

GIGABYTE™

MW22-SE0

Intel® Socket LGA1151 processor motherboard

User Manual

Rev. 2.0

Copyright

© 2019 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.

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

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE.

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

Documentation Classifications

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

- User Manual: detailed information & steps about the installation, configuration and use 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.

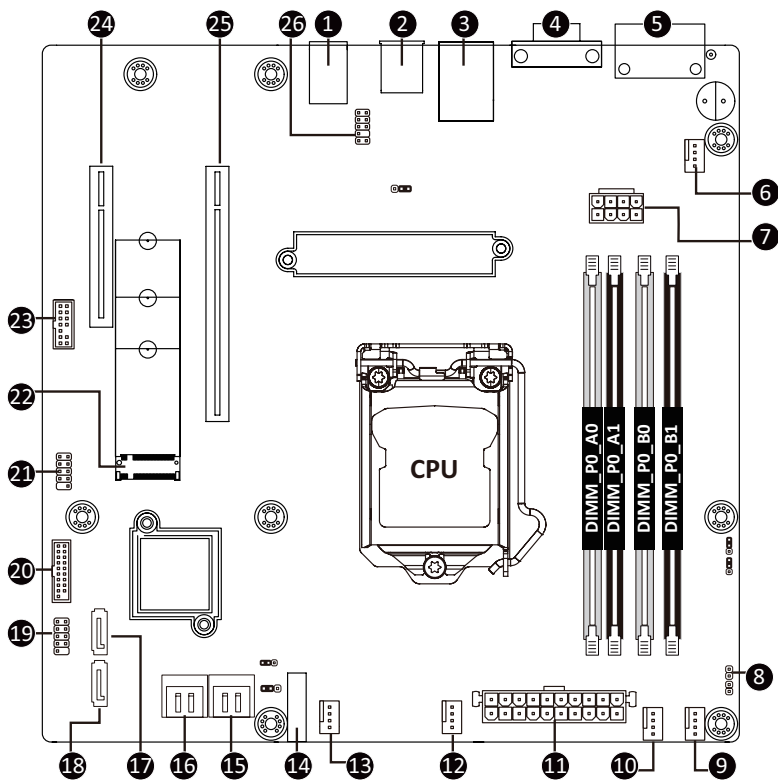
For any general sales or marketing enquires, you may message GIGABYTE server directly by email: server.grp@gigabyte.com.

Table of Contents

MW22-SE0 Motherboard Layout	5
Block Diagram	7
Chapter 1 Hardware Installation	8
1-1 Installation Precautions	8
1-2 Product Specifications	9
1-3 Installing the CPU and CPU Cooler	11
1-3-1 Installing the CPU	11
1-3-2 Installing the CPU Cooler	13
1-4 Installing the Memory	14
1-4-1 Installing a Memory	14
1-5 Installing the M.2 SSD Module	15
1-6 Back Panel Connectors	16
1-7 Internal Connectors	17
1-8 Jumper Settings	23
Chapter 2 BIOS Setup	24
2-1 The Main Menu	26
2-2 Advanced Menu	29
2-2-1 CPU Configuration	30
2-2-2 PCI Subsystem Settings	32
2-2-3 Power & Performance Settings	33
2-2-4 Server ME Configuration	36
2-2-5 Trusted Computing	37
2-2-6 Serial Port Console Redirection	38
2-2-7 Network Stack Configuration	41
2-2-8 USB Configuration	42
2-2-9 Runtime Error Logging Settings	43
2-2-10 Super IO Configuration	44
2-2-11 Hardware Monitor	45
2-2-12 S5 RTC Wake Settings	46
2-2-13 NVMe Configuration	47
2-2-14 OffBoard SATA Controller Configuration	48
2-2-15 Chipset Configuration	49
2-2-16 iSCSI Configuration	50
2-2-17 Intel(R) I219-LM Ethernet Connection	51
2-2-18 VLAN Configuration	53
2-2-19 Driver Health	54

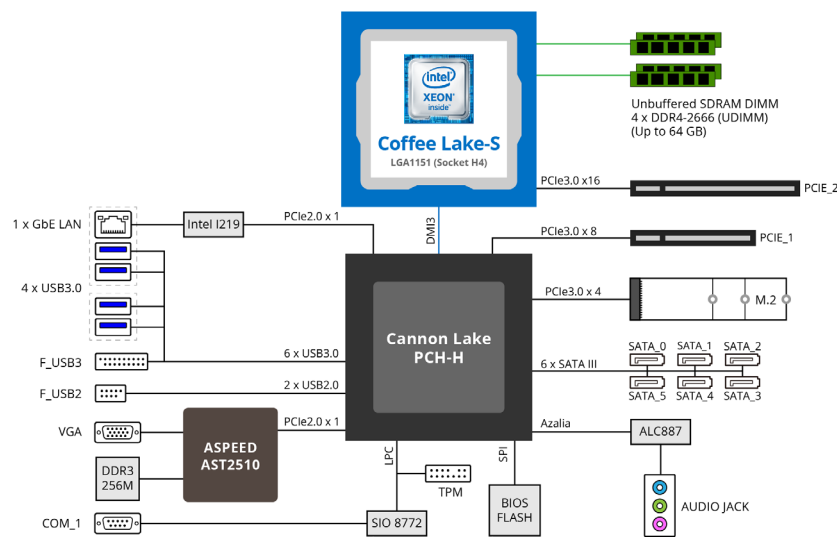
2-3	Chipset Setup Menu.....	55
2-3-1	Syetem Agent (SA) Configuration.....	56
2-3-2	PCH-IO Configuration	57
2-4	Security Menu	59
2-4-1	Secure Boot	60
2-5	Boot Menu.....	62
2-5-1	UEFI USB Drive BBS Priorities	64
2-5-2	UEFI NETWORK Drive BBS Priorities	65
2-5-3	UEFI Application Boot Priorities	66
2-6	Save & Exit Menu.....	67
2-7	BIOS POST Codes	69
2-7-1	AMI Standard - PEI.....	69
2-7-2	AMI Standard - DXE	69
2-7-3	AMI Standard - ERROR	71
2-7-4	Intel UPI POST Codes.....	72
2-7-5	Intel UPI Error Codes	72
2-7-6	Intel MRC POST Codes	73
2-7-7	Intel MRC Error Codes	73
2-7-8	Intel PM POST Codes	74
2-7-9	Intel PM POST Codes	74
2-8	BIOS POST Beep code (AMI standard)	75
2-8-1	PEI Beep Codes	75
2-8-2	DXE Beep Codes	75

MW22-SE0 Motherboard Layout



Item	Code	Description
1	HD_AUDIO	Audio Connectors
2	R_USB3	USB3.0 Ports
3	USB3_LAN1	GbE Ethernet LAN Port (top) / USB3.0 Ports (bottom)
4	VGA_1	VGA Port
5	COM1	Serial Port
6	SYS_FAN1	System Fan Connector #1
7	P12V_AUX	8 Pin Power Connector (for CPU, DDR)
8	CASE_OPEN	Case Open Intrusion Alert Header
9	SYS_FAN4	System Fan Connector #4
10	SYS_FAN3	System Fan Connector #3
11	ATX1	24 Pin Main Power Connector
12	CPU0_FAN	CPU Fan Connector
13	SYS_FAN2	System Fan Connector #2
14	BAT	Battery Socket
15	SATA_0_1	SATA III 6Gb/s Connectors
16	SATA_2_3	SATA III 6Gb/s Connectors
17	SATA4	SATA III 6Gb/s Connector #4
18	SATA5	SATA III 6Gb/s Connector #5
19	FP_1	Front Panel Header
20	F_USB3	USB 3.0 Connector
21	F_USB2	USB 2.0 Connector
22	M2_0	M.2 Slot (PCIe Gen3 x4, Support NGFF-2280, M-Key)
23	TPM	TPM Module Connector
24	PCIE_1	PCI Express x8 Slot (Gen3 x4 Signal)
25	PCIE_2	PCI Express x16 Slot (Gen3 x16 Signal)
26	F_AUDIO	Front Audio Header

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	<ul style="list-style-type: none"> ◆ Intel® Xeon® Processor E-2100/ E-2200 series ◆ 8th Gen. Intel Core™ i3/ Pentium®/ Celeron® Processors
 Chipset	<ul style="list-style-type: none"> ◆ Intel® C242 Express Chipset
 Memory	<ul style="list-style-type: none"> ◆ 4 x DIMM slots ◆ Dual channel memory architecture ◆ Supports 1.2V DDR4 memory ◆ ECC UDIMM modules supported ◆ Up to 64GB ◆ Supported speeds: 2666/2400 MHz
 Onboard Graphics	<ul style="list-style-type: none"> ◆ Integrated in Aspeed® AST2510 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp
 Audio	<ul style="list-style-type: none"> ◆ Realtek® ALC887 Controller
 LAN	<ul style="list-style-type: none"> ◆ 1 x GbE LAN port (Intel® I219LM)
 Expansion Slots	<ul style="list-style-type: none"> ◆ 1 x PCI Express x16 slot; running at Gen3 x16 ◆ 1 x PCI Express x8 slot; running at Gen3 x4 ◆ 1 x M.2 slot: <ul style="list-style-type: none"> - M-key - PCIe Gen3 x4 per slot - Supports NGFF-2280/2260/2242 cards - Intel® Optane™ Memory Ready
 Storage Interface	<ul style="list-style-type: none"> ◆ 6 x SATA III 6Gb/s connectors
 RAID	<ul style="list-style-type: none"> ◆ Intel® SATA RAID 0/1/10/5
 Internal I/O Connectors	<ul style="list-style-type: none"> ◆ 1 x 24-pin ATX main power connector ◆ 1 x 8-pin ATX 12V power connector ◆ 6 x SATA III 6Gb/s ports ◆ 1 x CPU fan header ◆ 4 x System fan headers ◆ 1 x USB 3.0 header ◆ 1 x USB 2.0 header ◆ 1 x Front panel header ◆ 1 x TPM header ◆ 1 x Case Open header
 Rear I/O Connectors	<ul style="list-style-type: none"> ◆ 1 x Serial port ◆ 1 x VGA port ◆ 1 x RJ45 ports ◆ 4 x USB 3.0 ports ◆ 3 x Audio Jacks
 TPM	<ul style="list-style-type: none"> ◆ 1 x TPM header



Form Factor

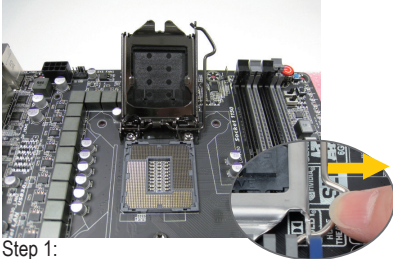
- ◆ microATX
- ◆ 244mm W x 244mm D

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

B. Follow the steps below to correctly install the CPU into the motherboard CPU socket.

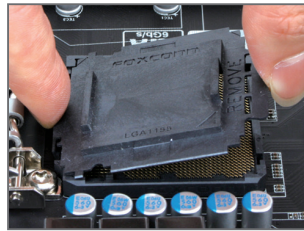


Before installing the CPU, make sure to turn off the computer and unplug the power cord from the power outlet power plug to prevent any damage to the CPU.



Step 1:

Gently press the CPU socket lever handle down and away from the socket with your finger. Then completely lift the CPU socket lever and the metal load plate will be lifted as well.



Step 2:

Remove the CPU socket cover as shown. Hold your index finger down on the rear grip of the socket cover and use your thumb to lift up the front edge (next to the "REMOVE" mark) and then remove the cover. (DO NOT touch socket contacts. To protect the CPU socket, always replace the protective socket cover when the CPU is not installed.)



Step 3:

Hold the CPU with your thumb and index fingers. Align the CPU pin one (triangle marking) with the pin one corner of the CPU socket (or you may align the CPU notches with the socket alignment keys). Gently insert the CPU into position.



