

GIGABYTE™

S252-ZC0

2U 24+2-Bay DP Storage Server (AMD MILAN/ ROME)

User Manual

Rev. 1.0

Copyright

© 2021 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.

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

Disclaimer

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

Documentation Classifications

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

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

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

For More Information

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




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

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

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

Conventions

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

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

Server Warnings and Cautions

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



WARNING!

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

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply 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 not suitable for use in locations where children are likely to be present.



CAUTION!

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



CAUTION!

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

Electrostatic Discharge (ESD)



CAUTION!

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

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

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

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

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

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

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

Table of Contents

Chapter 1 Hardware Installation	9
1-1 Installation Precautions	9
1-2 Product Specifications	10
1-3 System Block Diagram	13
Chapter 2 System Appearance	14
2-1 System Overview	14
2-2 Front View	15
2-3 Rear View	15
2-4 Side View	16
2-5 Front Panel LEDs and Buttons	17
2-6 Rear System LEDs and Buttons	18
2-7 Power Supply Unit LED	19
2-8 Hard Disk Drive LEDs	20
Chapter 3 System Hardware Installation	21
3-1 Removing Chassis Cover	22
3-2 Power Supply Module	23
3-3 Removing the Heat Sink	24
3-4 Installing the CPU	25
3-5 Installing the Memory	27
3-5-1 Eight Channel Memory Configuration	27
3-5-2 Installing a Memory	28
3-5-3 Processor and Memory Module Matrix Table	28
3-5-4 Memory Population Table	29
3-6 Installing the PCI Expansion Card	30
3-7 Installing the Hard Disk Drive	31
3-8 Removing and installing the Fan Wall	33
3-9 Replacing the Fan Assembly	34
3-10 Replacing the Power Supply	35
3-11 Cable Routing	36
Chapter 4 Motherboard Components	42
4-1 Motherboard Components	42
4-2 Jumper Settings	44
4-3 Backplane Board Storage Connector	45
4-3-1 Left Side: CBPD2C0	45

4-3-2	Right Side: CBPD2C1	45
4-3-3	Rear Side: CBPD020.....	45
Chapter 5	BIOS Setup	46
5-1	The Main Menu	48
5-2	Advanced Menu	51
5-2-1	Trusted Computing.....	53
5-2-2	PSP Firmware Versions.....	54
5-2-3	Legacy Video Select.....	55
5-2-4	AST2500 Super IO Configuration.....	56
5-2-5	S5 RTC Wake Settings.....	59
5-2-6	Serial Port Console Redirection	60
5-2-7	CPU Configuration.....	64
5-2-8	PCI Subsystem Settings.....	65
5-2-9	USB Configuration.....	67
5-2-10	Network Stack Configuration	69
5-2-11	NVMe Configuration	70
5-2-12	SATA Configuration.....	71
5-2-13	UEFI POST LOGO Configuration	72
5-2-14	AMD Mem Configuration Status.....	73
5-2-15	T1s Auth Configuration.....	74
5-2-16	iSCSI Configuration.....	75
5-3	AMD CBS Menu.....	76
5-3-1	CPU Common Options.....	77
5-3-2	DF Common Options.....	83
5-3-3	UMC Common Options	88
5-3-4	NBIO Common Options.....	103
5-3-5	FCH Common Options	109
5-3-6	NTB Common Options	113
5-3-7	SOC Miscellaneous Control	114
5-3-8	Workload Tuning.....	115
5-4	AMD PBS Menu.....	116
5-4-1	RAS.....	117
5-5	Chipset Setup Menu.....	119
5-5-1	North Bridge	120
5-5-2	Fabric Resource	121
5-6	Server Management Menu.....	122
5-6-1	System Event Log	124
5-6-2	View FRU Information	125
5-6-3	BMC Network Configuration.....	126
5-6-4	IPv6 BMC Network Configuration.....	127
5-7	Security Menu	128

5-7-1	Secure Boot	129
5-8	Boot Menu.....	131
5-9	Save & Exit Menu.....	133
5-10	BIOS POST Beep code (AMI standard).....	134
5-10-1	PEI Beep Codes.....	134
5-10-2	DXE Beep Codes	134

Chapter 1 Hardware Installation

1-1 Installation Precautions

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









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







1-2 Product Specifications



NOTE:

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

 System Dimension	<ul style="list-style-type: none"> ◆ 2U ◆ 438 (W) x 87 (H) x 880 (D) mm
 CPU	<ul style="list-style-type: none"> ◆ AMD EPYC™ 7003 series processor family ◆ Dual processors, 7nm, Socket SP3 ◆ Up to 64-core, 128 threads per processor ◆ cTDP up to 180W <p>Compatible with AMD EPYC™ 7002 series processor family</p>
 Chipset	<ul style="list-style-type: none"> ◆ System on Chip
 Hardware-Level Root of Trust Support	<ul style="list-style-type: none"> ◆ Supported <p>NOTE! The system will take extra time to boot as it goes through RoT authentication.</p>
 Memory	<ul style="list-style-type: none"> ◆ Total 16 x DIMM slots ◆ DDR4 memory supported only ◆ 8-Channel memory architecture ◆ RDIMM modules up to 128GB supported ◆ LRDIMM modules up to 128GB supported ◆ Memory speed: Up to 3200/ 2933 MHz
 LAN	<ul style="list-style-type: none"> ◆ 1 x 10/100/1000 management LAN
 Video	<ul style="list-style-type: none"> ◆ Integrated in Aspeed® AST2500 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
 Storage	<ul style="list-style-type: none"> ◆ Side-accessed: 24 x 3.5" SAS/SATA hot-swappable HDD/SSD bays ◆ LSI SAS35x36R expander ◆ SAS card is required to enable 24 drive bays ◆ Rear Side: 2 x 2.5" SATA hot-swappable HDD/SSD bays, NVMe supported with optional CNV3022 NVMe Card ◆ Default configuration supports: 2 x SATA drives in rear side ◆ Recommend optional 12Gb/s SAS cards: CRA4448 (Hardware RAID Card) CSA4648 (Software HBA Card)

	Expansion Slot	Total 6 x low profile PCIe Gen4 expansion slots
<ul style="list-style-type: none"> ◆ Slot_6: 1 x PCIe x16 (Gen4 x16 bus) slot ◆ Slot_5: 1 x PCIe x16 (Gen4 x16 bus) slot ◆ Slot_4: 1 x PCIe x16 (Gen4 x16 bus) slot ◆ Slot_3: 1 x PCIe x16 (Gen4 x16 bus) slot ◆ Slot_2: 1 x PCIe x16 (Gen4 x16 bus) slot ◆ Slot_1: 1 x PCIe x16 (Gen4 x16 bus) slot 		
	Internal I/O	<ul style="list-style-type: none"> ◆ 1 x CPU fan header ◆ 6 x System fan headers ◆ 1 x USB 3.0 header ◆ 1 x TPM header ◆ 1 x VROC connector ◆ 1 x Front panel header ◆ 1 x Buzzer
	Front I/O	<ul style="list-style-type: none"> ◆ 2 x USB 3.0 ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x Reset button ◆ 1 x System status LED ◆ 1 x HDD activity LED
	Rear I/O	<ul style="list-style-type: none"> ◆ 2 x USB 3.0 ◆ 1 x VGA ◆ 1 x MLAN ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x System status LED
	Backplane I/O	<ul style="list-style-type: none"> ◆ Left Side: CBPD2C0: 12 x 3.5" SAS/SATA ports with expander ◆ Right Side: CBPD2C1: 12 x 3.5" SAS/SATA ports ◆ Rear Side: CBPD020: 2 x 2.5" NVMe/SATA hybrid ports
	TPM	<ul style="list-style-type: none"> ◆ 1 x TPM header with SPI interface ◆ Optional TPM2.0 kit: CTM010



Power Supply

- ◆ 1+1 80 PLUS Platinum 1300W redundant PSU ; 80 PLUS Platinum
- ◆ AC Input:
 - 100-240V~/ 12-7A, 50-60Hz
 - 200-240V~/ 8A, 50-60Hz
- ◆ DC Input: 240Vdc/ 6.5A
- ◆ DC Output:
 - Max 1000W/ 100-240V~
 - +12V/ 80.5A
 - +12Vsb/ 3A
 - Max 1300W/ 200-240V~ or 240Vdc Input
 - +12V/ 105.4A
 - +12Vsb/ 3A



System Management

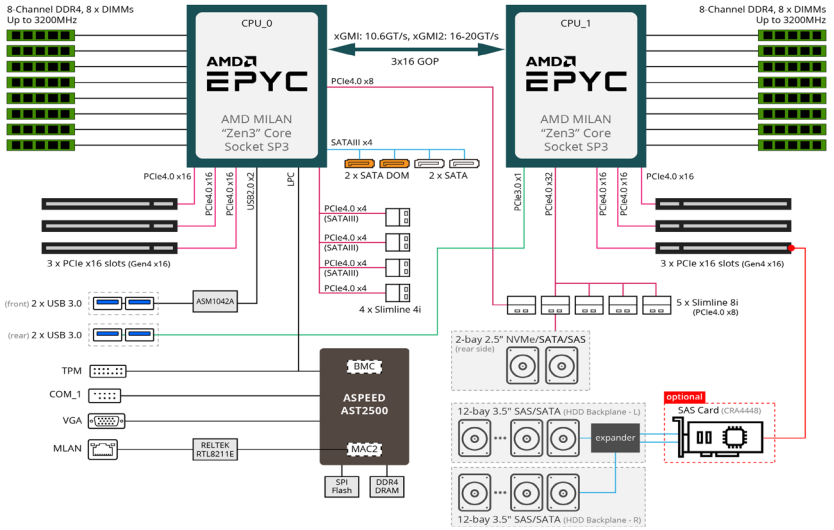
- ◆ Aspeed® AST2500 management controller
- ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface
- ◆ Dashboard
- ◆ JAVA Based Serial Over LAN
- ◆ HTML5 KVM
- ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)
- ◆ Sensor Reading History Data
- ◆ FRU Information
- ◆ SEL Log in Linear Storage / Circular Storage Policy
- ◆ Hardware Inventory
- ◆ Fan Profile
- ◆ System Firewall
- ◆ Power Consumption
- ◆ Power Control
- ◆ LDAP / AD / RADIUS Support
- ◆ Backup & Restore Configuration
- ◆ Remote BIOS/BMC/CPLD Update
- ◆ Event Log Filter
- ◆ User Management
- ◆ Media Redirection Settings
- ◆ PAM Order Settings
- ◆ SSL Settings
- ◆ SMTP Settings



Operating Properties

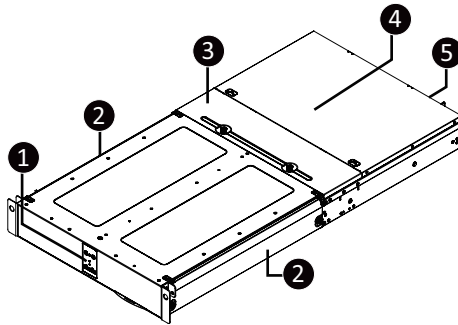
- ◆ Operating temperature: 10°C to 35°C
- ◆ Operating humidity: 8% to 80% (non-condensing)
- ◆ Non-operating temperature: -40°C to 60°C
- ◆ Non-operating humidity: 20% to 95% (non-condensing)

1-3 System Block Diagram



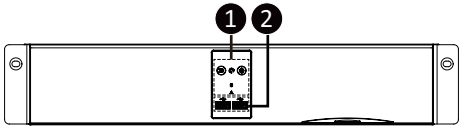
Chapter 2 System Appearance

2-1 System Overview



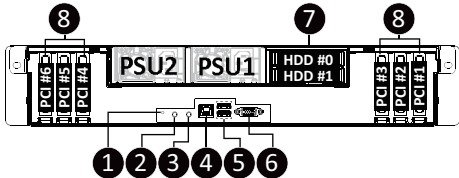
No.	Description
1.	Front Panel Buttons and LEDs
2.	Side 3.5" Hard Drives Cover
3.	System Middle Cover
4.	System Back Cover
5.	Power Supply Units

2-2 Front View



No.	Description
1.	Front Panel LEDs and Buttons
2.	USB 3.0 Port x 2

2-3 Rear View



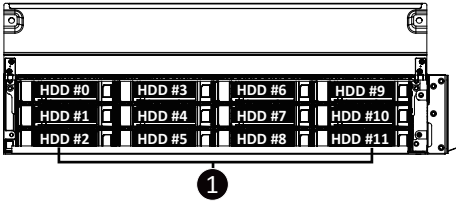
No.	Description
1.	System Status LED
2.	Power Button with LED
3.	ID Button with LED
4.	Server Management LAN Port
5.	USB3.0 Port x 2
6.	VGA Port
7.	2.5" HDD Bays
8.	PCIe Card Slot x6



Refer to section **2-5 Front Panel LEDs and Buttons** and section **2-6 Rear System LEDs and Buttons** for a detailed description of the function of the LEDs.

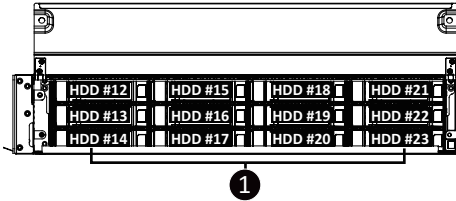
2-4 Side View

Left Side



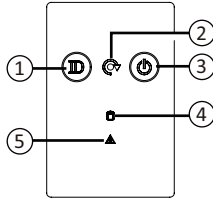
No.	Description
1.	3.5" HDD Bays

Right Side



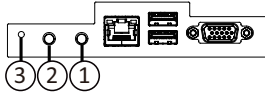
No.	Description
1.	3.5" HDD Bays

2-5 Front Panel LEDs and Buttons

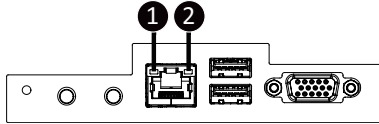


No.	Name	Color	Status	Description
1.	ID Button			Press the button to activate system identification
2.	Reset button	--	--	Press this button to reset the system.
3.	Power button with LED	Green	On	Indicates the system is powered on.
		Green	Blink	System is in ACPI S1 state (sleep mode).
		N/A	Off	<ul style="list-style-type: none"> System is not powered on or in ACPI S5 state (power off) System is in ACPI S4 state (hibernate mode)
4.	HDD Status LED	Amber	On	Indicates locating the HDD.
			Blink	Indicates accessing the HDD.
		N/A	On	Indicates HDD error.
5.	System Status LED	N/A	Solid On	System is operating normally.
			Solid On	Critical condition, may indicate: System fan failure; System temperature
		Red	Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion

2-6 Rear System LEDs and Buttons

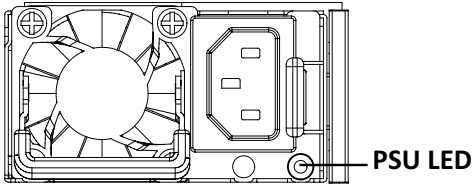


No.	Name	Color	Status	Description
1.	ID Button			Press the button to activate system identification
2.	Power button with LED	Green	On	Indicates the system is powered on.
		Green	Blink	System is in ACPI S1 state (sleep mode).
		N/A	Off	<ul style="list-style-type: none"> System is not powered on or in ACPI S5 state (power off) System is in ACPI S4 state (hibernate mode)
3.	System Status LED	Green	Solid On	System is operating normally.
		Red	Solid On	Critical condition, may indicate: System fan failure; System temperature
			Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion



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

2-7 Power Supply Unit LED



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

2-8 Hard Disk Drive LEDs



	LED1 (Green)	LED1 (Red)	LED2 (Blue)
Indicator	Drive activity	Drive locate/fault/rebuild	Drive present
Behavior	BLINK: Drives is active ON or OFF: Idle (depend on drive)	ON: Fault BLINK 4Hz: Locate BLINK 1Hz: Rebuild	ON: Drive is plugged in OFF: No drive

Chapter 3 System Hardware Installation



Pre-installation Instructions

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

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

3-1 Removing Chassis Cover

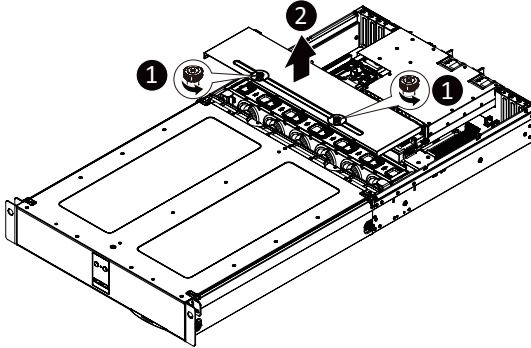


Before you remove or install the system cover

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

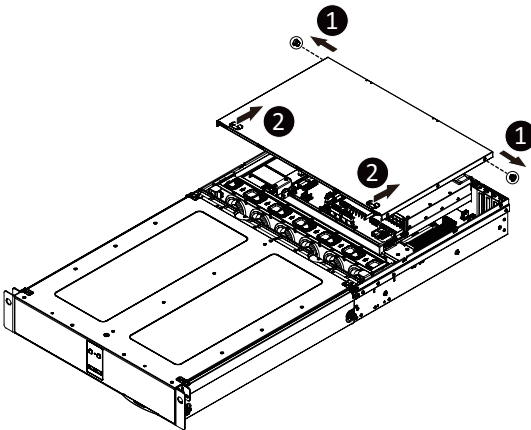
Follow these instructions to remove the middle chassis cover:

1. Loosen the thumbscrew securing the chassis cover.
2. Lift up to remove the middle chassis cover.
3. To reinstall the chassis cover reverse steps 1-2.



Follow these instructions to remove the back chassis cover:

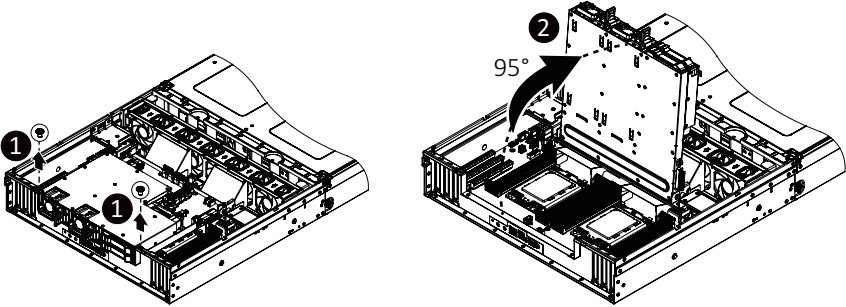
1. Remove the screw securing the chassis cover.
2. Push down the indentations and slide the cover backward to remove the cover.
3. To reinstall the chassis cover reverse steps 1-2.



3-2 Power Supply Module

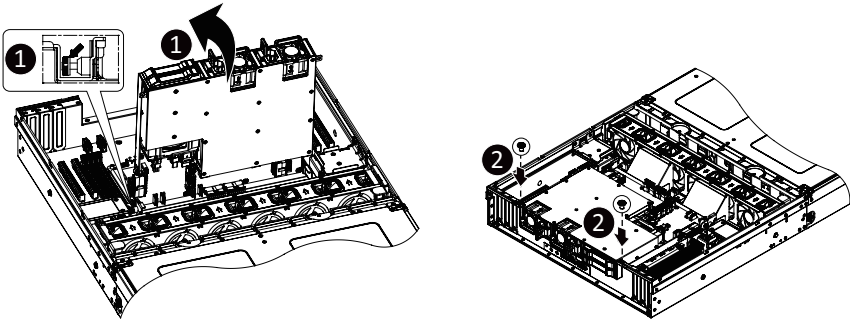
Follow these instructions to open the power supply module:

1. Remove the screw securing the power supply module.
2. Lift up the power supply module 95 degrees in the firmly position until a sound "Click" is heard.



Follow these instructions to close the power supply module:

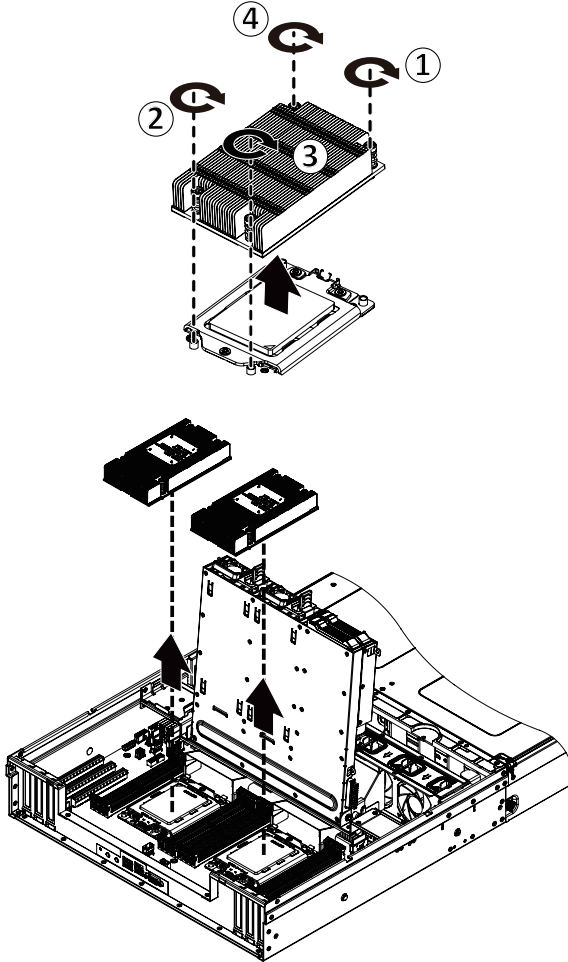
1. Push the latch to unlocked state and flip the power supply module into place simultaneously.
2. Tighten the power supply module with two screws.



3-3 Removing the Heat Sink

Follow these instructions to remove/install the fan duct:

1. Loosen the captive screws securing the heatsink in place in reverse order (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) as seen in the image below.



