

# **GIGABYTE™**

## **H263-S62-LAN1**

## **H263-S62-LAW1**

High Density Server - 4th/5th Gen Intel® Xeon® Scalable  
2U 4-Node DP 24-Bay Gen4 NVMe/SATA/SAS DLC  
Dual 2600W (240V) 80 PLUS Titanium redundant power supply (LAN1)  
Dual 3000W (240V) 80 PLUS Titanium redundant power supply (LAW1)

### **User Manual**

Rev. 1.0

## **Copyright**

© 2023 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](mailto:server.grp@gigabyte.com)

## Conventions

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

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

## Server Warnings and Cautions

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



### WARNING!

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

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



### 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 battery with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.



### CAUTION!

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



## Electrostatic Discharge (ESD)

### CAUTION!

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

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

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

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

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

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

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

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

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

# Table of Contents

Chapter 1 Hardware Installation .....	10
1-1 Installation Precautions .....	10
1-2 Product Specifications .....	11
1-3 System Block Diagram .....	16
Chapter 2 System Appearance .....	17
2-1 Front View .....	17
2-2 Rear View .....	18
2-3 Front Panel LED and Buttons .....	19
2-4 RoT LEDs .....	20
2-5 Rear System LAN LEDs .....	22
2-6 Power Supply Unit LED .....	23
2-7 Hard Disk Drive LEDs .....	24
Chapter 3 System Hardware Installation .....	25
3-1 Installing the Hard Disk Drive .....	26
3-2 Removing the Node .....	27
3-3 Removing Chassis Cover .....	28
3-4 Liquid Cooling Assembly Information .....	29
3-4-1 Liquid Cooling Specifications .....	30
3-5 Removing the Coolant Pipe Module .....	31
3-6 Installing the CPU and the Coolant Pipe Module .....	33
3-6-1 Installing the Memory .....	35
3-6-2 DIMM Population Table .....	36
3-6-3 Processor and Memory Module Matrix Table .....	37
3-7 Installing the PCI Expansion Card .....	38
3-8 Installing the Mezzanine Card .....	40
3-8-1 Installing the OCP 3.0 Mezzanine Card .....	40
3-9 Replacing the Fan Assembly .....	41
3-10 Replacing the Power Supply .....	42
3-11 Remoing the Power Supply Dummy Cover .....	43
3-12 Cable Routing .....	44

- Chapter 4 Motherboard Components .....52
  - 4-1 Motherboard Components ..... 52
  - 4-2 Jumper Setting ..... 53
  - 4-3 Backplane Board Storage Connector..... 54
    - 4-3-1 CBPH701.....54
- Chapter 5 BIOS Setup ..... 55
  - 5-1 The Main Menu ..... 57
  - 5-2 Advanced Menu ..... 60
    - 5-2-1 Trusted Computing.....61
    - 5-2-2 Serial Port Console Redirection .....62
    - 5-2-3 SIO Configuration .....65
    - 5-2-4 PCI Subsystem Settings.....66
    - 5-2-5 USB Configuration.....68
    - 5-2-6 Network Stack Configuration .....69
    - 5-2-7 Post Report Configuration .....70
    - 5-2-8 NVMe Configuration .....71
    - 5-2-9 Chipset Configuration.....72
    - 5-2-10 Tls Auth Configuration .....73
  - 5-3 Chipset Menu..... 74
    - 5-3-1 Processor Configuration .....75
    - 5-3-2 Common RefCode Configuration .....78
    - 5-3-3 UPI Configuration .....79
    - 5-3-4 Memory Configuration .....81
    - 5-3-5 IIO Configuration .....84
    - 5-3-6 Advanced Power Management Configuration .....86
    - 5-3-7 PCH Configuration.....88
    - 5-3-8 Miscellaneous Configuration .....90
    - 5-3-9 Server ME Configuration .....91
    - 5-3-10 Runtime Error Logging Settings .....92
    - 5-3-11 Power Policy.....94
  - 5-4 Server Management Menu..... 96
    - 5-4-1 System Event Log .....98
    - 5-4-2 View FRU Information .....99
    - 5-4-3 BMC VLAN Configuration.....100
    - 5-4-4 BMC Network Configuration.....101
    - 5-4-5 IPv6 BMC Network Configuration.....102
  - 5-5 Security Menu ..... 103

5-5-1	Secure Boot .....	104
5-6	Boot Menu.....	107
5-7	Save & Exit Menu.....	109
5-8	BIOS Recovery .....	111
5-9	BIOS POST Beep code (AMI standard).....	112
5-9-1	PEI Beep Codes .....	112
5-9-2	DXE Beep Codes .....	112

# 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"> <li>◆ 2U 4-Node - Rear access</li> <li>◆ 440 (W) x 87.5 (H) x 840 (D) mm</li> </ul>
	CPU	<ul style="list-style-type: none"> <li>◆ 5th Generation Intel® Xeon® Scalable Processors</li> <li>◆ 4th Generation Intel® Xeon® Scalable Processors</li> <li>◆ Intel® Xeon® CPU Max Series</li> <li>◆ Dual processor per node, CPU TDP up to 385W</li> </ul>
NOTE: If only 1 CPU is installed, some PCIe or memory functions might be unavailable		
	Socket	<p><b>Per Node:</b></p> <ul style="list-style-type: none"> <li>◆ 2 x LGA 4677</li> </ul> <p><b>Total:</b></p> <ul style="list-style-type: none"> <li>◆ 8 x LGA 4677</li> <li>◆ Socket E</li> </ul>
	Chipset	<ul style="list-style-type: none"> <li>◆ Intel® C741 Chipset</li> </ul>
	Memory	<p><b>Per Node:</b></p> <ul style="list-style-type: none"> <li>◆ 16 x DIMM slots</li> </ul> <p><b>Total:</b></p> <ul style="list-style-type: none"> <li>◆ DDR5 memory supported only</li> <li>◆ 8-Channel memory architecture</li> <li>◆ RDIMM modules up to 96GB supported</li> <li>◆ 3DS RDIMM modules up to 256GB supported</li> <li>◆ 5th Gen Intel® Xeon®: Up to 5600MHz</li> <li>◆ 4th Gen Intel® Xeon®: Up to 4800MHz</li> <li>◆ Intel® Xeon® Max Series: Up to 4800MHz</li> </ul>
	LAN	<p><b>Per Node:</b></p> <ul style="list-style-type: none"> <li>◆ 1 x Dedicated management port</li> </ul> <p><b>Total:</b></p> <ul style="list-style-type: none"> <li>◆ 4 x Dedicated management ports</li> </ul>
	Video	<ul style="list-style-type: none"> <li>◆ Integrated in Aspeed® AST2600</li> <li>◆ 2D Video Graphic Adapter with PCIe bus interface</li> <li>◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM</li> </ul> <p>Management chip on CMC board:</p> <ul style="list-style-type: none"> <li>◆ Integrated in Aspeed® AST2520A2-GP</li> </ul>

	Storage	<p><b>Per node:</b></p> <ul style="list-style-type: none"> <li>◆ 6 x 2.5" Gen4 NVMe/SATA/SAS hot-swappable bays</li> </ul> <p><b>Total:</b></p> <ul style="list-style-type: none"> <li>◆ 24 x 2.5" Gen4 NVMe/SATA/SAS hot-swappable bays</li> </ul> <p><b>SAS card is required for SAS devices support</b></p>
	SAS	<ul style="list-style-type: none"> <li>◆ Supported via add-on SAS Card</li> </ul>
	RAID	<ul style="list-style-type: none"> <li>◆ Intel® SATA RAID 0/1/10/5</li> </ul>
	Expansion Slots	<p><b>Per node:</b></p> <ul style="list-style-type: none"> <li>◆ 1 x Low profile half-length slot with PCIe x16 (Gen5 x16 bus), from CPU_0</li> <li>◆ 1 x OCP 3.0 mezzanine slot with PCIe Gen5 x16 bandwidth, from CPU_0</li> <li>◆ Supported NCSI function</li> </ul> <p>*1 x M.2 slot from CPU_1:</p> <ul style="list-style-type: none"> <li>◆ M-key</li> <li>◆ PCIe Gen4 x4</li> <li>◆ Supports NGFF-2280/22110 cards</li> </ul> <p><b>Total:</b></p> <ul style="list-style-type: none"> <li>◆ 4 x Low profile half-length slots with PCIe x16 (Gen5 x16 bus), from CPU_0</li> <li>◆ 4 x OCP 3.0 mezzanine slots with PCIe Gen5 x16 bandwidth, from CPU_0</li> <li>◆ Supported NCSI function</li> </ul> <p>*4 x M.2 slots from CPU_1:</p> <ul style="list-style-type: none"> <li>◆ M-key</li> <li>◆ PCIe Gen4 x4</li> <li>◆ Supports NGFF-2280/22110 cards</li> </ul> <p><b>Optional kit for M.2 extension riser card/PN: 9CMTP061NR-00</b></p>

	Internal I/O	<b>Per Node:</b>	<ul style="list-style-type: none"> <li>◆ 1 x TPM header</li> </ul>
	Front I/O	<b>Per node:</b>	<ul style="list-style-type: none"> <li>◆ 1 x Power button with LED</li> <li>◆ 1 x ID button with LED</li> <li>◆ 1 x Status LED</li> <li>◆ 1 x System reset button</li> </ul>
		<b>Total:</b>	<ul style="list-style-type: none"> <li>◆ 4 x Power button with LED</li> <li>◆ 4 x ID button with LED</li> <li>◆ 4 x Status LED</li> <li>◆ 4 x System reset button</li> <li>◆ *1 x CMC status LED</li> <li>◆ *1 x CMC reset button</li> </ul>
		<b>*Only one CMC status LED and reset button per system</b>	
	Rear I/O	<b>Per node:</b>	<ul style="list-style-type: none"> <li>◆ 2 x USB 3.2 Gen1</li> <li>◆ 1 x VGA</li> <li>◆ 1 x RJ45 MLAN</li> <li>◆ 1 x ID button with LED</li> </ul>
		<b>Total:</b>	<ul style="list-style-type: none"> <li>◆ 8 x USB 3.2 Gen1</li> <li>◆ 4 x VGA</li> <li>◆ 4 x RJ45 MLAN</li> <li>◆ 4 x ID button with LED</li> <li>◆ *1 x CMC global management port</li> </ul>
		<b>*Only one CMC status LED and reset button per system</b>	
	Backplane I/O	<ul style="list-style-type: none"> <li>◆ Speed and bandwidth:</li> <li>◆ PCIe Gen4 x4 or SATA 6Gb/s or SAS 12Gb/s</li> </ul>	
	TPM	<ul style="list-style-type: none"> <li>◆ 1 x TPM header with SPI interface</li> <li>◆ Optional TPM2.0 kit: CTM010</li> </ul>	



## Power Supply

### **H263-S62-LAN1**

- ◆ Dual 2600W (240V) 80 PLUS Titanium redundant power supply
- ◆ Available for 2+1 redundant power supply configuration (optional)

#### AC Input:

- ◆ 100-127V~/ 13.8A, 50-60Hz
- ◆ 200-240V~/ 15A, 50-60Hz

#### DC Input:

- ◆ 240Vdc/ 15A

#### DC Output:

- ◆ Max 1000W/ 100-127V~
- ◆ + 12.2V/ 81A
- ◆ + 12.2Vsb/ 4.5A
- ◆ Max 2600W/ 200-220V~
- ◆ + 12.2V/ 213A
- ◆ + 12Vsb/ 4.5A

NOTE: The system power supply requires C19 type power cord

### **H263-S62-LAW1**

- ◆ Dual 3000W (240V) 80 PLUS Titanium redundant power supply
- ◆ Available for 2+1 redundant power supply configuration (optional)

#### AC Input:

- ◆ 100-127V~/ 16A, 50-60Hz
- ◆ 200-240V~/ 16A, 50-60Hz

#### DC Input:

- ◆ 240Vdc/ 16A

#### DC Output:

- ◆ Max 1200W/ 100-127V~
- ◆ + 12.2V/ 98.36A
- ◆ + 12.2Vsb/ 3A
- ◆ Max 2600W/ 200-207V~
- ◆ + 12.2V/ 213A
- ◆ + 12.2Vsb/ 3A
- ◆ Max 3000W/ 208-240V~
- ◆ + 12.2V/ 245.9A
- ◆ + 12.2Vsb/ 3A

NOTE: The system power supply requires C19 type power cord



## System Management

- ◆ Aspeed® AST2600 management controller
- ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) 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
- ◆ 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



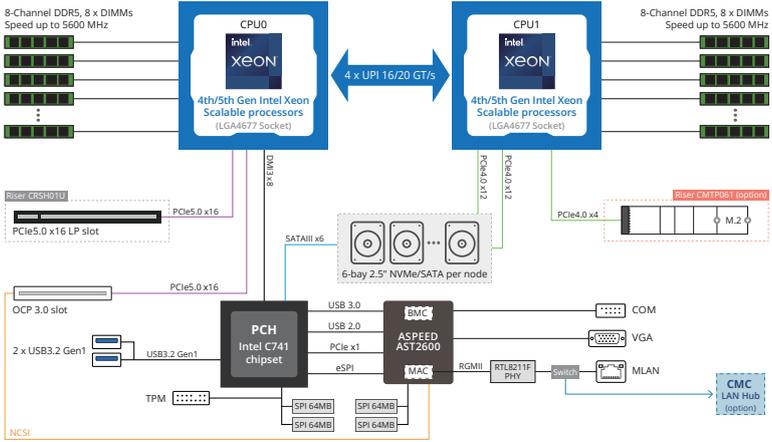
## Operating Properties

- ◆ 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)

### NOTE!

- ◆ **The environment ambient temperature and relative humidity are relative to the inlet supply water temperature and the coolant flow rate.**
- ◆ **In the event that the room's relative humidity exceeds 60% then the inlet water temperature must be set between 40° to 45°C to avoid condensation and to keep the system running optimally.**

# 1-3 System Block Diagram



• Please Go to Chapter 4 Motherboard Components for Riser Slot information.