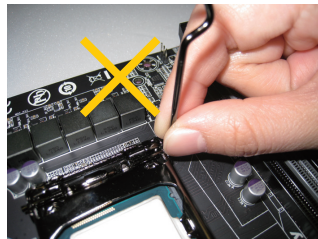
Step 4:

Once the CPU is properly inserted, use one hand to hold the socket lever and use the other to lightly replace the load plate. When replacing the load plate, make sure the front end of the load plate is under the shoulder screw.



Step 5:

Push the CPU socket lever back into its locked position.



NOTE:

Hold the CPU socket lever by the handle, not by the lever base position.

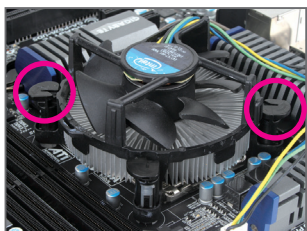
1-3-2 Installing the CPU Cooler

Follow the steps below to correctly install the CPU cooler on the motherboard. (The following procedure uses Intel® boxed cooler as the example cooler.)



Step 1:

Apply a thin, even layer of thermal paste onto the surface of the installed CPU.



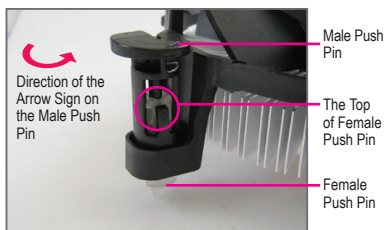
Step 3:

Place the cooler atop the CPU, aligning the four push pins through the pin holes on the motherboard. Push down on the push pins diagonally.




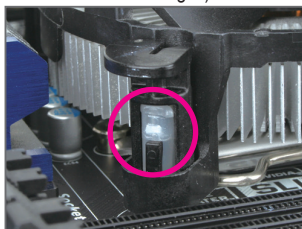
Step 5:

After the installation, check the back of the motherboard. If the push pin is inserted as the picture above shows, the installation is complete.



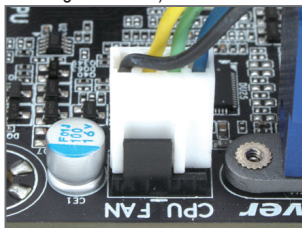
Step 2:

Before installing the cooler, note the direction of the arrow sign  on the male push pin. (Turning the push pin along the direction of the arrow is for removing the cooler, and the opposite direction is for installing it.)



Step 4:

You should hear a "click" when pushing down each push pin. Check that the Male and Female push pins are joined closely. (Refer to your CPU cooler installation manual for instructions on installing the cooler.)



Step 6:

Finally, attach the power connector of the CPU cooler to the CPU fan header (CPU_FAN) on the motherboard.



Use extreme care when removing the CPU cooler because the thermal grease/tape between the CPU cooler and CPU may adhere to the CPU. Inadequately removing the CPU cooler may damage the CPU.

1-4 Installing the Memory



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

- Make sure that the motherboard supports the memory. It is recommended 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 Installing a Memory



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

Be sure to install DDR4 UDIMMs on this motherboard.

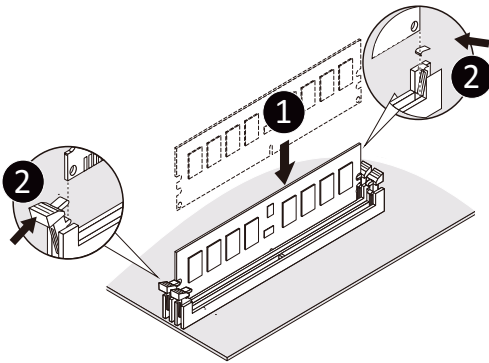
Installation Step:

Step 1. Insert the UDIMM memory module vertically into the UDIMM slot, and push it down.

Step 2. Close the plastic clip at both edges of the UDIMM slots to lock the UDIMM module.

Note: For dual-channel operation, UDIMMs must be installed in matched pairs.

Step 3. Reverse the installation steps when you wish to remove the UDIMM module.



Type	Ranks Per DIMM and Data Width	Supported Voltage	Speed (MT/s); Slot Per Channel(SPC) and DIMM Per Channel (DPC)	
			2 Slot Per Channel	
			1DPC	2DPC
UDIMM Unbuffered DDR4 ECC	SR, DR	1.2V	2133/ 2400/ 2666	2133/ 2400/ 2666
UDIMM Unbuffered DDR4 non-ECC	SR, DR	1.2V	2133/ 2400/ 2666	2133/ 2400/ 2666

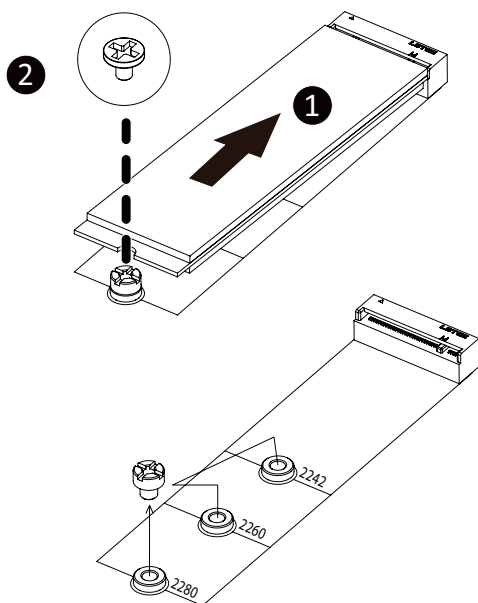
- All channels in system run at the fastest common frequency.
- Mixing ECC and non-ECC UDIMMs anywhere on the platform is not supported.
- UDIMM 2666 two DIMMs per channel (2DPC) is supported when channel is populated with the same UDIMM memory module.

1-5 Installing the M.2 SSD Module

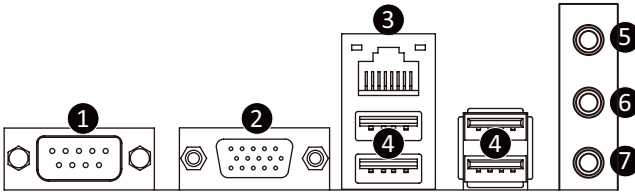
Follow the steps below to install a M.2 SSD module on your motherboard.

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



1 Serial Port

Connects to serial-based mouse or data processing devices.

2 VGA Port

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

3 RJ-45 LAN Port

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.

4 USB 3.0 Port

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.

5 Line In Jack (Blue)

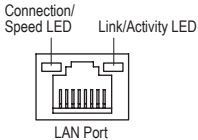
The default Line in jack. Use this audio jack for line in devices such as an optical drive, walkman, etc

6 Line Out Jack (Green)

The default Line Out jack. Use this audio jack for a headphone or 2-channel speaker. This jack can be used to connect front speakers in a 4/5.1/7.1-channel audio configuration.

7 Mic In (Pink)

The default MIC In jack. A microphone can be connected to the MIC In jack.



Connection/Speed LED:

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

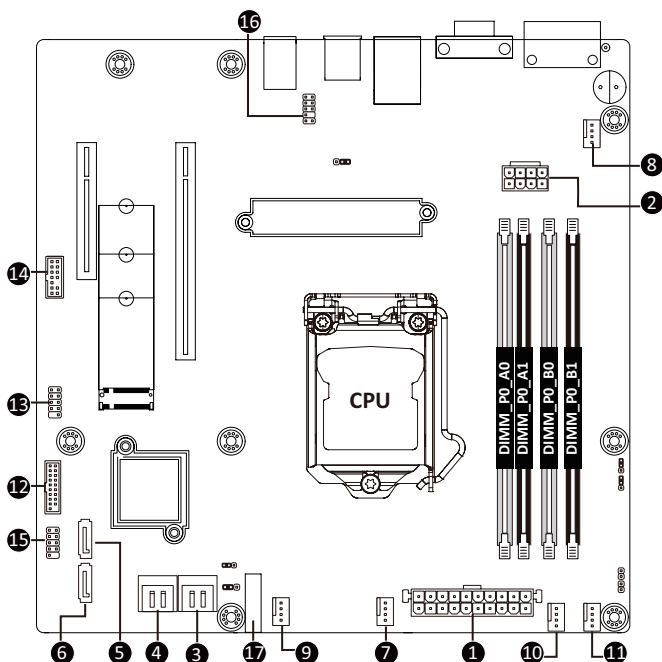
Activity LED:

State	Description
Blinking	Data transmission or receiving is occurring
Off	No data transmission or receiving is occurring



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

1-7 Internal Connectors



1) ATX	11) SYS_FAN4
2) ATX_12V	12) F_USB3
3) SATA0/ SATA1	13) F_USB2
4) SATA2/ SATA3	14) TPM
5) SATA4	15) FP_1
6) SATA5	16) F_AUDIO
7) CPU_FAN	17) BAT
8) SYS_FAN1	
9) SYS_FAN2	
10) SYS_FAN3	



Read the following guidelines before connecting external devices:

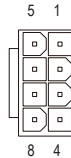
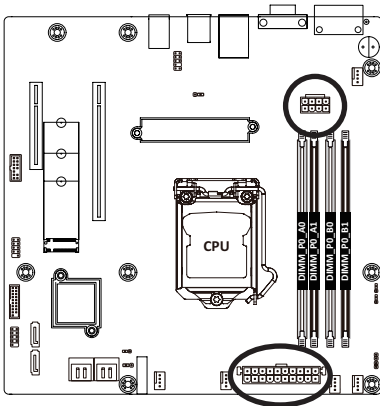
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the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

1/2) ATX/ATX_12V (2x12 Main Power Connector and 2x4 12V Power Connector)

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

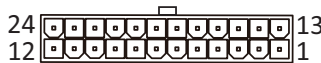


To meet expansion requirements, it is recommended that a power supply that can withstand high power consumption be used (500W or greater). If a power supply is used that does not provide the required power, the result can lead to an unstable or unbootable system.



ATX_12V

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

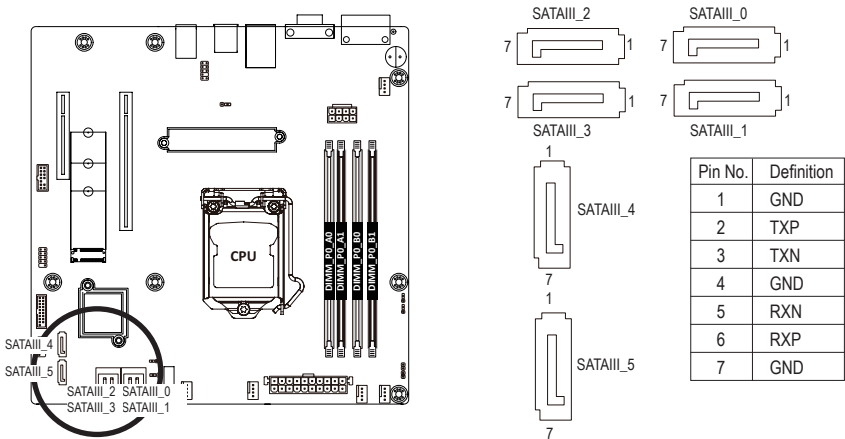


ATX

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

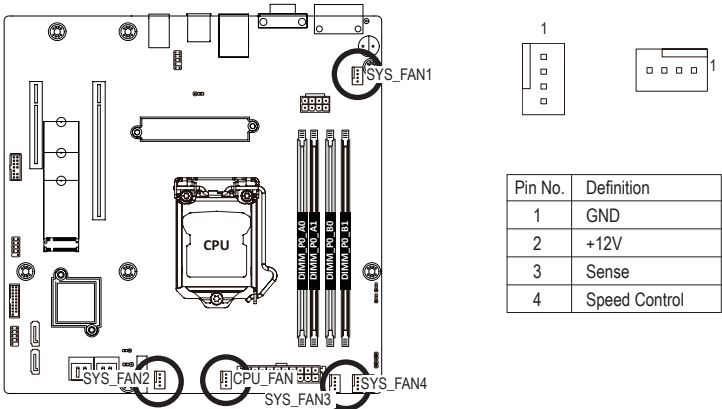
3/4/5/6) SATA0/SATA1/SATA2/SATA3/SATA4/SATA5(SATA 6Gb/s Connectors)

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.