When installing the heatsink to CPU, use PHILLIPS #2-Lobe driver to tighten 4 captive nuts in sequence as 1-4. The screw tightening torque: $0 \pm 0.5 \text{ kgf-cm}$ ($22.0 \pm 1.0 \text{ lbf-in}$).

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!

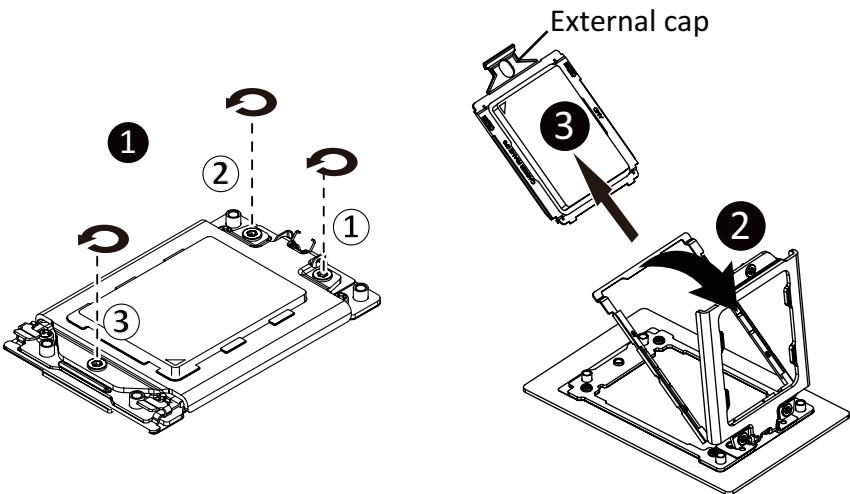
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

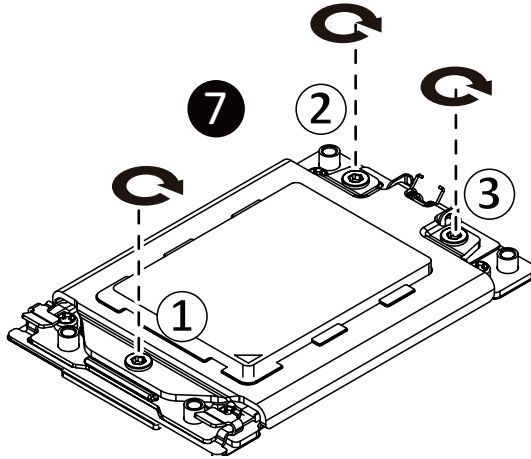
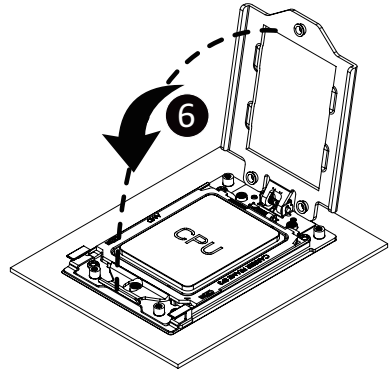
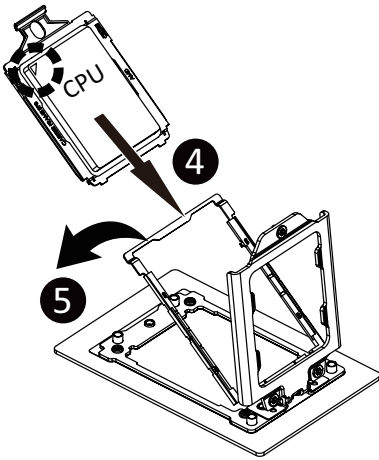
Follow these instructions to install the CPU:

1. Loosen the three captive screws securing the CPU cover in sequential order (1 → 2 → 3).
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 screws in sequential order (1 → 2 → 3) to secure the CPU cover in place.





- Tighten the CPU cover screws, use T20-Lobe driver to tighten 3 captive nuts in sequence as 1-3.
- The screw tightening torque: 16.1 ± 1.2 kgf-cm (14.0 ± 1.0 lbf-in).

3-5 Installing the Memory

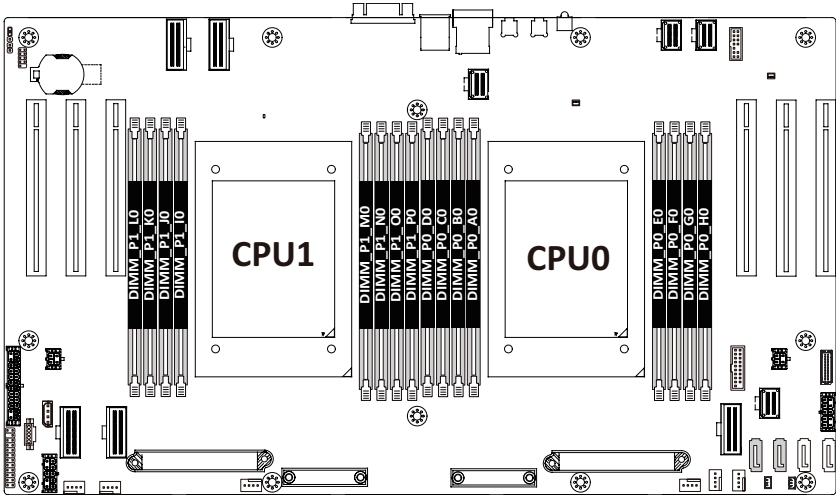


Read the following guidelines before you begin to install the memory:

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

3-5-1 Eight Channel Memory Configuration

This motherboard provides 16 DDR4 memory slots and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



3-5-2 Installing a Memory

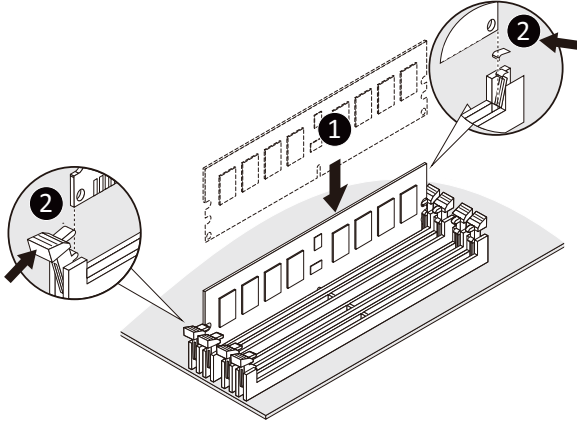


Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on this motherboard.

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

Processor and Memory Module Matrix Table																
CPU#	Channel A/I		Channel B/J		Channel C/K		Channel D/L		Channel E/M		Channel F/N		Channel G/O		Channel H/P	
8 DIMMs																
CPU0		A1		B1		C1		D1		E1		F1		G1		H1
16 DIMMs																
CPU0	A0	A1	B0	B1	C0	C1	D0	D1	E0	E1	F0	F1	G0	G1	H0	H1
16 DIMMs																
CPU0		A1		B1		C1		D1		E1		F1		G1		H1
CPU1		I1		J1		K1		L1		M1		N1		O1		P1
32 DIMMs																
CPU0	A0	A1	B0	B1	C0	C1	D0	D1	E0	E1	F0	F1	G0	G1	H0	H1
CPU1	I0	I1	J0	J1	K0	K1	L0	L1	M0	M1	N0	N1	O0	O1	P0	P1

3-5-4 Memory Population Table

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

DIMM Type	DIMM Population		Max EPYC 7003 DDR Frequency (MHz)
	DIMM 0		
RDIMM	1R (1 Rank)		3200
	2R or 2DR (2 Ranks)		3200
LRDIMM	4DR (4 Ranks)		3200
	2S2R (4 Ranks)		3200
	2S4R (8 Ranks)		3200
3DS	2S2R (4 Ranks)		3200
	2S4R (8 Ranks)		3200

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

DIMM Type	DIMM Population		Max EPYC 7003 DDR Frequency (MHz)
	DIMM 0	DIMM 1	
RDIMM	--	1R	3200
	1R	1R	2933
	--	2R or 2DR	3200
	1R	2R or 2DR	2933
	2R or 2DR	2R or 2DR	2933
LRDIMM	--	4DR	3200
	4DR	4DR	2933
	--	2S2R (4 Ranks)	3200
	--	2S4R (8 Ranks)	3200
	2S2R (4 Ranks)	2S2R (4 Ranks)	2933
	2S4R (8 Ranks)	2S4R (8 Ranks)	2933
3DS	--	2S2R (4 Ranks)	2933
	2S2R (4 Ranks)	2S2R (4 Ranks)	2666
	--	2S4R (8 Ranks)	2933
	2S4R (8 Ranks)	2S4R (8 Ranks)	2666

3-6 Installing the PCI Expansion Card

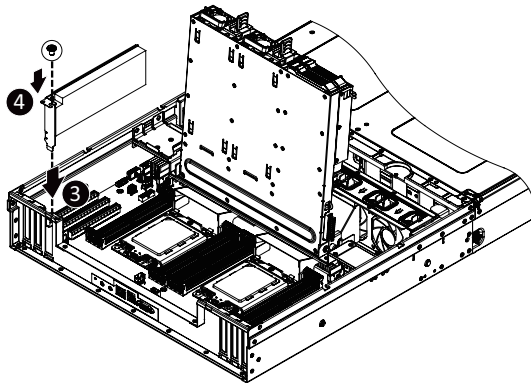
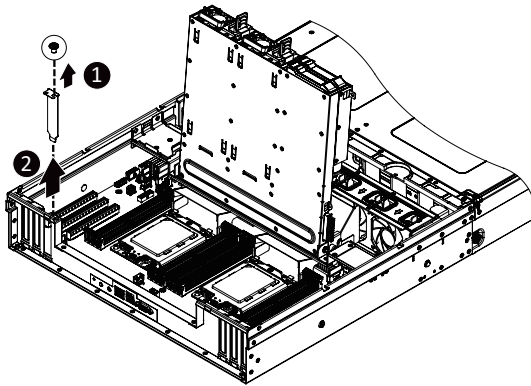


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to installing a PCIe card.

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

Follow these instructions to install PCI Expansion card:

1. Remove the screw securing the slot cover to the PCIe bracket.
2. Remove the slot cover from the PCIe bracket.
3. 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.
4. Secure the PCIe card with the screw.



3-7 Installing the Hard Disk Drive

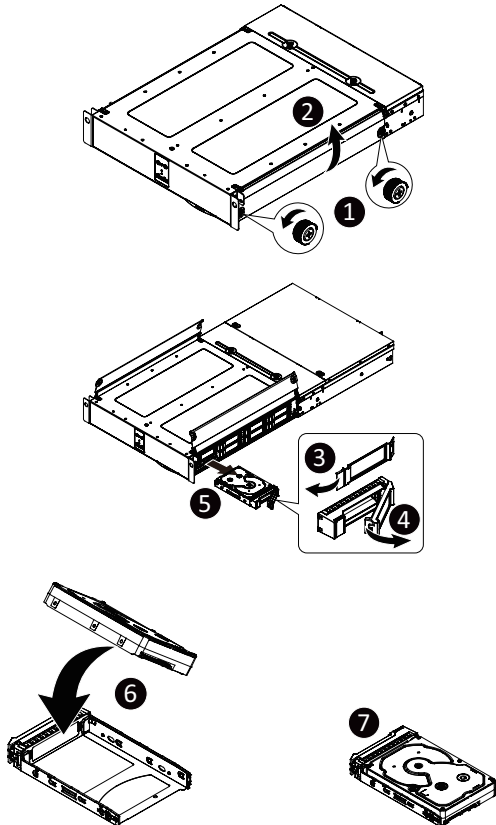


Read the following guidelines before you begin to install the Hard disk drive:

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

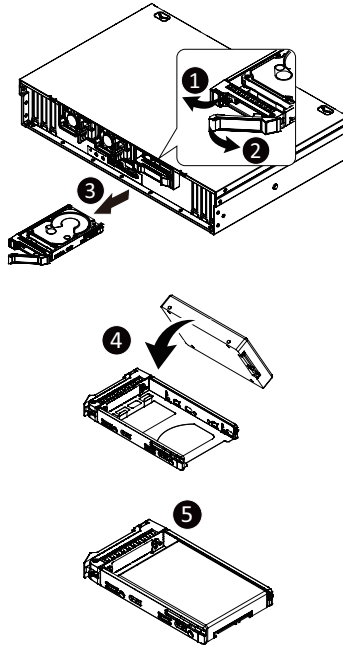
Follow these instructions to install a 3.5" hard disk drive:

1. Loosen the thumbscrew securing the left/right side chassis cover.
2. Open the left/right side cover.
3. Press the release button on the HDD tray.
4. Extend the locking lever.
5. Pull the locking lever in the direction indicated to remove the HDD tray.
6. Align the hard disk drive with the positioning stud on the HDD tray.
7. Slide the hard disk drive into the HDD tray.
8. Reinsert the HDD tray into the slot and close the locking lever.



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.



3-8 Removing and installing the Fan Wall

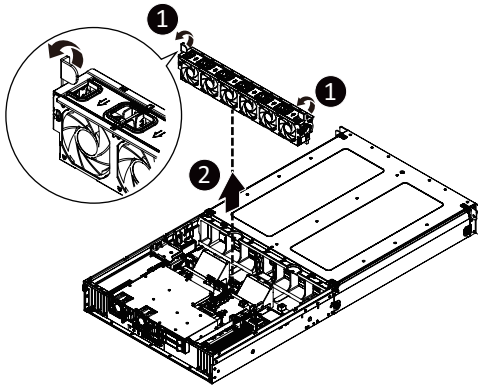


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

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

Follow these instructions to replace the fan assembly:

1. Open the latch on both sides of the fan wall.
2. Lift up the fan wall from the system
3. Reverse the previous steps to install the fan wall.



3-9 Replacing the Fan Assembly

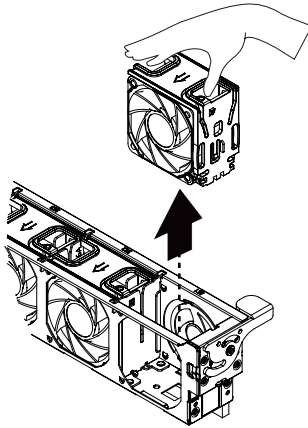


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

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

Follow these instructions to replace the fan assembly:

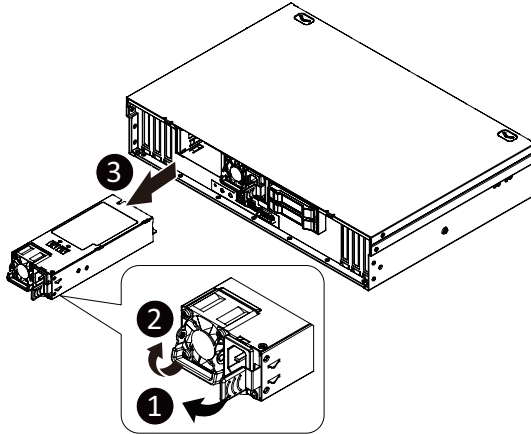
1. Squeeze the fan latch and lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



3-10 Replacing the Power Supply

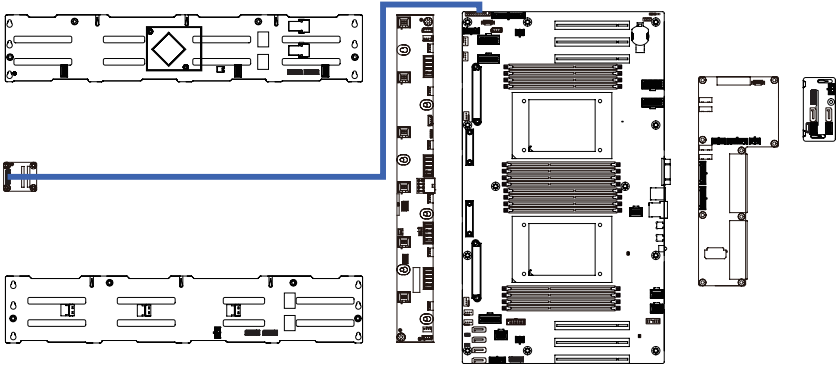
Follow these instructions to replace the power supply:

1. Press the retaining clip on the right side of the power supply along the direction of the arrow.
2. Pull out the power supply handle at the same time and pull out the power supply.
3. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.

