GIGABYTE™

MD71-HB1

Intel® Socket LGA3647 processor motherboard

User Manual

Rev. 1.0

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.

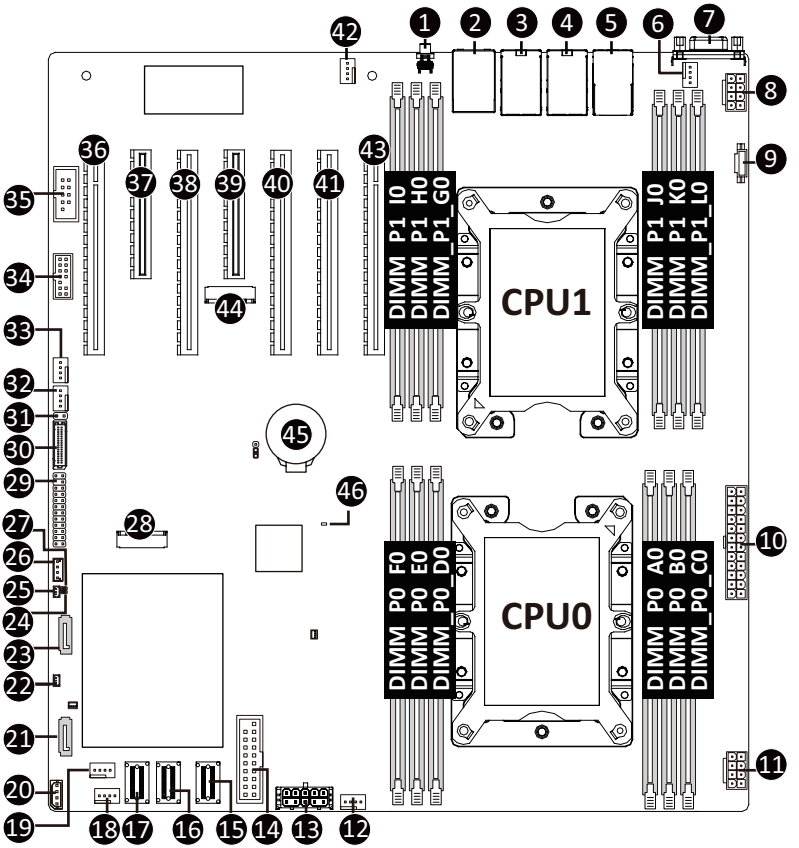
For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: http://reseller.b2b.gigabyte.com

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.

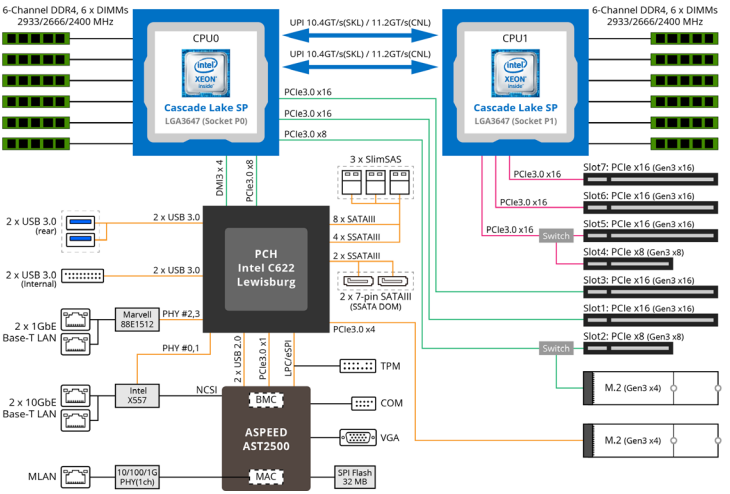
Table of Contents

MD71-HB1 Motherboard Layout



Item	Code	Description
1	SW_ID	ID Button with LED
2	USB3_MLAN	Server Management LAN Port (Top)/ USB 3.0 Ports (Bottom)
3	LAN1	GbE Ethernet LAN Port #1
4	LAN2	GbE Ethernet LAN Port #2
5	LAN3_4	GbE Ethernet LAN Port #3 (Top)/GbE LAN port #4 (Bottom)
6	SYS_FAN5	System Fan Connector #5
7	VGA_1	VGA Port
8	P12V_AUX2	2x4 Pin 12V Power Connector (for CPU1)
9	PMBUS	PMBus Connector
10	ATX1	2x12 Pin Main Power Connector
11	P12V_AUX1	2x4 Pin 12V Power Connector (for CPU0)
12	CPU0_FAN	CPU Fan Connector (for CPU0)
13	P12V_AUX3	2x5 Pin 12V Power Connector (for PCIe Slot)
14	F_USB3	Front Panel USB 3.0 Connector
15	SATA1	Slimline Connector #1 (SATA 6Gb/s Signal/ for SATA#4~#7)
16	SATA0	Slimline Connector #0 (SATA 6Gb/s Signal/ for SATA#0~#3)
17	SSATA0	Slimline Connector #0 (SATA 6Gb/s Signal/ for sSATA#0~#3)
18	SYS_FAN4	System Fan Connector #4
19	SYS_FAN3	System Fan Connector #3
20	IPMB	IPMB Connector
21	SSATA5	SATA 6Gb/s Connector #5
22	SATA_DOM2	SATA DOM Support Power Connector for SSATA Port #5
23	SSATA4	SATA 6Gb/s Connector #4
24	LAN4_ACT	LAN#4 Active LED
25	SATA_DOM1	SATA DOM Support Power Connector for SSATA Port #4
26	SW_RAID	SATA RAID Upgrade Key
27	LAN3_ACT	LAN#3 Active LED
28	M2_SK1	M.2 Slot #1 (PCIe Gen3 x4, Support NGFF-2260/2280)
29	FP_1	Front Panel Header
30	BP_1	HDD Back Plane Board Connector
31	CASE_OPEN	Case Open Intrusion Alert Header
32	SYS_FAN2	System Fan Connector #2
33	SYS_FAN1	System Fan Connector #1
34	LPC_TPM	TPM Connector
35	COM1	Serial Port Cable Connector
36	PCIE_1	PCIe x16 slot #1 (Gen3 x16)
37	PCIE_2	PCIe x8 slot #2 (Gen3 x8)
38	PCIE_3	PCIe x16 slot #3 (Gen3 x16)
39	PCIE_4	PCIe x8 slot #4 (Gen3 x8)
40	PCIE_5	PCIe x16 slot #5 (Gen3 x16)
41	PCIE_6	PCIe x16 slot #6 (Gen3 x16)
42	CPU1_FAN	CPU Fan Connector (for CPU1)
43	PCIE_7	PCIe x16 slot #7 (Gen3 x16)
44	M2_SK2	M.2 slot #2 (PCIe Gen3 x4, Support NGFF-2260/2280)
45	BAT	Battery Socket
46	LED_BMC	BMC Firmware Readiness LED

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

CPU	◆ 2nd Generation Intel® Xeon® Scalable Processors ◆ Intel® Xeon® Platinum Processor, Intel® Xeon® Gold Processor, Intel® Xeon® Silver Processor and Intel® Xeon® Bronze Processor ◆ 2 x LGA 3647, Socket P ◆ Recommended FAN Module: Dynatron B5 ◆ CPU TDP Up to 205W **NOTE: If only 1 CPU is installed, some PCIe or memory functions might be unavailable**
Chipset	◆ Intel® C622 Express Chipset
Memory	◆ 12 x DIMM Slots ◆ DDR4 Memory Supported Only ◆ 6-Channel Memory Architecture ◆ RDIMM Modules Up to 64GB Supported ◆ LRDIMM Modules Up to 128GB Supported ◆ 1.2V Modules: 2933/2666/2400 MHz
Onboard Graphics	◆ Integrated in Aspeed® AST2500 ◆ 2D Video Graphic Adapter with PCIe Bus Interface ◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
LAN	◆ 2 x 10Gb/s BASE-T LAN Ports ◆ 2 x 1Gb/s LAN Ports ◆ 1 x 10/100/1000 Management LAN
Expansion Slots	◆ Slot_7: 1 x PCIe x16 (Gen3 x16 bus) Slot from CPU_1 ◆ Slot_6: 1 x PCIe x16 (Gen3 x16 bus) Slot from CPU_1 ◆ Slot_5: 1 x PCIe x16 (Gen3 x16 bus) Slot from CPU_1 ◆ Slot_4: 1 x PCIe x8 (Gen3 x8 bus) Slot from CPU_1, shared with Slot_5 ◆ Slot_3: 1 x PCIe x16 (Gen3 x16 bus) Slot from CPU_0 ◆ Slot_2: 1 x PCIe x8 (Gen3 x8 bus) Slot from CPU_0, shared with M.2 PCIe x4 bus ◆ Slot_1: 1 x PCIe x16 (Gen3 x16 bus) Slot from CPU_0 ◆ 2 x M.2 Slots: - M-key - PCIe Gen3 x4 per Slot - Supports NGFF-22110/2280 Cards - From CPU_0
Storage Interface	◆ 3 x SlimSAS for 12 x SATA III 6Gb/s Ports ◆ 2 x 7-pin SATA III 6Gb/s with SATA DOM Supported
RAID	◆ Intel® SATA RAID 0/1/10/5

Internal I/O Connectors	◆ 1 x 24-pin ATX Main Power Connector ◆ 2 x 8-pin ATX 12V Power Connectors ◆ 2 x SATA DOM Power Pin Headers ◆ 3 x SlimSAS Connectors ◆ 2 x 7-pin SATA Connectors ◆ 2 x M.2 Slots ◆ 2 x CPU Fan Headers ◆ 5 x System Fan Headers ◆ 1 x USB 3.0 Header ◆ 1 x COM Header ◆ 1 x LPC TPM Header ◆ 1 x VROC Connector ◆ 1 x Front Panel Header ◆ 1 x HDD Back Plane Board Header ◆ 1 x PMBus Connector ◆ 1 x IPMB Connector ◆ 1 x Clear CMOS Jumper ◆ 1 x BIOS Recovery Jumper ◆ 1 x Case Open Header
Rear I/O Connectors	◆ 2 x USB 3.0 Ports ◆ 1 x VGA Port ◆ 4 x RJ45 Ports ◆ 1 x MLAN Port ◆ 1 x ID Button with LED
TPM	◆ 1 x TPM Header with LPC Interface ◆ Optional TPM2.0 kit: CTM000
Board Management	◆ Aspeed® AST2500 Management Controller ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface
Form Factor	◆ E-ATX ◆ 305mm W x 330mm D
GIGABYTE reserves the right to make any changes to the product specifications and product-related information without prior notice.	

1-3 Installing and Removing the CPU and Heat Sink

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

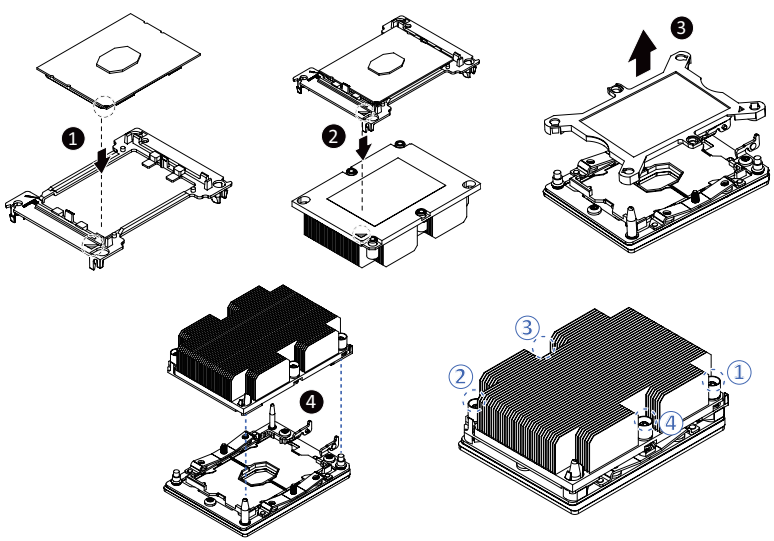
- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system 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. Align and install the processor on the carrier.
   Note: Apply thermal compound evenly on the top of the CPU. Remove the protective cover from the underside of the heat sink.
2. Carefully flip the heatsink over. Then install the carrier assembly on the bottom of the heatsink and make sure the gold arrow is located in the correct direction.
3. Remove the CPU cover.
   Note: Save and replace the CPU cover if the processor is removed from its socket.
4. Align the heatsink with the CPU socket by the guide pins and make sure the gold arrow is located in the correct direction. Then place the heatsink onto the top of the CPU socket.
5 To secure the heatsink, tighten the screws in a sequential order (1→2→3→4).
   Note: When dissambling the heatsink, loosen the screws in reverse order (4→3→2→1)



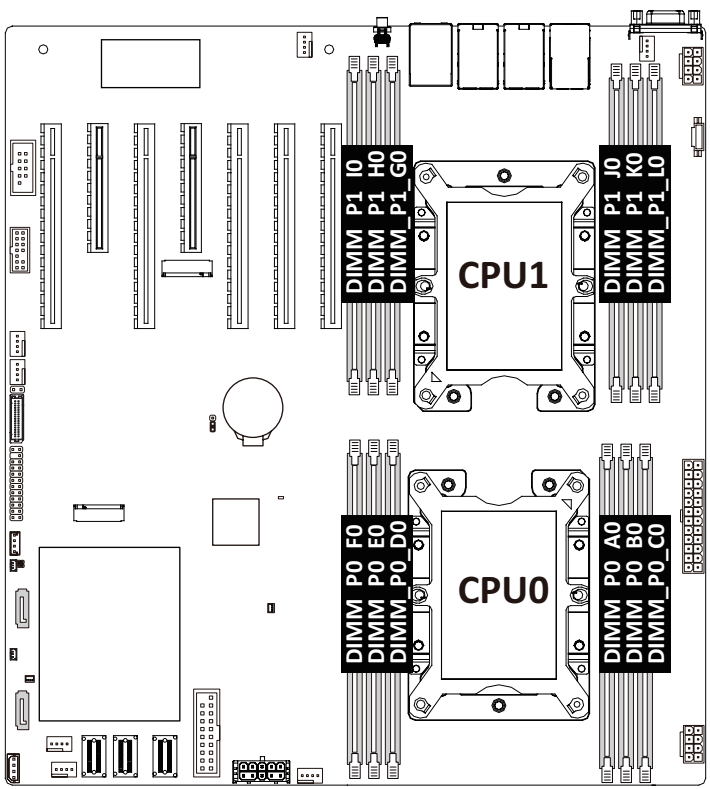
1-4 Installing and Removing Memory

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

- Make sure that the motherboard supports the memory. It is recommended to use memory of the same capacity, brand, speed, and chips.
- 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 6-Channel Memory Configuration

This motherboard provides 12 DDR4 memory sockets and supports 6-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.

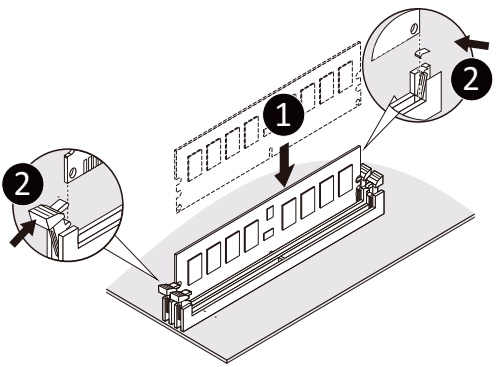


1-4-2 Installing and Removing a Memory Module

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 UDIMMs on 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.



