

LA20-10(S) Series

User's Manual

No. G03-LA20-F

Rev: 2.0

Release date: December 14, 2022

Trademark:

* Specifications and Information contained in this documentation are furnished for information use only, and are subject to change at any time without notice, and should not be construed as a commitment by manufacturer.

TABLE OF CONTENT

ENVIRONMENTAL SAFETY INSTRUCTION.....	iii
ENVIRONMENTAL PROTECTION ANNOUCEMENT.....	iii
USER'S NOTICE.....	iv
MANUAL REVISION INFORMATION.....	iv
ITEM CHECKLIST.....	iv
CHAPTER 1 INTRODUCTION OF THE MOTHERBOARD	
1-1 SPECIFICATION.....	1
1-2 LAYOUT DIAGRAM.....	2
CHAPTER 2 HARDWARE INSTALLATION	
2-1 JUMPER SETTINGS.....	6
2-2 CONNECTORS , HEADERS & WAFERS.....	9
2-2-1 REAR I/O BACK PANEL CONNECTORS.....	9
2-2-2 MOTHERBOARD INTERNAL CONNECTORS.....	11
2-2-3 PIN DEFINITION FOR HEADERS & WAFERS.....	14
2-2-4 MAXIMUM VOLTAGE & CURRENT LIMIT.....	17
CHAPTER 3 INTRODUCING BIOS	
3-1 ENTERNING SETUP.....	18
3-2 BIOS MENU SCREEN.....	19
3-3 FUNCTION KEYS.....	19
3-4 GETTING HELP.....	19
3-5 MENU BARS.....	20
3-6 MAIN MENU.....	20
3-7 ADVANCED MENU.....	21
3-8 CHIPSET MENU.....	30
3-9 BOOT MENU.....	32
3-10 SECURITY MENU.....	34
3-11 SAVE & EXIT MENU.....	35



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 figure comes from the request of the main chipset)
- 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.

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.



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 THE OWNER'S BENEFIT, WITHOUT INTENT TO INFRINGE.

