GIGABYTE™

G593-ZD1-AAX1

HPC/AI Server - AMD EPYC™ 9004 - 5U DP NVIDIA HGX™ H100 8-GPU

User Manual

Rev. 1.0

Copyright

© 2024 Giga Computing Technology CO., LTD. All rights reserved.
The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

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

Documentation Classifications

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

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

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

For More Information

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

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

For further technical assistance, please contact your GIGABYTE representative or visit https://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.

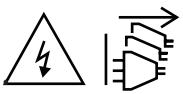
Server Warnings and Cautions

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.

WARNING!

The equipment should only be repaired, maintained or replaced by skilled personnel.

CAUTION!

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

CAUTION!

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

Electrostatic Discharge (ESD)

CAUTION!

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

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

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

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and discon-nect 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 sensi-tive 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 fin-gertips 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 dam-age the contacts inside the jumper, causing intermittent problems with the function con-trolled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

Table of Contents

Chapter 1 Hardware Installation 9
1-1 Installation Precautions 9
1-2 Product Specifications 10
1-3 System Block Diagram 14
1-4 PCIe Block Diagram 15
Chapter 2 System Appearance 16
2-1 Front View 16
2-2 Rear View 17
2-3 Top View 18
2-4 Front Panel LED and Buttons 19
2-4-1 RoT LEDs 20
2-5 Front Panel System LAN LEDs 22
2-6 Power Supply Unit (PSU) LED 23
2-7 Hard Disk Drive LEDs 24
Chapter 3 System Hardware Installation 25
3-1 Removing and Installing the Chassis Top Cover 26
3-2 Removing and Installing the GPU Tray 27
3-3 Removing the Heat Sink 28
3-4 Installing the CPU 29
3-5 Installing the Memory 30
3-5-1 Twelve Channel Memory Configuration 30
3-5-2 Installing the Memory 31
3-5-3 Processor and Memory Module Matrix Table 31
3-5-4 DIMM Population Table 32
3-6 Installing the M.2 Device and Heat Sink 33
3-7 Installing the PCI Expansion Card 34
3-8 Installing the Hard Disk Drive 36
3-9 Replacing the System Fan Module 37
3-10 Removing and Installing the Power Supply 38
3-11 Installing the System into the Cabinet 39
3-12 Removing the System from the Cabinet 40
3-13 Cable Connection 42
3-13-1 Motherboard to PCIe Board 42

3-13-2 Motherboard/Front IO Board to Rear Side FHHL Card Cable 44
3-13-3 Motherboard to PCIe Board and HDD Backplane Board 46
Chapter 4 Motherboard Components 48
4-1 Motherboard Components 48
4-2 Jumper Setting 50
4-3 Backplane Board Storage Connector 51
4-3-1 CBPG680 51
Chapter 5 BIOS Setup 52
5-1 The Main Menu 54
5-2 Advanced Menu 57
5-2-1 Trusted Computing 58
5-2-2 PSP Firmware Versions 59
5-2-3 Legacy Video Select 60
5-2-4 AST2600 Super IO Configuration 61
5-2-5 S5 RTC Wake Settings 63
5-2-6 Serial Port Console Redirection 64
5-2-7 CPU Configuration 68
5-2-8 PCI Subsystem Settings 69
5-2-9 USB Configuration 71
5-2-10 Network Stack Configuration 73
5-2-11 Post Report Configuration 74
5-2-12 NVMe Configuration 75
5-2-13 SATA Configuration 76
5-2-14 Graphic Output Configuration 77
5-2-15 AMD Mem Configuration Status 78
5-2-16 Tls Auth Configuration 79
5-2-17 RAM Disk Configuration 80
5-2-18 iSCSI Configuration 81
5-2-19 Intel(R) Ethernet Controller X710 for 10GBASE-T 82
5-2-20 VLAN Configuration 84
5-2-21 MAC IPv4 Network Configuration 85
5-2-22 MAC IPv6 Network Configuration 86
5-3 AMD CBS Menu 87
5-3-1 CPU Common Options 88
5-3-2 DF Common Options 94
5-3-3 UMC Common Options 101
5-3-4 NBIO Common Options 122
5-3-5 FCH Common Options 133
5-3-6 SOC Miscellaneous Control 142

5-3-7 CXL Common Options....144
5-4 AMD PBS Menu....145
5-4-1 RAS....146
5-5 Chipset Setup Menu....148
5-5-1 North Bridge....149
5-5-2 Fabric Resource....150
5-6 Server Management Menu....152
5-6-1 System Event Log....154
5-6-2 View FRU Information....155
5-6-3 BMC Network Configuration....156
5-6-4 IPv6 BMC Network Configuration....157
5-7 Security Menu....158
5-7-1 Secure Boot....159
5-8 Boot Menu....161
5-9 Save & Exit Menu....163
5-10 BIOS Recovery....164
5-11 BIOS POST Beep code (AMI standard)....165
5-11-1 PEI Beep Codes....165
5-11-2 DXE Beep Codes....165

Chapter 1 Hardware Installation

1-1 Installation Precautions

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

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

1-2 Product Specifications

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

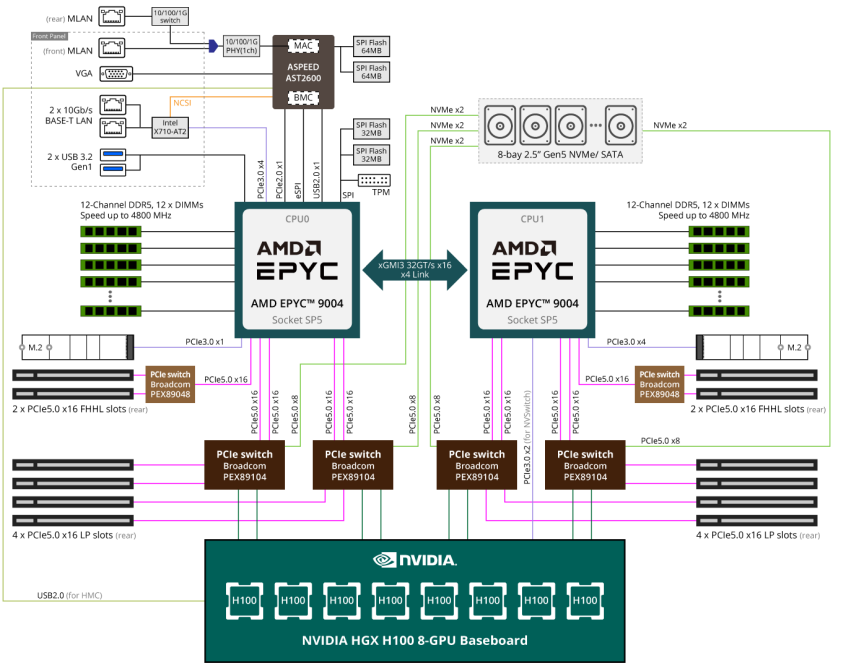
System Dimension	◆ 5U ◆ 447 x 219.7 x 945 (W x H x D, mm)
CPU	◆ AMD EPYC™ 9005 Series Processors ◆ AMD EPYC™ 9004 Series Processors ◆ Dual processor, cTDP up to 400W [1] [1] Please refer to the QVL on the support page or contact our sales representatives for verified CPU SKUs. [Note] If only 1 CPU is installed, some PCIe or memory functions might be unavailable.
Socket	◆ 2 x LGA 6096 ◆ Socket SP5
Chipset	◆ System on Chip
Security	◆ UEFI Secure Boot ◆ Silicon root of trust (Option) ◆ SNMP Support: V3
Memory	◆ 24 x DIMM slots ◆ DDR5 memory supported ◆ 12-Channel memory architecture ◆ RDIMM: Up to 4800 MT/s
LAN	**Front:** ◆ 2 x 10Gb/s LAN (1 x Intel® X710-AT2) - Support NCSI function ◆ 1 x 10/100/1000 Mbps Management LAN **Rear (MLAN board - CDB66):** ◆ 1 x 10/100/1000 Mbps Management LAN [Note] When both MLAN ports are connected with cables, the front MLAN port will be set as the default.
Video	◆ Integrated in Aspeed® AST2600 - 1 x VGA port

Storage	**Front hot-swap:** ◆ 8 x 2.5" Gen5 NVMe/**SATA/SAS-4** [1] - (NVMe from PEX89104) **Internal M.2:** ◆ 1 x M.2 (2280/22110), PCIe Gen3 x4, from CPU_1 ◆ 1 x M.2 (2280/22110), PCIe Gen3 x1, from CPU_0 [1] Storage card is required to support SATA and SAS drives.
SAS	◆ Require SAS add-in cards
RAID	◆ Require RAID add-in cards
Modular GPU	◆ NVIDIA HGX™ H100 with 8 x SXM5 GPUs
Expansion Slot	◆ **Extension Board CPBG044 x 2:** - 8 x LP x16 (Gen5 x16), from PEX89104 ◆ **Riser Card CPBGD20 x 2:** - 4 x FHHL x16 (Gen5 x16), from PEX89048
Front I/O	◆ 2 x USB 3.2 Gen1 ports (Type-A) ◆ 1 x VGA port ◆ 2 x RJ45 ports ◆ 1 x MLAN port (default) ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x NMI button ◆ 1 x Reset button ◆ 1 x Storage activity LED ◆ 1 x System status LED
Rear I/O	**MLAN board - CDB66:** ◆ 1 x MLAN port
Backplane Board	◆ Speed and bandwidth: PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s
Security Modules	◆ 1 x TPM header with SPI interface - **Optional** TPM2.0 kit: CTM010

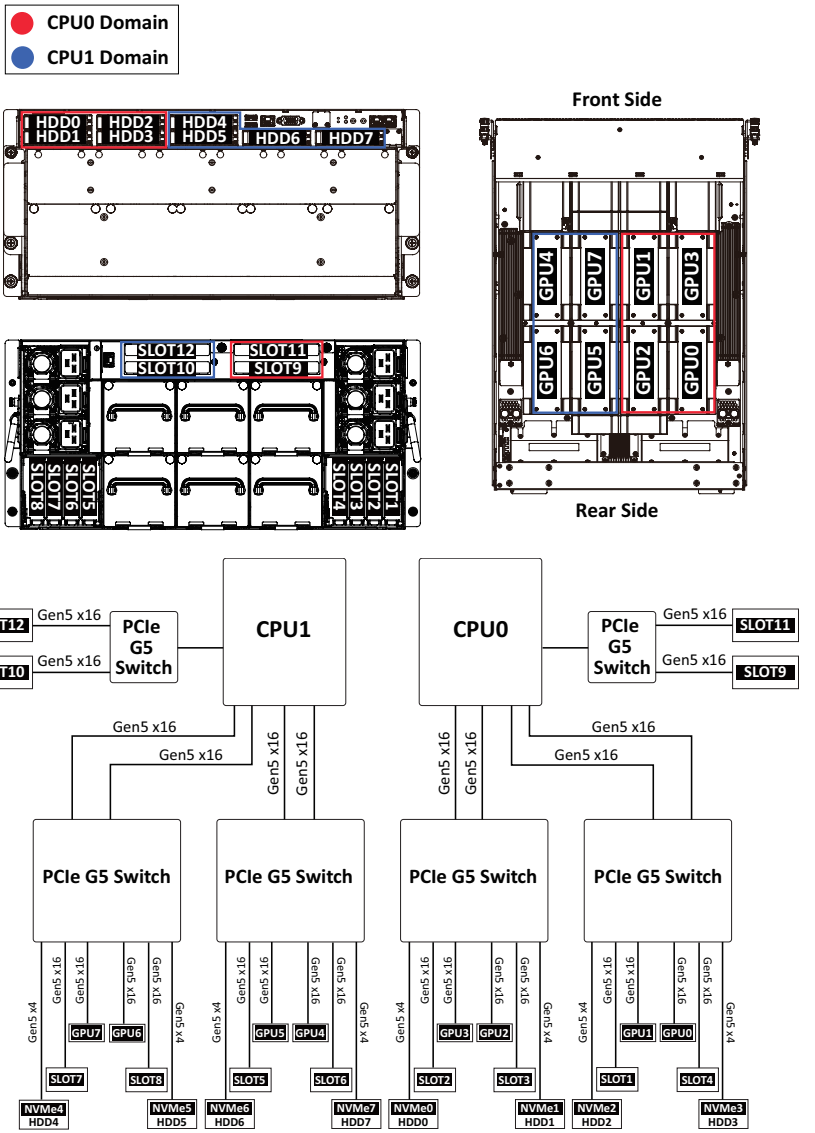
Power Supply	◆ 4+2 3000W 80 PLUS Titanium redundant power supplies [1] ◆ AC Input: - 115-127V~/ 14.2A, 50-60Hz - 200-220V~/ 15.8A, 50-60Hz - 220-240V~/ 14.9A, 50-60Hz ◆ DC Input: (Only for China) - 240Vdc/ 14A ◆ DC Output: - Max 1450W/ 115-127V~ +54V/ 26.6A +12Vsb/ 3A - Max 2900W/ 200-220V~ +54V/ 53.4A +12Vsb/ 3A - Max 3002.4W/ 220-240V~ or 240Vdc Input +54V/ 55.6A +12Vsb/ 3A [1] The system power supply requires C19 power cord.
System Management	Aspeed® AST2600 Baseboard Management Controller GIGABYTE Management Console web interface ◆ Dashboard ◆ HTML5 KVM ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status …etc.) ◆ Sensor Reading History Data ◆ FRU Information ◆ SEL Log in Linear Storage / Circular Storage Policy ◆ Hardware Inventory ◆ Fan Profile ◆ System Firewall ◆ Power Consumption ◆ Power Control ◆ Advanced power capping ◆ LDAP / AD / RADIUS Support ◆ Backup & Restore Configuration ◆ Remote BIOS/BMC/CPLD Update ◆ Event Log Filter ◆ User Management ◆ Media Redirection Settings ◆ PAM Order Settings ◆ SSL Settings ◆ SMTP Settings

System Fans	◆ Motherboard: - 2 x 40x40x56mm (32,000rpm) - 4 x 60x60x56mm (24,000rpm) ◆ PCIe slots: - 4 x 40x40x28mm (25,000rpm) - 2 x 40x40x56mm (32,000rpm) ◆ GPU tray: - 6 x 60x60x76mm (21,700rpm) - 11 x 80x80x80mm (17,000rpm)
Operating Properties	◆ Operating temperature: 10°C to 35°C ◆ Operating humidity: 8-80% (non-condensing) ◆ Non-operating temperature: -40°C to 60°C ◆ Non-operating humidity: 20%-95% (non-condensing)

1-3 System Block Diagram

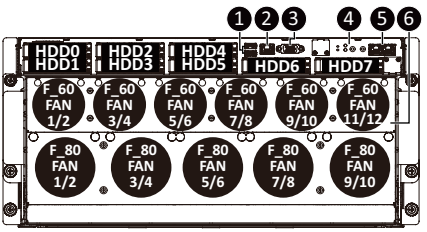


1-4 PCIe Block Diagram



Chapter 2 System Appearance

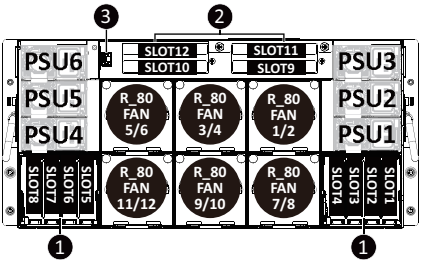
2-1 Front View



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

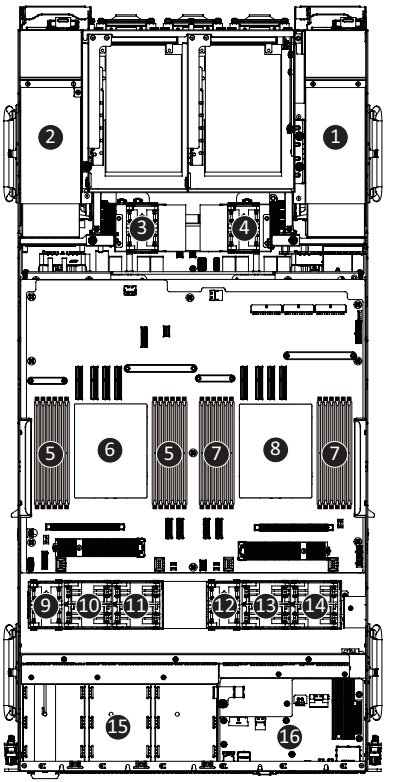
- Go to the section **2-4 Front Panel Buttons and LEDs** for detail description of function LEDs.

2-2 Rear View



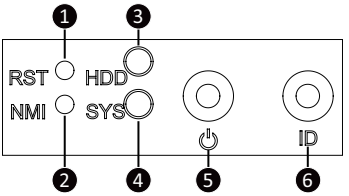
No.	Description
1.	PCIe Card Cage x 2
2.	PCIe Slot x 4
3.	Management LAN Port

2-3 Top View



No.	Description
1.	Power Supply Unit x 3 (Top)
	PCIe Slot x 4 (Bottom)
	Rear_BP_40_FAN_3/4 (Bottom)
2.	Power Supply Unit x 3 (Top)
	PCIe Slot x 4 (Bottom)
	Rear_BP_40_FAN_1/2 (Bottom)
3.	SYS_40_FAN5/6
4.	SYS_40_FAN7/8
5.	CPU0 DDR5 Memory
6.	CPU0
7.	CPU1 DDR5 Memory
8.	CPU1
9.	SYS_40_FAN1/2
10.	SYS_60_FAN1/2
11.	SYS_60_FAN3/4
12.	SYS_40_FAN3/4
13.	SYS_60_FAN5/6
14.	SYS_60_FAN7/8
15.	2.5” Storage Bays
16.	Front IO Board (Top)
	2.5” Storage Bays (Bottom)

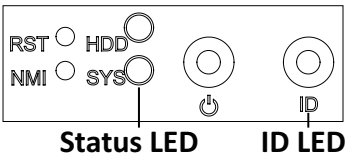
2-4 Front Panel LED and Buttons



No.	Name	Color	Status	Description
1.	Reset Button			Press the button to reset the system.
2.	NMI button			Press the button server generates a NMI to the processor if the multiple-bit ECC errors occur, which effectively halt the server.
3.	HDD Status LED	Green	On	HDD locate
			Blink	HDD access
		Amber	On	HDD fault
		Green/ Amber	Blink	HDD rebuilding
		N/A	Off	No HDD access or no HDD fault.
4.	System Status LED(Note)	Green	On	System is operating normally.
		Amber	On	Critical condition, may indicate: System fan failure System temperature
			Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion
		N/A	Off	System is not ready, may indicate: POST error NMI error Processor or terminator missing
5.	Power button with LED	Green	On	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)
6.	ID Button(Note)			Press the button to activate system identification

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

2-4-1 RoT LEDs



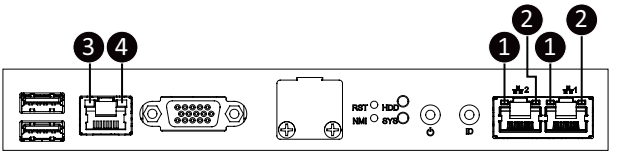
	LED on Front panel(Note5)	
	ID LED	Status LED
EC Firmware (FW) Authentication fail or not exit		
EC FW is broken or not exit (Note1)	OFF	OFF
Authenticating/Recovering BMC/BIOS Images		
Authenticating Images	OFF	OFF
Recovering BMC Active Flash	Blinks Blue 4 times per second	Blinks Green 4 times per second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

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

NOTE!

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

2-5 Front Panel System LAN LEDs

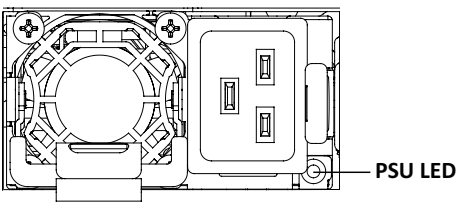


No.	Name	Color	Status	Description
1.	10GbE Speed LED	Green	On	10 Gbps data rate
		Yellow	On	5Gbps, 2.5Gbps, 1Gbps data rate
		N/A	Off	100 Mbps data rate
2.	10GbE Link / Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or reception is occurring.
		N/A	Off	No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

2-6 Power Supply Unit (PSU) LED

NOTE!

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



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

2-7 Hard Disk Drive LEDs

2.5" Drives



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

LED 2	HDD Present	No HDD
Green	ON	OFF

NOTE:

*1: Depends on HBA/Utility Spec.

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

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

Chapter 3 System Hardware Installation

Pre-installation Instructions

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

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

3-1 Removing and Installing the Chassis Top Cover

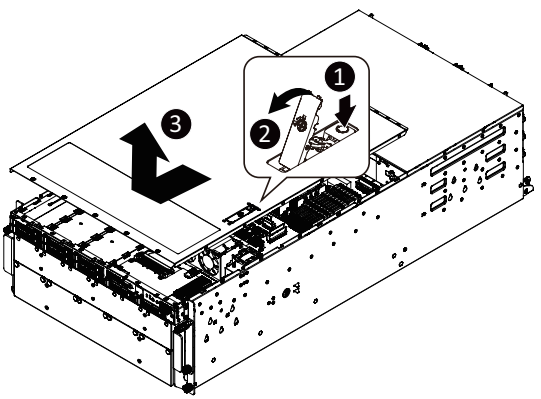
Before you remove or install the chassis top cover

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

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

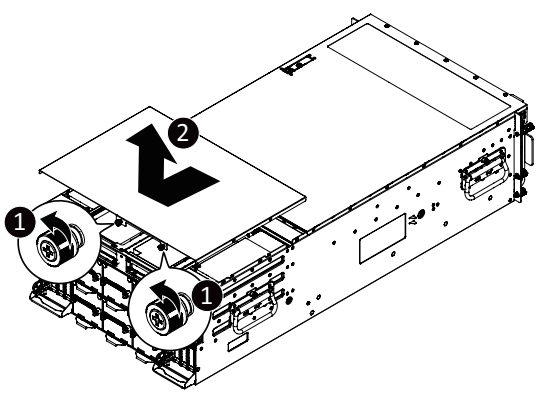
Front Cover

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



Rear Cover

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



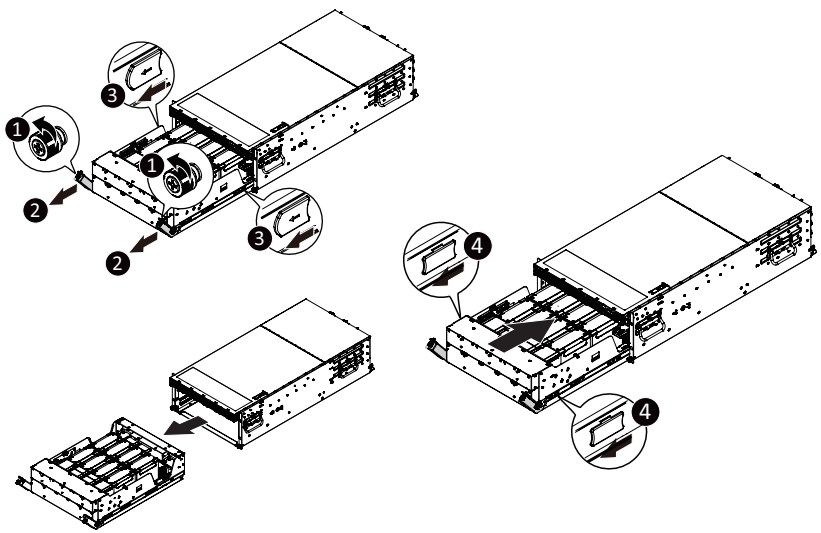
3-2 Removing and Installing the GPU Tray

Before you remove or install the GPU tray:

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

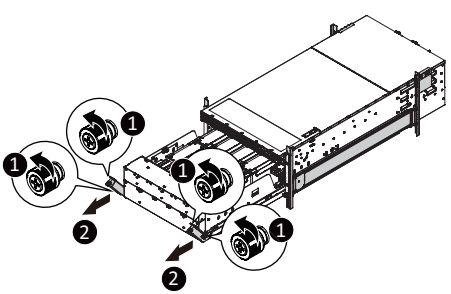
Follow these instructions to remove/install the GPU tray:

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



System in the cabinet

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



3-3 Removing the Heat Sink

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

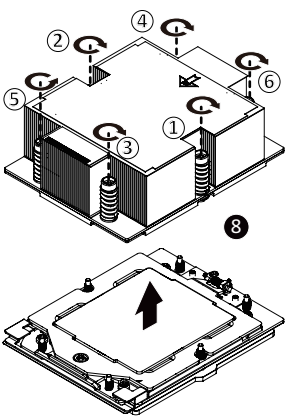
- Always turn off the computer and unplug the power cord from the power outlet before installing the heat sink to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open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

WARNING!

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

Follow these instructions to remove/install the heat sink:

1. Loosen the captive screws securing the heat sink in place in reverse order (6→5→4→3→2→1).
2. Lift and remove the heat sink from the system.
3. To reinstall the heat sink reverse steps 1-2 while ensuring that you tighten the captive screws in sequential order (1→2→3→4→5→6) as seen in the image below.



- When installing the heat sink to CPU, use a Torx T20 screwdriver to tighten 6 captive nuts in sequence as 1-6. Please refer to the Heat Sink Label for the screw tightening torque value.
- To ensure the system operates properly, make sure the heat sink is seated on the processor firmly.

3-4 Installing the CPU

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

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

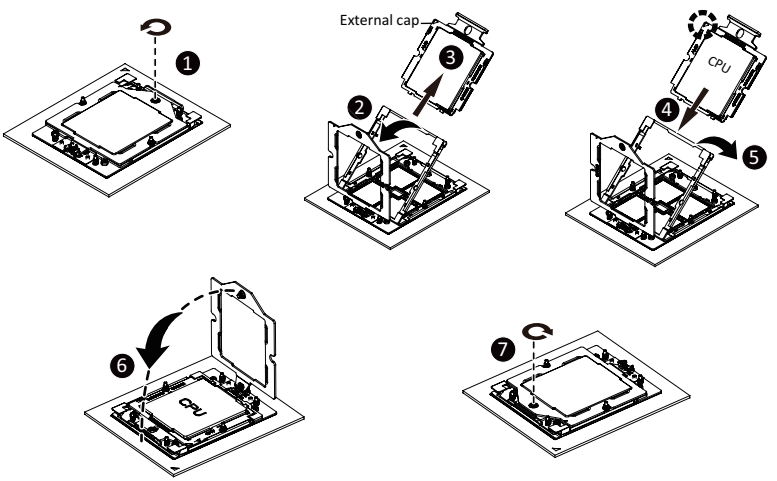
WARNING!

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

Follow these instructions to install the CPU:

1. Loosen the captive screw securing the CPU cover.
2. Flip open the CPU cover.
3. Remove the CPU carrier from the CPU frame using the handle on the CPU carrier.
4. Using the handle on the CPU carrier insert the new CPU carrier with CPU installed into the CPU frame.

   NOTE: Ensure the CPU is installed in the CPU carrier in the correct orientation, with the triangle on the CPU aligned to the top left corner of the CPU carrier.
5. Flip the CPU frame with CPU installed into place in the CPU socket.
6. Flip the CPU cover into place over the CPU socket.
7. Tighten the CPU cover screw to secure the CPU cover in place.



- Lock the CPU by using a Torx T20 screwdriver to tighten screw.
- Please refer to the Heat Sink Label for the screw tightening torque value.