# Chapter 2 System Appearance

## 2-1 Front View

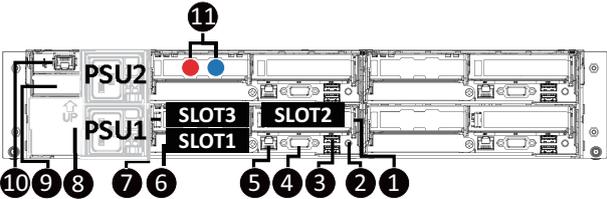


No.	Description
1.	Front Panel LEDs and buttons
<b>NOTE! Drives with green latches support NVMe.</b>	



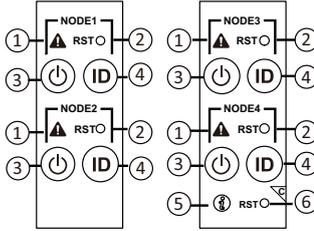
- Please Go to Chapter 2-3 Front Panel LED and Buttons for detail description of function LEDs.

## 2-2 Rear View



No.	Description
1.	PCIe Slot
2.	ID Button
3.	2 x USB 3.2 Gen1
4.	VGA Port
5.	BMC Server Management LAN Port
6.	OCP 3.0 Slot (SFF Type)
7.	PCIe Slot
8.	CMC LAN Port
9.	Ring Topology Kit (Option)
10.	2+1 Redundant Power Supply Unit (Option)
11.	Coolant Pipe Slot

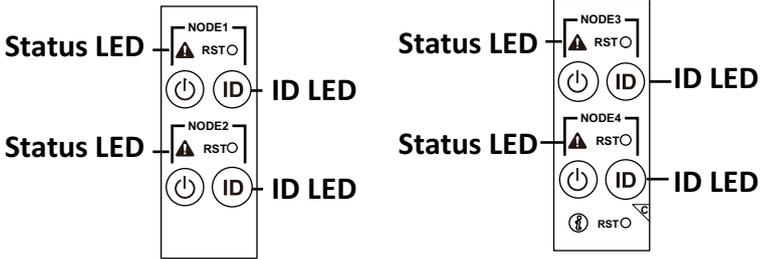
## 2-3 Front Panel LED and Buttons



No.	Name	Color	Status	Description
1.	System Status LED <sup>(Note)</sup>	Green	Solid On	System is operating normally.
		Amber	Solid On	Critical condition, may indicate: System fan failure System temperature
			Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion
		N/A	Off	System is not ready, may indicate: POST error NMI error Processor or terminator missing
2.	Reset Button	--	--	Press this button to reset the system.
3.	Power button with LED	Green	On	System is powered on
		Green	Blink	System is in ACPI S1 state (sleep mode)
		N/A	Off	<ul style="list-style-type: none"> <li>System is not powered on or in ACPI S5 state (power off)</li> <li>System is in ACPI S4 state (hibernate mode)</li> </ul>
4.	ID Button with LED <sup>(Note)</sup>	Blue	On	System identification is active.
		N/A	Off	System identification is disabled.
5.	Enclosure	Green	On	System is operating normally.
		Amber	On	Critical condition, may indicate: Power module failure System fan failure Power supply voltage issue System temperature
			Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue
6.	CMC Reset Button	--	--	Press this button to reset the CMC.

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

## 2-4 RoT LEDs



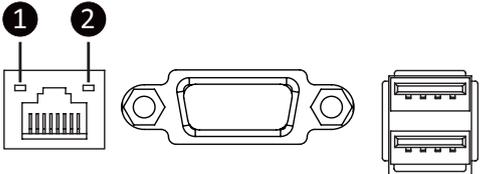
LED on Front panel <sup>(Note5)</sup>		
	ID LED	Status LED
<b>EC Firmware (FW) Authentication fail or not exit</b>		
EC FW is broken or not exit <sup>(Note1)</sup>	OFF	OFF
<b>Authenticating/Recovering BMC/BIOS Images</b>		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times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

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

## NOTE!

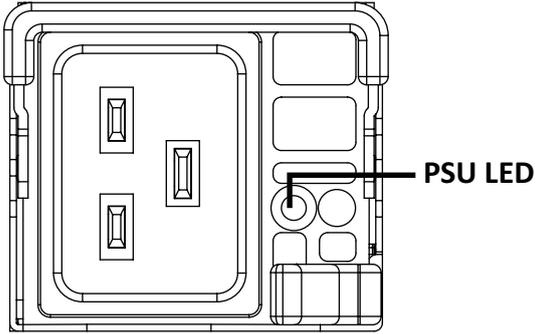
- EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
- (1) Authentication fail include below scenarios  
Configuration table is missing or modified  
Public key is missing or modified  
Protected area or signature is modified  
Flash empty
- if active flash is still authentication failed after recovery sequence, Microchip CEC1702 stop the process and showing LED behavior.
- 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.
- 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.

## 2-5 Rear System LAN LEDs



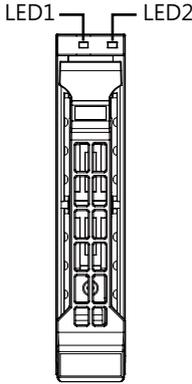
No.	Name	Color	Status	Description
1.	1GbE Speed LED	Yellow	On	1Gbps data rate
		Green	On	100 Mbps data rate
		N/A	Off	10 Mbps data rate
2.	1GbE Link/Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or receiving is occurring
		N/A	Off	No data transmission or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

## 2-6 Power Supply Unit LED



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

# 2-7 Hard Disk Drive LEDs



RAID SKU		LED1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA)	Disk LED (LED on Back Panel)	Green	ON(*1)	OFF		BLINK (*2)	OFF
		Amber	OFF	OFF		OFF	OFF
	Removed HDD Slot (LED on Back Panel)	Green	ON(*1)	OFF		--	--
		Amber	OFF	OFF		--	--
RAID configuration (via HW RAID Card or SW RAID Card)	Disk LED	Green	ON	OFF		BLINK (*2)	OFF
		Amber	OFF	ON	(Low Speed: 2 Hz)	OFF	OFF
	Removed HDD Slot	Green	ON(*1)	OFF	(*3)	--	--
		Amber	OFF	ON	(*3)	--	--

LED 2	HDD Present	No HDD
Green	ON	OFF

NOTE:

\*1: Depends on HBA/Utility Spec.

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

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

## Chapter 3 System Hardware Installation



### Pre-installation Instructions

Computer components and electronic circuit boards can be damaged 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 Installing the Hard Disk Drive

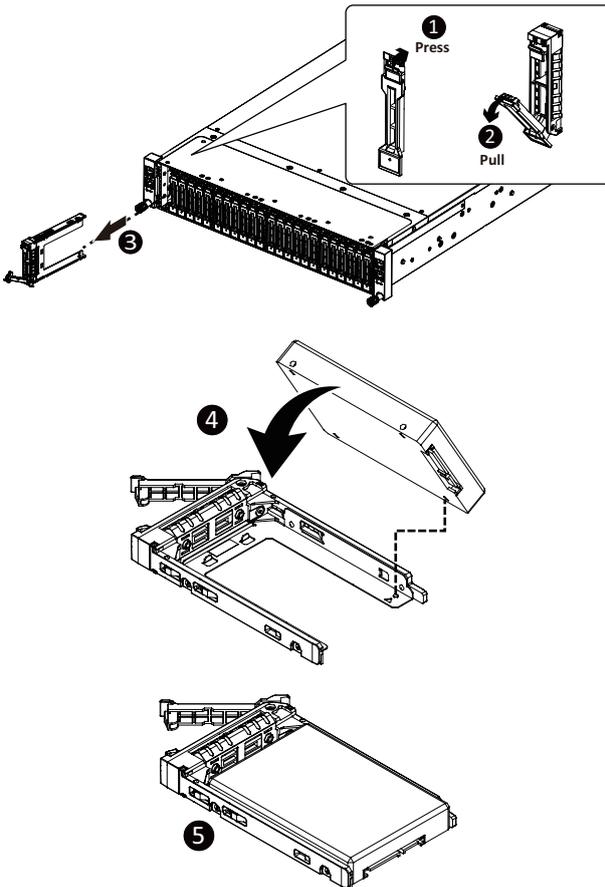


Read the following guidelines before you begin to install the Hard disk drive:

- 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 HDD is connected to the HDD connector on the backplane.

Follow these instructions to install the Hard disk drive:

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



## 3-2 Removing the Node

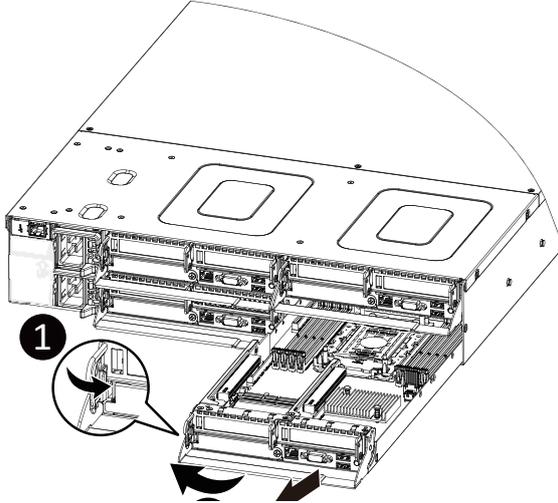


Read the following guidelines before you begin to replace a node:

- To make sure the system operates normally, please power off only the node that will be replaced or reconfigured.

Follow these instructions to remove a node:

1. Press the release latch while simultaneously pushing down the tray handle for the node.
2. Pull the node out of the system.
3. To install the node, push the node back into the system.



### 3-3 Removing Chassis Cover

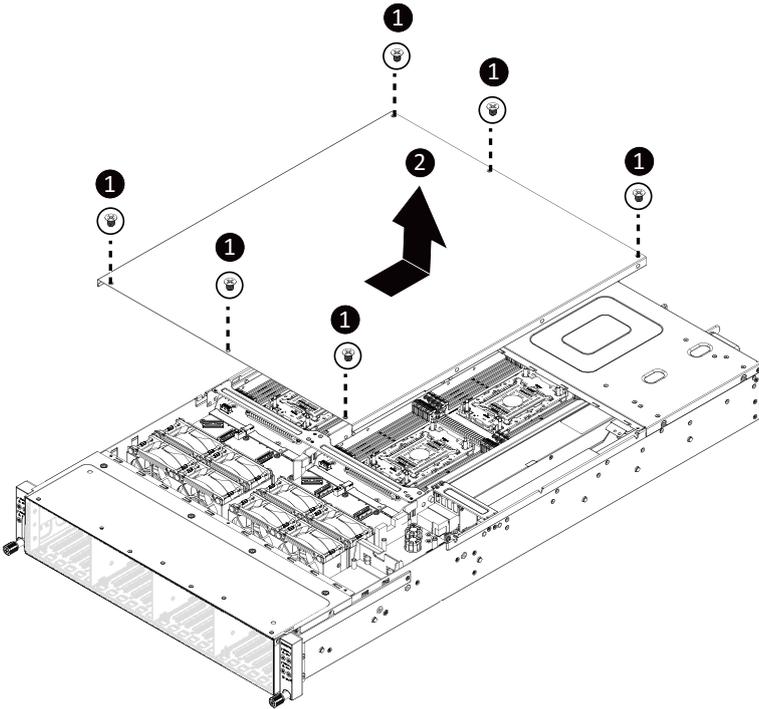


Before you remove or install the system cover

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

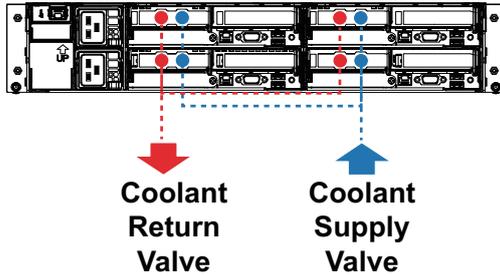
Follow these instructions to remove the system cover:

1. Loosen and remove the six screws securing the back cover.
2. Slide the cover to the rear of the system and remove the cover in the direction of the arrow.

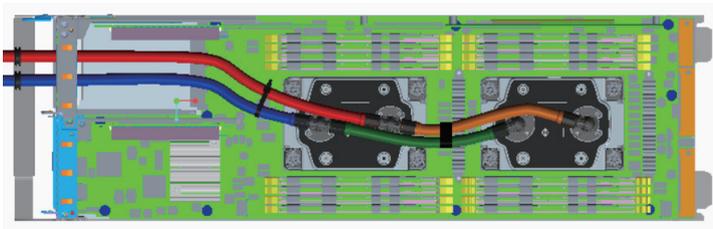


### 3-4 Liquid Cooling Assembly Information

The liquid cooling assembly is designed to capture heat from the processors in the node and cool the components. The coolant flow for the assembly is produced by the eight quick disconnects at the rear of the server chassis.



The flow of the coolant is shown below:



Flow Order	Component
First	CPU1 Cold Plate
Second	CPU0 Cold Plate
Third	To coolant return CPU1
Fourth	To coolant return

### 3-4-1 Liquid Cooling Specifications

The cold plate assembly in the liquid cooling assembly mounts directly on top of the processors.

The retention mechanism for installation on top of the processors is integrated into the cold plate. The liquid coolant contained within the tubes, is a mixture of demineralized water and propylene glycol with the following beneficial features: Anti-Freeze, Anti-Corrosion and Anti Bacterial. The following table lists the features and specifications of the liquid cooling assembly.

Specification	Value
Cold plate material	Copper
Thermal Interface Material	Dowsil TC-5622
Operating liquid temperature	Minimum: 2°C Maximum: 65°C
Operating Air temperature	40°C
Coolant Flow Rate	0.75 - 1.4 l/min (per node)
Operating Humidity	5 - 95%
Storage Temperature	-40°C to 70°C
Storage Humidity	5 - 95%
<b>Dimensions</b>	
Height	24.01 mm
Weight	1.87 lbs (848g per node)

**NOTE:** In the event that the room's relative humidity exceeds 60% then the inlet water temperature must be set between 40° to 45°C to avoid condensation and to keep the system running optimally.