Manual Revision Information

Reversion	Revision History	Date
2.0	Second Edition	December 14, 2022

Item Checklist

- Motherboard
- Cable(s)
- I/O Back panel shield

Chapter 1

Introduction of the Motherboard

1-1 Specification

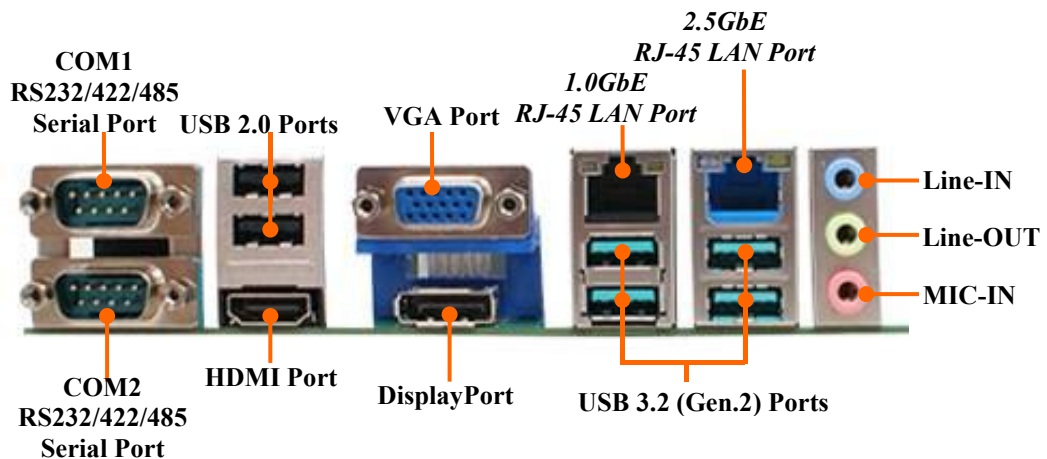
Spec	Description
Design	<ul style="list-style-type: none"> ● ATX form factor; PCB size: 30.5 x 24.4 cm
Chipset	<ul style="list-style-type: none"> ● Intel Q470E Chipset
CPU Socket	<ul style="list-style-type: none"> ● Intel LGA 1200 Socket supports 11th/10th Core processors (Max. 125W TDP) <p><i>*Note: for detailed CPU support information please visit our website</i></p>
Memory Slots	<ul style="list-style-type: none"> ● 4*DDR4 long DIMM DRAM module slot ● Supporting 4* 3200/2933 MHz DDR4 DRAM Modules, expandable to 128 GB (Maximum) <p><i>*Note:Memory frequency range also depends on CPU support</i></p> <ul style="list-style-type: none"> ● Support dual-channel function
Expansion Slots	<ul style="list-style-type: none"> ● 2 * PCI-Express x16 slot (PCIE1/PCIE3; by CPU) ● 5* PCIe x4 slots (PCIE2/4/5/6/7; PCIE2 by CPU; PCIE4/5/6/7 by PCH; *PCIE4 functions as PCIe x1 interface) ● 1* M.2 E-key (2230, CNVi+USB2.0 interface) slot, support WIFI/BT Module(M2E; by PCH) ● 1* M.2 B-key (3042/3052, USB3.2+PCI-Ex1 interface) slot, Support 4G/5G Module (M2B; by PCH) ● 1* SIM card slot co-function with M2B1slot (SIMCARD)
Storage	<ul style="list-style-type: none"> ● 4 * SATAIII 6Gb/s port (SATA_RA1/2;Support Raid 0/1/5/10) ● 2* M.2 M-key (2242/2280) slot, support NVMe (M2M/M2M1; M2M by PCH; M2M1 only by 11th CPU)
LAN Chip	<p><i>Integrated with:</i></p> <ul style="list-style-type: none"> ● 1* Intel i225V 2.5GbE PCI-E LAN chip of providing 10/100/1000/2500Mbps Ethernet data transfer rate <p><i>* Note: 2500Mbps high-speed transmission rate is only supported over CAT 5e UTP cable.</i></p> <ul style="list-style-type: none"> ● 1* Intel i219-LM Gigabit PHY LAN chip of providing 10/100/1000Mbps Ethernet data transfer rate ● Support Fast Ethernet LAN function
Audio Chip	<ul style="list-style-type: none"> ● Realtek HD Audio Codec integrated ● Audio driver and utility included
BIOS	<ul style="list-style-type: none"> ● 256Mb AMI Flash ROM
Multi I/O	<p><i>Rear Panel I/O:</i></p> <ul style="list-style-type: none"> ● 2*Serial port (COM1/COM2, support RS232/422/485 function) ● 2* USB 2.0 port ● 1* HDMI port

	<ul style="list-style-type: none"> ● 1* Display port ● 1* VGA port ● 4* USB 3.2 (Gen.2) 10Gbps port ● 1* 1.0GbE RJ-45 LAN port & 2.5GbE RJ-45 LAN port ● 1* 3-jack audio connector (Line-in, Line-out, MIC) <p>Internal I/O Connectors, Wafer & Headers:</p> <ul style="list-style-type: none"> ● 1*24-pin main power connector ● 1*8-pin 12V power connector ● 2*CPU FAN connector & 2* System FAN connector ● 1*Internal USB 3.2 (Gen.1) type-A port ● 1* Front panel header ● 1* Front panel audio header ● 1* HDMI_SPDIF header ● 1* 9-Pin USB 2.0 header for 2* expansion USB 2.0 ports ● 4* RS232 Serial port header (COM3/4/5/6) ● 1* 16-bit GPIO header ● 1* PS2 Keyboard & Mouse header ● 1* SMBUS header
TPM 2.0 Function	Optional for LA20-12(S) Series

***Note:** LA20-10(S) and LA20-12(S) series are basically the same in specifications & layout, except that LA20-12(S) supports TPM 2.0 function.

