GIGABYTE™

MZ72-HB2

AMD EPYC™ 7003 Dual Sockets Server Motherboard

User Manual

Rev. 3.0

Copyright

Disclaimer

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 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.

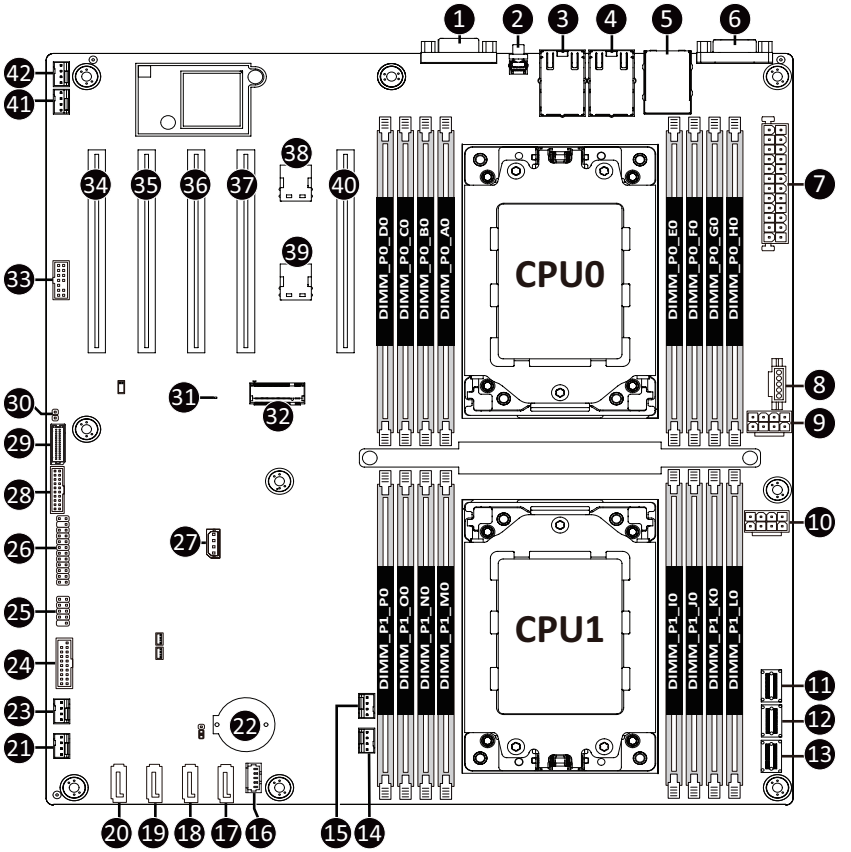
For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: http://reseller.b2b.gigabyte.com

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

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

Table of Contents

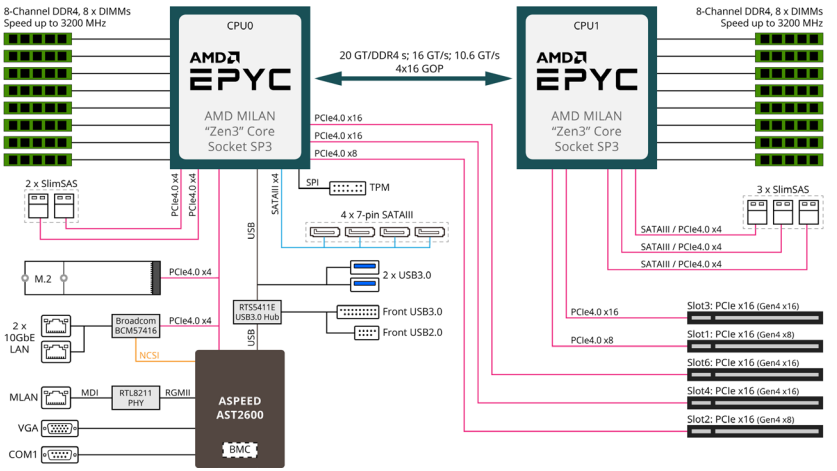
MZ72-HB2 Motherboard Layout



Item	Code	Description
1	VGA	VGA Port
2	SW_ID	ID Button with LED
3	LAN1	10GbE LAN Port #1
4	LAN2	10GbE LAN Port #2
5	USB3_MLAN	Server Management LAN Port (Top)/ USB3.0 Ports (Bottom)
6	COM1	Serial Port
7	ATX	2 x 12 Pin Main Power Connector
8	PMBUS	PMBus Connector
9	P12V_1	2 x 4 Pin 12V Power Connector (for CPU0)
10	P12V_2	2 x 4 Pin 12V Power Connector (for CPU1)
11	SLSAS_0	Slimline Connector #0 (SATAIII 6Gb/s Signal)
12	SLSAS_2	Slimline Connector #2 (SATAIII 6Gb/s Signal)
13	SLSAS_1	Slimline Connector #1 (SATAIII 6Gb/s Signal)
14	CPU1_FAN	CPU Fan Connector (for CPU1)
15	CPU0_FAN	CPU Fan Connector (for CPU0)
16	SATA_SGP	SATA SGPIO Connector
17	SATA3	SATAIII 6Gb/s Connector #3
18	SATA2	SATAIII 6Gb/s Connector #2
19	SATA1	SATAIII 6Gb/s Connector #1
20	SATA0	SATAIII 6Gb/s Connector #0
21	SYS_FAN2	System Fan Connector #2
22	BAT	Battery Socket
23	SYS_FAN1	System Fan Connector #1
24	F_USB3	Front Panel USB 3.0 Connector
25	F_USB2	USB 2.0 Header
26	FP_1	Front Panel Header
27	IPMB	IPMB Connector
28	CN_NCSI	NCSI Connector
29	BP_1	HDD Back Plane Board Connector
30	CASE_OPEN	Case Open Intrusion Alert Header
31	LED_BMC	BMC Firmware Readiness LED
32	M2_0	M.2 slot (PCIe Gen4 x4, Support NGFF-2280/22110)
33	SPI_TPM	TPM Module Connector
34	PCIE_1	PCIe x16 Slot #1 (Gen4 x8)
35	PCIE_2	PCIe x16 Slot #2 (Gen4 x8)
36	PCIE_3	PCIe x16 Slot #3 (Gen4 x16)
37	PCIE_4	PCIe x16 Slot #4 (Gen4 x16)
38	NVME_0	Slimline SAS 4i Connector (NVMe/PCIe Gen4 x4)
39	NVME_1	Slimline SAS 4i Connector (NVMe/PCIe Gen4 x4)
40	PCIE_6	PCIe x16 Slot #6 (Gen4 x16)
41	SYS_FAN4	System Fan Connector #4
42	SYS_FAN3	System Fan Connector #3

Block Diagram

MZ72-HB2 Motherboard Block Diagram



Chapter 1 Hardware Installation

1-1 Installation Precautions

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

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

1-2 Product Specifications

NOTE:

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

Form Factor	◆ E-ATX ◆ 305W x 330D (mm)
CPU	◆ AMD EPYC™ 7003 processors with AMD 3D V-Cache™ Technology ◆ AMD EPYC™ 7003 series processor family ◆ Dual processors, 7nm, Socket SP3 ◆ Up to 64-core, 128 threads per processor ◆ cTDP up to 280W ◆ Compatible with AMD EPYC™ 7002 series processor family
Chipset	◆ System on Chip
Memory	◆ 16 x DIMM slots ◆ DDR4 memory supported only ◆ 8-Channel memory architecture ◆ RDIMM modules up to 128GB supported ◆ LRDIMM modules up to 128GB supported ◆ 3DS RDIMM/LRDIMM modules up to 256GB supported ◆ Memory speed: Up to 3200/ 2933 MHz
LAN	◆ 2 x 10GbE LAN ports (1 x Broadcom® BCM57416) ◆ 1 x 10/100/1000 management LAN
Onboard Graphics	◆ Integrated in Aspeed® AST2600 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
Storage Interface	◆ 4 x 7-pin SATA 6Gb/s ports ◆ *3 x SlimSAS (with 12 x SATA 6Gb/s or 3 x NVMe PCIe Gen4 x4) ports ◆ 1 x M.2 slot: - M-key - PCIe Gen4 x4 - Supports NGFF-2280/22110 cards ◆ 2 x NVMe ports: - SlimSAS 4i type - PCIe Gen4 x4 per port ***Note!** **Default setting is SATA, please go to BIOS Setup section, Advances>PCI Sub-system setting for advanced configuration manually.**

Expansion Slots	◆	Slot_6: 1 x PCIe x16 (Gen4 x16 bus) slot (from CPU_0)
	◆	Slot_4: 1 x PCIe x16 (Gen4 x16 bus) slot (from CPU_0)
	◆	Slot_3: 1 x PCIe x16 (Gen4 x16 bus) slot (from CPU_1)
	◆	Slot_2: 1 x PCIe x16 (Gen4 x8 bus) slot (from CPU_0)
	◆	Slot_1: 1 x PCIe x16 (Gen4 x8 bus) slot (from CPU_1)
Internal I/O Connectors	◆	1 x 24-pin ATX main power connector
	◆	2 x 8-pin ATX 12V power connectors
	◆	5 x SlimSAS connectors
	◆	4 x SATA 7-pin connects
	◆	1 x M.2 slot
	◆	2 x CPU fan headers
	◆	4 x System fan headers
	◆	1 x USB 3.0 header
	◆	1 x USB 2.0 header
	◆	1 x TPM header
	◆	1 x Front panel header
	◆	1 x PMBus connector
	◆	1 x IPMB connector
	◆	1 x Clear CMOS jumper
	◆	1 x BIOS recovery jumper
Rear I/O Connectors	◆	2 x USB 3.0 ports
	◆	1 x VGA port
	◆	1 x Serial port
	◆	2 x RJ45 ports
	◆	1 x MLAN port
	◆	1 x ID button with LED
TPM	◆	1 x TPM header with SPI interface
	◆	Optional TPM2.0 kit: CTM010

	Board Management	◆ Aspeed® AST2600 management controller ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface ◆ Dashboard ◆ HTML5 KVM ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status …etc.) ◆ Sensor Reading History Data ◆ FRU Information ◆ SEL Log in Linear Storage / Circular Storage Policy ◆ Hardware Inventory ◆ Fan Profile ◆ System Firewall ◆ Power Consumption ◆ Power Control ◆ 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 40°C ◆ Operating humidity: 8-80% (non-condensing) ◆ Non-operating temperature: -40°C to 60°C ◆ Non-operating humidity: 20%-95% (non-condensing)

1-3 Installing and Removing the CPU and Heat Sink

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

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

WARNING!

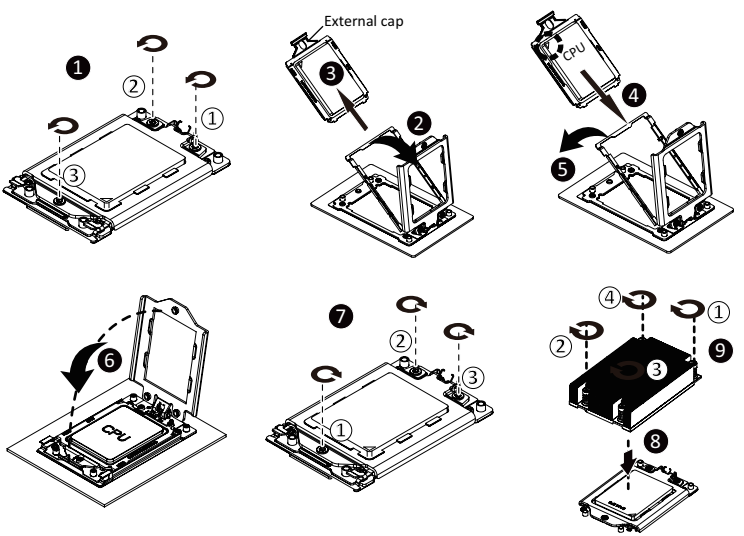
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

Follow these instructions to Install the CPU:

1. Loosen the three captive screws in sequential order (1→2→3) securing the CPU cover.
2. Flip open the CPU cover.
3. Remove the CPU cap with CPU from the CPU frame using the handle on the CPU cap.
4. Using the handle on the CPU cap insert the new CPU cap with CPU installed into the CPU frame.

   Note: Ensure that the CPU is installed in the CPU cap in the correct orientation, with the gold triangle on the CPU aligned to the top left corner of the CPU cap.

5 Flip the CPU frame with CPU installed into place in the CPU socket.



Note:

- Lock the CPU by using a T20-Lobe driver to tighten 3 captive nuts in sequence as 1-3.
- The screw tightening torque: 16.1 ± 1.2 kgf-cm

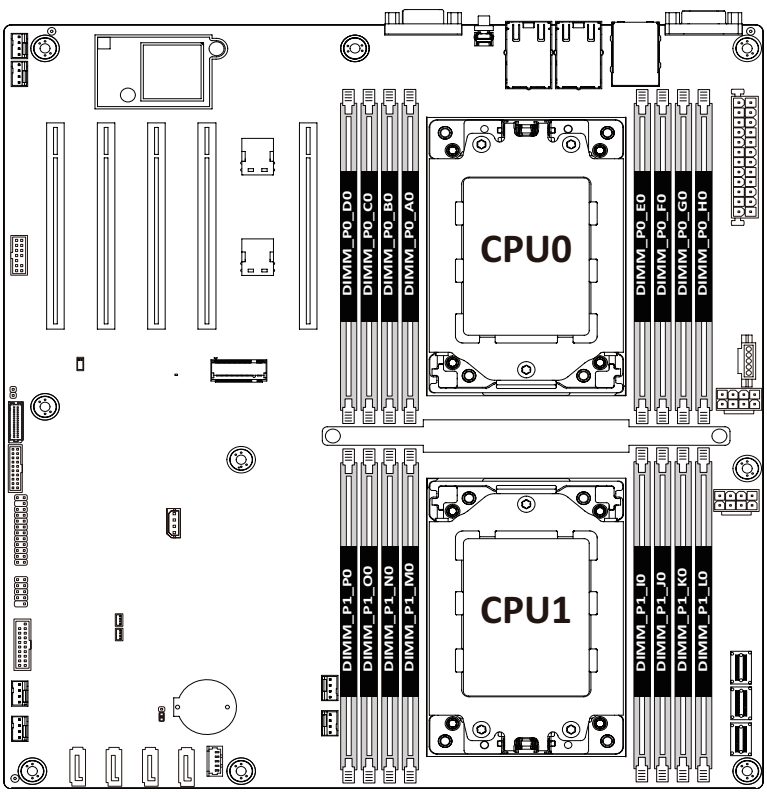
1-4 Installing and Removing Memory

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.

1-4-1 8-Channel Memory Configuration

This motherboard provides 16 DDR4 memory slots and supports 8-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.

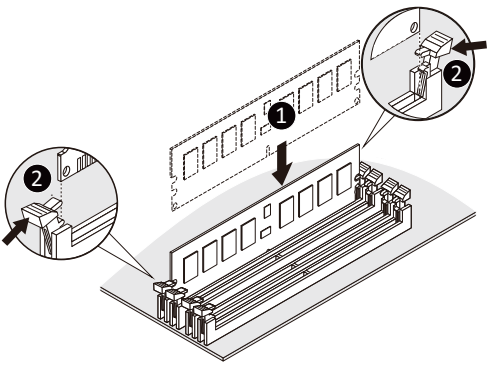


1-4-2 Installing and Removing the Memory Module

Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.
Be sure to install DDR4 DIMMs on to this motherboard.

Follow these instructions to install a DIMM module:

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



1-4-3 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

1-4-4 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

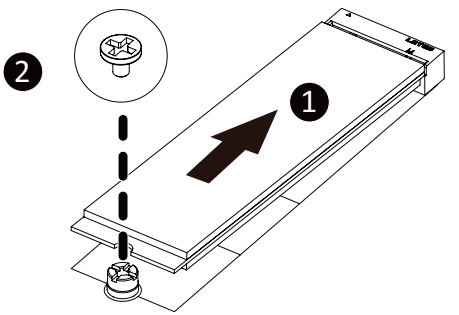
Note:

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

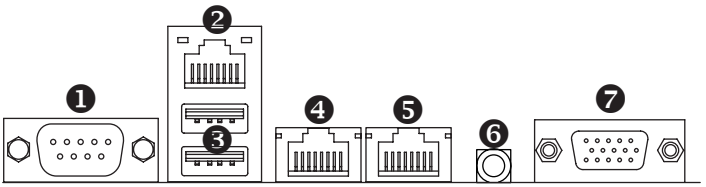
1-5 Installing and Removing the M.2 SSD Module

Follow the steps below to install an optional M.2 SSD module on your motherboard.

Step1. Insert the M.2 SSD module into the slot.
Step2. Secure it with the screw, tightening as necessary to fasten the M.2 SSD module in place.



1-6 Back Panel Connectors



❶ Serial Port

Connects to serial-based mouse or data processing devices.

❷ 10/100/1000 Server Management LAN Port

The LAN port provides Internet connection with data transfer speeds of 10/100/1000Mbps. This port is the dedicated LAN port for Server Management.

❸ USB 3.0 Ports

The USB port supports the USB 3.0 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

❹ 10GBASE-T RJ-45 LAN Port #2

The 10 Gigabit Ethernet LAN port provides Internet connection at up to 10 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

❺ 10GBASE-T RJ-45 LAN Port #1

The 10 Gigabit Ethernet LAN port provides Internet connection at up to 10 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

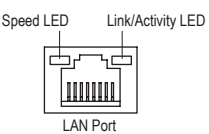
❻ ID button with LED

When the system identification is active, the ID LED on the front/ back panel glows blue.

❼ VGA Port

Connects to a monitor device.

LAN and ID Button LEDs



10GbE LAN LED:

State	Description
Yellow On	5Gbps, 2.5Gbps, 1Gps data rate
Green On	10Gbps data rate
Off	100Mbps data rate

10/100/1000 LAN LED:

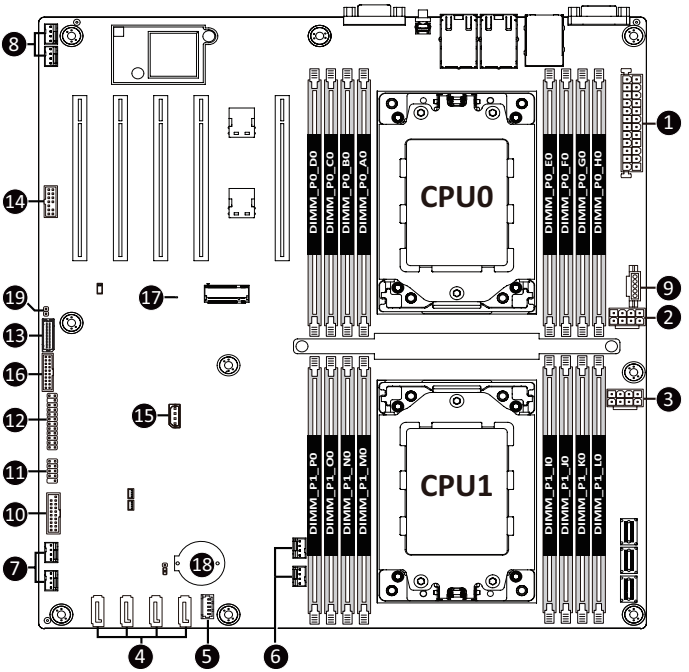
State	Description
Yellow On	1Gbps data rate
Green On	100Mbps data rate
Off	10Mbps data rate

ID button/LED:

State	Description
Blue On	System identification is active
Off	System identification is disabled

- When removing the cable connected to a back panel connector, first remove the cable from your device and then remove it from the motherboard.
- When removing the cable, pull it straight out from the connector. Do not rock it side to side to prevent an electrical short inside the cable connector.