### 3-5 Removing the Coolant Pipe Module



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

- Always turn off the computer and unplug the power cord from the power outlet before installing the module 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!**

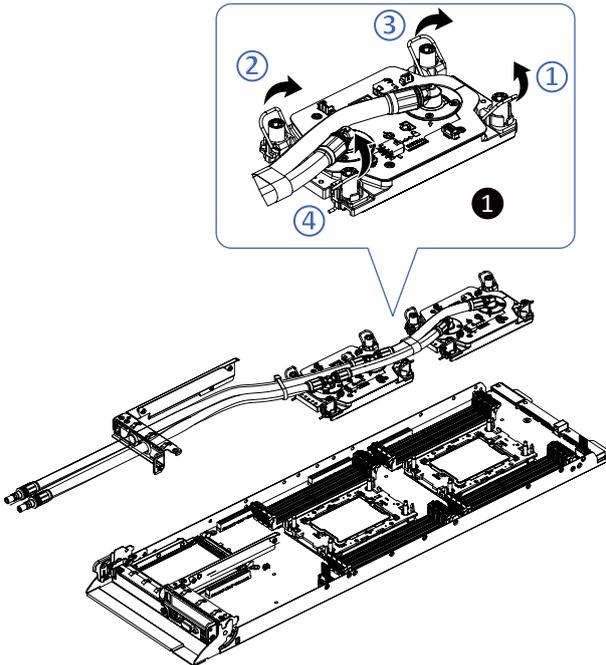
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

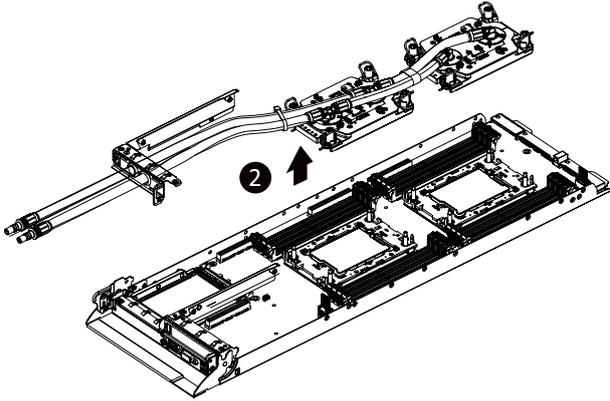
Follow these instructions to remove the coolant pipe module:

1. Remove the left PCIe riser before removing the CPU coolant module. To remove PCIe bracket, see page 38 Installing the PCI Expansion Card.
2. Loosen the four captive screws securing the coolant pipe module to the system.
3. Lift and remove the coolant pipe..



- Lock the CPU coolant by using a T30-Lobe driver to tighten screw.
- When installing the coolant to CPU, use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4.





### 3-6 Installing the CPU and the Coolant Pipe Module



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

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



**WARNING!**

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

Follow these instructions to install the CPU:

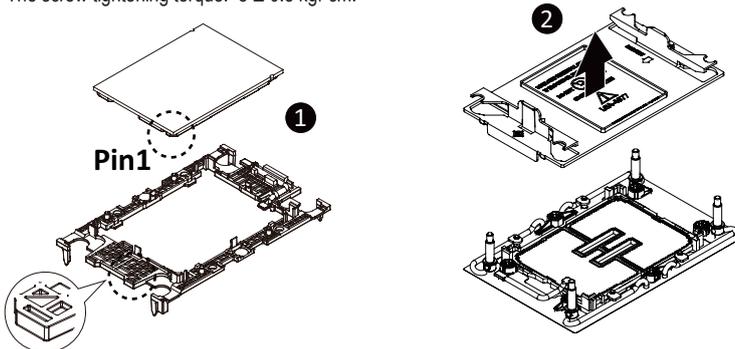
1. Align the processor to the carrier so that the gold triangle on the processor aligns with the triangle on the carrier, and then install the processor into the carrier.  
NOTE: Apply thermal compound evenly on the top of the CPU.
2. Remove the CPU socket cover.  
NOTE: Save and replace the CPU socket cover if the processor is removed from its socket.

#### Carrier Types used for Package Types

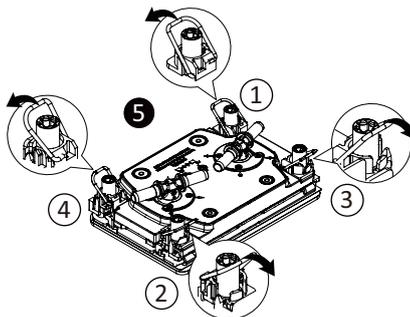
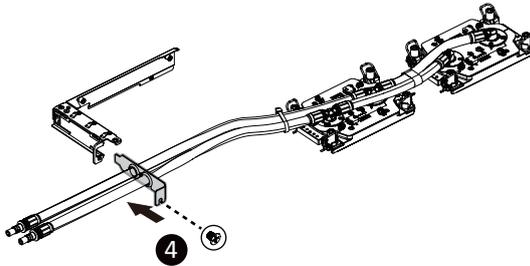
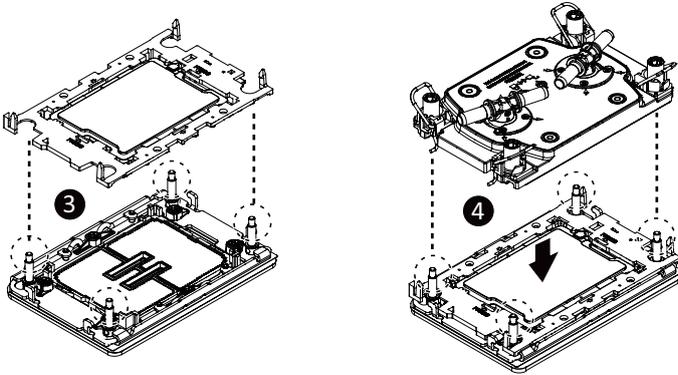
Package Type	Xeon® SP XCC	Xeon® SP MCC	Xeon® SP+HBM
Carrier Code	E1A	E1B	E1C

**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 coolant pipe module to CPU,use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4.
- The screw tightening torque:  $8 \pm 0.5$  kgf-cm.



3. Loosen the four captive screws securing the carrier assembly to the system.
4. Put the Coolant pipe through the PCIe 1 bracket and put the PCIe bracket and coolant bracket together. Use the retained screw to lock the PCIe 1 bracket.
5. Align the carrier assembly to the CPU socket using the guide pins and make sure the gold triangle is in the correct orientation. Then place the carrier assembly onto the top of the CPU socket.
6. Secure the carrier assembly by tightening the screws in sequential order (1→2→3→4).



### 3-6-1 Installing the Memory

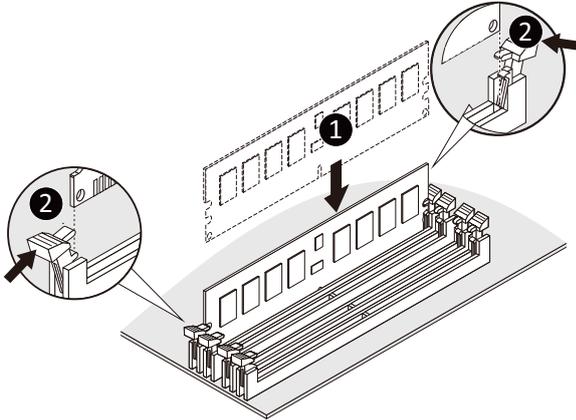


Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR5 DIMMs on this motherboard.

Follow these instructions to install the Memory:

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



### 3-6-2 DIMM Population Table

#### 4th Gen Intel Xeon Scalable Processors-SP Memory Support

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); DIMM per Channel (DPC)	
		16Gb	24Gb <sup>2</sup>	36Gb	1DPC <sup>1</sup>	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-SP Memory Support

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); DIMM per Channel (DPC)	
		16Gb	24Gb <sup>2</sup>	36Gb	1DPC <sup>1</sup>	2DPC
					1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	NA	5600 <sup>3</sup>	4400 <sup>3</sup>
	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 <sup>4</sup>	

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.

3-6-3 Processor and Memory Module Matrix Table

Memory Q'ty for each CPU	CPU0								CPU1							
	H0	G0	F0	E0	A0	B0	C0	D0	P0	O0	N0	M0	I0	J0	K0	L0
1 DIMM					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
12 DIMM	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

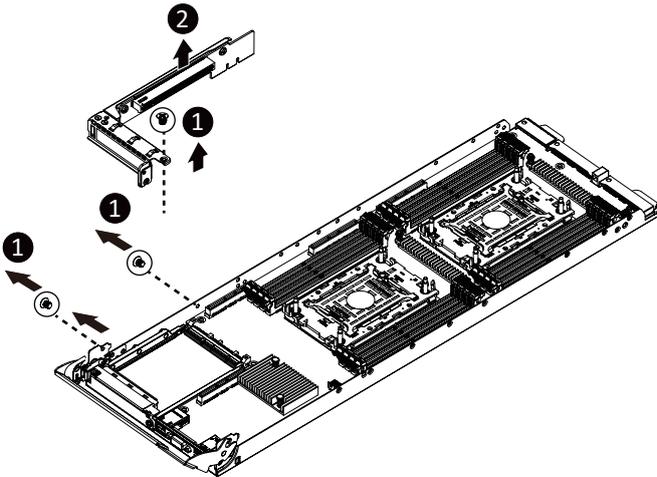
## 3-7 Installing the PCI Expansion Card

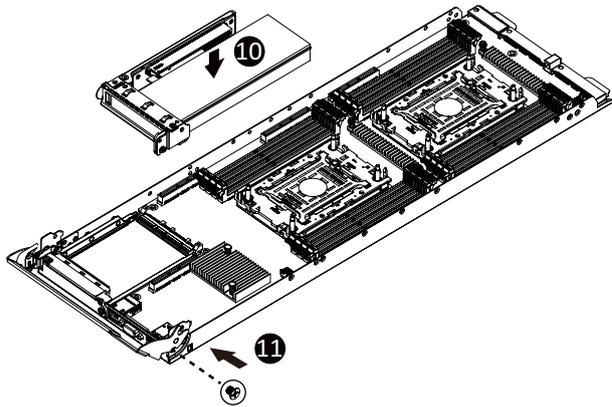
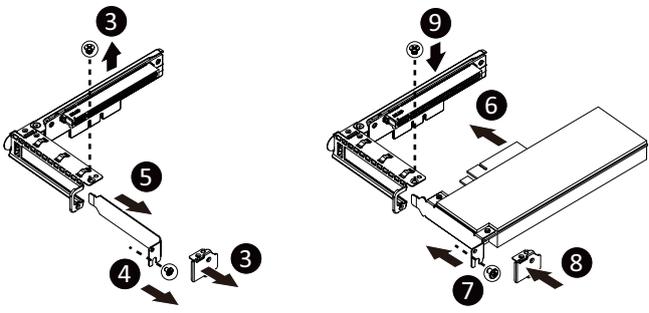
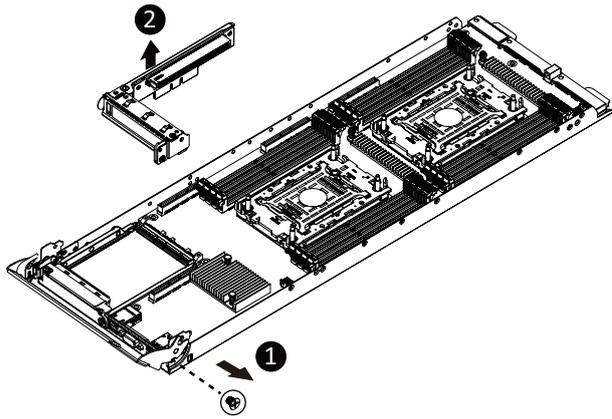


- The PCI riser assembly does not include a riser card or any cabling as standard. To install a PCI card, a riser card must be installed.

Follow these instructions to install the PCI Expansion card:

1. Remove the three screw on the riser bracket to the system.
2. Lift up the riser bracket out of system.
3. Remove the one screw securing the riser bracket to the system.
4. Lift up the riser bracket out of system.
5. Remove the PCI screw and bracket.
6. Remove the side bracket
7. Align the PCIe card to the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCI card connector.
8. Secure the PCIe card with a screw.
9. Install the side bracket to the riser bracket.
10. Reverse steps 1 - 9 to install the two riser brackets back into the system.





