Smart T6009

Intel® H310 Express Chipset

Based Mini-ITX M/B

User's Manual

Revision: 2.0

Release date: December 8, 2022

Nematron®

Open minds. Open systems. Real solutions.

Table Of Content

Environmental Protection Announcement

Do not dispose this electronic device into the trash while discarding. To minimize pollution and ensure environment protection of mother earth, please recycle.
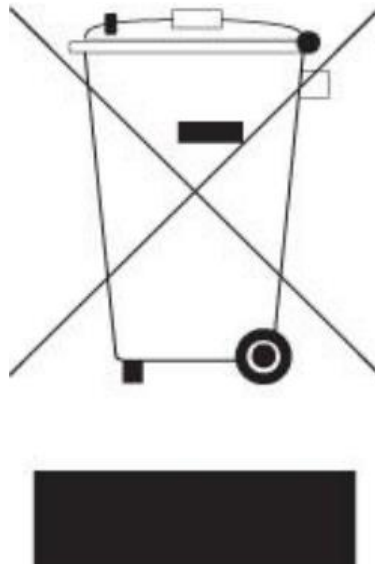
Environmental Safety Instruction

- Avoid the dusty, humidity and temperature extremes. Do not place the product in any area where it may become wet.
- 0 to 40 centigrade is the suitable temperature. (The temperature comes from the request of the chassis and thermal solution)
- Generally speaking, dramatic changes in temperature may lead to contact malfunction and crackles due to constant thermal expansion and contraction from the welding spots' that connect components and PCB. Computer should go through an adaptive phase before it boots when it is moved from a cold environment to a warmer one to avoid condensation phenomenon. These water drops attached on PCB or the surface of the components can bring about phenomena as minor as computer instability resulted from corrosion and oxidation from components and PCB or as major as short circuit that can burn the components. Suggest starting the computer until the temperature goes up.

- The increasing temperature of the capacitor may decrease the life of computer. Using the close case may decrease the life of other device because the higher temperature in the inner of the case.
- Attention to the heat sink when you over-clocking. The higher temperature may decrease the life of the device and burned the capacitor.

USER'S NOTICE

COPYRIGHT OF THIS MANUAL BELONGS TO THE MANUFACTURER. NO PART OF THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT MAY BE REPRODUCED, TRANSMITTED OR TRANSLATED INTO ANY LANGUAGE IN ANY FORM OR BY ANY MEANS WITHOUT WRITTEN PERMISSION OF THE MANUFACTURER. THIS MANUAL CONTAINS ALL INFORMATION REQUIRED TO USE THIS MOTHER-BOARD SERIES AND WE DO ASSURE THIS MANUAL MEETS USER'S REQUIREMENT BUT WILL CHANGE, CORRECT ANY TIME WITHOUT NOTICE. MANUFACTURER PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, AND WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFIT, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS AND THE LIKE). PRODUCTS AND CORPORATE NAMES APPEARING IN THIS MANUAL MAY OR MAY NOT BE REGISTERED TRADEMARKS OR COPYRIGHTS OF THEIR RESPECTIVE COMPANIES, AND THEY ARE USED ONLY FOR IDENTIFICATION OR EXPLANATION AND TO THEOWNER'S BENEFIT, WITHOUT INTENT TO INFRINGE.

Manual Revision Information

Reversion	Revision History	Date
1.0	First Edition	May 6, 2022
2.0	Second Edition	December 8, 2022

Item Checklist

- ☑ Motherboard
- ☑ Cable(s)

Chapter 1　Introduction of the Motherboard

1-1　Feature of Motherboard

- Intel® H310 express chipset
- LGA1151 CPU socket supports Intel® Coffee Lake-S series processor (TDP < 65W)
- Support DC 12~24V Input
- Support 2×DDR4 2133MHz SO-DIMM up to 64GB
- Integrated with 1×Intel I219-V 1.0Gigabit Ethernet LAN chip
- Integrated with 1×Intel I225V 2.5Gigabit Ethernet LAN chip
- Onboard 1×SATAIII (6Gb/s) port & 1×M.2 M-key 2242 slot
- Onboard 1×PCIE x4 Slot & 1×M.2 E-key 2230 PCIe slot (support CNVi)
- Support HDMI/VGA /LVDS/eDP output & Support dual independent displays
- Support 4×COM RS232 (COM1/2 Support 5V/12V TTL)
- Support 4×external USB 3.0 & 5×internal USB 2.0 for rich IO expansion
- Support Smart FAN function
- Supports ACPI S3 Function
- Compliance with ErP Standard
- Support Watchdog Timer Technology

1-2　Specification

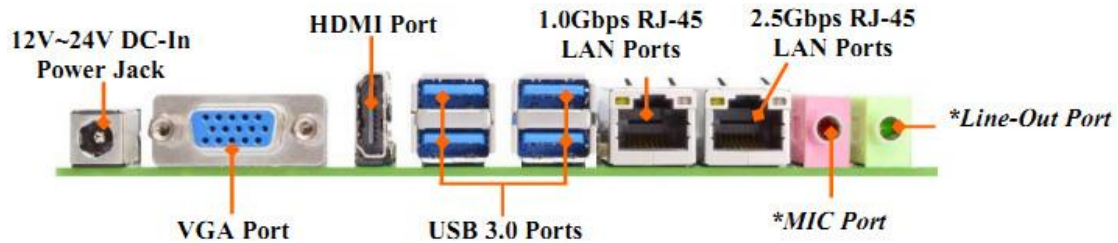| Spec	Description
Design	● Thin mini-ITX form factor; PCB size: 170×170mm
Chipset	● Intel® H310 Express Chipset
CPU Socket	● Intel® LGA 1151 Socket for Coffee Lake-S series processors
Memory Slot	● 2×DDR4 SO-DIMM slot ● Support DDR4 2133MHz SDRAM ● Maximum capacity: up to 64GB * Memory frequency range also depends on CPU support
Expansion Slot	● 1×PCIE x4 slot (PCIE1)

	● 1×M.2 E-key slot, type-2230 with PCIe interface (M2E)
Storage	● 1×SATAIII 6G/s port (SATA1) ● 1×M.2 M-key slot, type-2242 with SATA interface (M2M)
LAN Chip	● Integrated with 1×Intel I219-V 1.0Gigabit Ethernet LAN chip ● Integrated with 1×Intel I225V 2.5Gigabit Ethernet LAN chip ● Support Fast Ethernet LAN function of providing10/100/1000/2500Mbps Ethernet data transfer rate
Audio Chip	● Realtek HD Audio Codec integrated, with Audio driver and utilityincluded
BIOS	● AMI Flash ROM
Multi I/O	***Rear Panel I/O:*** ● 1×12V~24V DC-in Power Jack ● 1×VGA port ● 1×HDMI port ● 4×USB 3.0 ports ● 2×RJ-45 LAN ports ● 1×MIC port ● 1×Line-out port ***Internal I/O Connectors, Headers & Wafers:*** ● 1×CPUFAN connector & 1×SYSFAN connector ● 1×SATA Power-out connector ● 1×Front panel header ● 2×9-Pin USB 2.0 header for 4×USB 2.0 ports ● 1×4-Pin USB 2.0 header for 1×USB 2.0 port ● 1×PS/2 keyboard & mouse header ● 1×SMBUS header ● 1×Front panel audio header ● 1×SPEAK_CON:3W Amplifier wafer ● 4×RS232 serial ports header ● 1×GPIO header ● 1×LVDS wafer ● 1×LVDS Inverter wafer

	● 1×eDP wafer

1-3 Layout Diagram

Rear IO Diagram

12V~24V DC-In Power Jack • HDMI Port • 1.0Gbps RJ-45 LAN Ports • 2.5Gbps RJ-45 LAN Ports • *Line-Out Port • VGA Port • USB 3.0 Ports • *MIC Port

Motherboard Internal Diagram-Front

Internal 12V~24V DC-IN Power Connector • 12V~24V DC-IN Power Jack • CPUFAN Connector • LGA 1151 CPU Socket • VGA Port • LVDS INVERTER • eDP Wafer • LVDS Wafer • HDMI Port • M.2E-Key Slot (M2E) • USB 3.0 Ports • M.2 M-Key Slot (M2M) • SYSFAN Connector • 1.0GbpsRJ-45 LAN Ports • BATCON • H310 Chipset • 2.5GbpsRJ-45 LAN Ports • Serial Port Headers (COM1/2/3/4) • *MIC Port • DDR4 SODIMM Slots (SODIMM1/2) • *Line-Out Port • SMBUS Header • GPIO Header • Front Panel Header • PS/2 KB& MS Header • *SPEAK_CON Header • *Front Panel Audio Header • PCIE X4 Slot (PCIE1) • SATA Power Out Port • SATAIII Port • USB 2.0 Port Headers

Motherboard Jumper Position:
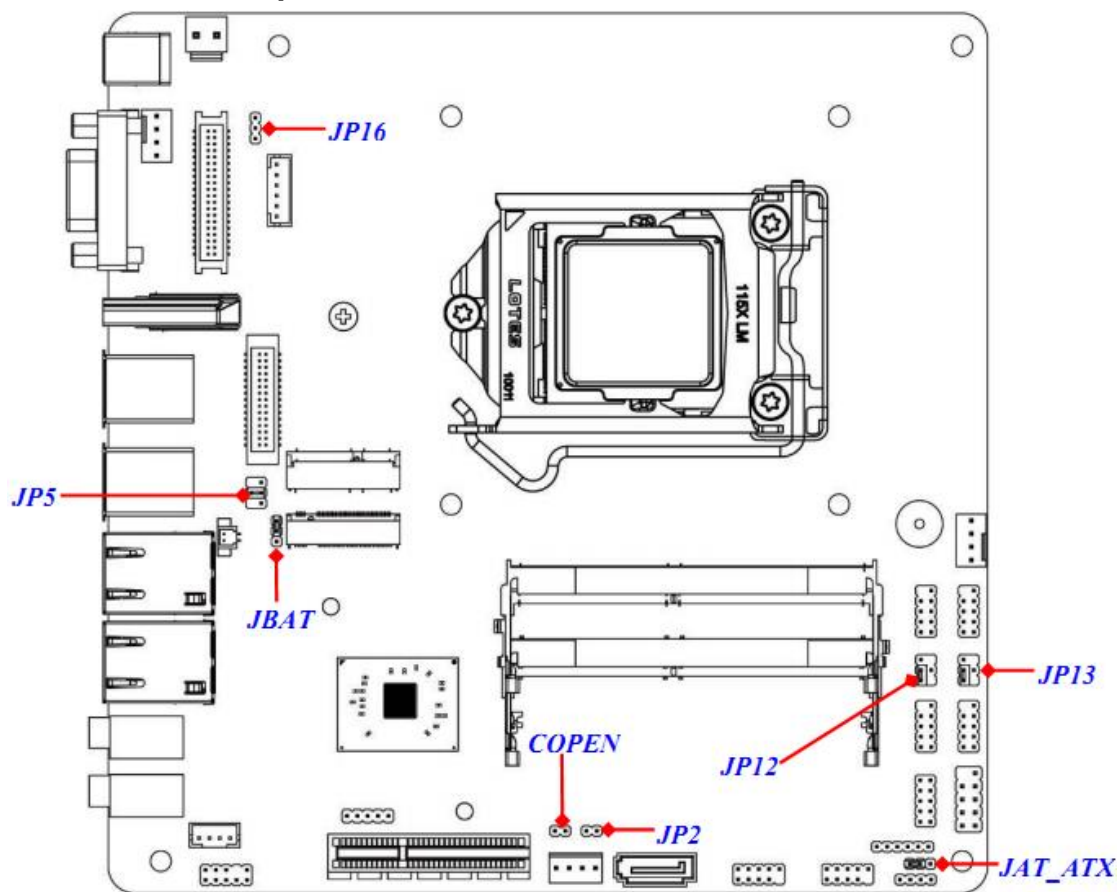
Connectors

P/N	Name
DCIN1	12V~24V DC–in Power Jack
VGA	VGA Port Connector
HDMI	HDMI Port Connector
USB1/USB2	USB 3.0 Port Connector X4
LAN1	1.0Gbps RJ-45 LAN Connector
LAN 2	2.5Gbps RJ-45 LAN Connector
HMIC	Audio MIC Connector
HOUT	Audio Line-out Connector
DCIN3	Internal 12V~24V DC–in Power Connector
SATA1	SATAIII Connector
PWROUT	SATA Power-out Connector
CPUFAN	CPUFAN Connector
SYSFAN	System Fan Connector

