

GIGABYTE™

T025-S10-AA01

ORv3 Compute Node
5th/4th Gen Intel® Xeon® Scalable - 2OU 2-Node UP 2-Bay E1.S NVMe

T025-BT0

ORv3 Node Tray - 2OU 2-Node

User Manual

Rev. 1.0

Copyright

© 2024 Giga Computing Technology CO., LTD. All rights reserved.

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

Disclaimer

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

Documentation Classifications

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

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

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

For More Information

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




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

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

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

Conventions

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

	NOTE! Pieces of additional information related to the current topic.
	CAUTION! Precautionary measures to avoid possible hardware or software problems.
	WARNING! 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	9
1-1	Installation Precautions	9
1-2	Product Specifications.....	10
1-2-1	TO25-S10.....	10
1-2-2	TO25-BT0.....	12
1-3	System Block Diagram.....	13
Chapter 2	System Appearance	14
2-1	Front View	14
2-2	Rear View.....	15
2-3	Front Panel LEDs and Buttons.....	16
	(Note) If your server features RoT function, please see the following section for detail LED behavior.	16
2-4	RoT LEDs.....	17
2-5	Front System LAN LEDs.....	19
2-6	Storage LEDs.....	20
Chapter 3	System Hardware Installation	21
3-1	Removing Shelf from the Rack	22
3-2	Removing Computing Node from the Shelf.....	23
3-3	Installing the EDSFF SSD.....	24
3-4	Removing and installing the Air Duct	25
3-5	Installing the CPU and Heat Sink.....	26
3-6	Installing Memory	28
3-6-1	Eight Channel Memory Configuration.....	28
3-6-3	Processor and Memory Module Matrix Table	29
3-6-2	Removing and Installing a Memory Module	29
3-6-4	Memory Population Table	30
3-7	Installing the PCI Expansion Card	31
3-8	Replacing the Fan Assembly.....	33
3-9	Cable Routing	34
Chapter 4	Motherboard Components	35
4-1	Motherboard Components	35
4-2	Jumper Setting	36
Chapter 5	BIOS Setup	37
5-1	The Main Menu	39
5-2	Advanced Menu	42

5-2-1	Trusted Computing	43
5-2-2	Serial Port Console Redirection	44
5-2-3	SIO Configuration	47
5-2-4	PCI Subsystem Settings	48
5-2-5	USB Configuration	49
5-2-6	Network Stack Configuration	50
5-2-7	Post Report Configuration	51
5-2-8	NVMe Configuration	52
5-2-9	Chipset Configuration	53
5-2-10	Tls Auth Configuration	54
5-2-11	iSCSI Configuration	55
5-3	Chipset Menu	56
5-3-1	Processor Configuration	57
5-3-2	Common RefCode Configuration	60
5-3-3	UPI Configuration	61
5-3-4	Memory Configuration	63
5-3-5	IIO Configuration	66
5-3-6	Advanced Power Management Configuration	68
5-3-7	PCH Configuration.....	70
5-3-8	Miscellaneous Configuration	72
5-3-9	Server ME Configuration	73
5-3-10	Runtime Error Logging Settings	74
5-3-11	Power Policy.....	76
5-4	Server Management Menu.....	78
5-4-1	System Event Log	80
5-4-2	View FRU Information	81
5-4-3	BMC VLAN Configuration.....	82
5-4-4	BMC Network Configuration	83
5-4-5	IPv6 BMC Network Configuration	84
5-5	Security Menu	85
5-5-1	Secure Boot	86
5-6	Boot Menu.....	89
5-7	Save & Exit Menu.....	91
5-8	BIOS Recovery	93
5-9	BIOS POST Beep code (AMI standard).....	94
5-9-1	PEI Beep Codes	94
5-9-2	DXE Beep Codes	94

Chapter 1 Hardware Installation

1-1 Installation Precautions

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

- Prior to installation, do not remove or break motherboard S/N (Serial Number) sticker or warranty sticker provided by your dealer. These stickers are required for warranty validation.
- 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





1-2-1 TO25-S10






NOTE:

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

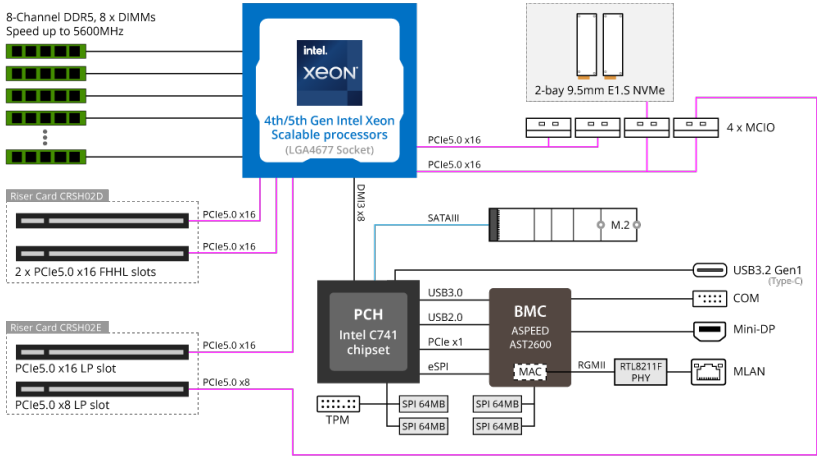
 System	<ul style="list-style-type: none">◆ 20U 2-Node
 Dimension	<ul style="list-style-type: none">◆ 262.7 (W) x 90 (H) x 740 (D) mm
 CPU	<ul style="list-style-type: none">◆ 5th Generation Intel® Xeon® Scalable Processors◆ 4th Generation Intel® Xeon® Scalable Processors◆ Intel® Xeon® CPU Max Series◆ Single processor, CPU TDP up to 350W
 Memory	<ul style="list-style-type: none">◆ 8 x DIMM slots◆ DDR5 memory supported only◆ 8-Channel memory architecture◆ RDIMM modules up to 96GB supported◆ 3DS RDIMM modules up to 256GB supported ◆ 5th Gen Intel® Xeon®: Up to 5600MHz◆ 4th Gen Intel® Xeon®: Up to 4800MHz◆ Intel® Xeon® Max Series: Up to 4800MHz
 LAN	<p>Front side:</p> <ul style="list-style-type: none">◆ 1 x Dedicated management LAN
 Storage	<p>Front side:</p> <ul style="list-style-type: none">◆ 2 x 9.5mm E1.S NVMe hot-swappable bays
 Expansion Slot	<p>Riser Card CRSH02D:</p> <ul style="list-style-type: none">◆ 2 x PCIe x16 (Gen5 x16) FHHL slots <p>Riser Card CRSH02E:</p> <ul style="list-style-type: none">◆ 1 x PCIe x16 (Gen5 x16) low-profile slot◆ 1 x PCIe x16 (Gen5 x8) low-profile slot <p>1 x M.2 slot (CFPH010):</p> <ul style="list-style-type: none">◆ M-key◆ SATA, from PCH◆ Supports 2242/2260/2280/22110 cards

	Front I/O	<ul style="list-style-type: none"> ◆ 1 x USB 3.2 Gen1 Type-C ◆ 1 x Mini-DP ◆ 1 x MLAN ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x ID LED ◆ 1 x System status LED
	Power Supply	<ul style="list-style-type: none"> ◆ Supports up to 1600W
	System Management	<ul style="list-style-type: none"> ◆ 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 ◆ Advanced power capping ◆ LDAP / AD / RADIUS Support ◆ Backup & Restore Configuration ◆ Remote BIOS/BMC/CPLD Update ◆ Event Log Filter ◆ User Management ◆ Media Redirection Settings ◆ PAM Order Settings ◆ SSL Settings ◆ SMTP Settings
	Operating Properties	<ul style="list-style-type: none"> ◆ Operating temperature: 10°C to 35°C ◆ Operating humidity: 8%-80% (non-condensing) ◆ Non-operating temperature: -40°C to 60°C ◆ Non-operating humidity: 20%-95% (non-condensing)

1-2-2 TO25-BT0

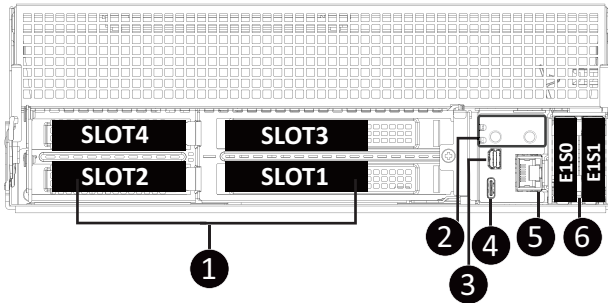
 System Dimension	<ul style="list-style-type: none">◆ 537 x 95.2 x 801.6 (w/o fans)◆ 2OU Node Tray◆ For 2 x ORv3 2OU nodes
 Open Rack Version	<ul style="list-style-type: none">◆ ORv3
 No. of Bus Bars	<ul style="list-style-type: none">◆ 1 x 48V Bus Bar

1-3 System Block Diagram



Chapter 2 System Appearance

2-1 Front View

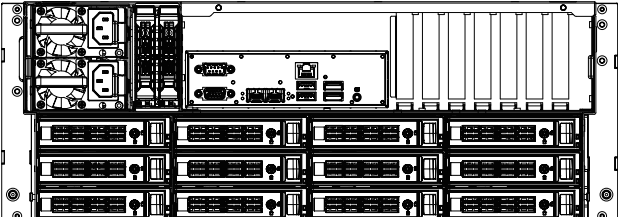


No.	Description
1.	PCIe Card Slot
2.	Front Panel LEDs and Buttons
3.	Mini-DP Port
4.	USB 3.2 Gen1 Type-C
5.	Server Management LAN Port
6.	EDSFF E1.S SSD Bay



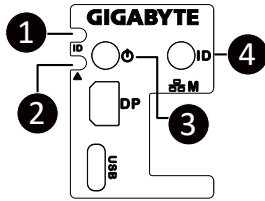
- Refer to section **2-3 Front Panel LEDs and Buttons** for a detailed description of the function of the LEDs.

2-2 Rear View



No.	Description
1.	Power Distribution Board to Bus Bar Connector

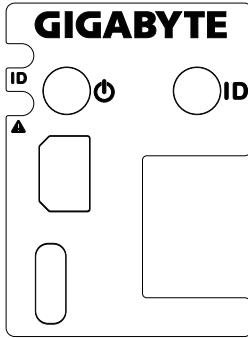
2-3 Front Panel LEDs and Buttons



No.	Name	Color	Status	Description
1.	ID LED ^(Note)	Blue	On	Indicates the system identification is active.
		N/A	Off	Indicates the system identification is disabled.
2.	System Status LED ^(Note)			This LED represents the RoT function LED behavior. Please see the following section for detail LED behavior.
3.	Power button with LED	Green	On	Indicates the system is powered on.
		Green	Blink	System is in ACPI S1 state (sleep mode).
		N/A	Off	- System is not powered on or in ACPI S5 state (power off) - System is in ACPI state (hibernate mode)
4.	ID Button with LED	Blue	On	Indicates the system identification is active. Press the button to activate system identification
		N/A	Off	Indicates the system identification is disabled.

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

2-4 RoT LEDs



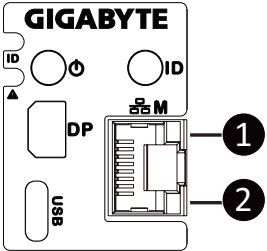
	LED on Front panel ^(Note5)	
	ID LED	Status LED
EC Firmware (FW) Authentication fail or not exit		
EC FW is broken or not exit ^(Note1)	OFF	OFF
Authenticating/Recovering BMC/BIOS Images		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per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

BIOS : AUTH fail ^(Note2)	Blinks Blue 1 time per second	Blinks Amber 1 time per second
BMC : AUTH fail after doing recovery ^(Note3)	Blinks Blue 2 times per second [ON OFF OFF]	Blinks Green 2 times per second [ON OFF OFF]
BIOS : AUTH fail after doing recovery ^(Note3)	Blinks Blue 2 times per second [ON OFF OFF]	Blinks Amber 2 times per second [ON OFF OFF]
Backup Flash Authentication Fail ^(Note4)		
BMC : AUTH fail	Blinks Blue 2 times per second [ON OFF ON OFF]	Blinks Green 2 times per second [ON OFF ON OFF]
BIOS : AUTH fail	Blinks Blue 2 times per second [ON OFF ON OFF]	Blinks Amber 2 times per second [ON OFF ON OFF]

NOTE!