1-7 Internal Connectors



1)	ATX	11)	F_USB2
2)	P12V_1 (for CPU0)	12)	FP_1
3)	P12V_2 (for CPU1)	13)	BP_1
4)	SATA0/SATA1/SATA2/SATA3	14)	SPI_TPM
5)	SATA_SGP	15)	IPMB
6)	CPU0_FAN/ CPU1_FAN	16)	CN_NSCI
7)	SYS_FAN1/SYS_FAN2	17)	LED_BMC
8)	SYS_FAN3/SYS_FAN4	18)	BAT
9)	PMBUS	19)	CASE_OPEN
10)	F_USB3	--	--

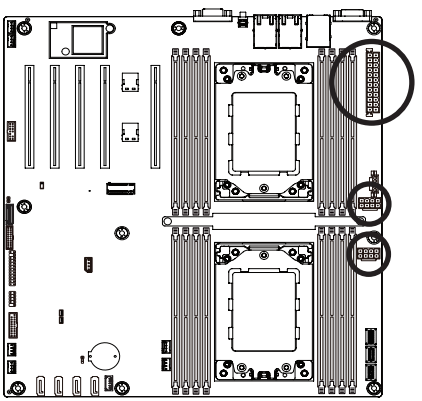
Read the following guidelines before connecting external devices:

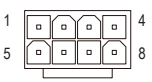
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the computer, make sure the device cable has been securely attached to the connector on the motherboard.

1/2/3) ATX/P12V_1/P12V_2 (2x12 Main Power Connector and 2x4 12V Power Connector)

With the use of the power connector, the power supply can supply enough stable power to all the components on the motherboard. Before connecting the power connector, first make sure the power supply is turned off and all devices are properly installed. The power connector possesses a foolproof design. Connect the power supply cable to the power connector in the correct orientation. The 12V power connector mainly supplies power to the CPU. If the 12V power connector is not connected, the computer will not start.

To meet expansion requirements, it is recommended that a power supply that can withstand high power consumption be used (500W or greater). If a power supply is used that does not provide the required power, the result can lead to an unstable or unbootable system.





P12V_1/ P12V_2

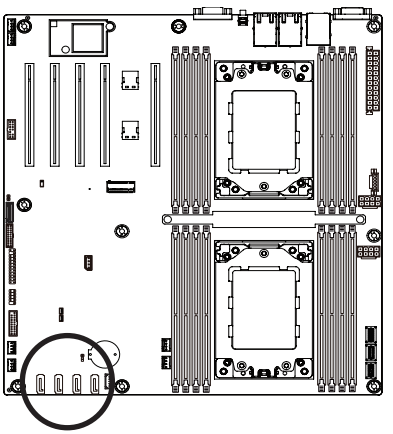
Pin No.	Definition
1	GND
2	GND
3	GND
4	GND
5	+12V
6	+12V
7	+12V
8	+12V

ATX

Pin No.	Definition	Pin No.	Definition
1	3.3V	13	3.3V
2	3.3V	14	-12V
3	GND	15	GND
4	+5V	16	PS_ON
5	GND	17	GND
6	+5V	18	GND
7	GND	19	GND
8	Power Good	20	-5V
9	5VSB	21	+5V
10	+12V	22	+5V
11	+12V	23	+5V
12	3.3V	24	GND

4) SATA0/SATA1/SATA2/SATA3 (SATA 6Gb/s Connectors)

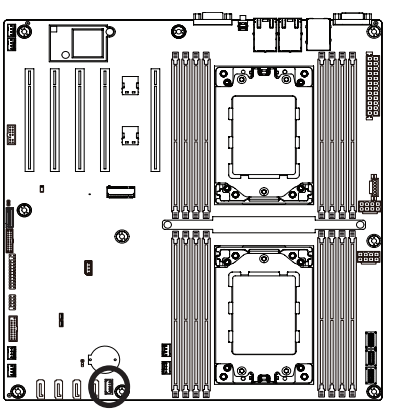
The SATA connectors conform to SATA 6Gb/s standard and are compatible with SATA 3Gb/s standard. Each SATA connector supports a single SATA device.



Pin No.	Definition
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND

5) SATA_SGP (SATA SGPIO) Connector

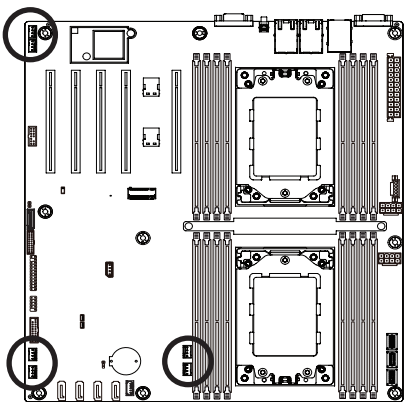
Serial General Purpose Input/Output (SGPIO) is a communication method used between a host bus adapter (HBA) and a main board.

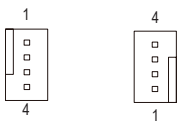


Pin No.	Definition
1	Data Out
2	GND
3	Data In
4	Load
5	Clock

6/7/8) CPU0_FAN//CPU1_FAN/SYS_FAN1/SYS_FAN2/SYS_FAN3/SYS_FAN4 (CPU FAN/System FAN Headers)

The motherboard has two 4-pin CPU fan header (CPU_FAN), and four 4-pin (SYS_FAN) system fan headers. Most fan headers possess a foolproof insertion design. When connecting a fan cable, be sure to connect it in the correct orientation (the black connector wire is the ground wire). The motherboard supports CPU fan speed control, which requires the use of a CPU fan with fan speed control design. For optimum heat dissipation, it is recommended that a system fan be installed inside the chassis.



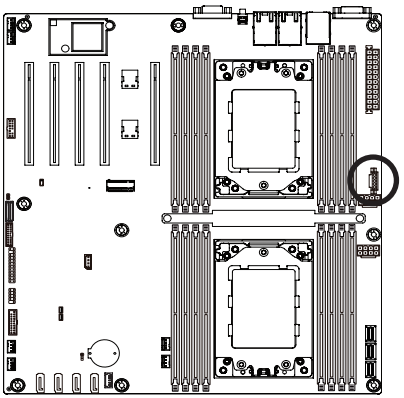


Pin No.	Definition
1	GND
2	+12V
3	Sense
4	Speed Control

- Be sure to connect fan cables to the fan headers to prevent your CPU and system from overheating. Overheating may result in damage to the CPU or the system may hang.
- These fan headers are not configuration jumper blocks. Do not place a jumper cap on the headers.

9) PMBus Connector

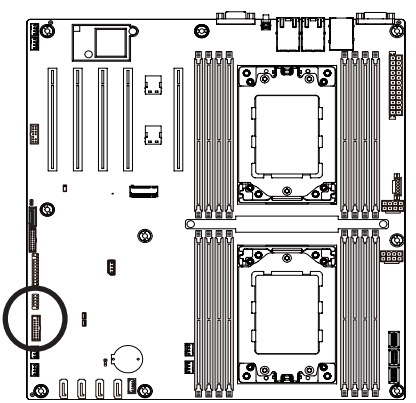
The Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



Pin No.	Definition
1	PMBus Clock
2	PMBus Data
3	PMBus Alert
4	GND
5	3.3V Sense

10/11) F_USB3/ F_USB2 (USB 3.0 Connector/ 2.0 Header)

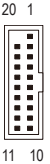
The connector/header conform to USB 2.0/ 3.0 specification. Each USB connector/header can provide two USB ports via an optional USB bracket. For purchasing the optional USB bracket, please contact the local dealer.



USB 2.0 Header

Pin No.	Definition	Pin No.	Definition
1	Power (5V)	6	USB DY+
2	Power (5V)	7	GND
3	USB DX-	8	GND
4	USB DY-	9	No Pin
5	USB DX+	10	No Connect

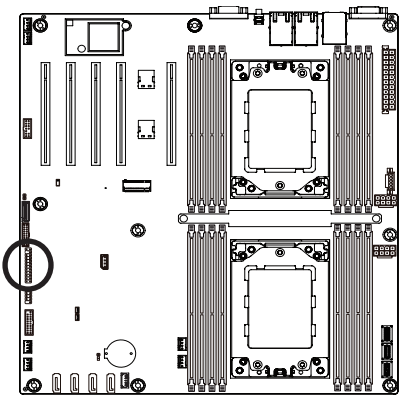
USB 3.0 Connector



Pin No.	Definition	Pin No.	Definition
1	Power	11	IntA_P2_D+
2	IntA_P1_SSRX-	12	IntA_P2_D-
3	IntA_P1_SSRX+	13	GND
4	GND	14	IntA_P2_SSTX+
5	IntA_P1_SSTX-	15	IntA_P2_SSTX-
6	IntA_P1_SSTX+	16	GND
7	GND	17	IntA_P2_SSRX+
8	IntA_P1_D-	18	IntA_P2_SSRX-
9	IntA_P1_D+	19	Power
10	NC	20	No Pin

12) FP_1 (Front Panel Header)

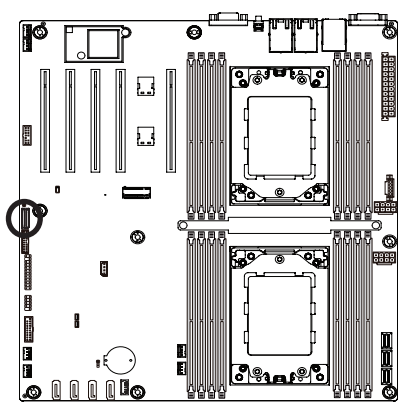
Connect the power switch, reset switch, speaker, chassis intrusion switch/sensor and system status indicator on the chassis to this header according to the pin assignments below. Note the positive and negative pins before connecting the cables.

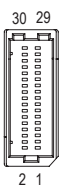


Pin No.	Definition	Pin No.	Definition
1	Power LED+	2	5V Standby
3	No Pin	4	ID LED+
5	Power LED-	6	ID LED-
7*	HDD LED+	8	System Status LED+
9*	HDD LED-	10	System Status LED-
11	Power Button	12	LAN1 Active LED+
13	GND	14	LAN1 Link LED-
15	Reset Button	16	SMBus Data
17	GND	18	SMBus Clock
19	ID Button	20	Case Open
21	GND	22	LAN2 Actve LED+
23	NMI Switch	24	LAN2 Link LED-
*Note: Pin 7 & Pin 9 are reserved for Gigabyte systems.			

The front panel design may differ by chassis. A front panel module mainly consists of power switch, reset switch, power LED, hard drive activity LED, speaker etc. When connecting your chassis front panel module to this header, make sure the wire assignments and the pin assignments are matched correctly.

13) BP_1 (HDD Backplane Board Header)

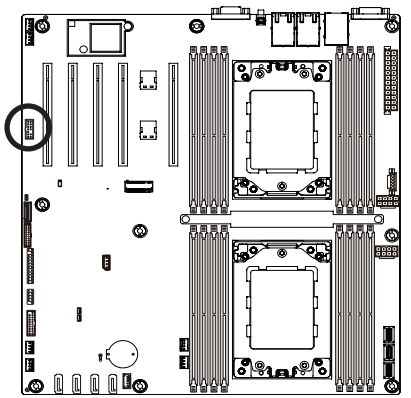


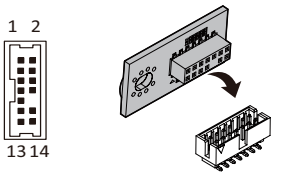


Pin No.	Definition	Pin No.	Definition
1	HP_ALERT_L	2	BPMI DIN/OUT
3	GND	4	BPMI DIN/IN
5	BPMI_LOAD	6	GND
7	BPMI_CLK	8	PLD_Program_EN
9	GLED_AMB_N	10	GLED_GRN_N
11	FAN_IRQ_N	12	Reserved
13	BP_SCL	14	GND
15	BP_SDA	16	BP_RST_N
17	SMB_U2_TMP_SCL	18	GND
19	SMB_U2_TMP_SDA	20	I2C_DEV_RST
21	PH_HP_SCL0	22	GND
23	PH_HP_SDA0	24	GND
25	PH_HP_SCL1	26	GND
27	PH_HP_SDA1	28	GND
15	P3V3_AUX	30	P3V3_AUX

14) SPI_TPM (Trusted Platform Module Connector)

Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

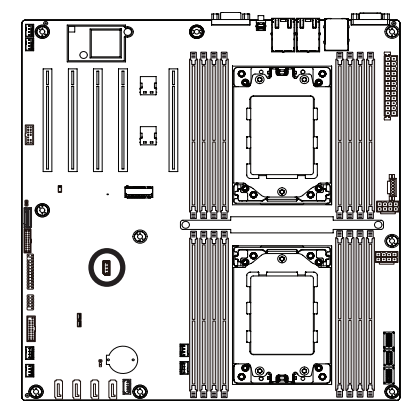




Pin No.	Definition	Pin No.	Definition
1	Clock	8	No Connect
2	P_3V3_AUX	9	LPC_LAD2
3	LPC_RST	10	No Pin
4	P3V3	11	LPC_LAD3
5	LPC_LAD0	12	GND
6	IRQ_SERIAL	13	LPC_FRAME_N
7	LPC_LAD1	14	GND

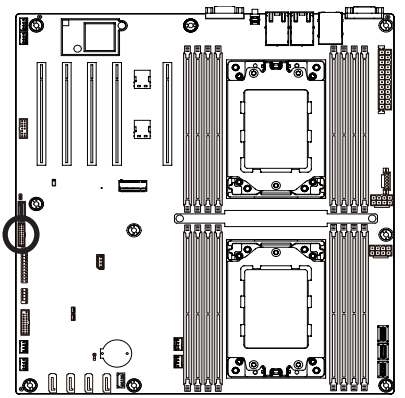
15) IPMB (Intelligent Platform Management Bus) Connector

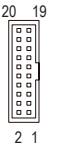
The Intelligent Platform Management Bus Communications Protocol defines a byte-level transport for transferring Intelligent Platform Management Interface Specification (IPMI) messages between intelligent I2C devices.



Pin No.	Definition
1	Clock
2	GND
3	Data
4	VCC

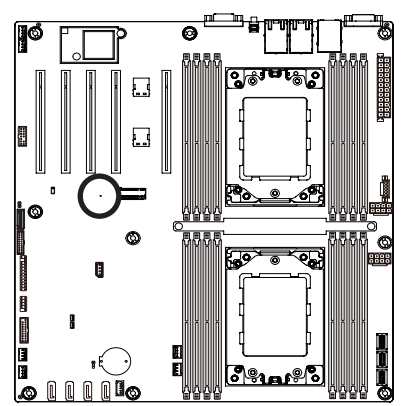
16) CN_NCSI (NCSI Connector)





Pin No.	Definition	Pin No.	Definition
1	NCSI_CLK	2	GND
3	NCSI_RX_D0	4	GND
5	NCSI_RX_D1	6	GND
7	NCSI_CRS_DV	8	GND
9	NCSI_RX_ER	10	GND
11	P3V3_AUX	12	GND
13	NCSI_TX_D1	14	GND
15	NCSI_TX_D0	16	GND
17	NCSI_TX_EN	18	GND
19	NCSI_PRESENT	20	P3V3_AUX

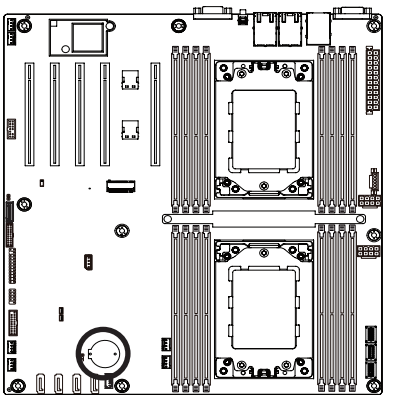
17) LED_BMC (BMC Firmware Readiness LED)

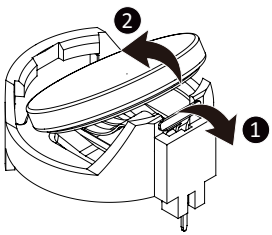


State	Description
On	BMC firmware is initial
Blink	BMC firmware is ready
Off	AC loss

18) BAT (Battery Socket)

The battery provides power to keep the values (such as BIOS configurations, date, and time information) in the CMOS when the computer is turned off. Replace the battery when the battery voltage drops to a low level, or the CMOS values may not be accurate or may be lost.

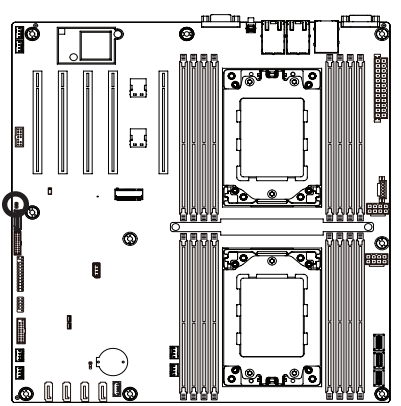




- Always turn off your computer and unplug the power cord before replacing the battery.
- Replace the battery with an equivalent one. Danger of explosion if the battery is replaced with an incorrect model.
- Contact the place of purchase or local dealer if you are not able to replace the battery by yourself or uncertain about the battery model.
- Used batteries must be handled in accordance with local environmental regulations.

19) CASE_OPEN (Case Open Intrusion Alert Header)

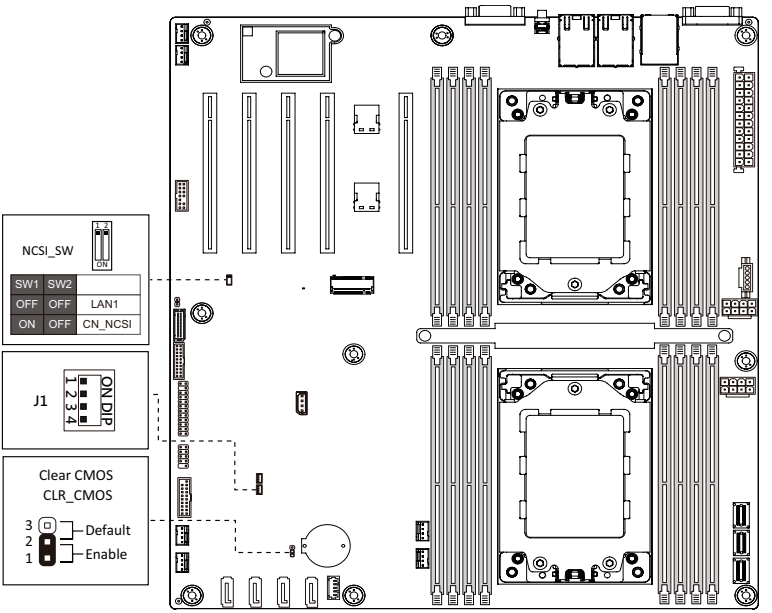
This motherboard provides a chassis detection feature that detects if the chassis cover has been removed. This function requires a chassis with chassis intrusion detection design.



Open: Normal Operation (Default)

Closed: Active Chassis Intrusion Alert

1-8 Jumper Settings



Jumper Name	Jumper Setting
Clear CMOS	1-2: Normal operation. (Default) 2-3: Clear CMOS data.

J1		ON	OFF
1	HSMB_SEL	BIOS Defined	
2	N/A	BIOS Defined	
3	BIOS PWD	Clear Supervisor Password	Normal [Default]
4	BIOS Recovery	BIOS Recovery Mode	Normal [Default]

Chapter 2 BIOS Setup

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

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

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

BIOS Setup Program Function Keys

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

- **Main**
  This setup page includes all the items of the standard compatible BIOS.
- **Advanced**
  This setup page includes all the items of AMI BIOS special enhanced features.
  (ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)
- **AMD CBS**
  This setup page includes the common items for configuration of AMD motherboard-related information.
- **AMD PBS Option**
  This setup page includes the common items for configuration of AMD CPM RAS related settings.
- **Chipset**
  This setup page includes all the submenu options for configuring the functions of the North Bridge.
- **Server Management**
  Server additional features enabled/disabled setup menus.
- **Security**
  Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.
  A supervisor password allows you to make changes in BIOS Setup.
  A user password only allows you to view the BIOS settings but not to make changes.
- **Boot**
  This setup page provides items for configuration of the boot sequence.
- **Save & Exit**
  Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)
  Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

2-1 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.

