

# **GIGABYTE™**

# **R284-S92-AAJ1**

Rack Server - Intel® Xeon® 6 Processors  
2U DP 24+2-Bay Gen5 NVMe/SATA/SAS-4

## **User Manual**

Rev. 1.0

## **Copyright**

© 2026 Giga Computing Technology CO., LTD. All rights reserved.

The trademarks mentioned in this manual are legally registered to their respective owners.

## **Disclaimer**

Information in this manual is protected by copyright laws and is the property of Giga Computing. Changes to the specifications and features in this manual may be made by Giga Computing without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without Giga Computing's prior written permission.

## **Documentation Classifications**

In order to assist in the use of this product, Giga Computing provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use of this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents.




## **For More Information**

For related product specifications, the latest firmware and software, and other information please visit our website at <http://www.gigabyte.com/Enterprise>

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email: [marketing@gigacomputing.com](mailto:marketing@gigacomputing.com)

## Conventions

The following conventions are used in this user's guide:

	<b>NOTE!</b> Pieces of additional information related to the current topic.
	<b>CAUTION!</b> Precautionary measures to avoid possible hardware or software problems.
	<b>WARNING!</b> Alerts to any damage that might result from doing or not doing specific actions.

## Server Warnings and Cautions

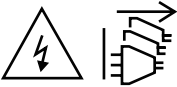
Before installing a server, be sure that you understand the following warnings and cautions.



### **WARNING!**

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

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.



- Shock Hazard! Disconnect all power supply cords before servicing.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.



### **WARNING!**

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



**This server is equipped with high speed fans. Keep away from hazardous moving fan blades during servicing.**



**This equipment is intended to be used in Restrict Access Location. The access can only be gained by Skilled person. Only authorized by well trained professional person can access the restrict access location.**

•



**This equipment is not intended for use by children.**

**CAUTION!**

- Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
- Danger of explosion if battery is incorrectly replaced.
- Replace only with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

**CAUTION!**

Risk of explosion if battery is replaced incorrectly or with an incorrect type. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

**Warning Stability hazard**

The slide-rail may tip over causing serious personal injury

- Before extending the rack to its installation position, read the installation instructions.
- Do not put any load on the slide-rail mounted equipment in the installation position.
- Do not leave the slide-rail mounted equipment in the installation position.



## Electrostatic Discharge (ESD)

### CAUTION!

ESD CAN DAMAGE DRIVES, BOARDS, AND OTHER PARTS. WE RECOMMEND THAT YOU PERFORM ALL PROCEDURES AT AN ESD WORKSTATION. IF ONE IS NOT AVAILABLE, PROVIDE SOME ESD PROTECTION BY WEARING AN ANTI-STATIC WRIST STRAP ATTACHED TO CHASSIS GROUND -- ANY UNPAINTED METAL SURFACE -- ON YOUR SERVER WHEN HANDLING PARTS.

Always handle boards carefully, they can be extremely sensitive to ESD. Hold boards only by their edges without touching any components or connectors. After removing a board from its protective ESD bag or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the ESD bag. Do not slide the board over any surface.

**System power on/off:** To service components within the server, please ensure the power has been disconnected.

e.g. Remove the node from the server chassis (to disconnect power) or disconnect the power from the server chassis.

Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

**Hazardous conditions, devices and cables:** Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system chassis and disconnect the cables attached to the system before servicing the chassis. Otherwise, personal injury or equipment damage can result.

**Electrostatic discharge (ESD) and ESD protection:** ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface on the server) when handling parts.

**ESD and handling boards:** Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

**Installing or removing jumpers:** A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fingertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

# Table of Contents

Chapter 1 Hardware Installation .....	11
1-1 Installation Precautions .....	11
1-2 Product Specifications .....	12
1-3 System Block Diagram .....	16
Chapter 2 System Appearance .....	17
2-1 Front View .....	17
2-2 Rear View .....	18
2-3 Front Panel LEDs and Buttons .....	19
2-4 RoT LEDs .....	20
2-5 Rear System LAN LEDs .....	22
2-6 Power Supply Unit LED .....	23
2-7 Hard Disk Drive LEDs .....	24
Chapter 3 System Hardware Installation .....	25
3-1 Removing and Installing the Chassis Cover .....	26
3-2 Removing and Installing the Hard Disk Drive .....	27
3-3 Removing and Installing the Fan Duct .....	28
3-4 Removing and Installing the Heat Sink .....	29
3-5 Installing the CPU and Heat Sink .....	30
3-6 Removing and Installing Memory .....	32
3-6-1 Eight Channel Memory Configuration .....	32
3-6-2 Removing and Installing a Memory Module .....	33
3-6-3 DIMM Population Table .....	34
3-6-4 Processor and Memory Module Matrix Table .....	36
3-7 Removing and Installing the PCIe Card .....	37
3-8 Installing the Mezzanine Card .....	38
3-8-1 Installing the OCP 3.0 Mezzanine Card .....	38
3-9 Replacing the Fan Assembly .....	39
3-10 Removing and Installing the Power Supply .....	40
3-11 Removing the LAN Cable .....	41
3-12 Cable Routing .....	42

- Chapter 4 Motherboard Components ..... 49
  - 4-1 Motherboard Components ..... 49
  - 4-2 Jumper Settings ..... 51
  - 4-3 Backplane Board Storage Connector ..... 52
    - 4-3-1 CBP20G0 (Front System Storage Board) ..... 52
    - 4-3-2 CBP2081 (Front System Storage Board) ..... 53
    - 4-3-3 CBP2025 (Rear System Storage Board) ..... 54
- Chapter 5 BIOS Setup ..... 55
  - 5-1 The Main Menu ..... 57
  - 5-2 Advanced Menu ..... 60
    - 5-2-1 Trusted Computing ..... 61
    - 5-2-2 Serial Port Console Redirection ..... 62
    - 5-2-3 SIO Configuration ..... 65
    - 5-2-4 PCI Subsystem Settings ..... 66
    - 5-2-5 USB Configuration ..... 68
    - 5-2-6 Network Stack Configuration ..... 69
    - 5-2-7 Post Report Configuration ..... 70
    - 5-2-8 KMIP Server Configuration ..... 71
    - 5-2-9 NVMe Configuration ..... 72
    - 5-2-10 Chipset Configuration ..... 73
    - 5-2-11 Tls Auth Configuration ..... 74
    - 5-2-12 iSCSI Configuration ..... 75
    - 5-2-13 Intel(R) i350 Gigabit Network Connection ..... 76
    - 5-2-14 VLAN Configuration ..... 78
    - 5-2-15 MAC IPv6 Network Configuration ..... 79
    - 5-2-16 MAC IPv4 Network Configuration ..... 80
    - 5-2-17 Driver Health ..... 81
  - 5-3 Chipset Menu ..... 82
    - 5-3-1 Processor Configuration ..... 83
    - 5-3-2 Common RefCode Configuration ..... 86
    - 5-3-3 UPI Configuration ..... 87
    - 5-3-4 Memory Configuration ..... 89
    - 5-3-5 IIO Configuration ..... 92
    - 5-3-6 Advanced Power Management Configuration ..... 93
    - 5-3-7 Miscellaneous Configuration ..... 95
    - 5-3-8 Runtime Error Logging Settings ..... 96
    - 5-3-9 Power Policy ..... 98

5-4	Server Management Menu.....	100
5-4-1	System Event Log .....	102
5-4-2	View FRU Information .....	103
5-4-3	BMC VLAN Configuration.....	104
5-4-4	BMC Network Configuration.....	105
5-4-5	IPv6 BMC Network Configuration.....	106
5-5	Security Menu .....	107
5-5-1	Secure Boot .....	108
5-6	Boot Menu.....	111
5-7	Save & Exit Menu.....	113
5-8	BIOS Recovery .....	115

# Chapter 1 Hardware Installation

## 1-1 Installation Precautions

The motherboard/system contain numerous delicate electronic circuits and components which can become damaged as a result of electrostatic discharge (ESD). Prior to installation, carefully read the service guide and follow these procedures:








- Prior to installation, do not remove or break motherboard S/N (Serial Number) sticker or warranty sticker provided by your dealer. These stickers are required for warranty validation.
- Always remove the AC power by unplugging the power cord from the power outlet before installing or removing the motherboard or other hardware components.
- When connecting hardware components to the internal connectors on the motherboard, make sure they are connected tightly and securely.
- When handling the motherboard, avoid touching any metal leads or connectors.
- It is best to wear an electrostatic discharge (ESD) wrist strap when handling electronic components such as a motherboard, CPU or memory. If you do not have an ESD wrist strap, keep your hands dry and first touch a metal object to eliminate static electricity.
- Prior to installing the motherboard, please have it on top of an antistatic pad or within an electrostatic shielding container.
- Before unplugging the power supply cable from the motherboard, make sure the power supply has been turned off.
- Before turning on the power, make sure the power supply voltage has been set according to the local voltage standard.
- Before using the product, please verify that all cables and power connectors of your hardware components are connected.
- To prevent damage to the motherboard, do not allow screws to come in contact with the motherboard circuit or its components.
- Make sure there are no leftover screws or metal components placed on the motherboard or within the computer casing.
- Do not place the computer system on an uneven surface.
- Do not place the computer system in a high-temperature environment.
- Turning on the computer power during the installation process can lead to damage to system components as well as physical harm to the user.
- If you are uncertain about any installation steps or have a problem related to the use of the product, please consult a certified computer technician.

# 1-2 Product Specifications



**NOTE:**

We reserve the right to make any changes to the product specifications and product-related information without prior notice.

 System Dimension	<ul style="list-style-type: none"><li>◆ 2U</li><li>◆ 438 (W) x 87.5 (H) x 815(D) mm</li></ul>
 CPU	<p>Intel® Xeon® 6 Processors</p> <ul style="list-style-type: none"><li>◆ Intel® Xeon® 6700-Series Processors</li><li>◆ Intel® Xeon® 6500-Series Processors</li></ul> <p>◆ Dual processor, TDP up to 350W</p> <p>NOTE: If only 1 CPU is installed, some PCIe or memory functions might be unavailable.</p>
 Socket	<ul style="list-style-type: none"><li>◆ 2 x LGA 4710</li><li>◆ Socket E2</li></ul>
 Chipset	<ul style="list-style-type: none"><li>◆ System on Chip</li></ul>
 Memory	<ul style="list-style-type: none"><li>◆ 32 x DIMM slots</li><li>◆ Support DDR5 RDIMM/MRDIMM <sup>[1]</sup></li><li>◆ 8-Channel memory per processor</li><li>◆ RDIMM: Up to 6400 MT/s (1DPC), 5200 MT/s (2DPC)</li><li>◆ MRDIMM: Up to 8000 MT/s</li></ul> <p><b>[1] MRDIMMs are supported only on select Intel® Xeon® 6 processors with P-cores and only in a 1DPC configuration.</b></p>
 LAN	<p><b>Rear (I/O board - CDCR010):</b></p> <ul style="list-style-type: none"><li>◆ 2 x 1Gb/s LAN ports (1 x Intel® I350-AM2)</li><li>◆ Support NCSI function</li><li>◆ 1 x 10/100/1000 Mbps Management LAN</li></ul>
 Video	<ul style="list-style-type: none"><li>◆ Integrated in Aspeed® AST2600</li><li>◆ 1 x Mini-DP</li></ul>



## Storage

### Front side:

- ◆ 24 x 2.5" Gen5 NVMe/**SATA/SAS-4** [1]
- ◆ 12 x NVMe from CPU\_0, 12 x NVMe from CPU\_1

### Rear hot-swap:

- ◆ 2 x 2.5" SATA/**SAS-4** [2]
- ◆ (SATA from CPU\_0, **through I/O board**)

### Internal M.2:

- ◆ 2 x M.2 (2280/22110), PCIe Gen5 x4, from CPU\_1

### Internal M.2 (I/O board - CDCR010):

- ◆ 1 x M.2 (2280), PCIe Gen5 x2, from CPU\_0, **occupied for SATA**

[1] Storage card is required to support SATA and SAS drives.

[2] SAS card is required to support SAS drives..



## SAS

- ◆ Require SAS add-in cards



## RAID

- ◆ Require RAID add-in cards
- ◆ Onboard VROC key header



## Expansion Slot

### PCIe Cable x 2:

- ◆ 1 x FHHL x16 (**Gen5 x16**), from CPU\_0 (Dual-slot)
- ◆ 1 x FHHL x16 (**Gen5 x16**), from CPU\_1 (Dual-slot)

### Riser Card CRS101K:

- ◆ 1 x FHHL x16 (Gen5 x16), from CPU\_1 (Single-slot)

1 x OCP NIC 3.0 (Gen5 x16), from CPU\_0






Supports NCSI function

1 x OCP NIC 3.0 (Gen5 x16), from CPU\_1, **disabled for NVMe**



## Front I/O

- ◆ 2 x USB 3.2 Gen1 ports (Type-A)
- ◆ 1 x Power button with LED
- ◆ 1 x ID button with LED
- ◆ 1 x NMI button
- ◆ 1 x Reset button
- ◆ 2 x LAN activity LEDs
- ◆ 1 x Storage activity LED
- ◆ 1 x System status LED

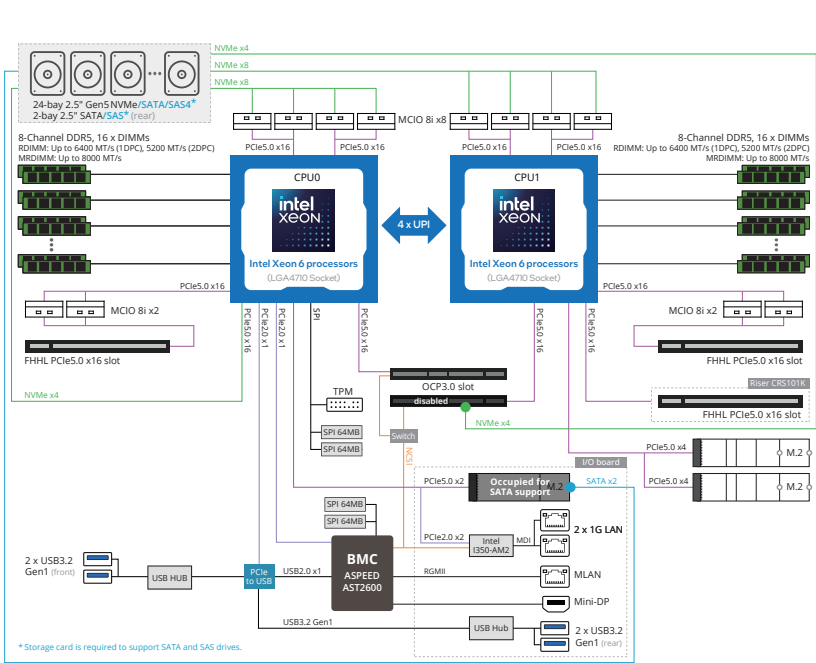
	Rear I/O	<p><b>I/O board - CDCR010:</b></p> <ul style="list-style-type: none"> <li>◆ 2 x USB 3.2 Gen1 ports (Type-A)</li> <li>◆ 1 x Mini-DP</li> <li>◆ 2 x RJ45 ports</li> <li>◆ 1 x MLAN port</li> <li>◆ 1 x ID LED</li> </ul>
	Backplane Board	<ul style="list-style-type: none"> <li>◆ Speed and bandwidth:</li> <li>◆ <b>Front side - CBP2081:</b> PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s</li> <li>◆ <b>Front side - CBP20G0:</b> PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s</li> <li>◆ <b>Rear side - CBP2025:</b> SATA 6Gb/s or SAS-4 24Gb/s</li> </ul>
	Security Modules	<ul style="list-style-type: none"> <li>◆ 1 x TPM header with SPI interface</li> <li>◆ <b>Optional</b> TPM2.0 kit: CTM012</li> <li>◆ 1 x PRoT connector (<b>only enabled on RoT SKU</b>)</li> </ul>
	Power Supply	<ul style="list-style-type: none"> <li>◆ 1+1 2000W 80 PLUS Titanium redundant power supplies</li> </ul> <p>[Note] GIGABYTE provides PSUs with various energy efficiency ratings and power outputs. Please contact our sales representatives to determine the best configuration for your system.</p> <p>[Note] Please refer to GIGABYTE Website for detail power supply specification.</p>
	System Management	<ul style="list-style-type: none"> <li>◆ Aspeed® AST2600 Baseboard Management Controller</li> <li>◆ GIGABYTE Management Console web interface</li> <li>◆ Dashboard</li> <li>◆ HTML5 KVM</li> <li>◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)</li> <li>◆ Sensor Reading History Data</li> <li>◆ FRU Information</li> <li>◆ SEL Log in Linear Storage / Circular Storage Policy</li> <li>◆ Hardware Inventory</li> <li>◆ Fan Profile</li> <li>◆ System Firewall</li> <li>◆ Power Consumption</li> <li>◆ Power Control</li> <li>◆ Advanced power capping</li> <li>◆ LDAP / AD / RADIUS Support</li> <li>◆ Backup &amp; Restore Configuration</li> <li>◆ Remote BIOS/BMC/CPLD Update</li> <li>◆ Event Log Filter</li> <li>◆ User Management</li> <li>◆ Media Redirection Settings</li> <li>◆ PAM Order Settings</li> <li>◆ SSL Settings</li> <li>◆ SMTP Settings</li> </ul>



Operating  
Properties

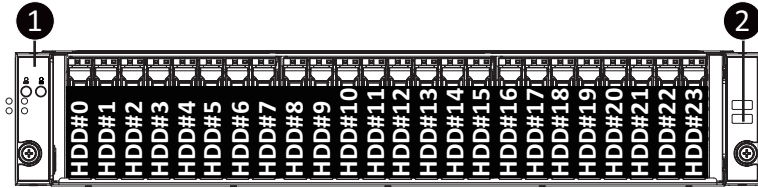
- ◆ Operating temperature: 10°C to 35°C
- ◆ Operating humidity: 8%-80% (non-condensing)
- ◆ Non-operating temperature: -40°C to 60°C
- ◆ Non-operating humidity: 20%-95% (non-condensing)

# 1-3 System Block Diagram



# Chapter 2 System Appearance

## 2-1 Front View

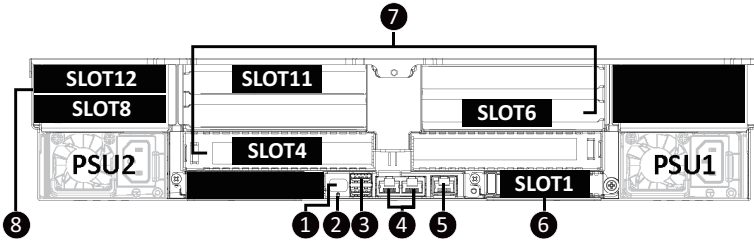


No.	Description
1.	Front Panel LEDs and Buttons
2.	USB 3.2 Gen1 Port x 2



- Refer to section **2-3 Front Panel LEDs and Buttons** for a detailed description of the function of the LEDs.