7/8/9/10/11) CPU_FAN/SYS_FAN1/SYS_FAN2/SYS_FAN3/SYS_FAN4
(CPU Fan/System Fan Headers)

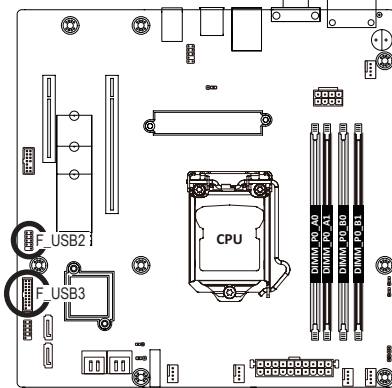
The motherboard has one 4-pin CPU fan header (CPU_FAN), and two 4-pin (SYS_FAN) system fan headers. Most fan headers possess a foolproof insertion design. When connecting a fan cable, be sure to connect it in the correct orientation (the black connector wire is the ground wire). The motherboard supports 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.



- 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.

12/13) F_USB3/ F_USB2 (USB 3.0/ 2.0 Headers)

The headers 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 2.0 Header



Pin No.	Definition
1	Power (5V)
2	Power (5V)
3	USB 7-
4	USB 11-
5	USB 7+
6	USB 11+
7	GND
8	GND
9	No Pin
10	No Connect

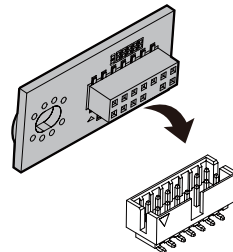
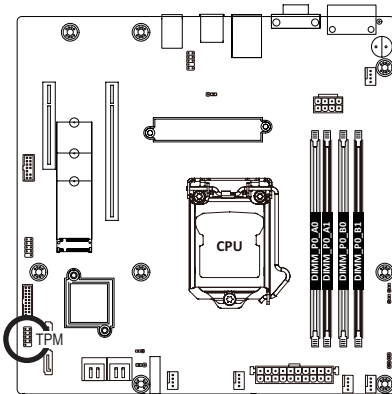
USB 3.0 Header



Pin No.	Definition	Pin No.	Definition
1	Power	11	USB6+
2	RXN1	12	USB6-
3	RXP1	13	GND
4	GND	14	TXP2
5	TXN1	15	TXN2-
6	TXP1	16	GND
7	GND	17	RXP2
8	USB5-	18	RXN2
9	USB5+	19	Power
10	No Connect	20	No Pin

14) TPM (Trusted Platform Module Connector)

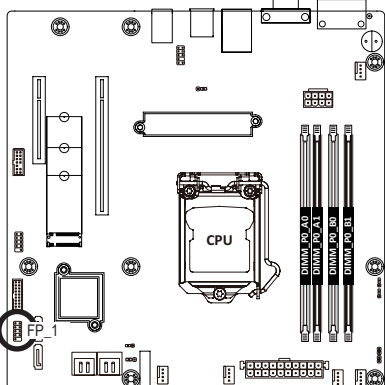
Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.



Pin No.	Definition	Pin No.	Definition
1	CLK_24M_TPM	8	NC
2	+V3.3A	9	LAD_2
3	-PLTRST	10	No Pin
4	+V3.3S	11	LAD_3
5	LAD_0	12	GND
6	SERIRQ	13	LFRAME
7	LAD_1	14	GND

15) 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.



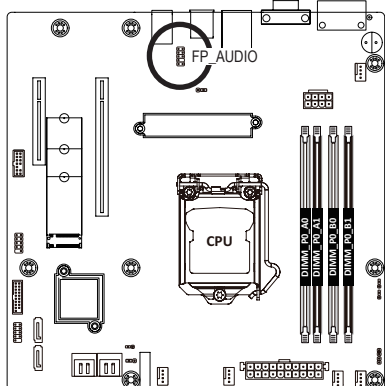
Pin No.	Definition	Pin No.	Definition
1	HDD LED+	6	Power Button+
2	Power LED+	7	Reset Button
3	HDD LED-	8	Power Button-
4	Power LED-	9	No Connect
5	GND	10	No Pin



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.

16) FP_AUDIO (Front Panel Audio Header)

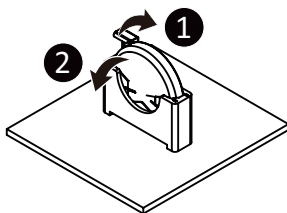
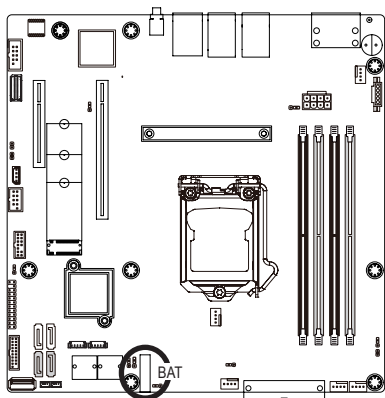
The front panel audio header supports Intel High Definition audio (HD) and AC'97 audio. You may connect your chassis front panel audio module to this header. Make sure the wire assignments of the module connector match the pin assignments of the motherboard header. Incorrect connection between the module connector and the motherboard header will make the device unable to work or even damage it.



Pin No.	Definition
1	MIC2_L
2	GND
3	MIC2_R
4	FP_AUDIO_DET
5	LINE2_R
6	GND
7	F_AUDIO_Sense
8	No Pin
9	LINE2_L
10	GND

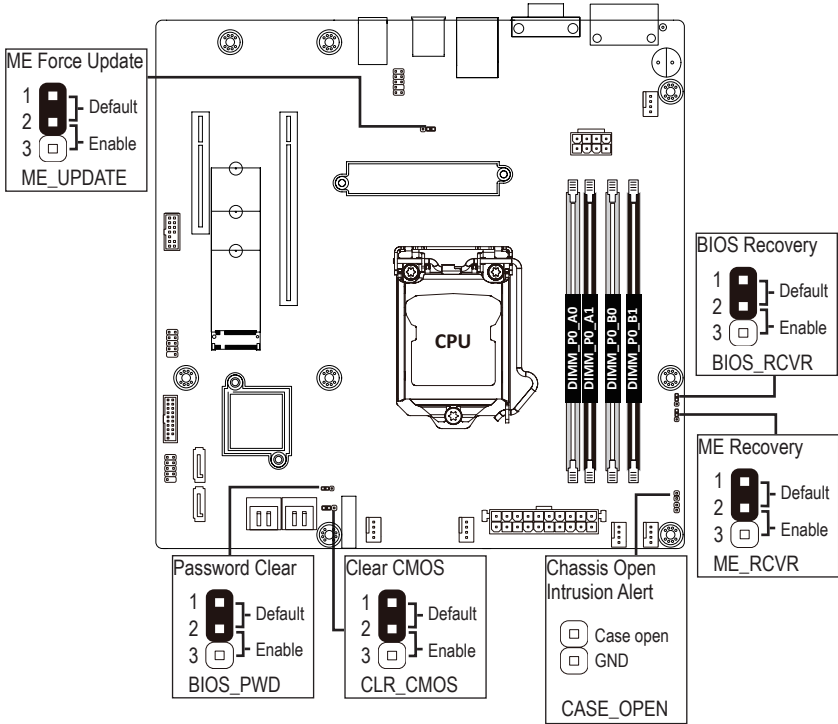
17) BAT (Battery Socket)

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



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

1-8 Jumper Settings



Jumper Name	Jumper Setting
ME Force Update	1-2: Nomal operation (Default) 2-3: Enable ME Force Update
ME Recovery	1-2: Nomal operation (Default) 2-3: Enable ME Recovery
Password Clear	1-2: Nomal operation (Default) 2-3: Clear administrator and user passwords
Clear CMOS	1-2: Nomal operation (Default) 2-3: Clear CMOS data
Chassis Open Intrusion Alert	1-2: Nomal operation (Default)
BIOS Recovery	1-2: Nomal operation (Default) 2-3: Enable BIOS Recovery

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 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

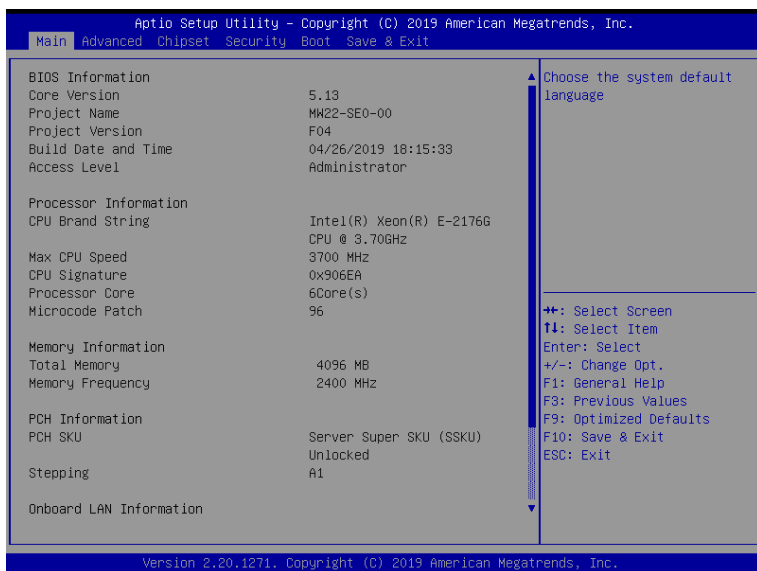
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

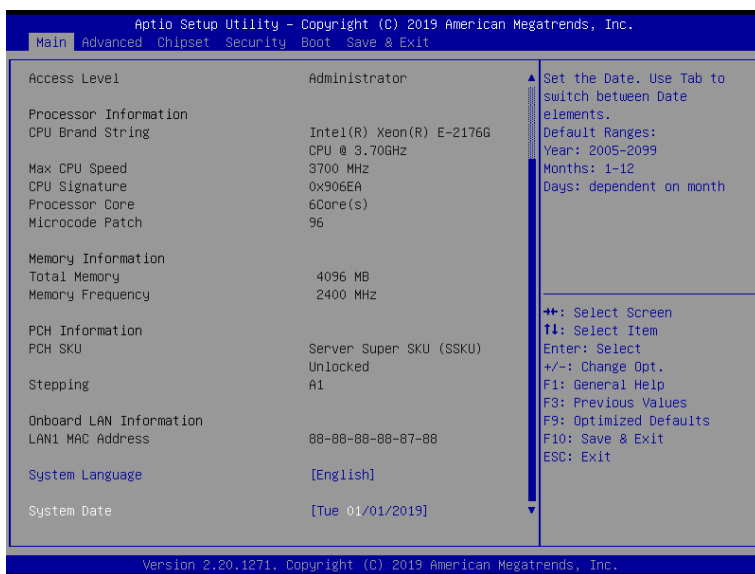
Submenu Help

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	
Core Version	Displays the Core version 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.
Access Level	Displays the access level information.
Processor Information	
CPU Brand String / Max CPU Speed / CPU Signature / Processor Core / Microcode Patch	Displays the technical specifications for the installed processor.
Memory Information	
Total Memory ^(Note)	Displays the total memory size of the installed memory.
Memory Frequency ^(Note)	Displays the frequency information of the installed memory.

