

GIGABYTE™

G593-SD1-AAX3

HPC/AI Server - 5th/4th Gen Intel® Xeon® Scalable - 5U DP NVIDIA HGX™ H200 8-GPU

User Manual

Rev. 1.0

Copyright

© 2024 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 GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: <http://reseller.b2b.gigabyte.com>

For further technical assistance, please contact your GIGABYTE representative or visit <https://support.gigabyte.com/> to create a new support ticket

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email: server.grp@gigabyte.com

Conventions

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

	NOTE! Gives bits and pieces of additional information related to the current topic.
	CAUTION! Gives precautionary measures to avoid possible hardware or software problems.
	WARNING! Alerts you to any damage that might result from doing or not doing specific actions.

Server Warnings and Cautions

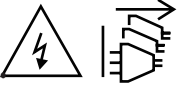
Before installing a server, be sure that you understand the following warnings and cautions.



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 all the power cords from the power supplies 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.



WARNING!

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



WARNING!

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



WARNING!

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.



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.

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 any component and pin touching. 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.

System power on/off: To remove power from system, you must remove the system from rack. 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 and disconnect the cables attached to the system before servicing it. 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.

**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.

Table of Contents

Chapter 1 Hardware Installation	10
1-1 Installation Precautions	10
1-2 Product Specifications	11
1-3 System Block Diagram	15
1-4 PCIe Block Diagram	16
Chapter 2 System Appearance	17
2-1 Front View	17
2-2 Rear View	18
2-3 Front Panel LED and Buttons	19
2-3-1 RoT LEDs	20
2-4 Front Panel System LAN LEDs	22
2-5 Power Supply Unit (PSU) LED	23
2-6 Hard Disk Drive LEDs	24
Chapter 3 System Hardware Installation	25
3-1 Removing and Installing the Chassis Top Cover	26
3-2 Removing and Installing the GPU Tray	27
3-3 Removing the Heat Sink	28
3-4 Installing the CPU	29
3-5 Installing the Memory	31
3-5-1 Eight Channel Memory Configuration	31
3-5-2 Installing the Memory	32
3-5-3 DIMM Population Table	33
3-5-4 Processor and Memory Module Matrix Table	33
3-6 Installing the PCI Expansion Card	34
3-7 Installing the Hard Disk Drive	36
3-8 Replacing the System Fan Module	37
3-9 Removing and Installing the Power Supply	38
3-10 Installing the System into the Cabinet	39
3-11 Removing the System from the Cabinet	40
3-12 Cable Connection	42
3-12-1 Motherboard/Front IO Board to PCIe Board	42
3-12-2 Motherboard/Front IO Board to Rear Side FHHL Card Cable	44
3-12-3 Motherboard to PCIe Board and HDD Backplane Board	46

Chapter 4 Motherboard Components	48
4-1 Motherboard Components	48
4-2 Jumper Setting	50
4-3 G-SC Module	51
4-3-1 CDCG120	51
4-4 Backplane Board Storage Connector	52
4-4-1 CBPG680	52
Chapter 5 BIOS Setup	53
5-1 The Main Menu	55
5-2 Advanced Menu	58
5-2-1 Trusted Computing	59
5-2-2 Serial Port Console Redirection	60
5-2-3 SIO Configuration	63
5-2-4 PCI Subsystem Settings	64
5-2-5 USB Configuration	66
5-2-6 Network Stack Configuration	67
5-2-7 Post Report Configuration	68
5-2-8 NVMe Configuration	69
5-2-9 Chipset Configuration	70
5-2-10 Tls Auth Configuration	72
5-2-11 iSCSI Configuration	73
5-2-12 Intel(R) Ethernet Controller X710 for 10GBASE-T	74
5-2-13 VLAN Configuration	76
5-2-14 Driver Health	77
5-3 Chipset Menu	78
5-3-1 Processor Configuration	79
5-3-2 Common RefCode Configuration	82
5-3-3 UPI Configuration	83
5-3-4 Memory Configuration	85
5-3-5 IIO Configuration	88
5-3-6 Advanced Power Management Configuration	90
5-3-7 PCH Configuration	93
5-3-8 Miscellaneous Configuration	95
5-3-9 Server ME Configuration	96
5-3-10 Runtime Error Logging Settings	97
5-3-11 Power Policy	99
5-4 Server Management Menu	101
5-4-1 System Event Log	103
5-4-2 View FRU Information	104

5-4-3	BMC VLAN Configuration	105
5-4-4	BMC Network Configuration	106
5-4-5	IPv6 BMC Network Configuration	107
5-5	Security Menu	108
5-5-1	Secure Boot	109
5-6	Boot Menu	112
5-7	Save & Exit Menu	114
5-8	BIOS Recovery	116
5-9	BIOS POST Beep code (AMI standard)	117
5-9-1	PEI Beep Codes	117
5-9-2	DXE Beep Codes	117

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 user manual 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"> ◆ 5U ◆ 447 x 219.7 x 945 (W x H x D, mm)
	CPU	<ul style="list-style-type: none"> ◆ 5th Generation Intel® Xeon® Scalable Processors ◆ 4th Generation Intel® Xeon® Scalable Processors ◆ Intel® Xeon® CPU Max Series ◆ Dual processor, TDP up to 350W <p>NOTE: If only 1 CPU is installed, some PCIe or memory functions might be unavailable</p>
	Socket	<ul style="list-style-type: none"> ◆ 2 x LGA4677 ◆ Socket E
	Chipset	<ul style="list-style-type: none"> ◆ Intel® C741
	Security	<ul style="list-style-type: none"> ◆ UEFI Secure Boot ◆ Silicon root of trust (Option) ◆ SNMP Support: V3
	Memory	<ul style="list-style-type: none"> ◆ 32 x DIMM slots ◆ DDR5 memory supported only ◆ 8-Channel memory architecture ◆ RDIMM up to 96GB supported ◆ 3DS RDIMM up to 256GB supported ◆ 5th Gen Intel® Xeon®: Up to *5600 MT/s (1DPC), 4400 MT/s (2DPC) ◆ 4th Gen Intel® Xeon®: Up to 4800 MT/s (1DPC), 4400 MT/s (2DPC) ◆ Intel® Xeon® Max Series: Up to 4800 MT/s (1DPC), 4400 MT/s (2DPC) <p>*5600 MT/s support under 2DPC configuration requires verified memory and BIOS setup. Please refer to the QVL for more information.</p>
	LAN	<p>Front side:</p> <ul style="list-style-type: none"> ◆ 2 x 10Gb/s LAN ports (1 x Intel® X710-AT2) ◆ Support NCSI function ◆ 1 x 10/100/1000 Mbps Management LAN <p>Rear side:</p> <ul style="list-style-type: none"> ◆ 1 x 10/100/1000 Mbps Management LAN <p>Notice: When both MLAN ports are connected with cables, the front MLAN port will be set as the default.</p>

 Video	<ul style="list-style-type: none"> ◆ Integrated in Aspeed® AST2600 - 1 x VGA port
 Storage	<p>Front side:</p> <ul style="list-style-type: none"> ◆ 8 x 2.5" Gen5 NVMe/SATA/SAS-4* hot-swappable bays, NVMe from PEX89104 <p>*SAS card is required to support SAS drives</p>
 SAS	<ul style="list-style-type: none"> ◆ Require SAS add-in cards
 RAID	<ul style="list-style-type: none"> ◆ Intel® SATA RAID 0/1/10/5 ◆ Support optional RAID add-in cards
 Expansion Slot	<ul style="list-style-type: none"> ◆ NVIDIA HGX™ H200 with 8 x SXM5 GPUs ◆ Extension Board CPBG044 x 2: - 8 x PCIe x16 (Gen5 x16) low-profile slots, from PEX89104 ◆ Riser Card CPBGD20 x 2: - 4 x PCIe x16 (Gen5 x16) FHHL slots, from PEX89048
 Internal I/O	<ul style="list-style-type: none"> ◆ 1 x TPM header ◆ 1 x VROC connector
 Front I/O	<ul style="list-style-type: none"> ◆ 2 x USB 3.2 Gen1 ◆ 1 x VGA ◆ 2 x RJ45 ◆ 1 x MLAN (default port) ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x NMI button ◆ 1 x Reset button ◆ 1 x Storage activity LED ◆ 1 x System status LED
 Rear I/O	<ul style="list-style-type: none"> ◆ 1 x MLAN
 Backplane I/O	<ul style="list-style-type: none"> ◆ Speed and bandwidth: PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s
 TPM	<ul style="list-style-type: none"> ◆ 1 x TPM header with SPI interface - Optional TPM2.0 kit: CTM010



Power Supply

- ◆ 4+2 3000W 80 PLUS Titanium redundant power supplies
 - ◆ AC Input:
 - 115-127V~/ 14.2A, 50-60Hz
 - 200-220V~/ 15.8A, 50-60Hz
 - 220-240V~/ 14.9A, 50-60Hz
 - ◆ DC Input: (Only for China)
 - 240Vdc/ 14A
 - ◆ DC Output:
 - Max 1450W/ 115-127V~
 - +54V/ 26.6A
 - +12Vsb/ 3A
 - Max 2900W/ 200-220V~
 - +54V/ 53.4A
 - +12Vsb/ 3A
 - Max 3002.4W/ 220-240V~ or 240Vdc Input
 - +54V/ 55.6A
 - +12Vsb/ 3A

NOTE:

- ◆ The system power supply requires C19 type power cord
- ◆ The power supply specifications provided herein is for the default server configuration. Different SKUs have different PSU specs, so please see the system rating label on the server for the accurate PSU specification.



System Management

Aspeed® AST2600 Baseboard Management Controller
GIGABYTE Management Console web interface

- ◆ Dashboard
- ◆ HTML5 KVM
- ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)
- ◆ Sensor Reading History Data
- ◆ FRU Information
- ◆ SEL Log in Linear Storage / Circular Storage Policy
- ◆ Hardware Inventory
- ◆ Fan Profile
- ◆ System Firewall
- ◆ Power Consumption
- ◆ Power Control
- ◆ Advanced power capping
- ◆ LDAP / AD / RADIUS Support
- ◆ Backup & Restore Configuration
- ◆ Remote BIOS/BMC/CPLD Update
- ◆ Event Log Filter
- ◆ User Management
- ◆ Media Redirection Settings
- ◆ PAM Order Settings
- ◆ SSL Settings
- ◆ SMTP Settings



System Fans

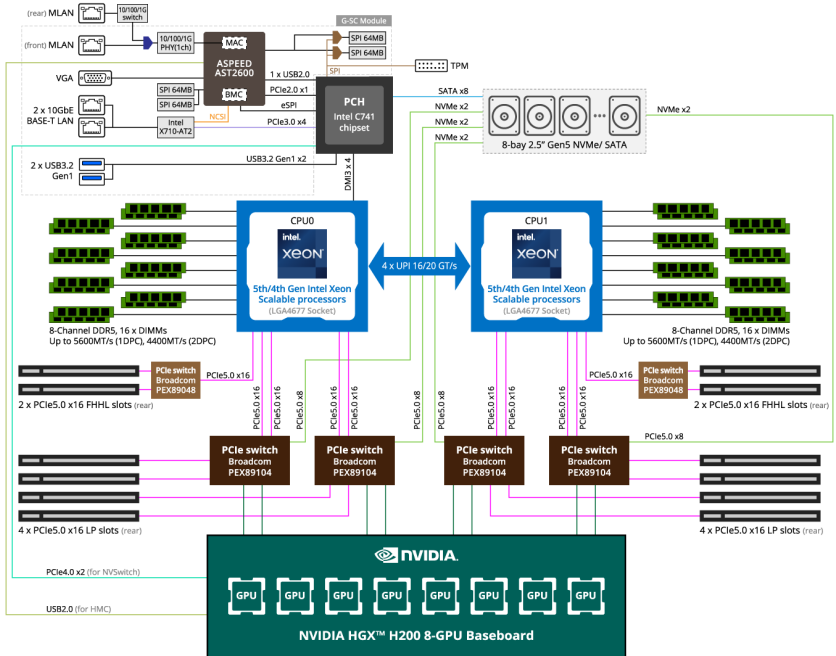
- ◆ Motherboard:
 - 2 x 40x40x28mm (25,000rpm)
 - 4 x 60x60x56mm (24,000rpm)
- ◆ PCIe slots:
 - 4 x 40x40x28mm (25,000rpm)
 - 2 x 40x40x56mm (32,000rpm)
- ◆ GPU tray:
 - 6 x 60x60x76mm (21,700rpm)
 - 11 x 80x80x80mm (17,000rpm)



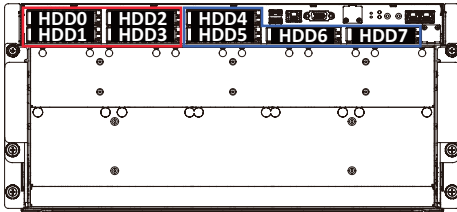
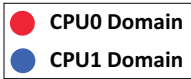
Operating Properties

- ◆ 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)

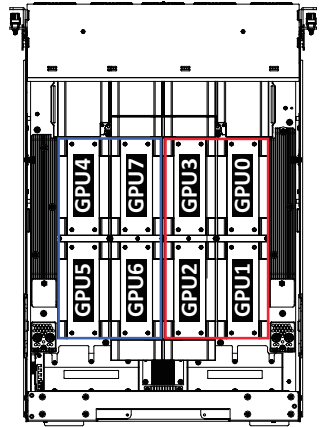
1-3 System Block Diagram



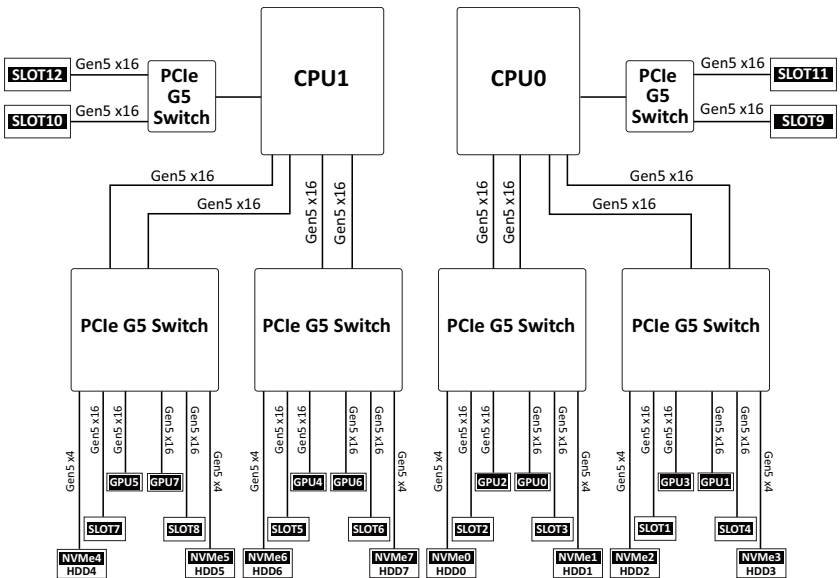
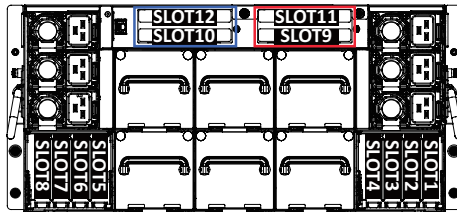
1-4 PCIe Block Diagram



Front Side

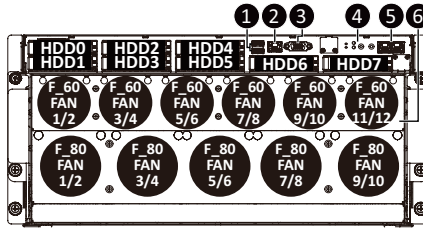


Rear Side



Chapter 2 System Appearance

2-1 Front View

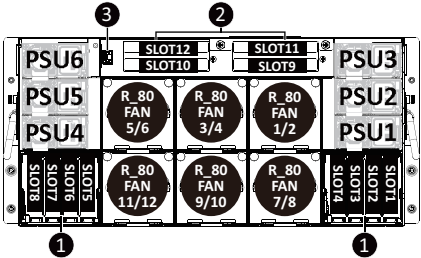


No.	Description
1.	USB 3.2 Gen1 Port x 2
2.	Management LAN Port
3.	VGA Port
4.	Front Panel LEDs and Buttons
5.	Data LAN Port x 2
6.	GPU Tray
NOTE! Drives with green latches support NVMe.	



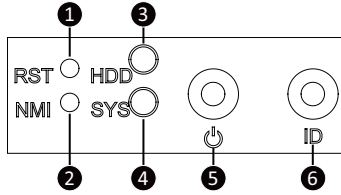
- Go to the section **2-3 Front Panel Buttons and LEDs** for detail description of function LEDs.

