

GIGABYTE™

G152-Z12

HPC Server - 1U UP Gen4 GPU Server

User Manual

Rev. 1.0

Copyright

© 2022 GIGA-BYTE 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 GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE 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>




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://esupport.gigabyte.com/> to create a new support ticket

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

Conventions

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

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

Server Warnings and Cautions

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



WARNING!

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

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



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



WARNING!

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



WARNING!

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



WARNING!

This equipment is intended to be used in Restrict Access Location. The access can only be gained by Skilled person.

Only authorized by well trained professional person can access the restrict access location.



CAUTION!

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

Electrostatic Discharge (ESD)



CAUTION!

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

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

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

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

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

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

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

**CAUTION!**

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

Table of Contents

Chapter 1	Hardware Installation	11
1-1	Installation Precautions	11
1-2	Product Specifications	12
1-3	System Block Diagram	15
Chapter 2	System Appearance	16
2-1	Front View	16
2-2	Rear View	17
2-3	Front Panel LEDs and Buttons	18
2-4	RoT LEDs	20
2-5	Front System LAN LEDs	22
2-6	Power Supply Unit LED	23
2-7	Hard Disk Drive LEDs	24
Chapter 3	System Hardware Installation	25
3-1	Removing Chassis Cover	26
3-2	Installing the CPU and Heat Sink	27
3-3	Installing the Memory	29
3-3-1	Eight Channel Memory Configuration	29
3-3-2	Installing a Memory	30
3-3-3	Processor and Memory Module Matrix Table	30
3-3-4	Memory Population Table	31
3-4	Installing the GPU Card	32
3-5	Installing the Hard Disk Drive	33
3-6	Installing the Mezzanine Card	35
3-7	Replacing the Power Supply	36
3-8	Cable Routing	37
Chapter 4	Motherboard Components	43
4-1	Motherboard Components	43
4-2	Jumper Setting	44
4-3	Backplane Board Storage Connector	45
4-3-1	System HDD Backplane Board (CBP2023)	45

Chapter 5 BIOS Setup46

- 5-1 The Main Menu 48
- 5-2 Advanced Menu 50
 - 5-2-1 Trusted Computing52
 - 5-2-2 PSP Firmware Versions.....53
 - 5-2-3 Legacy Video Select.....54
 - 5-2-4 AST2500 Super IO Configuration55
 - 5-2-5 S5 RTC Wake Settings.....58
 - 5-2-6 Serial Port Console Redirection59
 - 5-2-7 CPU Configuration.....63
 - 5-2-8 PCI Subsystem Settings.....64
 - 5-2-9 USB Configuration.....66
 - 5-2-10 Network Stack Configuration68
 - 5-2-11 NVMe Configuration69
 - 5-2-12 SATA Configuration.....70
 - 5-2-13 Graphic Output Configuration.....71
 - 5-2-14 AMD Mem Configuration Status72
 - 5-2-15 Tls Auth Configuration73
 - 5-2-16 iSCSI Configuration.....74
 - 5-2-17 Intel(R) Ethernet Controller X55075
 - 5-2-18 VLAN Configuration.....77
 - 5-2-19 MAC IPv4 Network Configuration78
 - 5-2-20 MAC IPv6 Network Configuration79
- 5-3 AMD CBS Menu 80
 - 5-3-1 CPU Common Options81
 - 5-3-2 DF Common Options.....87
 - 5-3-3 UMC Common Options92
 - 5-3-4 NBIO Common Options.....107
 - 5-3-5 FCH Common Options113
 - 5-3-6 SOC Miscellaneous Control117
 - 5-3-7 Workload Tuning.....118
- 5-4 AMD PBS Menu 119
 - 5-4-1 RAS120
- 5-5 Chipset Setup Menu..... 122
 - 5-5-1 North Bridge123
 - 5-5-2 Fabric Resource124
- 5-6 Server Management Menu..... 125
 - 5-6-1 System Event Log127
 - 5-6-2 View FRU Information128
 - 5-6-3 BMC Network Configuration.....129
 - 5-6-4 IPv6 BMC Network Configuration130

5-7	Security Menu	131
5-7-1	Secure Boot	132
5-8	Boot Menu.....	134
5-8-1	UEFI NETWORK Drive BBS Priorities	136
5-8-2	UEFI Application Boot Priorities	137
5-9	Save & Exit Menu.....	138
5-10	BIOS POST Beep code (AMI standard).....	139
5-10-1	PEI Beep Codes.....	139
5-10-2	DXE Beep Codes	139

This page intentionally left blank

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 ◆ 448 (W) x 44 (H) x 808(D) mm
	CPU	<ul style="list-style-type: none"> ◆ AMD EPYC™ 7003 series processor family ◆ Single processor, 7nm technology ◆ Up to 64-core, 128 threads per processor ◆ cTDP up to 280W <p style="margin-top: 10px;">Compatible with AMD EPYC™ 7002 series processor family</p>
	Chipset	◆ System on Chip
	Socket	◆ Socket SP3
	Memory	<ul style="list-style-type: none"> ◆ 8 x DIMM slots ◆ DDR4 memory supported only ◆ 8-Channel memory architecture ◆ RDIMM modules up to 128GB supported ◆ LRDIMM modules up to 128GB supported ◆ 3DS RDIMM/LRDIMM modules up to 256GB supported ◆ Memory speed: Up to 3200 MHz
	LAN	<ul style="list-style-type: none"> ◆ Add-on Card CFPG100 ◆ 2 x 10Gb/s BASE-T LAN ports (Intel® X550-AT2) ◆ NCSI supported ◆ 1 x 10/100/1000 management LAN
	Video	<ul style="list-style-type: none"> ◆ Integrated in Aspeed® AST2500 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
	Storage	<ul style="list-style-type: none"> ◆ 4 x 2.5" Gen4 NVMe internal HDD/SSD bays <p>NOTE: non-supported SATA devices</p>



Expansion Slot

2 x PCIe x16 slots (Gen4 x16) for 2 x double slot GPUs

Riser Card CRSG01G (Front Side):

- ◆ 1 x PCIe x16 slot (Gen4 x16), Low profile

Riser Card CRSH01E (Front Side):

- ◆ 1 x PCIe x16 slot (Gen4 x16), Low profile
- ◆ Support is not provided for mixed GPU populations



Internal I/O

- ◆ 1 x TPM header
- ◆ 1 x Front panel header



Front I/O

- ◆ 2 x USB 3.2 Gen1
- ◆ 1 x VGA
- ◆ 2 x RJ45
- ◆ 1 x MLAN
- ◆ 1 x ID LED
- ◆ 1 x Power button with LED
- ◆ 1 x ID button with LED
- ◆ 1 x Reset button
- ◆ 1 x NMI button
- ◆ 1 x System status LED
- ◆ 1 x HDD activity LED



Backplane I/O

- ◆ 2 x CBP2023: 4 x Gen4 NVMe ports
- ◆ Speed and bandwidth: PCIe Gen4 x4 per port



TPM

- ◆ 1 x TPM header with SPI interface
- ◆ Optional TPM2.0 kit: CTM010



Power Supply

- ◆ 2 x 2000W redundant PSU
- ◆ 80 PLUS Platinum

AC Input:

- ◆ 100-120V~/ 12A, 50-60Hz
- ◆ 180-240V~/ 10A, 50-60Hz

DC Input:

- ◆ 240Vdc/ 10A

DC Output:

- ◆ 1000W@100-120V, +12.2V/ 81.5A, +12Vsb/ 2.5A
- ◆ 1600W@180-199V, +12.2V/ 131A, +12Vsb/ 2.5A
- ◆ 1800W@200-220V, +12.2V/ 147.5A, +12Vsb/ 2.5A
- ◆ 2000W@221-240V, +12V/ 163.5A, +12Vsb/ 2.5A



System Management

- ◆ Aspeed® AST2500 management controller
- ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface

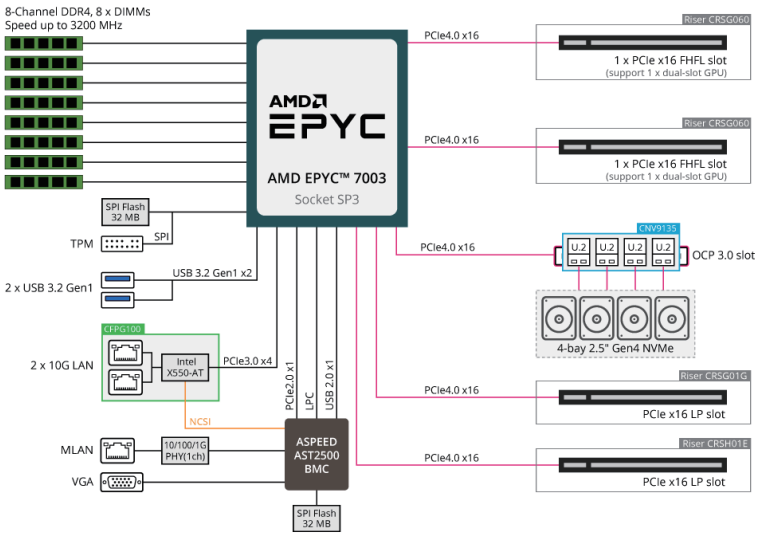
- ◆ Dashboard
- ◆ HTML5 KVM
- ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)
- ◆ Sensor Reading History Data
- ◆ FRU Information
- ◆ SEL Log in Linear Storage / Circular Storage Policy
- ◆ Hardware Inventory
- ◆ Fan Profile
- ◆ System Firewall
- ◆ Power Consumption
- ◆ Power Control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



Operating Properties

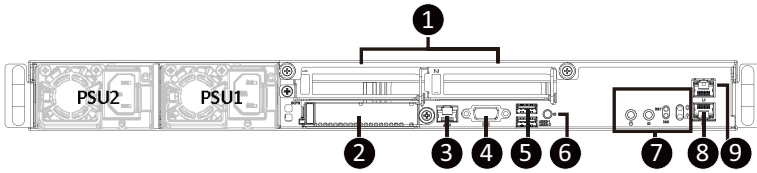
- ◆ Operating temperature: 10°C to 35°C
- ◆ Operating humidity: 8%-80% (non-condensing)
- ◆ Non-operating temperature: -40°C to 60°C
- ◆ Non-operating humidity: 20%-95% (non-condensing)

1-3 System Block Diagram



Chapter 2 System Appearance

2-1 Front View



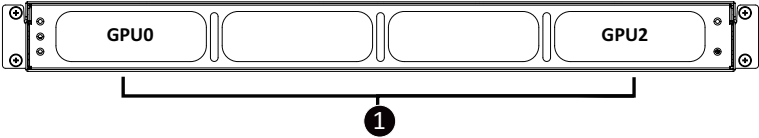
No.	Description
1.	PCIe Slots
2.	OCP 3.0 Slot (Option/SFF)
3.	Server Management LAN Port
4.	VGA Port
5.	USB 3.2 Gen1 Port x 2
6.	ID Button with LED
7.	Front Panel LEDs and Buttons
8.	10 GbE LAN #1
9.	10 GbE LAN #2



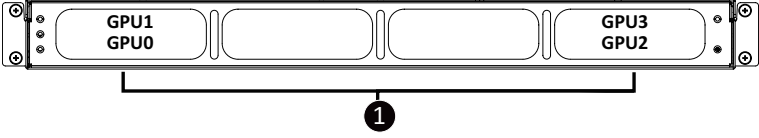
- Refer to section **2-3 Front Panel LEDs and Buttons** for a detailed description of the function of the LEDs.
- Refer to section **2-5 Front System LAN LEDs** for a detailed description of the function of the LEDs.

2-2 Rear View

2 GPU Configuration

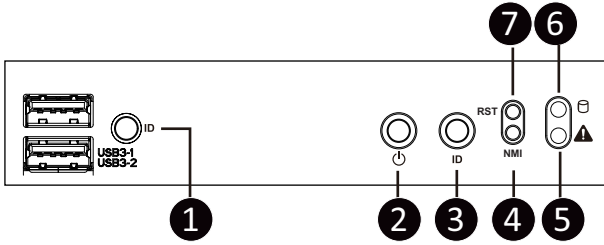


4 GPU Configuration



No.	Description
1.	GPU Card Slots

2-3 Front Panel LEDs and Buttons

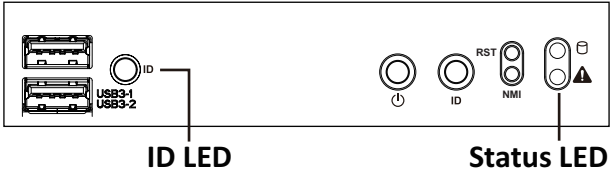


No.	Name	Color	Status	Description
1.	ID Button with LED ^(Note)	Blue	On	Indicates the system identification is active.
		N/A	Off	Indicates the system identification is disabled.
2.	Power button with LED	Green	On	Indicates the system is powered on.
		Green	Blink	System is in ACPI S1 state (sleep mode).
		N/A	Off	- System is not powered on or in ACPI S5 state (power off) - System is in ACPI S4 state (hibernate mode)
3.	ID Button with LED	Blue	On	Indicates the system identification is active.
		N/A	Off	Indicates the system identification is disabled.
4.	NMI button	--	--	Press this button for the server to generate a NMI to the processor. If multiple-bit ECC errors occur, the server will effectively be halted.
5.	System Status LED ^(Note)	Green	On	Indicates system is operating normally.
		Amber	On	Indicates a critical condition, may include: - System fan failure - System temperature
			Blink	Indicates non-critical condition, may include: - Redundant power module failure - Temperature and voltage issue - Chassis intrusion
		N/A	Off	Indicates system is not ready, may include: - POST error - NMI error - Processor or terminator is missing

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

6.	HDD Status LED	Green	On	Indicates locating the HDD.
			Blink	Indicates accessing the HDD.
		Amber	On	Indicates HDD error.
		Green/ Amber	Blink	Indicates HDD rebuilding.
		N/A	Off	Indicates no HDD access or no HDD error.
7.	Reset Button	--	--	Press this button to reset the system.

2-4 RoT LEDs



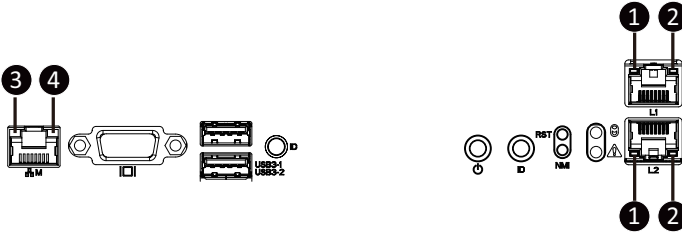
	LED on Front panel ^(Note5)	
	ID LED	Status LED
EC Firmware (FW) Authentication fail or not exit		
EC FW is broken or not exit ^(Note1)	OFF	OFF
Authenticating/Recovering BMC/BIOS Images		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per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

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

NOTE!

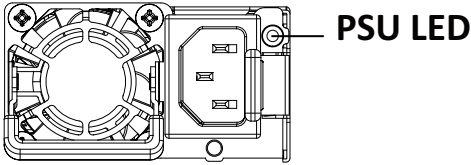
- EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
- (1) Authentication fail include below scenarios
Configuration table is missing or modified
Public key is missing or modified
Protected area or signature is modified
Flash empty
- if active flash is still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

2-5 Front System LAN LEDs



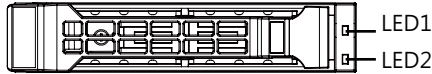
No.	Name	Color	Status	Description
1.	10GbE Speed LED	Green	On	10 Gbps data rate
		Yellow	On	1Gbps data rate
		N/A	Off	100 Mbps data rate
2.	10GbE Link / Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or reception is occurring.
		N/A	Off	No data transmission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

2-6 Power Supply Unit LED



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

2-7 Hard Disk Drive LEDs



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

LED #2	HDD Present	No HDD
Green	ON	OFF

NOTE:

*1: Depends on HBA/Utility Spec.

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

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

Chapter 3 System Hardware Installation



Pre-installation Instructions

Computer components and electronic circuit boards can be damaged 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

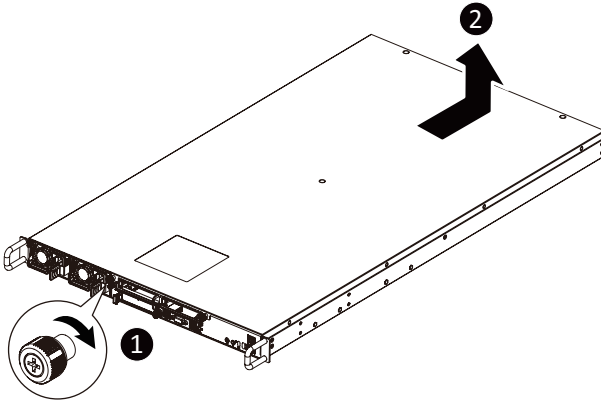


Before you remove or install the system cover

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

Follow these instructions to remove the rear system cover:

1. Loosen the thumbnail screw securing the chassis cover.
2. Slide the chassis cover to the rear of the system and then remove the cover in the direction of the arrow.
3. To reinstall the chassis cover reverse steps 1-3.



3-2 Installing the CPU and Heat Sink



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

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



WARNING!

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

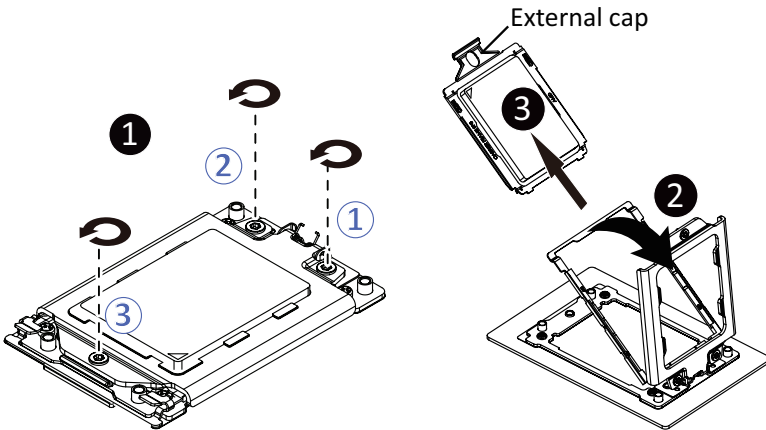
Follow these instructions to install the CPU:

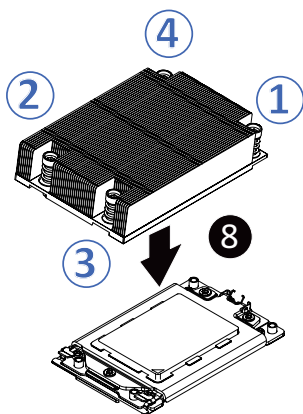
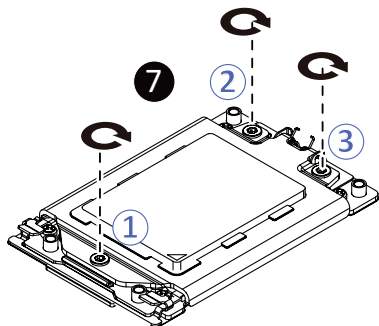
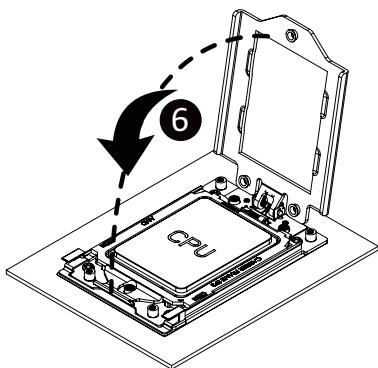
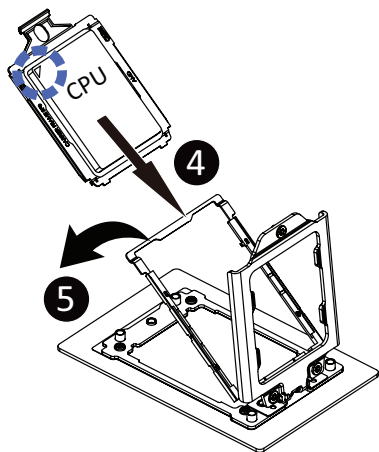
1. Align and install the processor on the carrier, making sure to line up the triangle markers on the corner of the CPU to the triangle mark on the corner of the CPU carrier.
2. Slide the carrier assembly into the channels of the carrier bracket.
3. Close the carrier bracket so that it firmly latches on to the CPU socket.
4. Close the CPU socket cover.
5. Tighten and secure the CPU socket cover screws in the following order (3→2→1).

NOTE: When removing the CPU socket cover, loosen the screws in reverse order (1→2→3).

NOTE: Apply thermal compound evenly on the top of the CPU. Remove the protective cover from the underside of the heat sink.

6. Align and place the heatsink onto the top of the CPU socket.
7. To secure the heatsink, tighten the four screws to the CPU socket.
8. Repeat steps 1-7 for the second CPU and heatsink.
9. To remove the heatsinks and CPUs, follow steps 1-7 in reverse order.