Headers & Wafer

P/N	Name	Description	Pitch
FP	Front Panel Header (PWR LED / HD LED / Power Button / Reset)	9-pin Block	2.54mm
FP_USB1/ FP_USB2	USB 2.0 Port Headers	9-pin Block	2.0mm
FP_USB3	USB 2.0 Port Header	4-pin Block	2.0mm
PS2KBMS	PS/2 Keyboard & Mouse Header	6-pin Block	2.0mm
SMBUS	SMBUS Header	5-pin Block	2.0mm
FP_AUDIO	Front Panel Audio Header	9-pin Block	2.0mm
SPEAK_CON	3W Amplifier Wafer	4-pin Block	2.0mm
COM1/2/3/4	RS232 Serial Port Headers	9-pin Block	2.0mm
GPIO	GPIO Port Header	10-pin Block	2.54mm
LVDS	LVDS Port Wafer	30-pin Block	1.25mm
INVERTER1	LVDS Inverter Wafer	6-pin Block	2.0mm
eDP	eDP Port Wafer	40-pin Block	1.25mm

Jumper

P/N	Name	Description	Pitch
JBAT	Clear CMOS RAM Settings	3-pin Block	2.0mm
JAT_ATX	ATX/AT Mode Select	3-pin Block	2.0mm
JP2	ME Features Select	2-pin Block	2.0mm
COPEN	Case Open Message Display Function	2-pin Block	2.0mm
JP5	Panel Power VCC Select	4-pin Block	2.0mm
JP16	Inverter Backlight VCC Select	3-pin Block	2.0mm
JP12	COM1 Port Pin9 Function Select	4-pin Block	2.0mm
JP13	COM2 Port Pin9 Function Select	4-pin Block	2.0mm

Chapter 2   Hardware Installation

2-1 Jumper Setting

JBAT (3-pin): Clear CMOS RAM Settings   Pitch=2.0mm
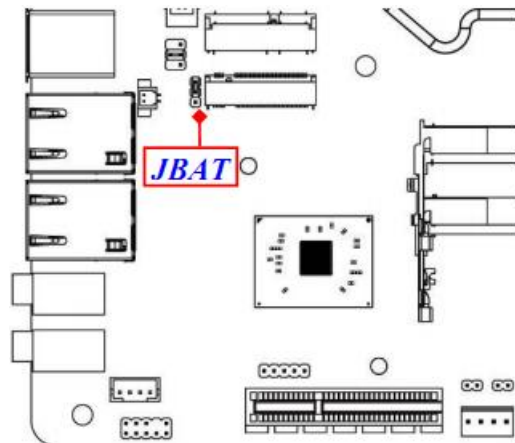
JBAT→Clear CMOS
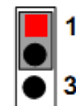
1-2 Closed: Normal(Default);
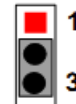
2-3 Closed: Clear CMOS Settings.

JAT_ATX(3-pin): ATX Mode/ AT Mode Select   Pitch=2.0mm
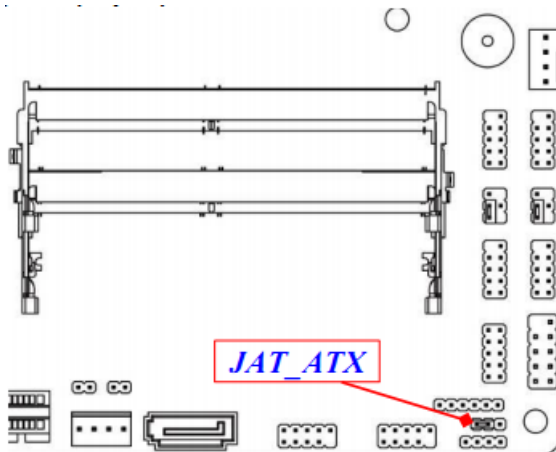
JAT_ATX→ATX/AT Mode Select
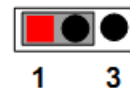
1-2 Closed: ATX Mode Selected;

2-3 Closed: AT Mode Selected.

ATX Mode Selected: Press power button to power on after power input ready;

AT Mode Selected: Directly power on as power input ready.

JP2 (2-pin): ME Features Select   Pitch=2.0mm
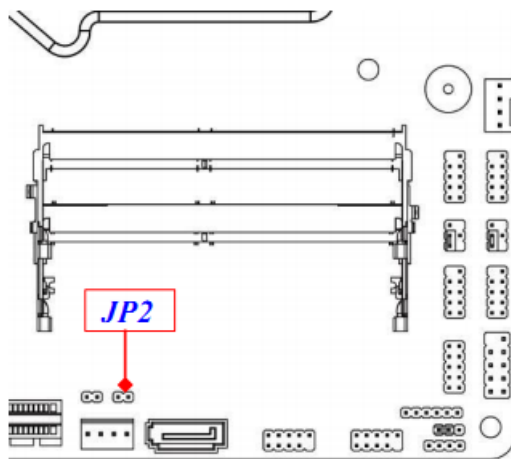
JP2→ME Features Select
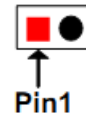
Pin1

1-2 Open: Enable ME Features;

Pin1

1-2 Closed: Disable ME Features.

COPEN (2-pin): Case Open Message Display Function   Pitch=2.0mm
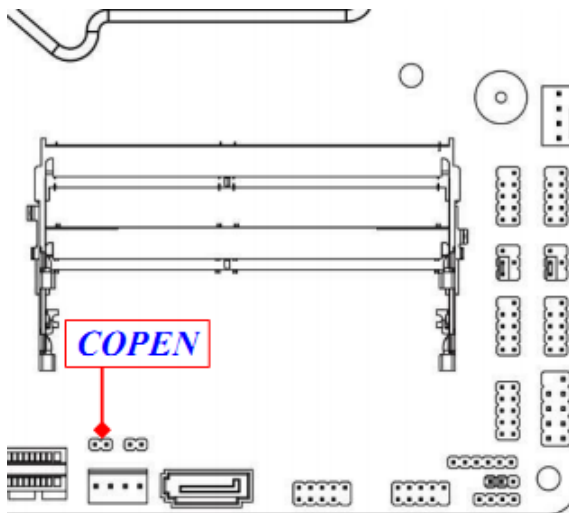
COPEN→Case Open Detection

CASE OPEN

GND
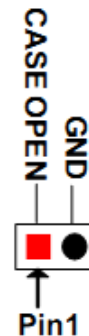
Pin1

Pin 1-2 Short: When Case open function pin short to GND, the Case open function was detected. When Used, needs to enter BIOS and enable 'Case Open Detect' function. In this case if your case is removed, next time when you restart your computer, a message will be displayed on screen to inform you of this.

JP5 (4-pin): LVDS Panel Power VCC Select   Pitch=2.0mm

JP5→LVDS Panel Power VCC Select

1 ● ● 2	1 ● ● 2	1 ● ● 2
3 ● ● 4	3 ● ● 4	3 ● ● 4
5 ● ● 6	5 ● ● 6	5 ● ● 6
2-4 Closed: VCC=3.3V;	**3-4 Closed:** VCC=5V;	**4-6 Closed:** VCC=12V.
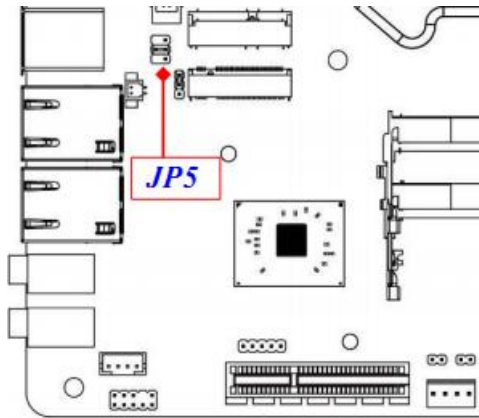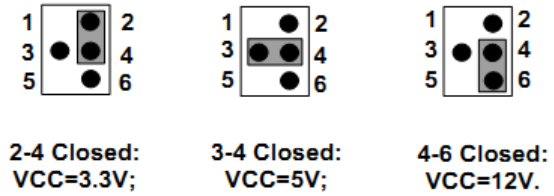
JP16 (3-pin): LVDS Inverter Backlight VCC Select   Pitch=2.0mm

JP16→LVDS INVERTER Backlight VCC

1-2 Closed: Inverter backlight VCC=5V;
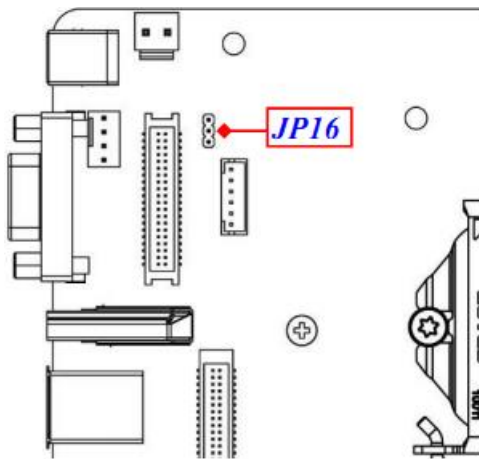
2-3 Closed: Inverter backlight VCC=12V.
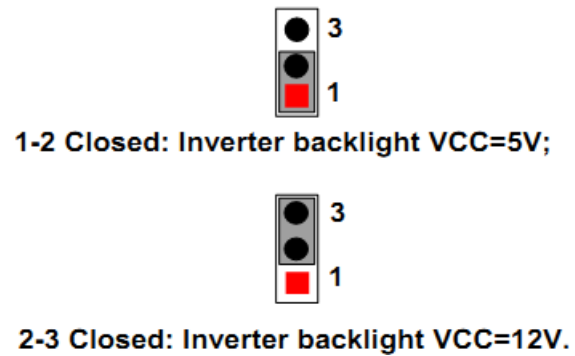
JP12 (4-pin): COM1 Pin9 Function Select   Pitch=2.0mm

JP12→COM1 Pin9 Function Select

6 ● ● 5	6 ● ● 5	6 ● ● 5
4 ● ● 3	4 ● ● 3	4 ● ● 3
2 ● ● 1	2 ● ● 1	2 ● ● 1
2-4 Closed: Pin9=RS232;	**3-4 Closed:** Pin9 = 5V;	**6-4 Closed:** Pin9 = 12V.
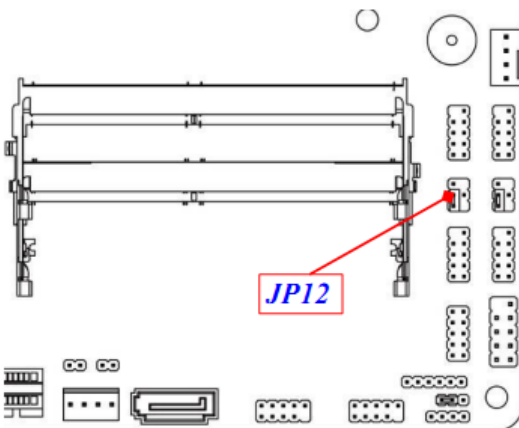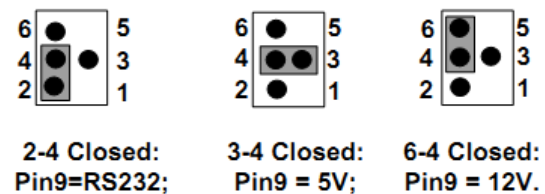
JP13 (4-pin): COM2 Pin9 Function Select   Pitch=2.0mm
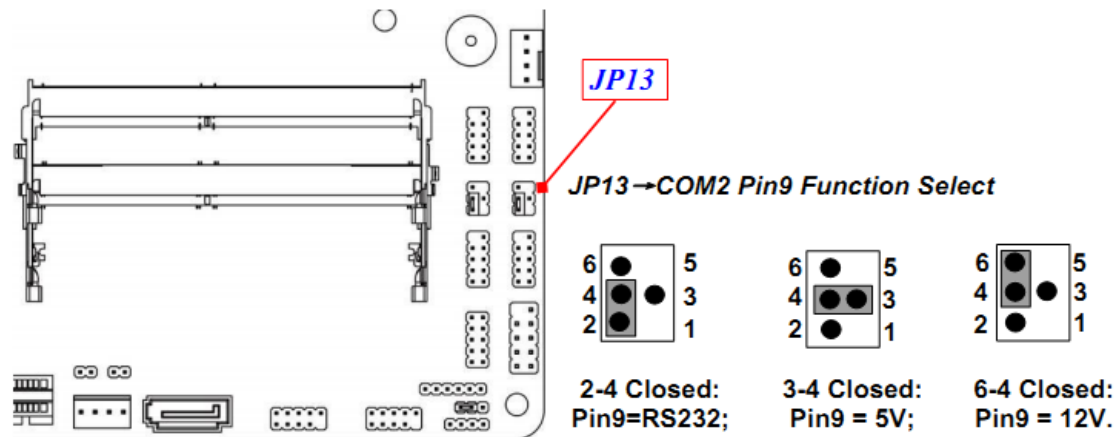
2-2 Connectors, Headers and Wafers

2-2-1   Connectors

(1) Rear Panel Connectors

*Refer to Page-3 Rear IO Diagram.

