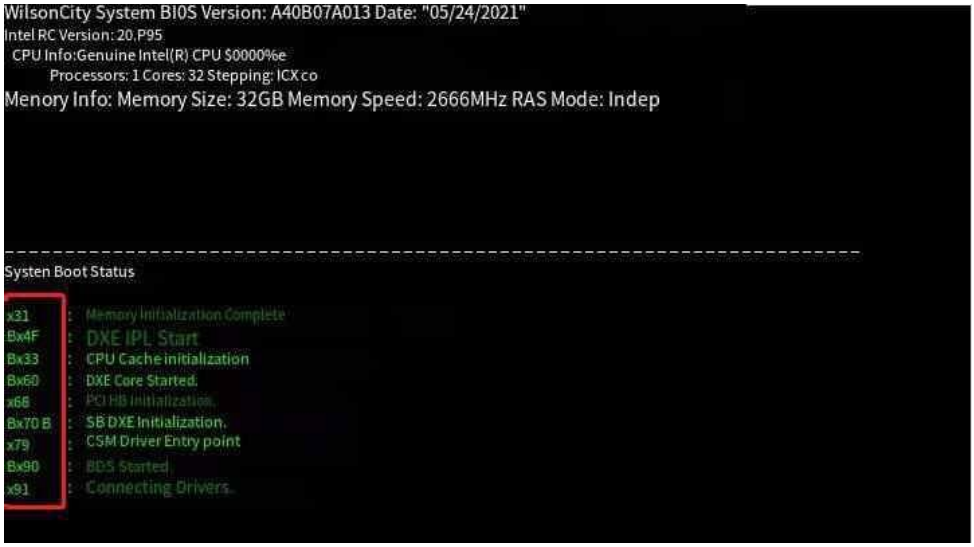


Figure 10-1 Startup codes for SEC and PEI phases

Figure 10-2 Startup codes for DXE and BDS phases

It is not possible to display all the boot codes during the boot process, and you may not notice the corresponding boot codes when a fault occurs. Therefore, you can log in to the BMC Web to view the details of the boot codes when a fault occurs. On the menu bar "Maintenance" as shown in Figure 10-3, select "Startup self-check code" to go to the page as shown in Figure 10-4. Check the current startup code or download it as required.