- When installing the heat sink over the CPU, use T30-Lobe driver to tighten the 4 captive nuts in sequential order (1→2→3→4).
- The screw tightening torque: $8 \pm 0.5\text{kgf-cm}$

3-3 Installing the Memory

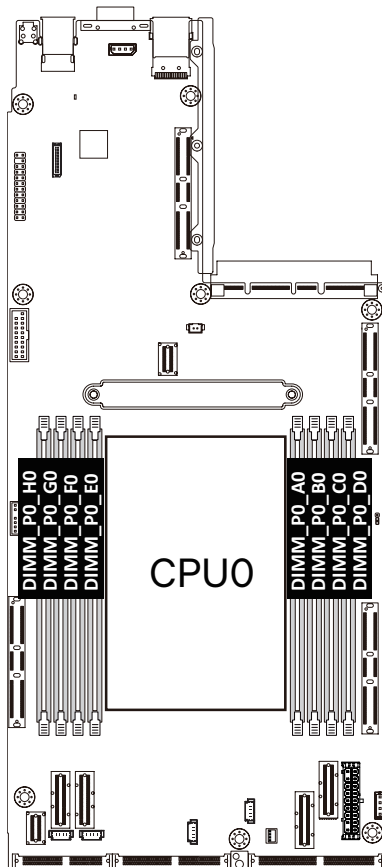


Read the following guidelines before you begin to install the memory:

- 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.

3-3-1 Eight Channel Memory Configuration

This motherboard provides 8 DDR4 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory. Enabling Four Channel memory mode will be four times of the original memory bandwidth.



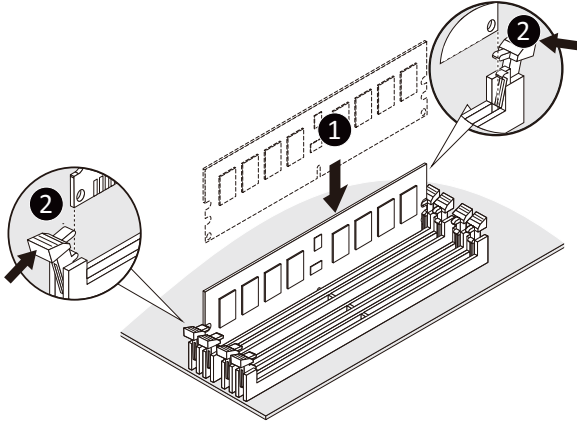
3-3-2 Installing a Memory



- 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 DDR4 DIMMs on this motherboard.
- Be sure all populated DIMMs have same capacity.

Follow these instructions to install the Memory:

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



3-3-3 Processor and Memory Module Matrix Table

Processor and Memory Module Matrix Table								
CPU	Channel A	Channel B	Channel C	Channel D	Channel E	Channel F	Channel G	Channel H
1 DIMM								
CPU0			✓					
2 DIMMs								
CPU0			✓	✓				
4 DIMMs								
CPU0			✓	✓			✓	✓
8 DIMMs								
CPU0	✓	✓	✓	✓	✓	✓	✓	✓

3-3-4 Memory Population Table



- When only one DIMM is used, it must be populated in memory slot DIMM1.

EPYC Memory Speed based on DIMM Population (One DIMM per Channel)

DIMM Type	DIMM Population	Max EPYC 7003 DDR Frequency (MHz)
	DIMM 0	
RDIMM	1R (1 Rank)	3200
	2R or 2DR (2 Ranks)	3200
LRDIMM	4DR (4 Ranks)	3200
	2S2R (4 Ranks)	3200
	2S4R (8 Ranks)	3200

3-4 Installing the GPU Card

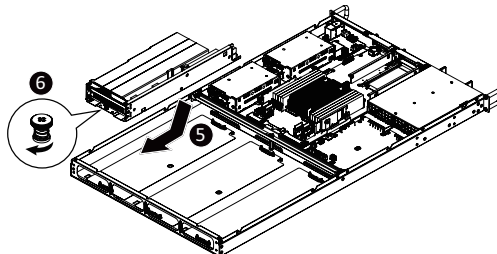
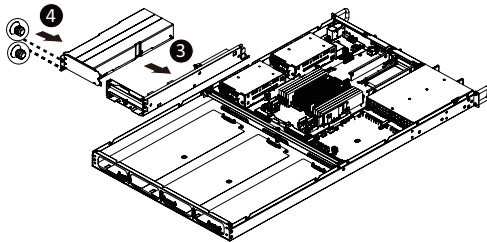
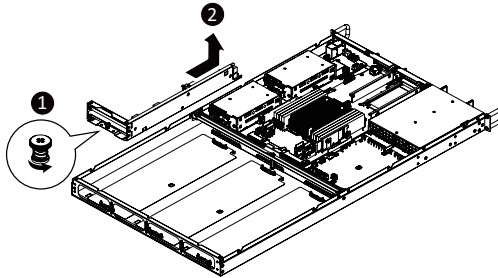


Before you install the GPU card:

- 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 GPU card. Make sure the system is not turned on or connected to AC power.
- Failure to observe these warnings could result in personal injury or damage to the equipment.

Follow these instructions to install the GPU card:

1. Loosen the thumbnail screw securing the riser bracket.
2. Lift up and remove the riser bracket.
3. Insert the GPU card into the selected slot. Make sure the GPU card is properly seated.
4. Install the two screws to secure the GPU card in place.
5. Slide the riser bracket to the system
6. Tighten the thumbnail screw to secure the riser bracket in place..



3-5 Installing the Hard Disk Drive

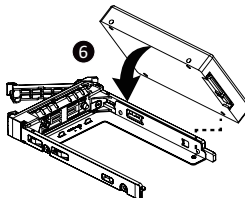
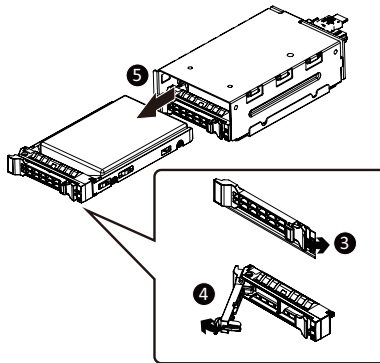
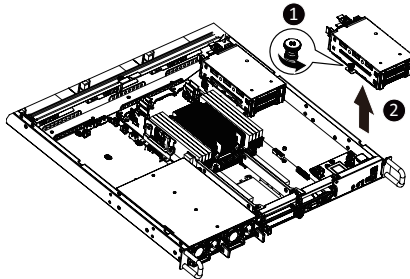


Read the following guidelines before you begin to install the Hard disk drive:

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

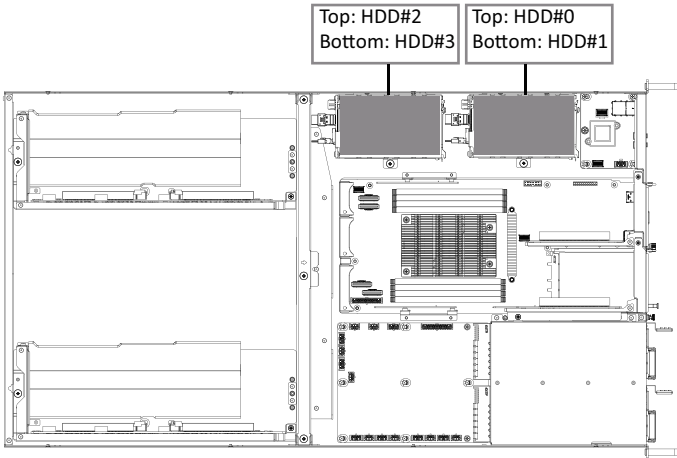
Follow these instructions to install a 2.5" hard disk drive:

1. Loosen the thumbnail screw securing the hard drive cage.
2. Lift up the hard drive cage and remove it from the system.
3. Extend the locking lever.
4. Pull the locking lever to remove the HDD tray.
5. Align the hard disk drive with the positioning stub on the HDD tray.
6. Slide hard disk drive into the blank HDD tray.
7. Reinsert the HDD tray into the slot and close the locking lever.





- Drives with green latches support NVMe.



3-6 Installing the Mezzanine Card

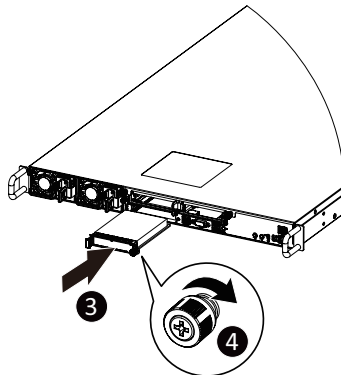
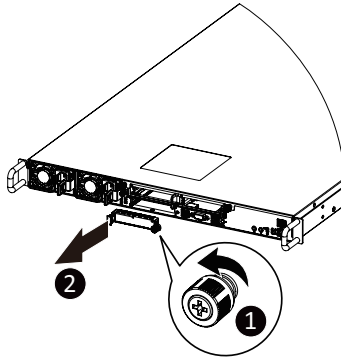


Use of the following type of OCP 3.0 NIC is recommended:

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

Follow these instructions to install an OCP 3.0 Mezzanine card:

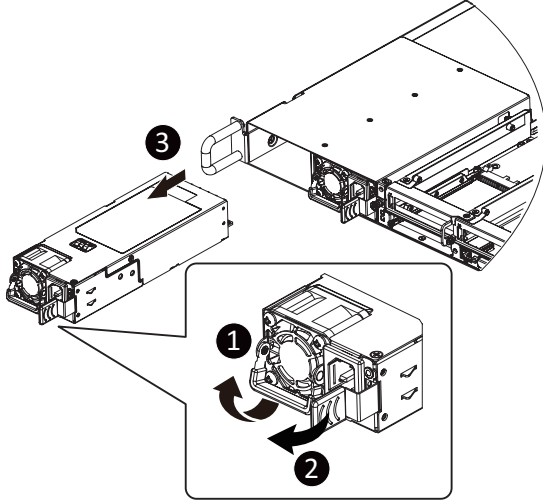
1. Loosen the thumbnail screw securing the OCP 3.0 card slot cover.
2. Remove the slot cover from the system.
3. Insert the OCP 3.0 card into the card slot ensuring that the card is firmly connected to the connector on the motherboard.
4. Tighten the thumbnail screw to secure the OCP 3.0 card in place.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



3-7 Replacing the Power Supply

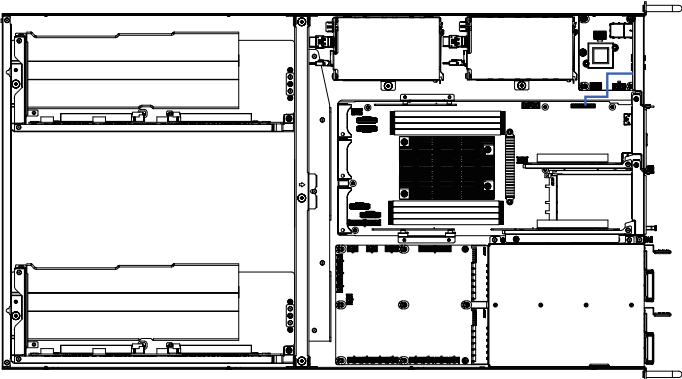
Follow these instructions to replace the power supply:

1. Flip up and then grasp the power supply handle.
2. Press the retaining clip on the left side of the power supply unit along the direction of the arrow.
3. Pull the power supply handle at the same time and pull out the power supply unit.
4. Insert the replacement power supply unit firmly into the chassis. Connect the AC power cord to the replacement power supply.
5. Repeat steps 1-4 for replacement of the second power supply.

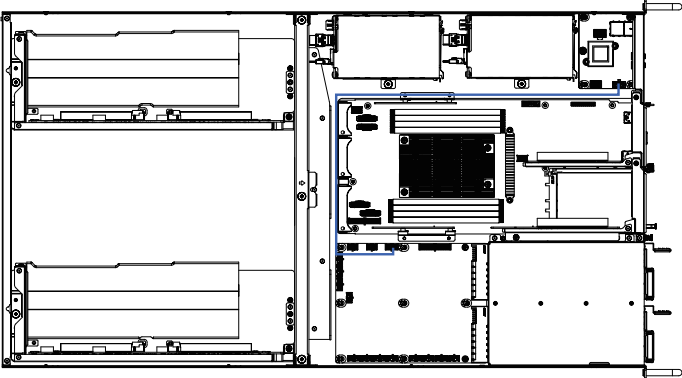


3-8 Cable Routing

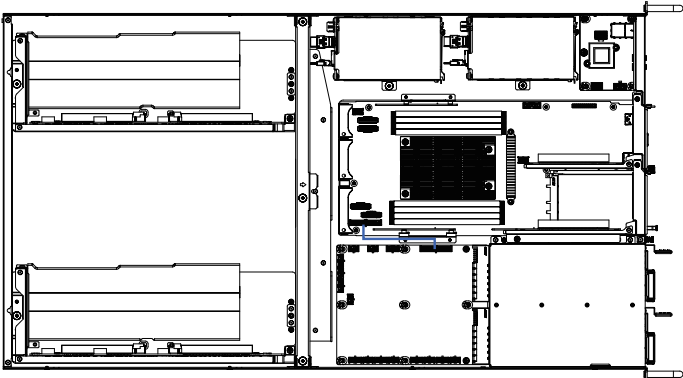
Front Panel LEDs and Buttons Cable



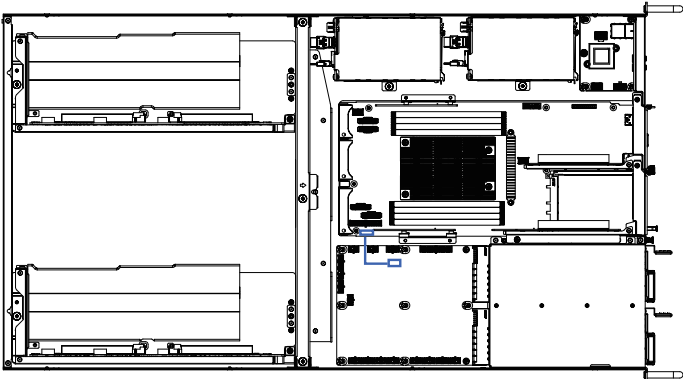
Front Panel Board Power Cable



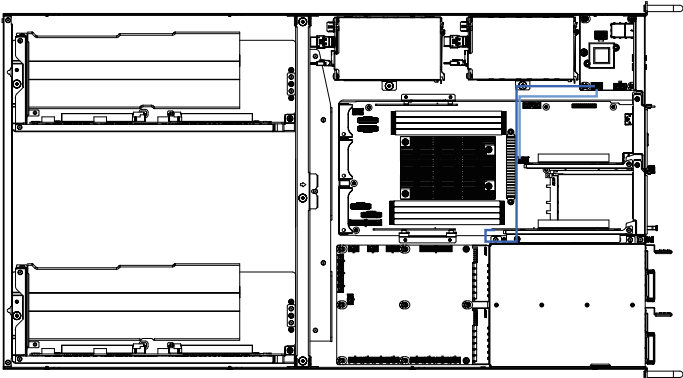
Motherboard Power Cable



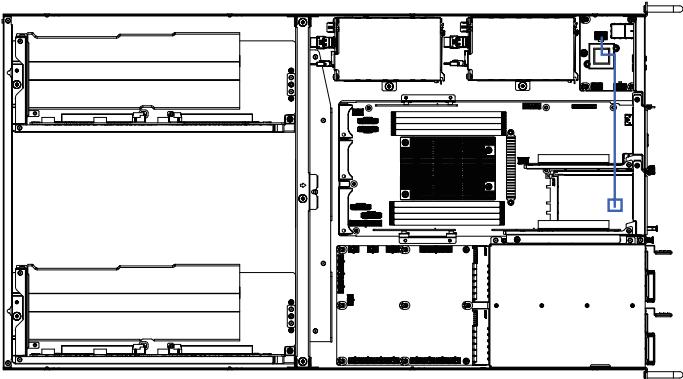
PMBus Cable



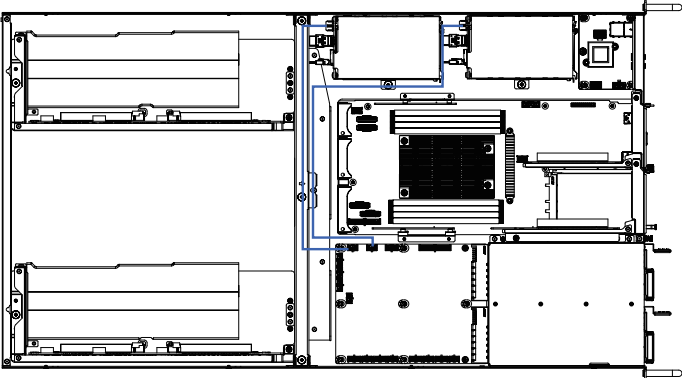
Management LAN Signal Cable



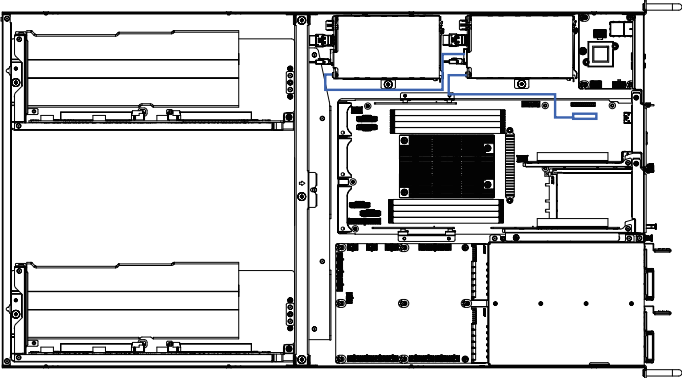
OCP 3 Signal Cable



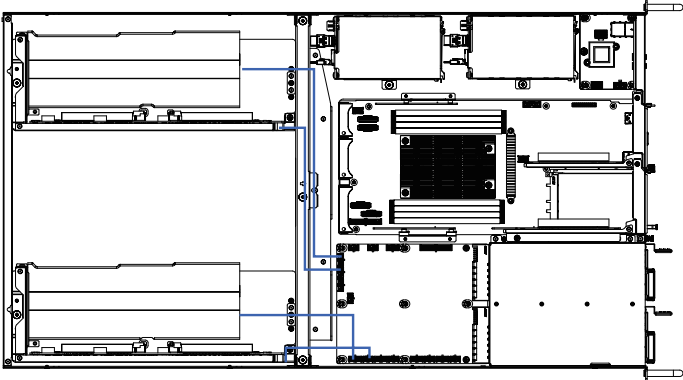
HDD Backplane Board Power Cable



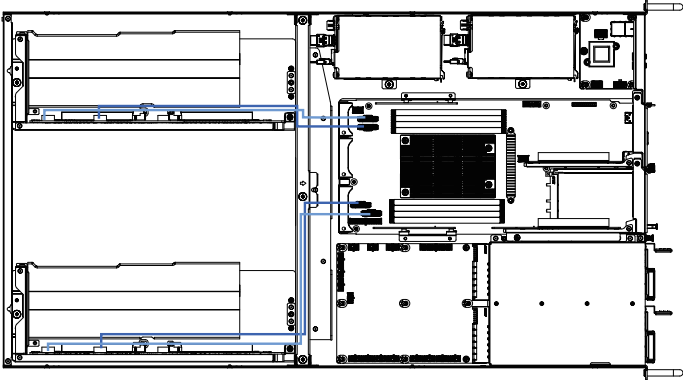
HDD Backplane Board Signal Cable



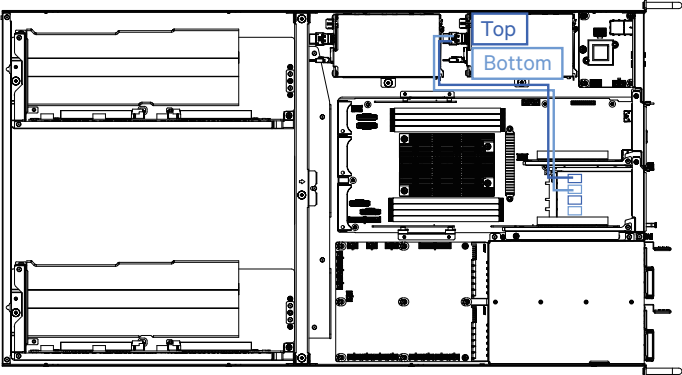
GPU Riser Card Power Cable



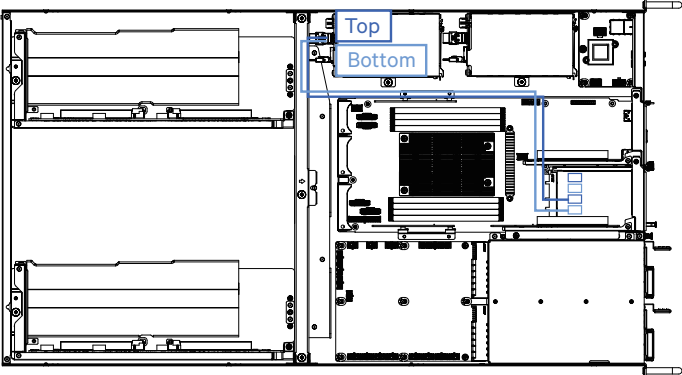
GPU Signal Cable



NVMe #1/#2 Cable

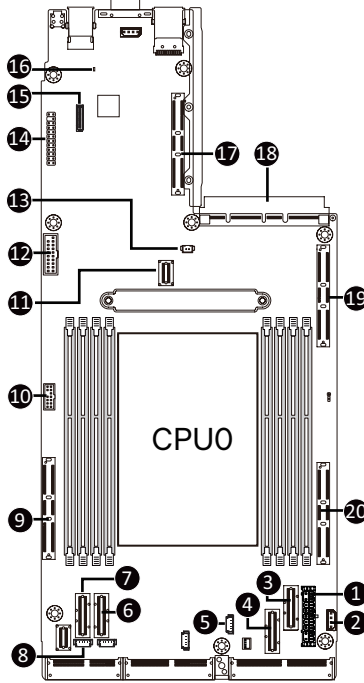


NVMe #3/#4 Cable



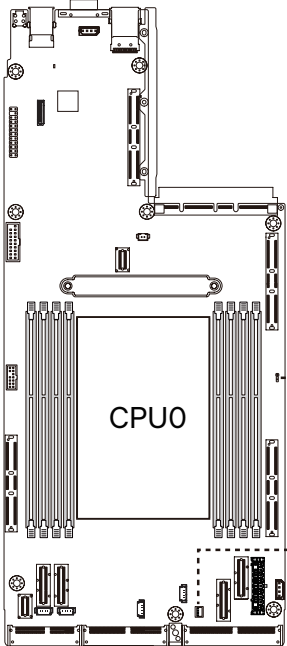
Chapter 4 Motherboard Components

4-1 Motherboard Components



Item	Description	Item	Description
1	2 x 12 Pin P12V GPU Power Connector	11	SlimLine SAS 4i Connector (SL_SATA0/PCIe Signal)
2	IPMB Connector	12	Front Panel USB 3.0 Connector
3	SlimLine SAS 8i Connector (U2_1B/PCIe Gen4)	13	System Battery Cable Connector
4	SlimLine SAS 8i Connector (U2_1A/PCIe Gen4)	14	Front Panel Header
5	SGPIO Connector (SGPIO2)	15	HDD Backplane Board Connector
6	SlimLine SAS 8i Connector (U2_2A/PCIe Gen4)	16	BMC Firmware Readiness LED
7	SlimLine SAS 8i Connector (U2_2B/PCIe Gen4)	17	Proprietary PCIe Slot (Gen 4/x16 slot/GENZ_2)
8	SGPIO Connector (SGPIO1)	18	OCP3 Slot
9	Proprietary PCIe Slot (Gen 4/x16 slot/GENZ_3)	19	Proprietary PCIe Slot (Gen 4/x16 slot/GENZ_1)
10	TPM Module Connector	20	Proprietary PCIe Slot (Gen 4/x16 slot/GENZ_4)

