

GIGABYTE™

R184-S90-AAV1

Rack Server - Intel® Xeon® 6 Processors - 1U DP 4-Bay Gen5 NVMe/SATA/SAS-4

User Manual

Rev. 1.0

Copyright

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

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

Disclaimer

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

Documentation Classifications

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

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

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

For More Information

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

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

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

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

Conventions

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

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

Server Warnings and Cautions

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



WARNING!

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

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



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



WARNING!

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



WARNING!

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



WARNING!

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



CAUTION!

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



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 any component and pin touching. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

System power on/off: To remove power from system, you must remove the system from rack. Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

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

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

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

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

Table of Contents

Chapter 1 Hardware Installation	9
1-1 Installation Precautions	9
1-2 Product Specifications	10
1-3 System Block Diagram	14
Chapter 2 System Appearance	15
2-1 Front View	15
2-2 Rear View	16
2-3 Front Panel LEDs and Buttons	17
2-3-1 RoT LEDs	18
2-4 Rear System LAN LEDs	20
2-5 Power Supply Unit (PSU) LED	21
2-6 Hard Disk Drive LEDs	22
Chapter 3 System Hardware Installation	23
3-1 Removing Chassis Cover	24
3-2 Removing and Installing the Fan Duct	25
3-3 Removing and installing the Heat Sink	26
3-4 Installing the CPU	27
3-5 Installing the Memory	29
3-5-1 Eight Channel Memory Configuration	29
3-5-2 Installing the Memory	30
3-5-3 DIMM Population Table	31
3-5-4 Processor and Memory Module Matrix Table	32
3-6 Installing the PCI Expansion Card	33
3-7 Installing the Mezzanine Card	34
3-7-1 OCP 3.0	34
3-8 Installing the Hard Disk Drive	35
3-9 Installing the M.2 Device and Heat Sink	37
3-9-1 M.2 device with Heatsink	37
3-10 Replacing the Fan Assembly	38
3-11 Replacing the Power Supply	39
3-12 Removing the LAN Cable	40
3-13 Cable Routing	41
Chapter 4 Motherboard Components	43

4-1	Motherboard Components	43
4-2	Jumper Setting	45
4-3	Backplane Board Storage Connector	46
4-3-1	CBP1048	46
Chapter 5 BIOS Setup		47
5-1	The Main Menu	49
5-2	Advanced Menu	52
5-2-1	Trusted Computing	53
5-2-2	Serial Port Console Redirection	54
5-2-3	SIO Configuration	57
5-2-4	PCI Subsystem Settings	58
5-2-5	USB Configuration	60
5-2-6	Network Stack Configuration	61
5-2-7	Post Report Configuration	62
5-2-8	KMIP Server Configuration	63
5-2-9	NVMe Configuration	64
5-2-10	Chipset Configuration	65
5-2-11	Tls Auth Configuration	66
5-2-12	iSCSI Configuration	67
5-2-13	Intel(R) i350 Gigabit Network Connection	68
5-2-14	VLAN Configuration	70
5-2-15	MAC IPv6 Network Configuration	71
5-2-16	MAC IPv4 Network Configuration	72
5-2-17	Driver Health	73
5-3	Chipset Menu	74
5-3-1	Processor Configuration	75
5-3-2	Common RefCode Configuration	78
5-3-3	UPI Configuration	79
5-3-4	Memory Configuration	81
5-3-5	IIO Configuration	84
5-3-6	Advanced Power Management Configuration	85
5-3-7	Miscellaneous Configuration	87
5-3-8	Runtime Error Logging Settings	88
5-3-9	Power Policy	90
5-4	Server Management Menu	92
5-4-1	System Event Log	94
5-4-2	View FRU Information	95
5-4-3	BMC VLAN Configuration	96
5-4-4	BMC Network Configuration	97

5-4-5	IPv6 BMC Network Configuration	98
5-5	Security Menu	99
5-5-1	Secure Boot	100
5-6	Boot Menu	103
5-7	Save & Exit Menu	105
5-8	BIOS Recovery	107
5-9	BIOS POST Beep code (AMI standard)	108
5-9-1	PEI Beep Codes	108
5-9-2	DXE Beep Codes	108

Chapter 1 Hardware Installation

1-1 Installation Precautions

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

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








1-2 Product Specifications



NOTE:

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

	System Dimension	<ul style="list-style-type: none"> ◆ 1U ◆ 438mm (W) x 43.5mm (H) x 815mm (D)
	CPU	<ul style="list-style-type: none"> ◆ Intel® Xeon® 6 Processors <ul style="list-style-type: none"> - Intel® Xeon® 6700E-Series Processors - Intel® Xeon® 6700P-Series Processors (available Q1'25) - Intel® Xeon® 6500P-Series Processors (available Q1'25) ◆ Dual processor, CPU TDP up to 350W
<p>Note: If only 1 CPU is installed, some PCIe or memory functions might be unavailable</p>		
	Socket	<ul style="list-style-type: none"> ◆ 2 x LGA 4710 ◆ Socket E2
	Chipset	<ul style="list-style-type: none"> ◆ System on Chip
	Security	<ul style="list-style-type: none"> ◆ UEFI Secure Boot ◆ Silicon root of trust (Option) ◆ SNMP Support: V3
	Memory	<ul style="list-style-type: none"> ◆ 32 x DIMM slots ◆ DDR5 memory supported ◆ MCR DIMM supported* ◆ 8-Channel memory architecture ◆ RDIMM: Up to 6400 MT/s (1DPC), 5200 MT/s (2DPC) ◆ MCR DIMM: Up to 8000 MT/s <p>*MCR DIMMs are only supported with Intel® Xeon® 6 Processors with P-cores and in a 1DPC configuration.</p>
	LAN	<p>Rear side:</p> <ul style="list-style-type: none"> ◆ On I/O board: <ul style="list-style-type: none"> - 2 x 1Gb/s LAN ports (1 x Intel® I350-AM2) - Support NCSI function - 1 x 10/100/1000 Mbps Management LAN
	Video	<ul style="list-style-type: none"> ◆ Integrated in Aspeed® AST2600 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp
	Storage	<p>Front side:</p> <ul style="list-style-type: none"> ◆ 4 x 3.5"/2.5" Gen5 NVMe/SATA/SAS-4* hot-swappable bays <ul style="list-style-type: none"> - (NVMe from CPU_0) <p>*Storage card is required to support SATA and SAS drives.</p>

	SAS	<ul style="list-style-type: none"> ◆ Require SAS add-in cards
	RAID	<ul style="list-style-type: none"> ◆ Require RAID add-in cards
	Expansion Slot	<ul style="list-style-type: none"> ◆ Riser Card CRS101J: <ul style="list-style-type: none"> - 1 x PCIe x16 slot (Gen5 x16), FHHL from CPU_0 ◆ Riser Card CRS101K: <ul style="list-style-type: none"> - 1 x PCIe x16 slot (Gen5 x16), FHHL from CPU_1 ◆ 1 x OCP 3.0 slot with PCIe Gen5 x16 bandwidth, from CPU_0 <ul style="list-style-type: none"> - Supports NCSI function ◆ 1 x OCP 3.0 slot with PCIe Gen5 x16 bandwidth, from CPU_1 <ul style="list-style-type: none"> - Supports NCSI function ◆ 2 x M.2 slots: <ul style="list-style-type: none"> - M-Key - PCIe Gen5 x4, from CPU_1 - Support 2280/22110 cards ◆ 1 x M.2 slot (On I/O board): <ul style="list-style-type: none"> - M-Key - PCIe Gen5 x2, from CPU_0 - Supports 2280 cards
	Internal I/O	<ul style="list-style-type: none"> ◆ 1 x VROC connector ◆ 1 x TPM header ◆ 1 x PRoT connector (only enabled on RoT SKU)
	Front I/O	<ul style="list-style-type: none"> ◆ 2 x USB 3.2 Gen1 ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x NMI button ◆ 1 x Reset button ◆ 2 x LAN activity LEDs ◆ 1 x Storage activity LED ◆ 1 x System status LED
	Rear I/O	<ul style="list-style-type: none"> ◆ On I/O board: <ul style="list-style-type: none"> - 2 x USB 3.2 Gen1 - 1 x Mini-DP - 2 x RJ45 - 1 x MLAN - 1 x ID LED
	Backplane I/O	<ul style="list-style-type: none"> ◆ Speed and bandwidth: PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s



TPM

- ◆ 1 x TPM header with SPI interface
 - **Optional** TPM2.0 kit: CTM012



Power Supply

- ◆ 1+1 1600W 80 PLUS Titanium redundant power supplies
- ◆ AC Input:
 - 100-127V~/ 12A, 50-60Hz
 - 200-240V~/ 10A, 50-60Hz
- ◆ DC Input: (Only for China)
 - 240Vdc/ 8A
- ◆ DC Output:
 - Max 1000W/ 100-127V~
 - +12.2V/ 82A
 - +12.2Vsb/ 3A
 - Max 1600W/ 200-240V~ or 240Vdc Input
 - +12.2V/ 132A
 - +12.2Vsb/ 3A

NOTE:

GIGABYTE provides PSUs with various energy efficiency ratings and power outputs. Please contact our sales representatives to determine the best configuration for your system.



System Management

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

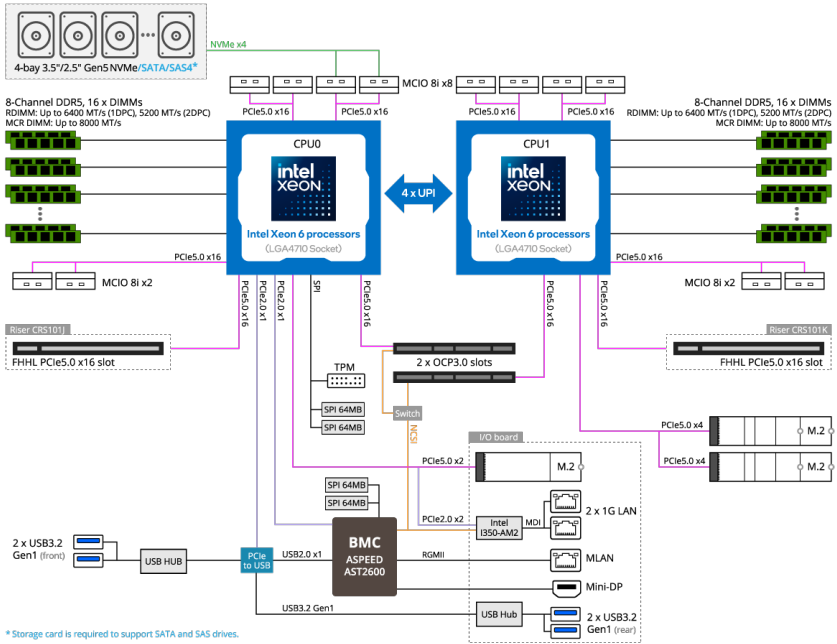
- ◆ Dashboard
- ◆ HTML5 KVM
- ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)
- ◆ Sensor Reading History Data
- ◆ FRU Information
- ◆ SEL Log in Linear Storage / Circular Storage Policy
- ◆ Hardware Inventory
- ◆ Fan Profile
- ◆ System Firewall
- ◆ Power Consumption
- ◆ Power Control
- ◆ 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

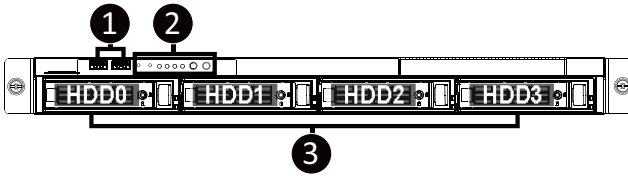
- ◆ Operating temperature: 10°C to 35°C
- ◆ Operating humidity: 8%-80% (non-condensing)
- ◆ Non-operating temperature: -40°C to 60°C
- ◆ Non-operating humidity: 20%-95% (non-condensing)

1-3 System Block Diagram



Chapter 2 System Appearance

2-1 Front View

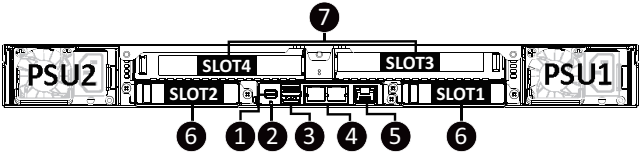


No.	Description
1.	Front USB 3.2 Gen1 Ports
2.	Front Panel LEDs and Buttons
3.	3.5"/2.5" Drive Bays
NOTE! Drives with green latches support NVMe.	



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

2-2 Rear View

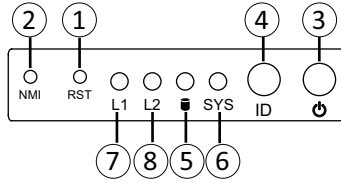


No.	Description
1.	Mini DisplayPort
2.	ID LED
3.	USB 3.2 Gen1 Port x 2
4.	Data LAN Port x 2
5.	Management LAN Port
6.	OCP 3.0 Slot (Option/SFF)
7.	PCIe Card Slot



- Remove the LAN Cable. See 3-11 Removing the LAN Cable on page 40.