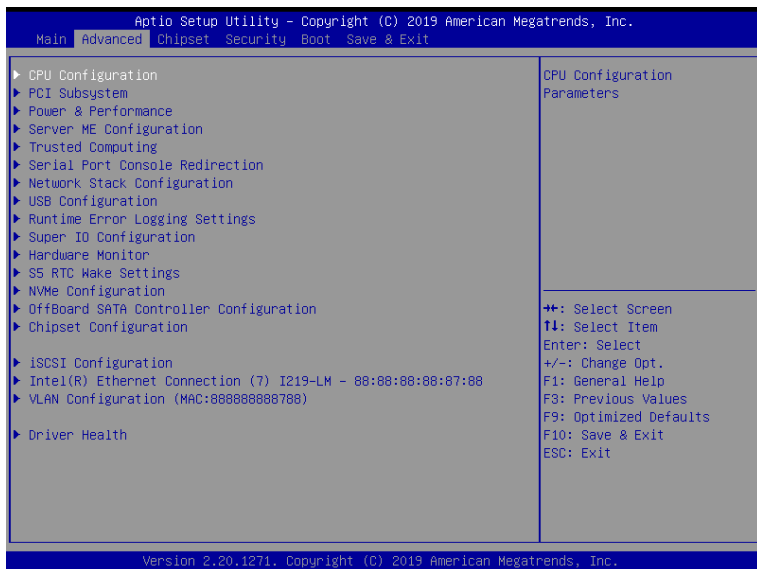
(Note) This section will display capacity and frequency information of the memory that the customer has installed.

Parameter	Description
PCH Information	
PCH SKU / Stepping	Displays the information for the installed Platform Controller Hub.
Onboard LAN Information	
LAN1 MAC Address ^(Note)	Displays LAN MAC address information.
System Language	Displays the information of system language.
System Date	Sets the date following the weekday-month-day-year 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 CPU Configuration



Parameter	Description
CPU Configuration	
Type / ID / Speed / L1 Data Cache / L1 Instruction Cache / L2 Cache/ L3 Cache	Displays the technical specifications for the installed processor
Software Guard Extensions (SGX)	Enable/Disable Software Guard Extensions (SGX). Options available: Enabled, Disabled, Software Controlled. Default setting is Enabled .
Hardware Prefetcher	Enable/Disable CPU Hardware Prefetcher. Options available: Enabled/Disabled. Default setting is Enabled .
Adjacent Cache Line Prefetch	Enable/Disable Adjacent Cache Line Prefetch. Options available: Enabled/Disabled. Default setting is Enabled .
VT-x	Enable/Disable VT-x function. Options available: Enabled/Disabled. Default setting is Enabled .
Active Processor Cores	To increase or decrease the number of active processor cores. Options available: All, 1, 2, 3, 4, and 5. Default setting is All .

Parameter	Description
Hyper-Threading	The Intel Hyper Threading Techonlogy 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: Enabled/Disabled. Default setting is Enabled .
Intel Trusted Execution Techonlogy	Enable/Disable Intel Trusted Execution Techonlogy. Options available: Enabled/Disabled. Default setting is Disabled .

2-2-2 PCI Subsystem Settings

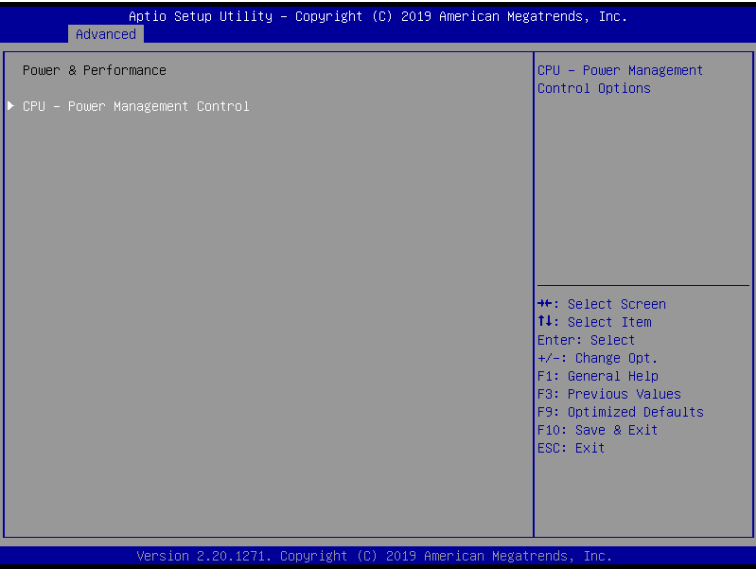


Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
PCI Express Slot #1 / #2 I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled/Disabled. Default setting is Enabled .
Onboard LAN1 Controller ^(Note2)	Enable/Disable the onboard LAN1 devices. Options available: Enabled/Disabled. Default setting is Enabled .
Onboard LAN1 I/O ROM ^(Note2)	Enable/Disable the onboard LAN1 devices, and initializes device expansion ROM. Options available: Enabled/Disabled. Default setting is Enabled .
PCI Devices Common Settings	
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 .

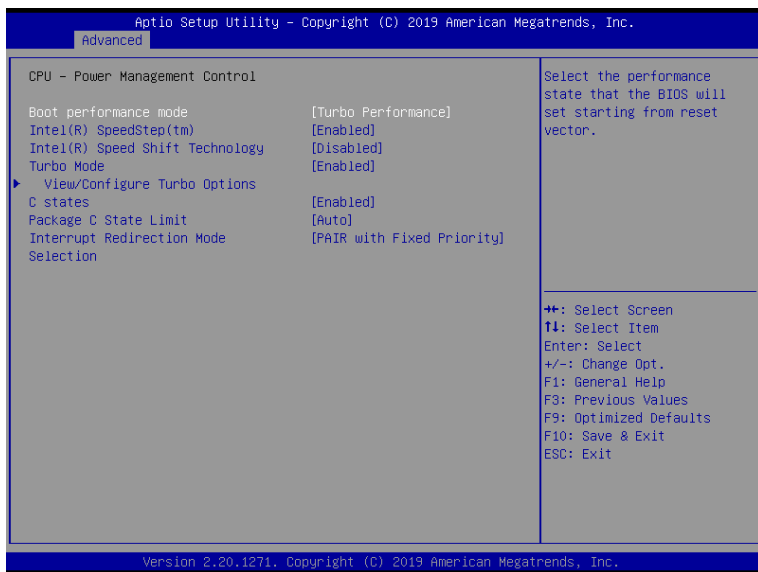
(Note1) This section is dependent on the available PCIe Slot.

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

2-2-3 Power & Performance Settings



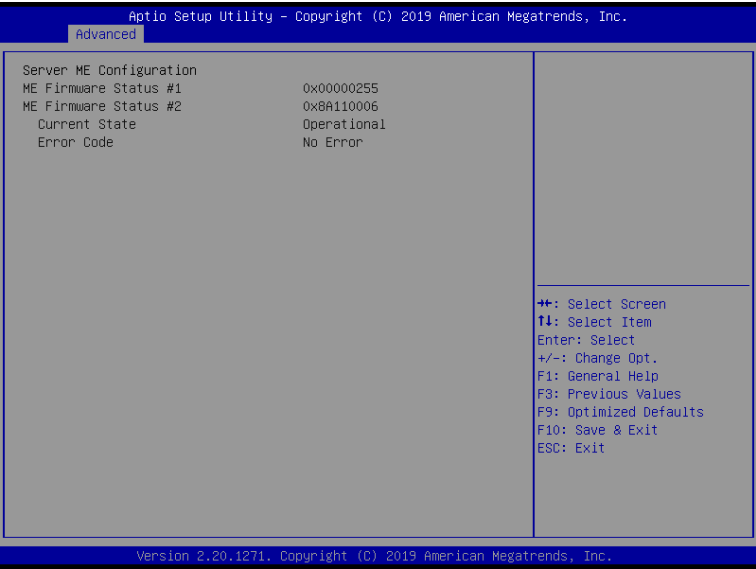
Parameter	Description
Power & Performance	
CPU-Power Management Control	Press [Enter] to configure advanced items.



Parameter	Description
CPU-Power Management Control	
Boot performance mode	Select the performance state that the BIOS will set starting from reset vector. Options available: Max Non-Turbo Performance, Turbo Performance. Default setting is Turbo Performance .
Intel(R) SpeedStep(tm)	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 Enabled .
Intel(R) Speed Shift Technology	Allows the system to dynamically adjust processor voltage and core frequency, decreasing average power consumption and heat production. Options available: Enable/Disable. Default setting is Disabled .
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 .

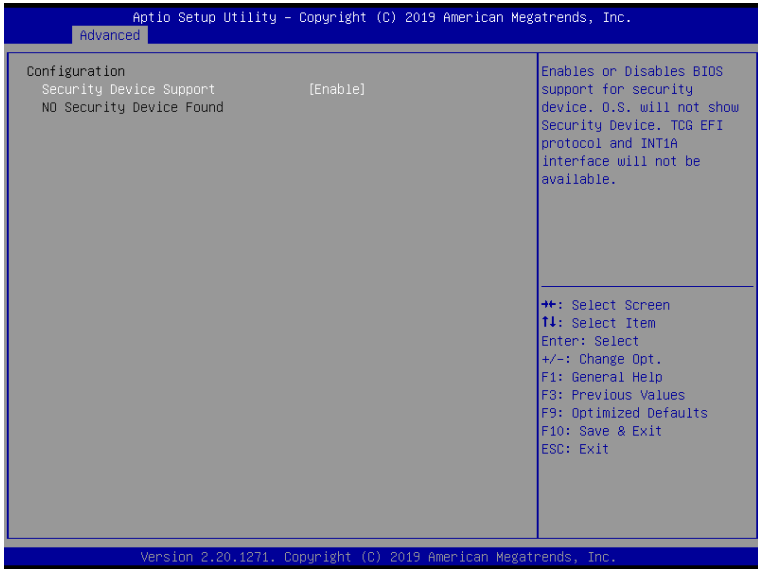
Parameter	Description
View / Configure Turbo Options	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ♦ Energy Efficient P-state <ul style="list-style-type: none"> – Enable/Disable Energy Efficient P-state feature. – Options available: Enabled/Disabled. Default setting is Enabled. • Energy Efficient Turbo <ul style="list-style-type: none"> – Enable/Disable Energy Efficient Turbo feature. – Options available: Enabled/Disabled. Default setting is Enabled.
C states	<p>Enable/Disable CPU power states.</p> <p>Options available: Enabled/Disabled. Default setting is Enabled.</p>
Package C State Limit	<p>Configures the limit on the C-State package register.</p> <p>Options available: C0/C1, C2, C3, C6, C7, C7S, C8, C9, C10 and Auto. Default setting is Auto.</p>
Interrupt Redirection Mode Selection	<p>Select an Interrupt Redirection Mode for logical interrupts.</p> <p>Options available: Fixed Priority, Round robin, Hash Vector, PAIR with Fixed Priority, PAIR with Round Robin, PAIR with Hash Vector and No Change. Default setting is PAIR with Fixed Priority.</p>

2-2-4 Server ME Configuration



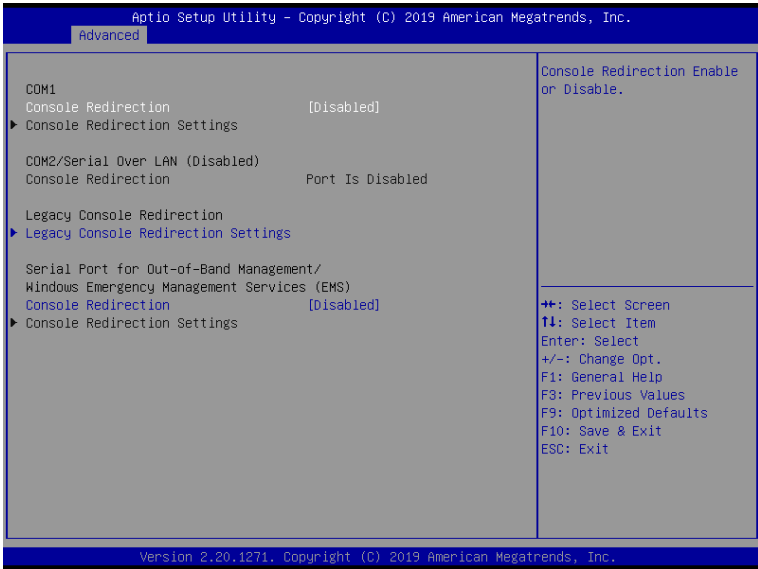
Parameter	Description
Server ME Configuration	
ME Firmware Status #1/#2	Displays ME Firmware status information.
Current State (for ME Firmware)	Displays ME Firmware current status information.
Error Code (for ME Firmware)	Displays ME Firmware status error code.