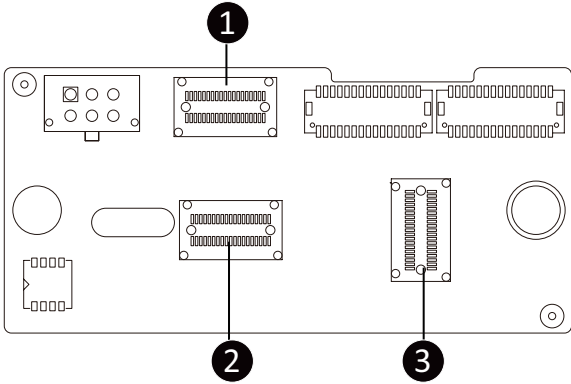
4-2 Jumper Setting



J1	ON	OFF
1	HOST_SMBUS_SEL BIOS Defined	
2	PMBUS_SEL BIOS Defined	
3	BIOS_PWD Clear supervisor password	Normal [Default]
4	BIOS_RCVR BIOS recovery mode	Normal [Default]

4-3 Backplane Board Storage Connector

4-3-1 System HDD Backplane Board (CBP2023)



Item	Description
1	SilmLine SAS Connector (U_2 0)
2	SilmLine SAS Connector (U_2 1)
3	SilmLine SAS Connector (SL_SAS0)

Chapter 5 BIOS Setup

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

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



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

BIOS Setup Program Function Keys

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

- **Main**

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

- **Advanced**

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

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

- **AMD CBS**

This setup page includes the common items for configuration of AMD motherboard-related information.

- **AMD PBS Option**

This setup page includes the common items for configuration of AMD CPM RAS related settings.

- **Chipset**

This setup page includes all the submenu options for configuring the functions of the North Bridge.

- **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.

BIOS Information

Project Name	M212-H07-D4
Project Version	M09b
Build Date and Time	08/31/2022 09:54:30
BMC Information	
BMC Firmware Version	12.60.23
Processor Information	
CPU 0 Brand String	AMD Eng Sample: 100-000000314-04_30/16_N
CPU Speed	1600 MHz
Processor Core	64 Cores 64 Threads
Microcode Patch	A001053
Total Memory	262144 MB
Memory Speed	3200 MT/s
VR Information	
Version	8260
AGESA PI Version	
PI Version	1.0.0.7

Version 2.21.1279 Copyright (C) 2022 AMI

Processor Information

CPU 0 Brand String	AMD Eng Sample: 100-000000314-04_30/16_N
CPU Speed	1600 MHz
Processor Core	64 Cores 64 Threads
Microcode Patch	A001053
Total Memory	262144 MB
Memory Speed	3200 MT/s
VR Information	
Version	8260
AGESA PI Version	
PI Version	1.0.0.7
Onboard LAN Information	
LAN1 MAC Address	D8-5E-D3-E0-3A-C4
LAN2 MAC Address	D8-5E-D3-E0-3A-C5
System Date	[Mon 10/10/2022]
System Time	[20:18:18]

Version 2.21.1279 Copyright (C) 2022 AMI

Function Keys:

- +/: Select Screen
- F1: Select Item
- Enter: Select
- +/-: Change Opt.
- F1: General Help
- F3: Previous Values
- F9: Optimized Defaults
- F10: Save & Exit
- ESC: Exit

Function Keys:

- +/: Select Screen
- F1: Select Item
- Enter: Select
- +/-: Change Opt.
- F1: General Help
- F3: Previous Values
- F9: Optimized Defaults
- F10: Save & Exit
- ESC: Exit

Item Help: Set the Time. Use Tab to switch between Time elements.

Parameter	Description
BIOS Information	
Project Name	Displays the project name information.
Project Version	Displays version number of the BIOS setup utility.
Build Date and Time	Displays the date and time when the BIOS setup utility was created.
BMC Information	
BMC Firmware Version	Displays BMC firmware version information.
CPU Speed / Processor Core / Microcode Patch	Displays the technical information for the installed processor(s).
Total Memory ^(Note2)	Displays the total memory size of the installed memory.
Memory Frequency ^(Note2)	Displays the frequency information of the installed memory.
VR Information Version	Displays VR version information.
AGESA PI Version PI Version	Displays AGESA PI version information.
Onboard LAN Information	
LAN1 MAC Address ^(Note1)	Displays LAN MAC address information.
LAN2 MAC Address ^(Note1)	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

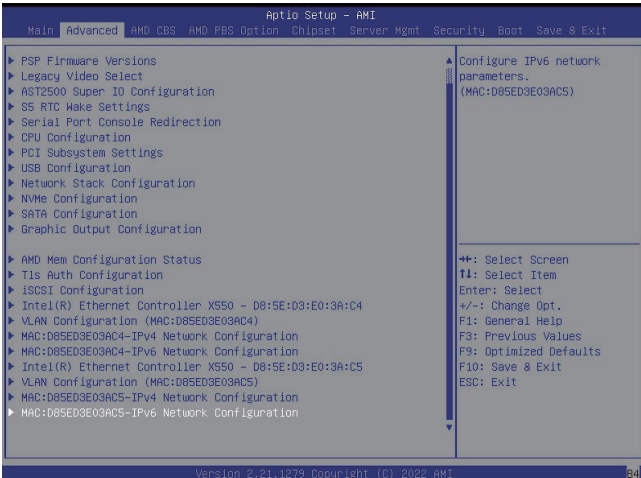
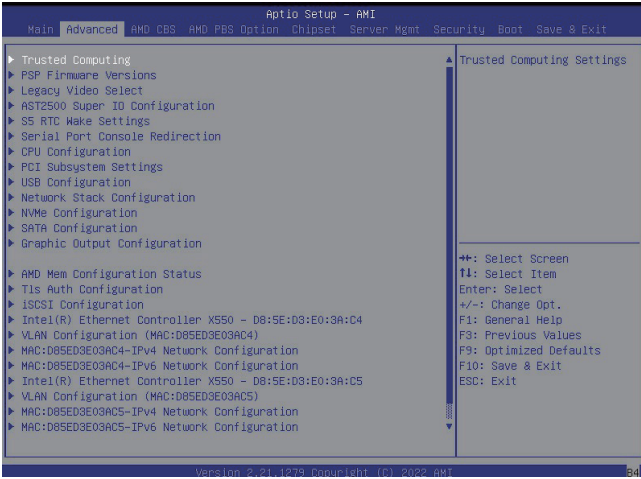
(Note1) The number of LAN ports listed will depend on the motherboard / system model.

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

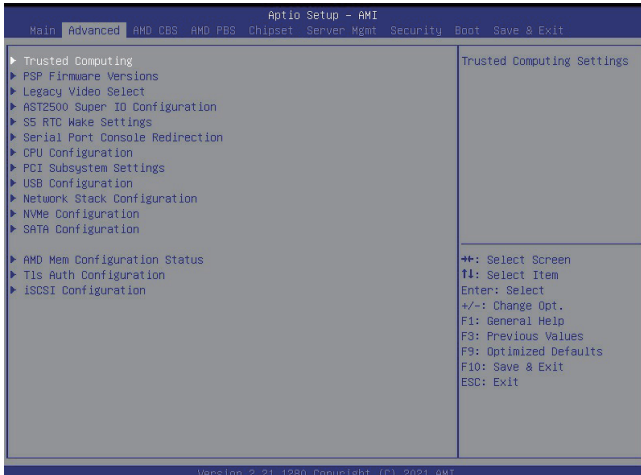
5-2 Advanced Menu

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.

When Boot Mode Select is set to UEFI (Default)



When "Boot Mode Select" is set to Legacy in the Boot > Boot Mode Select section



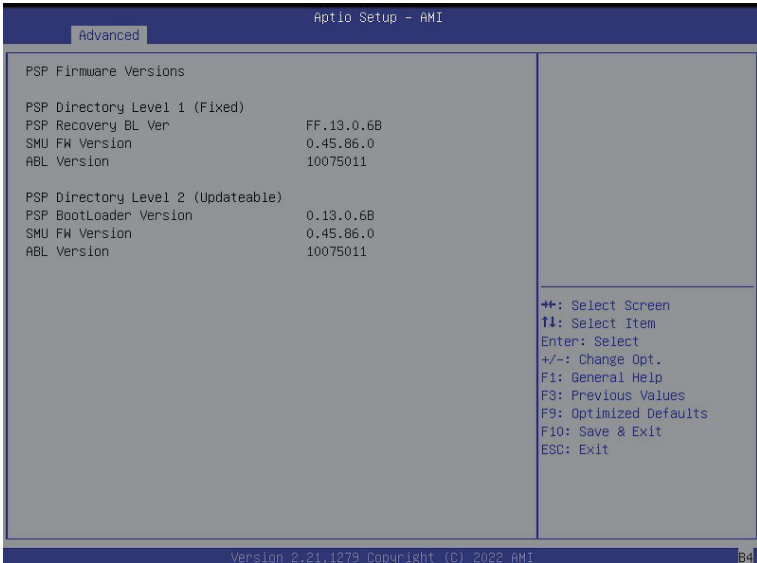
5-2-1 Trusted Computing



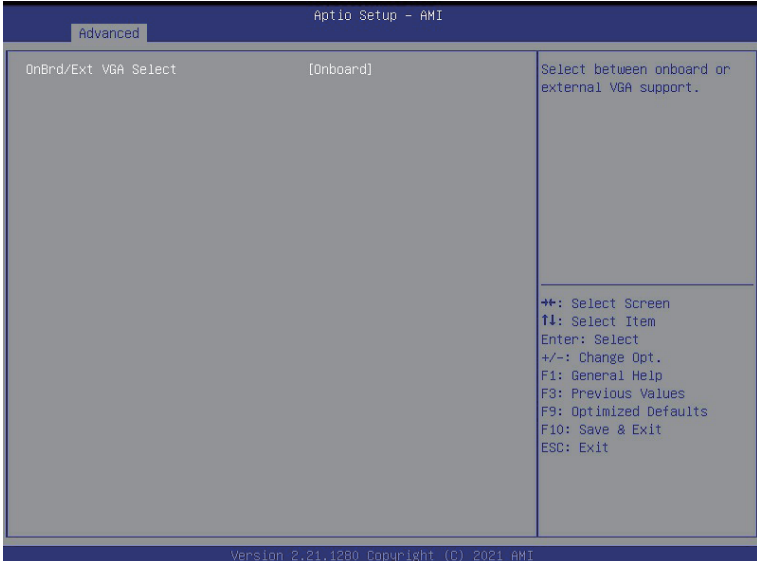
Parameter	Description
Configuration	
Security Device Support	Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. Options available: Enable/Disable. Default setting is Enable .
SPI TPM Support	Select Enable to activate TPM support feature. Options available: Enabled/Disabled. Default setting is Enabled .
Disable Block Sid	Override to allow SID authentication in TCG Storage device. Options available: Enabled/Disabled. Default setting is Disabled .

5-2-2 PSP Firmware Versions

The PSP Firmware Versions page displays the basic PSP firmware version information. Items on this window are non-configurable.



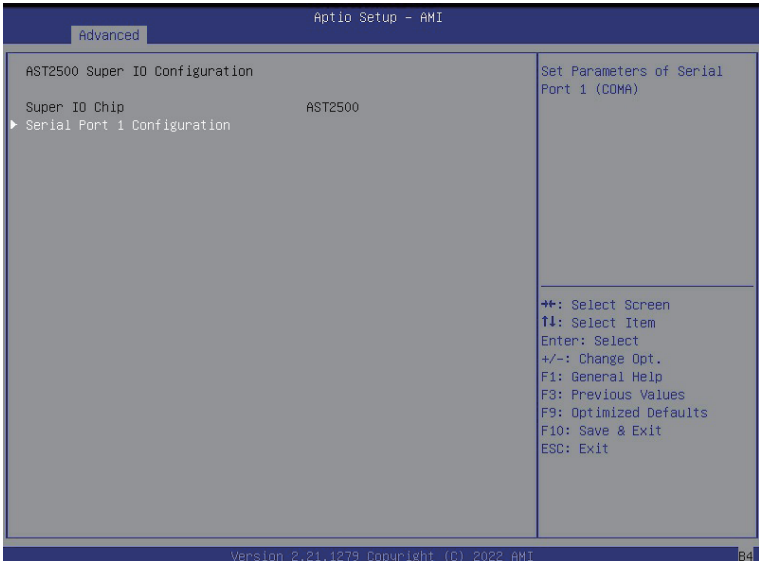
5-2-3 Legacy Video Select



Parameter	Description
OnBrd/Ext VGA Select ^(Note)	Selects between onboard or external VGA support. Options available: Auto, Onboard, External. Default setting is Onboard .

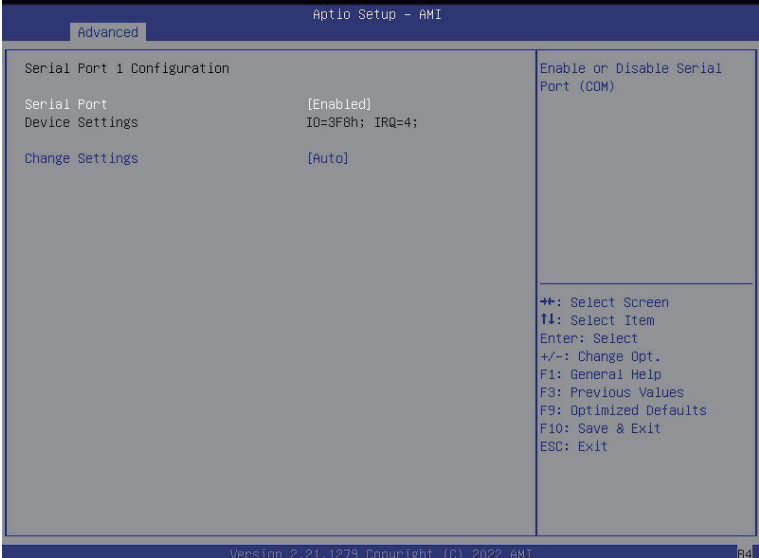
(Note) This configurable option will be displayed when "Boot Mode Select" is set to **Legacy** in the Boot > Boot Mode Select section.

5-2-4 AST2500 Super IO Configuration



Parameter	Description
AST2500 Super IO Configuration	
Super IO Chip	Displays the super IO chip information
Serial Port 1 Configuration	Press [Enter] for configuration of advanced items.

5-2-4-1 Serial Port 1 Configuration



Parameter	Description
Serial Port 1 Configuration	
Serial Port ^(Note1)	Enable/Disable the Serial Port (COM). When set to Enabled allows you to configure the Serial port 1/2 settings. When set to Disabled, displays no configuration for the serial port. Options available: Enabled/Disabled. Default setting is Enabled .
Devices Settings ^(Note2)	Displays the Serial Port 1/2 device settings.
Change Settings ^(Note2)	Select an optimal settings for Super IO Device. Options available for Serial Port 1: Auto IO=3F8h; IRQ=4; IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; Default setting is Auto . Options available for Serial Port 2: Auto IO=2F8h; IRQ=3; IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12; Default setting is Auto . Please note that this item is configurable when Serial Port is set to Enabled.

(Note1) Advanced items prompt when this item is defined.

(Note2) This item appears when **Serial Port** is set to **Enabled**.

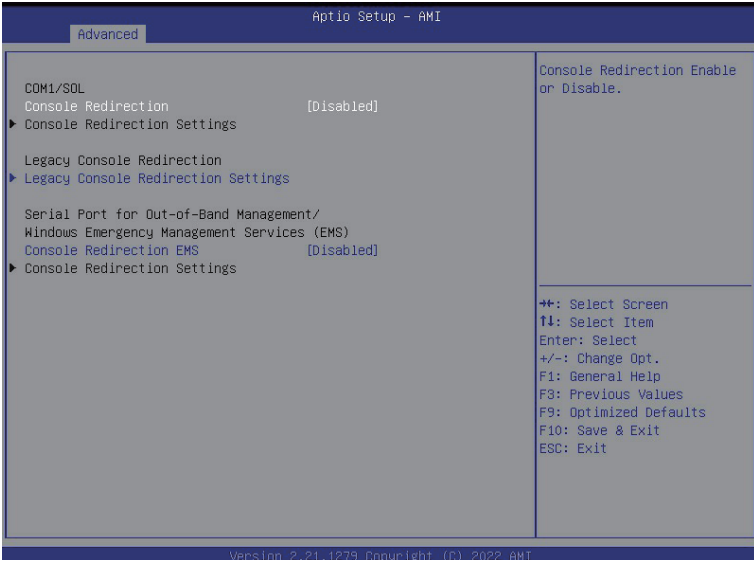
5-2-5 S5 RTC Wake Settings



Parameter	Description
Wake System from S5 ^(Note1)	<p>Enable/Disable system wake on alarm event.</p> <p>Options available: Disabled/Fixed Time. When Fixed Time enabled, system will wake on the hr::min::sec specified.</p> <p>Default setting is Disabled.</p>

(Note1) Advanced items prompt when this item is defined.

5-2-6 Serial Port Console Redirection



Parameter	Description
COM1 Serial Over LAN ^(Note)	<p>Select whether to enable console redirection for specified device. 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 Serial Over LAN Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p>Please note that this item is configurable when COM1/Serial Over LAN & COM2 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, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ 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/Serial Over LAN 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^(Note) <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^(Note) <ul style="list-style-type: none"> – Enable/Disable extended terminal resolution. – Options available: Enabled/Disabled. Default setting is Enabled. ◆ Putty KeyPad^(Note) <ul style="list-style-type: none"> – Selects FunctionKey and LeyPad on Putty. – Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is VT100.

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

Parameter	Description
Legacy Console Redirection	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Redirection COM Port <ul style="list-style-type: none"> – Selects a COM port for Legacy serial redirection. – Options available: COM1/Serial Over LAN, COM2. Default setting is COM1/Serial Over LAN. ◆ Resolution <ul style="list-style-type: none"> – Selects the number of rows and columns used in Console Redirection for legacy OS support. – Options available: 80x24, 80x25. Default setting is 80x24. ◆ Redirect After POST <ul style="list-style-type: none"> – When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. – Options available: Always Enable, BootLoader. Default setting is Always Enable.
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. – Options available: COM1/Serial Over LAN, COM2. Default setting is COM1/Serial Over LAN. ◆ Terminal Type <ul style="list-style-type: none"> – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ 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.

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

Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	<ul style="list-style-type: none">◆ 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, Software Xon/Xoff. Default setting is None.

5-2-7 CPU Configuration



Parameter	Description
SVM Mode	Enable/Disable the CPU Virtualization. Options available: Enabled/Disabled. Default setting is Enabled .
CPU 0 Information	Press [Enter] to view more information related to CPU0.