## 2-2 Rear View

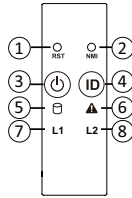


No.	Description	No.	Description
1.	Mini DisplayPort	5.	Server Management LAN Port
2.	ID LED	6.	OCP 3.0 Slot (Option/SFF)
3.	USB 3.2 Gen1 Port x 2	7.	PCIe Slot
4.	1GbE LAN Port x 2	8.	2.5" Hard Drive Bay



- Refer to section **2-5 Rear System LAN LEDs** for a detailed description of the function of the LEDs.

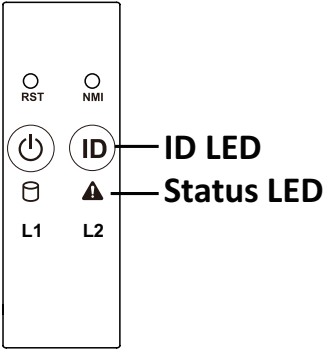
## 2-3 Front Panel LEDs and Buttons



No.	Name	Color	Status	Description
1.	Reset Button	--	--	Press this button to reset the system.
2.	NMI button	--	--	Press this button for the server to generate a NMI to the processor. If multiple-bit ECC errors occur, the server will effectively be halted.
3.	Power button with LED	Green	On	Indicates the system is powered on.
		N/A	Off	System is not powered on or in ACPI S5 state (power off)
4.	ID Button with LED <sup>(Note)</sup>	Blue	On	System identification is active.
		N/A	Off	System identification is disabled.
5.	HDD Status LED	Green	On	Indicates locating the HDD.
			Blink	Indicates accessing the HDD.
		Amber	On	Indicates HDD error.
		Green/ Amber	Blink	Indicates HDD rebuilding.
		N/A	Off	Indicates no HDD access or no HDD error.
6.	System Status LED <sup>(Note)</sup>	Green	Solid On	System is operating normally.
			Solid On	Critical condition, may indicate: System fan failure System temperature
		Amber	Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion
			N/A	Off
7/8.	LAN1/2 Active/Link LED	Green	On	Indicates a link between the system and the network or no access.
		Green	Blink	Indicates data transmission or receiving is occurring.
		N/A	Off	Indicates no data transmission or receiving is occurring.

(Note) If your server features RoT function, please see the following section for detail LED behavior.

## 2-4 RoT LEDs



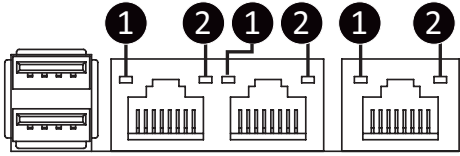
State	LED on Front Panel		LED on PRoT Module
	ID LED	Status LED	Live LED
<b>AST1060 FW Active Authentication fail</b>			
<b>AST1060:</b> Recovering active region	4Hz	Green and Amber Blink alternately at 4Hz [Green, Amber, Green, Amber, and so on]	4Hz
<b>AST1060 FW Active and Recovery Authentication fail</b>			
Endless attempts to boot from active or recovery.	On	Off	Off
<b>Authenticating BMC/BIOS Images</b>			
Authenticating Images	Off	Off	2Hz
<b>BMC/BIOS Images Authentication Pass</b>			
<b>BMC :</b> Authentication pass <b>BIOS :</b> Authentication pass	Off	Off	0.5Hz

State	LED on Front Panel		LED on PRoT Module
	ID LED	Status LED	Live LED
<b>Recovering BMC/BIOS Images</b>			
<b>BMC :</b> Recovering active region	4Hz	Green Blink at 4Hz	4Hz
<b>BIOS :</b> Recovering active region	4Hz	Amber Blink at 4Hz	4Hz
<b>BMC :</b> Recovering recovery region (If the staging region exists)	4Hz	Green On	4Hz
<b>BIOS :</b> Recovering recovery region (If the staging region exists)	4Hz	Amber On	4Hz
<b>BMC/BIOS Images Active and Recovery region Authentication Fail</b>			
<b>BMC :</b> Active and Recovery authentication fail	On	Green On	2Hz
<b>BIOS :</b> Active and Recovery authentication fail	On	Amber On	2Hz

**NOTE!**

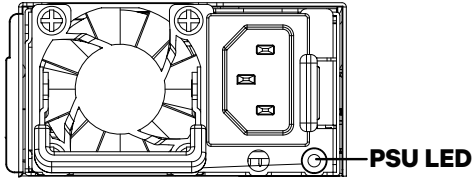
1. When the BMC/BIOS starts, the LEDs will be controlled by the BMC/BIOS.

## 2-5 Rear System LAN LEDs



No.	Name	Color	Status	Description
1.	1GbE Speed LED	Yellow	On	1 Gbps data rate
		Green	On	100 Mbps data rate
		N/A	Off	10 Mbps data rate
2.	1GbE Link / Activity LED	Green	On	Link between system and network or no access
		Green	Blink	Data transmission or reception is occurring.
		N/A	Off	No data transmission or reception is occurring.

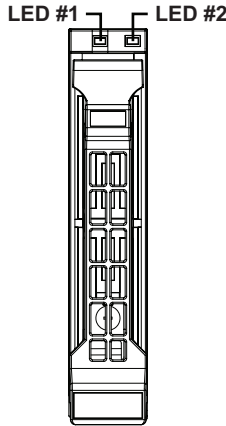
## 2-6 Power Supply Unit LED



State	Description
Off	No AC power to all power supplies
1Hz Green Blinking	AC present / only standby on / Cold redundant mode
2Hz Green Blinking	Power supply firmware updating mode
Amber	AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power
	Power supply critical event causing shut down: failure, OCP, OVP, fan failure and UVP
1Hz Amber Blinking	Power supply warning events where the power supply continues to operate: high temp, high power, high current and slow fan

## 2-7 Hard Disk Drive LEDs

### 2.5" HDD



RAID SKU		LED #1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA)	Disk LED (LED on Back Panel)	Green	ON(*1)	OFF		BLINK (*2)	OFF
		Amber	OFF	OFF		OFF	OFF
	Removed HDD Slot (LED on Back Panel)	Green	ON(*1)	OFF		--	--
		Amber	OFF	OFF		--	--
RAID configuration (via HW RAID Card or SW RAID Card)	Disk LED	Green	ON	OFF		BLINK (*2)	OFF
		Amber	OFF	ON	(Low Speed: 2 Hz)	OFF	OFF
	Removed HDD Slot	Green	ON(*1)	OFF	(*3)	--	--
		Amber	OFF	ON	(*3)	--	--

LED #2	HDD Present	No HDD
Green	ON	OFF

**NOTE:**

\*1: Depends on HBA/Utility Spec.

\*2: Blink cycle depends on HDD's activity signal.

\*3: If HDD is pulled out during rebuilding, the disk status of this HDD is regarded as faulty.

## Chapter 3 System Hardware Installation



### Pre-installation Instructions

Computer components and electronic circuit boards can be damaged by discharges of static electricity. Working on computers that are still connected to a power supply can be extremely dangerous. Follow the simple guidelines below to avoid damage to your computer or injury to yourself.

- Always disconnect the computer from the power outlet whenever you are working inside the computer case.
- If possible, wear a grounded wrist strap when you are working inside the computer case. Alternatively, discharge any static electricity by touching the bare metal system of the computer case, or the bare metal body of any other grounded appliance.
- Hold electronic circuit boards by the edges only. Do not touch the components on the board unless it is necessary to do so. Do not flex or stress the circuit board.
- Leave all components inside the static-proof packaging until you are ready to use the component for the installation.

### 3-1 Removing and Installing the Chassis Cover

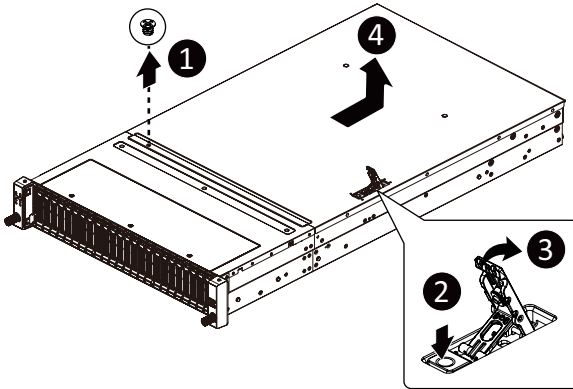


Before you remove or install the system cover

- Make sure the system is not turned on or connected to AC power.

**Follow these instructions to remove the chassis cover:**

1. Remove the screw securing the chassis cover.
2. Unlock the plastic handle and pull the grip handle to open the panel cover.
3. Slide the cover cover to the rear of the system and then remove the cover in the direction indicated by the arrow.
4. To reinstall the chassis cover follow steps 1-4 in reverse order.



## 3-2 Removing and Installing the Hard Disk Drive

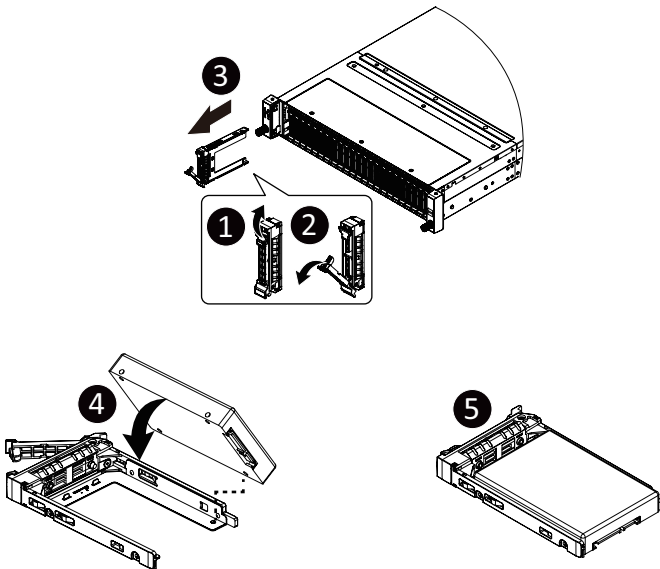


Read the following guidelines before you begin to install the hard disk drive:

- Take note of the HDD tray orientation before sliding it out.
- The tray will not fit back into the bay if it is inserted incorrectly.
- Make sure that the hard disk drive is connected to the connector on the backplane.

**Follow these instructions to install a 2.5" hard disk drive:**

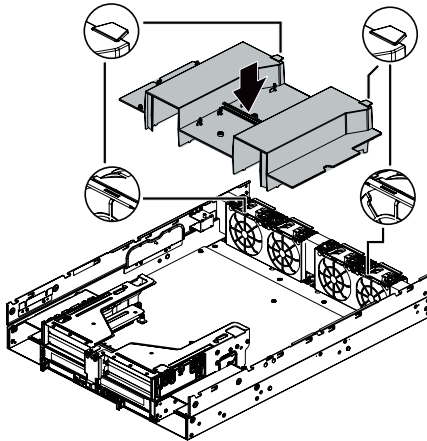
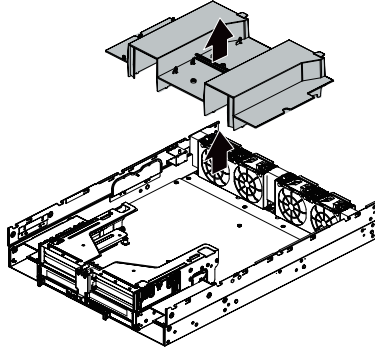
1. Press the release button.
2. Extend the locking lever.
3. Pull the locking lever in the direction indicated to remove the HDD tray.
4. Align the hard disk drive with the positioning stud on the HDD tray.
5. Slide the hard disk drive into the HDD tray.
6. Reinsert the HDD tray into the slot and close the locking lever.



### 3-3 Removing and Installing the Fan Duct

Follow these instructions to remove the fan duct:

1. Lift up to remove the fan duct.
2. To reinstall the fan duct, align the fan duct with the guiding groove. Push down the fan duct until it is firmly seated on the system.



## 3-4 Removing and Installing the Heat Sink



Read the following guidelines before you begin to install the heat sink:

- Always turn off the computer and unplug the power cord from the power outlet before installing the heat sink to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open the system according to the instructions.

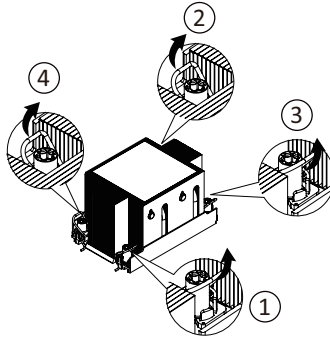


### **WARNING!**

Failure to turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

**Follow these instructions to install the heat sink:**

1. Loosen the screws securing the heat sink in place in reverse order (4→3→2→1).
2. Lift and remove the heat sink from the system.
3. To install the heat sink, reverse steps 1-2 while ensuring that you tighten the captive screws in sequential order (1→2→3→4) as seen in the image below.



## 3-5 Installing the CPU and Heat Sink



Read the following guidelines before you begin to install the CPU:

- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open the system according to the instructions.

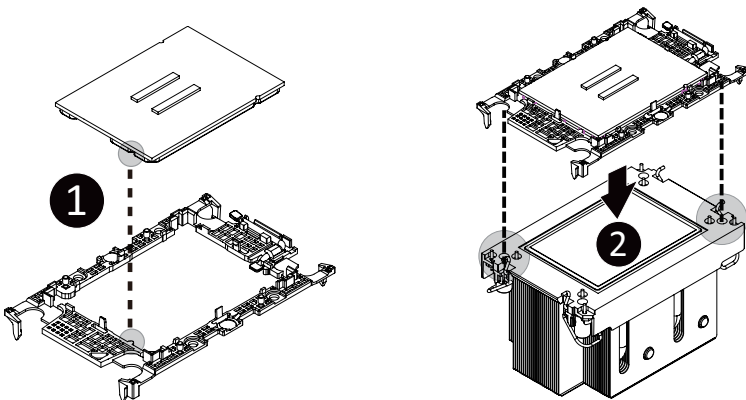


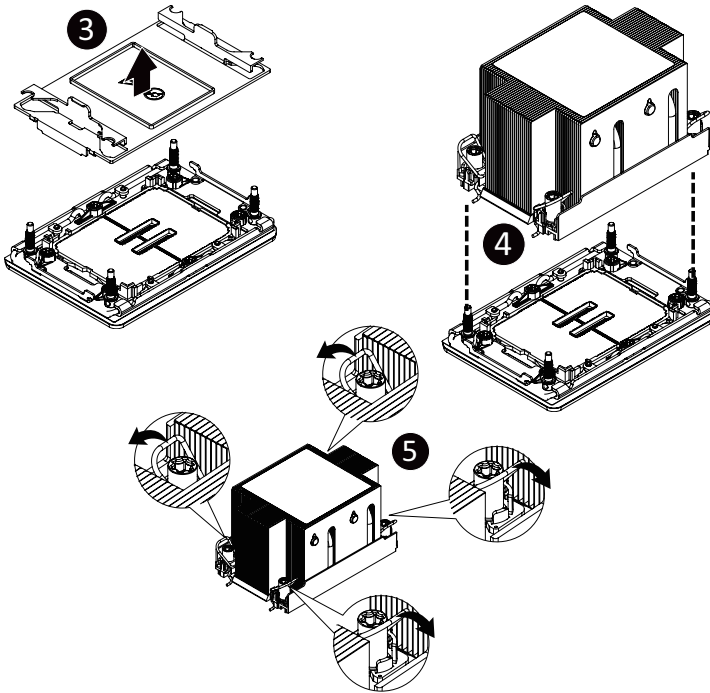
### **WARNING!**

Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

### **Follow these instructions to install the CPU:**

1. Align the processor to the carrier so that the gold triangle on the processor aligns with the triangle on the carrier, and then install the processor into the carrier.  
NOTE: Apply thermal compound evenly on the top of the CPU.
2. Carefully flip the heatsink over. Align the carrier assembly so that the triangle on the carrier aligns with the triangle on the heatsink, and then install the carrier assembly onto the bottom of the heatsink.
3. Remove the CPU socket cover.  
NOTE: Save and replace the CPU socket cover if the processor is removed from its socket.
4. Align the heatsink to the CPU socket using the guide pins and make sure the gold triangle is in the correct orientation. Then place the heatsink onto the top of the CPU socket.
5. Secure the heatsink by tightening the screws in sequential order (1→2→3→4).  
NOTE: When removing the heatsink, loosen the screws in reverse order (4→3→2→1).





### Carrier Types used for Package Types

<b>Package Type</b>	<b>Intel Xeon 6700P-series processors XCC</b>	<b>Intel Xeon 6500P/6700P-series processors HCC, LCC</b> <b>Intel Xeon 6700E-series processors HDCC</b>
<b>Carrier Code</b>	E2A	E2B

#### NOTE!

- The carrier code is marked on each carrier and matches a code laser marked on to the IHS(Integrated Heat Spreader) to ensure the right parts are used together.
- When installing the heatsink to CPU,use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4.
- The screw tightening torque:  $8 \pm 0.5$  kgf-cm.

## 3-6 Removing and Installing Memory

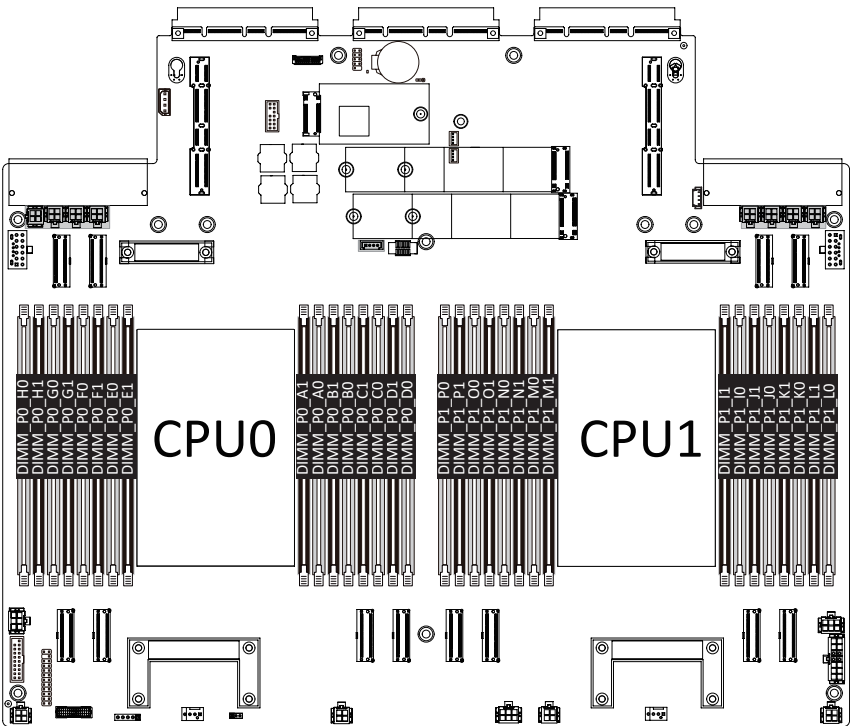


Read the following guidelines before you begin to install the memory:

- Make sure that the motherboard supports the memory. It is recommended that memory of the same capacity, brand, speed, and chips be used.
- Always turn off the computer and unplug the power cord from the power outlet before installing the memory to prevent hardware damage.
- Memory modules have a foolproof design. A memory module can be installed in only one direction. If you are unable to insert the memory, switch the direction.