Icon	Name	Function
	DC-In Power Jack	12V~24V DC–in system power connector For user to connect compatible power adapter to provide power supply for the system.
	VGA Port	To connect display device that support VGA specification.
	HDMI Port	To connect display device that support HDMI specification.
	USB 3.0 Port	To connect USB keyboard, mouse or other devices compatible with USB specification. USB 3.0 ports supports up to 5Gbps data transfer rate.
	RJ-45 LAN Port	This connector is standard RJ-45 LAN jack for Network connection.
	MIC Connector	User can connect microphone device to this port.
	Line-Out Connector	For user to connect external speaker, earphones, etc to transfer system audio output.

(2)   DCIN3 (2-pin block):Internal 12V~24V Power Connector

Pin No.	Definition
1	+12V～24V
2	GND
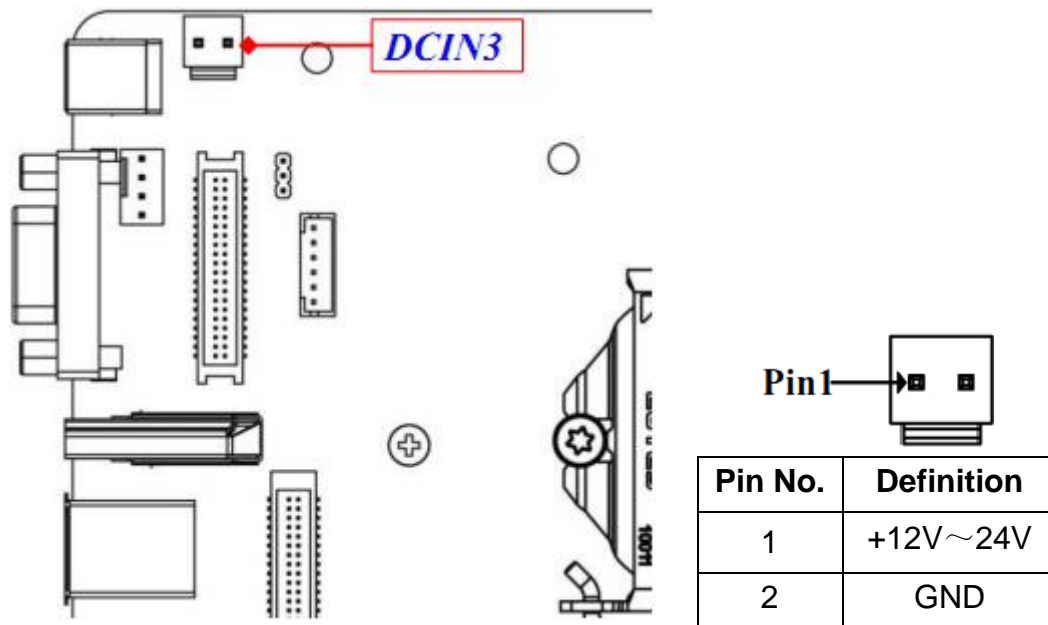
Warning: *Find Pin-1 position before connecting power cable to this 2-pin power connector.* **WRONG INSTALLATION DIRECTION WILL DAMAGE THE BOARD!!**

(3)   CPUFAN (4-pin): CPU Fan Connector

Pin1
GND
+12V Fan Power
Fan Speed
Control
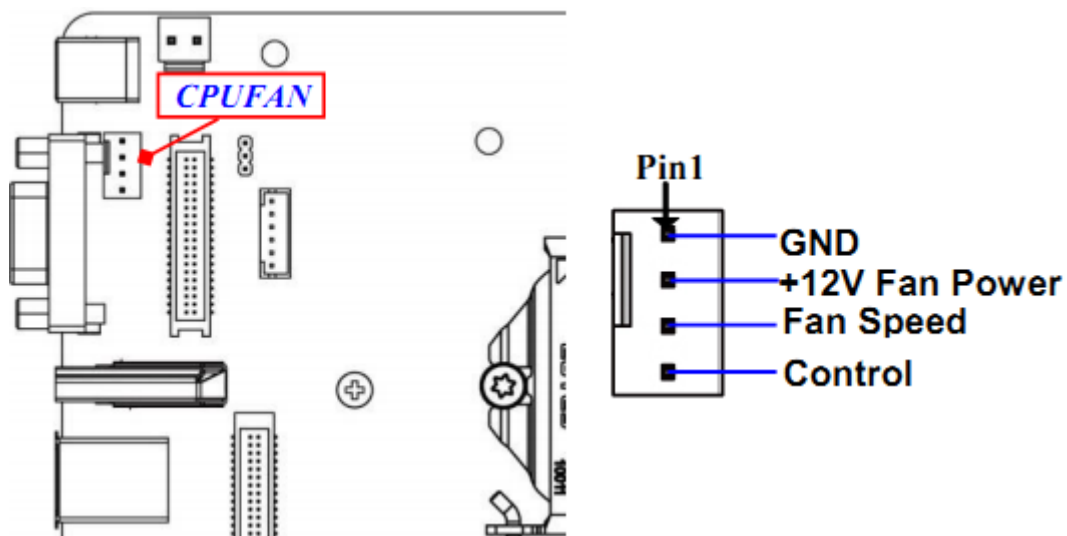
(4) SYSFAN (4-pin): System Fan Connector

Control ——
Fan Speed ——
+12V Fan Power ——
GND ——
Pin1
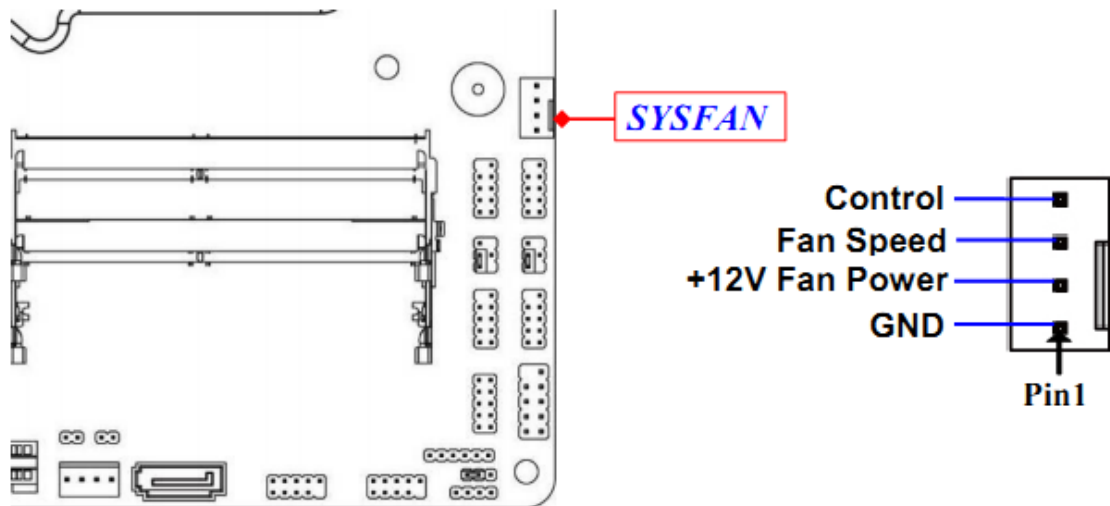
(5) SATA1 (7-pin): SATA III Port connector

SATA1 is a high-speed SATAIII port that supports 6GB/s transfer rate.

Pin No.	Definition
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND
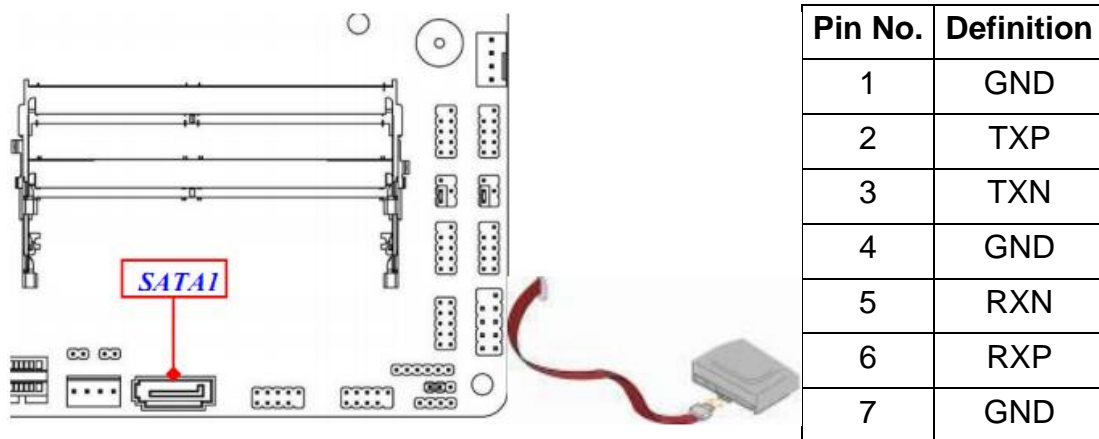
(6) PWROUT (4-pin): SATA Power Out Connector

Pin 1 →

+5V GND GND +12V
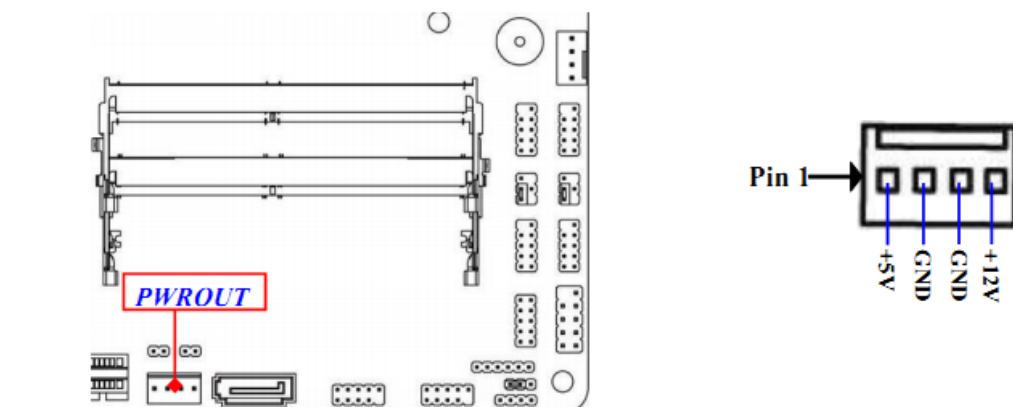
Warning: Make sure that Pin-1 of compatible SATA Power connector is inserted into corresponding Pin-1 of SATAPW to avoid possible damage to the board and hard disk driver!