2-2-5 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.

2-2-6 Serial Port Console Redirection



Parameter	Description
COM1/COM2 Serial Over LAN Console Redirection ^(Note)	Select whether to enable console redirection for specified device. Console redirection enables the users to manage the system from a remote location. Options available: Enabled/Disabled. Default setting is Disabled .
Legacy Console Redirection	Selects a COM port for legacy serial redirection. The options are dependent on the available COM ports.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection ^(Note)	Selects a COM port for EMS console redirection. 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 .
COM1/COM2 Serial LAN/ Legacy/Serial Port for Out-of-Band EMS Console Redirection Settings	Press [Enter] to configure advanced items. Please note that this item is configurable when COM1/COM2 Serial Over LAN/Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled. <ul style="list-style-type: none">Terminal Type<ul style="list-style-type: none">Selects a terminal type to be used for console redirection.Options available: VT100, VT100+, ANSI , VT-UTF8. Default setting is ANSI.

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

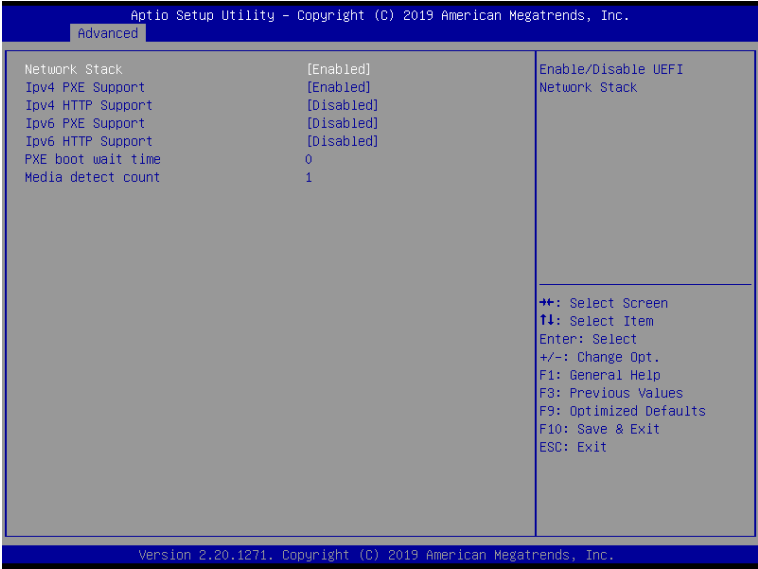
Parameter	Description
COM1/COM2 Serial LAN/ Legacy/Serial Port for Out- of-Band EMS Console Redirection Settings (continued)	<ul style="list-style-type: none"> ◆ Bits per second <ul style="list-style-type: none"> – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is 115200. ◆ Data Bits <ul style="list-style-type: none"> – Selects the number of data bits used for console redirection. – Options available: 7/8. Default setting is 8. ◆ Parity <ul style="list-style-type: none"> – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: parity bit is 0 if num of 1's in the data bits is odd. – Mark: parity bit is always 1. Space: Parity bit is always 0. – Mark and Space Parity do not allow for error detection. – Options available: None, Even, Odd, Mark, Space. Default setting is None. ◆ Stop Bits <ul style="list-style-type: none"> – Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. – Options available: 1/2. Default setting is 1. ◆ Flow Control <ul style="list-style-type: none"> – Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. – For COM1/COM2 Serial Over LAN: <ul style="list-style-type: none"> » Options available: None, Hardware RTS/CTS. Default setting is None. – For Serial Port for Out-of-Band EMS: <ul style="list-style-type: none"> » Options available: None, Hardware RTS/CTS and Software Xon/Xoff. Default setting is Hardware RTS/CTS. ◆ Legacy Console Redirection Settings <ul style="list-style-type: none"> – Selects a COM port to display redirection of Legacy OS and Legacy OPROM Messages. – Options available: COM1/COM2 Serial Over LAN. Default setting is COM1. ◆ Legacy OS Redirection Resolution^(Note) <ul style="list-style-type: none"> – Specifies the number of Rows and Columns supported for the Legacy OS redirection. – Options available: 80x24/80x25. Default setting is 80x24.

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

Parameter	Description
COM1/COM2 Serial LAN/ Legacy/Serial Port for Out- of-Band EMS Console Redirection Settings (continued)	<ul style="list-style-type: none"> ♦ Redirection After BIOS POST^(Note) <ul style="list-style-type: none"> – This item allows user to enable console redirection after OS has loaded. – Options available: Always Enable/Boot Loader. Default setting is Always Enable. ♦ Out-of-Band Mgmt Port <ul style="list-style-type: none"> – Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Options available: COM1/COM2 Serial Over LAN. Default setting is COM1.

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

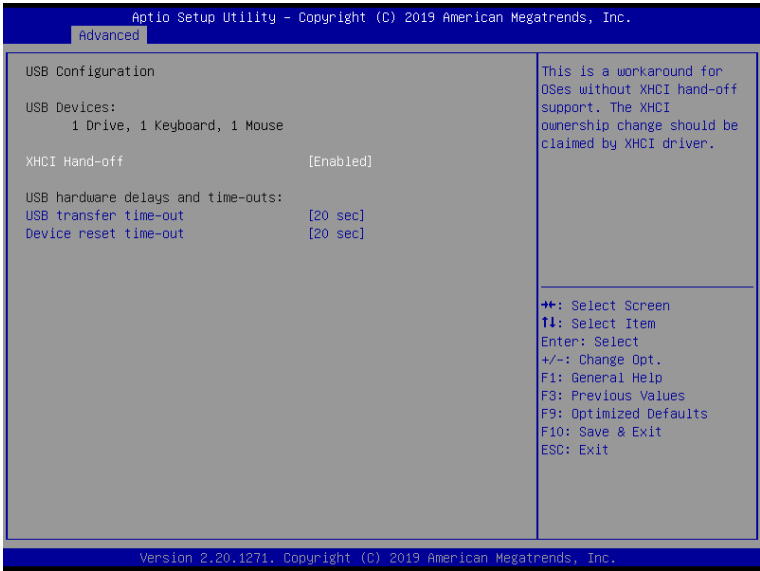
2-2-7 Network Stack Configuration



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 .
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**.

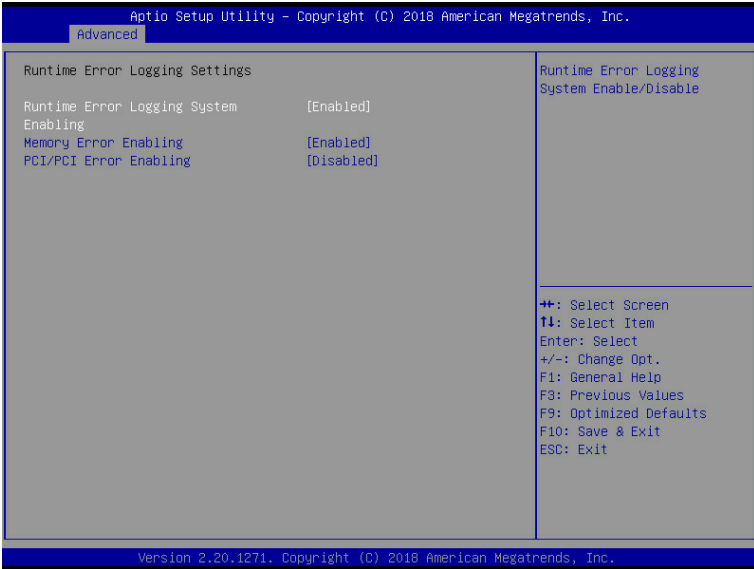
2-2-8 USB Configuration



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 hardware delays and time-outs	
USB transfer time-out	Select the time-out value for USB Control/Bulk/Interrupt transfers. Options available: 1 sec, 5 sec, 10 sec and 20sec. Default setting is 20 sec .
Device reset time-out	Select the time-out value during a USB mass storage device reset. Options available: 10 sec, 20 sec, 30 sec and 40sec. Default setting is 20 sec .

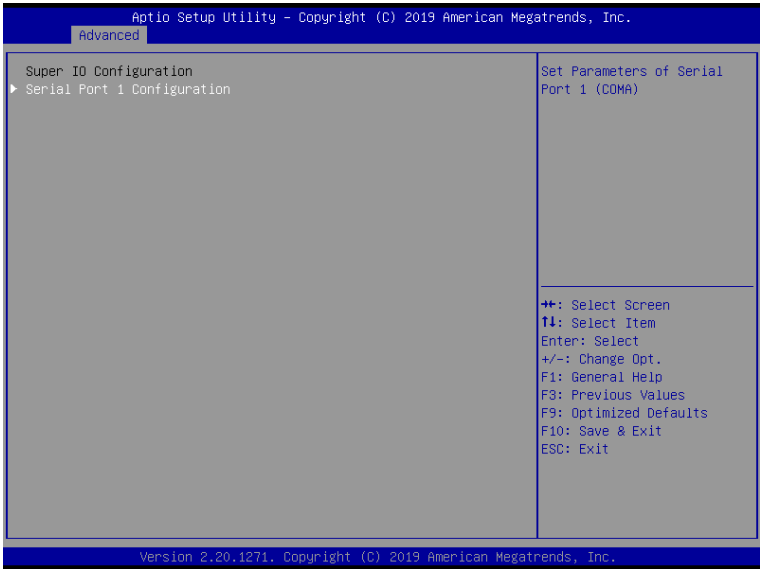
(Note) This item is present only if you attach USB devices.

2-2-9 Runtime Error Logging Settings



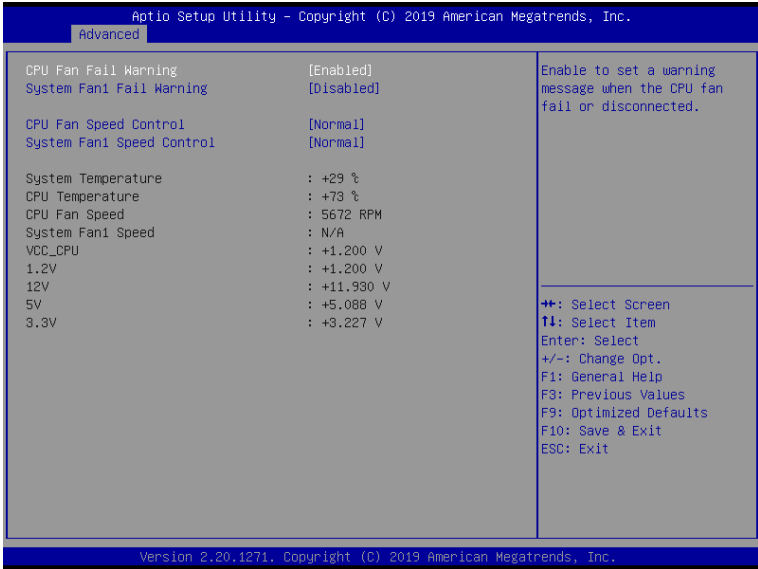
Parameter	Description
Runtime Error Logging Settings	
Runtime Error Logging System Enabling	Enable/Disable runtime logging error system function. Options available: Enable/Disabled. Default setting is Enable .
Memory Error Enabling	Enable/Disable the Memory Error log function Options available: Enable/Disabled. Default setting is Enable .
PCI/PCI Error Enabling	Enable/Disable the PCI/PCI log function Options available: Enable/Disabled. Default setting is Disabled .