### 3-6-1 Eight Channel Memory Configuration

This motherboard provides 32 DDR5 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



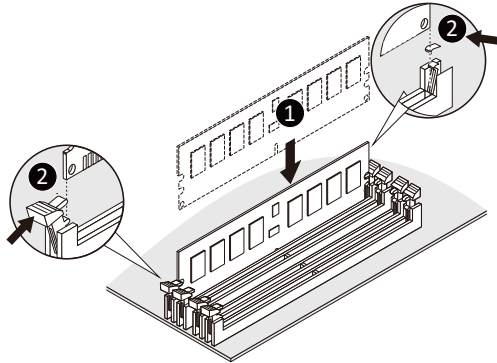
### 3-6-2 Removing and Installing a Memory Module



Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module. Be sure to install DDR5 DIMMs on to this motherboard.

**Follow these instructions to install a DIMM module:**

1. Insert the DIMM memory module vertically into the DIMM slot and push it down.
2. Close the plastic clip at both edges of the DIMM slots to lock the DIMM module.
3. Reverse the installation steps when you want to remove the DIMM module.



### 3-6-3 DIMM Population Table

#### Intel Xeon 6700E-Series Memory Support

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)						Channel Speed (MT/s); Voltage (V); Slots per Channel (SPC) & DIMMs per Channel (DPC)	
		DRAM Density						1DPC/2SPC	2DPC/2SPC
		16Gb		24Gb		32Gb			
		1DPC	2DPC	1DPC	2DPC	1DPC	2DPC	1.1V	
RDIMM	1Rx4	32GB						6400, 6000,	NA
	2Rx8	32GB						5600, 5200, 4800	NA
	2Rx4	64GB	64GB	96GB	96GB			(DDR5-6400 rated RDIMMS only)	5200, 4800
	2Rx4					128GB	128GB		(DDR5-6400 rated RDIMMS only) NA

#### Intel Xeon 6700E-Series CXL Memory Support

Native DDR5 Memory Per Socket				CXL Memory Per Socket				
Slot0 DIMM Ranks	Slot0 DIMM Capacity (GB)	DIMM Type	DRAM Density (Gb)	CXL Memory Channels	CXL Memory Type	CXL Capacity Per Device/Module	CXL Interleave	CXL Mode
2Rx4	64	10x4	16	2+2	DDR5 x8	64 GB	1x4*, 2x2, 4x1	1LM+Vol
2Rx4	64	10x4	16	1+1	DDR5 x16	128 GB	1x2*, 2x1	1LM+Vol
1Rx4	32	10x4	16	2	DDR5 x8	128 GB	1x2*	Intel® Flat Memory Mode

**NOTE:**

\* Default setting in BIOS

## Intel Xeon 6500P/6700P-Series Memory Support

Type	Ranks Per DIMM and	DIMM Capacity (GB)						Channel Speed (MT/s); Voltage (V); Slots per Channel (SPC) & DIMMs per Channel Density (DPC)	
		DRAM Density						1.1V	
	Data Width	16Gb		24Gb		32Gb			
		1DPC	2DPC	1DPC	2DPC	1DPC	2DPC		
RDIMM	1Rx8	16GB		24GB				6400, 6000,	5200, 4800 (DDR5-6400 rated RDIMMS only)
	1Rx4	32GB		48GB				5600, 5200, 4800	
	2Rx8	32GB	32GB	48GB				(DDR5-6400 rated RDIMMS only)	
	2Rx4	64GB*	64GB^A	96GB*	96GB^A	128GB*	128GB^A		
RDIMM 3DS	8Rx4		256GB*						
MRDIMM	2Rx8	32GB						8000, 7200	N/A (no 2DPC configs for MRDIMM)
	2Rx4	64GB						(MRDIMM-8800 only)	

### NOTE:

- \*Supported in 1S/2S/4S systems
- ^Supported in 8S systems

## Intel Xeon 6500P/6700P-Series CXL Memory Support

Native DDR5 Memory Per Socket				CXL Memory Per Socket					
Slot0 DIMM Ranks	Slot0 DIMM Capacity (GB)	DIMM Type	DRAM Density (Gb)	CXL Memory Channels	CXL Memory Type	CXL Capacity Per Device/Module	CXL Interleave	CXL Mode	4S & 8S Support
2Rx4	96	10x4	24	2+2	DDR5 x8	96 GB#	1x4*, 2x2, 4x1	1LM+Vol	Yes
2Rx4	128	10x4	32	2+2	DDR4x8# DDR5 x8	128 GB	1x4*, 2x2, 4x1	1LM+Vol	Yes
2Rx4	128	10x4	32	2+2	DDR4x8 DDR5 x8	128 GB	hetero x12	Hetero	Yes
2Rx4	64	10x4	16	2+2+2	DDR4x8 DDR5 x8	128 GB	1x6*, 2x3, 3x2	1LM+Vol	No
2Rx4	64	10x4	16	2	DDR4x8 DDR5 x8	128 GB	1x2*	1LM+Vol	No
2Rx4	64	10x4	16	1+1	DDR5 x16	2ch 128 GB	1x2*	Intel® Flat Memory Mode	Yes
2Rx4	64	10x4	16	2+2+2	DDR4 x8 DDR5 x8	256GB	1x8,8x1 4x2, 2x4	1LM+Vol	No

### NOTE:

- Intel Xeon 6500P/6700P-series processor CXL memory configurations are 1DPC (Slot0) only for native DDR5.
- CXL Memory Channel notation: # of devices per root port, with root ports separated by "+". i.e. 2+2+2+2= four root ports populated with two devices per root port.
- CXL Interleave notation: sets x ways. i.e. 2x4 = Set of two modules, interleaved four-way
- \* Default setting in BIOS
- \* Native DIMM speeds up to 6400 MT/s
- \* Trending to post PRQ enablement



## 3-7 Removing and Installing the PCIe Card



- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered off and all power sources have been disconnected from the server prior to installing a PCIe card.
- Failure to observe these warnings could result in personal injury or damage to equipment.



- The PCIe riser assembly does not include a riser card or any cabling as standard. To install a PCIe card, a riser card must be installed.

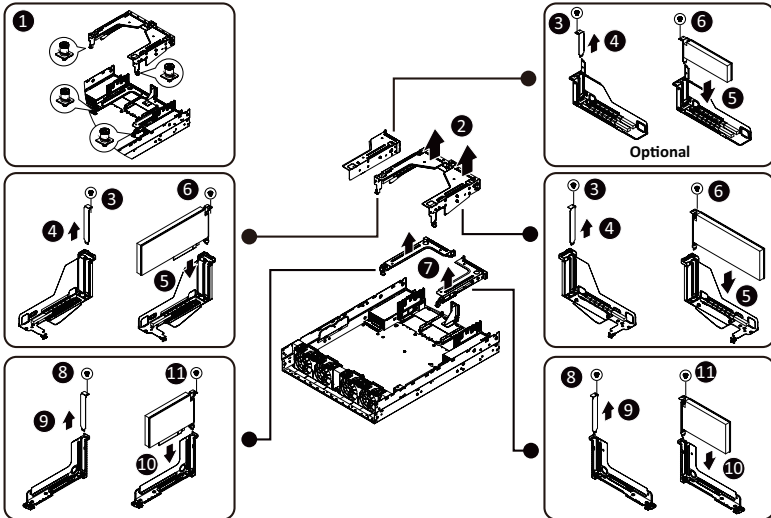
### Follow these instructions to install a PCIe card:

1. Loosen the two thumbnail screws securing the riser bracket inside the system.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the slot cover from riser bracket.
4. Orient the PCIe card with the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCIe card connector.

**NOTE:** Some riser brackets allow for single or multiple PCIe cards.

Repeat steps 3-4 as necessary.

5. Secure the PCIe card with the screw.
6. Repeat steps 1-2 to install the PCIe card into the system.



## 3-8 Installing the Mezzanine Card

### 3-8-1 Installing the OCP 3.0 Mezzanine Card

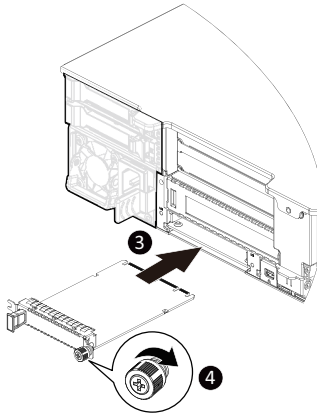
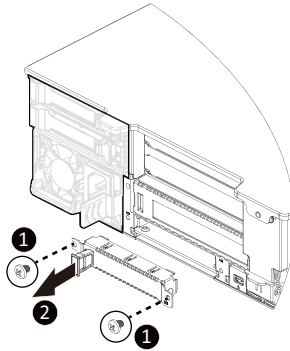


Use of the following type of OCP 3.0 NIC is recommended:

- OCP 3.0 SFF with pull tab
- OCP 3.0 SFF with ejector latch

**Follow these instructions to install an OCP 3.0 Mezzanine card:**

1. Remove the two screws securing the OCP 3.0 card slot cover.
2. Remove the slot cover from the system.
3. Insert the OCP 3.0 card into the card slot ensuring that the card is firmly connected to the connector on the motherboard.
4. Tighten the thumbnail screw to secure the OCP 3.0 card in place.
5. Reverse steps 3-4 to replace the OCP 3.0 card.



### 3-9 Replacing the Fan Assembly

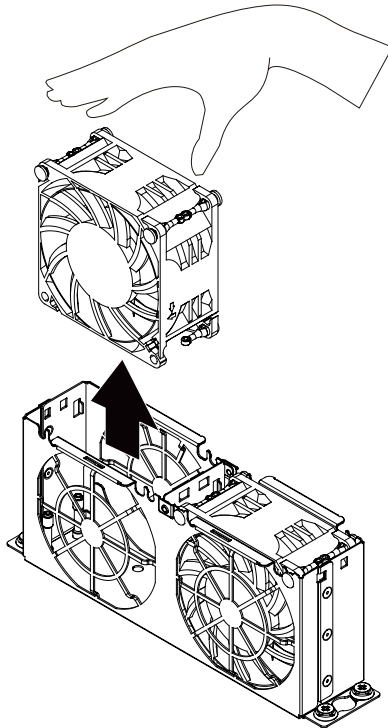


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

Failure to observe these warnings could result in personal injury or damage to equipment.

#### Follow these instructions to replace a fan assembly:

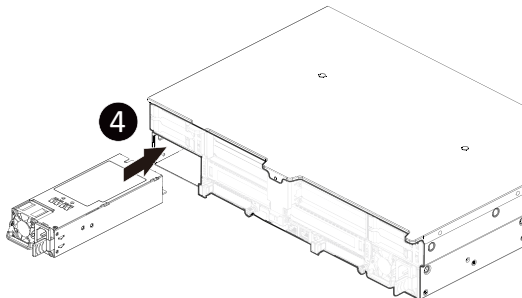
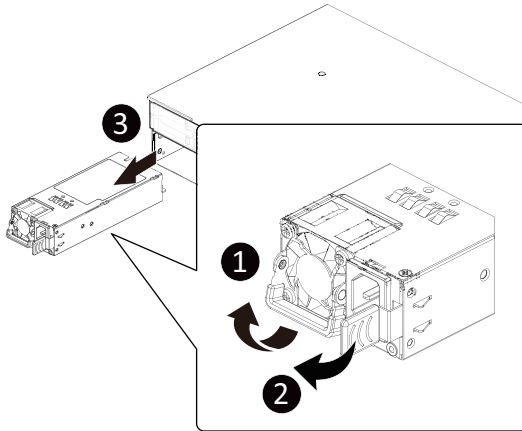
1. Using the latches, lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



## 3-10 Removing and Installing the Power Supply

Follow these instructions to replace the power supply:

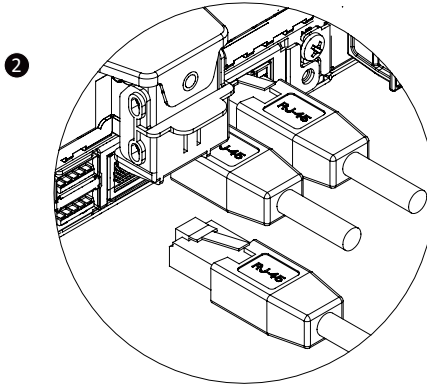
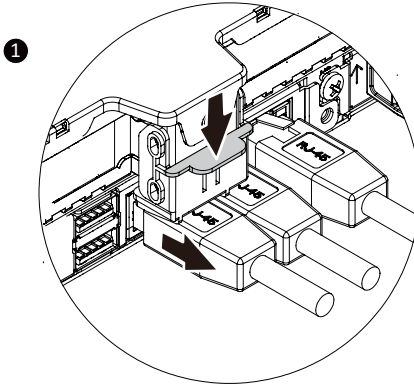
1. Flip up and then grasp the power supply handle.
2. Press the retaining clip on the right side of the power supply unit in the direction indicated.
3. Pull out the power supply unit using the handle.
4. Insert the replacement power supply unit firmly into the chassis. Connect the AC power cord to the replacement power supply.
5. Repeat steps 1-4 for replacement of the second power supply.



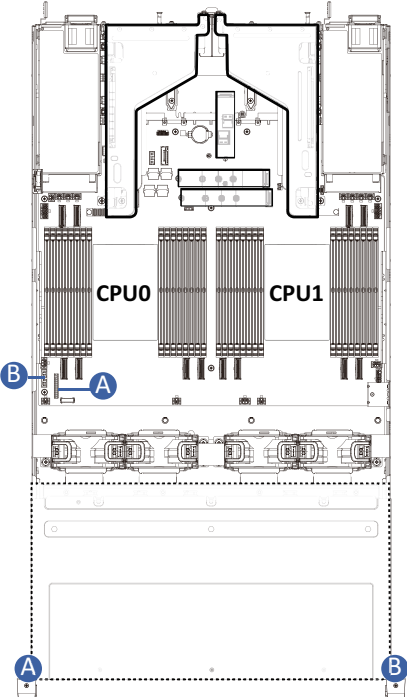
## 3-11 Removing the LAN Cable

Follow these instructions to remove the LAN cable:

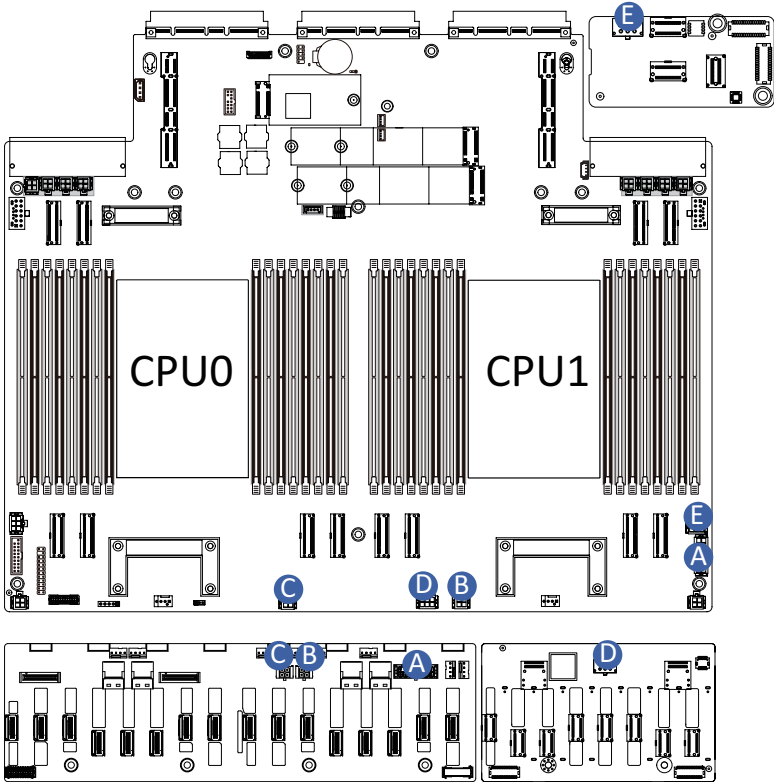
1. Press the release latch while simultaneously pulling out the LAN cable



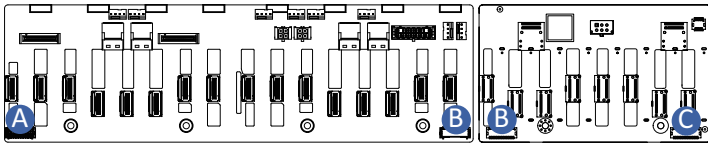
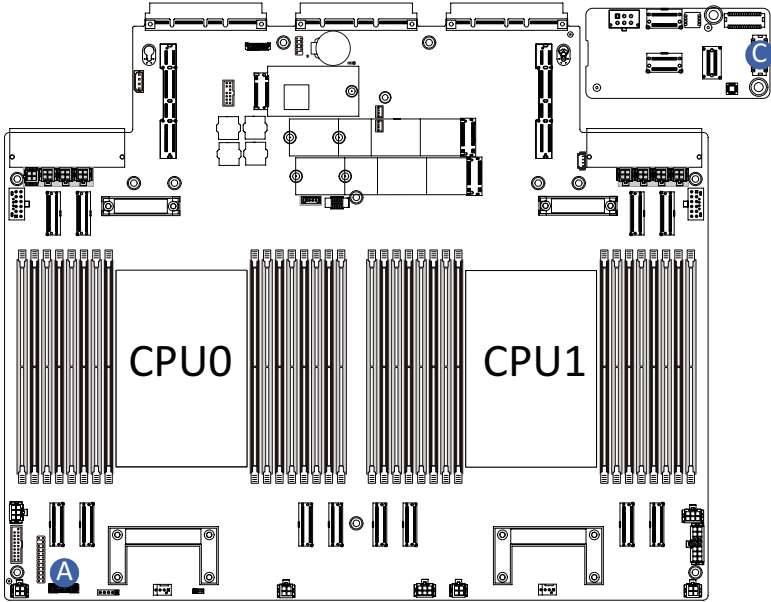
### 3-12 Cable Routing