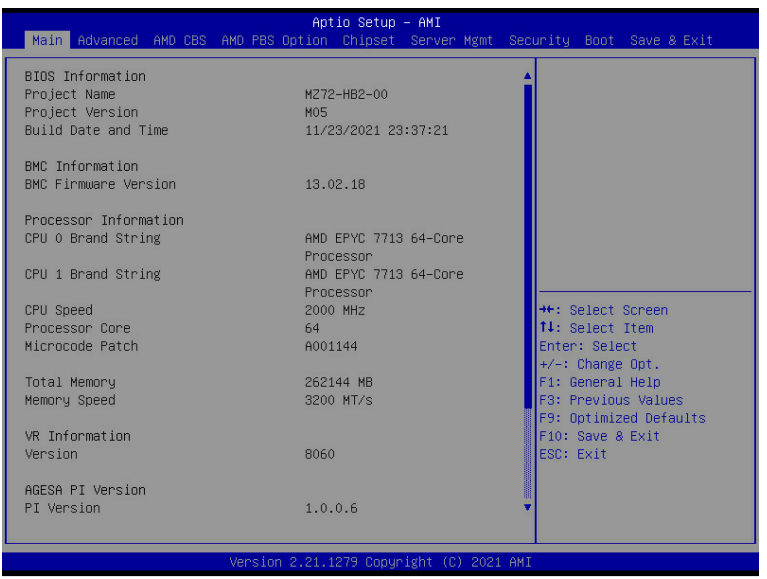
Main Menu Help

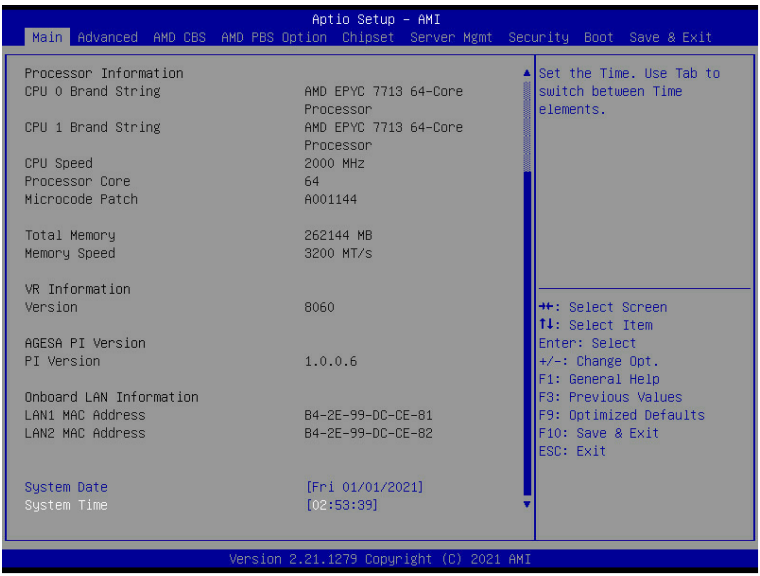
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

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.

(Note1) Functions available on selected models.

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

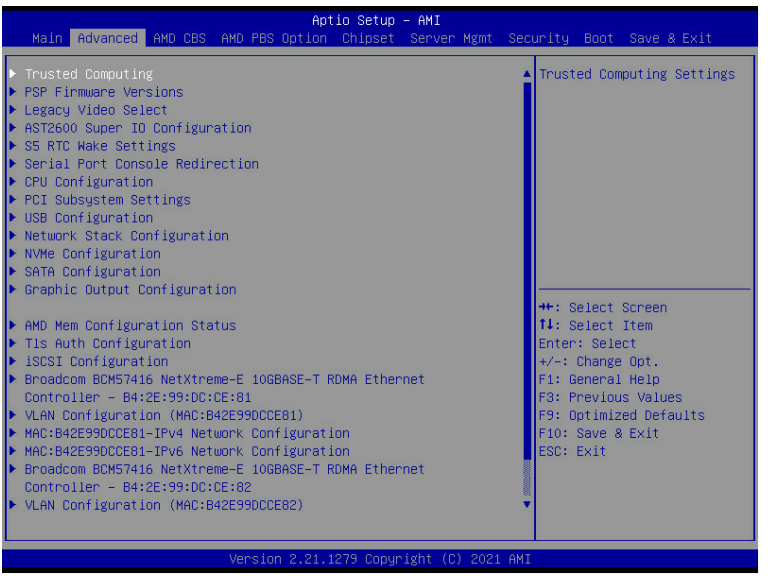
Parameter	Description
AGESA PI Version	
PI Version	Displays AGESA PI version information.
Onboard LAN Information	
LAN1 MAC Address(Note3)	Displays LAN MAC address information.
LAN2 MAC Address(Note3)	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

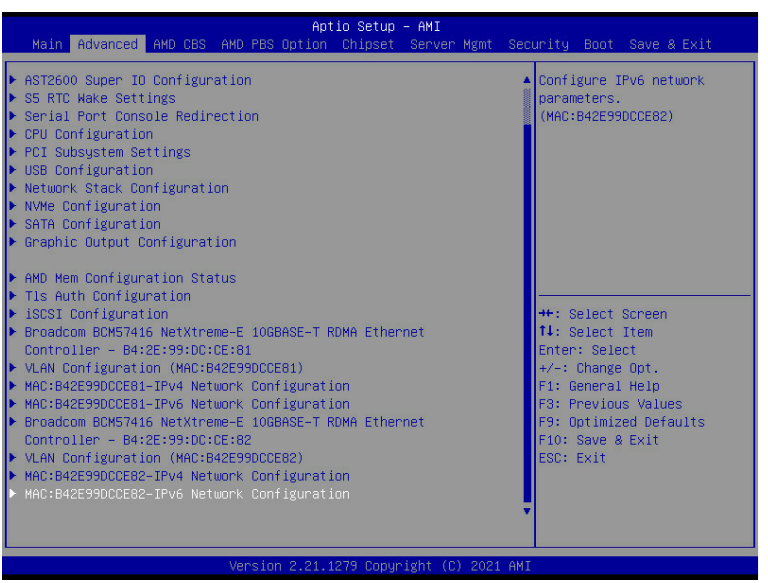
(Note3) The number of LAN ports listed will depend on the motherboard / system model.

2-2 Advanced Menu

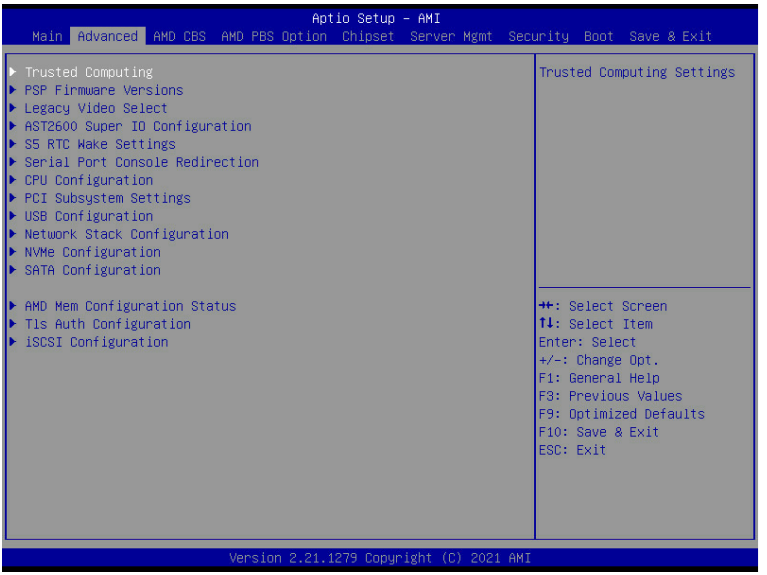
The Advanced Menu displays submenu options for configuring the function of various hardware components. Select a submenu item, then press <Enter> to access the related submenu screen.

When Boot Mode Select is set to UEFI (Default)

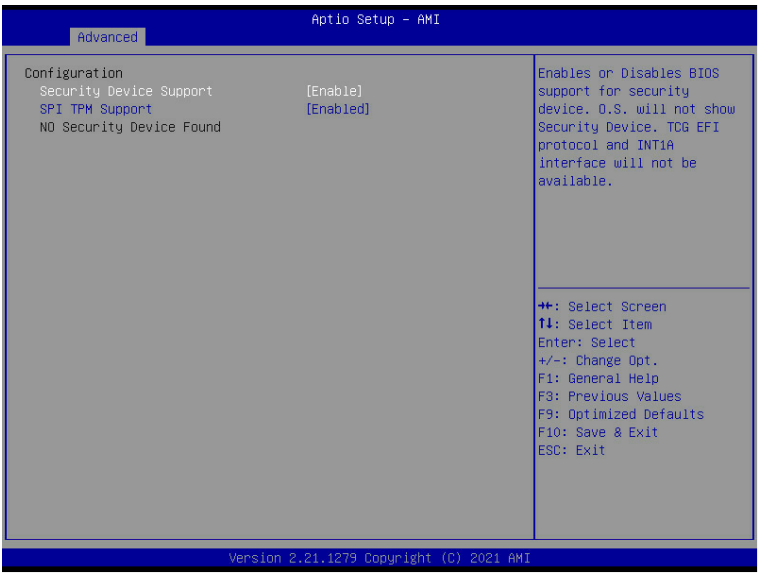




When "Boot Mode Select" is set to Legacy in the Boot > Boot Mode Select section



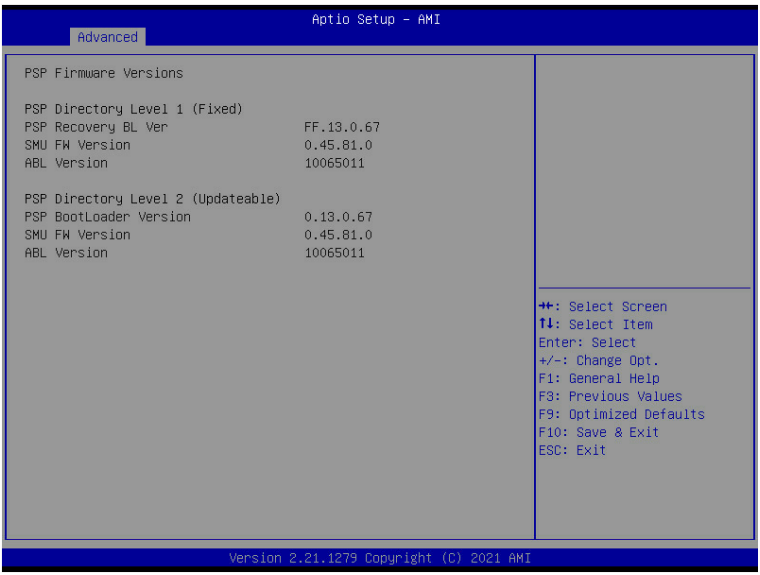
2-2-1 Trusted Computing



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

2-2-2 PSP Firmware Versions

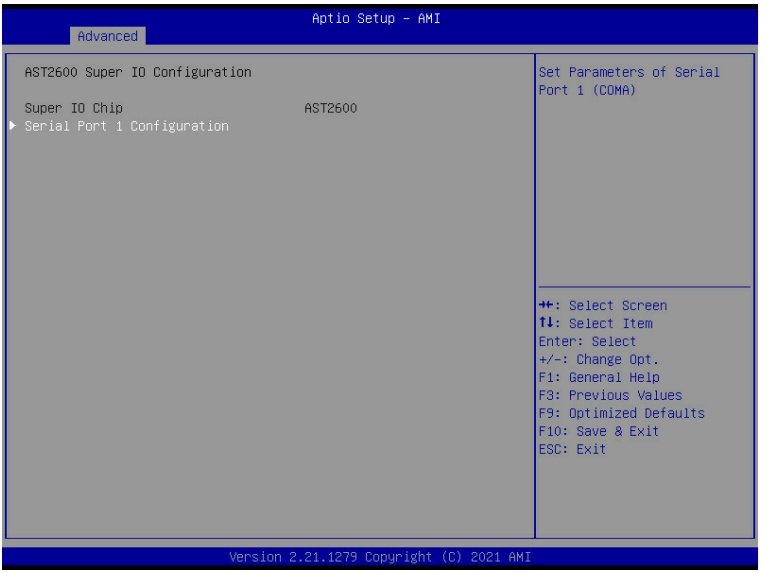
The PSP Firmware Versions page displays the basic PSP firmware version information. Items on this window are non-configurable.



2-2-3 Legacy Video Select

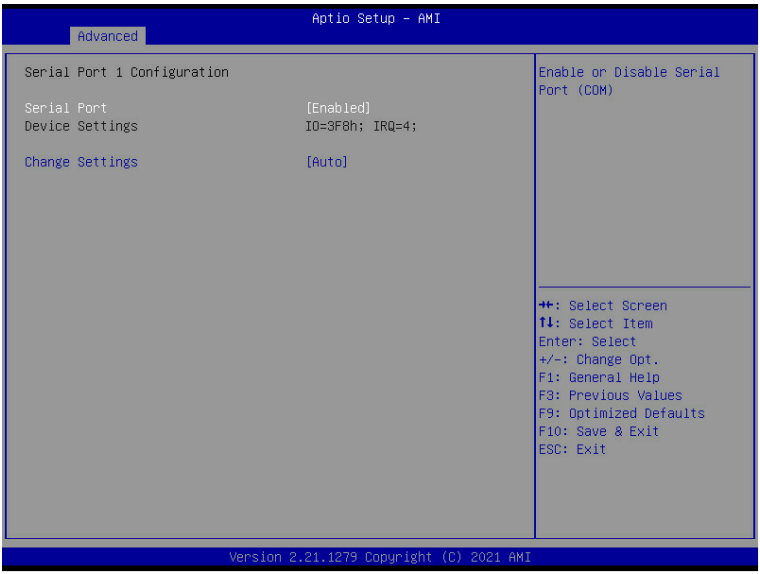
Parameter	Description
OnBrd/Ext VGA Select	Selects between onboard or external VGA support. Options available: Auto, Onboard, External. Default setting is **Onboard**.

2-2-4 AST2600 Super IO Configuration



Parameter	Description
AST2600 Super IO Configuration	
Super IO Chip	Displays the super IO chip information
Serial Port 1 Configuration	Press [Enter] for configuration of advanced items.

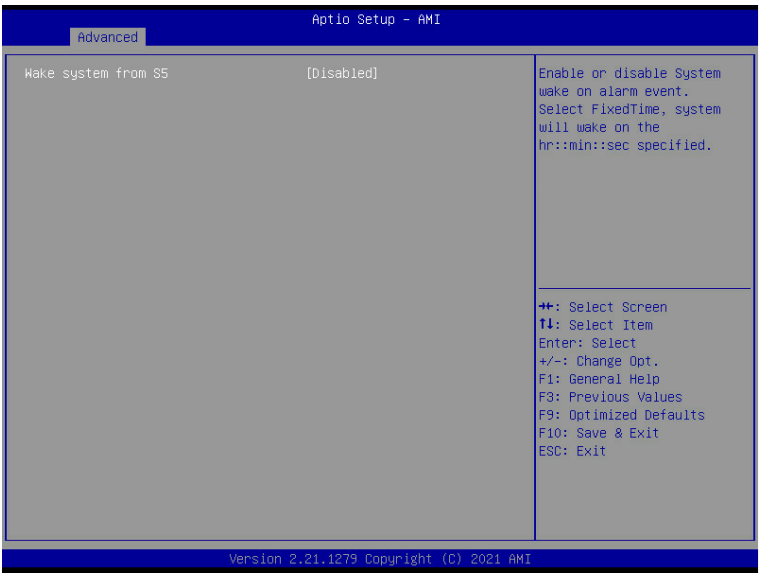
2-2-4-1 Serial Port 1 Configuration



Parameter	Description
Serial Port 1 Configuration	
Serial Port(Note1)	Enable/Disable the Serial Port (COM). When set to Enabled allows you to configure the Serial port 1 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 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**.

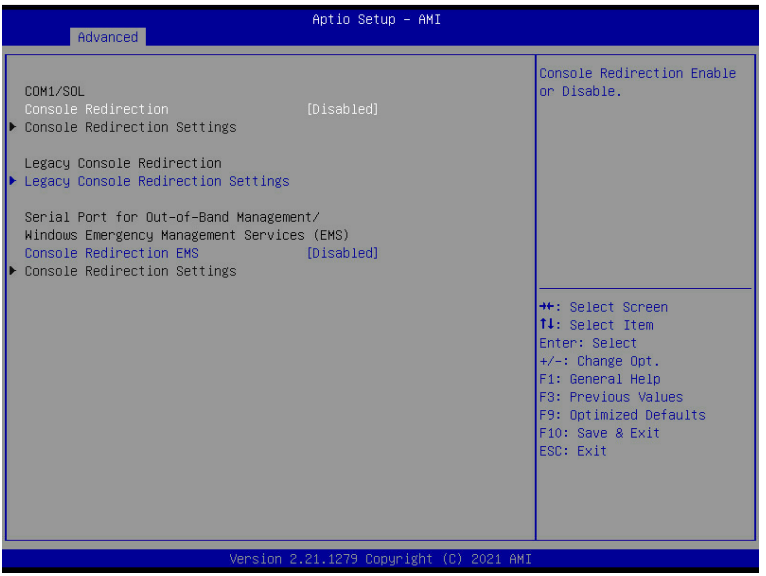
(Note1) Advanced items prompt when this item is defined.
(Note2) This item is configurable when **Serial Port** is set to **Enabled**.

2-2-5 S5 RTC Wake Settings



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

2-2-6 Serial Port Console Redirection



Parameter	Description
COM1/Serial Over LAN Console Redirection(Note)	Select whether to enable console redirection for specified device. Console redirection enables the users to manage the system from a remote location. Options available: Enabled, Disabled. Default setting is **Disabled**.
COM1/Serial Over LAN & Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when COM1/Serial Over LAN Console Redirection is set to Enabled.** ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is 115200. ◆ Data Bits – Selects the number of data bits used for console redirection. – Options available: 7, 8. Default setting is 8.

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

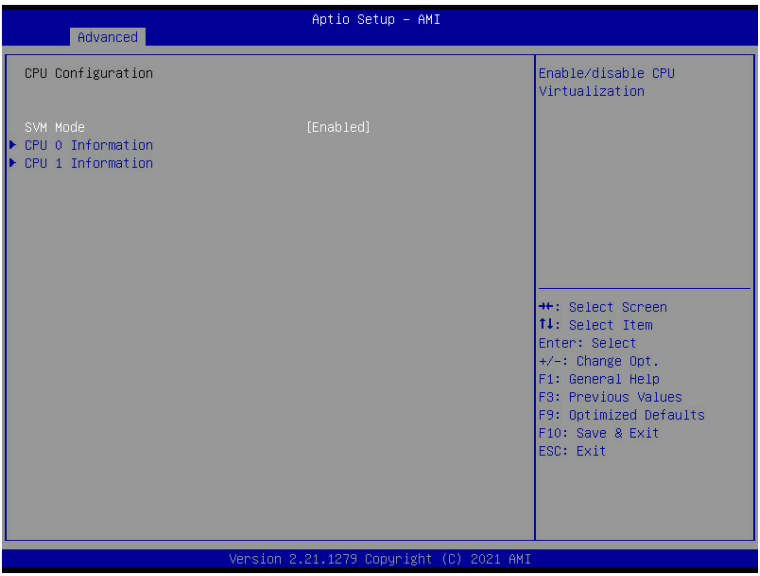
Parameter	Description
COM1/Serial Over LAN & Console Redirection Settings (continued)	◆ Parity – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: parity bit is 0 if num of 1's in the data bits is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

Parameter	Description
Legacy Console Redirection	
Legacy Console Redirection Settings	Press [Enter] to configure advanced items. ◆ Redirection COM Port – Selects a COM port for Legacy serial redirection. – Default setting is COM1/SOL. ◆ Resolution – Selects the number of rows and columns used in Console Redirection for legacy OS support. – Options available: 80x24, 80x25. Default setting is 80x24. ◆ Redirect After POST – When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. – Options available: Always Enable, BootLoader. Default setting is Always Enable.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection(Note)	EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management. Options available: Enabled, Disabled. Default setting is **Disabled**.
Serial Port for Out-of-Band EMS Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.** ◆ Out-of-Band Mgmt Port – Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Default setting is COM1/SOL. ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is ANSI. ◆ Bits per second – 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.