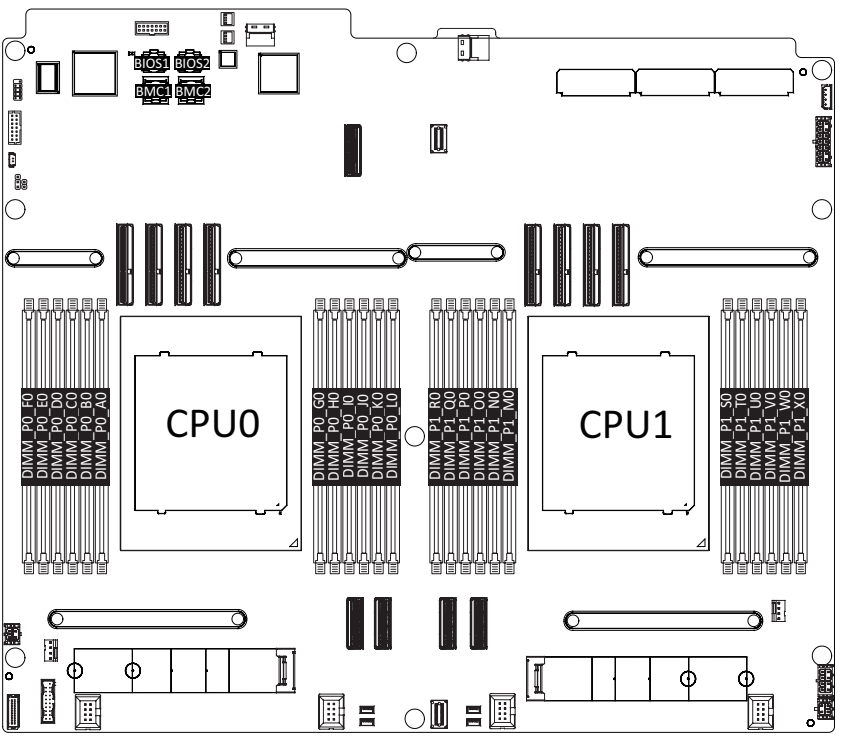
3-5 Installing the Memory

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

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

3-5-1 Twelve Channel Memory Configuration

This motherboard provides 24 DDR5 memory slots and supports 12-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



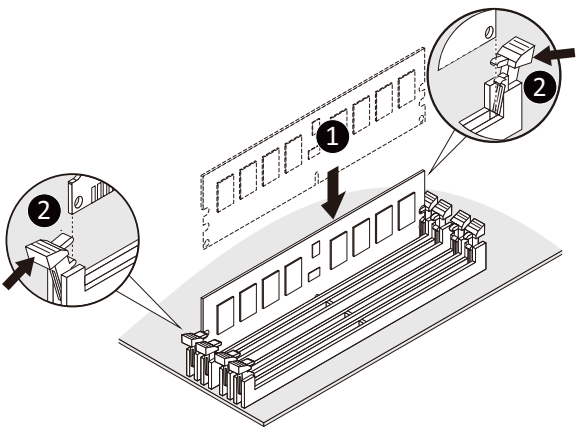
3-5-2 Installing the Memory

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

Be sure to install DDR5 DIMMs on this motherboard.

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.



3-5-3 Processor and Memory Module Matrix Table

Memory Q'ty	CPU0												CPU1											
for each CPU	F0	E0	D0	C0	B0	A0	G0	H0	I0	J0	K0	L0	R0	Q0	P0	O0	N0	M0	S0	T0	U0	V0	W0	X0
1 DIMM						v												v						
2 DIMM						v	v											v	v					
4 DIMM				v		v	v		v							v		v	v		v			
6 DIMM				v	v	v	v	v	v							v	v	v	v	v	v			
8 DIMM		v		v	v	v	v	v	v		v			v		v	v	v	v	v	v		v	
10 DIMM		v	v	v	v	v	v	v	v	v	v			v	v	v	v	v	v	v	v	v	v	
12 DIMM	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v

3-5-4 DIMM Population Table

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

DIMM Type	DIMM Population	Max EPYC 9004 DDR5 Frequency (MT/s)
	DIMM 0	
RDIMM	1R (1 Rank)	4800
	2R (2 Ranks)	4800
3DS RDIMM	2S2R (4 Ranks)	4800
	2S4R (8 Ranks)	4800
	2S8R (16 ranks)	4800

NOTE!

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

3-6 Installing the M.2 Device and Heat Sink

CAUTION

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

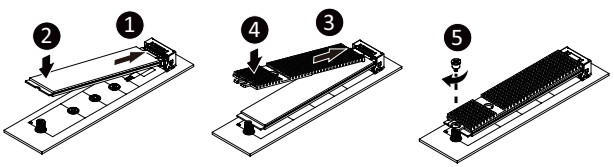
WARNING:

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

- To install/remove the M.2 module and Heat sink use a No. 1 Phillips-head screwdriver with a screw torque of 1.5 ± 0.2 kgf*cm

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

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



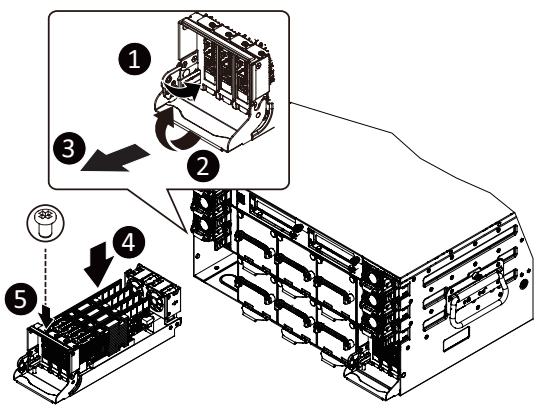
3-7 Installing the PCI Expansion Card

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

Follow these instructions for a PCI Expansion card:

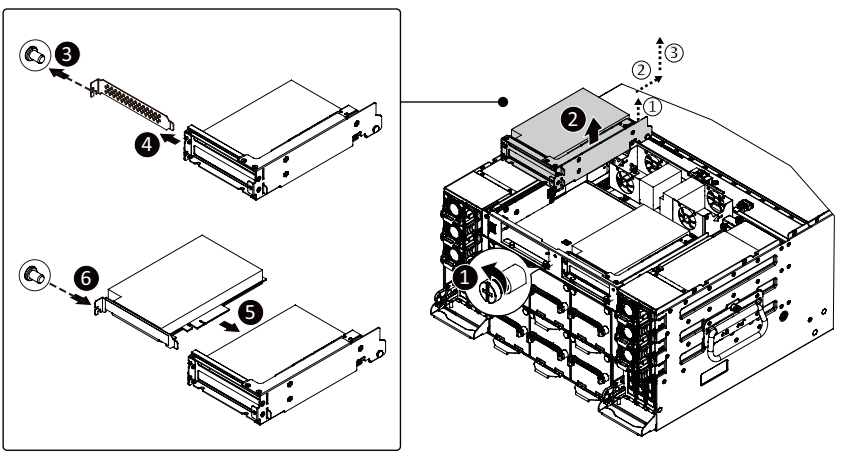
PCIe Card Cage

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



Rear System PCIe Card

1. Loosen the screw securing the riser bracket.
2. Gently lift the riser bracket. Then, move it backward and lift it upward.
3. Remove the screw securing the slot cover from the riser bracket.
4. Remove the slot cover from the riser bracket.
5. Orient the PCIe card with the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCIe card connector.
6. Secure the PCIe card with the screw.
7. Reverse the previous steps to install the riser bracket.



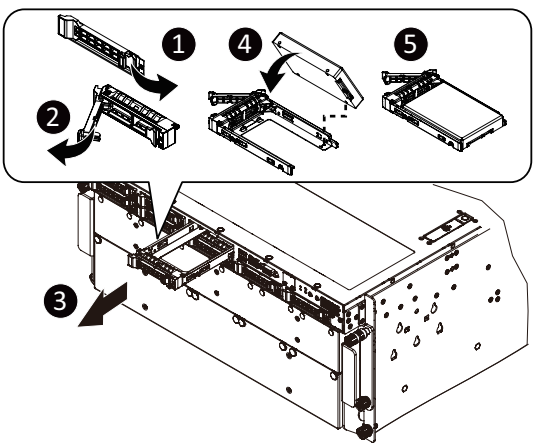
3-8 Installing the Hard Disk Drive

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

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

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

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



3-9 Replacing the System Fan Module

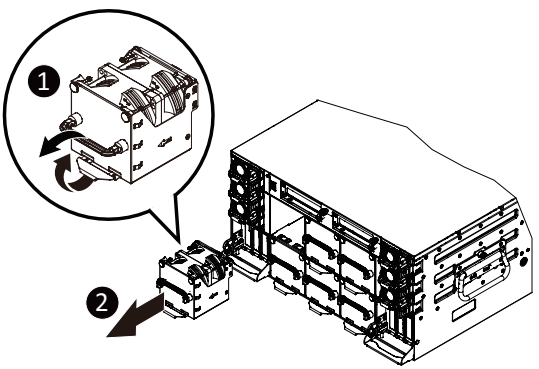
CAUTION!

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

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

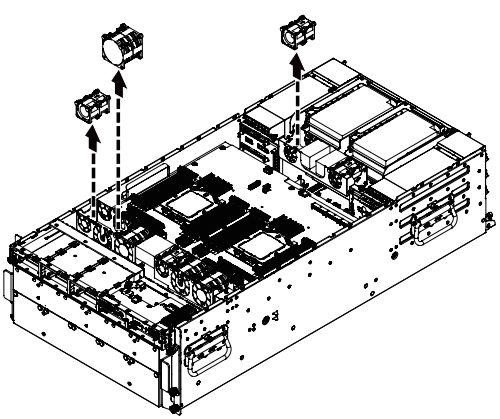
Follow these instructions to replace the fan assembly:

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



Internal System Fan

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



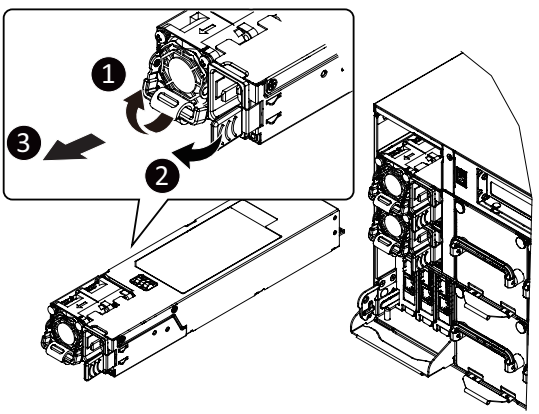
3-10 Removing and Installing the Power Supply

CAUTION!

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

Follow these instructions to replace the power supply:

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



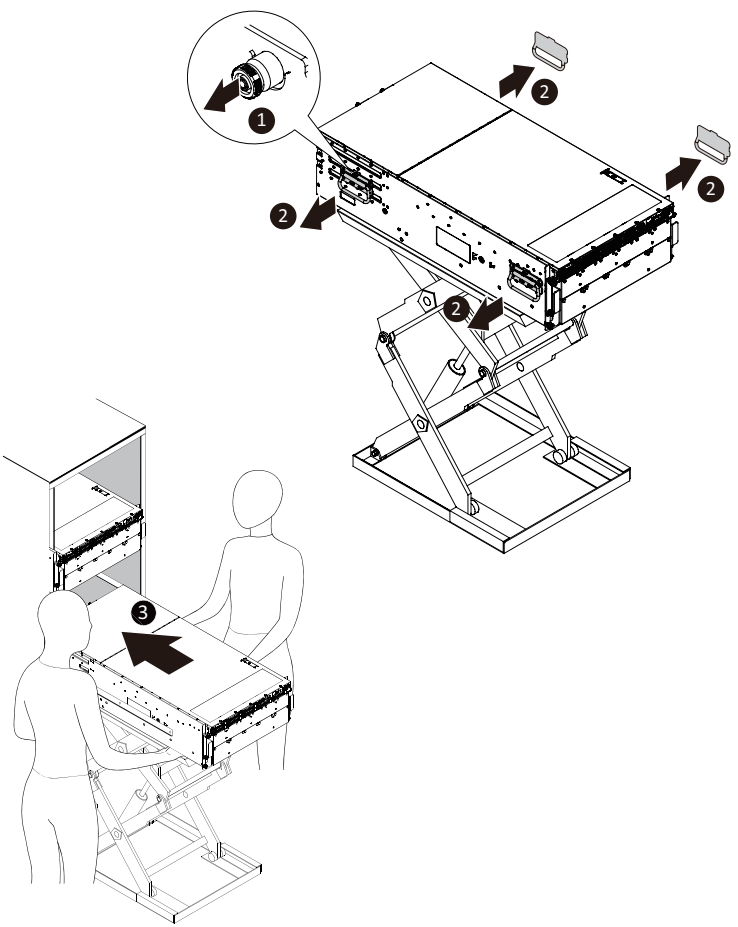
3-11 Installing the System into the Cabinet

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

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

Follow these instructions to install the system into the cabinet:

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



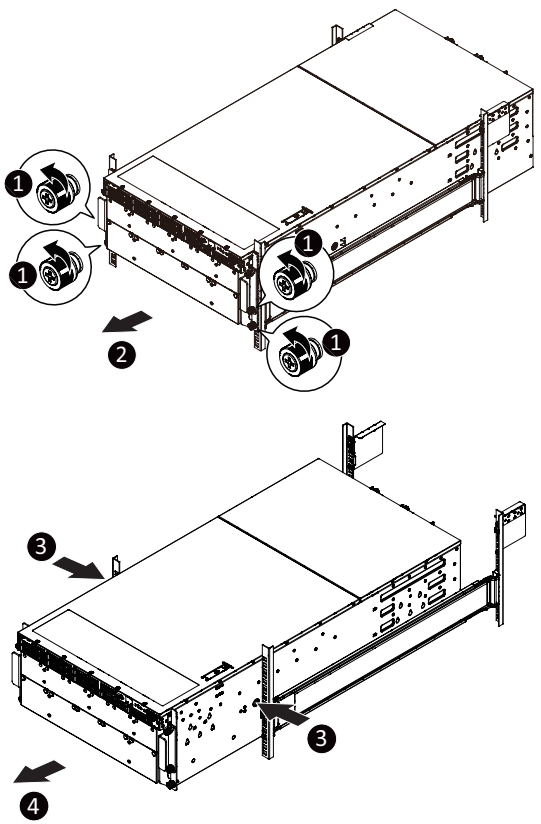
3-12 Removing the System from the Cabinet

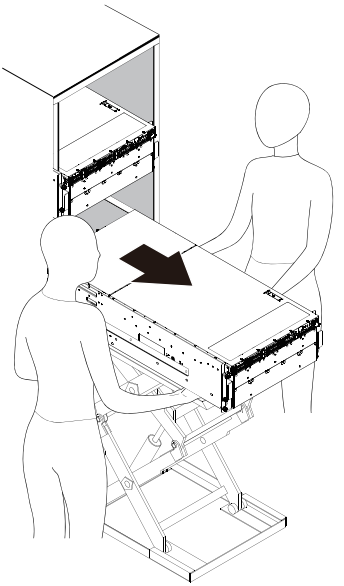
Read the following guidelines before you begin to remove the system from the cabinet:

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

Follow these instructions to remove the system from the cabinet:

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



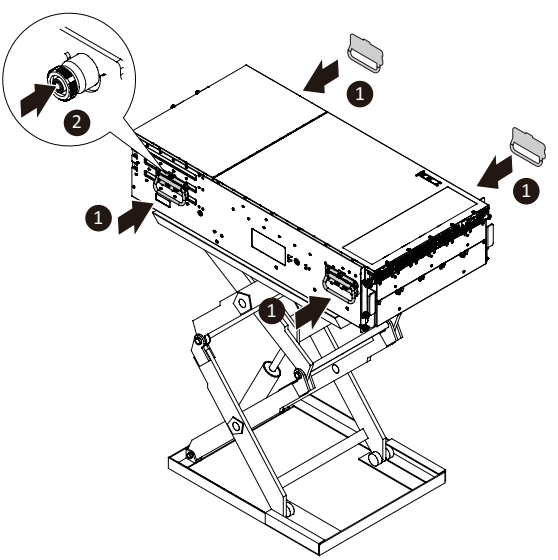


NOTE!

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

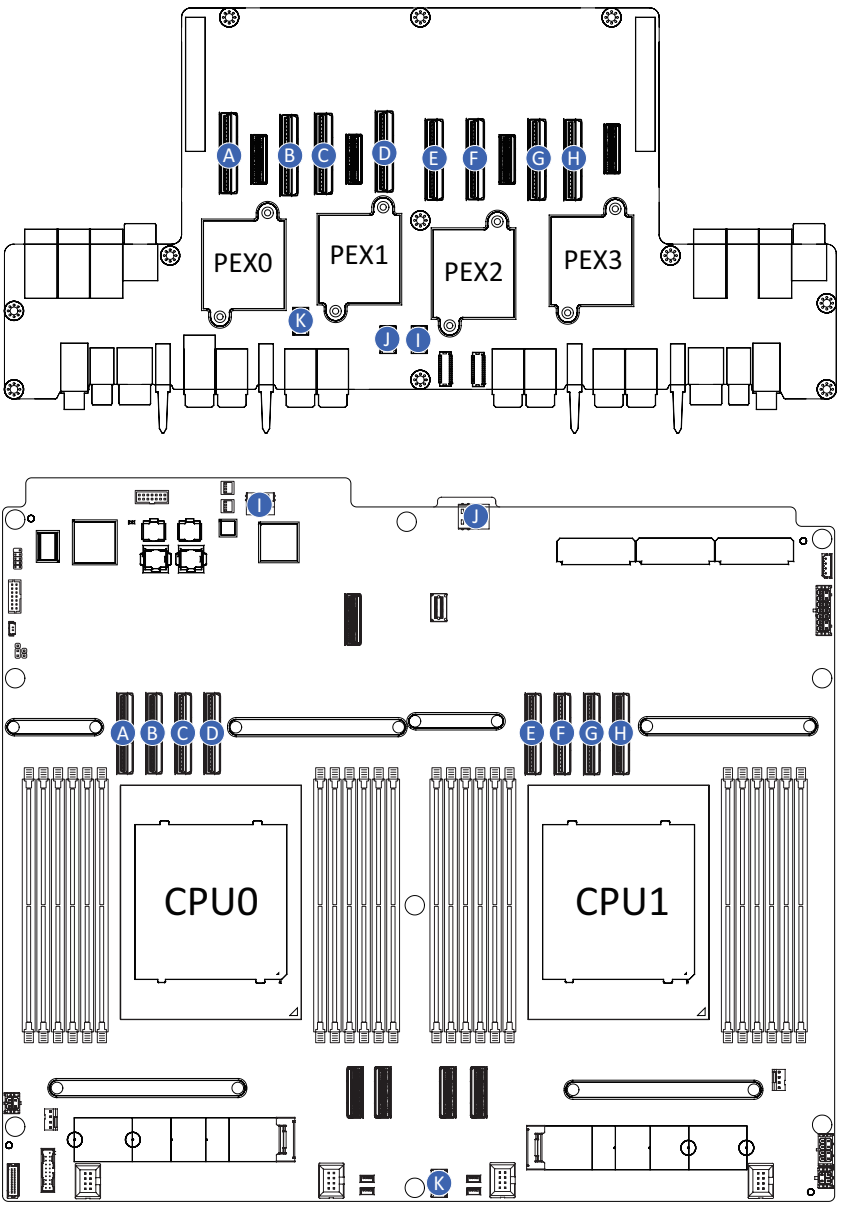
Follow these instructions to install the chassis handles on the system:

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



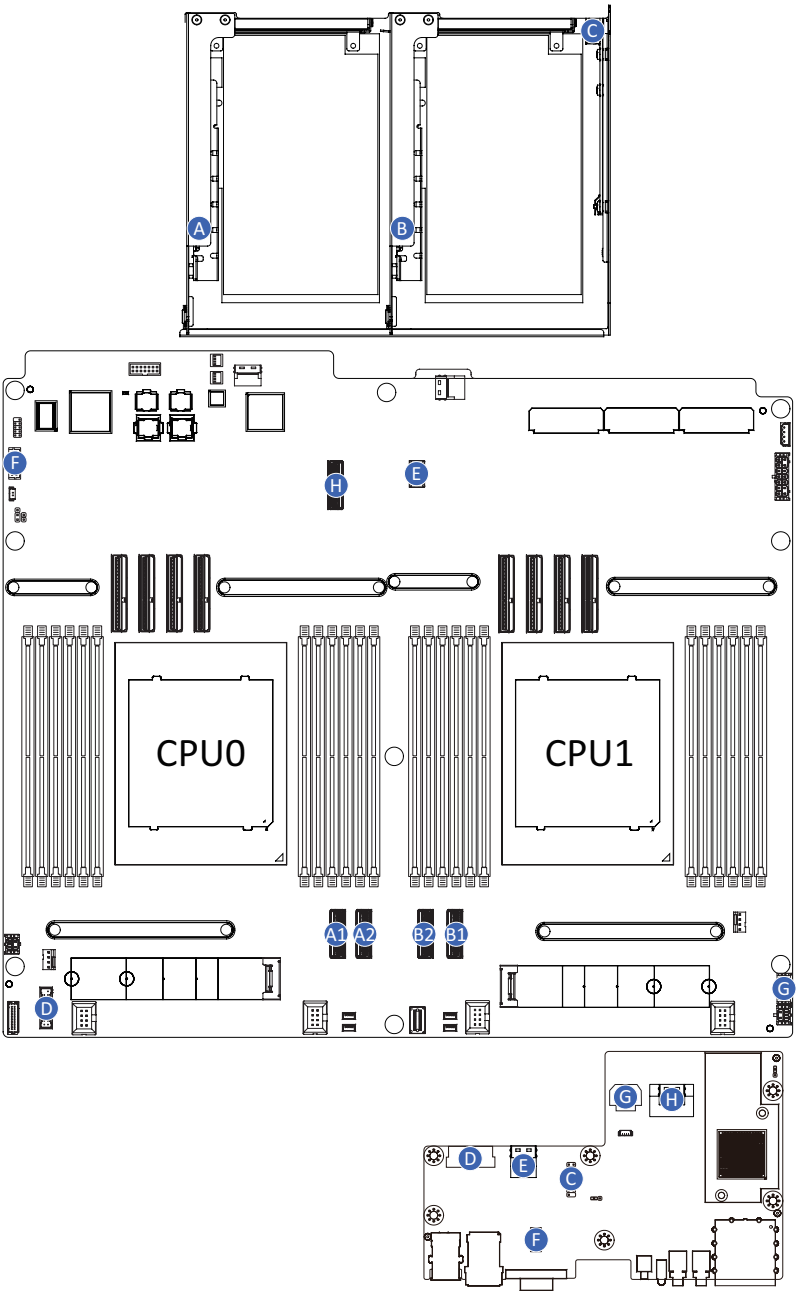
3-13 Cable Connection

3-13-1 Motherboard to PCIe Board



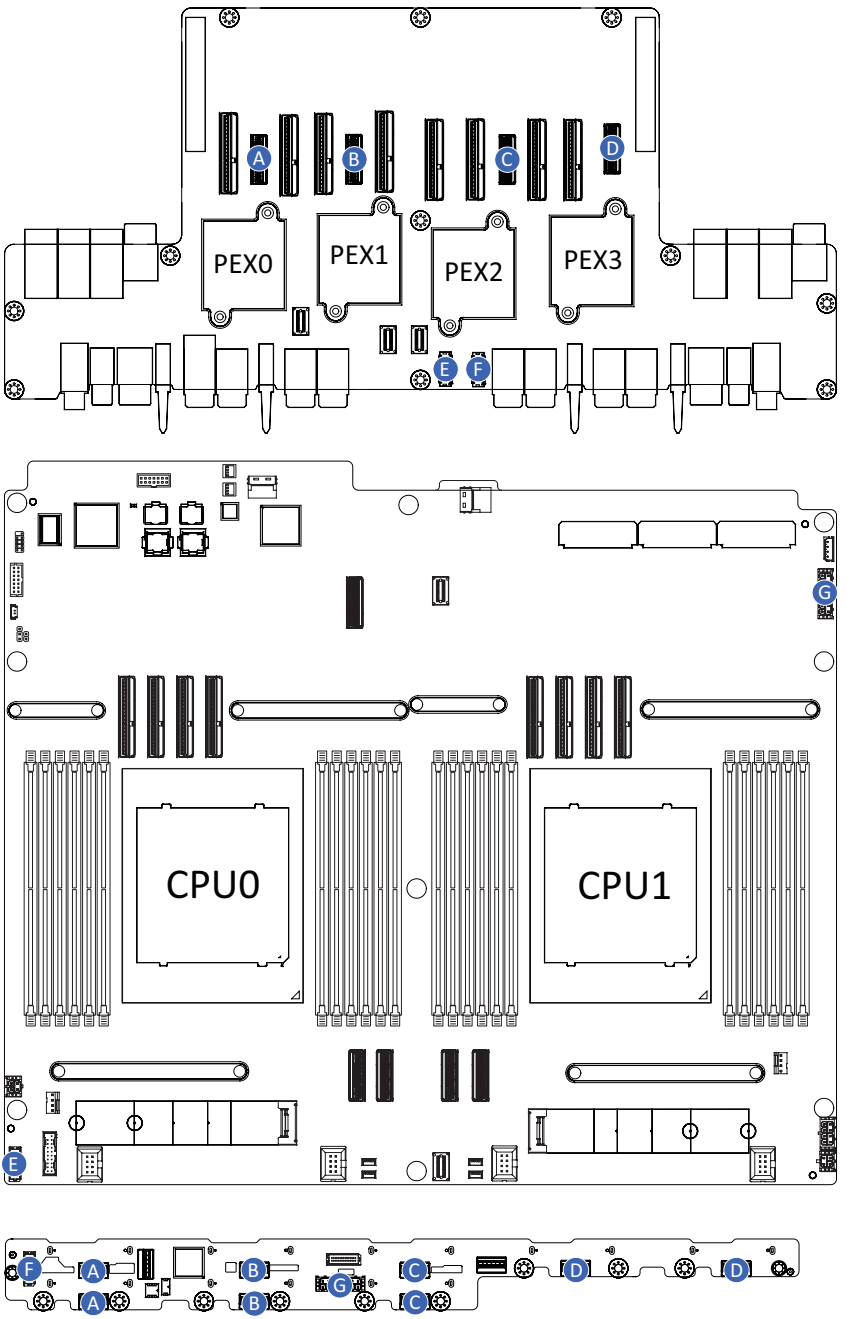
A	PCIe Slot Signal Cable	Motherboard: U2_P0_P0
		PCIe Board: U2_PEX0A
B	PCIe Slot Signal Cable	Motherboard: U2_P0_P1
		PCIe Board: U2_PEX0B
C	PCIe Slot Signal Cable	Motherboard: U2_P0_P2
		PCIe Board: U2_PEX1A
D	PCIe Slot Signal Cable	Motherboard: U2_P0_P3
		PCIe Board: U2_PEX1B
E	PCIe Slot Signal Cable	Motherboard: U2_P1_P0
		PCIe Board: U2_PEX2A
F	PCIe Slot Signal Cable	Motherboard: U2_P1_P1
		PCIe Board: U2_PEX2B
G	PCIe Slot Signal Cable	Motherboard: U2_P1_P2
		PCIe Board: U2_PEX3B
H	PCIe Slot Signal Cable	Motherboard: U2_P1_P3
		PCIe Board: U2_PEX3A
I	Baseboard Management Cable	Motherboard: DELTA1
		PCIe Board: DELTA
J	Power Board Side Band Signal Cable	Motherboard: PDB_IO
		PCIe Board: PDB_IO
K	Baseboard Management Cable	Motherboard: DELTA_UP
		PCIe Board: U2_NVS

3-13-2 Motherboard/Front IO Board to Rear Side FHHL Card Cable



A	PCIe Slot Signal Cable	Motherboard: U2_P0_G3A1/ U2_P0_G3B1
		Riser Card: U2_1 (SLOT9/ SLOT11)
B	PCIe Slot Signal Cable	Motherboard: U2_P1_G1A1/ U2_P1_G1B1
		Riser Card: U2_1 (SLOT10/ SLOT12)
C	Rear Side MLAN Cable	Front IO Board: REAR_LAN
		Rear MLAN
D	USB Cable	Motherboard: F_USB1
		Front IO Board: F_USB3_CON
E	Management LAN Signal Cable	Motherboard: U2_11
		Front IO Board: U2_2
F	VGA Cable	Motherboard: VGA_CON
		Front IO Board: F_VGA1_CON
G	Front Board Power Cable	Motherboard: FP_PWR1
		Front IO Board: P12V_2
H	Data LAN Signal Cable	Motherboard: U2_8
		Front IO Board: U2_1