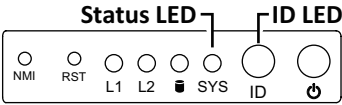
2-3 Front Panel LEDs and Buttons



No.	Name	Color	Status	Description
1.	Reset Button			Press the button to reset the system.
2.	NMI button			Press the button server generates a NMI to the processor if the multiple-bit ECC errors occur, which effectively halt the server.
3.	Power button with LED	Green	On	System is powered on
		N/A	Off	System is not powered on or in ACPI S5 state (power off)
4.	ID Button ^(Note)			Press the button to activate system identification
5.	HDD Status LED	Green	On	HDD locate
			Blink	HDD access
		Amber	On	HDD fault
		Green/Amber	Blink	HDD rebuilding
		N/A	Off	No HDD access or no HDD fault.
6.	System Status LED ^(Note)	Green	On	System is operating normally.
			On	Critical condition, may indicate: System fan failure System temperature
		Amber	Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion
			N/A	Off
7/8.	LAN 1/2 Active/Link LEDs	Green	On	Link between system and network or no access.
		Green	Blink	Data transmission or receiving is occurring
		N/A	Off	No data transmission or receiving is occurring

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

2-3-1 RoT LEDs



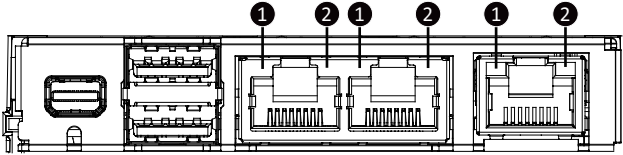
	LED on Front panel ^(Note5)	
	ID LED	Status LED
EC Firmware (FW) Authentication fail or not exit		
EC FW is broken or not exit ^(Note1)	OFF	OFF
Authenticating/Recovering BMC/BIOS Images		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per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

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

2-4 Rear System LAN LEDs



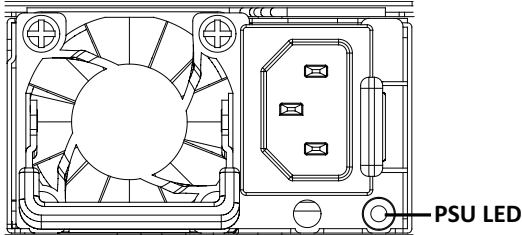
No.	Name	Color	Status	Description
1.	1GbE Speed LED	Yellow	On	1 Gbps data rate
		Green	On	100 Mbps data rate
		N/A	Off	10 Mbps data rate
2.	1GbE Link/ Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or receiving is occurring
		N/A	Off	No data transmission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

2-5 Power Supply Unit (PSU) LED



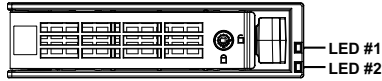
NOTE!

The power supply may be vary based on the system configuration.



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

2-6 Hard Disk Drive LEDs



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

LED #2	HDD Present	No HDD
Green	ON	OFF

NOTE:

*1: Depends on HBA/Utility Spec.

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

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

Chapter 3 System Hardware Installation



Pre-installation Instructions

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

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

3-1 Removing Chassis Cover

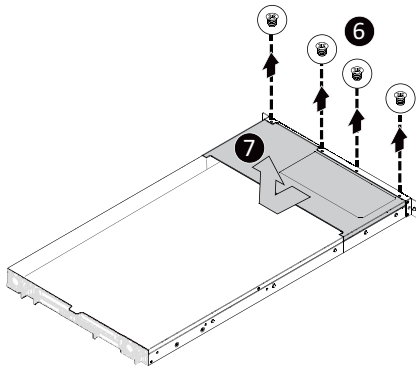
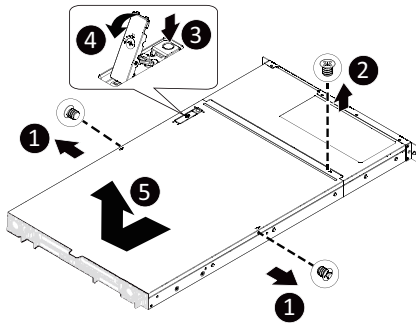


Before you remove or install the system cover

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

Follow these instructions to remove the chassis cover:

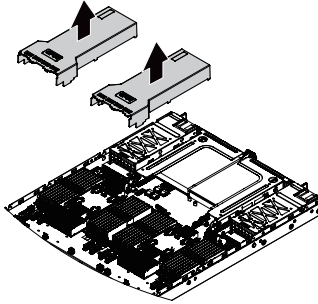
1. Remove the screws on both sides of the back chassis cover. (Note: For safe shipping, installation screws are added and should be removed before deployment/putting it in the server cabinet.)
2. Remove the screw securing the back chassis cover.
3. Push button to unlock the handle.
4. Pull the grip handle to open the panel cover.
5. Slide the back chassis cover towards the rear and remove the chassis cover in the direction indicated.
6. Remove the screws securing the front chassis cover.
7. Slide the front chassis cover towards the rear and remove the chassis cover in the direction indicated.
8. To reinstall the chassis cover reverse steps 2-7.



3-2 Removing and Installing the Fan Duct

Follow these instructions to remove/install the fan duct:

1. Lift up to remove the fan duct
2. To install the fan duct, align the fan duct with the guiding groove. Push down the fan duct into chassis until it is firmly seated.



3-3 Removing and installing the Heat Sink



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

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

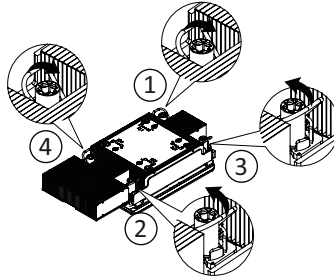


WARNING!

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

Follow these instructions to remove/install the heat sink:

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



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

3-4 Installing the CPU



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

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

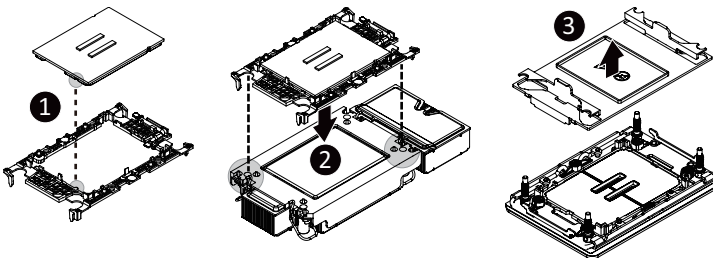


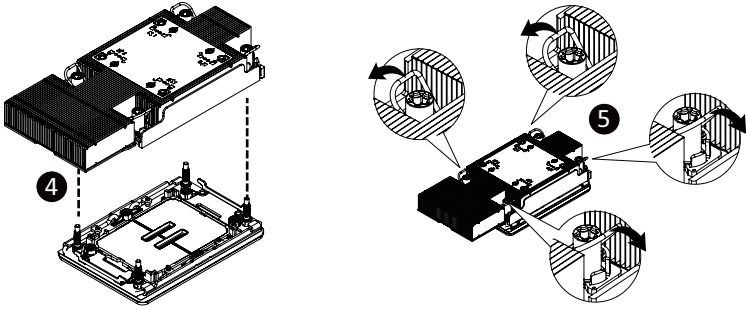
WARNING!

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

Follow these instructions to Install the CPU:

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





Carrier Types used for Package Types

Package Type	Granite Rapids-SP XCC	Granite Rapids-SP HCC Granite Rapids-SP LCC Sierra Forest-SP Clearwater Forest-SP
Carrier Code	E2A	E2B
Shim?	No	Yes
Integrated TIM Break Lever	Yes	Yes

NOTE!

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

3-5 Installing the Memory

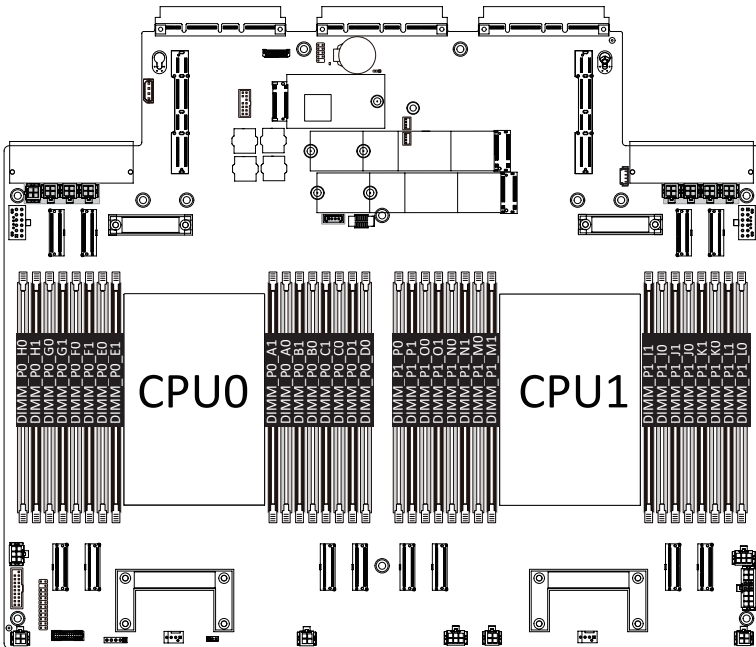


Read the following guidelines before you begin to install the memory:

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

3-5-1 Eight Channel Memory Configuration

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



3-5-2 Installing the Memory



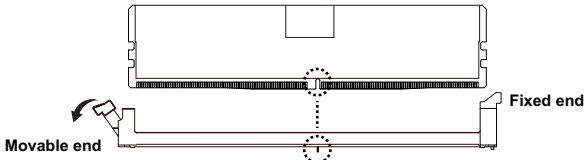
Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR5 DIMMs on this motherboard.

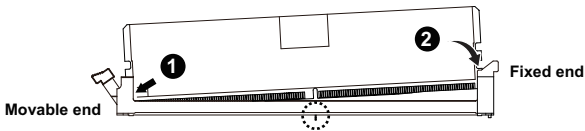
Make sure your DIMM slots have a single latch or a double latch.

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

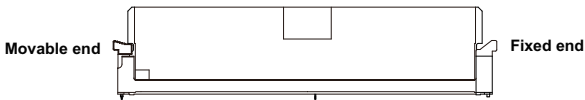
1. Open the plastic latch of the memory slot, then place the memory module as pre-inserted vertically position.



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



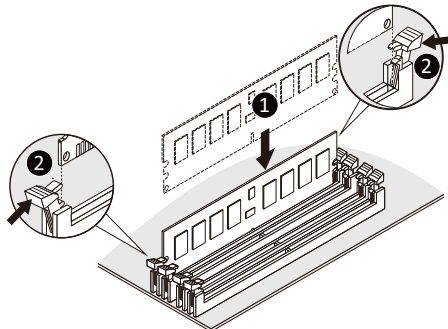
3. Then use both hands to insert the memory module vertically into the DIMM slot and push it down. Close the plastic latch at the edge of the DIMM slots to lock the memory module.



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

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

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



3-5-3 DIMM Population Table

Intel Xeon 6700E-Series Memory Support

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

NOTE:

- Only DDR5-6400 Rated RDIMMs Supported.

Intel Xeon 6700E-Series CXL Memory Support

Native DDR5 Memory Per Socket				CXL Memory Per Socket				
Slot 0 DIMM Ranks	Slot 0 DIMM Capacity (GB)	DIMM Type	DRAM Density (Gb)	CXL Memory Channels	CXL Memory Type	CXL Capacity Per Device/Module	CXL Interleave	CXL Mode
2Rx4	64	10x4	16	2+2	DDR5 x8	64 GB	1x4*, 2x2, 4x1	1LM+Vol
2Rx4	64	10x4	16	1+1	DDR5 x16	128 GB	1x2*, 2x1	1LM+Vol
1Rx4	32	10x4	16	2	DDR5 x8	128 GB	1x2*	Intel® Flat Memory Mode

NOTE:

- * Default setting in BIOS
- Intel Xeon 6700E-series (formerly codenamed Sierra Forest-SP) CXL memory configs are 1DPC ('Slot 0') only for native DDR5
- CXL Memory Channel notation: # of devices per root port, with root ports separated by "+". i.e. 2+2+2+2 = four root ports populated with two devices per root port
- CXL Interleave notation: sets x ways. i.e. 2x4 = One set of two modules, interleaved four-way
- CXL Modes:
 - 1LM+Vol = DDR5 ('1LM') and (Volatile) CXL memory visible to SW as separate tiers, separately interleaved
 - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW

3-5-4 Processor and Memory Module Matrix Table

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

NOTE:

- Xeon 6700E/6500E-series do not support 12 DIMMs Configuration.

3-6 Installing the PCI Expansion Card



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

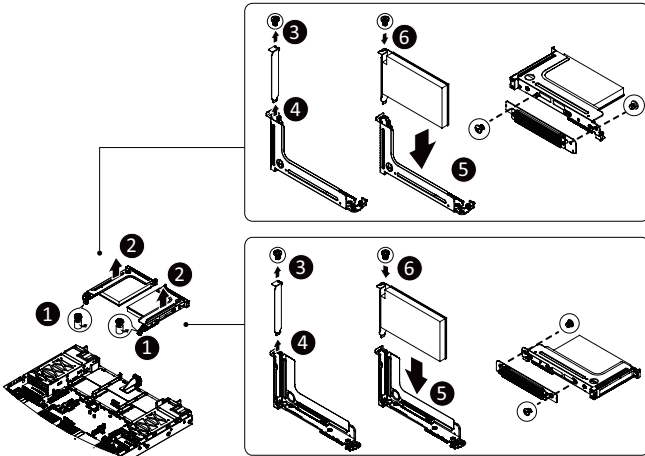
Failure to observe these warnings could result in personal injury or damage to equipment.