2-2-10 Super IO Configuration



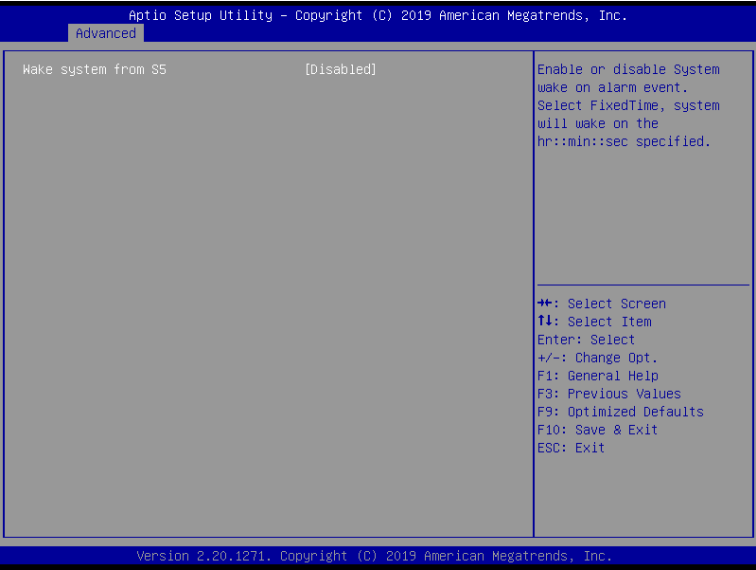
Parameter	Description
Serial Port 1 Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none">Serial Port<ul style="list-style-type: none">When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port.Options available: Enabled/Disabled. Default setting is Enabled.Device Settings<ul style="list-style-type: none">Displays the serial port base I/O address and IRQ.Change Settings:<ul style="list-style-type: none">Configures the serial port base I/O address and IRQ.<ul style="list-style-type: none">Serial Port 1 :<ul style="list-style-type: none">Auto;IO=3F8h; IRQ=4;IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;Default setting is Auto.

2-2-11 Hardware Monitor



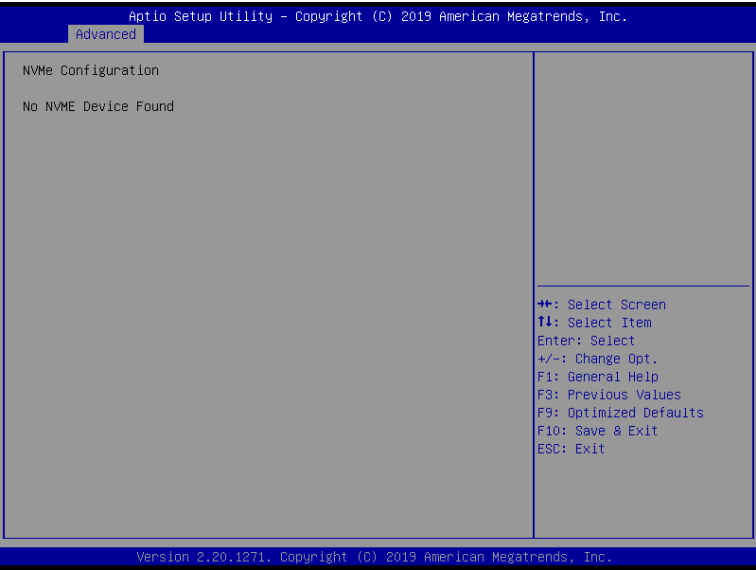
Parameter	Description
CPU FAN Fail Warning	Enable/Disable CPU FAN Fail Warning alert function. Options available: Enable/Disabled. Default setting is Enabled .
System FAN1 Fail Warning	Enable/Disable CPU FAN Fail Warning alert function. Options available: Enable/Disabled. Default setting is Disabled .
CPU FAN Speed Control	Enable CPU FAN Speed Control function. Options available: Normal/Full Speed. Default setting is Normal .
System FAN1 Speed Control	Enable System FAN Speed Control function. Options available: Normal/Full Speed. Default setting is Normal .
System Temperature	Displays the System temperature information.
CPU Temperature	Displays the CPU temperature information.
CPU FAN Speed	Displays the RPM (Ratio Per Minute) of CPU Fan speed.
System FAN1 Speed	Displays the RPM (Ratio Per Minute) of System Fan1 speed.
VCC_CPU/ 1.2V/ 12V/ 5V/ 3.3V	Displays the CPU/ System voltages information.

2-2-12 S5 RTC Wake Settings



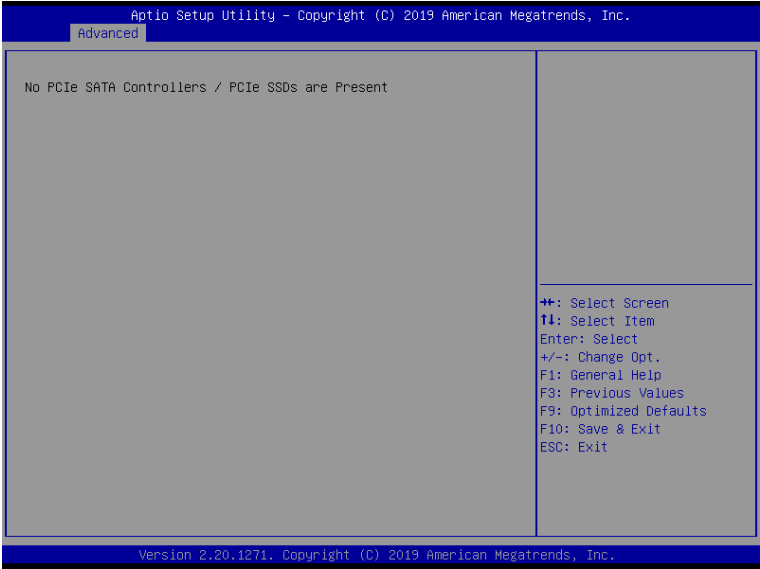
Parameter	Description
Wake System from S5	Enable/Disable system wake on alarm event. Options available: Disabled/Fixed Time. When Fixed Time enabled, system will wake on the hr::min::sec specified. Default setting is Disabled .

2-2-13 NVMe Configuration



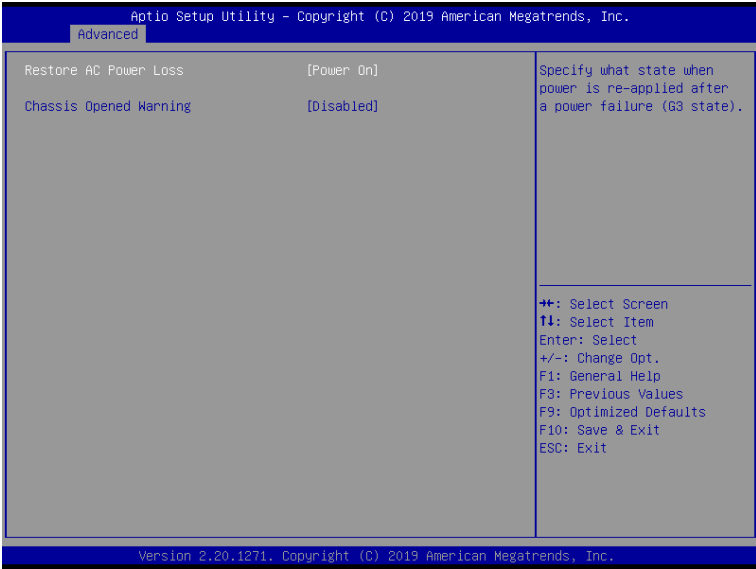
Parameter	Description
MVMe Configuration	Displays the NVMe devices connected to the system

2-2-14 OffBoard SATA Controller Configuration



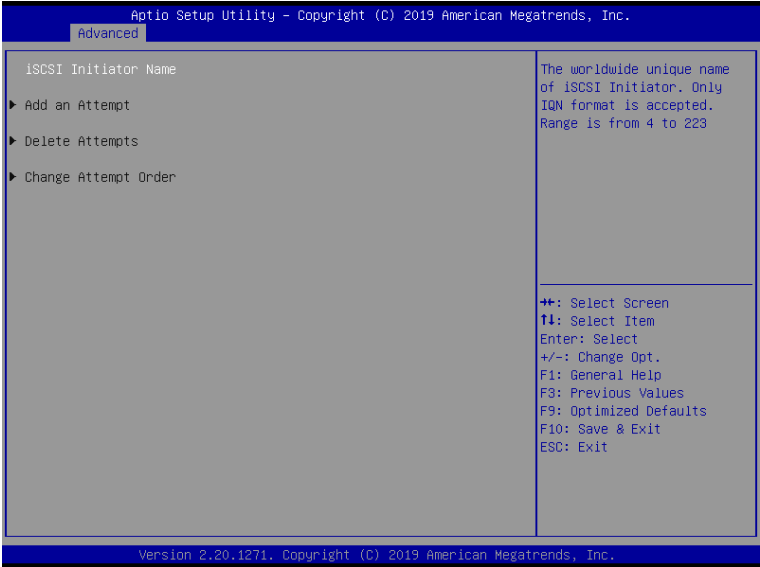
Parameter	Description
Offboard SATA Controller Configuration	Displays the information on your PCIe SATA controllers/ PCIe SSD if installed

2-2-15 Chipset Configuration



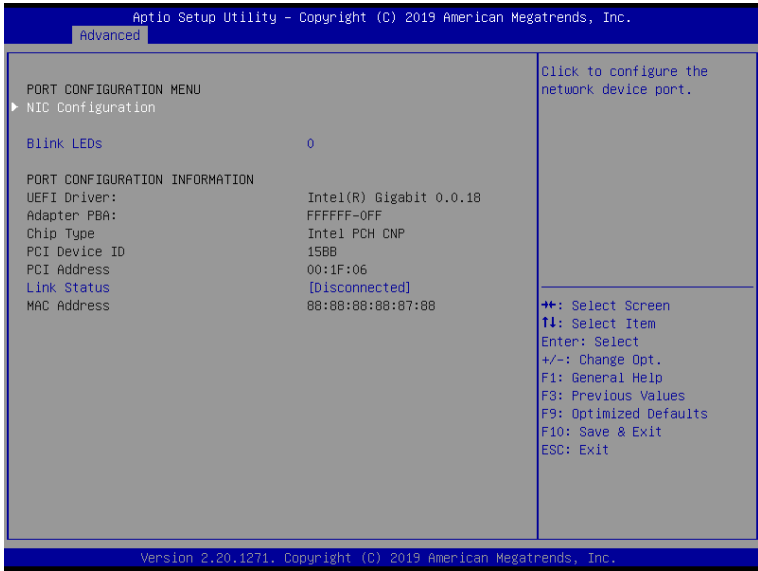
Parameter	Description
Restore on AC Power Loss	<p>This option provides user to set the mode of operation if an AC/ Power loss occurs.</p> <ul style="list-style-type: none">• Power On: System power state when AC cord is re-plugged.• Power Off: Do not power on system when AC power is back.• Last State: Set system to the last state when AC power is removed. <p>Options available: Power On, Power Off, Last State. Default setting is Power On.</p>
Chassis Opened Warning	<p>Enable/Disable the chassis intrusion alert function.</p> <p>Options available: Enabled, Disabled, Clear. Default setting is Disabled.</p>