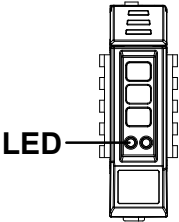
- EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
- (1) Authentication fail include below scenarios
Configuration table is missing or modified
Public key is missing or modified
Protected area or signature is modified
Flash empty
- If active flash is still 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 Front System LAN LEDs



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

2-6 Storage LEDs



RAID SKU		Color	Locate	NVMe Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA)	NVMe LED (On NVMe Module)	Amber	OFF	ON(*1)			
RAID configuration (via HW RAID Card or SW RAID Card)	NVMe LED	Amber	BLINK	ON	Alternately		

NOTE:

*1: Depends on HBA/Utility Spec.

Chapter 3 System Hardware Installation



Pre-installation Instructions

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

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

3-1 Removing Shelf from the Rack

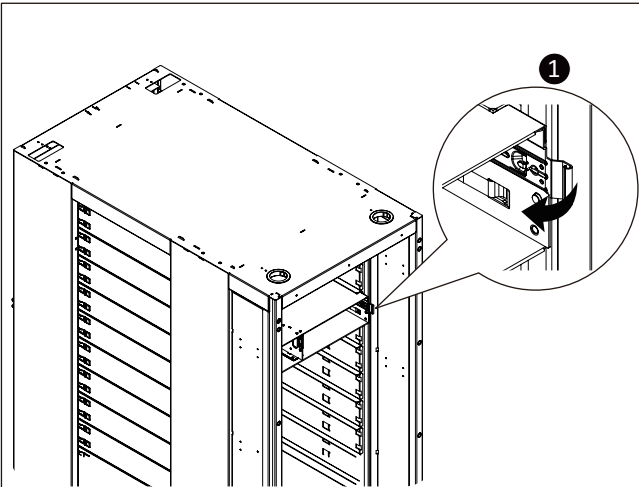
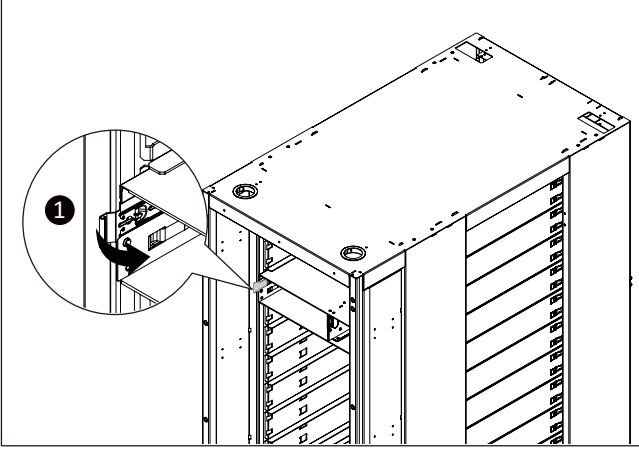


Before you remove or install the computing node:

Remove the computing node before removing the shelf.

Follow these instructions to remove the Shelf from the rack:

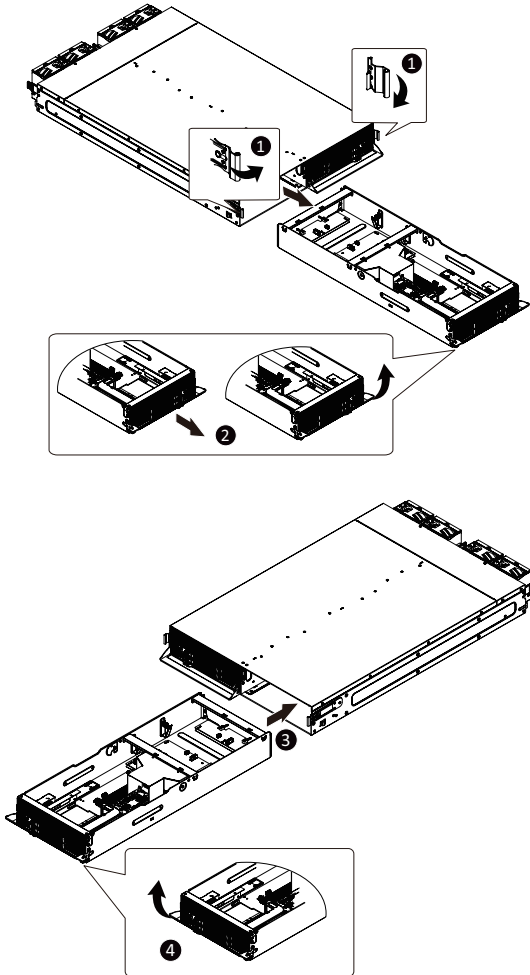
1. Press the release latches inward while simultaneously pulling the handle for the shelf.
2. Pull the shelf out of the cabinet.
3. To install the shelf, push the shelf back into the cabinet.



3-2 Removing Computing Node from the Shelf

Follow these instructions to remove a computing node from the shelf:

1. Press the retaining clip on the Left side of the computing node in the direction indicated.
2. Turn the handle upward.
3. Pull out the computing using the handle.
4. Insert the replacement computing node.
5. Turn the handle down when installing the replacement node into the shelf.



3-3 Installing the EDSFF SSD

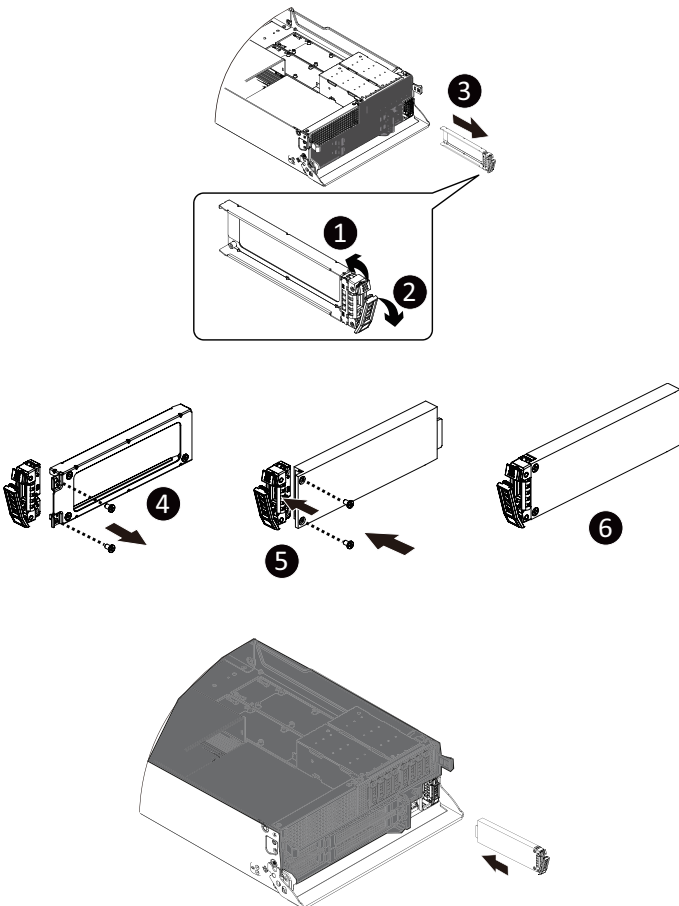


Read the following guidelines before you begin to install the EDSFF SSD:

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

Follow these instructions to install the SSD:

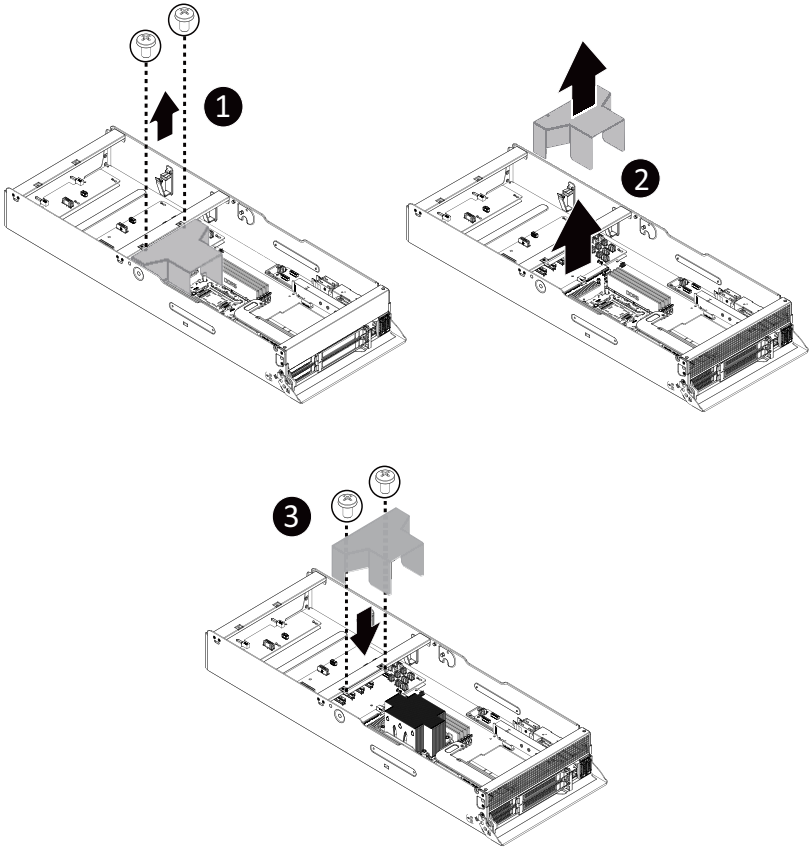
1. Press the release latch of the storage tray.
2. Pull out the locking lever.
3. Use the locking lever to slide out the storage tray.
4. Remove two screws on the storage tray.
5. Install the SSD into the storage tray , secure the SSD with two screws.
6. Re-install the storage tray with SSD into the system until it clicks.



3-4 Removing and installing the Air Duct

Follow these instructions to remove and install the Air Duct:

1. Loosen the screws and remove them.
2. Lift up to remove the air duct.
3. Align the air duct with the guiding groove. Push down the air duct until it is firmly seated on the system. Secure the air duct by tightening the screws.



3-5 Installing the CPU and Heat Sink



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

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

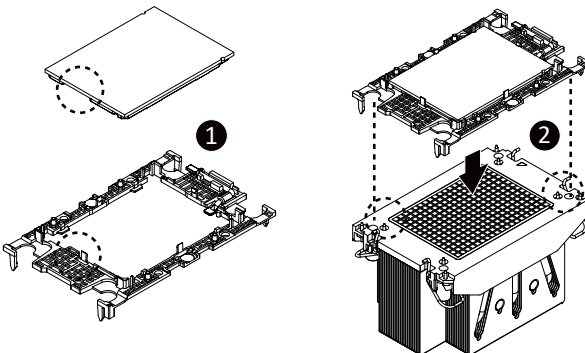


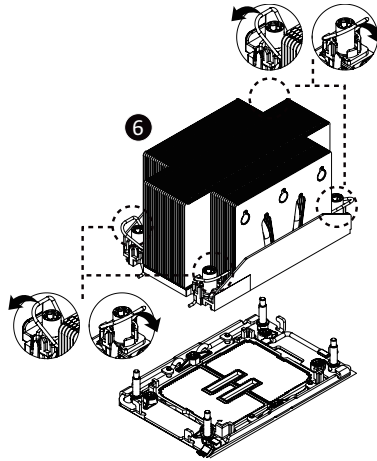
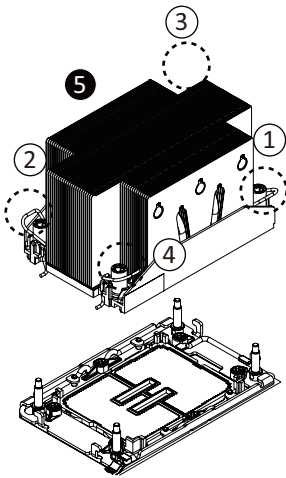
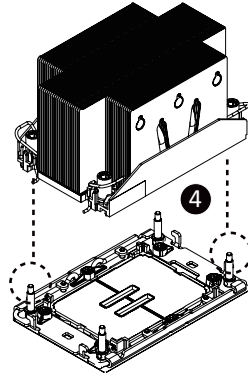
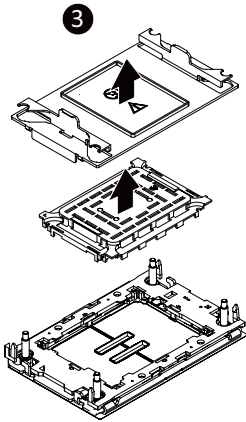
WARNING!