(7) BATCON (2-pin): Battery Connector
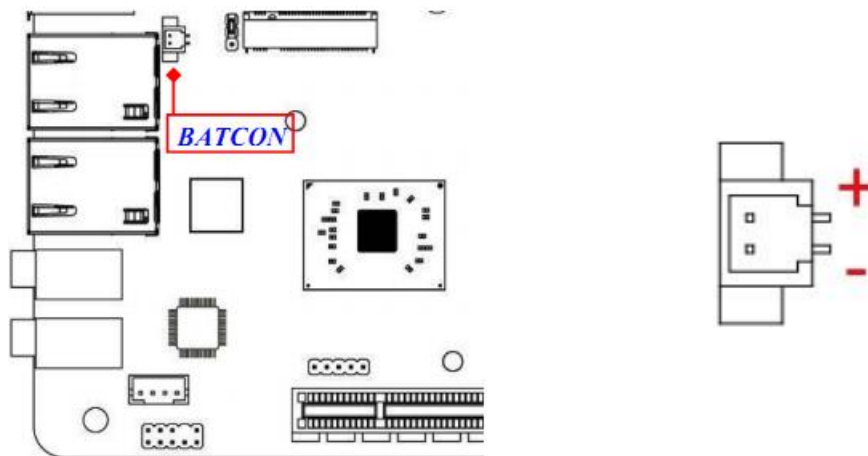
2-2-2   Headers & Wafers

(1) FP (9-pin): Front Panel Header   Pitch=2.54mm
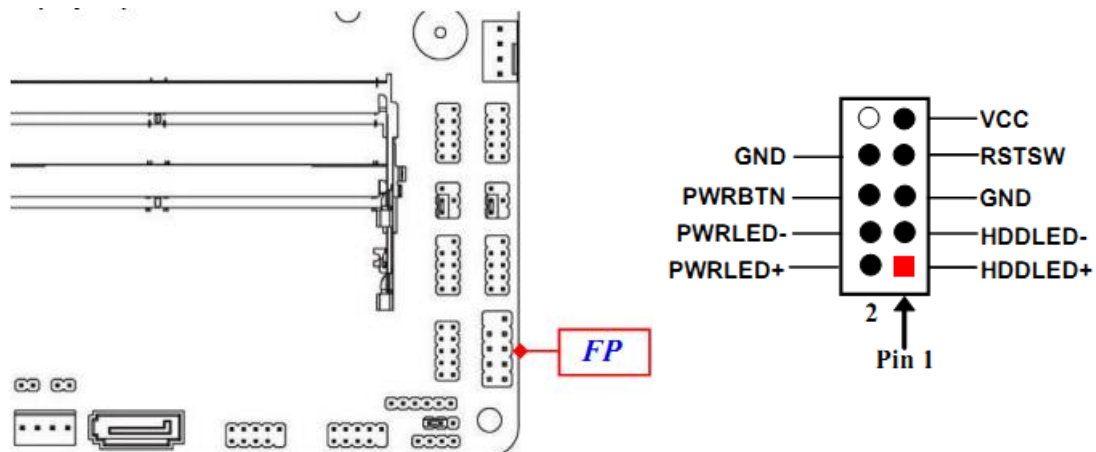
(2) FP_USB1/FP_USB2 (9-pin): USB 2.0 Port Headers   Pitch=2.0mm
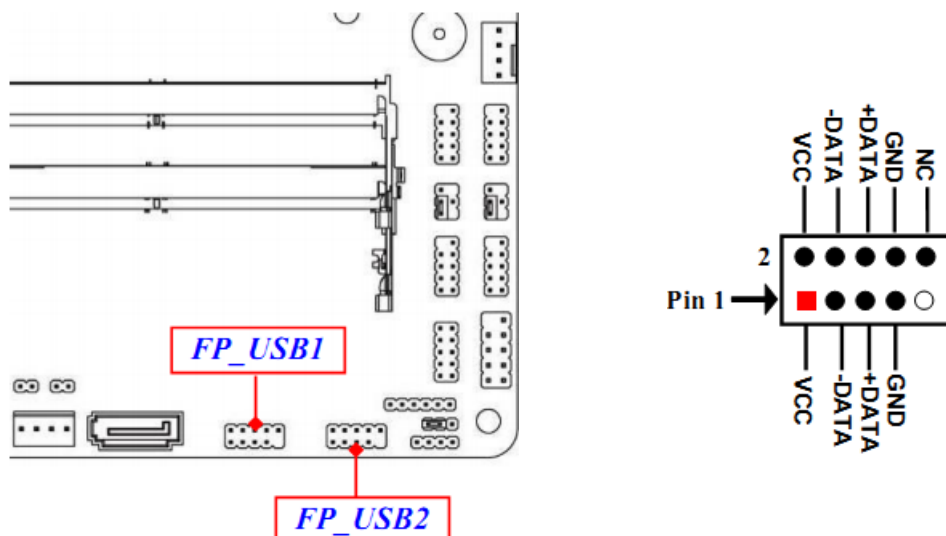
(3) FP_USB3 (4-pin): USB 2.0 Port Header   Pitch=2.0mm
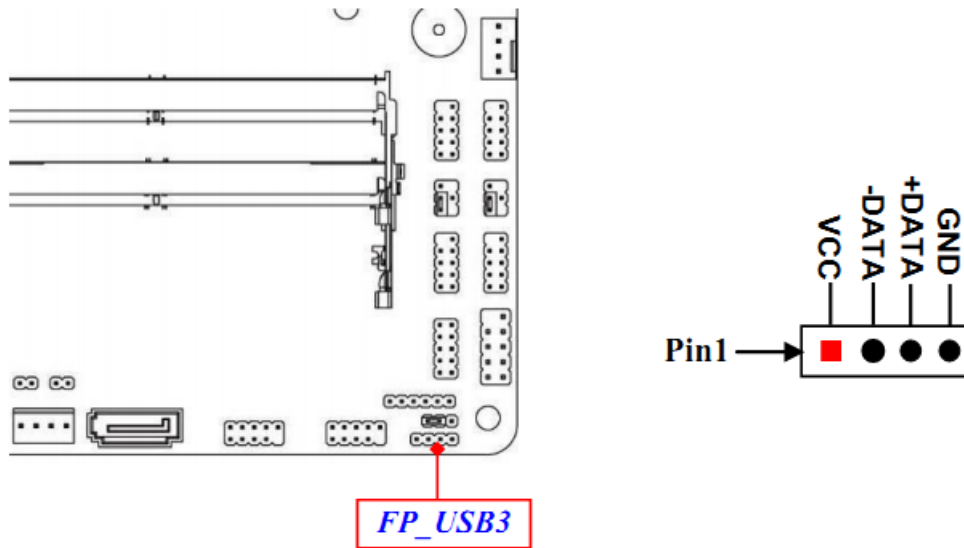
(4) PS2KBMS (6-pin): PS/2 Keyboard & Mouse Header   Pitch=2.0mm
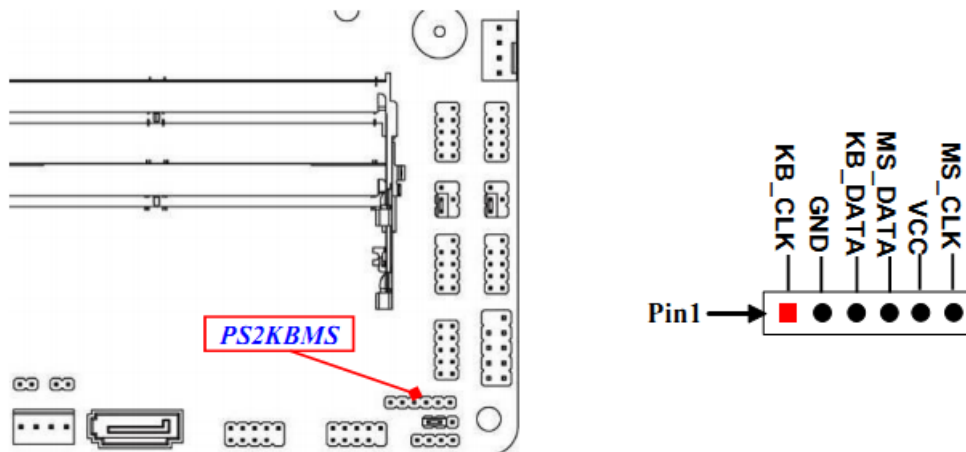
(5) SMBUS (5-Pin): SMBUS Header   Pitch=2.0mm
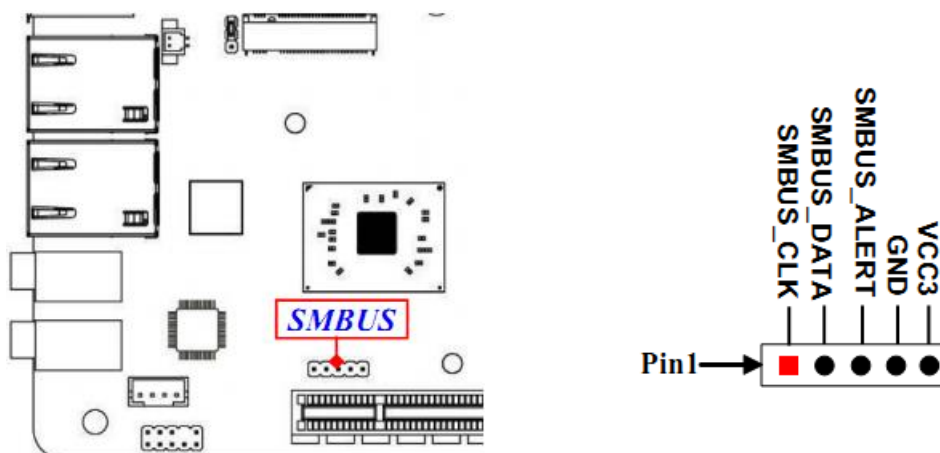
(6) FP_AUDIO (9-pin): Front Panel Audio Header   Pitch=2.0mm

This header connects to Front Panel Line-out, MIC-In connector with cable.

FP_AUDIO

GND	LINE_OUT_JD
DETECT	
MIC_JD	
	LINE OUT-L
MIC2-L	SENSE
MIC2-R	LINE OUT-R
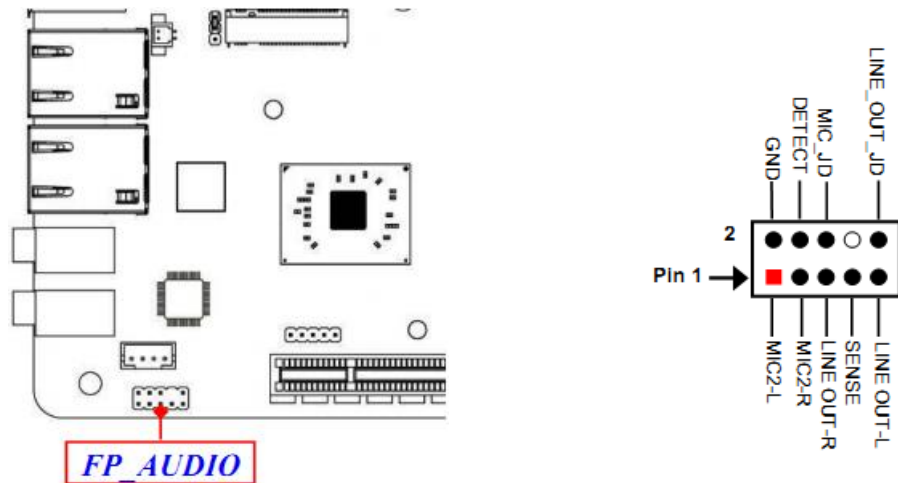
(7) SPEAK_CON (4-pin): 3W Amplifier Wafer   Pitch=2.0mm

SPEAK_CON

Pin No.	Definition
1	L-
2	L+
3	R+
4	R-
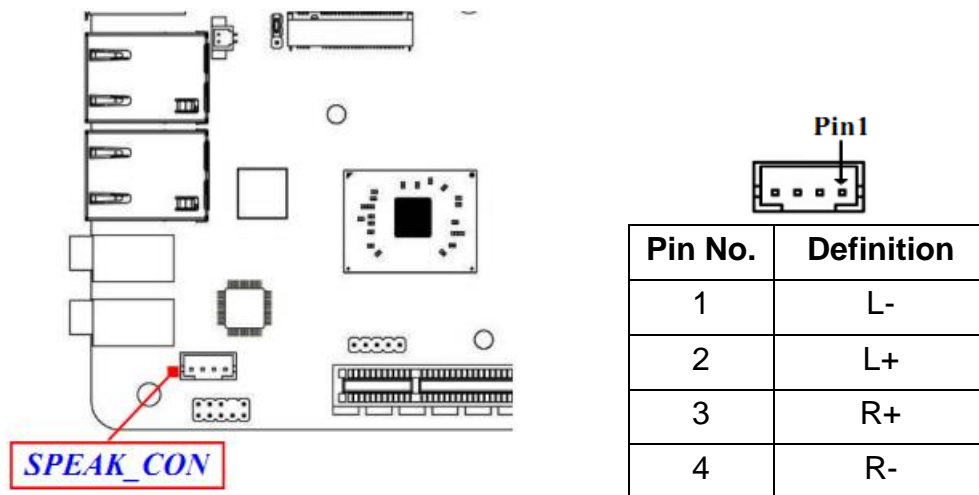
(8) COM1/2/3/4 (9-pin): RS232 Serial Port Header   Pitch=2.0mm