## 3-8 Installing the Mezzanine Card

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

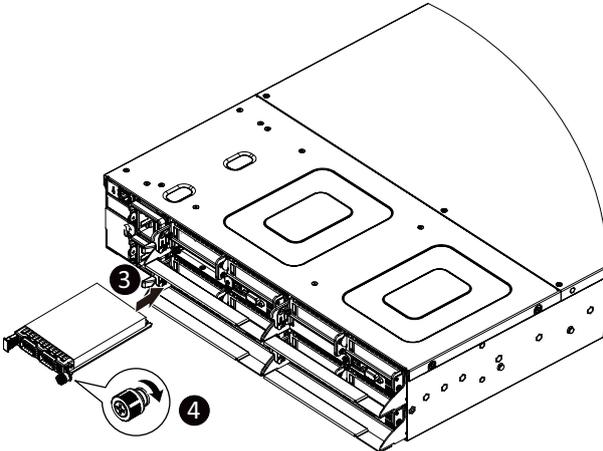
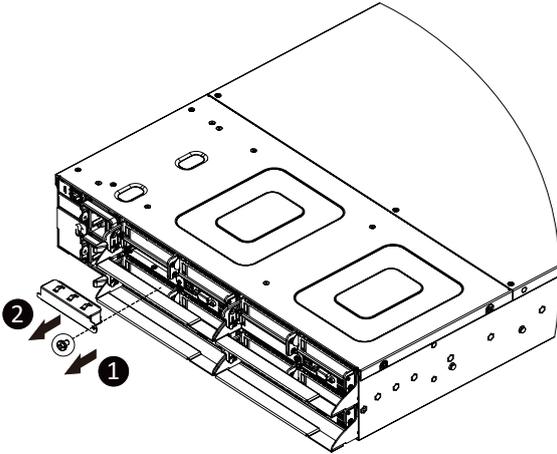


Use of the following type of OCP 3.0 NIC is recommended:

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

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

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



### 3-9 Replacing the Fan Assembly

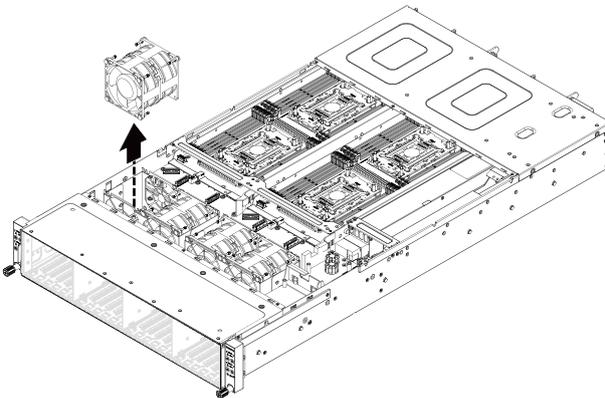
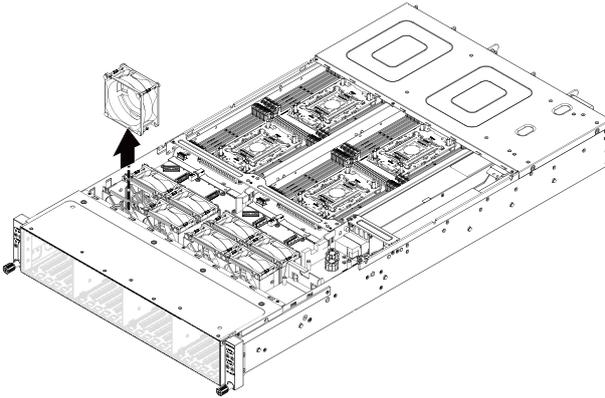


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

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

Follow these instructions to replace the fan assembly:

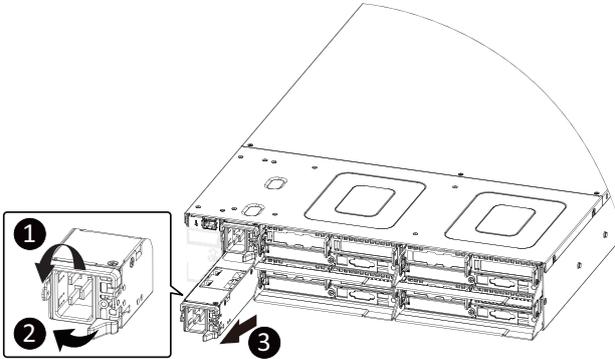
1. Lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



## 3-10 Replacing the Power Supply

Follow these instructions to replace the power supply:

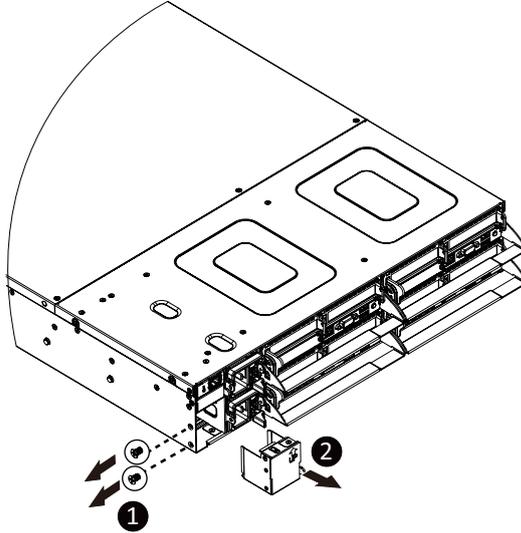
1. Pull up the power supply handle and press the retaining clip on the right side of the power supply along the direction of the arrow. At the same time, pull out the power supply by using its handle.
2. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.



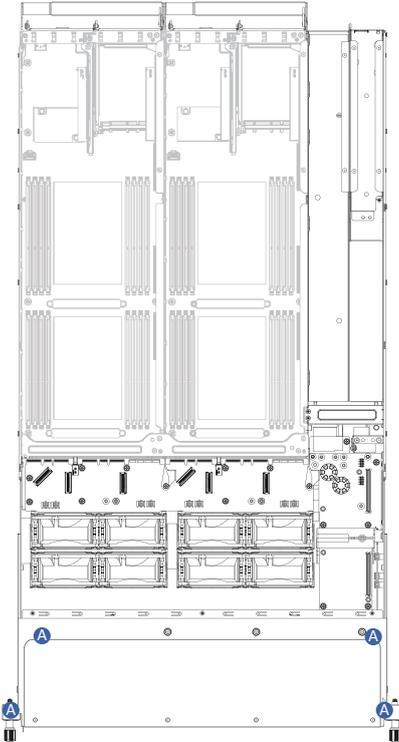
### 3-11 Removing the Power Supply Dummy Cover

Follow these instructions to remove the power supply dummy cover:

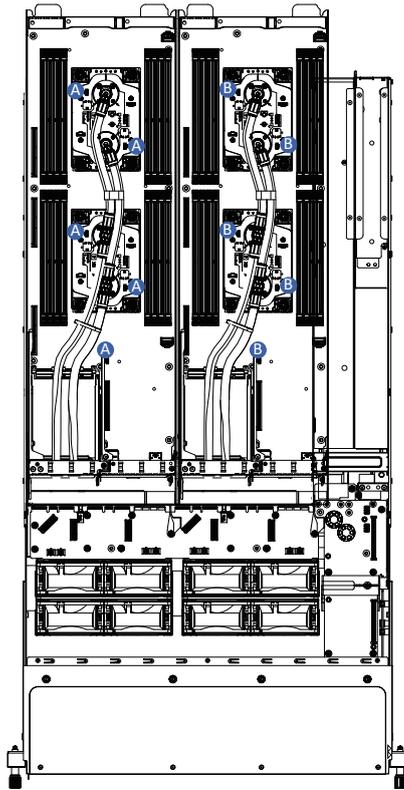
1. Remove the two screws on the system.
2. Pull up the cover handle, at the same time, pull out the metal cover by using its handle.
3. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.



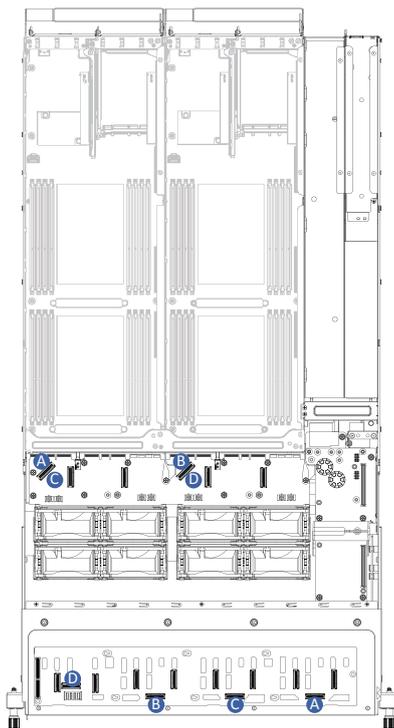
### 3-12 Cable Routing



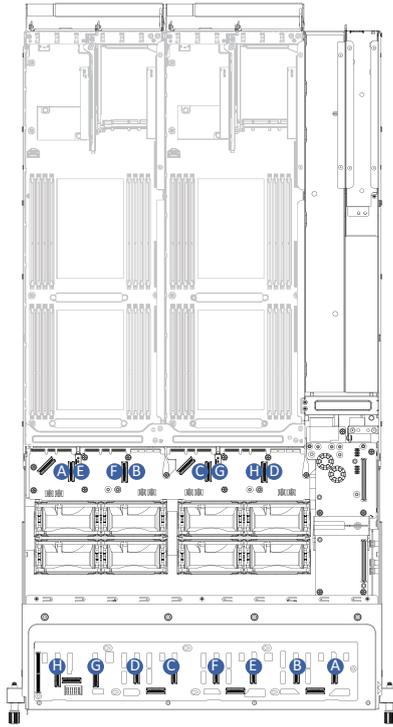
A	Front Panel LEDs and Buttons Cable	Motherboard: FP_1 Front IO Board: FP_1
		Front IO Board: FP_1



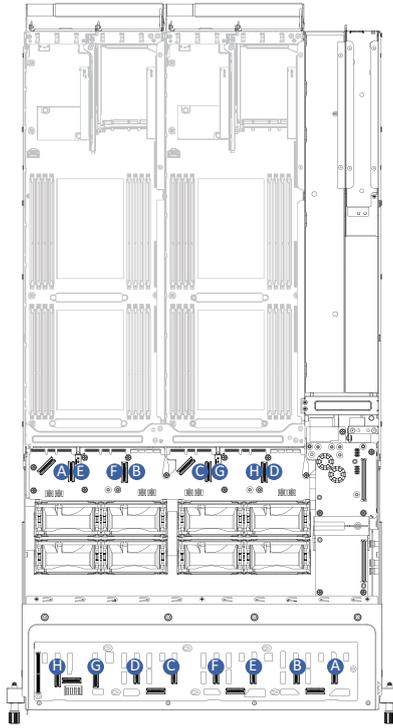
A	Leak Sensor Board Cable	Sensor Board: LEAK_TOP
		PCIe Board: CON
B	Leak Sensor Board Cable	Sensor Board: LEAK_TOP
		PCIe Board: CON



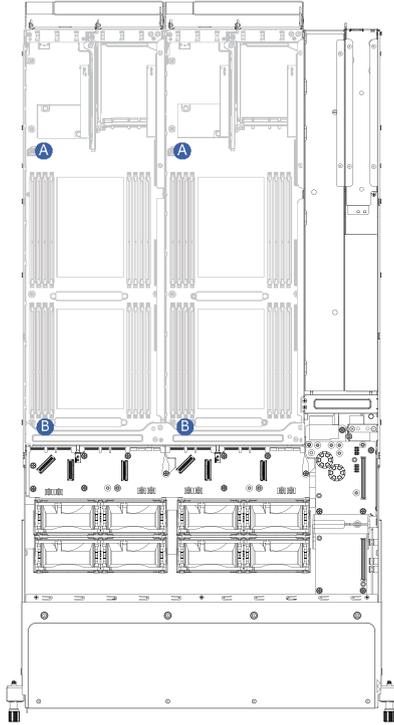
A	Top Middle Board to HDD Back Plane Board Cable (SATA1)	Middle Board: N1_SATA
		F/ HDD Board: N1 SATA
B	Top Middle Board to HDD Back Plane Board Cable (SATA3)	Middle Board: N3_SATA
		F/ HDD Board: N3 SATA
C	Bottom Middle Board to HDD Back Plane Board Cable (SATA2)	Middle Board: N2_SATA
		F/ HDD Board: N2 SATA
D	Bottom Middle Board to HDD Back Plane Board Cable (SATA4)	Middle Board: N4_SATA
		F/ HDD Board: N4 SATA



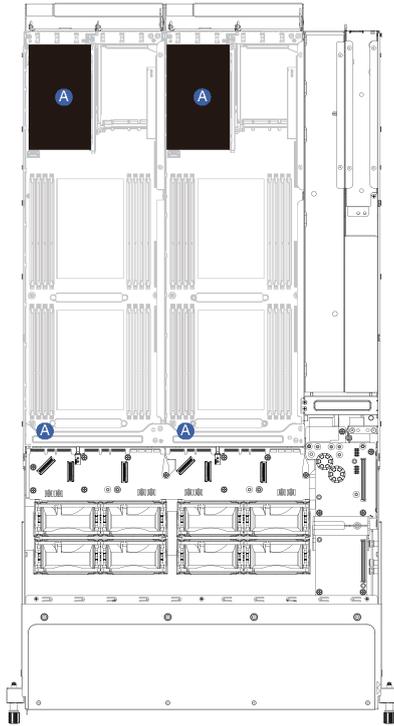
A	Top Middle Board to HDD Back Plane Board Cable (NVMe/Node1)	Middle Board: N1_U2_B
		F/ HDD Board: N1 U.2 A
B	Top Middle Board to HDD Back Plane Board Cable (NVMe/Node1)	Middle Board: N1_U2_A
		F/ HDD Board: N1 U.2 B
C	Top Middle Board to HDD Back Plane Board Cable (NVMe/Node3)	Middle Board: N3_U2_B
		F/ HDD Board: N3 U.2 A
D	Top Middle Board to HDD Back Plane Board Cable (NVMe/Node3)	Middle Board: N3_U2_A
		F/ HDD Board: N3 U.2 B



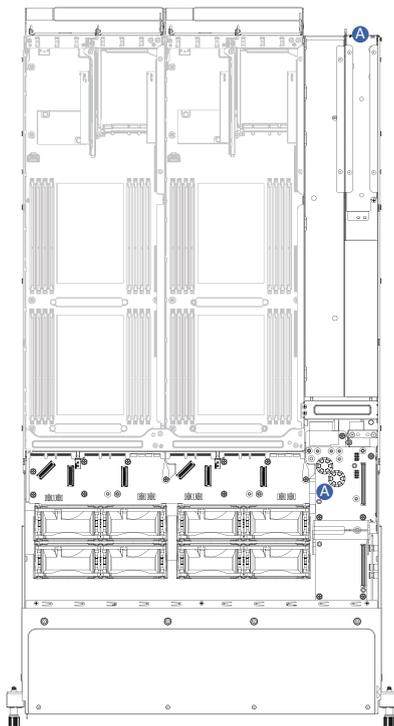
E	Bottom Middle Board to HDD Back Plane Board Cable (NVMe/Node2)	Middle Board: N2_U2_B
		F/ HDD Board: N2_U.2 A
F	Bottom Middle Board to HDD Back Plane Board Cable (NVMe/Node2)	Middle Board: N1_U2_A
		F/ HDD Board: N2_U.2 B
G	Bottom Middle Board to HDD Back Plane Board Cable (NVMe/Node4)	Middle Board: N4_U2_B
		F/ HDD Board: N4_U.2 A
H	Bottom Middle Board to HDD Back Plane Board Cable (NVMe/Node4)	Middle Board: N1_U2_A
		F/ HDD Board: N4_U.2 B