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

Follow these instructions to install the CPU:

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





Carrier Types used for Package Types

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



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

3-6 Installing Memory

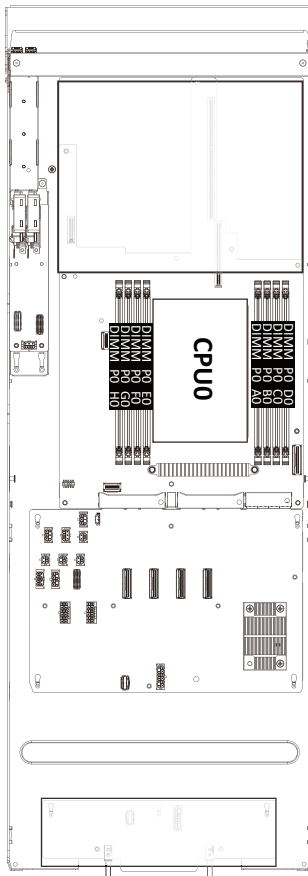


Read the following guidelines before you begin to install the memory:

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

3-6-1 Eight Channel Memory Configuration

This motherboard provides 8 DDR5 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory. Enabling eight Channel memory mode will be eight times of the original memory bandwidth.



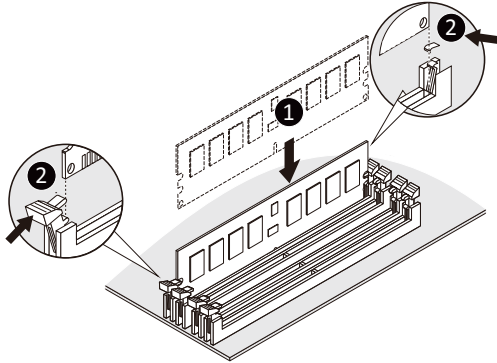
3-6-2 Removing and Installing a Memory Module



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

Follow these instructions to install a DIMM module:

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



3-6-3 Processor and Memory Module Matrix Table

Memory Q'ty for each CPU	CPU0							
	H0	G0	F0	E0	A0	B0	C0	D0
1 DIMM					V			
2 DIMM		V			V			
4 DIMM		V		V	V		V	
6 DIMM		V	V	V	V		V	V
8 DIMM	V	V	V	V	V	V	V	V

3-6-4 Memory 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 ²	36Gb	1DPC ¹	2DPC
					1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	NA	4800	4400
	SRx4 (RC C)	32GB	48GB	NA		
	SRx4 (RC F) 9x4	32GB	NA	NA		
	DRx8 (RC E)	32GB	48GB	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
	DRx4 (RC B) 9x4	64GB	NA	NA		
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 ²	36Gb	1DPC ¹	2DPC
					1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	NA	5600 ³	4400 ³
	SRx4 (RC C)	32GB	48GB	NA		
	SRx4 (RC F) 9x4	NA	NA	NA		
	DRx8 (RC E)	32GB	48GB	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
	DRx4 (RC B) 9x4	NA	NA	NA		
RDIMM 3DS	(4R/8R)x4 (RC A)	2H-128GB 4H-256GB	NA	NA	5600 ⁴	

NOTE:

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

NOTE!

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

3-7 Installing the PCI Expansion Card



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

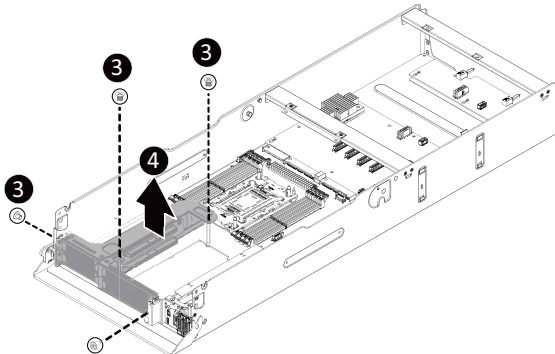
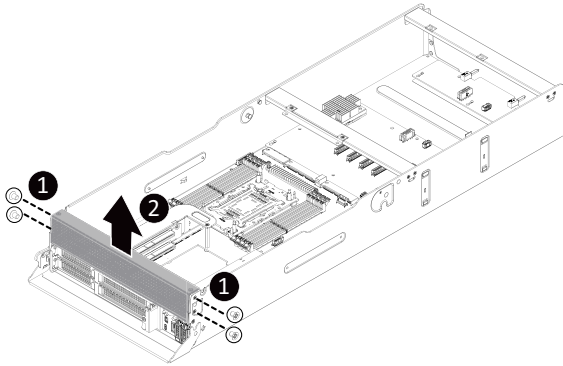
Failure to observe these warnings could result in personal injury or damage to equipment.

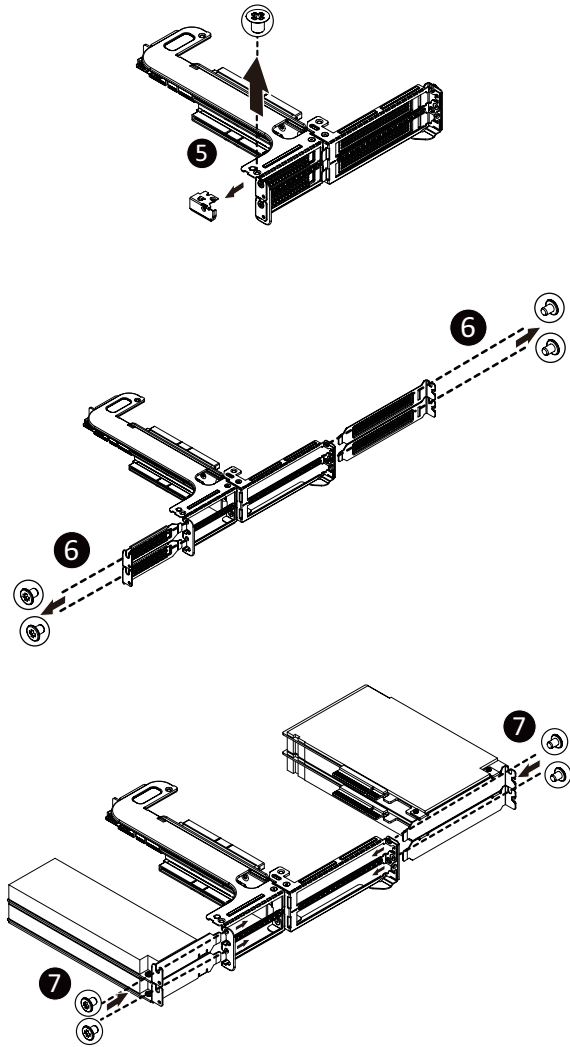


- The PCI riser assembly does not include a riser card or any cabling as standard. To install a PCI card, a riser card must be installed.

Follow these instructions to install the PCI Expansion card:

1. Remove the screw securing the panel frame to the system.
 2. Lift up the panel frame out of system.
 3. Remove the screw securing on the riser bracket
 4. Lift up the riser bracket.
 - 5 - 6. Remove the screw securing the side bracket to the riser bracket.
 7. Align the PCI card to the riser guide slot and push in the direction of the arrow until the PCI card sits in the PCI card connector. Secure the PCI card with the screw.
- Reverse steps 1 - 4 to install the riser bracket back into the system.

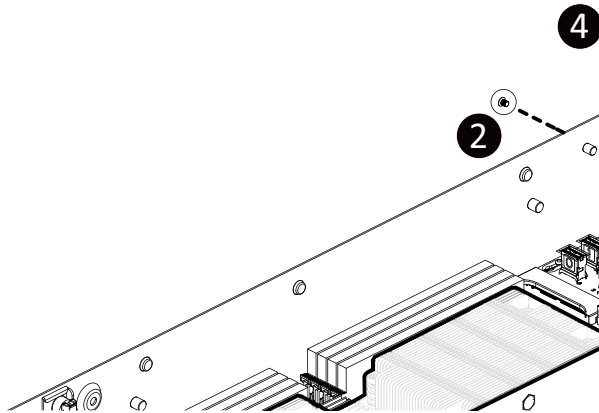




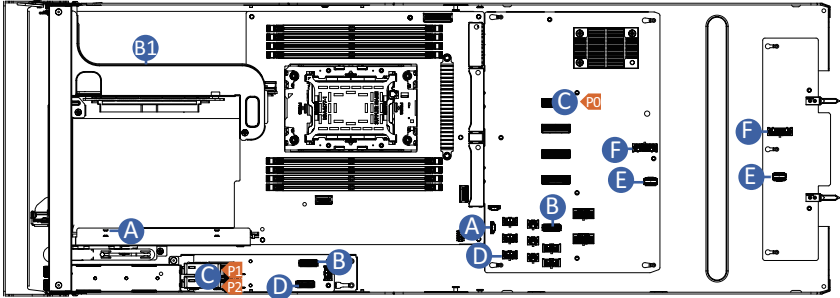
3-8 Replacing the Fan Assembly

Follow these instructions to replace the fan assembly:

1. Press the release latches on the bottom-left and top-right sides of the fan assembly inwards while pulling the fan out of its compartment
2. To install the replacement fan assembly, push the assembly into the compartment.



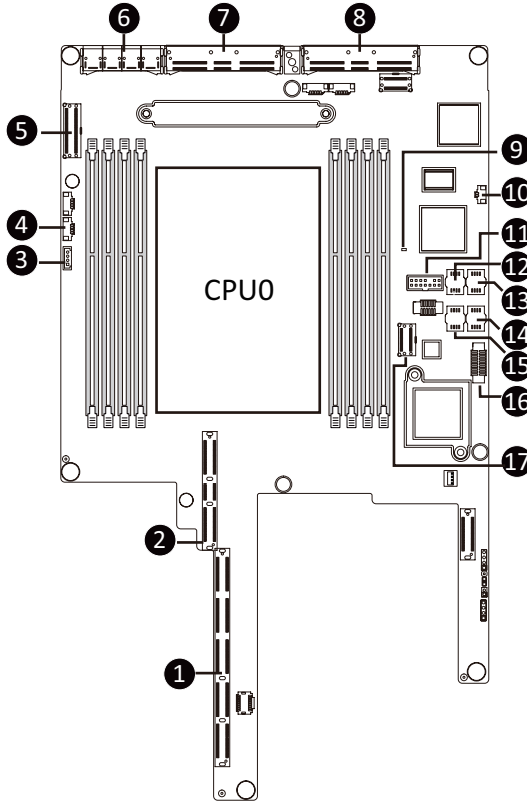
3-9 Cable Routing



A	Front Panel LEDs and Buttons Cable	Front Board: BP_1	
		Power Distribution Board(COPDD5): FP_1	
B	Storage Board Signal Cable	Power Distribution Board: BP_1	
		Motherboard: BMC_SGP10	
		Storage Board(COBP721): BP_1	
C	MCIO Cable	Power Distribution Board(COPDD5): MCIO_A2	P0
		Storage Board(COBP740): C15-3	P2
		Storage Board(COBP740): C15-2	P1
D	Storage Board Power Cable	Power Distribution Board(COPDD5): BP_PWR1	
		Storage Board(COBP740): ATX1	
E	Bus Bar Signal Cable	Power Distribution Board(COPDD5): FAN_CN1	
		Bus Bar Board(CORC211): FAN_CN1	
F	Bus Bar Power Cable	Power Distribution Board(COPDD5): BUS_PWR1	
		Bus Bar Board(CORC211): BUS_PWR1	

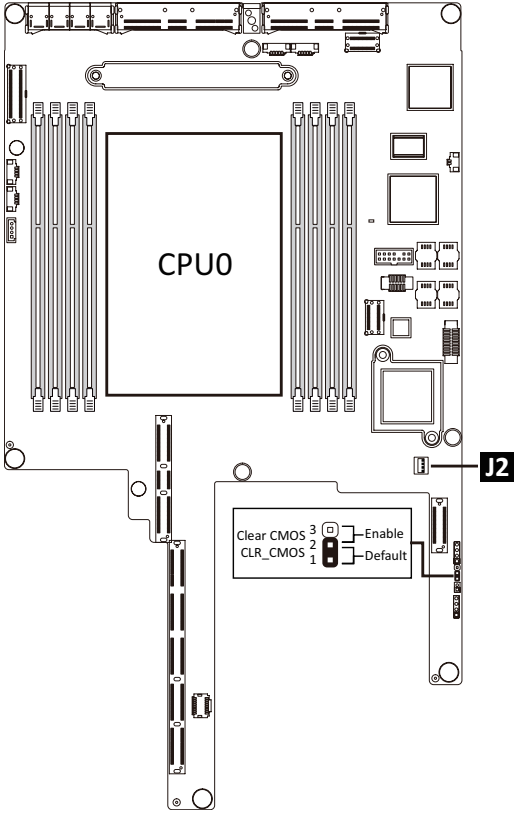
Chapter 4 Motherboard Components

4-1 Motherboard Components



Item	Description	Item	Description
1	Proprietary PCIe Slot (Gen 5/x16 slot/GENZ_1_3)	10	System Battery Cable Connector
2	Proprietary PCIe Slot (Gen 5/x16 slot/GENZ_2_4)	11	TPM Module Connector
3	VROC Module Connector	12	BIOS Flash ROM #2
4	PSOUT Connector	13	BIOS Flash ROM #1
5	MCIO Connector (MCIO0_4AB/PCIe Gen5)	14	BMC Flash ROM #2
6	Power Connector (12V for middle board)	15	BMC Flash ROM #1
7	MCIO Connector (CA_1_1/PCIe Gen5)	16	NCSI Cable Connector
8	MCIO Connector (CA_1_2/PCIe Gen5)	17	SlimSAS Connector (SL_SATA0)
9	BMC Readiness LED	18	

4-2 Jumper Setting



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]

Chapter 5 BIOS Setup

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

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



- BIOS flashing is potentially risky, if you do not encounter any problems when using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 4 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

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

■ **Main**

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

■ **Advanced**

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

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

■ **Chipset**

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

■ **Server Management**

Server additional features enabled/disabled setup menus.