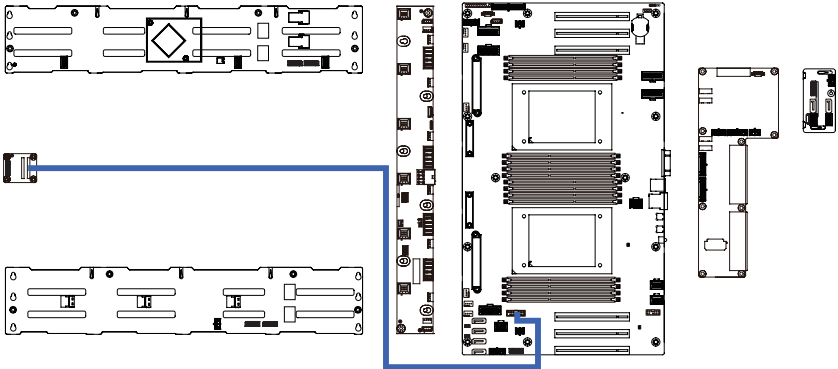


3-11 Cable Routing

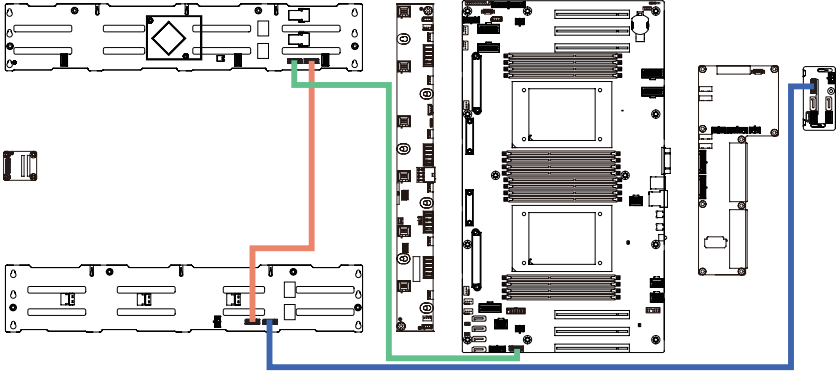
Front Switch Cable/Front LED Cable



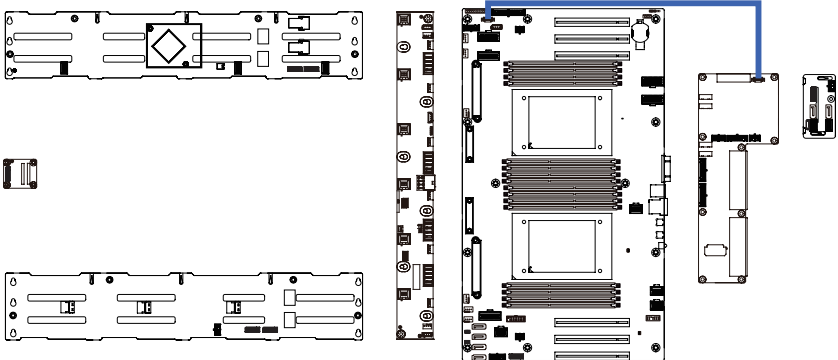
Front Panel USB 3.0 Cable



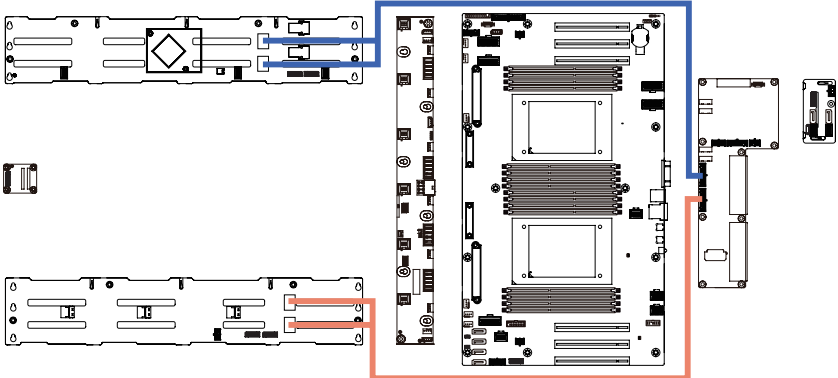
HDD Backplane Board Signal Cable



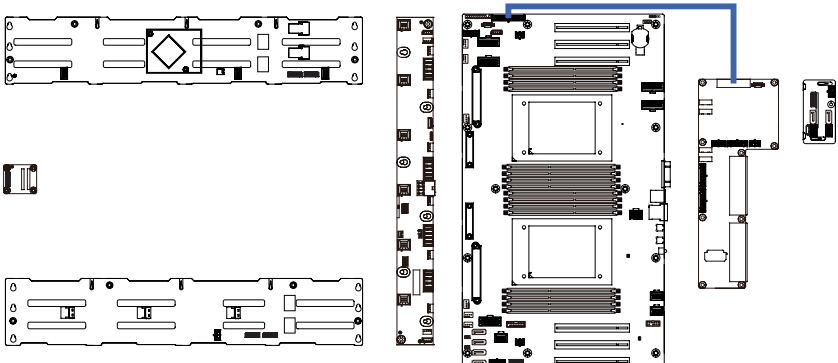
PMBus Signal Cable



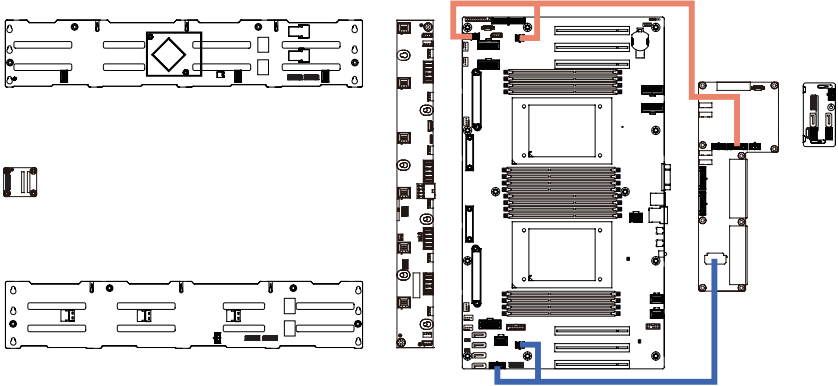
HDD Backplane Board Power Cable #1/#2



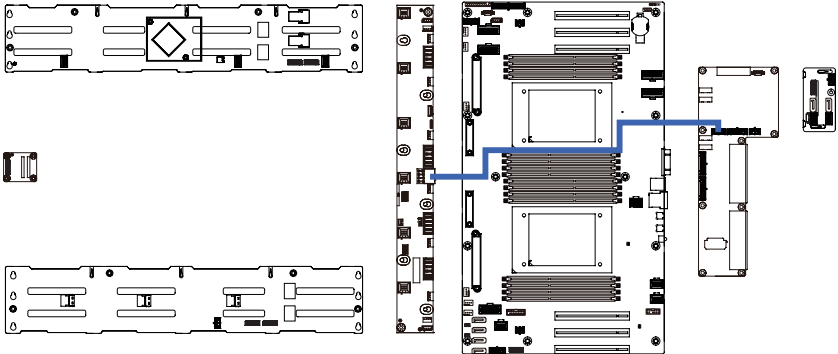
ATX Power Cable



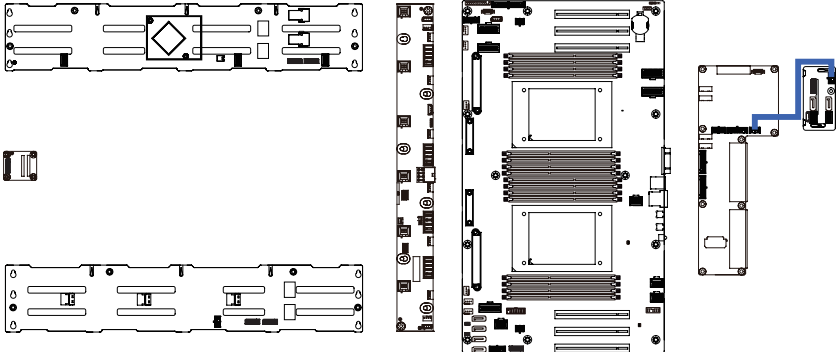
GPU Power Cable #0/#1



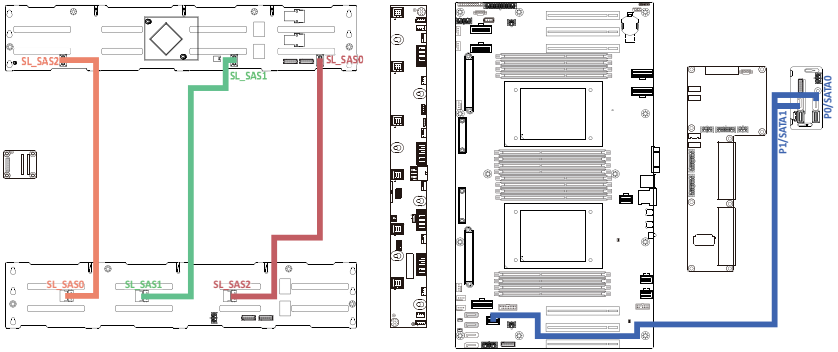
Fan Power Cable



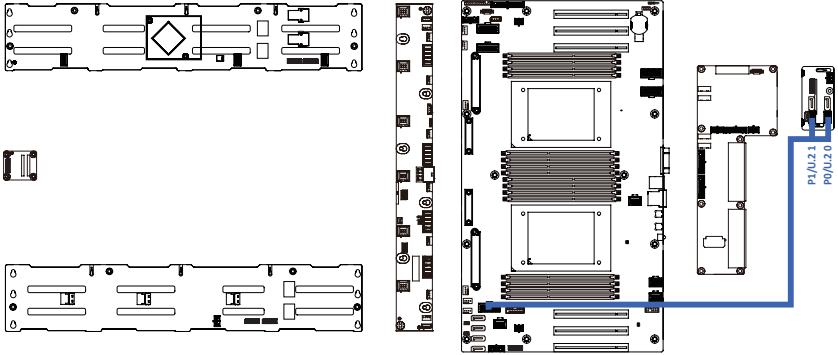
HDD Power Cable



SlimLine to SATA Cable

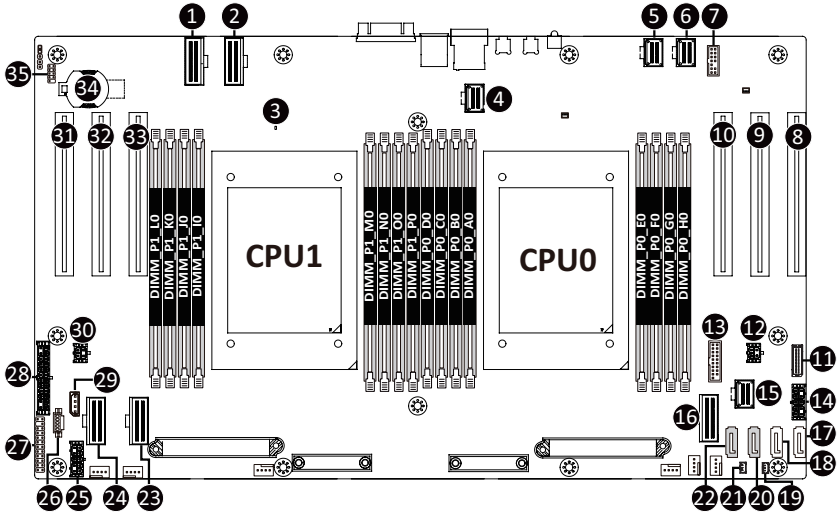


SlimLine to NVMe Cable #0/#1



Chapter 4 Motherboard Components

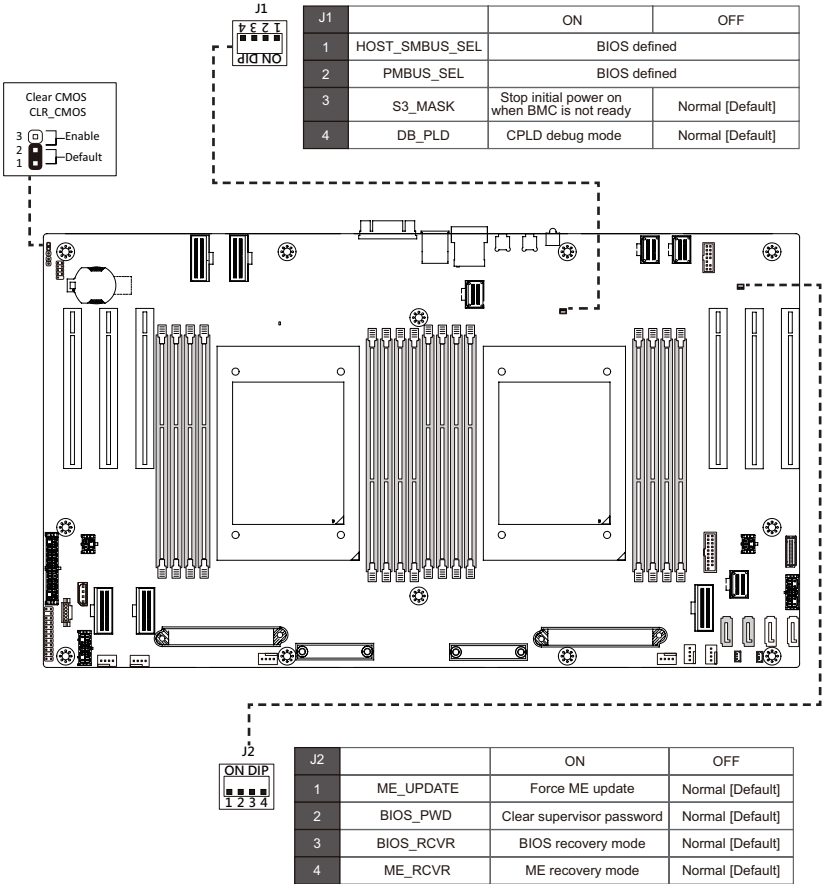
4-1 Motherboard Components



Item	Description
1	Slimline SAS 8i Connector (PCIe Gen4/Defined by SKU)
2	Slimline SAS 8i Connector (PCIe Gen4/Defined by SKU)
3	BMC Firmware Readiness LED
4	Slimline SAS 4i Connector (SATA 6Gb/s /Defined by SKU)
5	Slimline SAS 4i Connector (SATA 6Gb/s /Defined by SKU)
6	Slimline SAS 4i Connector (SATA 6Gb/s /Defined by SKU)
7	TPM Module Connector (SPI Interface)
8	PCIe x16 Slot (Gen4 x16)
9	PCIe x16 Slot (Gen4 x16)
10	PCIe x16 Slot (Gen4 x16)
11	HDD Back Plane Board Connector
12	2 x 2 Pin 12V Power Connector (P12V_MB1)
13	Front Panel USB3.0 Connector
14	2 x 5 Pin Power Connector (for CPU0)
15	Slimline SAS 4i Connector (SATA 6Gb/s)
16	Slimline SAS 8i Connector (PCIe Gen4)
17	SATA Connector (SATA4/Defined by SKU)
18	SATA Connector (SATA3/Defined by SKU)
19	SATA DOM Support Power Connector (for SATA2)

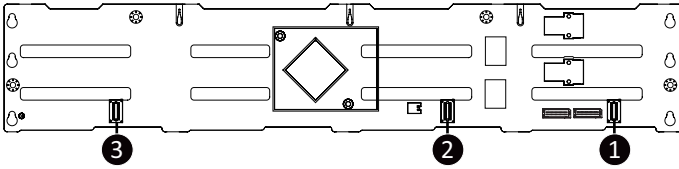
20	SATA Connector (SATA2)
21	SATA DOM Support Power Connector (for SATA1)
22	SATA Connector (SATA1)
23	Slimline SAS 8i Connector (PCIe Gen4/Defined by SKU)
24	Slimline SAS 8i Connector (PCIe Gen4/Defined by SKU)
25	2 x 5 Pin Power Connector (for CPU1)
26	PMBUS Connector
27	Front Panel Header
28	2 x 12 Pin Main Power Connector
29	IPMB Connector
30	2 x 2 Pin 12V Power Connector (P12V_MB)
31	PCIe x16 Slot (Gen4 x16)
32	PCIe x16 Slot (Gen4 x16)
33	PCIe x16 Slot (Gen4 x16)
34	System Battery
35	Serial Port Cable Header

4-2 Jumper Settings



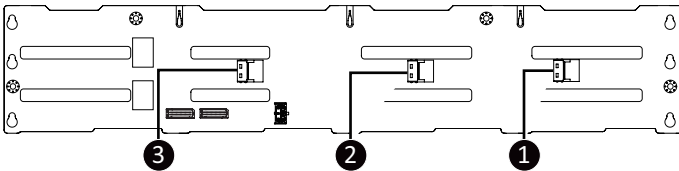
4-3 Backplane Board Storage Connector

4-3-1 Left Side: CBPD2C0



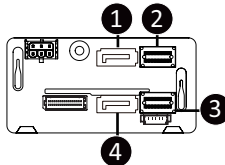
Item	Description
1	Slimline SAS 4i Connector (SL_SAS0/SATA 6Gb/s Signal)
2	Slimline SAS 4i Connector (SL_SAS1/SATA 6Gb/s Signal)
3	Slimline SAS 4i Connector (SL_SAS2/SATA 6Gb/s Signal)

4-3-2 Right Side: CBPD2C1



Item	Description
1	Slimline SAS 4i Connector (SL_SAS0/SATA 6Gb/s Signal)
2	Slimline SAS 4i Connector (SL_SAS1/SATA 6Gb/s Signal)
3	Slimline SAS 4i Connector (SL_SAS2/SATA 6Gb/s Signal)

4-3-3 Rear Side: CBPD020



Item	Description
1	SATA Connector (SATA0)
2	Slimline SAS 4i Connector (U.2 0/NVMe Signal)
3	Slimline SAS 4i Connector (U.2 1/NVMe Signal)
4	SATA Connector (SATA1)

Chapter 5 BIOS Setup

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

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



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

BIOS Setup Program Function Keys

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

- **Main**

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

- **Advanced**

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

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

- **AMD CBS**

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

- **AMD PBS Option**

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

- **Chipset**

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

- **Server Management**

Server additional features enabled/disabled setup menus.

- **Security**

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

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

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

- **Boot**

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

- **Save & Exit**

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

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

5-1 The Main Menu

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

Main Menu Help

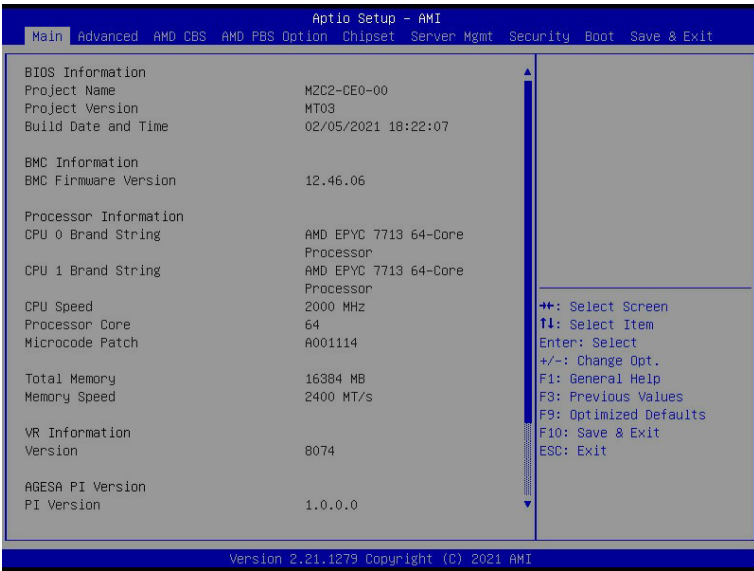
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

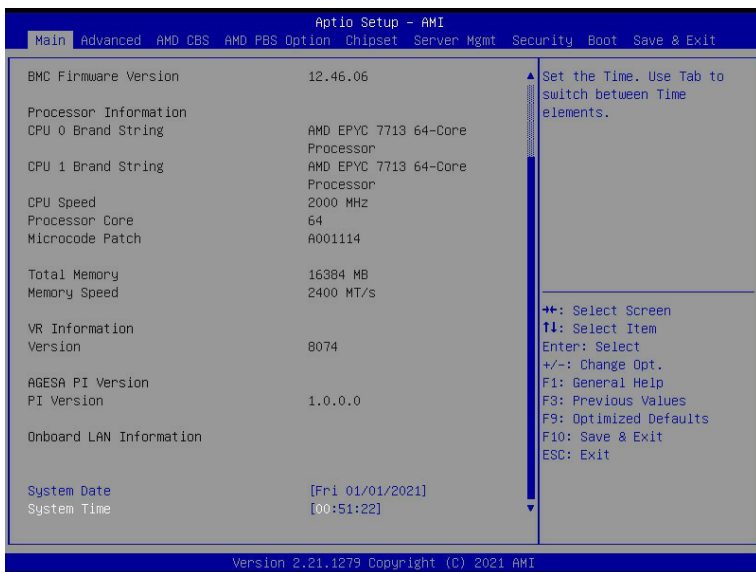
Submenu Help

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



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





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.

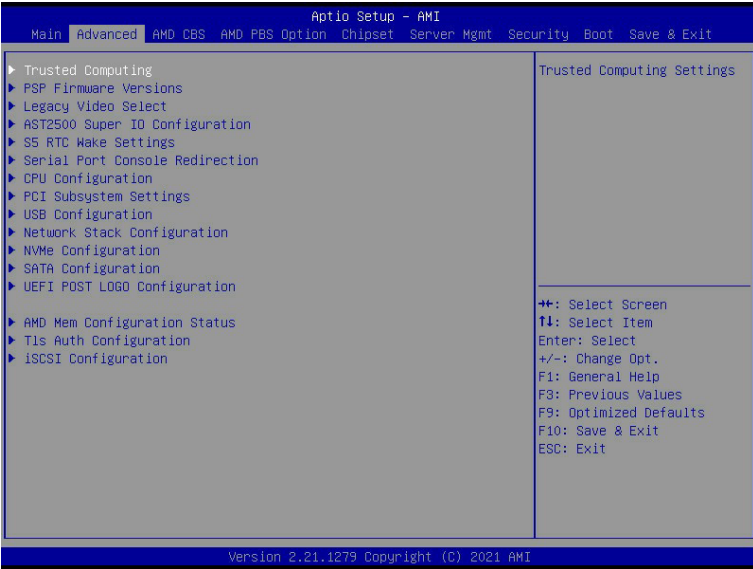
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

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

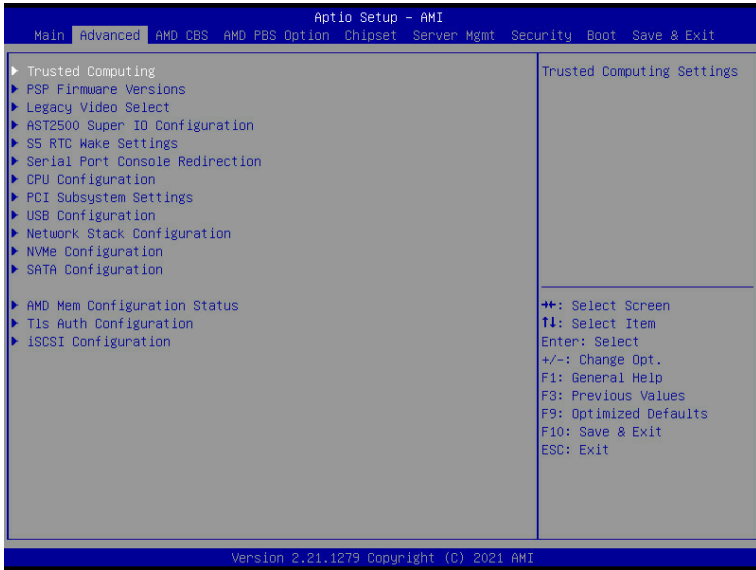
5-2 Advanced Menu

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

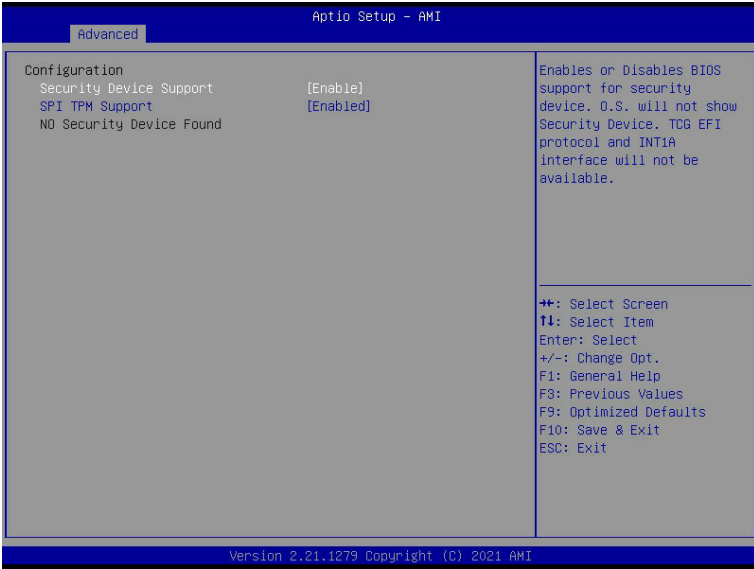
When Boot Mode Select is set to UEFI (Default)



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



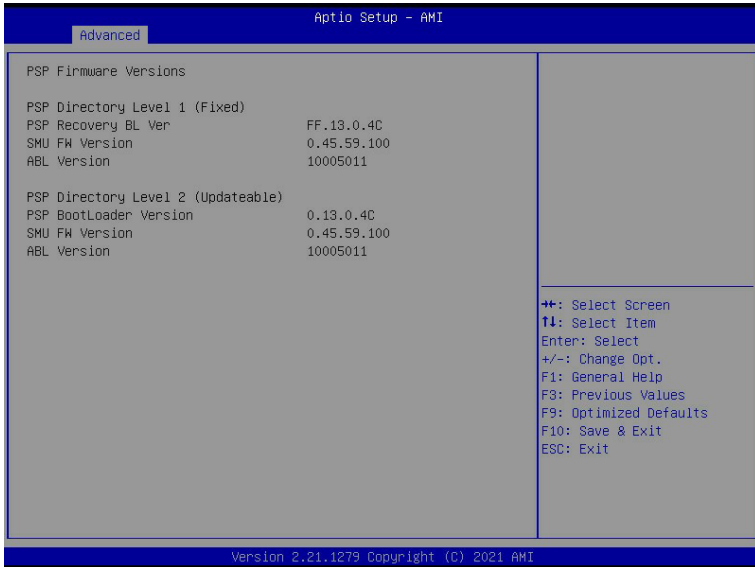
5-2-1 Trusted Computing



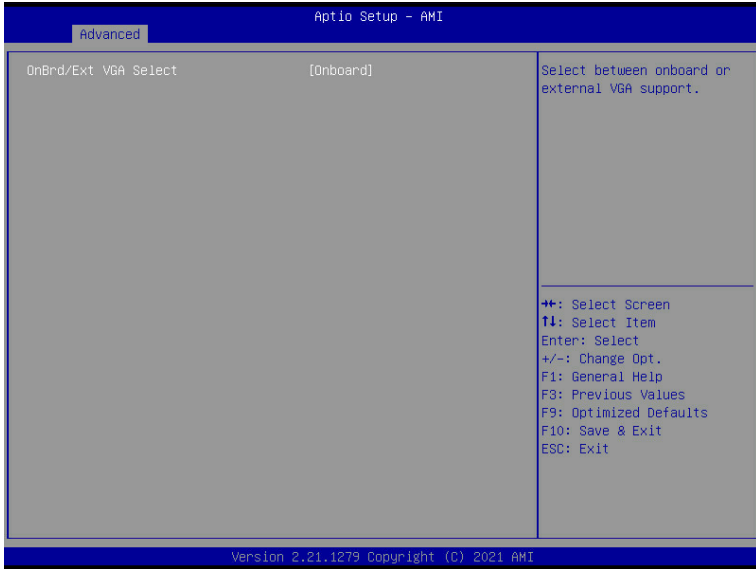
Parameter	Description
Configuration	
Security Device Support	<p>Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
SPI TPM Support	<p>Select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

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.