COM3
COM4
COM2
COM1

	GND
RI	DTR
CTS	SOUT
RTS	SIN
DSR	DCD

6
Pin 1
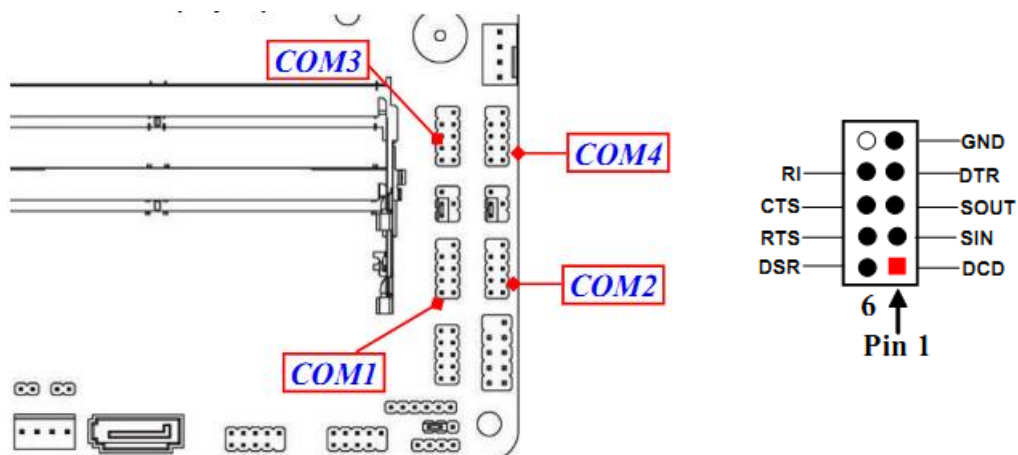
(9)   GPIO (10-pin): GPIO Header   Pitch=2.54mm
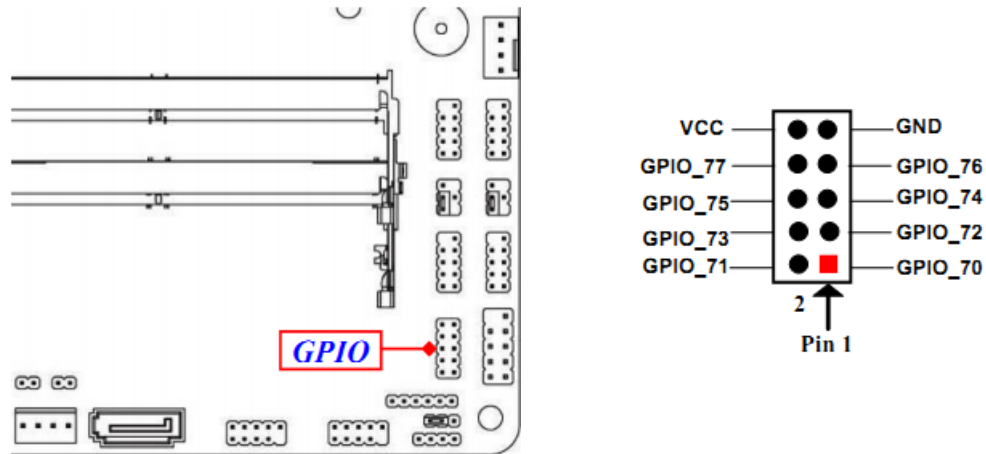
(10) INVERTER1 (6-Pin): LVDS Inverter Header   Pitch=2.0mm

Pin No.	Definition
1	BKLT_PWR1
2	BKLT_PWR2
3	BKLT_EN
4	BKLT_PWM
5	GND1
6	GND2
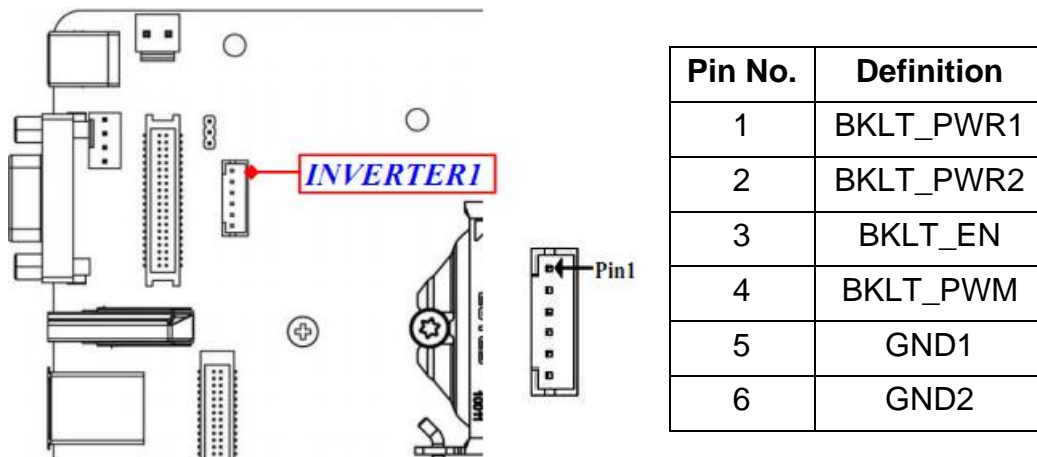
Warning! *Find Pin-1 location of the inverter and make sure that the installation direction is correct! Otherwise serious harm will occur to the board/display panel!!*

(11) LVDS (30-Pin): LVDS Port Wafer   Pitch=1.25mm
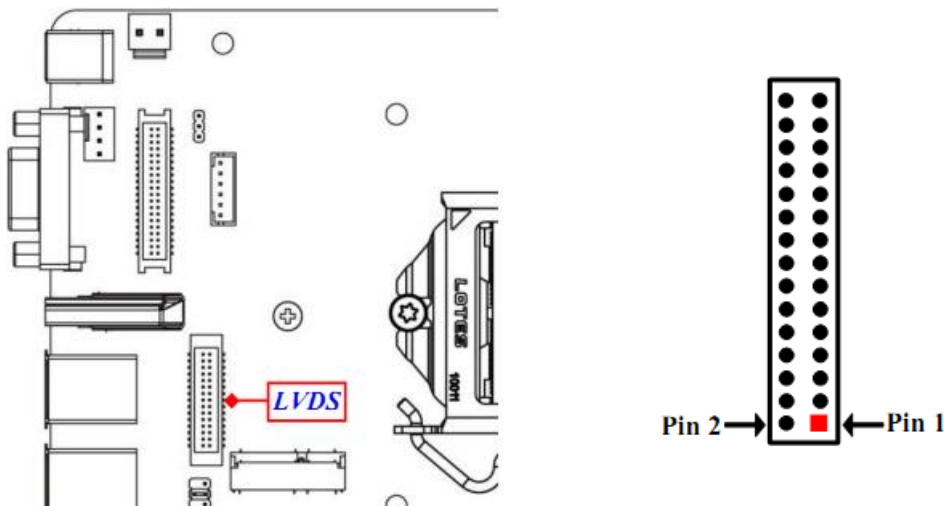
Pin NO.	Pin Define	Pin NO.	Pin Define
Pin 1	LVDSB_DATAN3	Pin 2	LVDSB_DATAP3
Pin 3	LVDS_CLKBN	Pin 4	LVDS_CLKBP
Pin 5	LVDSB_DATAN2	Pin 6	LVDSB_DATAP2
Pin 7	LVDSB_DATAN1	Pin 8	LVDSB_DATAP1
Pin 9	LVDSB_DATAN0	Pin 10	LVDSB_DATAP0
Pin 11	NC/DDC_DATA	Pin 12	NC/DDC_CLK
Pin 13	GND	Pin 14	GND
Pin 15	GND	Pin 16	GND
Pin 17	LVDSA_DATAP3	Pin 18	LVDSA_DATAN3
Pin 19	LVDS_CLKAP	Pin 20	LVDS_CLKAN
Pin 21	LVDSA_DATAP2	Pin 22	LVDSA_DATAN2
Pin 23	LVDSA_DATAP1	Pin 24	LVDSA_DATAN1
Pin 25	LVDSA_DATAP0	Pin 26	LVDSA_DATAN0
Pin 27	PVCC	Pin 28	PVCC
Pin 29	PVCC	Pin 30	PVCC

(12) eDP (40-pin): eDP Port Wafer   Pitch=1.25mm
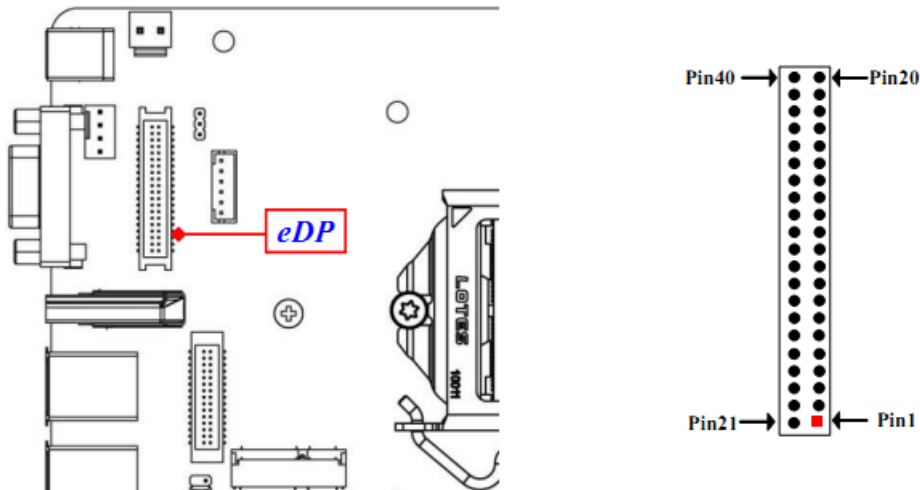
Pin NO.	Pin Define	Pin NO.	Pin Define
Pin 1	NC	Pin 21	NC
Pin 2	GND	Pin 22	NC
Pin 3	Lane3_N	Pin 23	GND
Pin 4	Lane3_P	Pin 24	GND
Pin 5	GND	Pin 25	GND

Pin 6	Lane2_N	Pin 26	GND
Pin 7	Lane2_P	Pin 27	HPD
Pin 8	GND	Pin 28	GND
Pin 9	Lane1_N	Pin 29	GND
Pin 10	Lane1_P	Pin 30	GND
Pin 11	GND	Pin 31	GND
Pin 12	Lane0_N	Pin 32	BL_ENABLE
Pin 13	Lane0_P	Pin 33	BL_PWM_DIM
Pin 14	GND	Pin 34	NC
Pin 15	AUX_CH_P	Pin 35	NC
Pin 16	AUX_CH_N	Pin 36	BL_PWR
Pin 17	GND	Pin 37	BL_PWR
Pin 18	LCD_VCC	Pin 38	BL_PWR
Pin 19	LCD_VCC	Pin 39	BL_PWR
Pin 20	LCD_VCC	Pin 40	NC

Chapter 3   Introducing BIOS

Notice! The BIOS options in this manual are for reference only. Different configurations may lead to difference in BIOS screen and BIOS screens in manuals are usually the first BIOS version when the board is released and may be different from your purchased motherboard.

The BIOS is a program located on a Flash Memory on the motherboard. This program is a bridge between motherboard and operating system. When you start the computer, the BIOS program will gain control. The BIOS first operates an auto-diagnostic test called POST (power on self test) for all the necessary hardware, it detects the entire hardware device and configures the parameters of the hardware synchronization. Only when these tasks are completed done it gives up control of the computer to operating system (OS). Since the BIOS is the only channel for hardware and software to communicate, it is the key factor for system stability, and in ensuring that your system performance as its best.