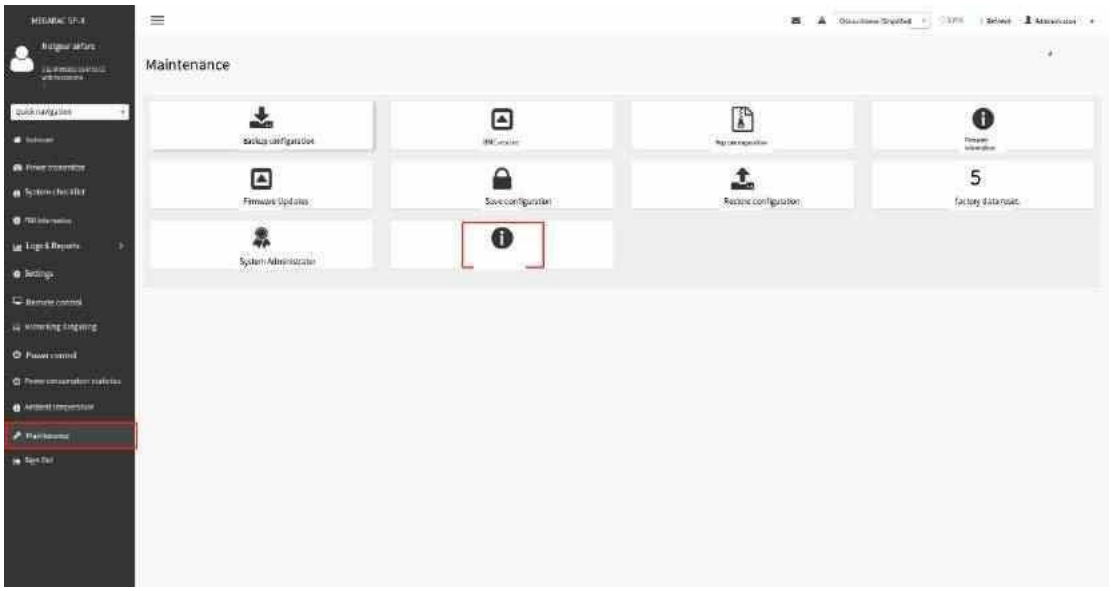


Figure 10-3 BMC Web Startup self-check code page

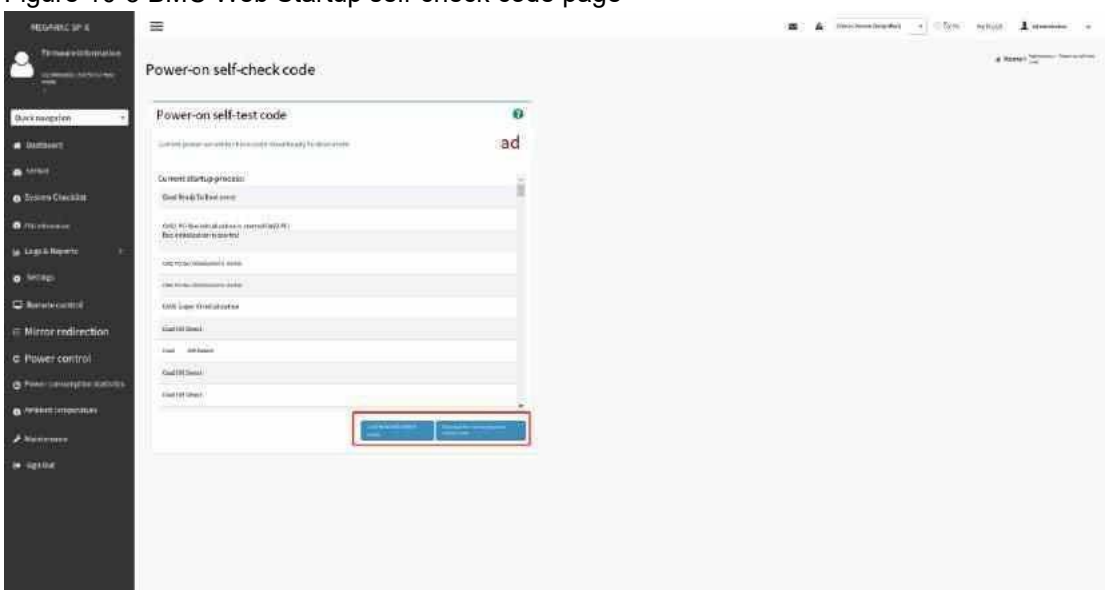


Figure 10-4 BMC Web startup self-check code content

10.1.2 SEC error code and status

SEC is the first phase when a server is added or started. The error codes in this phase are listed in Table 10-2:

Table 10-2 SEC error codes and their descriptions

SEC error code	Description
0x0C – 0x0D	SEC error code reserved field
0x0E	Microcode not found
0x0F	Microcode not loaded

10.1.3 PEI Error code and status

After completing SEC phase initialization, proceed to PEI phase to initialize memory in preparation for DXE. The error codes in this phase are shown in Table 10-3, 10-4, and 10-5:

Table 10-3 PEI error codes and descriptions

PEI Error Codes	Description
0x50	Memory initialization error, invalid memory type or speed incompatible
0x51	Memory initialization error, SPD read failed
0x52	Memory initialization error, invalid memory size or module mismatch
0x53	Memory initialization error, no available memory detected
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch
0x58	Failed CPU self-test or possible CPU cache error
0x59	CPU microcode not found or microcode update error
0x5A	Internal CPU error
0x5B	Reset PPI unavailable
0x5C	PEI phase BMC self-test failed
0x5D-0x5F	Error code reserve field

Table 10-4 PEI Phase S3 restart codes and descriptions

Phase PEI S3 Restart code	Description
0xE8	S3 Restart Failure
0xE9	S3 Restart PPI not found

0xEA	S Restart boot script error
0xEB	S3 OS wake up error
0xE8 – 0xEF	Reserved fields

Table 10-5 PEI Phase Recovery error codes and descriptions

Phase PEI Recovery error codes	Description
0xF8	Restoring a PPI is ineffective
0xF9	Restore Protection not found
0xFA	Invalid Restore protection
0xFB - 0xFF	Reserved field

10.1.4 DXE error code and status

In the DXE stage, the memory is fully initialized and ready for use, allowing for more complex work. The error codes in this stage are shown in Table 10-6:

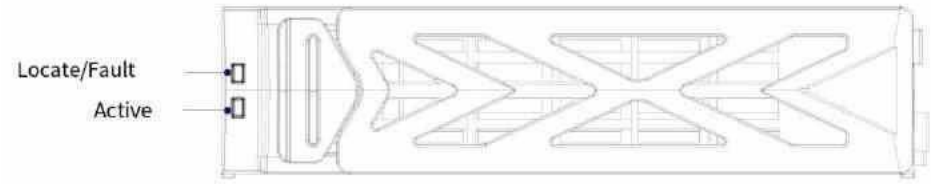
Table 10-6 DXE error codes and their descriptions