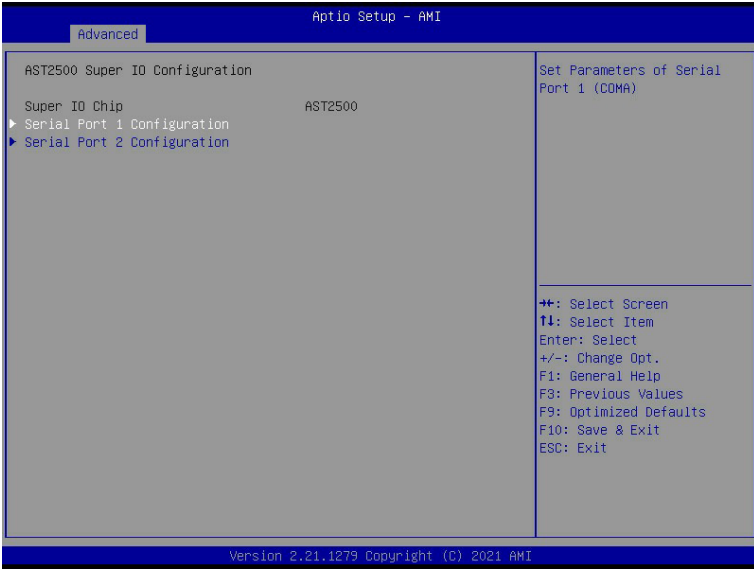


5-2-3 Legacy Video Select



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

5-2-4 AST2500 Super IO Configuration



Parameter	Description
AST2500 Super IO Configuration	
Super IO Chip	Displays the super IO chip information
Serial Port 1/2 Configuration	Press [Enter] for configuration of advanced items.

5-2-4-1 Serial Port 1/2 Configuration

Aptio Setup - AMI

Advanced

Serial Port 1 Configuration		Enable or Disable Serial Port (COM)
Serial Port	[Enabled]	
Device Settings	IO=3F6h; IRQ=4;	
Change Settings	[Auto]	

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

Version 2.21.1279 Copyright (C) 2021 AMI

Aptio Setup - AMI

Advanced

Serial Port 2 Configuration		Enable or Disable Serial Port (COM)
Serial Port	[Enabled]	
Device Settings	IO=2F6h; IRQ=3;	
Change Settings	[Auto]	

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

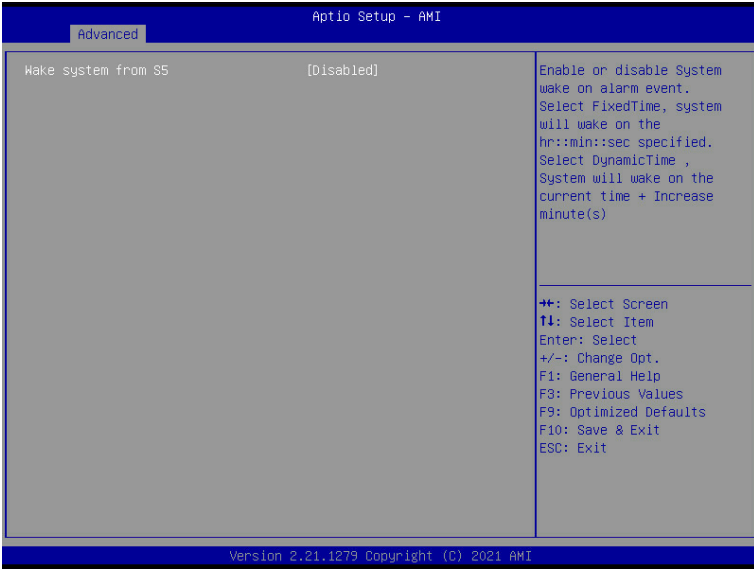
Version 2.21.1279 Copyright (C) 2021 AMI

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

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

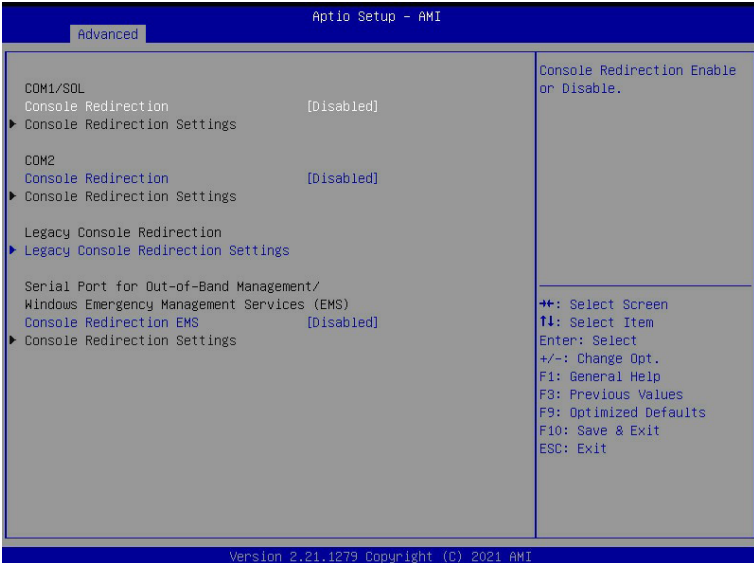
(Note2) This item appears when **Serial Port** is set to **Enabled**.

5-2-5 S5 RTC Wake Settings



Parameter	Description
Wake System from S5	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 & COM2 Console Redirection ^(Note)	<p>Select whether to enable console redirection for specified device. Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>
COM1/Serial Over LAN & COM2 Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p>Please note that this item is configurable when COM1/Serial Over LAN & COM2 Console Redirection is set to Enabled.</p> <ul style="list-style-type: none"> ◆ Terminal Type <ul style="list-style-type: none"> – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ Bits per second <ul style="list-style-type: none"> – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is 115200. ◆ Data Bits <ul style="list-style-type: none"> – Selects the number of data bits used for console redirection. – Options available: 7, 8. Default setting is 8.

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

Parameter	Description
COM1/Serial Over LAN & COM2 Console Redirection Settings (continued)	<ul style="list-style-type: none"> ◆ Parity <ul style="list-style-type: none"> – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: parity bit is 0 if num of 1's in the data bits is odd. – Mark: parity bit is always 1. Space: Parity bit is always 0. – Mark and Space Parity do not allow for error detection. – Options available: None, Even, Odd, Mark, Space. Default setting is None. ◆ Stop Bits <ul style="list-style-type: none"> – Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. – Options available: 1, 2. Default setting is 1. ◆ Flow Control <ul style="list-style-type: none"> – Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. – Options available: None, Hardware RTS/CTS. Default setting is None. ◆ VT-UTF8 Combo Key Support <ul style="list-style-type: none"> – Enable/Disable the VT-UTF8 Combo Key Support. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Recorder Mode^(Note) <ul style="list-style-type: none"> – When this mode enabled, only texts will be send. This is to capture Terminal data. – Options available: Enabled, Disabled. Default setting is Disabled. ◆ Resolution 100x31^(Note) <ul style="list-style-type: none"> – Enable/Disable extended terminal resolution. – Options available: Enabled, Disabled. Default setting is Enabled. ◆ Putty KeyPad^(Note) <ul style="list-style-type: none"> – Selects FunctionKey and KeyPad on Putty. – Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is VT100.

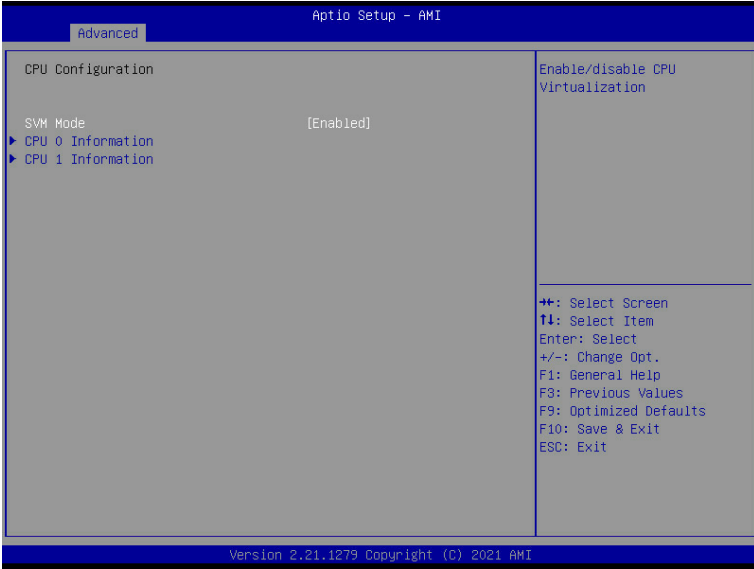
(Note) Advanced items prompt when this item is defined.

Parameter	Description
Legacy Console Redirection	
Legacy Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Redirection COM Port <ul style="list-style-type: none"> – Selects a COM port for Legacy serial redirection. – Options available: COM1/SOL, COM2. Default setting is COM1/SOL. ◆ Resolution <ul style="list-style-type: none"> – Selects the number of rows and columns used in Console Redirection for legacy OS support. – Options available: 80x24, 80x25. Default setting is 80x24. ◆ Redirect After POST <ul style="list-style-type: none"> – When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. – Options available: Always Enable, BootLoader. Default setting is Always Enable.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection ^(Note)	<p>EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>
Serial Port for Out-of-Band EMS Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p>Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.</p> <ul style="list-style-type: none"> ◆ Out-of-Band Mgmt Port <ul style="list-style-type: none"> – Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Options available: COM1/SOL, COM2. Default setting is COM1/SOL. ◆ Terminal Type <ul style="list-style-type: none"> – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ Bits per second <ul style="list-style-type: none"> – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is 115200.

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

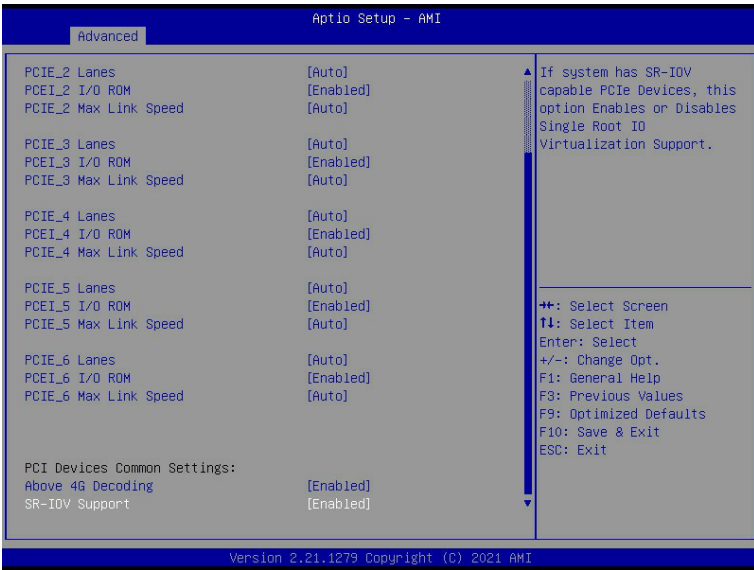
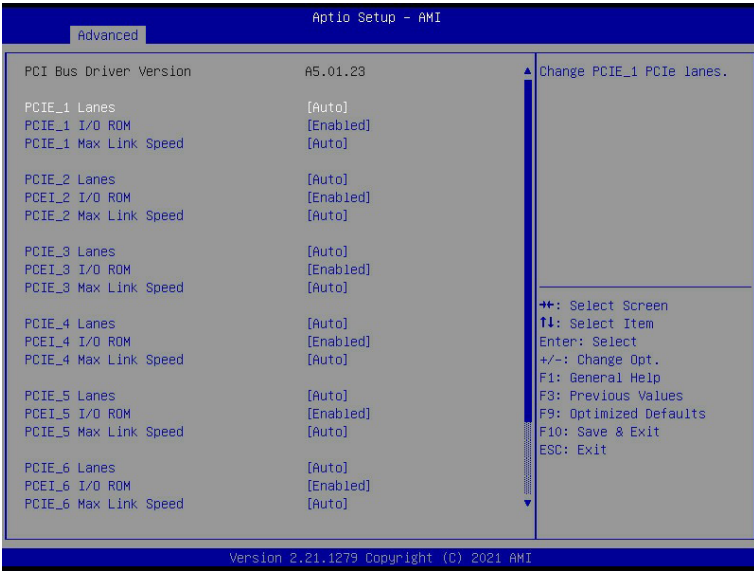
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	<ul style="list-style-type: none">◆ Flow Control<ul style="list-style-type: none">– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is None.

5-2-7 CPU Configuration



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

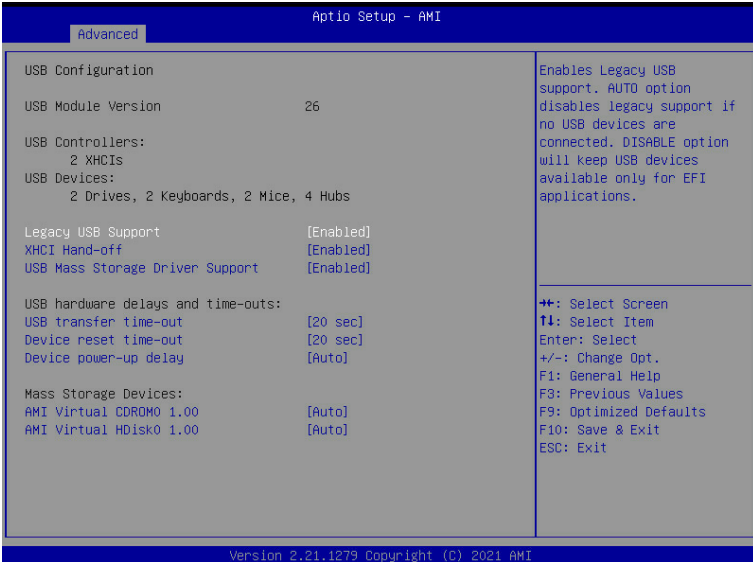
5-2-8 PCI Subsystem Settings



Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
PCIE_# Lanes Configuration ^(Note1)	Change the PCIe lanes. Options available: Disabled, Auto, x8, x4x4, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is Auto .
PCIE_# I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is Enabled .
PCIE#_Max Link Speed ^(Note1)	Configure PCIe max link speed. Options available: Auto, Maximum, Gen1, Gen2, Gen3, Gen4. Default setting is Auto .
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled, Disabled. Default setting is Enabled .
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is Enabled .

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

5-2-9 USB Configuration

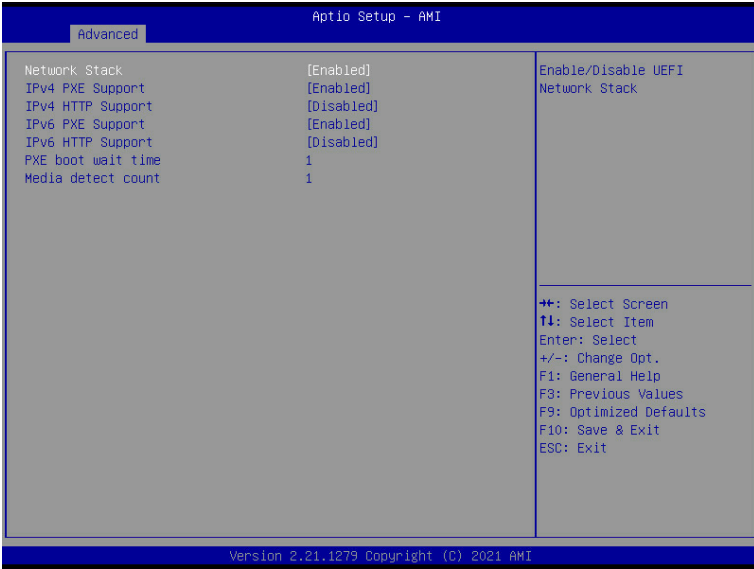


Parameter	Description
USB Configuration	
USB Module Version	Displays the USB module version information.
USB Controllers	Displays the supported USB controllers.
USB Devices:	Displays the USB devices connected to the system.
Legacy USB Support	Enable/Disable the Legacy USB support function. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. Options available: Auto, Enabled, Disabled. Default setting is Enabled .
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled, Disabled. Default setting is Enabled .
USB Mass Storage Driver Support ^(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled, Disabled. Default setting is Enabled .

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

Parameter	Description
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 .
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.

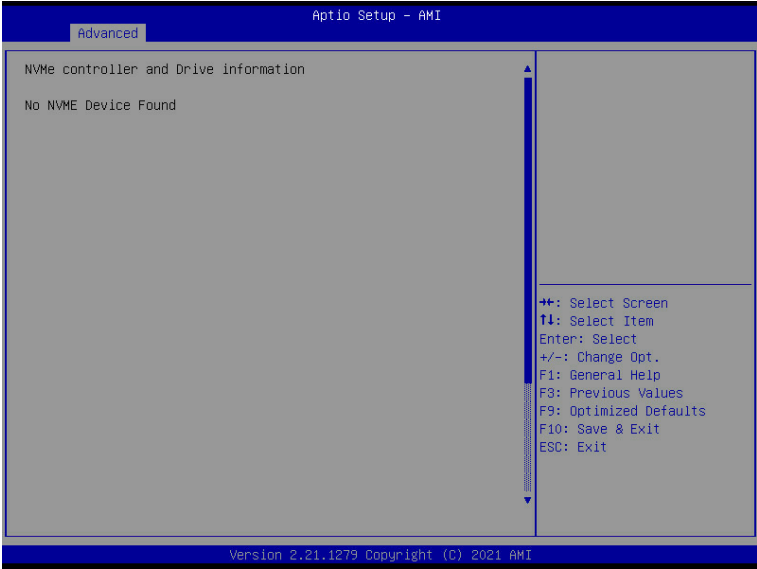
5-2-10 Network Stack Configuration



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.

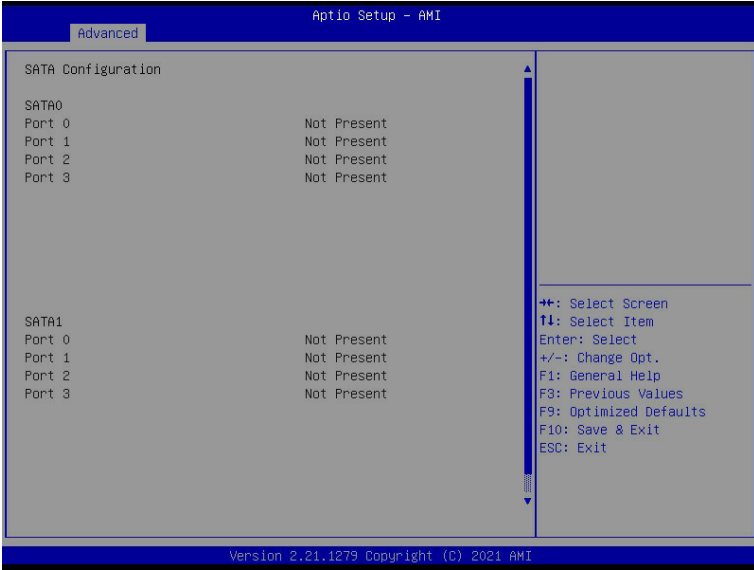
(Note) This item appears when **Network Stack** is set to **Enabled**.

5-2-11 NVMe Configuration



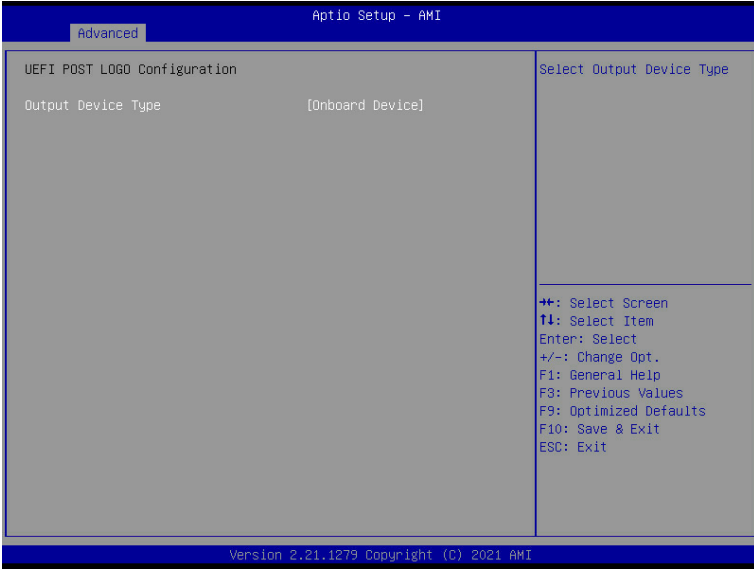
Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.