3-1 Entering Setup

Power on the computer and by pressing <Del> immediately allows you to enter Setup. If the message disappears before your respond and you still wish to enter Setup, restart the system to try again by turning it OFF then ON or pressing the "RESET" button on the system case. You may also restart by simultaneously pressing <Ctrl>,<Alt> and <Delete> keys. If you do not press the keys at the correct time and the system does not boot, an error message will be displayed and you will again be asked to

```
        Please select boot device:

Enter Setup

    ↑ and ↓ to move selection
   ENTER to select boot device
    ESC to boot using defaults
```
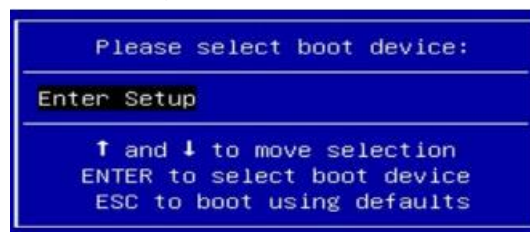
Press <Del> to enter Setup; press < F7> to enter pop-up Boot menu.

3-2 BIOS Menu Screen

The following diagram show a general BIOS menu screen:

Menu Bar

```
                Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
  Main  Advanced  Chipset  Security  Boot  Save & Exit

  BIOS Information                                             Set the Date. Use Tab to
  BIOS Vendor            American Megatrends                   switch between Date elements
  Filename              C8H31A07
  Build Date and Time   04/18/2022 16:37:08

  System Date           [Fri 04/29/2022]                      General Help Items
  System Time           [00:03:08]


                                                              →←: Select Screen
                                                              ↑↓: Select Item
                                                              Enter: Select
                                                              +/-: Change Opt.
                                                              F1: General Help
                                                              F2: Previous Values
                                                              F3: Optimized Defaults
                                                              F4: Save & Exit
                                                              ESC: Exit



                Version 2.20.1271. Copyright (C) 2022 American Megatrends, Inc.
```

Menu Items

Current Setting Value

Function Keys

BIOS Menu Screen

3-3 Function Keys

In the above BIOS Setup main menu of, you can see several options. We will explain these options step by step in the following pages of this chapter, but let us first see a short description of the function keys you may use here:

- Press ← → (left, right) to select screen;
- Press ↑ ↓ (up, down) to choose, in the main menu, the option you want to confirm or to modify.
- Press **<Enter>** to select.
- Press **<+>** / **<−>** keys when you want to modify the BIOS parameters for the active option.
- **[F1]:** General help.
- **[F2]:** Previous values.
- **[F3]:** Optimized defaults.
- **[F4]:** Save & Exit.
- Press **<Esc>** to exit from BIOS Setup.

3-4 Getting Help

Main Menu

The on-line description of the highlighted setup function is displayed at the top right corner the screen.

Status Page Setup Menu/Option Page Setup Menu

Press **[F1]** to pop up a small help window that describes the appropriate keys to use and the possible selections for the highlighted item. To exit the Help Window, press **<Esc>**.

3-5 Menu Bars

There are six menu bars on top of BIOS screen:

Main	To change system basic configuration
Advanced	To change system advanced configuration
Chipset	To change chipset configuration
Security	Password settings
Boot	To change boot settings
Save & Exit	Save setting, loading and exit options.

User can press the right or left arrow key on the keyboard to switch from menu bar. The selected one is highlighted.

3-6 Main Menu

Main menu screen includes some basic system information. Highlight the item and then use the **<+>** or **<->** and numerical keyboard keys to select the value you want in each item.

```
              Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

 BIOS Information                                              Set the Date. Use Tab to
 BIOS Vendor                   American Megatrends            switch between Date elements.
 Filename                      C8H31A07
 Build Date and Time           04/18/2022 16:37:08

 System Date                   [Fri 04/29/2022]
 System Time                   [00:03:08]



                                                             →←: Select Screen
                                                             ↑↓: Select Item
                                                             Enter: Select
                                                             +/-: Change Opt.
                                                             F1: General Help
                                                             F2: Previous Values
                                                             F3: Optimized Defaults
                                                             F4: Save & Exit
                                                             ESC: Exit



              Version 2.20.1271. Copyright (C) 2022 American Megatrends, Inc.
```

System Date

Set the date. Please use [Tab] to switch between date elements.

System Time

Set the time. Please use [Tab] to switch between time elements.

3-7 Advanced Menu

```
              Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

 ► Connectivity Configuration                                Configure Connectivity related
 ► CPU Configuration                                         options
 ► SATA Configuration
 ► PCH-FW Configuration
 ► Trusted Computing
 ► ACPI Settings
 ► Wake-up Function Settings
 ► Super IO Configuration
 ► PC Health Status
 ► Serial Port Console Redirection
 ► USB Configuration
 ► Network Stack Configuration
 ► CSM Configuration
 ► NVMe Configuration                                        →←: Select Screen
                                                             ↑↓: Select Item
 ► Intel(R) Ethernet Controller I225-V - 00:30:18:07:DB:45   Enter: Select
 ► Intel(R) Ethernet Connection (7) I219-V - 00:30:18:97:00:6D  +/-: Change Opt.
                                                             F1: General Help
                                                             F2: Previous Values
                                                             F3: Optimized Defaults
                                                             F4: Save & Exit
                                                             ESC: Exit



              Version 2.20.1271. Copyright (C) 2022 American Megatrends, Inc.
```

► **Connectivity Configuration**

Use this item to configure Connectivity related options. Press **[Enter]** to

make settings for the following sub-items:

CNVi present

CNVi Configuration

CNVi Mode

This option configures Connectivity.

The optional settings: [Disabled Integrated]; [Auto Detection].

[Auto Detection] means that if Discrete Solution is discovered it will be enabled by default. Otherwise Integrated Solution (CNVi) will be enabled;

[Disabled Integrated] disables Integrated Solution.

► **CPU Configuration**

Press **[Enter]** to view current CPU configuration and make settings for the following sub-items:

Intel (VMX) Virtualization Technology

The optional settings: [Enabled]; [Disabled].

When set as [Enabled], a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

Intel(R) SpeedStep(tm)

This item allows more than two frequency ranges to be supported.

The optional settings: [Disabled]; [Enabled].

C states

Use this item to enable or disable CPU power management.

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], it allows CPU to go to C states when it is not 100% utilized.

Turbo Mode

Use this item to enable or disable Turbo Mode.

The optional settings: [Disabled]; [Enabled].

*Note: This item might not be available depending on configuration.

► **SATA Configuration**

Press **[Enter]** to make settings for the following sub-items:

SATA Configuration

SATA Controller(s)

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], user can make further settings in the following items:

SATA Mode Selection

Use this item to Determines how SATA controller(s) operate. This PCH SKU doesn't support RST feature

The default setting is: [AHCI].

SATA1

26

Port

Use this item to enable or disable device connected respective port.

The optional settings: [Disabled]; [Enabled].

Hot Plug

Use this item to Designates this port as Hot Pluggable

The optional settings: [Disabled]; [Enabled].

M.2

Port

The optional settings: [Disabled]; [Enabled].

Use this item to enable or disable M2M port.

► **PCH-FW Configuration**

Press **[Enter]** to view ME information and make settings in the following sub-item:

TPM Device Selection

Selects TPM device: PTT or dTPM. PTT-Enables PTT in SkuMgr dTPM 1.2 Disables PTT in SkuMgr

The optional settings: [dTPM]; [PTT].

Warning! PTT/dTPM will be disabled and all data saved on it will be lost.

► Firmware Update Configuration

Use this item to configure Management Engine Technology parameters.

Press **[Enter]** to make settings for '**ME FW Image RE-Flash**'.

ME FW Image Re-Flash

Use this item to enable or disable ME FW Image Re-Flash function.

The optional settings: [Disabled]; [Enabled].

* In the case that user needs to update ME firmware, user should set '**ME FW Image Re-Flash**' as [Enabled], save the settings and exit. The system will turn off and reboot after 4 seconds. If the user goes to BIOS screen again will find this item is set again as [Disabled], but user can still re-flash to update firmware next time.

► **Trusted Computing**

Press **[Enter]** to make settings for the following sub-items:

Configuration

Security Device Support

Use this item to enables or disables BIOS support for securlty device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available

NO Security Device Found

► **ACPI Settings**

Press **[Enter]** to make settings for the following sub-items:

ACPI Settings

ACPI Sleep State

Use this item to select the highest ACPI sleep state the system will enter when the suspend button is pressed.

The optional settings are: [Suspend Disabled]; [S3 (Suspend to RAM)].

► **Wake-up Function Settings**

Press **[Enter]** to make settings for the following sub-items:

Wake-up System with Fixed Time

Use this item to enable or disable system wake on alarm event.

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], system will wake on the hour/min/sec specified.

Wake-up Hour

Use this item to select 0-23 for example enter 3 for 3am and 15 for 3pm

Wake-up Minute

Use this item to select 0-59

Wake-up Second

Use this item to select 0-59

Wake-up System with Dynamic Time

Use this item to enable or disable system wake on alarm event.

System will wake on the current time + Increase minute(s).

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], system will wake on the current time + increased minute(s).

Wake-up Minute Increase

Use this item to select 1-60

PS2 KB/MS Wake-up

Use this item to enable or disable PS2 KB/MS wake-up from S3/S4/S5.

The optional settings: [Enabled]; [Disabled].

*Note: This function is supported when '**ERP Support**' is set as [Disabled].*

USB S3/S4 Wake-up

Use this item to enable or disable USB S3/S4 wakeup. This function is only supported when ERP function is disabled.

The optional settings: [Enabled]; [Disabled].

*Note: This function is supported when '**ERP Support**' is set as* [Disabled].

USB S5 Power

Use this item to enable or disable USB power after power shutdown.\The optional settings: [Enabled]; [Disabled].

*Note: This function is supported when '**ERP Support**' is set as [Disabled].

► **Super I/O Configuration**

Press **[Enter]** to make settings for the following sub-items:

Super IO Configuration

ERP Support

The optional settings: [Disabled]; [Auto].

Note: *This item should be set as [Disabled] if you wish to have all active wake-up functions.*

► **Serial Port 1 Configuration**

Press **[Enter]** to make settings for the following items:

Serial Port

Use this item to enable or disable serial port (COM).

The optional settings: [Disabled]; [Enabled].

Press **[Enter]** to make settings for the following sub-items:

Device Settings

Change Settings

Use this item to select an optimal setting for super IO device.

Changing setting may conflict with system resources.

The optional settings: [IO=3F8h; IRQ=4]; [IO=3F8h; IRQ=3,4,5,7,10,11] ; [IO=2F8h; IRQ=3,4,5,7,10,11] ; [IO=3E8h; IRQ=3,4,5,7,10,11] ; [IO=2E8h; IRQ=3,4,5,7,10,11]

► **Serial Port 2 Configuration**

Press **[Enter]** to make settings for the following items:

Serial Port

Use this item to enable or disable serial port (COM).

The optional settings: [Disabled]; [Enabled].

Press **[Enter]** to make settings for the following sub-items:

Device Settings

Change Settings

Use this item to select an optimal setting for super IO device.

Changing setting may conflict with system resources.

The optional settings: [IO=2F8h; IRQ=3]; [IO=3F8h; IRQ=3,4,5,7,10,11] ; [IO=2F8h; IRQ=3,4,5,7,10,11] ; [IO=3E8h; IRQ=3,4,5,7,10,11] ; [IO=2E8h; IRQ=3,4,5,7,10,11]

► **Serial Port 3 Configuration**

Press **[Enter]** to make settings for the following items:

Serial Port

Use this item to enable or disable serial port (COM).

The optional settings: [Disabled]; [Enabled].

Press **[Enter]** to make settings for the following sub-items:

Device Settings

29

Change Settings

Use this item to select an optimal setting for super IO device.

Changing setting may conflict with system resources.

The optional settings: [IO=3E8h; IRQ=11]; [IO=3F8h; IRQ=3,4,5,7,10,11] ; [IO=2F8h; IRQ=3,4,5,7,10,11] ; [IO=3E8h; IRQ=3,4,5,7,10,11] ; [IO=2E8h; IRQ=3,4,5,7,10,11]]; [IO=3E0h; IRQ=3,4,5,7,10,11]]; [IO=2E0h; IRQ=3,4,5,7,10,11]

► **Serial Port 4 Configuration**

Press **[Enter]** to make settings for the following items:

Serial Port

Use this item to enable or disable serial port (COM).