DXE error codes	**Description**
0xD0	CPU initialization error
0xD1	Northbridge initialization error
0xD2	Error initializing Southbridge
0xD3	Some architecture agreements are not in effect
0xD4	PCI resource allocation error, resource exceeded
0xD5	No room for Legacy OpRom
0xD6	Console output device not found
0xD7	Console input device not found
0xD8	Invalid password
0xD9	Error loading boot option (loading Image returns error)
0xDA	Boot option failed (start Image returns error)
0xDB	Flash update failed
0xDC	Reset protocol unavailable
0xDD	BMC self-check failed in DXE phase

10.2 Indicator Alarm

10.2.1 Hard Drive Indicator

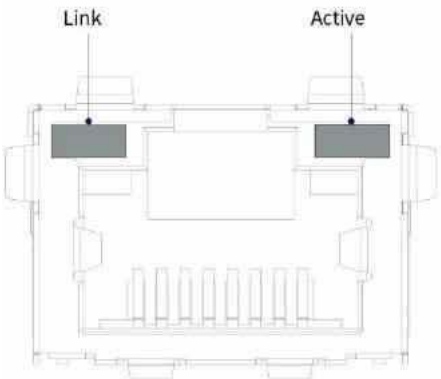
The hard disk indicators on the panel indicate the status of a hard disk. The following figure shows the hard disk indicators (using a 3.5-inch hard disk as an example) :



Yellow (Locate/Fault) and green (Active)	Function definition
Green steady on Yellow light off	Hard drive present
The green light is blinking (4HZ) and the yellow light is off	Hard Drive Read and write
Steady green, blinking yellow (1HZ)	Hard drive is located
Blinking green (1HZ) and blinking yellow (1HZ)	Hard disk is under reconstruction
The green light is off and the yellow light is on	A hard disk in the RAID group is removed
The green light is steady on and the yellow light is steady on	Hard drive failure

10.2.2 Network Adapter Indicators

The network port indicator is used to indicate that the network port is in different working states. The network port indicator is shown as follows:

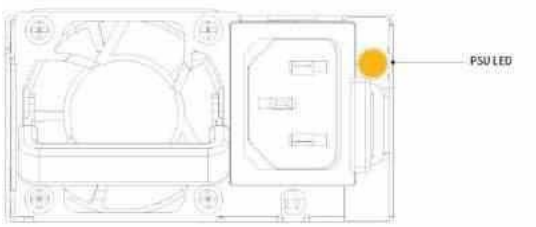


Indicator name	Indicator color	Function definition
Link LED	Continuous green	Network links at 1Gbps
	Persistent yellow	Network links at 100Mbps

	destroy	The network is connected or not connected at 10Mbps
	Flashing yellow	The network has data receiving and sending
Active LED	destroy	No data is received or sent on the network

10.2.3 Power Indicator

The power indicator refers to the LED on the PSU body, and the PSU LED is shown below:



LED action and color	Function definition
Continuous green	Inputs and outputs are normal
Blinking green (1HZ)	Input Normal, standby state
Blinking green (2HZ)	Upgrading firmware
Steady on in tan	Normal input, no output
destroy	No AC power input is available

10.3 Log Alarm

Logs record the status changes of major devices for fault diagnosis.

10.3.1 CPU Alarms and Handling Suggestions

Sensors	Log description	Handling suggestions
CPU_STATUS	IERR	Switch the position of the CPU for which the alarm is generated to that of the normal CPU, identify the faulty component, replace the faulty CPU, and check whether the alarm is cleared Replace the mainboard of the server. Then check whether the alarm is cleared
	Thermal Trip	1. Check whether the fan module is faulty.

		Then replace the fan module Check whether the ambient temperature in the equipment room exceeds the threshold. Adjust the ambient temperature to the threshold. Then check whether the alarm is cleared Check whether the air intake or air exhaust of the server is blocked. Then remove the foreign matter and check whether the alarm is cleared Check whether the air duct is properly installed inside the server. Then install the air duct Check whether the CPU heat sink is correctly installed. Then check whether this alarm is cleared Apply silica gel to the CPU and reinstall it. Then check whether the alarm is cleared Replace the mainboard. Then check whether the alarm is cleared Replace the CPU. Then check whether the alarm is cleared
	Processor Configuration Error	Switch the position of the CPU where the alarm is generated to that of the normal CPU. Locate the faulty component and replace the faulty CPU Replace the mainboard of the server. Then check whether the alarm is cleared