2-2 Rear View



No.	Description
1.	PCIe Card Cage x 2
2.	PCIe Slot x 4
3.	Management LAN Port

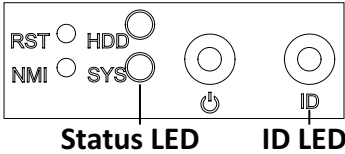
2-3 Front Panel LED and Buttons



No.	Name	Color	Status	Description
1.	Reset Button			Press the button to reset the system.
2.	NMI button			Press the button server generates a NMI to the processor if the multiple-bit ECC errors occur, which effectively halt the server.
3.	HDD Status LED	Green	On	HDD locate
			Blink	HDD access
		Amber	On	HDD fault
			Blink	HDD rebuilding
		N/A	Off	No HDD access or no HDD fault.
4.	System Status LED ^(Note)	Green	On	System is operating normally.
			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
5.	Power button with LED	Green	On	System is powered on
		N/A	Off	System is not powered on or in ACPI S5 state (power off)
6.	ID Button ^(Note)			Press the button to activate system identification

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

2-3-1 RoT LEDs



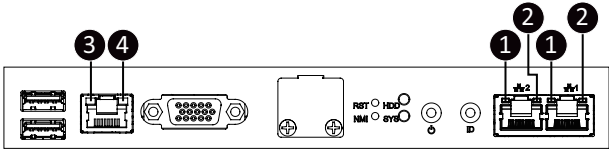
	LED on Front panel ^(Note5)	
	ID LED	Status LED
EC Firmware (FW) Authentication fail or not exit		
EC FW is broken or not exit ^(Note1)	OFF	OFF
Authenticating/Recovering BMC/BIOS Images		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per second
Recovering BIOS Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per second
Authentication (AUTH) Pass		
Recovering BIOS Active Flash	OFF	OFF
BMC : AUTH pass after doing recovery	OFF	OFF
BIOS : AUTH pass after doing recovery	OFF	OFF
BMC : AUTH pass	OFF	OFF
BIOS : AUTH pass	OFF	OFF
BMC : AUTH pass after doing recovery	OFF	OFF
BIOS : AUTH pass after doing recovery	OFF	OFF
Active Flash Authentication (AUTH) Fail		
BMC : AUTH Fail ^(Note2)	Blinks Blue 1 time per second	Blinks Green 1 time per second
BIOS : AUTH fail ^(Note2)	Blinks Blue 1 time per second	Blinks Amber 1 time per second

BMC : AUTH fail after doing recovery^(Note3)	Blinks Blue 2 times per second [ON OFF OFF]	Blinks Green 2 times per second [ON OFF OFF]
BIOS : AUTH fail after doing recovery^(Note3)	Blinks Blue 2 times per second [ON OFF OFF]	Blinks Amber 2 times per second [ON OFF OFF]
Backup Flash Authentication Fail^(Note4)		
BMC : AUTH fail	Blinks Blue 2 times per second [ON OFF ON OFF]	Blinks Green 2 times per second [ON OFF ON OFF]
BIOS : AUTH fail	Blinks Blue 2 times per second [ON OFF ON OFF]	Blinks Amber 2 times per second [ON OFF ON OFF]

NOTE!

1. EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
2. (1) Authentication fail include below scenarios
Configuration table is missing or modified
Public key is missing or modified
Protected area or signature is modified
Flash empty
3. If active flash is still authentication failed after recovery sequence, Microchip CEC1702 stop the process and showing LED behavior.
4. If backup flash authentication is failed cause by configuration table, public key or protected area is broken. Microchip CEC1702 stop the process and showing LED behavior.
5. Front panel LED is controlled by BMC or Microchip CEC1702. Once Microchip CEC1702 is working(Auth or recovery), the front panel LED is controlled by Microchip CEC1702 and vice versa.

2-4 Front Panel System LAN LEDs



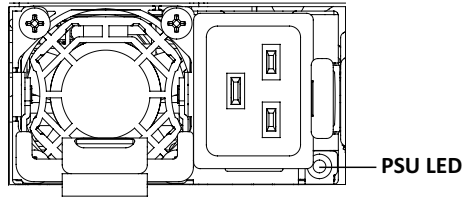
No.	Name	Color	Status	Description
1.	10GbE Speed LED	Green	On	10 Gbps data rate
		Yellow	On	5Gbps, 2.5Gbps, 1Gbps data rate
		N/A	Off	100 Mbps data rate
2.	10GbE Link / Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or reception is occurring.
		N/A	Off	No data transmission or reception is occurring.
3.	1GbE Speed LED	Yellow	On	1 Gbps data rate
		Green	On	100 Mbps data rate
		N/A	Off	10 Mbps data rate
4.	1GbE Link / Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or reception is occurring.
		N/A	Off	No data transmission or reception is occurring.

2-5 Power Supply Unit (PSU) LED



NOTE!

The power supply may vary based on the system configuration.



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

2-6 Hard Disk Drive LEDs



RAID SKU		LED1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via PCH, 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 electrostatic discharge. 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 Top Cover



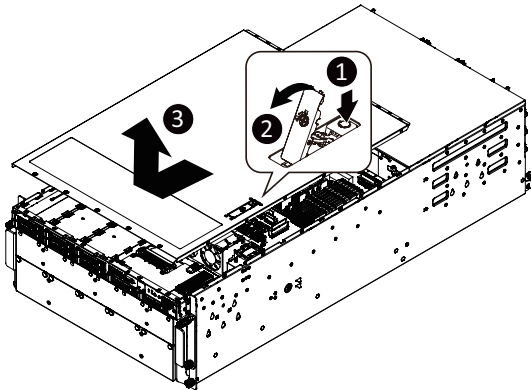
Before you remove or install the chassis top cover

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

Follow these instructions to remove/install the chassis top cover:

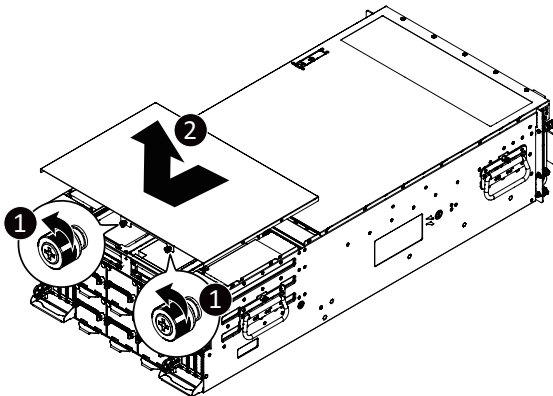
Front Cover

1. Push button to unlock the handle.
2. Pull the grip handle to open the panel cover.
3. Slide the cover towards the front of the system and then remove the cover in the direction indicated by the arrow.
4. Follow steps 1-3 in reverse order to re-install the front top cover



Rear Cover

1. Loosen the two thumbail screws securing the chassis cover.
2. Slide the cover towards the rear of the system and then remove the cover in the direction indicated by the arrow.
3. Follow steps 1-2 in reverse order to re-install the rear top cover



3-2 Removing and Installing the GPU Tray

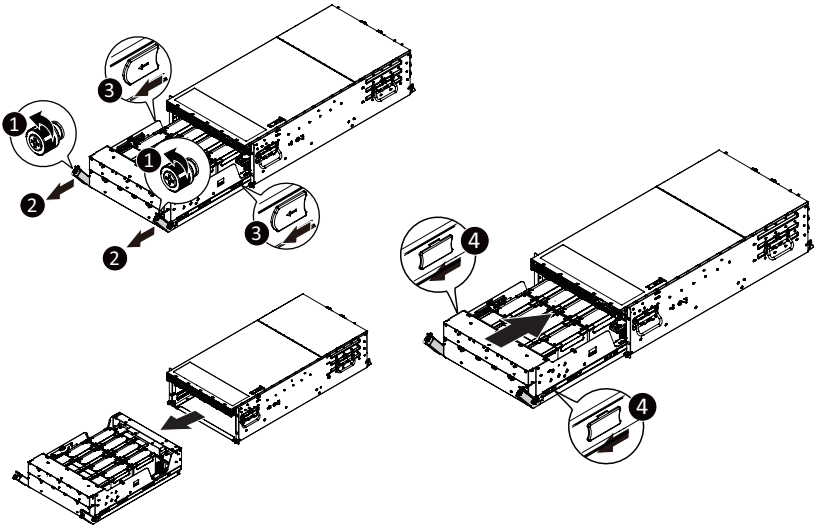


Before you remove or install the GPU tray:

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

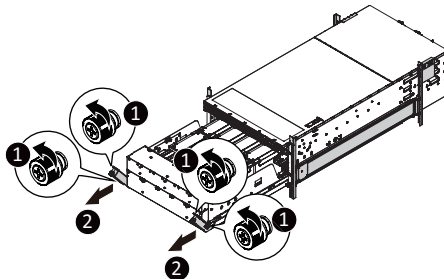
Follow these instructions to remove/install the GPU tray:

1. Loosen the top thumbnail screw securing the handles on both sides of the system.
2. Pull the grip handles on both sides of the system slide the tray to the front of the system at the same time to pull out the tray.
3. Slide the white latch on both sides of the tray rail and carefully remove the GPU tray.
4. To reinstall the GPU tray, align it with the rails on both sides and push the blue latches on each side of the tray rail backward to slide it into the system. Then, reverse steps 1-2 to secure the GPU tray in position.



System in the cabinet

1. Loosen the thumbnail screws securing the handles on both sides of the system.
2. Pull the grip handles on both sides of the system slide the tray to the front of the system at the same time to remove the tray.
3. Follow steps 1-2 in reverse order to re-install the GPU tray.



3-3 Removing the Heat Sink



Read the following guidelines before you begin to remove/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.

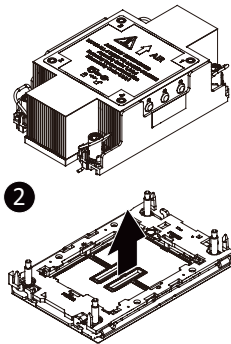
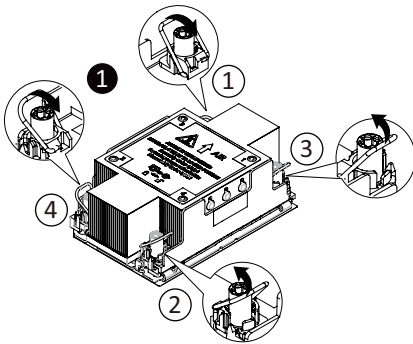


WARNING!

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 remove/install the heat sink:

1. Loosen the captive screws securing the heat sink in place in reverse order (4→3→2→1). Move the rotating wires into the unlatch position.
2. Lift and remove the heat sink from the system.
3. To reinstall the heat sink reverse steps 1-2 while ensuring that you tighten the captive screws in sequential order (1→2→3→4).



- When installing the heat sink to CPU, use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4. Please refer to the Heatsink Label for the screw tightening torque value.
- To ensure the system operates properly, make sure the heat sink is seated on the processor firmly.

3-4 Installing the CPU



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.

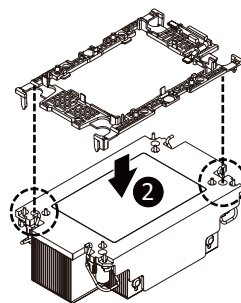
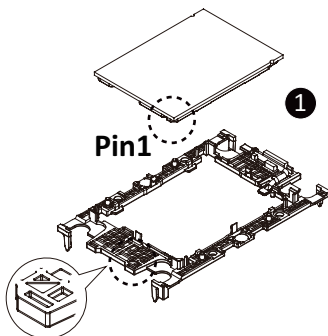


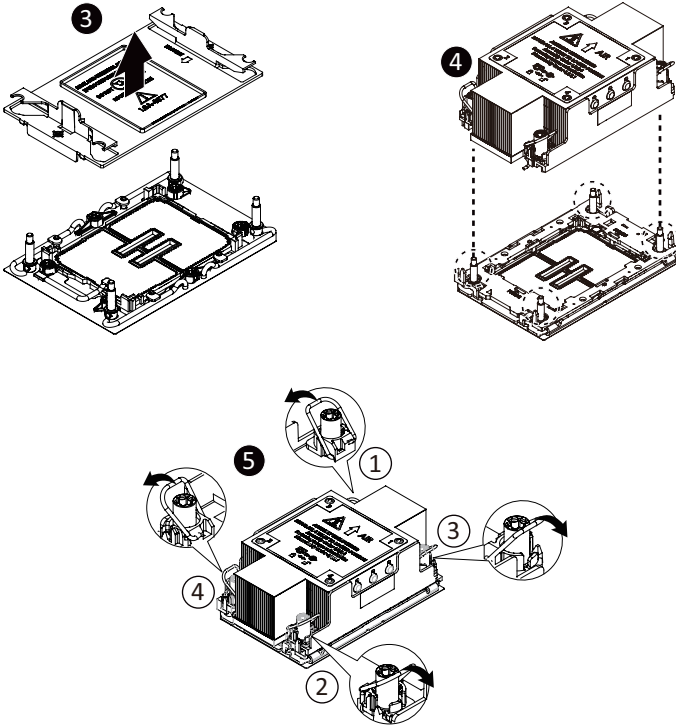
WARNING!

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 and install the processor on the carrier.
NOTE: Apply thermal compound evenly on the top of the CPU. Remove the protective cover from the underside of the heat sink.
2. Carefully flip the heat sink cover. Then install the carrier assembly on the bottom of the heat sink and make sure the gold arrow is located in the correct direction.
3. Remove the CPU cover.
NOTE: Save the CPU cover in the event that you need to remove the CPU from the socket.
4. Align the heat sink with the CPU socket by the guide pins and make sure the gold arrow is located in the correct direction. Then place the heat sink onto the top of the CPU socket.
5. Position the rotating wires into the latch position. Tighten the screws in sequential order (1→2→3→4).
NOTE: When disassembling the heat sink, loosen the screws in reverse order (4→3→2→1) and then move the rotating wires into the unlatch position.





Carrier Types used for Package Types

Package Type	Xeon® SP XCC	Xeon® SP MCC	Xeon® SP+HBM
Carrier Code	E1A	E1B	E1C

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.
- Please refer to the Heatsink Label for the screw tightening torque value.

3-5 Installing the Memory

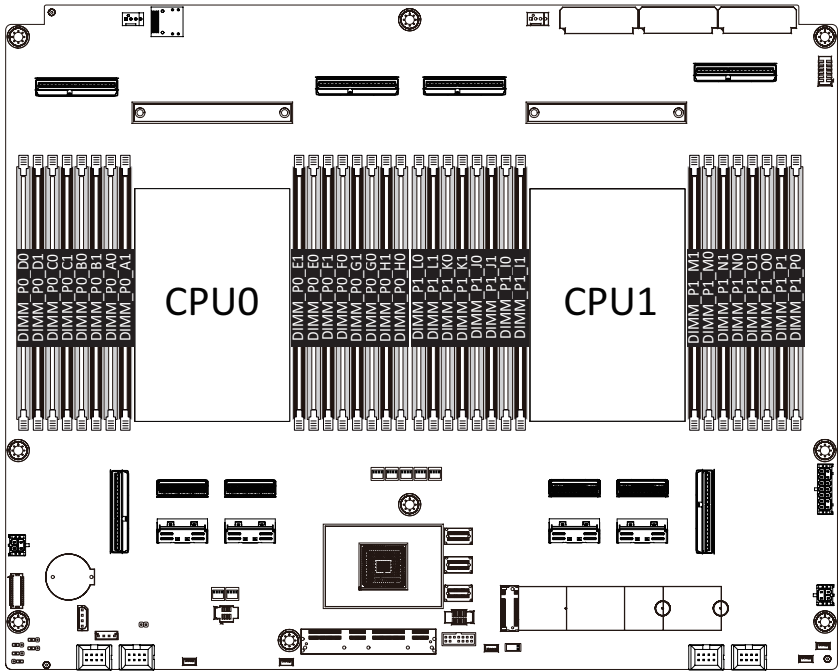


Read the following guidelines before you begin to install the memory:

- 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.

3-5-1 Eight Channel Memory Configuration

This motherboard provides 32 DDR5 memory slots and supports 8-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



3-5-2 Installing the Memory



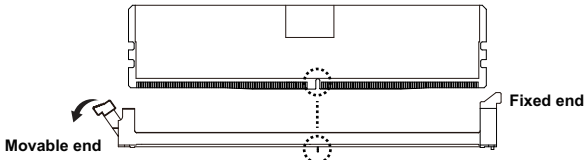
Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR5 DIMMs on this motherboard.

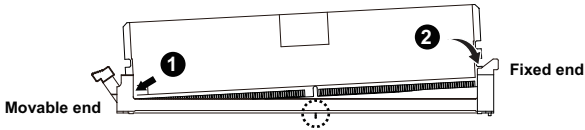
Make sure your DIMM slots have a single latch or a double latch.

Follow these instructions to install a DIMM module with Single Latch :

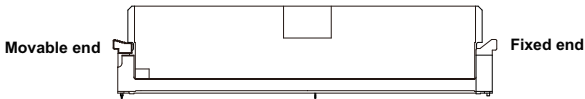
1. Open the plastic latch of the memory slot, then place the memory module as pre-inserted vertically position.



2. Hold it with both hands, insert the memory module into the movable end first, and then insert the memory module into the fixed end.



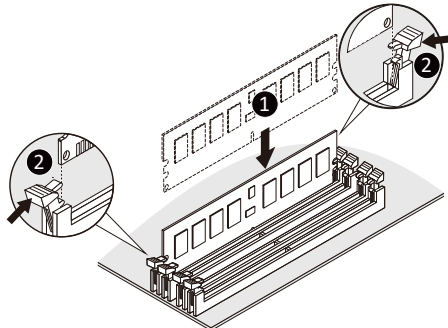
3. Then use both hands to insert the memory module vertically into the DIMM slot and push it down. Close the plastic latch at the edge of the DIMM slots to lock the memory module.



4. Reverse the installation steps when you want to remove the memory module.

Follow these instructions to install a DIMM module with Double Latch:

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.



3-5-3 DIMM Population Table

4th Gen Intel Xeon Scalable Processors Memory Support

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); DIMM per Channel (DPC)	
		16Gb	24Gb ²	36Gb	1DPC ¹	2DPC
		1.1V				
RDIMM	SRx8 (RC D)	16GB	24GB	NA	4800	4400
	SRx4 (RC C)	32GB	48GB	NA		
	SRx4 (RC F) 9x4	32GB	NA	NA		
	DRx8 (RC E)	32GB	48GB	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
RDIMM 3DS	(4R/8R)x4 (RC A)	2H-128GB 4H-256GB	NA	NA		

NOTE:

- 1DPC applies to 1SPC or 2SPC implementations (SPC - Sockets Per Channel)
- 24Gb XCC only w/ limited configs: 1DPC all DIMM types, 2DPC 96GB only. Only 8 and 16 DIMM configs, no fallbacks.

5th Gen Intel Xeon Scalable Processors Memory Support

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); DIMM per Channel (DPC)	
		16Gb	24Gb ²	36Gb	1DPC ¹	2DPC
		1.1V				
RDIMM	SRx8 (RC D)	16GB	24GB	NA	5600 ³	4400 ³
	SRx4 (RC C)	32GB	48GB	NA		
	SRx4 (RC F) 9x4	NA	NA	NA		
	DRx8 (RC E)	32GB	48GB	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
RDIMM 3DS	(4R/8R)x4 (RC A)	2H-128GB 4H-256GB	NA	NA	5600 ⁴	

NOTE:

- 1DPC applies to 1SPC or 2SPC implementations (SPC - Sockets Per Channel)
- 24Gb 2DPC not POR w/ 24GB and 48GB DIMMs.
- DDR5-5600 RDIMMs will be limited to 5600 MT/s 1DPC and 4400 MT/s 2DPC. DDR5-4800 DIMMs will be limited to 4800 MT/s 1DPC and 4400 MT/s 2DPC.
- DDR5-5600 DIMMs are required for 5600 and 5200 1DPC speeds.