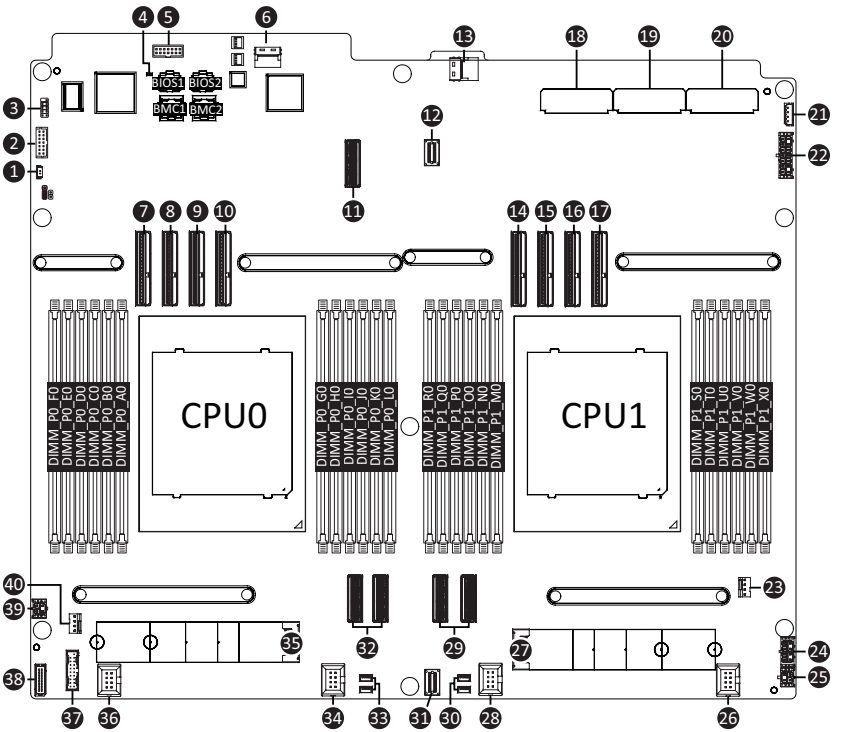
3-13-3 Motherboard to PCIe Board and HDD Backplane Board



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

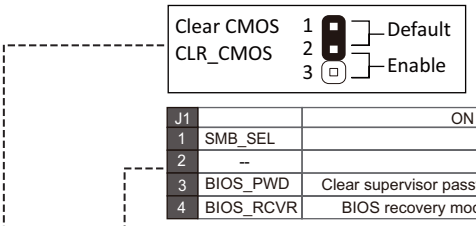
Chapter 4 Motherboard Components

4-1 Motherboard Components

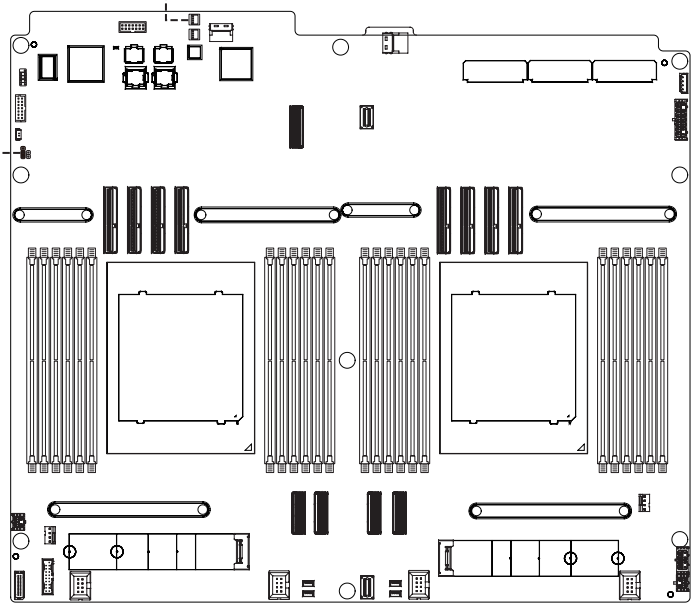


Item	Description
1	Battery Cable Connector
2	VGA Connector
3	Serial Port Header
4	BMC Firmware Readiness LED
5	TPM Module Connector
6	SlimLine Connector (for Delta Module Link)
7	MCIO Connector (U2_P0_P0/PCIe Gen5)
8	MCIO Connector (U2_P0_P1/PCIe Gen5)
9	MCIO Connector (U2_P0_P2/PCIe Gen5)
10	MCIO Connector (U2_P0_P3/PCIe Gen5)
11	MCIO Connector (for System I/O)
12	SlimLine Connector (for MLAN)
13	SlimLine Connector (for Power Board Side Band Signal)
14	MCIO Connector (U2_P1_P0/PCIe Gen5)
15	MCIO Connector (U2_P1_P1/PCIe Gen5)
16	MCIO Connector (U2_P1_P2/PCIe Gen5)
17	MCIO Connector (U2_P1_P3/PCIe Gen5)
18	CPU0 Power Connector
19	CPU1 Power Connector
20	System Power Connector
21	IPMB Connector
22	2 x 7 Pin HDD Backplane Board Power Connector
23	CPU1 Fan Connector (for CPU1 Heatsink)
24	2 x 4 Front IO Board Power Connector
25	2 x 2 Pin PCIE2 Power Connector
26	FAN_11_12 Connector
27	M.2 Slot (PCIe Gen3 x4, Support NGFF-22110)
28	FAN_9_10 Connector
29	MCIO Connector (U2_P1_G1B1/U2_P1_G1A1/PCIe Gen5)
30	FAN_7/FAN_8 Connector
31	SlimLine Connector (for Delta Module Link)
32	MCIO Connector (U2_P0_G3A1/U2_P0_G3B1/PCIe Gen5)
33	FAN_5/FAN_6 Connector
34	FAN_3_4 Connector
35	M.2 Slot (PCIe Gen3 x1, Support NGFF-22110)
36	FAN_1_2 Connector
37	Front USB 3.2 Gen1 Connector
38	HDD Backplane Board Connector
39	2 x 2 Pin PCIE3 Power Connector
40	CPU0 Fan Connector (for CPU0 Heatsink)

4-2 Jumper Setting

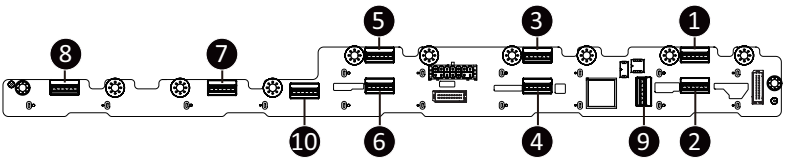


J1		ON	OFF
1	SMB_SEL	BIOS Defined	
2	--	--	
3	BIOS_PWD	Clear supervisor password	Normal [Default]
4	BIOS_RCVR	BIOS recovery mode	Normal [Default]



4-3 Backplane Board Storage Connector

4-3-1 CBPG680



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

Chapter 5 BIOS Setup

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

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



- BIOS flashing is potentially risky, if you do not encounter any problems when using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 1 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

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

- **Main**
  This setup page includes all the items of the standard compatible BIOS.
- **Advanced**
  This setup page includes all the items of AMI BIOS special enhanced features.
  (ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)
- **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

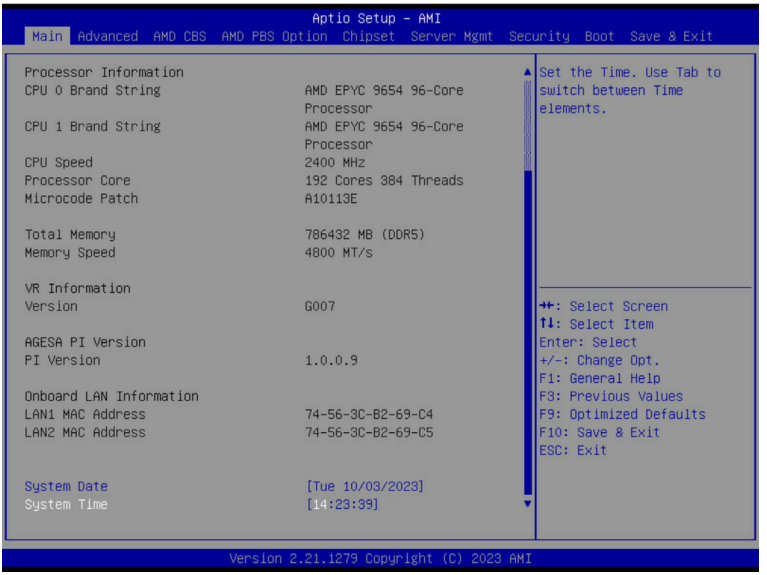
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

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.





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

(Note1) Functions available on selected models.

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

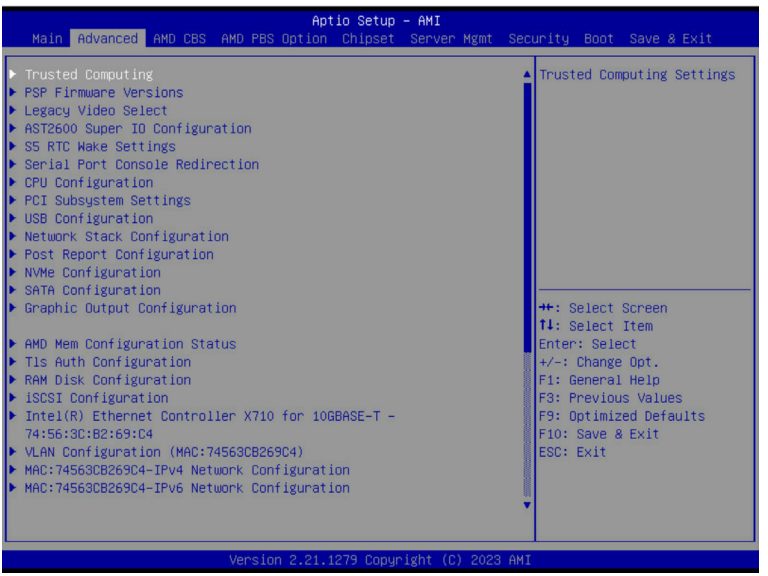
Parameter	Description
Onboard LAN Information	
LAN1/LAN2 MAC Address(Note)	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

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

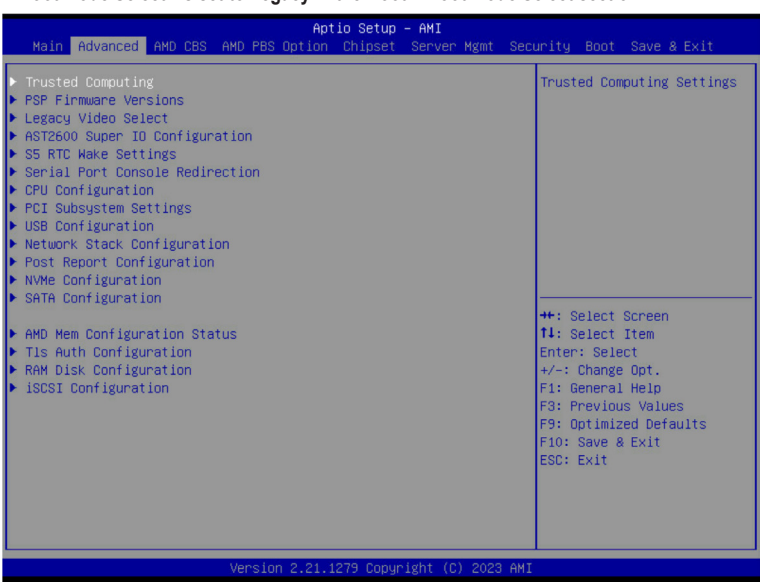
5-2 Advanced Menu

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

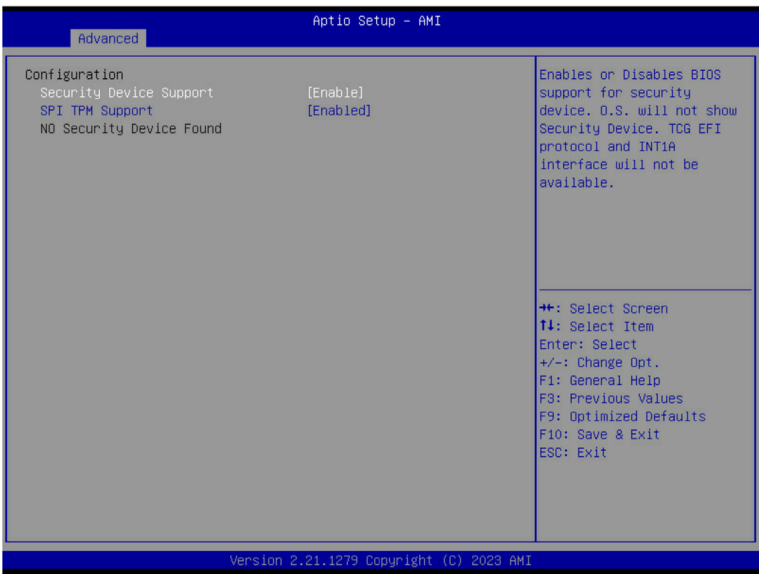
When Boot Mode Select is set to UEFI (Default)



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



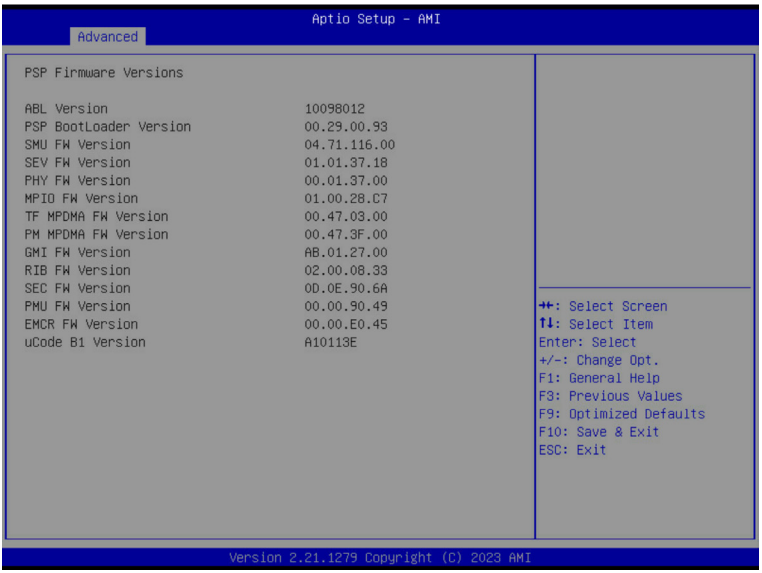
5-2-1 Trusted Computing



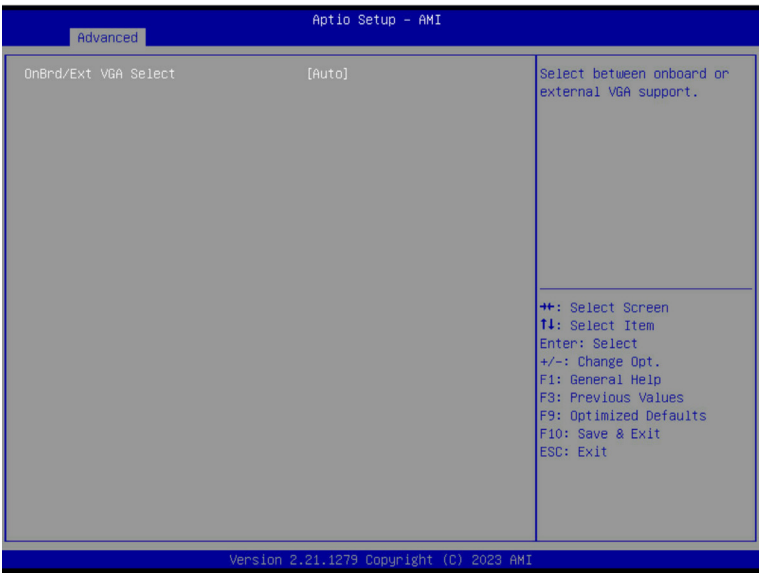
Parameter	Description
Configuration	
Security Device Support	Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. Options available: Disable, Enable. Default setting is **Enable**.
SPI TPM Support	Select Enable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

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	Selects between onboard or external VGA support. Options available: Auto, Onboard, External. Default setting is **Auto**.

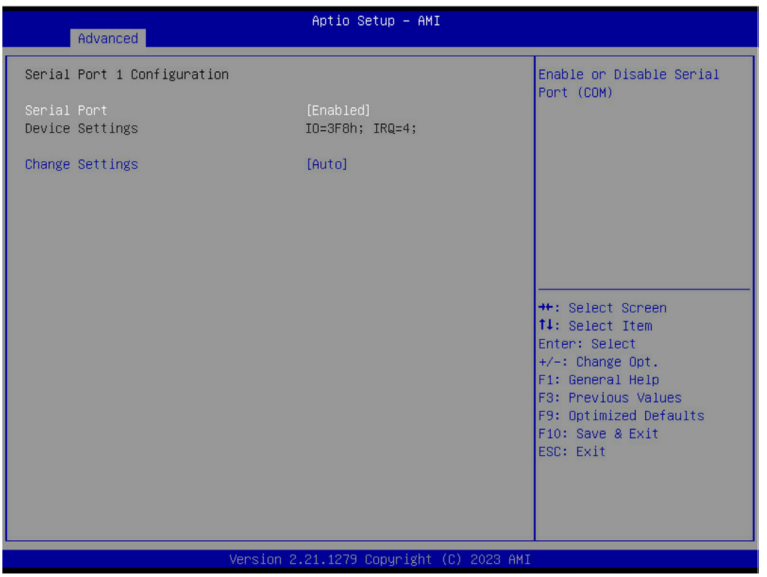
(Note) This configurable option will be displayed when **"Boot Mode Select"** is set to **Legacy** in the **Boot > Boot Mode Select section.**

5-2-4 AST2600 Super IO Configuration



Parameter	Description
AST2600 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(Note)	Enable/Disable the Serial Port (COM). When set to Enabled allows you to configure the Serial port 1 settings. When set to Disabled, displays no configuration for the serial port. Options available: Disabled, Enabled. Default setting is **Enabled**.
Devices Settings	Displays the Serial Port 1 device settings.
Change Settings	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**.

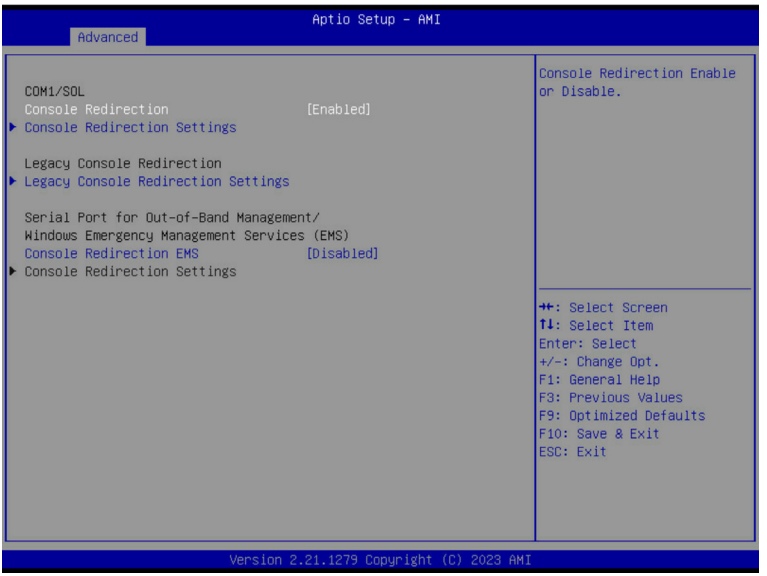
(Note) Advanced items prompt when this item is defined.

5-2-5 S5 RTC Wake Settings



Parameter	Description
Wake System from S5	Enable/Disable system wake on alarm event. Options available: Disabled, Fixed Time, Dynamic Time. When Fixed Time is selected, system will wake on the hr::min::sec specified. Default setting is **Disabled**.

5-2-6 Serial Port Console Redirection



Parameter	Description
COM1/Serial Over LAN Console Redirection(Note)	Select whether to enable console redirection for specified device. Console redirection enables the users to manage the system from a remote location. Options available: Enabled, Disabled. Default setting is **Disabled**.
COM1/Serial Over LAN Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when COM1/Serial Over LAN Console Redirection is set to Enabled.** ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100Plus, ANSI, VT-UTF8. Default setting is **VT100Plus**. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is **115200**. ◆ Data Bits – 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.

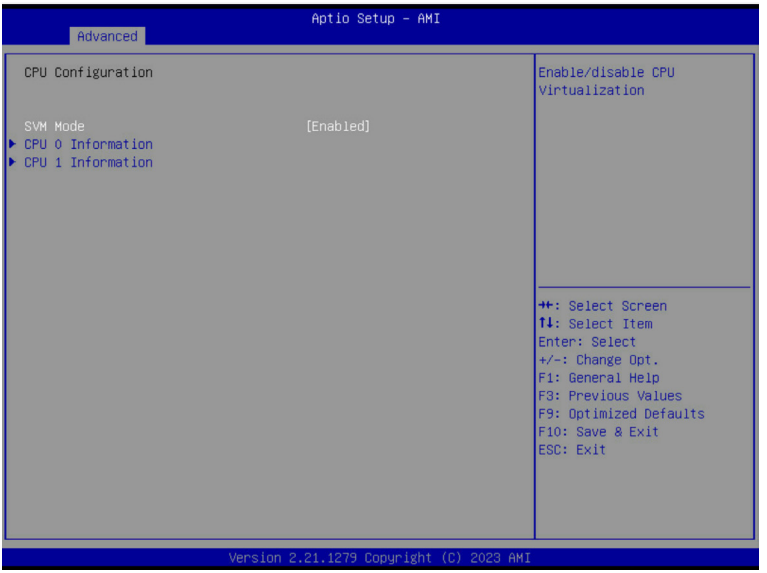
Parameter	Description
COM1/Serial Over LAN Console Redirection Settings (continued)	◆ Parity – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: parity bit is 0 if num of 1's in the data bits is odd. – 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 – 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 – 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 – Enable/Disable the VT-UTF8 Combo Key Support. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Recorder Mode – 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 – Enable/Disable extended terminal resolution. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Putty KeyPad – Selects Function Key and KeyPad on Putty. – Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is **VT100**.

Parameter	Description
Legacy Console Redirection	
Legacy Console Redirection Settings	Press [Enter] to configure advanced items. ◆ Redirection COM Port – Selects a COM port for Legacy serial redirection. – Default setting is **COM1/SOL**. ◆ Resolution – 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 – 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)	EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management. Options available: Disabled, Enabled. Default setting is **Disabled**.
Serial Port for Out-of-Band EMS Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.** ◆ Out-of-Band Mgmt Port – Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Default setting is **COM1/SOL**. ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100Plus, ANSI, VT-UTF8. Default setting is **ANSI**. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 57600, 115200. Default setting is **115200**.

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

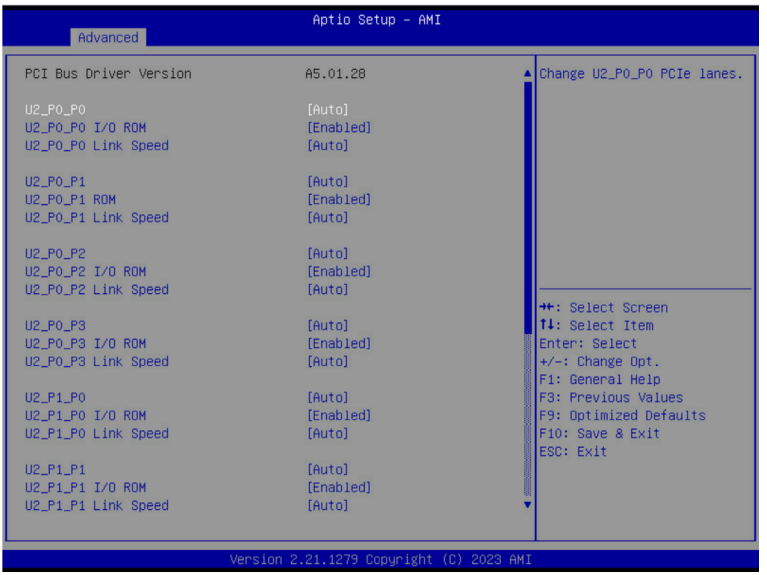
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	◆ Flow Control – Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, 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**.

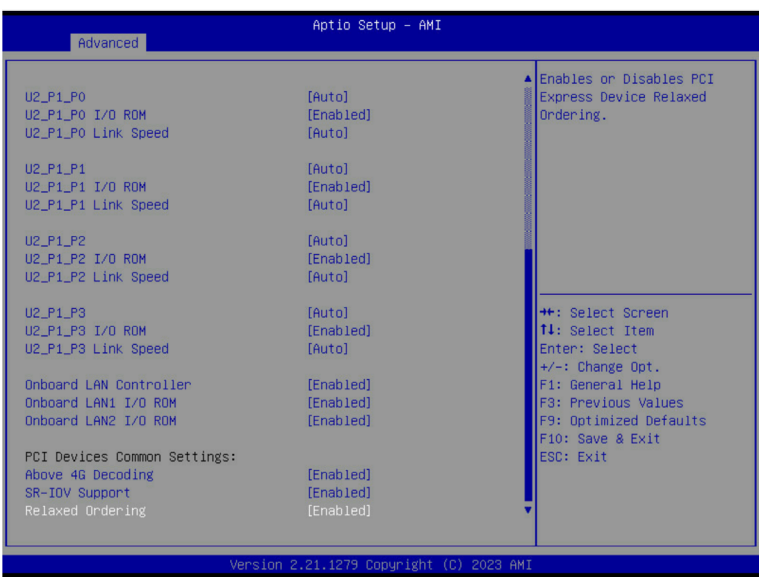
5-2-7 CPU Configuration



Parameter	Description
SVM Mode	Enable/Disable the CPU Virtualization. Options available: Disabled, Enabled. Default setting is **Enabled**.
CPU 0/1 Information	Press [Enter] to view the memory information related to CPU 0/1.

5-2-8 PCI Subsystem Settings



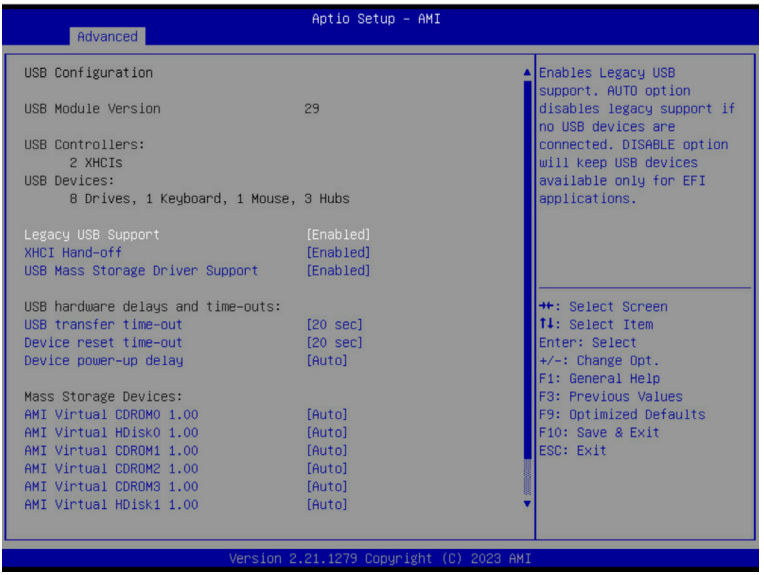


Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
U2_P0_P#/G#, U2_P1_P#/G#(Note1)	Change the MCIO PCIe lanes. Options available: Disabled, Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is **Auto**.
U2_P0_P#/G#, U2_P1_P#/G# I/O ROM(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Disabled, Enabled. Default setting is **Enabled**.
U2_P0_P#/G#, U2_P1_P#/G#(Link Speed(Note1)	Configure MCIO PCIe max link speed. Options available: Auto, Gen4, Gen3, Gen2, Gen1. Default setting is **Auto**.
Onboard LAN Controller(Note2)	Enable/Disable the onboard LAN devices. Options available: Disabled, Enabled. Default setting is **Enabled**.
Onboard LAN# I/O ROM(Note2)	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available: Disabled, Enabled. 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: Disabled, Enabled. 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: Disabled, Enabled. Default setting is **Enabled**.
Relaxed Ordering	Enable/Disable PCI express device relaxed ordering. Options available: Disabled, Enabled. Default setting is **Enabled**.