The optional settings: [Disabled]; [Enabled].

Press **[Enter]** to make settings for the following sub-items:

Device Settings

Change Settings

Use this item to select an optimal setting for super IO device.

Changing setting may conflict with system resources.

The optional settings: [IO=2E8h; IRQ=10]; [IO=3F8h; IRQ=3,4,5,7,10,11] ; [IO=2F8h; IRQ=3,4,5,7,10,11] ; [IO=3E8h; IRQ=3,4,5,7,10,11] ; [IO=2E8h; IRQ=3,4,5,7,10,11]]; [IO=3E0h; IRQ=3,4,5,7,10,11]]; [IO=2E0h; IRQ=3,4,5,7,10,11]

WatchDog Reset Timer

Use this item to enable or disable WDT reset function.

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], the following sub-items shall appear:

WatchDog Reset Timer Value

User can select a value in the range of [10] to [255] seconds when '**WatchDog Reset Timer Unit**' set as [Sec]; or in the range of [1] to [255] minutes when '**WatchDog Reset Timer Unit**' set as [Min].

WatchDog Reset Timer Unit

The optional settings are: [Sec.]; [Min.].

Case Open Detect

Use this item to detect case has already open or not, show message in POST.

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], system will detect if COPEN has been short or not (refer to **Page 9** COPEN jumper for case open detection); if COPEN is short, system will show Case Open Message during POST.

► **PC Health Status**

Press **[Enter]** to view current hardware health status, or make further

settings in '**SmartFAN Configuration**'.

► **SmartFAN Configuration**

Press **[Enter]** to make settings for SmartFan Configuration:

SmartFAN Configuration

CPUFAN / SYSFAN Smart Mode

The optional settings are: [Disabled]; [Enabled].

When set as [Enabled], the following sub-items shall appear:

CPUFAN / SYSFAN Full-Speed Temperature

Use this item to set CPUFAN/SYSFAN full speed temperature. Fan will run at full speed when above this pre-set temperature.

CPUFAN / SYSFAN Full-Speed Duty

Use this item to set CPUFAN/SYSFAN full-speed duty. Fan will run at full speed when above this pre-set duty.

CPUFAN / SYSFAN Idle-Speed Temperature

Use this item to set CPUFAN /SYSFAN idle speed temperature. Fan will run at idle speed when below this pre-set temperature.

CPUFAN / SYSFAN Idle-Speed Duty

Use this item to set CPUFAN/SYSFAN idle speed duty. Fan will run at idle speed when below this pre-set duty.

► **Serial Port Console Redirection**

COM1

Console Redirection

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], the following sub-items shall appear:

► **Console Redirection Settings**

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

Press **[Enter]** to make settings for the following items:

Terminal Type

The optional settings: [VT100]; [VT100+]; [VT-UTF8]; [ANSI].
Emulation: [ANSI]: Extended ASCII char set; [VT100]: ASCII char set; [VT100+]: Extends VT100 to support color, function keys, etc.; [VT-UTF8]: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.

Bits per second

Use this item to select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

The optional settings: [9600]; [19200]; [38400]; [57600]; [115200].

Data Bits

The optional settings: [7]; [8].

Parity

A parity bit can be sent with the data bits to detect some transmission errors.

The optional settings: [None]; [Even]; [Odd]; [Mark]; [Space].

[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.

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.

The optional settings: [1]; [2].

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.

The optional settings: [None]; [Hardware RTS/CTS].

VT-UTF8 Combo Key Support

Use this item to enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.

The optional settings: [Disabled]; [Enabled].

Recorder Mode

With this mode enable only text will be sent. This is to capture Terminal data.

The optional settings: [Disabled]; [Enabled].

Resolution 100x31

Use this item to enable or disable extended terminal resolution.

The optional settings: [Disabled]; [Enabled].

Putty KeyPad

Use this item to select FunctionKey and KeyPad on Putty.

The optional settings: [VT100]; [Linux]; [XTERMR6]; [SCO]; [ESCN]; [VT400].

__Legacy Console Redirection__

► **Legacy Console Redirection Settings**

Press **[Enter]** to make settings for the following item: Legacy

Console Redirection Settings

Redirection COM Port

For user to select a COM port to display redirection of legacy OS and Legacy OPROM messages.

The optional settings are: [COM1]; [COM1(Pci Bus0, Dev0, Func0) (Disabled)].

Resolution

This item is for user to select the number of Rows and Columns supported redirection.

The optional settings are: [80x24]; [80x25].

Redirect After POST

The optional settings are: [Always Enable]; [Bootloader].

When [Bootloader] is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When [Always Enabled] is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to [Always Enabled].

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

Console Redirection

The optional settings: [Disabled]; [Enabled]. When set as [Enabled], the following sub-items shall appear:

► **Console Redirection Settings**

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

Press **[Enter]** to make settings for the following items:

Out-of-Band Mgmt Port

Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port

The optional settings: [COM1]; [COM1(Pci Bus0, Dec0,Func0) (Disabled)].

Terminal Type

The optional settings: [VT100]; [VT100+]; [VT-UTF8]; [ANSI].

[VT-UTF8] is the preferred terminal type for out-of-band management. The next best choice is [VT100+] and them [VT100]. See above, in Console Redirection Settings page, for more help with Terminal Type/Emulation.

Bits per second

Use this item to select serial port transmission speed. The speed

must be matched on the other side. Long or noisy lines may require lower speeds.

The optional settings: [9600]; [19200]; [57600]; [115200].

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.

The optional settings: [None]; [Hardware RTS/CTS]; [Software Xon/Xoff].

Data Bits

The default setting is: [8].

* This item may or may not show up, depending on different configuration.

Parity

The default setting is: [None].

* This item may or may not show up, depending on different configuration. **Stop Bits**

The default setting is: [1].

* This item may or may not show up, depending on different configuration.

► **USB Configuration**

Use this item to set USB Configuration Parameters.

Press **[Enter]** to make settings for the following sub-items:

__USB Configuration__

Legacy USB Support

The optional settings are: [Enabled]; [Disabled]; [Auto].

[Enabled]: To enable legacy USB support.

[Disabled]: to keep USB devices available only for EFI specification,

[Auto]: To disable legacy support if no USB devices are connected.

XHCI Hand-off

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

The optional settings are: [Enabled]; [Disabled].

USB Mass Storage Driver Support

Use this item to enable/disable USB Mass Storage Driver Support

The optional settings are: [Disabled]; [Enabled].

__USB hardware delay and time-out:__

USB Transfer time-out

Use this item to set the time-out value for control, bulk, and interrupt transfers.

The optional settings are: [1 sec]; [5 sec]; [10 sec]; [20 sec].

Device reset time-out

Use this item to set USB mass storage device start unit command time-out.

The optional settings are: [10 sec]; [20 sec]; [30 sec]; [40 sec].

Device power-up delay

Use this item to set maximum time the device will take before it properly reports itself to the host controller.

The optional settings: [Auto]; [Manual].

[Auto] uses default value: for a root port it is 100 ms, for a hub port the delay is taken from hub descriptor. Select [Manual] you can set value for the following sub-item: **Device Power-up delay in seconds**, the delay range in from 1 to 40 seconds, in one second increments.

► **Network Stack Configuration**

Press **[Enter]** to go to '**Network Stack**' screen to make further settings.

Network Stack

Use this item to enable or disable UEFI Network Stack.

The optional settings: [Disabled]; [Enabled].

When set as [Enabled], the following sub-items shall appear:

Ipv4 PXE Support

The optional settings are: [Disabled]; [Enabled].

Use this item to enable Ipv4 PXE Boot Support. When set as [Disabled], Ipv4 boot option will not be created.

Ipv6 PXE Support

The optional settings are: [Disabled]; [Enabled].

Use this item to enable Ipv6 PXE Boot Support. When set as [Disabled], Ipv6 boot optional will not be created.

PXE boot wait time

Use this item to set wait time to press **[ESC]** key to abort the PXE boot.

Use either +/- or numeric keys to set the value.

Media Detect Count

Use this item to set number of times presence of media will be checked.

Use either +/- or numeric keys to set the value.

► **CSM Configuration**

Press **[Enter]** to make settings for the following sub-items: CSM Support

Use this item to enable or disable CSM Support The optional settings are: [Disabled]; [Enabled].

When set as [Enabled], the following sub-items shall appear:

Option ROM execution

Network

This option controls the execution of UEFI and Legacy PXE OpROM. The optional settings are: [Do not launch]; [Legacy].

Storage

This option controls the execution of UEFI and Legacy Storage OpROM. The optional settings are: [Do not launch]; [UEFI]; [Legacy].

Other PCI devices

This item is for PCI devices other than Network, Mass storage or video defines which OpROM to launch.

The optional settings are: [Do not launch]; [UEFI]; [Legacy].

► **NVMe Configuration**

Press **[Enter]** to check NVMe controller and driver information.

NVMe Configuration
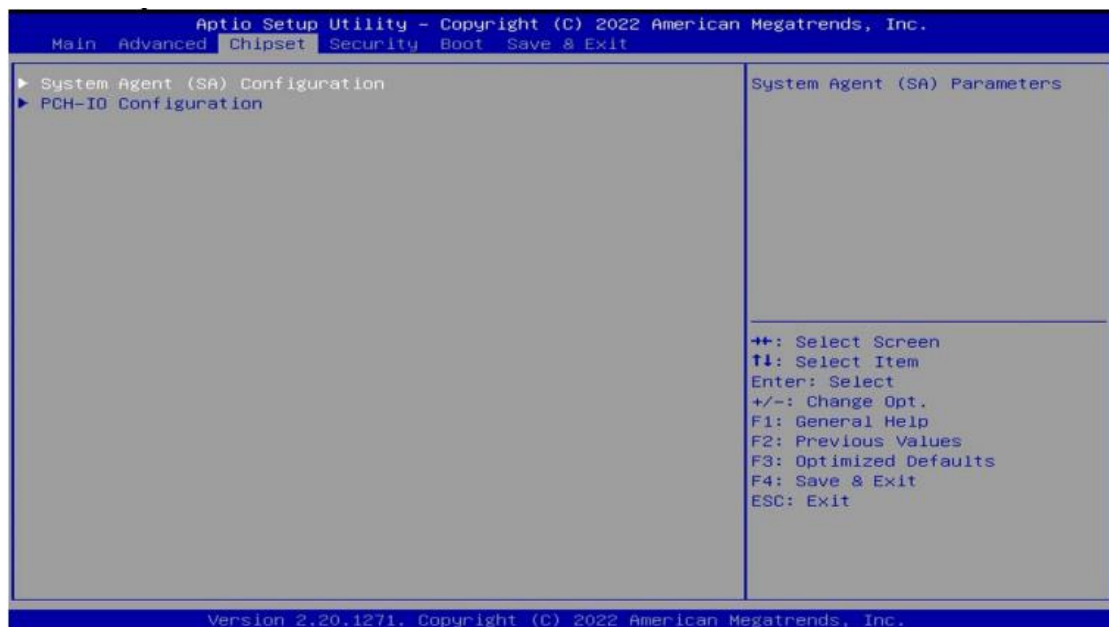
No NVME Device Found

► **Intel(R) Ethernet Controller I225-V- XX:XX:XX:XX:XX:XX**

► **Intel(R) Ethernet Connection (7) I219-V- XX:XX:XX:XX:XX:XX**

These items show current network brief information.

3-8 Chipset Menu

► **System Agent (SA) Configuration**

Press **[Enter]** to make settings for the following sub-items: VT-d

Use this item to enable or disable VT-d capability.

The optional settings are: [Enabled]; [Disabled].

► **Memory Configuration**

Press **[Enter]** to view brief information for the working memory module.

► **Graphics Configuration**

Press **[Enter]** to make further settings for Graphics Configuration.

Graphics Configuration

Primary IGFX Boot Display

Use this item to select the video device which will be activated during POST.

This has no effect if external graphics present.

The optional settings are: [VBIOS Default]; [HDMI]; [VGA]; [LVDS]; [eDP].