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

Follow these instructions for a PCI Expansion card:

1. Loosen the thumbscrew securing the riser bracket.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the slot cover from the riser bracket.
4. Remove the slot covers from the riser bracket.
5. Orient the PCIe card with the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCIe card connector.
6. Secure the PCIe card with the screw.
7. Reverse the previous steps to install the riser bracket.



3-7 Installing the Mezzanine Card

3-7-1 OCP 3.0

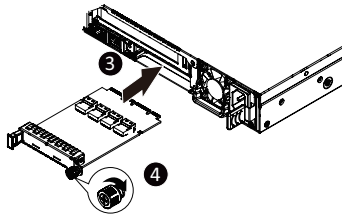
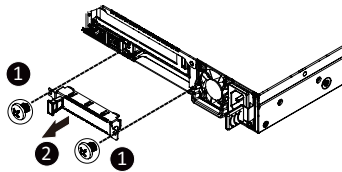


Use of the following type of OCP 3.0 NIC is recommended:

- OCP 3.0 SFF with Pull Tab
- OCP 3.0 SFF with Ejector Latch

Follow these instructions to install an OCP 3.0 mezzanine card:

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



3-8 Installing the Hard Disk Drive

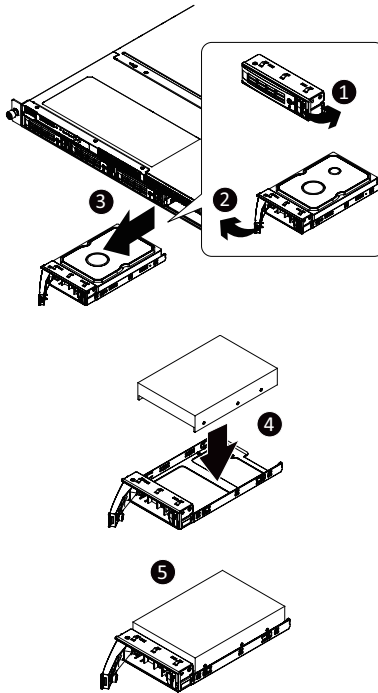


Read the following guidelines before you begin to install the HDD:

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

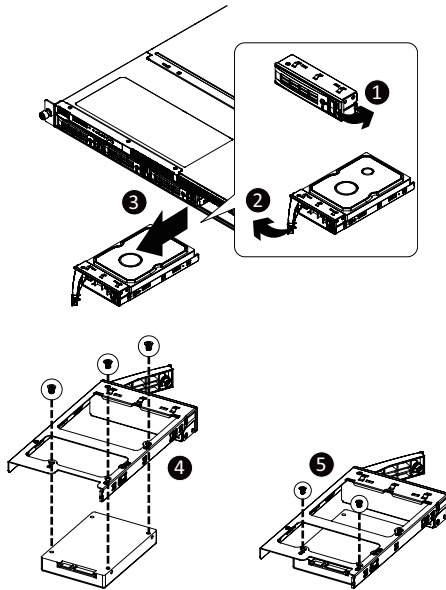
Follow these instructions to install a 3.5" HDD:

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



Follow these instructions to install 2.5" hard disk drive into 3.5" HDD Tray:

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



3-9 Installing the M.2 Device and Heat Sink

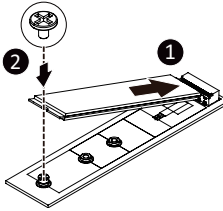


CAUTION

The position of the stand-off screw will depend on the size of the M.2 device. The stand-off screw is pre-installed for 22110 cards as standard. Refer to the size of the M.2 device and change the position of the stand-off screw accordingly.

Follow these instructions to install the M.2 device:

1. Insert the M.2 SSD module into the slot.
2. Secure it with the screw, tightening as necessary to fasten the M.2 SSD module in place.



3-9-1 M.2 device with Heatsink



WARNING:

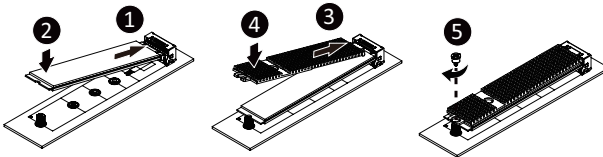
Please ensure a heatsink is attached to any M.2 device installed into the system. Installing an M.2 device without any heatsink may result in the system overheating or system performance being throttled.



- Please Go to [4-1 Motherboard Component](#) for specific M.2 Slot location.
- To install/remove the M.2 module and Heatsink use a No. 1 Phillips-head screwdriver with a screw torque of $1.5 \pm 0.2 \text{ kg}^{\ast}\text{cm}$

Follow these instructions to install the M.2 device and heat sink:

1. Insert the M.2 device into the M.2 connector.
2. Press down on the M.2 device.
3. Install the thermal pad of the M.2 device to the M.2 device.
4. Press down on the thermal pad.
5. Secure the M.2 device and its thermal pad to the motherboard with a single screw.
6. Reverse steps 1-2 to remove the M.2 device.



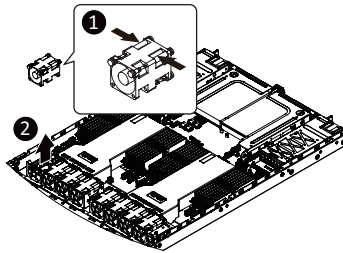
3-10 Replacing the Fan Assembly



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

Follow these instructions to replace the fan assembly:

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



3-11 Replacing the Power Supply

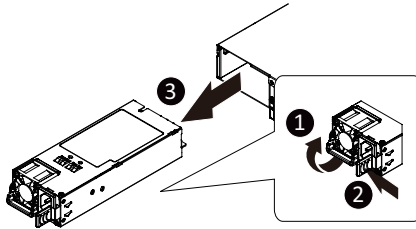


CAUTION!

- In order to reduce the risk of injury from electric shock, disconnect AC power from the power supply before removing the power supply from the system

Follow these instructions to replace the power supply:

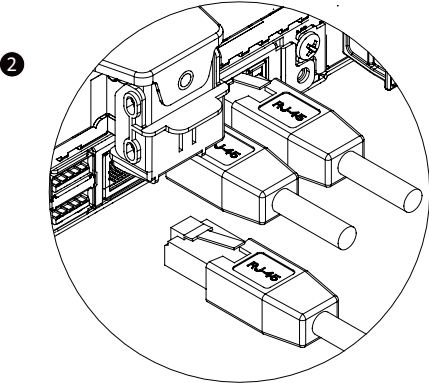
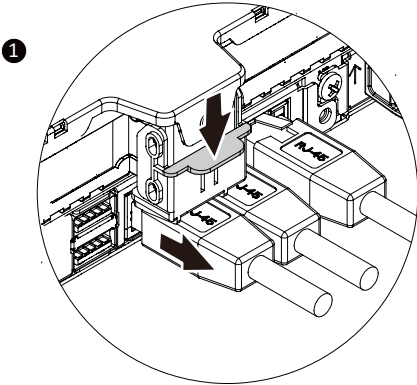
1. Flip and then grasp the power supply handle.
2. Press the retaining clip on the top side of the power supply in the direction indicated.
3. Pull out the power supply using the handle.
4. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power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



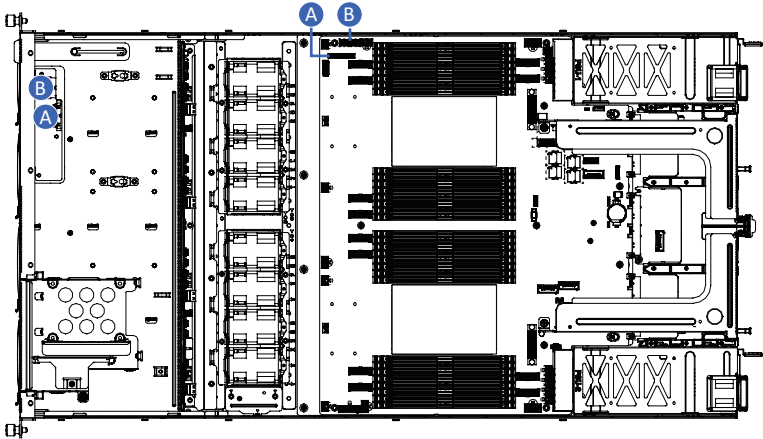
3-12 Removing the LAN Cable

Follow these instructions to remove the LAN cable:

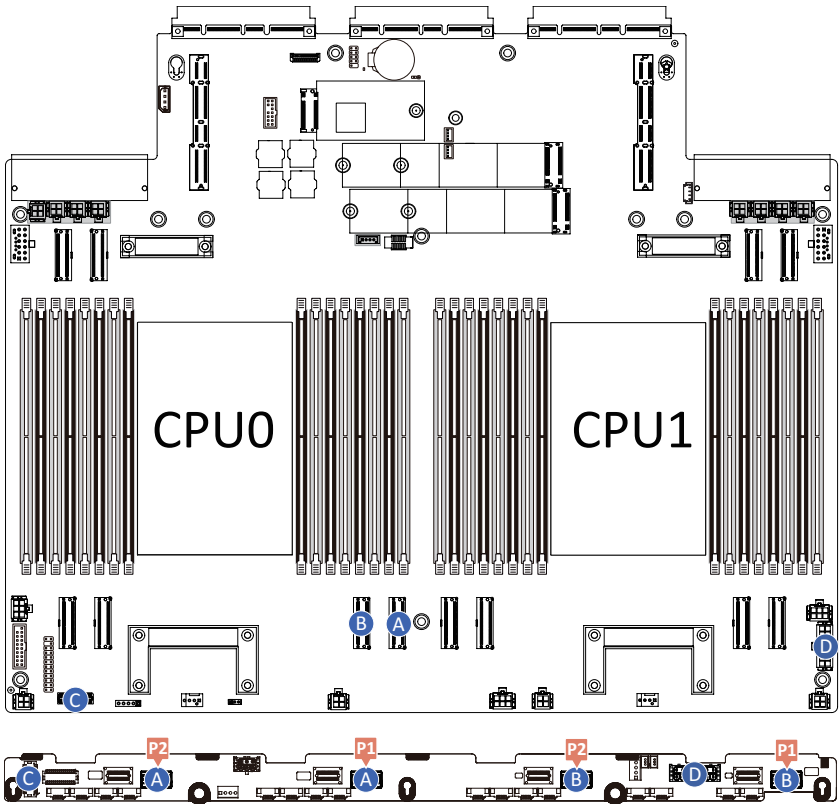
1. Press the release latch while simultaneously pulling out the LAN cable.



3-13 Cable Routing



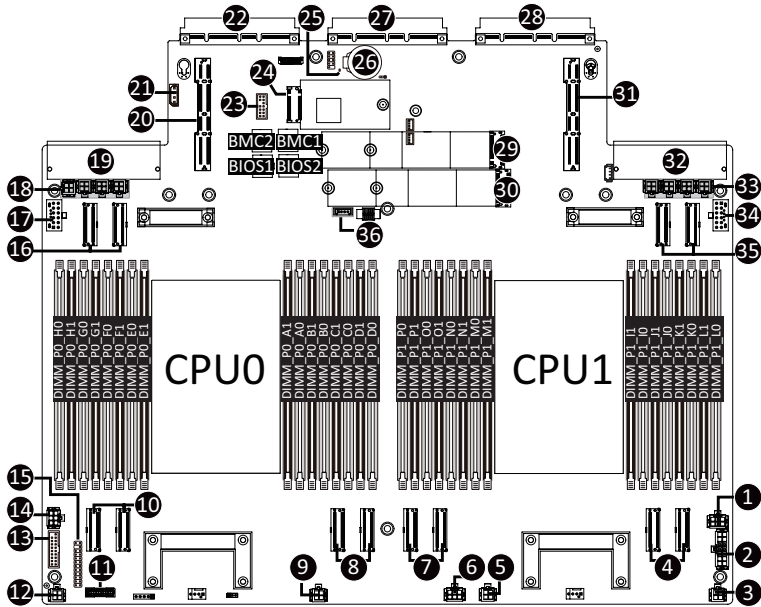
A	Front Switch/LED Cable	Motherboard: FP_1
		Front IO Board: FP_1
B	Front USB 3 Cable	Motherboard: F_USB1
		Front IO Board: F_USB3



A	NVMe 0-1 Cable	Motherboard: U2_P0_4CA
		Backplane Board: U.2 0/ U.2 1
B	NVMe 2-3 Cable	Motherboard: U2_P0_4GE
		Backplane Board: U.2 2/ U.2 3
C	Backplane Board Signal Cable	Motherboard: BP_1
		Backplane Board: BP_1
D	Backplane Board Power Cable	Motherboard: ATX1
		Backplane Board: BP_2X7