5-2-12 SATA Configuration



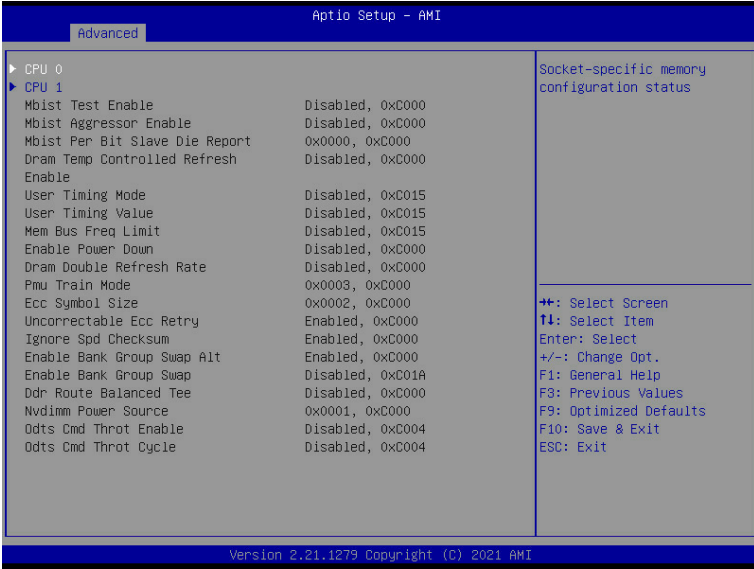
Parameter	Description
SATA Configuration	Displays the installed HDD devices information. System will automatically detect HDD type.

5-2-13 UEFI POST LOGO Configuration



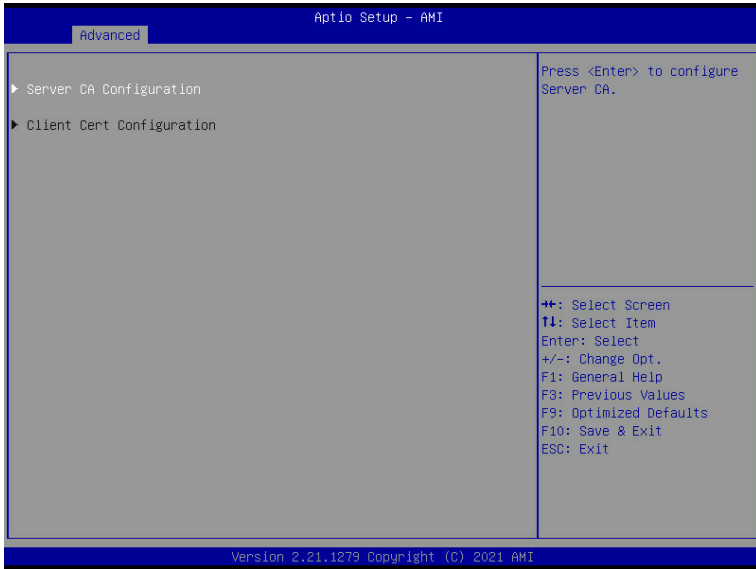
Parameter	Description
Output Device Type	Selects output device type. Options available: First loaded Device, Onboard Device, External Device, Specific Device. Default setting is Onboard Device .

5-2-14 AMD Mem Configuration Status



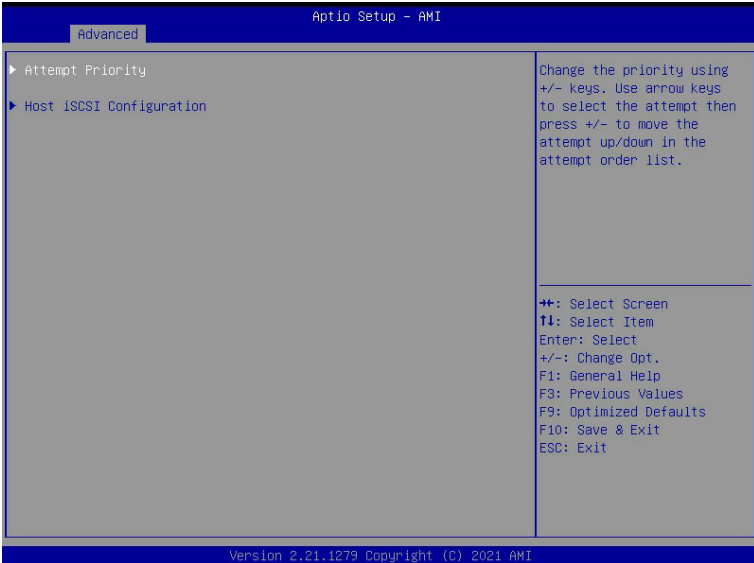
Parameter	Description
CPU 0/1	Press [Enter] to view the memory configuration status related to CPU 0/1.

5-2-15 T1s Auth Configuration



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

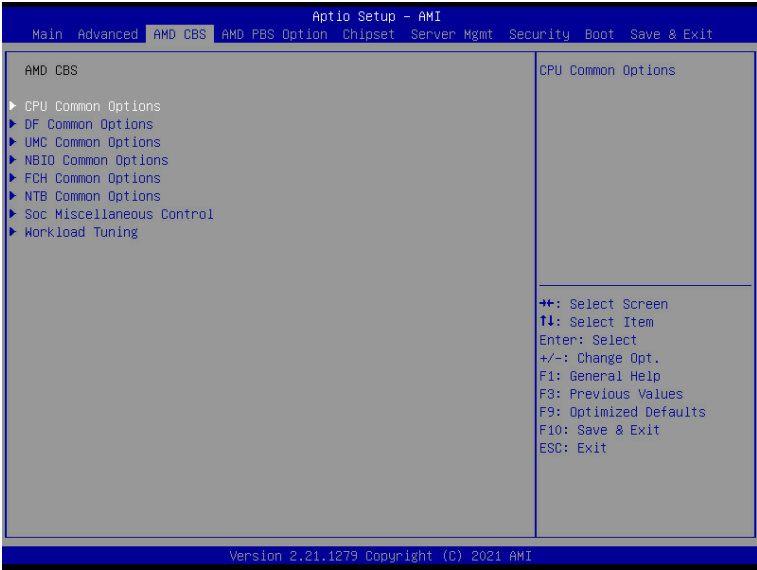
5-2-16 iSCSI Configuration



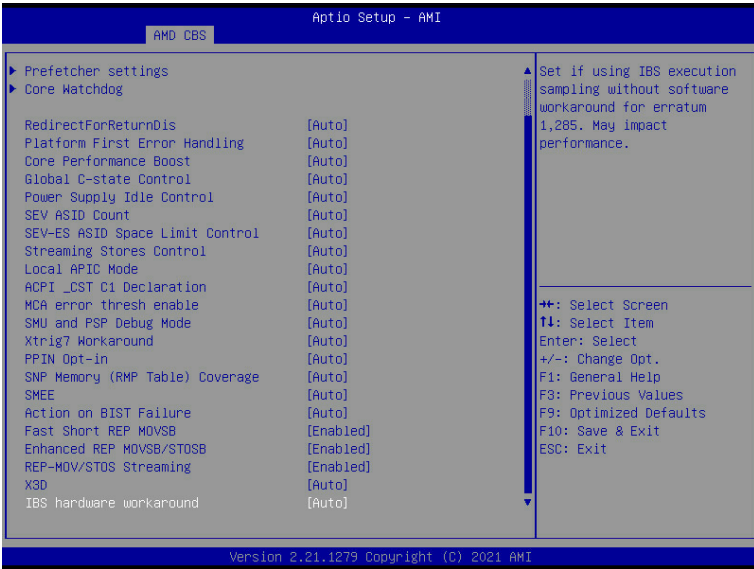
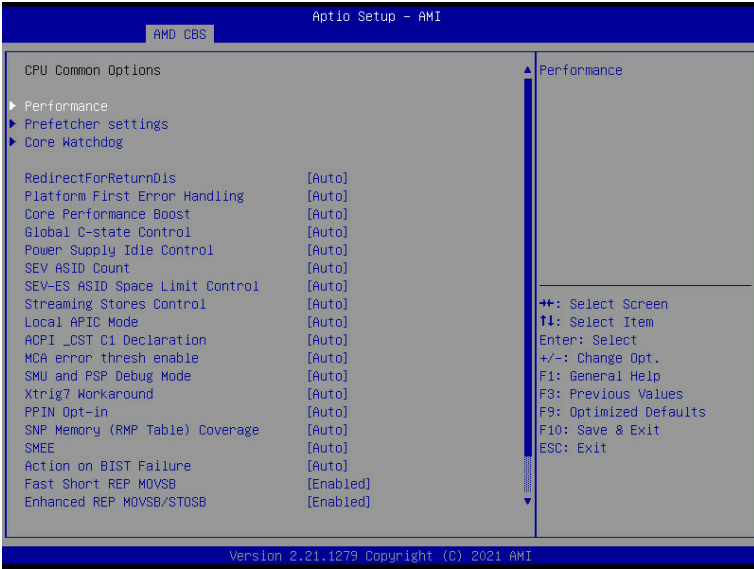
Parameter	Description
Attempt Priority	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Attempt Priority <ul style="list-style-type: none"> – Change the priority using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the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

5-3 AMD CBS Menu

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



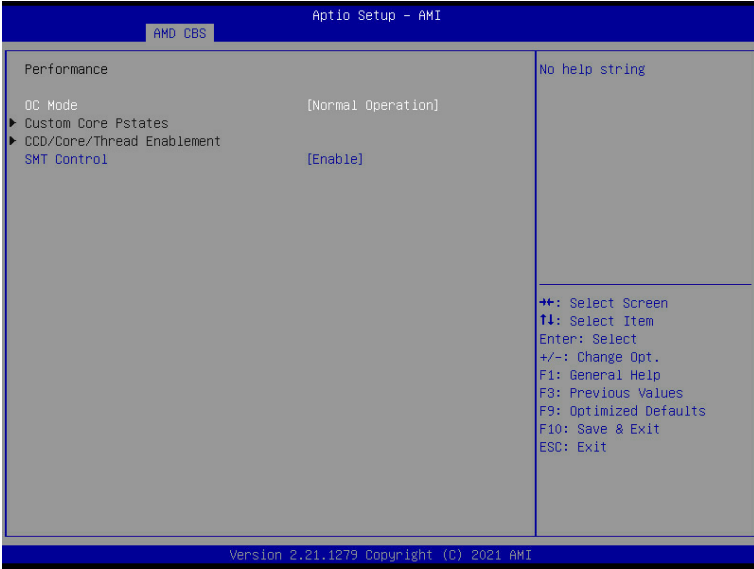
5-3-1 CPU Common Options



Parameter	Description
CPU Common Options	
Performance	Press [Enter] for configuration of advanced items.
Prefetcher settings	Press [Enter] for configuration of advanced items.
Core Watchdog	Press [Enter] for configuration of advanced items.
RedirectForReturnDis	From a workaround for GCC/C000005 issue for XV Core on CZ A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrctForReturns] to 1. Options available: Auto, 1, 0. Default setting is Auto .
Platform First Error Handling	Enable/Disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Core Performance Boost	Enable/Disable the Core Performance Boost function. Options available: Auto, Disabled. Default setting is Auto .
Global C-State Control	Controls the IO based C-state generation and DF C-states. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Power Supply Idle Control	Configures the Power Supply Idle Control. Options available: Auto, Low Current Idle, Typical Current Idle. Default setting is Auto .
SEV ASID Count	Specifies the maximum valid ASID, which affects the maximum system physical address space. Options available: Auto, 253 ASIDs, 509 ASIDs. Default setting is Auto .
SEV-ES ASID Space Limit Control	Space limit control for SEV-ES ASIDs. Options available: Auto, Manual. Default setting is Auto .
Streaming Stores Control	Enable/Disable the Streaming Stores functionality. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Local APIC Mode	Sets the Local APIC Mode. Options available: Auto, xAPIC, x2APIC. Default setting is Auto .
ACPI_CST C1 Declaration	Determines whether or not to declare the C1 state to the OS.. Options available: Auto, Enabled, Disabled. Default setting is Auto .
MCA error thresh enable	Enable MCA error thresholding. Options available: Auto, False, True. Default setting is Auto .
SMU and PSP Debug Mode	When this option is enabled, specific uncorrected errors detected by the PSP FW or SMU FW will hand and not reset the system. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Xtrig7 Workaround	Options available: Auto, No Workaround, Bronze Workaround, Sliver Workaround. Default setting is Auto .
PPIN Opt-in	Enable/Disable the PPIN feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
SNP Memory (RMP Table) Coverage	Enabled: Enter system memory is covered. Options available: 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 .

Parameter	Description
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	Default is 1, can be set to zero for analysis purpose as long as OS supports it. Options available: Disabled, Enabled. Default setting is Enabled .
Enhanced REP MOVSB/ STOSB	Default is 1, can be set to zero for analysis purpose as long as OS supports it. Options available: Disabled, Enabled. Default setting is Enabled .
REP-MOV/STOS Streaming	Allows REP-MOV/STOS to use non-caching streaming stores for large sizes. Options available: Disabled, Enabled. Default setting is Enabled .
X3D	Override of X3D technology. Options available: Auto, Disable, 1 stack, 2 stacks, 4 stacks. Default setting is Auto .
IBS hardware workaround	Sets if using IBS execution sampling without software workaround for erratum 1,285. May impact performance. Options available: Auto, Enabled. Default setting is Auto .

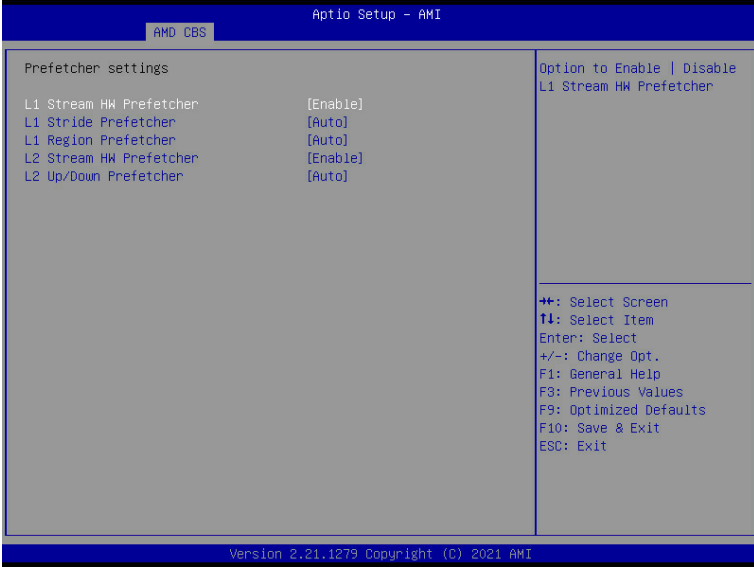
5-3-1-1 Performance



Parameter	Description
Performance	
OC Mode ^(Notes)	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. <ul style="list-style-type: none"> ◆ CCD Control <ul style="list-style-type: none"> – Options available: Auto, 2 CCDs, 3 CCDs, 4 CCDs, 6 CCDs. Default setting is Auto. ◆ Core Control <ul style="list-style-type: none"> – 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 .

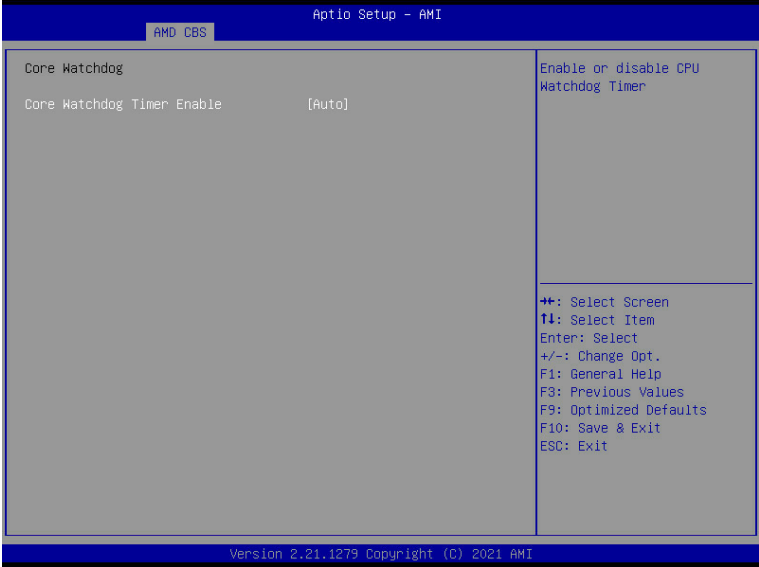
(Note) Advanced items are configurable when this item is defined.

5-3-1-2 Prefetcher Settings



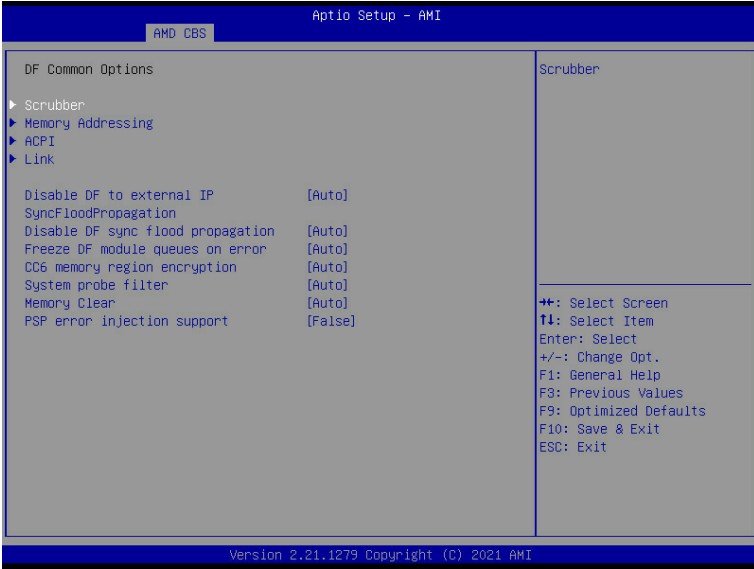
Parameter	Description
Prefetcher settings	
L1 Stream HW Prefetcher	Enable/Disable L1 Stream HW Prefetcher. Options available: Auto, Enable, Disable. Default setting is Enable .
L1 Stride Prefetcher	Use memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous. Enable/Disable L1 Stride Prefetcher. Options available: Auto, Enable, Disable. Default setting is Auto .
L1 Region Prefetcher	Use memory access history to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses. Enable/Disable L1 Region Prefetcher. Options available: Auto, Enable, Disable. Default setting is Auto .
L2 Stream HW Prefetcher	Enable/Disable L2 Stream HW Prefetcher. Options available: Auto, Enable, Disable. Default setting is Enable .
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: Auto, Enable, Disable. Default setting is Auto .