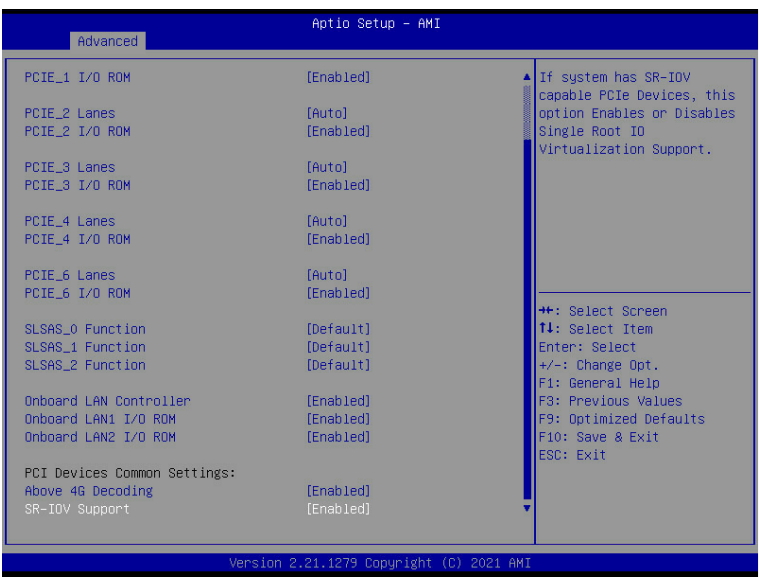
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	◆ Flow Control – Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty,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

2-2-7 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.

2-2-8 PCI Subsystem Settings



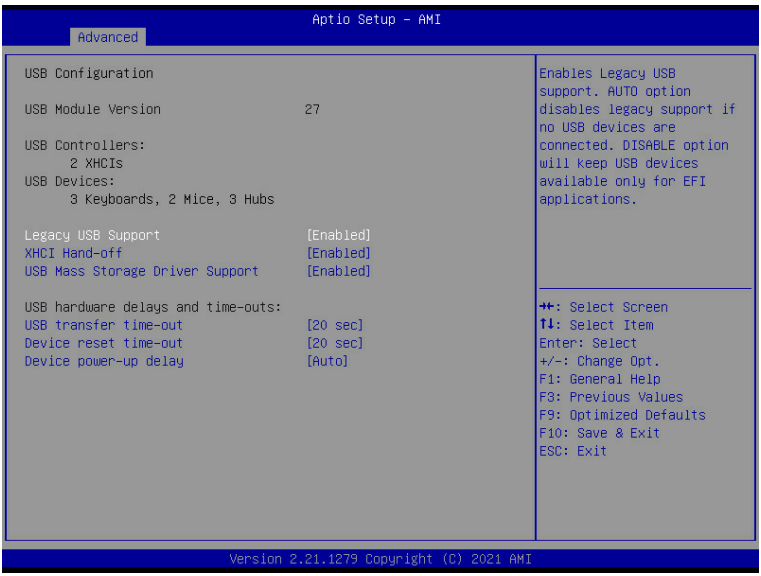
Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
PCIE_# Lanes (Note1)	Change the PCIe lanes. Options available: Disabled, Auto, x8, x4x4, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is **Auto**.
PCIE_ # I/O ROM(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is **Enabled**.
SLSAS_# Function(Note2)	Change Slimline SAS function to SATA/NVMe setting. Options available: Disabled, Default, SATA, PCIe x4. Default setting is **Default**. **Note: The setting [Default] is SATA, to use NVMe drives select [PCIe x4].**
Onboard LAN Controller(Note3)	Enable/Disable the onboard LAN devices. Options available: Enabled, Disabled. Default setting is **Enabled**.
Onboard LAN# I/O ROM(Note3)	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available: Enabled, Disabled. Default setting is **Enabled**.
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled, Disabled. Default setting is **Enabled**.
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is **Enabled**.

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

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

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

2-2-9 USB Configuration

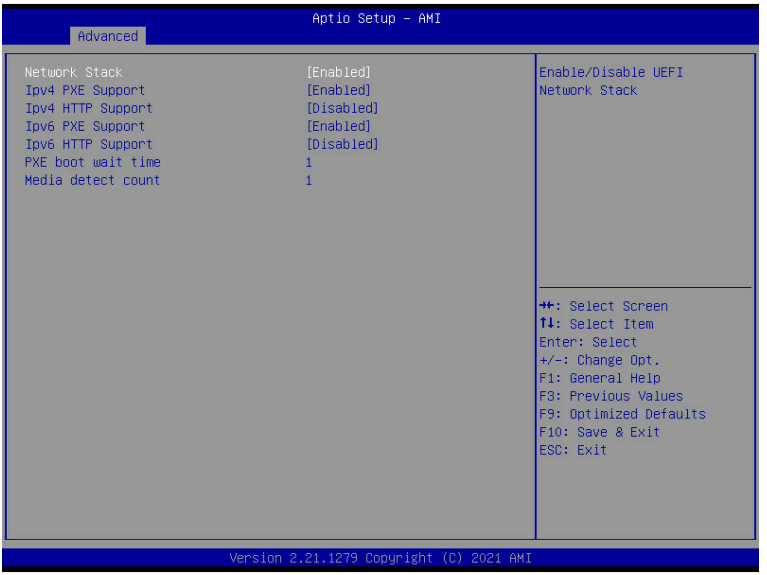


Parameter	Description
USB Configuration	
USB Module Version	Displays the USB module version information.
USB Controllers	Displays the supported USB controllers.
USB Devices:	Displays the USB devices connected to the system.
Legacy USB Support	Enable/Disable the Legacy USB support function. AUTO option 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**.

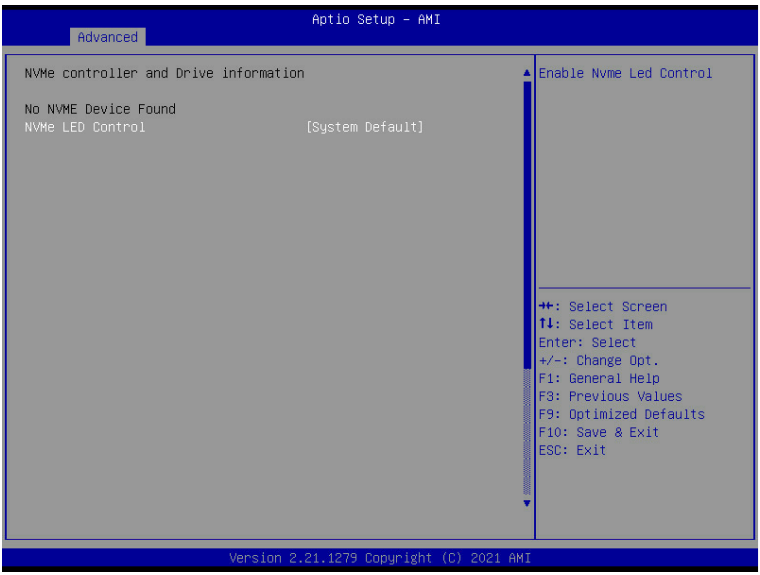
2-2-10 Network Stack Configuration



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.

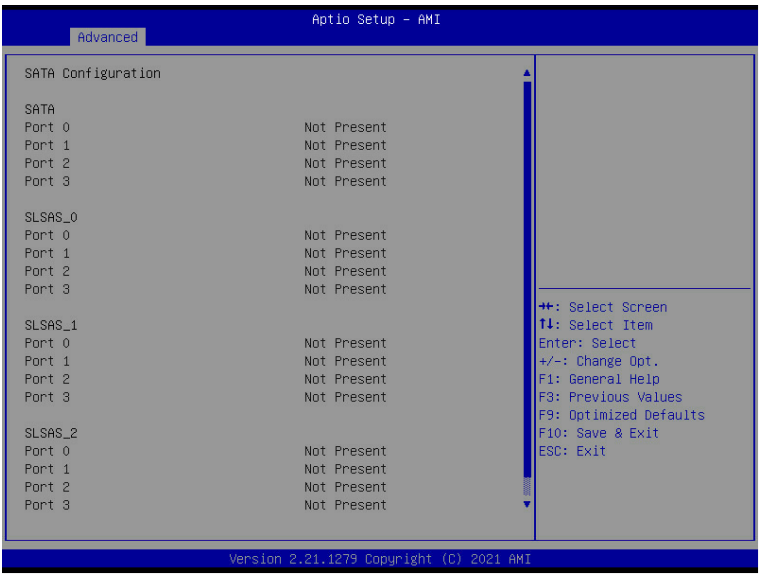
(Note) This item appears when **Network Stack** is set to **Enabled**.

2-2-11 NVMe Configuration



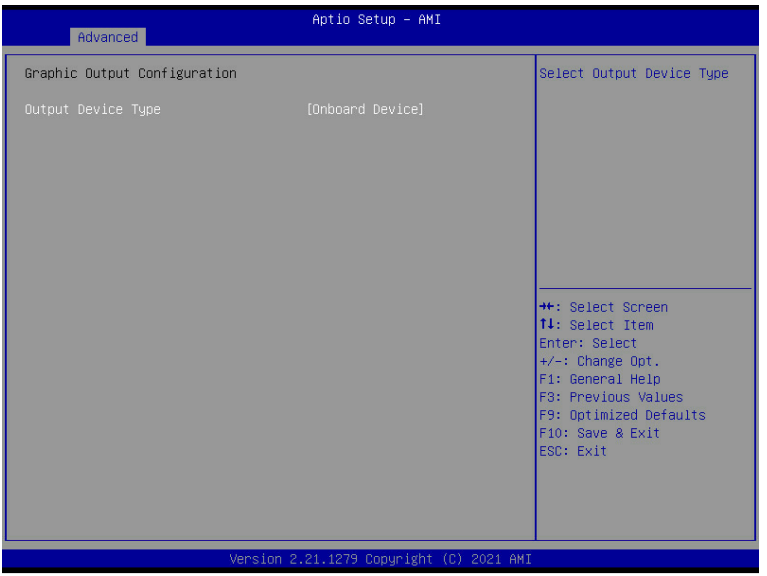
Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.
NVMe LED Control	Enable/Disable NVMe LED Control. Options available: System Default, Disabled, Enabled. Default setting is **System Default**.

2-2-12 SATA Configuration



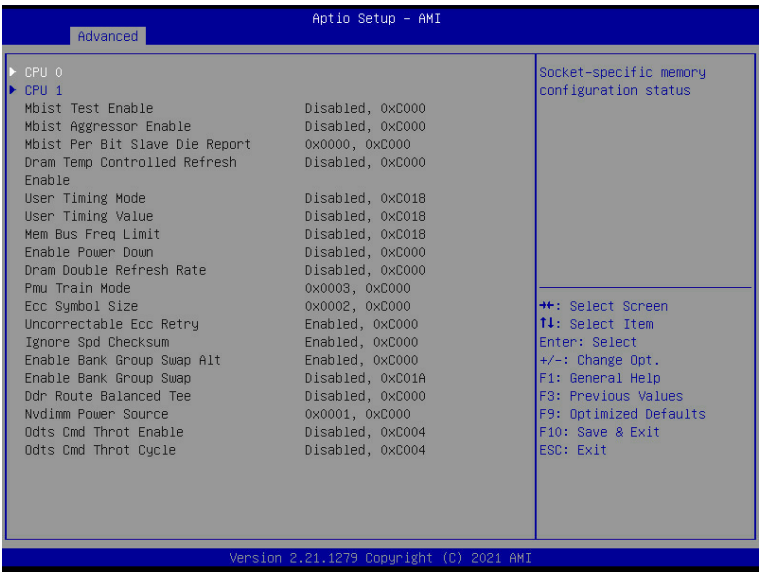
Parameter	Description
SATA Configuration	Displays the installed HDD devices information. System will automatically detect HDD type.

2-2-13 Graphic Output Configuration



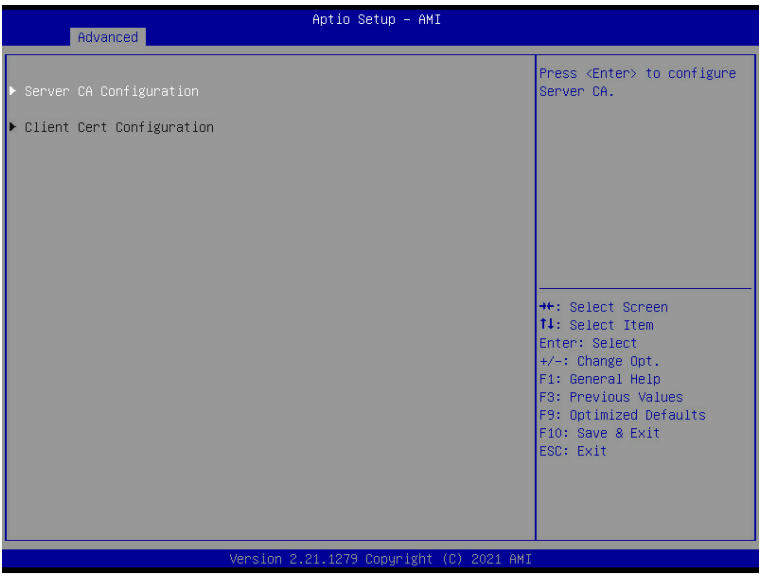
Parameter	Description
Output Device Type	Selects output device type. Options available: First loaded Device, Onboard Device, External Device, Specific Device. Default setting is **Onboard Device**.

2-2-14 AMD Mem Configuration Status



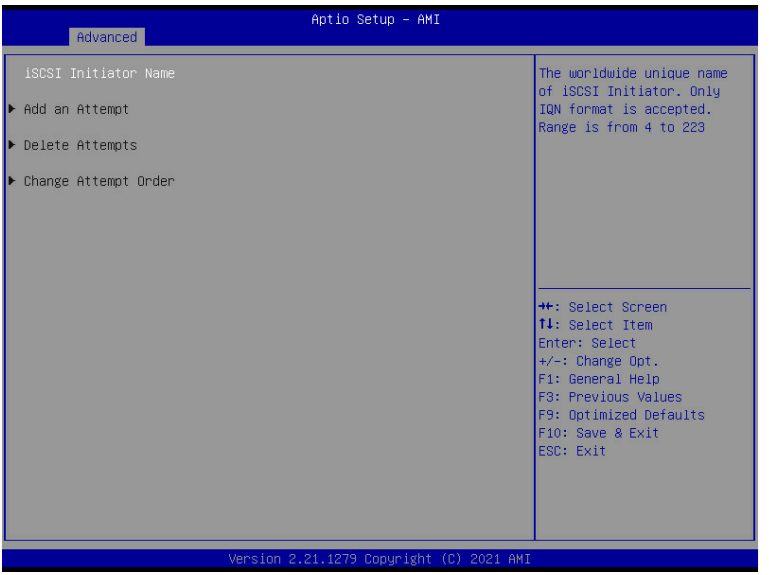
Parameter	Description
CPU0/1	Press [Enter] to view the memory configuration status related to CPU 0/1.

2-2-15 Tls Auth Configuration



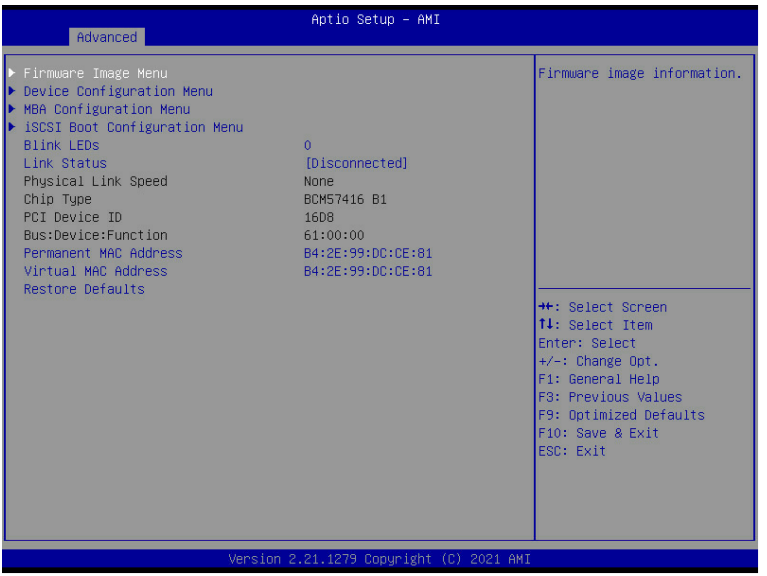
Parameter	Description
Server CA Configuration	Press [Enter] for configuration of advanced items. ◆ Enroll Cert – Press [Enter] to enroll a certificate • Enroll Cert Using File • Cert GUID Input digit character in 1111111-2222-3333-4444-1234567890ab format. – Commit Changes and Exit – Discard Changes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

2-2-16 iSCSI Configuration



Parameter	Description
iSCSI Initiator Name	
Add an Attempt	Press [Enter] to configure advanced items.
Delete Attempts	Press [Enter] to configure advanced items.
Change Attempt Order	Press [Enter] to configure advanced items.

2-2-17 Broadcom BCM57416 10GBASE-T Network Connection

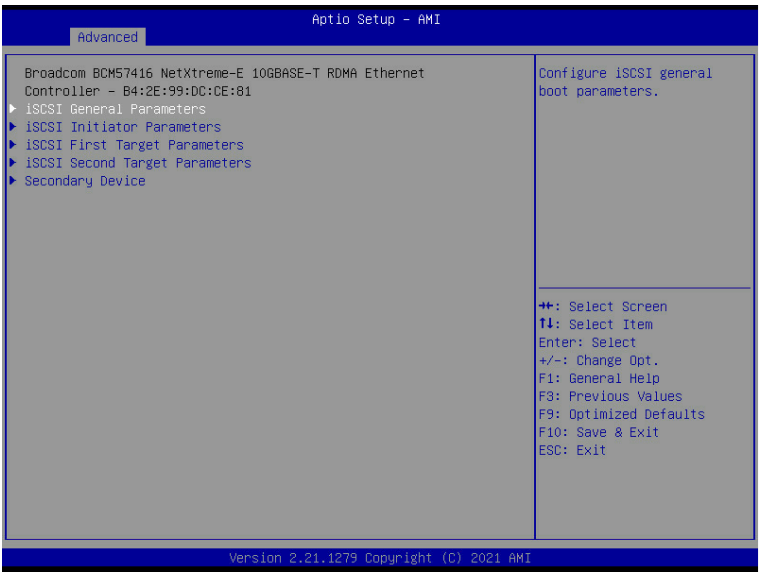


Parameter	Description
Firmware Image Menu	Press [Enter] to view firmware image information.
Device Configuration Menu	Press [Enter] to configure advanced items. ◆ Multi-Function Mode – Configures the NIC Hardware Mode. – Options available: SF, NPAR 1.0. Default setting is **SF**. ◆ Number of VFs Per PF – Configures the number of Virtual Functions Per Physical Function in multiples of 8 (1-128). This field is only applicable when SR-IOV is enabled. – Default setting is **8**. ◆ SR-IOV – Enable/Disable Single Root I/O Virtualization. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Number of MSI-X Vectors per VF – Configures the number of MSI-X Vectors per VF (0-128). – Default setting is **4**. ◆ Maximum Number of PF MSI-X Vectors – Configures the maximum number of PF MSI-X Vectors (0-512 per controller). – Default setting is **74**.