Note: When populating DIMMs into a channel, slot numbers having the suffix "0" must be populated first, then followed by slot numbers having the suffix "1".

1-4-3 DIMM Population Table

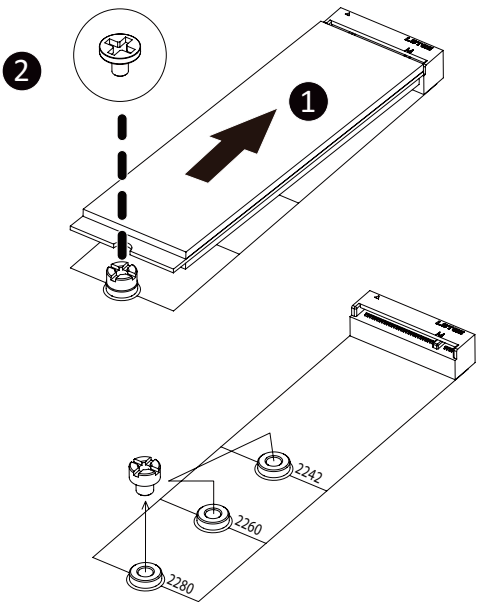
Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); Slots per Channel(SPC) and DIMM per Channel (DPC)
					1 Slot Per Channel
		DRAM Density			1DPC
		4Gb*	8Gb	16Gb	1.2V
RDIMM	SRx8	4GB	8GB	16GB	2933
RDIMM	SRx4	8GB	16GB	32GB	
RDIMM	DRx8	8GB	16GB	32GB	
RDIMM	DRx4	16GB	32GB	64GB	
RDIMM 3DS	QRx4	N/A	2H-64GB	2H-128GB	
	8Rx4	N/A	4H-128GB	4H-256GB	
LRDIMM	QRx4	32GB	64GB	128GB	
LRDIMM 3DS	QRx4	N/A	2H-64GB	2H-128GB	
	8Rx4	N/A	4H-128GB	4H-256GB	

* 4Gb DRAM density is only supported on speeds up to 2666MT/s.

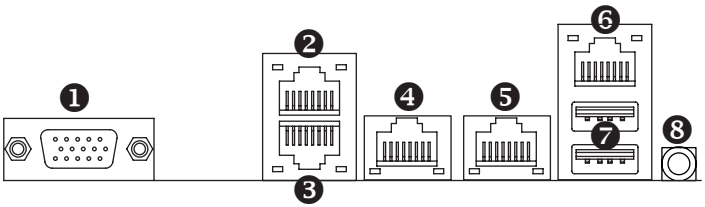
1-5 Installing the M.2 SSD Module

Follow the steps below to install a 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 VGA Port

The video-in port allows connection via video in, which can also apply to the video loop thru function.

❷ RJ-45 LAN Port #3

The Gigabit Ethernet LAN port provides Internet connection at up to 1 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

❸ RJ-45 LAN Port #4

The Gigabit Ethernet LAN port provides Internet connection at up to 1 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

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 Server Management LAN Port

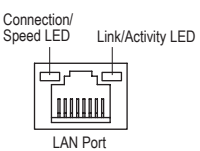
The LAN port provides Internet connection with data transfer speeds of 10/100/1000Mbps. This port is the dedicated LAN port for Server Management.

❼ 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.

❽ ID button with LED

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



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:

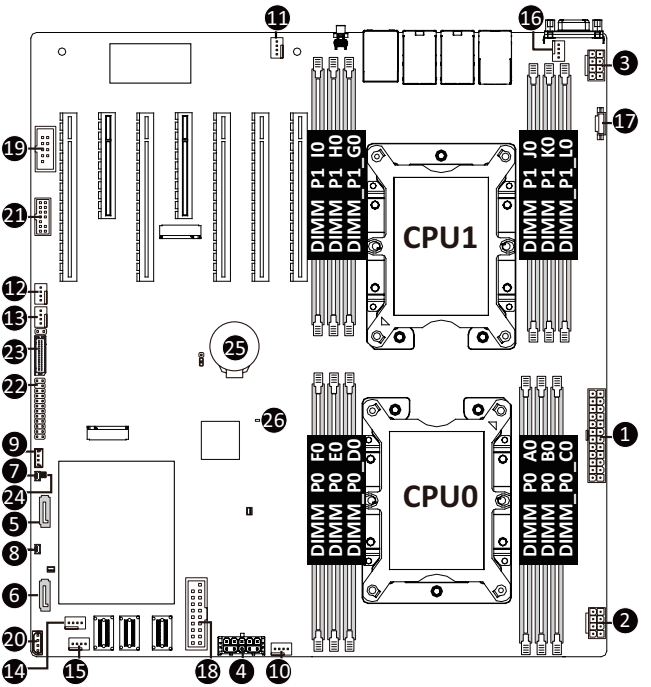
State	Description
Yellow On	1Gbps data rate
Green On	100Mbps data rate
Off	10Mbps data rate

ID button/LED:

State	Description
Bule 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)	ATX1	14)	SYS_FAN3
2)	P12V_AUX1 (for CPU0)	15)	SYS_FAN4
3)	P12V_AUX2 (for CPU1)	16)	SYS_FAN5
4)	P12V_AUX3 (for PCIe Slot)	17)	PMBUS
5)	SSATA4	18)	F_USB3
6)	SSATA5	19)	COM1
7)	SATA_DOM1 (for SSATA4)	20)	IPMB
8)	SATA_DOM2 (for SSATA5)	21)	LPC_TPM
9)	SW_RAID	22)	FP_1
10)	CPU0_FAN	23)	BP_1
11)	CPU1_FAN	24)	LAN3_ACT/ LAN4_ACT
12)	SYS_FAN1	25)	BAT
13)	SYS_FAN2	26)	LED_BMC

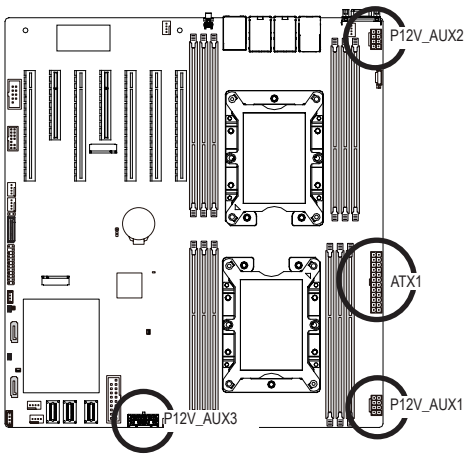
Read the following guidelines before connecting external devices:

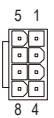
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the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

1/2/3/4) ATX1/P12V_AUX1/P12V_AUX2/P12V_AUX3
(2x12 Main Power Connector and 2x4/2x5 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.

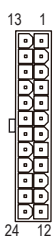




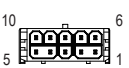
P12V_AUX1/P12V_AUX2

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

ATX1



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

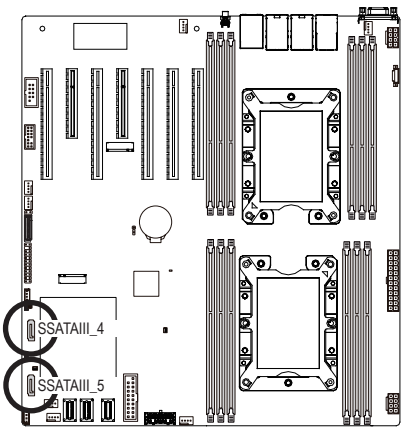


P12V_AUX3

Pin No.	Definition
1	GND
2	GND
3	GND
4	GND
5	GND
6	+12V
7	+12V
8	+12V
9	+12V
10	+12V

5/6) SSATA4/SSATA5 (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.

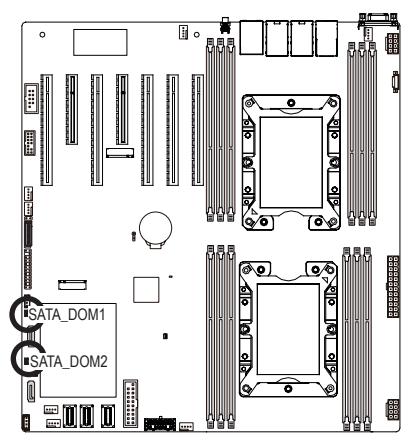


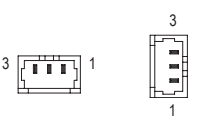
(Support SATA DOM Power)

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

7/8) SATA_DOM1/ SATA_DOM2 Power Connector

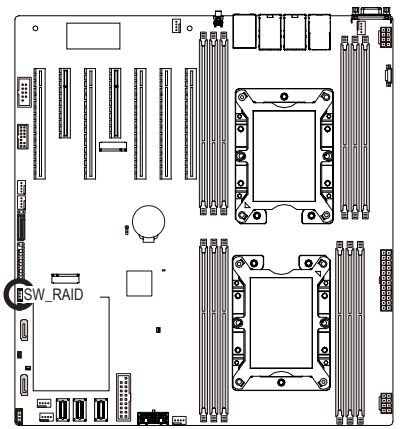
SATA-DOM (Disk on Module) is available to allow for standalone boot and diagnostics direct through SATA connections on the board.





Pin No.	Definition
1	5V for SATA DOM
2	GND
3	No Connect

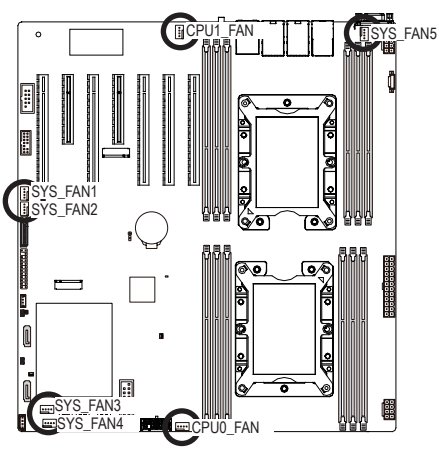
9) SW_RAID (SATA RAID Upgrade Key)

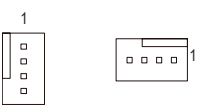


Pin No.	Definition
1	GND
2	P_3V3_AUX
3	GND
4	PCH_SATA_RAID_KEY

10/11/12/13/14/15/16) CPU0_FAN/CPU1_FAN/SYS_FAN1/SYS_FAN3/SYS_FAN2/SYS_FAN4 SYS_FAN5 (CPU Fan/System Fan Headers)

The motherboard has one 4-pin CPU fan header (CPU_FAN), and two 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.



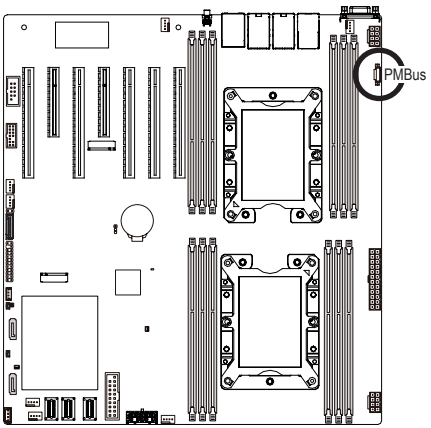


Pin No.	Definition
1	GND
2	+12V
3	Sense
4	Speed Control

- 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.

17) PMBus Connector

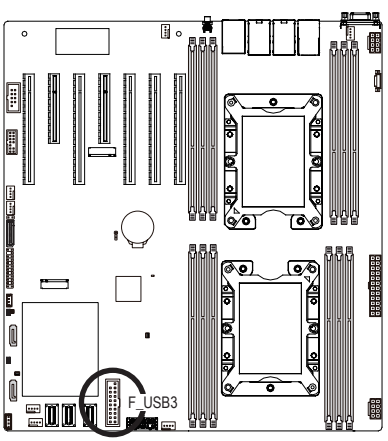
The Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



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

18) F_USB3 (USB 3.0 Header)

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

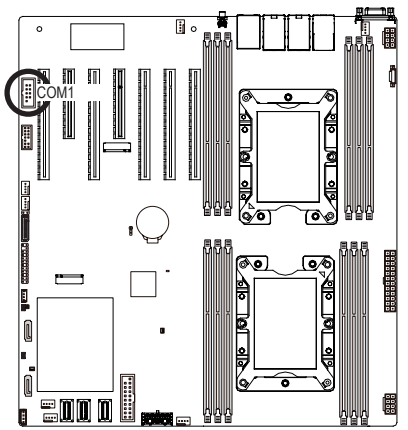


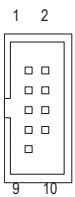
USB 3.0 Header

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_SSRX+
5	IntA_P1_SSRX-	15	IntA_P2_SSRX-
6	IntA_P1_SSRX+	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

19) COM1 (Serial Port Cable Connector)

The COM header can provide one serial port via an optional COM port cable. For purchasing the optional COM port cable, please contact the local dealer.

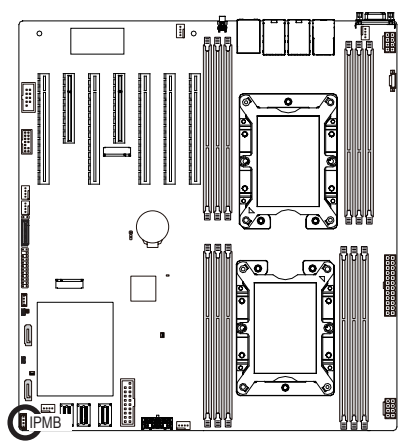




Pin No.	Definition
1	NDCD-
2	NSIN
3	NSOUT
4	NDTR-
5	GND
6	NDSR-
7	NRTS-
8	NCTS-
9	NRI-
10	No Pin

20) IPMB (Intelligent Platform Management Bus) Connector

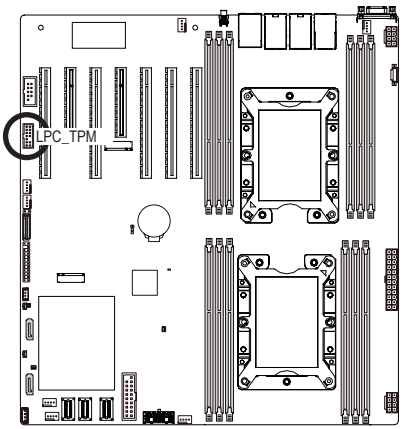
The Intelligent Platform Management Bus Communications Protocol defines a byte-level transport for transferring Intelligent Platform Management Interface Specification (IPMI) messages between intelligent I2C devices.

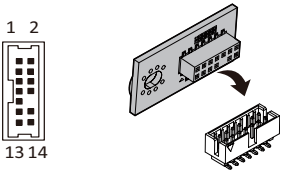


Pin No.	Definition
1	Clock
2	GND
3	Data
4	VCC

21) LPC_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.