5-2-8 PCI Subsystem Settings

Advanced Aptio Setup - AMI

PCI Bus Driver Version	A5.01.24	▲ Change GEN2_1 PCIe lanes.
GEN2_1 Lanes	[Auto]	
GEN2_1 I/O ROM	[Enabled]	
GEN2_1 Max Link Speed	[Auto]	
GEN2_2 Lanes	[Auto]	
GEN2_2 ROM	[Enabled]	
GEN2_2 Max Link Speed	[Auto]	
ODP3_1 Lanes	[x4 x4 x4 x4]	
ODP3_1 I/O ROM	[Enabled]	
ODP3_1 Max Link Speed	[Auto]	
GEN2_4 Lanes	[Auto]	
GEN2_4 I/O ROM	[Enabled]	
GEN2_4 Max Link Speed	[Auto]	
U2_1 Lanes	[Auto]	
U2_1 I/O ROM	[Enabled]	
U2_1 Max Link Speed	[Auto]	
GEN2_3 Lanes	[Auto]	
GEN2_3 I/O ROM	[Enabled]	
GEN2_3 Max Link Speed	[Auto]	

▲+: Select Screen
 ▼: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F8: Previous Values
 F9: Optimized Defaults
 F10: Save & Exit
 ESC: Exit

Version 2.21.1279 Copyright (C) 2022 AMI

Advanced Aptio Setup - AMI

GEN2_4 Lanes	[Auto]	▲ If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.
GEN2_4 I/O ROM	[Enabled]	
GEN2_4 Max Link Speed	[Auto]	
U2_1 Lanes	[Auto]	
U2_1 I/O ROM	[Enabled]	
U2_1 Max Link Speed	[Auto]	
GEN2_3 Lanes	[Auto]	
GEN2_3 I/O ROM	[Enabled]	
GEN2_3 Max Link Speed	[Auto]	
U2_2 Lanes	[Auto]	
U2_2 I/O ROM	[Enabled]	
U2_2 Max Link Speed	[Auto]	
Onboard LAN Controller	[Enabled]	
Onboard LAN1 I/O ROM	[Enabled]	
Onboard LAN2 I/O ROM	[Enabled]	
PCI Devices Common Settings:		
Above 4G Decoding	[Enabled]	
SR-IOV Support	[Enabled]	

▲+: Select Screen
 ▼: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F8: Previous Values
 F9: Optimized Defaults
 F10: Save & Exit
 ESC: Exit

Version 2.21.1279 Copyright (C) 2022 AMI

Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
GENZ_# ^(Note1) Lanes Configuration U2_# ^(Note1) Lanes Configuration OCP 3 Lanes Configuration	Change the PCIe/U2/OCP3 lanes. Options available: Disabled, Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting for PCIe/U2 is Auto . Default setting for OCP3 is x4x4x4x4 .
GEN_# I/O ROM ^(Note1) U2_# I/O ROM ^(Note1) OCP3 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 .
GEN_# Link Speed ^(Note1) U2_# Max Link Speed ^(Note1) OCP3 Max Link Speed ^(Note1)	Configure mezzanine PCIe max link speed. Options available: Auto/Maximum/Gen1/Gen2/Gen3/Gen4. Default setting is Auto .
Onboard LAN Controller ^(Note2)	Enable/Disable the onboard LAN devices. Options available: Enabled/Disabled. Default setting is Enabled .
Onboard LAN I/O ROM ^(Note2)	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available: Enabled/Disabled. Default setting is Enabled .
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled/Disabled. Default setting is Enabled .
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/U2 Connector/OCP 3 Slot.

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

5-2-9 USB Configuration



Parameter	Description
USB Configuration	
USB Module Version	Displays the USB version.
USB Controllers	Displays the supported USB controllers.
USB Devices	Displays the USB devices connected to the system.
Legacy USB Support	Enable/disable the Legacy USB support function. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. Options available: Auto/Enabled/Disabled. Default setting is Enabled .
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 .
USB hardware delays and time-outs	
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers. Options available: 1 sec/5 sec/10 sec/20 sec. Default setting is 20 sec .
USB reset time-out	Options available: 1 sec/5 sec/10 sec/20 sec. Default setting is 20 sec .

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

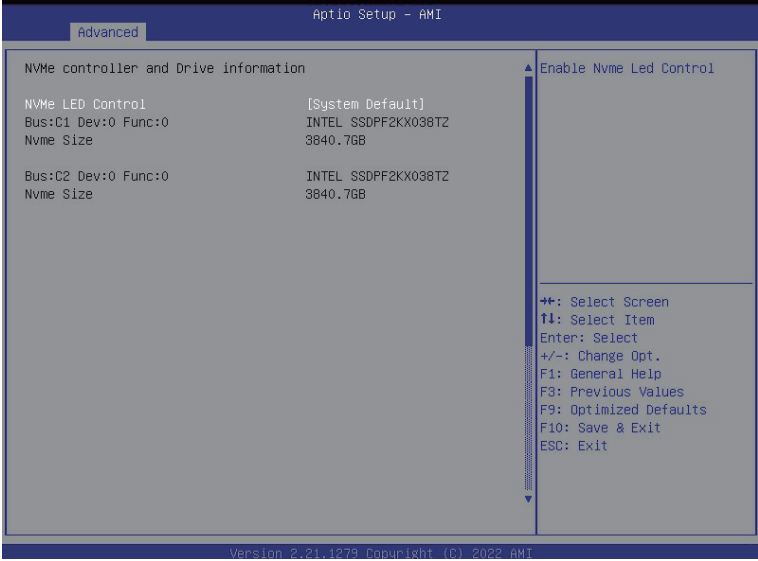
Parameter	Description
Device power-up delay	<p>Maximum time the device will take before it properly reports itself to the Host Controller. "Auto" uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.</p> <p>Options available: Auto/Manual. Default setting is Auto.</p>
<hr/> Mass Storage Devices <hr/>	
AMI Virtual CDROM/HDisk_#	<p>Mass storage device emulation type. AUTO enumerates devices according to their media format. Optical drives are emulated as CDROM, drives with no media will be emulated according to a drive type.</p> <p>Options available: Auto/Floppy/Forced FDD/Hard Disk/CD-ROM. Default setting is Auto.</p>

5-2-10 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 Enabled .
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.

5-2-11 NVMe Configuration



Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.
NVMe LED Control	Options available: System Default/Enabled/Disabled. Default setting is System Default .

5-2-12 SATA Configuration



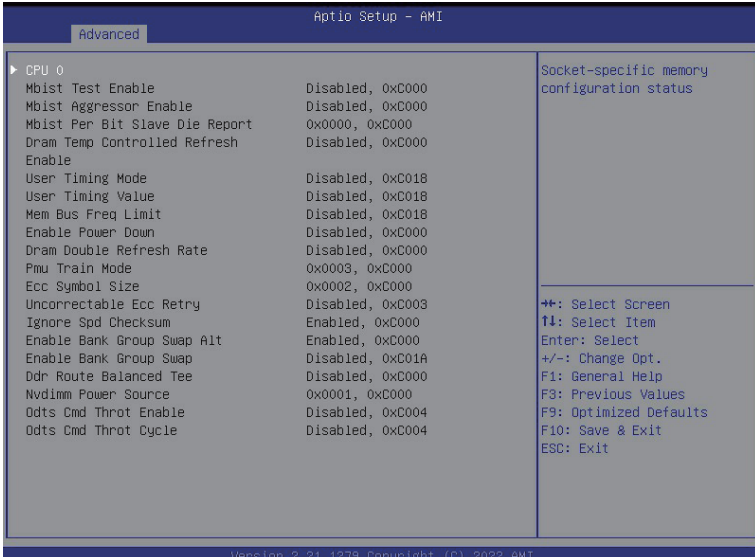
Parameter	Description
SATA Configuration	Displays the installed HDD devices information. System will automatically detect HDD type.

5-2-13 Graphic Output Configuration



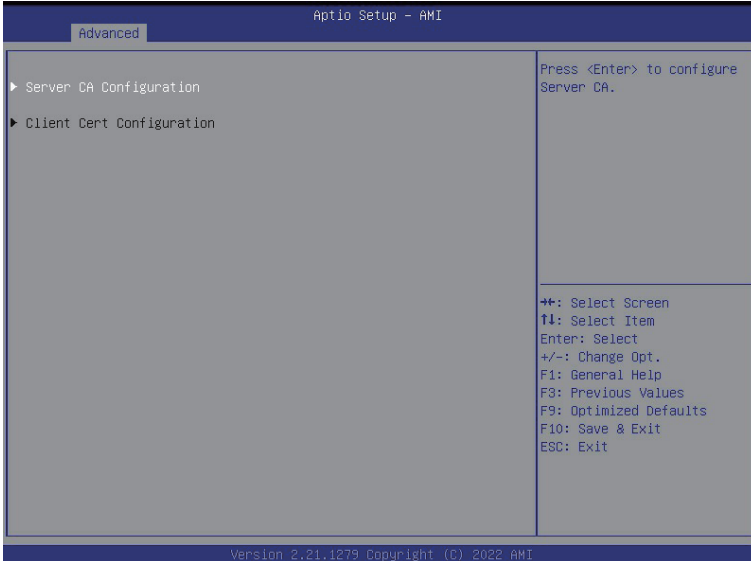
Parameter	Description
Graphic Output Configuration	
Output Device Type	Select output device. Options available: First loaded Device, Onboard Device, External Device, Specific Device. Default setting is Onboard Device .

5-2-14 AMD Mem Configuration Status



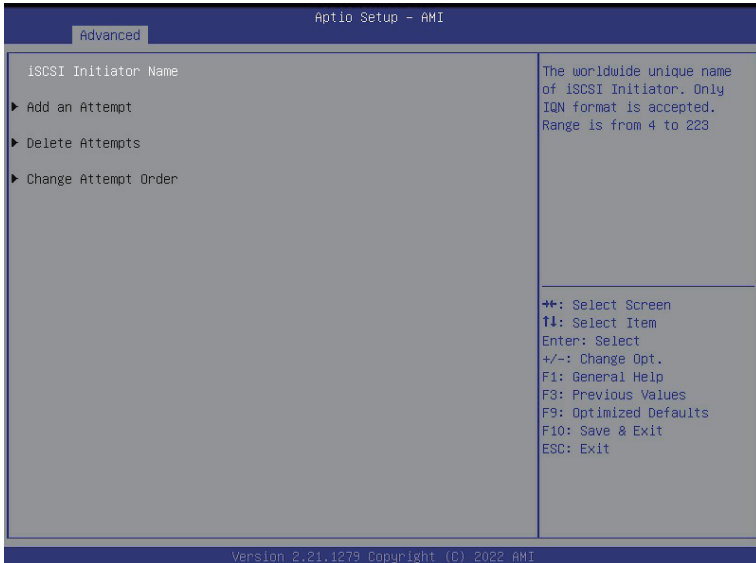
Parameter	Description
CPU0	Press [Enter] to view the memory configuration status related to CPU 0.

5-2-15 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.
Enroll Cert	Press [Enter] for configuration of advanced items.
Delete Cert	Press [Enter] for configuration of advanced items.

5-2-16 iSCSI Configuration



Parameter	Description
iSCSI Initiator Name	Press [Enter] and name iSCSI Initiator. Only IQN format is accepted. Range: from 4 to 223
Add Attempt	Press [Enter] for configuration of advanced items.
Delete Attempt	Press [Enter] for configuration of advanced items.
Change Attempt Order	Press [Enter] for configuration of advanced items.

5-2-17 Intel(R) Ethernet Controller X550

Advanced Aptio Setup - AMI

▶ Firmware Image Properties		View device firmware version information.
▶ NIC Configuration		
Blink LEDs	0	
UEFI Driver	Intel(R) 10GbE Driver 7.9.05 X64	
Adapter PBA	000000-000	
Device Name	Intel(R) Ethernet Controller X550	
Chip Type	Intel X550	
PCI Device ID	1563	
PCI Address	01:00:00	
Link Status	[Disconnected]	
MAC Address	D8:5E:D3:E0:3A:C4	
Virtual MAC Address	00:00:00:00:00:00	

++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

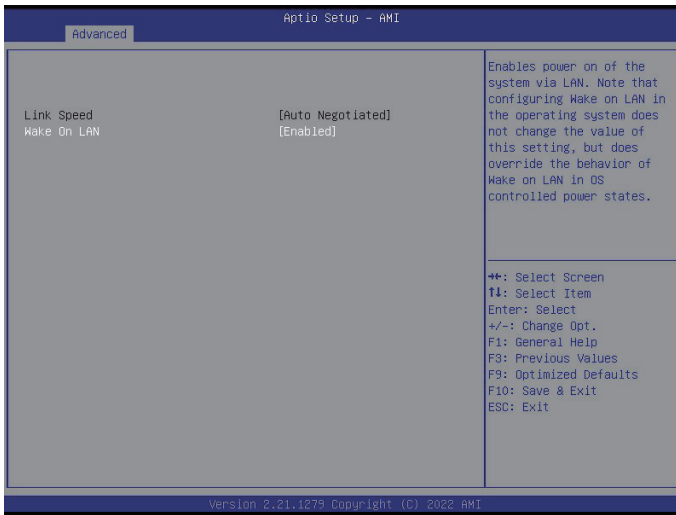
Version 2.21.1279 Copyright (C) 2022 AMI

Advanced Aptio Setup - AMI

Option ROM version	1.2926.0	
Unique NVM/EEPROM ID	0x80001578	
NVM Version	3.3	

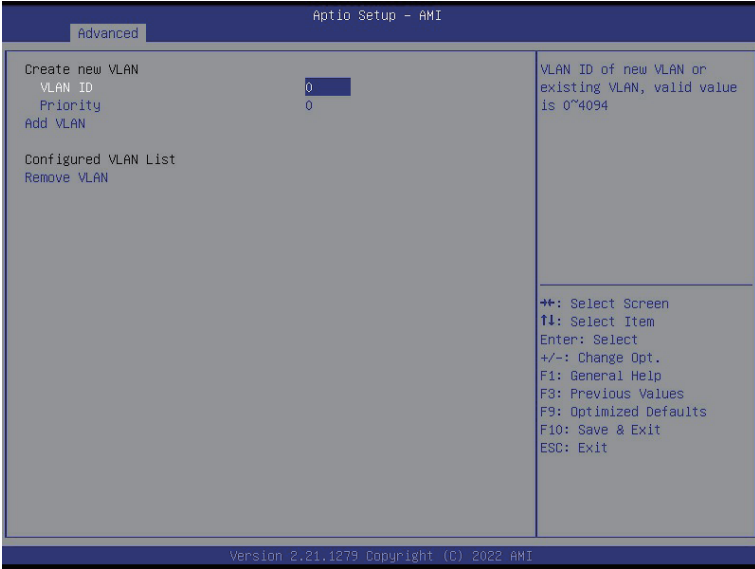
++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

Version 2.21.1279 Copyright (C) 2022 AMI



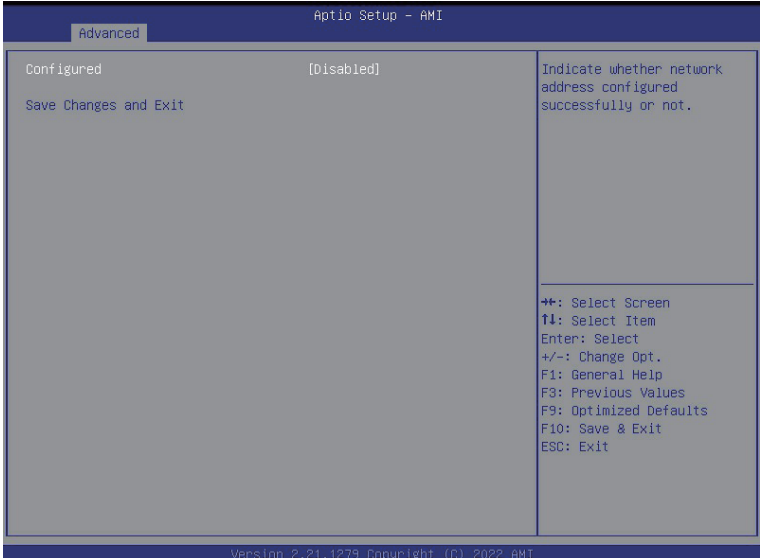
Parameter	Description
Firmware Image Properties	Press [Enter] to configure advanced items.
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Link Speed <ul style="list-style-type: none"> – Allows for automatic link speed adjustment. – Options available: 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	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.
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.

5-2-18 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.

5-2-19 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 Enabled .
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**.

5-2-20 MAC IPv6 Network Configuration



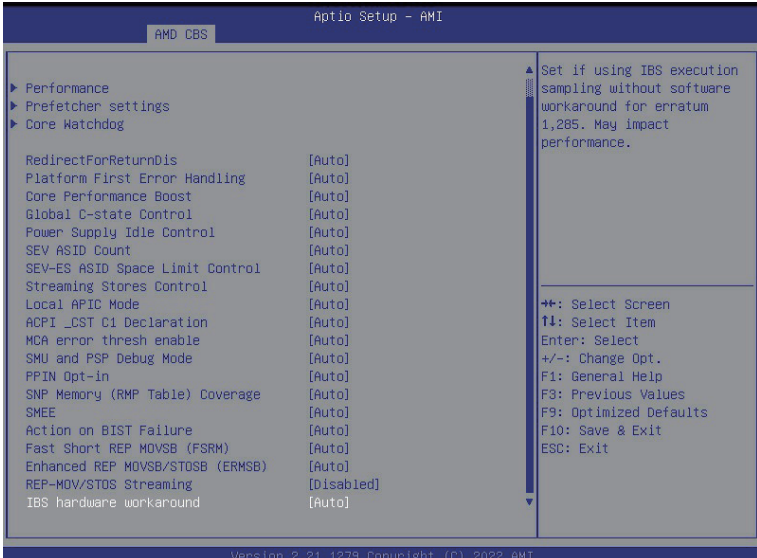
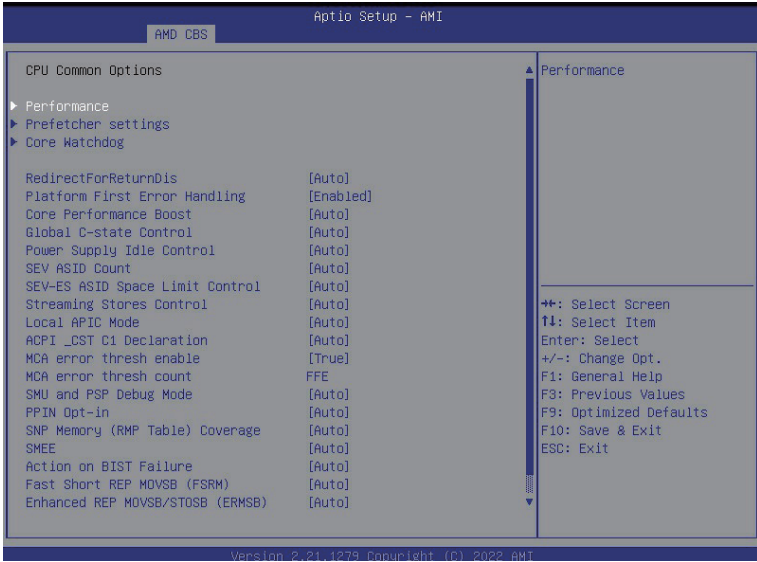
Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Displays the MAC Address information. ◆ Interface ID <ul style="list-style-type: none"> – The 64 bit alternative interface ID for the device. The string is colon separated. 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.

5-3 AMD CBS Menu

AMD CBS menu displays submenu options for configuring the CPU-related information that the BIOS automatically sets. Select a submenu item, then press [Enter] to access the related submenu screen.



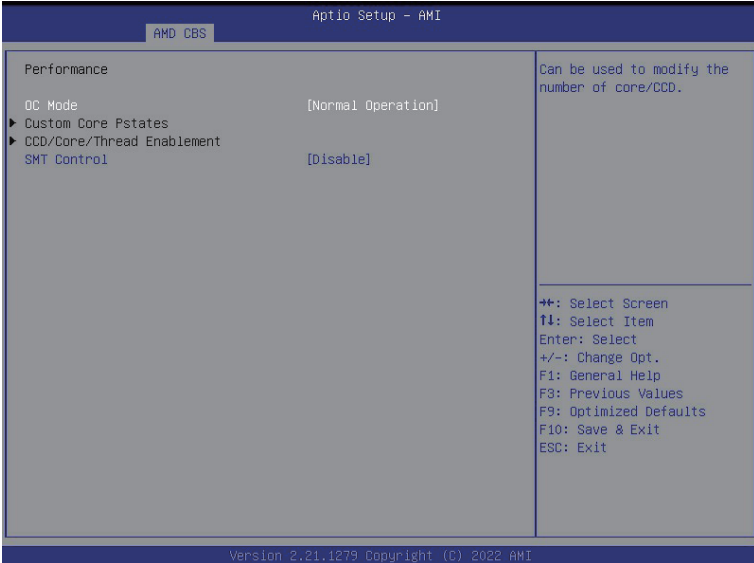
5-3-1 CPU Common Options



Parameter	Description
CPU Common Options	
Performance	Press [Enter] for configuration of advanced items.
Prefetcher settings	Press [Enter] for configuration of advanced items.
Core Watchdog	Press [Enter] for configuration of advanced items.
RedirectForReturnDis	From a workaround for GCC/C000005 issue for XV Core on CZ A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrctForReturns] to 1. Options available: Auto, 1, 0. Default setting is Auto .
Platform First Error Handling	Enable/Disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Core Performance Boost	Enable/Disable the Core Performance Boost function. Options available: Auto/Disabled. Default setting is Auto .
Global C-State Control	Controls the IO based C-state generation and DF C-states. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Power Supply Idle Control	Configures the Power Supply Idle Control. Options available: Auto, Low Current Idle, Typical Current Idle. Default setting is Auto .
SEV ASID Count	Specifies the maximum valid ASID, which affects the maximum system physical address space. Options available: Auto, 253 ASIDs, 509 ASIDs. Default setting is Auto .
SEV-ES ASID Space Limit Control	Space limit control for SEV-ES ASIDs. Options available: Auto/Manual. Default setting is Auto .
Streaming Stores Control	Enable/Disable the Streaming Stores functionality. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Local APIC Mode	Sets the Local APIC Mode. Options available: Auto, xAPIC, x2APIC. Default setting is Auto .
ACPI_CST C1 Decaration	Determines whether or not to declare the C1 state to the OS.. Options available: Auto, Enabled, Disabled. Default setting is Auto .
MCA error thresh enable	Enable MCA error thresholding. Options available: Auto, False, True. Default setting is Auto .
SMU and PSP Debug Mode	When this option is enabled, specific uncorrected errors detected by the PSP FW or SMU FW will hand and not reset the system. Options available: Auto, Enabled, Disabled. Default setting is Auto .