2-2-16 iSCSI Configuration



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

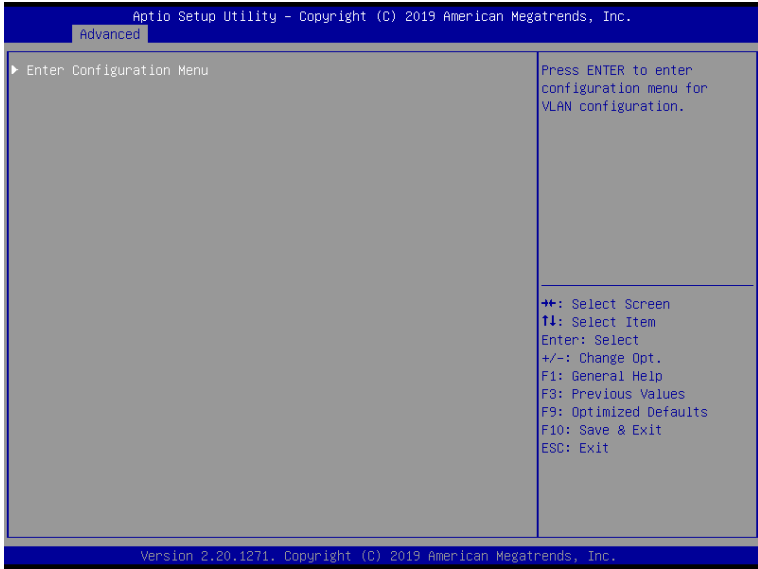
2-2-17 Intel(R) I219-LM Ethernet Connection



Parameter	Description
PORT CONFIGURATION MENU	
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none">♦ Link Speed<ul style="list-style-type: none">– Allows for automatic link speed adjustment.– Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. Default setting is Auto Negotiated.♦ Wake On LAN<ul style="list-style-type: none">– Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.– Options available: Enabled/Disabled. Default setting is Enabled.
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.

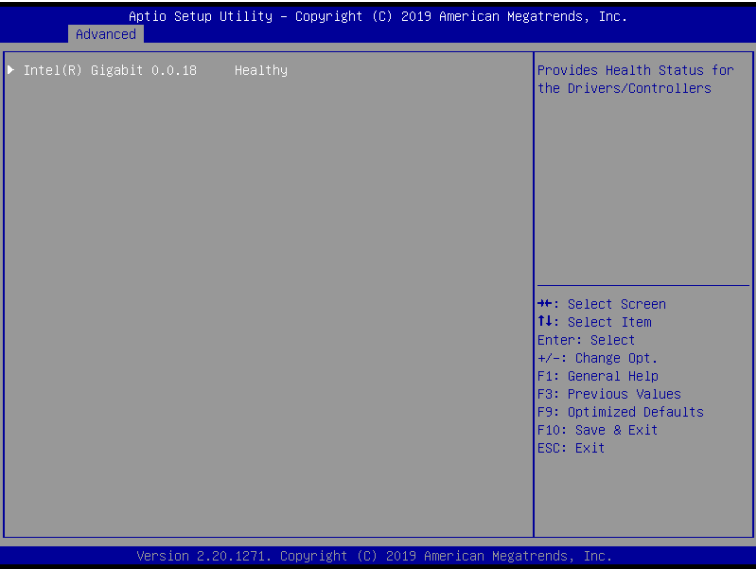
Parameter	Description
PORT CONFIGURATION INFORMATION	
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface 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.

2-2-18 VLAN Configuration



Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none">♦ Create new VLAN♦ VLAN ID<ul style="list-style-type: none">– Sets VLAN ID for a new VLAN or an existing VLAN.– Press the <+> / <-> keys to increase or decrease the desired values.– The valid range is from 0 to 4094.♦ Priority<ul style="list-style-type: none">– Sets 802.1Q Priority for a new VLAN or an existing VLAN.– Press the <+> / <-> keys to increase or decrease the desired values.– The valid range is from 0 to 7.♦ Add VLAN<ul style="list-style-type: none">– Press [Enter] to create a new VLAN or update an existing VLAN.♦ Configured VLAN List♦ Remove VLAN<ul style="list-style-type: none">– Press [Enter] to remove an existing VLAN.

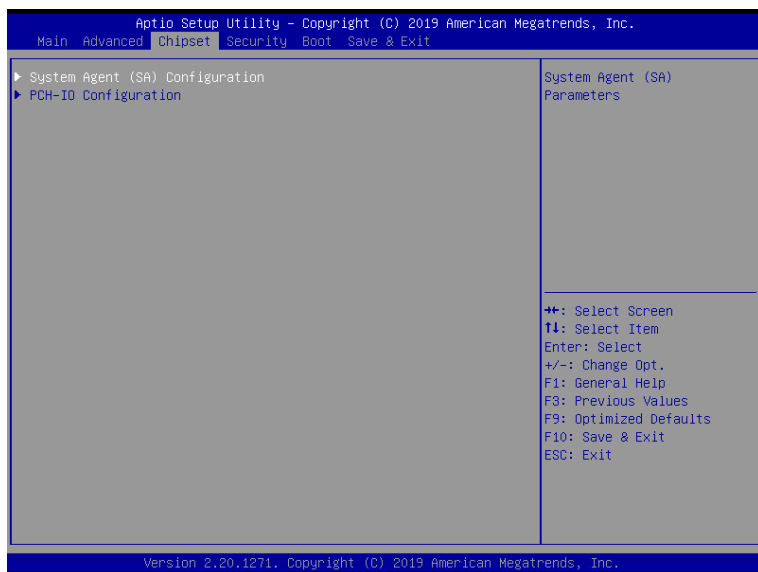
2-2-19 Driver Health



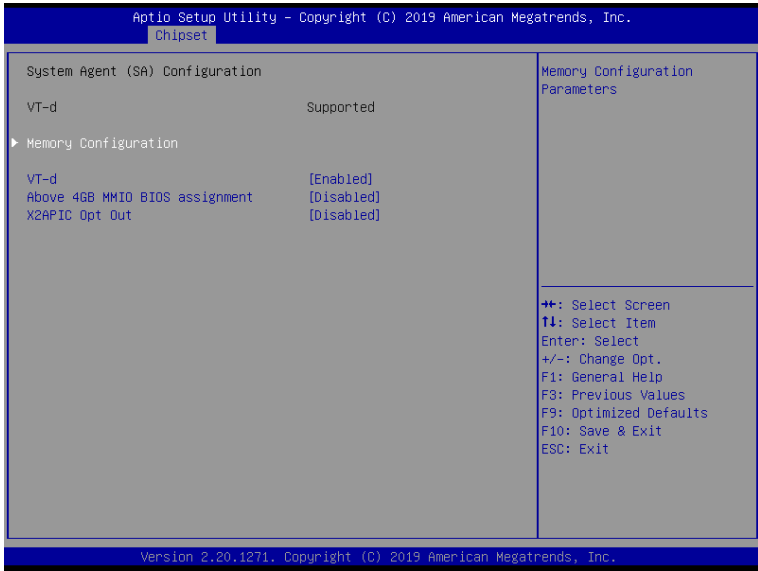
Parameter	Description
Driver Health	Displays driver health status of the devices/controllers if installed

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.

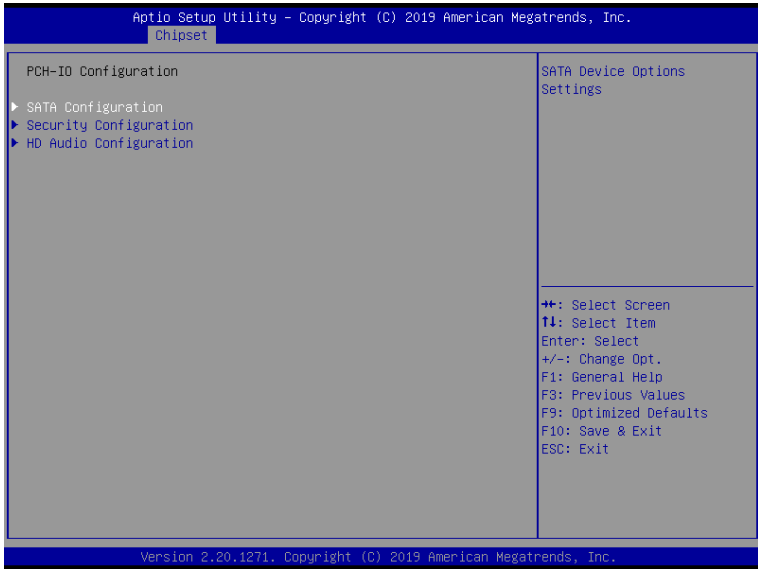


2-3-1 System Agent (SA) Configuration



Parameter	Description
Memory Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none">♦ Memory Frequency<ul style="list-style-type: none">– Displays the frequency information of installed memory.♦ Channel and slot information of memory DIMMs.♦ Maximum Memory Frequency<ul style="list-style-type: none">– Configure the maximum memory frequency.– Default setting is Auto.♦ Max TOLUD<ul style="list-style-type: none">– Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller– Options available: 1GB, 2GB, 3GB. Default setting is Auto.
VT-d	<p>Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) feature.</p> <p>Options available: Enabled/Disabled. Default setting is Enabled.</p>
Above 4GB MMIO BIOS assignment	<p>Enable/Disable the Above 4G Memory Mapped IO BIOS Assignment.</p> <p>Options available: Enabled/Disabled. Default setting is Disabled</p>
X2APIC Opt Out	<p>Enable/Disable X2APIC Opt Out function.</p> <p>Options available: Enabled/Disabled. Default setting is Disabled</p>

2-3-2 PCH-IO Configuration

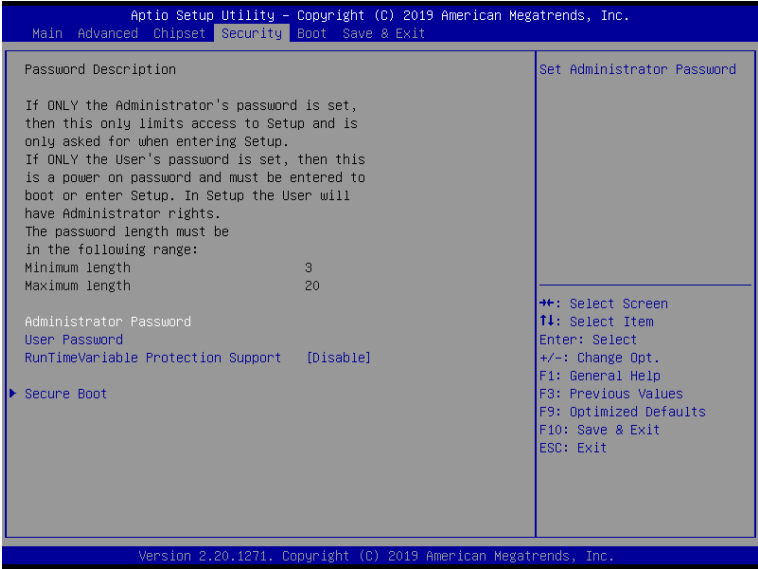


Parameter	Description
PCH-IO Configuration	
SATA Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none">◆ SATA Controller<ul style="list-style-type: none">– Enable/Disable SATA controller.– Options available: Enabled/Disabled. Default setting is Enabled.◆ SATA Mode Selection<ul style="list-style-type: none">– 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.◆ SATA Port 0/1/2/3/4/5<ul style="list-style-type: none">– The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.