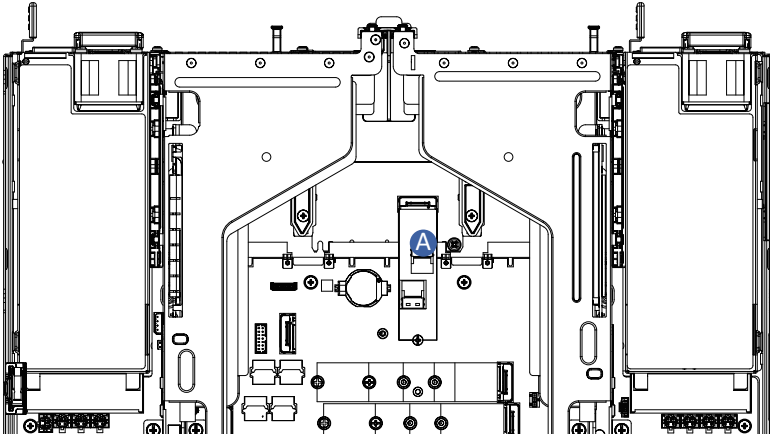
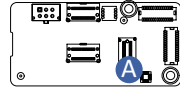
A	Front Panel LEDs and Buttons Cable	Motherboard: FP_1
		Front IO Board: FP_1
B	Front Panel USB 3 Ports Cable	Motherboard: FUSB_1
		--



A	HDD Backplane Board Power Cable	Motherboard: ATX1
		Front HDD Board: ATX1
B	HDD Backplane Board Power Cable	Motherboard: 12V_BP3
		Front HDD Board: 12V_IN2
C	HDD Backplane Board Power Cable	Motherboard: 12V_BP2
		Front HDD Board: 12V_IN1
D	HDD Backplane Board Power Cable	Motherboard: ATX3
		Front HDD Board: ATX1
E	HDD Backplane Board Power Cable	Motherboard: ATX2
		Rear HDD Board: BP_2X3

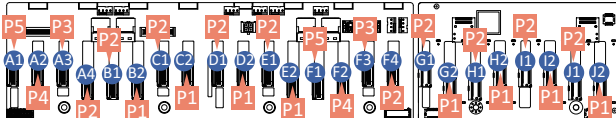
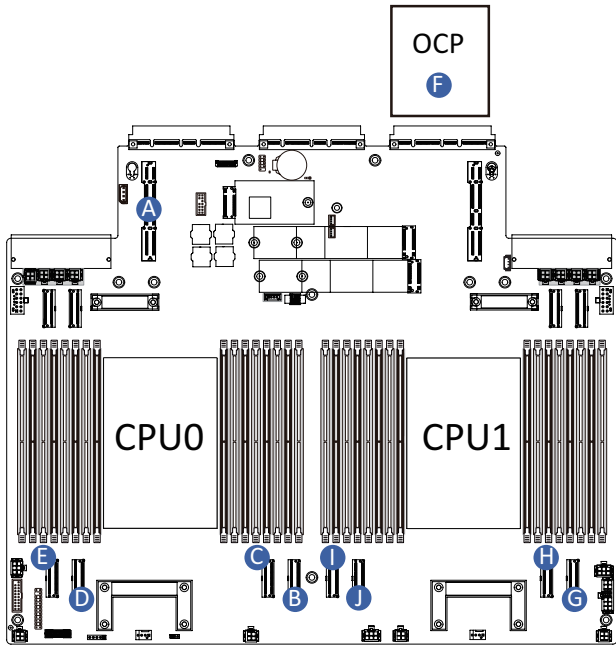


A	HDD Backplane Board Signal Cable	Motherboard: BP_1
		Front HDD Board: BP_1
B	HDD Backplane Board Signal Cable	Front HDD Board: BP_SERIES
		Motherboard: BP_1
C	HDD Backplane Board Signal Cable	Rear HDD Board: BP_1
		Front HDD Board: BP_SERIES

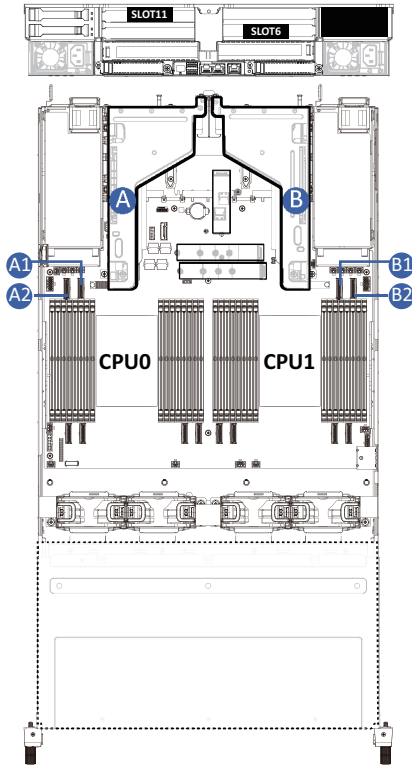


A	SATA Cable	M.2 type SATA card: SATA_RA4
		Rear HDD Board: SL_SAS0





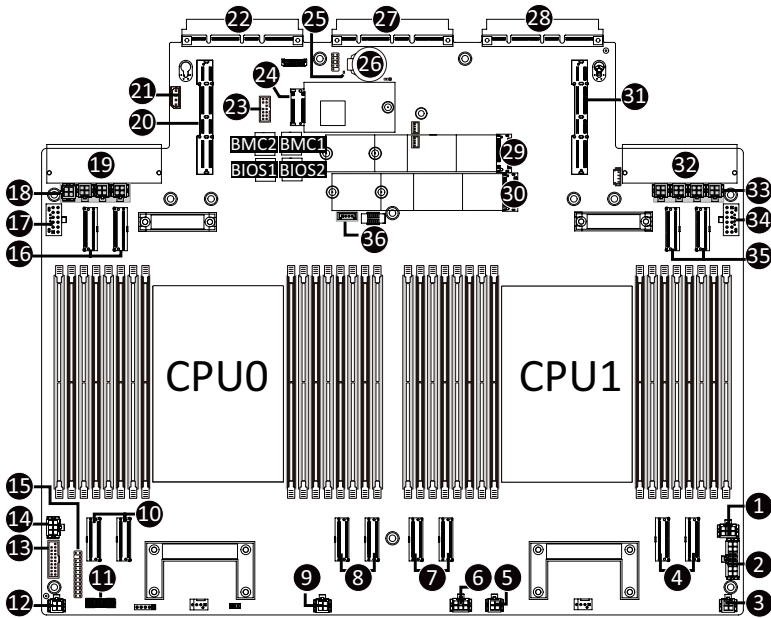
G	NVMe 16-17 Cable	Motherboard: U2_P1_4CA	I	NVMe 20-21 Cable	Motherboard: U2_P1_5CA
		Front HDD Board: G1: U.2_0 G2: U.2_1			Front HDD Board: G1: U.2_4 G2: U.2_5
H	NVMe 18-19 Cable	Motherboard: U2_P1_4GE	J	NVMe 22-23 Cable	Motherboard: U2_P1_5GE
		Front HDD Board: H1: U.2_2 H2: U.2_3			Front HDD Board: H1: U.2_6 H2: U.2_7



A	System Rear Side PCIe Cable	PCIe Riser Bracket: Slot 6
		Motherboard: A1: U2_P0_3AC A2: U2_P0_3EG
B	System Rear Side PCIe Cable	PCIe Riser Bracket: Slot 11
		Motherboard: B1: U2_P1_2AC B2: U2_P1_2EG

# Chapter 4 Motherboard Components

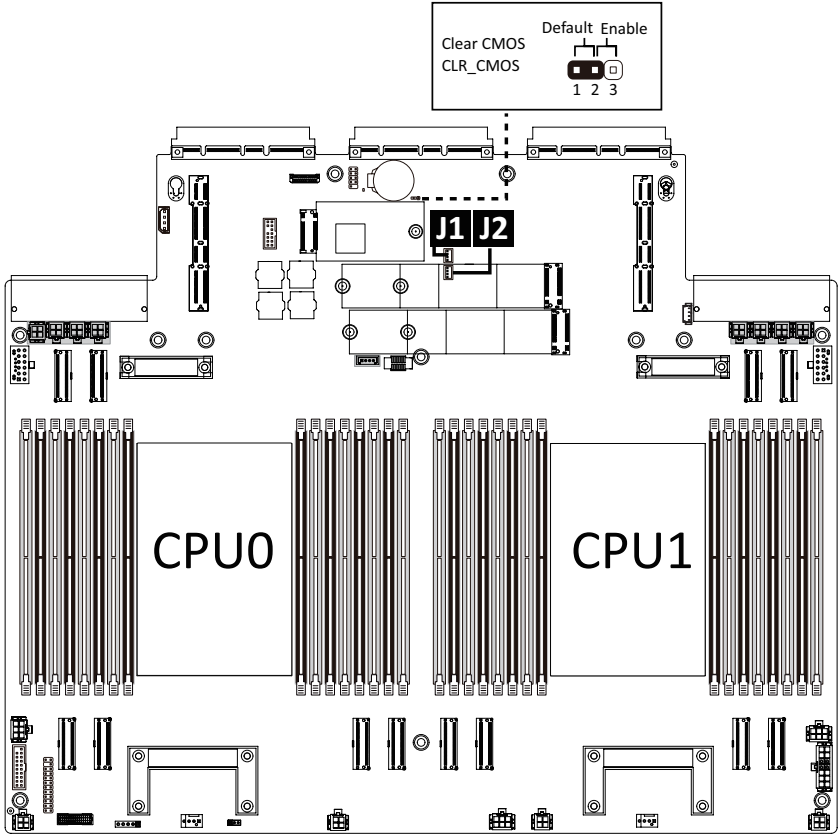
## 4-1 Motherboard Components



Item	Description
1	2 x 3 Pin ATX Power Connector (ATX2)
2	2 x 7 Pin ATX Power Connector (ATX1)
3	2 x 2 P12V Backplane Power Connector (P12V_BP4)
4	MCIO Connector (U2_P1_4GE/4CA/PCIe Gen5)
5	2 x 2 P12V Backplane Power Connector (P12V_BP3)
6	2 x 3 Pin ATX Power Connector (ATX3)
7	MCIO Connector (U2_P1_5GE/5CA/PCIe Gen5)
8	MCIO Connector (U2_P0_4GE/4CA/PCIe Gen5)
9	2 x 2 P12V Backplane Power Connector (P12V_BP2)
10	MCIO Connector (U2_P0_5GE/5CA/PCIe Gen5)
11	HDD Back Plane Board Connector
12	2 x 2 P12V Backplane Power Connector (P12V_BP1)
13	Front Panel USB 3.2 Gen1 Connector
14	2 x 3 Pin ATX Power Connector (ATX4)
15	Front Panel Connector
16	MCIO Connector (U2_P0_3AC/3EG/PCIe Gen5)
17	P12V GPU Power Connector (P12V_S6)
18	PCIe Power Connector (PCIE1/2/3/4_PWR)

Item	Description
19	Power Supply Connector#1 (Primary)
20	Riser Connector (GENZ1/PCIe Gen5)
21	IPMB Connector
22	OCP 3.0 Connector (OCP1/PCIe Gen5 x16)
23	TPM Module Connector (SPI Interface)
24	PRoT Module Connector (M.2 M-Key/only enabled on RoT SKU)
25	BMC Readiness LED
26	System Battery Socket
27	IO Card Connector
28	OCP 3.0 Connector (OCP2/PCIe Gen5 x16)
29	M.2 Slot (PCIe Gen5 x4, NGFF-22110/Supports heatsink)
30	M.2 Slot (PCIe Gen5 x4, NGFF-22110/Supports heatsink)
31	Riser Connector (GENZ2/PCIe Gen5)
32	Power Supply Connector#2 (Secondary)
33	PCIe Power Connector (PCIe5/6/7/8_PWR/for GENZ2)
34	P12V GPU Power Connector (P12V_S11)
35	MCIO Connector (U2_P1_2AC/2EG/PCIe Gen5)
36	VROC Module Connector

## 4-2 Jumper Settings

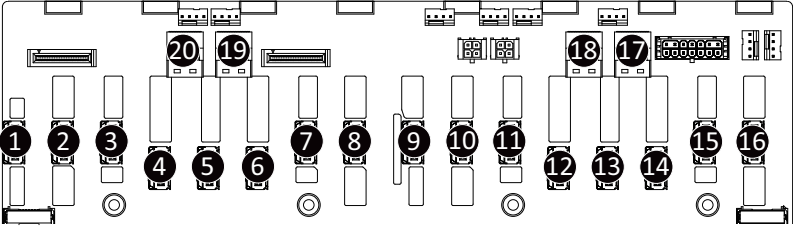


J1		ON	OFF
1	S3_MASK	Stop initial power on when BMC is not ready	Normal [Default]
2	BIOS_RCVR	BIOS recovery mode	Normal [Default]
3	BIOS_PWD	Clear supervisor password	Normal [Default]
4	RST BMC_EN	ID button to enable BMC reset	Normal [Default]

J2		
SW.1	SW.2	
ON	OFF	Slot#1 OCP3.0
ON	ON	Slot#2 OCP3.0
OFF	--	I/O Module

## 4-3 Backplane Board Storage Connector

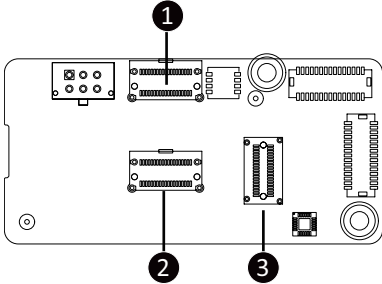
### 4-3-1 CBP20G0 (Front System Storage Board)



Item	Description
1.	MCIO 4i (SFF-TA1016/U.2_0)
2.	MCIO 4i (SFF-TA1016/U.2_1)
3.	MCIO 4i (SFF-TA1016/U.2_2)
4.	MCIO 4i (SFF-TA1016/U.2_3)
5.	MCIO 4i (SFF-TA1016/U.2_4)
6.	MCIO 4i (SFF-TA1016/U.2_5)
7.	MCIO 4i (SFF-TA1016/U.2_6)
8.	MCIO 4i (SFF-TA1016/U.2_7)
9.	MCIO 4i (SFF-TA1016/U.2_8)
10.	MCIO 4i (SFF-TA1016/U.2_9)
11.	MCIO 4i (SFF-TA1016/U.2_10)
12.	MCIO 4i (SFF-TA1016/U.2_11)
13.	MCIO 4i (SFF-TA1016/U.2_12)
14.	MCIO 4i (SFF-TA1016/U.2_13)
15.	MCIO 4i (SFF-TA1016/U.2_14)
16.	MCIO 4i (SFF-TA1016/U.2_15)
17.	SlimSAS Connector (SFF-8654/SL_SAS3)
18.	SlimSAS Connector (SFF-8654/SL_SAS2)
19.	SlimSAS Connector (SFF-8654/SL_SAS1)
20.	SlimSAS Connector (SFF-8654/SL_SAS0)



### 4-3-3 CBP2025 (Rear System Storage Board)



Item	Description
1	MCIO 4i (SFF-TA1016/U_2_0)
2	MCIO 4i (SFF-TA1016/U_2_1)
3	SlimSAS Connector (SFF-8654/SL_SAS0)

## Chapter 5 BIOS Setup

BIOS (Basic Input and Output System) records hardware parameters of the system in the EFI on the motherboard. Its major functions include conducting the Power-On Self-Test (POST) during system startup, saving system parameters, loading the operating system etc. The BIOS includes a BIOS Setup program that allows the user to modify basic system configuration settings or to activate certain system features. When the power is turned off, the battery on the motherboard supplies the necessary power to the CMOS to keep the configuration values in the CMOS.

To access the BIOS Setup program, press the <DEL> key during the POST when the power is turned on.



- BIOS flashing is potentially risky, if you do not encounter any problems when using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 1 for how to clear the CMOS values.)

### BIOS Setup Program Function Keys

<<-><->>	Move the selection bar to select the screen
<↑><↓>	Move the selection bar to select an item
<+>	Increase the numeric value or make changes
<->	Decrease the numeric value or make changes
<Enter>	Execute command or enter the submenu
<Esc>	Main Menu: Exit the BIOS Setup program Submenus: Exit current submenu
<F1>	Show descriptions of general help
<F3>	Restore the previous BIOS settings for the current submenus
<F9>	Load the Optimized BIOS default settings for the current submenus
<F10>	Save all the changes and exit the BIOS Setup program

■ **Main**

This setup page includes all the items of the standard compatible BIOS.

■ **Advanced**

This setup page includes all the items of AMI BIOS special enhanced features.

(ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)

■ **Chipset**

This setup page includes all the submenu options for configuring the functions of the Platform Controller Hub.

■ **Server Management**

Server additional features enabled/disabled setup menus.

■ **Security**

Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.

A supervisor password allows you to make changes in BIOS Setup.

A user password only allows you to view the BIOS settings but not to make changes.

■ **Boot**

This setup page provides items for configuration of the boot sequence.

■ **Save & Exit**

Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)

Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

# 5-1 The Main Menu

Once you enter the BIOS Setup program, the Main Menu (as shown below) appears on the screen. Use arrow keys to move among the items and press <Enter> to accept or enter other sub-menu.

## Main Menu Help

The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

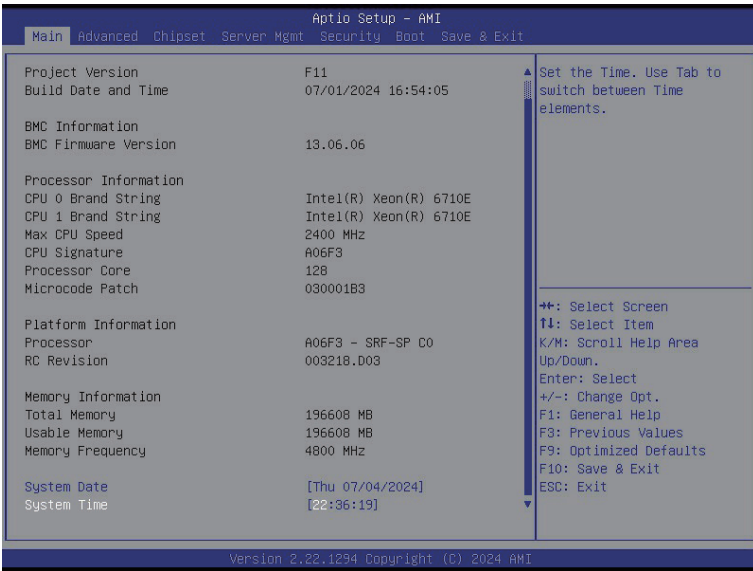
## Submenu Help

While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.



- When the system is not stable as usual, select the **Restore Defaults** item to set your system to its defaults.
- The BIOS Setup menus described in this chapter are for reference only and may differ by BIOS version.