Parameter	Description
PPIN Opt-in	Enable/Disable the PPIN feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
SNP Memory (RMP Table) Coverage	Enabled: Enter system memory is covered. Options available: Auto, Enabled, Disabled, Custom. Default setting is Auto .
SMEE	Control secure memory encryption enable. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Action on BIST Failure	Action to take when a CCD BIST failure is detected. Options available: Auto, Do nothing, Down-CCD. Default setting is Auto .
Fast Short REP MOVSB	Default is 1, can be set to zero for analysis purpose as long as OS supports it. Options available: Enabled, Disabled. Default setting is Enabled .
Enhanced REP MOVSB/STOSB	Default is 1, can be set to zero for analysis purpose as long as OS supports it. Options available: Enabled, Disabled. Default setting is Enabled .
REP-MOV/STOS Steaming	Allows REP-MOV/STOS to use non-caching streaming stores for large sizes. Options available: Enabled, Disabled. Default setting is Enabled .
IBS hardware work around	Set if using IBS execution sampling without software workaround for erratum 1,285. May impact performance.. Options available: Enabled, Auto. Default setting is Enabled .

5-3-1-1 Performance



Parameter	Description
Performance	
OC Mode ^(Note1)	Option Available: Normal Operation, Customized Default setting is Normal Operation .
Custom Core Pstates	Allows you to accept or decline enabling Custom Core Pstates. When accepted, you can disable or customize core pstates.
CCD/Core/Thread Enablement	Allows you to accept or decline enabling CCDs, processor cores and threads. When accepted, you can control the number of CCDs to be used, the number of cores to be used, and whether to enable or disable Simultaneous Multithreading Technology (SMT) support.
SMT Control	Can be used to disable symmetric multithreading. To re-enable SMT, a Power CYCLE is needed after select the 'Enable' option. Select 'Auto' base on BIOS PCD. (PcdAmdSmtMode) default setting. Option Available: Enable, Disable. Default setting is Disable .

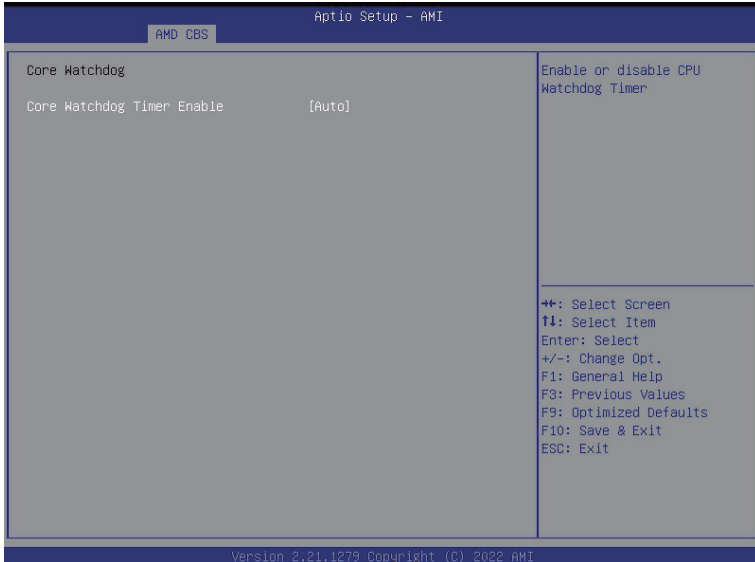
(Note1) Advanced items are configurable when this item is defined.

5-3-1-2 Prefetcher Settings



Parameter	Description
Prefetcher settings	
L1 Stream HW Prefetcher	Enable/Disable L1 Stream HW Prefetcher. Options available: Auto, Enable, Disabled. Default setting is Auto .
L1 Stride Prefetcher	Use memory access history of individual instruction to fetch additional lines Enable/Disable L1 Stream HW Prefetcher. Options available: Auto, Enable, Disable. Default setting is Auto .
L1 Region Prefetcher	Use memory access history to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses. Options available: Auto, Enable, Disable. Default setting is Auto .
L2 Stream HW Prefetcher	Enable/Disable L2 Stream HW Prefetcher. Options available: Auto, Enable, Disabled. Default setting is Auto .
L2 Up/Down Prefetcher	Use memory access history to determine whether to fetch the next or previous line for all memory accesses. . Options available: Auto, Enable, Disable. Default setting is Auto .

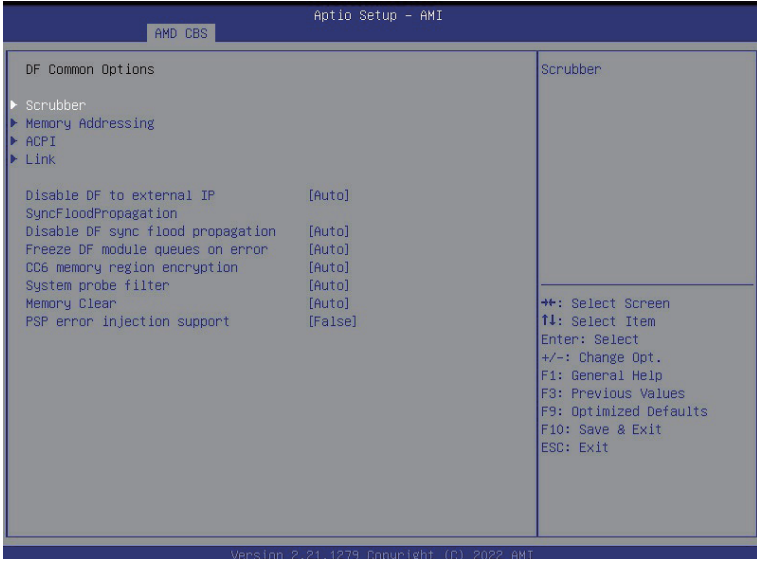
5-3-1-3 Core Watchdog



Parameter	Description
Core Watchdog	
Core Watchdog Timer Enable	Enable/Disable CPU Watchdog Timer. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Core Watchdog Timer Interval ^(Note)	Options available: Auto, 2.461s, 10.730s, 5.364s, 2.681s, 1.340s, 669.41ms, 334.05ms, 166.37ms, 82.53ms, 40.61ms, 20.970ms, 10.484ms, 5.241ms, 2.620ms, 1.309ms, 654.08us, 326.4us, 165.56us, 80.64us, 39.68us. Default setting is Auto .
Core Watchdog Timer Severity ^(Note)	Specify the CPU watch dog timer severity. Options available: Auto, No Error, Transparent, Corrected, Deferred, Uncorrected, Fatal. Default setting is Auto .

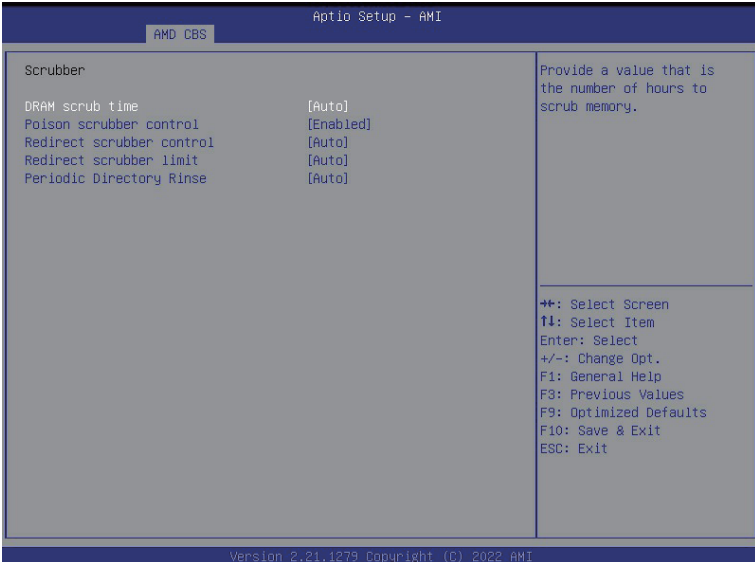
(Note) This item appears when **Core Watchdog Timer Enable** is set to **Enabled**.

5-3-2 DF Common Options



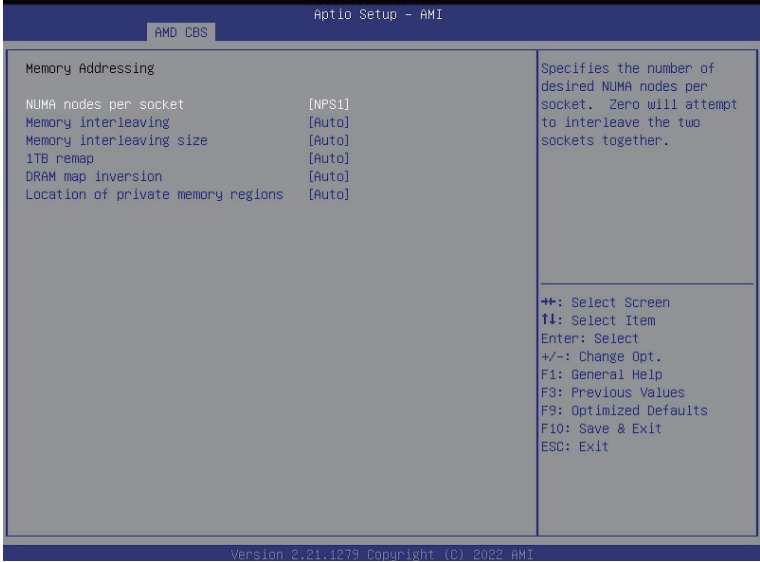
Parameter	Description
DF Common Options	
Scrubber	Press [Enter] for configuration of advanced items.
Memory Addressing	Press [Enter] for configuration of advanced items.
ACPI	Press [Enter] for configuration of advanced items.
Link	Press [Enter] for configuration of advanced items.
Disable DF to external IP sync flood propagation	Enable/Disable SyncFlood to UMC & downstream slaves. Options available: Auto, Sync flood disabled, Sync flood enabled. Default setting is Auto .
Disable DF sync flood propagation	Enable/Disable DF Sync Flood propagation. Options available: Auto, Sync flood disabled, Sync flood enabled. Default setting is Auto .
Freeze DF module queues on error	Options available: Auto, Enabled, Disabled. Default setting is Auto .
CC6 memory region encryption	Controls whether or not the CC6 save/restor memory is encrypted. Options available: Auto, Enabled, Disabled. Default setting is Auto .
System probe filter	Enable/Disable System probe filter. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Memory Clear	Enable/Disable the Memory Clear feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
PSP error injection support	Enable/Disable PSP error injection support. Options available: False/True. Default setting is False .

5-3-2-1 Scrubber



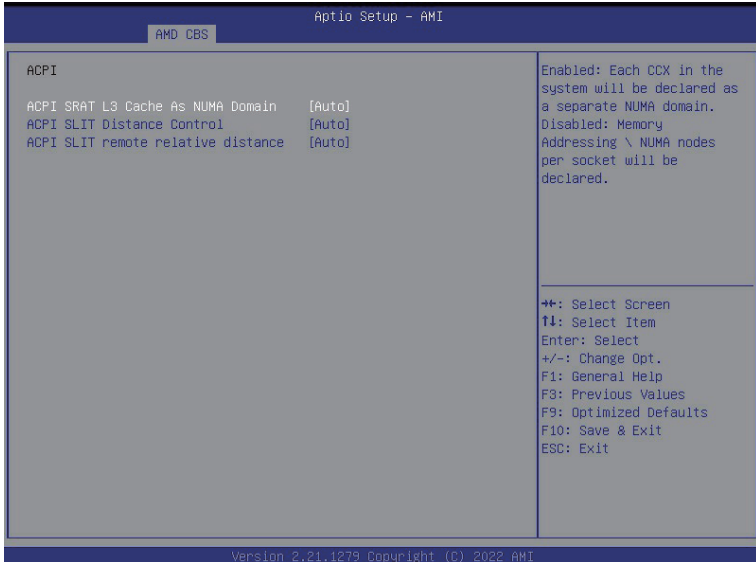
Parameter	Description
Scrubber	
DRAM scrub time	Provide a value that is the number of hours to scrub memory. Options available: Auto, Disabled, 1 hour, 4 hours, 8 hours, 16 hours, 24 hours, 48 hours. Default setting is Auto .
Poison scrubber control	Enable/Disable the Poison scrubber control feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Redirect scrubber control	Enable/Disable the Redirect scrubber control feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Redirect scrubber limit	Sets the redirect scrubber limit. Options available: Auto, 2, 4, 8, Infinite. Default setting is Auto .
Periodic Directory Rinse	Control Periodic Directory Rinse Mode. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-2-2 Memory Addressing



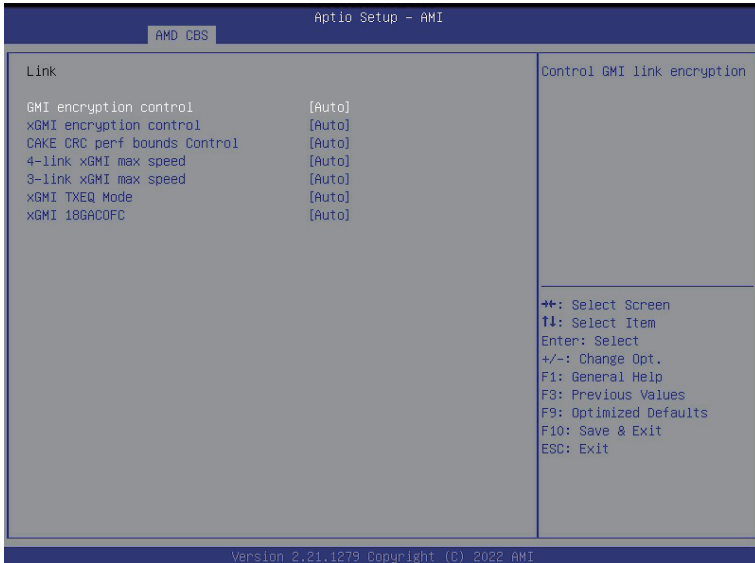
Parameter	Description
Memory Addressing	
NUMA nodes per socket	Specifies the number of desired NUMA nodes per socket. Options available: Auto, NPS0, NPS1, NPS2, NPS4. Default setting is NPS4 .
Memory inerleaving	Enable/Disable the Memory interleaving feature. Options available: Auto/Disabled. Default setting is Auto .
Memory interleaving size	Controls the memory interleaving size. This determines the starting address of the interleave (bit 8, 9, 10 or 11). Options available: Auto, 256Bytes, 512Bytes, 1KB, 2KB. Default setting is Auto .
1TB remap	Enable/Disable to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection, and may not always be possible. Options available: Auto, Do not remap, Attempt to remap. Default setting is Auto .
DRAM map inversion	Enable/Disable the DRAM map inversion function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Location of private memory regions	Control whether or not the rprivate memory regions (PSP, SMU, and CC6) are at the top of DRAM or distributed. Note that distributed requires memory on all dies. Note that it will always be at the top of DRAM if some dies don't have memory regardless of this. Options available: Auto, Distributed, Consolidated. Default setting is Auto .

5-3-2-3 ACPI



Parameter	Description
ACPI	
ACPI SRAT L3 Cache As NUMA Domain	Enable/Disable the ACPI SRAT L3 Cache As NUMA Domain function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
ACPI SLIT Distance Control	Determines how the SLIT distances are declared. Options available: Auto/Manual. Default setting is Auto .
ACPI SLIT remote relative distance	Sets the remote socket distance for 2P systems as near (2.8) or far (3.2). Options available: Auto, Near, Far. Default setting is Auto .

5-3-2-4 Link



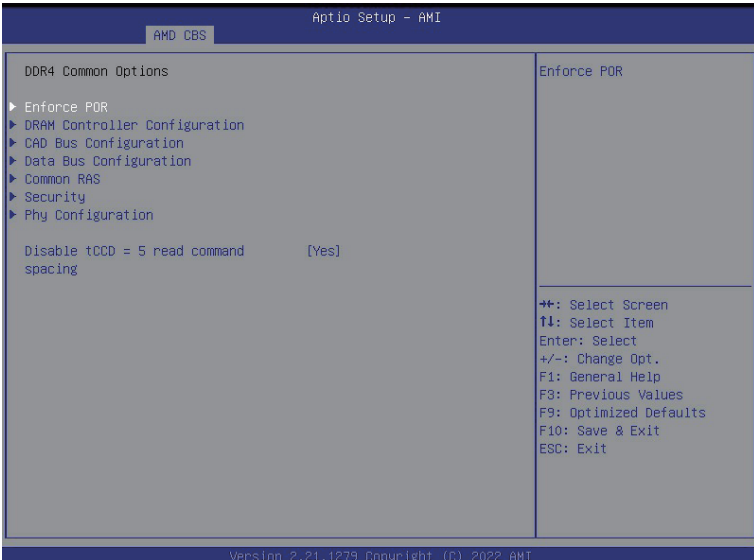
Parameter	Description
Link	
GMI encryption control	Enable/Disable GMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is Auto .
xGMI encryption control	Enable/Disable xGMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is Auto .
CAKE CRC perf bounds Control	Options available: Auto/Manual. Default setting is Auto .
4-link xGMI max speed	Specifies the max speed of 4-link xGMI. Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps. Default setting is 10.667Gbps .
3-link xGMI max speed	Specifies the max speed of 3-link xGMI. Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps. Default setting is 10.667Gbps .
xGMI TXEQ Mode	Configures xGMI TXEQ/RX vetting Mode. Options available: Auto, TXEQ_Disabled, TXEQ_Lane, TXEQ_Link, TXEQ_RX_Vet. Default setting is 10.667Gbps .
xGMI 18GACOFD	Configures xGMI 18GACOFD. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-3 UMC Common Options



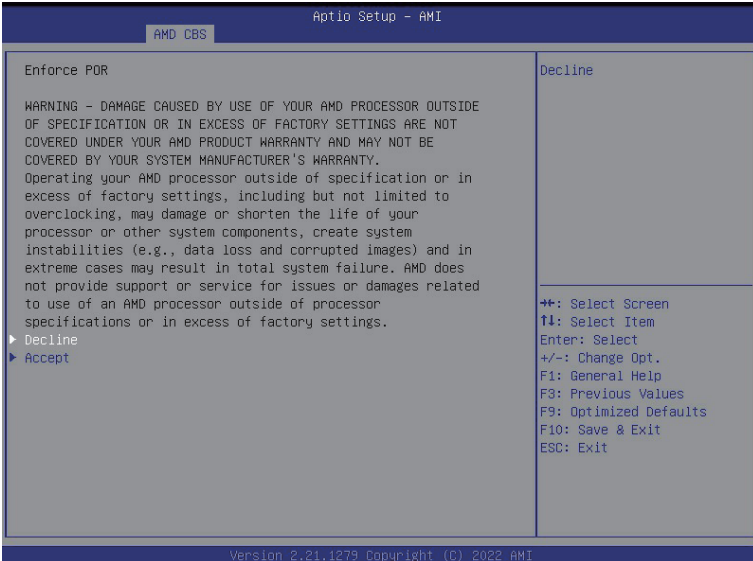
Parameter	Description
UMC Common Options	
DDR4 Common Options	Press [Enter] for configuration of advanced items.
DRAM Memory Mapping	Press [Enter] for configuration of advanced items.
NVDIMM	Press [Enter] for configuration of advanced items.
Memory MBIST	Press [Enter] for configuration of advanced items.