Parameter	Description
Security Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ♦ BIOS Lock <ul style="list-style-type: none"> – Enable/Disable the PCH BIOS Lock Enable feature. – Options available: Enabled/Disabled. Default setting is Disabled.
HD Audio Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ♦ Onboard Audio Controller <ul style="list-style-type: none"> – Enable/Disable Onboard Audio Controller. – Options available: Enabled/Disabled. Default setting is Enabled.

2-4 Security Menu

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



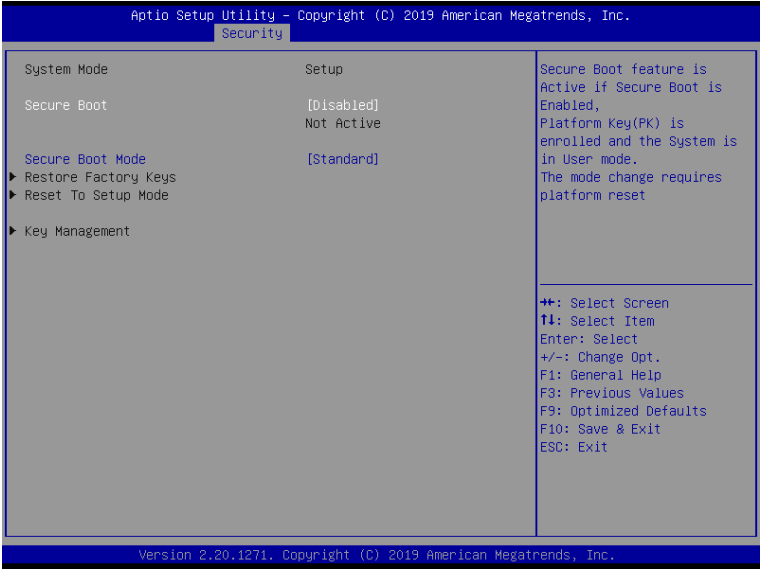
There are two types of passwords that you can set:

- 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.
RuntimeVariable Protection Support	Enable/Disable Runtime Variable protection support. Options available: Enable/Disable. Default setting is Disable .
Secure Boot	Press [Enter] to configure advanced items.

2-4-1 Secure Boot

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



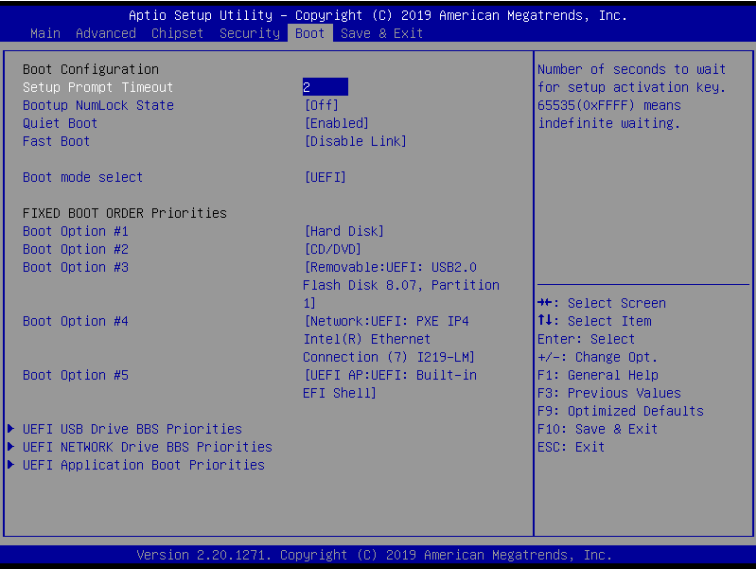
Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available:Enabled/Disabled. Default setting is Disabled .
Secure Boot Mode ^(Note)	Secure Boot requires all the applications that are running during the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

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

Parameter	Description
Key Management	<p>Press [Enter] to configure advanced items.</p> <p>Please note that this item is configurable when Secure Boot Mode is set to Custom.</p> <ul style="list-style-type: none"> ◆ Factory Key Provision <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – Installs all factory default keys. It will force the system in User Mode. – Options available: Yes/No. ◆ Enroll Efi Image <ul style="list-style-type: none"> – Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). ◆ Restore DB defaults <ul style="list-style-type: none"> – Restore DB variable to factory defaults. ◆ Secure Boot variable <ul style="list-style-type: none"> – Displays the current status of the variables used for secure boot. ◆ Platform Key (PK) <ul style="list-style-type: none"> – Displays the current status of the Platform Key (PK). – Press [Enter] to configure a new PK. – Options available: Set New. ◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> – 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) <ul style="list-style-type: none"> – 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) <ul style="list-style-type: none"> – 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) <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – 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.

2-5 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.

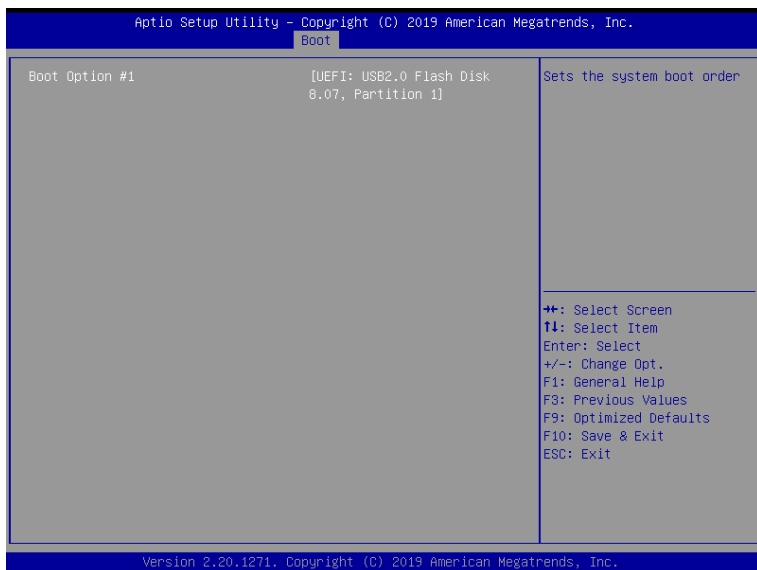


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On/Off. Default setting is Off .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled/Disabled. Default setting is Enabled .
Fast Boot	If enabled, the BIOS will shorten the booting process by skipping some tests and shortening others. Options available: Enabled/Disable Link. Default setting is Disable Link .
Boot mode select	Selects the boot mode. Options available: LEGACY/UEFI. Default setting is UEFI .

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

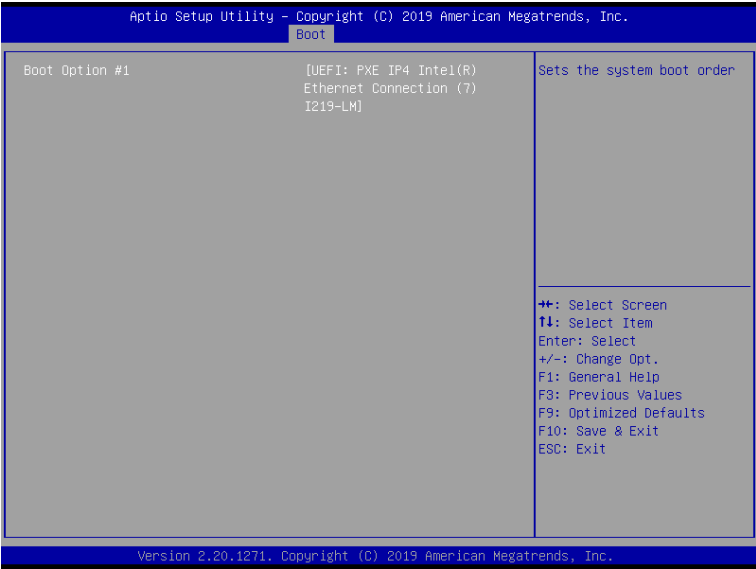
2-5-1 UEFI USB Drive BBS Priorities

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



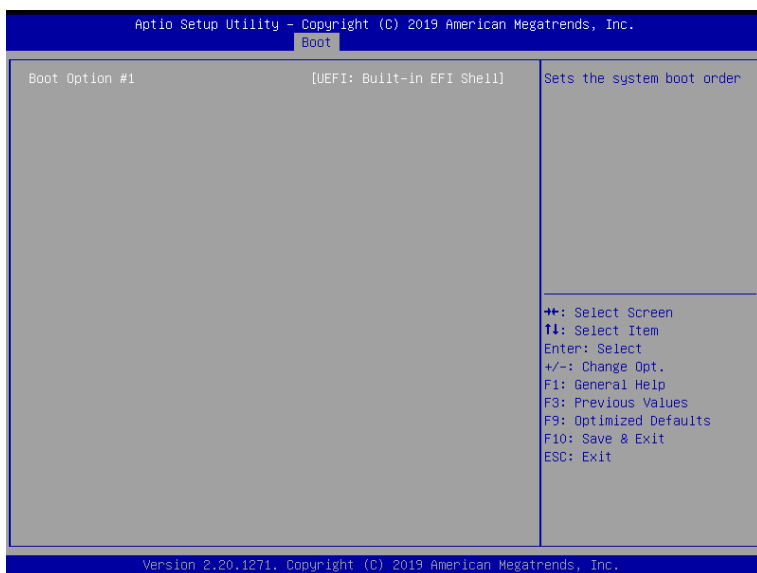
2-5-2 UEFI NETWORK Drive BBS Priorities

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.



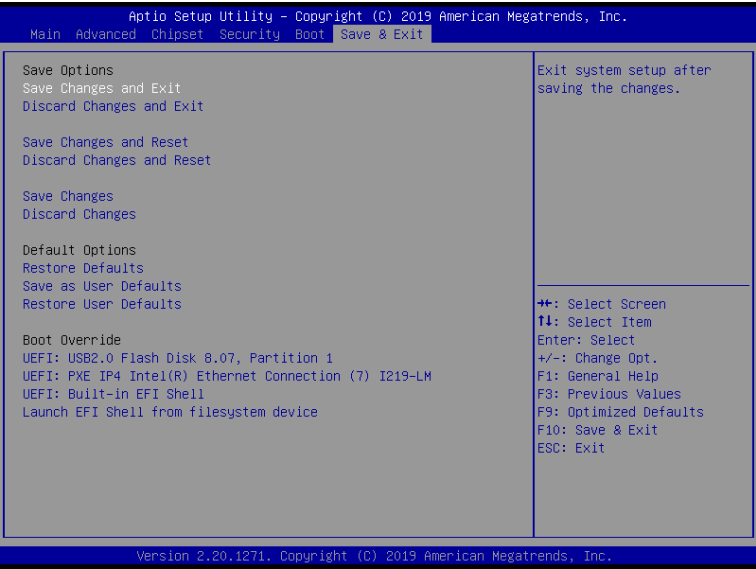
2-5-3 UEFI Application Boot Priorities

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.



2-6 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	<p>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.</p> <p>Options available: Yes/No.</p>
Save as User Defaults	<p>Saves the changes made as the user default settings.</p> <p>Options available: Yes/No.</p>
Restore User Defaults	<p>Loads the user default settings for all BIOS setup parameters.</p> <p>Options available: Yes/No.</p>
Boot Override	Press [Enter] to configure the device as the boot-up drive.

2-7 BIOS POST Codes

2-7-1 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

2-7-2 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

2-7-3 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

2-7-4 Intel UPI POST Codes

Initialize KTIRC input 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

2-7-5 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. <i>RC Behavior: System Halt</i>	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. <i>RC Behavior: The current Socket is not added to the tree.</i> 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 <i>RC Behavior: System Halt</i>	0xDB
Unsupported topology <i>RC Behavior: System Halt</i>	0xDC
SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry. <i>RC Behavior: System Halt</i>	0xDD

2-7-6 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

2-7-7 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

2-7-8 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

2-7-9 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

2-8 BIOS POST Beep code (AMI standard)

2-8-1 PEI Beep Codes

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

2-8-2 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