(Note1) This section is dependent on the available MCIO connector.

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

5-2-9 USB Configuration

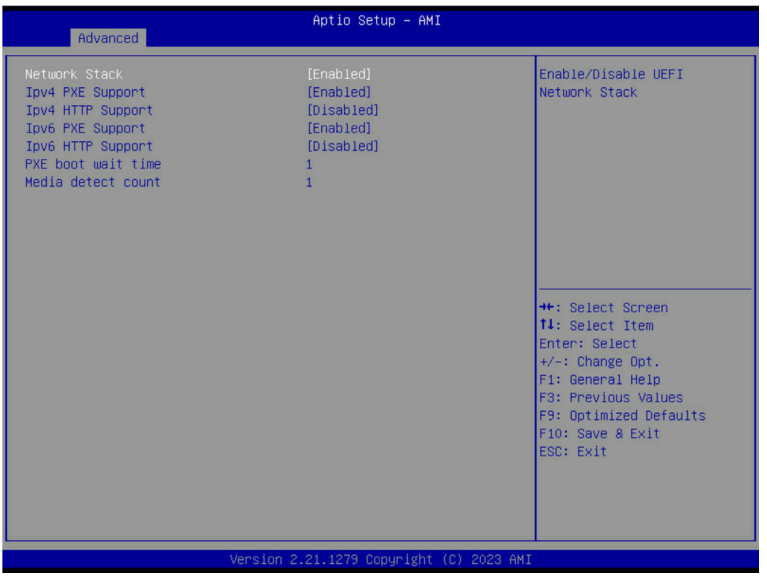


Parameter	Description
USB Configuration	
USB Module Version	Displays the USB module version information.
USB Controllers	Displays the supported USB controllers.
USB Devices:	Displays the USB devices connected to the system.
Legacy USB Support	Enable/Disable the Legacy USB support function. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. Options available: Enabled, Disabled, Auto. Default setting is **Enabled**.
XHCI Hand-off	Enable/Disable the XHCI 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: Disabled, Enabled. Default setting is **Enabled**.
USB hardware delays and time-outs	
USB transfer time-out	Selects the time-out value for USB Control/Bulk/Interrupt transfers. 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 reset time-out	Selects the time-out value during a USB mass storage device reset. Options available: 10 sec, 20 sec, 30 sec, 40 sec. Default setting is **20 sec**.
Device power-up delay	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. Options available: Auto, Manual. Default setting is **Auto**.
Mass Storage Devices	Displays the mass storage devices available on the system.

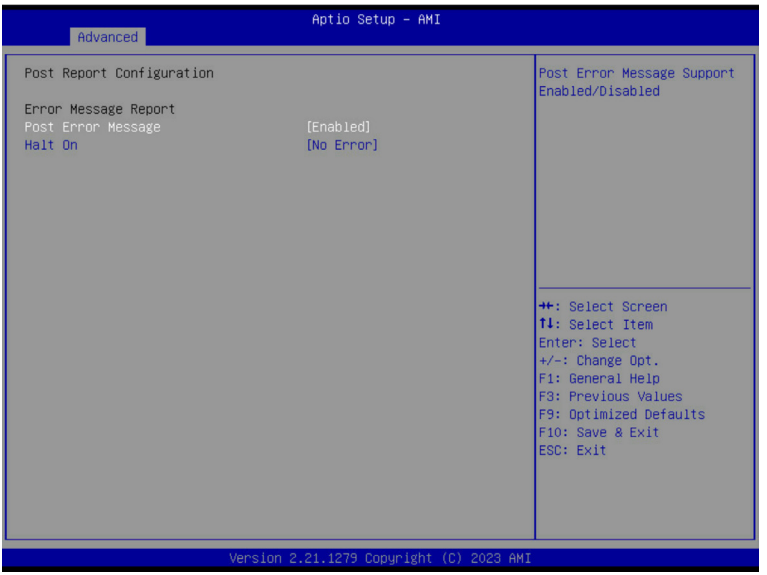
5-2-10 Network Stack Configuration



Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is **Enabled**.
Ipv4 PXE Support(Note)	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is **Enabled**.
Ipv4 HTTP Support(Note)	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled, Disabled. Default setting is **Disabled**.
Ipv6 PXE Support(Note)	Enable/Disable the Ipv6 PXE feature. Options available: Enabled, Disabled. Default setting is **Enabled**.
Ipv6 HTTP Support(Note)	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled, Disabled. Default setting is **Disabled**.
PXE boot wait time(Note)	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(Note)	Number of times the presence of media will be checked. Press the <+> / <-> keys to increase or decrease the desired values.

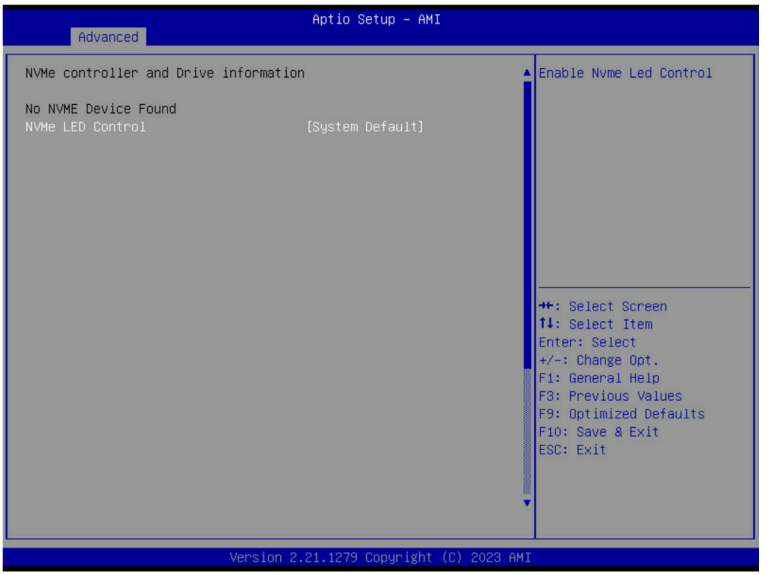
(Note) This item appears when **Network Stack** is set to **Enabled**.

5-2-11 Post Report Configuration



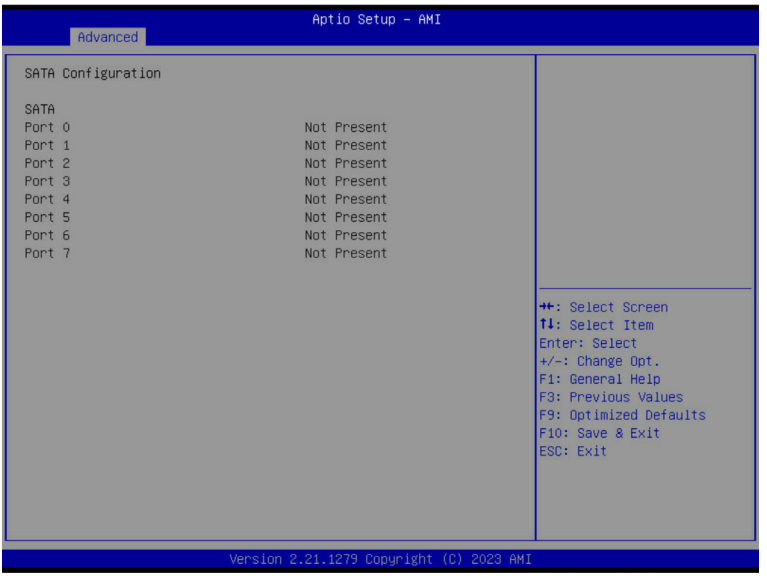
Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is **Enabled**.
Halt On	Options available: No Error, All Error. Default setting is **No Error**.

5-2-12 NVMe Configuration



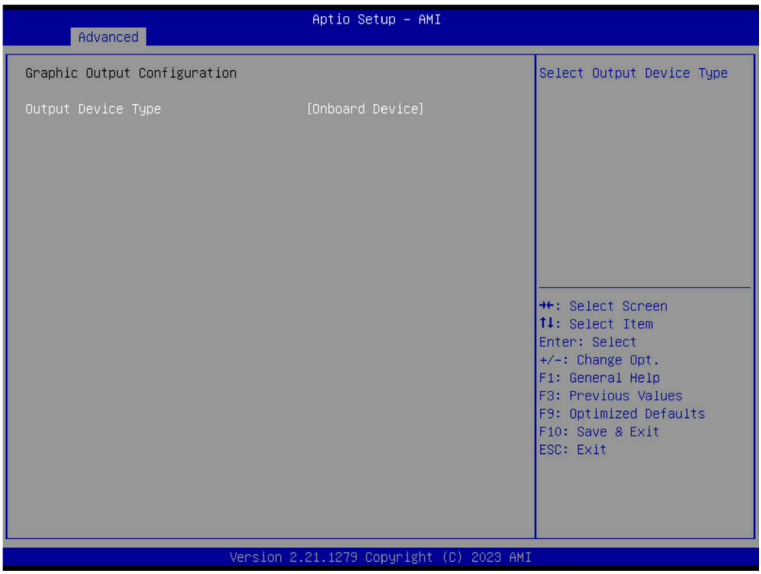
Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.
NVMe LED Control	Enable/Disable NVMe LED Control. Options available: System Default, Disabled, Enabled. Default setting is **System Default**.

5-2-13 SATA Configuration



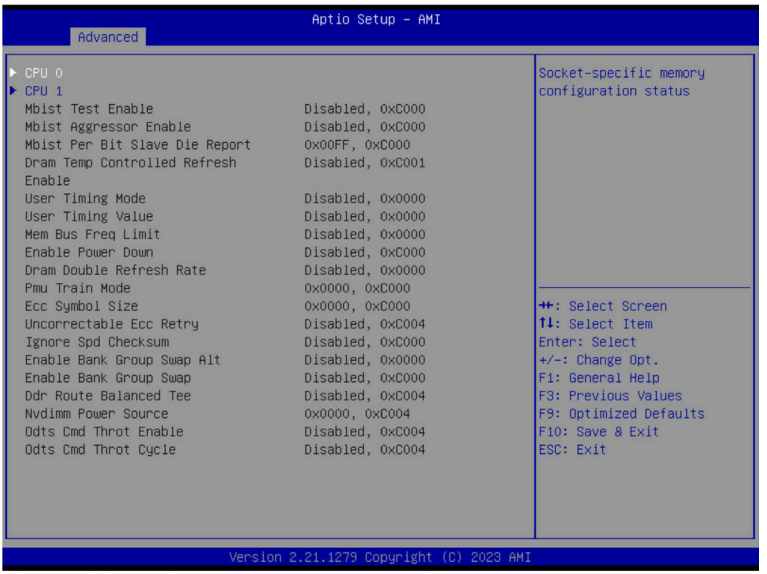
Parameter	Description
SATA Configuration	Displays the installed HDD devices information. System will automatically detect HDD type.

5-2-14 Graphic Output Configuration



Parameter	Description
Output Device Type	Selects output device type. Options available: First loaded Device, Onboard Device, External Device, Specific Device. Default setting is **Onboard Device**.

5-2-15 AMD Mem Configuration Status



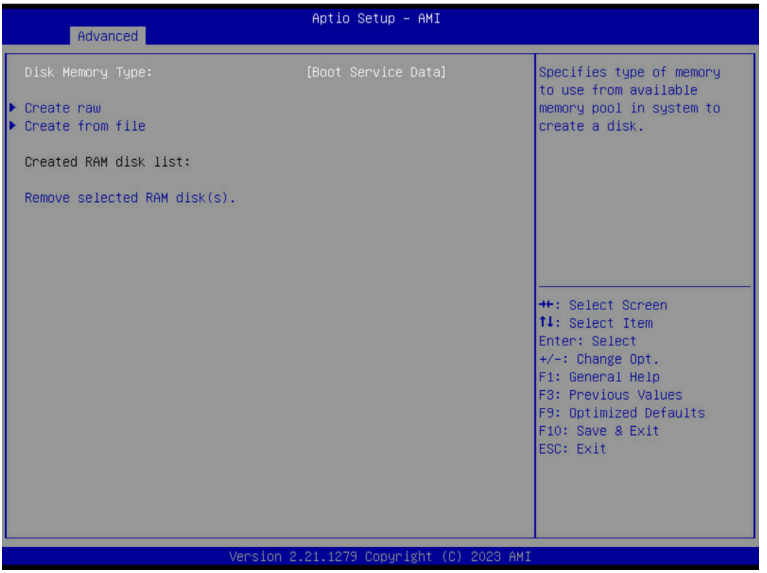
Parameter	Description
CPU 0/1	Press [Enter] to view the memory configuration status related to CPU 0/1.

5-2-16 Tls Auth Configuration



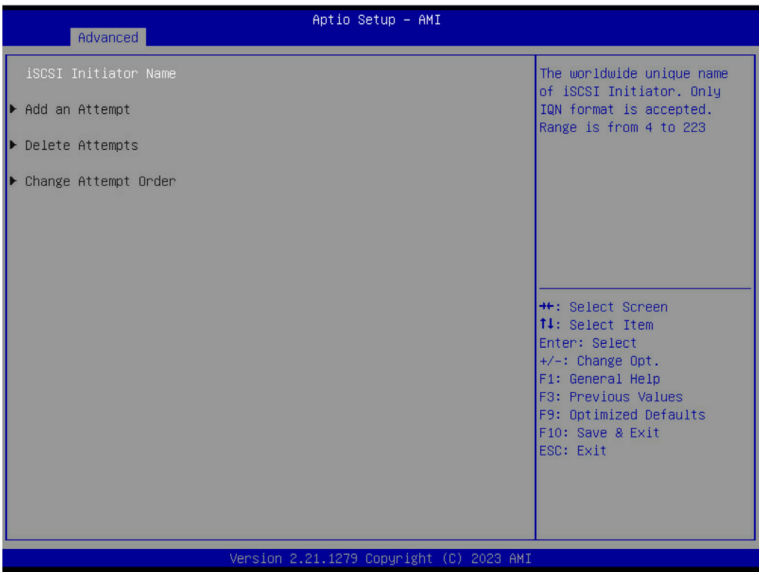
Parameter	Description
Server CA Configuration	Press [Enter] for configuration of advanced items. ◆ Enroll Cert – Press [Enter] to enroll a certificate • Enroll Cert Using File • Cert GUID Input digit character in 1111111-2222-3333-4444-1234567890ab format. – Commit Changes and Exit – Discard Changes and Exit ◆ Delete Cert
Client Cert Configuration	Press [Enter] for configuration of advanced items.

5-2-17 RAM Disk Configuration



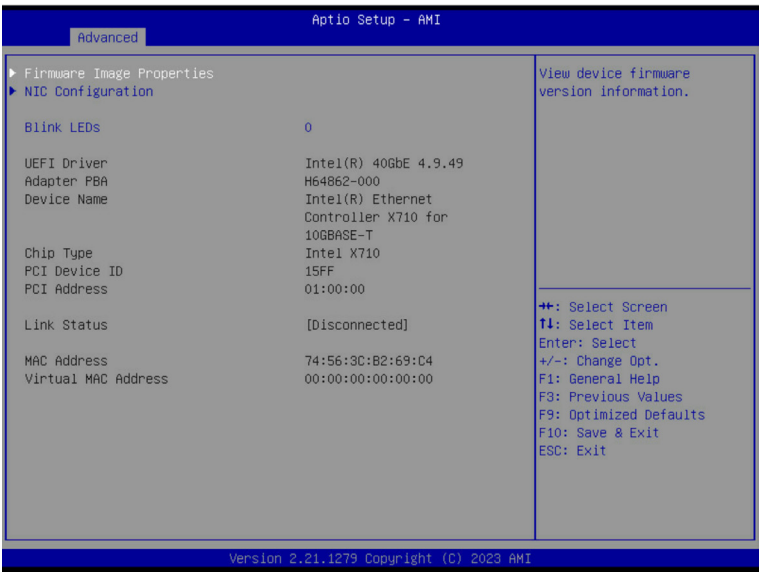
Parameter	Description
Disk Memory Type	Specifies the type of memory to use from available memory pool in system to create a disk. Options available: Boot Service Data, Reserved. Default setting is **Boot Service Data**.
Create Raw	Creates a raw RAM disk. ◆ Size (Hex) – Input a valid RAM disk size that should be multiple of the RAM disk block size. ◆ Create & Exit ◆ Discard & Exit
Create from file	Creates a RAM disk from a given file.
Created RAM disk list	
Remove selected RAM disk(s)	Selects the RAM disk(s) to remove.

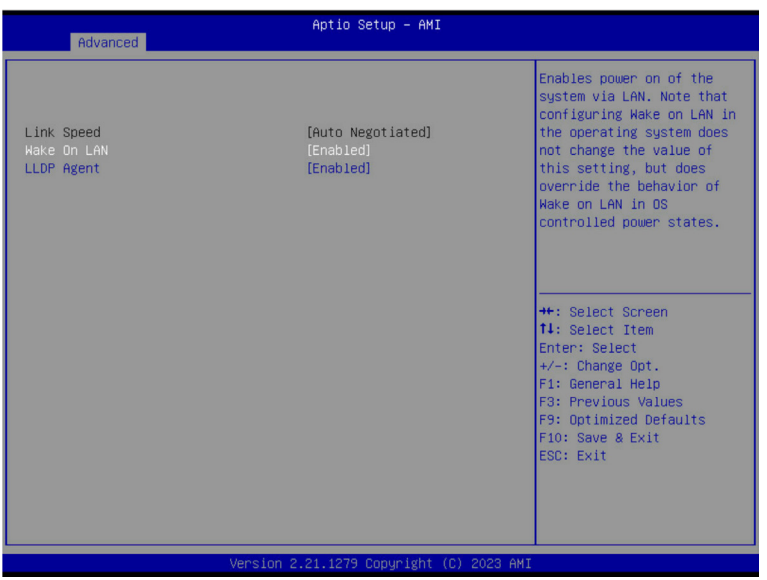
5-2-18 iSCSI Configuration



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

5-2-19 Intel(R) Ethernet Controller X710 for 10GBASE-T





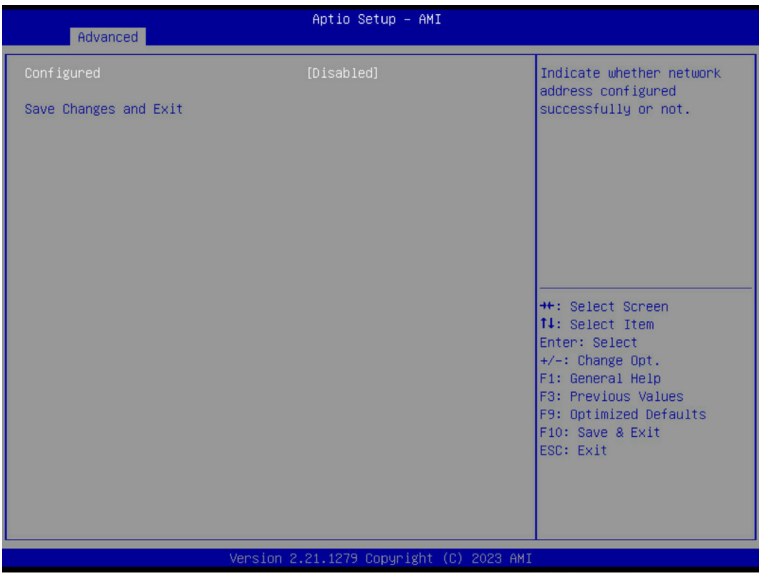
Parameter	Description
Firmware Image Properties	Press [Enter] to view device firmware version information.
NIC Configuration	Press [Enter] to configure advanced items. ◆ Link Speed – Default setting is **Auto Negotiated**. ◆ Wake On LAN – Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ LLDP Agent – Enable/Disable firmware's LLDP Agent. – Options available: Enabled, Disabled. Default setting is **Enabled**
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

5-2-20 VLAN Configuration



Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Create new VLAN ◆ VLAN ID – 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 – 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 – Press [Enter] to create a new VLAN or update an existing VLAN. ◆ Configured VLAN List ◆ Remove VLAN – Press [Enter] to remove an existing VLAN.

5-2-21 MAC IPv4 Network Configuration



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

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

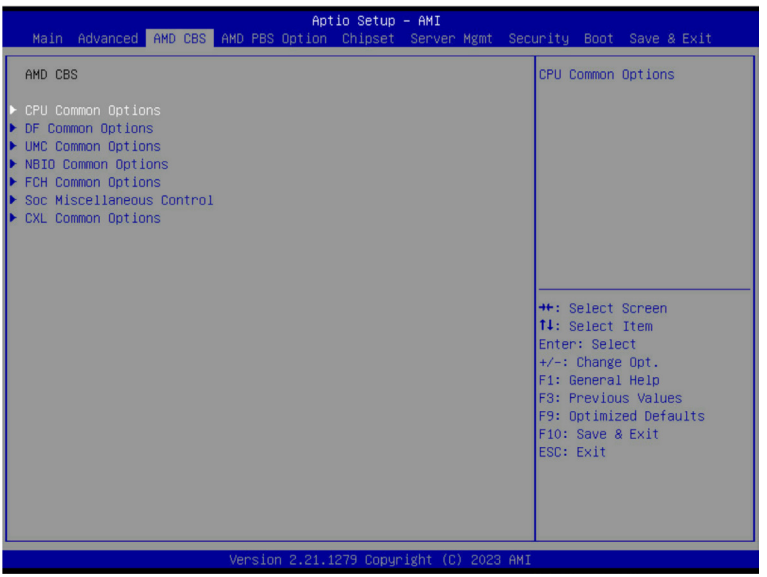
5-2-22 MAC IPv6 Network Configuration



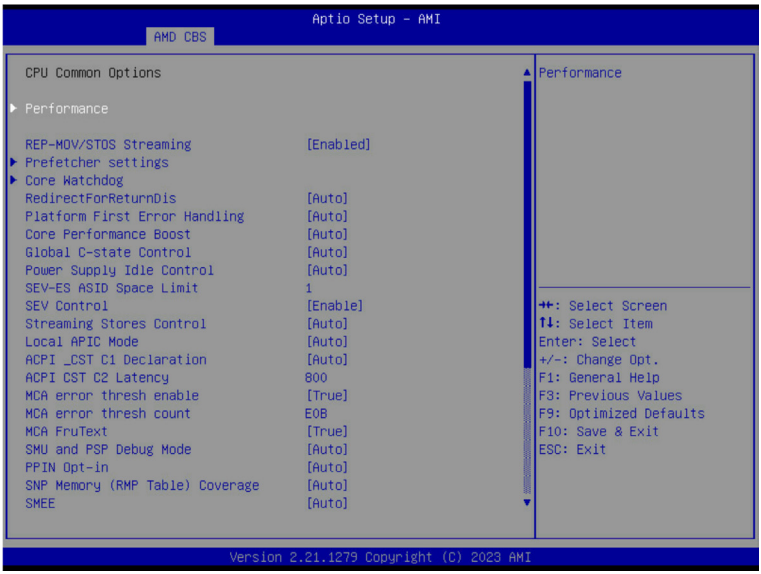
Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Displays the MAC Address information. ◆ Interface ID – The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3. ◆ DAD Transmit Count – The number of consecutive 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 – Options available: automatic, manual. Default setting is **automatic**. ◆ Save Changes and Exit – Press [Enter] to save all configurations.

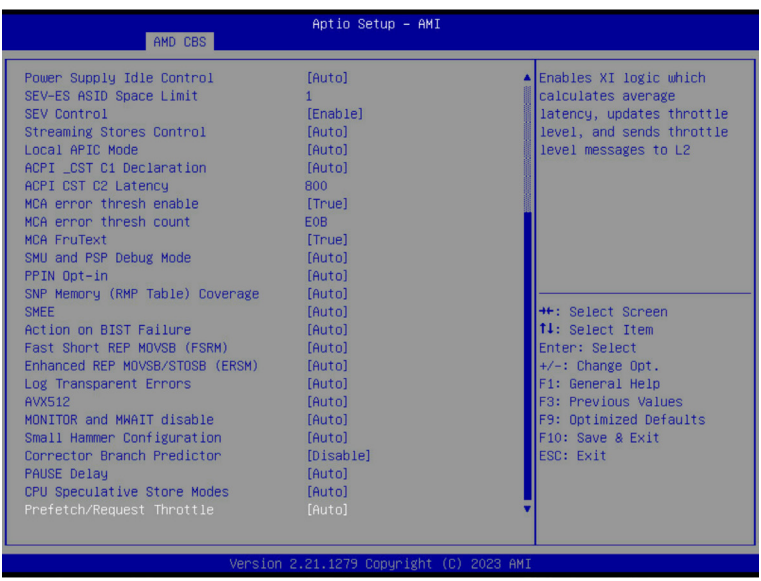
5-3 AMD CBS Menu

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

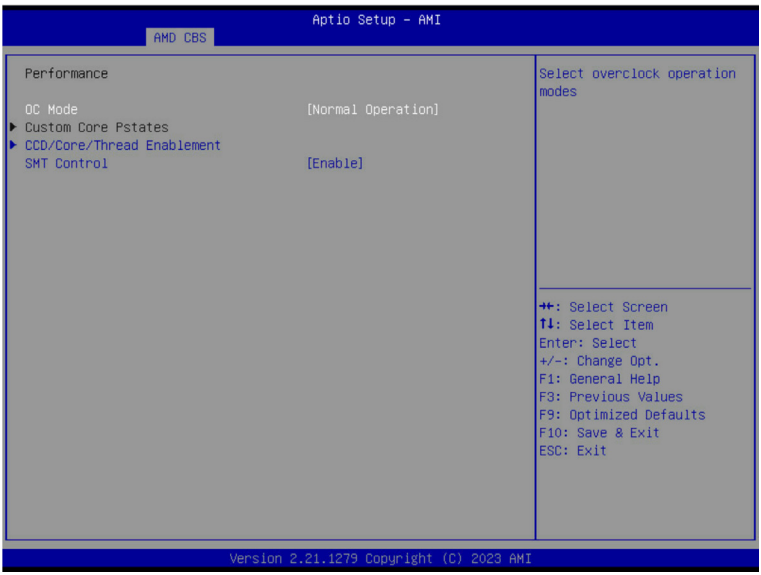




Parameter	Description
CPU Common Options	
Performance	Press [Enter] for configuration of advanced items.
REP-MOV/STOS Streaming	Allow REP-MOV/STOS to use non-caching streaming stores for large sizes. Options available: Disabled, Enabled. Default setting is **Enabled**.
Prefetcher settings	Press [Enter] 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: Enabled, Disabled, Auto. Default setting is **Auto**.
Core Performance Boost	Enable/Disable the Core Performance Boost function. Options available: Disabled, Auto. Default setting is **Auto**.
Global C-state Control	Controls the IO based C-state generation and DF C-states. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Power Supply Idle Control	Configures the Power Supply Idle Control. Options available: Low Current Idle, Typical Current Idle, Auto. Default setting is **Auto**.
SEV-ES ASID Space Limit	Configures the Space limit for SEV-ES ASIDs. Default setting is **1**.
SEV Control	Enable/Disable SEV control. Options available: Enable, Disable. Default setting is **Enable**.
Streaming Stores Control	Enable/Disable the Streaming Stores functionality. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Local APIC Mode	Sets the Local APIC Mode. Options available: Compatibility, xAPIC, x2APIC, Auto. Default setting is **Auto**.
ACPI_CST C1 Declaration	Determines whether or not to declare the C1 state to the OS.. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
ACPI CST C2 Latency	Enter in microseconds (decimal value).
MCA error thresh enable	Enable MCA error thresholding. Options available: False, True, Auto. Default setting is **True**.
MCA error thresh count	Effective error threshold count = 0xFFF(4095) - <this value> (e.g. the default value of 0xFF5(4085) results in a threshold of 0xA (10)).
MCA FruText	Enable MCA FruText. Options available: False, True. Default setting is **True**.
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: Disabled, Enabled, Auto. Default setting is **Auto**.