5-3-3-1 DDR4 Common Options

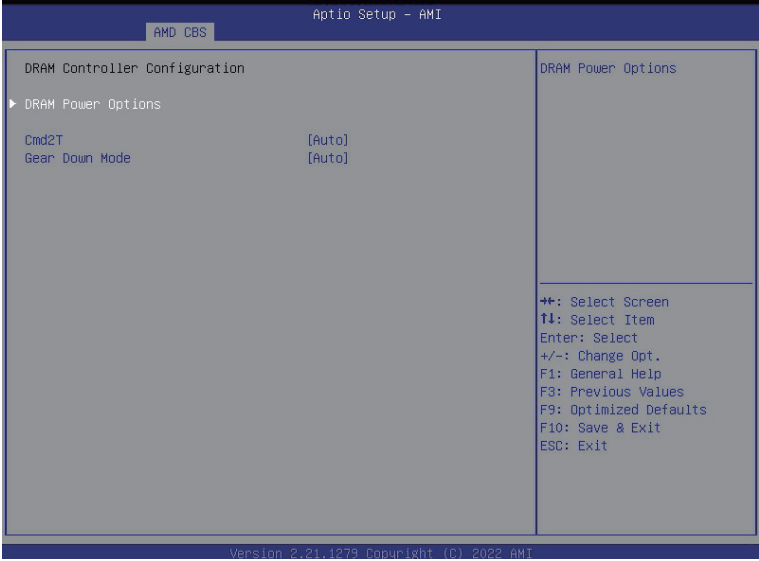


Parameter	Description
DDR4 Common Options	
Enforce POR	Press [Enter] to configure the Plan of Record (POR) to accept/decline restrictions for DDR4 frequency and voltage programming. Memory speeds will be capped at AMD guidelines.
DRAM Controller Configuration	Press [Enter] to configure DRAM Controller Configuration.
CAD Bus Configuration	Press [Enter] to configure CAD Bus Configuration.
Data Bus Configuration	Press [Enter] to configure Data Bus Configuration.
Common RAS	Press [Enter] to configure Common RAS.
Security	Press [Enter] to configure Security.
Phy Configuration	Press [Enter] to configure Phy Configuration.
Disable tCCD = 5 read command spacing	Options available: Yes,No.. Default setting is Yes .

5-3-3-1-1 Enforce POR

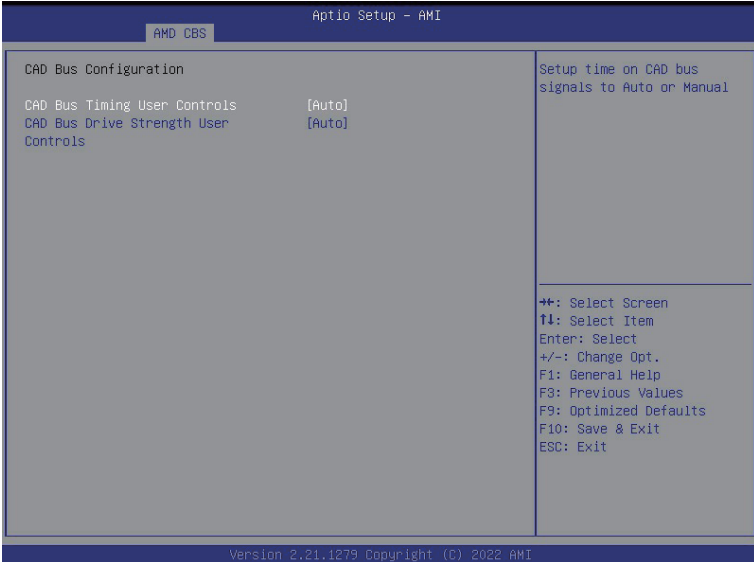


5-3-3-1-2 DRAM Controller Configuration



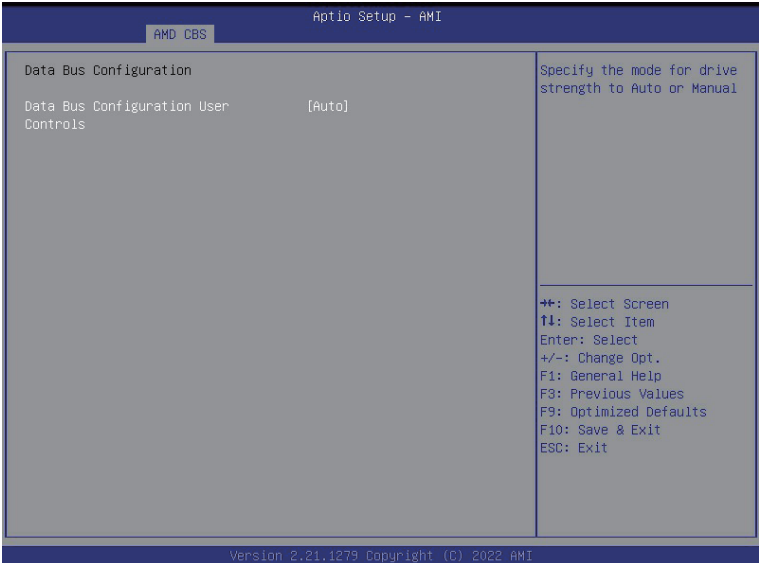
Parameter	Description
DRAM Controller Configuration	
DRAM Power Options	<p>Press [Enter] to configure DRAM Power OptionsMa.</p> <ul style="list-style-type: none"> ◆ Power Down Enable <ul style="list-style-type: none"> – Enable/Disable DDR power down mode. – Options available: Auto, Enabled, Disabled. Default setting is Auto. ◆ Power Down Entry Delay ◆ SubUrgRefLowerBound ◆ UrgRefLimit ◆ DRAM Maximum Activate Count <ul style="list-style-type: none"> – Options available: Auto, Unlimited MC, 200K,300K, 400K, 500K, 600K, 700K. Default setting is Auto. ◆ DRAM Refresh Rate <ul style="list-style-type: none"> – Options available: 7.8 usec, 3.9 usec. Default setting is 7.8 usec. ◆ Self-Refresh Exit Staggering <ul style="list-style-type: none"> – Options available: Disabled, Trfc/3, Trfc/4. Default setting is Disabled.
Cmd2T	<p>Selects the Cmd2T mode on ADDR/CMD.</p> <p>Options available: Auto, 1T, 2T. Default setting is Auto.</p>
Gear Down Mode	<p>Enable/Disable the Gear Down Mode function.</p> <p>Options available: Auto, Enabled, Disabled. Default setting is Auto.</p>

5-3-3-1-3 CAD Bus Configuration



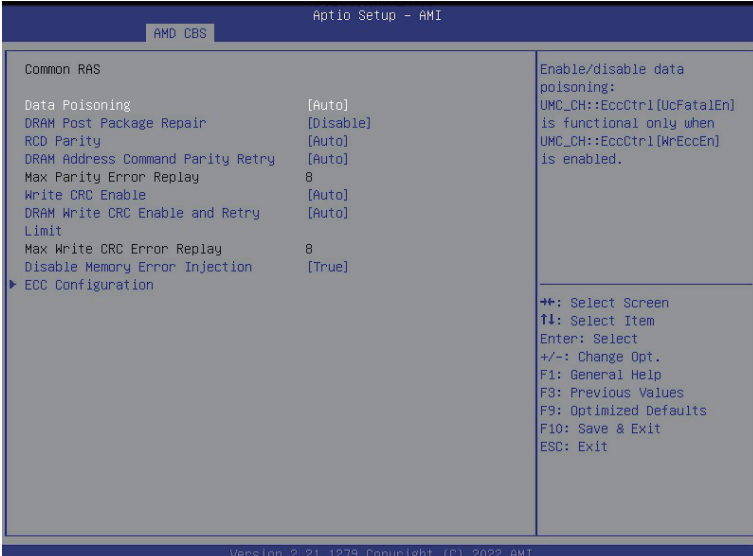
Parameter	Description
CAD Bus Configuration	
CAD Bus Timing User Controls	Setup time on CAD bus signals to Auto or Manual. Options available: Auto/Manual. Default setting is Auto .
CAD Bus Drive Strength User Controls	Drive Strength on CAD bus signals to Auto or Manual. Options available: Auto/Manual. Default setting is Auto .

5-3-3-1-4 Data Bus Configuration



Parameter	Description
Data Bus Configuration	
Data Bus Configuration User Controls	Specifies the mode for drive strength to Auto or Manual. Options available: Auto/Manual. Default setting is Auto .

5-3-3-1-5 Common RAS



Parameter	Description
Common RAS	
Data Poisoning	Enable/Disable the Data Poisoning function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
DRAM Post Package Repair	Enable/Disable the DRAM Post Package Repair function. Options available: Enabled/Disabled. Default setting is Auto .
RCD Parity	Enable/Disable the RCD Parity function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
DRAM Address Command Parity Retry	Enable/Disable the DRAM Address Command Parity Retry function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Max Parity Error Replay	Configures the Max Parity Error Replay. (0-0x3f) Default setting is 8 . Please note that this item is configurable when DRAM Address Command Parity Retry is set to Enabled.
Write CRC Enable	Enable/Disable the Write CRC function. Options available: Auto, Enabled, Disabled. Default setting is Auto .
DRAM Write CRC Enable and Retry Limit	Enable/Disable DRAM Write CRC Enable and Retry Limit. Options available: Auto, Enabled, Disabled. Default setting is Auto . Configures the Max Write CRC Error Replay. (0-0x3f)
Max Write CRC Error Replay	Default setting is 8 . Please note that this item is configurable when DRAM Write CRC Enable and Retry Limit is set to Enabled.

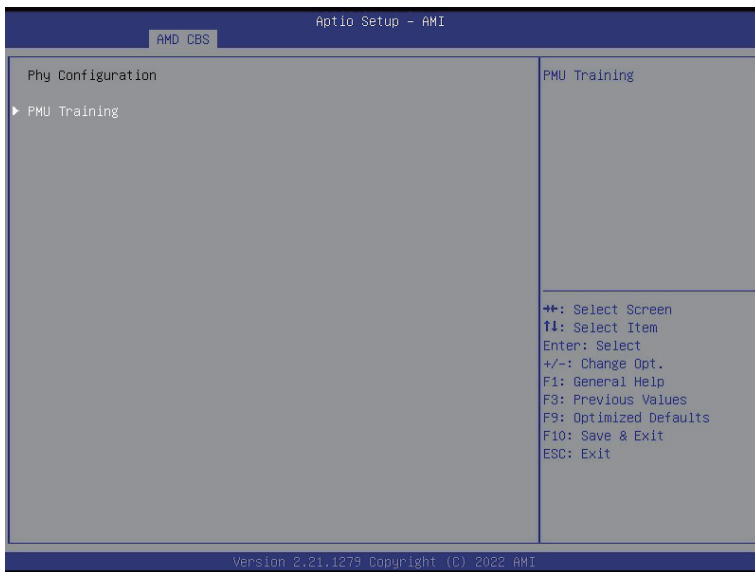
Parameter	Description
Disable Memory Error Injection	Options available: False/True. Default setting is True .
ECC Configuration	<p data-bbox="396 189 732 213">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="396 221 954 299">◆ DRAM ECC Symbol Size <ul style="list-style-type: none"> <li data-bbox="434 244 783 268">– Configures the DRAM ECC Symbol Size. <li data-bbox="434 271 926 294">– Options available: Auto, x4, x8, x16. Default setting is Auto. <li data-bbox="396 307 954 417">◆ DRAM ECC Enable <ul style="list-style-type: none"> <li data-bbox="434 330 942 385">– Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable. <li data-bbox="434 388 954 443">– Options available: Auto, Enabled, Disabled. Default setting is Auto. <li data-bbox="396 451 954 561">◆ DRAM UECC Retry <ul style="list-style-type: none"> <li data-bbox="434 475 740 498">– Enable/Disable DRAM UECC Retry. <li data-bbox="434 501 954 556">– Options available: Auto, Enabled, Disabled. Default setting is Auto.

5-3-3-1-6 Security



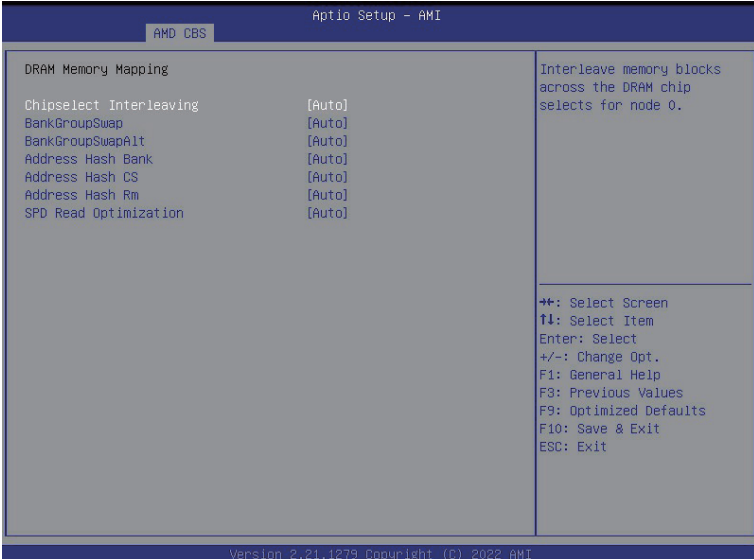
Parameter	Description
Security	
TSME	Enable/Disable Transparent SME. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Data Scramble	Enable/Disable Data Scrambling. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-3-1-7 Phy Configuration



Parameter	Description
Phy Configuration	
PMU Training	<p>Press [Enter] to configure PMU Training.</p> <ul style="list-style-type: none"> ◆ DFE Traing <ul style="list-style-type: none"> – Enable/Disable DDR power down mode. – Options available: Auto, Enabled, Disabled. Default setting is Auto. ◆ FFE Write Training <ul style="list-style-type: none"> – Auto, Enabled, Disabled. Default setting is Auto. ◆ PMU Pattern Bits Controls <ul style="list-style-type: none"> – Auto, Manual. Default setting is Auto.

5-3-3-2 DRAM Memory Mapping



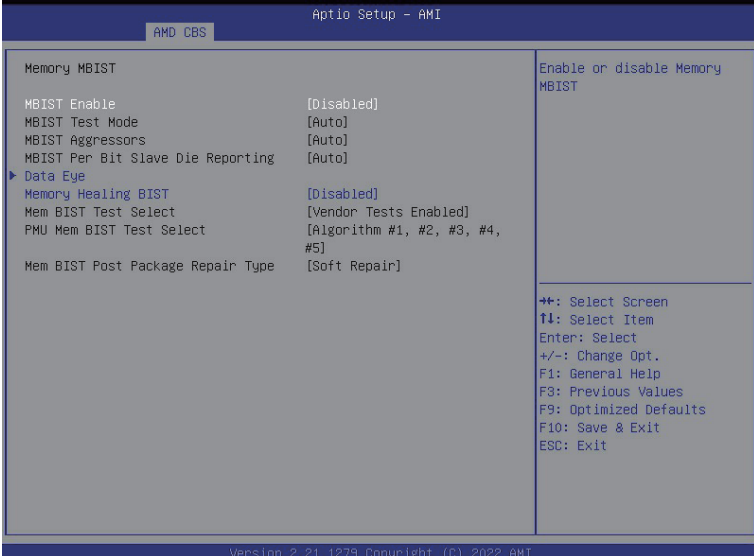
Parameter	Description
DRAM Memory Mapping	
Chipselect Interleaving	Interleave memory blocks across the DRAM chip selects for CPU 0. Options available: Auto/Disabled. Default setting is Auto .
BankGroupSwap	Configures the BankGroupSwap. BankGroupSwap (BGS) is a new memory mapping option in AGESA that alters how applications get assigned to physical locations within the memory modules. When this option sets to Auto, it is null: No help string. Options available: Auto, Enabled, Disabled. Default setting is Auto .
BankGroupSwapAlt	Configures the BankGroupSwapAlt. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Address Hash Bank	Enable/Disable bank address hashing. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Address Hash CS	Enable/Disable CS address hashing. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Address Hash Rm	Enable/Disable RM address hashing. Options available: Auto, Enabled, Disabled. Default setting is Auto .
SPD Read Optimization	Enable/Disable SPD Read Optimization. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-3-3 NVDIMM



Parameter	Description
NVDIMM	Disable NVDIMM-N feature for memory margin tool. Options available: No, Yes. Default setting is No .

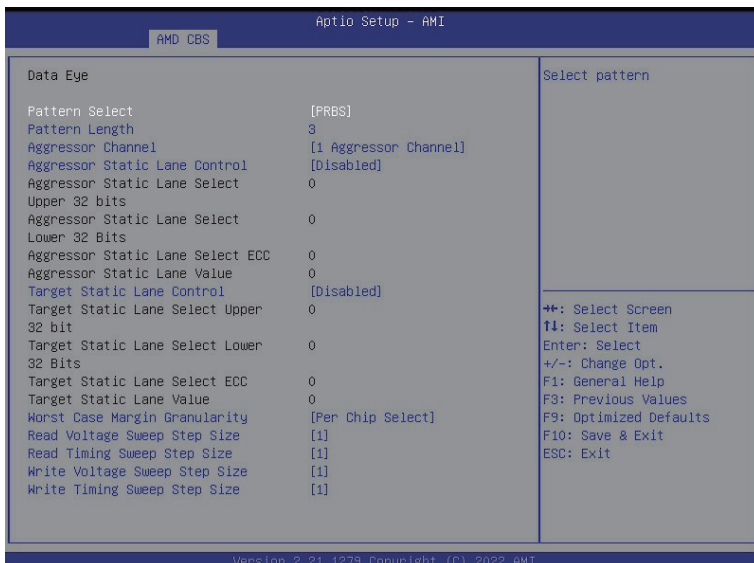
5-3-3-4 Memory MBIST



Parameter	Description
Memory MBIST	
MBIST Enable	Enable/Disable the Memory MBIST function. Options available: Enabled/Disabled. Default setting is Disabled .
MBIST Test Mode ^(Note)	Selects MBIST Test Mode. Interface Mode: Tests Single and Multiple CS transactions and Basic Connectivity. Data Eye Mode: Measures Voltage vs. Timing. Options available: Auto, Both, Interface Mode, Data Eye Mode. Default setting is Auto .
MBIST Aggressors ^(Note)	Enable/Disable MBIST Aggressor test. Options available: Auto, Enabled, Disabled. Default setting is Auto .
MBIST Per Bit Slave Die Reporting ^(Note)	Enable/Disable to report 2D data eye results in ABL log for each DQ, Chipselect, and Channel. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Data Eye	Press [Enter] to configure advanced items.
Memory Healing BIST	Enable/Disable memory healing BIST. Options available: Auto, Enabled, Disabled. Default setting is Disabled .

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

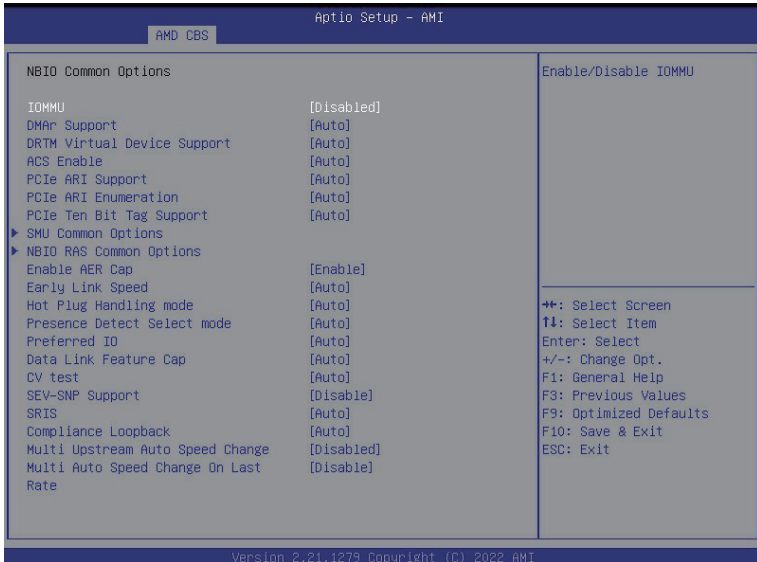
5-3-3-4-1 Data Eye



Parameter	Description
Data Eye	
Pattern Select	Options available: PRBS, SSO, Both. Default setting is PRBS .
Pattern Length	Determines the pattern length. The possible options are N=3....12.
Aggressor Channel	This item helps read the aggressors channels. Options available: Disabled, 1 Aggressor Channel, 3 Aggressor Channels, 7 Aggressor Channels. Default setting is 1 Aggressor Channel .
Aggressor Static Lane Control	Enable/Disable the Aggressor Static Lane Control function. Options available: Enabled/Disabled. Default setting is Disabled .
Aggressor Static Lane Select Upper 32 bits	This item is configurable when Aggressor Static Lane Control is set to Enabled .
Aggressor Static Lane Select Lower 32 bits	This item is configurable when Aggressor Static Lane Control is set to Enabled .
Aggressor Static Lane Select ECC	This item is configurable when Aggressor Static Lane Control is set to Enabled .
Aggressor Static Lane Value	This item is configurable when Aggressor Static Lane Control is set to Enabled .
Target Static Lane Control	Enable/Disable the Target Static Lane Control function. Options available: Enabled/Disabled. Default setting is Disabled .

Parameter	Description
Target Static Lane Select Upper 32 bits	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Select Lower 32 bits	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Select ECC	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Value	This item is configurable when Target Static Lane Control is set to Enabled .
Worst Case Margin Granularity	Configures Worst Case Margin Granularity. Options available: Per Chip Select, Per Nibble. Default setting is Worst Case Margin Only .
Read Voltage Sweep Step Size	Configures the step size for read Data Eye voltage sweep. Options available: 1, 2, 4. Default setting is 2 .
Read Timing Sweep Step Size	Configures the step size for read Data Eye timing sweep. Options available: 1, 2, 4. Default setting is 1 .
Write Voltage Sweep Step Size	Configures the step size for write Data Eye voltage sweep. Options available: 1, 2, 4. Default setting is 2 .
Write Timing Sweep Step Size	Configures the step size for write Data Eye timing sweep. Options available: 1, 2, 4. Default setting is 1 .