■ **Security**

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

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

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

■ **Boot**

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

■ **Save & Exit**

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

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

5-1 The Main Menu

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

Main Menu Help

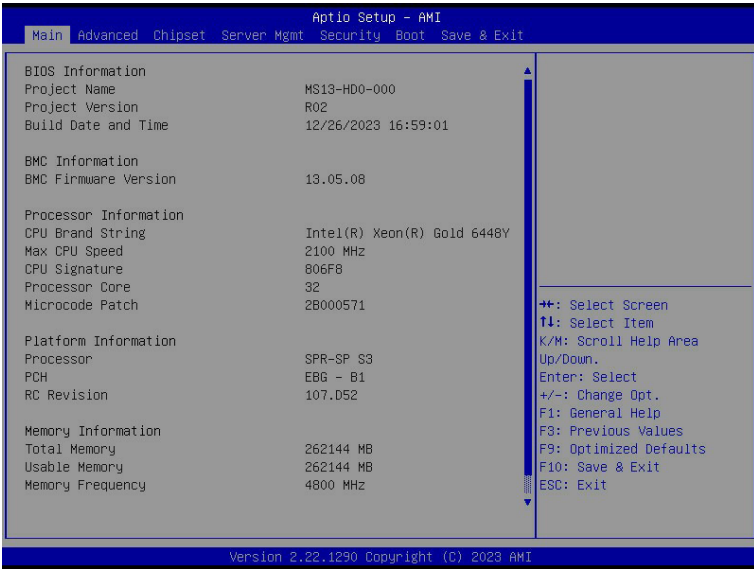
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

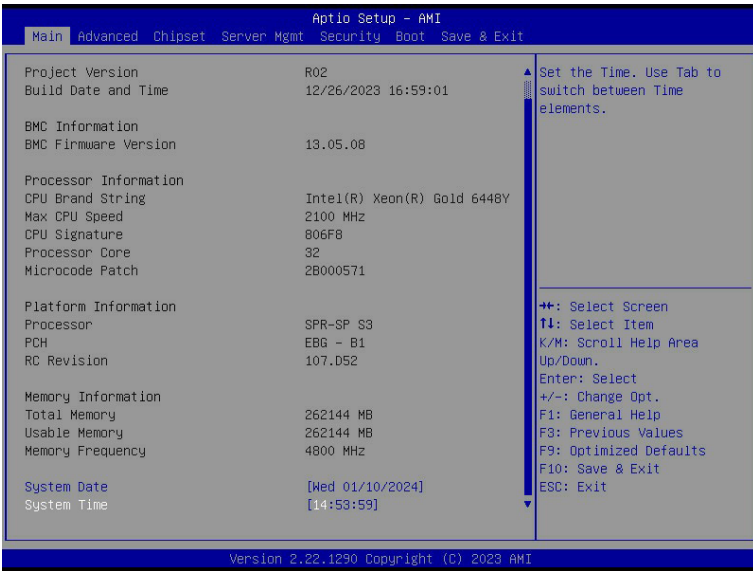
Submenu Help

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



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





Parameter	Description
BIOS Information	
Project Name	Displays the project name information.
Project Version	Displays version number of the BIOS setup utility.
Build Date and Time	Displays the date and time when the BIOS setup utility was created.
BMC Information ^(Note1)	
BMC Firmware Version ^(Note1)	Displays BMC firmware version information.
Processor Information	
CPU Brand String/ Max CPU Speed / CPU Signature / Processor Core / Microcode Patch	Displays the technical information for the installed processor(s).
Platform Information	
Processor/ PCH/ RC Revision	Displays the information of the installed processor(s) and PCH.
Memory Information ^(Note2)	
Total Memory	Displays the total memory size of the installed memory.
Usable Memory	Displays the usable memory size of the installed memory.

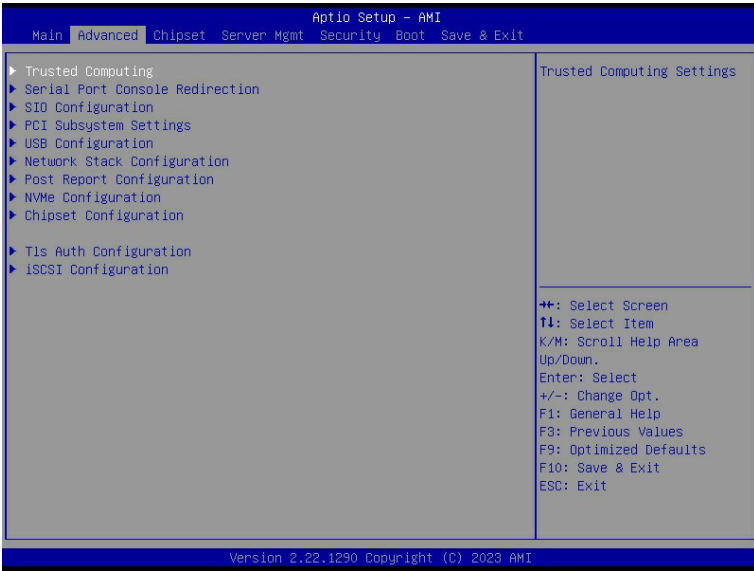
(Note1) Functions available on selected models.

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

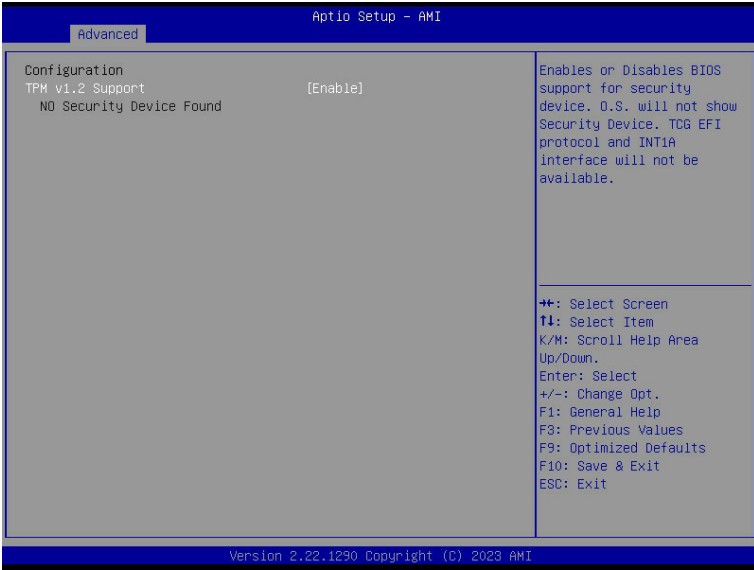
Parameter	Description
Memory Frequency	Displays the frequency information of the installed memory.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

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.

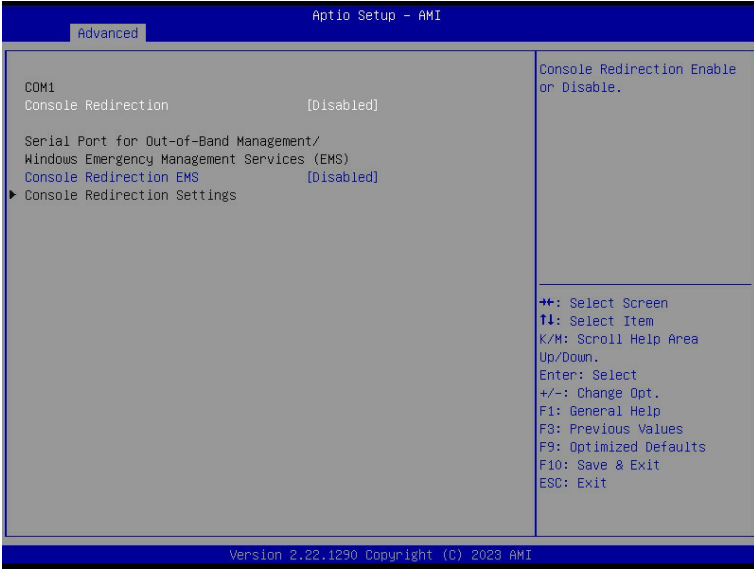


5-2-1 Trusted Computing



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 Enable.</p>

5-2-2 Serial Port Console Redirection



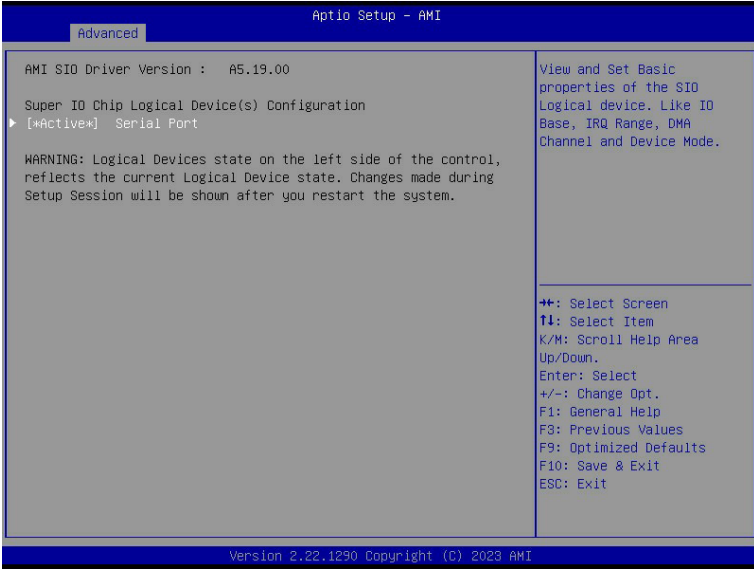
Parameter	Description
COM1 Console Redirection ^(Note)	<p>Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>
COM1 Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p>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

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

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

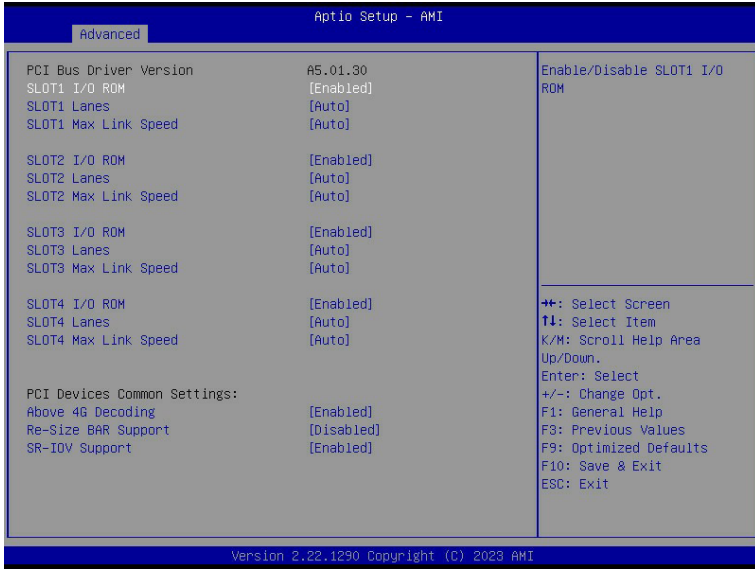
Parameter	Description
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection ^(Note)	<p>EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.</p> <p>Options available: Enabled,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

5-2-3 SIO Configuration



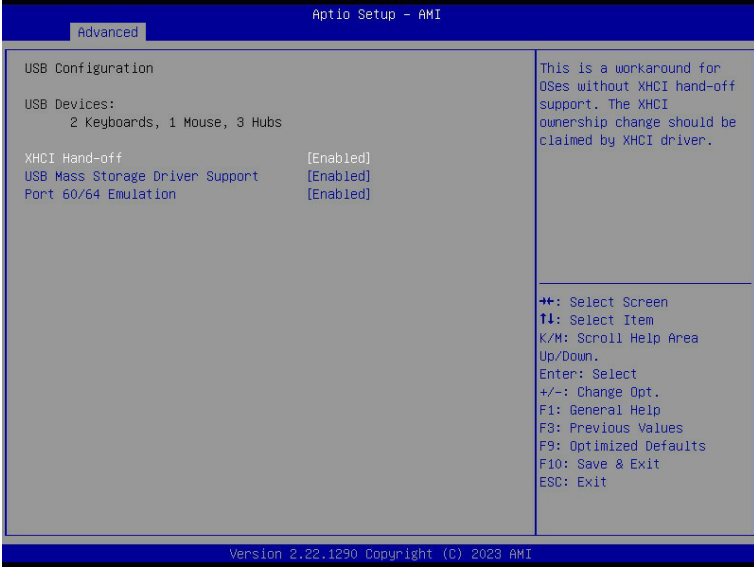
Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	
[*Active*] Serial Port	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Use This Device <ul style="list-style-type: none">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

5-2-4 PCI Subsystem Settings



Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT_# I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is Enabled .
SLOT_# Lanes ^(Note1)	Change the PCIe lanes. Default setting is Auto .
SLOT_#_Max Link Speed ^(Note1)	Configure PCIe max link speed. Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5. Default setting is Auto .
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled, Disabled. Default setting is Enabled .
Re-Size BAR Support	Enable/Disable Re-Size BAR Support. Options available: Enabled, Disabled. Default setting is Disabled .
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is Enabled .