Parameter	Description
Project Name	Displays the project name information.
Project Version	Displays version number of the BIOS setup utility.
Build Date and Time	Displays the date and time when the BIOS setup utility was created.
BMC Information	
BMC Firmware Version	Displays BMC firmware version information.
Processor Information	
CPU Brand String/ Max CPU Speed / CPU Signature / Processor Core / Microcode Patch	Displays the technical information for the installed processor(s).
Platform Information	
Processor/RC Revision	Displays the information of the installed processor(s).
Memory Information <sup>(Note2)</sup>	
Total Memory	Displays the total memory size of the installed memory.
Usable Memory	Displays the usable memory size of the installed memory.
Memory Frequency	Displays the installed memory frequency information.

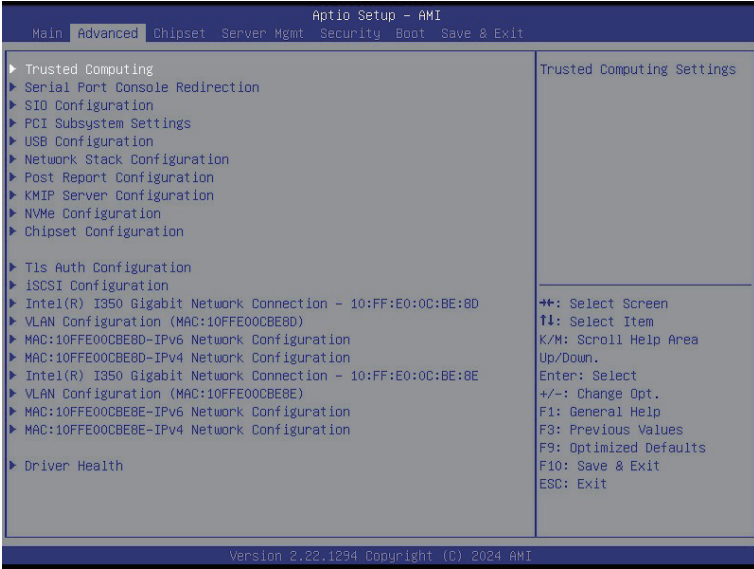
(Note1) Functions available on selected models.

(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

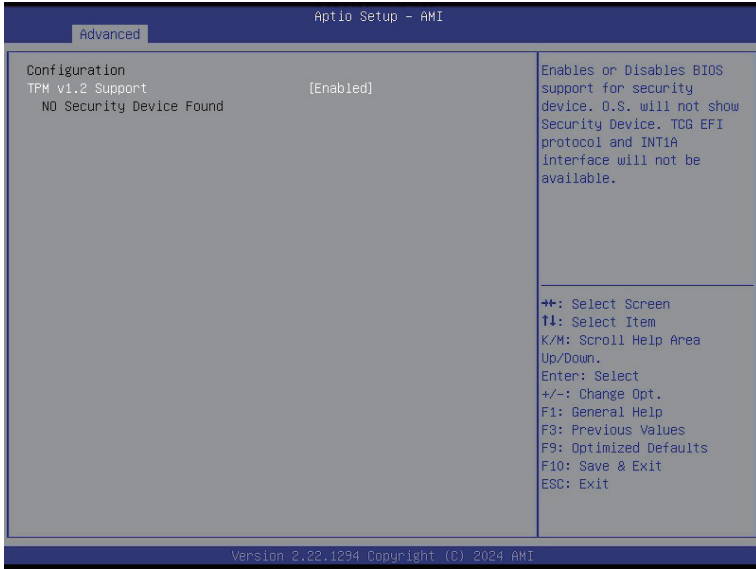
<b>Parameter</b>	<b>Description</b>
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

# 5-2 Advanced Menu

The Advanced Menu displays submenu options for configuring the function of various hardware components. Select a submenu item, then press <Enter> to access the related submenu screen.

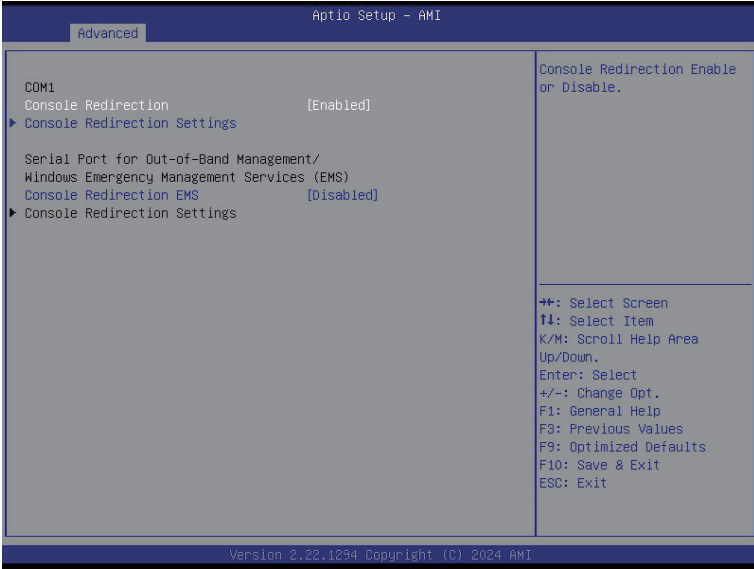


## 5-2-1 Trusted Computing



Parameter	Description
Configuration	
TPM v1.2 Support	<p>Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.</p> <p>Options available: Disable, Enable. Default setting is <b>Enable</b>.</p>

## 5-2-2 Serial Port Console Redirection



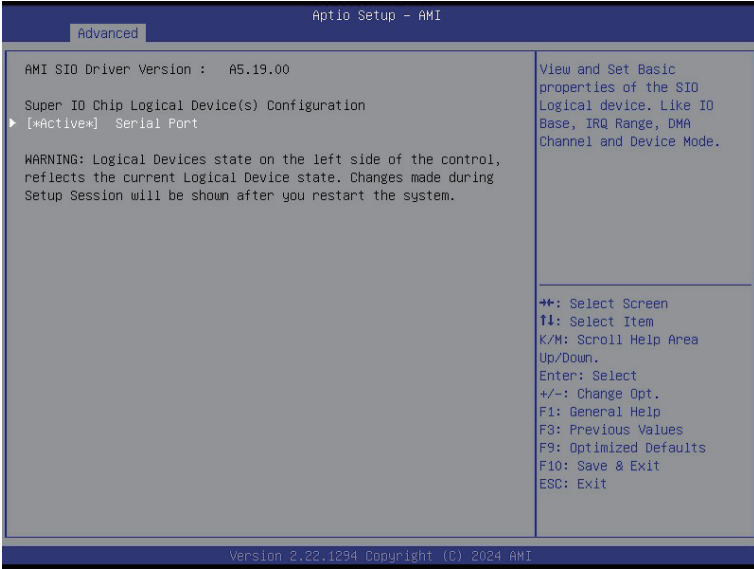
Parameter	Description
COM1 Console Redirection <sup>(Note)</sup>	<p>Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</p>
COM1 Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when COM1 Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Terminal Type <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is <b>VT100PLUS</b>.</li> </ul> </li> <li>◆ Bits per second <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 38400, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> <li>◆ Data Bits <ul style="list-style-type: none"> <li>– Selects the number of data bits used for console redirection.</li> <li>– Options available: 7, 8. Default setting is <b>8</b>.</li> </ul> </li> </ul>

(Note) Advanced items prompt when this item is defined.

Parameter	Description
COM1 Console Redirection Settings (continued)	<ul style="list-style-type: none"> <li>◆ Parity <ul style="list-style-type: none"> <li>– A parity bit can be sent with the data bits to detect some transmission errors.</li> <li>– Even: parity bit is 0 if the num of 1's in the data bits is even.</li> <li>– Odd: parity bit is 0 if num of 1's in the data bits is odd.</li> <li>– Mark: parity bit is always 1. Space: Parity bit is always 0.</li> <li>– Mark and Space Parity do not allow for error detection.</li> <li>– Options available: None, Even, Odd, Mark, Space. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ Stop Bits <ul style="list-style-type: none"> <li>– Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.</li> <li>– Options available: 1, 2. Default setting is <b>1</b>.</li> </ul> </li> <li>◆ Flow Control <ul style="list-style-type: none"> <li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li> <li>– Options available: None, Hardware RTS/CTS. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ VT-UTF8 Combo Key Support <ul style="list-style-type: none"> <li>– Enable/Disable the VT-UTF8 Combo Key Support.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Recorder Mode <ul style="list-style-type: none"> <li>– When this mode enabled, only texts will be send. This is to capture Terminal data.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Resolution 100x31 <ul style="list-style-type: none"> <li>– Enable/Disable extended terminal resolution.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Putty Keypad <ul style="list-style-type: none"> <li>– Selects Function Key and Keypad on Putty.</li> <li>– Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is <b>VT100</b>.</li> </ul> </li> </ul>

Parameter	Description
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection <sup>(Note)</sup>	<p>EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.</p> <p>Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</p>
Serial Port for Out-of-Band EMS Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Out-of-Band Mgmt Port <ul style="list-style-type: none"> <li>– Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port.</li> <li>– Default setting is <b>COM1</b>.</li> </ul> </li> <li>◆ Terminal Type EMS <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is <b>VT100PLUS</b>.</li> </ul> </li> <li>◆ Bits per second EMS <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> <li>◆ Flow Control EMS <ul style="list-style-type: none"> <li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li> <li>– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is <b>None</b>.</li> </ul> </li> </ul>

### 5-2-3 SIO Configuration



Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	
[*Active*] Serial Port	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Use This Device               <ul style="list-style-type: none"> <li>– When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Logical Device Settings/Current:               <ul style="list-style-type: none"> <li>– Displays the serial port base I/O address and IRQ.</li> </ul> </li> <li>◆ Possible:               <ul style="list-style-type: none"> <li>– Configures the serial port base I/O address and IRQ.                   <ul style="list-style-type: none"> <li>Use Automatic Settings</li> <li>IO=3F8h; IRQ=4; DMA;</li> <li>IO=3F8h; IRQ=4; DMA;</li> <li>IO=2F8h; IRQ=4; DMA;</li> <li>IO=3E8h; IRQ=4; DMA;</li> <li>IO=2E8h; IRQ=4; DMA;</li> </ul> </li> <li>Default setting is <b>Use Automatic Settings</b>.</li> </ul> </li> </ul>

## 5-2-4 PCI Subsystem Settings

Aptio Setup - AMI

Advanced

PCI Bus Driver Version	A5.01.32	Enable/Disable SLOT1 I/O ROM ++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT1 I/O ROM	[Enabled]	
SLOT1 Lanes	[Auto]	
SLOT1 Max Link Speed	[Auto]	
SLOT2 I/O ROM	[Enabled]	
SLOT2 Lanes	[Auto]	
SLOT2 Max Link Speed	[Auto]	
SLOT3 I/O ROM	[Enabled]	
SLOT3 Lanes	[Auto]	
SLOT3 Max Link Speed	[Auto]	
SLOT4 I/O ROM	[Enabled]	
SLOT4 Lanes	[Auto]	
SLOT4 Max Link Speed	[Auto]	
SLOT6 I/O ROM	[Enabled]	
SLOT6 Lanes	[Auto]	
SLOT6 Max Link Speed	[Auto]	
SLOT11 I/O ROM	[Enabled]	
SLOT11 Lanes	[Auto]	
SLOT11 Max Link Speed	[Auto]	

Version 2.22.1294 Copyright (C) 2024 AMI

Aptio Setup - AMI

Advanced

SLOT6 Lanes	[Auto]	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support. ++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT6 Max Link Speed	[Auto]	
SLOT11 I/O ROM	[Enabled]	
SLOT11 Lanes	[Auto]	
SLOT11 Max Link Speed	[Auto]	
M2A I/O ROM	[Enabled]	
M2A Lanes	[Auto]	
M2A Max Link Speed	[Auto]	
M2B I/O ROM	[Enabled]	
M2B Lanes	[Auto]	
M2B Max Link Speed	[Auto]	
LAN I/O ROM	[Enabled]	
M2C I/O ROM	[Enabled]	
PCI Devices Common Settings:		
Re-Size BAR Support	[Disabled]	
SR-IOV Support	[Enabled]	

Version 2.22.1294 Copyright (C) 2024 AMI

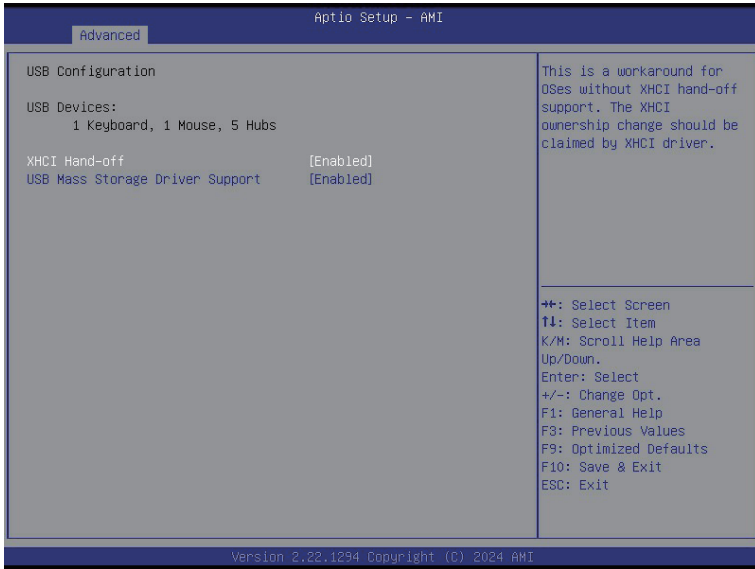
Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT_# I/O ROM <sup>(Note1)</sup>	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
SLOT_# Lanes <sup>(Note1)</sup>	Change the PCIe lanes. Default setting is <b>Auto</b> .
SLOT_#_Max Link Speed <sup>(Note1)</sup>	Configure PCIe max link speed. Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5. Default setting is <b>Auto</b> .
M2A/B I/O ROM <sup>(Note2)</sup>	Enable/Disable M2A I/O ROM. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
M2A/B Lanes <sup>(Note2)</sup>	Change the M2 PCIe lanes. Default setting is <b>Auto</b> .
M2A/B_Max Link Speed <sup>(Note1)</sup>	Configure M2 PCIe max link speed. Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5. Default setting is <b>Auto</b> .
LAN I/O ROM <sup>(Note3)</sup>	Enable/Disable the LAN devices, and initializes device expansion ROM. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
M2C I/O ROM	Enable/Disable M2A I/O ROM. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
PCI Devices Common Settings	
Re-Size BAR Support	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

(Note1) This section is dependent on the available PCIe Slot.

(Note2) This section is dependent on the available M2 Slot.

(Note3) This section is dependent on the available LAN controller.

## 5-2-5 USB Configuration



Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
USB Mass Storage Driver Support <sup>(Note)</sup>	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

(Note) This item is present only if you attach USB devices.

## 5-2-6 Network Stack Configuration



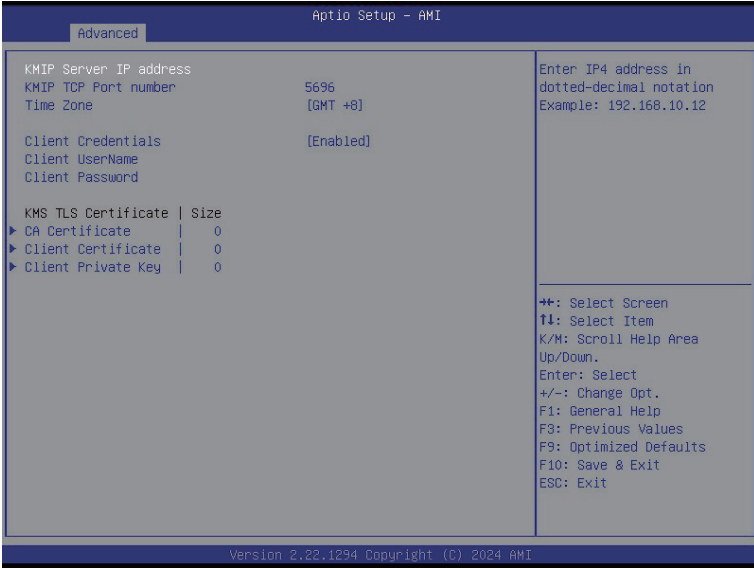
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Ipv4 HTTP Support	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Ipv6 PXE Support	Enable/Disable the Ipv6 PXE feature. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Ipv6 HTTP Support	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Press the <+> / <-> keys to increase or decrease the desired values.
Media detect count	Number of times the presence of media will be checked. Press the <+> / <-> keys to increase or decrease the desired values.

## 5-2-7 Post Report Configuration



Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Halt On	Options available: No Error, All Error. Default setting is <b>No Error</b> .

## 5-2-8 KMIP Server Configuration



Parameter	Description
KMIP Server IP address	
KMIP TCP Port Number	
Time Zone	Enter the correct timem zone for this server. Default setting is <b>GMT+8</b> .
Client Credentials	Use User and password credentials to authenticate the Client. Options available: Enabled, Disabled, Clear. Default setting is <b>Enabled</b> .
Client UserName	Enter Client identify: UserName. Name Length: 0-63 characters.
Client Password	Enter Client identify: Password. Password Length: 0-31 characters.
KMS TLS Certificate / Size	
CA Certificate	Enroll factory defaults or load the KMS TLS certificates from the file.
Client Certificate	Enroll factory defaults or load the KMS TLS certificates from the file.
Client Private Key	Enroll factory defaults or load the KMS TLS certificates from the file.

## 5-2-9 NVMe Configuration



Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.

## 5-2-10 Chipset Configuration



Parameter	Description
Restore on AC Power Loss <sup>(Note)</sup>	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
P2P Bridge IO Size	Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is <b>0x1000</b> .
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
NVMe SSD Security Frozen	Attempt to send freeze lock command to NVMe SSDs during boot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
NVMe OPROM Select	BIOS Build-In is default setting. Select Device Itself, then this NVMe page will not display any device. Unless the device doesn't have OPROM. Options available: BIOS Build-In, NVMe Device, Disables. Default setting is <b>BIOS Build-In</b> .
NVMe LED Control	Enable/Disable allow user control NVMe LED. It only available the NVMe device direct connect to CPU. Default setting is <b>Disable</b> .

(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

## 5-2-11 Tls Auth Configuration



Parameter	Description
Server CA Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ Enroll Cert                             <ul style="list-style-type: none"> <li>– Press [Enter] to enroll a certificate                                     <ul style="list-style-type: none"> <li>• Enroll Cert Using File</li> <li>• Cert GUID   <ul style="list-style-type: none"> <li>Input digit character in 1111111-2222-3333-4444-1234567890ab format.</li> </ul> </li> </ul> </li> <li>– Commit Changes and Exit</li> <li>– Discard Changes and Exit</li> </ul> </li> <li>◆ Delete Cert</li> </ul>
Client Cert Configuration	Press [Enter] for configuration of advanced items.