Chapter 4 Motherboard Components

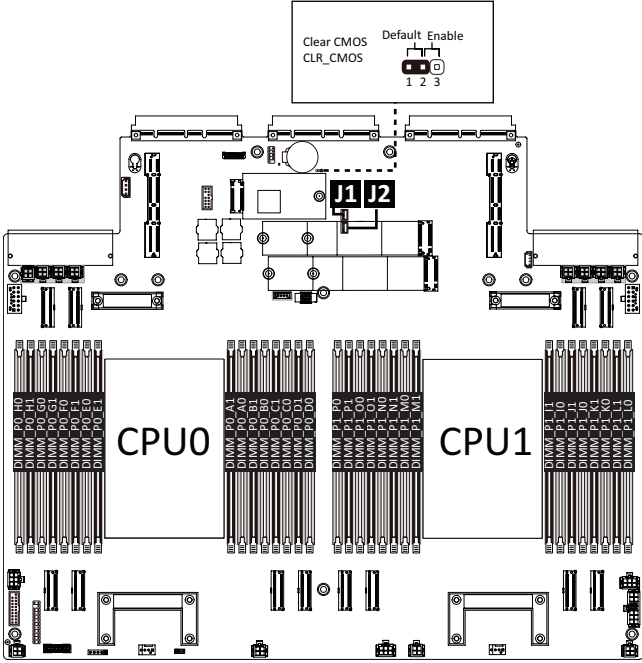
4-1 Motherboard Components



Item	Description
1	2 x 3 Pin ATX Power Connector (ATX2)
2	2 x 7 Pin ATX Power Connector (ATX1)
3	2 x 2 Pin P12V Backplane Power Connector (P12V_BP4)
4	MCI/O Connector (U2_P1_4GE/4CA/PCIe Gen5)
5	2 x 2 Pin P12V Backplane Power Connector (P12V_BP3)
6	2 x 3 Pin ATX Power Connector (ATX3)
7	MCI/O Connector (U2_P1_5GE/5CA/PCIe Gen5)
8	MCI/O Connector (U2_P0_4GE/4CA/PCIe Gen5)
9	2 x 2 Pin P12V Backplane Power Connector (P12V_BP2)
10	MCI/O Connector (U2_P0_5GE/5CA/PCIe Gen5)
11	HDD Backplane Board Connector
12	2 x 2 Pin P12V Backplane Power Connector (P12V_BP1)
13	Front Panel USB 3.2 Gen1 Connector
14	2 x 3 Pin ATX Power Connector (ATX4)
15	Front Panel Connector
16	MCI/O Connector (U2_P0_3AC/3EG/PCIe Gen5)
17	P12V GPU Power Connector (P12V_S6)
18	PCIe Power Connector (PCIE1/2/3/4_PWR)
19	Power Supply Connector#1 (Primary)
20	Riser Connector (GENZ1/PCIe Gen5)
21	IPMB Connector

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

4-2 Jumper Setting

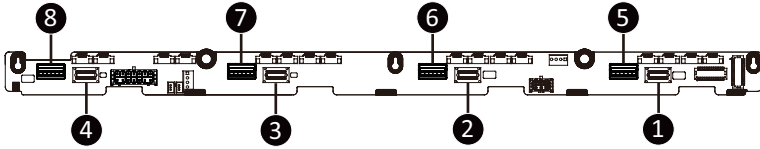


J1		ON	OFF
1	S3_MASK	Stop initial power on when BMC is not ready	Normal [Default]
2	BIOS_RCVR	BIOS Recovery Mode	Normal [Default]
3	BIOS_PWD	Clear Supervisor Password	Normal [Default]
4	RST BMC_EN	ID button to enable BMC reset	Normal [Default]

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

4-3 Backplane Board Storage Connector

4-3-1 CBP1048



Item	Description
1	SlimSAS 4i Connector (SFF-8654 / SATA0)
2	SlimSAS 4i Connector (SFF-8654 / SATA1)
3	SlimSAS 4i Connector (SFF-8654 / SATA2)
4	SlimSAS 4i Connector (SFF-8654 / SATA3)
5	MCIO 4i (SFF-TA-1016 / U.2 0)
6	MCIO 4i (SFF-TA-1016 / U.2 1)
7	MCIO 4i (SFF-TA-1016 / U.2 2)
8	MCIO 4i (SFF-TA-1016 / U.2 3)

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 1 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

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

■ **Main**

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

■ **Advanced**

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

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

■ **Chipset**

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

■ **Server Management**

Server additional features enabled/disabled setup menus.

■ **Security**

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

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

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

■ **Boot**

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

■ **Save & Exit**

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

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

5-1 The Main Menu

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

Main Menu Help

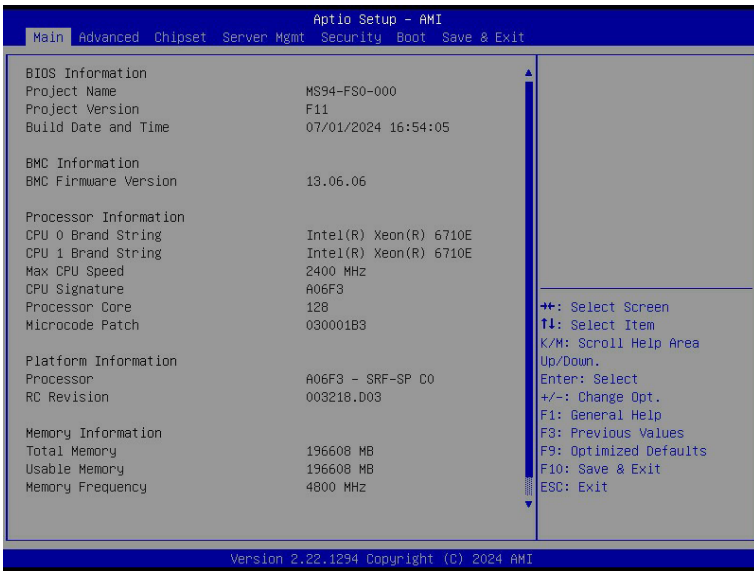
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

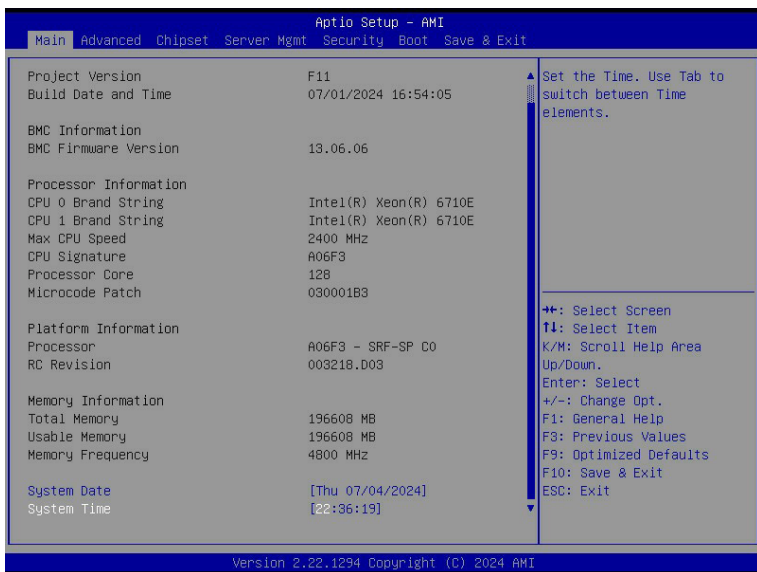
Submenu Help

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



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





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

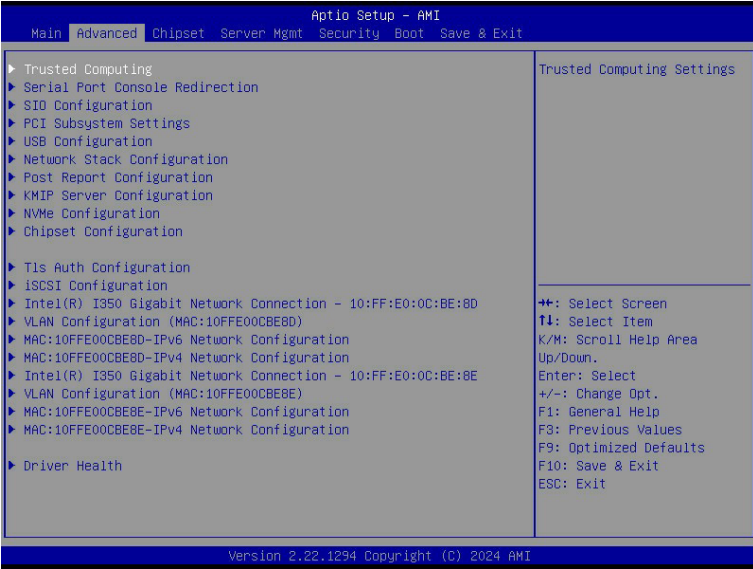
(Note1) Functions available on selected models.

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

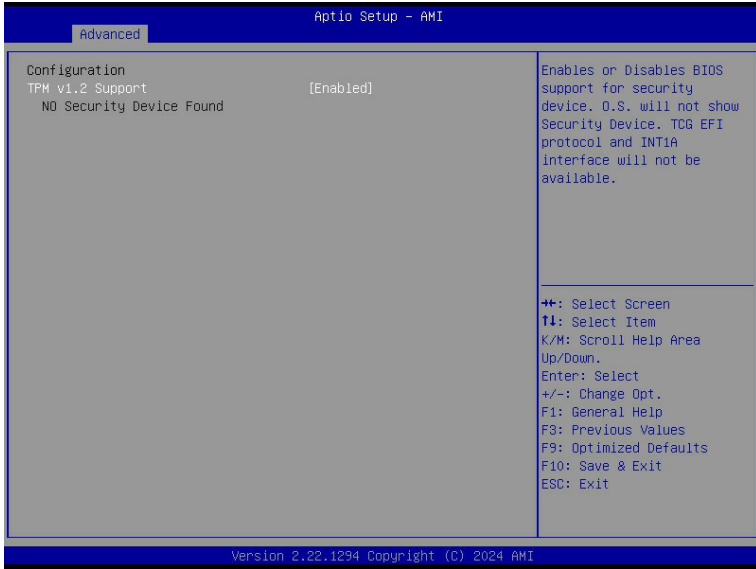
Parameter	Description
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

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.

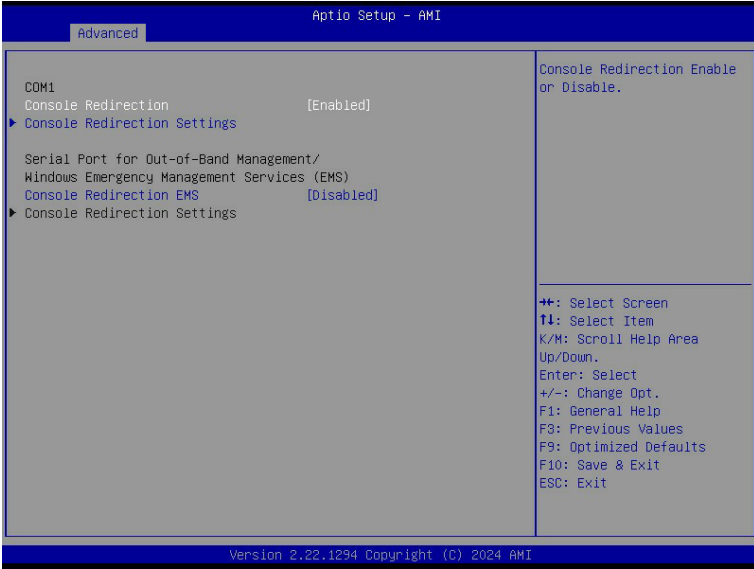


5-2-1 Trusted Computing



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



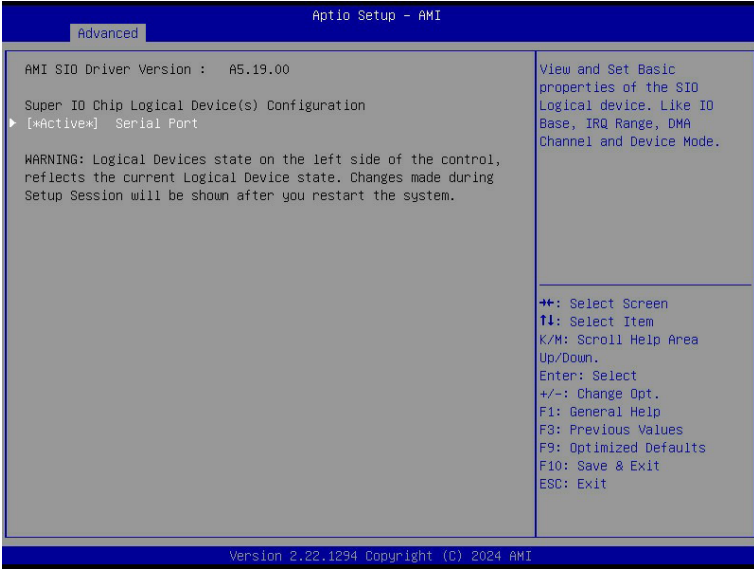
Parameter	Description
COM1 Console Redirection ^(Note)	<p>Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>
COM1 Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <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	
	Press [Enter] to configure advanced items.
	<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.
[*Active*] Serial Port	

5-2-4 PCI Subsystem Settings

Aptio Setup - AMI

Advanced

PCI Bus Driver Version	A5.01.32	Enable/Disable SLOT1 I/O ROM ++: Select Screen T1: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT1 I/O ROM	[Enabled]	
SLOT1 Lanes	[Auto]	
SLOT1 Max Link Speed	[Auto]	
SLOT2 I/O ROM	[Enabled]	
SLOT2 Lanes	[Auto]	
SLOT2 Max Link Speed	[Auto]	
SLOT3 I/O ROM	[Enabled]	
SLOT3 Lanes	[Auto]	
SLOT3 Max Link Speed	[Auto]	
SLOT4 I/O ROM	[Enabled]	
SLOT4 Lanes	[Auto]	
SLOT4 Max Link Speed	[Auto]	
SLOT6 I/O ROM	[Enabled]	++: Select Screen T1: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT6 Lanes	[Auto]	
SLOT6 Max Link Speed	[Auto]	
SLOT11 I/O ROM	[Enabled]	
SLOT11 Lanes	[Auto]	
SLOT11 Max Link Speed	[Auto]	