Parameter	Description
PPIN Opt-in	Enable/Disable the PPIN feature. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SNP Memory (RMP Table) Coverage	Enabled: Enter system memory is covered. Options available: Disabled, Enabled, Custom, Auto. Default setting is **Auto**.
SMEE	Controls the Secure Memory Encryption Enable (SMEE) function. Options available: Disable, Enable, Auto. Default setting is **Auto**.
Action on BIST Failure	Action to take when a CCD BIST failure is detected. Options available: Do nothing, Down-CCD, Auto. Default setting is **Auto**.
Fast Short REP MOVSB (FSRM)	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Enhanced REP MOVSB/ STOSB (ERSM)	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Log Transparent Errors	Enable/Disable the log Transparent errors function. Options available: Auto, Disabled, Enabled. Default setting is **Auto**.
AVX512	Enable/Disable AVX512. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
MONITOR and MWAIT disable	The MONITOR, MWAIT, MONITORX and MWAITX opcodes become invalid when enabled. Options available: Enabled, Disabled, Auto. Default setting is **Auto**
Small Hammer Configuration	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Corrector Branch Predictor	Options available: Disable, Enable. Default setting is **Disable**.
PAUSE Delay	Number a cycles thread will be idle after a PAUSE instruction. Options available: Auto, Disable, 16 cycles, 32 cycles, 64 cycles, 128 cycles. Default setting is **Auto**.
CPU Speculative Store Modes	Select the CPU speculative store modes. Options available: Balanced, More Speculative, Less Speculative, Auto. Default setting is **Auto**.
Prefetch/Request Throttle	Enables XI logic which calculates average latency, updates throttle level, and sends throttle level messages to L2. Options available: Disable, Enable, Auto. Default setting is **Auto**.

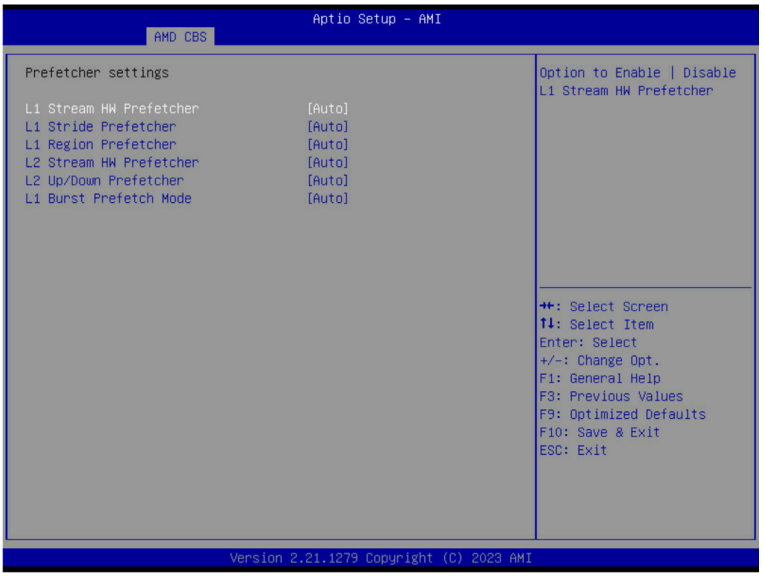
5-3-1-1 Performance



Parameter	Description
Performance	
OC Mode(Note)	Options 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, and the number of cores to be used. ◆ CCD Control – Options available: Auto, 2 CCDs, 4 CCDs, 6 CCDs, 8 CCDs, 10 CCDs. Default setting is **Auto**. ◆ Core Control – Options available: Auto, ONE(1+0), TWO(2+0), THREE(3+0) FOUR(4+0), FIVE(5+0), SIX(6+0), SEVEN(7+0). – Default setting is **Auto**.
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. Options available: Disable, Enable, Auto. Default setting is **Enable**.

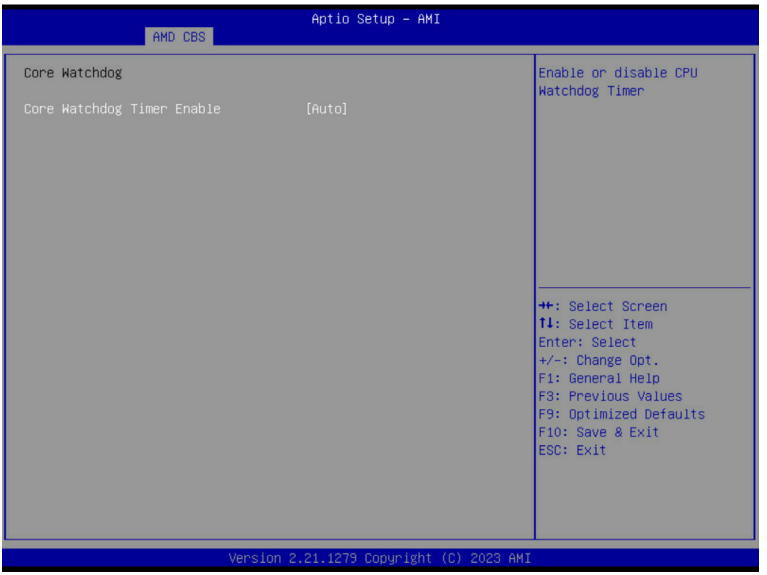
(Note) Advanced items are configurable when this item is defined.

5-3-1-2 Prefetcher Settings



Parameter	Description
Prefetcher settings	
L1 Stream HW Prefetcher	Enable/Disable L1 Stream HW Prefetcher. Options available: Disable, Enable, Auto. Default setting is **Auto**.
L1 Stride Prefetcher	Use memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous. Enable/Disable L1 Stride Prefetcher. Options available: Disable, Enable, Auto. 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. Enable/Disable L1 Region Prefetcher. Options available: Disable, Enable, Auto. Default setting is **Auto**.
L2 Stream HW Prefetcher	Enable/Disable L2 Stream HW Prefetcher. Options available: Disable, Enable, Auto. 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. Enable/Disable L2 Up/Down Prefetcher. Options available: Disable, Enable, Auto. Default setting is **Auto**.
L1 Burst Prefetch Mode	Enable/Disable L1 Burst Prefetch Mode. Options available: Disable, Enable, Auto. Default setting is **Auto**.

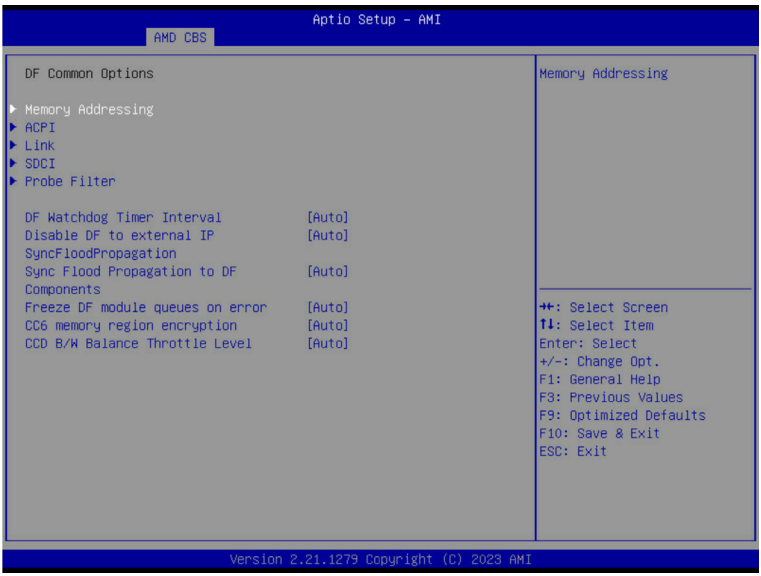
5-3-1-3 Core Watchdog



Parameter	Description
Core Watchdog	
Core Watchdog Timer Enable(Note)	Enable/Disable CPU Watchdog Timer. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Core Watchdog Timer Interval	Select the CPU Watchdog Timer interval. Options available: 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, 162.56us, 80.64us, 39.68us, Auto. Default setting is **Auto**.
Core Watchdog Timer Severity	Options available: No Error, Transparent, Corrected, Deferred, Uncorrected, Fatal, Auto. Default setting is **Auto**.

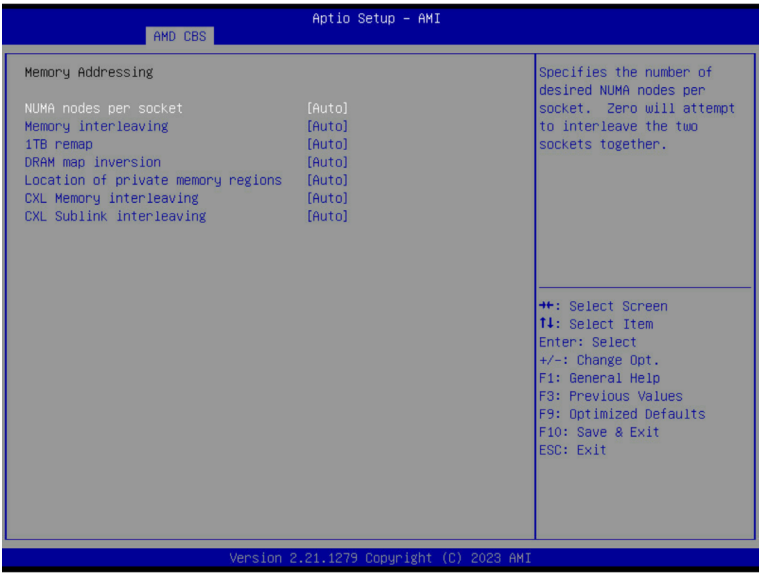
(Note) Advanced items prompt when this item is defined.

5-3-2 DF Common Options



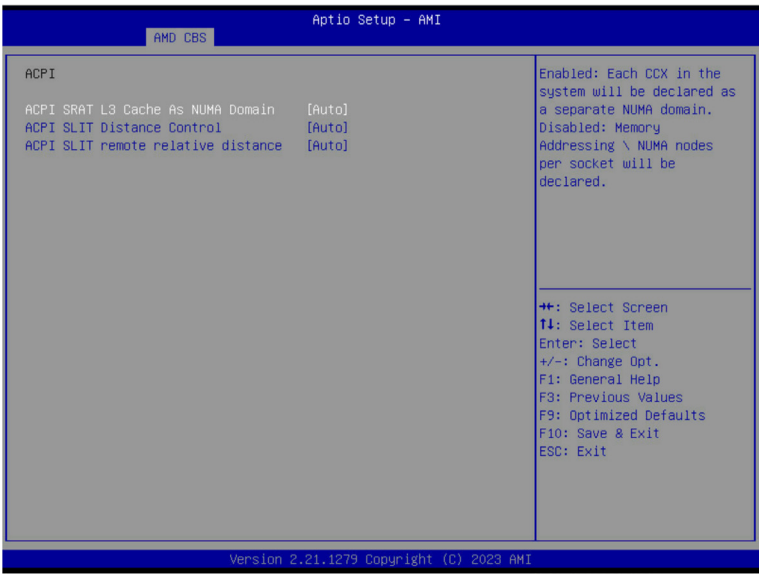
Parameter	Description
DF Common Options	
Memory Addressing	Press [Enter] for configuration of advanced items.
ACPI	Press [Enter] for configuration of advanced items.
Link	Press [Enter] for configuration of advanced items.
SDCI	Press [Enter] for configuration of advanced items.
Probe Filter	Press [Enter] for configuration of advanced items.
DF Watchdog Timer Interval	Configures the Data Fabric watchdog timer interval. Options available: Auto, 41ms, 166ms, 334ms, 669ms, 1.34 seconds, 2.68 seconds, 5.36 seconds. Default setting is **Auto**.
Disable DF to external IP sync flood propagation	Enable/Disable SyncFlood to UMC & downstream slaves. Options available: Sync flood disabled, Sync flood enabled, Auto. Default setting is **Auto**.
Sync flood propagation to DF Components	Enable/Disable DF Sync Flood propagation. Options available: Sync flood disabled, Sync flood enabled, Auto. Default setting is **Auto**.
Freeze DF module queues on error	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
CC6 memory region encryption	Controls whether or not the CC6 save/restor memory is encrypted. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
CCD B/W Balance Throttle Level	Options available: Auto, Level 0, Level 1, Level 2, Level 3, Level 4. Default setting is **Auto**.

5-3-2-1 Memory Addressing



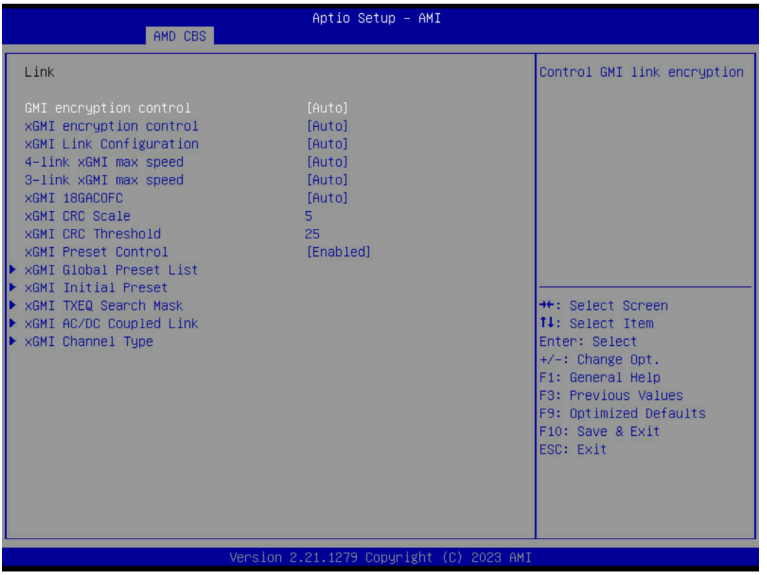
Parameter	Description
Memory Addressing	
NUMA nodes per socket	Specifies the number of desired NUMA nodes per socket. Options available: NPS0, NPS1, NPS2, NPS4, Auto. Default setting is **Auto**. NOTE! • **Available options may vary by system configuration.** • **Only dual processor configuration supports NPS0.**
Memory interleaving	Enable/Disable the Memory interleaving feature. Options available: Disabled, Auto, Enabled. 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: Do not remap, Attempt to remap, Auto. Default setting is **Auto**.
DRAM map inversion	Enable/Disable the DRAM map inversion function. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Location of private memory regions	Controls whether or not the private memory regions (PSP, SMU and CC6) are at the top of DRAM or distributed. Options available: Distributed, Consolidated, Auto. Default setting is **Auto**.
CXL Memory interleaving	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
CXL Sublink interleaving	Options available: Enable, Disable, Auto. Default setting is **Auto**.

5-3-2-2 ACPI



Parameter	Description
ACPI	
ACPI SRAT L3 Cache As NUMA Domain	Enable/Disable report each L3 cache as a NUMA Domain to the OS. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
ACPI SLIT Distance Control	Determines how the SLIT distances are declared. Options available: Manual, Auto. 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: Near, Far, Auto. Default setting is **Auto**.

5-3-2-3 Link

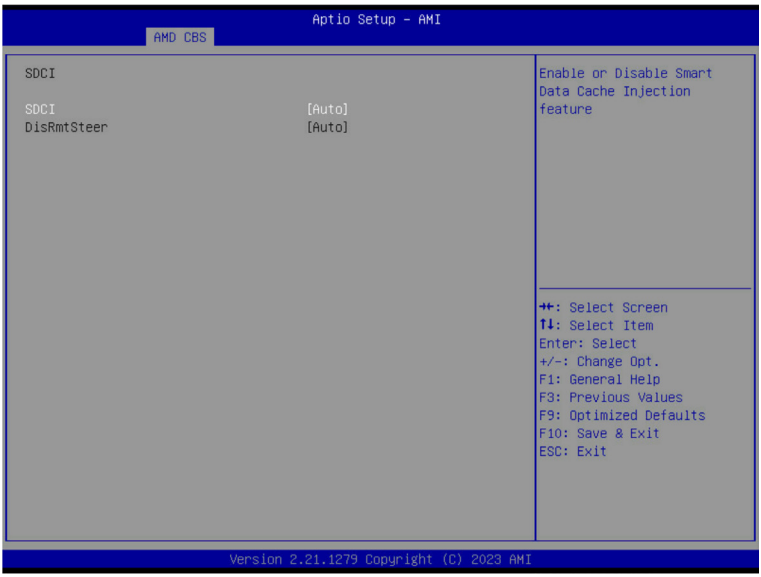


Parameter	Description
GMI encryption control	Enable/Disable GMI link encryption. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
xGMI encryption control	Enable/Disable xGMI link encryption. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
xGMI Link Configuration	Configures the number of xGMI2 links used on a multi-socket system. Options available: Auto, 3 xGMI Links, 4 xGMI Links, 2 xGMI Links + 2 PCI Links. Default setting is **Auto**.
4-link xGMI max speed	Specifies the max speed of 4-link xGMI. Options available: 12Gbps, 16Gbps, 17Gbps, 18Gbps, 20Gbps, 22Gbps, 23Gbps, 24Gbps, 25Gbps, 26Gbps, 27Gbps, 30Gbps, 32Gbps, Auto. Default setting is **Auto**.
3-link xGMI max speed	Specifies the max speed of 3-link xGMI. Options available: 12Gbps, 16Gbps, 17Gbps, 18Gbps, 20Gbps, 22Gbps, 23Gbps, 24Gbps, 25Gbps, 26Gbps, 27Gbps, 30Gbps, 32Gbps, Auto. Default setting is **Auto**.
xGMI 18GACOFC	Configures xGMI 18GACOFC. Options available: Auto, Enable, Disable. Default setting is **Auto**.
xGMI CRC Scale	Configures leaky bucket scale for xGMI and WAFL CRC errors. Every scale milliseconds an error will leak from the CRC counter. Default setting is **5**.
xGMI CRC Threshold	Configures leaky bucket threshold for xGMI and WAFL CRC errors. If link CRC counter exceeds this threshold, an error will be logged. Default setting is **25**.
xGMI Preset Control	Enable/Disable xGMI Preset control. Options available: Disabled, Enabled, Auto. Default setting is **Enabled**.

Parameter	Description
xGMI Global Preset List	Press [Enter] to configure the xGMI Preset list.
xGMI Initial Preset	Press [Enter] to configure the xGMI Initial Preset CPU0/1 link.
xGMI TXEQ Search Mask	Press [Enter] to configure the xGMI TXEQ Search Mask CPU0/1 link.
xGMI AC/DC Coupled Link	Press [Enter] to configure the xGMI AC/DC Coupled link. ◆ xGMI AC/DC Coupled Link Control(Note) – Options available: Manual, Auto. Default setting is **Auto**.
xGMI Channel Type	Press [Enter] to configure the xGMI Channel Type. ◆ xGMI Channel Type Control(Note) – Options available: Manual, Auto. Default setting is **Auto**.

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

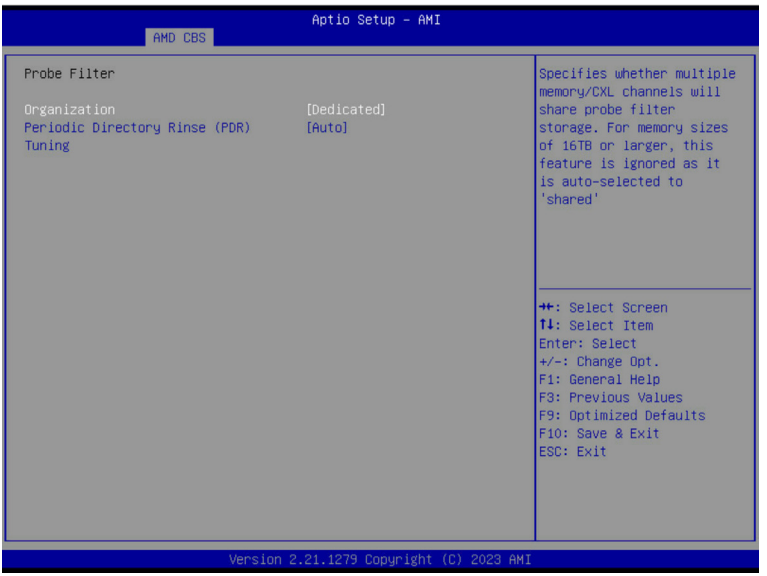
5-3-2-4 SDCI



Parameter	Description
SDCI(Note)	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
DisRmSteer	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

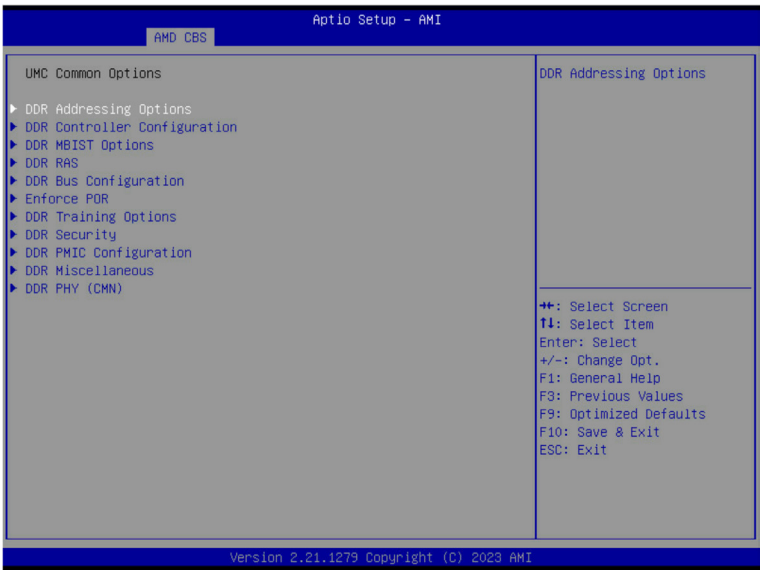
(Note) Advanced items prompt when this item is defined.

5-3-2-5 Probe Filter



Parameter	Description
Organization	Specifies whether multiple memory/CXL channels will share probe filter storage. Options available: Auto, Dedicated, Shared. Default setting is **Dedicated**.
Periodic Directory Rinse (PDR) Tuning	Controls PDR settings that may impact performance by workload and/or processor. Options available: Memory-Sensitive, Cache-Bound, Neutral, Adaptive, Auto. Default setting is **Auto**.

5-3-3 UMC Common Options



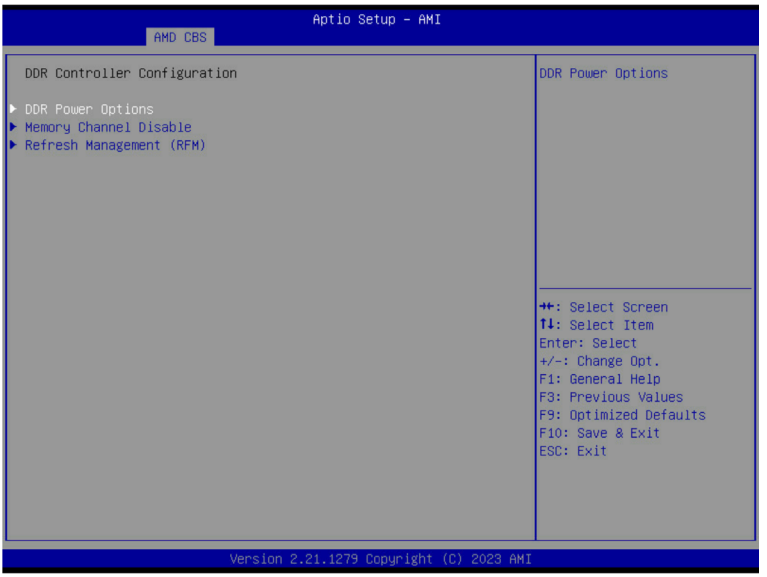
Parameter	Description
UMC Common Options	
DDR Addressing Options	Press [Enter] for configuration of advanced items.
DDR Controller Configuration	Press [Enter] for configuration of advanced items.
DDR MBIST Options	Press [Enter] for configuration of advanced items.
DDR RAS	Press [Enter] for configuration of advanced items.
DDR Bus Configuration	Press [Enter] for configuration of advanced items.
Enforce POR	Press [Enter] for configuration of advanced items.
DDR Training Options	Press [Enter] for configuration of advanced items.
DDR Security	Press [Enter] for configuration of advanced items.
DDR PMIC Configuration	Press [Enter] for configuration of advanced items.
DDR Miscellaneous	Press [Enter] for configuration of advanced items.
DDR PHY (CMN)	Press [Enter] for configuration of advanced items.

5-3-3-1 DDR Addressing Options



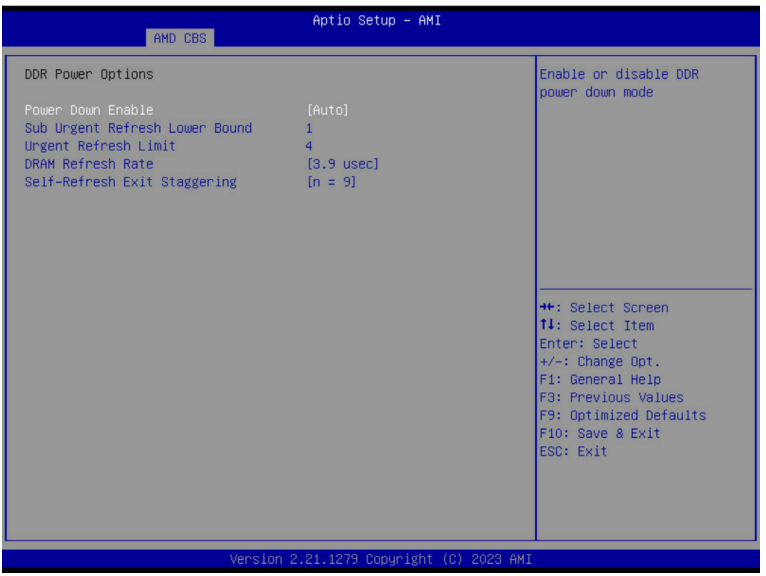
Parameter	Description
DDR Addressing Options	
Chipselect Interleaving	Interleaves memory blocks across the DRAM chip selects for node 0. Options available: Disabled, Auto. Default setting is **Auto**.
Address Hash Bank	Enable or disable bank addressing hashing. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Address Hash CS	Enable or disable CS addressing hashing. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Address Hash RM	Enable or disable RM address hashing for 3DS DIMMs. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Address Hash Subchannel	Enable or disable sub-channel addressing hashing. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
BankSwapMode	Options available: Auto, Disabled, Swap CPU. Default setting is **Auto**.

5-3-3-2 DDR Controller Configuration



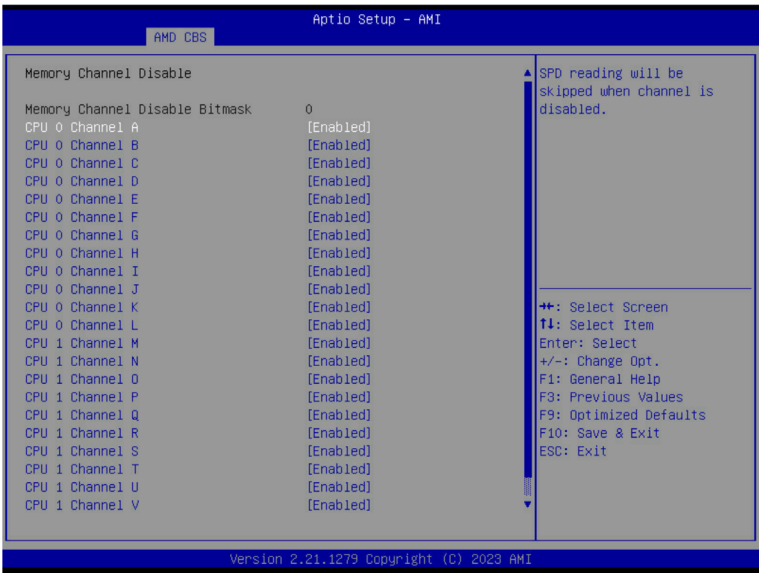
Parameter	Description
DDR Controller Configuration	
DDR Power Options	Press [Enter] for configuration of advanced items.
Memory Channel Disable	Press [Enter] for configuration of advanced items.
Refresh Management (RFM)	Press [Enter] for configuration of advanced items.