	Correctable Machine Check Error	If multiple MCES occur in a row, switch the position of the CPU that generates the alarm to that of the normal CPU. Locate the faulty component, replace the faulty CPU, and check whether the alarm is cleared Replace the mainboard of the server. Then
		check whether the alarm is cleared

10.3.2 Memory Alarms and Handling Suggestions

Sensors	**Log description**	**Handling suggestions**
DIMMxx_Status	Uncorrectable ECC	Remove and reinsert the DIMM where the alarm is generated. Then check whether the alarm is cleared. 2. Swap the DIMM where the alarm is generated with the DIMM and check whether the alarm is migrated to the DIMM. 3. Replace the DIMM where the alarm is generated. Then check whether the alarm is cleared. 4
	Correctable ECC logging limit reached	1. When this alarm is generated, the server can operate normally. Replace the DIMM in an appropriate time and environment. Then check whether the alarm is cleared

10.3.3 PCIE Device Alarms and Handling Suggestions

Sensors	**Log description**	**Handling suggestions**

PCIE_Status	Bus Correctable Error	Check whether the PCIE device and its corresponding slot are damaged or in poor contact. Remove and reinstall the PCIE device. Then check whether the alarm is cleared. Replace the PCIE device. Then check whether the alarm is cleared
	Bus Uncorrectable Error	1. Check whether the PCIE device and its corresponding slot are damaged or in poor contact. Remove and reinstall the PCIE device. Replace the PCIE device. Then check whether the alarm is cleared

	Bus Fatal Error	1. Check whether the PCIE device is damaged or in poor contact with the corresponding slot. Then remove and reinstall the PCIE device. Replace the PCIE device. Then check whether the alarm is cleared
	Bus Degraded	1. Check whether the PCIE device and its slot are damaged or in poor contact. Remove and reinstall the PCIE device. Replace the PCIE device. Then check whether the alarm is cleared

10.3.4 Hard Disk Alarms and Handling Suggestions

Sensors	Log description	Handling suggestions
xHDD_BP_DISKx	Drive Fault	1. Replace the storage device where the alarm is generated. Then check whether the alarm is cleared

10.3.5 Power Supply Alarms and Handling Suggestions

Sensors	Log description	Handling suggestions
PSUx_Status	Power Supply Failure detected	Remove and reinstall the power supply. Then check whether the alarm is cleared Replace the power module. Then check whether the alarm is cleared

	error	standby PSU is not 8V higher than that of the active PSU Cross the input power cables of the active and standby PSU. Then check whether the alarm is cleared Replace the PSU. Then check whether the alarm is cleared
	Power Supply input lost or out-of-range	Remove and reinsert the cable of the power supply module. Then check whether the alarm is cleared Replace the power cable. Then check whether the alarm is cleared Replace the power module where the alarm is generated. Then check whether the alarm is cleared
	Configuration	1. In active/standby mode, the input voltage of the

10.3.6 Fan Alarms and Handling Suggestions

Sensors	**Log description**	**Handling suggestions**
FANx _Status	Device Absent	Check whether the fan module is removed. If yes, reinstall the fan module and check whether the alarm is cleared Remove and reinstall the fan module. Then check whether the alarm is cleared Replace the alarm fan module. Then check whether the alarm is cleared

10.3.7 Threshold Sensor Alarms and Handling Suggestions

Sensors	**Log description**	**Handling suggestions**

Power Sensor	Upper Critical going high	The read value of the sensor exceeds the upper critical going high threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
FANx_Speed	Lower Critical going low	The read value of the sensor exceeds the low critical going low threshold View the components corresponding to the sensor and check whether the environment is

		properly configured 3. Restart the BMC after confirming that the environment is normal
	Upper Critical going high	The read value of the sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
PSUx_Input_Vol	Lower Non-critical going low	The read value of the corresponding sensor exceeds the low recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal

	Upper Non-critical ging high	The read value of the corresponding sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
PSUx_Pin	Upper Non-critical ging high	The read value of the corresponding sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured After the environment is normal, restart the BMC
PSUx_Pout		The read value of the sensor exceeds the high recoverable threshold View the components corresponding to the