5-3-1-3 Core Watchdog



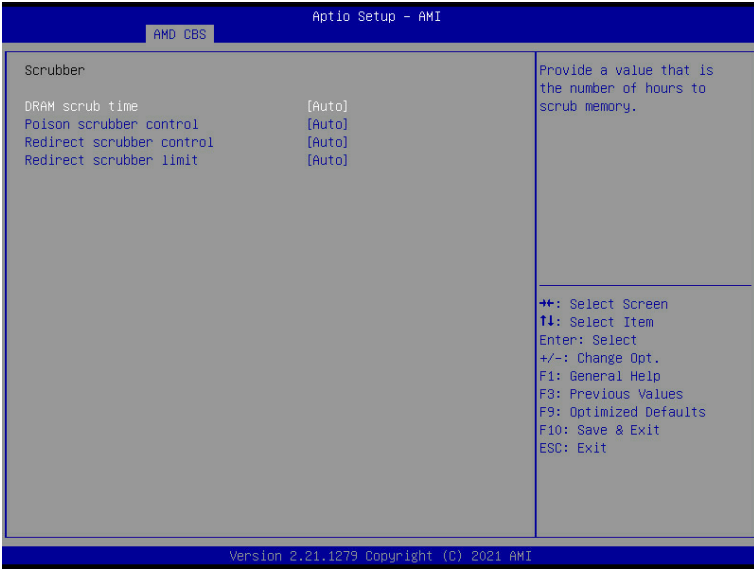
Parameter	Description
Core Watchdog	
Core Watchdog Timer Enable	Enable/Disable CPU Watchdog Timer. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-2 DF Common Options



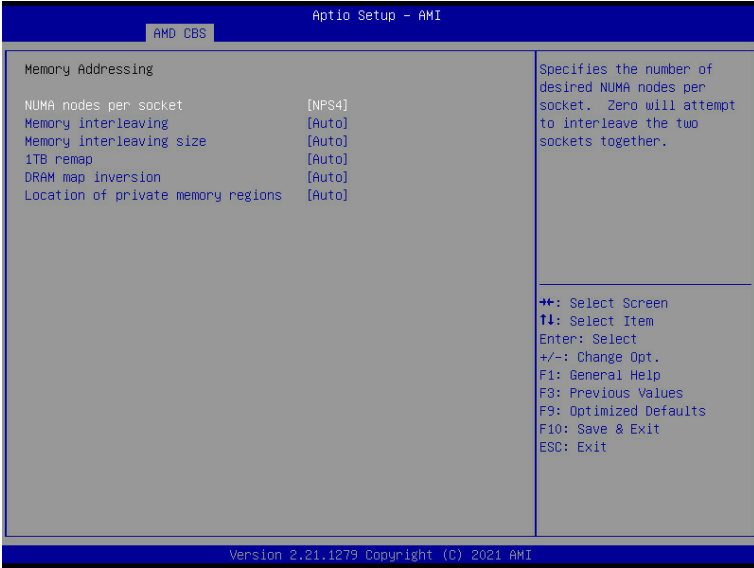
Parameter	Description
DF Common Options	
Scrubber	Press [Enter] for configuration of advanced items.
Memory Addressing	Press [Enter] for configuration of advanced items.
ACPI	Press [Enter] for configuration of advanced items.
Link	Press [Enter] for configuration of advanced items.
Disable DF to external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

5-3-2-1 Scrubber



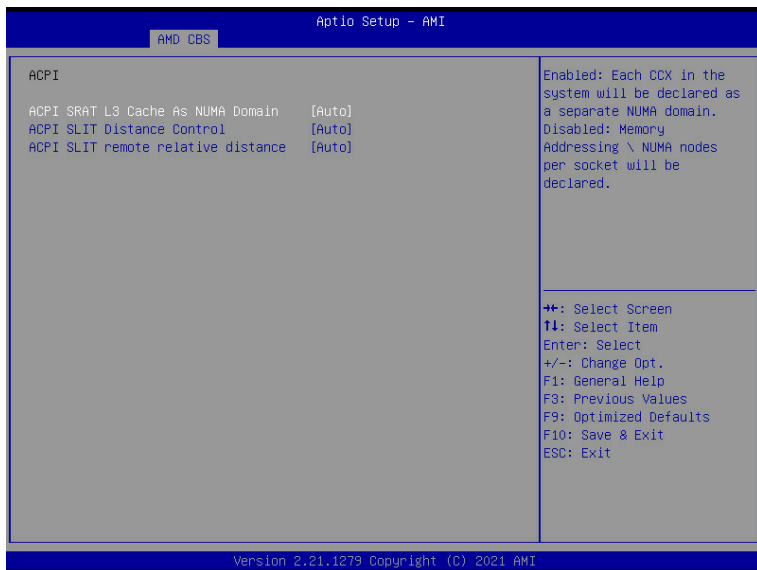
Parameter	Description
Scrubber	
DRAM scrub time	Provide a value that is the number of hours to scrub memory. Options available: Auto, Disabled, 1 hour, 4 hours, 8 hours, 16 hours, 24 hours, 48 hours. Default setting is Auto .
Poison scrubber control	Enable/Disable the Poison scrubber control feature.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

5-3-2-2 Memory Addressing



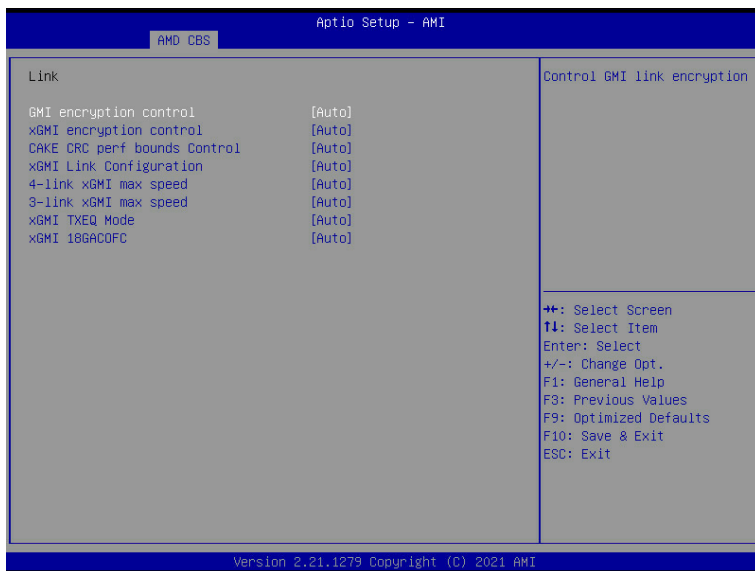
Parameter	Description
Memory Addressing	
NUMA nodes per socket	Specifies the number of desired NUMA nodes per socket. Options available: Auto, NPS0, NPS1, NPS2, NPS4. Default setting is Auto .
Memory interleaving	Enable/Disable the Memory interleaving feature. Options available: Auto, Disabled. Default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

5-3-2-3 ACPI



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

5-3-2-4 Link



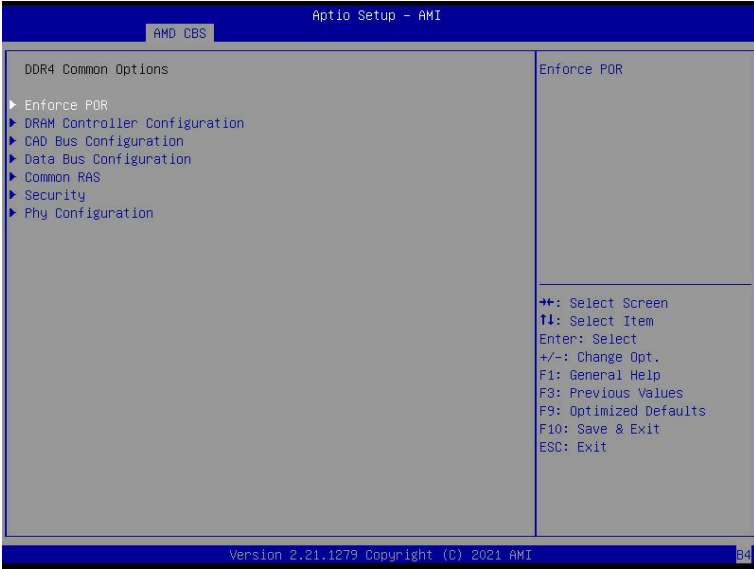
Parameter	Description
Link	
GMI encryption control	Enable/Disable GMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is Auto .
xGMI encryption control	Enable/Disable xGMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is Auto .
CAKE CRC perf bounds Control	Options available: Auto, Manual. Default setting is Auto .
xGMI Link Configuration	Configures the number of xGMI2 links used on a multi-socket system. Options available: Auto, 2 xGMI Links, 3 xGMI Links, 4 xGMI Links. Default setting is Auto .
4-link xGMI max speed	Specifies the max speed of 4-link xGMI. Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps. Default setting is 10.667Gbps .
3-link xGMI max speed	Specifies the max speed of 3-link xGMI. Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps. Default setting is 10.667Gbps .
xGMI TXEQ Mode	Configures xGMI TXEQ/RX vetting Mode. Options available: Auto, TXEQ_Disabled, TXEQ_Lane, TXEQ_Link, TXEQ_RX_Vet. Default setting is Auto .
xGMI 18GACOFc	Configures xGMI 18GACOFc. Options available: Auto, Enable, Disable. Default setting is Auto .

5-3-3 UMC Common Options



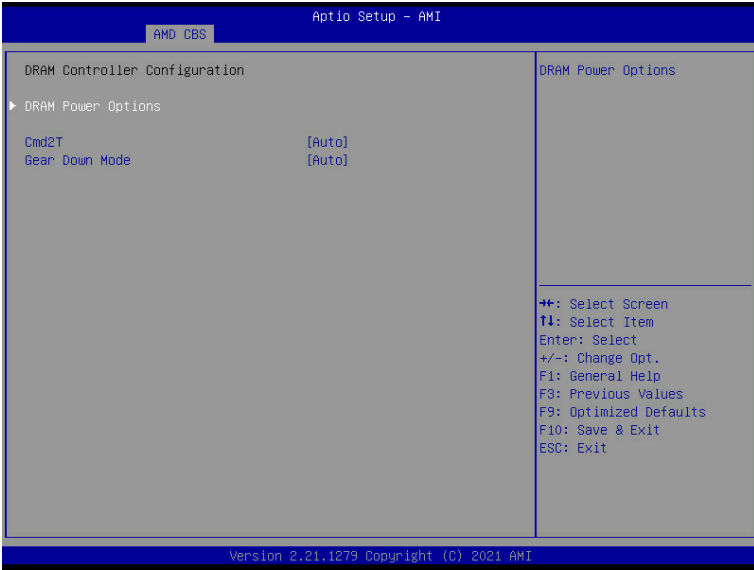
Parameter	Description
UMC Common Options	
DDR4 Common Options	Press [Enter] for configuration of advanced items.
DRAM Memory Mapping	Press [Enter] for configuration of advanced items.
NVDIMM	Press [Enter] for configuration of advanced items.
Memory MBIST	Press [Enter] for configuration of advanced items.

5-3-3-1 DDR4 Common Options



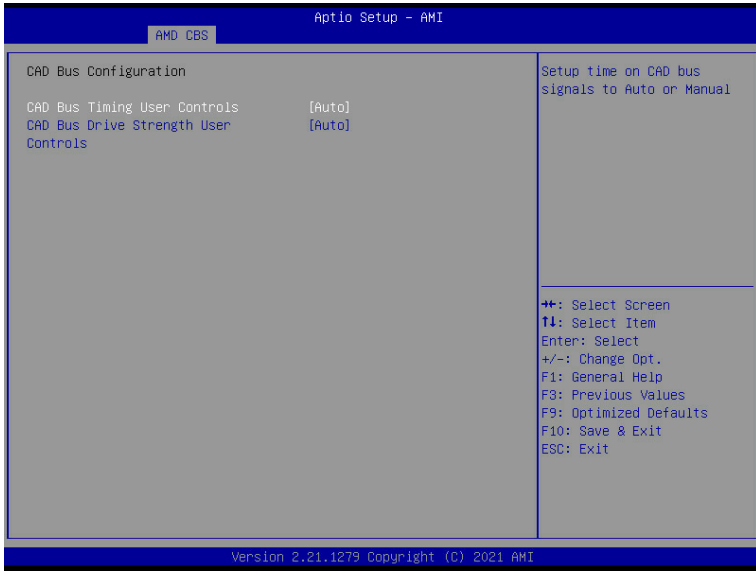
Parameter	Description
DDR4 Common Options	
Enforce POR	<p>Press [Enter] to configure the Plan of Record (POR) to enable / disable restrictions for DDR4 frequency and voltage programming. Memory speeds will be capped at AMD guidelines.</p> <ul style="list-style-type: none"> ◆ Decline ◆ Accept <ul style="list-style-type: none"> – Overclock <ul style="list-style-type: none"> » Enable/Disable Memory Overclock Settings » Options available: Auto, Enabled. Default setting is Auto. <p>Note: To enable 2 DIMMs per Channel at 3200MHz function, select [Accept] at warning message, change Overclock from [Auto] to [Enabled], and then set memory speed to 3200MHz.</p>
DRAM Controller Configuration	Press [Enter] to configure DRAM Controller Configuration.
CAD Bus Configuration	Press [Enter] to configure CAD Bus Configuration.
Data Bus Configuration	Press [Enter] to configure Data Bus Configuration.
Common RAS	Press [Enter] to configure Common RAS.
Security	Press [Enter] to configure Security.
Phy Configuration	Press [Enter] to configure Phy Configuration.

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



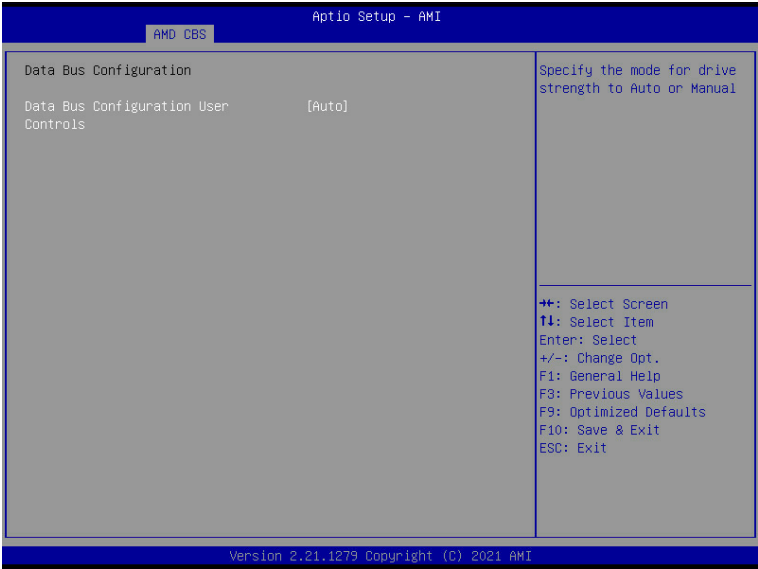
Parameter	Description
DRAM Controller Configuration	
DRAM Power Options	<p>Press [Enter] to configure DRAM Power Options.</p> <ul style="list-style-type: none"> ◆ Power Down Enable <ul style="list-style-type: none"> – Enable/Disable DDR power down mode. – Options available: Auto, Enabled, Disabled. Default setting is Auto.
Cmd2T	<p>Selects the Cmd2T mode on ADDR/CMD.</p> <p>Options available: Auto, 1T, 2T. Default setting is Auto.</p>
Gear Down Mode	<p>Enable/Disable the Gear Down Mode function.</p> <p>Options available: Auto, Enabled, Disabled. Default setting is Auto.</p>

5-3-3-1-2 CAD Bus Configuration



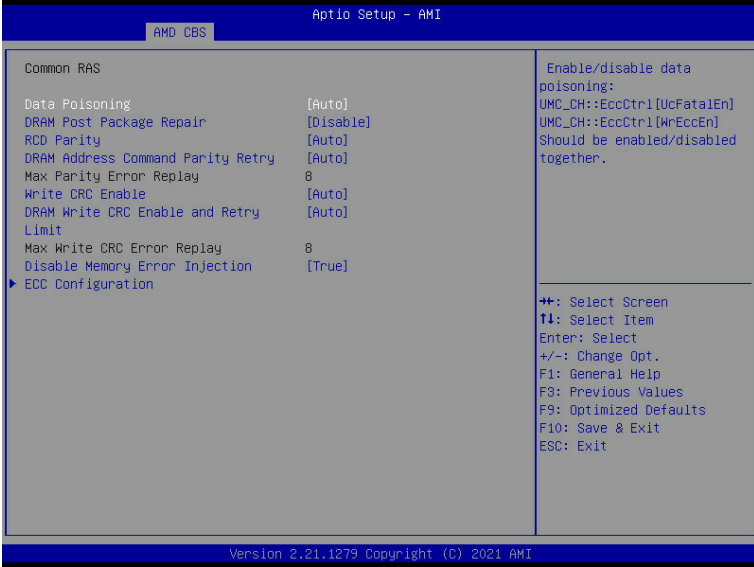
Parameter	Description
CAD Bus Configuration	
CAD Bus Timing User Controls	Setup time on CAD bus signals to Auto or Manual. Options available: Auto, Manual. Default setting is Auto .
CAD Bus Drive Strength User Controls	Drive Strength on CAD bus signals to Auto or Manual. Options available: Auto, Manual.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

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



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

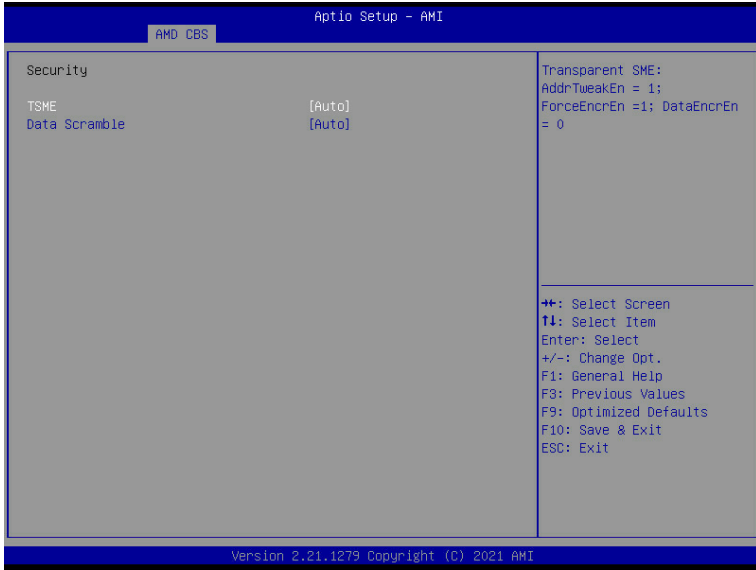
5-3-3-1-4 Common RAS



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

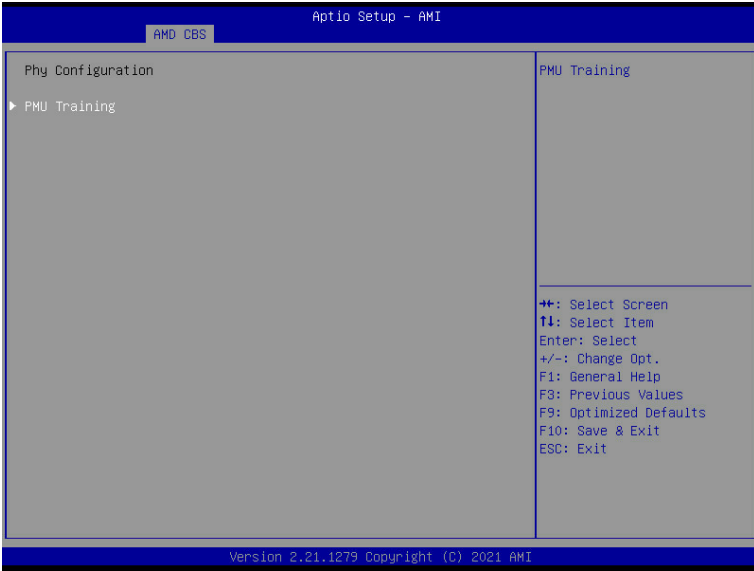
Parameter	Description
Disable Memory Error Injection	Options available: False, True. Default setting is True .
ECC Configuration	<p data-bbox="396 189 732 213">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="396 221 954 299">◆ DRAM ECC Symbol Size <ul style="list-style-type: none"> <li data-bbox="434 244 783 268">– Configures the DRAM ECC Symbol Size. <li data-bbox="434 275 926 299">– Options available: Auto, x4, x8, x16. Default setting is Auto. <li data-bbox="396 307 954 417">◆ DRAM ECC Enable <ul style="list-style-type: none"> <li data-bbox="434 330 942 385">– Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable. <li data-bbox="434 393 954 448">– Options available: Auto, Enabled, Disabled. Default setting is Auto. <li data-bbox="396 456 954 561">◆ DRAM UECC Retry <ul style="list-style-type: none"> <li data-bbox="434 479 740 503">– Enable/Disable DRAM UECC Retry. <li data-bbox="434 511 954 561">– Options available: Auto, Enabled, Disabled. Default setting is Auto.

5-3-3-1-5 Security



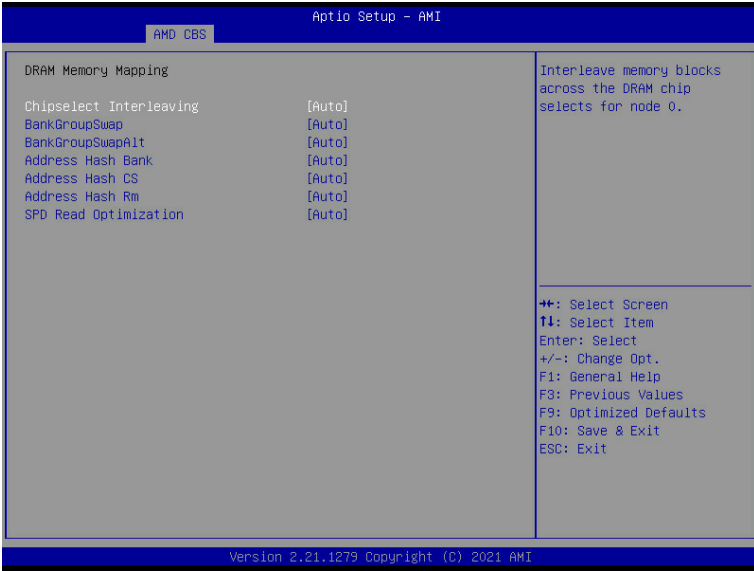
Parameter	Description
Security	
TSME	Enable/Disable transparent secure memory encryption. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Data Scramble	Enable/Disable Data Scrambling. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-3-1-6 Phy Configuration



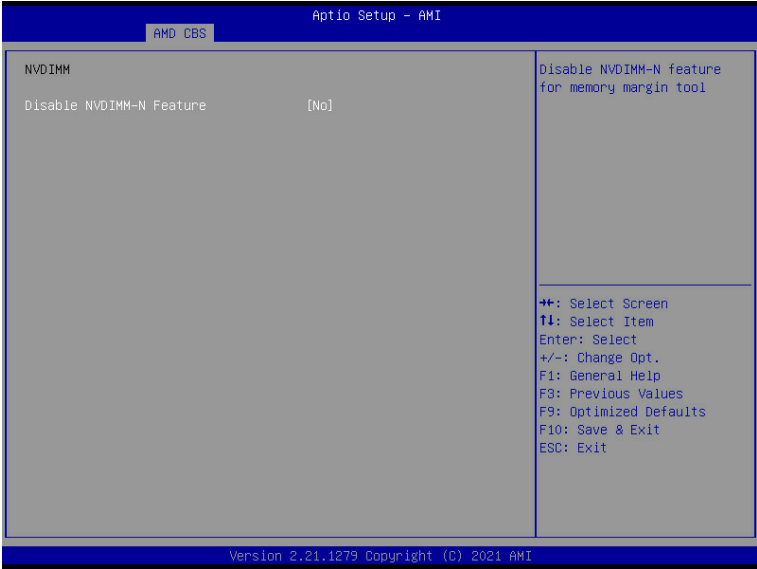
Parameter	Description
Phy Configuration	Press [Enter] to configure PMU Training.
PMU Training	<ul style="list-style-type: none"> ◆ DFE Read Training <ul style="list-style-type: none"> – Perform 2D Read Training with DFE on. – Options available: Auto, Enable, Disable. Default setting is Auto. ◆ FFE Write Training <ul style="list-style-type: none"> – Perform 2D Write Training with FFE on. – Options available: Auto, Enable, Disable. Default setting is Auto. ◆ PMU Pattern Bits Controls <ul style="list-style-type: none"> – Options available: Auto, Manual. Default setting is Auto.