Parameter	Description
Device Configuration Menu (continued)	◆ Energy Efficient Ethernet – Enable/Disable Energy Efficient Ethernet operation. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Operational Link Speed – Configures the link speed setting to be used as the default link speed for the selected port. – Options available: AutoNeg. Default setting is **AutoNeg**. ◆ Support RDMA – Enable/Disable RDMA support for this port. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ DCB Protocol – Enable/Disable DCB protocol. – Options available: Disabled, Enabled (IEEE only), CEE (only), Both (IEEE preferred with fallback to CEE). Default setting is **Disabled**. ◆ LLDP nearest bridge – Enable/Disable LLDP nearest bridge state. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Default EVB Mode – Configures the default Edge Virtual Bridging mode. – Options available: VEB, VEPA, None. Default setting is **VEB**. ◆ Enable PME Capability – Enable/Disable PME Capability support. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Flow Offload – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Live Firmware Upgrade – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Adapter Error Recovery – Options available: Enabled, Disabled. Default setting is **Disabled**.
MBA Configuration Menu	Press [Enter] to configure advanced items. ◆ Option ROM – Enable/Disable Boot Option ROM. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ Legacy Boot Protocol – Selects non-UEFI Boot Protocol: Preboot Execution Environment (PXE)/iSCSI. – Options available: PXE, iSCSI, NONE. Default setting is **PXE**. ◆ Boot Strap Type – Selects the boot strap type. Options available: Auto Detect, BBS, Int 18h, Int 19h. Default setting is **Auto Detect**. ◆ Hide Setup Prompt – Configures whether the Setup Prompt is displayed during ROM initialization. – Options available: Enabled, Disabled. Default setting is **Disabled**.

Parameter	Description
MBA Configuration Menu (continued)	◆ Setup Key Stroke – Configures key strokes to invoke the configuration menu. – Options available: Ctrl-S, Ctrl-B. Default setting is **Ctrl-S**. ◆ Banner Message Timeout – Selects the timeout value. (0 defaults to 4 seconds, 15 is no delay, 1-14 is timeout value in seconds) – Default setting is **4**. ◆ Pre-boot Wake On LAN – Configures Pre-boot Wake on LAN (WOL). – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ VLAN Mode – Configures the virtual LAN (VLAN) mode. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ VLAN ID – Configures the VLAN ID (1…4094). – This item is available only when VLAN Mode is Enabled. ◆ Boot Retry Count – Selects the number of boot retries. – Options available: No Retry, 1 Retry, 2 Retries, 3 Retries, 4 Retries, 5 Retries, 6 Retries, Indefinite Retries. Default setting is **No Retry**.
iSCSI Boot Configuration Menu	Press [Enter] to configure advanced items.
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.
Link Status	Specifies the link status of the port.
Physical Link Speed	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
Bus:Device:Function	Displays the technical specifications for the Network Interface Controller.
Permanent MAC Address	Displays the MAC address of the Ethernet controller.
Virtual MAC Address	Displays the virtual MAC address of the Ethernet controller.
Restore Defaults	Resets the adapter to factory defaults.

2-2-17-1 iSCSI Boot Configuration Menu

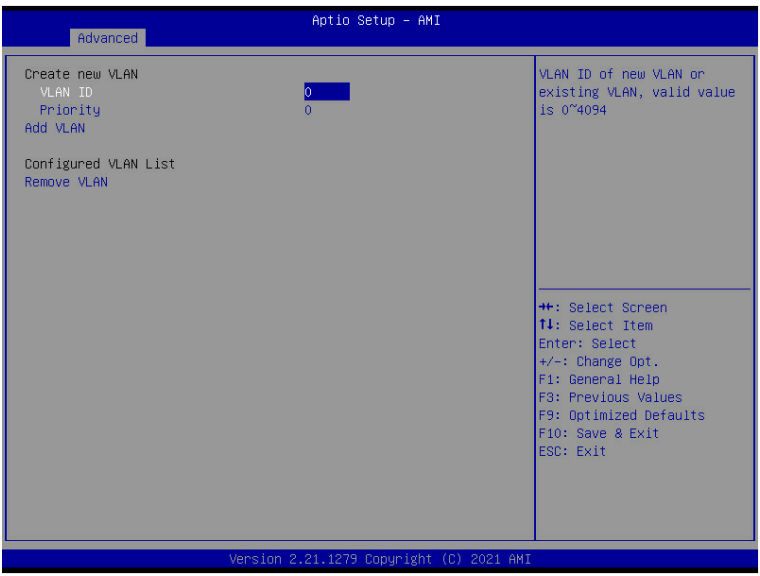


Parameter	Description
iSCSI General Parameters	Press [Enter] to configure advanced items. ◆ TCP/IP Parameters via DHCP – Acquires TCP/IP Parameters via DHCP. – Options available: Enabled, Disabled. Default setting is **Enabled**. ◆ IP Autoconfiguration – Auto-configures the IP configuration. – Options available: Enabled, Disabled. Default setting is **Enabled**. – This item is configurable when TCP/IP Parameters via DHCP is set to Disabled. ◆ iSCSI Parameters via DHCP – Acquires iSCSI Parameters via DHCP. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ CHAP Authentication – Enable/Disable the CHAP authentication. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Boot to iSCSI Target – Enable/Disable booting to iSCSI target after log-on. – Options available: Enabled, Disabled, One Time Disabled. Default setting is **Enabled**. ◆ DHCP Vendor ID – Configures the DHCP vendor ID (up to 32 characters long).

Parameter	Description
iSCSI General Parameters (continued)	◆ Link Up Delay Time – Configures the link up delay time in seconds (0-225). ◆ Use TCP Timestamp – Enable/Disable the TCP timestamp. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Target as First HDD – Enable/Disable target appears as first hard disk drive (HDD) in the system. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ LUN Busy Retry Count – Configures the number of retries in 2 second intervals when LUN is busy (0-60). – Default setting is **0**. ◆ IP Version – Displays the IP version supported. Modifying this parameter will reset all IP-related fields. – Options available: IPv4, IPv6. Disabled. Default setting is **IPv4**.
iSCSI Initiator Parameters	Press [Enter] to configure advanced items. ◆ IP Address – Configures the initiator IP address. ◆ Subnet Mask – Configures the IP subnet mask. ◆ Default Gateway – Configures the default gateway IP address. ◆ Primary DNS – Configures the primary DNS IP address. ◆ Secondary DNS – Configures the secondary DNS IP address. ◆ iSCSI Name – Configures the iSCSI name. ◆ CHAP ID – Configures the Challenge-Handshake Authentication Protocol (CHAP) ID (up to 128 characters in length). ◆ CHAP Secret – Configure the Challenge-Handshake Authentication Protocol (CHAP) Secret (12 to 16 characters in length).
iSCSI First/Second Target Parameters	Press [Enter] to configure advanced items. ◆ Connect – Enable/Disable the target establishment. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ IP Address – Configures the Target IP address. ◆ TCP Port – Configures the Target TCP port number (1-65535).

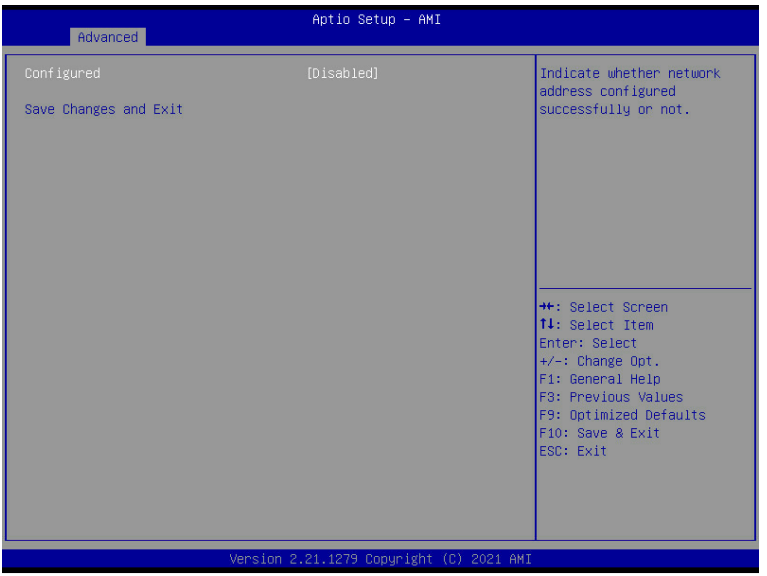
Parameter	Description
iSCSI First/Second Target Parameters (continued)	◆ Boot LUN – Configures the Target boot LUN number (0-255). ◆ iSCSI Name – Configures the iSCSI name. ◆ CHAP ID – Configures the Challenge-Handshake Authentication Protocol (CHAP) ID (up to 128 characters in length). ◆ CHAP Secret – Configure the Challenge-Handshake Authentication Protocol (CHAP) Secret (12 to 16 characters in length).
Secondary Device	Press [Enter] to configure advanced items. ◆ Secondary Device – Inputs the secondary device MAC address. ◆ Use Independent Target Portal – Use Independent target portal when multipath I/O is enabled. – Options available: Enabled, Disabled. Default setting is **Disabled**. ◆ Use Independent Target Name – Use Independent target name when multipath I/O is enabled. – Options available: Enabled, Disabled. Default setting is **Disabled**.

2-2-18 VLAN Configuration



Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Create new VLAN ◆ VLAN ID – Sets VLAN ID for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the desired values. – The valid range is from 0 to 4094. ◆ Priority – Sets 802.1Q Priority for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the desired values. – The valid range is from 0 to 7. ◆ Add VLAN – Press [Enter] to create a new VLAN or update an existing VLAN. ◆ Configured VLAN List ◆ Remove VLAN – Press [Enter] to remove an existing VLAN.

2-2-19 MAC IPv4 Network Configuration



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

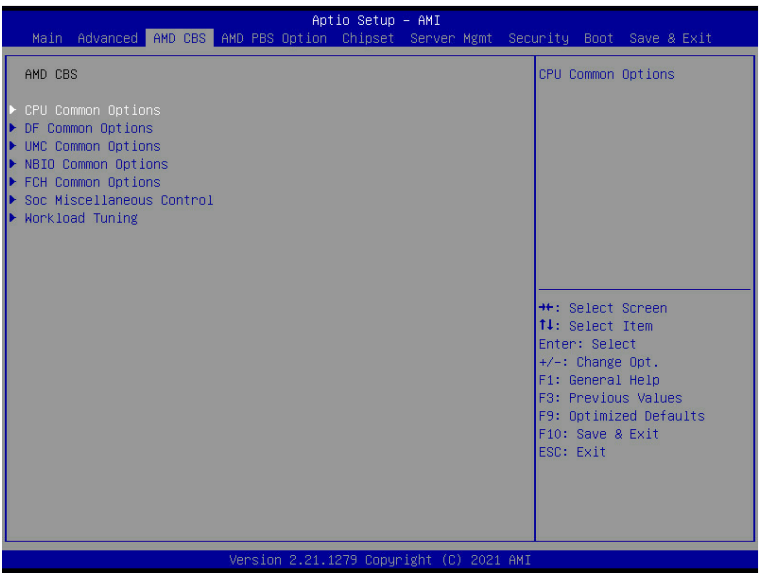
(Note) This item appears when **Configured** is set to **Enabled**.

2-2-20 MAC IPv6 Network Configuration

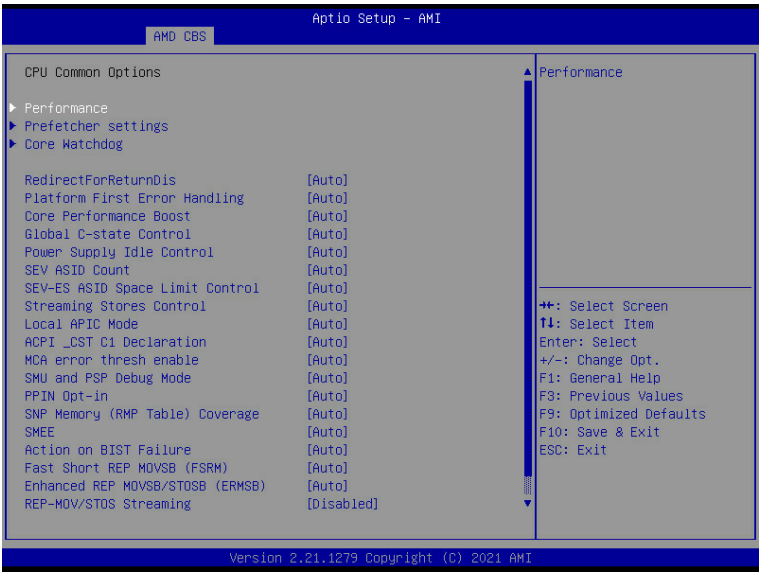
Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Displays the MAC Address information. ◆ Interface ID – The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3. ◆ DAD Transmit Count – The number of consecutive Neighbor solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed. ◆ Policy – Options available: automatic, manual. Default setting is automatic. ◆ Save Changes and Exit – Press [Enter] to save all configurations.

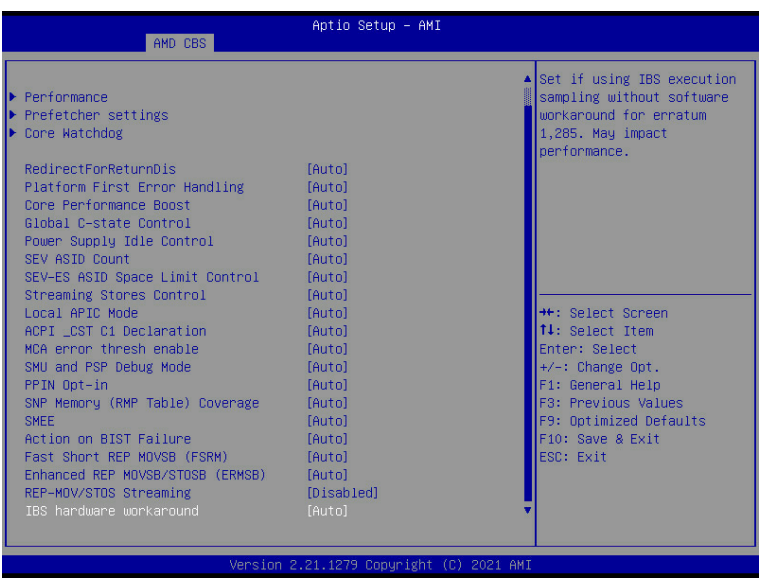
2-3 AMD CBS Menu

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.



2-3-1 CPU Common Options

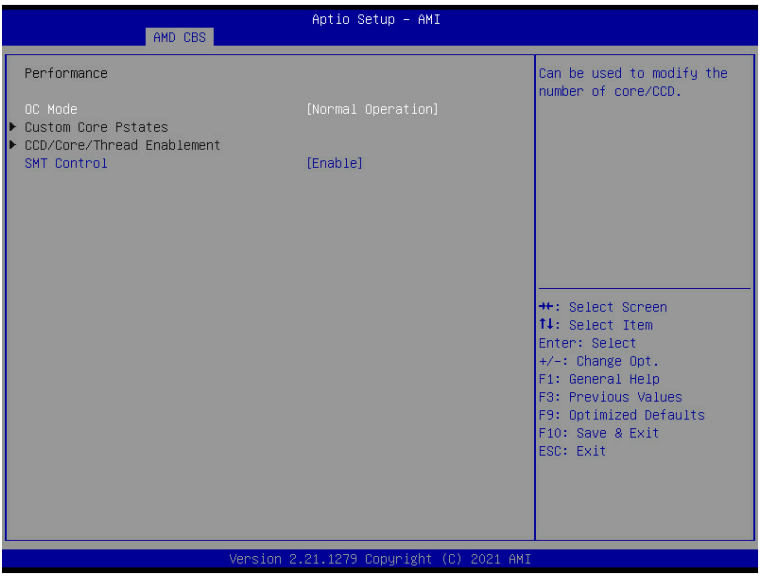




Parameter	Description
CPU Common Options	
Performance	Press [Enter] for configuration of advanced items.
Prefetcher settings	Press [Enter] for configuration of advanced items.
Core Watchdog	Press [Enter] for configuration of advanced items.
RedirectForReturnDis	From a workaround for GCC/C000005 issue 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**.
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**.
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**.

Parameter	Description
Fast short REP MOVSB (FSRM)	Default is 1, cab be set to zero for analysis purpose as long as OS supports it. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
Enhanced REP MOVSB/ STOSB (ERMSB)	Default is 1, cab be set to zero for analysis purpose as long as OS supports it. Options available: Disabled, Enabled, Auto. Default setting is **Auto**.
REP-MOV/STOS Streaming	Allows REP-MOVS/STOS to use non-caching streaming stores for large sizes. Options available: Disabled, Enabled. Default setting is **Disabled**.
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**.

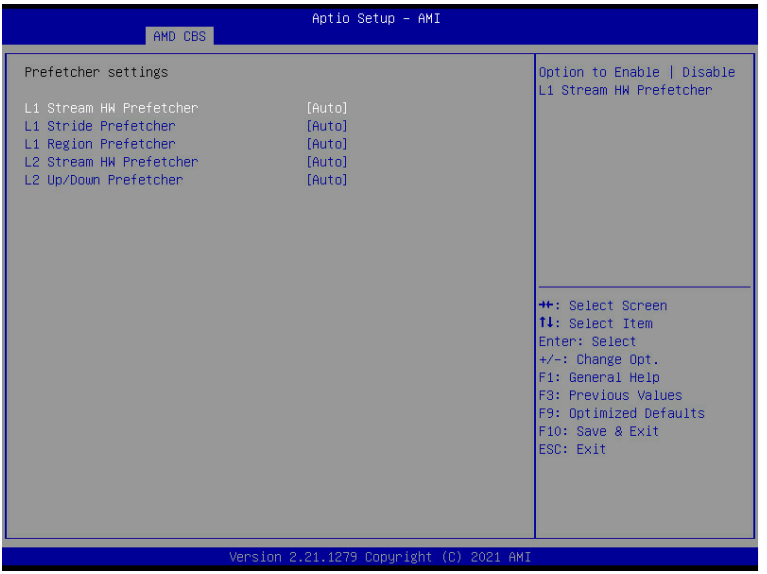
2-3-1-1 Performance



Parameter	Description
Performance	
OC Mode(Note)	Options available: Normal Operation, Customized. Default setting is **Normal Operation**.
Custom Core Pstates	Allows you to accept or decline enabling Custom Core Pstates. When accepted, you can disable or customize core pstates.
CCD/Core/Thread Enablement	Allows you to accept or decline enabling CCDs, processor cores and threads. When accepted, you can control the number of CCDs to be used, and the number of cores to be used. ◆ CCD Control – Options available: Auto, 2 CCDs, 3 CCDs, 4 CCDs, 6 CCDs. Default setting is **Auto**. ◆ Core Control – Options available: Auto, ONE(1+0), TWO(2+0), THREE(3+0), FOUR(4+0), FIVE(5+0), SIX(6+0), SEVEN(7+0). – Default setting is **Auto**.
SMT Control	Can be used to disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after select the 'Enable' option. Select 'Auto' base on BIOS PCD. (PcdAmdSmtMode) default setting. Options available: Disable, Enable, Auto. Default setting is **Enable**.