A	On board SATA Cable	Motherboard: SL4_SATA0
B		Motherboard: SL4_SATA1



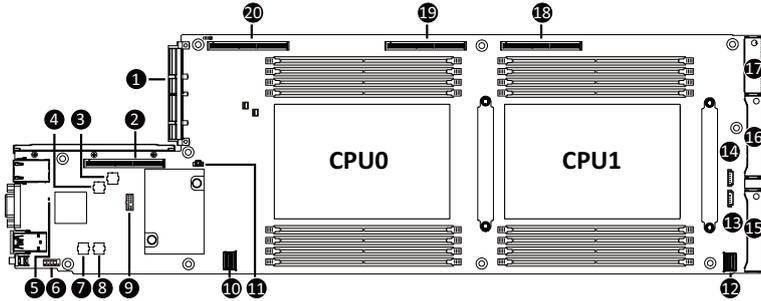
A	SAS RAID Card Cable	Motherboard: SL4_SATA1
		RAID Card



A	Rera LAN Module Cable	PDB Board: R_MLAN
		LAN Module Board: F_MLAN

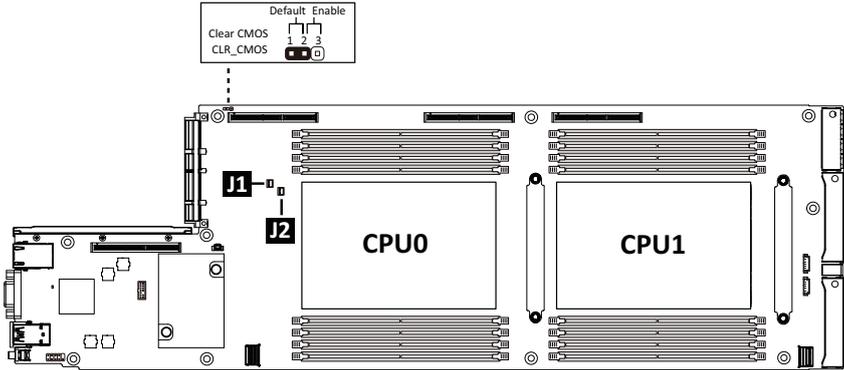
# Chapter 4 Motherboard Components

## 4-1 Motherboard Components



Item	Description
1	OCP 3.0 Connector (PCIe Gen5 x16)
2	Proprietary PCIe Slot (Gen 5/ x16 slot/ GENZ_2)
3	BIOS Flash ROM #2
4	BIOS Flash ROM #1
5	BMC Readiness LED
6	Serial Port Cable Connector
7	BMC Flash ROM #1
8	BMC Flash ROM #2
9	TPM Module Connector
10	SlimLine SAS Connector (SL4_SATA0/SATA Signal)
11	System Battery Cable Connector
12	SlimLine SAS Connector (SL4_SATA1/SATA Signal)
13	SGPIO Connector (SGPA1)
14	SGPIO Connector (SGPB1)
15	PCIe/SATA Connector
16	PCIe Connector
17	Power Connector
18	Proprietary PCIe Slot (Gen 5/ x16 slot/ GENZ_3)
19	Proprietary PCIe Slot (Gen 5/ x16 slot/ GENZ_3)
20	Proprietary PCIe Slot (Gen 5/ x16 slot/ GENZ_1)

## 4-2 Jumper Setting

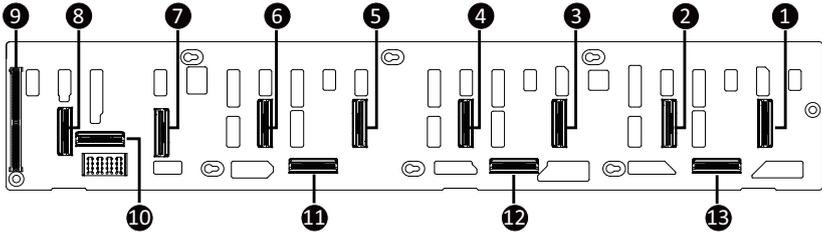


J1		ON	OFF
1	HSMB_SEL	BIOS defined	
2	SPD_SEL	BIOS defined	
3	S3_MASK	Stop initial power on when BMC is not ready	Normal [Default]
4	DP_PLD	CPLD debug mode	Normal [Default]

J2		ON	OFF
1	ME_UPDATE	Force ME update	Normal [Default]
2	BIOS_PWD	Clear supervisor password	Normal [Default]
3	BIOS_RCVR	BIOS recovery mode	Normal [Default]
4	ME_RCVR	ME recovery mode	Normal [Default]

## 4-3 Backplane Board Storage Connector

### 4-3-1 CBPH701



Item	Description
1	SlimLine SAS Connector (N1 U.2 A)
2	SlimLine SAS Connector (N1 U.2 B)
3	SlimLine SAS Connector (N2 U.2 A)
4	SlimLine SAS Connector (N2 U.2 B)
5	SlimLine SAS Connector (N3 U.2 A)
6	SlimLine SAS Connector (N3 U.2 B)
7	SlimLine SAS Connector (N4 U.2 A)
8	SlimLine SAS Connector (N4 U.2 B)
9	Proprietary PCIe Slot (x8 slot/ GF_HDD)
10	SlimLine SAS Connector (N4 SATA)
11	SlimLine SAS Connector (N3 SATA)
12	SlimLine SAS Connector (N2 SATA)
13	SlimLine SAS Connector (N1 SATA)

## Chapter 5 BIOS Setup

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

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



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

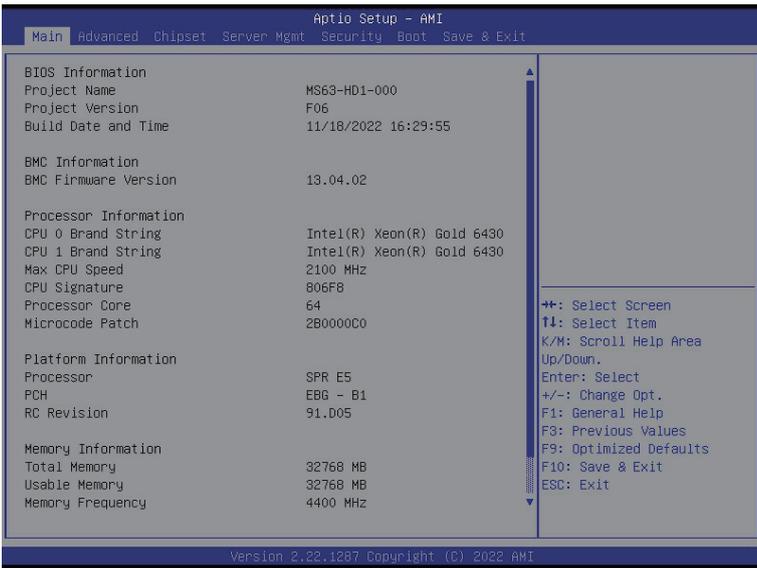
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

## 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 <sup>(Note1)</sup>	
BMC Firmware Version <sup>(Note1)</sup>	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 <sup>(Note2)</sup>	
Total Memory	Displays the total memory size of the installed memory.
Usable Memory	Displays the usable memory size of the installed memory.

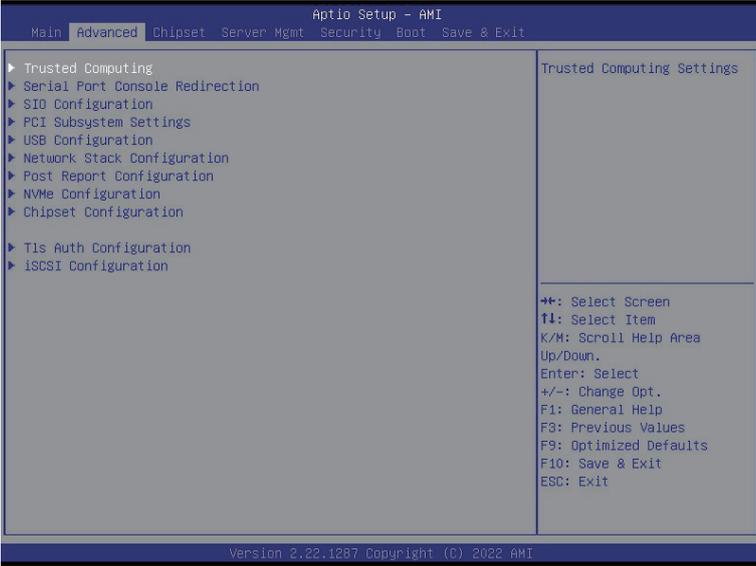
(Note1) Functions available on selected models.

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

<b>Parameter</b>	<b>Description</b>
Memory Frequency	Displays the frequency information of the installed memory.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

## 5-2 Advanced Menu

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

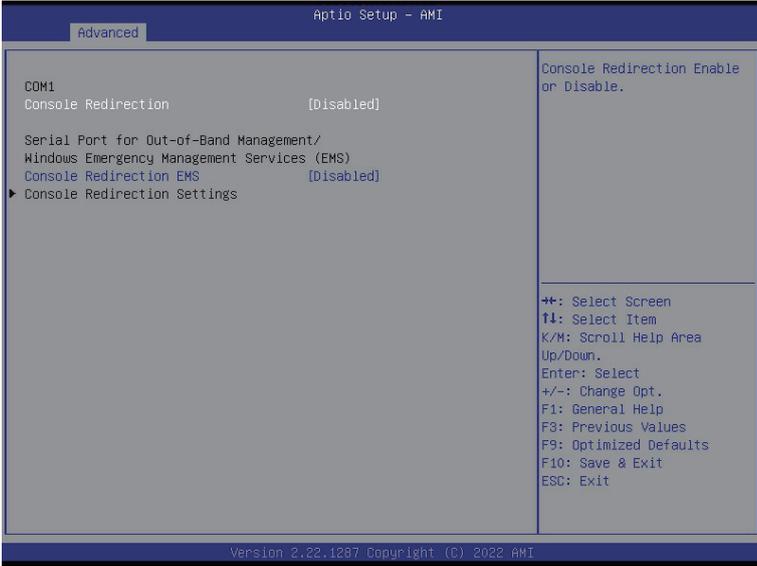


## 5-2-1 Trusted Computing



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

## 5-2-2 Serial Port Console Redirection



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

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

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

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

### 5-2-3 SIO Configuration



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

## 5-2-4 PCI Subsystem Settings

Aptio Setup - AMI

Advanced

PCI Bus Driver Version	A5.01.29	Enable/Disable SLOT1_OCP3 I/O ROM ++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT1_OCP3 I/O ROM	[Enabled]	
SLOT1_OCP3 Lanes	[Auto]	
SLOT1_OCP3 Max Link Speed	[Auto]	
SLOT2_G2_2 I/O ROM	[Enabled]	
SLOT2_G2_2 Lanes	[Auto]	
SLOT2_G2_2 Max Link Speed	[Auto]	
SLOT3_G2_1 I/O ROM	[Enabled]	
SLOT3_G2_1 Lanes	[Auto]	
SLOT3_G2_1 Max Link Speed	[Auto]	
GEN2_3 I/O ROM	[Enabled]	
GEN2_3 Lanes	[Auto]	
GEN2_3 Max Link Speed	[Auto]	
GEN2_4 I/O ROM	[Enabled]	
GEN2_4 Lanes	[Auto]	
GEN2_4 Max Link Speed	[Auto]	
PCI Devices Common Settings:		
Above 4G Decoding	[Enabled]	
SR-IOV Support	[Enabled]	

Version 2.22.1287 Copyright (C) 2022 AMI

Aptio Setup - AMI

Advanced

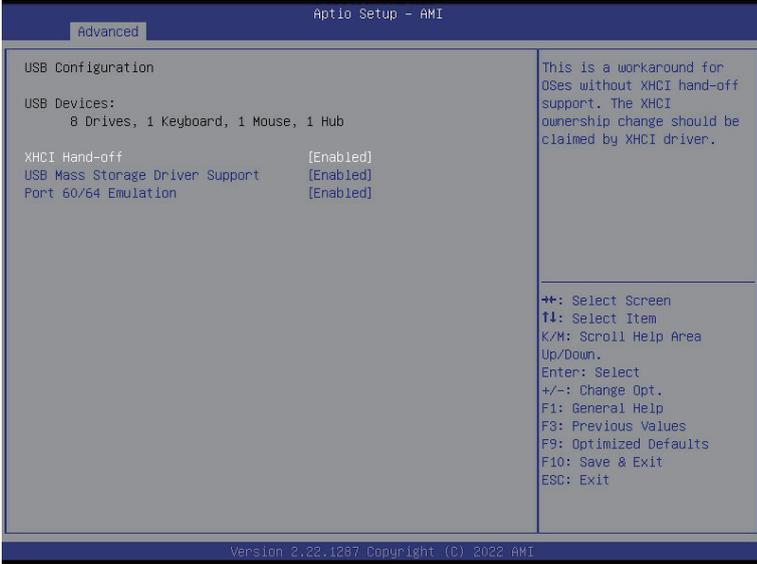
SLOT1_OCP3 Lanes	[Auto]	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root ID Virtualization Support. ++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT1_OCP3 Max Link Speed	[Auto]	
SLOT2_G2_2 I/O ROM	[Enabled]	
SLOT2_G2_2 Lanes	[Auto]	
SLOT2_G2_2 Max Link Speed	[Auto]	
SLOT3_G2_1 I/O ROM	[Enabled]	
SLOT3_G2_1 Lanes	[Auto]	
SLOT3_G2_1 Max Link Speed	[Auto]	
GEN2_3 I/O ROM	[Enabled]	
GEN2_3 Lanes	[Auto]	
GEN2_3 Max Link Speed	[Auto]	
GEN2_4 I/O ROM	[Enabled]	
GEN2_4 Lanes	[Auto]	
GEN2_4 Max Link Speed	[Auto]	
PCI Devices Common Settings:		
Above 4G Decoding	[Enabled]	
SR-IOV Support	[Enabled]	