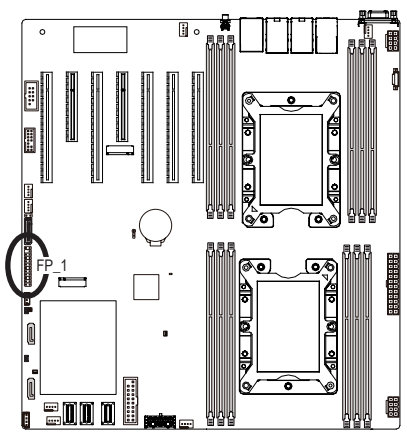




Pin No.	Definition	Pin No.	Definition
1	Clock	8	No Connect
2	P_3V3_AUX	9	LPC_LAD_2
3	LPC_RST	10	No Pin
4	P3V3	11	LPC_LAD_3
5	LPC_LAD_0	12	GND
6	IRQ_SERIAL	13	LPC_FRAME_N
7	LPC_LAD_1	14	GND

22) FP_1 (Front Panel Header)

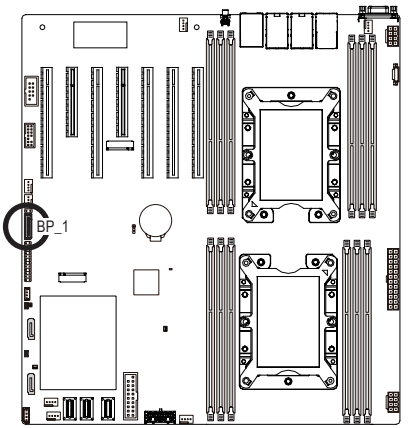
Connect the power switch, reset switch, speaker, chassis intrusion switch/sensor and system status indicator on the chassis to this header according to the pin assignments below. Note the positive and negative pins before connecting the cables.

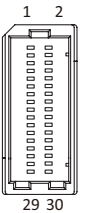


Pin No.	Definition	Pin No.	Definition
1	Power LED+	13	GND
2	5V Standby	14	LAN1 Link LED-
3	No Pin	15	Reset Button
4	ID LED+	16	SMBus Data
5	Power LED-	17	GND
6	ID LED-	18	SMBus Clock
7	HDD LED+	19	ID Button
8	System Status LED+	20	Case Open
9	HDD LED-	21	GND
10	System Status LED-	22	LAN2 Active LED+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

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.

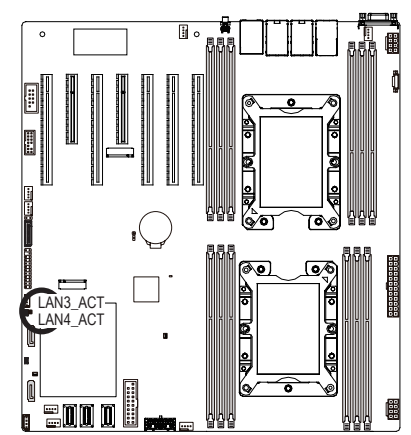
23) BP_1 (HDD Backplane Board Header)





Pin No.	Definition	Pin No.	Definition
1	Reserved	2	BPMI DIN/OUT
3	GND	4	BPMI DOUT/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	12C_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
29	P3V3_AUX	30	P3V3_AUX

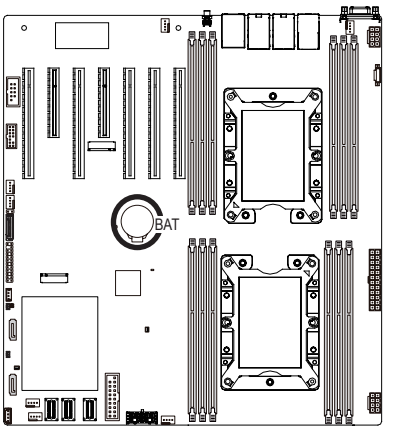
24) LAN3_ACT/ LAN4_ACT (LAN3 and LAN4 Active LED Header)

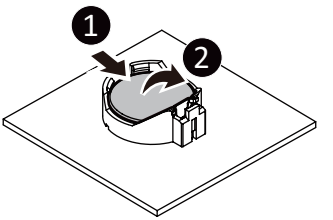


Pin No.	Definition
1	Enable LAN Link/ Active LED
2	P_3V3_AUX

25) BAT (Battery Scoket)

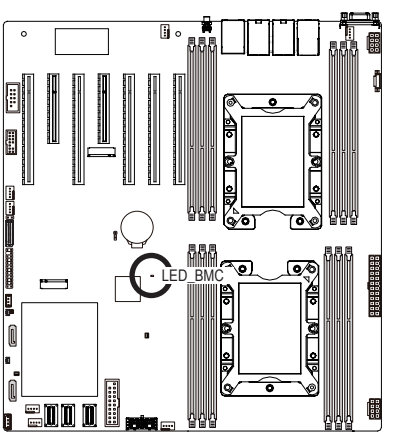
The battery provides power to keep the values (such as BIOS configurations, date, and time information) in the CMOS when the computer is turned off. Replace the battery when the battery voltage drops to a low level, or the CMOS values may not be accurate or may be lost.





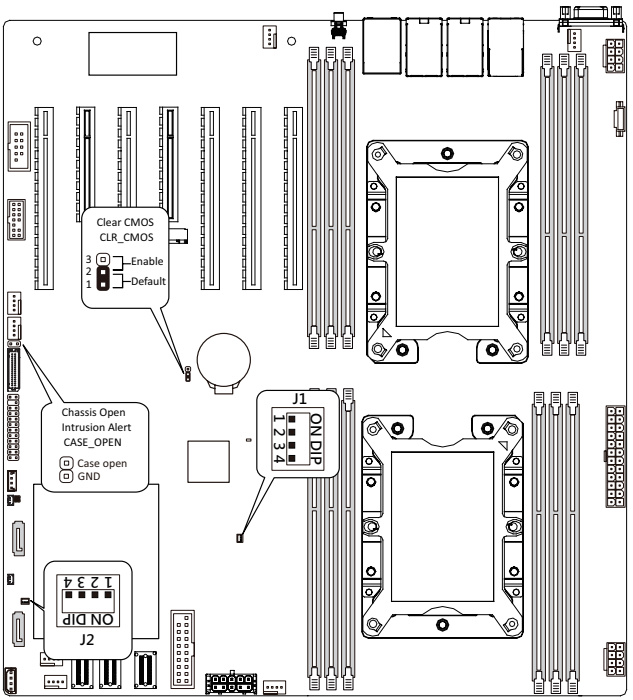
- Always turn off your computer and unplug the power cord before replacing the battery.
- Replace the battery with an equivalent one. Danger of explosion if the battery is replaced with an incorrect model.
- Contact the place of purchase or local dealer if you are not able to replace the battery by yourself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

26) LED_BMC (BMC Firmware Readiness LED)



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

1-8 Jumper Settings



Jumper Name	Jumper Setting
Clear CMOS	1-2: Nomal operation (Default) 2-3: Clear CMOS data
Chassis Open Intrusion Alert	Open: Nomal operation (Default) Closed: Active Chassis Intrusion Alert.

J1		ON	OFF
1	HOST_SMBUS_SEL	BIOS defined	
2	PMBUS_SEL	BIOS defined	
3	S3_MASK	Stop initial power on when BMC is not ready	Normal [Default]
4	DB_PLD	CPLD debug mode	Normal [Default]

J2		ON	OFF
1	ME_UPDATE	Force ME update	Normal [Default]
2	BIOS_PWD	Clear supervisor password	Normal [Default]
3	BIOS_RCVR	BIOS recovery mode	Normal [Default]
4	ME_RCVR	ME 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.)
- **Chipset**
  This setup page includes all the submenu options for configuring the functions of the Platform Controller Hub.
- **Server Management**
  Server additional features enabled/disabled setup menus.
- **Security**
  Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.
  A supervisor password allows you to make changes in BIOS Setup.
  A user password only allows you to view the BIOS settings but not to make changes.
- **Boot**
  This setup page provides items for configuration of the boot sequence.
- **Save & Exit**
  Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)
  Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

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.

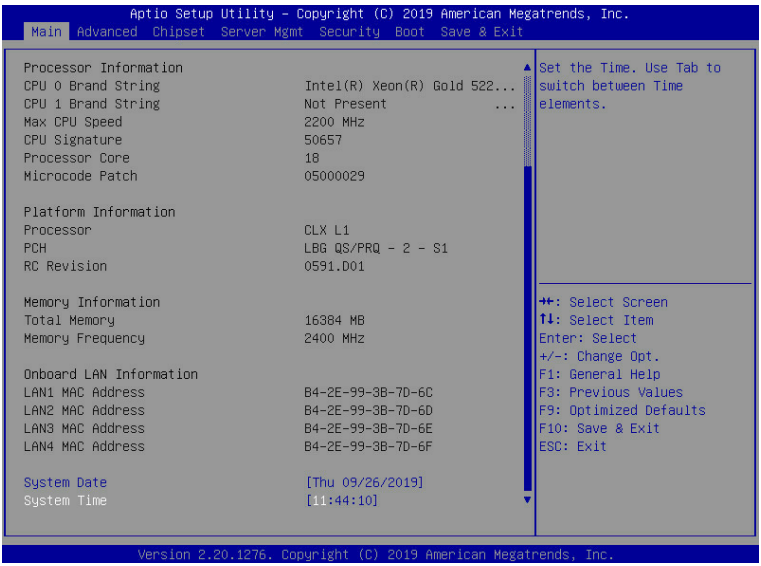
Main Menu Help

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	
CPU0 Brand String/ CPU1 Brand String/ Max CPU Speed / CPU Signature / Processor Core / Microcode Patch	Displays the technical specifications for the installed processor(s).
Memory Information	
Total Memory(Note2)	Displays the total memory size of the installed memory.
Memory Frequency(Note2)	Displays the frequency information of the installed memory.

(Note1) Functions available on selected models.

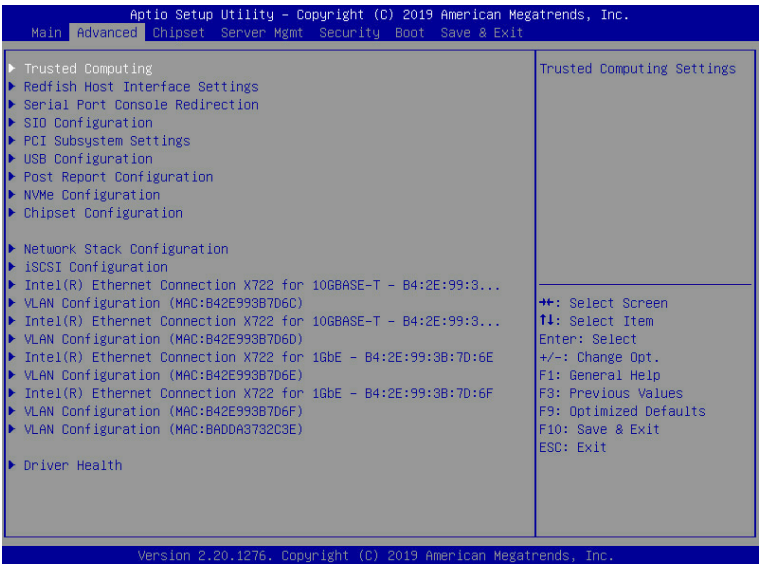
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

Parameter	Description
Onboard LAN Information	
LAN1 MAC Address(Note)	Displays LAN MAC address information.
LAN2 MAC Address (Note)	Displays LAN MAC address information.
LAN3 MAC Address(Note)	Displays LAN MAC address information.
LAN4 MAC Address (Note)	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

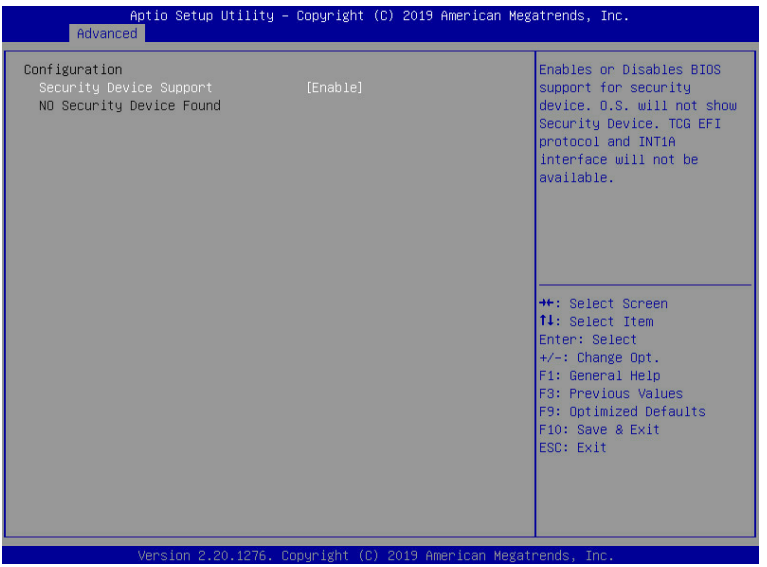
(Note) The number of LAN ports listed will depend on the motherboard / system model.

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.

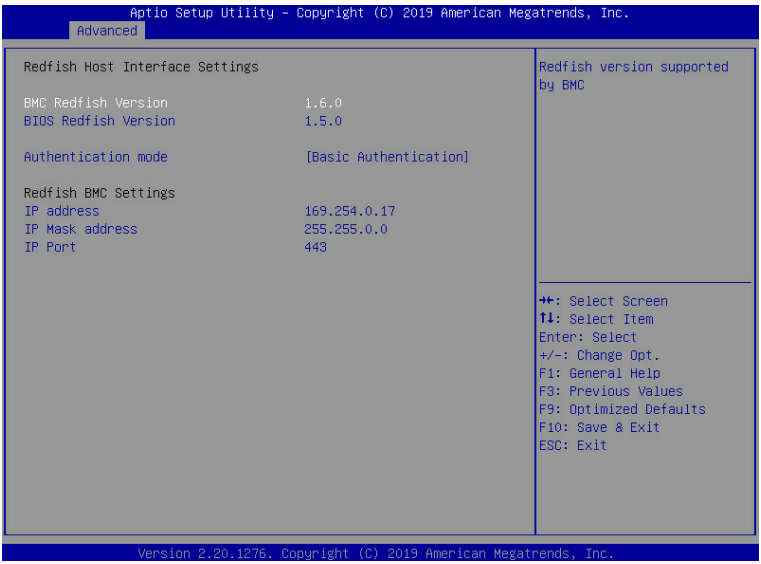


2-2-1 Trusted Computing



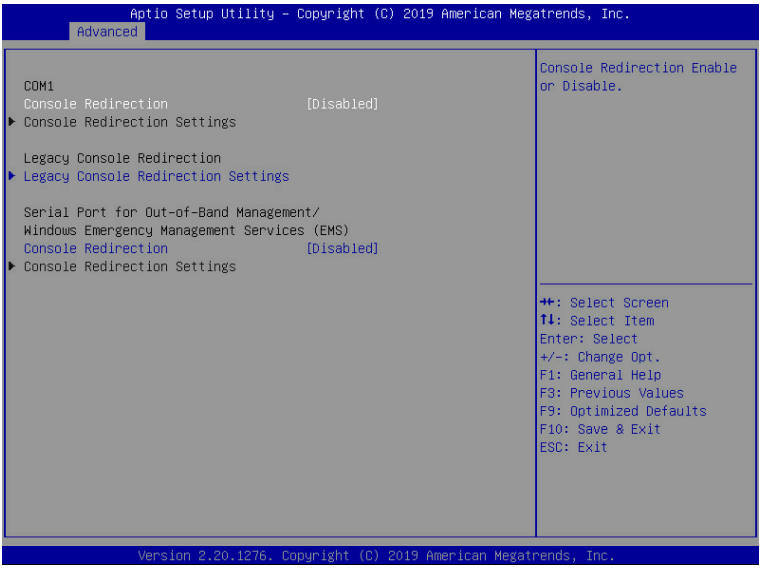
Parameter	Description
Configuration	
Security Device Support	Enable/Disable the TPM support feature. Options available: Enable/Disable. Default setting is **Enable**.
Current Status Information	Displays current TPM status information.