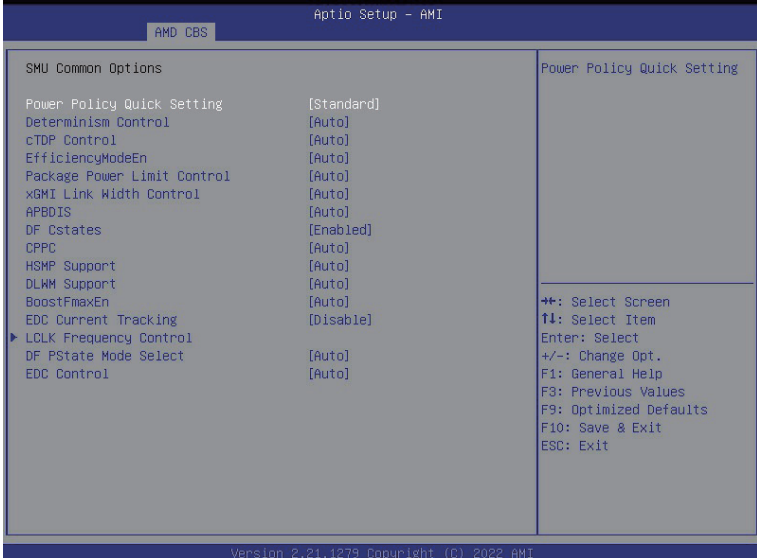
5-3-4 NBIO Common Options



Parameter	Description
NBIO Common Options	
IOMMU	Enable/Disable the IOMMU function. Options available: Enabled/Disabled. Default setting is Disabled .
DMAr Support	Enable DMAr system protection during POST. Options available: Auto, Enabled/Disabled. Default setting is Auto .
PCIe ARI Support	Enable/Disable Alternative Routing-ID Interpretation. Options available: Auto, Enabled, Disabled. Default setting is Auto .
PCIe ARI Enumeration	ARI Forwarding Enable for each downstream port. Options available: Auto, Enabled, Disabled. Default setting is Auto .
PCIe Ten Bit Tag Support	Enable/Disable PCIe ten bit tags for supported devices. (Auto=Disabled) Options available: Auto, Enabled, Disabled. Default setting is Auto .
SMU Common Options	Press [Enter] for configuration of advanced items.
NBIO RAS Common Options	Press [Enter] for configuration of advanced items.
Enable AER Cap	Enable/Disable Advanced Error Reporting Capability. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Early Link Speed	Configures Early Link Speed. Options available: Auto, Gen1, Gen2. Default setting is Auto .

Parameter	Description
Hot Plug Handling mode	Controls the Hot Plug Handling mode. Options available: Auto, A0 Mode, OS First (No Error Handling), OS First (Error Handling-Not Implemented), Firmware First (Not Implemented). Default setting is Auto .
Presence Detect Select mode	Controls the Presence Detect Select mode. Options available: Auto, OR, AND. Default setting is Auto .
Preferred IO Device	Configures Preferred IO Device. Options available: Auto, Manual. Default setting is Auto .
Data Link Feature Cap	Data Link Feature capacity. Options available: Auto, Enabled, Disabled.. Default setting is Auto .
CV test	Set this to Enabled to support running PCIECV tool. Auto: preserve hardware defaults. Options available: Auto, Enabled, Disabled. Default setting is Auto .
SEV-SNP Support	Enable or Disable SEV-SNP Support. Options available: Enable, Disable. Default setting is Disable .
SRIS	Options available: Auto, Enable, Disable. Default setting is Auto .
Compliance Loopback	Options available: Auto, Enable, Disable. Default setting is Auto .
Multi Upstream Auto Speed Change	Defines the setting of this feature for all PCIe devices. Options available: Enabled, Disabled. Default setting is Disabled .
Multi Auto Speed Change On Last Rate	Force PCIe link training speed to last advertised for all ports. Options available: Enable, Disable. Default setting is Disable .

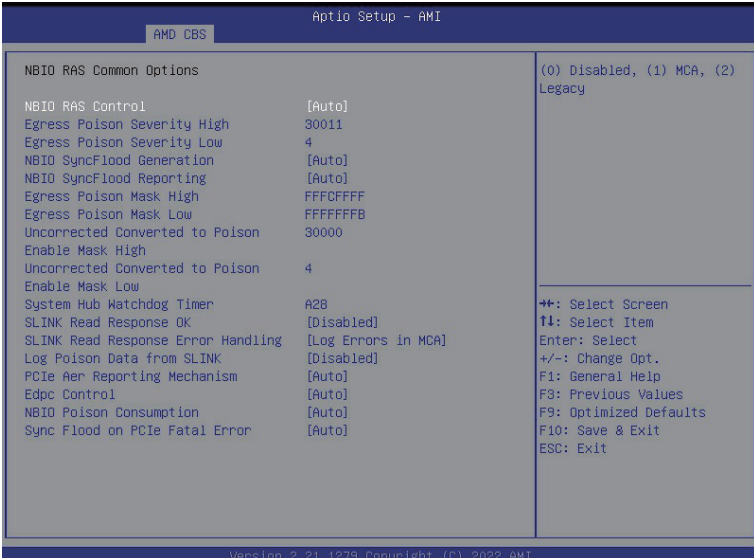
5-3-4-1 SMU Common Options



Parameter	Description
SMU Common Options	
Power Policy Quick Setting	Options available: Standard, Best Performance, Energy Efficient. Default setting is Standard .
Determinism Control	Selects use the fused Determinism or set customized Determinism. Options available: Auto/Manual. Default setting is Auto .
Determine Slider	Options available: Auto/Power, Performance. Default setting is Power .
cTDP Control	Selects use the fused TDP or set customized TDP. **TDP is used to define the RC thermal model only** Options available: Auto/Manual. Default setting is Auto .
EfficiencyModeEn	Options available: Auto/Enabled. Default setting is Auto .
Package Power Limit Control	Selects use the fused PPT or set customized PPT. **PPT will be used as the ASIC power limit** Options available: Auto/Manual. Default setting is Auto .
xGMI Link Width Control	Options available: Auto/Enabled. Default setting is Auto .
APBDIS	Options available: Auto, 0, 1. Default setting is Auto .

Parameter	Description
DF Cstates	Enable/Disable DF C-states. Options available: Auto, Enabled, Disabled. Default setting is Auto .
CPPC	Enable/Disable the CPPC feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
HSMP Support	Select HSMP support enable or disable. Options available: Auto, Enabled, Disabled. Default setting is Auto .
DLMM Support	Select DLMM support enable or disable. Options available: Auto, Enabled, Disabled. Default setting is Auto .
BoostFmaxEn	Options available: Auto/Enabled. Default setting is Auto .
EDC Current	Options available: Enable, Disable. Default setting is Disable .
LCLK Frequency Control	Press [Enter] for advanced configuration. <ul style="list-style-type: none"> ◆ Root Complex 0x00 LCLK Frequency <ul style="list-style-type: none"> – Options available: Auto, 593Mhx. Default setting is Auto. ◆ Root Complex 0x40 LCLK Frequency <ul style="list-style-type: none"> – Options available: Auto, 593Mhx. Default setting is Auto. ◆ Root Complex 0x80 LCLK Frequency <ul style="list-style-type: none"> – Options available: Auto, 593Mhx. Default setting is Auto. ◆ Root Complex 0xC0 LCLK Frequency <ul style="list-style-type: none"> – Options available: Auto, 593Mhx. Default setting is Auto.
DF PSTATE Mode Select	Option available: Normal, limit Highest, Limit All, Auto. Default setting is Auto .
EDC Control	Options available: Auto/Enabled. Default setting is Auto .

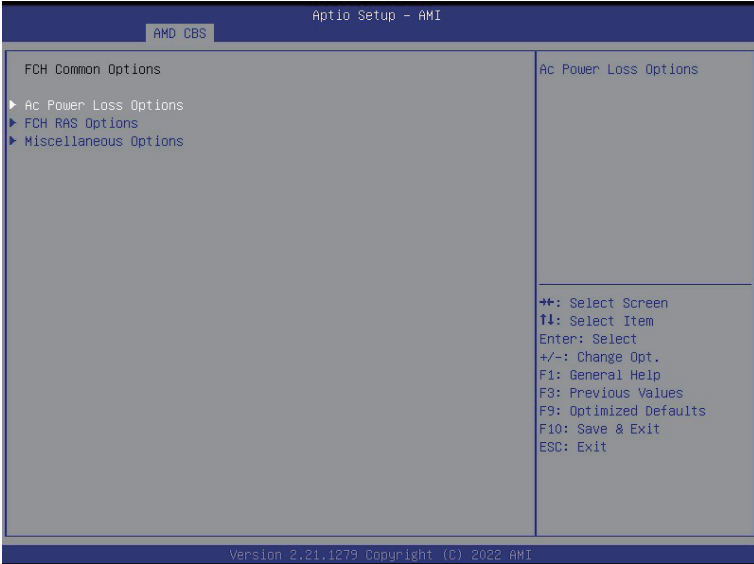
5-3-4-2 NBIO RAS Common Options



Parameter	Description
NBIO RAS Common Options	
NBIO RAS Control	Options available: Disabled, MCA, Legacy. Default setting is MCA .
Egress Poison Serverity High	Configures the Egress Poison High Serverity. Each bit set to 1 enables High servery on the associated IOHC egress port. A bit of 0 indicates LOW servery.
Egress Poison Servery Low	Configures the Egress Poison Low Servery. Each bit set to 1 enables High servery on the associated IOHC egress port. A bit of 0 indicates LOW servery.
NBIO SyncFlood Generation	The value may be used to mask SyncFlood caused by NBIO RAS options. Options available: Auto, Enabled, Disabled. Default setting is Auto .
NBIO SyncFlood Reporting	The value may be used to enanle SyncFlood reporting to APML. Options available: Enabled/Disabled. Default setting is Disabled .
Egress Poison Mask High	Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.
Egress Poison Mask Low	Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.

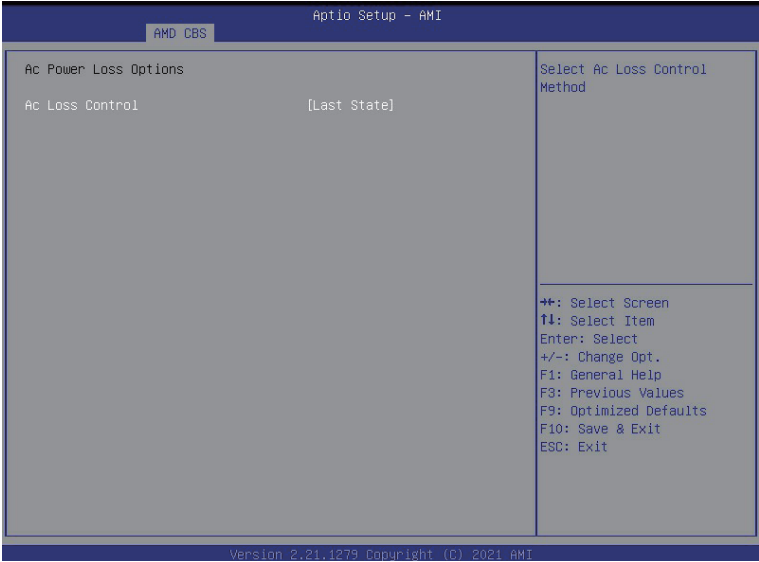
Parameter	Description
Uncorrected Converted to Poison Enable Mask High	Enables mask for masking of uncorrectable parity errors on internal arrays.
Uncorrected Converted to Poison Enable Mask Low	Enables mask for masking of uncorrectable parity errors on internal arrays.
System Hub Watchdog Timer	Specifies the timer interval of the SYSHUB Watchdog timer in milliseconds.
SLINK Read Response OK	This item specifies whether SLINK read response errors are converted to an Okay response. Options available: Enabled/Disabled. Default setting is Disabled .
SLINK Read Response Error Handling	Options available: Enabled, Trigger MCOMMIT Error, Log Errors in MCA. Default setting is Log Errors in MCA .
Log Poison Data from SLINK	Enable/Disable the Log Poison Data from SLINK feature. Options available: Enabled/Disabled. Default setting is Disabled .
PCIe Aer Reporting Mechanism	Selects the method of reporting AER errors from PCI Express. Options available: Auto, Firmware First, OS First, MCA. Default setting is Auto .
Edpc Control	Options available: Auto, Enabled, Disabled. Default setting is Disabled .
NBIO Poison Consumption	Options available: Auto, Enabled, Disabled. Default setting is Auto .
Sync Flood on PCIe Fatal Error	Options available: Auto, True, False. Default setting is Auto .

5-3-5 FCH Common Options



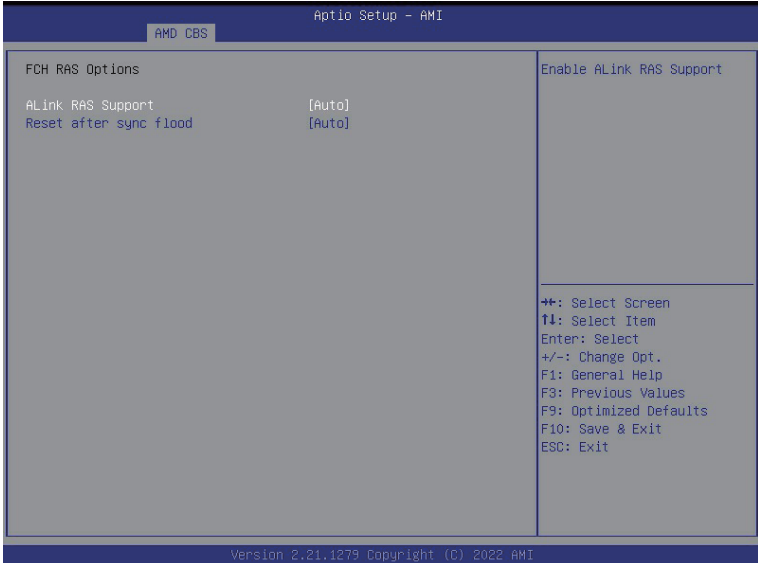
Parameter	Description
FCH Common Options	
AC Power Loss Options	Press [Enter] for configuration of advanced items.
FCH RAS Options	Press [Enter] for configuration of advanced items.
Miscellaneous Options	Press [Enter] for configuration of advanced items.

5-3-5-1 AC Power Loss Options



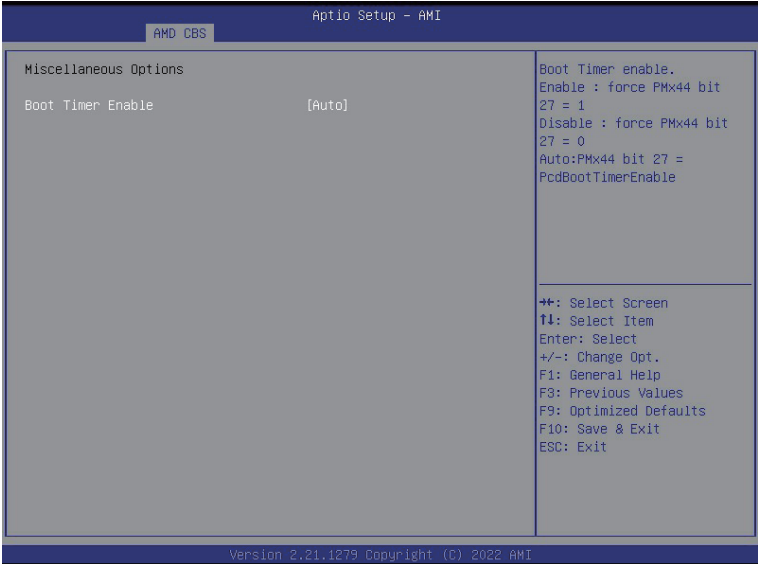
Parameter	Description
AC Power Loss Options	
AC Loss Control	Selects the AC Loss Control Method. Options available: Power Off, Power On, Last State. Default setting is Power off .

5-3-5-2 FCH RAS Options



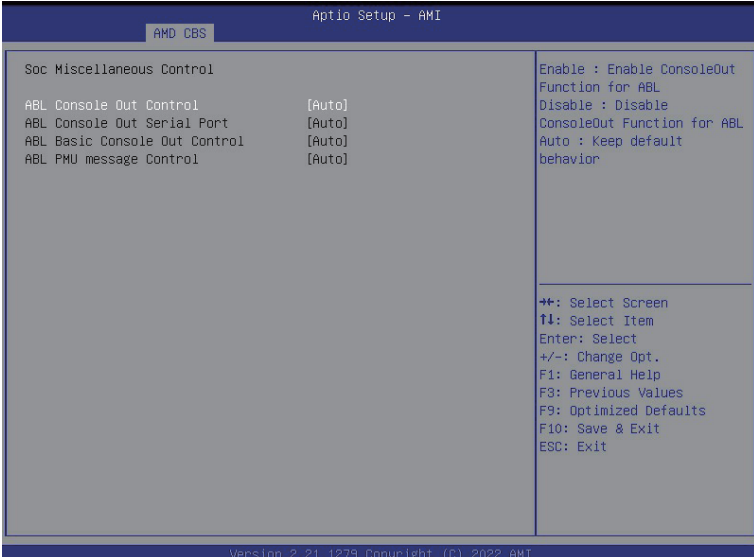
Parameter	Description
FCH RAS Options	
ALink RAS Support	Enable/Disable the ALink RAS Support. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Reset after sync flood	Enable/Disable AB to forward downstream sync-flood message to system controller. Options available: Auto, Enable, Disable. Default setting is Auto .

5-3-5-3 Miscellaneous Options



Parameter	Description
Miscellaneous Options	
Boot Time Enable	Options available: Auto, Enabled, Disabled. Default setting is Auto .

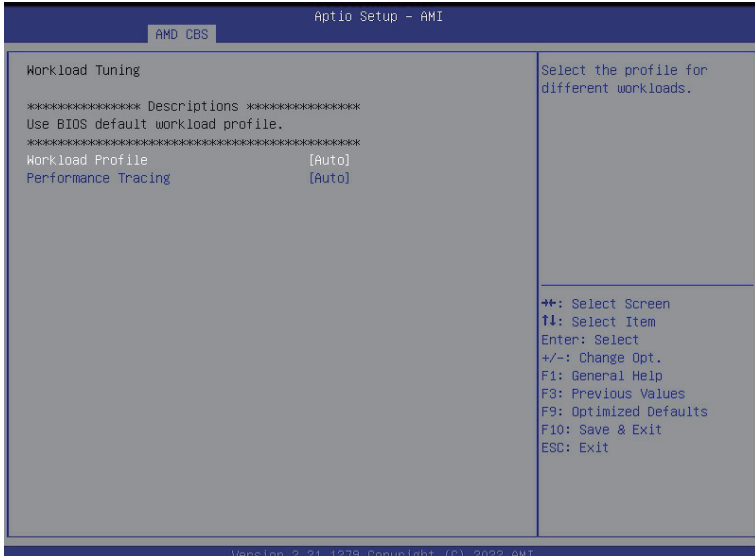
5-3-6 SOC Miscellaneous Control



Parameter	Description
SOC Miscellaneous Control	
ABL Console Out Control	Enable/Disable the ConsoleOut function for ABL. Options available: Auto, Enabled, Disabled. Default setting is Auto .
ABL PMU message Control ^(Note)	To Control the total number of PMU debug messages. Options available: Auto, Enabled, Disabled. Default setting is Auto .

(Note) This item appears when **ABL Console Out Control** is set to **Enabled**.

5-3-7 Workload Tuning



Parameter	Description
Workload Tuning	
Workload Profile	Select the profile for different workloads. Default setting is Auto .
Performance Tracing	Enable to allow capturing performance traces. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-4 AMD PBS Menu

AMD PBS Option menu displays submenu options for configuring the function of AMD PBS. Select a submenu item, then press [Enter] to access the related submenu screen.



Parameter	Description
RAS	Press [Enter] for configuration of advanced items.
iLA TraceMemoryEn	Reserved 1M bytes MMIO space on 1M boundary when iLA TraceMemoryEn disabled. Options available: Enabled/Disabled. Default setting is Disabled .
iLA TraceMemoryEn reserved MMIO	Reserved function.
SRIS mode debug	Control SRIS mode debug. Options available: Auto/Enabled/Disabled. Default setting is Auto .
SRIS Autodetect	Control SRIS Autodetect. Options available: Auto/Enabled/Disabled. Default setting is Auto .