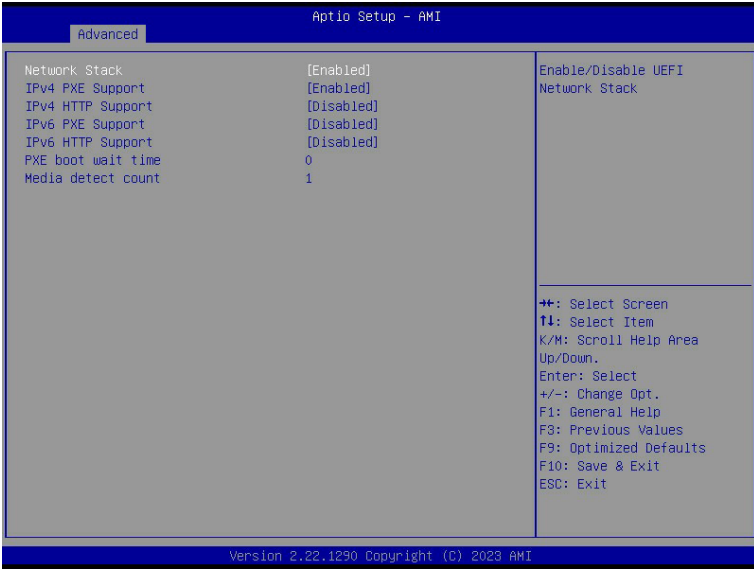
5-2-5 USB Configuration



Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled, Disabled. Default setting is Enabled .
USB Mass Storage Driver Support ^(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled, Disabled. Default setting is Enabled .
Port 60/64 Emulation	Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OSes. Options available: Enabled, Disabled. Default setting is Enabled .

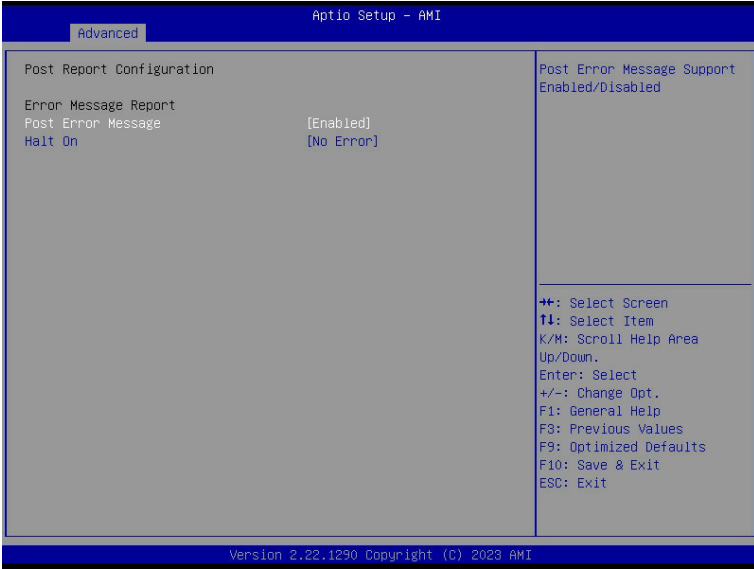
(Note) This item is present only if you attach USB devices.

5-2-6 Network Stack Configuration



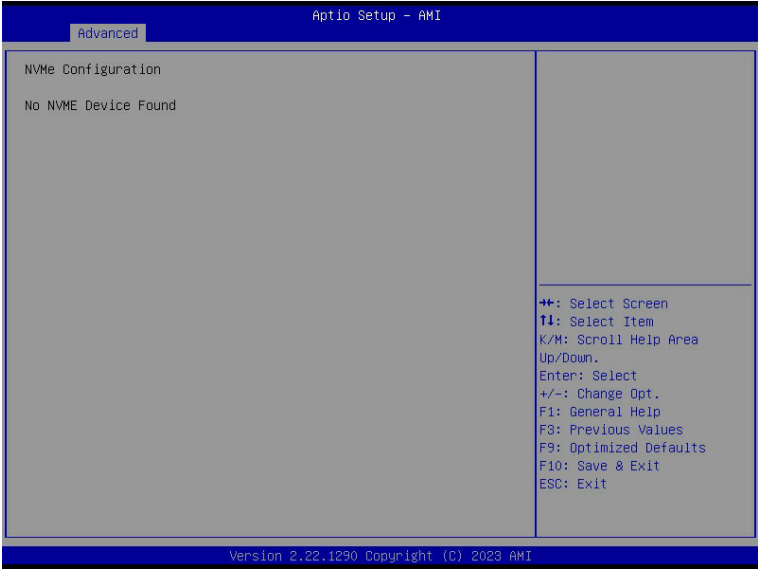
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 HTTP Support	Enable/Disable the Ipv4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

5-2-7 Post Report Configuration



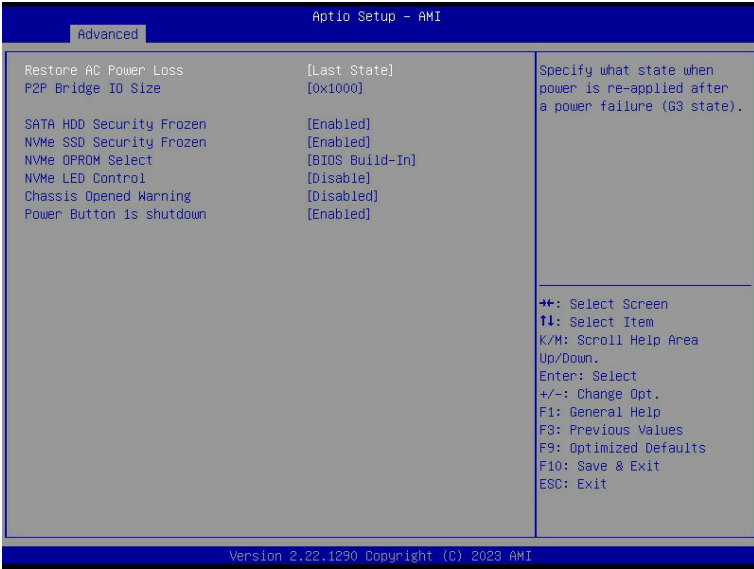
Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is Enabled .
Halt On	Options available: No Error, All Error. Default setting is No Error .

5-2-8 NVMe Configuration



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

5-2-9 Chipset Configuration

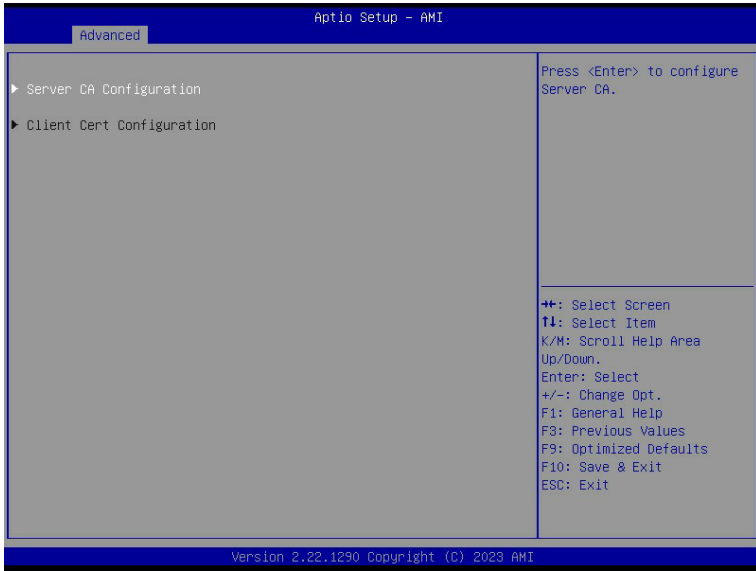


Parameter	Description
Restore on AC Power Loss ^(Note1)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
P2P Bridge IO Size	Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is 0x1000 .
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is Enabled .
NVMe SSD Security Frozen	Attempt to send freeze lock command to NVMe SSDs during boot. Options available: Enabled, Disabled. Default setting is Enabled .
Chassis Opened Warning ^(Note2)	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is Disabled .
Power Button is Shutdown	Options available: Enabled, Disabled, Clear. Default setting is Enabled .

(Note1) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

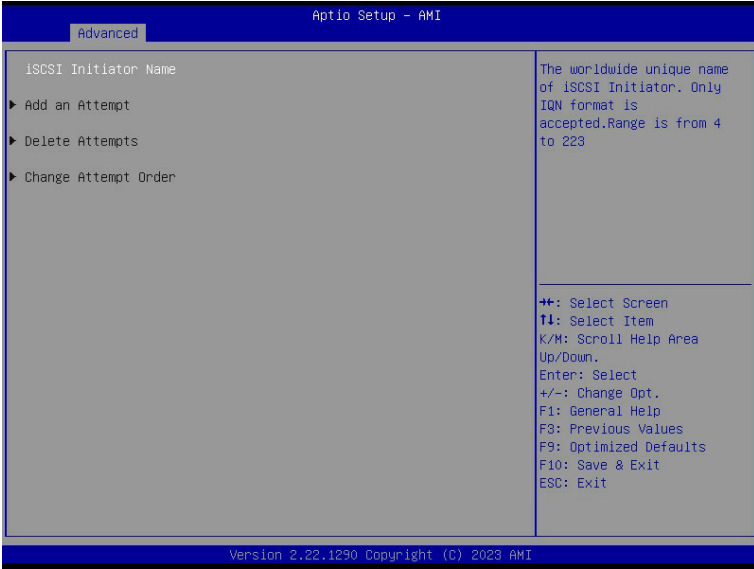
(Note2) Functions available on selected models.