Note: *In the case that the '**Primary IGFX Boot Display**' is select as [HDMI],[VGA] [LVDS] or [eDP], user can make further settings in* '**Secondary IGFX Boot Display**':

Secondary IGFX Boot Display

Use this item to select the secondary Display device.

The optional settings are: [Disabled]; [HDMI]; [VGA] and [LVDS].

Aperture Size

Use this item to select the Aperture Size. Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture.

To use this feature, please disable CSM Support.

The optional settings are: [128MB]; [256MB]; [512MB]; [1024MB]; [2048MB].

DVMT Pre-Allocated

Use this item to select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

The optional settings are: [32M]; [64M].

DVMT Total Gfx Mem

Use this item to select DVMT 5.0 Total Graphic Memory size used by the Internal Graphics Device.

The optional settings are: [128M]; [256M]; [MAX].

eDP Backlight Control

Use this item to select Back Light Control settings.

The optional settings are: [PWM Inverted]; [PWM Normal].

LVDS Panel Type

Use this item to manually select LCD panel type.

The optional setting are: [800x 480 18bit Single]; [800x 600 18bit Single]; [800x 600 24bit Single]; [1024 x 600 18bit Single]; [1024 x 768 18bit Single]; [1024 x 768 24bit Single]; [1280 x 768 24bit Single]; [1280 x 800 18bit Single]; [1280 x 800 24bit Single]; [1366 x 768 18bit Single]; [1366 x

768 24bit Single]; [1440 x 900 18bit Dual]; [1440 x 900 24bit Dual]; [1280 x 1024 24bit Dual]; [1680 x 1050 24bit Dual]; [1920 x 1080 24bit Dual].

► **PCH-IO Configuration**

Press **[Enter]** to make settings for the following sub-items:

PCH-IO Configuration

HD Audio

This item controls detection of the HD-Audio device.

The optional settings are: [Disabled]; [Enabled].

[Disabled]: HDA will be unconditionally disabled.

[Enabled]: HDA will be unconditionally enabled.

Onboard Lan1 Controller

Use this item to enable or disable corresponding onboard NIC device or controller.

The optional settings are: [Disabled]; [Enabled].

* When set as [Enabled], the following sub-items shall appear:

    Wake on LAN Enable

    Use this item to enable or disable integrated LAN to wake the system.

    The optional settings are: [Disabled]; [Enabled].

Onboard Lan2 Controller

Use this item to enable or disable corresponding onboard NIC device or controller.

The optional settings are: [Disabled]; [Enabled].

M2E Slot

Use this item to enable or disable M2E slot PCI Express root port function.

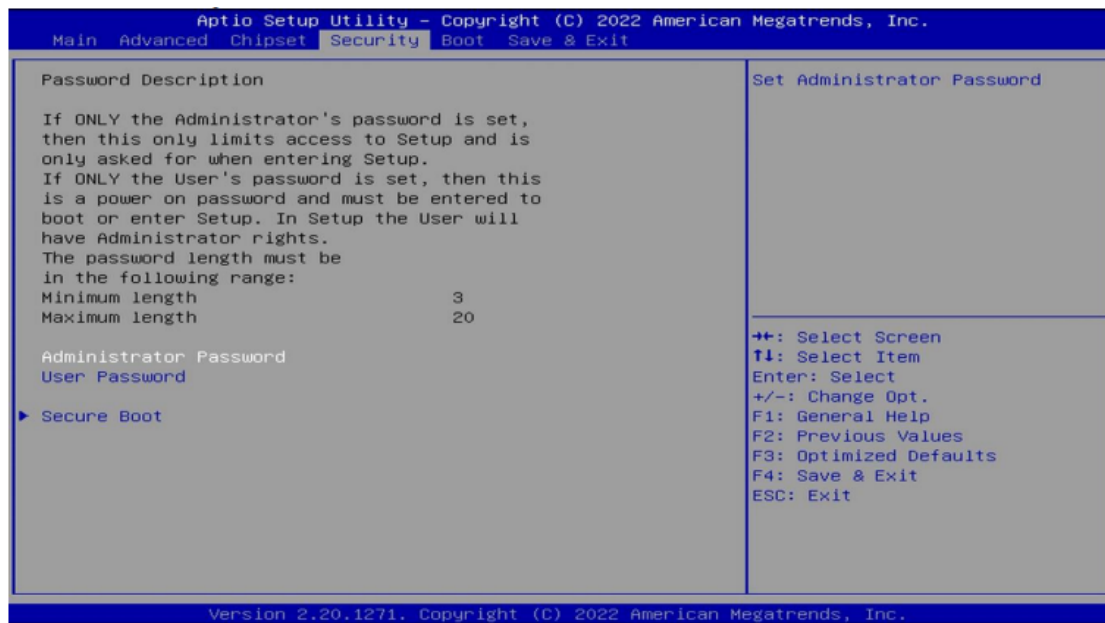The optional settings are: [Disabled]; [Enabled].

PCIE1 Slot

Use this item to enable or disable PCIE1 slot PCI Express root port function. The optional settings are: [Disabled]; [Enabled].

State After G3

Use this item to specify what state to go to when power re-applied after a power failure (G3 state).

The optional settings are: [Always On]; [Always Off]; [Former State].

3-9 Security Menu

```
          Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

   Password Description                               Set Administrator Password

   If ONLY the Administrator's password is set,
   then this only limits access to Setup and is
   only asked for when entering Setup.
   If ONLY the User's password is set, then this
   is a power on password and must be entered to
   boot or enter Setup. In Setup the User will
   have Administrator rights.
   The password length must be
   in the following range:
   Minimum length                    3
   Maximum length                    20
                                                     →←: Select Screen
   Administrator Password                            ↑↓: Select Item
   User Password                                     Enter: Select
                                                     +/-: Change Opt.
 ► Secure Boot                                       F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit



          Version 2.20.1271. Copyright (C) 2022 American Megatrends, Inc.
```

Security menu allow users to change administrator password and user password settings.

Administrator Password

If there is no password present on system, please press **[Enter]** to create new administrator password. If password is present on system, please press **[Enter]** to verify old password then to clear/change password. Press again to confirm the new administrator password.

User Password

If there is no password present on system, please press **[Enter]** to create new administrator password. If password is present on system, please press **[Enter]** to verify old password then to clear/change password. Press again to confirm the new administrator password.

► **Secure Boot**

   Press **[Enter]** to make customized secure settings:

   Secure Boot

   The optional settings are: [Disabled]; [Enabled].

   Secure Boot feature is active if Secure Boot is enabled, Platform Key (PK) is enrolled and the system is in User mode. The mode change requires platform reset.

   Secure Boot Mode

   The optional settings are: [Standard]; [Custom].

   Set UEFI Secure Boot Mode to Standard mode or Custom mode. This change is effective after save. After reset, this mode will return to

39

Standard mode.

In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.

When set as [Custom], user can make further settings in the following items that show up:

► **Restore Factory Keys**

Use this item to force system to User Mode, to install factory default Secure Boot key databases.

► **Reset To Setup Mode**

Use this item to delete all Secure Boot Key databases from NVRAM.

► **Key Management**

This item enables experienced users to modify Secure Boot variables, which includes the following items:

Factory Key Provision

This item is for user to install factory default secure boot keys after the platform reset and while the system is in Setup mode.

The optional settings are: [Disabled]; [Enabled].

► **Restore Factory Keys**

Use this item to force system into User Mode. Install factory default Secure Boot Key databases.

► **Reset to Setup Mode**

Use this item to delete all Secure Boot key databases from NVRAM.

► **Export Secure Boot variables**

Use this item to copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.

► **Enroll Efi Image**

This item allows the image to run in Secure Boot Mode.

Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).

Device Guard Ready

► **Remove 'UEFI CA' from DB**

Device Guard ready system must not list 'Microsoft EFI CA' Certificate in Authorized Signature database (db).

► **Restore DB defaults**

Use this item to restore DB variable to factory defaults.

Secure Boot Variable/Size/Keys/Key Source

► **Platform Key (PK)/Key Exchange Keys/Authorized Signature/Forbidden Signature/ Authorized TimeStamps/OS Recovery Signatures**

Use this item to enroll Factory Defaults or load the keys from a file with:

1. Public Key Certificate in:
    a)   EFI_SIGNATURE_LIST
    b)   EFI_ CERT_X509 (DER encoded)
    c)   EFI_ CERT_RSA2048 (bin)
    d)   EFI_ CERT_SHAXXX (bin)
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)
    Key Source: Factory, External, Mixed.

3-10   Boot Menu
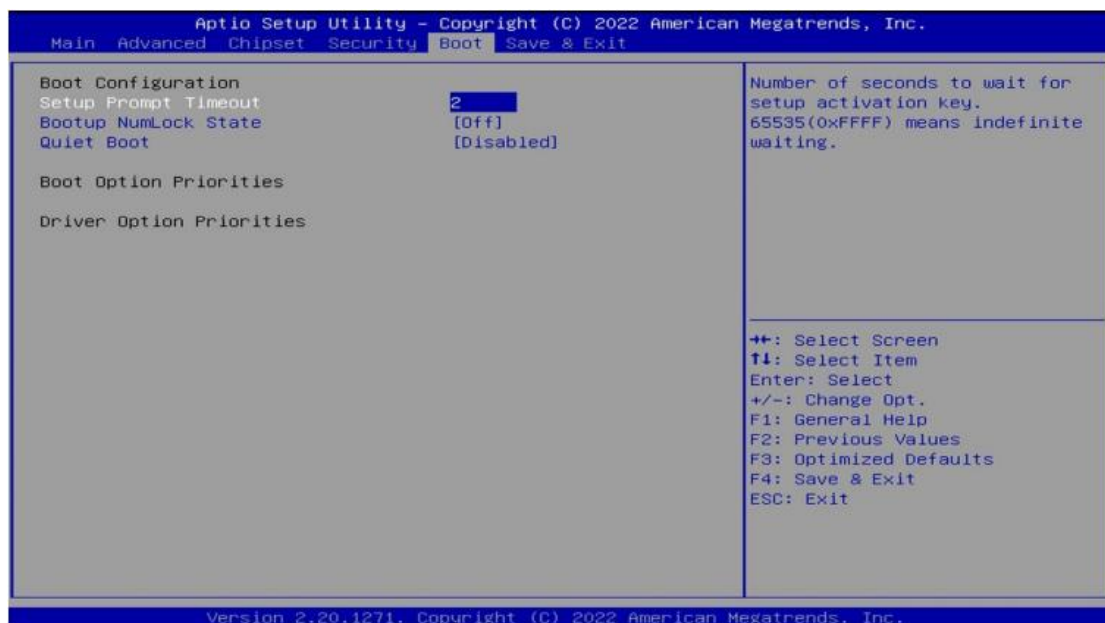
Boot Configuration

Setup Prompt Timeout

Use this item to set number of seconds to wait for setup activation key.

Bootup Numlock State

Use this item to select keyboard numlock state.

The optional settings are: [On]; [Off].

Quiet Boot

The optional settings are: [Disabled]; [Enabled].

Boot Option Priorities

Driver Option Priorities

3-11 Save & Exit Menu

```
              Aptio Setup Utility - Copyright (C) 2022 American Megatrends, Inc.
         Main  Advanced  Chipset  Security  Boot  Save & Exit

         Save Options                                      Reset the system after saving
         Save Changes and Reset                            the changes.
         Discard Changes and Reset

         Default Options
         Restore Defaults
         Save as User Defaults
         Restore User Defaults

         Boot Override


                                                           →←: Select Screen
                                                           ↑↓: Select Item
                                                           Enter: Select
                                                           +/-: Change Opt.
                                                           F1: General Help
                                                           F2: Previous Values
                                                           F3: Optimized Defaults
                                                           F4: Save & Exit
                                                           ESC: Exit




                  Version 2.20.1271. Copyright (C) 2022 American Megatrends, Inc.
```

Save Options

Save Changes and Reset

This item allows user to reset the system after saving the changes.

Discard Changes and Reset

This item allows user to reset the system without saving any changes.

Default Options

Restore Defaults

Use this item to restore /load default values for all the setup options.

Save as User Defaults

Use this item to save the changes done so far as user defaults.

Restore User Defaults

Use this item to restore the user defaults to all the setup options.

Boot Override