5-3-3-2-1 DDR Power Options



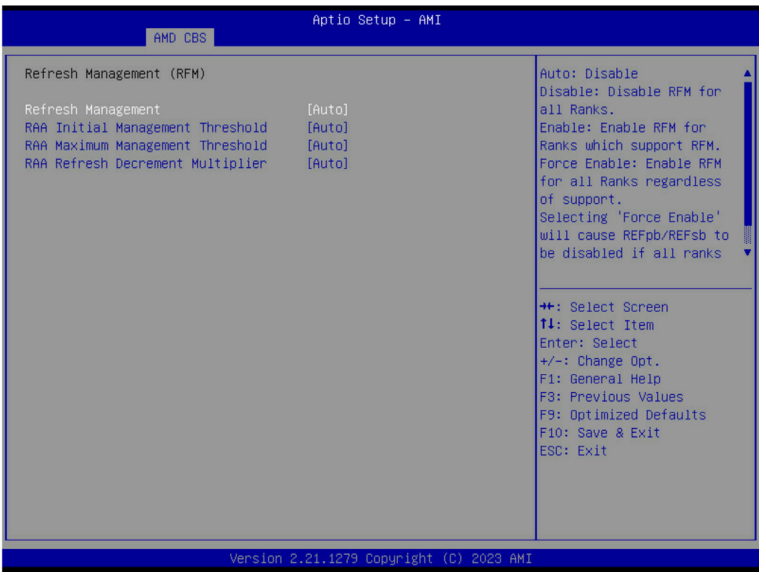
Parameter	Description
DDR Power Options	
Power Down Enable	Enable or disable DDR power down mode. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Sub Urgent Refresh Lower Bound	Specifies the stored refresh limit required to enter sub-urgent refresh mode.
Urgent Refresh Limit	Specifies the stored refresh limit required to enter urgent refresh mode.
DRAM Refresh Rate	DRAM refresh rate: 1.95us or 3.9us. Options available: 3.9 usec, 1.95 usec. Default setting is **3.9 usec**.
Self-Refresh Exit Staggering	Options available: Disabled, n=1~9. Default setting is **n=9**.

5-3-3-2-2 Memory Channel Disable



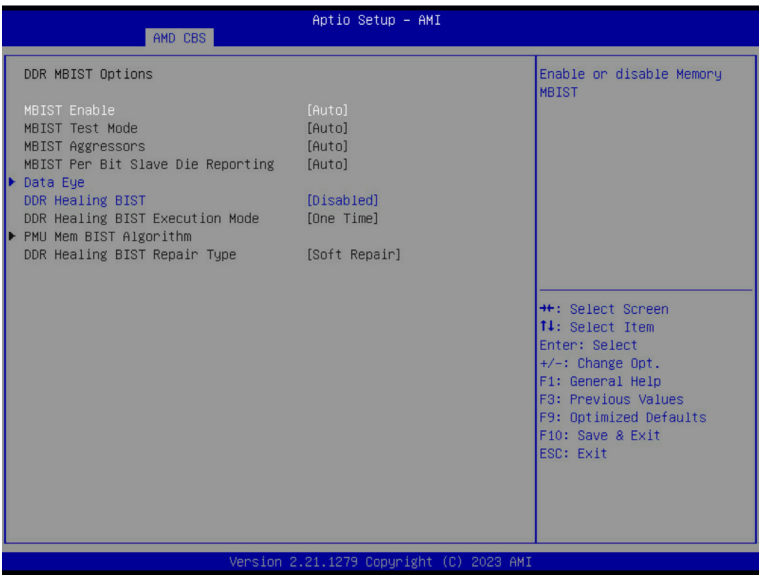
Parameter	Description
Memory Channel Disable	
Memory Channel Disable Bitmask	
CPU0/1 Channel_#	Press [Enter] to enable/disable specific memory channel.

5-3-3-2-3 Refresh Management (RFM)



Parameter	Description
Refresh Management (RFM)	
Refresh Management	Configure Refresh Management. Options available: Enable, Disable, Auto, Force Enable. Default setting is **Auto**.
RAA Initial Management Threshold	Override Rolling Accumulated ACT Initial Management Threshold. Options available: 32, 40, 48, 56, 64, 72, 80, Auto. Default setting is **Auto**.
RAA Maximum Management Threshold	Override Rolling Accumulated ACT Maximum Management Threshold. Options available: 3X, 4X, 5X, 6X, Auto. Default setting is **Auto**.
RAA Refresh Decrement Multiplier	Override RAA Refresh Decrement Multiplier. Options available: 0.5, 1, Auto. Default setting is **Auto**.

5-3-3-3 DDR MBIST Options



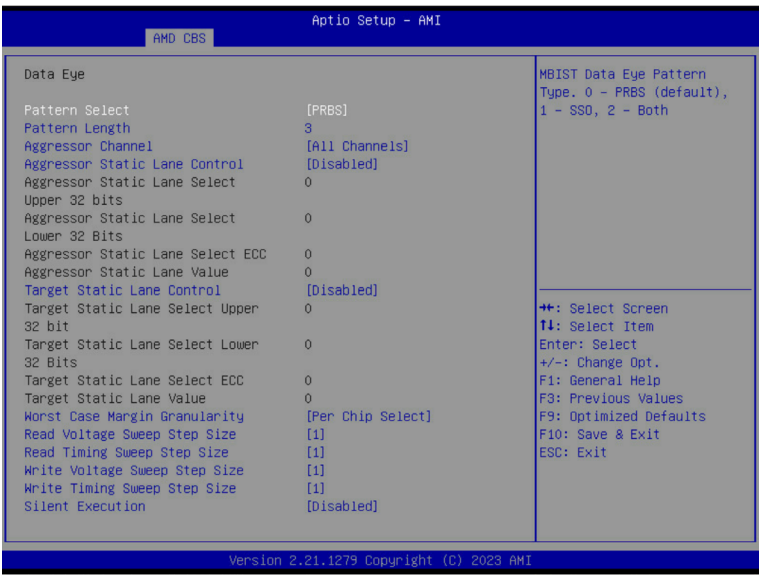
Parameter	Description
DDR MBIST Options	
MBIST Enable	Enable/Disable the Memory MBIST function. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
MBIST Test Mode(Note1)	Selects MBIST Test Mode. **Interface Mode**: Tests Single and Multiple CS transactions and Basic Connectivity. **Data Eye Mode**: Measures Voltage vs. Timing. Options available: Auto, Both, Interface Mode, Data Eye Mode. Default setting is **Auto**.
MBIST Aggressors(Note1)	Enable/Disable MBIST Aggressor test. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
MBIST Per Bit Slave Die Reporting(Note1)	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: Disabled, PMU Mem BIST, Self-Healing Mem BIST, PMU and Self-Healing Mem BIST. Default setting is **Disabled**.

(Note1) This item appears when **MBIST Enable** is set to **Enabled**.

Parameter	Description
DDR Healing BIST Execution Mode(Note2)	Options available: One Time, Every boot. Default setting is **One Time**.
PMU Mem BIST Algorithm(Note2)	Press [Enter] to enable/disable PMU Mem BIST Algorithm.
DDR Healing BIST Repair Type(Note2)	For DRAM errors found in the BIOS memory BIST select the repair type. Options available: Soft Repair, Hard Repair, No Repairs -Test only. Default setting is **Soft Repair**.

(Note2) This item appears when **DDR Healing BIST** is defined.

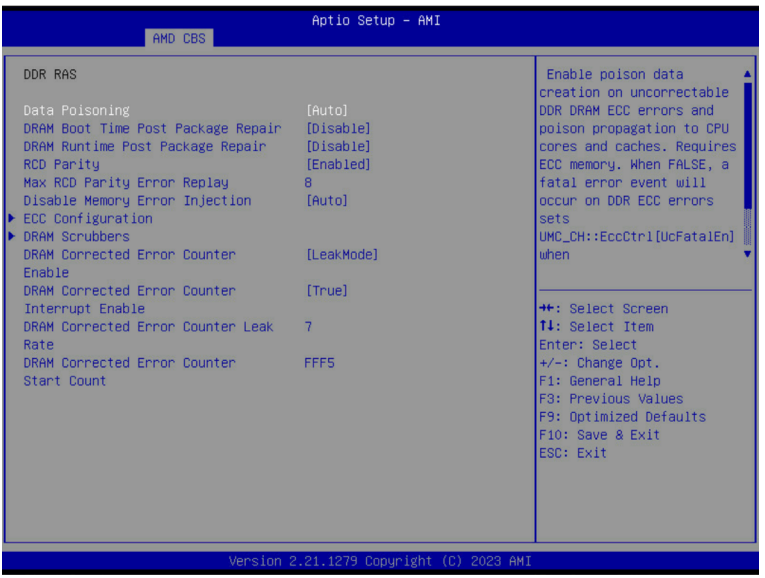
5-3-3-3-1 Data Eye



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: One Sub-Channel, Half Channels, All Channels. Default setting is **All Channels**.
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 **Per Chip Select.**
Read Voltage Sweep Step Size	Configures the step size for read Data Eye voltage sweep. Options available: 1, 2, 4. Default setting is **1**.
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 **1**.
Write Timing Sweep Step Size	Configures the step size for write Data Eye timing sweep. Options available: 1, 2, 4. Default setting is **1**.
Silent Execution	Execute MBIST Data Eye silently without ABL log output. Options available: Enabled, Disabled. Default setting is **Disabled**.

5-3-3-4 DDR RAS



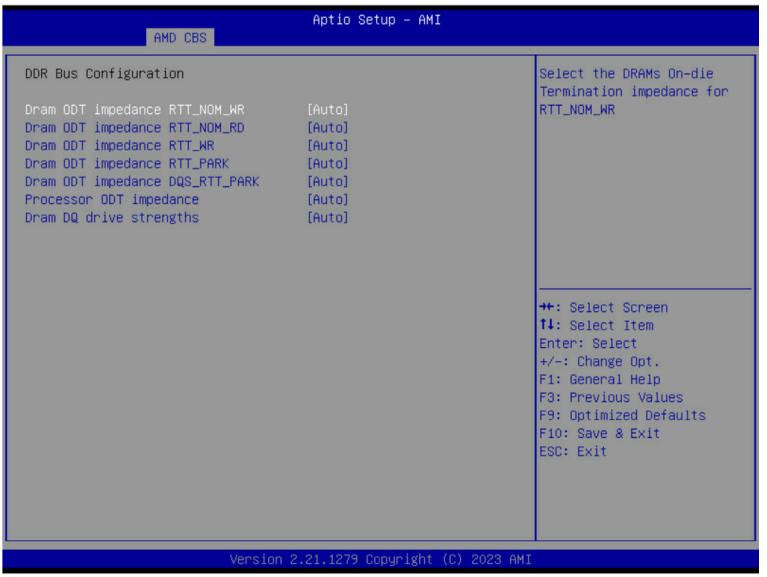
Parameter	Description
DDR RAS	
Data Poisoning	Enable/Disable the Data Poisoning function. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
DRAM Boot Time Post Package Repair	Enable/Disable the DRAM Boot Time Post Package Repair function. Options available: Enable, Disable. Default setting is **Disable**.
DRAM Runtime Post Package Repair	Enable/Disable the DRAM Runtime Post Package Repair function. Options available: Enable, Disable. Default setting is **Disable**.
RCD Parity	Enable/Disable the RCD Parity function. Options available: Auto, Enabled, Disabled. Default setting is **Enabled**.
Max RCD Parity Error Replay	Default setting is **8**.
Disable Memory Error Injection	Options available: False, True, Auto. Default setting is **Auto**.
ECC Configuration	Press [Enter] to configure advanced items. ◆ DRAM ECC Symbol Size – Configures the DRAM ECC Symbol Size. – Options available: Auto, x4, x16. Default setting is **Auto**. ◆ DRAM ECC Enable – Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable. – Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

Parameter	Description
ECC Configuration (continued)	◆ DRAM UECC Retry – Enable/Disable DRAM UECC Retry. – Options available: Auto, Enabled, Disabled. Default setting is **Disabled**. ◆ Max DRAM UECC Error Replay(Note) – Default setting is **8**. ◆ Memory Clear – Options available: Auto, Enabled, Disabled. Default setting is **Auto**. ◆ Address X0R after ECC – Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
DRAM Scrubbers	Press [Enter] to configure advanced items. ◆ DRAM ECS Mode – Options available: Auto, AutoECS, ManualECS, DisableECS. Default setting is **Auto**. ◆ DRAM Redirect Scrubber Enable – Options available: Auto, Enabled, Disabled. Default setting is **Auto**. ◆ DRAM Scrub Redirection Limit – Options available: Auto, 8 Scrubs, 4 Scrubs, 2 Scrubs, 1 Scrub. Default setting is **Auto**. ◆ DRAM Scrub Time – Options available: Disabled, 1 hour, 4 hours, 6 hours, 8 hours, 12 hours, 16 hours, 24 hours, 48 hours. Default setting is **24 Hours**. ◆ DRAM Error Threshold Count – Options available: Auto, ETC_4, ETC_16, ETC_64, ETC_256, ETC_1024, ETC_4096. Default setting is **Auto**. ◆ DRAM ECS Count Mode – Options available: Auto, Row Count Mode, Code Word Count Mode. Default setting is **Auto**. ◆ DRAM AutoEcs during Self Refresh – Options available: Auto, AutoEcs Disabled, AutoEcs Enabled. Default setting is **Auto**. ◆ DRAM ECS WriteBack Suppression – Options available: Auto, Enable, Disable. Default setting is **Auto**. ◆ DRAM X4 WriteBack Suppression – Options available: Auto, Enable, Disable. Default setting is **Auto**.

(Note) This item available when **DRAM UECC Retry** is set to **Enabled**.

Parameter	Description
DRAM Corrected Error Counter Enable	Configure DRAM Corrected Error Counter function. Options available: Disable, NoLeakMode, LeakMode. Default setting is **LeakMode**.
DRAM Corrected Error Counter Interrupt Enable	Enable SMI when DRAM corrected Error Counter count exceeds the threshold value. Options available: False, True. Default setting is **True**.
DRAM Corrected Counter Leak Rate	Program Rate value for DRAM Corrected Error Counter function. Default setting is **7**.
DRAM Corrected Error Counter Start Count	Program starting value for DRAM Corrected Error Counter function. Default setting is **FFF5**.

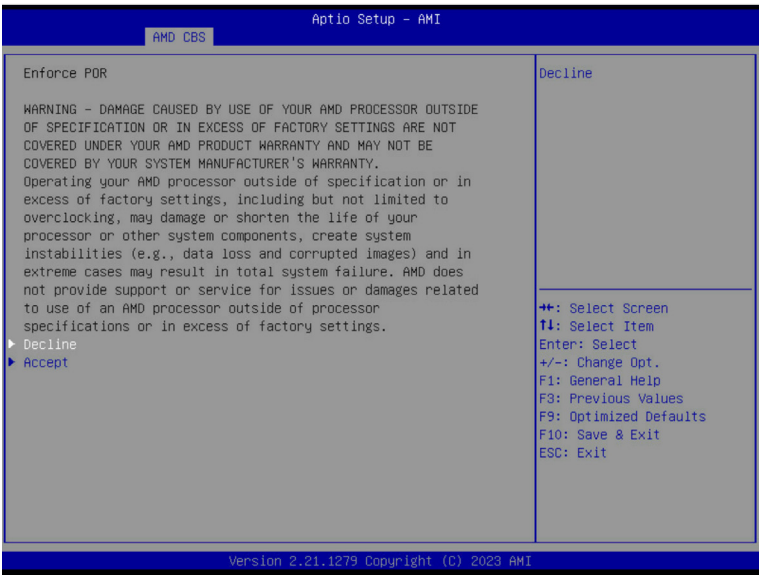
5-3-3-5 DDR Bus Configuration



Parameter	Description
DDR Bus Configuration	
Dram ODT impedance RTT_NOM_WR	Select the DRAMs On-die Termination impedance for RTT_NOM_WR. Options available: Auto, RTT_OFF, RZQ (240), RZQ/2 (120), RZQ/3 (80) RZQ/4 (60), RZQ/5(48), RZQ/6(40), RZQ/7(34). Default setting is **Auto**.
Dram ODT impedance RTT_NOM_RD	Select the DRAMs On-die Termination impedance for RTT_NOM_RD. Options available: Auto, RTT_OFF, RZQ (240), RZQ/2 (120), RZQ/3 (80) RZQ/4 (60), RZQ/5(48), RZQ/6(40), RZQ/7(34). Default setting is **Auto**.
Dram ODT impedance RTT_WR	Select the DRAMs On-die Termination impedance for RTT_WR. Options available: Auto, RTT_OFF, RZQ (240), RZQ/2 (120), RZQ/3 (80) RZQ/4 (60), RZQ/5(48), RZQ/6(40), RZQ/7(34). Default setting is **Auto**.
Dram ODT impedance RTT_PARK	Select the DRAMs On-die Termination impedance for RTT_PARK. Options available: Auto, RTT_OFF, RZQ (240), RZQ/2 (120), RZQ/3 (80) RZQ/4 (60), RZQ/5(48), RZQ/6(40), RZQ/7(34). Default setting is **Auto**.
Dram ODT impedance DQS_RTT_PARK	Select the DRAMs On-die Termination impedance for DQS_RTT_PARK. Options available: Auto, RTT_OFF, RZQ (240), RZQ/2 (120), RZQ/3 (80) RZQ/4 (60), RZQ/5(48), RZQ/6(40), RZQ/7(34). Default setting is **Auto**.

Parameter	Description
Processor ODT impedance	Select the ODT impedance for all DBYTE IOs. Options available: Auto, High Impedance, 480 ohm, 240 ohm, 160 ohm, 120 ohm, 96 ohm, 80 ohm, 68.6 ohm, 60 ohm, 53.3 ohm,48 ohm, 43.6 ohm, 40 ohm, 36.9 ohm, 34.3 ohm, 32 ohm, 30 ohm, 28.2 ohm, 26.7 ohm, 25.3 ohm. Default setting is **Auto**.
Dram DQ drive strengths	Select the Dram Pull-up and Pull-Down Output Driver Impedance for all DQ and DMI IOs. Options available: Auto, 48 ohm, 40 ohm, 34 ohm, Default setting is **Auto**.

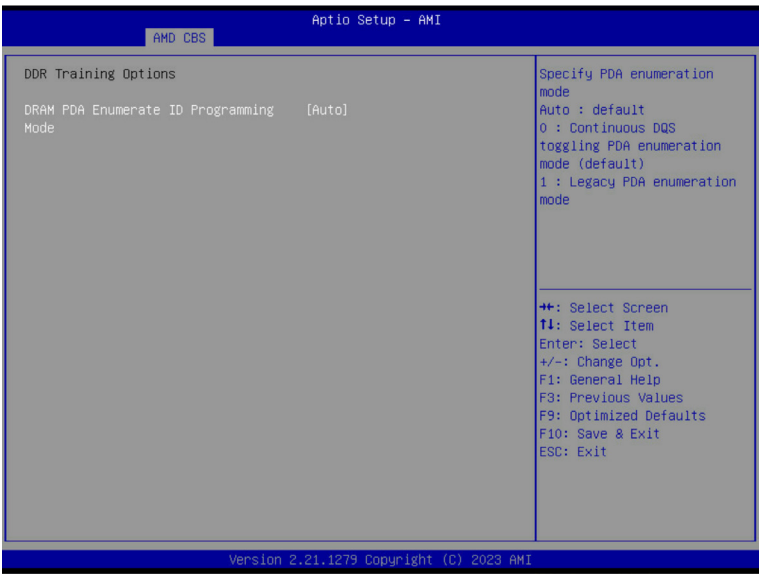
5-3-3-6 Enforce POR



Parameter	Description
Enforce POR	Decline/Accept to configure the advanced items.
Accept	
Active Memory Timing Settings(Note)	Active memory Timing Settings. Options available: Auto, Enabled. Default setting is **Auto**.
Memory Target Speed	Specifies the memory target speed in MT/s. Options available: Auto, DDR3200, DDR3600, DDR4000, DDR4400, DDR4800, DDR5200, DDR5600. Default setting is **Auto**.
SPD Timing	Press [Enter] to configure advanced items.
Non-SPD Timing	Press [Enter] to configure advanced items.

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

5-3-3-7 DDR Training Options



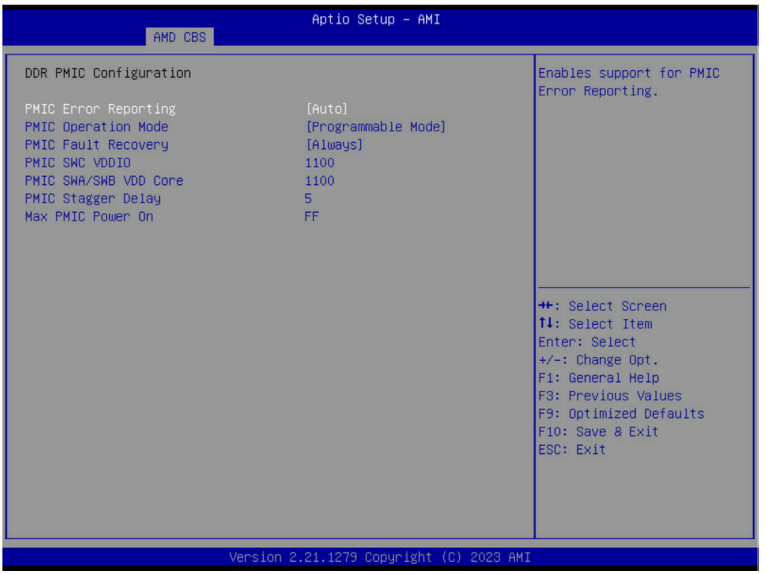
Parameter	Description
DDR Training Options	
DRAM PDA Enumerate ID Programming Mode	Specify PDA enumeration mode. Options available: Auto, Toggling PDA enumeration mode, Legacy PDA enumeration mode. Default setting is **Auto**.

5-3-3-8 DDR Security



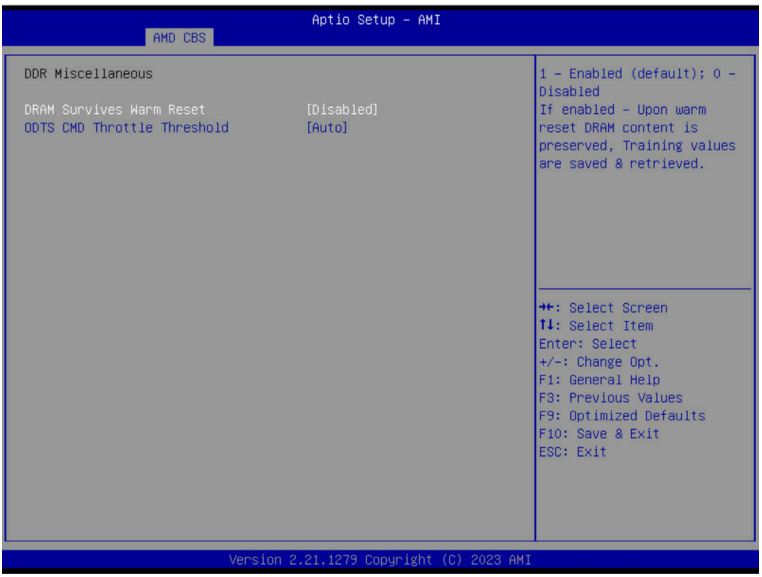
Parameter	Description
Security	
TSME	Enable/Disable Transparent SME. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
AES	Options available: AES-128, AES-256. Default setting is **AES-256**.
Data Scramble	Enable/Disable Data Scrambling. Options available: Enabled, Disabled. Default setting is **Enabled**.
SME-MK	Options available: Enabled, Disabled. Default setting is **Disabled**.

5-3-3-9 DDR PMIC Configuration



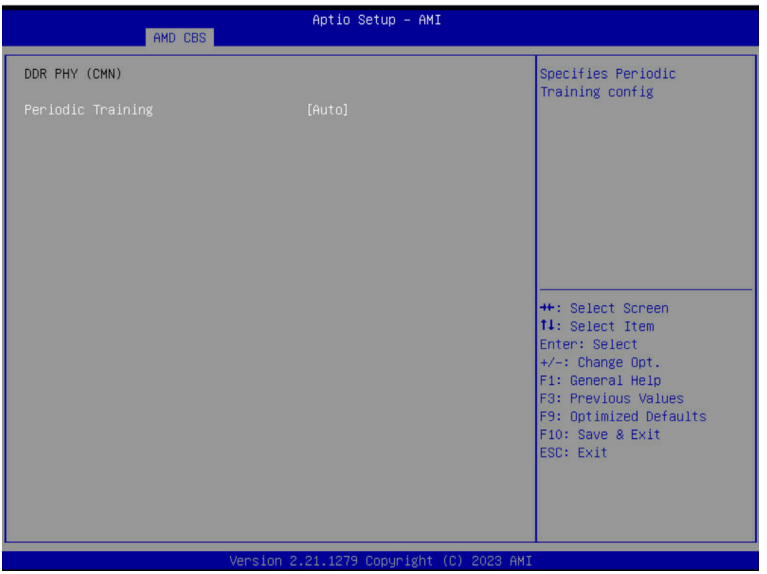
Parameter	Description
DDR PMIC Configuration	
PMIC Error Reporting	Enables support for PMIC Error Reporting. Options available: Auto, False, True. Default setting is **Auto**.
PMIC Operation Mode	Options available: Secure Mode, Programmable Mode. Default setting is **Programmable Mode**.
PMIC Fault Recovery	Options available: Always, Never, Once. Default setting is **Always**.
PMIC SWC VDDIO	Default setting is **1100**.
PMIC SWA/SWB VDD Core	Default setting is **1100**.
PMIC Stagger Delay	Default setting is **5**.
Max PMIC Power On	Default setting is **FF**.

5-3-3-10 DDR Miscellaneous



Parameter	Description
DDR Miscellaneous	
DRAM Survives Warm Reset	Options available: Enabled, Disabled. Default setting is **Disabled**.
ODTS CMD Throttle Threshold	Options available: Auto, > 85'C, > 90'C, > 95'C. Default setting is **Auto**.