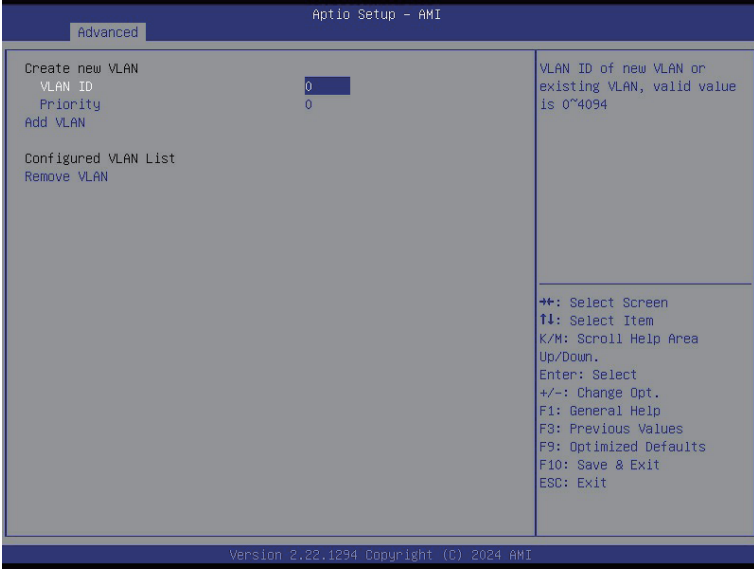
## 5-2-13 Intel(R) i350 Gigabit Network Connection

Advanced		Aptio Setup - AMI	
<p>▶ NIC Configuration</p> <p>Blink LEDs 0</p> <p>UEFI Driver Intel(R) PRO/1000 9.1.12 PCI-E</p> <p>Adapter PBA 106300-000</p> <p>Device Name Intel(R) I350 Gigabit Network Connection</p> <p>Chip Type Intel i350</p> <p>PCI Device ID 1521</p> <p>PCI Address 2A:00:00</p> <p>Link Status [Disconnected]</p> <p>MAC Address 10:FF:E0:0C:BE:8D</p> <p>Virtual MAC Address 00:00:00:00:00:00</p>		<p>Click to configure the network device port.</p>	
		<p>↔: Select Screen            ↑↓: Select Item            K/M: Scroll Help Area Up/Down.            Enter: Select            +/-: Change Opt.            F1: General Help            F8: Previous Values            F9: Optimized Defaults            F10: Save &amp; Exit            ESC: Exit</p>	
Version 2.22.1294 Copyright (C) 2024 AMI			

Advanced		Aptio Setup - AMI	
<p>Link Speed [Auto Negotiated]</p> <p>Wake On LAN [Enabled]</p>		<p>Specifies the port speed used for the selected boot protocol.</p>	
		<p>↔: Select Screen            ↑↓: Select Item            K/M: Scroll Help Area Up/Down.            Enter: Select            +/-: Change Opt.            F1: General Help            F8: Previous Values            F9: Optimized Defaults            F10: Save &amp; Exit            ESC: Exit</p>	
Version 2.22.1294 Copyright (C) 2024 AMI			

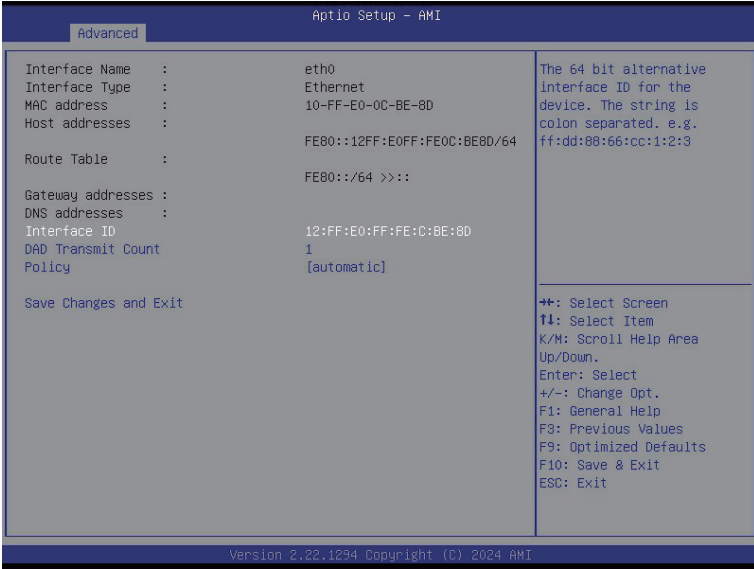
Parameter	Description
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Link Speed <ul style="list-style-type: none"> <li>– Allows for automatic link speed adjustment.</li> <li>– Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. Default setting is <b>Auto Negotiated</b>.</li> </ul> </li> <li>◆ Wake On LAN <ul style="list-style-type: none"> <li>– Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul>
Blink LEDs	<p>Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).</p>
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

## 5-2-14 VLAN Configuration



Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Create new VLAN</li> <li>◆ VLAN ID                             <ul style="list-style-type: none"> <li>– Sets VLAN ID for a new VLAN or an existing VLAN.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li>– The valid range is from 0 to 4094.</li> </ul> </li> <li>◆ Priority                             <ul style="list-style-type: none"> <li>– Sets 802.1Q Priority for a new VLAN or an existing VLAN.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li>– The valid range is from 0 to 7.</li> </ul> </li> <li>◆ Add VLAN                             <ul style="list-style-type: none"> <li>– Press [Enter] to create a new VLAN or update an existing VLAN.</li> </ul> </li> <li>◆ Configured VLAN List</li> <li>◆ Remove VLAN                             <ul style="list-style-type: none"> <li>– Press [Enter] to remove an existing VLAN.</li> </ul> </li> </ul>

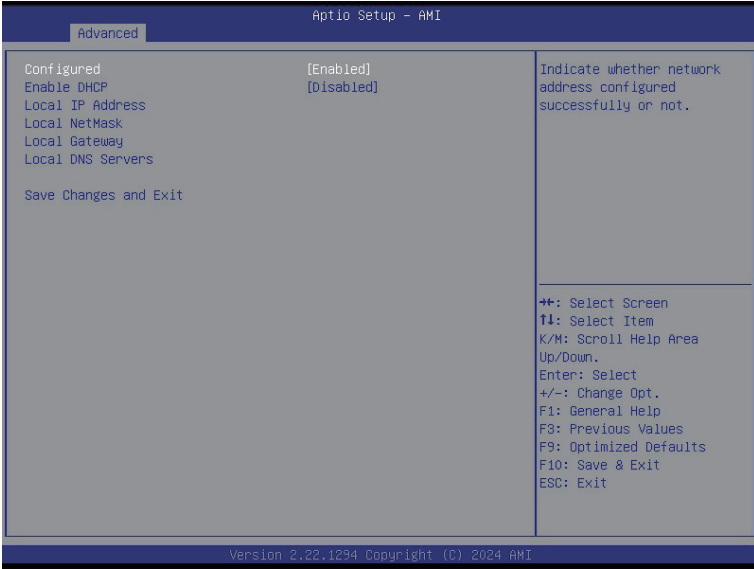
## 5-2-15 MAC IPv6 Network Configuration



Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Displays the MAC Address information.</li> <li>◆ Interface ID <ul style="list-style-type: none"> <li>– The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3.</li> </ul> </li> <li>◆ DAD Transmit Count <ul style="list-style-type: none"> <li>– The number of consecutive Neighbor solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.</li> </ul> </li> <li>◆ Policy <ul style="list-style-type: none"> <li>– Options available: automatic, manual. Default setting is <b>automatic</b>.</li> </ul> </li> <li>◆ Save Changes and Exit <ul style="list-style-type: none"> <li>– Press [Enter] to save all configurations.</li> </ul> </li> </ul>

(Note) This item appears when **Configured** is set to **Enabled**.

## 5-2-16 MAC IPv4 Network Configuration



Parameter	Description
Configured	Indicates whether network address is configured successfully or not. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Enable DHCP <sup>(Note)</sup>	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Local IP Address <sup>(Note)</sup>	Press [Enter] to configure local IP address.
Local NetMask <sup>(Note)</sup>	Press [Enter] to configure local NetMask.
Local Gateway <sup>(Note)</sup>	Press [Enter] to configure local Gateway
Local DNS Servers <sup>(Note)</sup>	Press [Enter] to configure local DNS servers
Save Changes and Exit	Press [Enter] to save all configurations.

(Note) This item appears when **Configured** is set to **Enabled**.

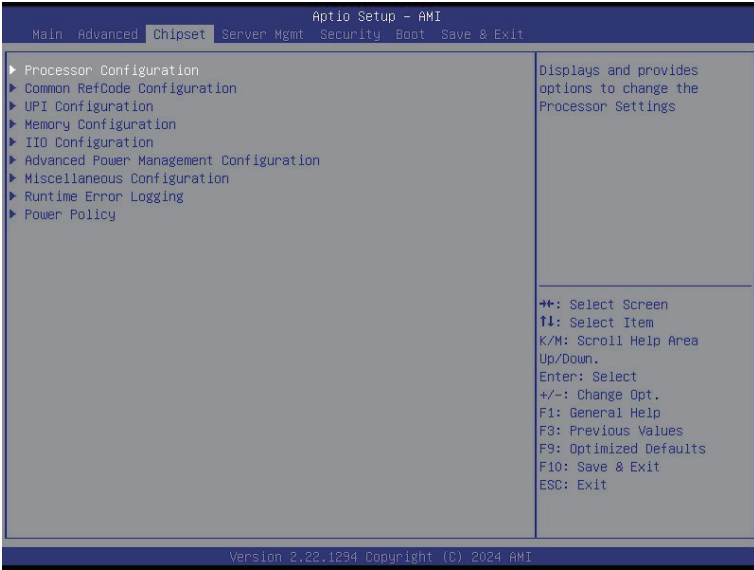
## 5-2-17 Driver Health



Parameter	Description
Driver Health	Displays driver health status of the devices/controllers if installed

## 5-3 Chipset Menu

The Chipset Setup menu displays submenu options for configuring the chipset functions. Select a submenu item, then press <Enter> to access the related submenu screen.



## 5-3-1 Processor Configuration

Aptio Setup - AMI

Chipset

Processor Configuration		Change Per-Socket Settings	
-----			
▶ Per-Socket Configuration			
Processor Socket	Socket 0	Socket 1	
Processor ID	000A06F3*	000A06F3	
Processor Frequency	2.400GHz	2.400GHz	
Processor Max Ratio	18H	18H	
Processor Min Ratio	08H	08H	
Microcode Revision	030001B3	030001B3	
L1 Cache RAM(Per Core)	96KB	96KB	
L2 Cache RAM(Per Package)	65536KB	65536KB	
L3 Cache RAM(Per Package)	98304KB	98304KB	
Processor 0 Version	Intel(R) Xeon(R) 6710E		
Processor 1 Version	Intel(R) Xeon(R) 6710E		
Hardware Prefetcher	[Enable]		
Adjacent Cache Prefetch	[Enable]		
DCU Streamer Prefetcher	[Auto]		
DCU IP Prefetcher	[Enable]		
L1 Next Page Prefetcher	[Enable]		
Enable Intel(R) TXT	[Disable]		
VMX	[Enable]		
Enable SMX	[Disable]		
-----			
++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit			
Version 2.22.1294 Copyright (C) 2024 AMI			

Aptio Setup - AMI

Chipset

Processor Reserved Memory [Outputs]		Enable/Disable Software Guard Extensions (SGX) Package Info In-Band Access	
PRMRR Min Size per domain	2 MiB		
PRMRR Max Size per domain	64 GiB		
-----			
Processor Reserved Memory [Outputs]			
PRMRR Size per domain	16 MiB		
PRM Size per socket	16 MiB		
PRM Size per system	16 MiB		
-----			
Software Guard Extension (SGX) [Outputs]			
SGX activation state	Deactivated		
SGX memory population for SGX enabling is not PDR. Please check your memory population.			
SGX error code (HEX)	16		
-----			
Software Guard Extension (SGX) [Inputs]			
SGX Factory Reset	[Disabled]		
SW Guard Extensions (SGX)	[Disabled]		
SGX Package Info In-Band Access	[Disabled]		
SGX PRMRR Size Requested	[Auto]		
-----			
In Field Scan (IFS)			
-----			
++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit			
Version 2.22.1294 Copyright (C) 2024 AMI			

Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ CPU Socket 0/1 Configuration <ul style="list-style-type: none"> <li>– Core Disable Bitmap(Hex) <ul style="list-style-type: none"> <li>• Number of Cores to enable. 0 means all cores. FFFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.</li> </ul> </li> </ul> </li> </ul>
Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Package) / L3 Cache RAM(Per Package) / Processor # Version	Displays the technical specifications for the installed processor(s).
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enable, Disable. Default setting is <b>Enable</b> .
L2 RF0 Prefetch Disable	Options available: Enable, Disable. Default setting is <b>Disable</b> .
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable, Disable. Default setting is <b>Enable</b> .
DCU Streamer Prefetcher	Enable/Disable DCU streamer prefetcher. Options available: Enable, Disable. Default setting is <b>Enable</b> .
DCU IP Prefetcher	Enable/Disable DCU IP Prefetcher. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Enable Intel(R) TXT	Enable/Disable the Intel Trusted Execution Technology support function. Options available: Enable, Disable. Default setting is <b>Disable</b> .
VMX	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Enable SMX	Enable/Disable the Safer Mode Extensions (SMX) support function. Options available: Enable, Disable. Default setting is <b>Disable</b> .
AES-NI	Enable/Disable the AES-NI support. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Debug Consent	Options available: Enable, Disable. Default setting is <b>Disable</b> .
Parameter	Description
Memory Encryption (TME) <sup>(Note)</sup>	Enable/Disable memory encryption (TME). Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Total Memory Encryption Multi-Tenant (TME-MT)	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .

Memory integrity	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Trust Domain Extension (TDX)	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
SGX error code [HEX]	Shows hexadecimal SGX internal error code.
SGXx Factory Reset	Perform SGX Factory Reset, on subsequent boot: delete all registration data, if SGX enabled will force Initial Platform Establishment flow. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
SW Guard Extension (SGX)	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
SGX Package Inf In-Band Access	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
SGX PRMR Size Requested	Options available: Enabled, Disabled. Default setting is <b>Auto</b> .
In-Field Scan (IFS)	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Enable SAF <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled.</li> <li>– Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ SAF PRMR Size Requested <ul style="list-style-type: none"> <li>– Default setting is <b>8M</b>.</li> </ul> </li> </ul>

(Note) Advanced items prompt when this item is defined.

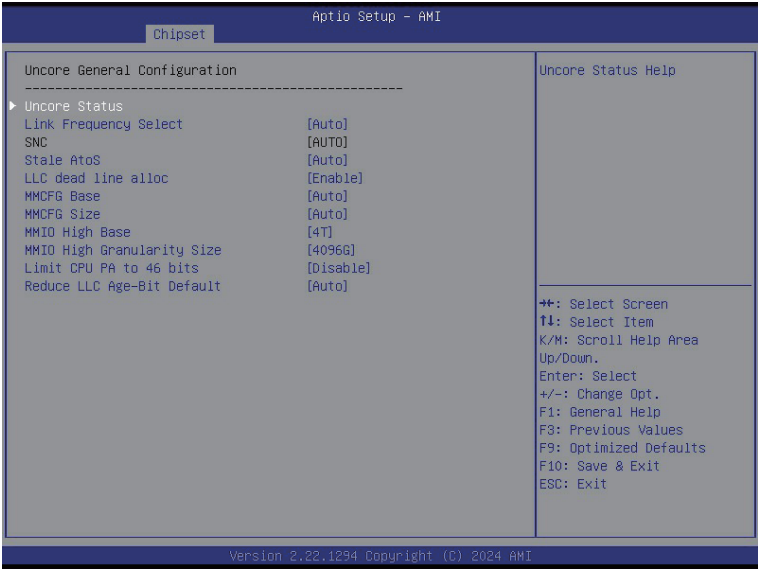
### 5-3-2 Common RefCode Configuration



Parameter	Description
Common RefCode Configuration	
Virtual Numa <sup>(note)</sup>	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors. Options available: Enable, Disable. Default setting is <b>Disable</b> .
Number of Virtual Numa Nodes	The number of virtual NUMA nodes per physical NUMA nodes. 0 means automatically set the number of virtual NUMA nodes baes on system configuration. 1 equals disabling virtual NUMA.

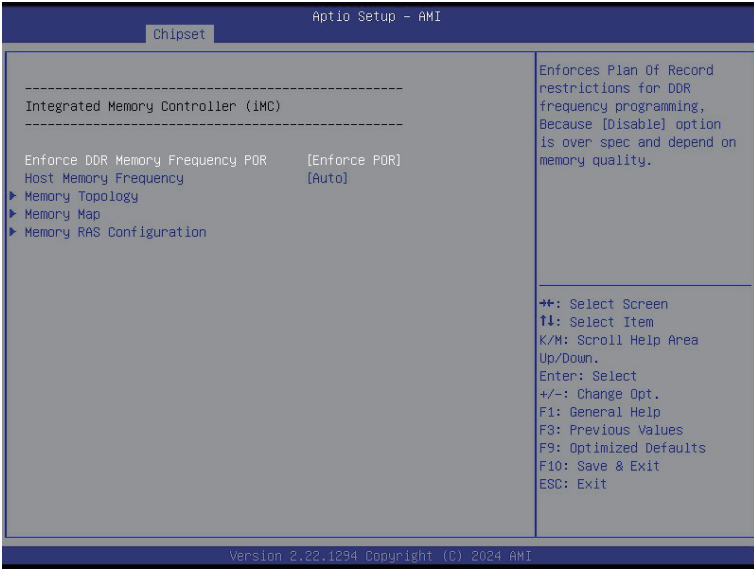
(Note) Advanced items prompt when this item is defined.