Version 2.22.1294 Copyright (C) 2024 AMI

Aptio Setup - AMI

Advanced

SLOT6 Lanes	[Auto]	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root ID Virtualization Support. ++: Select Screen T1: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
SLOT6 Max Link Speed	[Auto]	
SLOT11 I/O ROM	[Enabled]	
SLOT11 Lanes	[Auto]	
SLOT11 Max Link Speed	[Auto]	
M2A I/O ROM	[Enabled]	
M2A Lanes	[Auto]	
M2A Max Link Speed	[Auto]	
M2B I/O ROM	[Enabled]	
M2B Lanes	[Auto]	
M2B Max Link Speed	[Auto]	
LAN I/O ROM	[Enabled]	++: Select Screen T1: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
M2C I/O ROM	[Enabled]	
PCI Devices Common Settings:		
Re-Size BAR Support	[Disabled]	
SR-IOV Support	[Enabled]	

Version 2.22.1294 Copyright (C) 2024 AMI

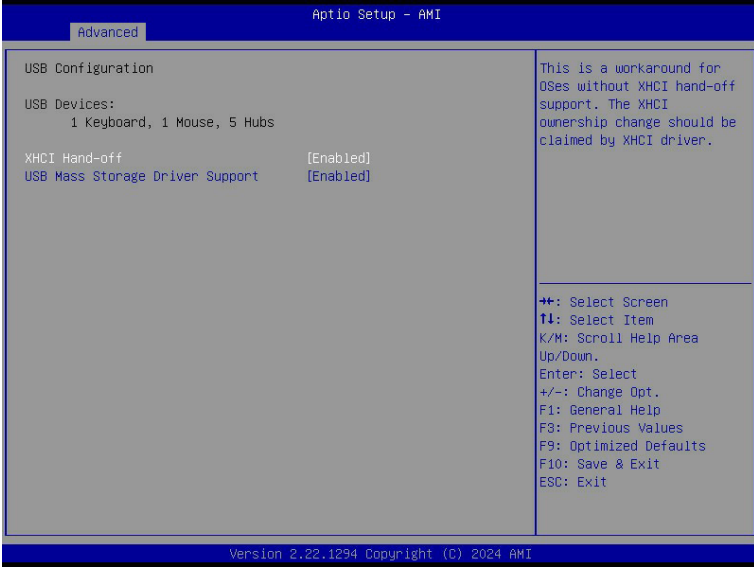
Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT_# I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is Enabled .
SLOT_# Lanes ^(Note1)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

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

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

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

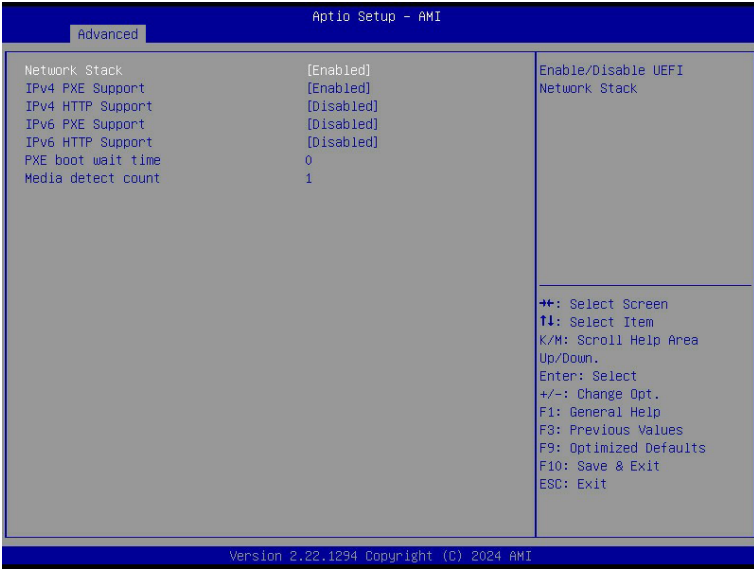
5-2-5 USB Configuration



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

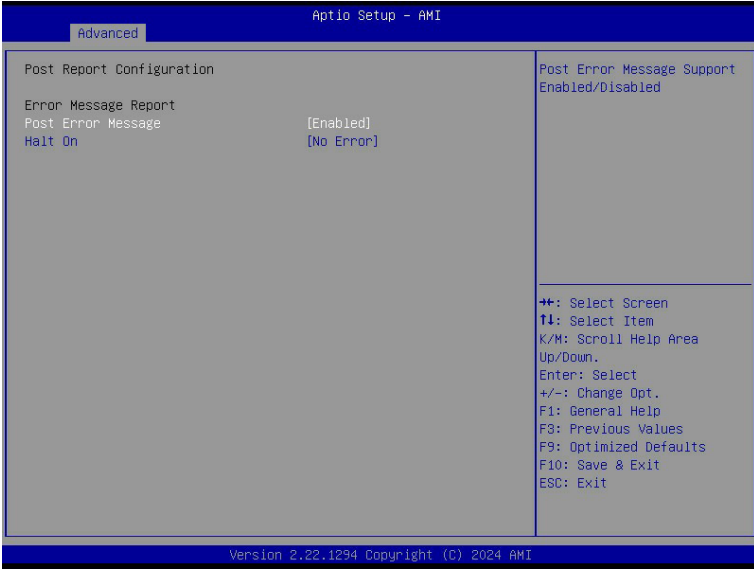
(Note) This item is present only if you attach USB devices.

5-2-6 Network Stack Configuration



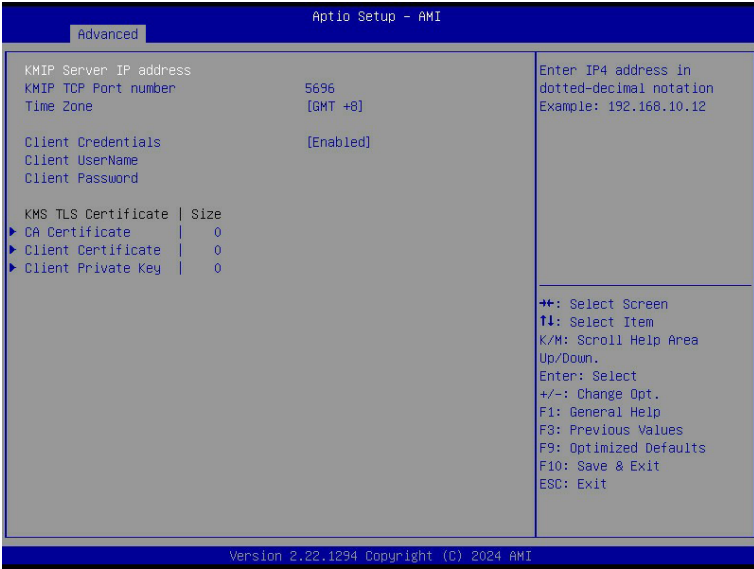
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is Enabled .
Ipv4 HTTP Support	Enable/Disable the Ipv4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



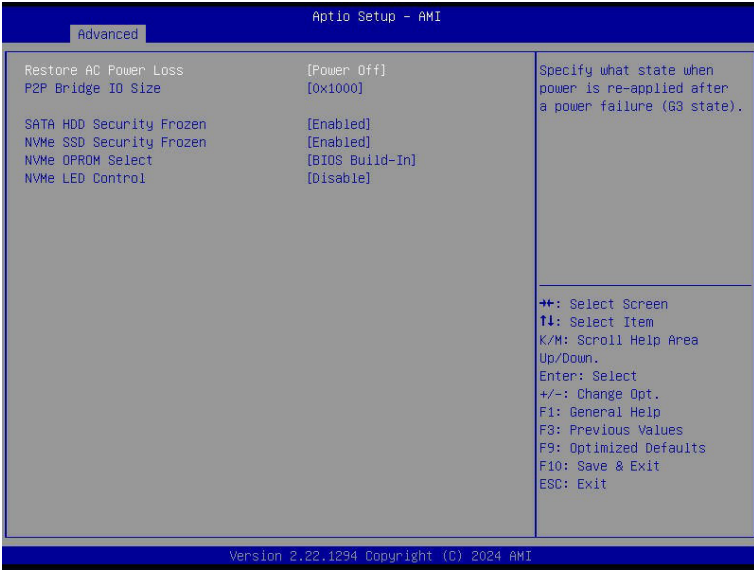
Parameter	Description
KMIP Server IP address	
KMIP TCP Port Number	
Time Zone	Enter the correct timem zone for this server. Default setting is GMT+8 .
Client Credentials	Use User and password credentials to authenticate the Client. Options available: Enabled, Disabled, Clear. Default setting is Enabled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

5-2-9 NVMe Configuration



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

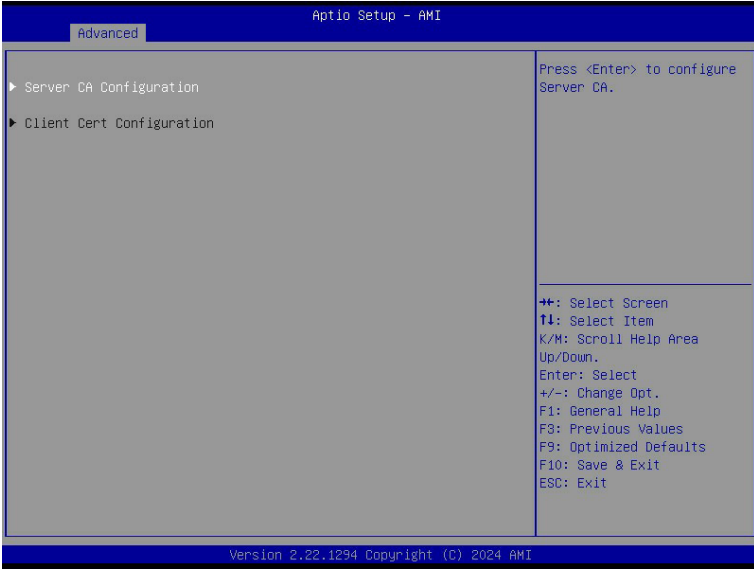
5-2-10 Chipset Configuration



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

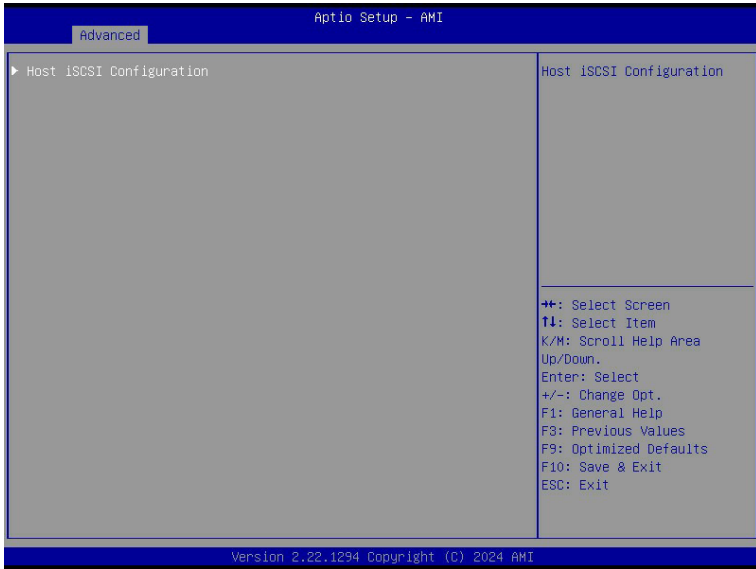
(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

5-2-11 Tls Auth Configuration



Parameter	Description
Server CA Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> ◆ 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.