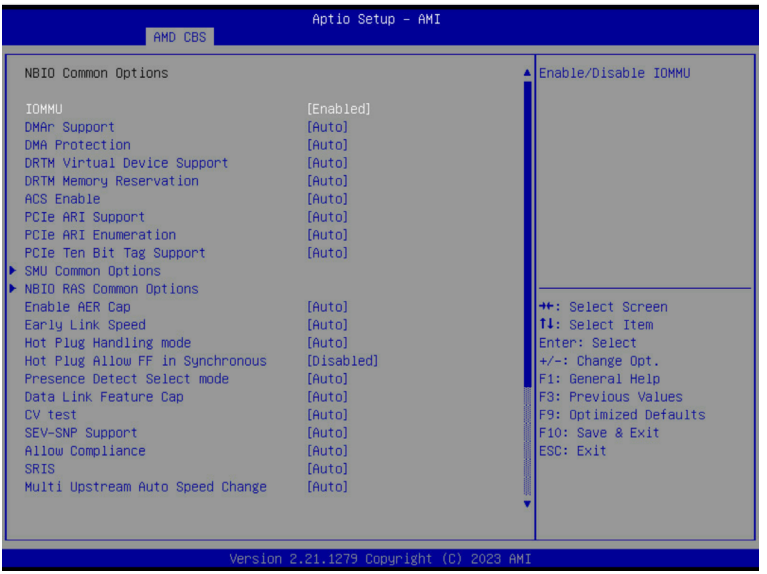
5-3-3-11 DDR PHY (CMN)

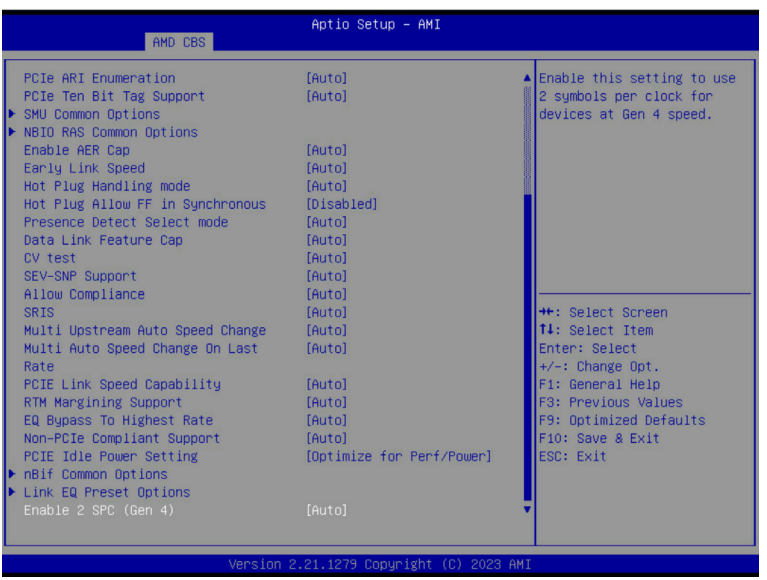


Parameter	Description
DDR PHY (CMN)	
Periodic Training(Note)	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Periodic Training Interval	Specifies the Periodic Training interval in millisecond.

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

5-3-4 NBIO Common Options

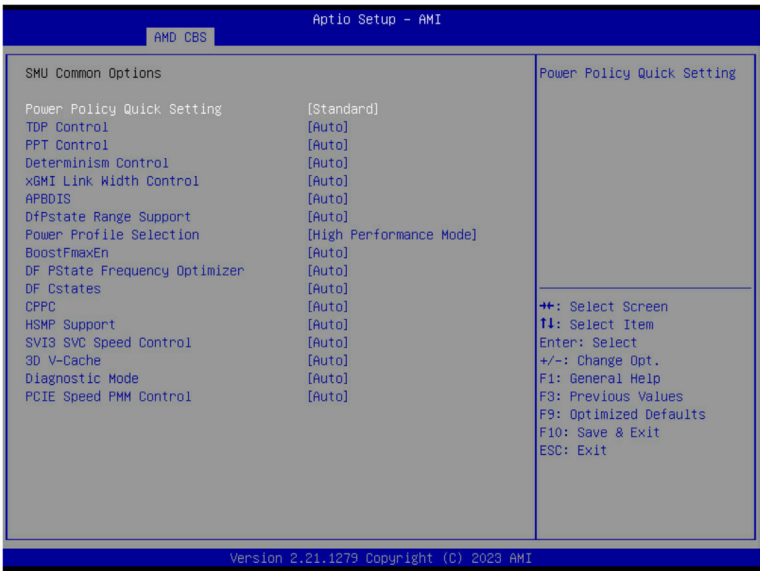




Parameter	Description
NBIO Common Options	
IOMMU	Enable/Disable the IOMMU function. Options available: Disabled, Enabled. Default setting is **Enabled**.
DMAr Support	Enable/Disable DMAr system protection during POST. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
DMA Protection	Enable/Disable DMA remap support in IVRS IVinfo Field. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
DRTM Virtual Device Support	Enable/Disable DRTM ACPI virtual device. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
DRTM Memory Reservation	Enable/Disable DRTM Memory reservation. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
ACS Enable	Enable/Disable ACS. Options available: Enable, Disabled, Auto. Default setting is **Auto**.
PCIe ARI Support	Enable/Disable Alternative Routing-ID Interpretation. Options available: Disable, Enable, Auto. Default setting is **Auto**.
PCIe ARI Enumeration	ARI Forwarding Enable for each downstream port. Options available: Disable, Enable, Auto. Default setting is **Auto**.
PCIe Ten Bit Tag Support	Enable/Disable PCIe ten bit tags for supported devices. (Auto=Disabled) Options available: Disable, Enable, Auto. 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: Enable, Disabled, Auto. Default setting is **Auto**.
Early Link Speed	Configures Early Link Speed. Options available: Auto, Gen1, Gen2. Default setting is **Auto**.
Hot Plug Handling mode	Controls the Hot Plug Handling mode. Options available: OS First, Firmware First/EDR if OS supports, Firmware First but allow OS First, System Firmware Intermediary, Auto. Default setting is **Auto**.
Hot Plug Allow FF in Synchronous	Allows firmware first hot plug handling mode to operate in mode A and mode B synchronous mappings. Options available: Disabled, Enabled. Default setting is **Disabled**.
Presence Detect Select mode	Controls the Presence Detect Select mode. Options available: OR, AND, Auto. Default setting is **Auto**.

Parameter	Description
Data Link Feature Cap	Enable/Disable the data link feature capability. Options available: Enabled, Disabled, Auto. Default setting is **Auto**.
CV test	Enable/Disable the running PCIE CV tool support. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
SEV-SNP Support	Enable/Disable the SEV-SNP support. Options available: Disable, Enable. Default setting is **Disable**.
Allow Compliance	When enabled, allows the PCIe RP to enter Polling.Compliance state. Options available: Auto, Disable, Enable. Default setting is **Auto**.
SRIS	Options available: Auto, Disable, Enable. Default setting is **Auto**.
Multi Upstream Auto Speed Change	Defines the setting of this feature for all PCIe devices. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Multi Auto Speed Change On Last Rate	Options available: Disable, Enable, Auto. Default setting is **Auto**.
PCIE Link Speed Capability	Options available: Maximum speed, Gen1, Gen2, Gen3, Gen4, Gen5, Auto. Default setting is **Auto**.
RTM Margining Support	Options available: Disable, Enable, Auto. Default setting is **Auto**.
EQ Bypass To Highest Rate	Options available: Disable, Enable, Auto. Default setting is **Auto**.
Non-PCIe Compliant Support	Options available: Disable, Enable, Auto. Default setting is **Auto**.
PCIE Idle Power Setting	Modify PCIE Power Savings Features that can impact lightly loaded latency. Options available: Optimize for Latency, Optimize for Perf/Power. Default setting is **Optimize for Latency**.
nBif Common Options	Press [Enter] for configuration of advanced items.
Link EQ Preset Options	Press [Enter] for configuration of advanced items.
Enable 2 SPC (Gen4)	Enable this setting to use 2 symbols per clock for devices at Gen4 speed. Options available: Auto, Enabled. Default setting is **Auto**.

5-3-4-1 SMU Common Options

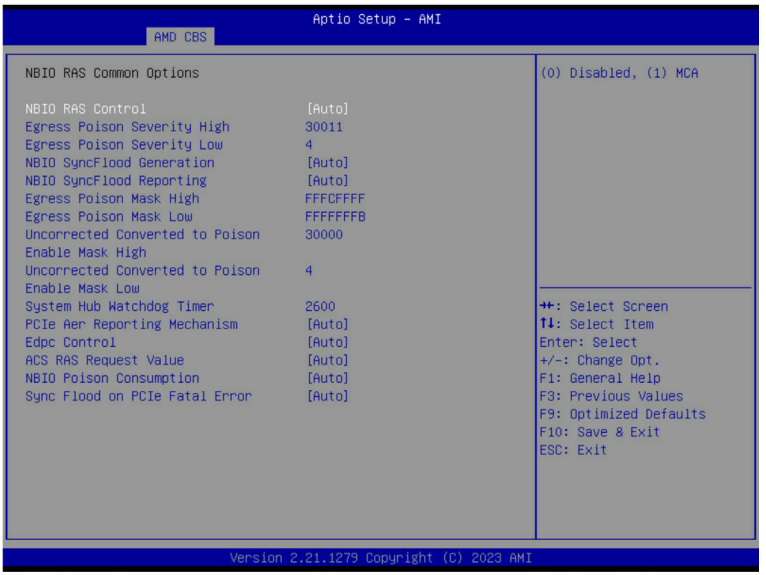


Parameter	Description
SMU Common Options	
Power Policy Quick Setting	Options available: Standard, Best Performance, Energy Efficient. Default setting is **Standard**.
TDP Control	Options available: Manual, Auto. Default setting is **Auto**.
PPT Control	Options available: Manual, Auto. Default setting is **Auto**.
Determinism Control	Selects use the fused Determinism or set customized Determinism. Options available: Manual, Auto. Default setting is **Auto**.
xGMI Link Width Control	Options available: Manual, Auto. Default setting is **Auto**.
APBDIS	Options available: 0, 1, Auto. Default setting is **Auto**.
DfPstate(Note)	DfPstate index to set when APBDIS =1.
DfPstate Range Support	Options available: Disable, Enable, Auto. Default setting is **Auto**.
Power Profile Selection	Options available: High Performance Mode, Efficiency Mode, Maximum IO Performance Mode. Default setting is **High Performance Mode**.
BoostFmaxEn	Options available: Manual, Auto. Default setting is **Auto**.
DF PState Frequency Optimizer	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

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

Parameter	Description
DF Cstates	Options available: Disabled, Enabled, Auto. Default setting is **Disabled**.
CPPC	Enable/Disable the CPPC feature. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
HSMP Support	Enable/Disable the HSMP support. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SVI3 SVC Speed Control	Options available: Auto, Manual. Default setting is **Auto**.
3D V-Cache	Options available: Auto, Disable, 1 stack, 2 stack, 4 stack. Default setting is **Auto**.
Diagnostic Mode	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
PCIE Speed PMM Control	Options available: Dynamic link speed determined by Power Management functionality, Static Target Link Speed (GEN4),Static Target Link Speed (GEN5), Auto. Default setting is **Auto**.

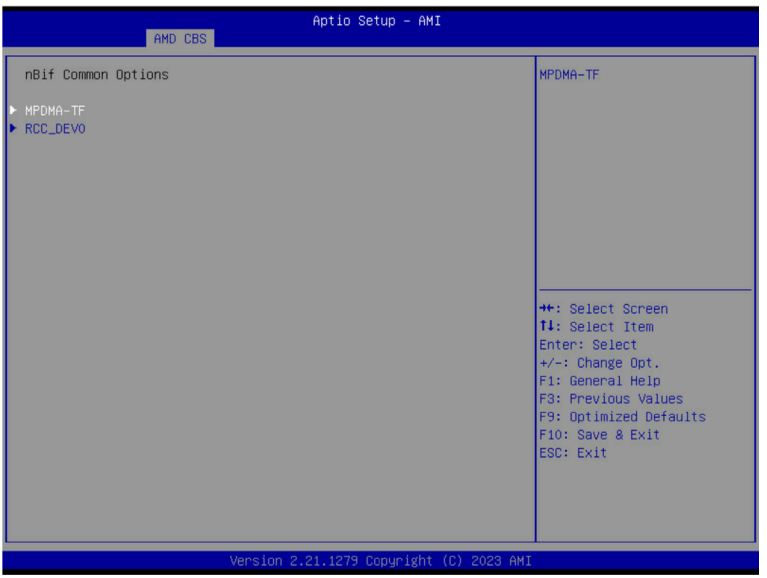
5-3-4-2 NBIO RAS Common Options



Parameter	Description
NBIO RAS Common Options	
NBIO RAS Control	Options available: Disabled, MCA, Auto. Default setting is **Auto**.
Egress Poison Severity High	Configures the Egress Poison High Severity. Each bit set to 1 enables High severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.
Egress Poison Severity Low	Configures the Egress Poison Low Severity. Each bit set to 1 enables High severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.
NBIO SyncFlood Generation	The value may be used to mask SyncFlood caused by NBIO RAS options. Options available: Enabled, Disabled, Auto. Default setting is **Auto**.
NBIO SyncFlood Reporting	The value may be used to enable SyncFlood reporting to APML. Options available: Enabled, Disabled, Auto. Default setting is **Auto**.
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.
PCIe Aer Reporting Mechanism	Selects the method of reporting AER errors from PCI Express. Options available: Firmware First, Firmware First but allow OS First, OS First, Auto. Default setting is **Auto**.
Edpc Control	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
ACS RAS Request Value	Options available: Direct Request Access Enabled, Request Blocking Enabled, Request Redirect Enabled, Auto. Default setting is **Auto**.
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**.

5-3-4-3 nBif Common Options

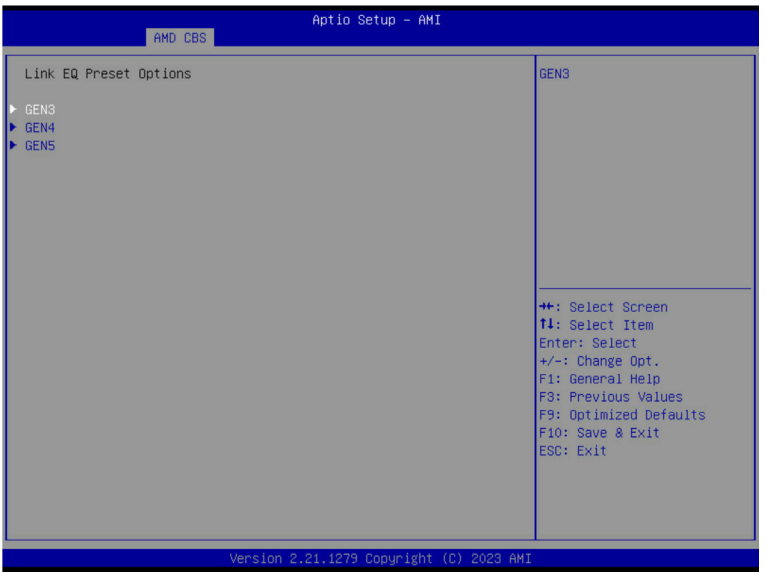


Parameter	Description
MPDMA-TF	◆ SRIOV – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ ARI – Options available: Auto/Default, Disabled, Enabled. Default setting is **Auto/Default**. ◆ AER – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ ACS – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ ATS – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PASID – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ RTR – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PAGE_REQ – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PWR – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ ATC_ENABLE – Options available: Auto, Disabled, Enabled. Default setting is **Auto**.

Parameter	Description
MPDMA-TF (continued)	◆ SDXI Class Code – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PASID Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ ATOMICOP_REQUEST – Options available: Auto, Disabled, Enabled. Default setting is **Auto**.
RCC_DEV0	◆ ACS Rcc_Dev0 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ AER Rcc_Dev0 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ DlfEnableStrap1 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ Phy16GTStrap1 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ MarginEnStrap1 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ SourceValStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ TranslationalBlockingStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ P2pReq ACS Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ P2pCompStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ UpstreamFwdStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ P2PEgressStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ DirectTranslatedStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ SsidEnStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PriEnPageReq – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ PriResetPageReq – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ SourceVal ACS cntl – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ TranslationalBlocking ACS Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ P2pComp ACS Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ UpstreamFwd ACS Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**.

Parameter	Description
RCC_DEV0 (continued)	◆ P2PEgress ACS Control – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ P2pReqStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ E2E_PREFIX – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ EXTENDED_FMT – Options available: Auto, Disabled, Enabled. Default setting is **Auto**. ◆ AtomicRoutingStrap5 – Options available: Auto, Disabled, Enabled. Default setting is **Auto**.

5-3-4-4 Link EQ Preset Options



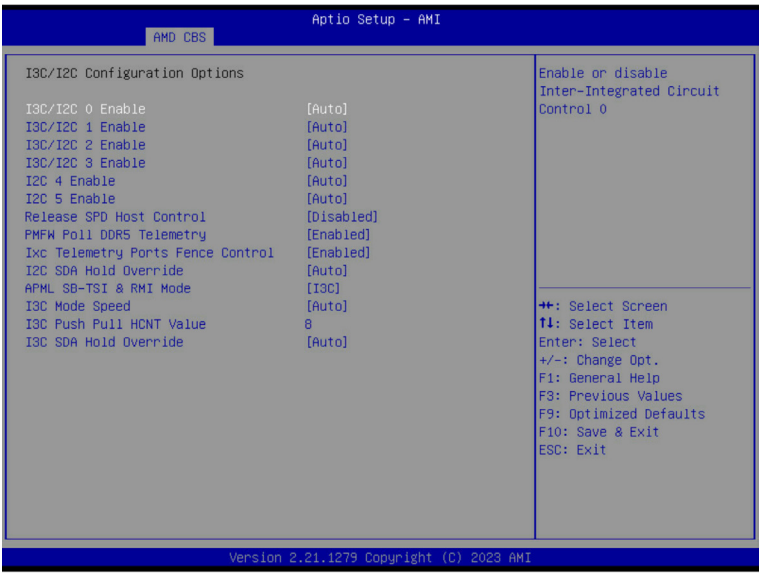
Parameter	Description
GEN3/4/5	Press [Enter] to configure advanced items. ◆ Preset Search Mask Configuration – Options available: Custom, Auto. Default setting is **Auto**.

5-3-5 FCH Common Options



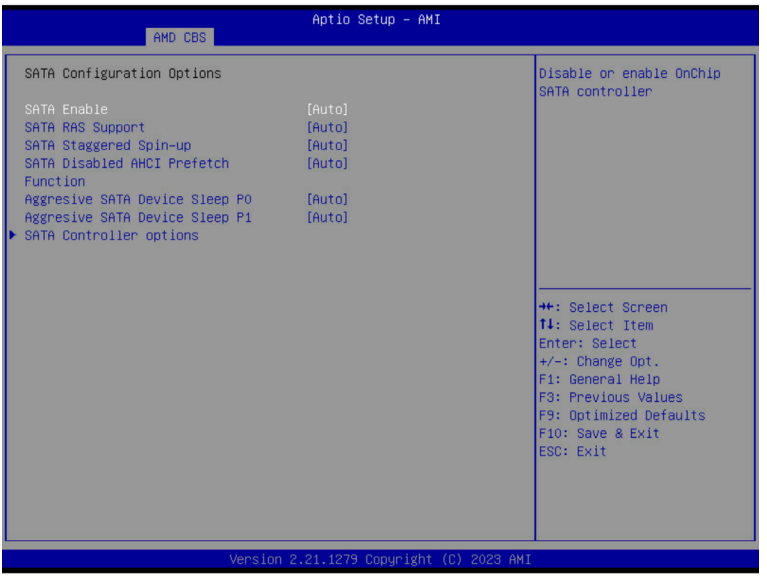
Parameter	Description
FCH Common Options	
I3C/I2C Configuration Options	Press [Enter] for configuration of advanced items.
SATA Configuration Options	Press [Enter] for configuration of advanced items.
USB Configuration Options	Press [Enter] for configuration of advanced items.
AC Power Loss Options	Press [Enter] for configuration of advanced items.
Uart Configuration Options	Press [Enter] for configuration of advanced items.
ESPI Configuration 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 I3C/I2C Configuration Options



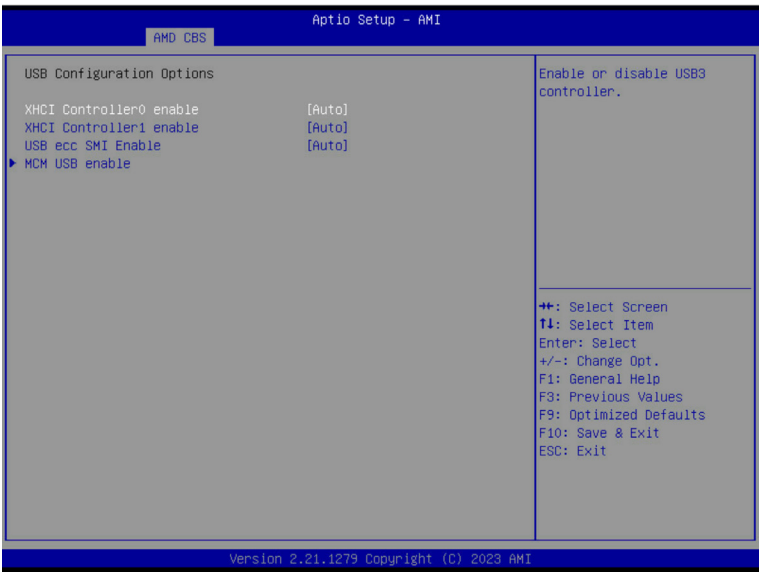
Parameter	Description
I3C/I2C Configuration Options	
I3C/I2C 0/1/2/3 Enable	Options available: Both Disabled, I3C Enabled, I2C Enabled, Auto. Default setting is **Auto**.
I2C 4/5 Enable	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Release SPD Host Control	Options available: Disabled, Enabled. Default setting is **Disabled**.
PMFW Poll DDR5 Telemetry	Options available: Disabled, Enabled. Default setting is **Enabled**.
Ixc Telemetry Ports Fence Control	Options available: Disabled, Enabled. Default setting is **Disabled**.
I2C SDA Hold Override	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
APML SB-TSI $ RMI Mode	Options available: I3C, I2C. Default setting is **I3C**.
I3C Mode Speed	Options available: SDR2(6MHz), SDR0(12.5MHz), Auto. Default setting is **Auto**.
I3C Push Pull HCNT Value	SCL push-pull High count for I3C transfers targeted to I3C devices.
I3C SDA Hold Override	Override I3C SDA Hold value. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

5-3-5-2 SATA Configuration Options



Parameter	Description
SATA Configuration Options	
SATA Enable	Enable/Disable OnChip SATA controller. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SATA RAS Support	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SATA Staggered Spin-up	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SATA Disabled AHCI Prefetch Function	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Aggressive SATA Device Sleep P0/P1	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
SATA Controller options	Press [Enter] for configuration of advanced items. ◆ SATA Controller Enable ◆ SATA Controller eSATA ◆ SATA Controller DevSlp ◆ SATA Controller SGPIO

5-3-5-3 USB Configuration Options



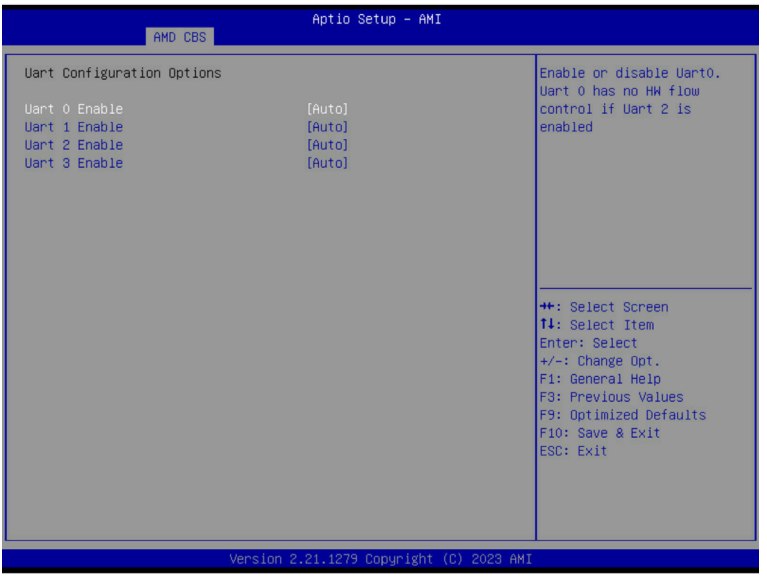
Parameter	Description
USB Configuration Options	
XHCI Controller0/1 enable	Enable/Disable USB controller. Options available: Enabled, Disabled, Auto. Default setting is **Auto**.
USB ecc SMI Enable	Options available: Enable, Off, Auto. Default setting is **Auto**.
MCM USB enable	Press [Enter] for configuration of advanced items. ◆ XHCI2/ XHCI3 enable (Socket1) – Options available: Enabled, Disabled, Auto. Default setting is **Auto**.

5-3-5-4 AC Power Loss Options



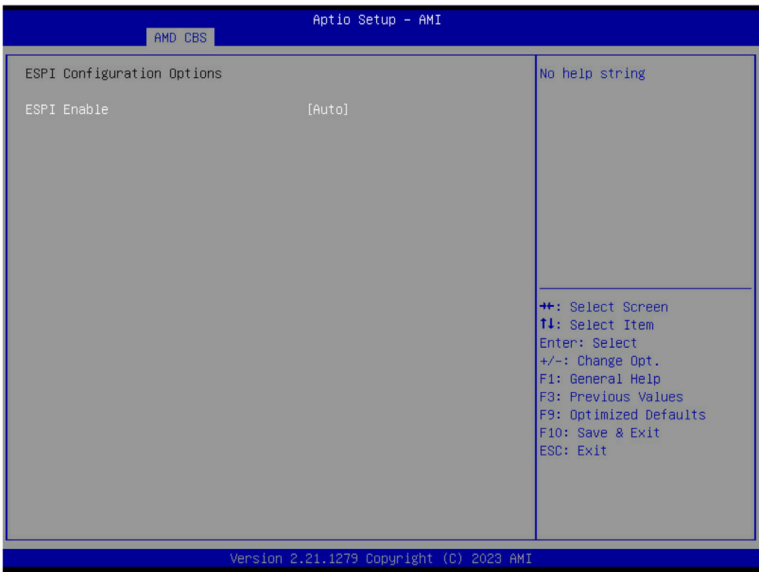
Parameter	Description
AC Power Loss Options	
AC Loss Control	Selects the AC Loss Control Method. Options available: Power Off, Power On, Last State. Default setting is **Last State**.