3-5-4 Processor and Memory Module Matrix Table

Memory Q'ty for each CPU	CPU0														CPU1																	
	D0	D1	C0	C1	B0	B1	A0	A1	E1	E0	F1	F0	G1	G0	H1	H0	L0	L1	K0	K1	J0	J1	I0	I1	M1	M0	N1	N0	O1	O0	P1	P0
1 DIMM		v					v																	v								
2 DIMM							v							v										v						v		
4 DIMM			v				v		v				v						v				v		v				v			
6 DIMM	v		v				v		v	v			v				v		v				v		v		v		v			
8 DIMM	v	v	v	v			v		v	v	v		v				v	v	v	v			v		v		v		v	v	v	
12 DIMM	v	v	v	v	v		v	v	v	v	v		v	v			v	v	v	v	v		v	v	v	v	v	v	v	v	v	
16 DIMM	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v		v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v

NOTE!

- There should be at least one DDR5 DIMM per socket.

3-6 Installing the PCI Expansion Card

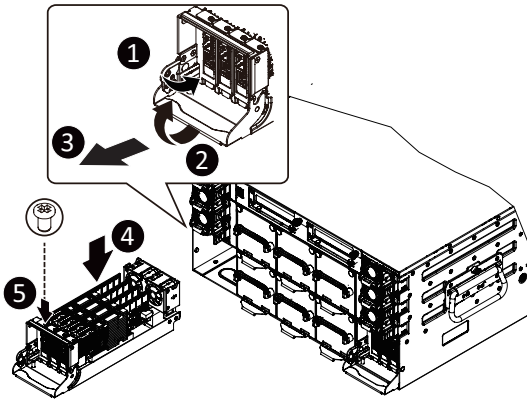


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to installing a PCIe card.
-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

Follow these instructions for a PCI Expansion card:

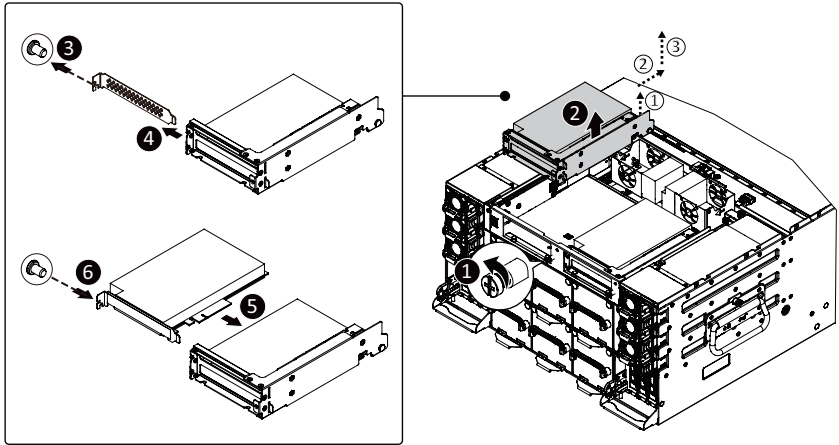
PCIe Card Cage

1. Press the release latch.
2. Simultaneously pulling up the tray handle for the PCIe card cage.
3. Pull the cage out of the system.
4. Align the PCIe card onto the slot and push in the direction of the arrow until the PCIe card sits in the PCIe card connector.
5. Secure the PCIe card with the screw.
6. To install the PCIe card cage, push the cage back into the system. Reverse the previous steps to remove the PCI expansion card.



Rear System PCIe Card

1. Loosen the screw securing the riser bracket.
2. Gently lift the riser bracket. Then, move it backward and lift it upward.
3. Remove the screw securing the slot cover from the riser bracket.
4. Remove the slot cover from the riser bracket.
5. 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.
6. Secure the PCIe card with the screw.
7. Reverse the previous steps to install the riser bracket.



3-7 Installing the Hard Disk Drive

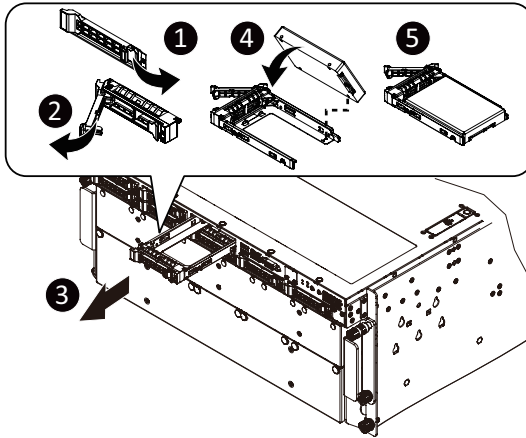


Read the following guidelines before you begin to install the hard disk drive:

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



3-8 Replacing the System Fan Module



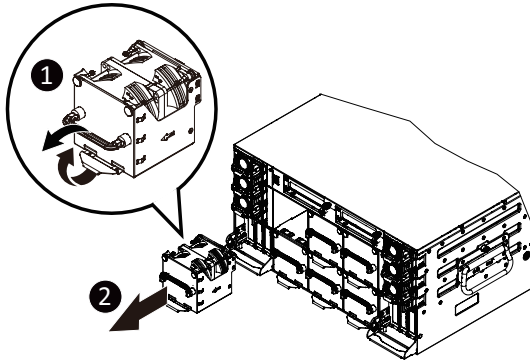
CAUTION!

Before you remove or install the system fans follow these steps:

- Disconnect all necessary cable connections. Failure to observe these warnings could result in personal injury or damage to the equipment

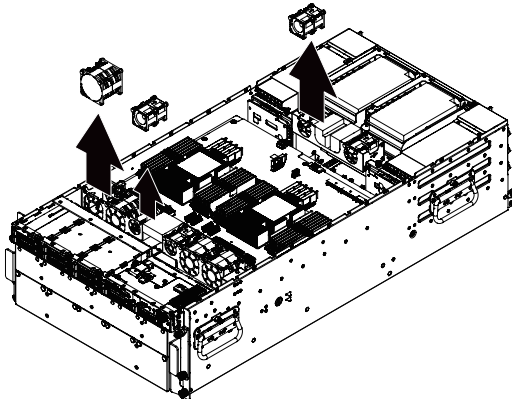
Follow these instructions to replace the fan assembly:

1. Flip and then grasp the handle and simultaneously press the retaining clip on the bottom side of the fan module in the direction indicated.
2. Pull out the fan module.
3. Reverse the previous steps to install the replacement fan module.



Internal System Fan

1. Lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



3-9 Removing and Installing the Power Supply

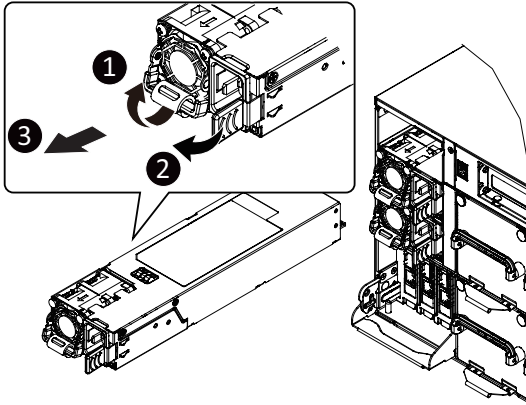


CAUTION!

Please see Section 2-2 "Rear View" for installation sequence.

Follow these instructions to replace the power supply:

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



3-10 Installing the System into the Cabinet

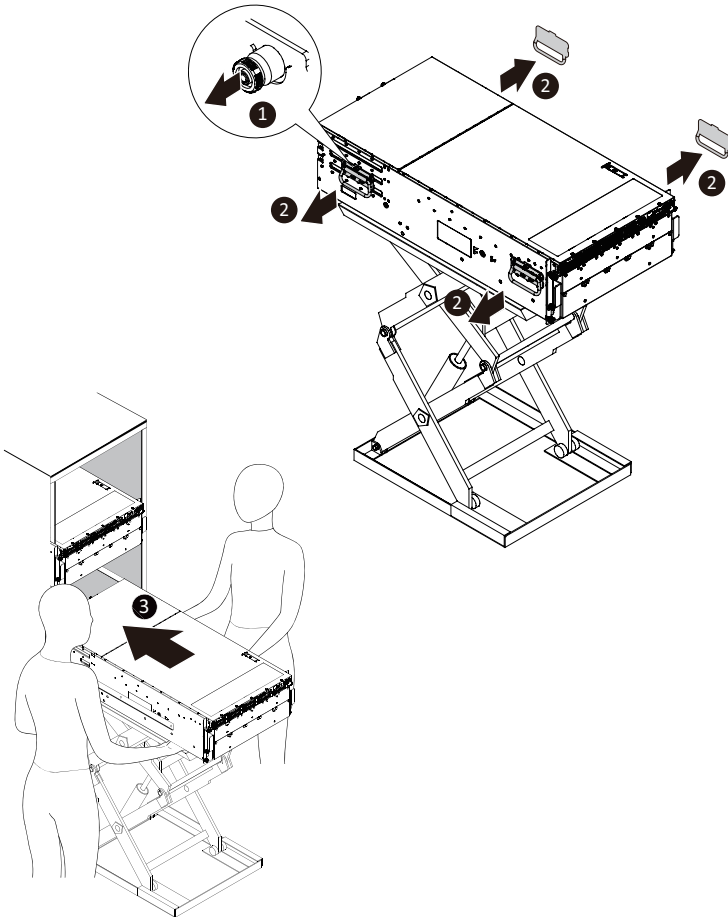


Read the following guidelines before you begin to install the system into the cabinet:

- Make sure the system is not turned on or connected to AC power.
- A Lift Table is required. Place the system unit on Lift Table.
- Four Person lift required. Firmly hold the bottom of the system when required to lift and carry the system.
- Failure to observe these warnings could result in personal injury or damage to the equipment.

Follow these instructions to install the system into the cabinet:

1. Pull out and release the thumbnail screw securing the chassis handle in place.
2. Remove the four handles on each side of the system.
3. Carefully slide the system into the cabinet.



3-11 Removing the System from the Cabinet

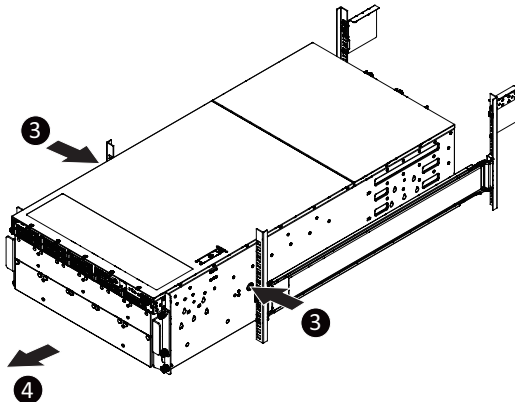
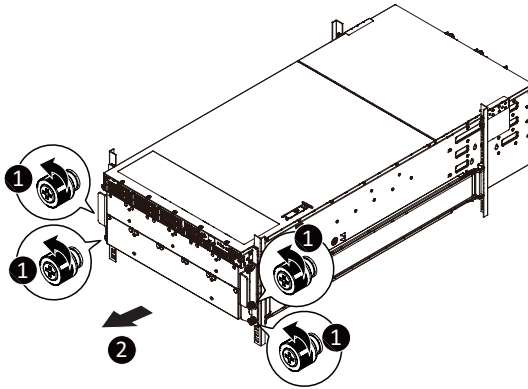


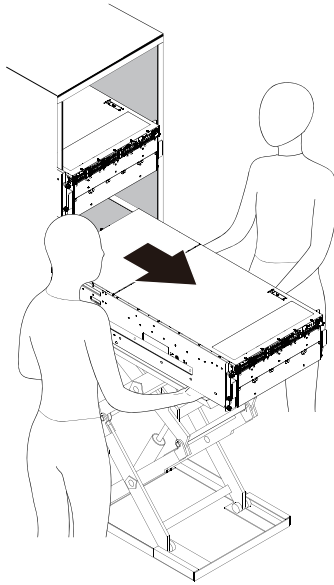
Read the following guidelines before you begin to remove the system from the cabinet:

- Always turn off the computer and unplug the power cord from the power outlet before removing the system from the cabinet.
- Disconnect all necessary cable connections.
- A Lift Table is required. Place the system unit on Lift Table.
- Four Person lift required. Firmly hold the bottom of the system when required to lift and carry the system.
- Failure to observe these warnings could result in personal injury or damage to the equipment.

Follow these instructions to remove the system from the cabinet:

1. Loosen the thumbnail screws on each side that secure the system.
2. Carefully pull out the system from the cabinet and stop at the security hook on the side of the system.
3. Push the button to unlock.
4. Gently pull out the system from the cabinet and place it on Lift table.



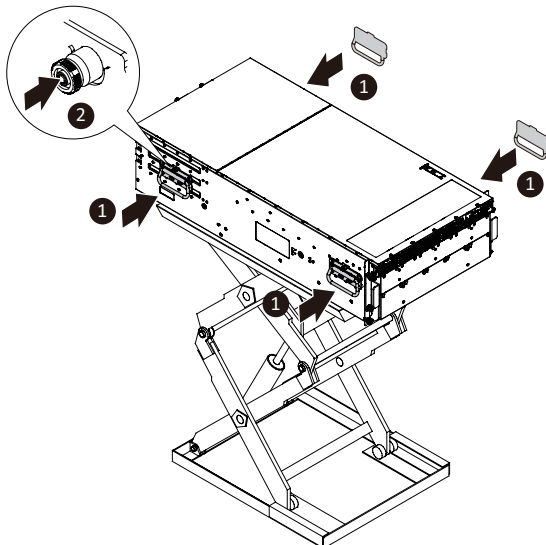


NOTE!

- Before lifting the system, installing the four chassis handles on the system is required.

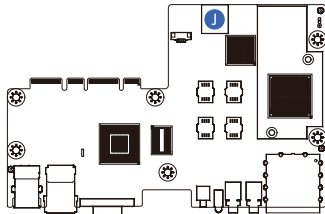
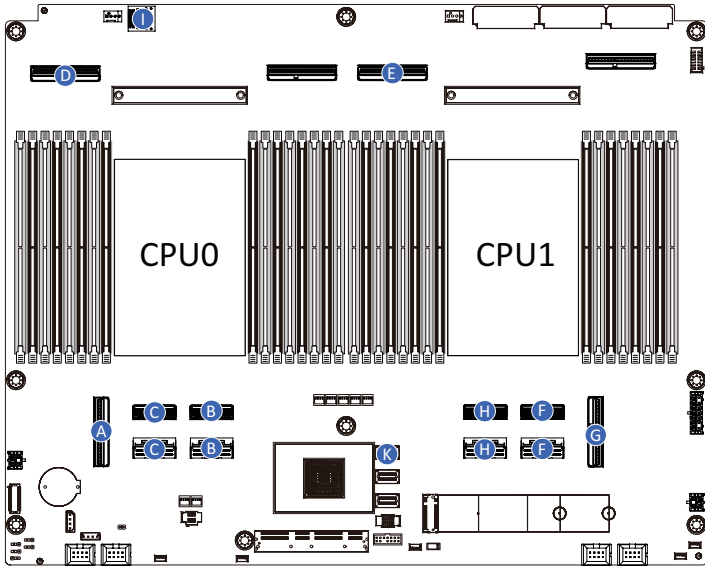
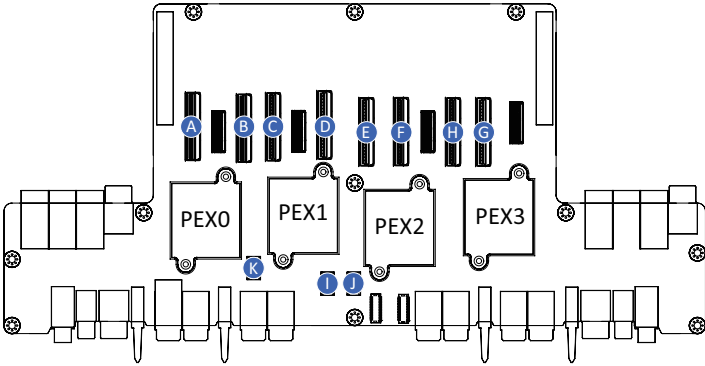
Follow these instructions to install the chassis handles on the system:

1. Attach the four chassis handles to the system.
2. Push and lock the thumbnail screw to secure the chassis handle in place.