5-2-12 iSCSI Configuration



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

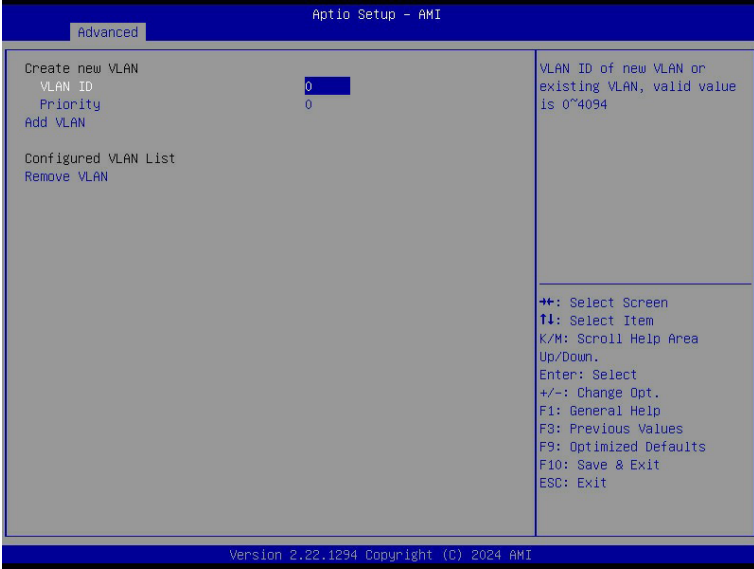
5-2-13 Intel(R) i350 Gigabit Network Connection

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

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

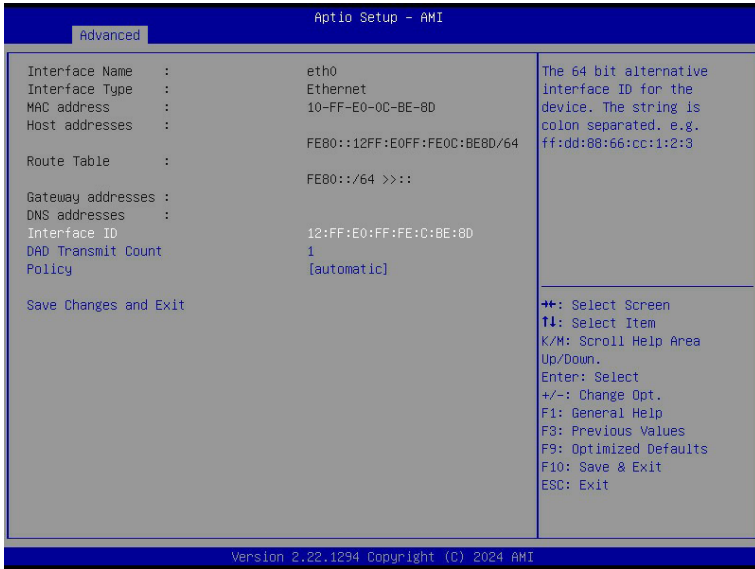
Parameter	Description
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Link Speed <ul style="list-style-type: none"> – Allows for automatic link speed adjustment. – Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100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

5-2-14 VLAN Configuration



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

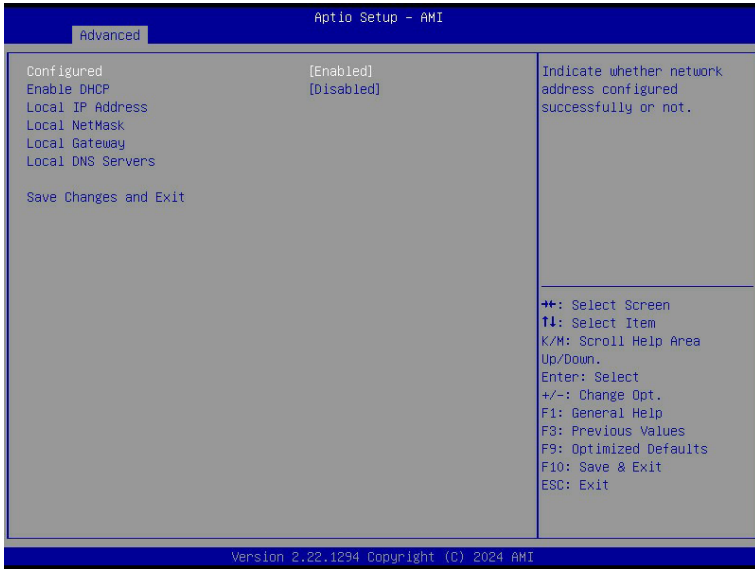
5-2-15 MAC IPv6 Network Configuration



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

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

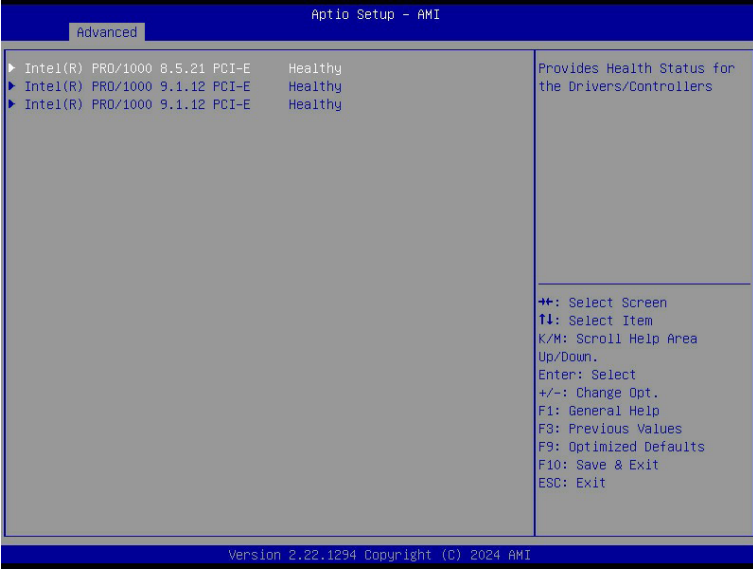
5-2-16 MAC IPv4 Network Configuration



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

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

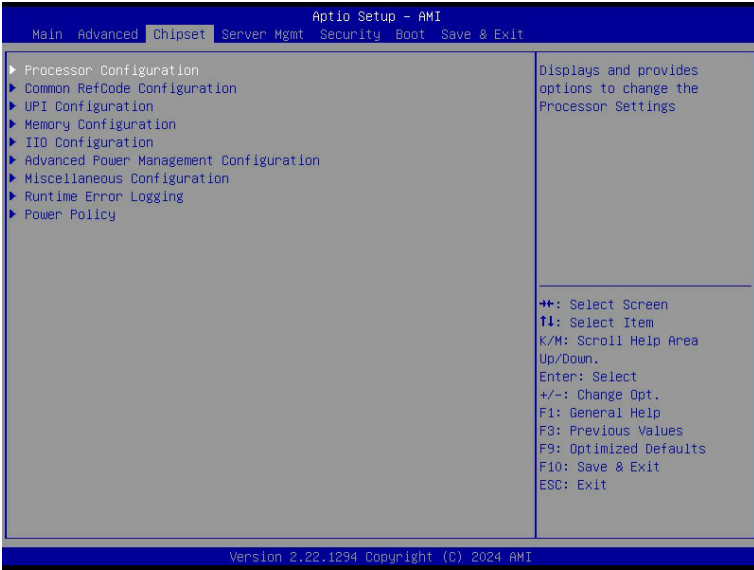
5-2-17 Driver Health



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

5-3 Chipset Menu

Chipset Setup menu displays submenu options for configuring the function of Platform Controller Hub(PCH). Select a submenu item, then press <Enter> to access the related submenu screen.



5-3-1 Processor Configuration

Aptio Setup - AMI

Chipset

Processor Configuration		Change Per-Socket Settings

▶ Per-Socket Configuration		
Processor Socket	Socket 0	Socket 1
Processor ID	000A06F3*	000A06F3
Processor Frequency	2.400GHz	2.400GHz
Processor Max Ratio	18H	18H
Processor Min Ratio	08H	08H
Microcode Revision	030001B3	030001B3
L1 Cache RAM(Per Core)	96KB	96KB
L2 Cache RAM(Per Package)	65536KB	65536KB
L3 Cache RAM(Per Package)	98304KB	98304KB
Processor 0 Version	Intel(R) Xeon(R) 6710E	
Processor 1 Version	Intel(R) Xeon(R) 6710E	

Hardware Prefetcher	[Enable]	
Adjacent Cache Prefetch	[Enable]	
DCU Streamer Prefetcher	[Auto]	
DCU IP Prefetcher	[Enable]	
L1 Next Page Prefetcher	[Enable]	
Enable Intel(R) TXT	[Disable]	
VMX	[Enable]	
Enable SMX	[Disable]	

++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit		

Version 2.22.1294 Copyright (C) 2024 AMI

Aptio Setup - AMI

Chipset

PRMRR Min Size per domain	2 MiB	
PRMRR Max Size per domain	64 GiB	

Processor Reserved Memory [Outputs]		

PRMRR Size per domain	16 MiB	
PRM Size per socket	16 MiB	
PRM Size per system	16 MiB	

Software Guard Extension (SGX) [Outputs]		

SGX activation state	Deactivated	
SGX memory population for SGX enabling is not PDR. Please check your memory population.		
SGX error code (HEX)	16	

Software Guard Extension (SGX) [Inputs]		

SGX Factory Reset	[Disabled]	
SW Guard Extensions (SGX)	[Disabled]	
SGX Package Info In-Band Access	[Disabled]	
SGX PRMRR Size Requested	[Auto]	

In Field Scan (IFS)		

++: Select Screen ↑↓: Select Item K/M: Scroll Help Area Up/Down. Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit		

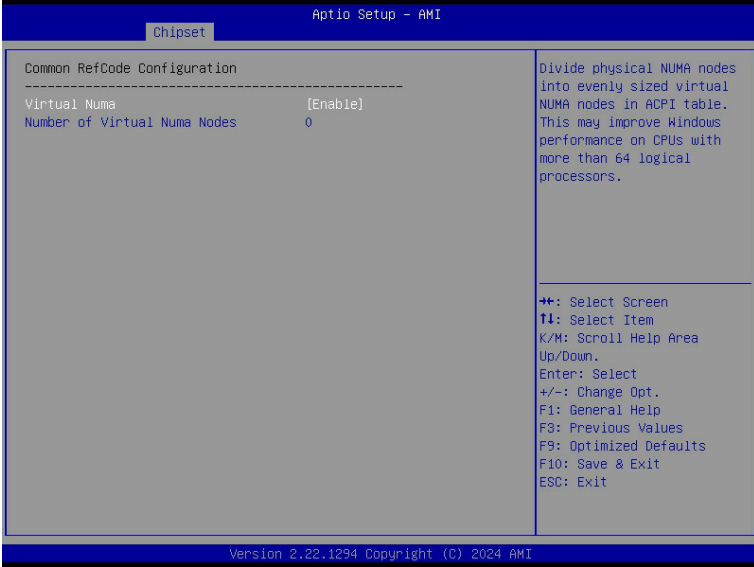
Version 2.22.1294 Copyright (C) 2024 AMI

Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ 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 Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Package) / L3 Cache RAM(Per Package) / Processor # Version	Displays the technical specifications for the installed processor(s).
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enable, Disable. Default setting is Enable .
L2 RF0 Prefetch Disable	Options available: Enable, Disable. Default setting is Disable .
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable, Disable. Default setting is Enable .
DCU Streamer Prefetcher	Enable/Disable DCU streamer prefetcher. Options available: Enable, Disable. Default setting is Enable .
DCU IP Prefetcher	Enable/Disable DCU IP Prefetcher. Options available: Enable, Disable. Default setting is Enable .
Enable Intel(R) TXT	Enable/Disable the Intel Trusted Execution Technology support function. Options available: Enable, Disable. Default setting is Disable .
VMX	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable, Disable. Default setting is Enable .
Enable SMX	Enable/Disable the Safer Mode Extensions (SMX) support function. Options available: Enable, Disable. Default setting is Disable .
AES-NI	Enable/Disable the AES-NI support. Options available: Enable, Disable. Default setting is Enable .
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 .

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

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

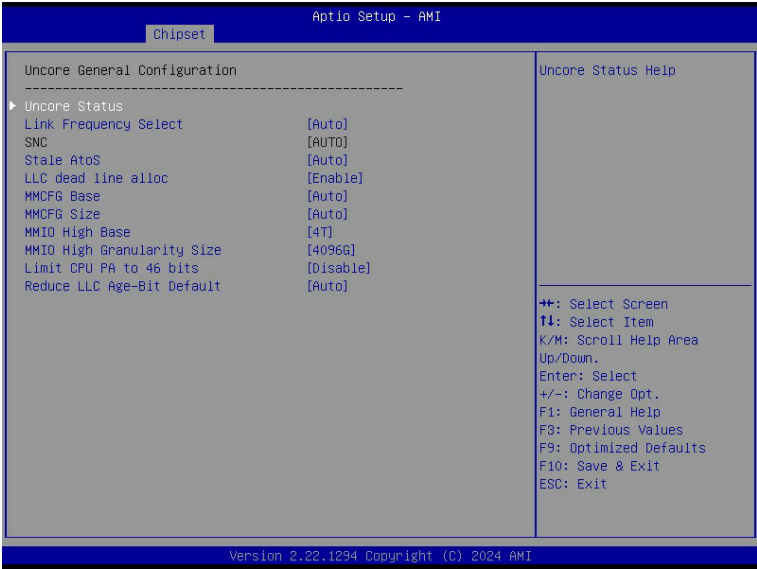
5-3-2 Common RefCode Configuration



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 .
Number of Virtual Numa Nodes ^(note)	The number of virtual NUMA nodes per physical NUMA nodes. 0 means automatically set the number of virtual NUMA nodes baes on system configuration. 1 equals disabling virtual NUMA.

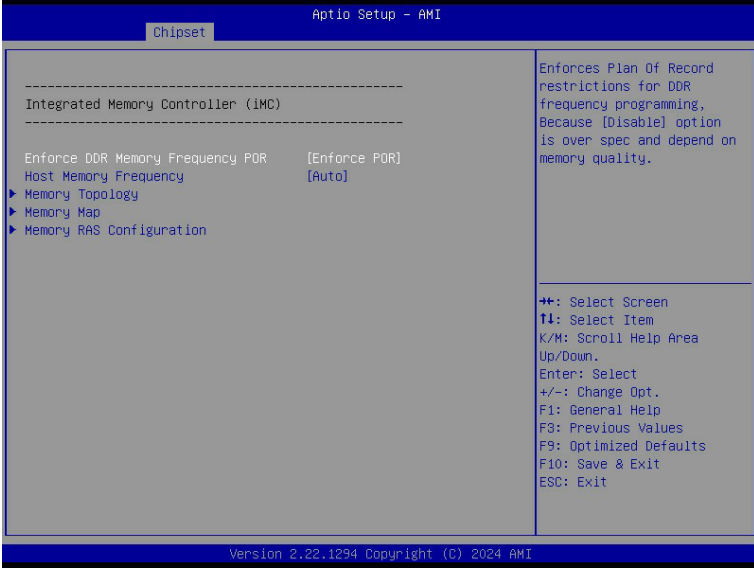
(Note) Advanced items prompt when this item is defined.