Version 2.22.1287 Copyright (C) 2022 AMI

Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT1_OCP3 SLOT2_GZ_2 SLOT3_GZ_1 GENZ_3_ GENZ_4 I/O ROM <sup>(Note1)</sup>	When enabled, this setting will initialize the device expansion ROM for the related PCIe/OCF slot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
SLOT1_OCP3 SLOT2_GZ_2 SLOT3_GZ_1 GENZ_3 GENZ_4 Lanes <sup>(Note1)</sup>	Change the PCIe/OCF lanes. Default setting is <b>Auto</b> .
SLOT1_OCP3 SLOT2_GZ_2 SLOT3_GZ_1 GENZ_3 GENZ_4 Max Link Speed <sup>(Note1)</sup>	Configure PCIe max link speed. Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5. Default setting is <b>Auto</b> .
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 <b>Enabled</b> .
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

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

## 5-2-5 USB Configuration



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

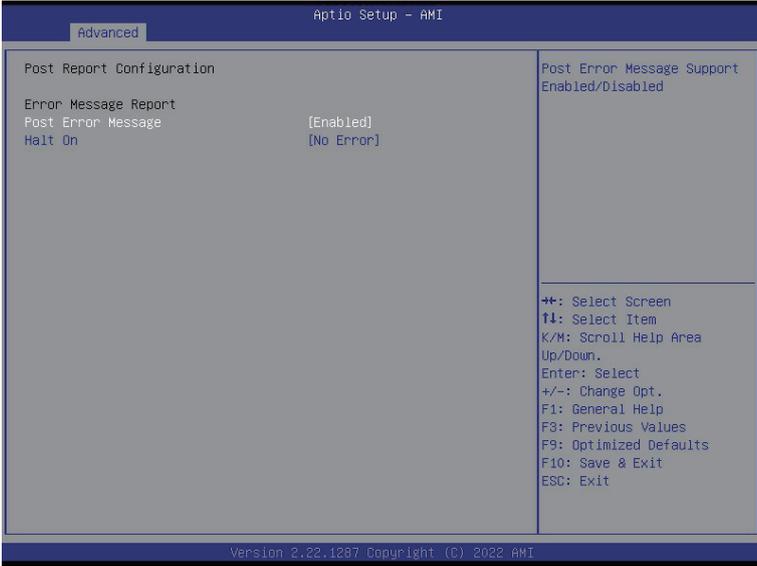
(Note) This item is present only if you attach USB devices.

## 5-2-6 Network Stack Configuration



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

## 5-2-7 Post Report Configuration



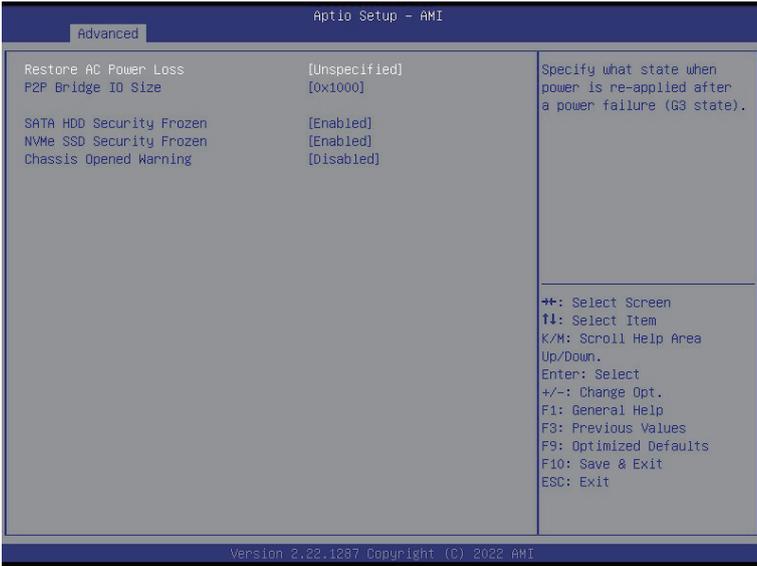
Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Halt On	Options available: No Error, All Error. Default setting is <b>No Error</b> .

## 5-2-8 NVMe Configuration



Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.
NVMe OPROM Select	Options available: BIOS Build-In, NVMe Device. Default setting is <b>BIOS Build-In</b> .

## 5-2-9 Chipset Configuration



Parameter	Description
Restore on AC Power Loss <sup>(Note)</sup>	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
P2P Bridge IO Size	Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is <b>0x1000</b> .
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
NVMe SSD Security Frozen	Attempt to send freeze lock command to NVMe SSDs during boot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Chassis Opened Warning	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is <b>Disabled</b> .

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

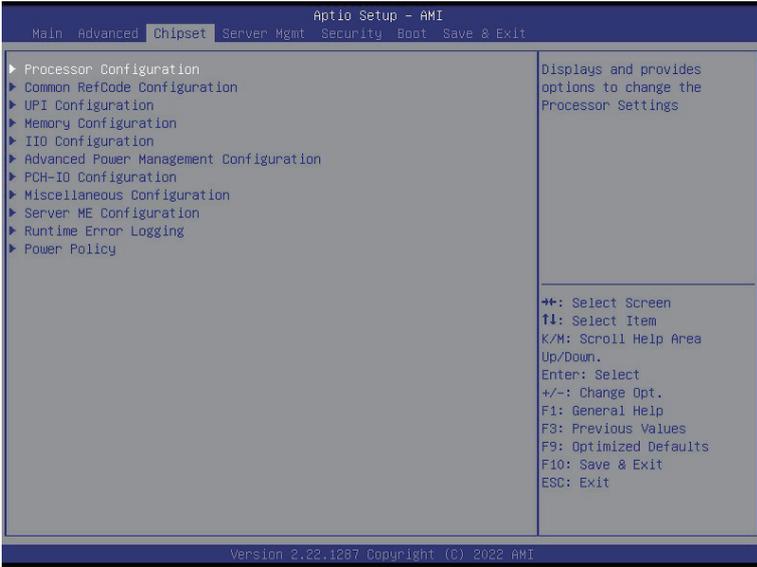
## 5-2-10 Tls Auth Configuration



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

## 5-3 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	000806FB*   000806FB	
Processor Die Type	XCC   XCC	
Processor Frequency	2.100GHz   2.100GHz	
Processor Max Ratio	15H   15H	
Processor Min Ratio	08H   08H	
Microcode Revision	2B0000C0   2B0000C0	
L1 Cache RAM(Per Core)	80KB   80KB	
L2 Cache RAM(Per Core)	2048KB   2048KB	
L3 Cache RAM(Per Package)	61440KB   61440KB	
Processor 0 Version	Intel(R) Xeon(R) Gold 6430	
Processor 1 Version	Intel(R) Xeon(R) Gold 6430	
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
		F8: Previous Values
		F9: Optimized Defaults
		F10: Save & Exit
		ESC: Exit

Version 2.22.1287 Copyright (C) 2022 AMI

Aptio Setup - AMI

Chipset

Processor Configuration		Displays and provides option to change the Processor CFR Settings
Processor 0 Version	Intel(R) Xeon(R) Gold 6430	
Processor 1 Version	Intel(R) Xeon(R) Gold 6430	
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
Enable Intel(R) TXT	[Disable]	F3: Previous Values
VMX	[Enable]	F9: Optimized Defaults
Enable SMX	[Disable]	F10: Save & Exit
AES-NI	[Enable]	ESC: Exit
Debug Consent	[Disable]	
-----		
TME, TME-MT, TDX		
Memory Encryption (TME)	[Disabled]	
SBX setup configuration preconditions for enabling were NOT met. Please check TME, MirrorMode or Extended APIC settings.		
-----		
▶ Processor CFR Configuration		

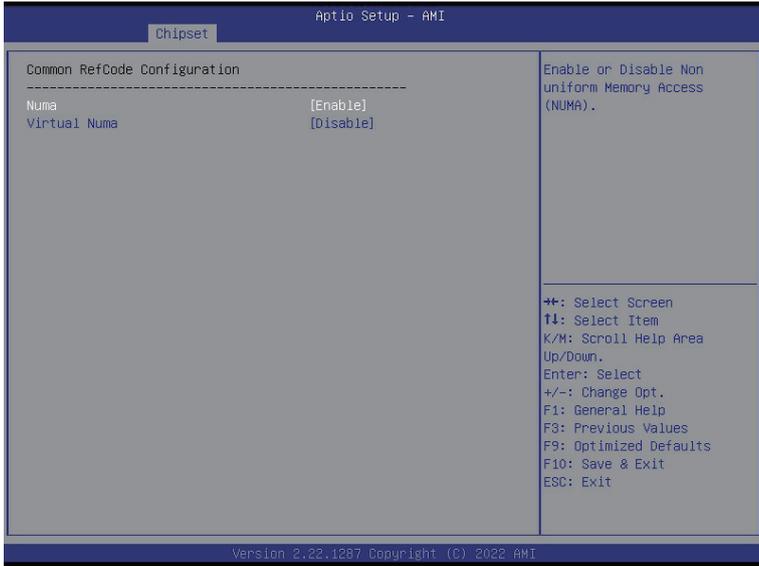
Version 2.22.1287 Copyright (C) 2022 AMI

Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ CPU Socket 0 Configuration <ul style="list-style-type: none"> <li>– Core Disable Bitmap(Hex) <ul style="list-style-type: none"> <li>• Number of Cores to enable. 0 means all cores. FFFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.</li> </ul> </li> </ul> </li> </ul>
Processor Socket / Processor ID / Processor 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 <b>ALL LPs</b>.</p>
Hardware Prefetcher	<p>Select whether to enable the speculative prefetch unit of the processor.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>
L2 RF0 Prefetch Disable	Options available: Enable, Disable. Default setting is <b>Disable</b> .
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 <b>Enable</b>.</p>
DCU Streamer Prefetcher	<p>Enable/Disable DCU streamer prefetcher.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>
DCU IP Prefetcher	<p>Enable/Disable DCU IP Prefetcher.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</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 <b>Enable</b>.</p>
Enable Intel(R) TXT	<p>Enable/Disable the Intel Trusted Execution Technology support function.</p> <p>Options available: Enable, Disable. Default setting is <b>Disable</b>.</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 <b>Enable</b>.</p>
Enable SMX	<p>Enable/Disable the Safer Mode Extensions (SMX) support function.</p> <p>Options available: Enable, Disable. Default setting is <b>Disable</b>.</p>
AES-NI	<p>Enable/Disable the AES-NI support.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>
Debug Consent	Options available: Enable, Disable. Default setting is <b>Disable</b> .

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

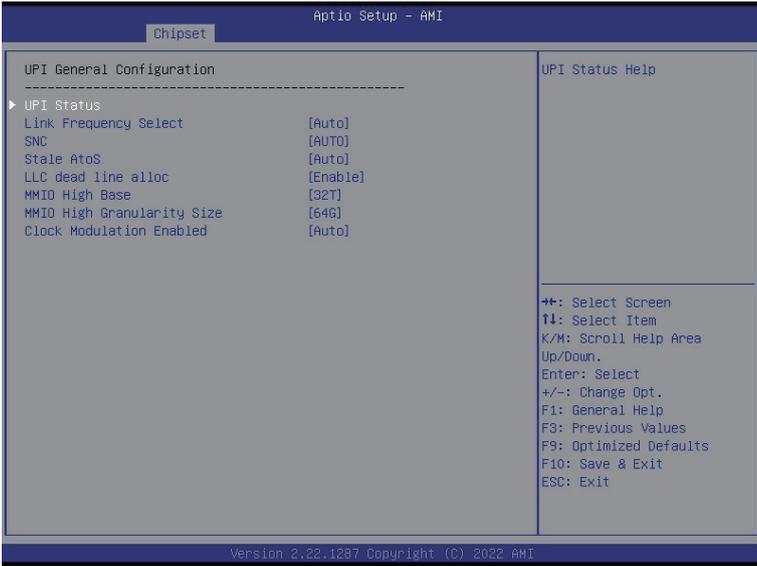
(Note) Advanced items prompt when this item is defined.

## 5-3-2 Common RefCode Configuration



Parameter	Description
Common RefCode Configuration	
Virtual Numa	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors. Options available: Enable, Disable. Default setting is <b>Disable</b> .