2-2-2 Redfish Host Interface Settings



Parameter	Description
Redfish Host Interface Settings	
BMC Redfish Version	Displays the Redfish version supported by BMC.
BIOS Redfish Version	Displays the Redfish version supported by BIOS.
Authenticaion mode	Selects Authentication mode. Options available: Basic Authentication/Session Authentication. Default setting is **Enable**.
Redfish BMC Settings	
IP address	Enter IP address.
IP Mask address	Enter IP Mask address.
IP Port	Enter IP Port.

2-2-3 Serial Port Console Redirection



Parameter	Description
COM1 Console Redirection(Note))	Console redirection enables the users to manage the system from a remote location. Options available: Enabled/Disabled. Default setting is **Disabled**.
COM1 Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when COM1 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 **VT100+**. ◆ 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 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(Note) – When this mode enabled, only texts will be send. This is to capture Terminal data. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ Resolution 100x31(Note) – Enable/Disable extended terminal resolution. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Putty KeyPad(Note) – Selects FunctionKey and LeyPad on Putty. – Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is **VT100**.

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

Parameter	Description
Legacy Console Redirection	
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**. ◆ 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 Emerency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Default setting is **COM1**. ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is **VT100+**. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is **115200**.

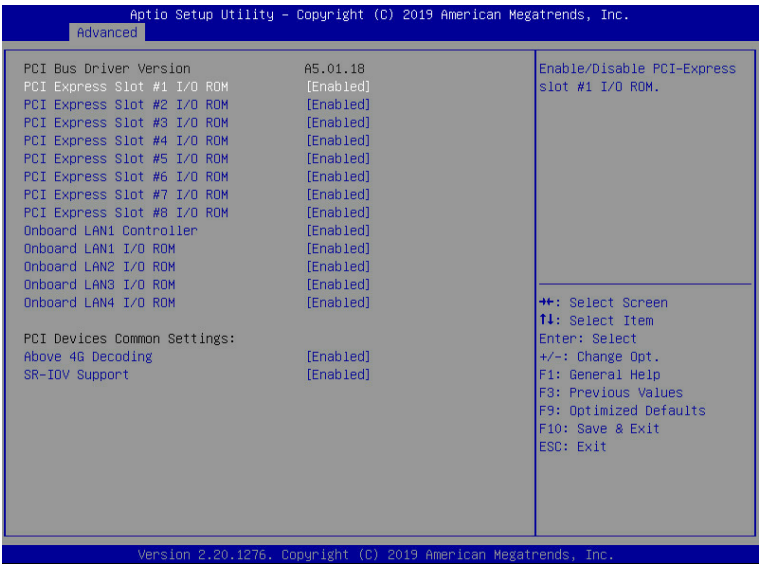
(Note) Advanced items prompt when this item is defined.

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**.

2-2-4 SIO Configuration

Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	
[*Active*] Serial Port	Press [Enter] to configure advanced items. ◆ Use This Device – When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Current: – Displays the serial port base I/O address and IRQ. ◆ Possible: – Configures the serial port base I/O address and IRQ. Use Automatic Settings IO=3F8h; IRQ=4; DMA; IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; Default setting is **Use Automatic Settings**.

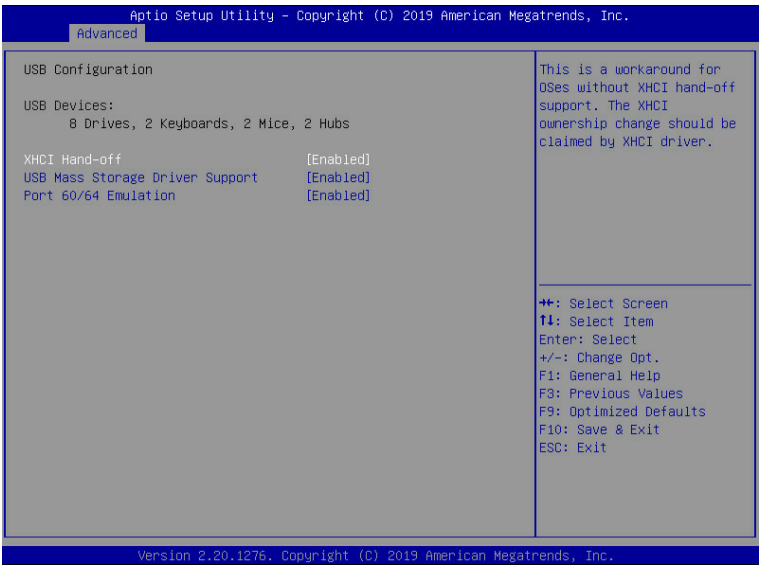
2-2-5 PCI Subsystem Settings



Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
PCI Express Slot # I/O ROM(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled/Disabled. Default setting is **Enabled**.
Onboard LAN1 Controller(Note2)	Enable/Disable the onboard LAN1 controller. Options available: Enabled/Disabled. Default setting is **Enabled**.
Onboard LAN1 / LAN2 / LAN3 / LAN4 I/O ROM(Note2)	Enable/Disable the onboard LAN1/ LAN2/ LAN3/ LAN4 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 LAN controller.

2-2-6 USB Configuration



Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled/Disabled. Default setting is **Enabled**.
USB Mass Storage Driver Support(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled/Disabled. Default setting is **Enabled**.
Port 60/64 Emulation	Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OS. Options available: Enabled/Disabled. Default setting is **Enabled**.

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

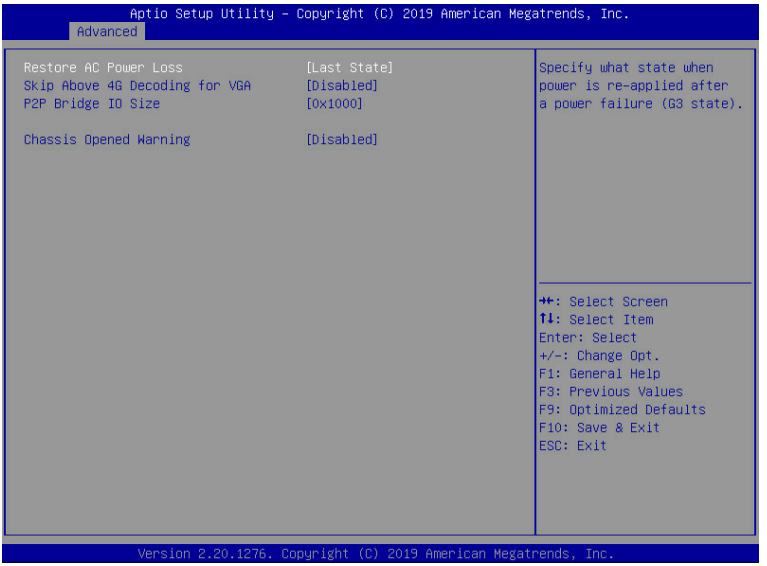
2-2-7 Post Report Configuration

Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled/Disabled. Default setting is **Enabled**.

2-2-8 NVMe Configuration

Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system
NVMe OPROM Select	Options available: BIOS Build-In/NVMe Device. Default setting is **BIOS Build-In**.

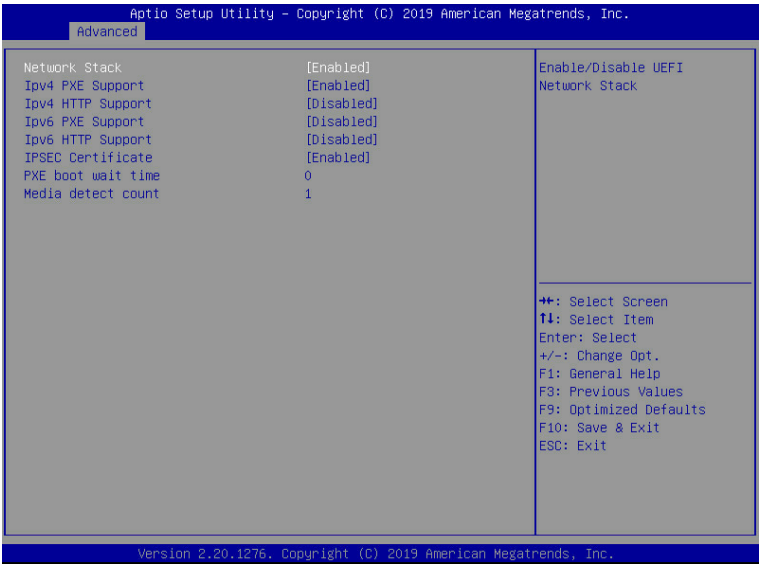
2-2-9 Chipset Configuration



Parameter	Description
Restore on AC Power Loss(Note)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
Skip Above 4G Decoding for VGA	Enable/Disable 64bit capable devices to be decoded in Skip Above 4G Address VGA Space. Options available: Enabled/Disabled. Default setting is **Disabled**.
P2P Bridge IO Size	Sets P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is **0x1000**.
Chassis Opened Warning	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is **Disabled**.

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

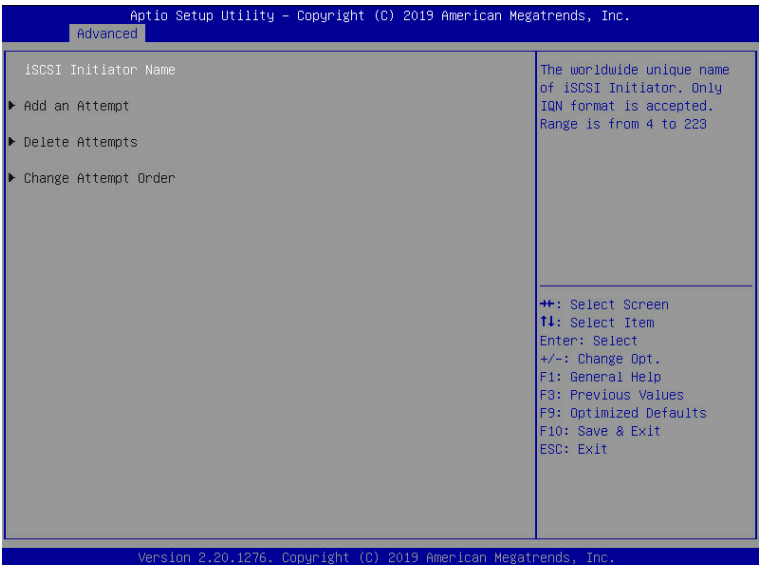
2-2-10 Network Stack Configuration



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 **Disabled**.
Ipv6 HTTP Support(Note)	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled/Disabled. Default setting is **Disabled**.
IPSEC Certificate(Note)	Enable/Disable the IPSEC Certificate feature. Options available: Enabled/Disabled. Default setting is **Enabled**.
PXE boot wait time(Note)	Press the <+> / <-> keys to increase or decrease the desired values.
Media detect count(Note)	Press the <+> / <-> keys to increase or decrease the desired values.

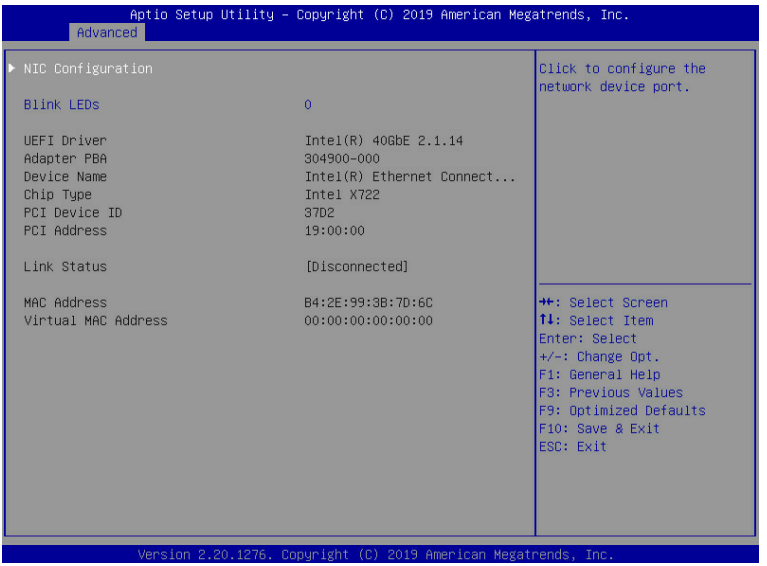
(Note) This item appears when **Network Stack** is set to **Enabled**.

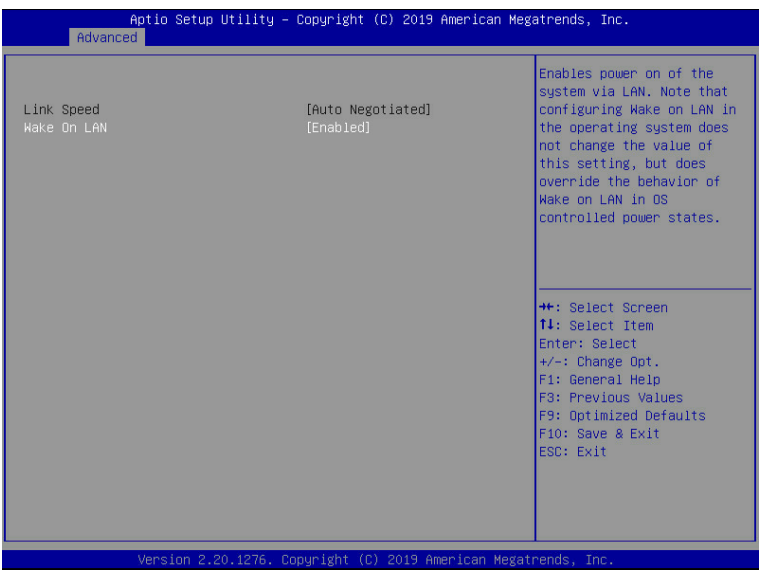
2-2-11 iSCSI Configuration



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.