5-3-3-2 DRAM Memory Mapping



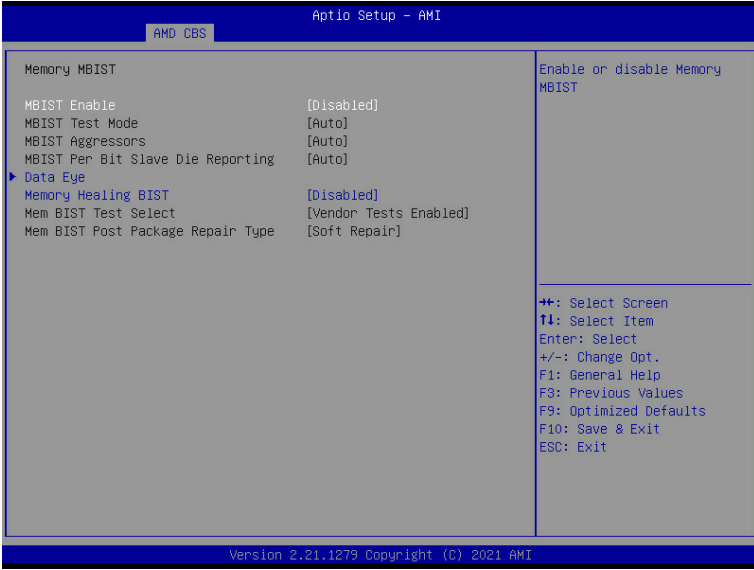
Parameter	Description
DRAM Memory Mapping	
Chipselect Interleaving	Interleave memory blocks across the DRAM chip selects for node 0. Options available: Auto, Disabled. Default setting is Auto .
BankGroupSwap	Configures the BankGroupSwap. BankGroupSwap (BGS) is a new memory mapping option in AGESA that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

5-3-3-3 NVDIMM



Parameter	Description
NVDIMM	Displays the information of the devices/controllers if installed
Disable NVDIMM-N Feature	Enable/Disable NVDIMM-N feature for memory margin tool. Options available: No, Yes. Default setting is NO .

5-3-3-4 Memory MBIST



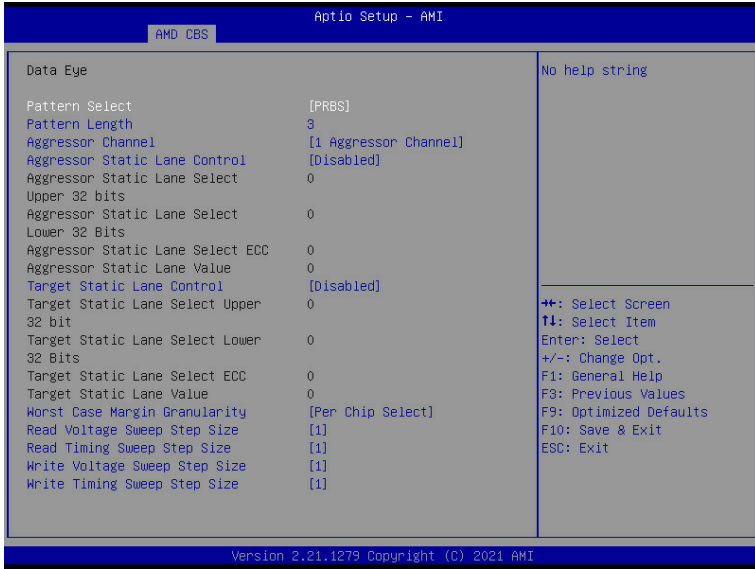
Parameter	Description
Memory MBIST	
MBIST Enable	Enable/Disable the Memory MBIST function. Options available: Enabled, Disabled. Default setting is Disabled .
MBIST Test Mode ^(Note)	Selects MBIST Test Mode. Interface Mode: Tests Single and Multiple CS transactions and Basic Connectivity. Data Eye Mode: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

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

Parameter	Description
Mem BIST Test Select ^(Note1)	Selects the Vendor specific tests to use with BIOS memory healing BIST. Options available: Vendor Tests Enabled, Vendor Tests Disabled, All Tests - All Vendors. Default setting is Vendor Tests Enabled .
Mem BIST Post Package Repair Type ^(Note1)	Selects the repair type for dram errors found in the BIOS memory BIST. Options available: Soft Repair, Hard Repair, No Repairs - Test only. Default setting is Soft Repair .

(Note1) This item is available when **Memory Healing BIST** is set to **BIOS Mem BIST**.

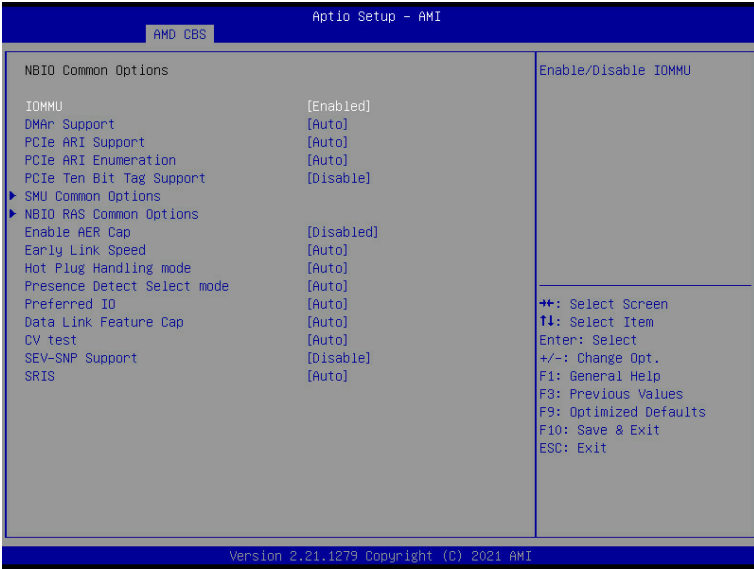
5-3-3-4-1 Data Eye



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

Parameter	Description
Target Static Lane Select Upper 32 bits	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Select Lower 32 bits	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Select ECC	This item is configurable when Target Static Lane Control is set to Enabled .
Target Static Lane Value	This item is configurable when Target Static Lane Control is set to Enabled .
Worst Case Margin Granularity	Configures Worst Case Margin Granularity. Options available: Per Chip Select, Per Nibble. Default setting is 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.

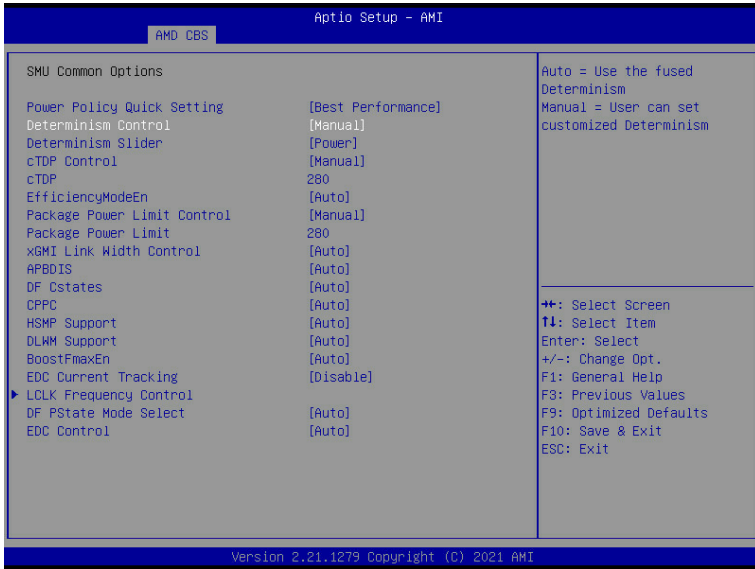
5-3-4 NBIO Common Options



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

Parameter	Description
Hot Plug Handling mode	Controls the Hot Plug Handling mode. Options available: Auto, A0 Mode, OS First (No Error Handling), OS First (Error Handling-Not Implemented), Firmware First (Not Implemented). Default setting is Auto .
Presence Detect Select mode	Controls the Presence Detect Select mode. Options available: Auto, OR, AND. Default setting is Auto .
Preferred IO	Preferred IO select type. Manual: Bus Number manually. Auto: Default. Options available: Auto, Manual. Default setting is Auto .
Data Link Feature Cap	Enable/Disable the data link feature capability. Options available: Auto, Enabled, Disabled. Default setting is Auto .
CV test	Enable/Disable the running PCIECV tool support. Options available: Auto, Enabled, Disabled. Default setting is Auto .
SEV-SNP Support	Enable/Disable the SEV-SNP support. Options available: Enable, Disable. Default setting is Disable .
SRIS	Options available: Auto, Enable, Disable. Default setting is Disable .

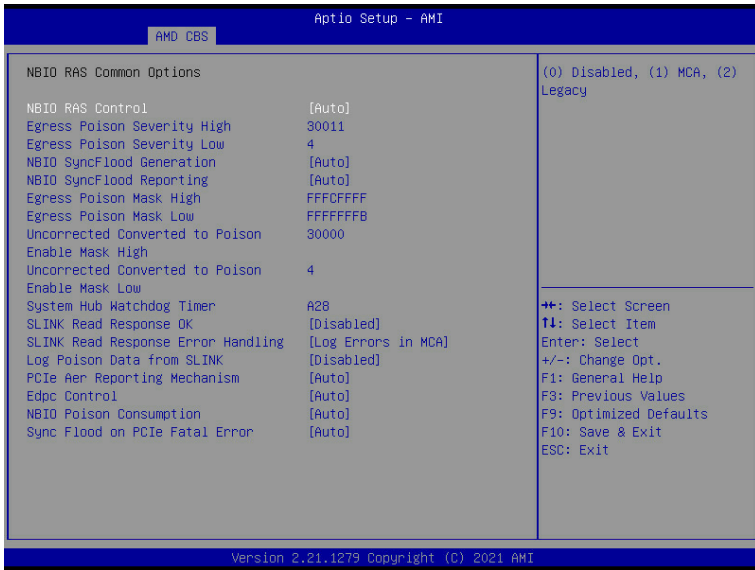
5-3-4-1 SMU Common Options



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

Parameter	Description
DF Cstates	Enable/Disable DF C-states. Options available: Auto, Enabled, Disabled. Default setting is Auto .
CPPC	Enable/Disable the CPPC feature. Options available: Auto, Enabled, Disabled. Default setting is Auto .
HSMP Support	Enable/Disable the HSMP support. Options available: Auto, Enabled, Disabled. Default setting is Auto .
DLWM Support	Enable/Disable the DLWM support. Options available: Auto, Enabled, Disabled. Default setting is Auto .
BoostFmaxEn	Options available: Auto, Enabled. Default setting is Auto .
EDC Current Tracking	Options available: Enable, Disable. Default setting is Disable .
LCLK Frequency Control	Press [Enter] for advanced configuration.
DF PSTATE Mode Select	Selects the DF PState Mode. Option available: Normal, limit Highest, Limit All, Auto. Default setting is Auto .
EDC Control	Options available: Auto, Manual. Default setting is Auto .

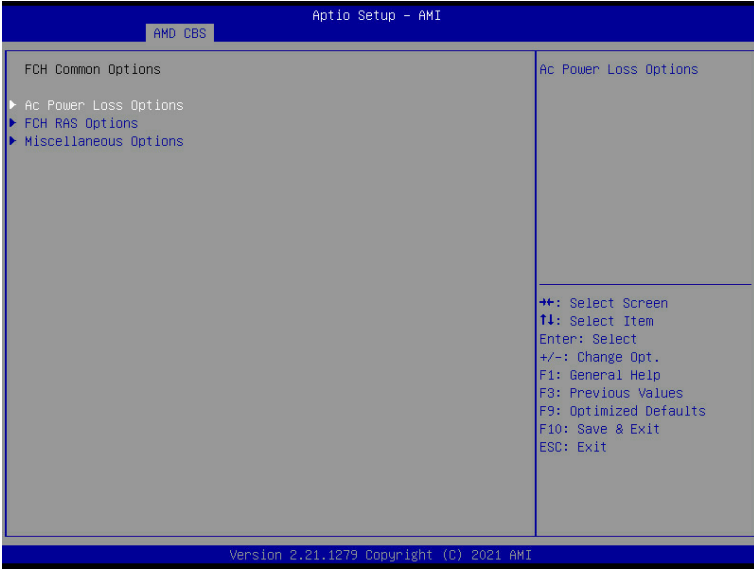
5-3-4-2 NBIO RAS Common Options



Parameter	Description
NBIO RAS Common Options	
NBIO RAS Control	Options available: Disabled, MCA, Legacy. Default setting is MCA .
Egress Poison 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: Auto, Enabled, Disabled. Default setting is Auto .
NBIO SyncFlood Reporting	The value may be used to enable SyncFlood reporting to APML. Options available: Enabled, Disabled. Default setting is Disabled .
Egress Poison Mask High	Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.
Egress Poison Mask Low	Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.

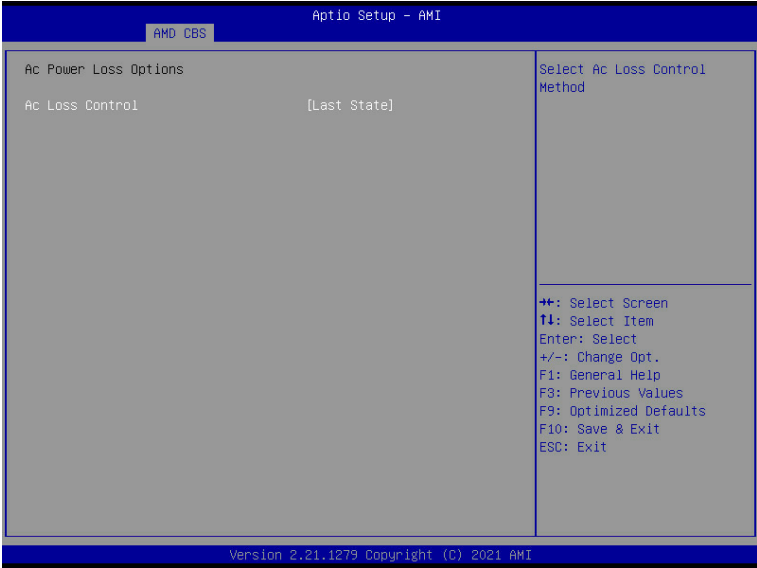
Parameter	Description
Uncorrected Converted to Poison Enable Mask High	Enables mask for masking of uncorrectable parity errors on internal arrays.
Uncorrected Converted to Poison Enable Mask Low	Enables mask for masking of uncorrectable parity errors on internal arrays.
System Hub Watchdog Timer	Specifies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

5-3-5 FCH Common Options



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

5-3-5-1 AC Power Loss Options



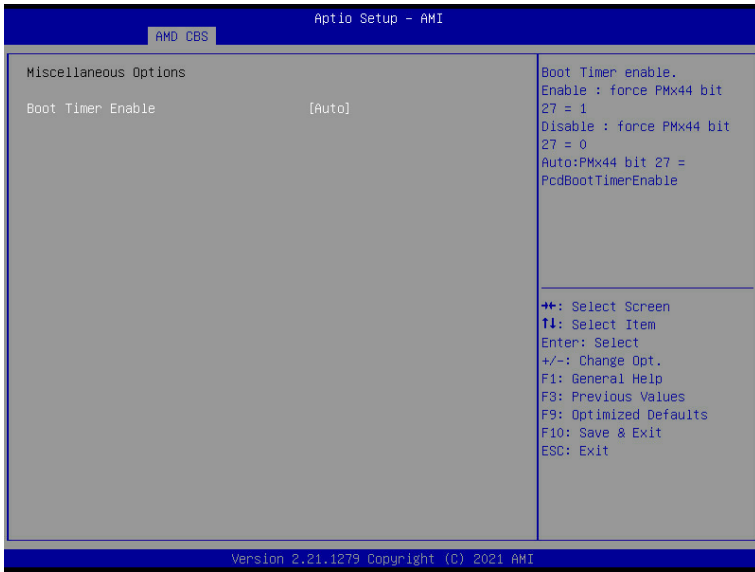
Parameter	Description
AC Power Loss Options	
AC Loss Control	Selects the AC Loss Control Method. Options available: Power Off, Power On, Last State. Default setting is Last State .

5-3-5-2 FCH RAS Options



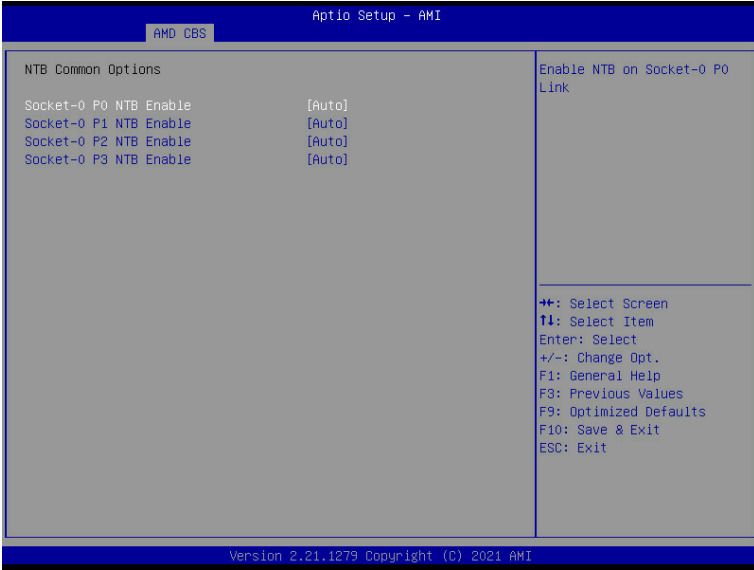
Parameter	Description
FCH RAS Options	
ALink RAS Support	Enable/Disable the ALink RAS Support. Options available: Auto, Enabled, Disabled. Default setting is Auto .
Reset after sync flood	Enables AB to forward downstream sync-flood message to system controller. Options available: Auto, Enabled, Disabled.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

5-3-5-3 Miscellaneous Options



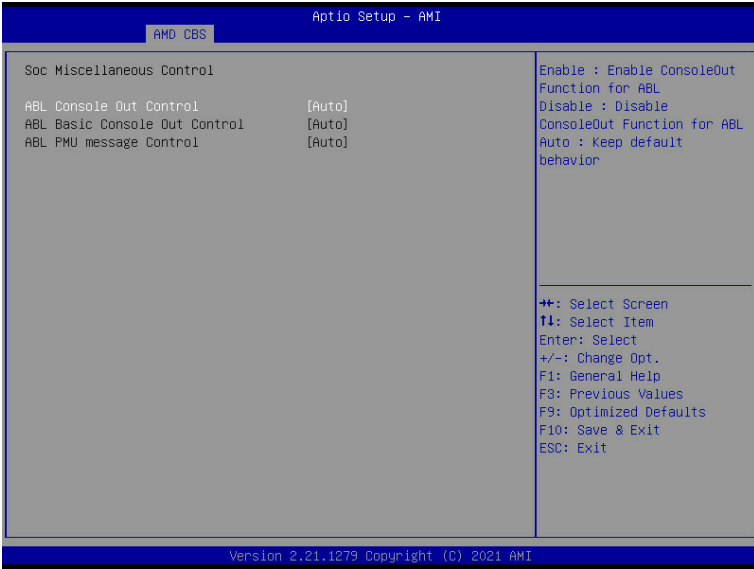
Parameter	Description
Miscellaneous Options	
Boot Timer Enable	Enable/Disable Boot Timer. Options available: Auto, Enabled, Disabled. Default setting is Auto .

5-3-6 NTB Common Options



Parameter	Description
NTB Common Options	
Socket-0 P0 NTB Enable	Options available: Auto, Enable. Default setting is Auto .
Socket-0 P1 NTB Enable	Options available: Auto, Enable. Default setting is Auto .
Socket-0 P2 NTB Enable	Options available: Auto, Enable. Default setting is Auto .
Socket-0 P3 NTB Enable	Options available: Auto, Enable. Default setting is Auto .