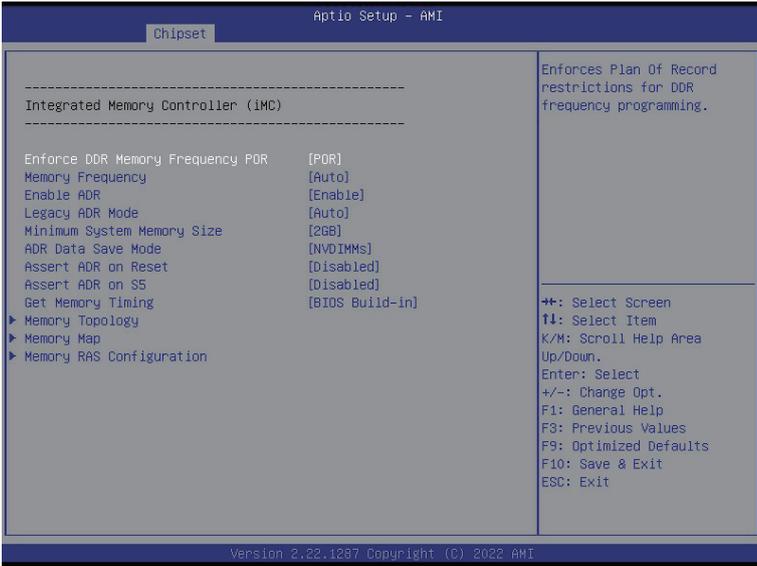
### 5-3-3 UPI Configuration



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

Parameter	Description
UPI General Configuration (continued)	<ul style="list-style-type: none"><li>◆ MMIO High Granularity Size<ul style="list-style-type: none"><li>– Selects the allocation size used to assign mmioh resources.</li><li>– Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is <b>64G</b>.</li></ul></li><li>◆ Clock Modulation Enabled<ul style="list-style-type: none"><li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li></ul></li></ul>

### 5-3-4 Memory Configuration



Parameter	Description
Integrated Memory Controller (iMC)	
Enforce DDR Memory Frequency POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR frequency programming. Options available: POR, Disable. Default setting is <b>POR</b> .
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 <b>Auto</b> .
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Legacy ADR Mode	Enable/Disable the Legacy ADR Mode. Options available: Enable, Disable, Auto. Default setting is <b>Auto</b> .
Minimum System Memory Size	Configures the minimum memory size. Options available: 2GB, 4GB, 6GB, 8GB. Default setting is <b>2GB</b> .
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 <b>NVDIMMs</b> .
Assert ADR on Reset	Enable/Disable Assert ADR on Reset. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .

Parameter	Description
Assert ADR on S5	Enable/Disable Assert ADR on S5. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
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 <b>BIOS Build-in</b> .
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Volatile Memory Mode <ul style="list-style-type: none"> <li>– Selects 1LM or 2LM mode for volatile memory.</li> <li>– Options available: 1LM, 2LM. Default setting is <b>2LM</b>.</li> </ul> </li> </ul>
Memory RAS Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Mirror Mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch.</li> <li>– Options available: Disabled, Full Mirror Mode, Partial Mirror Mode. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Partial Mirror 1 Size (GB) <ul style="list-style-type: none"> <li>– Selects multiplier of 1GB for the size of the SAD to be created.</li> </ul> </li> <li>◆ Correctable Error Threshold <ul style="list-style-type: none"> <li>– Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Trigger SW Error Threshold<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable Sparing trigger SW Error Match Threshold.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ SW Per Bank Threshold <ul style="list-style-type: none"> <li>– SW Per Bank Threshold (1-0x7FFF) used for DDR bank level error.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ SW Correctable Error Time Window <ul style="list-style-type: none"> <li>– SW Correctable Error time window based interface in hour (0-24).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket time window based interface <ul style="list-style-type: none"> <li>– Enable/Disable leaky bucket time window based interface.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>

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

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

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

### 5-3-5 I/O Configuration



Parameter	Description
I/O Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel® VT for Directed I/O <ul style="list-style-type: none"> <li>– 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.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ ACS Control <ul style="list-style-type: none"> <li>– Enable: Programs ACS only to Chipset PCIe Root Ports Bridges.</li> <li>– Disable: Programs ACS to all PCIe bridges.</li> <li>– Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Intel® VT for Directed I/O (VT-d)	<ul style="list-style-type: none"> <li>◆ Cache Allocation <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Opt-Out Illegal MSI Mitigation <ul style="list-style-type: none"> <li>– Enable/Disable Opt-Out Illegal 0xFEE Platform Mitigation.</li> <li>– Options available: Disable, Enable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> <li>– Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>◆ Interrupt Remapping <ul style="list-style-type: none"> <li>– Enable/Disable the interrupt remapping support function.</li> <li>– Options available: Auto, Enable, Disable. Default setting is <b>Auto</b></li> </ul> </li> <li>◆ x2APIC Opt Out <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Pre-boot DMA Protection <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>
Intel® VMD technology	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel® VMD Configuration <ul style="list-style-type: none"> <li>– Enable/Disable Intel® VMD technology.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Intel® VMD for Non-Hotplug NVMe<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable Intel® VMD for Non-Hotplug NVMe.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

(Note) 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"> <li>◆ SpeedStep (Pstates) <ul style="list-style-type: none"> <li>– Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Turbo Mode <ul style="list-style-type: none"> <li>– When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Hardware P-States <ul style="list-style-type: none"> <li>– When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States).</li> <li>– In Native mode, the processor hardware chooses a P-state based on OS guidance.</li> <li>– In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance).</li> <li>– Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is <b>Native Mode</b>.</li> </ul> </li> </ul>

Parameter	Description
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Enable Monitor MWAIT <ul style="list-style-type: none"> <li>– Allows Monitor and MWAIT instructions.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ CPU C6 Report <ul style="list-style-type: none"> <li>– Enable/Disable CPU C6(ACPI C3) report to OS.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> <li>– Core C1E auto promotion control. Takes effect after reboot.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Package C State <ul style="list-style-type: none"> <li>– Configures the state for the C-State package limit.</li> <li>– Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
CPU - Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Energy Perf BIAS <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>» Power Performance Tuning <ul style="list-style-type: none"> <li>• Options available: OS Controls EPB, BIOS Controls EPB, PECL Controls EPB. Default setting is <b>OS Controls EPB</b>.</li> </ul> </li> <li>» Energy_PERF_BIAS_CFG mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>• Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is <b>Balanced Performance</b>.</li> </ul> </li> </ul> </li> </ul> </li> </ul>

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

### 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"> <li>◆ SATA Configuration                             <ul style="list-style-type: none"> <li>– Enable/Disable SATA controller.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ SATA Mode Selection                             <ul style="list-style-type: none"> <li>– Configures on chip SATA type.</li> <li>– 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.</li> <li>– 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.</li> <li>– Options available: AHCI, RAID. Default setting is <b>AHCI</b>.</li> </ul> </li> <li>◆ RAID Device ID<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Choose RAID Device ID.</li> <li>– Options available: Client, Alternate, Server. Default setting is <b>Server</b>.</li> </ul> </li> <li>◆ SATA Port 0/1/2/3/4/5/6/7                             <ul style="list-style-type: none"> <li>– The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.</li> </ul> </li> </ul>

(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"> <li>◆ Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> <li>– Enable/Disable Port 0/1/2/3/4/5/6/7 device.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Hot Plug (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> <li>– Enable/Disable HDD Hot-Plug function.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Spin Up Device (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> <li>– On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>
SATA And RST Configuration/ sSATA Controller And RST Configuration	<ul style="list-style-type: none"> <li>◆ SATA Configuration <ul style="list-style-type: none"> <li>– Enable/Disable SATA controller.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ SATA Mode Selection <ul style="list-style-type: none"> <li>– Configures on chip SATA type.</li> <li>– 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.</li> <li>– 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.</li> <li>– Options available: AHCI, RAID. Default setting is <b>AHCI</b>.</li> </ul> </li> <li>◆ RAID Device ID<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Choose RAID Device ID.</li> <li>– Options available: Client, Alternate, Server. Default setting is <b>Server</b>.</li> </ul> </li> <li>◆ SATA Port 4/5/6/7 <ul style="list-style-type: none"> <li>– The category identifies sSATA hard drives that are installed in the computer. System will automatically detect HDD type.</li> </ul> </li> <li>◆ SATA Port 4/5/6/7 <ul style="list-style-type: none"> <li>– Enable/Disable Port 4/5/6/7 device.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Hot Plug (for Port 4/5/6/7) <ul style="list-style-type: none"> <li>– Enable/Disable HDD Hot-Plug function.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Spin Up Device (for Port 4/5/6/7) <ul style="list-style-type: none"> <li>– On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>

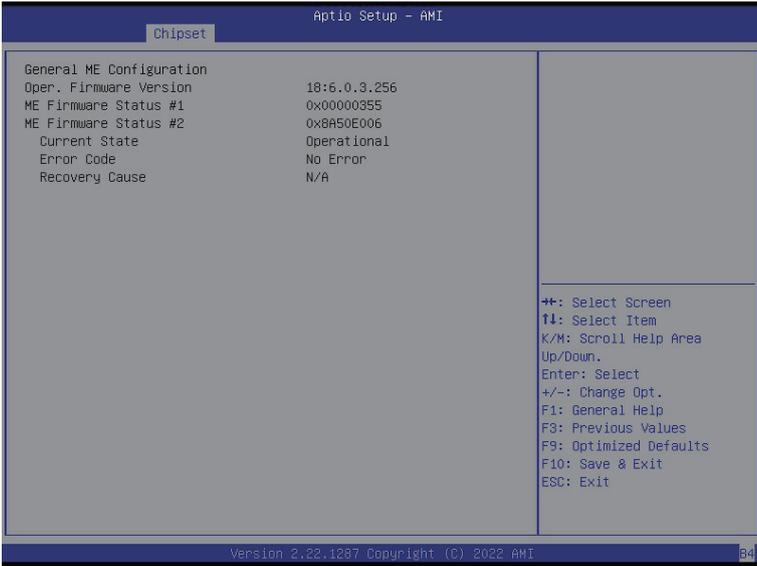
(Note) Only appears when HDD sets to **RAID Mode**.

### 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 <b>Auto</b> .
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 <b>SSC Off</b> .

### 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

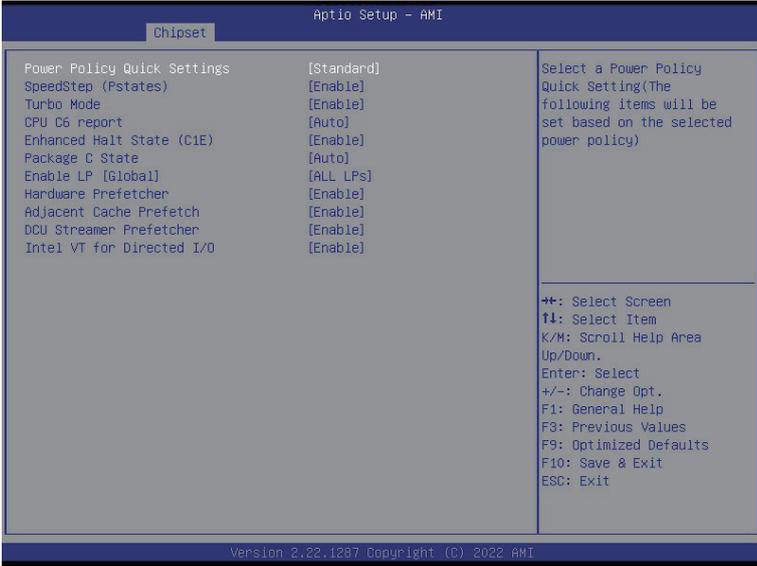


Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable, Disable. Default setting is <b>Enable</b> .
S/W Error Injection Support	Enable/Disable software injection error logging function. Options available: Enable, Disable. Default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

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> <li data-bbox="344 228 852 252">– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li data-bbox="309 257 923 338">◆ Uncorrected Error<sup>(Note)</sup> <ul style="list-style-type: none"> <li data-bbox="344 286 923 310">– Enables and escalates Uncorrectable/Recoverable Errors to error pins.</li> <li data-bbox="344 315 846 338">– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 343 846 424">◆ Fatal Error Enable<sup>(Note)</sup> <ul style="list-style-type: none"> <li data-bbox="344 373 749 396">– Enables and escalates Fatal Errors to error pins.</li> <li data-bbox="344 401 846 424">– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 429 940 545">◆ Assert NMI on SERR<sup>(Note)</sup> <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> <li data-bbox="344 519 876 542">– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li data-bbox="309 550 940 663">◆ Assert NMI on PERR<sup>(Note)</sup> <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> <li data-bbox="344 639 876 663">– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul>

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

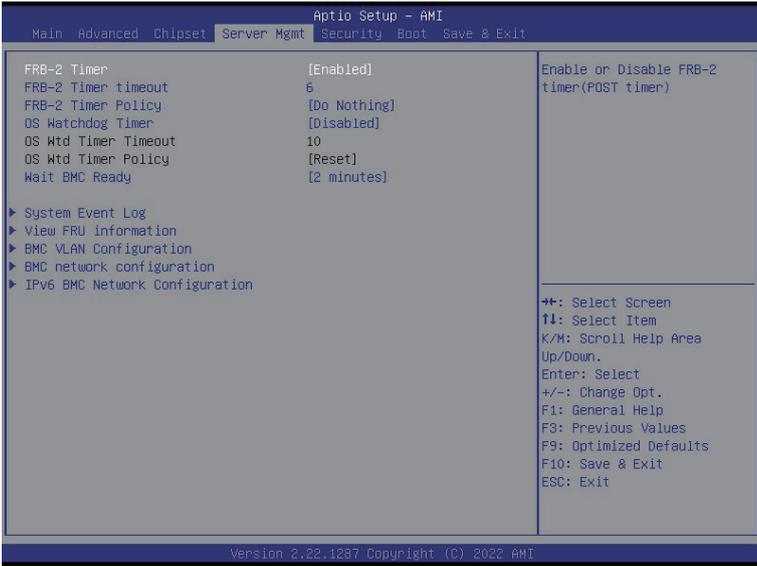
### 5-3-11 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient. Default setting is <b>Standard</b> .
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enable, Disable. Default setting is <b>Enable</b> .
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 <b>Auto</b> .
Enhanced Halt State (C1E)	Enable/Disable the C1E support for lower power consumption. Takes effect after reboot. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Package C State	Configures the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b> .

Parameter	Description
Enable LP [Global]	Enables Logical processor (Software Method to Enable/Disable Logical Processor threads). Options available: ALL LPs, Single LP. Default setting is <b>ALL LPs</b> .
Hardware Prefetcher	Options available: Enable, Disable. Default setting is <b>Enable</b> .
Adjacent Cache Prefetch	Options available: Enable, Disable. Default setting is <b>Enable</b> .
DCU Streamer Prefetcher	Options available: Enable, Disable. Default setting is <b>Enable</b> .
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 <b>Enable</b> .