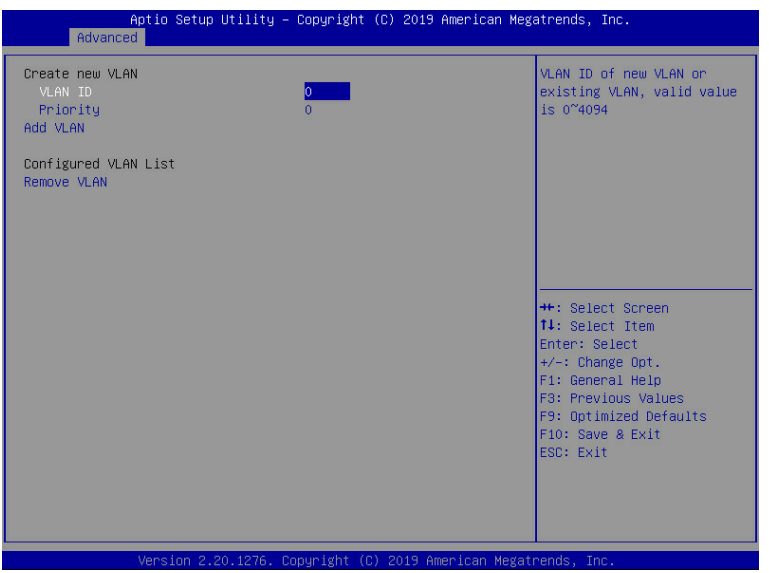
2-2-12 Intel(R) X722 Gigabit Network Connection





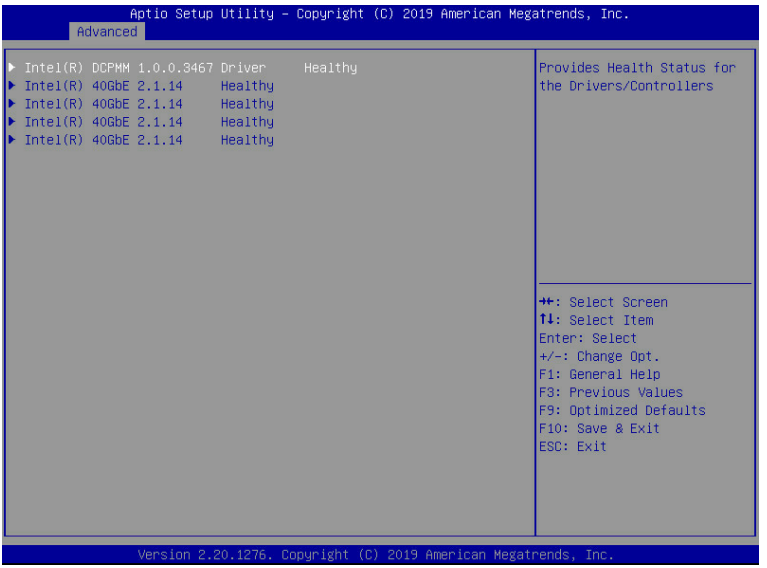
Parameter	Description
NIC Configuration	Press [Enter] to configure advanced items. ◆ Link Speed – Allows for automatic link speed adjustment. – Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. Default setting is **Auto Negotiated**. ◆ Wake On LAN – Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states. – Options available: Enabled/Disabled. Default setting is **Enabled**.
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

2-2-13 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.

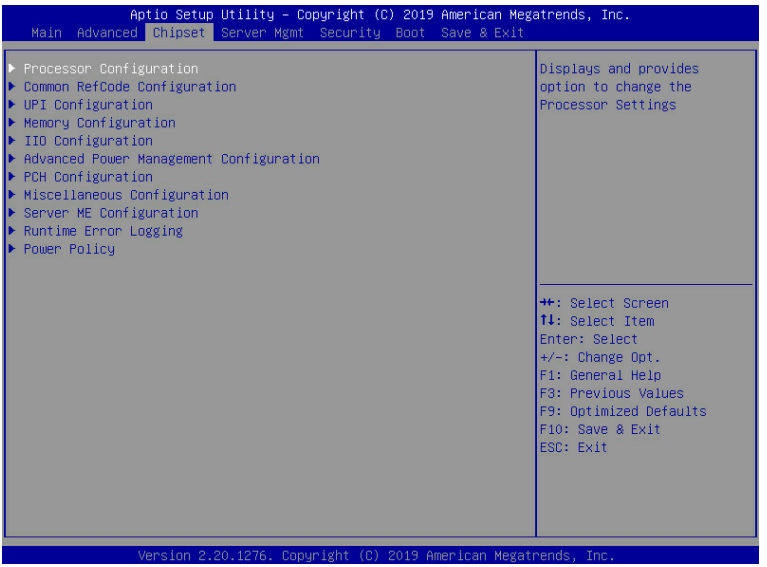
2-2-14 Driver Health



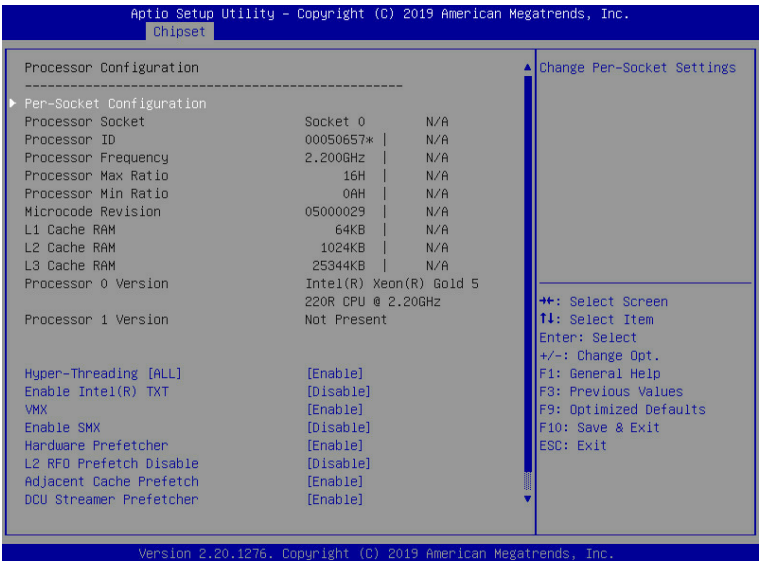
Parameter	Description
Driver Health	Displays driver health status of the devices/controllers if installed

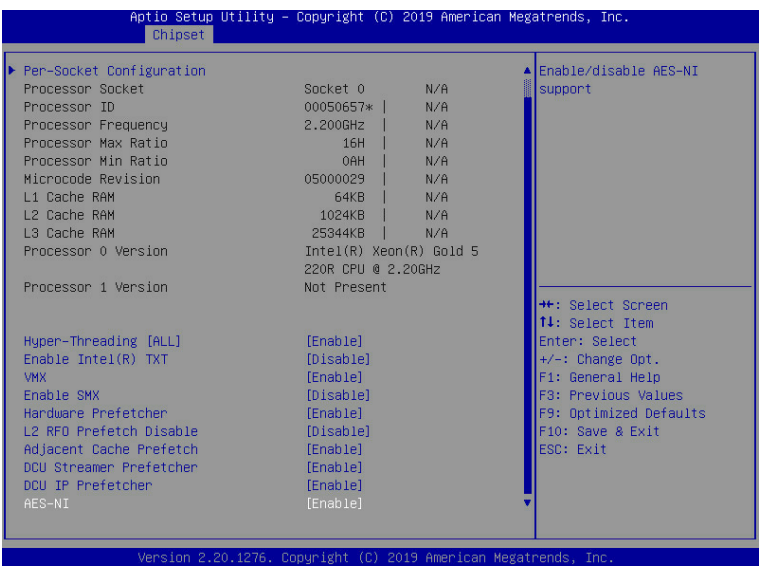
2-3 Chipset Setup Menu

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



2-3-1 Processor Configuration



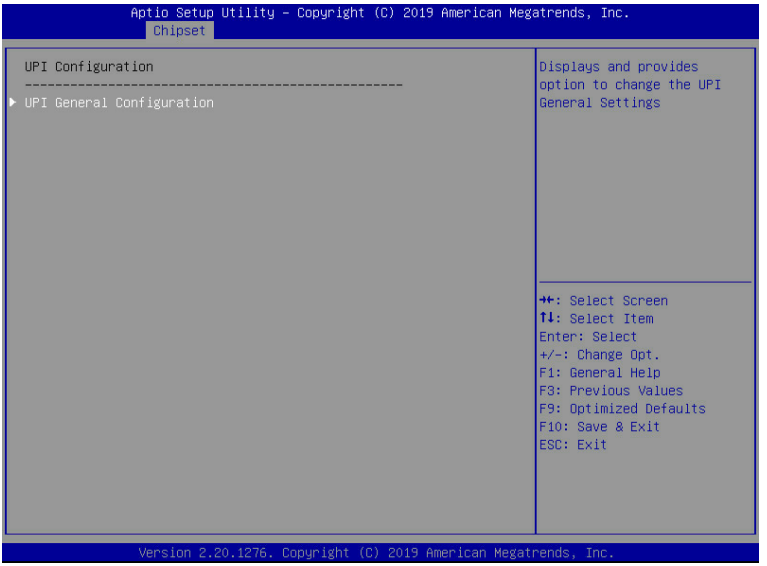


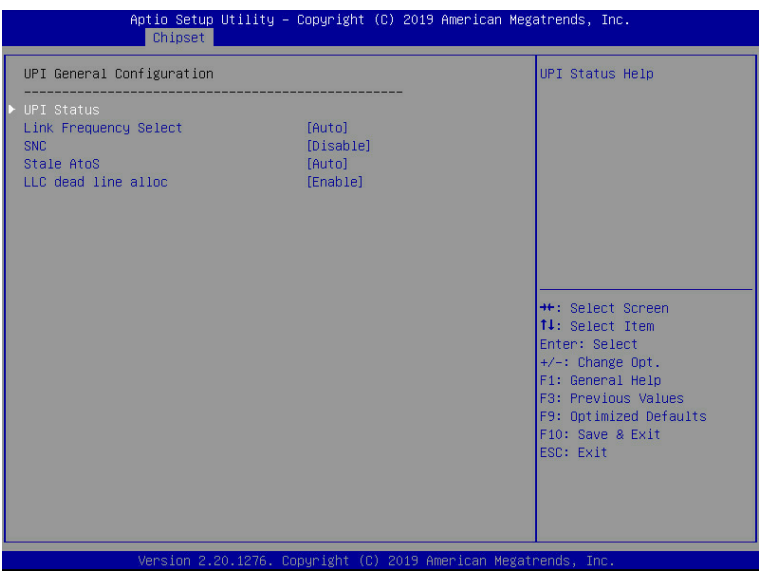
Parameter	Description
Processor Configuration	
Per-Socket Configuration	Press [Enter] to configure advanced items. ◆ CPU Socket 0/1 Configuration – Press [Enter] to configure advanced items. ◆ Core Disable Bitmap(Hex) (for CPU socket 0/1) – Number of Cores to enable. 0 means all cores. FFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.
Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM / L2 Cache RAM / L3 Cache RAM / Processor 0 Version / Processor 1 Version	Displays the technical specifications for the installed processor(s).
Hyper-Threading [All]	The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance. Options available: Enable/Disable. Default setting is **Enable**.
Enable Intel(R) TXT	Enable/Disable the Intel Trusted Execution Technology support function. Options available: Enable/Disable. Default setting is **Disable.**
VMX (Vanderpool Technology)	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable/Disable. Default setting is Enable.
Enable SMX	Enable/Disable the Secure Mode Extensions (SMX) support function. Options available: Enable/Disable. Default setting is **Disable**.
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enable/Disable. Default setting is **Disable**.
L2 RF0 Prefetch Disable	Options available: Enable/Disable. Default setting is **Disable**.
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable/Disable. Default setting is **Enable**.
DCU Streamer Prefetcher	Prefetches the next L1 data line based upon multiple loads in same cache line. Options available: Enable/Disable. Default setting is **Enable**.
DCU IP Prefetcher	Prefetches the next L1 Data line based upon sequential load history. Options available: Enable/Disable. Default setting is **Enable**.
AES-NI	Enable/Disable the AES-NI (Intel Advanced Encryption Standard New Instructions) support function. Options available: Enable/Disable. Default setting is **Enable**.

2-3-2 Common RefCode Configuration

Parameter	Description
Common RefCode Configuration	
MMIO High Base	Selects the MMIO High Base setting. Options available: 56T, 40T, 24T, 16T, 4T, 1T. Default setting is **56T**.
MMIO High Granularity Size	Selects the allocation size used to assign mmioh resources. Total mmioh space can be up to 32xgranularity. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation. Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is **256G**.
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enable, Disable. Default setting is **Auto**.
Numa (Non-Uniform Memory Access)	Enable/Disable Non-uniform Memory Access (NUMA) support to improve the system performance. Options available: Enable/Disable. Default setting is **Enable**.

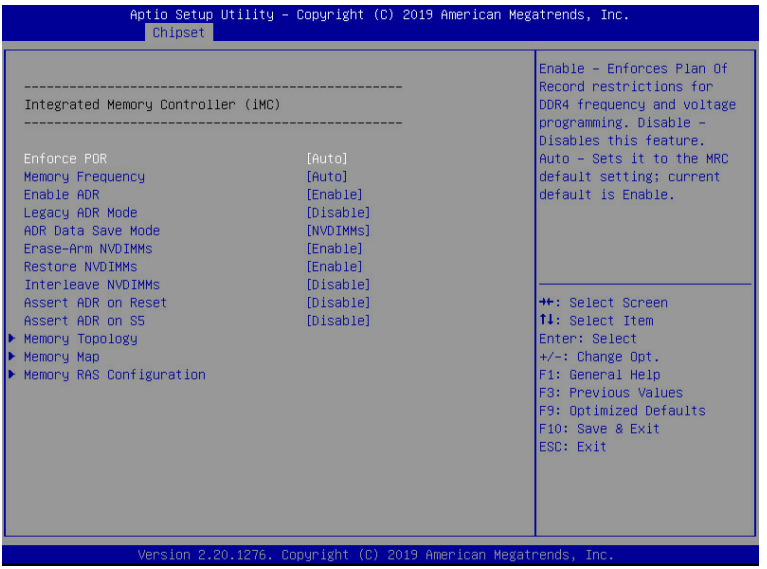
2-3-3 UPI Configuration





Parameter	Description
UPI Configuration	
UPI General Configuration	Press [Enter] to configure advanced items. ◆ UPI Status – Press [Enter] to view the UPI status. ◆ Link Frequency Select – Selects the UPI link frequency. – Options available: 9.6GB/s, 10.4GB/s, Auto. Default setting is **Auto**. ◆ SNC – Enable/Disable Sub NUMA Cluster function. – Options available: Disable, Enable, Auto. Default setting is **Disable**. ◆ Stale AtoS – Enable/Disable Stale A to S directory optimization. – Options available: Disable, Enable, Auto. Default setting is **Disable**. ◆ LLC dead line alloc – Enable/Disable fill dead lines in LLC. – Options available: Disable, Enable, Auto. Default setting is **Auto**.