5-3-3 UPI Configuration



Parameter	Description
UPI General Configuration	<p data-bbox="348 142 682 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="348 170 719 224">◆ Uncore Status <ul style="list-style-type: none"> <li data-bbox="384 200 719 224">– Press [Enter] to view the Uncore status. <li data-bbox="348 228 650 341">◆ Link Frequency Select <ul style="list-style-type: none"> <li data-bbox="384 258 650 282">– Selects the UPI link frequency. <li data-bbox="384 286 954 341">– Options available: 12.8GT/s, 14.4GT/s, 16.0GT/s, Auto, Use Per Link Setting. Default setting is Auto. <li data-bbox="348 346 934 459">◆ SNC <ul style="list-style-type: none"> <li data-bbox="384 376 753 399">– Enable/Disable Sub NUMA Cluster function. <li data-bbox="384 404 934 459">– Options available: Auto, Disable, Enable SNC2 (2-clusters), Enable SNC4 (4-clusters). Default setting is Auto. <li data-bbox="348 464 912 548">◆ Stale AtoS <ul style="list-style-type: none"> <li data-bbox="384 493 801 517">– Enable/Disable Stale A to S directory optimization. <li data-bbox="384 522 912 548">– Options available: Disable, Enable, Auto. Default setting is Auto. <li data-bbox="348 553 932 638">◆ LLC dead line alloc <ul style="list-style-type: none"> <li data-bbox="384 583 695 606">– Enable/Disable fill dead lines in LLC. <li data-bbox="384 611 932 638">– Options available: Disable, Enable, Auto. Default setting is Enable. <li data-bbox="348 642 859 727">◆ MMCFG Base <ul style="list-style-type: none"> <li data-bbox="384 672 859 696">– Options available: 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, Auto. <li data-bbox="384 700 591 727">– Default setting is Auto. <li data-bbox="348 732 873 816">◆ MMCFG Size <ul style="list-style-type: none"> <li data-bbox="384 762 873 785">– Options available: 64M, 128M, 256M, 512M, 1G, 2G, Auto . <li data-bbox="384 790 591 816">– Default setting is Auto. <li data-bbox="348 821 954 906">◆ MMIO High Base <ul style="list-style-type: none"> <li data-bbox="384 851 954 906">– Options available: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T. Default setting is Auto. <li data-bbox="348 911 876 1014">◆ MMIO High Granularity Size <ul style="list-style-type: none"> <li data-bbox="384 939 876 962">– Selects the allocation size used to assign mmioh resources. <li data-bbox="384 967 954 1014">– Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is 64G. <li data-bbox="348 1019 937 1072">◆ Limit CPU PA to 46 bits <ul style="list-style-type: none"> <li data-bbox="384 1048 937 1072">– Options available: Disable, Enable, Auto. Default setting is Disable. <li data-bbox="348 1077 727 1161">◆ Reduce LLC Age-Bit Default <ul style="list-style-type: none"> <li data-bbox="384 1107 727 1130">– Options available: Disable, Enable, Auto. <li data-bbox="384 1135 700 1161">– 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 .
Host Memory Frequency	Maximum Host DDR Memory Frequency Selections in MT/s. If the AUTO option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. Options available: Auto, 4800, 5200, 5600, 6000, 6400. Default setting is Auto .

Parameter	Description
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel(R) Flat Memory Mode Support. <ul style="list-style-type: none"> – Options available: Enabled, Disabled. Default setting is Disabled. ◆ DDR CXL Heterogeneous Interleave support. <ul style="list-style-type: none"> – Options available: Enabled, Disabled. Default setting is Disabled.
Memory RAS Configuration	<p>Press [Enter] to configure advanced items.</p> <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. ◆ 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. ◆ 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. ◆ 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.

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

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

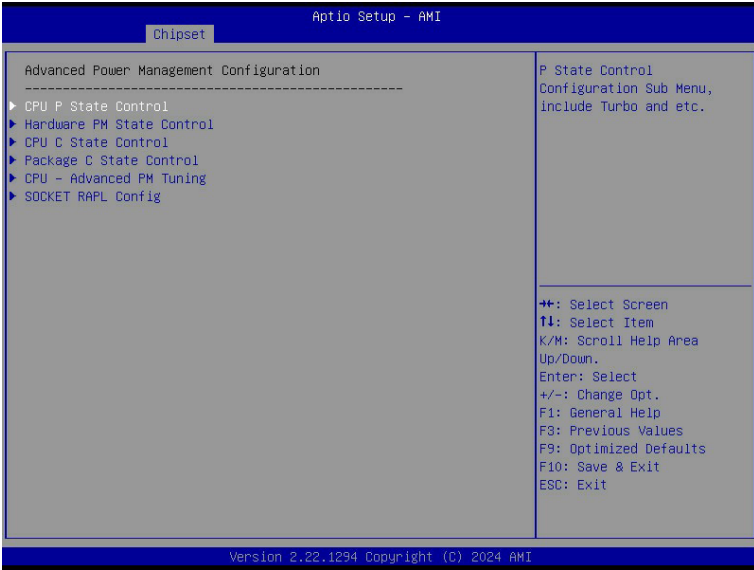
(Note) Advanced items prompt when this item is defined.

5-3-5 IIO Configuration



Parameter	Description
IIO Configuration	
Intel VMD Configuration	<p>Enable/Disable Intel VMD technology. Options available: Enable, Disable. Default setting is Disable.</p>
Intel VT for Directed I/O (VT-d)	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ 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). ◆ Pre-boot DMA Protection <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ PCIe ACSCTL <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ Cache Allocation <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable.
Global Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Max Read Request Size <ul style="list-style-type: none"> – Options available: Auto, 128B, 256B, 512B, 1024B, 2048B, 4096B. Default setting is Auto. ◆ Relaxed Ordering <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable.

5-3-6 Advanced Power Management Configuration

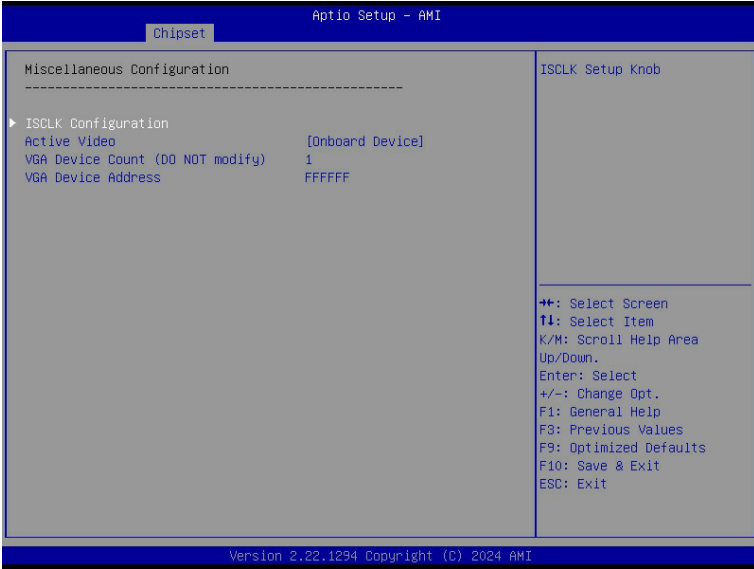


Parameter	Description
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel SST-PP <ul style="list-style-type: none"> – Intel SST-PP Select allows user to choose level. – Options available: Auto, Level 0, Level 1. Default setting is Auto. ◆ SpeedStep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

Parameter	Description
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Hardware P-State <ul style="list-style-type: none"> – Options available: Disable, Native mode, Out of Band mode, Native Mode with No Legacy Support. Default setting is Native Mode.
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Monitor MWAIT <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Enable. ◆ ACPI C1 Enumeration <ul style="list-style-type: none"> – Options available: C1, C1e . Default setting is C1e. ◆ ACPI C6x Enumeration <ul style="list-style-type: none"> – Options available: Dsiable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto . – Default setting is Auto.
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 Time Window <ul style="list-style-type: none"> • Default setting is 1. ◆ PL2 Power Limit <ul style="list-style-type: none"> – Press the <+> / <-> keys to increase or decrease the desired values. ◆ PL2 Time Window <ul style="list-style-type: none"> • Default setting is 1.

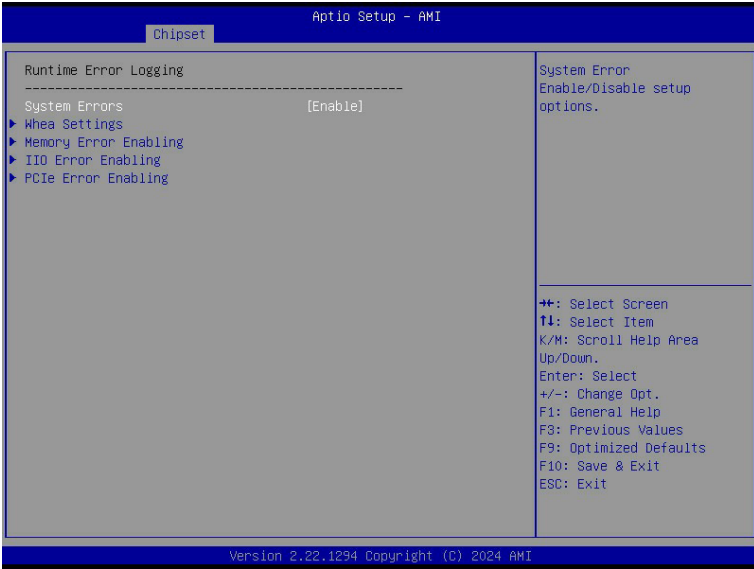
(Note) This item is configurable when **Power Performance Tuning** is set to **BIOS Controls EPB**.

5-3-7 Miscellaneous Configuration



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

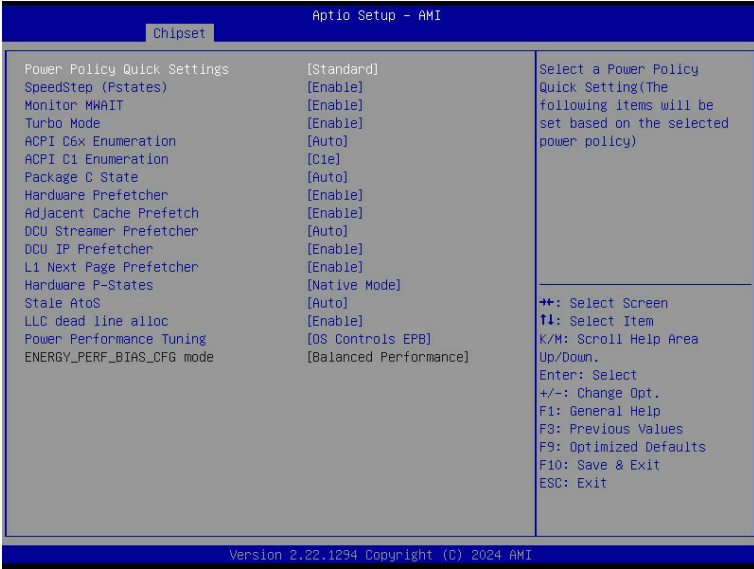
5-3-8 Runtime Error Logging Settings



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

Parameter	Description
PCIe Error Enabling	<p data-bbox="309 142 642 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="309 170 852 252">◆ Corrected Error <ul style="list-style-type: none"> <li data-bbox="344 200 795 224">– Enables and escalates correctable Errors to error pins. <li data-bbox="344 228 852 252">– Options available: Enable, Disable. Default setting is Disable. <li data-bbox="309 257 923 338">◆ Uncorrected Error <ul style="list-style-type: none"> <li data-bbox="344 286 923 310">– Enables and escalates Uncorrectable/Recoverable Errors to error pins. <li data-bbox="344 315 846 338">– Options available: Enable, Disable. Default setting is Enable. <li data-bbox="309 343 846 424">◆ Fatal Error Enable <ul style="list-style-type: none"> <li data-bbox="344 373 749 396">– Enables and escalates Fatal Errors to error pins. <li 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 <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 <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.