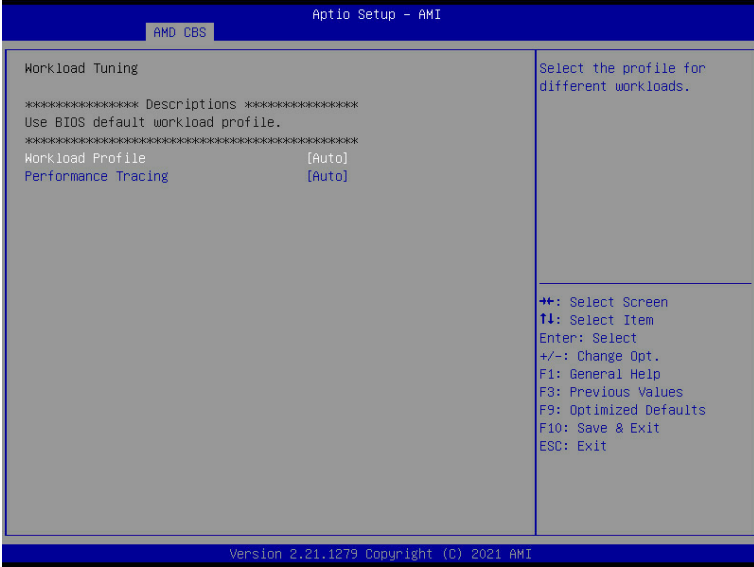
5-3-7 SOC Miscellaneous Control



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

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

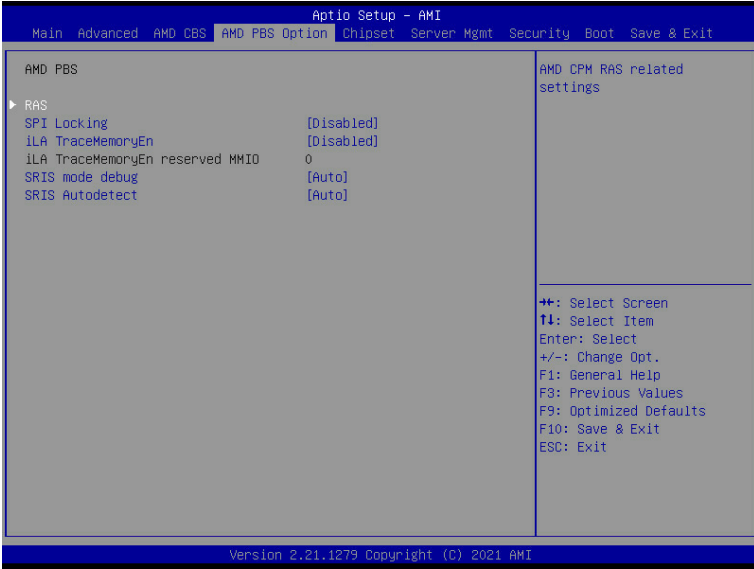
5-3-8 Workload Tuning



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

5-4 AMD PBS Menu

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



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

5-4-1 RAS

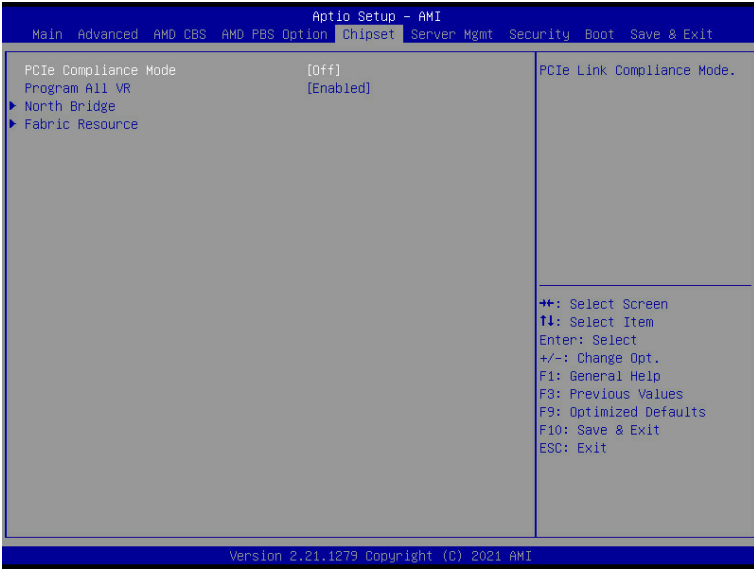


Parameter	Description
RAS Periodic SMI Control	Enable/Disable the Periodic SMI for polling [MCA Threshold] error. Options available: Enabled, Disabled. Default setting is Enabled .
SMI Threshold	Configures the SMI Threshold value.
SMI Scale	Configures the SMI Scale value.
SMI Scale Unit	Defines the unit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

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

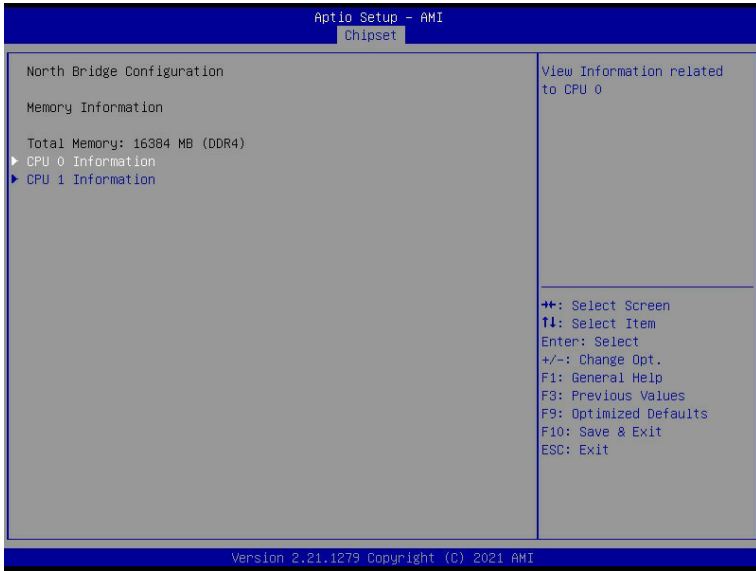
5-5 Chipset Setup Menu

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



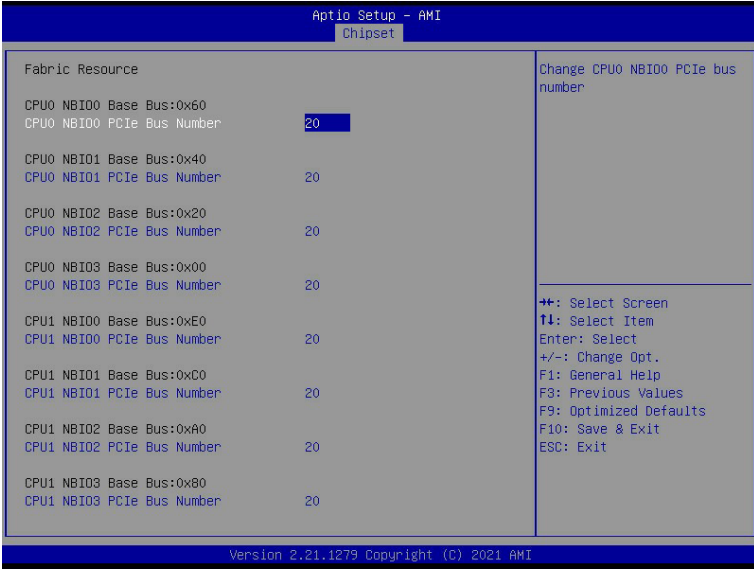
Parameter	Description
PCIe Compliance Mode	Options available: On, Off. Default setting is Off .
Program All VR	Enable/Disable program all VR on MB. Options available: Enabled, Disabled. Default setting is Enabled .
North Bridge	Press [Enter] for configuration of advanced items.
Fabric Resource	Press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

5-5-1 North Bridge



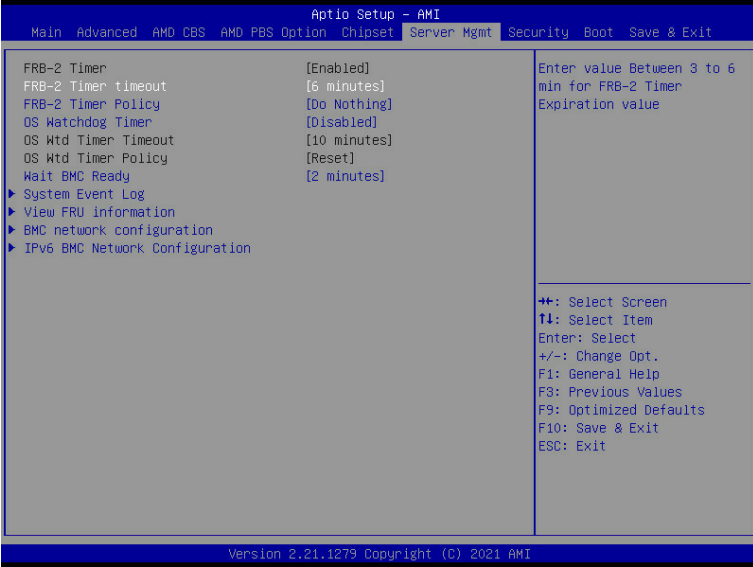
Parameter	Description
North Bridge Configuration	
Memory Information	
Total Memory	Displays the total memory information.
CPU 0/1 Information	Press [Enter] to view information related to CPU 0/1.

5-5-2 Fabric Resource



Parameter	Description
Fabric Resource	
CPU 0/1 NBIO_# PCIe Bus Number	Change CPU 0/1 NBIO_# PCIe Bus Number.

5-6 Server Management Menu



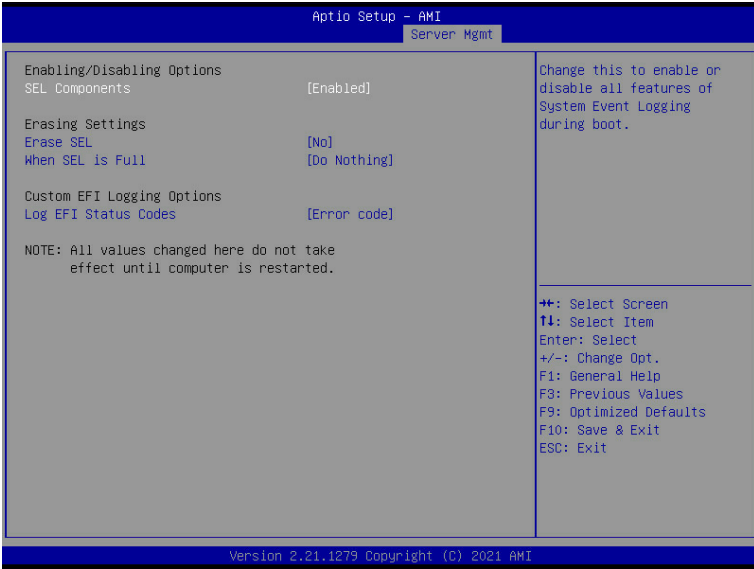
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is Enabled .
FRB-2 Timer ^(Note1) timeout	Configures the FRB2 Timer timeout. Options available: 3 minutes, 4 minutes, 5 minutes, 6 minutes. Default setting is 6 minutes .
FRB-2 Timer Policy ^(Note1)	Configures the FRB2 Timer policy. Options available: Do Nothing, Reset, Power Down. Default setting is Do Nothing .
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled, Disabled. Default setting is Disabled .
OS Wtd Timer Timeout ^(Note2)	Configures OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is 10 minutes .
OS Wtd Timer Policy ^(Note2)	Configure OS Watchdog Timer Policy. Options available: Reset, Do Nothing, Power Down. Default setting is Reset .
Wait BMC Ready	Post wait BMC ready and reboot system. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is 2 minutes .

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

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

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

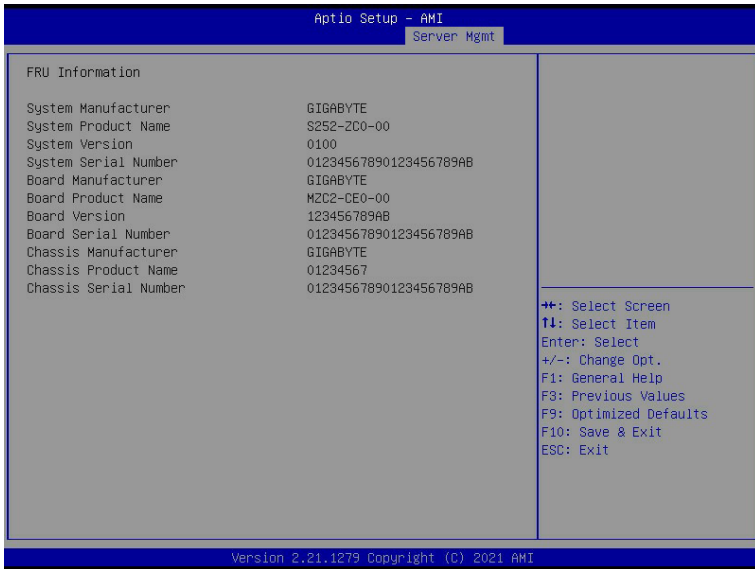
5-6-1 System Event Log



Parameter	Description
Enabling / Disabling Options	
SEL Components	Change this item to enable or disable all features of System Event Logging during boot. Options available: Enabled, Disabled. Default setting is Enabled .
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: No/Yes, On next reset/Yes, On every reset. Default setting is No .
When SEL is Full	Choose options for reactions to a full SEL. Options available: Do Nothing, 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 .

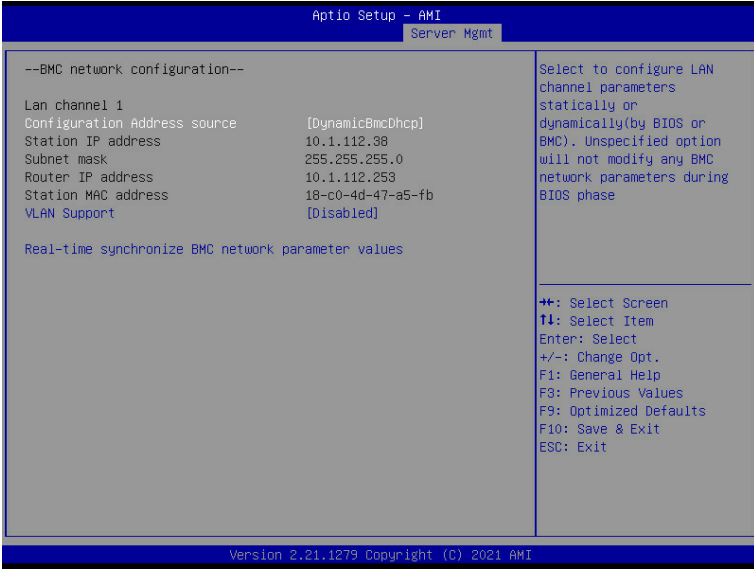
5-6-2 View FRU Information

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.



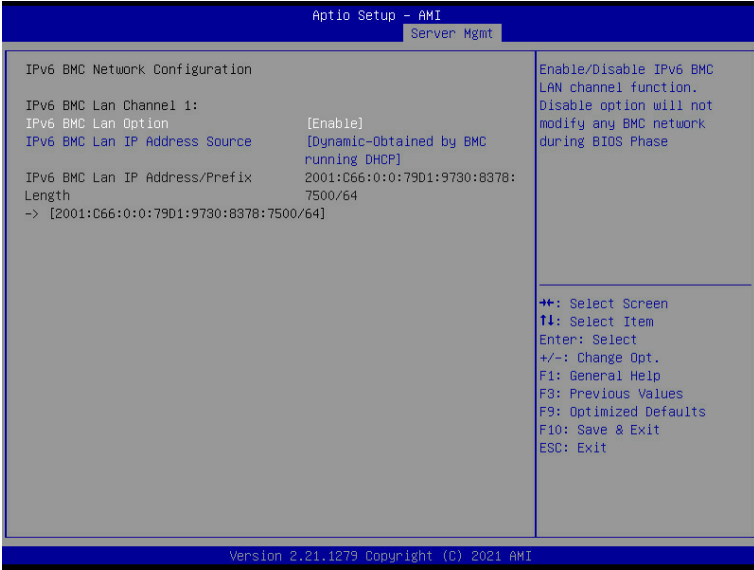
(Note) The model name will vary depends on the product you purchased

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.

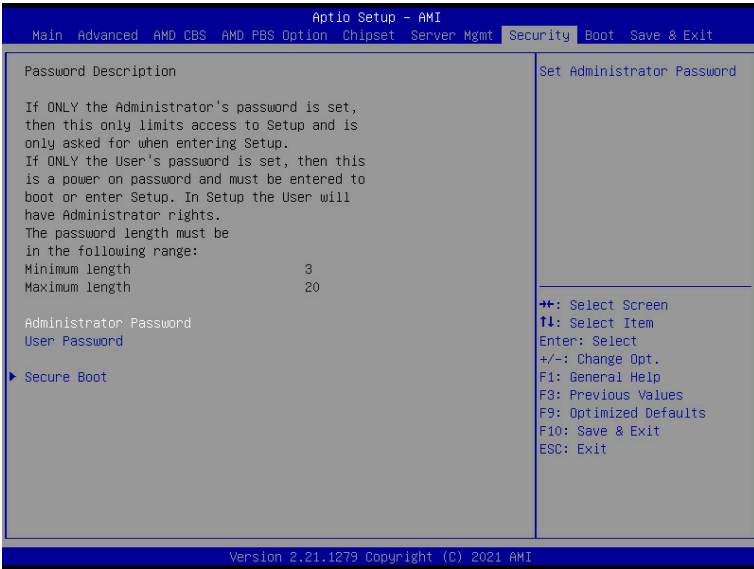
5-6-4 IPv6 BMC Network Configuration



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



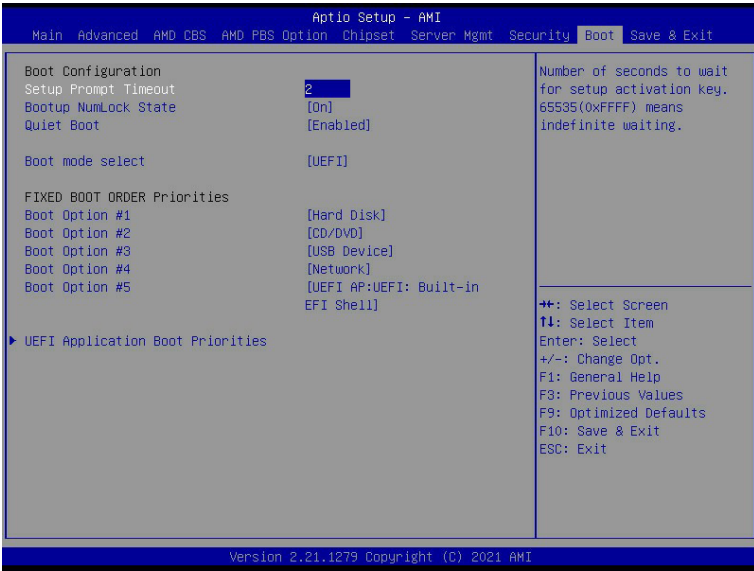
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, Disabled. Default setting is Disabled .
Secure Boot Mode ^(Note)	Secure Boot requires all the applications that are running during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

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

Parameter	Description
Key Management	<p data-bbox="333 158 666 181">Press [Enter] to configure advanced items.</p> <p data-bbox="333 186 937 236">Please note that this item is configurable when Secure Boot Mode is set to Custom.</p> <ul style="list-style-type: none"> <li data-bbox="333 241 945 349">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="370 268 945 318">– Allows to provision factory default Secure Boot keys when system is in Setup Mode. <li data-bbox="370 323 905 349">– Options available: Enabled, Disabled. Default setting is Disabled. <li data-bbox="333 354 926 432">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="370 381 926 406">– Installs all factory default keys. It will force the system in User Mode. <li data-bbox="370 410 605 432">– Options available: Yes, No. <li data-bbox="333 437 902 519">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="370 464 902 519">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). <li data-bbox="333 523 701 573">◆ Restore DB defaults <ul style="list-style-type: none"> <li data-bbox="370 550 701 573">– Restore DB variable to factory defaults. <li data-bbox="333 578 896 628">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="370 605 896 628">– Displays the current status of the variables used for secure boot. <li data-bbox="333 633 802 741">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="370 660 802 685">– Displays the current status of the Platform Key (PK). <li data-bbox="370 689 678 715">– Press [Enter] to configure a new PK. <li data-bbox="370 719 602 741">– Options available: Update. <li data-bbox="333 746 942 882">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="370 773 942 851">– Displays the current status of the Key Exchange Key Database (KEK). <li data-bbox="370 799 905 851">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="370 856 671 882">– Options available: Update, Append. <li data-bbox="333 887 905 1023">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="370 914 905 939">– Displays the current status of the Authorized Signature Database. <li data-bbox="370 943 945 994">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="370 998 671 1023">– Options available: Update, Append. <li data-bbox="333 1028 902 1165">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="370 1055 902 1080">– Displays the current status of the Forbidden Signature Database. <li data-bbox="370 1085 892 1135">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="370 1139 671 1165">– Options available: Update, Append. <li data-bbox="333 1169 928 1306">◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li data-bbox="370 1196 928 1221">– Displays the current status of the Authorized TimeStamps Database. <li data-bbox="370 1226 905 1276">– Press [Enter] to configure a new DBT or load additional DBT from storage devices. <li data-bbox="370 1281 671 1306">– Options available: Update, Append. <li data-bbox="333 1310 919 1440">◆ OsRecovery Signatures <ul style="list-style-type: none"> <li data-bbox="370 1337 919 1362">– Displays the current status of the OsRecovery Signature Database. <li data-bbox="370 1367 887 1417">– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices. <li data-bbox="370 1422 671 1440">– 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.

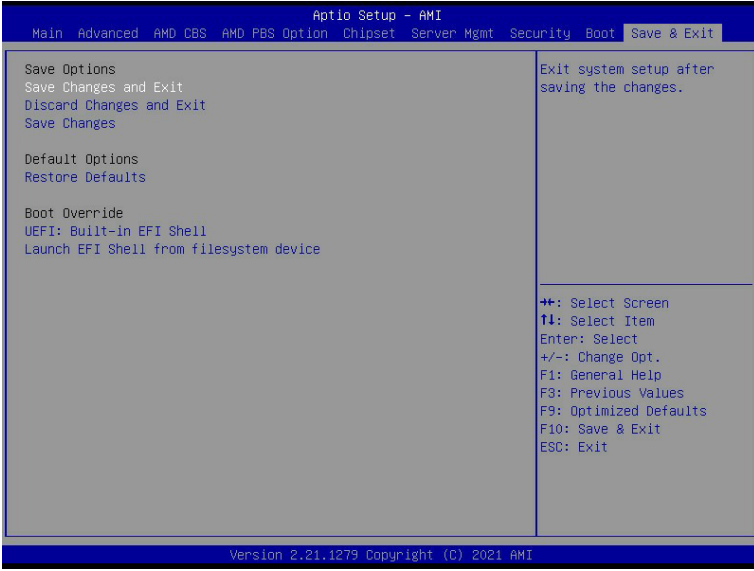


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off. Default setting is Off .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled, Disabled. Default setting is Enabled .
Boot mode select	Selects the boot mode. Options available: LEGACY, UEFI. Default setting is UEFI .

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

5-10-1 PEI Beep Codes

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

5-10-2 DXE Beep Codes

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