5-2-10 Tls Auth Configuration



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

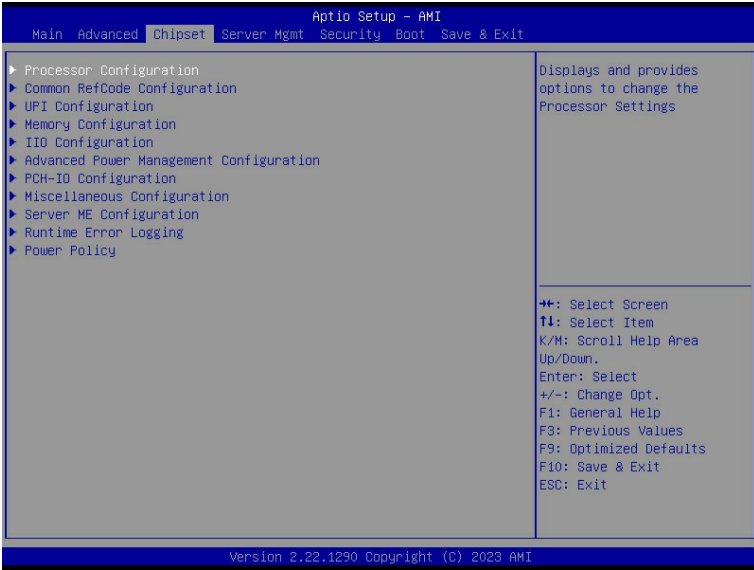
5-2-11 iSCSI Configuration



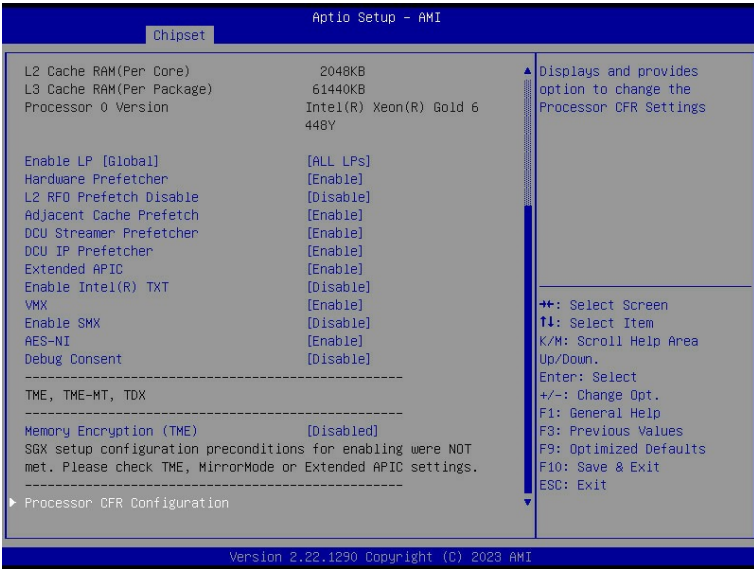
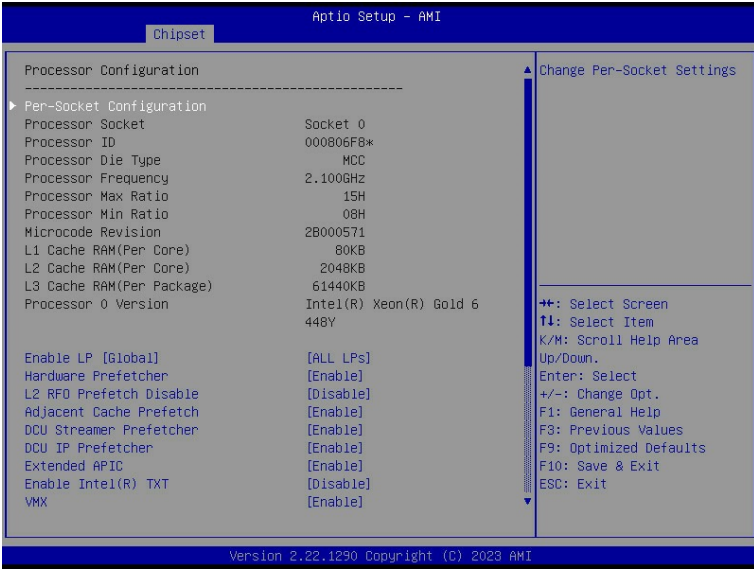
Parameter	Description
Attempt Priority	<p>Press [Enter] configure advanced items.</p> <ul style="list-style-type: none"> ◆ Attempt Priority <ul style="list-style-type: none"> – Use arrow keys to select the attempt, then press +/- keys to move the attempt up/down in the attempt order list. ◆ Commit Changes and Exit
Host iSCSI Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ iSCSI Initiator Name <ul style="list-style-type: none"> – Only IQN format is accepted. Range: from 4 to 223 ◆ Add an Attempt ◆ Delete Attempts ◆ Change Attempt Order

5-3 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

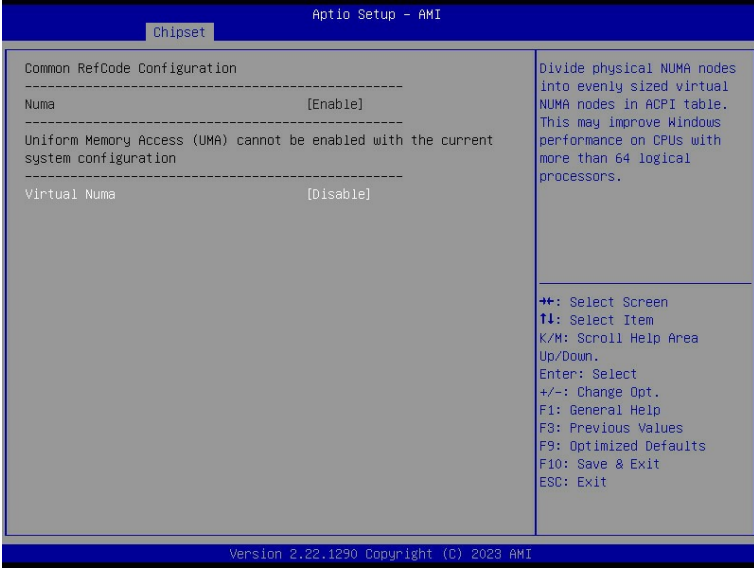


Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ CPU Socket 0/1 Configuration <ul style="list-style-type: none"> – Core Disable Bitmap(Hex) <ul style="list-style-type: none"> • Number of Cores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

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

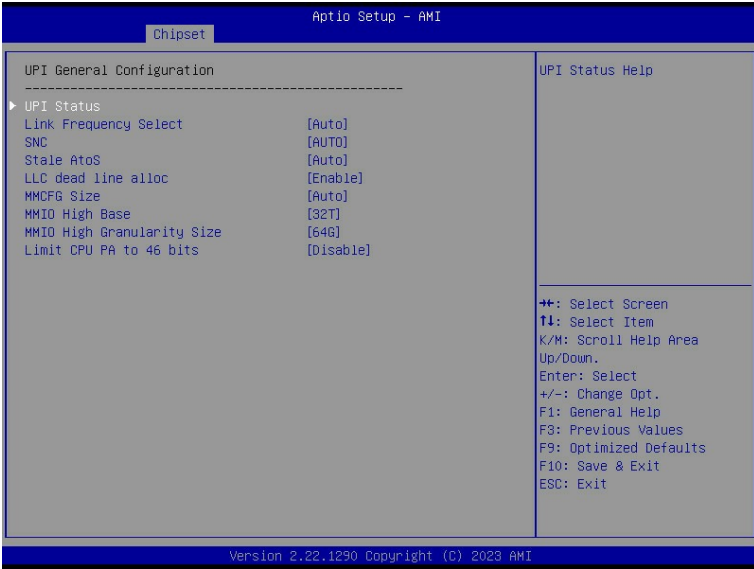
(Note) Advanced items prompt when this item is defined.

5-3-2 Common RefCode Configuration



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

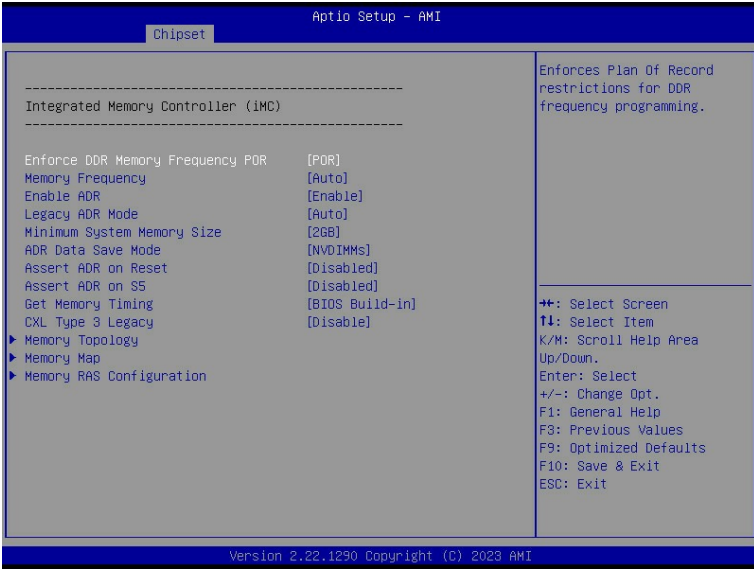
5-3-3 UPI Configuration



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

Parameter	Description
UPI General Configuration (continued)	<ul style="list-style-type: none"> <li data-bbox="352 142 956 197">◆ MMIO High Granularity Size <ul style="list-style-type: none"> <li data-bbox="386 169 956 197">– Selects the allocation size used to assign mmioh resources. <li data-bbox="386 200 956 255">– Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is 64G. <li data-bbox="352 258 956 313">◆ Clock Modulation Enabled <ul style="list-style-type: none"> <li data-bbox="386 285 956 313">– Options available: Disable, Enable, Auto. Default setting is Auto.

5-3-4 Memory Configuration



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

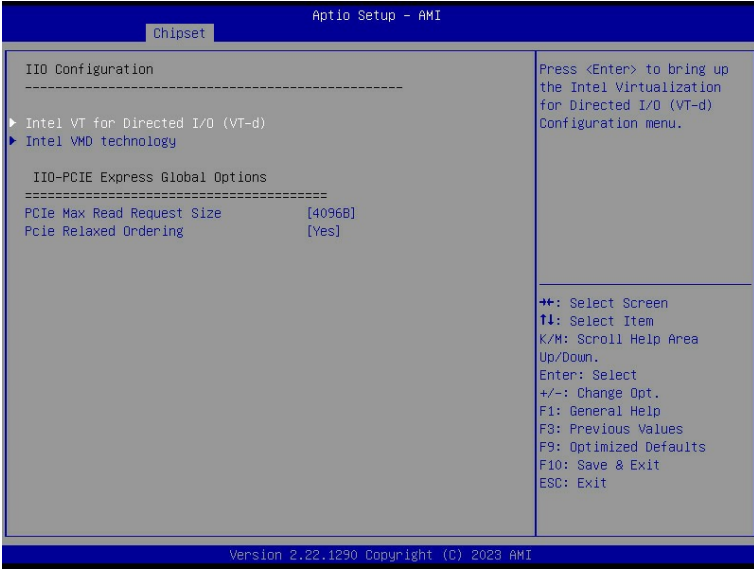
Parameter	Description
Assert ADR on S5	Enable/Disable Assert ADR on S5. Options available: Enabled, Disabled. Default setting is Disabled .
Get Memory Timing	Auto is the detected SPD value and use it, otherwise use BIOS Build-in. Options available: Auto, BIOS Build-in. Default setting is BIOS Build-in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

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

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

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

5-3-5 I/O Configuration

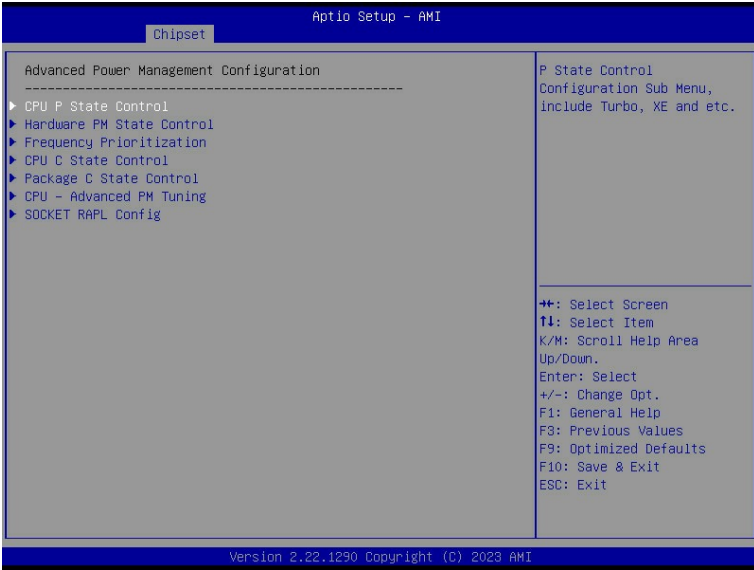


Parameter	Description
I/O Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel® VT for Directed I/O <ul style="list-style-type: none"> – Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to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