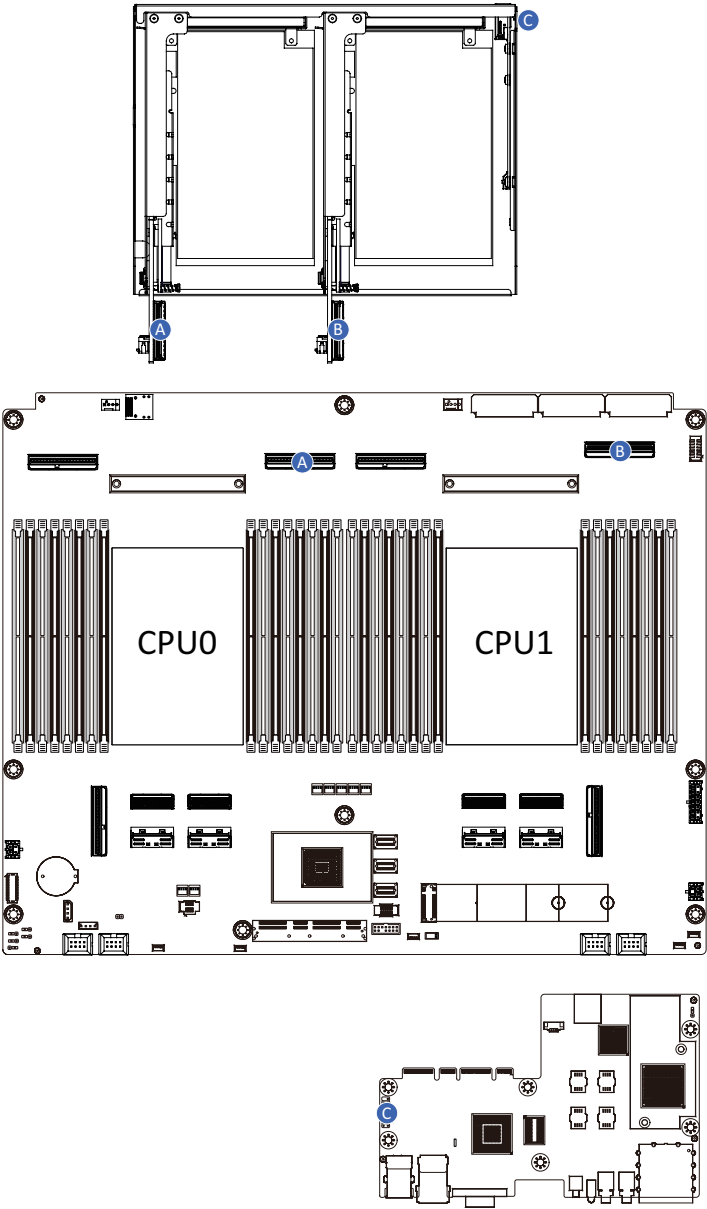
3-12 Cable Connection

3-12-1 Motherboard/Front IO Board to PCIe Board



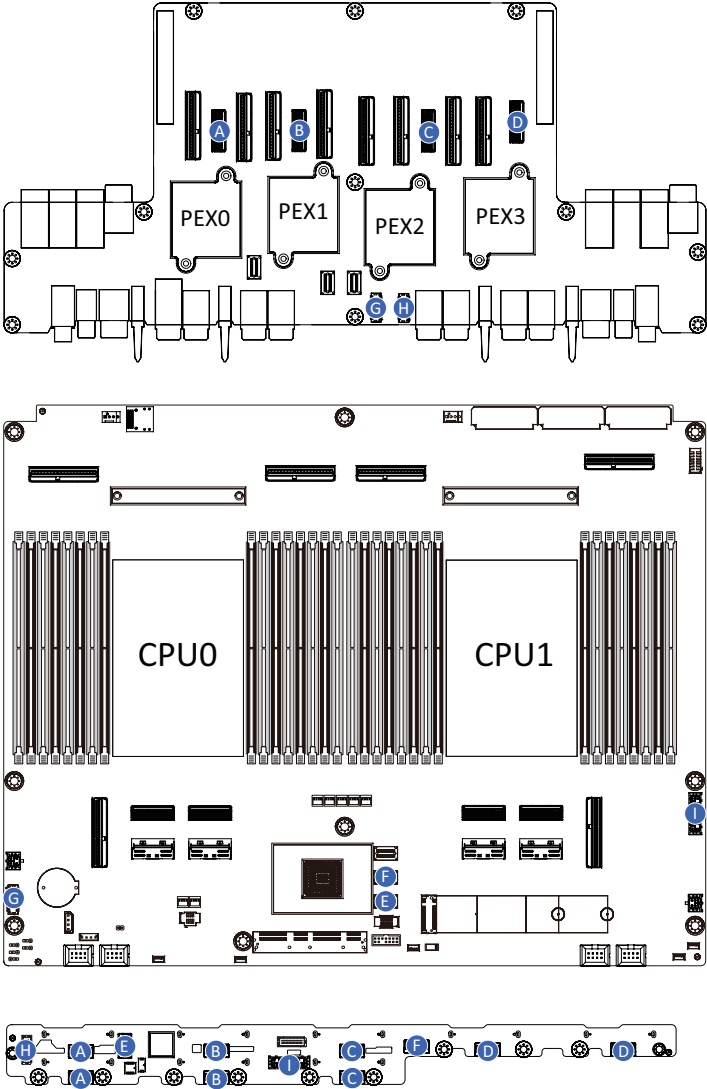
A	PCIe Slot Signal Cable	Motherboard: U2_P0_PE0
		PCIe Board: U2_PEX0A
B	PCIe Slot Signal Cable	Motherboard: U2_P0_PE2A/ U2_P0_PE2B
		PCIe Board: U2_PEX0B
C	PCIe Slot Signal Cable	Motherboard: U2_P0_PE1A/ U2_P0_PE1B
		PCIe Board: U2_PEX1A
D	PCIe Slot Signal Cable	Motherboard: U2_P0_PE4
		PCIe Board: U2_PEX1B
E	PCIe Slot Signal Cable	Motherboard: U2_P1_PE4
		PCIe Board: U2_PEX2A
F	PCIe Slot Signal Cable	Motherboard: U2_P1_PE1A/U2_P1_PE1B
		PCIe Board: U2_PEX2B
G	PCIe Slot Signal Cable	Motherboard: U2_P1_PE2
		PCIe Board: U2_PEX3A
H	PCIe Slot Signal Cable	Motherboard: U2_P1_PE0A/U2_P1_PE0B
		PCIe Board: U2_PEX3B
I	Power Board Side Band Signal Cable	Motherboard: PDB_IO
		PCIe Board: PDB_IO
J	Baseboard Management Cable	PCIe Board: DELTA
		Front IO Board: DELTA
K	Baseboard Management Cable	Motherboard: U2_NVHS
		PCIe Board: U2_NVNS

3-12-2 Motherboard/Front IO Board to Rear Side FHHL Card Cable



A	PCIe Slot Signal Cable	Motherboard: U2_P0_PE3
		Riser Card: U2_1 (SLOT9/SLOT11)
B	PCIe Slot Signal Cable	Motherboard: U2_P1_PE3
		Riser Card: U2_1 (SLOT10/SLOT12)
C	Rear Side MLAN Cable	Front IO Board: REAR_LAN
		Rear MLAN

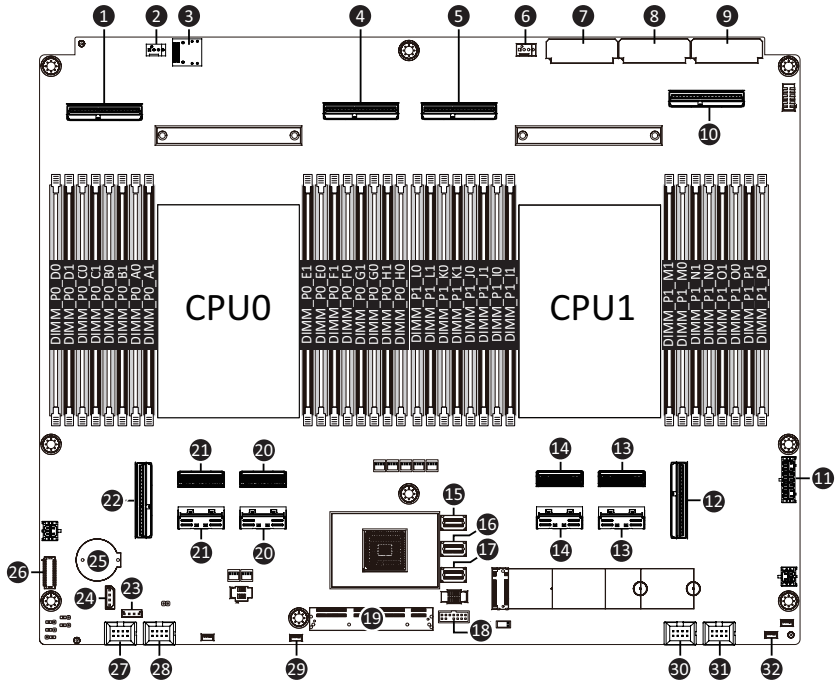
3-12-3 Motherboard to PCIe Board and HDD Backplane Board



A	NVMe Cable	PCIe Board: P0_NV
		Backplane Board: U_2_0/ U_2_1
B	NVMe Cable	PCIe Board: P1_NV
		Backplane Board: U_2_2/ U_2_3
C	NVMe Cable	PCIe Board: P2_NV
		Backplane Board: U_2_4/ U_2_5
D	NVMe Cable	PCIe Board: P3_NV
		Backplane Board: U_2_6/ U_2_7
E	SATA Cable	Motherboard: SL_CN1
		Backplane Board: SL_SAS0
F	SATA Cable	Motherboard: SL_CN2
		Backplane Board: SL_SAS1
G	Backplane Board Sideband Signal Cable	Motherboard: BP_1
		PCIe Board: BP_1
H	Backplane Board Sideband Signal Cable	PCIe Board: BP_SERIES
		Backplane Board: BP_1
I	Backplane Board Power Cable	Motherboard: HDD_PWR1
		Backplane Board: ATX1

Chapter 4 Motherboard Components

4-1 Motherboard Components



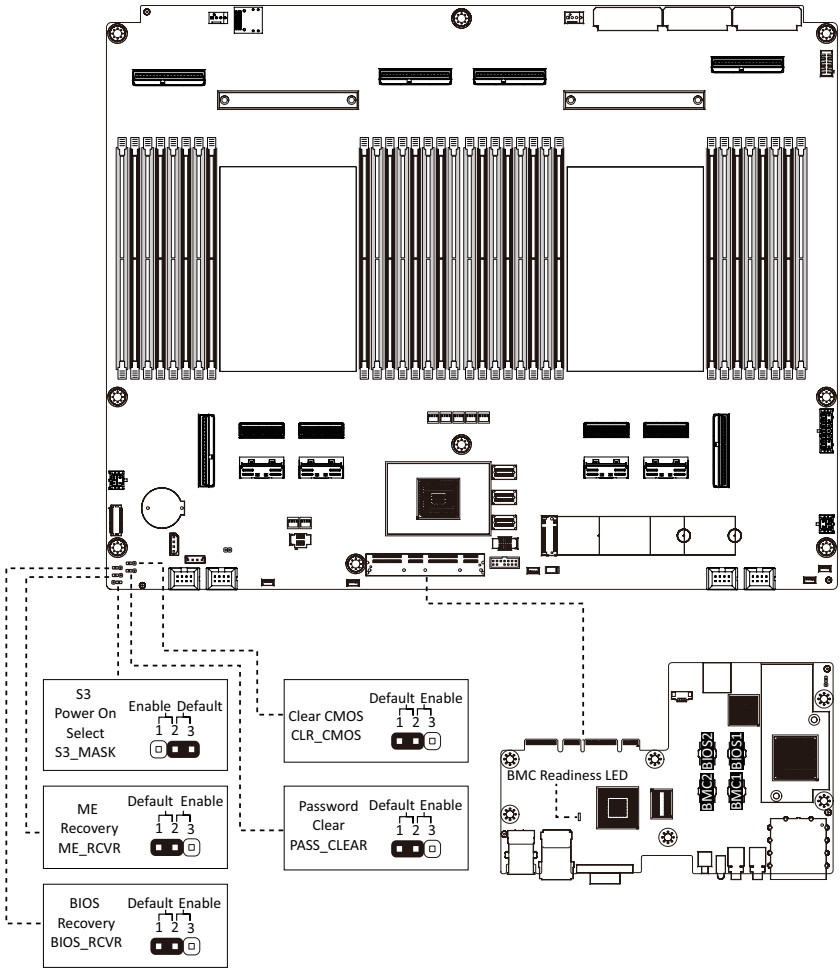
Item	Description
1	M.2 Connector (U2_P0_PE4/PCIe Gen5)
2	CPU0 Fan Connector (for CPU0 Heatsink)
3	SlimLine Connector (for Power Board Side Band Signal)
4	M.2 Connector* (U2_P0_PE3/PCIe Gen5)
5	M.2 Connector (U2_P1_PE4/PCIe Gen5)
6	CPU1 Fan Connector (for CPU1 Heatsink)
7	System Power Connector (PWR1)
8	System Power Connector (PWR2)
9	System Power Connector (PWR3)
10	M.2 Connector* (U2_P1_PE3/PCIe Gen5)
11	2 x 7 Pin HDD Backplane Board Power Connector
12	M.2 Connector (U2_P1_PE2/PCIe Gen5)
13	M.2 Connector (U2_P1_PE1B/U2_P1_PE1A/PCIe Gen5)
14	M.2 Connector (U2_P1_PE0B/U2_P1_PE0A/PCIe Gen5)
15	SlimLine Connector (for Delta Module Link)
16	SlimLine Connector (SATA #4 - #7)
17	SlimLine Connector (SATA #0 - #3)
18	TPM Module Connector
19	G-SC Module Connector

Item	Description
20	MCIO Connector (U2_P0_PE2A/U2_P0_PE2B/PCIe Gen5)
21	MCIO Connector (U2_P0_PE1A/U2_P0_PE1B/PCIe Gen5)
22	MCIO Connector (U2_P0_PE0/PCIe Gen5)
23	VROC Module Connector
24	IPMB Connector
25	Battery Socket
26	HDD Backplane Board Connector
27	FAN_1_2 Connector
28	FAN_3_4 Connector
29	FAN9 Connector
30	FAN_5_6 Connector
31	FAN_7_8 Connector
32	FAN11 Connector

NOTE!

*Base on CPU configuration

4-2 Jumper Setting

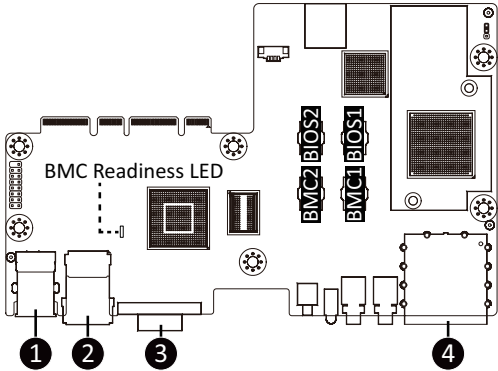


NOTE!

- **ME_RCVR:** Setting "ME_RCVR" to [2-3] will force the system's Management Engine into recovery mode. This allows the user to update the BIOS image, including the Management Engine region. Note that this jumper does not need to be set when using the Gigabyte BIOS update utility and SOP.
- **S3 Mask:** Reserve for development only.
- **BIOS Recovery** please refer to page 116.
- **CLR_CMOS** used to reset the BIOS settings of a computer to their default values.
- **PASS_CLEAR** used to clear or reset the BIOS password, which can be necessary if you've forgotten the password and need to regain access to the system.

4-3 G-SC Module

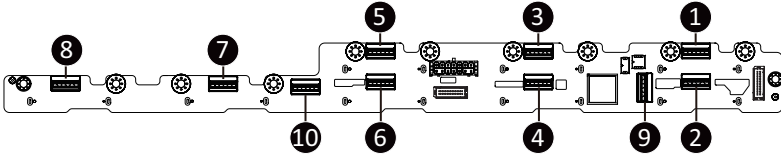
4-3-1 CDCG120



Item	Description
1	USB 3.2 Gen1 Port x 2
2	Management LAN Port
3	VGA Port
4	Data LAN Port x 2

4-4 Backplane Board Storage Connector

4-4-1 CBPG680



Item	Description
1.	MCIO 4i (SFF-TA-1016 / U_2_0)
2.	MCIO 4i (SFF-TA-1016 / U_2_1)
3.	MCIO 4i (SFF-TA-1016 / U_2_2)
4.	MCIO 4i (SFF-TA-1016 / U_2_3)
5.	MCIO 4i (SFF-TA-1016 / U_2_4)
6.	MCIO 4i (SFF-TA-1016 / U_2_5)
7.	MCIO 4i (SFF-TA-1016 / U_2_6)
8.	MCIO 4i (SFF-TA-1016 / U_2_7)
9.	MCIO 4i (SFF-TA-1016 / SL_SAS0)
10.	MCIO 4i (SFF-TA-1016 / SL_SAS1)

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 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 4 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

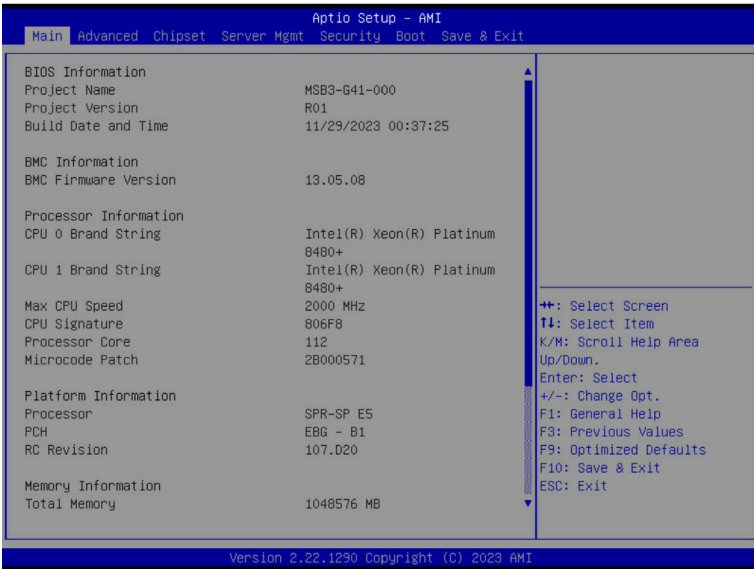
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

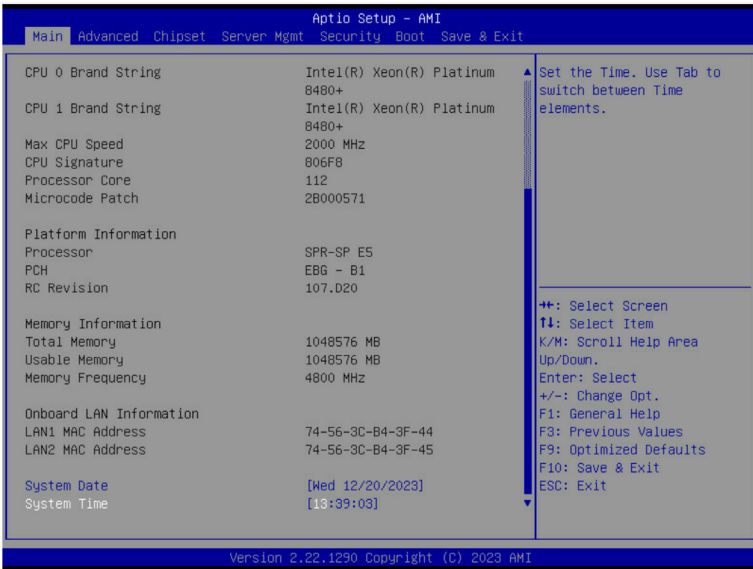
Submenu Help

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
BIOS Information	
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^(Note1)	
BMC Firmware Version ^(Note1)	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/ PCH/ RC Revision	Displays the information of the installed processor(s) and PCH.
Memory Information^(Note2)	
Total Memory	Displays the total memory size of the installed memory.
Usable Memory	Displays the usable memory size of the installed memory.