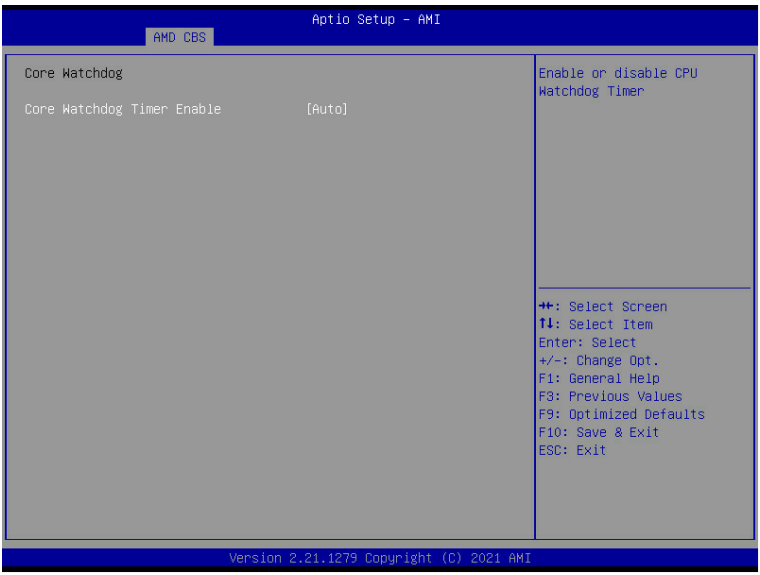
(Note) Advanced items are configurable when this item is defined.

2-3-1-2 Prefetcher Settings



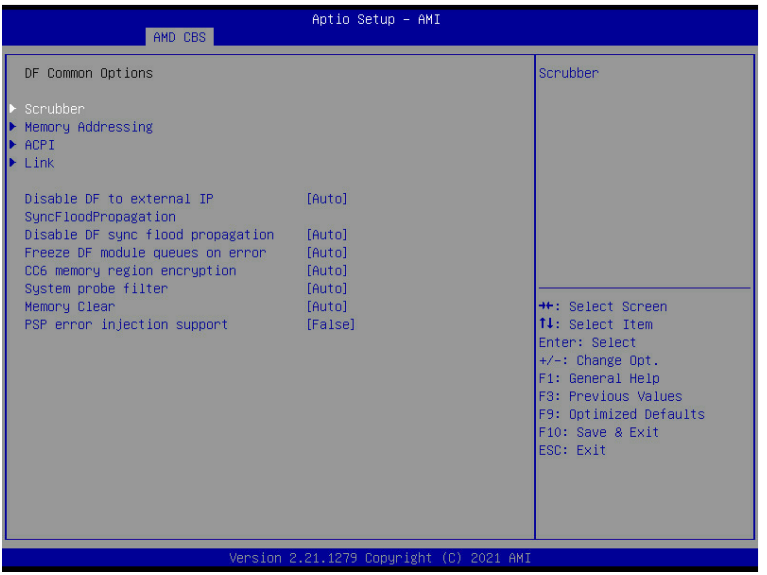
Parameter	Description
Prefetcher settings	
L1 Stream HW Prefetcher	Enable/Disable L1 Stream HW Prefetcher. Options available: Auto, Enable, Disable. Default setting is **Auto**.
L1 Stride Prefetcher	Use memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous. Enable/Disable L1 Stride Prefetcher. Options available: 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 **Auto**.
L2 Up/Down Prefetcher	Use memory access history to determine whether to fetch the next or previous line for all memory accesses. Enable/Disable L2 Up/Down Prefetcher. Options available: Auto, Enable, Disable. Default setting is **Auto**.

2-3-1-3 Core Watchdog



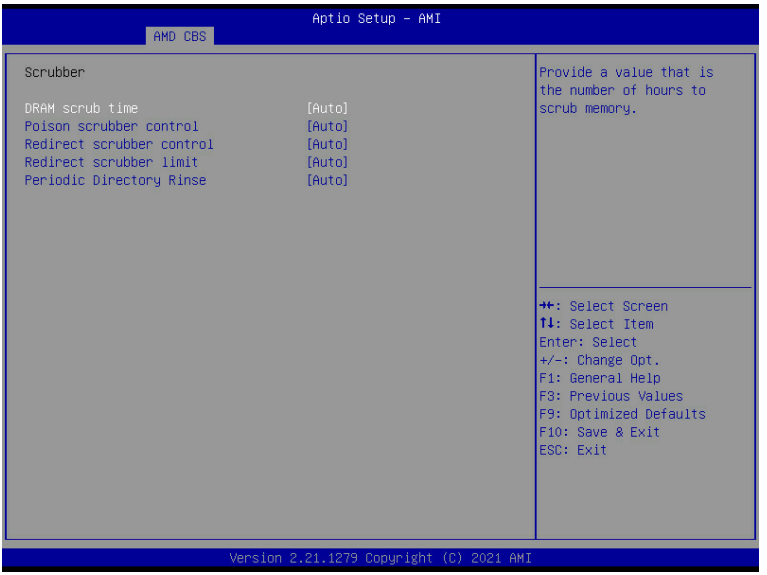
Parameter	Description
Core Watchdog	
Core Watchdog Timer Enable	Enable/Disable CPU Watchdog Timer. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

2-3-2 DF Common Options



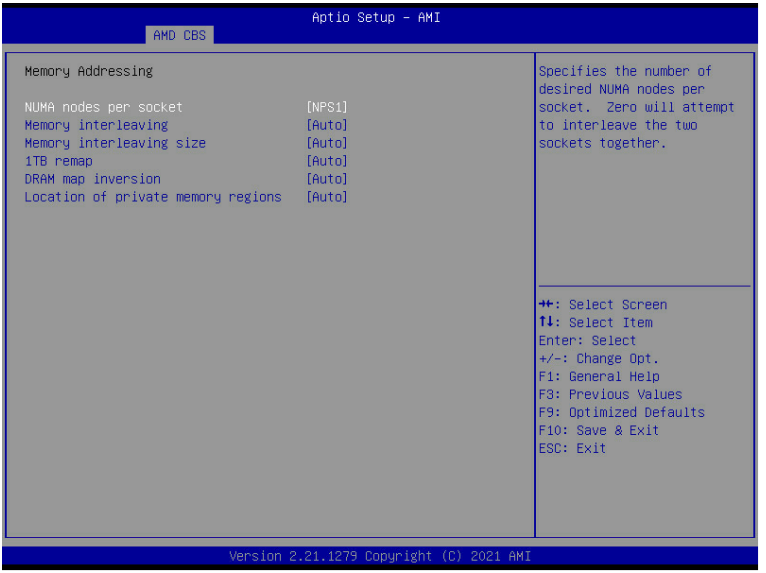
Parameter	Description
DF Common Options	
Scrubber	Press [Enter] for configuration of advanced items.
Memory Addressing	Press [Enter] for configuration of advanced items.
ACPI	Press [Enter] for configuration of advanced items.
Link	Press [Enter] for configuration of advanced items.
Disable DF to external 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**.

2-3-2-1 Scrubber



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

2-3-2-2 Memory Addressing

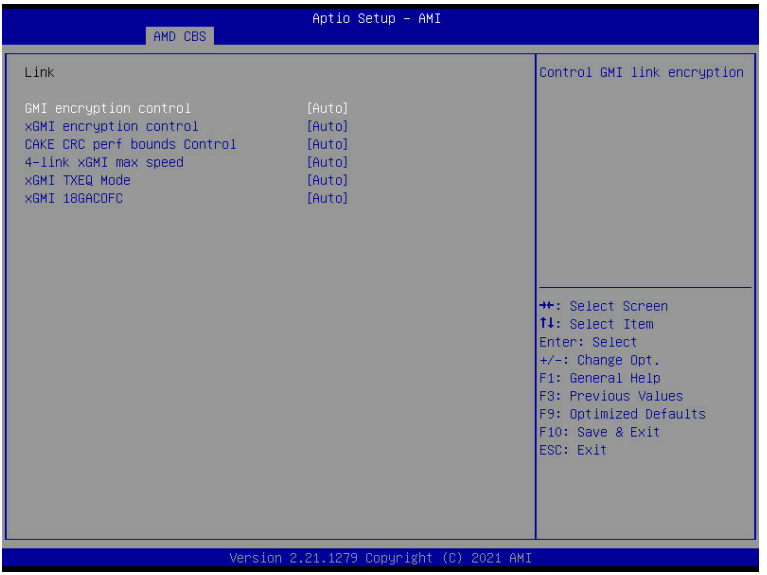


Parameter	Description
Memory Addressing	
NUMA nodes per socket	Specifies the number of desired NUMA nodes per socket. Options available: Auto, NPS0, NPS1, NPS2, NPS4. Default setting is **NPS1**.
Memory interleaving	Enable/Disable the Memory interleaving feature. Options available: Auto, Disabled. Default 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**.

2-3-2-3 ACPI

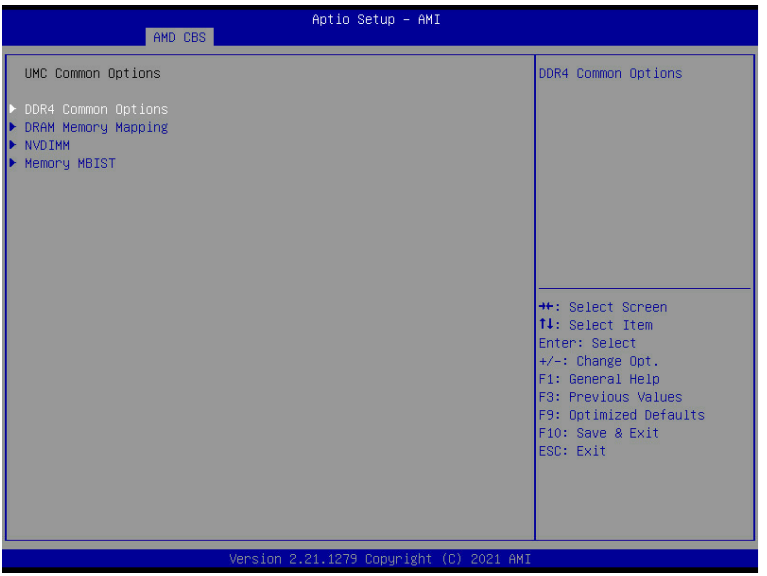
Parameter	Description
ACPI	
ACPI SRAT L3 Cache As NUMA Domain	Enable/Disable report each L3 cache as a NUMA Domain to the OS. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
ACPI SLIT Distance Control	Determines how the SLIT distances are declared. Options available: Auto, Manual.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

2-3-2-4 Link



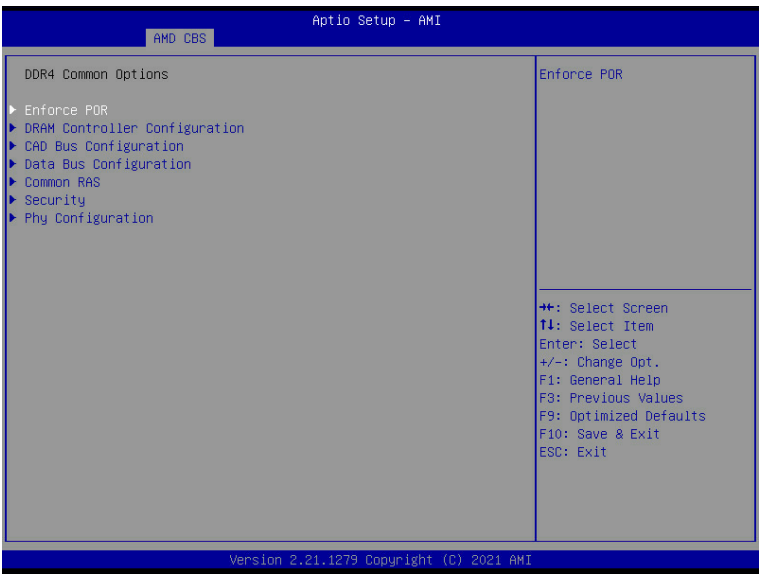
Parameter	Description
Link	
GMI encryption control	Enable/Disable GMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
xGMI encryption control	Enable/Disable xGMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
CAKE CRC perf bounds Control	Options available: Auto, Manual. Default setting is **Auto**.
4-link xGMI max speed	Specifies the max speed of 4-link xGMI. Default setting is **Auto**.
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**.

2-3-3 UMC Common Options



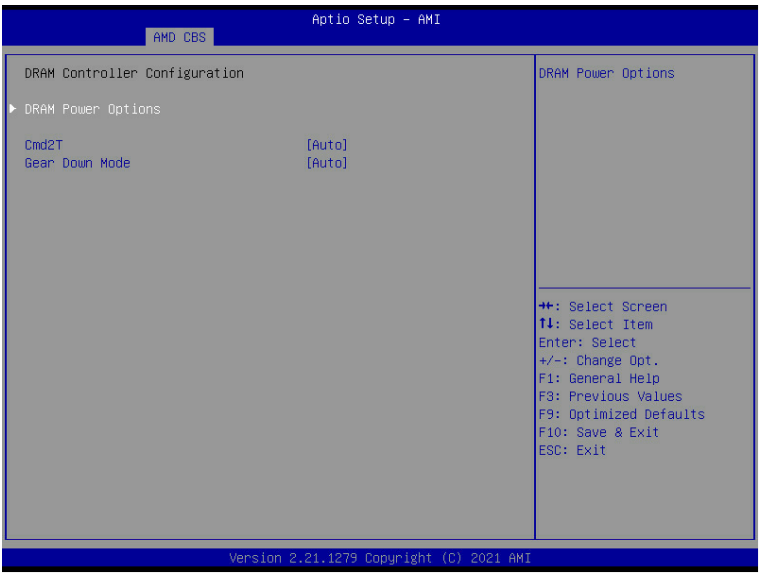
Parameter	Description
UMC Common Options	
DDR4 Common Options	Press [Enter] for configuration of advanced items.
DRAM Memory Mapping	Press [Enter] for configuration of advanced items.
NVDIMM	Press [Enter] for configuration of advanced items.
Memory MBIST	Press [Enter] for configuration of advanced items.

2-3-3-1 DDR4 Common Options



Parameter	Description
DDR4 Common Options	
Enforce POR	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. ◆ Decline ◆ Accept – Overclock » Enable/Disable Memory Overclock Settings » Options available: Auto, Enabled. Default setting is **Auto.** **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.**
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.

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

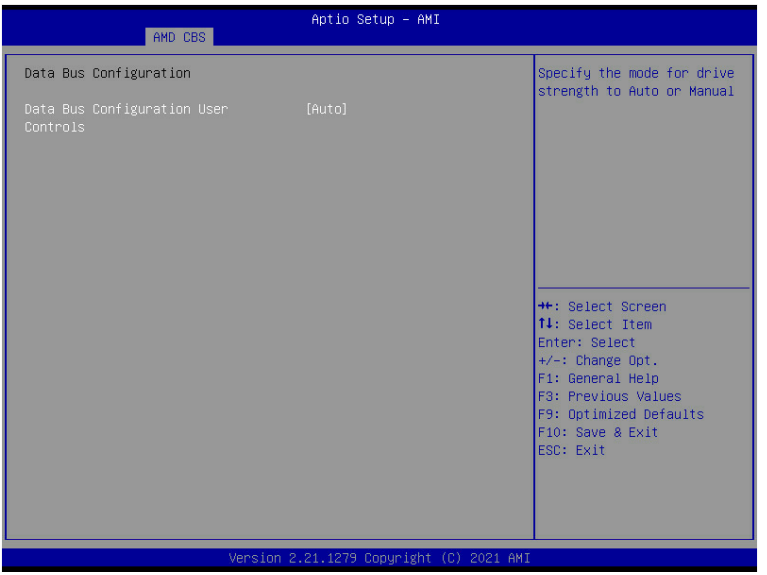


Parameter	Description
DRAM Controller Configuration	
DRAM Power Options	Press [Enter] to configure DRAM Power Options. ◆ Power Down Enable – Enable/Disable DDR power down mode. – Options available: Auto, Enabled, Disabled. Default setting is **Auto**. ◆ Power Down Entry Delay – Specifies the value. ◆ SubUrgRefLowerBound – Specifies the value. Valid value: 6~1. ◆ UrgRefLimit – Specifies the value. Valid value: 6~1. ◆ DRAM Maximum Activate Count – Options available: Untested MAC, 700K, 600K, 500K, 400K, 300K, 200K, Unlimited MAC, Auto. Default setting is **Auto**. ◆ DRAM Refresh Rate – Options available: 7.8 usec, 3.9 usec. Default setting is **Auto**. ◆ Self-Refresh Exit Staggering – Options available: Disabled, Trfc/3, Trfc/4. Default setting is **Disabled**.
Cmd2T	Selects the Cmd2T mode on ADDR/CMD. Options available: Auto, 1T, 2T. Default setting is **Auto**.
Gear Down Mode	Enable/Disable the Gear Down Mode function. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

2-3-3-1-2 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**.

2-3-3-1-3 Data Bus Configuration



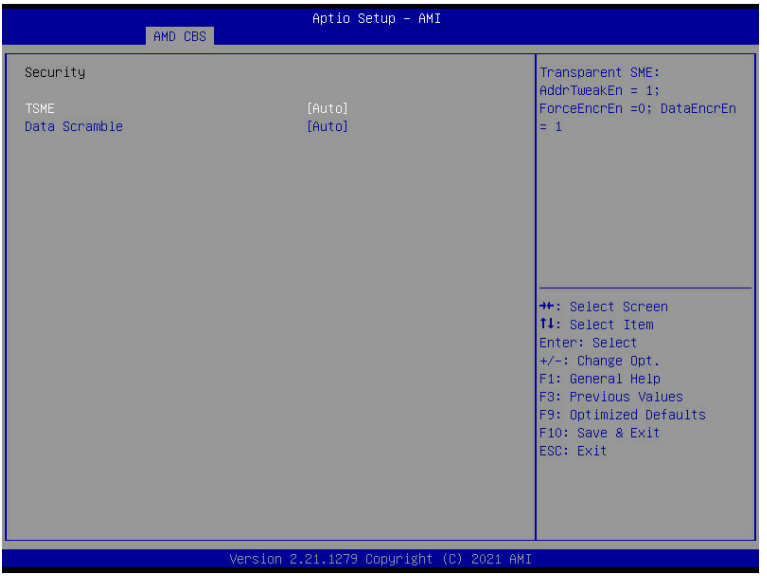
Parameter	Description
Data Bus Configuration	
Data Bus Configuration User Controls	Specifies the mode for drive strength to Auto or Manual. Options available: Auto, Manual. Default setting is **Auto**.