5-3-5-5 Uart Configuration Options



Parameter	Description
Uart Configuration Options	
Uart 0/1/2/3 Enable	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

5-3-5-6 ESPI Configuration Options



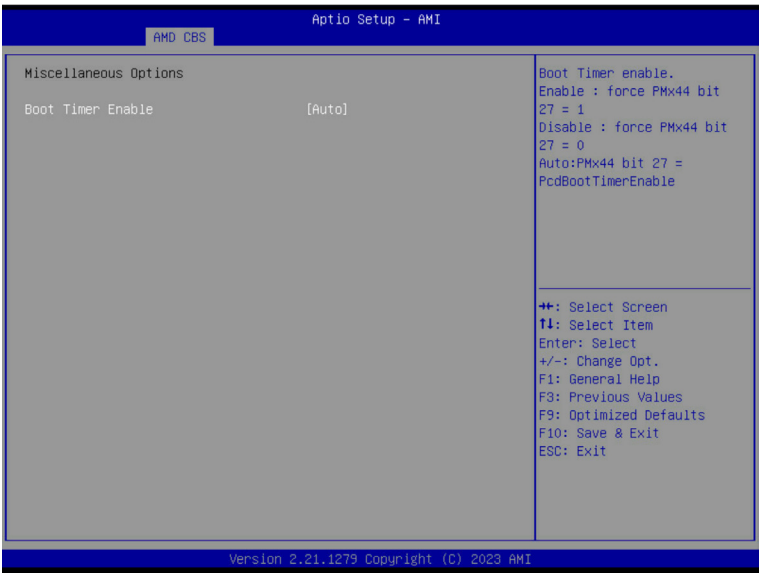
Parameter	Description
ESPI Configuration Options	
ESPI Enable	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

5-3-5-7 FCH RAS Options



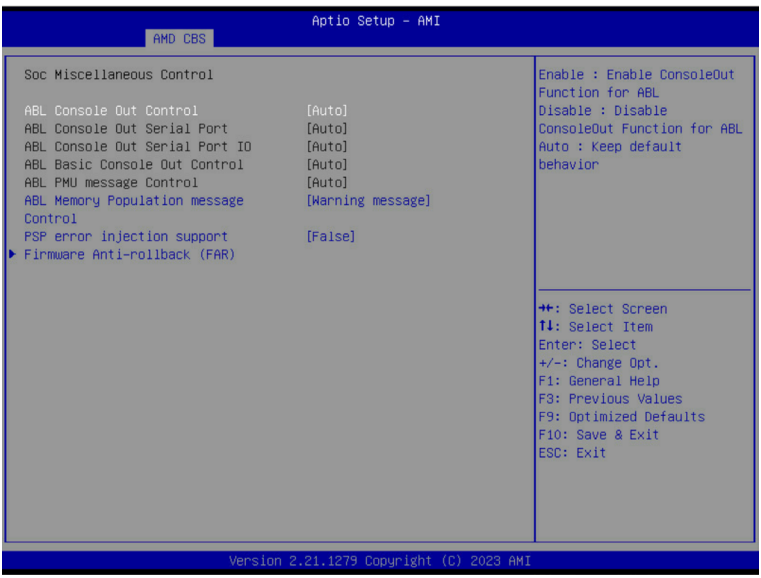
Parameter	Description
FCH RAS Options	
ALink RAS Support	Enable/Disable the ALink RAS Support. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Reset After Sync-Flood	Enables AB to forward downstream sync-flood message to system controller. Options available: Enable, Disable,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

5-3-5-8 Miscellaneous Options



Parameter	Description
Miscellaneous Options	
Boot Timer Enable	Enable/Disable Boot Timer. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

5-3-6 SOC Miscellaneous Control

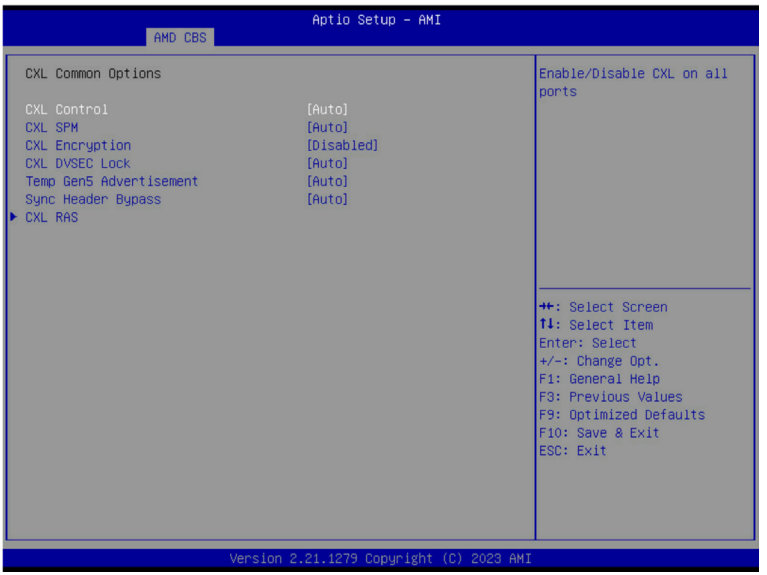


Parameter	Description
SOC Miscellaneous Control	
ABL Console Out Control(Note)	Enable/Disable the ConsoleOut function for ABL. Options available: Disable, Enable, Auto. Default setting is **Auto**.
ABL Console Out Serial Portl(Note)	Options available: eSPI, SOC UART0, SOC UART1, Auto. Default setting is **Auto**.
ABL Console Out Serial Port IO	Options available: 0x3F8, 0x2F8, 0x3E8, 0x2E8, Auto. Default setting is **Auto**.
ABL Basic Console Out Control	Enable/Disable the Basic ConsoleOut function for ABL. Options available: Disable, Enable, Auto. Default setting is **Auto**.
ABL PMU message Control	To Control the total number of PMU debug messages. Options available: Auto, Detailed debug message, Coarse debug message, Stage completion, Assertion messages, Firmware completion message only. Default setting is **Auto**.
ABL Memory Population message Control	Options available: Warning message, Fatal error. Default setting is **Warning message**.
PSP error injection support	Options available: False, True. Default setting is **False**.

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

Parameter	Description
Firmware Anti-rollback (FAR)	Press [Enter] for configuration of advanced items. ◆ FAR enforcement state – Default setting is **Enabled**. ◆ SPL value in the CPU Fuse ◆ SPL value in the SPL table ◆ FAR Switch – Options available: Disabled, Enabled, Auto. Default setting is **Auto**.

5-3-7 CXL Common Options



Parameter	Description
CXL Common Options	
CXL Control	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
CXL SPM	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
CXL Encryption	Options available: Enabled, Disabled. Default setting is **Disabled**.
CXL DVSEC Lock	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Temp Gen5 Advertisement	Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Sync Header Bypass	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
CXL RAS	Press [Enter] for configuration of advanced items. ◆ CXL Protocol Error Reporting – Options available: Disabled, SameAsPcieAer, ForceAerFwFirstIfCxlPresent. Default setting is **SameAsPcieAer**. ◆ CXL Component Error Reporting – Options available: OS First, FW-First. Default setting is **FW-First**.

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.
SPI Locking	Enable/Disable SPI Locking for protect ROM part. Options available: Disabled, Enabled. Default setting is **Disabled**.
CXL Range Encryption	Press [Enter] for configuration of advanced items. ◆ Range1/2/3/4/5/6/7 – Configure the Range 1/2/3/4/5/6/7 Memory Base. – Configure the Range 1/2/3/4/5/6/7 Memory Limit/Size. ◆ Start CXL Range Encryption

5-4-1 RAS

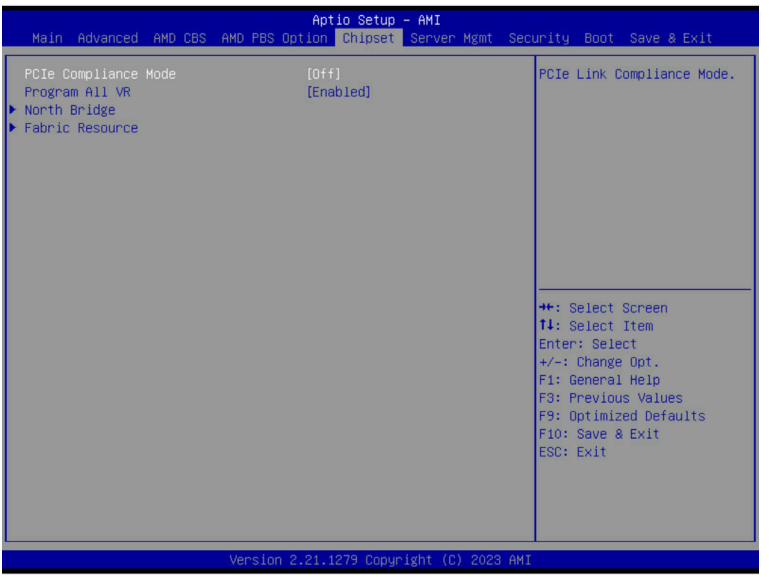


Parameter	Description
RAS Periodic SMI Control	Enable/Disable the Periodic SMI for polling [MCA Threshold] error. Options available: Disabled, Enabled. Default setting is **Enabled**.
SMI Threshold	Configures the SMI Threshold value.
SMI Scale	Configures the SMI Scale value.
SMI Scale Unit	Defines the 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.
DRAM Hard Post Package Repair	This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism. Options available: Disabled, Enabled. Default setting is **Disabled**.
HEST DMC Structure Support	HEST DMC (Deferred Machine Check) Structure Support. Options available: Disabled, Enabled. Default setting is **Disabled**.
CXL Error Report Support	Enable/Disable CXL Error Reporting. Options available: Disabled, Enabled. Default setting is **Disabled**.

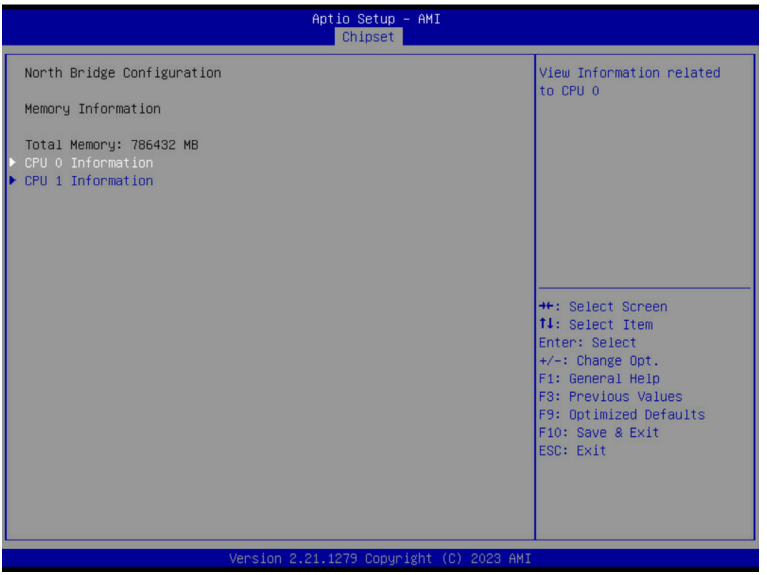
5-5 Chipset Setup Menu

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.



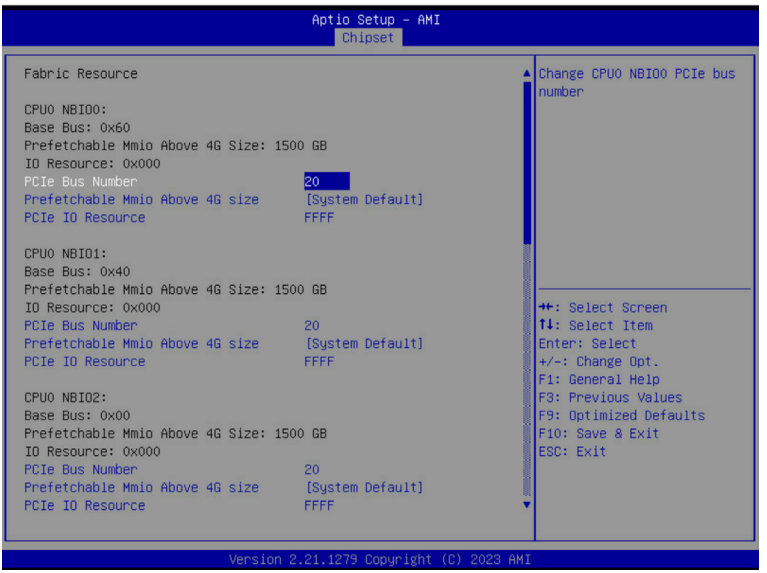
Parameter	Description
PCIe Compliance Mode	Options available: Off, On. Default setting is **Off.**
Program All VR	Enable/Disable program all VR on MB. Options available: Disabled, Enabled. Default setting is **Enabled**.
North Bridge	Press [Enter] for configuration of advanced items.
Fabric Resource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

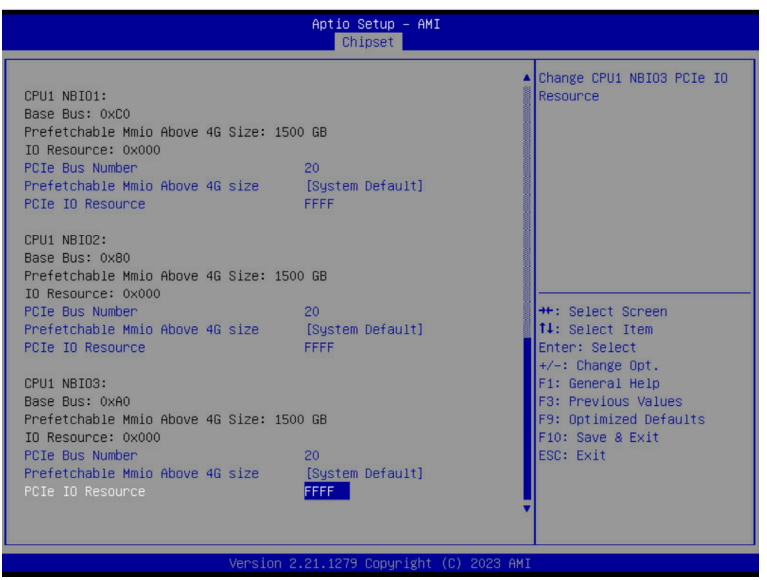
5-5-1 North Bridge



Parameter	Description
North Bridge Configuration Memory Information	
Total Memory	Displays the total memory information.
CPU 0/1 Information	Press [Enter] to view information related to CPU 0/1.

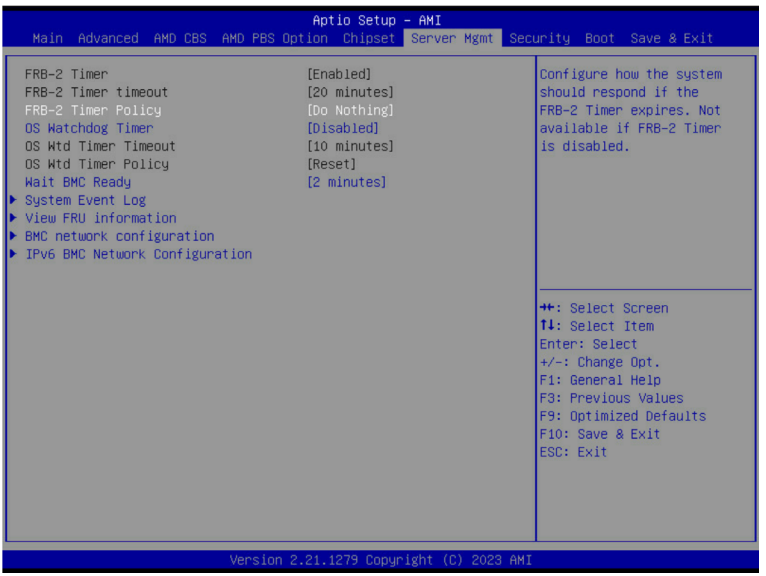
5-5-2 Fabric Resource





Parameter	Description
Fabric Resource	
CPU 0/1 NBIO_# PCIe Bus Number	Change CPU 0/1 NBIO_# PCIe Bus Number.
Prefetchable Mmio Above 4G size	Change CPU 0/1 NBIO_# Prefetchable MMIO Above 4G Size. Options available: System Default, 0, 1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, 512G, 1T, 2T, 4T, 8T. Default setting is **System Default**.
PCIe IO Resource	Change CPU 0/1 NBIO_# PCIe IO Resource.

5-6 Server Management Menu

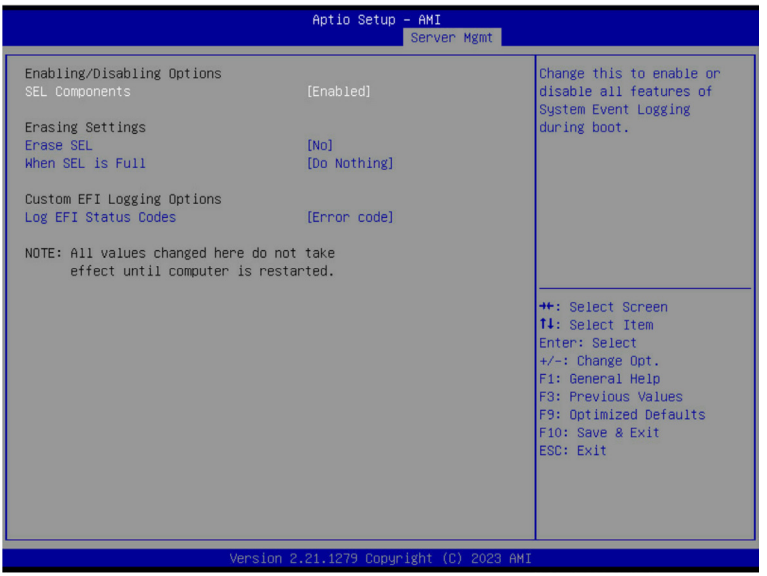


Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Default setting is **Enabled**.
FRB-2 Timer timeout	Configures the FRB-2 Timer timeout. Default setting is **20 minutes**.
FRB-2 Timer Policy	Configures the FRB-2 Timer policy. Options available: Do Nothing, Reset, Power Down, 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(Note)	Configures OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is **10 minutes**.
OS Wtd Timer Policy(Note)	Configure OS Watchdog Timer Policy. Options available: Do Nothing, Reset, Power Down, Power Cycle. Default setting is **Reset**.
Wait BMC Ready	Post wait BMC ready and reboot system. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is **2 minutes**.

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

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

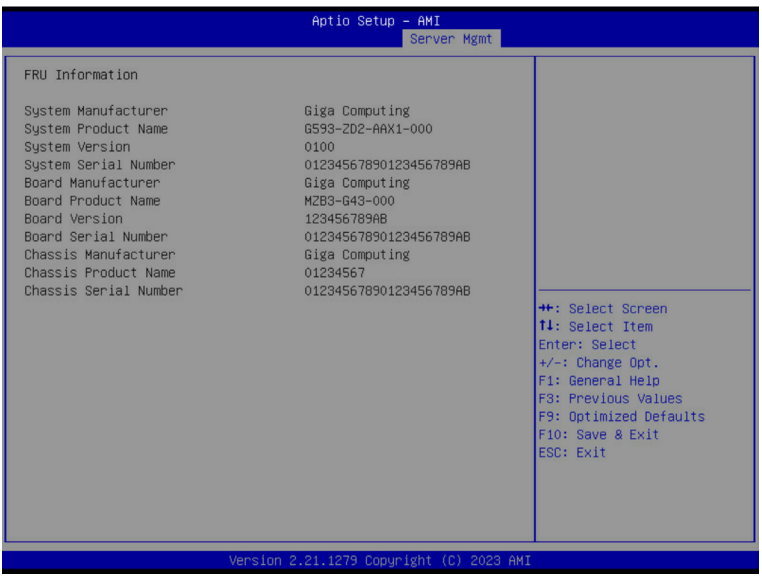
5-6-1 System Event Log



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

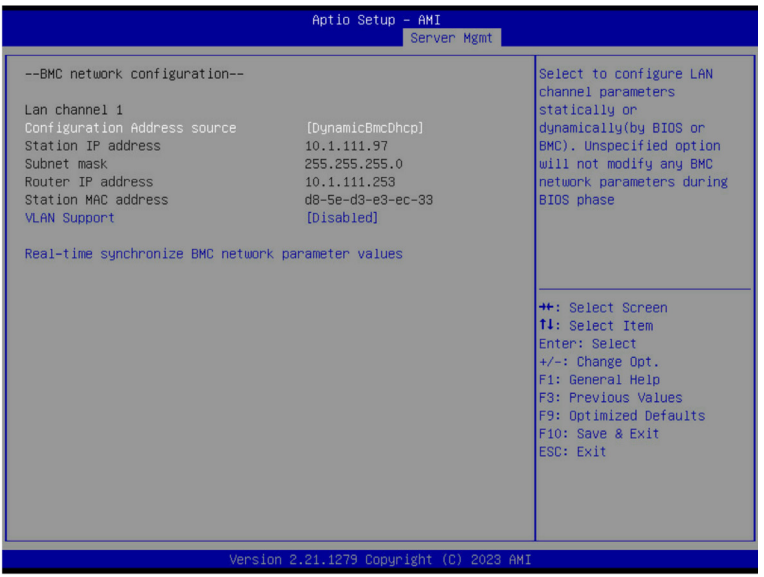
5-6-2 View FRU Information

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 BMC to enable/disable VLAN support. Options available: Enabled, Disabled. Default setting is **Disabled**.
Real-time synchronize BMC network parameter values	Press [Enter] will set Address source(Static/DHCP) to BMC and then get Station IP address, Subnet mask and Router IP address from BMC.

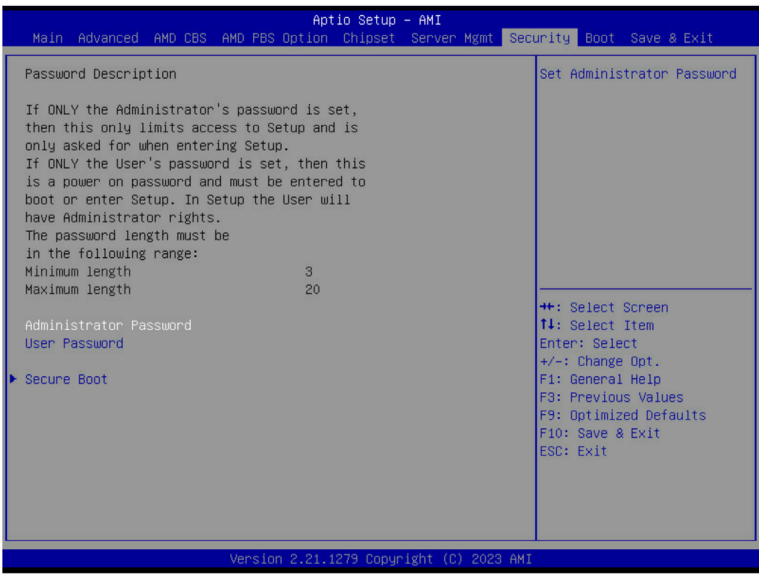
5-6-4 IPv6 BMC Network Configuration



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 **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 feature is applicable if supported by your Operating System. If your Operating System is not supporting Secure Boot, the system will hang when starting the Operating System.



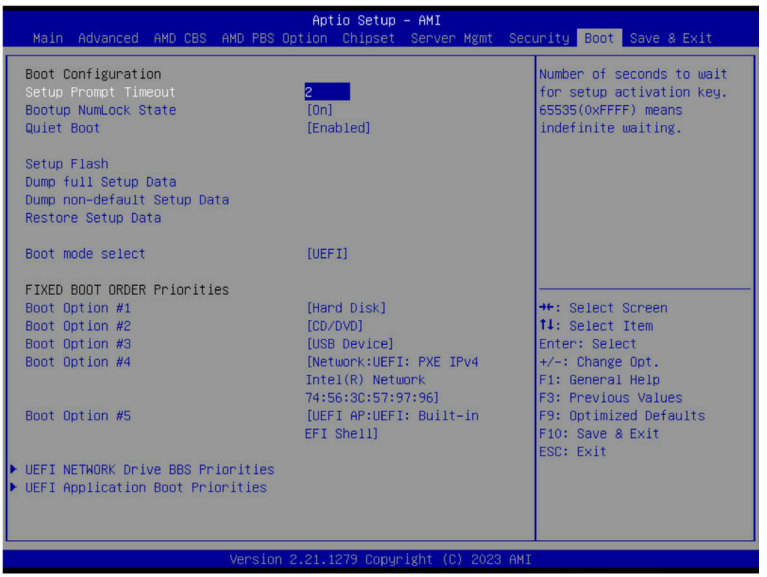
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, Disabled. Default setting is **Disabled**.
Secure Boot Mode(Note)	Secure Boot requires all the applications that are running during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

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

Parameter	Description
Key Management	Press [Enter] to configure advanced items. **Please note that this item is configurable when Secure Boot Mode is set to Custom.** ◆ Factory Key Provision – Allows to provision factory default Secure Boot keys when system is in Setup Mode. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Restore Factory Keys – Installs all factory default keys. It will force the system in User Mode. – Options available: Yes, No. ◆ Enroll Efi Image – Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). ◆ Secure Boot variable – Displays the current status of the variables used for secure boot. ◆ Platform Key (PK) – Displays the current status of the Platform Key (PK). – Press [Enter] to configure a new PK. – Options available: Update. ◆ Key Exchange Keys (KEK) – Displays the current status of the Key Exchange Key Database (KEK). – Press [Enter] to configure a new KEK or load additional KEK from storage devices. – Options available: Update, Append. ◆ Authorized Signatures (DB) – Displays the current status of the Authorized Signature Database. – Press [Enter] to configure a new DB or load additional DB from storage devices. – Options available: Update, Append. ◆ Forbidden Signatures (DBX) – Displays the current status of the Forbidden Signature Database. – Press [Enter] to configure a new dbx or load additional dbx from storage devices. – Options available: Update, Append. ◆ Authorized TimeStamps (DBT) – Displays the current status of the Authorized TimeStamps Database. – Press [Enter] to configure a new DBT or load additional DBT from storage devices. – Options available: Update, Append. ◆ OsRecovery Signatures – Displays the current status of the OsRecovery Signature Database. – Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices. – Options available: Update, Append.

5-8 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.

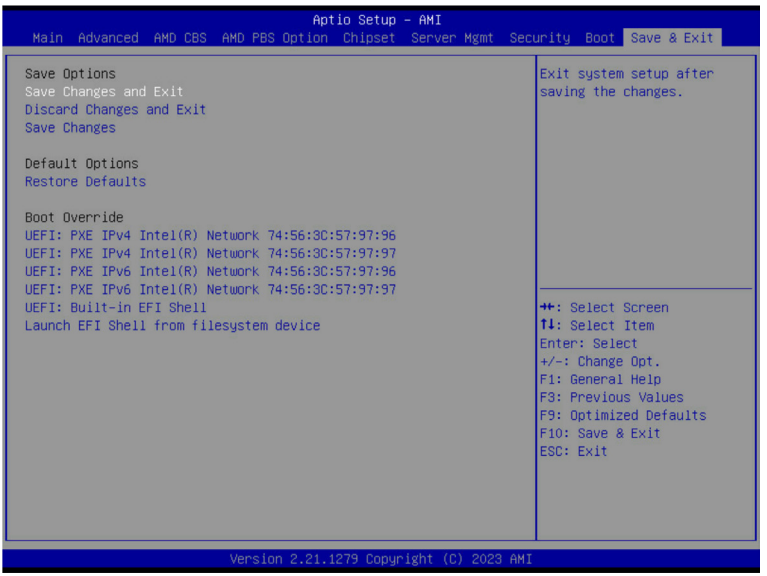


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off.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

5-9 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>.



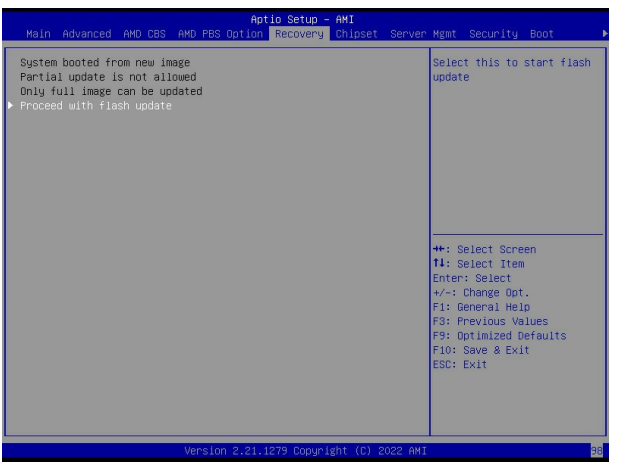
Parameter	Description
Save Options	
Save Changes and Exit	Saves changes made and closes the BIOS setup. Options available: Yes, No.
Discard Changes and Exit	Discards changes made and exits the BIOS setup. Options available: Yes, No.
Save Changes	Saves changes done so far to any of the setup options. 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 file system devices.

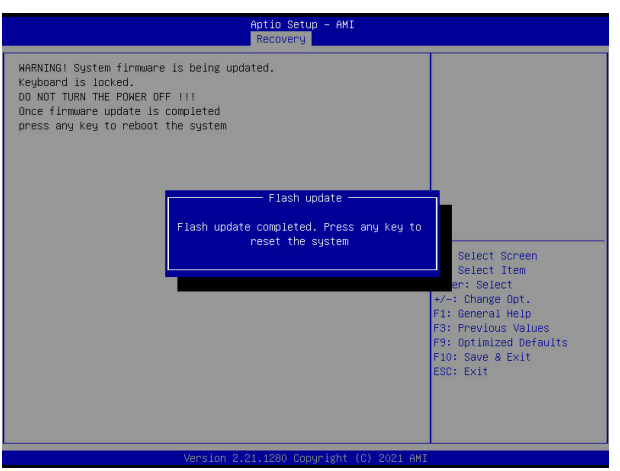
5-10 BIOS Recovery

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

Recovery Instruction:

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





5-11 BIOS POST Beep code (AMI standard)

5-11-1 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	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

5-11-2 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