## 5-4 Server Management Menu



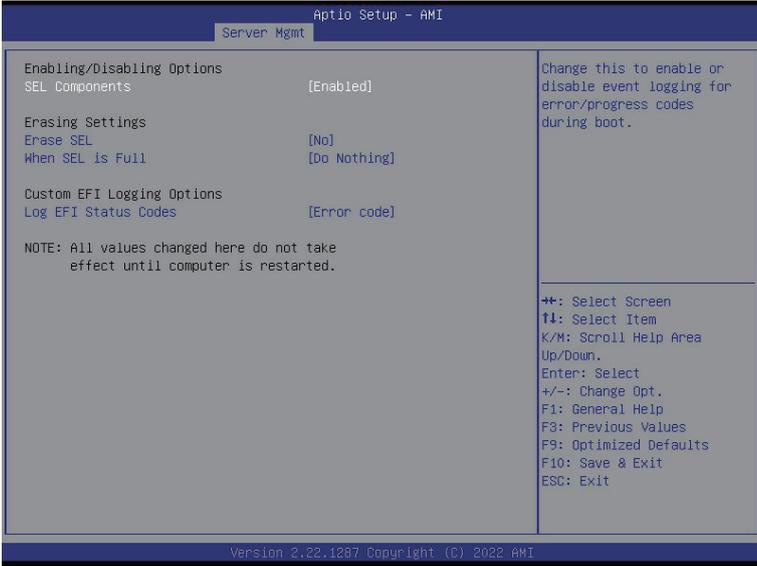
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
FRB-2 Timer <sup>(Note1)</sup> timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is <b>6 minutes</b> .
FRB-2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

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

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

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

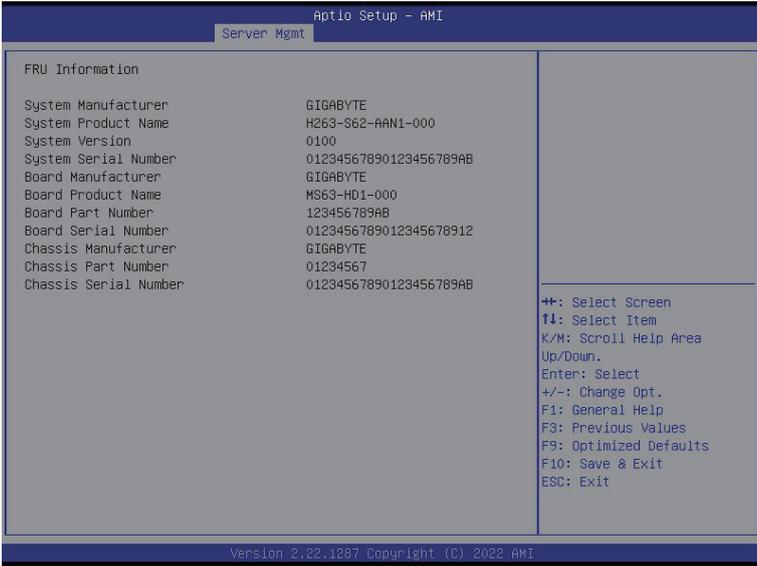
# 5-4-1 System Event Log



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

## 5-4-2 View FRU Information

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



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

### 5-4-3 BMC VLAN Configuration



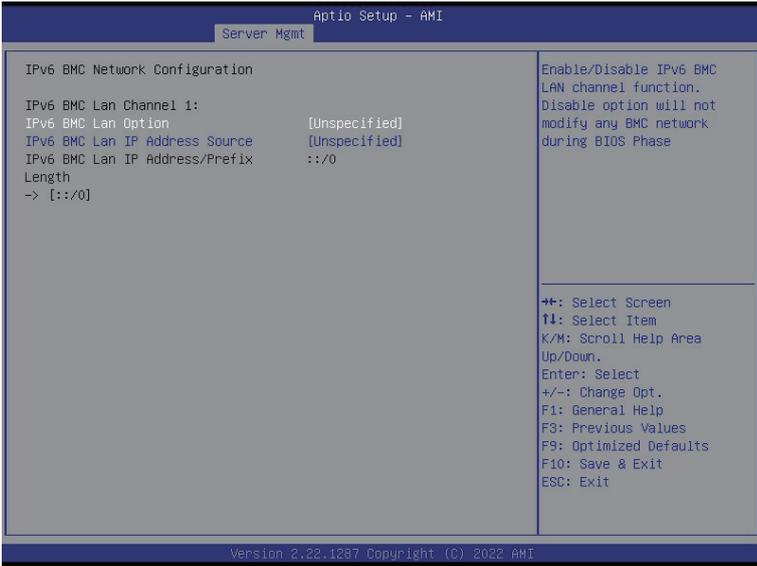
Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority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

## 5-4-4 BMC Network Configuration



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

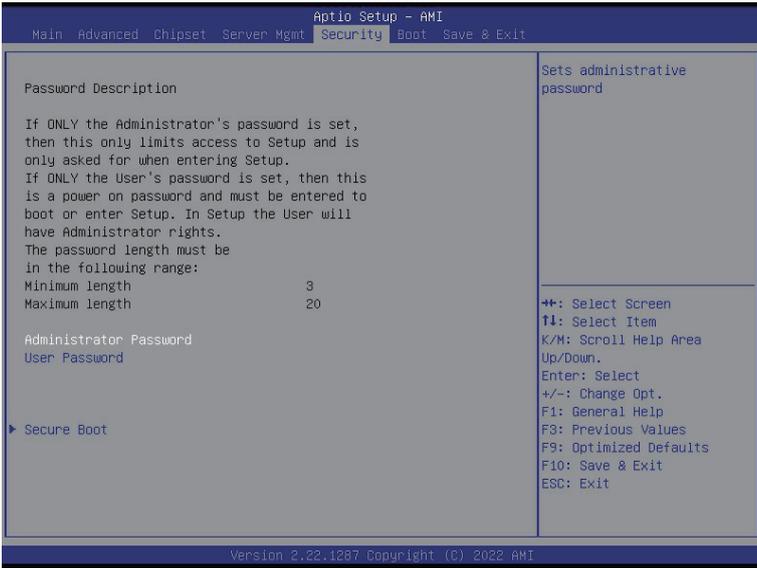
## 5-4-5 IPv6 BMC Network Configuration



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

# 5-5 Security Menu

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



There are two types of passwords that you can set:

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

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

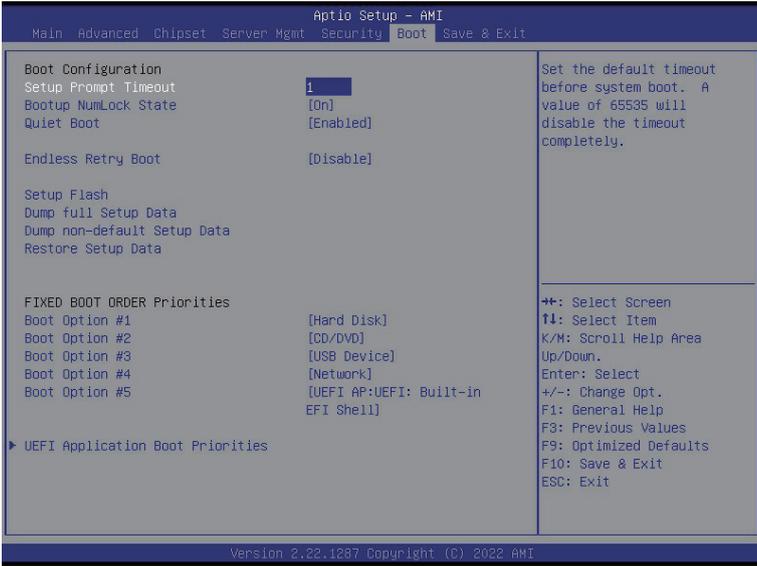
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235"><b>Please note that this item is configurable when Secure Boot Mode is set to Custom.</b></p> <ul style="list-style-type: none"> <li data-bbox="335 243 941 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 941 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li data-bbox="367 326 904 352">– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="335 357 925 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 925 404">– Installs all factory default keys. It will force the system in User Mode.</li> <li data-bbox="367 409 606 431">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 435 654 509">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode.</li> <li data-bbox="367 487 606 509">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 514 899 595">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 537 899 595">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li data-bbox="335 600 936 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 624 936 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.</li> </ul> </li> <li data-bbox="335 686 893 736">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 893 736">– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li data-bbox="335 741 803 846">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 765 803 788">– Displays the current status of the Platform Key (PK).</li> <li data-bbox="367 793 675 816">– Press [Enter] to configure a new PK.</li> <li data-bbox="367 821 601 846">– Options available: Update.</li> </ul> </li> <li data-bbox="335 851 941 987">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 874 941 898">– Displays the current status of the Key Exchange Key Database (KEK).</li> <li data-bbox="367 903 904 956">– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li data-bbox="367 961 670 987">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 992 941 1128">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1016 904 1039">– Displays the current status of the Authorized Signature Database.</li> <li data-bbox="367 1044 941 1097">– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li data-bbox="367 1102 670 1128">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 1133 899 1270">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1157 899 1180">– Displays the current status of the Forbidden Signature Database.</li> <li data-bbox="367 1185 888 1238">– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li data-bbox="367 1243 670 1270">– Options available: Update, Append.</li> </ul> </li> </ul>

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

## 5-6 Boot Menu

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

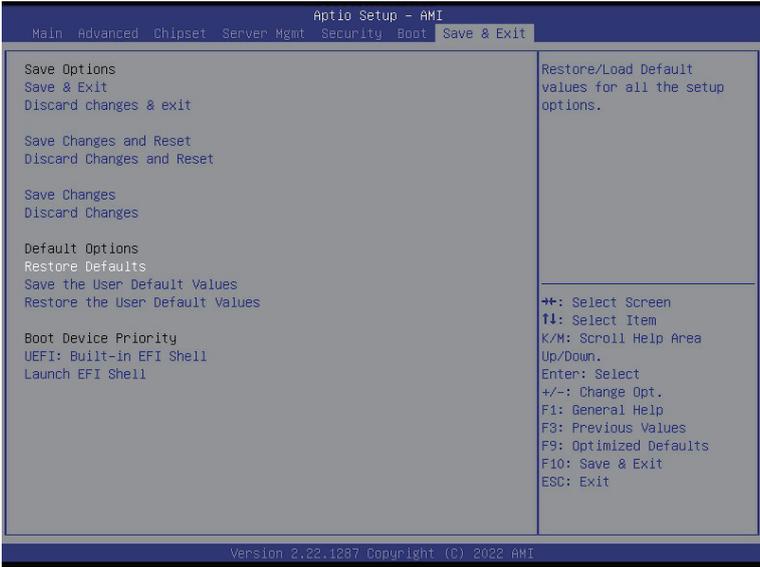


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off. Default setting is <b>On</b> .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Endless Retry Boot	Options available: Disable, Enable. Default setting is <b>Disable</b> .
Setup Flash	Press [Enter] to run setup flash.
Dump full Setup Data	Press [Enter] to dump full setup data to file.
Dump non-default Setup Data	Press [Enter] to dump non-default setup data to file.
Restore Setup Data	Press [Enter] to restore setup data from file.

Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	<p data-bbox="402 200 948 283">Press [Enter] to configure the boot order priority. By default, the server searches for boot devices in the following sequence:</p> <ol data-bbox="440 288 948 426" style="list-style-type: none"> <li data-bbox="440 288 948 310">1. Hard drive.</li> <li data-bbox="440 315 948 337">2. CD-COM/DVD drive.</li> <li data-bbox="440 341 948 363">3. USB device.</li> <li data-bbox="440 368 948 390">4. Network.</li> <li data-bbox="440 395 948 417">5. UEFI.</li> </ol>
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Application Boot Priorities	Press [Enter] to configure the boot priority.

# 5-7 Save & Exit Menu

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



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

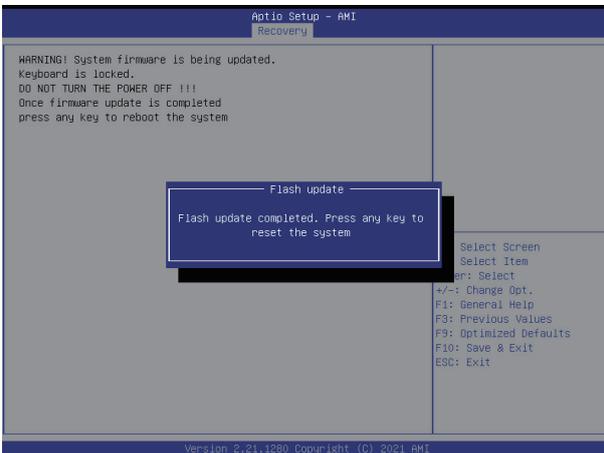
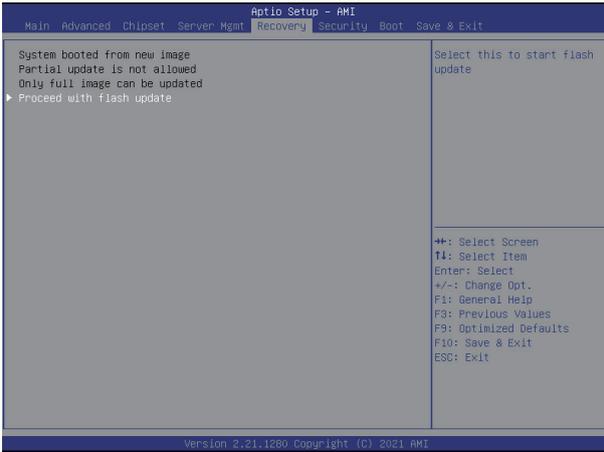
<b>Parameter</b>	<b>Description</b>
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings,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

# 5-8 BIOS Recovery

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

Recovery Instruction:

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



## 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