(Note1) Functions available on selected models.

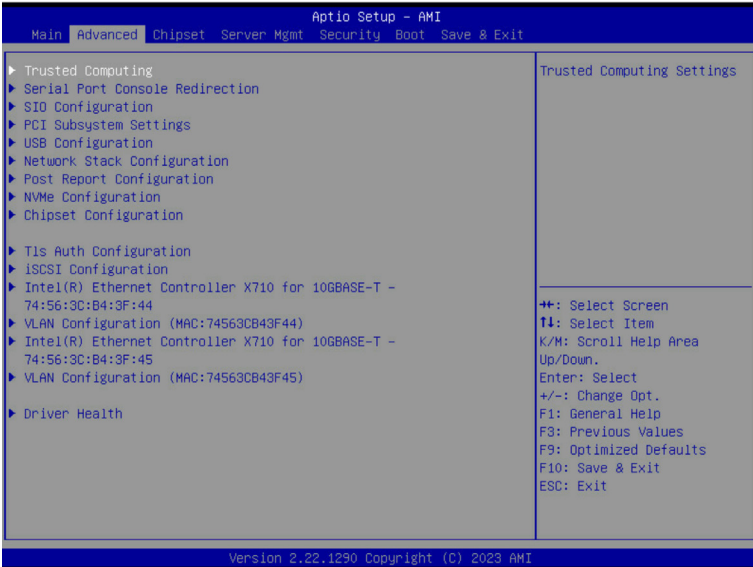
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

Parameter	Description
Memory Frequency	Displays the frequency information of the installed memory.
Onboard LAN Information ^(Note3)	
LAN# MAC Address	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

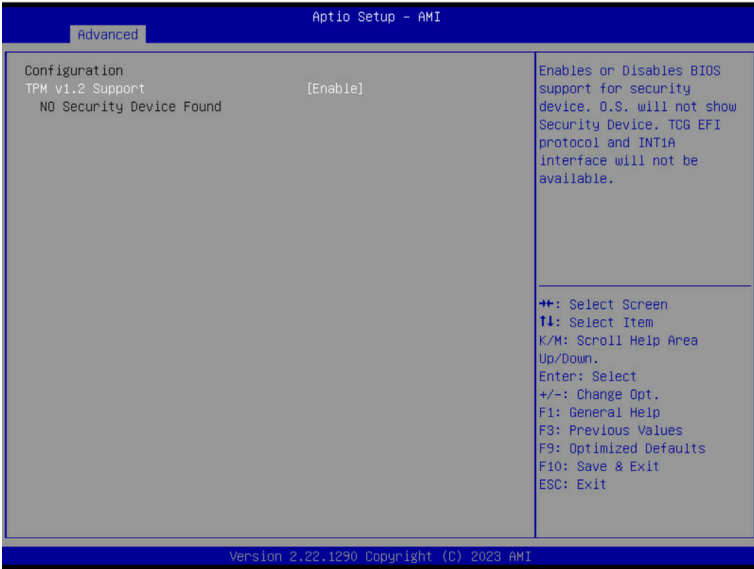
(Note3) The number of LAN ports listed will depend on the motherboard / system model.

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 Enable.</p>

5-2-2 Serial Port Console Redirection



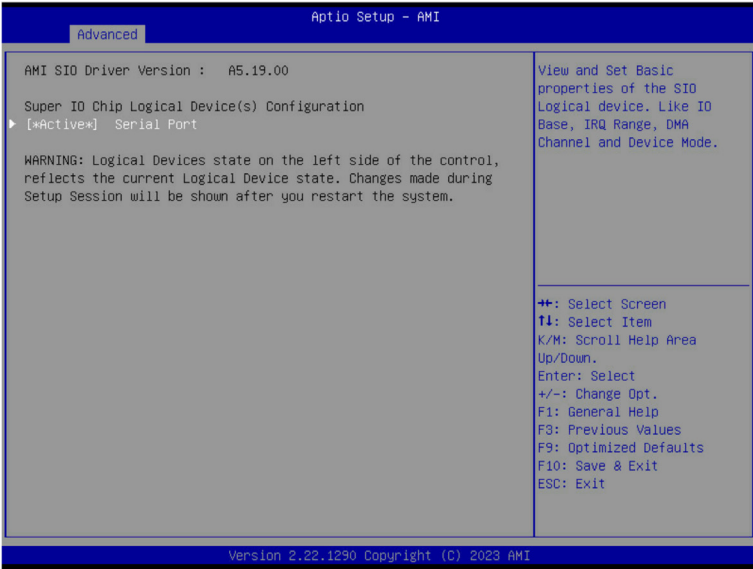
Parameter	Description
COM1 Console Redirection ^(Note)	<p>Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>
COM1 Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p>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

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

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

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

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

5-2-4 PCI Subsystem Settings

Aptio Setup - AMI

Advanced

PCI Bus Driver Version	A5.01.30	Enable/Disable SLOT1 I/O ROM ++: Select Screen T1: 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]	
SLOT2 I/O ROM	[Enabled]	
SLOT3 I/O ROM	[Enabled]	
SLOT4 I/O ROM	[Enabled]	
SLOT5 I/O ROM	[Enabled]	
SLOT6 I/O ROM	[Enabled]	
SLOT7 I/O ROM	[Enabled]	
SLOT8 I/O ROM	[Enabled]	
SLOT9 I/O ROM	[Enabled]	
SLOT10 I/O ROM	[Enabled]	
SLOT11 I/O ROM	[Enabled]	
SLOT12 I/O ROM	[Enabled]	

Version 2.22.1290 Copyright (C) 2023 AMI

Aptio Setup - AMI

Advanced

GPU0 I/O ROM	[Enabled]	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root ID Virtualization Support. ++: Select Screen T1: 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
GPU1 I/O ROM	[Enabled]	
GPU2 I/O ROM	[Enabled]	
GPU3 I/O ROM	[Enabled]	
GPU4 I/O ROM	[Enabled]	
GPU5 I/O ROM	[Enabled]	
GPU6 I/O ROM	[Enabled]	
GPU7 I/O ROM	[Enabled]	
Onboard LAN1 I/O ROM	[Enabled]	
Onboard LAN2 I/O ROM	[Enabled]	
PCI Devices Common Settings:		
Above 4G Decoding	[Enabled]	
Re-Size BAR Support	[Disabled]	
SR-IOV Support	[Enabled]	

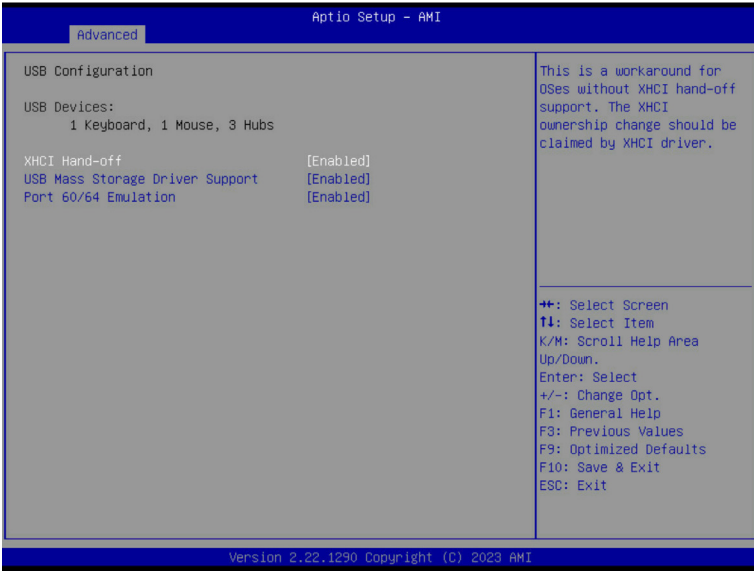
Version 2.22.1290 Copyright (C) 2023 AMI

Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT#/GPU# I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is Enabled .
Onboard LAN1/ LAN2 I/O ROM ^(Note2)	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available: Enabled, Disabled. Default setting is Enabled .
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled, Disabled. Default setting is Enabled .
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 Disabled .
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 Enabled .

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

(Note2) This section is dependent on the available LAN controller.

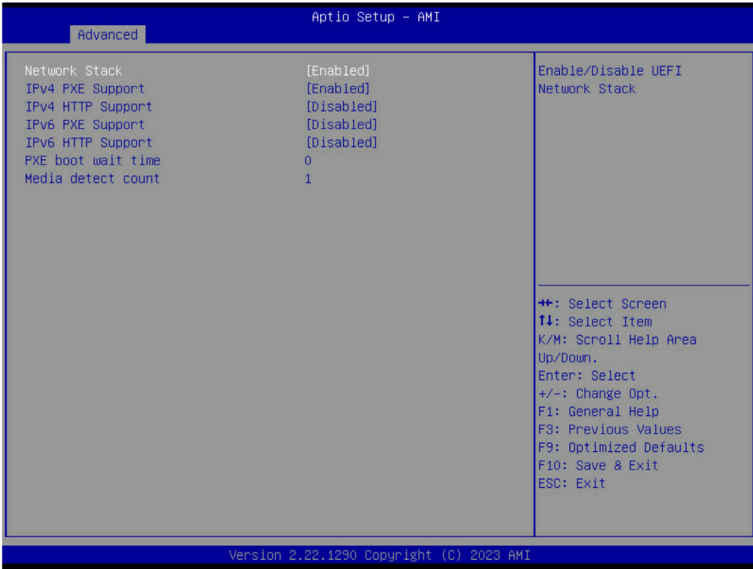
5-2-5 USB Configuration



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 Enabled .
USB Mass Storage Driver Support ^(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled, Disabled. Default setting is Enabled .
Port 60/64 Emulation	Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OSes. Options available: Enabled, Disabled. Default setting is Enabled .

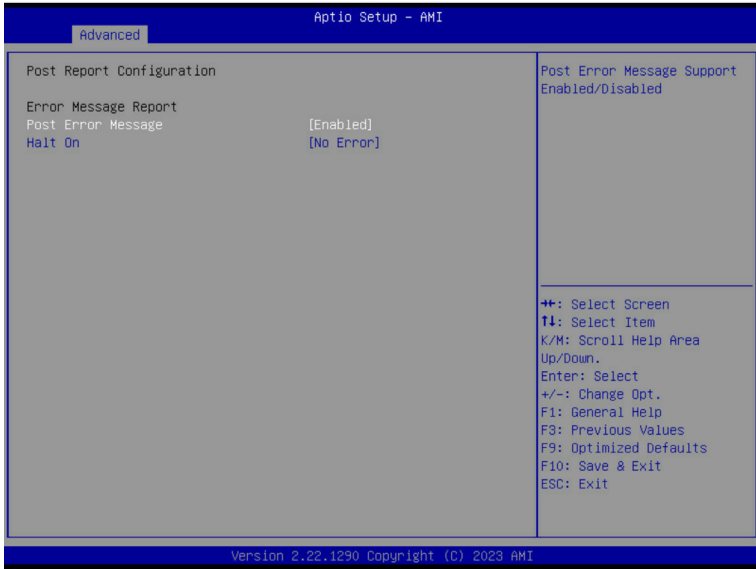
(Note) This item is present only if you attach USB devices.

5-2-6 Network Stack Configuration



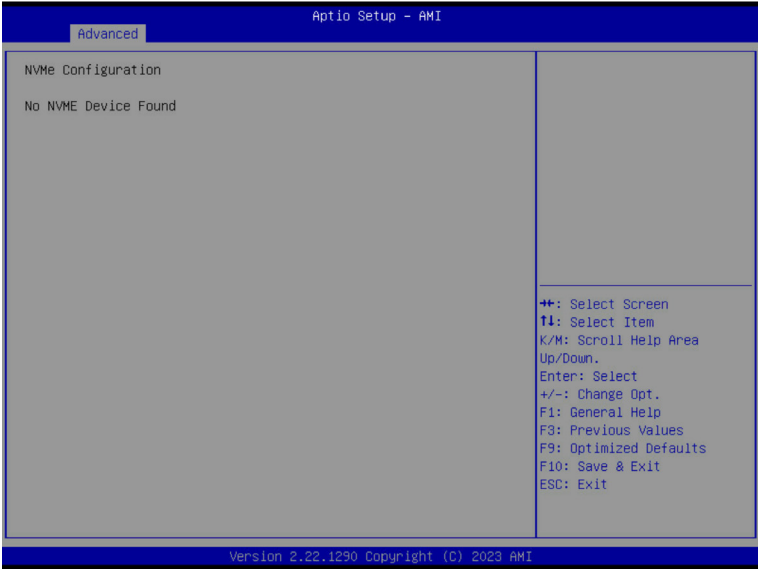
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 HTTP Support	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled, Disabled. Default setting is Disabled .
Ipv6 PXE Support	Enable/Disable the Ipv6 PXE feature. Options available: Enabled, Disabled. Default setting is Disabled .
Ipv6 HTTP Support	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled, Disabled. Default setting is Disabled .
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



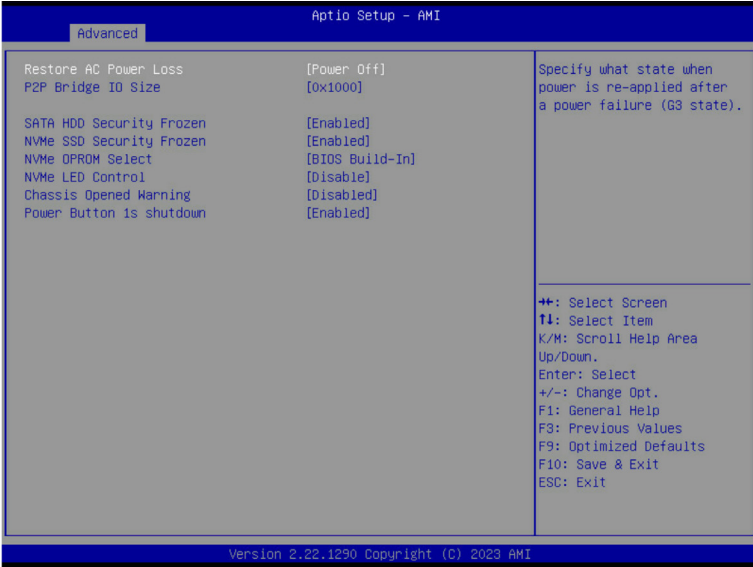
Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is Enabled .
Halt On	Options available: No Error, All Error. Default setting is No Error .

5-2-8 NVMe Configuration



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

5-2-9 Chipset Configuration

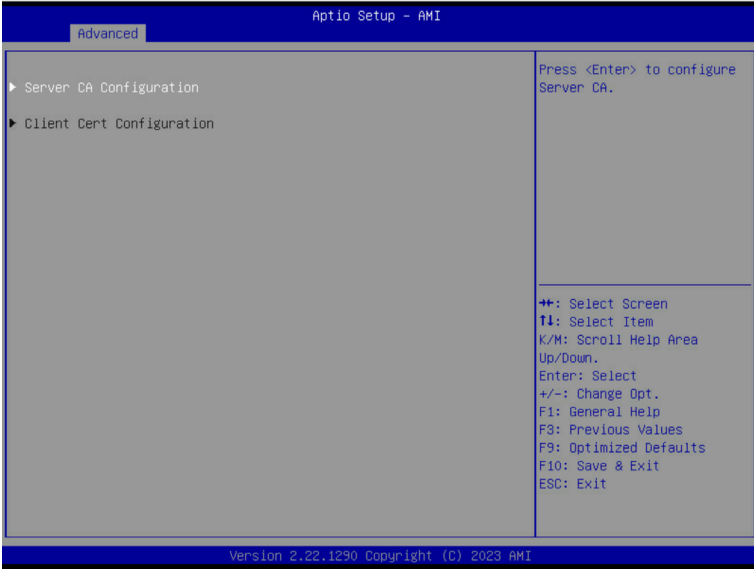


Parameter	Description
Restore on AC Power Loss ^(Note)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after 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 0x1000 .
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is Enabled .
NVMe SSD Security Frozen	Attempt to send freeze lock command to NVMe SSDs during boot. Options available: Enabled, Disabled. Default setting is Enabled .
NVMe OPROM Select	Options available: BIOS Build-In, NVMe Device, Disabled. Default setting is BIOS Build-In .
NVMe LED Control	Enable/Disable allow user control NVMe LED. It only available the NVMe device direct connect to CPU. Options available: Disable, Enable. Default setting is Disable .

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

Parameter	Description
Chassis Opened Warning	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is Disabled .
Power Button 1s shutdown	Enable/Disable Press power button 1 sec shutdown. Options available: Disabled, Enabled. Default setting is Enabled .