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

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

5-3-6 Advanced Power Management Configuration

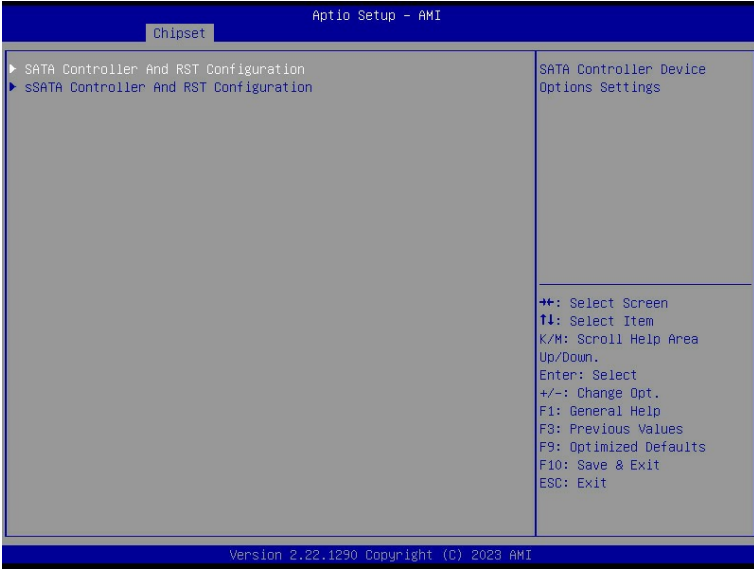


Parameter	Description
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ SpeedStep (Pstates) <ul style="list-style-type: none"> – Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in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

Parameter	Description
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Enable Monitor MWAIT <ul style="list-style-type: none"> – Allows Monitor and MWAIT instructions. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ CPU C6 Report <ul style="list-style-type: none"> – Enable/Disable CPU C6(ACPI C3) report to OS. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> – Core C1E auto promotion control. Takes effect after reboot. – Options available: Enable, Disable. Default setting is Enable.
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Package C State <ul style="list-style-type: none"> – Configures the state for the C-State package limit. – Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is Auto.
CPU - Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Energy Perf BIAS <ul style="list-style-type: none"> – Press [Enter] to configure advanced items. <ul style="list-style-type: none"> » Power Performance Tuning <ul style="list-style-type: none"> • Options available: OS Controls EPB, BIOS Controls EPB, PECL Controls EPB. Default setting is OS Controls EPB. » Energy_PERF_BIAS_CFG mode^(Note) <ul style="list-style-type: none"> • Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is Balanced Performance.
SOCKET RAPL Config	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ PL1 Power Limit <ul style="list-style-type: none"> – Press the <+> / <-> keys to increase or decrease the desired values. ◆ PL1 Timer Window <ul style="list-style-type: none"> – Configure PL1 Timer Window. ◆ PL2 Power Limit <ul style="list-style-type: none"> – Press the <+> / <-> keys to increase or decrease the desired values. ◆ PL2 Timer Window <ul style="list-style-type: none"> – Configure PL1 Timer Window.

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

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

Parameter	Description
SATA And RST Configuration/ sSATA Controller And RST Configuration (continued)	<ul style="list-style-type: none"> ◆ Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> – Enable/Disable Port 0/1/2/3/4/5/6/7 device. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Hot Plug (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> – Enable/Disable HDD Hot-Plug function. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Spin Up Device (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> – On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. – Options available: Enabled, Disabled. Default setting is Disabled.
SATA And RST Configuration/ tSATA Controller And RST Configuration	<ul style="list-style-type: none"> ◆ SATA Configuration <ul style="list-style-type: none"> – Enable/Disable SATA controller. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ SATA Mode Selection <ul style="list-style-type: none"> – Configures on chip SATA type. – AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time. – RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time. – Options available: AHCI, RAID. Default setting is AHCI. ◆ RAID Device ID^(Note) <ul style="list-style-type: none"> – Choose RAID Device ID. – Options available: Client, Alternate, Server. Default setting is Server. ◆ SATA Port 4/5/6/7 <ul style="list-style-type: none"> – The category identifies sSATA hard drives that are installed in the computer. System will automatically detect HDD type. ◆ SATA Port 4/5/6/7 <ul style="list-style-type: none"> – Enable/Disable Port 4/5/6/7 device. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Hot Plug (for Port 4/5/6/7) <ul style="list-style-type: none"> – Enable/Disable HDD Hot-Plug function. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Spin Up Device (for Port 4/5/6/7) <ul style="list-style-type: none"> – On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. – Options available: Enabled, Disabled. Default setting is Disabled.

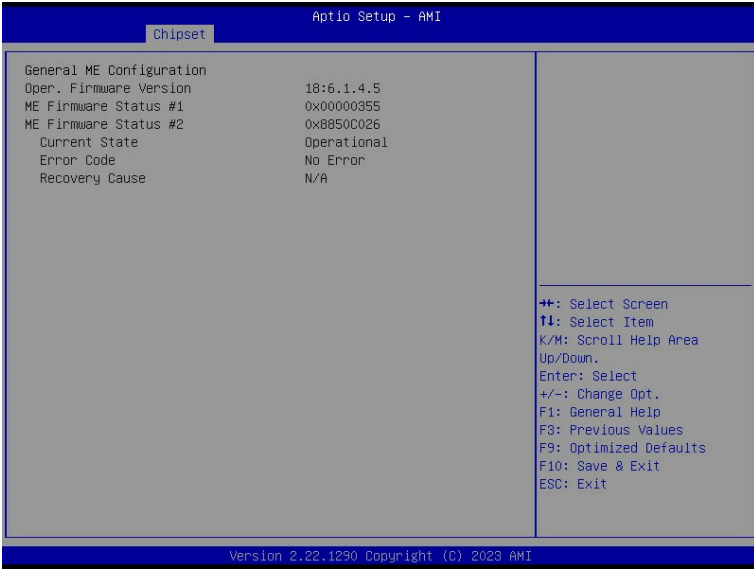
(Note) Only appears when HDD sets to **RAID Mode**.

5-3-8 Miscellaneous Configuration



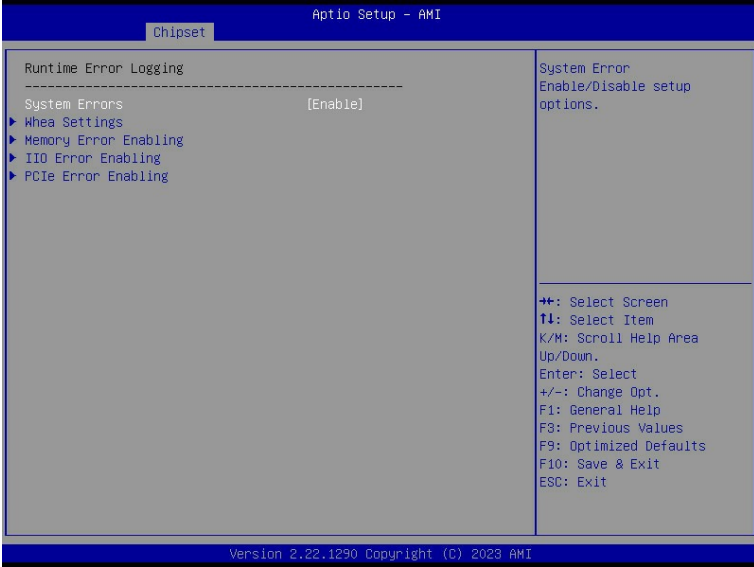
Parameter	Description
Miscellaneous Configuration	
Active Video	Selects the active video type. Options available: Auto, Onboard Device, PCIE Device, Specific PCIE Device. Default setting is Auto .
External SSC - CK440	Enables Spread spectrum - only affects external clock generator. Options available: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

5-3-9 Server ME Configuration



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

5-3-10 Runtime Error Logging Settings

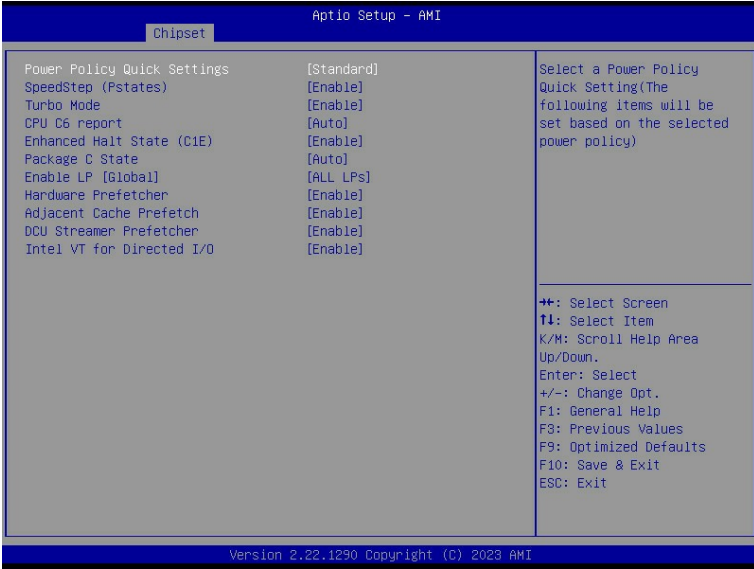


Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable, Disable. Default setting is Enable .
S/W Error Injection Support	Enable/Disable software injection error logging function. Options available: Enable, Disable. Default setting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

Parameter	Description
PCIe Error Enabling	<p data-bbox="309 142 642 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="309 170 852 252">◆ PCIe Error <ul style="list-style-type: none"> <li data-bbox="344 200 580 224">– Enable/Disable PCIe error. <li data-bbox="344 228 852 252">– Options available: Enable, Disable. Default setting is Disable. <li data-bbox="309 257 923 338">◆ Uncorrected Error^(Note) <ul style="list-style-type: none"> <li data-bbox="344 286 923 310">– Enables and escalates Uncorrectable/Recoverable Errors to error pins. <li data-bbox="344 315 846 338">– Options available: Enable, Disable. Default setting is Enable. <li data-bbox="309 343 846 424">◆ Fatal Error Enable^(Note) <ul style="list-style-type: none"> <li data-bbox="344 373 749 396">– Enables and escalates Fatal Errors to error pins. <li data-bbox="344 401 846 424">– Options available: Enable, Disable. Default setting is Enable. <li data-bbox="309 429 940 545">◆ Assert NMI on SERR^(Note) <ul style="list-style-type: none"> <li data-bbox="344 459 940 514">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. <li data-bbox="344 519 876 542">– Options available: Enabled, Disabled. Default setting is Enabled. <li data-bbox="309 550 940 663">◆ Assert NMI on PERR^(Note) <ul style="list-style-type: none"> <li data-bbox="344 580 940 635">– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. <li data-bbox="344 639 876 663">– Options available: Enabled, Disabled. Default setting is Enabled.

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

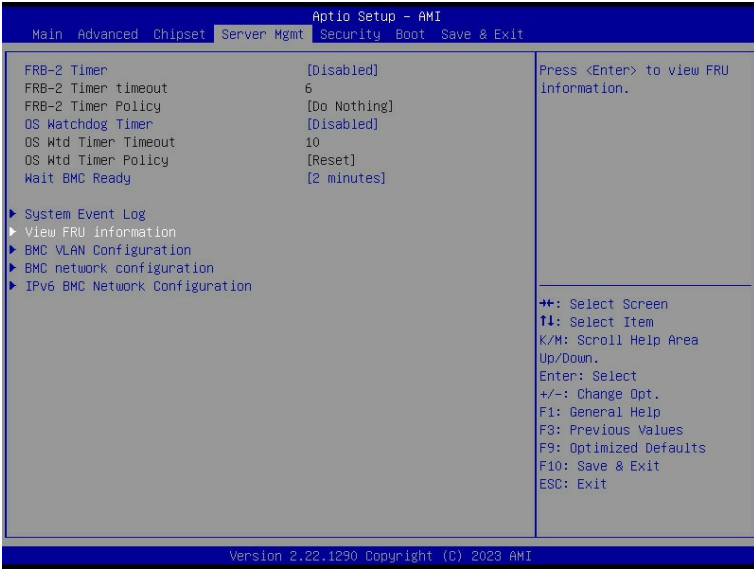
5-3-11 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient. Default setting is Standard .
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enable, Disable. Default setting is Enable .
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enable, Disable. Default setting is Enable .
CPU C6 report	Enable/Disable the BIOS to enable the report from the CPU C6 state (ACPI C3) to the OS. Options available: Disable, Enable, Auto. Default setting is Auto .
Enhanced Halt State (C1E)	Enable/Disable the C1E support for lower power consumption. Takes effect after reboot. Options available: Enable, Disable. Default setting is Enable .
Package C State	Configures the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is Auto .