### 5-3-3 UPI Configuration



Parameter	Description
UPI General Configuration	<p data-bbox="348 142 682 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="348 170 501 194">◆ Uncore Status <ul style="list-style-type: none"> <li data-bbox="384 199 719 222">– Press [Enter] to view the Uncore status.</li> </ul> </li> <li data-bbox="348 227 564 250">◆ Link Frequency Select <ul style="list-style-type: none"> <li data-bbox="384 255 650 279">– Selects the UPI link frequency.</li> <li data-bbox="384 283 956 338">– Options available: 12.8GT/s, 14.4GT/s, 16.0GT/s, Auto, Use Per Link Setting. Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 343 426 366">◆ SNC <ul style="list-style-type: none"> <li data-bbox="384 371 753 395">– Enable/Disable Sub NUMA Cluster function.</li> <li data-bbox="384 399 935 454">– Options available: Auto, Disable, Enable SNC2 (2-clusters), Enable SNC4 (4-clusters). Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 459 472 482">◆ Stale AtoS <ul style="list-style-type: none"> <li data-bbox="384 487 802 511">– Enable/Disable Stale A to S directory optimization.</li> <li data-bbox="384 515 913 539">– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 544 538 567">◆ LLC dead line alloc <ul style="list-style-type: none"> <li data-bbox="384 572 695 595">– Enable/Disable fill dead lines in LLC.</li> <li data-bbox="384 600 932 624">– Options available: Disable, Enable, Auto. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="348 628 501 652">◆ MMCFG Base <ul style="list-style-type: none"> <li data-bbox="384 656 859 680">– Options available: 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, Auto.</li> <li data-bbox="384 685 589 708">– Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 713 493 736">◆ MMCFG Size <ul style="list-style-type: none"> <li data-bbox="384 741 871 765">– Options available: 64M, 128M, 256M, 512M, 1G, 2G, Auto .</li> <li data-bbox="384 769 589 793">– Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 798 522 821">◆ MMIO High Base <ul style="list-style-type: none"> <li data-bbox="384 826 956 881">– Options available: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T. Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="348 885 607 909">◆ MMIO High Granularity Size <ul style="list-style-type: none"> <li data-bbox="384 914 876 937">– Selects the allocation size used to assign mmioh resources.</li> <li data-bbox="384 942 956 997">– Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is <b>64G</b>.</li> </ul> </li> <li data-bbox="348 1001 568 1025">◆ Limit CPU PA to 46 bits <ul style="list-style-type: none"> <li data-bbox="384 1030 937 1053">– Options available: Disable, Enable, Auto. Default setting is <b>Disable</b>.</li> </ul> </li> <li data-bbox="348 1058 610 1081">◆ Reduce LLC Age-Bit Default <ul style="list-style-type: none"> <li data-bbox="384 1086 727 1110">– Options available: Disable, Enable, Auto.</li> <li data-bbox="384 1114 701 1138">– Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>

### 5-3-4 Memory Configuration



Parameter	Description
Integrated Memory Controller (iMC)	
Enforce DDR Memory Frequency POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR frequency programming. Options available: POR, Disable. Default setting is <b>POR</b> .
Host Memory Frequency	Maximum Host DDR Memory Frequency Selections in MT/s. If the AUTO option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. Options available: Auto, 4800, 5200, 5600, 6000, 6400. Default setting is <b>Auto</b> .

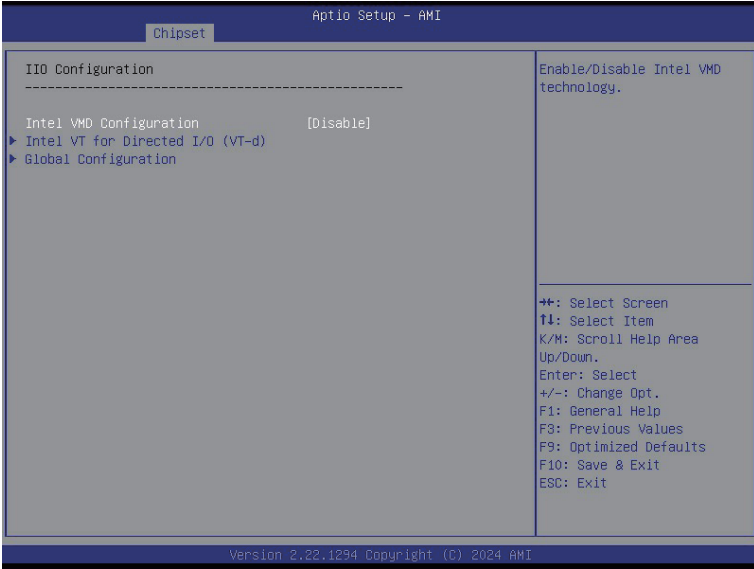
Parameter	Description
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel(R) Flat Memory Mode Support. <ul style="list-style-type: none"> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ DDR CXL Heterogeneous Interleave support. <ul style="list-style-type: none"> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>
Memory RAS Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Mirror Mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch.</li> <li>– Options available: Disabled, Full Mirror Mode, Partial Mirror Mode. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Correctable Error Threshold <ul style="list-style-type: none"> <li>– Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket time window based interface <ul style="list-style-type: none"> <li>– Enable/Disable leaky bucket time window based interface.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Leaky bucket low bit <ul style="list-style-type: none"> <li>– Configures leaky bucket low bit (0x1 - 0x29).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket high bit <ul style="list-style-type: none"> <li>– Configures leaky bucket high bit (0x1 - 0x29).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> </ul>

(Note) Advanced items prompt when this item is defined.

Parameter	Description
Memory RAS Configuration (continued)	<ul style="list-style-type: none"> <li>◆ ADDDC Sparing<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable ADDDC Sparing.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Enable ADDDC Error Injection <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Patrol Scrub <ul style="list-style-type: none"> <li>– Options available: Disabled, Enable at End of POST. Default setting is <b>Enable at End of POST</b>.</li> </ul> </li> <li>◆ Patrol Scrub Interval <ul style="list-style-type: none"> <li>– Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto.</li> </ul> </li> <li>◆ DDR5 ECS <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled, Enable ECS with Result Collection. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul>

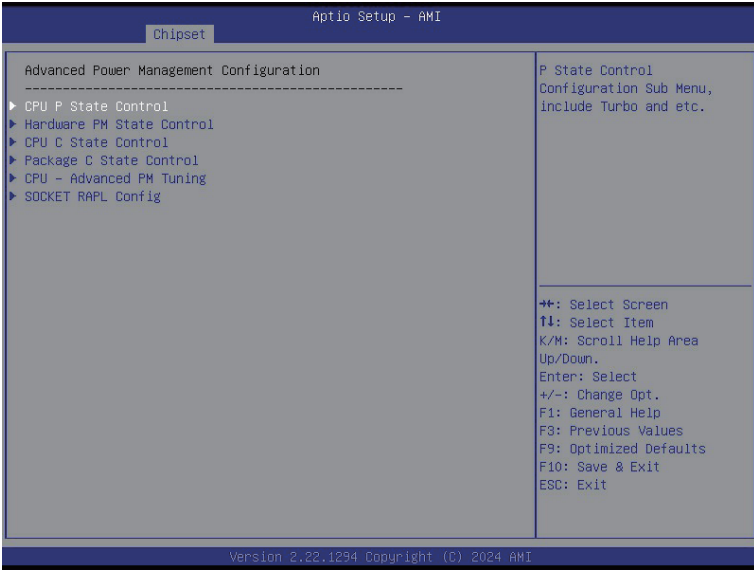
(Note) Advanced items prompt when this item is defined.

### 5-3-5 IIO Configuration



Parameter	Description
IIO Configuration	
Intel VMD Configuration	Enable/Disable Intel VMD technology. Options available: Enable, Disable. Default setting is <b>Disable</b> .
Intel VT for Directed I/O (VT-d)	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> <li>– Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).</li> </ul> </li> <li>◆ Pre-boot DMA Protection <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ PCIe ACSCTL <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Cache Allocation <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Global Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Max Read Request Size <ul style="list-style-type: none"> <li>– Options available: Auto, 128B, 256B, 512B, 1024B, 2048B, 4096B. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Relaxed Ordering <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>

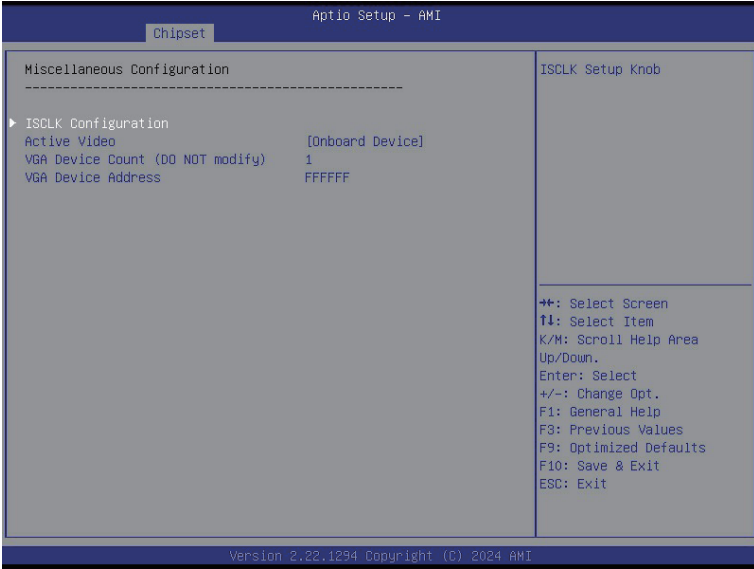
### 5-3-6 Advanced Power Management Configuration



Parameter	Description
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel SST-PP               <ul style="list-style-type: none"> <li>– Intel SST-PP Select allows user to choose level.</li> <li>– Options available: Auto, Level 0, Level 1. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ SpeedStep (Pstates)               <ul style="list-style-type: none"> <li>– Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Turbo Mode               <ul style="list-style-type: none"> <li>– When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>

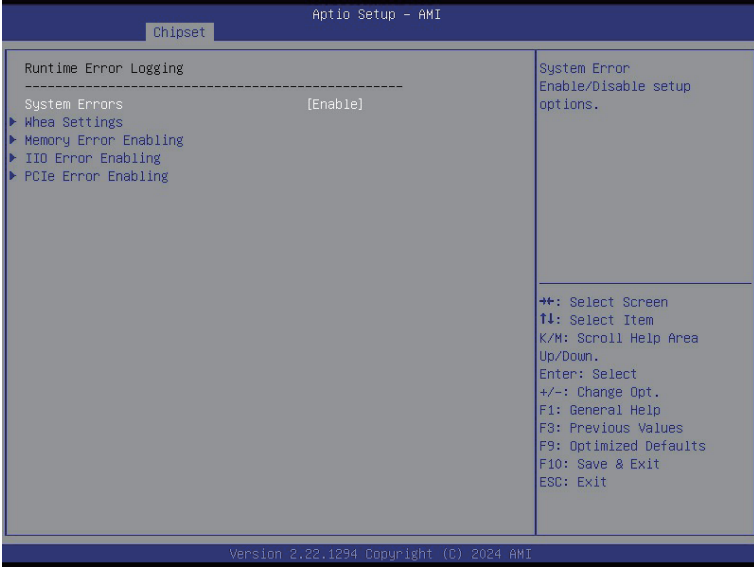
Parameter	Description
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Hardware P-States <ul style="list-style-type: none"> <li>– When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States).</li> <li>– In Native mode, the processor hardware chooses a P-state based on OS guidance.</li> <li>– In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance).</li> <li>– Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is <b>Native Mode</b>.</li> </ul> </li> </ul>
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Monitor MWAIT <ul style="list-style-type: none"> <li>– Options available: Disable, Enable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ ACPI C1 Enumeration <ul style="list-style-type: none"> <li>– Options available: C1, C1e . Default setting is <b>C1e</b>.</li> </ul> </li> <li>◆ ACPI C6x Enumeration <ul style="list-style-type: none"> <li>– Options available: Dsiable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto .</li> <li>– Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Package C State <ul style="list-style-type: none"> <li>– Configures the state for the C-State package limit.</li> <li>– Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
CPU - Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Energy Perf BIAS <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>» Power Performance Tuning <ul style="list-style-type: none"> <li>• Options available: OS Controls EPB, BIOS Controls EPB, PECL Controls EPB. Default setting is <b>OS Controls EPB</b>.</li> </ul> </li> <li>» Energy_PERF_BIAS_CFG mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>• Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is <b>Balanced Performance</b>.</li> </ul> </li> </ul> </li> </ul> </li> </ul>
SOCKET RAPL Config	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ PL1 Power Limit <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ PL1 Time Window <ul style="list-style-type: none"> <li>• Default setting is <b>1</b>.</li> </ul> </li> <li>◆ PL2 Power Limit <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ PL2 Time Window <ul style="list-style-type: none"> <li>• Default setting is <b>1</b>.</li> </ul> </li> </ul>

### 5-3-7 Miscellaneous Configuration



Parameter	Description
Miscellaneous Configuration	
ISCLK Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>- SSC1 Enable</li> <li>- Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> <li>- SSC2 Enable</li> <li>- Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul>
Active Video	Selects the active video type. Options available: Auto, Onboard Device, PCIE Device, Specific PCIE Device. Default setting is <b>Auto</b> .
VGA Device Count (NOT modify)	
VGA Device Address	VGA Device Address

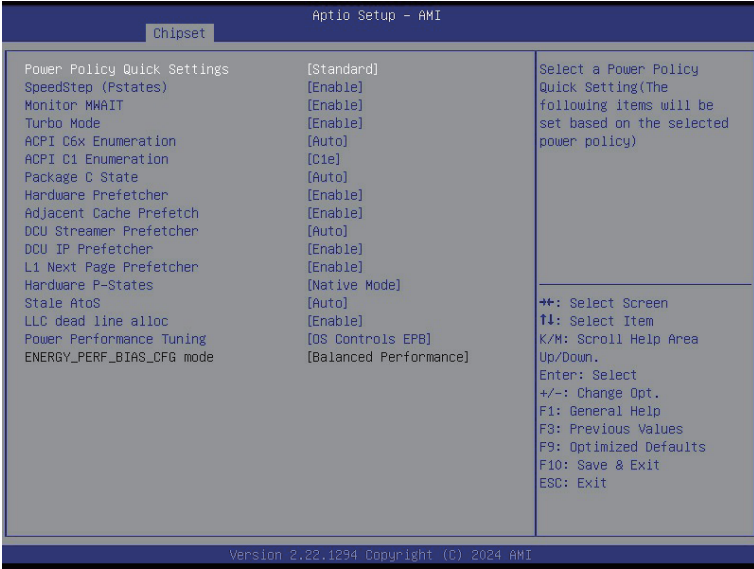
### 5-3-8 Runtime Error Logging Settings



Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Whea Settings	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ WHEA (Windows Hardware Error Architecture) Support <ul style="list-style-type: none"> <li>– Enable/Disable WHEA Support.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Memory Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Memory Corrected Error <ul style="list-style-type: none"> <li>– Enable/Disable Memory Corrected Error.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Uncorrected Error disable Memory <ul style="list-style-type: none"> <li>– Enable/Disable the Memory that triggers Uncorrected Error.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>
IIO Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ OS Native AER Support <ul style="list-style-type: none"> <li>– Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

Parameter	Description
PCIe Error Enabling	<p data-bbox="309 142 642 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="309 170 852 252">◆ Corrected Error <ul style="list-style-type: none"> <li data-bbox="344 200 795 224">– Enables and escalates correctable Errors to error pins.</li> <li data-bbox="344 228 852 252">– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li data-bbox="309 257 923 338">◆ Uncorrected Error <ul style="list-style-type: none"> <li data-bbox="344 286 923 310">– Enables and escalates Uncorrectable/Recoverable Errors to error pins.</li> <li data-bbox="344 315 846 338">– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 343 846 424">◆ Fatal Error Enable <ul style="list-style-type: none"> <li data-bbox="344 373 749 396">– Enables and escalates Fatal Errors to error pins.</li> <li data-bbox="344 401 846 424">– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 429 940 542">◆ Assert NMI on SERR <ul style="list-style-type: none"> <li data-bbox="344 459 940 515">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs.</li> <li data-bbox="344 520 876 542">– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li data-bbox="309 547 940 660">◆ Assert NMI on PERR <ul style="list-style-type: none"> <li data-bbox="344 577 940 633">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs.</li> <li data-bbox="344 638 876 660">– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul>

### 5-3-9 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient. Default setting is <b>Standard</b> .
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Monitor MWAIT	Allows Monitor and MWAIT instructions. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enable, Disable. Default setting is <b>Enable</b> .
ACPI C6x Enumeration	Options available: Disable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto. Default setting is <b>Auto</b> .
ACPI C1 Enumeration	Options available: C1, C1e. Default setting is <b>C1e</b> .
Package C State	Configures the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b> .

Parameter	Description
Hardware Prefetcher	Options available: Enable, Disable. Default setting is <b>Enable</b> .
Adjacent Cache Prefetch	Options available: Enable, Disable. Default setting is <b>Enable</b> .
DCU Streamer Prefetcher	Options available: Enable, Disable. Default setting is <b>Enable</b> .
L1 Next page Prefetcher	Options available: Enable, Disable. Default setting is <b>Enable</b> .
Hardware P-States	Options available: Disable, Native mode, Out of Band mode, Native Mode with No Legacy Support. Default setting is <b>Native Mode</b> .
Stale AtoS	Options available: Auto, Enable, Disable. Default setting is <b>Auto</b> .
LLC dead line alloc	Options available: Auto, Enable, Disable. Default setting is <b>Enable</b> .
Power Performance Tuning	Options available: OS Controls EPB, BIOS Controls EPB, PECC Controls EPB. Default setting is <b>BIOS Controls EPB</b> .
ENERGY_PERF_BIAS_CFG mode	Performance, Balanced Performance, Balanced Power, Power. Default setting is <b>Balanced Performance</b> .

## 5-4 Server Management Menu



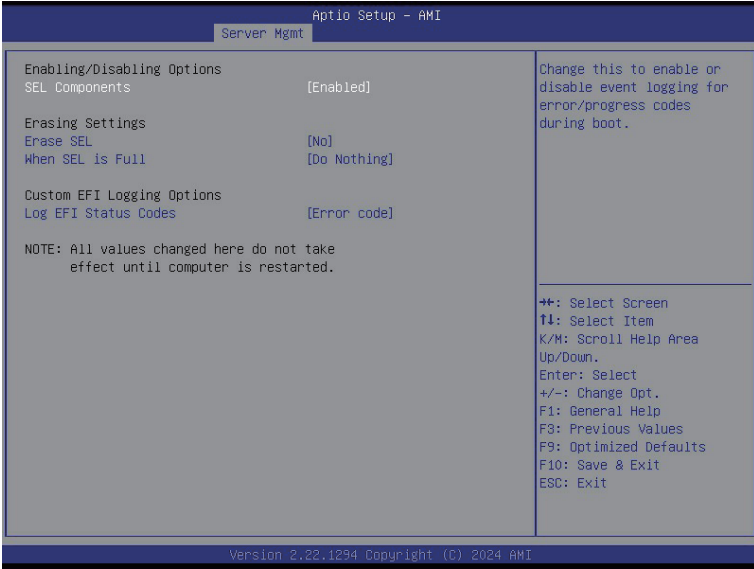
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
FRB-2 Timer <sup>(Note1)</sup> timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is <b>6 minutes</b> .
FRB-2 Timer Policy <sup>(Note1)</sup>	Configures the FRB2 Timer policy. Options available: Do Nothing, Reset, Power Down, Power Cycle. Default setting is <b>Do Nothing</b> .
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
OS Wtd Timer Timeout <sup>(Note2)</sup>	Configures OS Watchdog Timer. The value is between 1 to 30 minutes. Default setting is <b>10 minutes</b> .
OS Wtd Timer Policy <sup>(Note2)</sup>	Configure OS Watchdog Timer Policy. Options available: Reset, Do Nothing, Power Down, Power Cycle. Default setting is <b>Reset</b> .
Wait BMC Ready	POST wait BMC ready and reboot system. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is <b>2 minutes</b> .