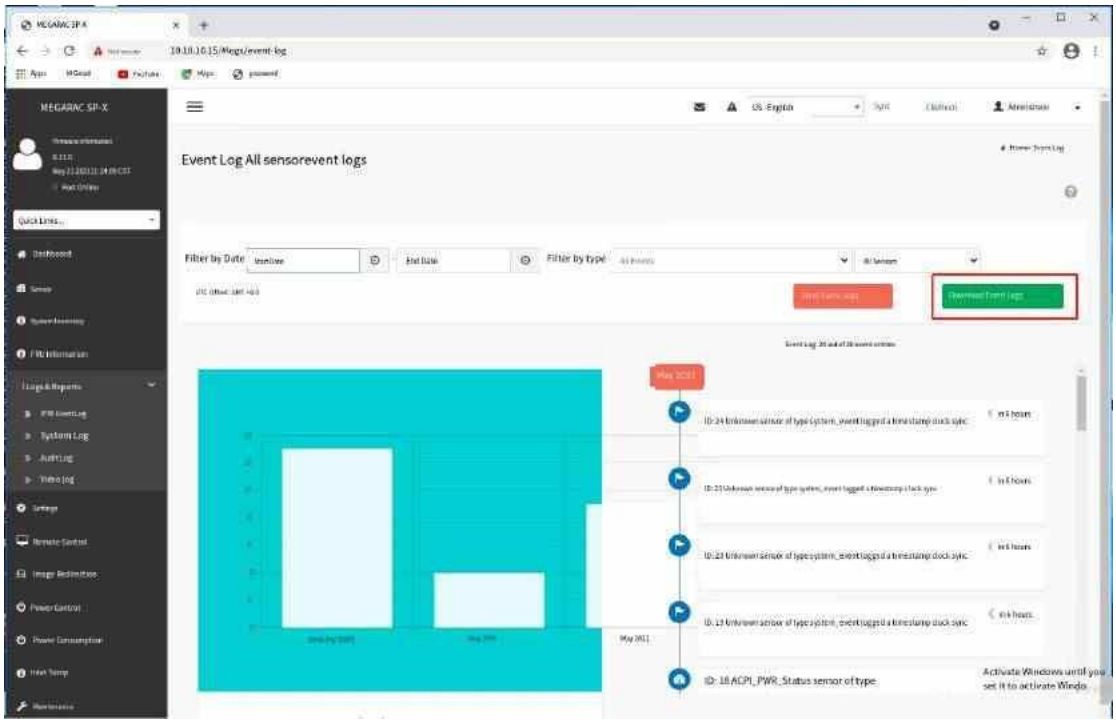
		sensor and check whether the environment is properly configured 3. Restart the BMC after confirming that the environment is normal
PSUx_Temp		The read value of the sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal

PSUx_Fan		The read value of the sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
Voltage Sensor	Upper Non-critical ging high	The read value of the corresponding sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
	Upper Critical going high	The read value of the sensor exceeds the upper critical going high threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
	Lower Non-critical	1. The read value of the corresponding sensor exceeds the low recoverable threshold
	going low	View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal

	Lower Critical going low	The read value of the sensor exceeds the low critical going low threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
Temp Sensor	Upper Non-critical ging high	The read value of the corresponding sensor exceeds the high recoverable threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal
	Upper Critical going high	The read value of the sensor exceeds the upper critical going high threshold View the components corresponding to the sensor and check whether the environment is properly configured Restart the BMC after confirming that the environment is normal

10.3.8 Collecting Logs

Web Download the IPMI Event Log


MEGARAC SP-X
Event Log All sensorevent logs
Filter By Date
Filter by type
Download Event Logs
Dashboard
Sensor
FRU Information
Logs & Reports
IPMI Event Log
System Log
Audit Log
Video Log
Settings
Remote Control
Image Redirection
Power Control
Power Consumption
Host Temp
Maintenance
Activate Windows until you set it to activate Windo

Appendix: Acronyms and abbreviations

Abbreviations	Explanations
BIOS	Short for BASIC INPUT/OUTSYSTEM.
CMOS	Short for COMPLEMENTARY METAL OXIDE SEMICONDUCTOR.
PXE	Short for Preboot eXecution Environment.
UEFI	Short for Unified Extensible Firmware Interface.
CPU	Short for Central Processing Unit.
PCH	PCH, short for Platform Controller Hub.
SATA	Short for Serial ATA.
Server Mgmt	Short for Server Management.
ROM	Short for READ ONLY MEMORY.
ACPI	Acpi, short for Advanced Configuration and Power Management Interface.
PCI	Short for Peripheral Component Interconnect Standard.
ME	Short for Management Engine.
UPI	Short for Ultra Path Interconnect.
FRU	Short for Field Replace Unit
HDD	Short for Hard Disk Drive.
CSM	Short for Compatibility Support Module.