5-2-10 Tls Auth Configuration



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

5-2-11 iSCSI Configuration



Parameter	Description
Host iSCSI Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ iSCSI Initiator Name <ul style="list-style-type: none"> – Only IQN format is accepted. Range: from 4 to 223 ◆ Add an Attempt ◆ Delete Attempts ◆ Change Attempt Order

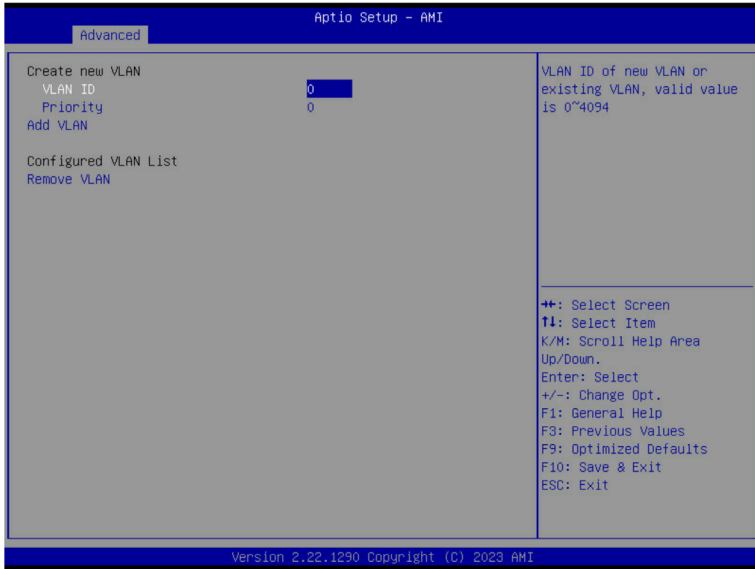
5-2-12 Intel(R) Ethernet Controller X710 for 10GBASE-T

Aptio Setup - AMI		
Advanced		
▶ Firmware Image Properties ▶ NIC Configuration		View device firmware version information.
Blink LEDs	0	
UEFI Driver Adapter PBA Device Name	Intel(R) 40GbE 4.9.13 H64862-000 Intel(R) Ethernet Controller X710 for 10GBASE-T	
Chip Type	Intel X710	
PCI Device ID	15FF	
PCI Address	09:00:00	
Link Status	[Connected]	
MAC Address	74:56:3C:B4:3F:44	
Virtual MAC Address	00:00:00:00:00:00	
		++: Select Screen T1: 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
Version 2.22.1290 Copyright (C) 2023 AMI		

Aptio Setup - AMI		
Advanced		
Link Speed	[Auto Negotiated]	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.
Wake On LAN	[Enabled]	
LLDP Agent	[Enabled]	
		++: Select Screen T1: 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
Version 2.22.1290 Copyright (C) 2023 AMI		

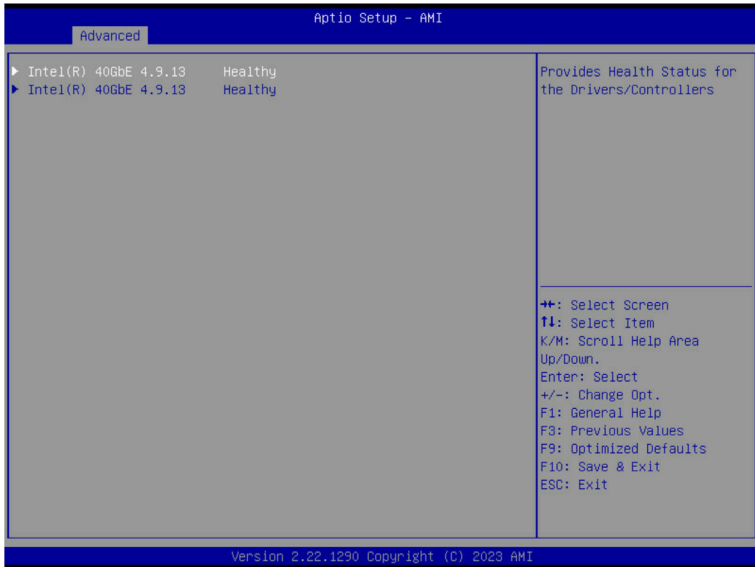
Parameter	Description
Firmware Image Properties	Press [Enter] to view device firmware version information.
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Link Speed <ul style="list-style-type: none"> – Default setting is Auto Negotiated. ◆ Wake On LAN <ul style="list-style-type: none"> – 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. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ LLDP Agent <ul style="list-style-type: none"> – Enable/Disable firmware's LLDP Agent. – Options available: Enabled, Disabled. Default setting is Enabled
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).
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.

5-2-13 VLAN Configuration



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

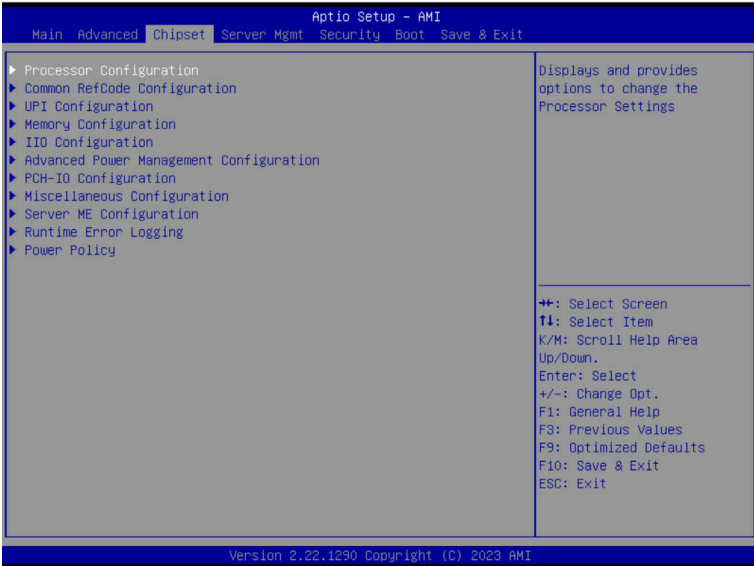
5-2-14 Driver Health



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

5-3 Chipset Menu

Chipset Setup menu displays submenu options for configuring the function of Platform Controller Hub(PCH). 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	000806F8*	000806F8
Processor Die Type	XCC	XCC
Processor Frequency	2.000GHz	2.000GHz
Processor Max Ratio	14H	14H
Processor Min Ratio	08H	08H
Microcode Revision	2B000571	2B000571
L1 Cache RAM(Per Core)	80KB	80KB
L2 Cache RAM(Per Core)	2048KB	2048KB
L3 Cache RAM(Per Package)	107520KB	107520KB
Processor 0 Version	Intel(R) Xeon(R) Platin um 8480+	
Processor 1 Version	Intel(R) Xeon(R) Platin um 8480+	
Enable LP [Global]	[ALL LPs]	↕: Select Screen
Hardware Prefetcher	[Enable]	↑↓: Select Item
L2 RFO Prefetch Disable	[Disable]	K/M: Scroll Help Area
Adjacent Cache Prefetch	[Enable]	Up/Down.
DCU Streamer Prefetcher	[Enable]	Enter: Select
DCU IP Prefetcher	[Enable]	+/-: Change Opt.
Extended APIC	[Enable]	F1: General Help
		F3: Previous Values
		F9: Optimized Defaults
		F10: Save & Exit
		ESC: Exit

Version 2.22.1290 Copyright (C) 2023 AMI

Aptio Setup - AMI

Chipset

Processor 0 Version	Intel(R) Xeon(R) Platin um 8480+	▶ Displays and provides option to change the Processor CFR Settings
Processor 1 Version	Intel(R) Xeon(R) Platin um 8480+	
Enable LP [Global]	[ALL LPs]	↕: 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
Hardware Prefetcher	[Enable]	
L2 RFO Prefetch Disable	[Disable]	
Adjacent Cache Prefetch	[Enable]	
DCU Streamer Prefetcher	[Enable]	
DCU IP Prefetcher	[Enable]	
Extended APIC	[Enable]	
Enable Intel(R) TXT	[Disable]	
VMX	[Enable]	
Enable SMX	[Disable]	
AES-NI	[Enable]	
Debug Consent	[Disable]	

TME, TME-MT, TDX		

Memory Encryption (TME)	[Disabled]	
SGX setup configuration preconditions for enabling were NOT met. Please check TME, MirrorMode or Extended APIC settings.		

▶ Processor CFR Configuration		

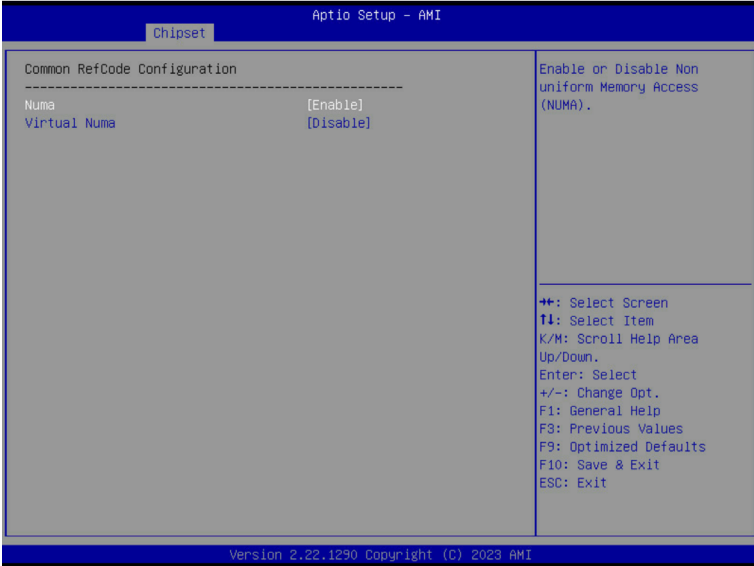
Version 2.22.1290 Copyright (C) 2023 AMI

Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ CPU Socket 0/1 Configuration <ul style="list-style-type: none"> – Core Disable Bitmap(Hex) <ul style="list-style-type: none"> • 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.
Processor Socket / Processor ID / Processor Die Type / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Per Core) / L3 Cache RAM(Per Package) / Processor # Version	Displays the technical specifications for the installed processor(s).
Enable LP [Global]	<p>Enables Logical processor (Software Method to Enable/Disable Logical Processor threads).</p> <p>Options available: ALL LPs, Single LP. Default setting is ALL LPs.</p>
Hardware Prefetcher	<p>Select whether to enable the speculative prefetch unit of the processor.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
L2 RF0 Prefetch Disable	Options available: Enable, Disable. Default setting is Disable .
Adjacent Cache Prefetch	<p>When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
DCU Streamer Prefetcher	<p>Enable/Disable DCU streamer prefetcher.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
DCU IP Prefetcher	<p>Enable/Disable DCU IP Prefetcher.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Extended APIC	<p>Enable/Disable extended APIC support. Note: The VT-d will be enabled automatically when x2APIC is enabled.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Enable Intel(R) TXT	<p>Enable/Disable the Intel Trusted Execution Technology support function.</p> <p>Options available: Enable, Disable. Default setting is Disable.</p>
VMX	<p>Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Enable SMX	<p>Enable/Disable the Safer Mode Extensions (SMX) support function.</p> <p>Options available: Enable, Disable. Default setting is Disable.</p>
AES-NI	<p>Enable/Disable the AES-NI support.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Debug Consent	Options available: Enable, Disable. Default setting is Disable .

Parameter	Description
Memory Encryption (TME) ^(Note)	Enable/Disable memory encryption (TME). Options available: Enabled, Disabled. Default setting is Disabled .
Total Memory Encryption Multi-Tenant (TME-MT)	Options available: Enabled, Disabled. Default setting is Disabled .
Processor CFR Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Provision S3M CFR <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Enable. ◆ Manual Commit S3M FW CFR <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Enable. ◆ Provision PUcode CFR <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Enable. ◆ Manual Commit PUcode CFR <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Enable. ◆ Socket0/1 CFR Revision Info <ul style="list-style-type: none"> – Displays CFR Revision information of the socket.

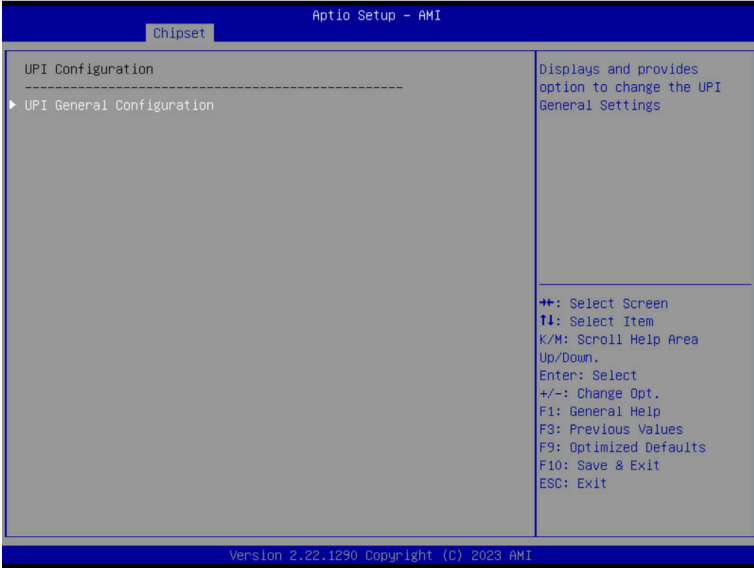
(Note) Advanced items prompt when this item is defined.

5-3-2 Common RefCode Configuration



Parameter	Description
Common RefCode Configuration	
Numa	Enable/Disable Non uniform Memory Access(NUMA). Options available: Enable, Disable. Default setting is Enable .
Virtual Numa	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 Disable .

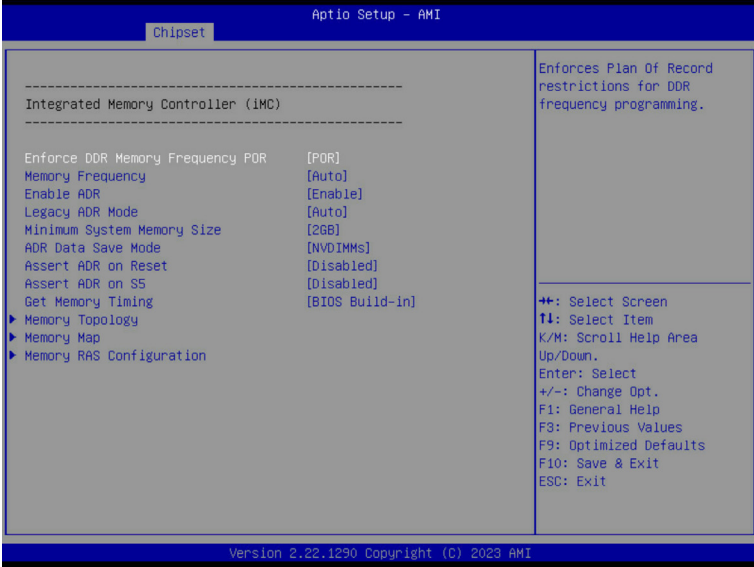
5-3-3 UPI Configuration



Parameter	Description
UPI General Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ UPI Status <ul style="list-style-type: none"> – Press [Enter] to view the Uncore status. ◆ Link Frequency Select <ul style="list-style-type: none"> – Selects the UPI link frequency. – Options available: 12.8GT/s, 14.4GT/s, 16.0GT/s, Auto, Use Per Link Setting. Default setting is Auto. ◆ SNC <ul style="list-style-type: none"> – Enable/Disable Sub NUMA Cluster function. – Options available: Auto, Disable, Enable SNC2 (2-clusters), Enable SNC4 (4-clusters). Default setting is Auto. ◆ Stale AtoS <ul style="list-style-type: none"> – Enable/Disable Stale A to S directory optimization. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ LLC dead line alloc <ul style="list-style-type: none"> – Enable/Disable fill dead lines in LLC. – Options available: Disable, Enable, Auto. Default setting is Enable. ◆ MMCFG Size <ul style="list-style-type: none"> – Options available: 128M, 256M, 512M, 1G, 2G, Auto. Default setting is Auto. ◆ MMIO High Base <ul style="list-style-type: none"> – Options available: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T. Default setting is 4T.

Parameter	Description
UPI General Configuration (continued)	<ul style="list-style-type: none"> <li data-bbox="352 142 955 252">◆ MMIO High Granularity Size <ul style="list-style-type: none"> <li data-bbox="384 169 955 192">– Selects the allocation size used to assign mmioh resources. <li data-bbox="384 200 955 252">– Options available: 1G, 4G, 16G, 64G, 256G, 1024G, 4096G. Default setting is 1024G. <li data-bbox="352 260 955 313">◆ Limit CPU PA to 46 bits <ul style="list-style-type: none"> <li data-bbox="384 286 955 313">– Options available: Disable, Enable. Default setting is Disable.

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 POR .
Memory Frequency	Configures the maximum memory frequency. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Default setting is Auto .
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable, Disable. Default setting is Enable .
Legacy ADR Mode	Enable/Disable the Legacy ADR Mode. Options available: Enable, Disable, Auto. Default setting is Auto .
Minimum System Memory Size	Configures the minimum memory size. Options available: 2GB, 4GB, 6GB, 8GB. Default setting is 2GB .
ADR Data Save Mode	Specifies the Data Save Mode for ADR. Batterybacked or Type 01 NVDIMM. Options available: Disable, Batterybacked DIMMs, NVDIMMs, Copy to Flash. Default setting is NVDIMMs .
Assert ADR on Reset	Enable/Disable Assert ADR on Reset. Options available: Enabled, Disabled. Default setting is Disabled .

Parameter	Description
Assert ADR on S5	Enable/Disable Assert ADR on S5. Options available: Enabled, Disabled. Default setting is Disabled .
Get Memory Timing	Auto is the detected SPD value and use it, otherwise use BIOS Build-in. Options available: Auto, BIOS Build-in. Default setting is BIOS Build-in .
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map ^(Note1)	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Volatile Memory Mode <ul style="list-style-type: none"> – Selects 1LM or 2LM mode for volatile memory. – Options available: 1LM, 2LM. Default setting is 2LM.
Memory RAS Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Mirror Mode^(Note2) <ul style="list-style-type: none"> – 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. – Options available: Disabled, Full Mirror Mode, Partial Mirror Mode. Default setting is Disabled. ◆ Partial Mirror 1 Size (GB) <ul style="list-style-type: none"> – Selects multiplier of 1GB for the size of the SAD to be created. ◆ Correctable Error Threshold <ul style="list-style-type: none"> – Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket. – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Trigger SW Error Threshold^(Note2) <ul style="list-style-type: none"> – Enable/Disable Sparing trigger SW Error Match Threshold. – Options available: Disabled, Enabled. Default setting is Disabled. ◆ SW Per Bank Threshold <ul style="list-style-type: none"> – SW Per Bank Threshold (1-0x7FFF) used for DDR bank level error. – Press the <+> / <-> keys to increase or decrease the desired values. ◆ SW Correctable Error Time Window <ul style="list-style-type: none"> – SW Correctable Error time window based interface in hour (0-24). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket time window based interface^(Note2) <ul style="list-style-type: none"> – Enable/Disable leaky bucket time window based interface. – Options available: Disabled, Enabled. Default setting is Disabled.