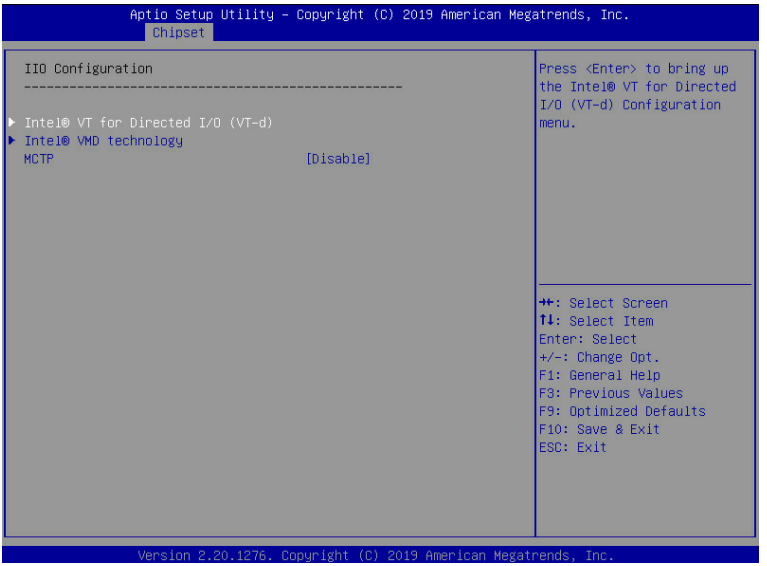
2-3-4 Memory Configuration



Parameter	Description
Integrated Memory Controller (iMC)	
Enforce POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. When set to Auto, the system sets it to the MRC default settings. Options available: Auto, POR, Disable. Default setting is **Auto**.
Memory Frequency	Configures the maximum memory frequency. Options available: Auto, 2133, 2400, 2666, 2933. Default setting is **Auto**.
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable/Disable. Default setting is **Enable**.
Legacy ADR Mode	Enable/Disable the Legacy ADR Mode. Options available: Enable/Disable. Default setting is **Disable**.
ADR Data Save Mode	Specifies the Data Save Mode for ADR. Batterybacked or Type 01 NVDIMM. Options available: Disable, Batterybacked DIMMs, NVDIMMs. Default setting is **NVDIMMs**.
Erase-ARM NVDIMMs	Enable/Disable Erasing and Arming NVDIMMs. Options available: Enable/Disable. Default setting is **Enable**.
Restore NVDIMMs	Enable/Disable Automatic restoring of NVDIMMs. Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
Interleave NVDIMMs	Controls if NVDIMMs are interleaved together or not. Options available: Enable/Disable. Default setting is **Disable**.
Assert ADR on Reset	Enable/Disable Assert ADR on Reset. Options available: Enable/Disable. Default setting is **Disable**.
Assert ADR on S5	Enable/Disable Assert ADR on S5. Options available: Enable/Disable. Default setting is **Disable**.
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map	Press [Enter] to configure advanced items. ◆ IMC Interleaving – controls the interleaving between the Integrated Memory Controllers (IMCs). – Options available: Auto, 1-way Interleave, 2-way Interleave. Default setting is **Auto**.
Memory RAS Configuration	Press [Enter] to configure advanced items. ◆ RAS Type – Displays the RAS type. ◆ Static Virtual Lockstep Mode – Enable/Disable the Static Virtual Lockstep mode. – Options available: Disable/Enable. Default setting is **Disable**. ◆ Mirror Mode – Mirror Mode will set entire 1LM/2LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch. – Options available: Disable/Enable Mirror Mode (1LM). Default setting is **Disable**. ◆ Memory Rank Sparing – Enable/Disable Memory Rank Sparing. This feature is only available on 1LM. – Options available: Disable/Enable. Default setting is **Disable**. ◆ Correctable Error Threshold – Correctable Error Threshold (1-32767) used for sparing, tagging, and leaky bucket. – Press the <+> / <-> keys to increase or decrease the desired values. ◆ SDDC Plus One – Enable/Disable SDDC Plus One. – Options available: Disable/Enable. Default setting is **Disable**.

2-3-5 IIO Configuration



Parameter	Description
IIO Configuration	
Intel® VT for Directed I/O (VT-d)	Press [Enter] to configure advanced items. ◆ Intel® VT for Directed I/O (VT-d) – Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. – Options available: Enable/Disable. Default setting is **Enable**. ◆ ACS Control – Enable: Programs ACS only to Chipset Pcie Root Ports Bridges. – Disable: Programs ACS to all PCIe bridges. – Default setting is **Enable**. ◆ Interrupt Remapping – Enable/Disable the interrupt remapping support function. – Options available: Enable/Disable. Default setting is **Enable**. ◆ PassThrough DMA – Enable/Disable the Non-Isoch VT_D Engine PassThrough DMA support function. – Options available: Enable/Disable. Default setting is **Enable**. ◆ ATS – Enable/Disable Non-Isoch VT_D Engine ATS support. – Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
Intel® VT for Directed I/O (VT-d) (continued)	◆ Post Interrupt – Enable/Disable VT_D posted interrupt. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Coherency Support (Non-Isoch) – Enable/Disable Non-Isoch VT_D Engine Coherency support. – Options available: Enable/Disable. Default setting is **Enable**.
Intel® VMD technology	Press [Enter] to configure advanced items. ◆ Intel® VMD technology ◆ Intel® VMD Configuration – Enable/Disable the Intel VMD support function. – Options available: Enable/Disable. Default setting is **Disable**.
MCTP	Enable/Disable MCTP (Management Component Transport Protocol). Options available: Enable/Disable. Default setting is **Disable**.

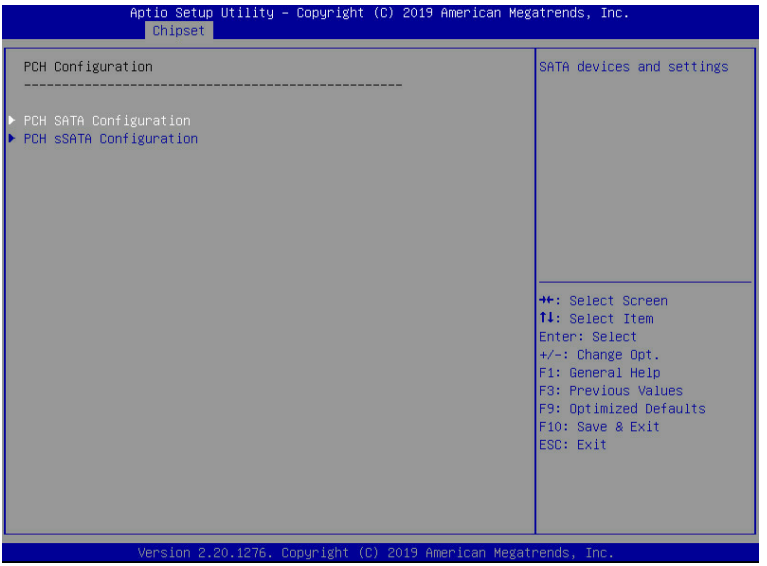
2-3-6 Advanced Power Management Configuration

Parameter	Description
Advanced Power Management Configuration	
CPU P State Control	Press [Enter] to configure advanced items. ◆ SpeedStep (Pstates) – Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Turbo Mode – When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. – Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
Hardware PM State Control	Press [Enter] to configure advanced items. ◆ Hardware P-States – When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States). – In Native mode, the processor hardware chooses a P-state based on OS guidance. – In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance). – Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is **Native Mode**.
CPU C State Control	Press [Enter] to configure advanced items. ◆ Autonomous Core C-State – Enable/Disable the Autonomous Core C-State Control. – Options available: Enable/Disable. Default setting is **Disable**. ◆ CPU C6 Report – Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced power-saving state than C1. – Options available: Disable/Enable/Auto. Default setting is **Auto**. ◆ Enhanced Halt State (C1E)(Note) – Core C1E auto promotion control. Takes effect after reboot. – Options available: Enable/Disable. Default setting is **Enable**.
Package C State Control	Configures the state for the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is **Auto**.
CPU - Advanced PM Tuning	Press [Enter] to configure advanced items. ◆ Energy Perf BIAS – Enters the Energy Perf BIAS submenu. ◆ Power Performance Tuning(Note) – Tunes the Power Performance Configuration mode. When enabled, uses IA32_ENERGY_PERF_BIAS input from the core. When disabled, uses alternate performance BIAS input from ENERGY_PERF_BIAS_CONFIG. – Options available: OS Controls EPB/BIOS Controls EPB. Default setting is **OS Controls EPB**. ◆ Energy_PERF_BIAS_CFG mode – Selects the Energy Performance Bias Configuration Mode. – Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is **Balanced Performance**. – Please note that this item is configurable when Power Performance Tuning is set to BIOS Controls EPB.

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

2-3-7 PCH Configuration

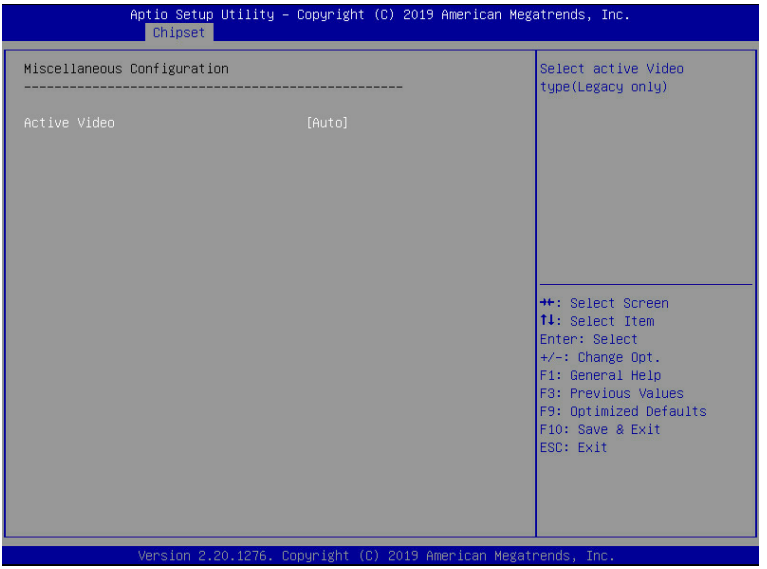


Parameter	Description
PCH Configuration	
PCH SATA Configuration	Press [Enter] to configure advanced items. ◆ SATA Controller – Enable/Disable SATA controller. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Configure SATA as – Configures on chip SATA type. – AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time. – RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time. – Options available: AHCI/RAID. Default setting is **AHCI**. ◆ Alternate Device ID on RAID(Note 1) – Enable/Disable Alternate Device ID on RAID mode. – Options available: Enable/Disable. Default setting is Disabled – Please note that this option appears when HDD is in **RAID Mode**. ◆ SATA Port 0/1/2/3/4/5/6/7 – The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.

Parameter	Description
PCH SATA Configuration (continued)	◆ Port 0/1/2/3/4/5/6/7 – Enable/Disable Port 0/1/2/3/4/5/6/7 device. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Hot Plug (for Port 0/1/2/3/4/5/6/7)(Note 2) – Enable/Disable HDD Hot-Plug function. – Options available: Enable/Disable. Default setting is **Disable**. ◆ Spin Up Device (for Port 0/1/2/3/4/5/6/7)(Note 2) – On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. – Options available: Enable/Disable. Default setting is **Disable**.
PCH sSATA Configuration	◆ sSATA Controller – Enable/Disable sSATA controller. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Configure sSATA as – Configures on chip SATA type. – AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time. – RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time. – Options available: AHCI/RAID. Default setting is **AHCI**. ◆ Alternate Device ID on RAID(Note 1) – Enable/Disable Alternate Device ID on RAID mode. – Options available: Enable/Disable. Default setting is **Disabled**. – **Please note that this option appears when HDD is in RAID Mode.** ◆ sSATA Port 0/1/2/3/4/5 – The category identifies sSATA hard drives that are installed in the computer. System will automatically detect HDD type. ◆ Port 0/1/2/3/4/5 – Enable/Disable Port 0/1/2/3/4/5 device. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Hot Plug (for Port 0/1/2/3/4/5)(Note 2) – Enable/Disable HDD Hot-Plug function. – Options available: Enable/Disable. Default setting is **Disable**. ◆ Spin Up Device (for Port 0/1/2/3/4/5)(Note 2) – On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. – Options available: Enable/Disable. Default setting is **Disabled**.

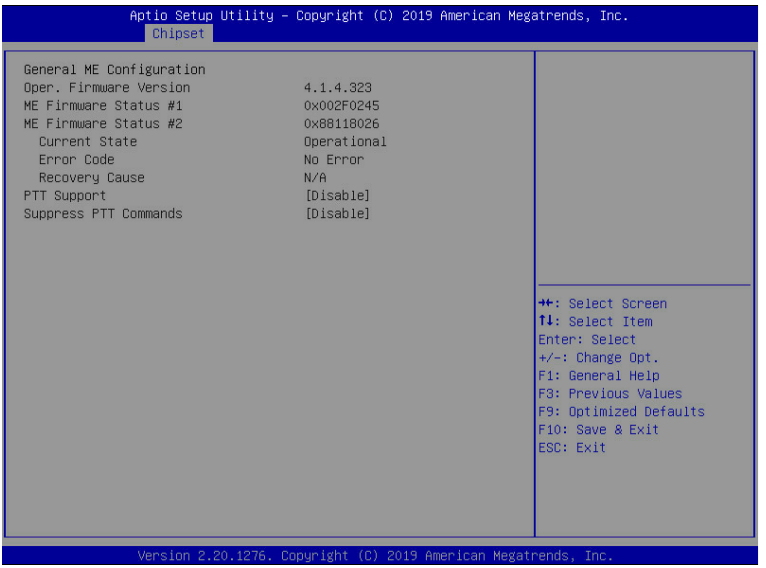
(Note 1) Only appears when HDD sets to **RAID** Mode.
(Note 2) Only Supported when HDD is in **AHCI** or **RAID** Mode.

2-3-8 Miscellaneous Configuration



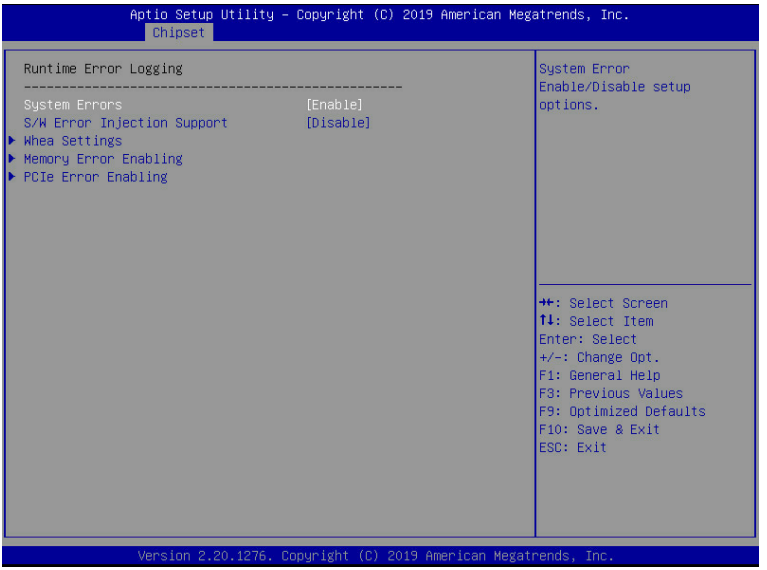
Parameter	Description
Miscellaneous Configuration	
Active Video	Selects the active video type. Options available: Auto, Onboard Device, PCIE Device. Default setting is **Auto**.