2-3-3-1-4 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	Press [Enter] to configure advanced items. ◆ DRAM ECC Symbol Size – Configures the DRAM ECC Symbol Size. – Options available: Auto, x4, x8, x16. Default setting is **Auto**. ◆ DRAM ECC Enable – Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable. – Options available: Auto, Enabled, Disabled. Default setting is **Auto**. ◆ DRAM UECC Retry – Enable/Disable DRAM UECC Retry. – Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

2-3-3-1-5 Security

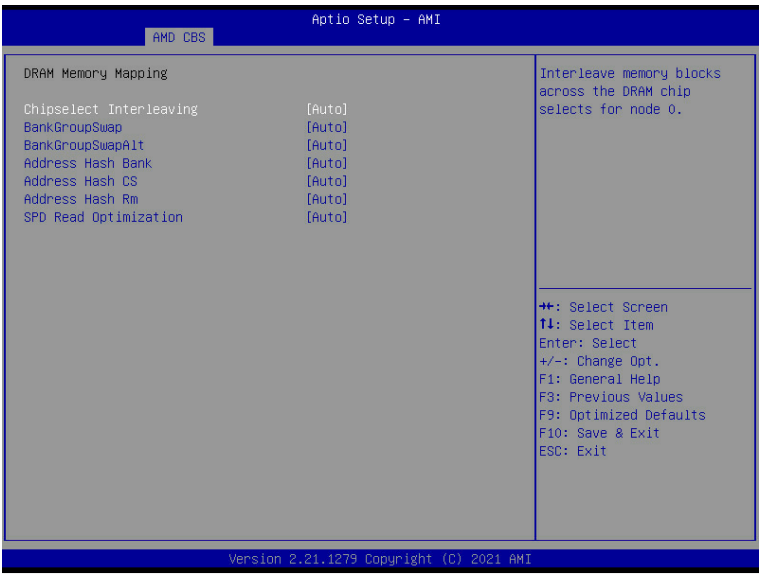


Parameter	Description
Security	
TSME	Enable/Disable transparent secure memory encryption. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Data Scramble	Enable/Disable Data Scrambling. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.

2-3-3-1-6 Phy Configuration

Parameter	Description
Phy Configuration	
PMU Training	Press [Enter] to configure PMU Training. ◆ DFE Read Training – Perform 2D Read Training with DFE on. – Options available: Auto, Enable, Disable. Default setting is **Auto**. ◆ FFE Write Training – Perform 2D Write Training with FFE on. – Options available: Auto, Enable, Disable. Default setting is **Auto**. ◆ PMU Pattern Bits Controls – Options available: Auto, Manual. Default setting is **Auto**.

2-3-3-2 DRAM Memory Mapping

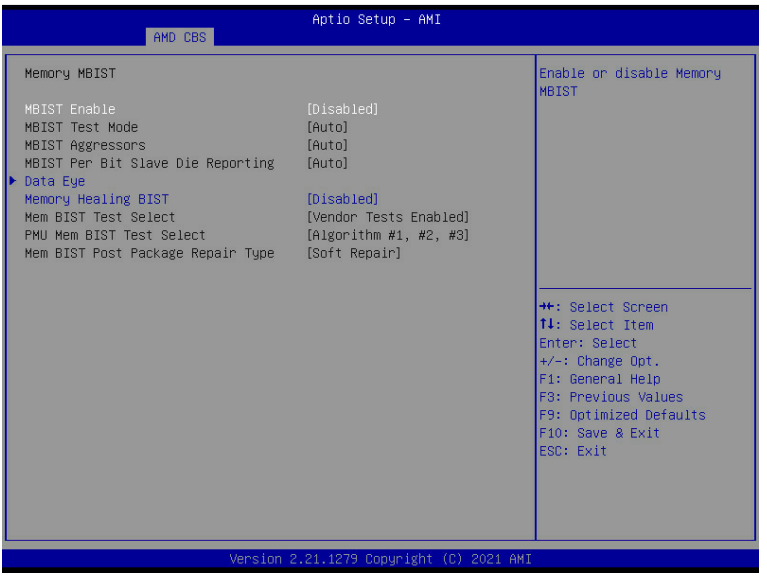


Parameter	Description
DRAM Memory Mapping	
Chipselect Interleaving	Interleave memory blocks across the DRAM chip selects for node 0. Options available: Auto, Disabled. Default setting is **Auto**.
BankGroupSwap	Configures the BankGroupSwap. BankGroupSwap (BGS) is a new memory mapping option in AGESA 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**

2-3-3-3 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**.

2-3-3-4 Memory MBIST



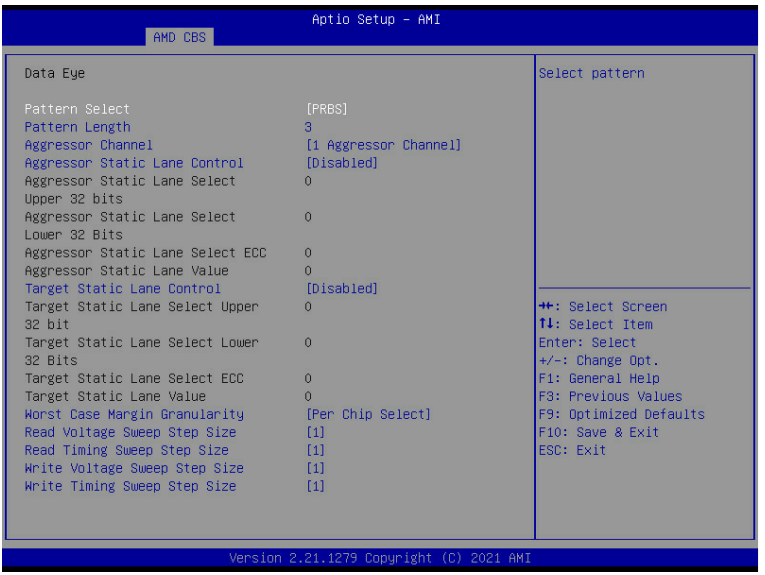
Parameter	Description
Memory MBIST	
MBIST Enable	Enable/Disable the Memory MBIST function. Options available: Enabled, Disabled. Default setting is **Disabled**.
MBIST Test Mode(Note)	Selects MBIST Test Mode. **Interface Mode**: Tests Single and Multiple CS transactions and Basic Connectivity. **Data 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	Options available: Disabled, BIOS Mem BIST, Self-Healing Mem BIST, PMU Mem BIST, BIOS and Self-Healing Mem BIST, BIOS and PMU Mem BIST, PMU and Self-Healing Mem BIST, BIOS and PMU 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**.
PMU Mem BIST Test Select(Note1)	Selects the algorithms to use with PMU Mem BIST. Default setting is **Algorithm #1, #2, #3, #4, #5**.
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 defined.

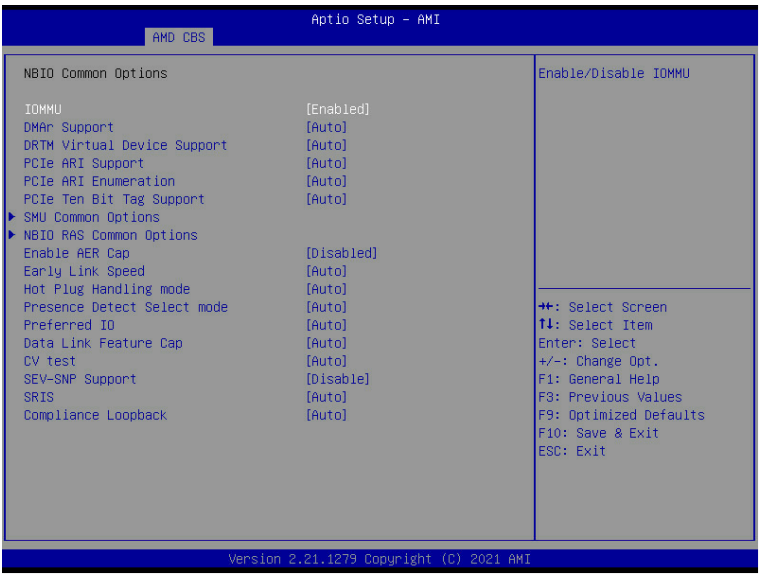
2-3-3-4-1 Data Eye



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**.

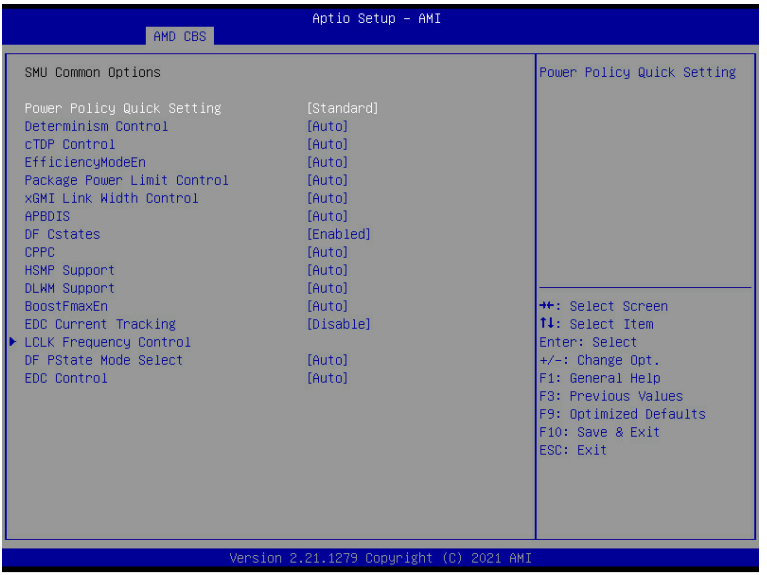
2-3-4 NBIO Common Options



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**.
DRTM Virtual Device Support	Enable/Disable DRTM ACPI virtual device. 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 **Disabled**.

Parameter	Description
Early Link Speed	Configures Early Link Speed. Options available: Auto, Gen1, Gen2. Default setting is **Auto**.
Hot Plug Handling mode	Controls the Hot Plug Handling mode. Options available: 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 **Auto**.
Compliance Loopback	Options available: Auto, Enable, Disable. Default setting is **Auto**.

2-3-4-1 SMU Common Options

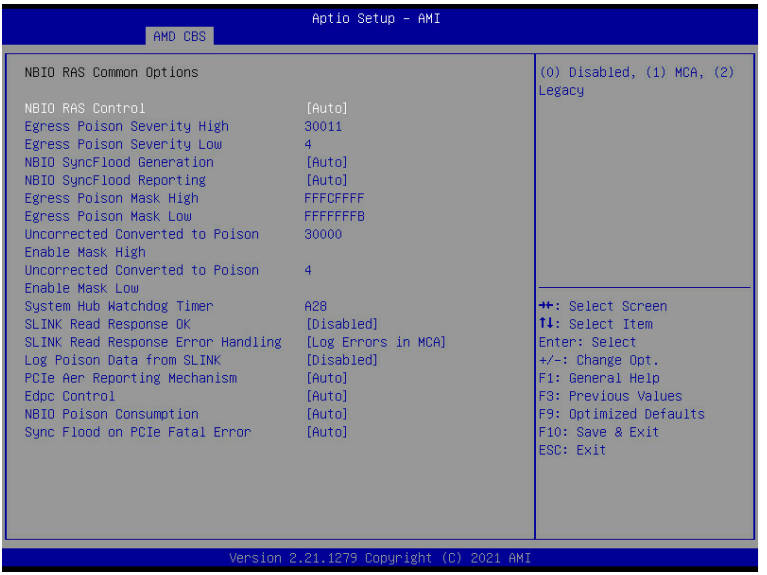


Parameter	Description
SMU Common Options	
Power Policy Quick Setting	Options available: Standard, Best Performance, Energy Efficient. Default setting is **Standard**.
Determinism Control	Selects use the fused Determinism or set customized Determinism. Options available: Auto, Manual. Default setting is **Auto**.
cTDP Control(Note)	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(Note)	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**.

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

Parameter	Description
DF Cstates	Enable/Disable DF C-states. Options available: Auto, Enabled, Disabled. Default setting is **Enabled**.
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**.

2-3-4-2 NBIO RAS Common Options



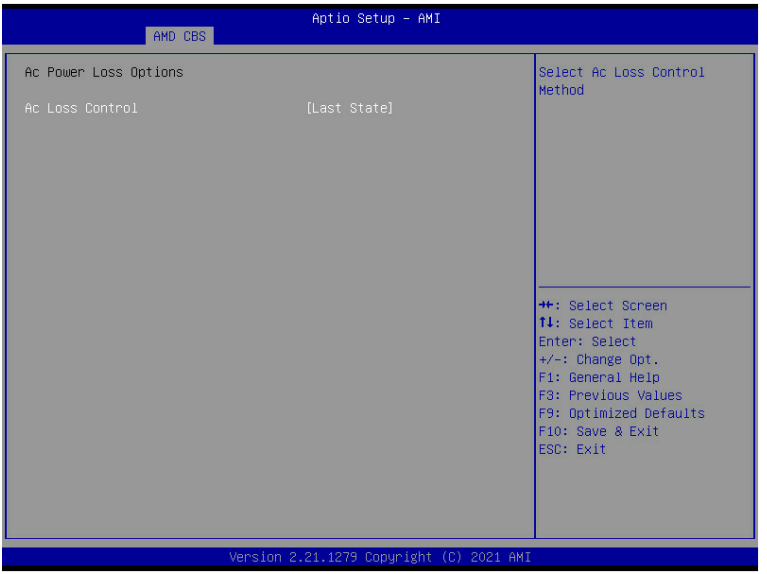
Parameter	Description
NBIO RAS Common Options	
NBIO RAS Control	Options available: Disabled, MCA, Legacy, Auto. Default setting is **Auto**.
Egress Poison Severity High	Configures the Egress Poison High Severity. Each bit set to 1 enables High severity on the associated IOHC egress port. A bit of 0 indicates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

Parameter	Description
Uncorrected Converted to Poison Enable Mask High	Enables mask for masking of uncorrectable parity errors on internal arrays.
Uncorrected Converted to Poison Enable Mask Low	Enables mask for masking of uncorrectable parity errors on internal arrays.
System Hub Watchdog Timer	Specifies the timer interval of the SYSHUB Watchdog timer in milliseconds.
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 **Auto**.
NBIO Poison Consumption	Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Sync Flood on PCIe Fatal Error	Options available: Auto, True, False. Default setting is **Auto**.

2-3-5 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.

2-3-5-1 AC Power Loss Options

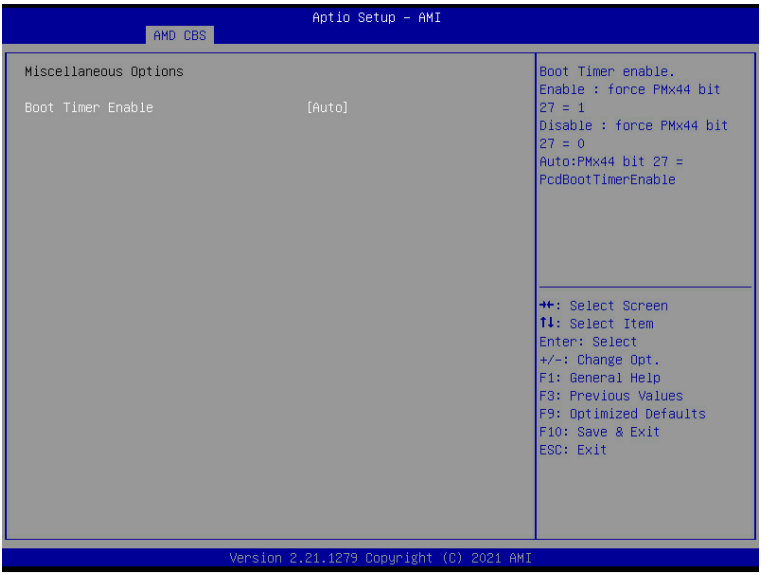


Parameter	Description
AC Power Loss Options	
AC Loss Control	Selects the AC Loss Control Method. Options available: Power Off, Power On, Last State. Default setting is **Last State**.

2-3-5-2 FCH RAS Options

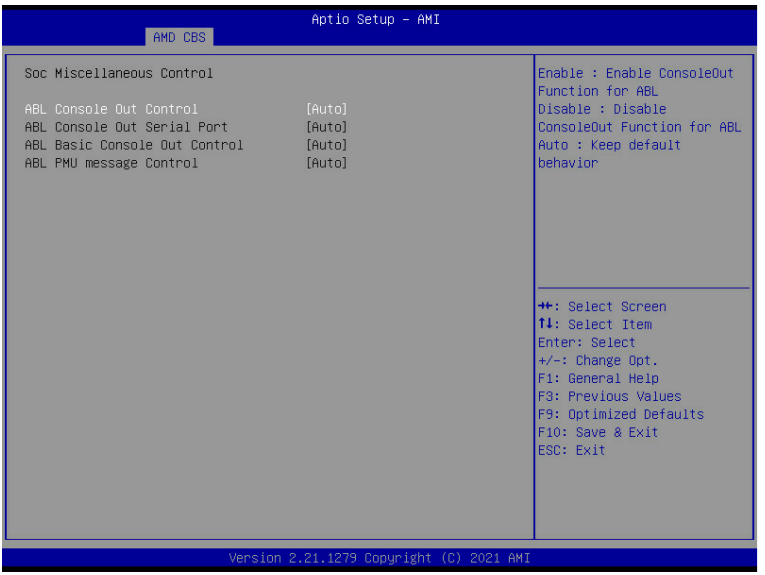
Parameter	Description
FCH RAS Options	
ALink RAS Support	Enable/Disable the ALink RAS Support. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
Reset after sync flood	Enables AB to forward downstream sync-flood message to system controller. Options available: Auto, Enabled, Disabled.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

2-3-5-3 Miscellaneous Options



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

2-3-6 SOC Miscellaneous Control



Parameter	Description
SOC Miscellaneous Control	
ABL Console Out Control	Enable/Disable the ConsoleOut function for ABL. Options available: Auto, Enabled, Disabled. Default setting is **Auto**.
ABL Console Out Serial Port(Note)	Options available: LPC UART, SOC UART0, SOC UART1, Auto. 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**.

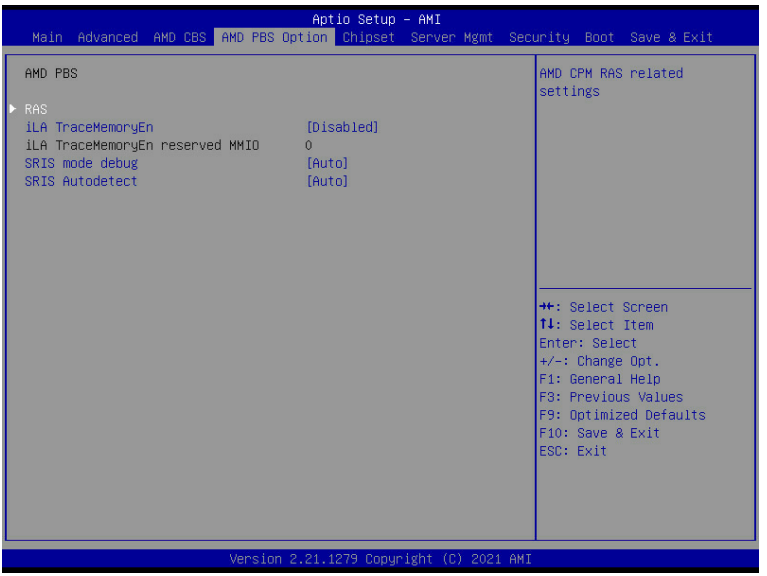
(Note) This item is configurable when **ABL Console Out Control** is set to **Enabled**.

2-3-7 Workload Tuning

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

2-4 AMD PBS Menu

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



Parameter	Description
RAS	Press [Enter] for configuration of advanced items.
iLA TraceMemoryEn	Reserved 1M bytes MMIO space on 1M boundary when iLA TraceMemoryEn 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**.