5-4-1 RAS

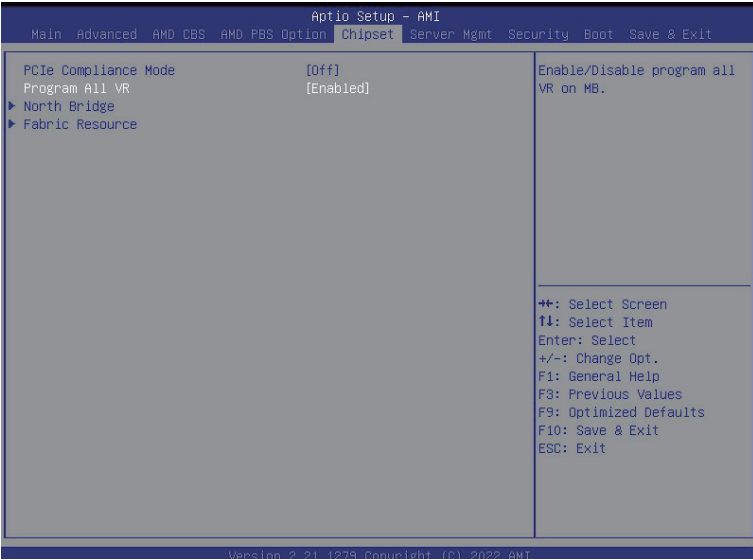


Parameter	Description
RAS Periodic SMI Control	Enable/Disable the Periodic SMI for polling [MCA Threshold] error. Options available: Enabled/Disabled. Default setting is Enabled .
SMI Threshold	Configures the SMI Threshold value.
SMI Scale	Configures the SMI Scale value.
SMI Scale Unit	Defines the unit of time scale. Options available: millisecond, second, minute. Default setting is millisecond .
SMI Period	Configures the SMI Period.
GHES Notify Type	Selects the Notification type for deferred/ corrected errors. Options available: Polled/SCI. Default setting is Polled .
GHES UnCorr Notify Type	Selects the Notification type for uncorrected errors. Options available: Polled/NMI. Default setting is NMI .
PCIe GHES Notify Type	Selects the Notification type for PCIe corrected errors. Options available: Polled/SCI. Default setting is Polled .
PCIe UnCorr GHES Notify Type	Selects the Notification type for PCIe uncorrected errors. Options available: Polled/NMI. Default setting is NMI .
PCIe Root Port Corr Err Mask Reg	Initialize the PCIe AER Corrected Error Mask register of Root Port.

Parameter	Description
PCIe Root Port UnCorr Err Mask Reg	Initialize the PCIe AER Uncorrected Error Mask register of Root Port.
PCIe Root Port UnCorr Err Sev Reg	Initialize the PCIe AER Uncorrected Error Severity register of Root Port.
PCIe Device Corr Err Mask Reg	Initialize the PCIe AER Corrected Error Mask register of PCIe device.
PCIe Device UnCorr Err Mask Reg	Initialize the PCIe AER Uncorrected Error Mask register of PCIe device.
PCIe Device UnCorr Err Sev Reg	Initialize the PCIe AER Uncorrected Error Severity register of PCIe device.
CCIX GHES Deferred ERR Notify Type	Selects the Notification type for CCIX deferred error. Options available: Polled/SCI. Default setting is Polled .
CCIX GHES Corrected Err Notify Type	Selects the Notification type for CCIX corrected error. Options available: Polled/SCI. Default setting is Polled .
DDR4 DRAM Hard Post Package Repair	This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism. Options available: Enabled/Disabled. Default setting is Disabled .
HEST DMC Structure Support	HEST DMC (Deferred Machine Check) Structure Support. Options available: Enabled/Disabled. Default setting is Disabled .
RAS EINJ Mode	BIOS: Send APEI EINJ actions to PSP via CPM EINJSMI callback; PSP: Send APEI EINJ actions to RSP via PSP Mailbox. Option available: BIOS, PSP. Default setting is PSP .

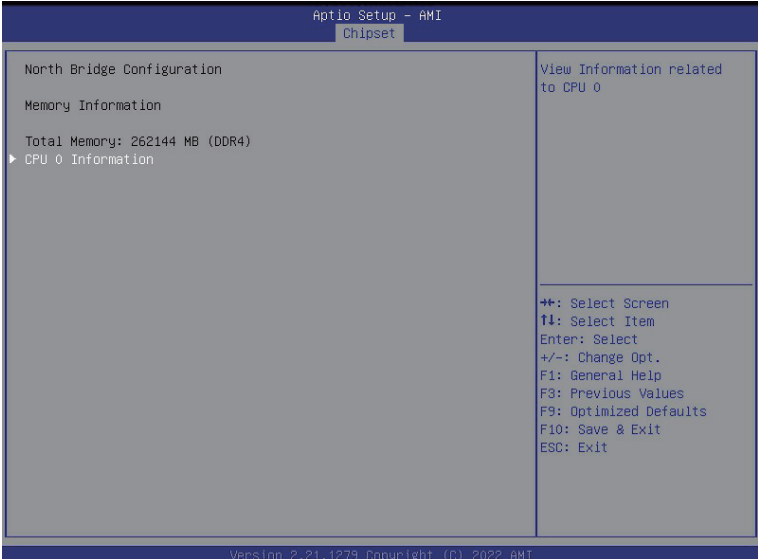
5-5 Chipset Setup Menu

Chipset Setup menu displays submenu options for configuring the function of the North Bridge. Select a submenu item, then press <Enter> to access the related submenu screen.



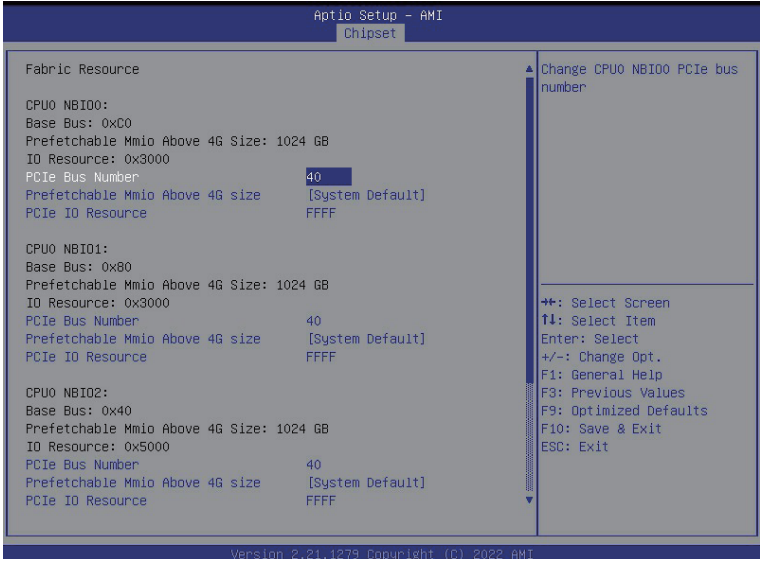
Parameter	Description
PCIe Compliance Mode	Options available: On/Off. Default setting is Off .
Program All VR	Enable/Disable program all VR on MB. Options available: Enabled/Disabled. Default setting is Enabled .
North Bridge	Press [Enter] for configuration of advanced items.
Fabric Resource	Press [Enter] for configuration of advanced items.

5-5-1 North Bridge



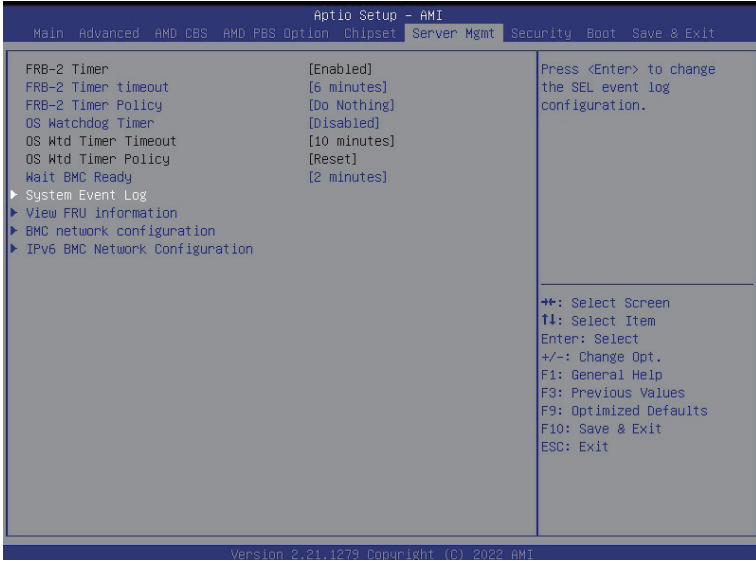
Parameter	Description
North Bridge Configuration	
Memory Information	
Total Memory	Displays the total memory information.
CPU0 Information	Press [Enter] to view information related to CPU 0.

5-5-2 Fabric Resource



Parameter	Description
Fabric Resource	
CPU0 NBIO_# PCIe Bus Number	Change CPU 0 NBIO_# PCIe Bus Number.

5-6 Server Management Menu



Parameter	Description
FRB-2 Timer	Display the FRB-2 Timer status. This item is not configurable.
FRB-2 Timer timeout	Configures the FRB2 Timer timeout. Options available: 3 minutes, 4 minutes, 5 minutes, 6 minutes. Default setting is 6 minutes .
FRB-2 Timer Policy	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	Configures OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is 10 minutes . Please note that this item is configurable when OS Watchdog Timer is set to Enabled.
OS Wtd Timer Policy	Configure OS Watchdog Timer Policy. Options available: Reset, Do Nothing, Power Down. Default setting is Reset . Please note that this item is configurable when OS Watchdog Timer is set to Enabled.

Parameter	Description
Wait BMC Ready	POST wait BMC ready and reboot system. Options available: Disabled/2 minutes/4 minutes/6 minutes. Default setting is 2 minutes .
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the FRU information.
BMC network configuration	Press [Enter] to configure advanced items.
IPv6 BMC Network Configuration	Press [Enter] to configure advanced items.

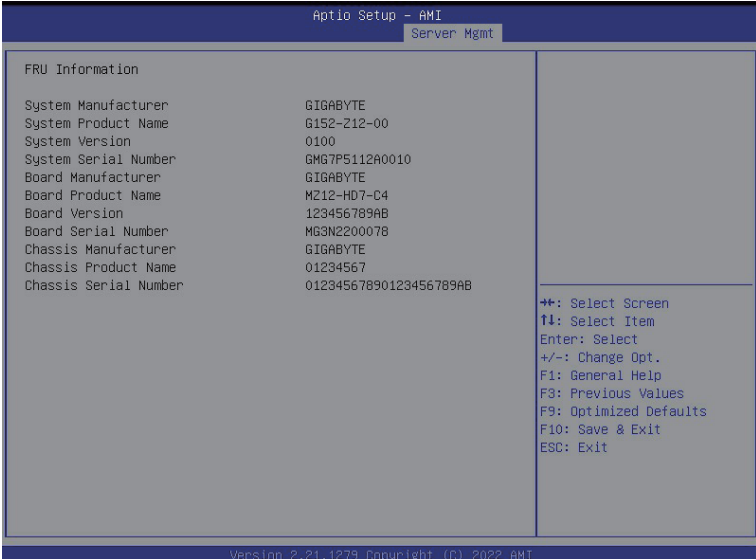
5-6-1 System Event Log



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/Erased Immediately. 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 and Progress code. Default setting is Error code .

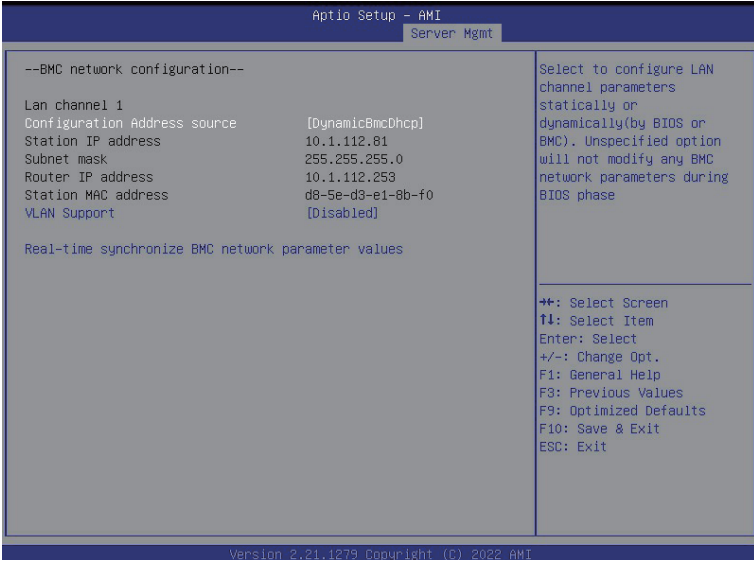
5-6-2 View FRU Information

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.



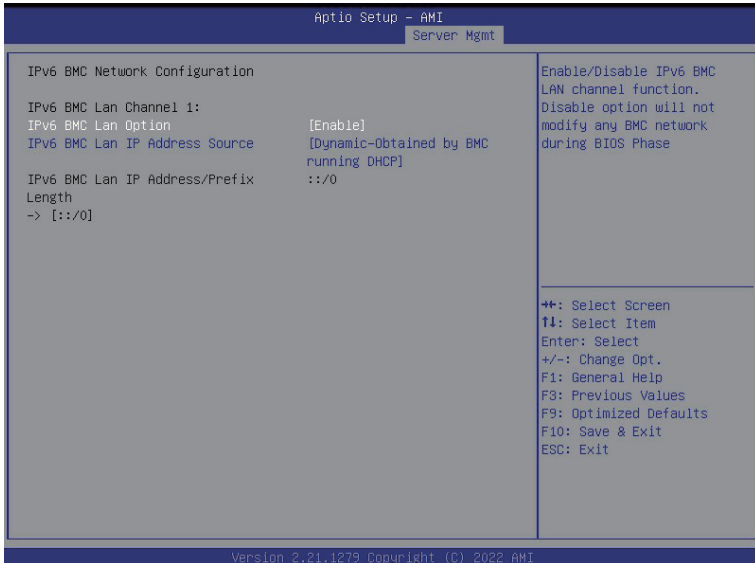
(Note) The model name will vary depends on the product you purchased

5-6-3 BMC Network Configuration



Parameter	Description
BMC network configuration	
Lan Channel 1	
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase. 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.
VLAN Support	Set to BMC enabled/disabled VLAN. Options available: Enabled, Disabled. Default setting is Disabled .
Real-time get BMC network address	Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.

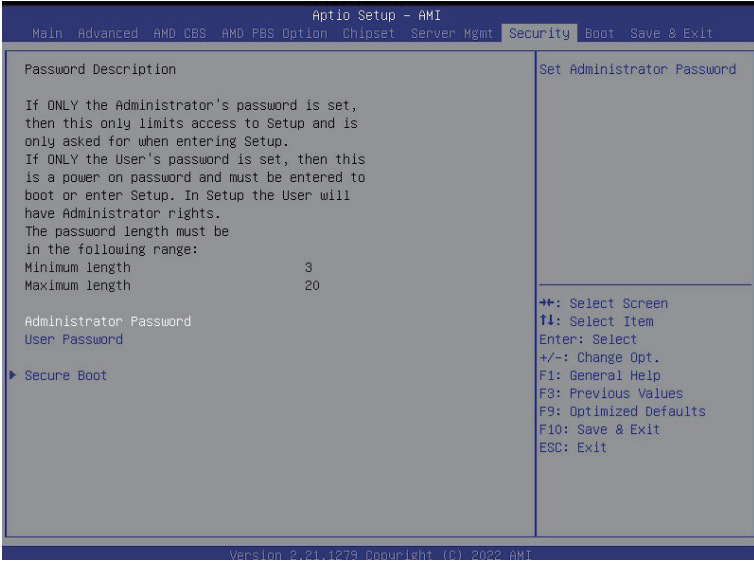
5-6-4 IPv6 BMC Network Configuration



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 Enable 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.

5-7 Security Menu

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



There are two types of passwords that you can set:

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

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

5-7-1 Secure Boot

The Secure Boot submenu is applicable when your device is installed the Windows® 8 (or above) operating system.



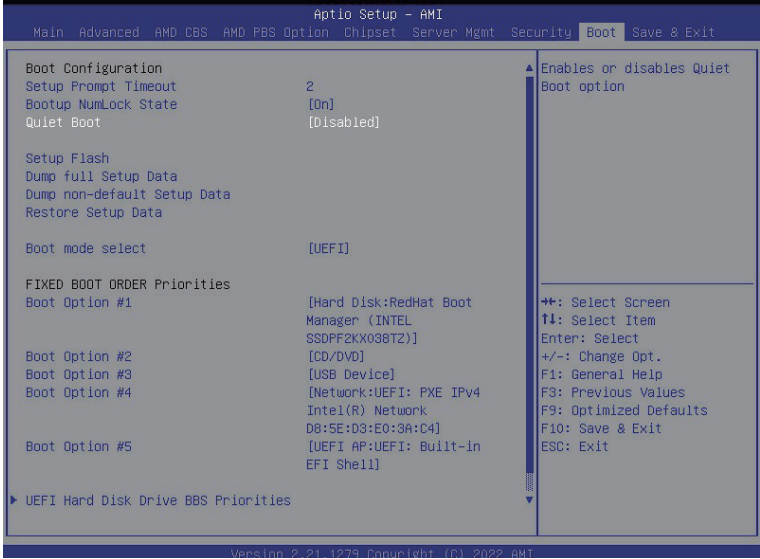
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available:Enabled/Disabled. Default setting is Disabled .
Secure Boot Mode ^(Note)	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before Windows 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 ^(Note)	
Enter Audit Mode	Enter Audit Mode workflow. Transitions from User to Audit. Mode will result in erasing of PK variable.

(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="367 326 899 352">– 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="367 409 601 431">– Options available: Yes/No. <li data-bbox="335 435 899 517">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 459 899 517">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). <li data-bbox="335 522 696 572">◆ Restore DB defaults <ul style="list-style-type: none"> <li data-bbox="367 545 696 572">– Restore DB variable to factory defaults. <li data-bbox="335 577 893 627">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 600 893 627">– Displays the current status of the variables used for secure boot. <li data-bbox="335 631 803 736">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 655 803 682">– Displays the current status of the Platform Key (PK). <li data-bbox="367 686 675 713">– Press [Enter] to configure a new PK. <li data-bbox="367 718 611 736">– Options available: Set New. <li data-bbox="335 741 941 878">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 765 941 846">– Displays the current status of the Key Exchange Key Database (KEK). <li data-bbox="367 851 904 854">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="367 859 675 878">– Options available: Set New/Append. <li data-bbox="335 882 904 1019">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 906 904 932">– Displays the current status of the Authorized Signature Database. <li data-bbox="367 937 946 987">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="367 992 675 1019">– Options available: Set New/Append. <li data-bbox="335 1023 899 1160">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1047 899 1074">– Displays the current status of the Forbidden Signature Database. <li data-bbox="367 1078 888 1128">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="367 1133 675 1160">– Options available: Set New/Append. <li data-bbox="335 1165 925 1301">◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li data-bbox="367 1188 925 1215">– Displays the current status of the Authorized TimeStamps Database. <li data-bbox="367 1219 904 1270">– Press [Enter] to configure a new DBT or load additional DBT from storage devices. <li data-bbox="367 1274 675 1301">– Options available: Set New/Append. <li data-bbox="335 1306 915 1434">◆ OsRecovery Signatures <ul style="list-style-type: none"> <li data-bbox="367 1329 915 1356">– Displays the current status of the OsRecovery Signature Database. <li data-bbox="367 1361 888 1411">– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices. <li data-bbox="367 1415 675 1434">– Options available: Set New/Append.

5-8 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 Off .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled/Disabled. Default setting is Enabled .
Boot mode select	Selects the boot mode. Options available: LEGACY/UEFI. Default setting is UEFI .

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

5-8-1 UEFI NETWORK Drive BBS Priorities

The UEFI network drive BBS priorities submenu allows you to specify the boot device priority from the available UEFI network drives during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



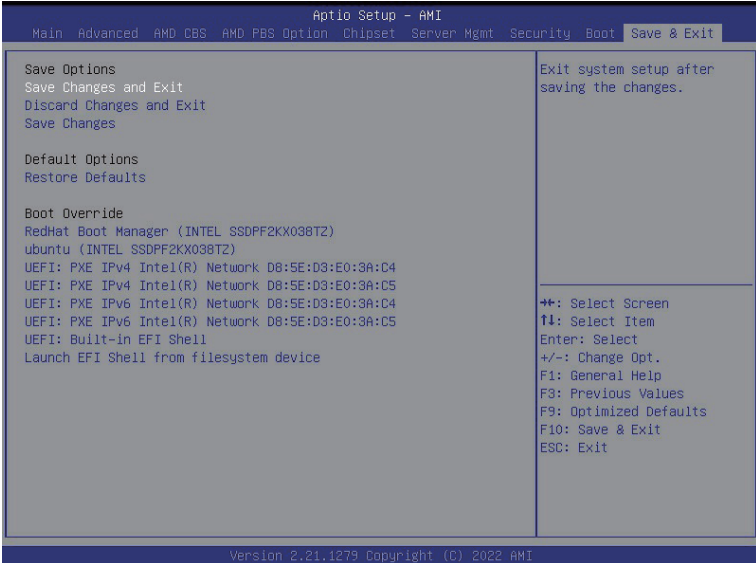
5-8-2 UEFI Application Boot Priorities

The UEFI application boot priorities submenu allows you to specify the boot device priority from the available UEFI applications during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



5-9 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 Changes 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	Saves changes done so far to any of the setup options. Options available: Yes/No.
Default Options	
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly. Options available: Yes/No.
Boot Override	Press [Enter] to configure the device as the boot-up drive.
Launch EFI Shell from filesystem device	Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

5-10 BIOS POST Beep code (AMI standard)

5-10-1 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

5-10-2 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

This page intentionally left blank