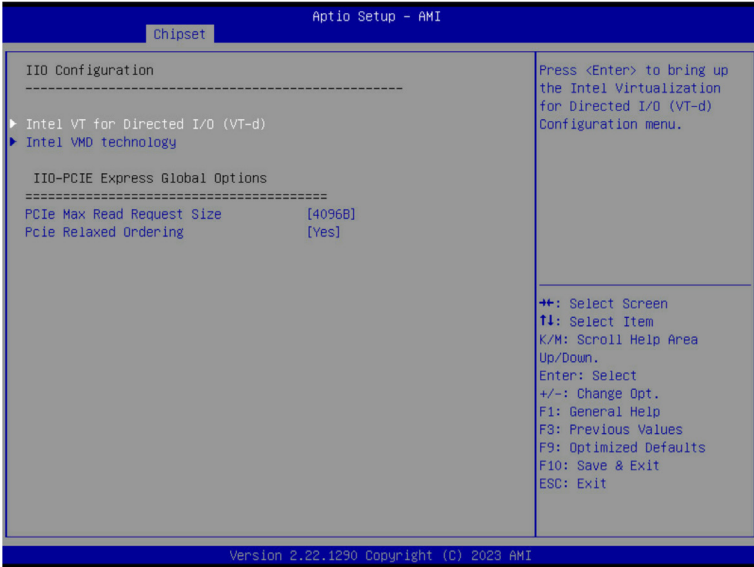
(Note1) Advanced items prompt when HBM CPU is installed.

(Note2) Advanced items prompt when this item is defined.

Parameter	Description
Memory RAS Configuration (continued)	<ul style="list-style-type: none"> ◆ Leaky bucket time window based interface Hour <ul style="list-style-type: none"> – Leaky bucket time window based interface hour used for DDR (0-24). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket time window based interface Minute <ul style="list-style-type: none"> – Leaky bucket time window based interface minute used for DDR (0-60). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket low bit <ul style="list-style-type: none"> – Configures leaky bucket low bit (0x1 - 0x29). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket high bit <ul style="list-style-type: none"> – Configures leaky bucket high bit (0x1 - 0x29). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ ADDDC Sparing^(Note) <ul style="list-style-type: none"> – Enable/Disable ADDDC Sparing. – Options available: Disabled, Enabled. Default setting is Disabled. ◆ Enable ADDDC Error Injection <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Enabled. ◆ Patrol Scrub <ul style="list-style-type: none"> – Options available: Disabled, Enable at End of POST. Default setting is Enable at End of POST. ◆ Patrol Scrub Interval <ul style="list-style-type: none"> – Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto. ◆ DDR5 ECS <ul style="list-style-type: none"> – Options available: Disabled, Enabled, Enable ECS with Result Collection. Default setting is Enabled.

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

5-3-5 IIO Configuration



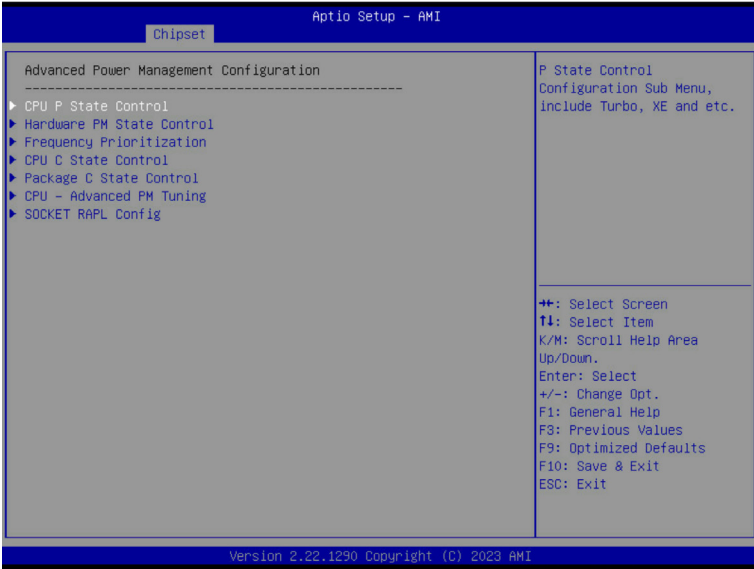
Parameter	Description
IIO Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel® VT for Directed I/O <ul style="list-style-type: none"> – Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. – Options available: Enable, Disable. Default setting is Enable. ◆ Cache Allocation <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable. ◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> – Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA). – Options available: Enable, Disable. Default setting is Disable. ◆ Interrupt Remapping <ul style="list-style-type: none"> – Enable/Disable the interrupt remapping support function. – Options available: Auto, Enable, Disable. Default setting is Auto ◆ x2APIC Opt Out <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ Pre-boot DMA Protection <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable.
Intel® VT for Directed I/O (VT-d)	

Parameter	Description
Intel® VT for Directed I/O (VT-d) (continued)	<ul style="list-style-type: none"> ◆ PCIe ACSCTL <ul style="list-style-type: none"> – Enable/Disable overwrite of PCI Access Control Services Control register in PCI root ports. – Options available: Disable, Enable. Default setting is Disable. ◆ Source Validation^(Note) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Disabled. ◆ Translation Blocking^(Note) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Disabled. ◆ P2P Request Redirect^(Note) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Enabled. ◆ P2P Completion Redirect^(Note) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Enabled. ◆ Upstream Forwarding Enable^(Note) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Enabled.
Intel® VMD technology	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel® VMD Configuration <ul style="list-style-type: none"> – Enable/Disable Intel® VMD technology. – Options available: Enable, Disable. Default setting is Disable. ◆ Intel® VMD for Non-Hotplug NVMe^(Note1) <ul style="list-style-type: none"> – Enable/Disable Intel® VMD for Non-Hotplug NVMe. – Options available: Enable, Disable. Default setting is Disable.
I/O-PCIe Express Global Options	
PCIe Max Read Request Size	Options available: Auto, 128B, 256B, 512B, 1024B, 2048B, 4096B. Default setting is 4096B .
Pcie Relaxed Ordering	Options available: No, Yes. Default setting is Yes .

(Note) This item is available when **PCIe ACSCTL** is set to **Enable**.

(Note1) This item appears when **Intel® VMD Configuration** is set to **Enable**.

5-3-6 Advanced Power Management Configuration



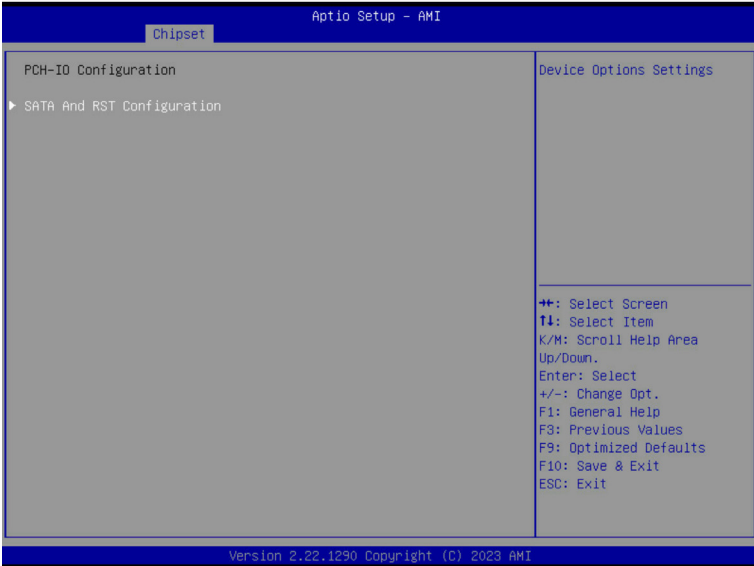
Parameter	Description
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Activate SST-BF <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ Configure SST-BF <ul style="list-style-type: none"> – This option allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure. – Options available: Enable, Disable. Default setting is Enable. ◆ SpeedStep (Pstates) <ul style="list-style-type: none"> – 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 Enable. ◆ Turbo Mode <ul style="list-style-type: none"> – 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 Enable.

Parameter	Description
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Hardware P-States <ul style="list-style-type: none"> – When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States). – In Native mode, the processor hardware chooses a P-state based on OS guidance. – In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance). – Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is Native Mode.
Frequency Prioritization	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ SST-CP <ul style="list-style-type: none"> – This knob controls whether SST-CP is enabled. When enabled it activates per core power budgeting. NOTE: HWP Native Mode is a pre-requisite for enabling SST-CP. – Options available: Disable, Enable. Default setting is Disable.
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Enable Monitor MWAIT <ul style="list-style-type: none"> – Allows Monitor and MWAIT instructions. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ CPU C6 Report <ul style="list-style-type: none"> – Enable/Disable CPU C6(ACPI C3) report to OS. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> – Core C1E auto promotion control. Takes effect after reboot. – Options available: Enable, Disable. Default setting is Enable.
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Package C State <ul style="list-style-type: none"> – Configures the state for 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 Auto.
CPU - Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Energy Perf BIAS <ul style="list-style-type: none"> – Press [Enter] to configure advanced items. <ul style="list-style-type: none"> » Power Performance Tuning <ul style="list-style-type: none"> • Options available: OS Controls EPB, BIOS Controls EPB, PECl Controls EPB. Default setting is OS Controls EPB. » Energy_PERF_BIAS_CFG mode^(Note) <ul style="list-style-type: none"> • Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is Balanced Performance.

(Note) This item is configurable when **Power Performance Tuning** is set to **BIOS Controls EPB**.

Parameter	Description
SOCKET RAPL Config	<p data-bbox="362 147 695 174">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="362 178 953 288">◆ PL1 Power Limit <ul style="list-style-type: none"> <li data-bbox="397 205 953 260">– PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. <li data-bbox="397 264 575 288">– Default setting is 0. <li data-bbox="362 293 953 374">◆ PL1 Time Window <ul style="list-style-type: none"> <li data-bbox="397 319 953 346">– PL1 value in seconds. The value may vary from 0 to 448. <li data-bbox="397 351 575 374">– Default setting is 1. <li data-bbox="362 379 953 489">◆ PL2 Power Limit <ul style="list-style-type: none"> <li data-bbox="397 406 953 460">– PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 120% * TDP. <li data-bbox="397 465 575 489">– Default setting is 0. <li data-bbox="362 493 953 575">◆ PL2 Time Window <ul style="list-style-type: none"> <li data-bbox="397 520 953 547">– PL1 value in seconds. The value may vary from 0 to 0.438. <li data-bbox="397 551 610 575">– Default setting is 0.012.

5-3-7 PCH Configuration



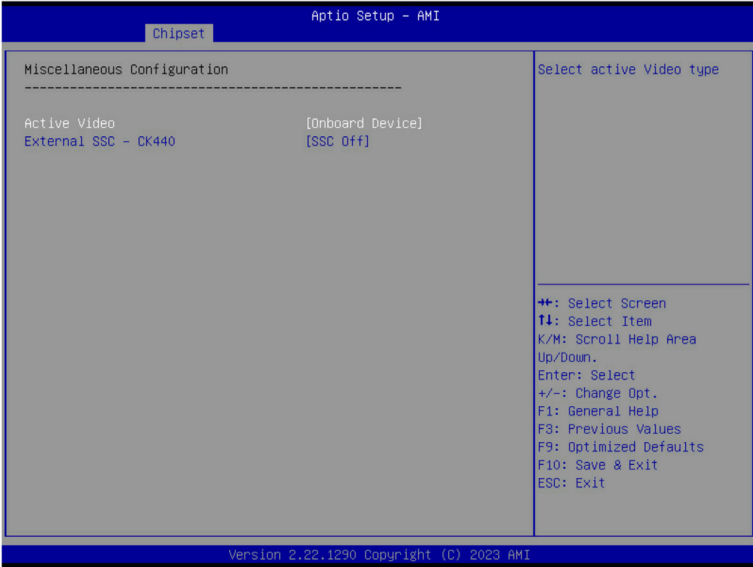
Parameter	Description
PCH-IO Configuration	Press [Enter] to configure advanced items.
SATA And RST Configuration/ SATA Controller And RST Configuration	<ul style="list-style-type: none"> ◆ SATA Configuration <ul style="list-style-type: none"> – Enable/Disable SATA controller. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ SATA Mode Selection <ul style="list-style-type: none"> – Configures on chip SATA type. – AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time. – RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time. – Options available: AHCI, RAID. Default setting is AHCI. ◆ RAID Device ID^(Note) <ul style="list-style-type: none"> – Choose RAID Device ID. – Options available: Client, Alternate, Server. Default setting is Server. ◆ SATA Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> – The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.

(Note) Only appears when HDD sets to **RAID Mode**.

Parameter	Description
SATA And RST Configuration/ SATA Controller And RST Configuration (continued)	<ul style="list-style-type: none"> ◆ SATA Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> – Enable/Disable Port 0/1/2/3/4/5/6/7 device. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Hot Plug (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> – Enable/Disable HDD Hot-Plug function. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Spin Up Device (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> – On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. – Options available: Enabled, Disabled. Default setting is Disabled.

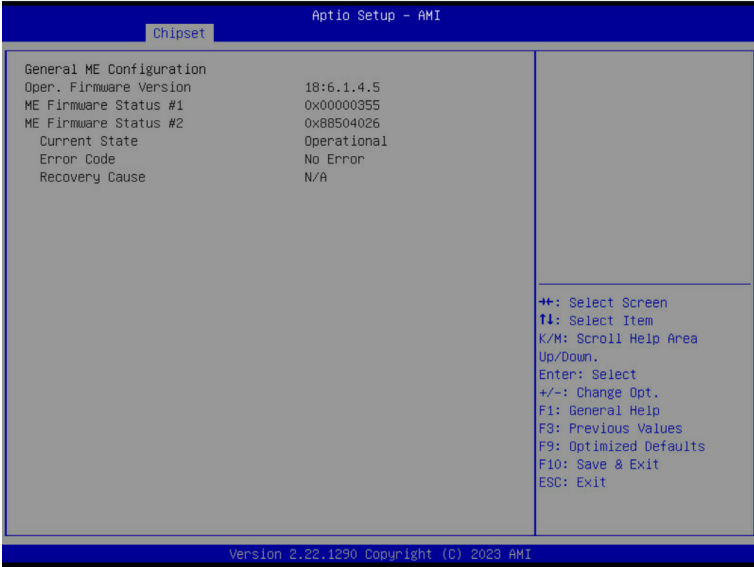
(Note) Only appears when HDD sets to **RAID** Mode.

5-3-8 Miscellaneous Configuration



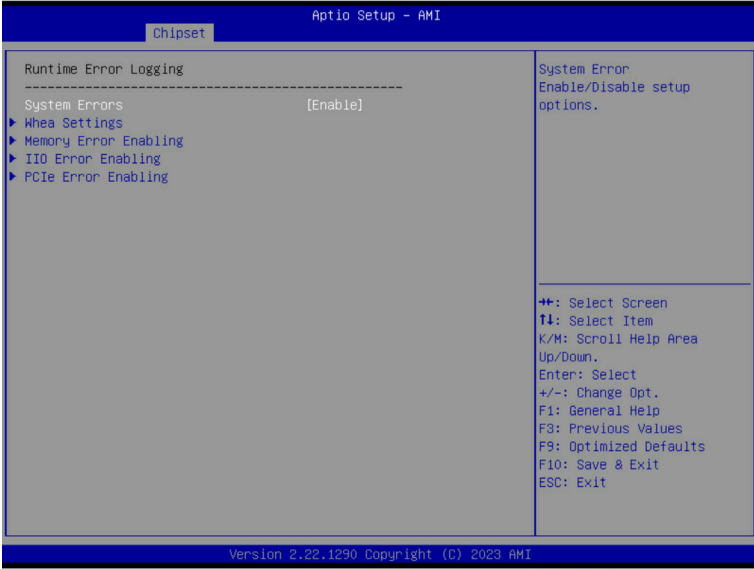
Parameter	Description
Miscellaneous Configuration	
Active Video	Selects the active video type. Options available: Auto, Onboard Device, PCIE Device, Specific PCIE Device. Default setting is Onboard Device .
External SSC - CK440	Enables Spread spectrum - only affects external clock generator. Options available: SSC Off, SSC = -0.3%, SSC = -0.5%, Hardware. Default setting is SSC Off .

5-3-9 Server ME Configuration



Parameter	Description
General ME Configuration	
Oper. Firmware Version	Displays the operational firmware version.
ME Firmware Status #1/#2	Displays ME Firmware status information.
Current State	Displays ME Firmware current status information.
Error Code	Displays ME Firmware status error code.
Recovery Cause	Displays ME Firmware recovery cause.

5-3-10 Runtime Error Logging Settings

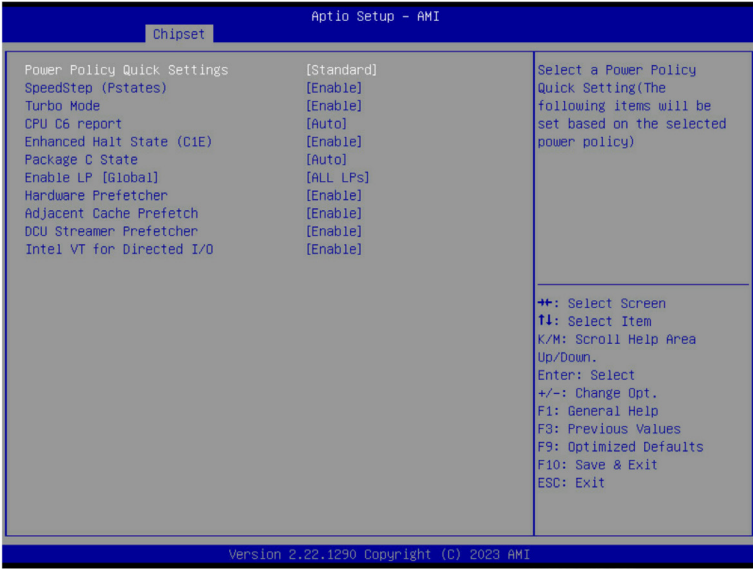


Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable, Disable. Default setting is Enable .
Whea Settings	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ WHEA (Windows Hardware Error Architecture) Support <ul style="list-style-type: none"> - Enable/Disable WHEA Support. - Options available: Enable, Disable. Default setting is Enable.
Memory Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Memory Corrected Error <ul style="list-style-type: none"> - Enable/Disable Memory Corrected Error. - Options available: Enable, Disable. Default setting is Enable. ◆ Uncorrected Error disable Memory <ul style="list-style-type: none"> - Enable/Disable the Memory that triggers Uncorrected Error. - Options available: Enable, Disable. Default setting is Disable.
IIO Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Os Native AER Support <ul style="list-style-type: none"> - 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. - Options available: Enable, Disable. Default setting is Disable.