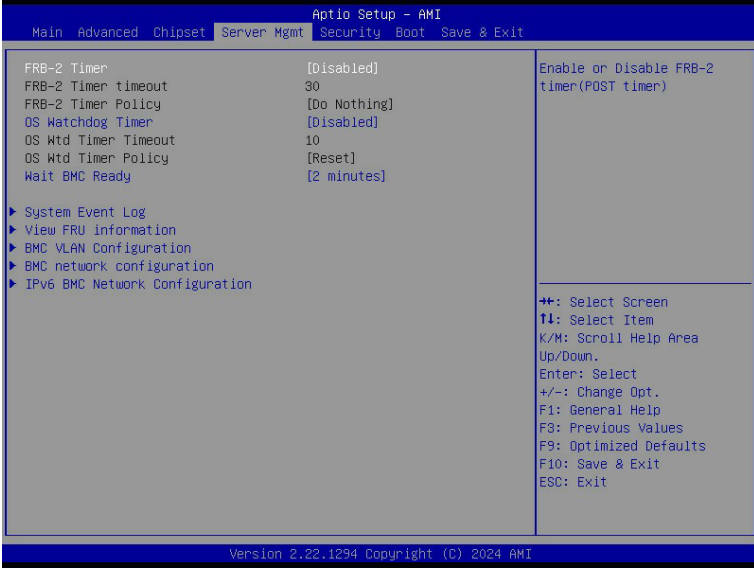
5-3-9 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient. Default setting is 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 .
Monitor MWAIT	Allows Monitor and MWAIT instructions. 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 .
ACPI C6x Enumeration	Options available: Disable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto. Default setting is Auto .
ACPI C1 Enumeration	Options available: C1, C1e. Default setting is C1e .
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
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 .
L1 Next page Prefetcher	Options available: Enable, Disable. Default setting is Enable .
Hardware P-States	Options available: Disable, Native mode, Out of Band mode, Native Mode with No Legacy Support. Default setting is Native Mode .
Stale AtoS	Options available: Auto, Enable, Disable. Default setting is Auto .
LLC dead line alloc	Options available: Auto, Enable, Disable. Default setting is Enable .
Power Performance Tuning	Options available: OS Controls EPB, BIOS Controls EPB, PECC Controls EPB. Default setting is BIOS Controls EPB .
ENERGY_PERF_BIAS_CFG mode	Performance, Balanced Performance, Balanced Power, Power. Default setting is Balanced Performance .

5-4 Server Management Menu



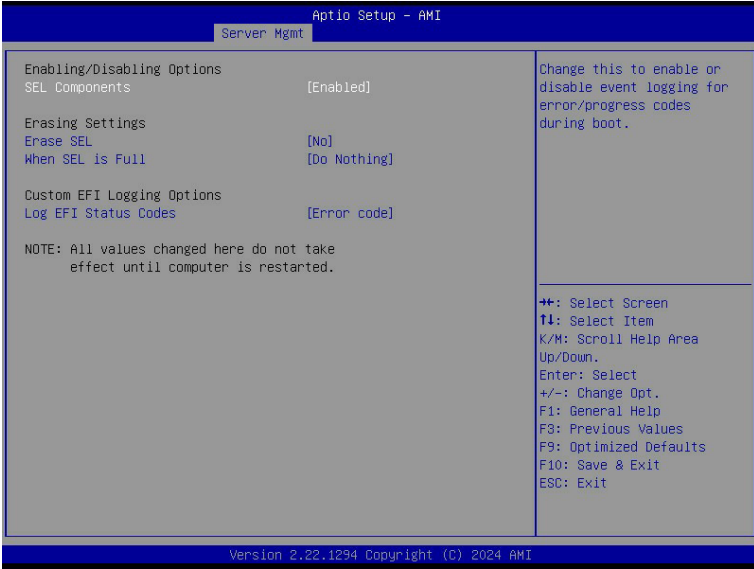
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is Enabled .
FRB-2 Timer ^(Note1) timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is 6 minutes .
FRB-2 Timer Policy ^(Note1)	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.

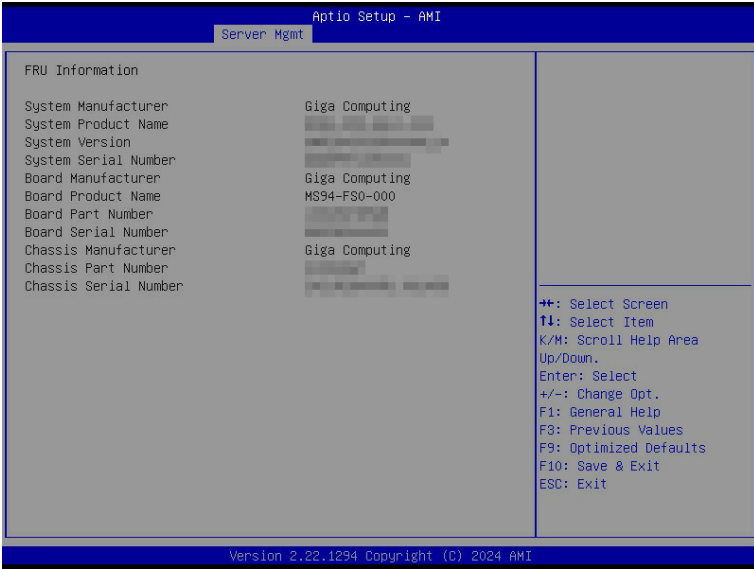
5-4-1 System Event Log



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



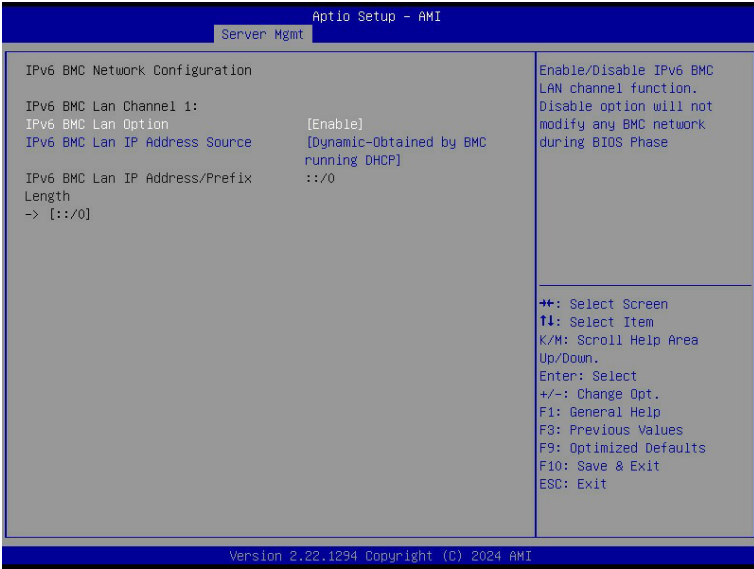
Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority 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.
Media Ssanitization	Press [Enter] to configure advanced items.
Secure Boot	Press [Enter] to configure advanced items.
Secure Flash Update	Press [Enter] to configure advanced items.

5-5-1 Secure Boot

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

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



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

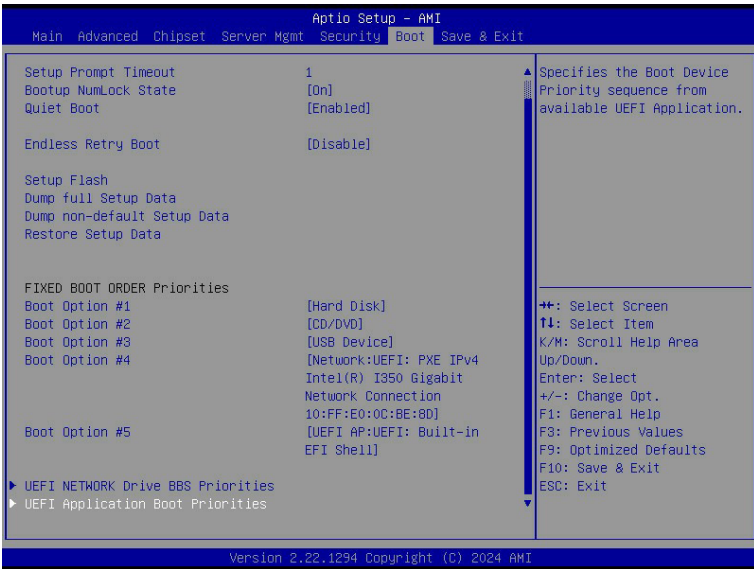
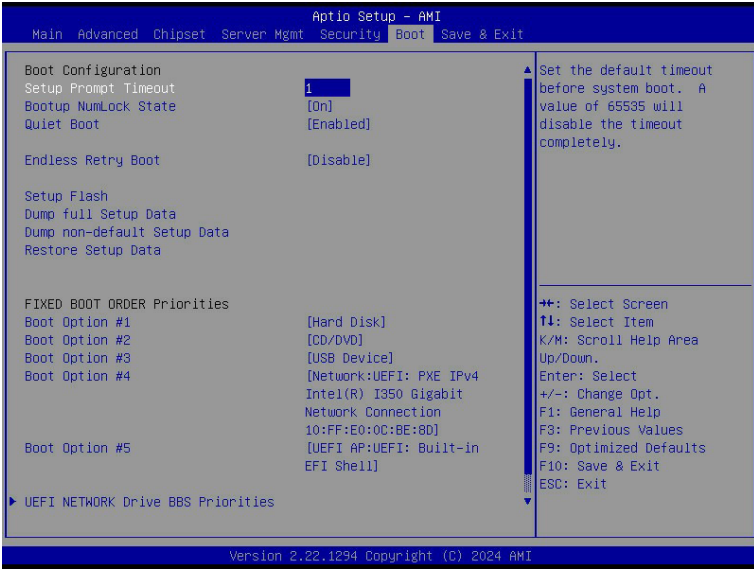
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235">Please note that this item is configurable when Secure Boot Mode is set to Custom.</p> <ul style="list-style-type: none"> <li data-bbox="335 243 941 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 941 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode. <li data-bbox="367 326 904 352">– Options available: Enabled, Disabled. Default setting is Disabled. <li data-bbox="335 357 925 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 925 404">– Installs all factory default keys. It will force the system in User Mode. <li data-bbox="367 409 606 431">– Options available: Yes, No. <li data-bbox="335 435 654 517">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode. <li data-bbox="367 487 606 509">– Options available: Yes, No. <li data-bbox="335 522 899 603">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 545 899 603">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). <li data-bbox="335 608 936 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 631 936 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device. <li data-bbox="335 686 893 744">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 893 744">– Displays the current status of the variables used for secure boot. <li data-bbox="335 749 803 854">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 773 803 796">– Displays the current status of the Platform Key (PK). <li data-bbox="367 801 675 823">– Press [Enter] to configure a new PK. <li data-bbox="367 827 601 854">– Options available: Update. <li data-bbox="335 859 941 995">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 882 941 906">– Displays the current status of the Key Exchange Key Database (KEK). <li data-bbox="367 911 904 964">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="367 969 670 995">– Options available: Update, Append. <li data-bbox="335 1000 941 1136">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1023 904 1047">– Displays the current status of the Authorized Signature Database. <li data-bbox="367 1052 941 1105">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="367 1110 670 1136">– Options available: Update, Append. <li data-bbox="335 1141 899 1277">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1165 899 1188">– Displays the current status of the Forbidden Signature Database. <li data-bbox="367 1193 893 1246">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="367 1251 670 1277">– 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

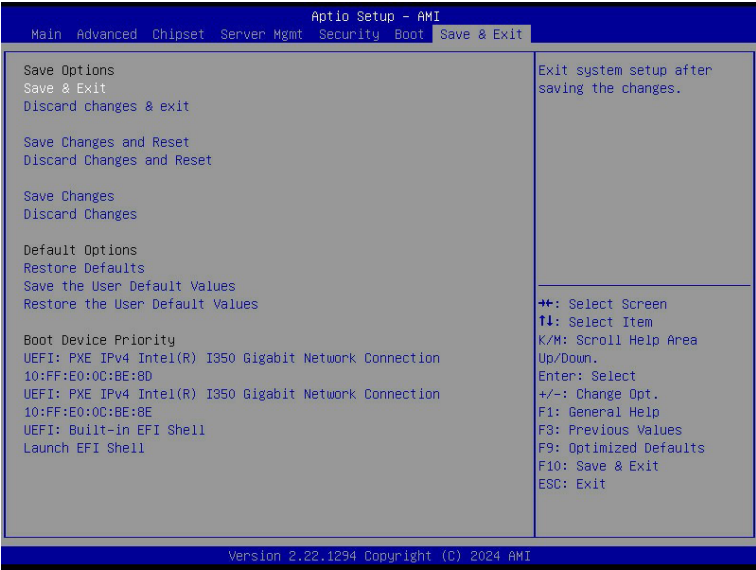
The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



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

5-7 Save & Exit Menu

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



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

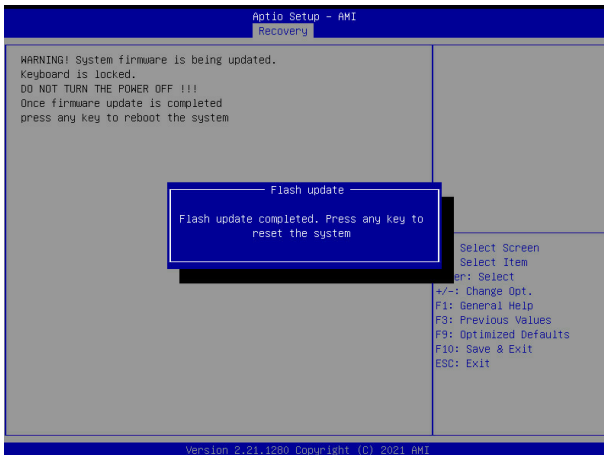
Parameter	Description
Restore Defaults	<p>Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system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

5-8 BIOS Recovery

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

Recovery Instruction:

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



5-9 BIOS POST Beep code (AMI standard)

5-9-1 PEI Beep Codes

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

5-9-2 DXE Beep Codes

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