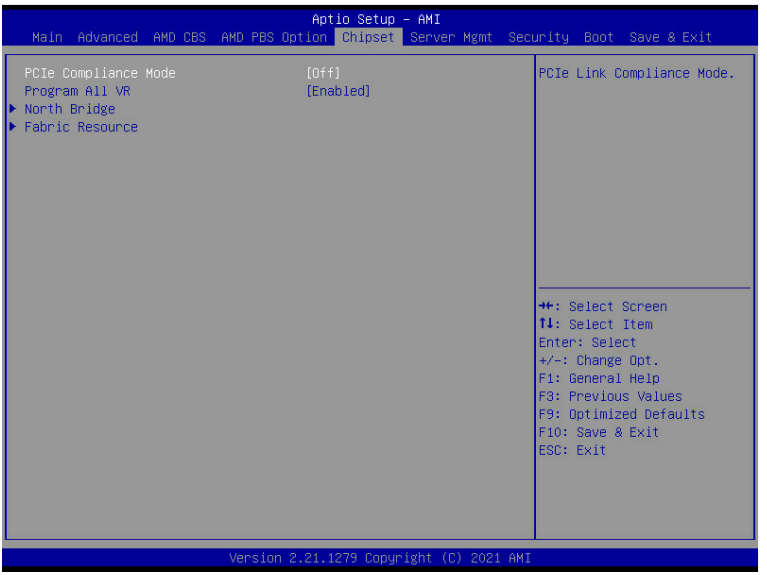
2-4-1 RAS

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 **minute**.
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**.

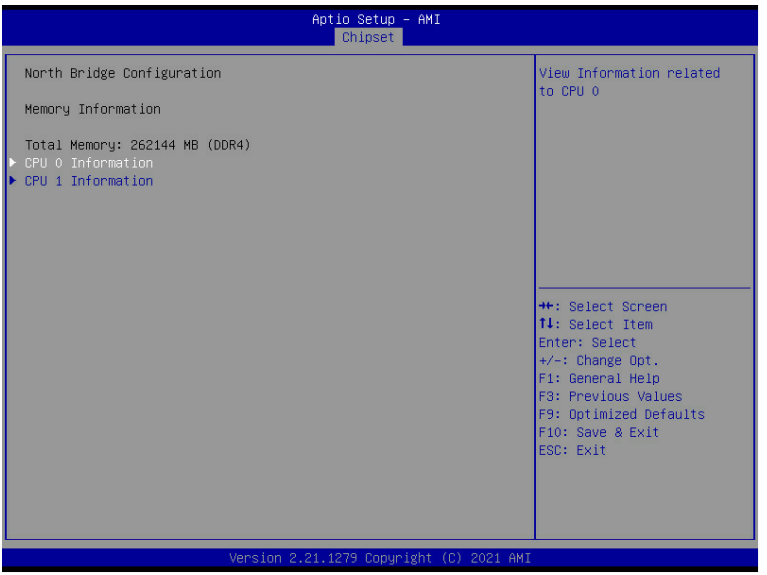
2-5 Chipset Setup Menu

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.



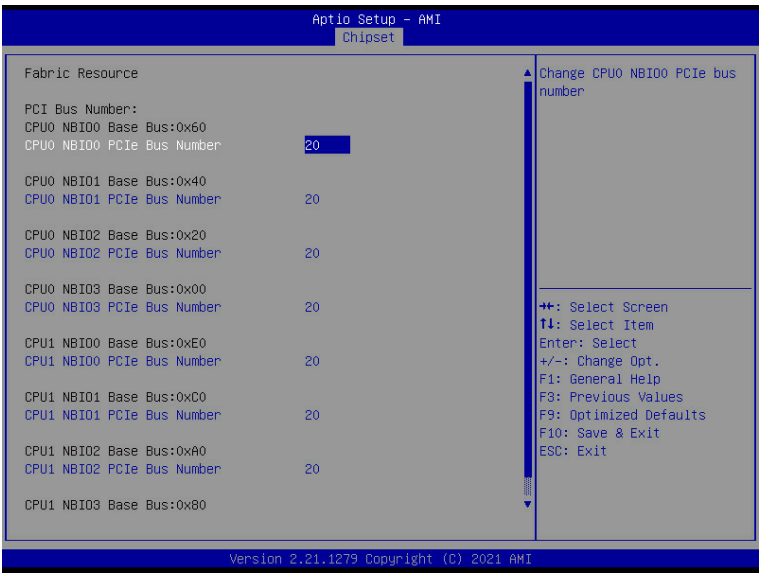
Parameter	Description
PCIe Compliance Mode	Options available: On, Off. Default setting is **Off.**
Program All VR	Enable/Disable program all VR on MB. Options available: Enabled, Disabled. Default setting is **Enabled**.
North Bridge	Press [Enter] for configuration of advanced items.
Fabric Resource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

2-5-1 North Bridge



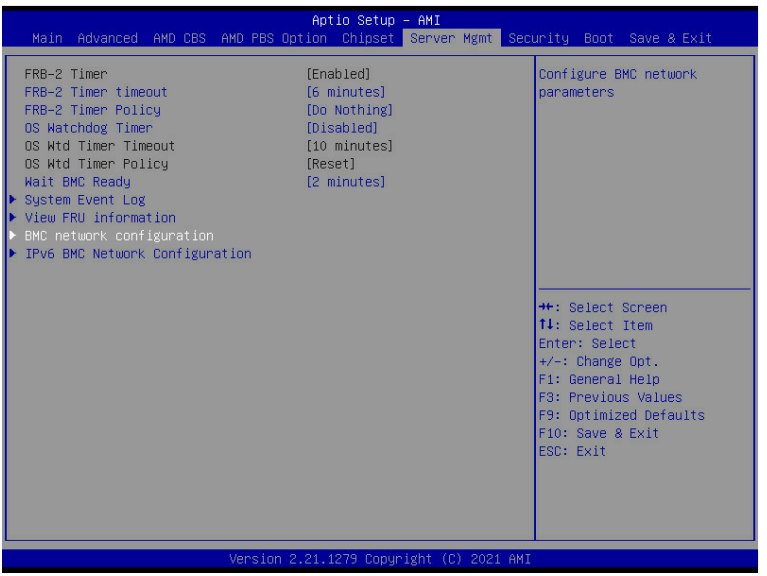
Parameter	Description
North Bridge Configuration Memory Information	
Total Memory	Displays the total memory information.
CPU 0/1 Information	Press [Enter] to view information related to CPU 0/1.

2-5-2 Fabric Resource



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

2-6 Server Management Menu

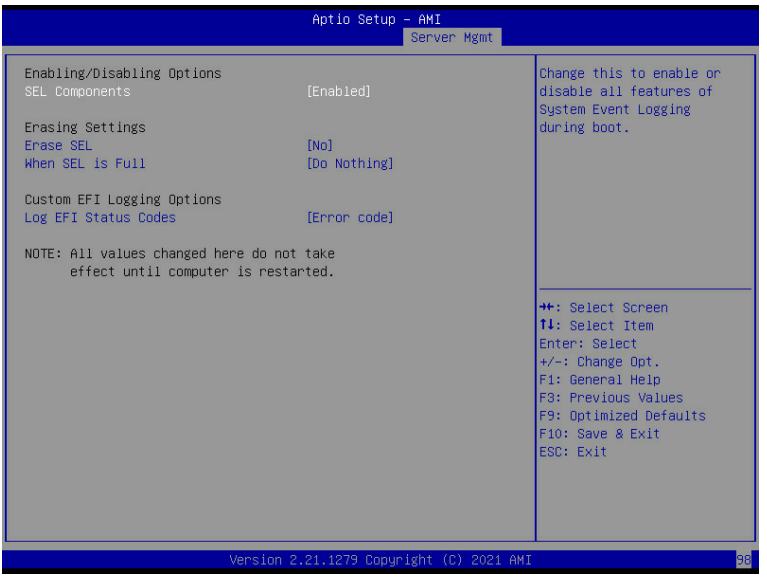


Parameter	Description
FRB-2 Timer	Default setting is **Enabled**.
FRB-2 Timer timeout	Configures the FRB2 Timer timeout. Options available: 3 minutes, 4 minutes, 5 minutes, 6 minutes. Default setting is **6 minutes**.
FRB-2 Timer Policy	Configures the FRB2 Timer policy. Options available: Do Nothing, Reset, Power Down. Default setting is **Do Nothing**.
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled, Disabled. Default setting is **Disabled**.
OS Wtd Timer Timeout(Note)	Configures OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is **10 minutes**.
OS Wtd Timer Policy(Note)	Configure OS Watchdog Timer Policy. Options available: 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**.

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

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

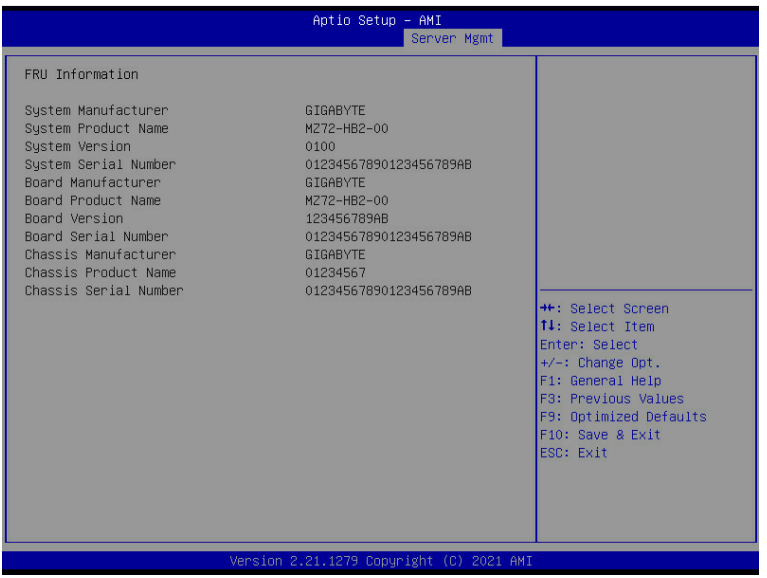
2-6-1 System Event Log



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**.

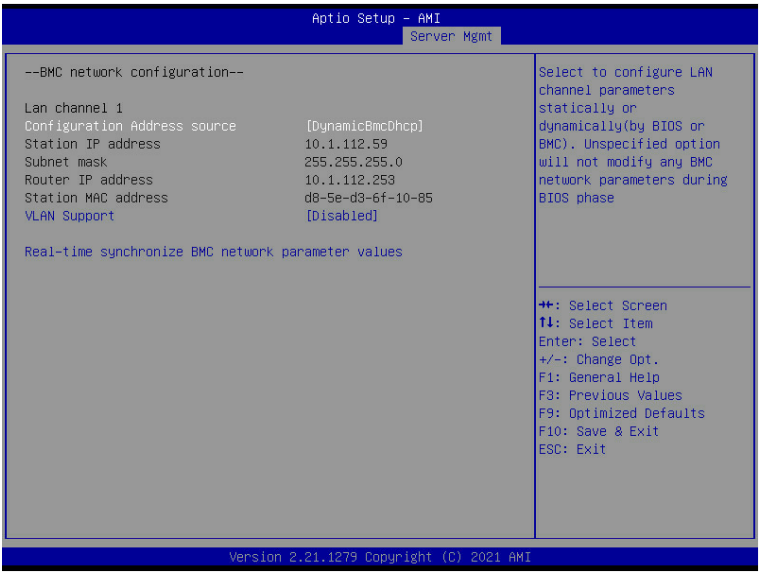
2-6-2 View FRU Information

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

2-6-3 BMC Network Configuration



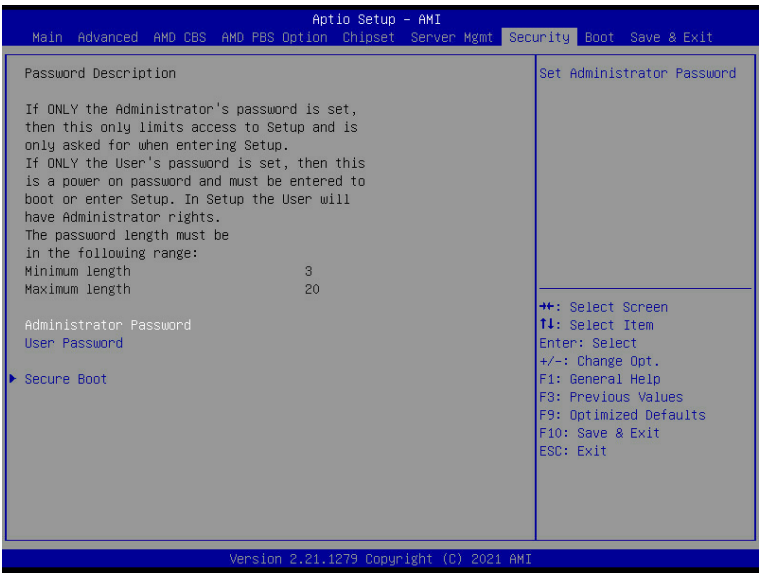
Parameter	Description
BMC network configuration	
Lan Channel 1	
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase. Options available: Unspecified, Static, DynamicBmcDhcp. 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.

2-6-4 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.

2-7 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.

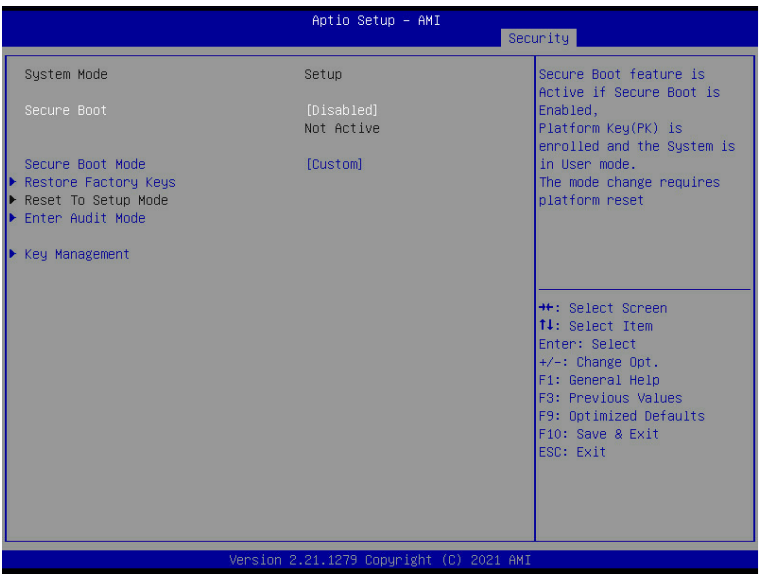
- User Password

  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.

2-7-1 Secure Boot

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



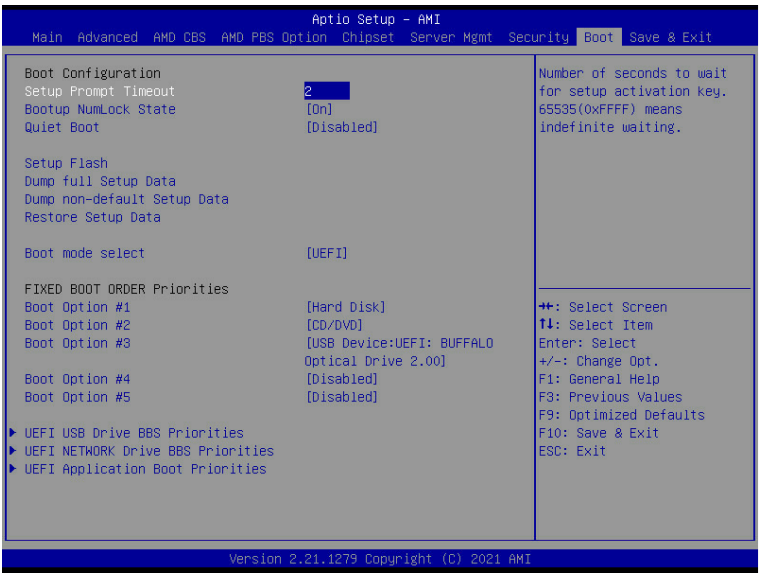
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, Disabled. Default setting is **Disabled**.
Secure Boot Mode(Note)	Secure Boot requires all the applications that are running during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

2-8 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.

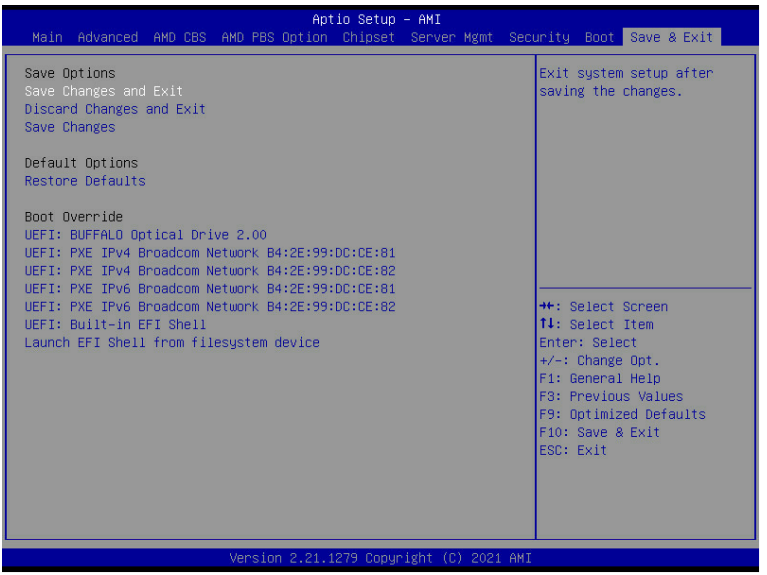


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off.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

Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	Press [Enter] to configure the boot priority. By default, the server searches for boot devices in the following sequence: 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Application Boot Priorities	Press [Enter] to configure the boot priority.

2-9 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>.



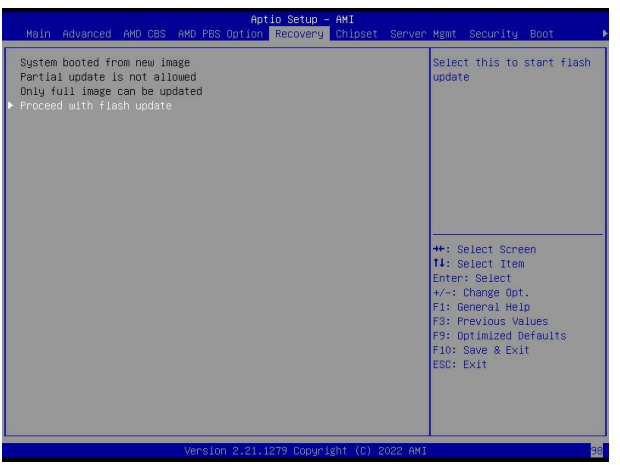
Parameter	Description
Save Options	
Save Changes and Exit	Saves changes made and closes the BIOS setup. Options available: Yes, No.
Discard Changes and Exit	Discards changes made and exits the BIOS setup. Options available: Yes, No.
Save Changes	Saves changes done so far to any of the setup options.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

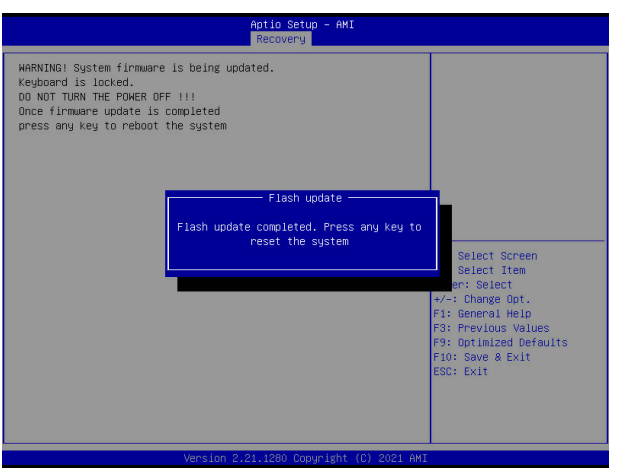
2-10 BIOS Recovery

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

Recovery Instruction:

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





2-11 BIOS POST Beep code (AMI standard)

2-11-1 PEI Beep Codes

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

2-11-2 DXE Beep Codes

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