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">◆ PCIe Error <ul style="list-style-type: none"> <li data-bbox="344 200 580 224">– Enable/Disable PCIe error. <li data-bbox="344 228 852 252">– Options available: Enable, Disable. Default setting is Disable. <li data-bbox="309 257 923 338">◆ Uncorrected Error^(Note) <ul style="list-style-type: none"> <li data-bbox="344 286 923 310">– Enables and escalates Uncorrectable/Recoverable Errors to error pins. <li data-bbox="344 315 846 338">– Options available: Enable, Disable. Default setting is Enable. <li data-bbox="309 343 846 424">◆ Fatal Error Enable^(Note) <ul style="list-style-type: none"> <li data-bbox="344 373 749 396">– Enables and escalates Fatal Errors to error pins. <li data-bbox="344 401 846 424">– Options available: Enable, Disable. Default setting is Enable. <li data-bbox="309 429 940 545">◆ Assert NMI on SERR^(Note) <ul style="list-style-type: none"> <li data-bbox="344 459 940 514">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. <li data-bbox="344 519 876 542">– Options available: Enabled, Disabled. Default setting is Enabled. <li data-bbox="309 550 940 663">◆ Assert NMI on PERR^(Note) <ul style="list-style-type: none"> <li data-bbox="344 580 940 635">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. <li data-bbox="344 639 876 663">– Options available: Enabled, Disabled. Default setting is Enabled.

(Note) This item appears when **PCIe Error** is set to **Enable**.

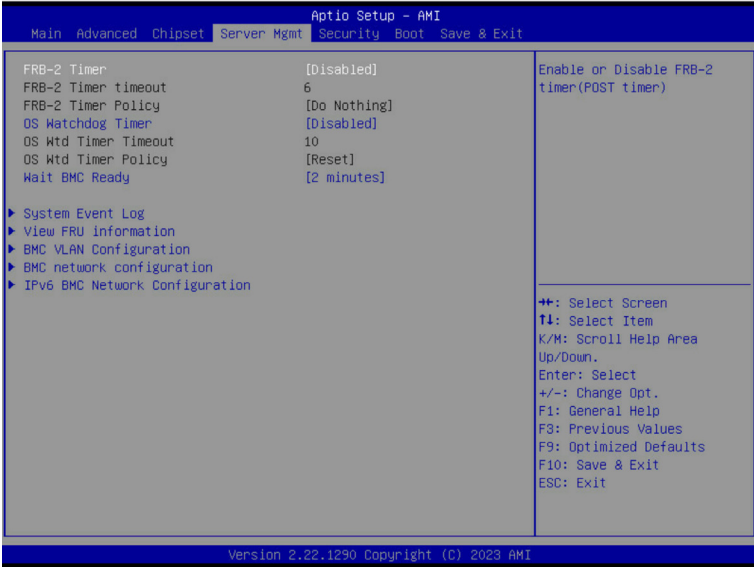
5-3-11 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient. Default setting is Standard .
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 Enable .
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 Enable .
CPU C6 report	Enable/Disable the BIOS to enable the report from the CPU C6 state (ACPI C3) to the OS. Options available: Disable, Enable, Auto. Default setting is Auto .
Enhanced Halt State (C1E)	Enable/Disable the C1E support for lower power consumption. Takes effect after reboot. Options available: Enable, Disable. Default setting is Enable .
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 Auto .

Parameter	Description
Enable LP [Global]	Enables Logical processor (Software Method to Enable/Disable Logical Processor threads). Options available: ALL LPs, Single LP. Default setting is ALL LPs .
Hardware Prefetcher	Options available: Enable, Disable. Default setting is Enable .
Adjacent Cache Prefetch	Options available: Enable, Disable. Default setting is Enable .
DCU Streamer Prefetcher	Options available: Enable, Disable. Default setting is Enable .
Intel® VT for Directed I/O	Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. Options available: Enable, Disable. Default setting is Enable .

5-4 Server Management Menu



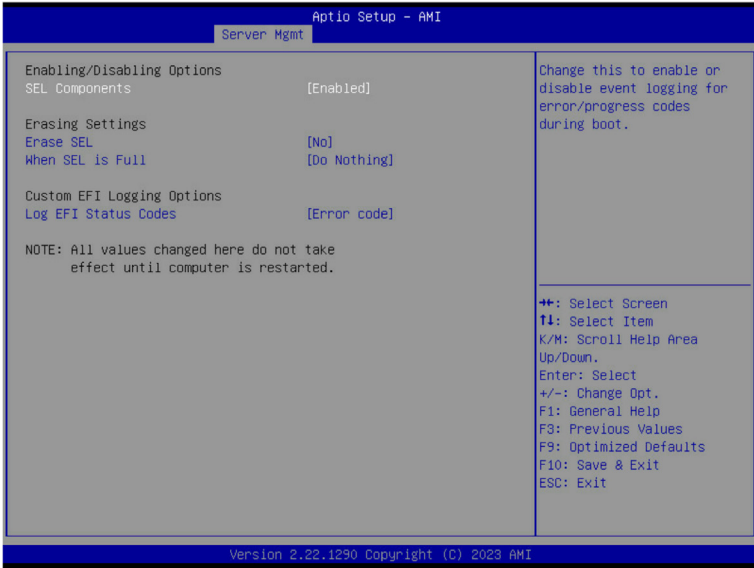
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is Enabled .
FRB-2 Timer ^(Note1) timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is 6 minutes .
FRB-2 Timer Policy ^(Note1)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

(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**.

Parameter	Description
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.

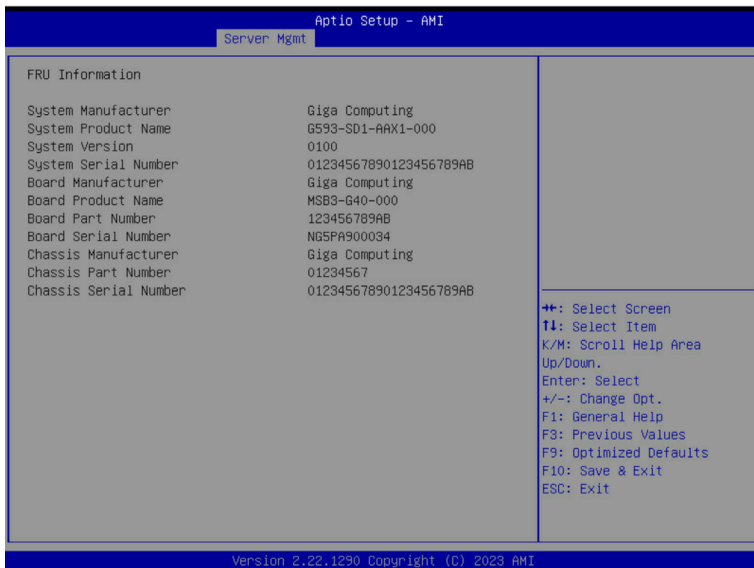
5-4-1 System Event Log



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 Enabled .
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: No, Yes, On next reset, Yes, On every reset. Default setting is No .
When SEL is Full	Choose options for reactions to a full SEL. Options available: Do Nothing, Erase Immediately, Delete Oldest Record. Default setting is Do Nothing .
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 Error code .

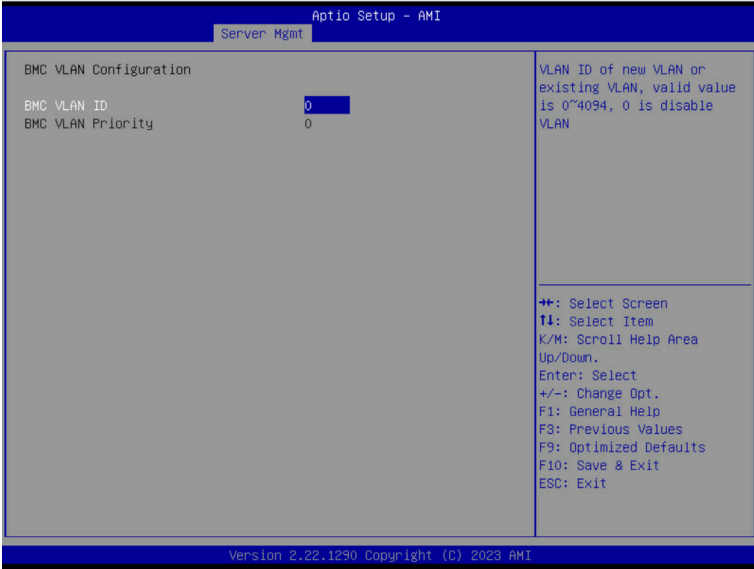
5-4-2 View FRU Information

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.



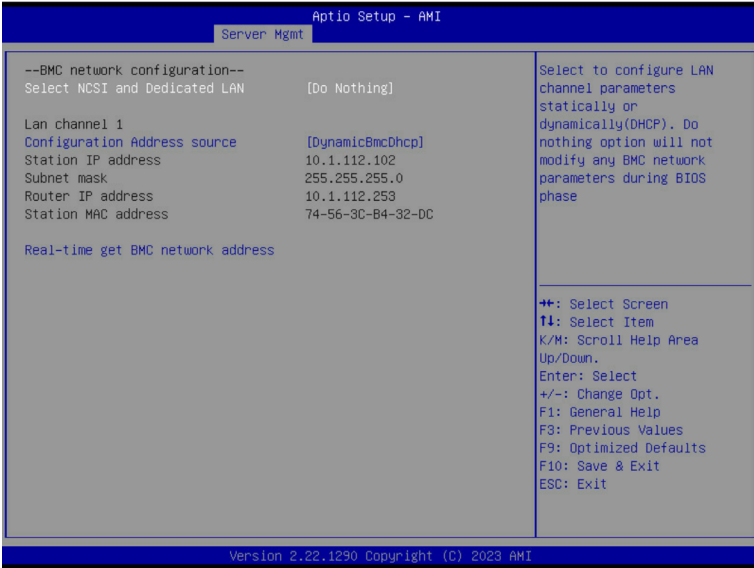
(Note) The model name will vary depends on the product you purchased

5-4-3 BMC VLAN Configuration



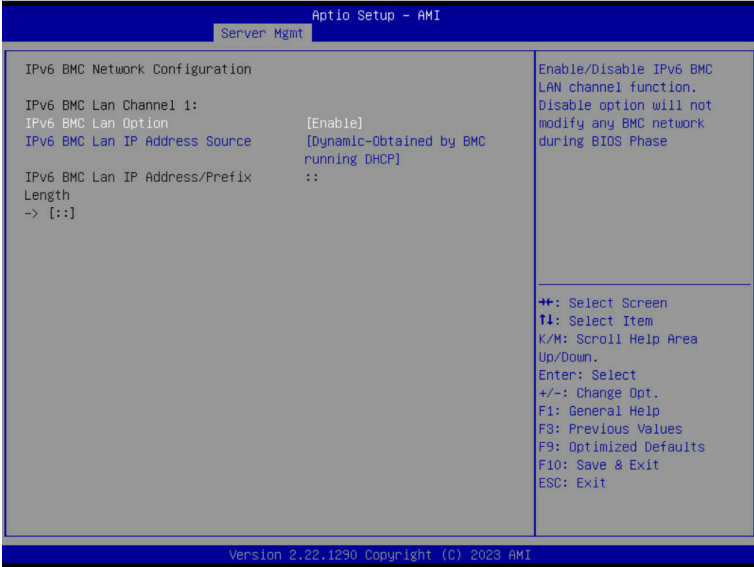
Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority 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 Do Nothing .
Lan Channel 1	
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (DHCP). Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is DynamicBmcDhcp .
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.

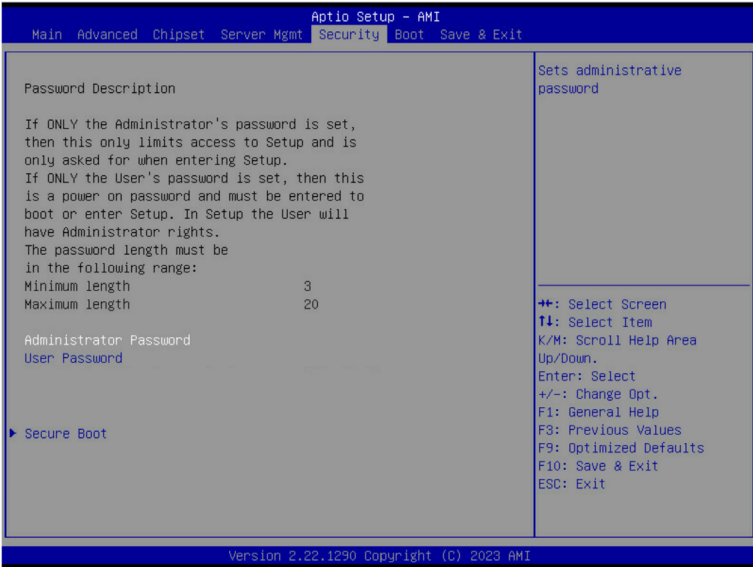
5-4-5 IPv6 BMC Network Configuration



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 Enable .
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 Dynamic-Obtained by BMC running DHCP .
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.
Secure Boot	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 Disabled .
Secure Boot Mode ^(Note)	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 Custom .
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.

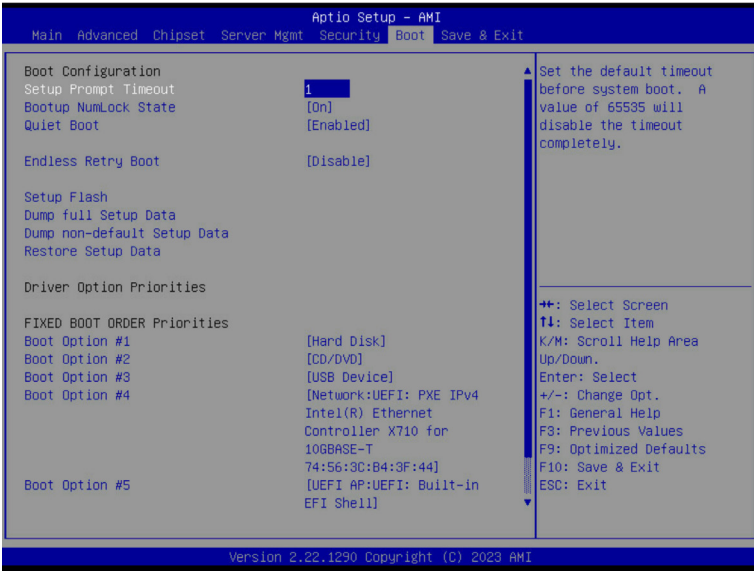
(Note) Advanced items prompt when this item is set to **Custom**.

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">Please note that this item is configurable when Secure Boot Mode is set to Custom.</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 data-bbox="367 326 904 352">– Options available: Enabled, Disabled. Default setting is Disabled. <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 data-bbox="367 409 606 431">– Options available: Yes, No. <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 data-bbox="367 487 606 509">– Options available: Yes, No. <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 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 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 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 data-bbox="367 793 675 816">– Press [Enter] to configure a new PK. <li data-bbox="367 821 601 846">– Options available: Update. <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 data-bbox="367 903 904 961">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="367 965 670 987">– Options available: Update, Append. <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 data-bbox="367 1044 941 1102">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="367 1107 670 1128">– Options available: Update, Append. <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 data-bbox="367 1185 893 1243">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="367 1248 670 1270">– Options available: Update, Append.

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

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.

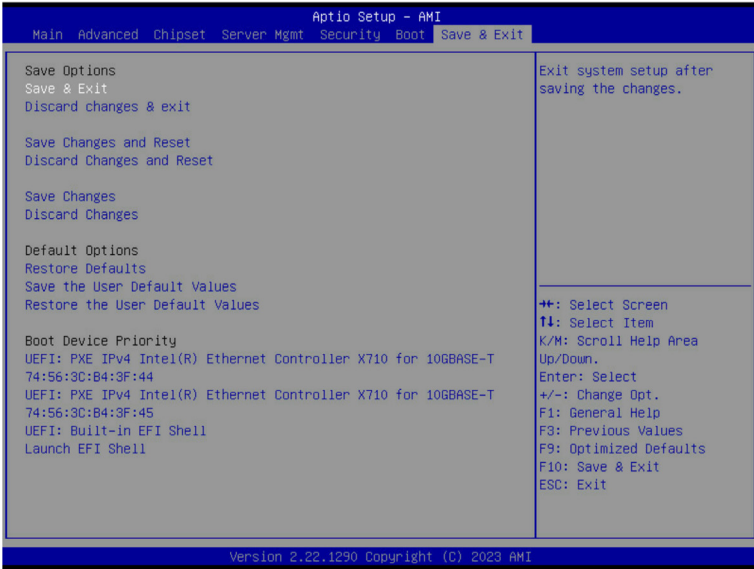


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off. Default setting is On .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled, Disabled. Default setting is Enabled .
Endless Retry Boot	Options available: Disable, Enable. Default setting is Disable .
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.

Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	<p>Press [Enter] to configure the boot order priority. By default, the server searches for boot devices in the following sequence:</p> <ol style="list-style-type: none"> 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
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	

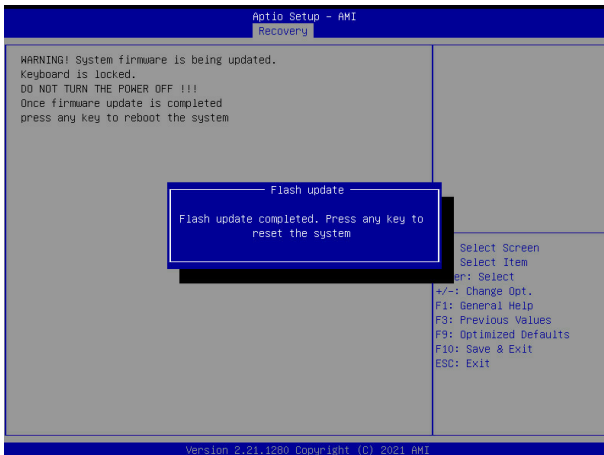
Parameter	Description
Restore Defaults	<p>Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system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

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.



5-9 BIOS POST Beep code (AMI standard)

5-9-1 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed.
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXE IPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

5-9-2 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met