2-3-9 Server ME Configuration



Parameter	Description
General ME Configuration	
Oper. Firmware Version	Displays the operational firmware version.
ME Firmware Status #1/#2	Displays ME Firmware status information.
Current State (for ME Firmware)	Displays ME Firmware current status information.
Error Code (for ME Firmware)	Displays ME Firmware status error code.
Recovery Cause (for ME Firmware)	Displays ME Firmware recovery cause.
PTT Support	Displays if the system supports the Intel® Platform Trust Technology.
Suppress PTT Commands	Displays if the system supports to Bypass TPM2 commands submitting to PTT Firmware.

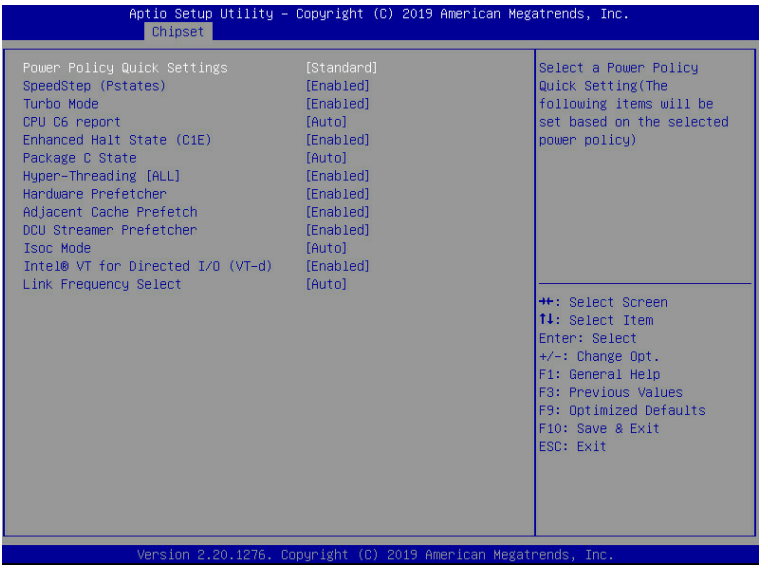
2-3-10 Runtime Error Logging Settings



Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable/Disable. Default setting is **Enable**.
S/W Error Injection Support	Enable/Disable software injection error logging function. Options available: Enable/Disable. Default setting is **Disable**.
Whea Settings	Press [Enter] to configure advanced items. ◆ WHEA (Windows Hardware Error Architecture) Support – Enable/Disable WHEA Support. – Options available: Enable/Disable. Default setting is **Enable**.
Memory Error Enabling	Press [Enter] to configure advanced items. ◆ Memory Error – Enable/Disable Memory Error. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Memory Corrected Error – Enable/Disable Memory Corrected Error. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Uncorrected Error disable Memory – Enable/Disable the Memory that triggers Uncorrected Error. – Options available: Enable/Disable. Default setting is **Disable**.

Parameter	Description
PCIe Error Enabling	Press [Enter] to configure advanced items. ◆ Corrected Error – Enables and escalates Correctable Errors to error pins. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Uncorrected Error – Enables and escalates Uncorrectable/Recoverable Errors to error pins. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Fatal Error Enable – Enables and escalates Fatal Errors to error pins. – Options available: Enable/Disable. Default setting is **Enable**. ◆ SERR Propagation – Enable/Disable SERR propagation. – Options available: Enable/Disable. Default setting is **Enable**. ◆ PERR Propagation – Enable/Disable PERR propagation. – Options available: Enable/Disable. Default setting is **Enable**.

2-3-11 Power Policy

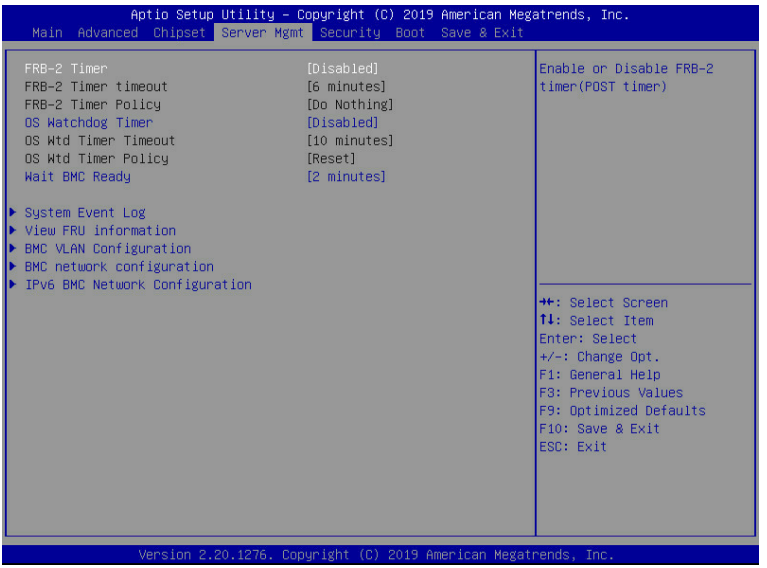


Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient, Turbo Lock.
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enable/Disable. Default setting is **Enable**.
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enable/Disable. Default setting is **Enable**.
CPU C6 report	Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced powersaving state than C1. Options available: Disable, Enable, Auto. Default setting is **Auto**.
Enhanced Halt State (C1E)(Note)	Core C1E auto promotion control. Takes effect after reboot. Options available: Enable/Disable. Default setting is Enable.

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

Parameter	Description
Package C State	Configures the state for the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is **Auto**.
Hyper-Threading [ALL]	The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance. Options available: Enable/Disable. Default setting is **Enable**.
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enable/Disable. Default setting is **Disable**.
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable/Disable. Default setting is **Enable**.
DCU Streamer Prefetcher	Prefetches the next L1 data line based upon multiple loads in same cache line. Options available: Enable/Disable. Default setting is **Enable**.
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enable, Disable. Default setting is **Auto**.
Intel® VT for Directed I/O (VT-d)	Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. Options available: Enable/Disable. Default setting is **Enable**.
Link Frequency Select	Selects the UPI link frequency. Options available: 9.6GB/s, 10.4GB/s, Auto. Default setting is **Auto**.

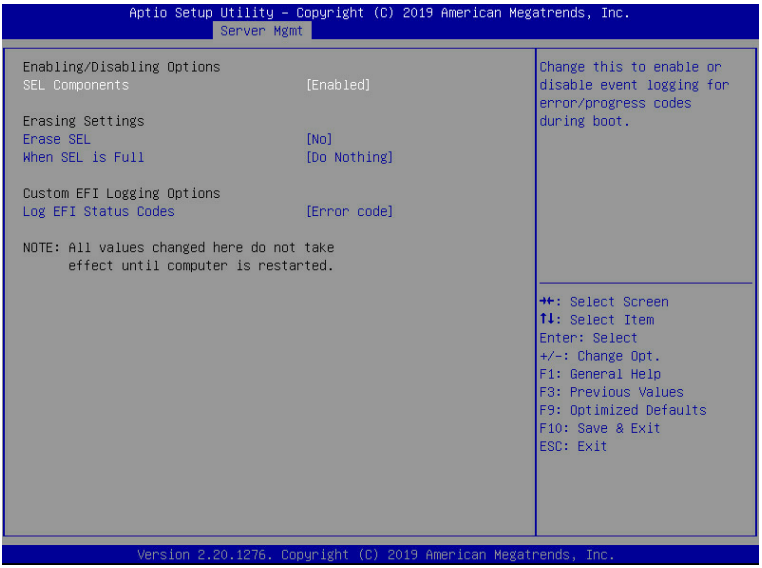
2-4 Server Management Menu



Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled/Disabled. Default setting is **Disabled**.
FRB-2 Timer timeout	Configure the FRB2 Timer timeout. Options available: 3 minutes, 4 minutes, 5 minutes, 6 minutes. Default setting is **6 minutes**. **Please note that this item is configurable when FRB-2 Timer is set to Enabled.**
FRB-2 Timer Policy	Configure the FRB2 Timer policy. Options available: Do Nothing, Reset, Power Down, Power Cycle. Default setting is **Do Nothing**. **Please note that this item is configurable when FRB-2 Timer is set to Enabled.**
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled/Disabled. Default setting is **Disabled**.
OS Wtd Timer Timeout	Configure OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is **5 minutes**. **Please note that this item is configurable when OS Watchdog Timer is set to Enabled.**

Parameter	Description
OS Wtd Timer Policy	Configure OS Watchdog Timer Policy. Options available: Reset, Do Nothing, Power Down, Power Cycle. Default setting is **Reset**. **Please note that this item is configurable when OS Watchdog Timer is set to Enabled.**
Wait BMC Ready	POST wait BMC ready and reboot system. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is **2 minutes**.
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the advanced items.
BMC VLAN Configuration	Press [Enter] to configure advanced items.
BMC network configuration	Press [Enter] to configure advanced items.
IPv6 BMC Network Configuration	Press [Enter] to configure advanced items.

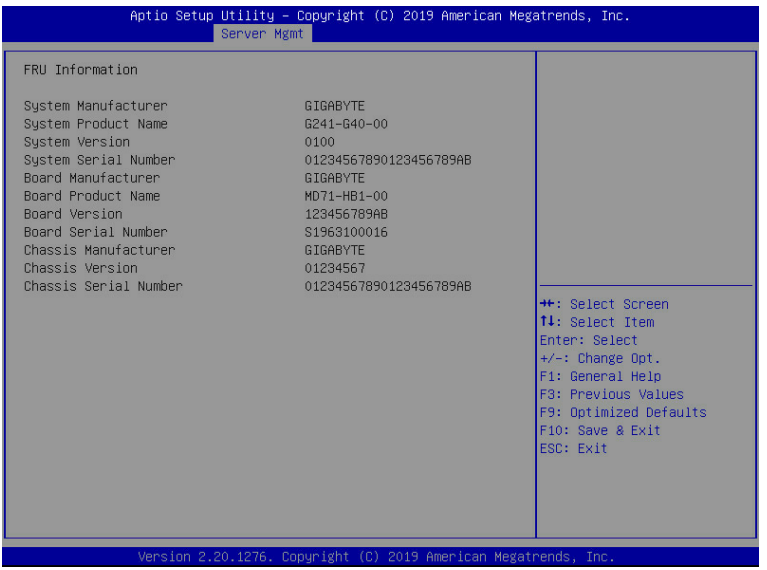
2-4-1 System Event Log



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

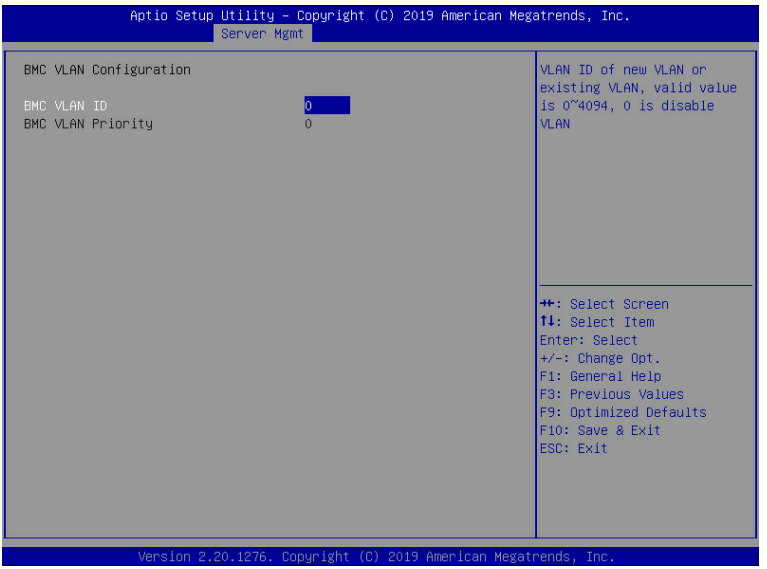
2-4-2 View FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information. Items on this window are non-configurable.



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

2-4-3 BMC VLAN Configuration



Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority will not be selected.

2-4-4 BMC Network Configuration

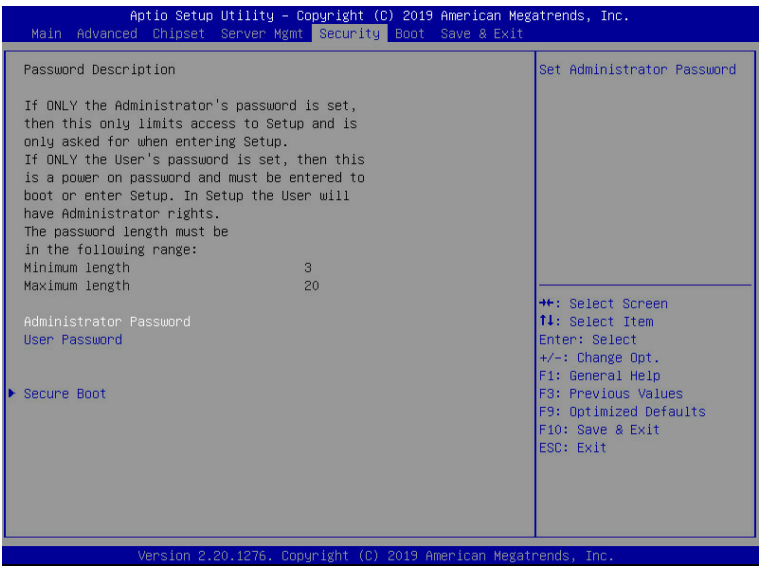
Parameter	Description
BMC network configuration	
Lan Channel 1	
Configuration Address source	Select to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase. Options available: Unspecified, Static, DynamicBmcDhcp. 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.
Real-time get BMC network address	Press [Enter] to synchronize the BMC network parameter values.

2-4-5 IPv6 BMC Network Configuration

Parameter	Description
IPv6 BMC Network Configuration	
IPv6 BMC Lan Channel 1	
IPv6 BMC Lan Option	Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase. Options available: Unspecified, Enable, Disable. Default setting is **Enable**.
IPv6 BMC Lan IP Address Source	Select 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.

2-5 Security Menu

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



There are two types of passwords that you can set:

- Administrator Password

  Entering this password will allow the user to access and change all settings in the Setup Utility.

- User Password

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

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

2-5-1 Secure Boot

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

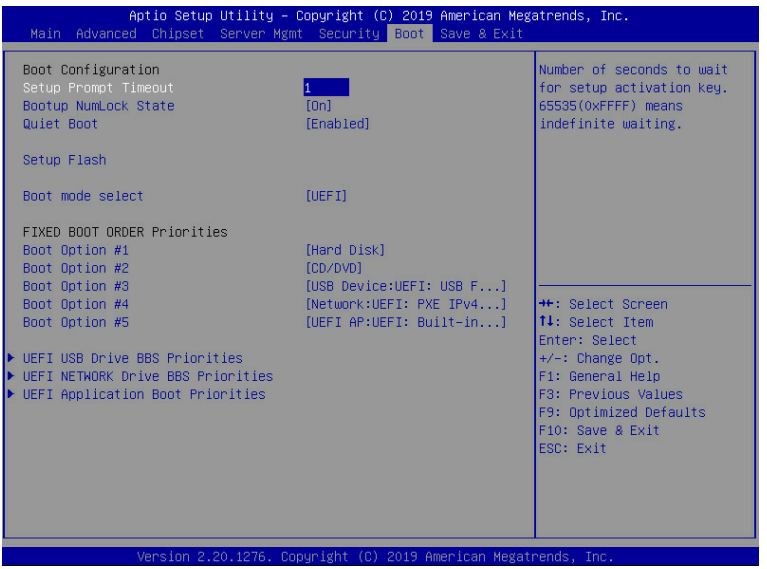
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options avaiable:Enabled/Disabled. Default setting is **Disabled**.
Secure Boot Mode(Note)	Secure Boot requires all the applications that are running during the 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	Installs all factory default keys. It will force the system in User Mode..
Reset To Setup Mode	Installs the default keys when system is in setup mode.