(Note1) This item is configurable when **FRB-2 Timer** is set to **Enabled**.

(Note2) This item is configurable when **OS Watchdog Timer** is set to **Enabled**.

<b>Parameter</b>	<b>Description</b>
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the FRU information.
BMC VLAN Configuration	Press [Enter] to configure advanced items.
BMC network Configuration	Press [Enter] to configure advanced items.
IPv6 BMC Network Configuration	Press [Enter] to configure advanced items.

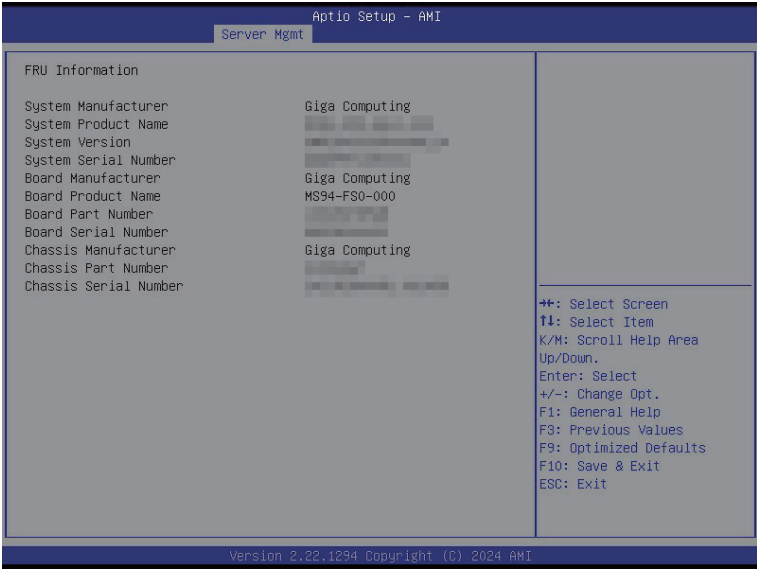
# 5-4-1 System Event Log



Parameter	Description
Enabling / Disabling Options	
SEL Components	Change this item to enable or disable all features of System Event Logging during boot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: No, Yes, On next reset, Yes, On every reset. Default setting is <b>No</b> .
When SEL is Full	Choose options for reactions to a full SEL. Options available: Do Nothing, Erase Immediately, Delete Oldest Record. Default setting is <b>Do Nothing</b> .
Custom EFI Logging Options	
Log EFI Status Codes	Enable/Disable the logging of EFI Status Codes (if not already converted to legacy). Options available: Disabled, Both, Error code, Progress code. Default setting is <b>Error code</b> .

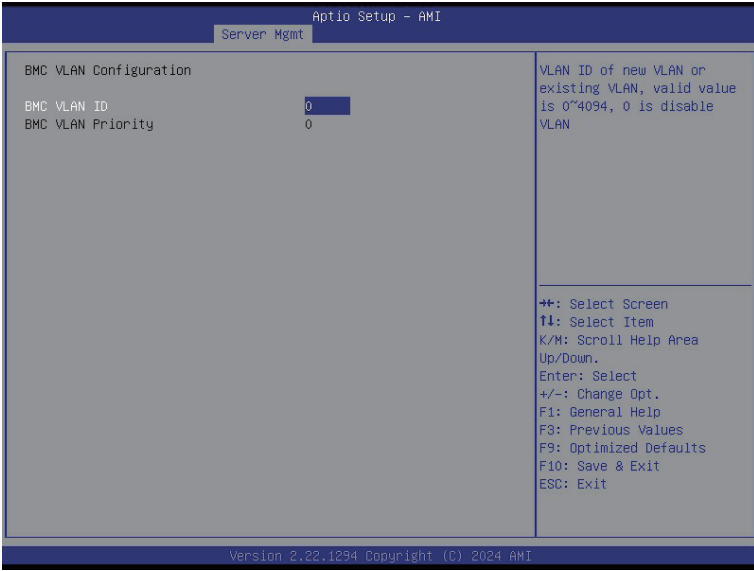
## 5-4-2 View FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information. Items on this window are non-configurable.



(Note) The model name will vary depends on the product you purchased

### 5-4-3 BMC VLAN Configuration



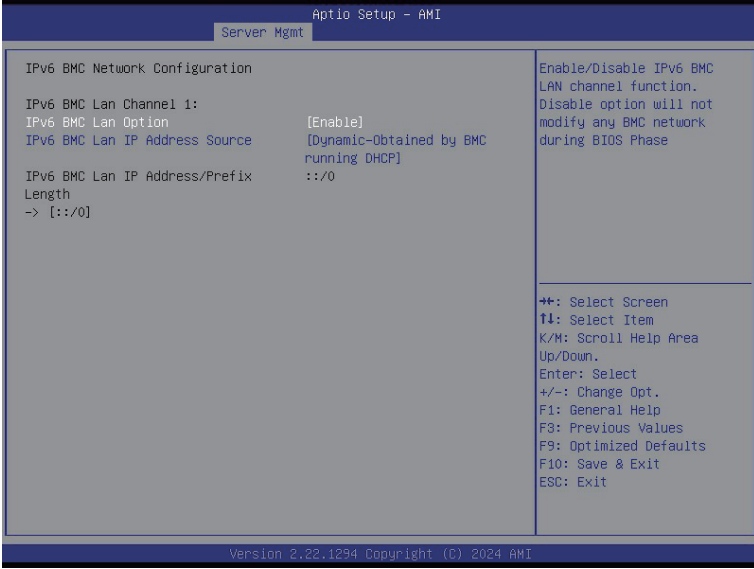
Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority will not be selected.

## 5-4-4 BMC Network Configuration



Parameter	Description
BMC network configuration	
Select NCSI and Dedicated LAN	Options available: Do Nothing, Model1(Dedicated), Model2(NCSI), Mode3(Failover). Default setting is <b>Do Nothing</b> .
Lan Channel 1	
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (DHCP). Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is <b>DynamicBmcDhcp</b> .
Station IP address	Displays IP Address information.
Subnet mask	Displays Subnet Mask information. Please note that the IP address must be in three digitals, for example, 192.168.000.001.
Router IP address	Displays the Router IP Address information.
Station MAC address	Displays the MAC Address information.
Real-time get BMC network address	Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.

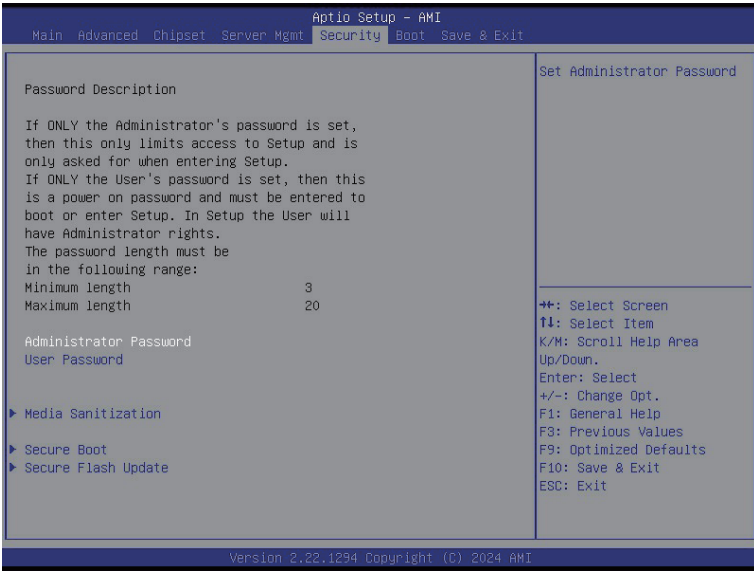
## 5-4-5 IPv6 BMC Network Configuration



Parameter	Description
IPv6 BMC network configuration	
IPv6 BMC Lan Channel 1	
IPv6 BMC Lan Option	Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase. Options available: Unspecified, Disable, Enable. Default setting is <b>Enable</b> .
IPv6 BMC Lan IP Address Source	Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Options available: Unspecified, Static, Dynamic-Obtained by BMC running DHCP. Default setting is <b>Dynamic-Obtained by BMC running DHCP</b> .
IPv6 BMC Lan IP Address/Prefix Length	Check if the IPv6 BMC LAN IP address matches those displayed on the screen.

## 5-5 Security Menu

The Security menu allows you to safeguard and protect the system from unauthorized use by setting up access passwords.



There are two types of passwords that you can set:

- **Administrator Password**

Entering this password will allow the user to access and change all settings in the Setup Utility.
- **User Password**

Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

Parameter	Description
Administrator Password	Press [Enter] to configure the administrator password.
User Password	Press [Enter] to configure the user password.
Media Ssanitization	Press [Enter] to configure advanced items.
Secure Boot	Press [Enter] to configure advanced items.
Secure Flash Update	Press [Enter] to configure advanced items.

## 5-5-1 Secure Boot

The Secure Boot feature is applicable if supported by your Operating System.

If your Operating System is not supporting Secure Boot, the system will hang when starting the Operating System.



Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Secure Boot Mode <sup>(Note)</sup>	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before the Operating System loads to the login screen have not been tampered with. When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases. When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database. Options available: Standard, Custom. Default setting is <b>Standard</b> .
Restore Factory Keys	Forces the system to user mode and installs factory default Secure Boot key database.
Reset To Setup Mode	Reset the system to Setup Mode.

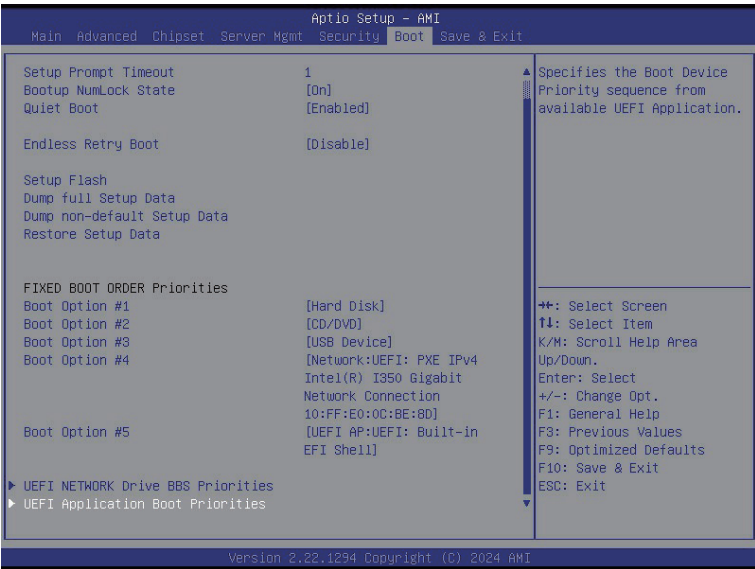
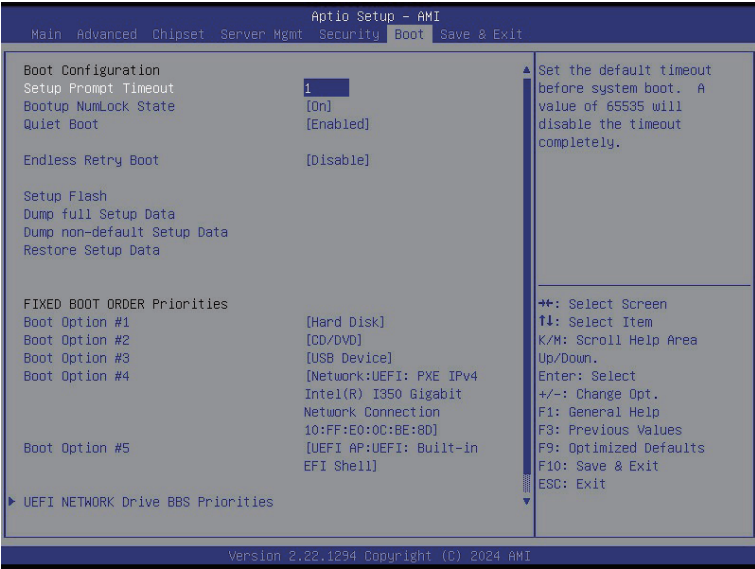
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235"><b>Please note that this item is configurable when Secure Boot Mode is set to Custom.</b></p> <ul style="list-style-type: none"> <li data-bbox="335 243 941 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 941 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li data-bbox="367 326 904 352">– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="335 357 925 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 925 404">– Installs all factory default keys. It will force the system in User Mode.</li> <li data-bbox="367 409 606 431">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 435 654 509">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode.</li> <li data-bbox="367 487 606 509">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 514 899 595">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 537 899 595">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li data-bbox="335 600 936 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 624 936 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.</li> </ul> </li> <li data-bbox="335 686 893 736">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 893 736">– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li data-bbox="335 741 803 846">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 765 803 788">– Displays the current status of the Platform Key (PK).</li> <li data-bbox="367 793 675 816">– Press [Enter] to configure a new PK.</li> <li data-bbox="367 821 601 846">– Options available: Update.</li> </ul> </li> <li data-bbox="335 851 941 987">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 874 941 898">– Displays the current status of the Key Exchange Key Database (KEK).</li> <li data-bbox="367 903 904 956">– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li data-bbox="367 961 670 987">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 992 941 1128">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1016 904 1039">– Displays the current status of the Authorized Signature Database.</li> <li data-bbox="367 1044 941 1097">– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li data-bbox="367 1102 670 1128">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 1133 899 1270">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1157 899 1180">– Displays the current status of the Forbidden Signature Database.</li> <li data-bbox="367 1185 893 1238">– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li data-bbox="367 1243 670 1270">– Options available: Update, Append.</li> </ul> </li> </ul>

Parameter	Description
Key Management (continued)	<ul style="list-style-type: none"> <li>◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li>– Displays the current status of the Authorized TimeStamps Database.</li> <li>– Press [Enter] to configure a new DBT or load additional DBT from storage devices.</li> <li>– Options available: Update, Append.</li> </ul> </li> <li>◆ OsRecovery Signatures <ul style="list-style-type: none"> <li>– Displays the current status of the OsRecovery Signature Database.</li> <li>– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.</li> <li>– Options available: Update, Append.</li> </ul> </li> </ul>

# 5-6 Boot Menu

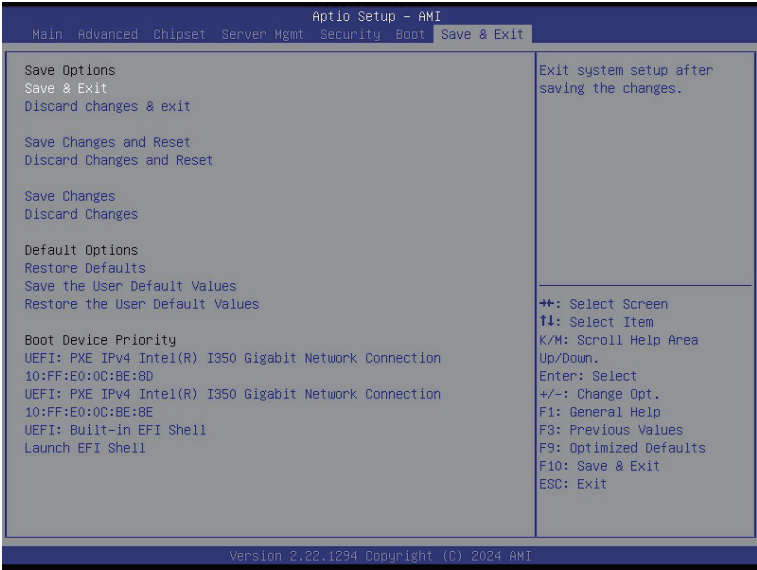
The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off. Default setting is <b>On</b> .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Endless Retry Boot	Options available: Disable, Enable. Default setting is <b>Disable</b> .
Setup Flash	Press [Enter] to run setup flash.
Dump full Setup Data	Press [Enter] to dump full setup data to file.
Dump non-default Setup Data	Press [Enter] to dump non-default setup data to file.
Restore Setup Data	Press [Enter] to restore setup data from file.
FIXED BOOT ORDER	
Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	Press [Enter] to configure the boot order priority. By default, the server searches for boot devices in the following sequence: <ol style="list-style-type: none"> <li>1. Hard drive.</li> <li>2. CD-COM/DVD drive.</li> <li>3. USB device.</li> <li>4. Network.</li> <li>5. UEFI.</li> </ol>
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Application Boot Priorities	Press [Enter] to configure the boot priority.

# 5-7 Save & Exit Menu

The Save & Exit menu displays the various options to quit from the BIOS setup. Highlight any of the exit options then press <Enter>.



Parameter	Description
Save Options	
Save and Exit	Saves changes made and closes the BIOS setup. Options available: Yes, No.
Discard changes and exit	Discards changes made and exits the BIOS setup. Options available: Yes, No.
Save Changes and Reset	Restarts the system after saving the changes made. Options available: Yes, No.
Discard Changes and Reset	Restarts the system without saving any changes. Options available: Yes, No.
Save Changes	Saves changes done so far to any of the setup options. Options available: Yes, No.
Discard Changes	Discards changes made and closes the BIOS setup. Options available: Yes, No.
Default Options	

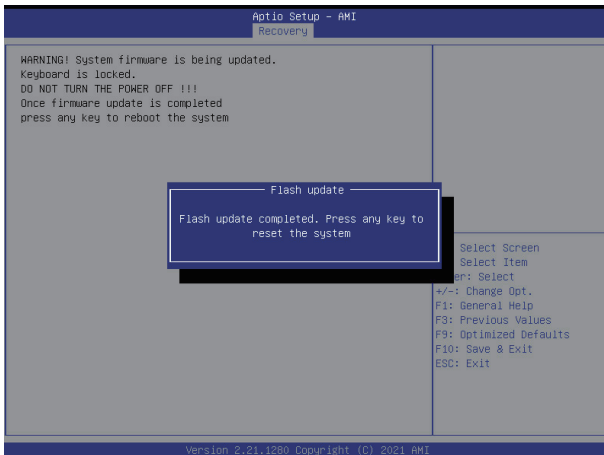
<b>Parameter</b>	<b>Description</b>
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly. Options available: Yes, No.
Save the User Default Values	Saves the changes made as the user default settings. Options available: Yes, No.
Restore the User Default Values	Loads the user default settings for all BIOS setup parameters. Options available: Yes, No.
Boot Device Priority	Press [Enter] to configure the device as the boot-up drive.
Launch EFI Shell	Attempts to Launch EFI Shell application (Shell.efi) from one of the available file system devices.

# 5-8 BIOS Recovery

The system has an embedded recovery technique. In the event that the BIOS becomes corrupt the boot block can be used to restore the BIOS to a working state. To restore your BIOS, please follow the instructions listed below:

Recovery Instruction:

1. Copy the XXX.rom to USB diskette.
2. Setting BIOS Recovery jump to enabled status.
3. Boot into BIOS recovery.
4. Run Proceed with flash update.
5. BIOS updated.





Designed by

**GIGA  
COMPUTING**