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

5-4 Server Management Menu



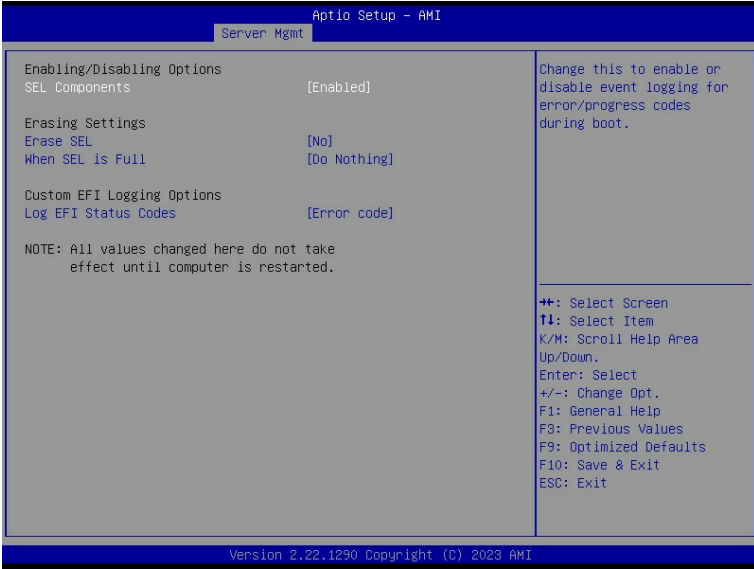
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is Enabled .
FRB-2 Timer ^(Note1) timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is 6 minutes .
FRB-2 Timer Policy ^(Note1)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

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

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

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

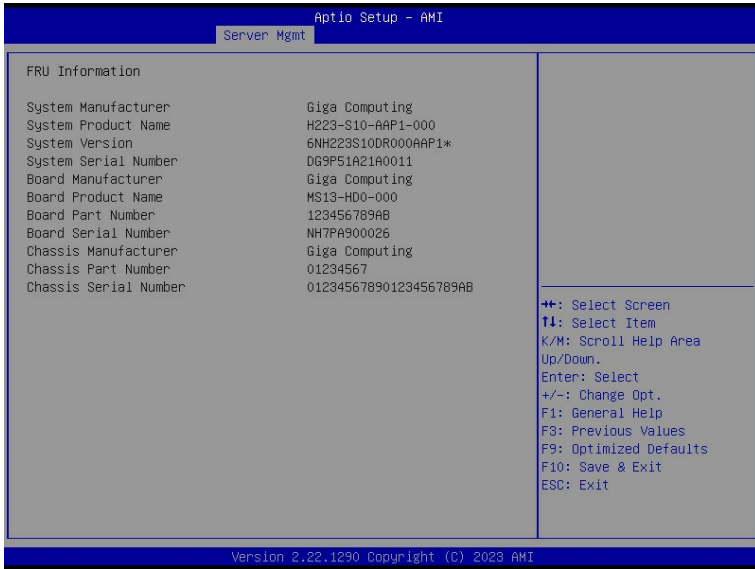
5-4-1 System Event Log



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

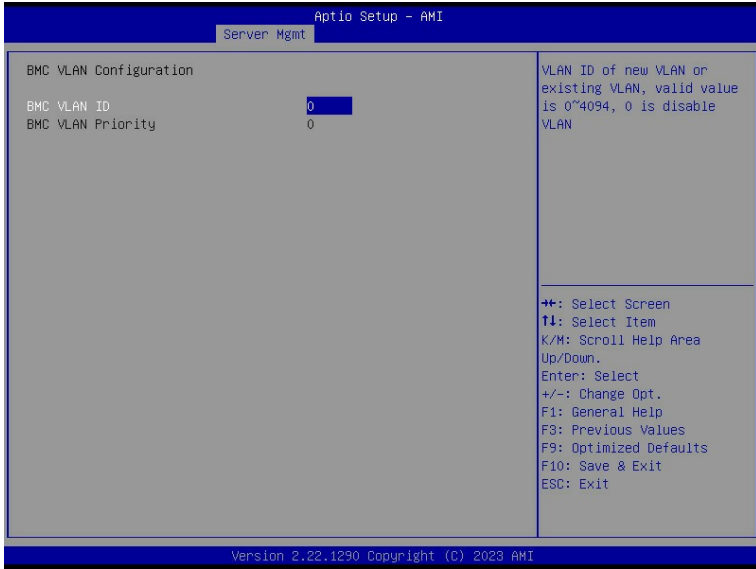
5-4-2 View FRU Information

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



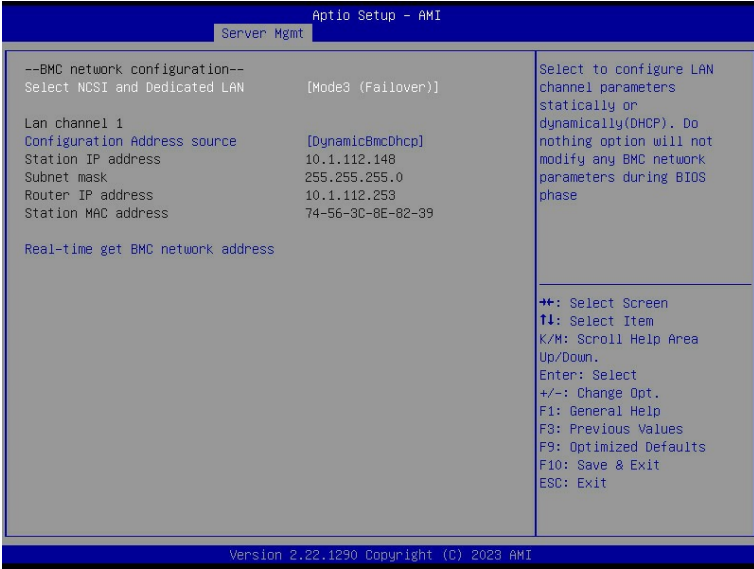
(Note) The model name will vary depends on the product you purchased

5-4-3 BMC VLAN Configuration



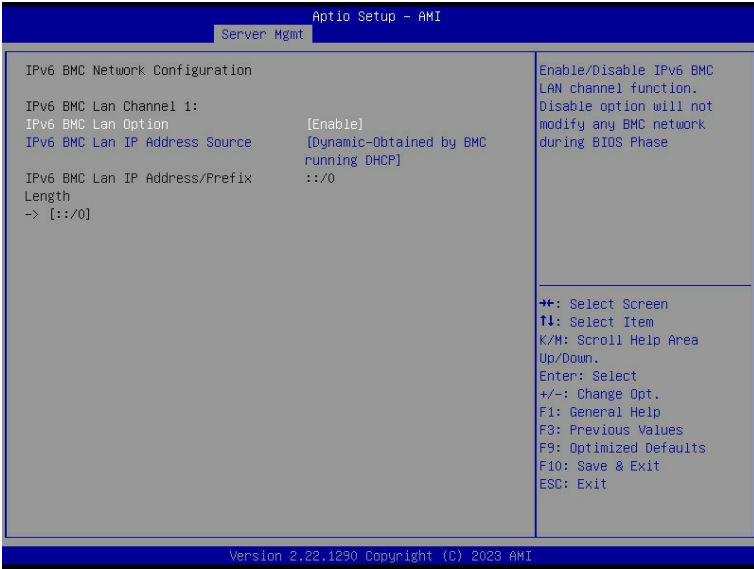
Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority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

5-4-4 BMC Network Configuration



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

5-4-5 IPv6 BMC Network Configuration



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

5-5 Security Menu

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



There are two types of passwords that you can set:

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

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

5-5-1 Secure Boot

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

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



Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, Disabled. Default setting is Disabled .
Secure Boot Mode ^(Note)	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before the Operating System loads to the login screen have not been tampered with. When set to Standard, it will automatically load the Secure Boot keys 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 Standard .
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.

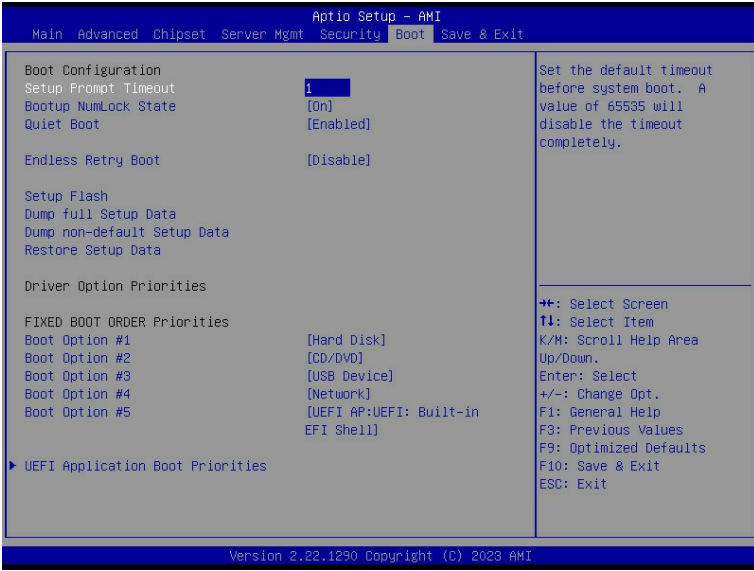
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Expert Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 941 235">Please note that this item is configurable when Secure Boot Mode is set to Custom.</p> <ul style="list-style-type: none"> <li data-bbox="335 243 946 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 946 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode. <li data-bbox="367 326 909 352">– Options available: Enabled, Disabled. Default setting is Disabled. <li data-bbox="335 357 931 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 931 404">– Installs all factory default keys. It will force the system in User Mode. <li data-bbox="367 409 611 431">– Options available: Yes, No. <li data-bbox="335 435 654 509">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode. <li data-bbox="367 487 611 509">– Options available: Yes, No. <li data-bbox="335 514 904 595">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 537 904 595">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). <li data-bbox="335 600 941 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 624 941 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device. <li data-bbox="335 686 899 736">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 899 736">– Displays the current status of the variables used for secure boot. <li data-bbox="335 741 803 846">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 765 803 788">– Displays the current status of the Platform Key (PK). <li data-bbox="367 793 680 816">– Press [Enter] to configure a new PK. <li data-bbox="367 821 601 846">– Options available: Update. <li data-bbox="335 851 946 987">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 874 946 898">– Displays the current status of the Key Exchange Key Database (KEK). <li data-bbox="367 903 909 961">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="367 965 675 987">– Options available: Update, Append. <li data-bbox="335 992 946 1128">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1016 909 1039">– Displays the current status of the Authorized Signature Database. <li data-bbox="367 1044 946 1102">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="367 1107 675 1128">– Options available: Update, Append. <li data-bbox="335 1133 904 1270">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1157 904 1180">– Displays the current status of the Forbidden Signature Database. <li data-bbox="367 1185 893 1243">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="367 1248 675 1270">– Options available: Update, Append.

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

5-6 Boot Menu

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

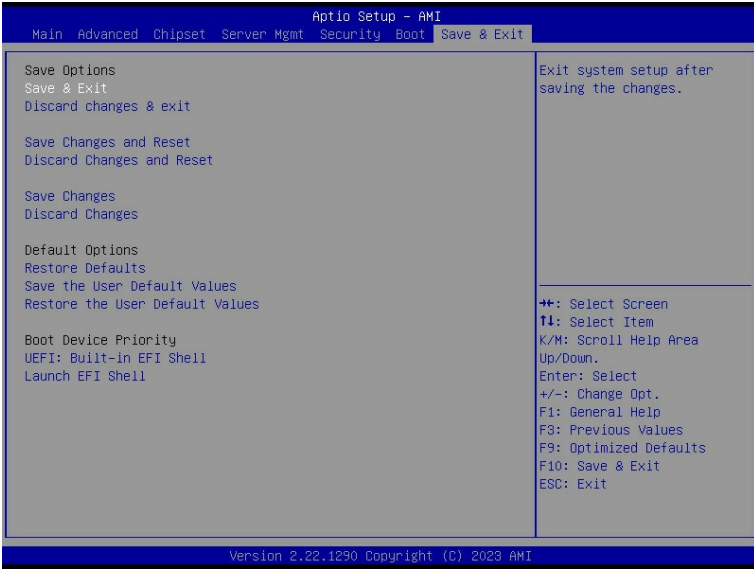


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off.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

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

5-7 Save & Exit Menu

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



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

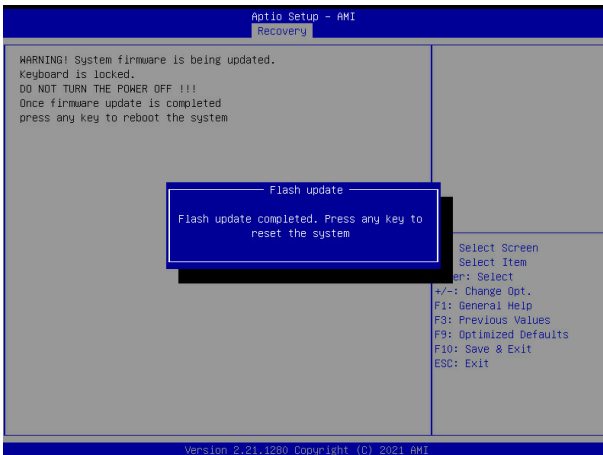
Parameter	Description
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system 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