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

Parameter	Description
Key Management	Press [Enter] to configure advanced items. **Please note that this item is configurable when Secure Boot Mode is set to Custom.** ◆ Factory Key Provision – Allows to provision factory default Secure Boot keys when system is in Setup Mode. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ Restore Factory Keys – Installs all factory default keys. It will force the system in User Mode. – Options available: Yes/No. ◆ Enroll Efi Image – Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). ◆ 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: Set New. ◆ 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: Set New/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: Set New/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: Set New/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: Set New/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: Set New/Append.

2-6 Boot Menu

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



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

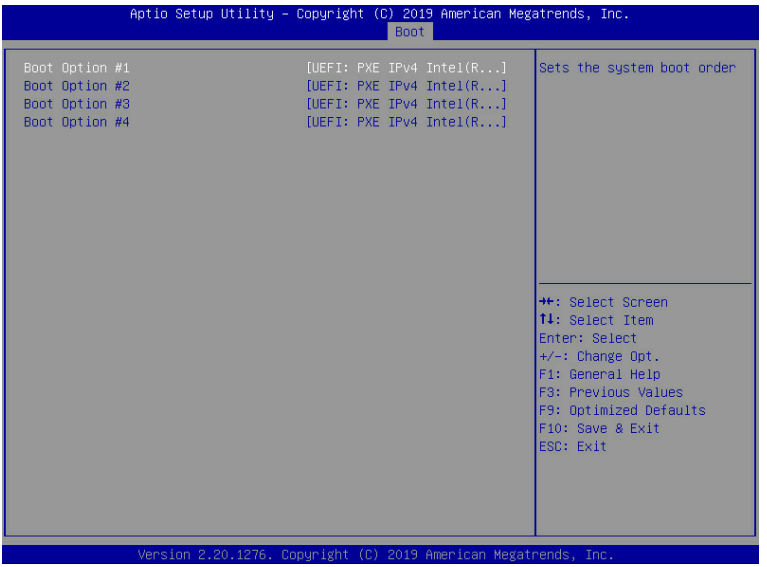
Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	Press [Enter] to configure the boot priority. By default, the server searches for boot devices in the following sequence: 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
UEFI USB Drive BBS Priorities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

2-6-1 UEFI USB Drive BBS Priorities

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

2-6-2 UEFI NETWORK Drive BBS Priorities

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

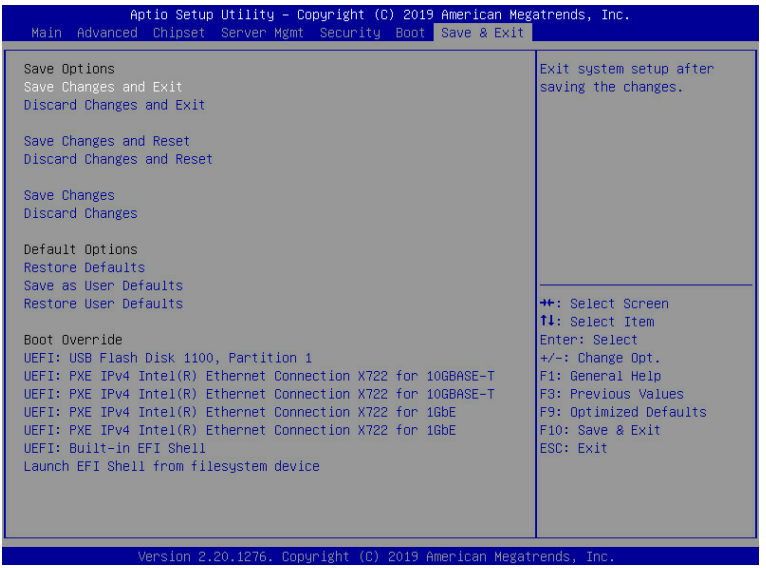


2-6-3 UEFI Application Boot Priorities

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

2-7 Save & Exit Menu

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



Parameter	Description
Save Options	
Save 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 and Reset	Restarts the system after saving the changes made. Options available: Yes/No.
Discard Changes and Reset	Restarts the system without saving any changes. Options available: Yes/No.
Save Changes	Saves changes made in the BIOS setup. Options available: Yes/No.
Discard Changes	Discards changes made and closes the BIOS setup. Options available: Yes/No.

Parameter	Description
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.
Save as User Defaults	Saves the changes made as the user default settings. Options available: Yes/No.
Restore User Defaults	Loads the user default settings for all BIOS setup parameters. Options available: Yes/No.
Boot Override	Press [Enter] to configure the device as the boot-up drive.

2-8 BIOS POST Codes

2-8-1 AMI Standard - PEI

PEI_CORE_STARTED	0x10
PEI_CAR_CPU_INIT	0x11
PEI_CAR_NB_INIT	0x15
PEI_CAR_SB_INIT	0x19
PEI_MEMORY_SPD_READ	0x2B
PEI_MEMORY_PRESENCE_DETECT	0x2C
PEI_MEMORY_TIMING	0x2D
PEI_MEMORY_CONFIGURING	0x2E
PEI_MEMORY_INIT	0x2F
PEI_MEMORY_INSTALLED	0x31
PEI_CPU_INIT	0x32
PEI_CPU_CACHE_INIT	0x33
PEI_CPU_AP_INIT	0x34
PEI_CPU_BSP_SELECT	0x35
PEI_CPU_SMM_INIT	0x36
PEI_MEM_NB_INIT	0x37
PEI_MEM_SB_INIT	0x3B
PEI_DXE_IPL_STARTED	0x4F
DXE_CORE_STARTED	0x60
//Recovery	
PEI_RECOVERY_AUTO	0xF0
PEI_RECOVERY_USER	0xF1
PEI_RECOVERY_STARTED	0xF2
PEI_RECOVERY_CAPSULE_FOUND	0xF3
PEI_RECOVERY_CAPSULE_LOADED	0xF4
//S3	
PEI_S3_STARTED	0xE0
PEI_S3_BOOT_SCRIPT	0xE1
PEI_S3_VIDEO_REPOST	0xE2
PEI_S3_OS_WAKE	0xE3

2-8-2 AMI Standard - DXE

DXE_CORE_STARTED	0x60
DXE_NVRAM_INIT	0x61
DXE_SBRUN_INIT	0x62
DXE_CPU_INIT	0x63
DXE_NB_HB_INIT	0x68
DXE_NB_INIT	0x69
DXE_NB_SMM_INIT	0x6A

DXE_SB_INIT	0x70
DXE_SB_SMM_INIT	0x71
DXE_SB_DEVICES_INIT	0x72
DXE_ACPI_INIT	0x78
DXE_CSM_INIT	0x79
DXE_BDS_STARTED	0x90
DXE_BDS_CONNECT_DRIVERS	0x91
DXE_PCI_BUS_BEGIN	0x92
DXE_PCI_BUS_HPC_INIT	0x93
DXE_PCI_BUS_ENUM	0x94
DXE_PCI_BUS_REQUEST_RESOURCES	0x95
DXE_PCI_BUS_ASSIGN_RESOURCES	0x96
DXE_CON_OUT_CONNECT	0x97
DXE_CON_IN_CONNECT	0x98
DXE_SIO_INIT	0x99
DXE_USB_BEGIN	0x9A
DXE_USB_RESET	0x9B
DXE_USB_DETECT	0x9C
DXE_USB_ENABLE	0x9D
DXE_IDE_BEGIN	0xA0
DXE_IDE_RESET	0xA1
DXE_IDE_DETECT	0xA2
DXE_IDE_ENABLE	0xA3
DXE_SCSI_BEGIN	0xA4
DXE_SCSI_RESET	0xA5
DXE_SCSI_DETECT	0xA6
DXE_SCSI_ENABLE	0xA7
DXE_SETUP_VERIFYING_PASSWORD	0xA8
DXE_SETUP_START	0xA9
DXE_SETUP_INPUT_WAIT	0xAB
DXE_READY_TO_BOOT	0xAD
DXE_LEGACY_BOOT	0xAE
DXE_EXIT_BOOT_SERVICES	0xAF
RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN	0xB0
RT_SET_VIRTUAL_ADDRESS_MAP_END	0xB1
DXE_LEGACY_OPROM_INIT	0xB2
DXE_RESET_SYSTEM	0xB3
DXE_USB_HOTPLUG	0xB4
DXE_PCI_BUS_HOTPLUG	0xB5
DXE_NVRAM_CLEANUP	0xB6
DXE_CONFIGURATION_RESET	0xB7

2-8-3 AMI Standard - ERROR

PEI_MEMORY_INVALID_TYPE	0x50
PEI_MEMORY_INVALID_SPEED	0x50
PEI_MEMORY_SPD_FAIL	0x51
PEI_MEMORY_INVALID_SIZE	0x52
PEI_MEMORY_MISMATCH	0x52
PEI_MEMORY_NOT_DETECTED	0x53
PEI_MEMORY_NONE_USEFUL	0x53
PEI_MEMORY_ERROR	0x54
PEI_MEMORY_NOT_INSTALLED	0x55
PEI_CPU_INVALID_TYPE	0x56
PEI_CPU_INVALID_SPEED	0x56
PEI_CPU_MISMATCH	0x57
PEI_CPU_SELF_TEST_FAILED	0x58
PEI_CPU_CACHE_ERROR	0x58
PEI_CPU_MICROCODE_UPDATE_FAILED	0x59
PEI_CPU_NO_MICROCODE	0x59
PEI_CPU_INTERNAL_ERROR	0x5A
PEI_CPU_ERROR	0x5A
PEI_RESET_NOT_AVAILABLE	0x5B
//Recovery	
PEI_RECOVERY_PPI_NOT_FOUND	0xF8
PEI_RECOVERY_NO_CAPSULE	0xF9
PEI_RECOVERY_INVALID_CAPSULE	0xFA
//S3 Resume	
PEI_MEMORY_S3_RESUME_FAILED	0xE8
PEI_S3_RESUME_PPI_NOT_FOUND	0xE9
PEI_S3_BOOT_SCRIPT_ERROR	0xEA
PEI_S3_OS_WAKE_ERROR	0xEB
DXE_CPU_ERROR	0xD0
DXE_NB_ERROR	0xD1
DXE_SB_ERROR	0xD2
DXE_ARCH_PROTOCOL_NOT_AVAILABLE	0xD3
DXE_PCI_BUS_OUT_OF_RESOURCES	0xD4
DXE_LEGACY_OPROM_NO_SPACE	0xD5
DXE_NO_CON_OUT	0xD6
DXE_NO_CON_IN	0xD7
DXE_INVALID_PASSWORD	0xD8
DXE_BOOT_OPTION_LOAD_ERROR	0xD9
DXE_BOOT_OPTION_FAILED	0xDA
DXE_FLASH_UPDATE_FAILED	0xDB
DXE_RESET_NOT_AVAILABLE	0xDC

2-8-4 Intel UPI POST Codes

Initialize KTIRC inuput structure default values	0xA0
Collect info such as SBSP, Boot Mode, Reset type etc	0xA1
Setup IO SADs in SBSP to access the config space	0xA2
Setup up minimum path between SBSP & other sockets Add the node to the tree Parse the LEP of the discovered socket Check if the system has the supported topology Setup the boot path for the parent which is not directly connected to Legacy CPU Setup path from SBSP to the new found node	0xA3
Setup IO SADs in PBSP to access the config space	0xA4
System configurations that require some kind of reset	0xA5
Sync up with PBSPs	0xA6
Topology discovery and route calculation	0xA7
Program final route	0xA8
Program final IO SAD setting	0xA9
Protocol layer and other Uncore settings	0xAA
Transition links to full speed operation	0xAB
Phy layer settings	0xAC
Link layer settings	0xAD
Coherency Settings	0xAE
KTIRC is done	0xAF

2-8-5 Intel UPI Error Codes

When system BSP tries to setup path for remote sockets or sends a Boot_Go command to remote socket in SetupSbspPathToAllSockets() or SyncUpPbspForReset(). If the remote socket(s) hasn't checked-in, assert; it is a fatal condition, this error will be logged. No retry. *RC Behavior: System Halt*	0xD8
When SBSP tries to add this remote socket into system topology tree in SetupSbspPathToAllSockets(), there are some errors occur in the data structure. No retry. *RC Behavior: The current Socket is not added to the tree.* When SBSP setups the boot path for the parent which is not directly connected to Legacy CPU in SetupSbspPathToAllSockets(). The Child is not an immediate neighbor of Parent. No retry.	0xDA
SAD setup error *RC Behavior: System Halt*	0xDB

Unsupported topology *RC Behavior: System Halt*	0xDC
SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry. *RC Behavior: System Halt*	0xDD

2-8-6 Intel MRC POST Codes

Detect DIMM population	0xB0
Set DDR frequency	0xB1
Gather remaining SPD data	0xB2
Program registers on the memory controller level	0xB3
Evaluate RAS modes and save rank information	0xB4
Program registers on the channel level	0xB5
DDRIO Initialization	0xB6
Train DDR	0xB7
Initialize CLTT/OLTT	0xB8
Hardware memory test and init	0xB9
Execute memory init	0xBA
Program memory map and interleaving	0xBB
Program RAS configuration	0xBC
Rank margin tool	0xBD
MRC is done	0xBF

2-8-7 Intel MRC Error Codes

No memory was detected	0xE8
Memory test failure	0xEB
Different dimm types are detected installed in the system	0xED
Number of HAs found in system greater than MAX_HA defined in MRC build	0xEE
Indicates a CLTT table structure error	0xEF
Invalid VR mode, unable to set DRAM VDD	0xF0
Failure occurred reserving memory for IOT	0xF1
Reference code assert	0xF2
Unsupported MC frequency set	0xF3
Unable to get current MC frequency	0xF4

2-8-8 Intel PM POST Codes

Start of PPM structure initialization	0xD0
PPM CSR programming	0xD1
PPM MSR programming	0xD2
Start of PState transition init	0xD3
PPM exit	0xD4
PPM On ready to boot event	0xD5

2-8-9 Intel PM POST Codes

Start of IIO early Initialization	0xE0
Pre Link training	0xE1
Start of Gen3 EQ training	0xE2
Start of PState transition init	0xE3
Gen3 parameters override	0xE4
End of IIO Early Initialization	0xE5
Start of IIO Late initialization	0xE6
PCIE port initialization	0xE7
IOAPIC initialization	0xE8
VTD initialization	0xE9
IOAT initialization	0xEA
DFX initialization	0xEB
NTB initialization	0xEC
Security Initialization	0xED
IIO late initialization	0xEE
IIO On ready to boot event	0xEF

2-9 BIOS POST Beep code (AMI standard)

2-9-1 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed.
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	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

2-9-2 DXE Beep Codes

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