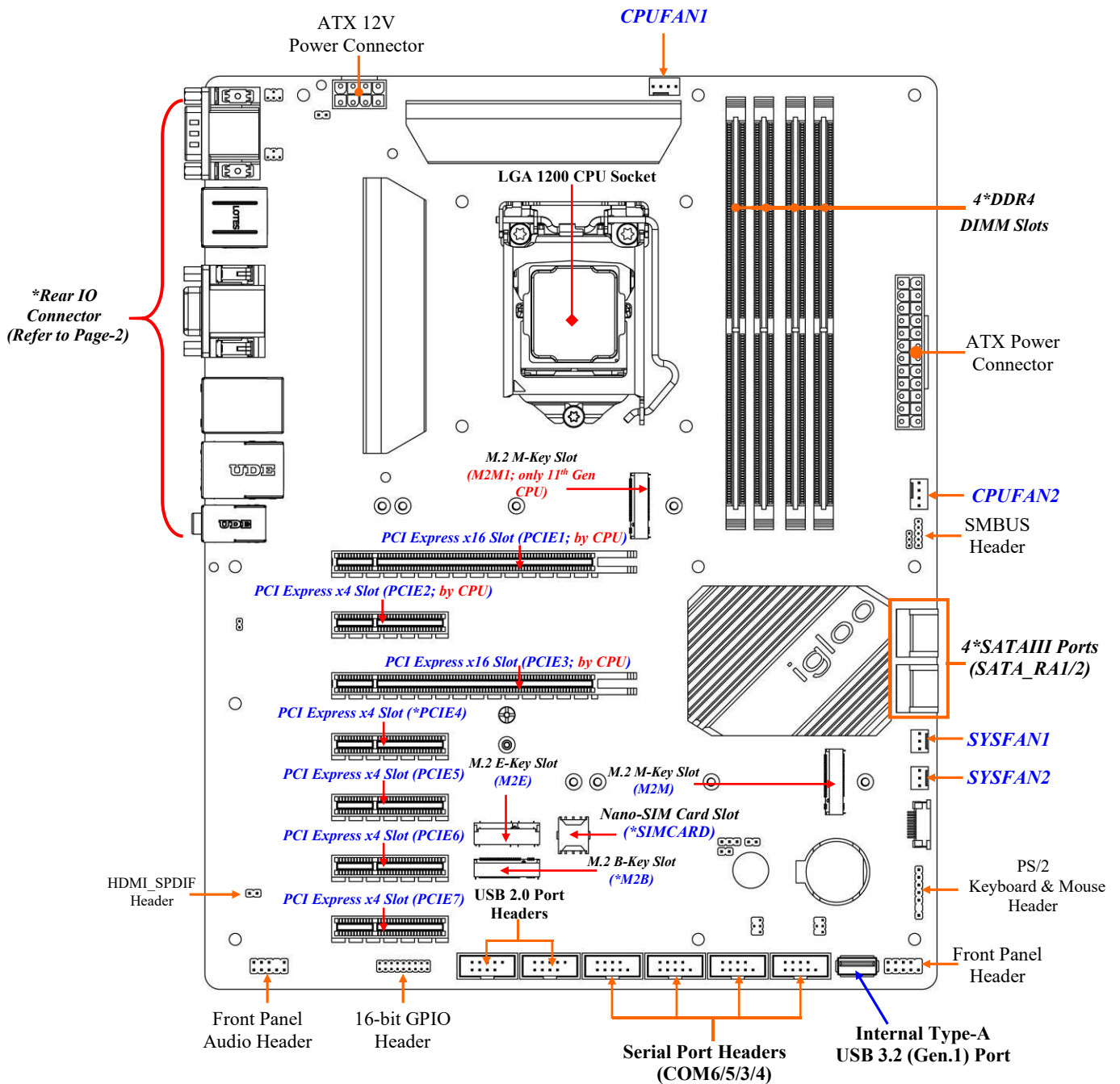
1-2 Layout Diagram

Rear IO Diagram



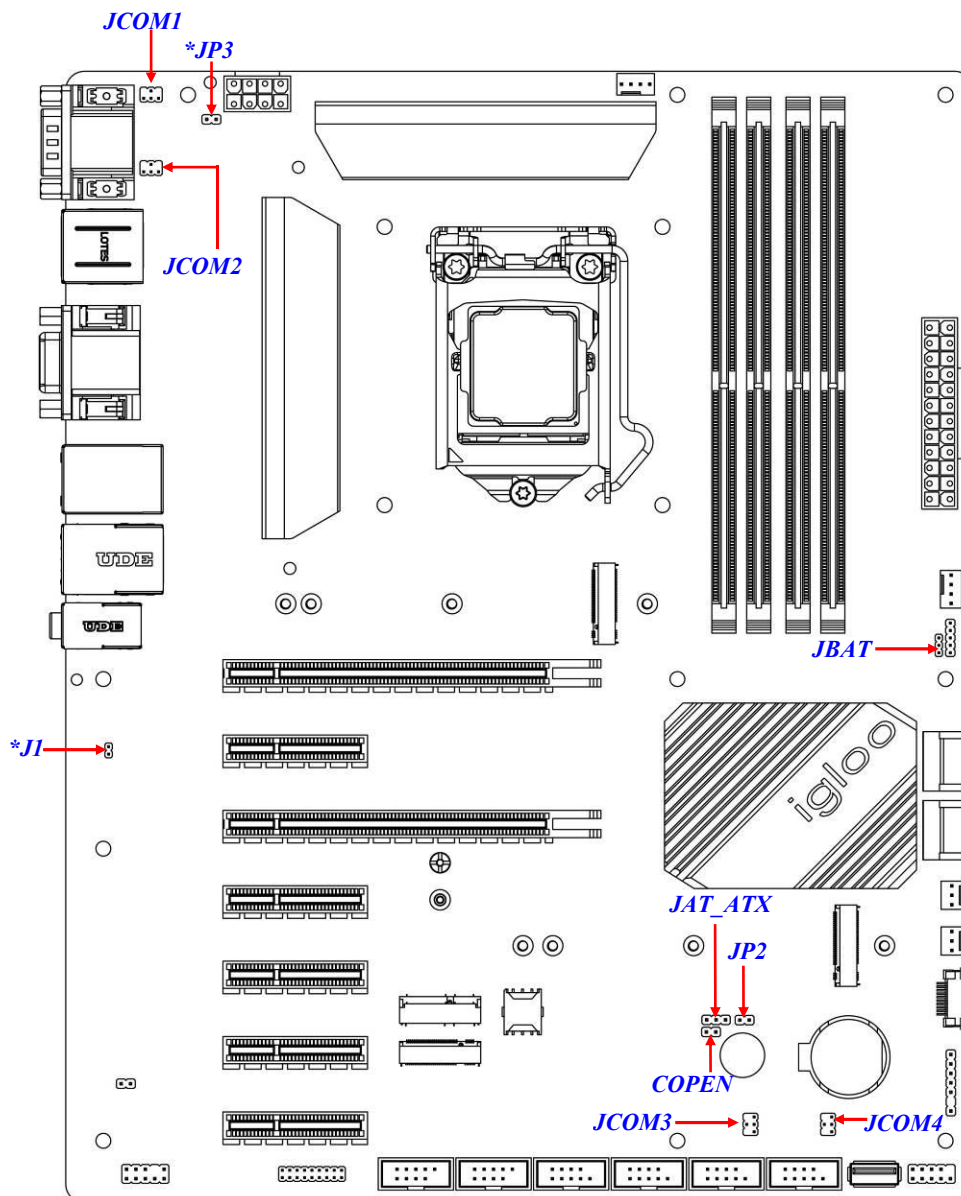
*** Note:** Many PCs now include XHCI USB controllers which allow for the support of USB 3.0(or higher version) and higher USB speeds. This inclusion of XHCI controllers has lessened the need for EHCI USB controllers within platforms. However, legacy operating systems (OS) may not natively recognize XHCI controllers. You might need to pre-install XHCI driver while desiring to install a non-XHCI OS (ex.Windows* 7) on Intel platforms which do not include EHCI controllers. Please contact your representative for more details.

Motherboard Internal Diagram



***Note:** 1.SIMCARD slot only work when compatible Nano-SIM card installed & 4G/5G LAN card installed in M2B slot; 2.PCIE4 slot functions as PCIe x1 interface due to specification restriction.

Motherboard Jumper Positions



Jumpers

Jumper	Name	Description	Pitch
JCOM1	COM1 Port Pin9 Function Select	4-pin Block	2.0mm
JCOM2	COM2 Port Pin9 Function Select	4-pin Block	2.0mm
JCOM3	COM3 Header Pin9 Function Select	4-pin Block	2.0mm
JCOM4	COM4 Header Pin9 Function Select	4-pin Block	2.0mm
JBAT	CMOS RAM Clear Function Setting	3-pin Block	2.0mm
JAT_ATX	ATX/AT Mode Select	3-pin Block	2.54mm
COPEN	Case Open Message Display Detect	2-pin Block	2.54mm
JP2	ME Features Select	2-pin Block	2.0mm
*JP3	Debug Jumper (Lab only)	2-pin Block	2.54mm
*J1	Debug Jumper (Lab only)	2-pin Block	2.0mm

***Note:** JP3 & J1 is designed for laboratory debug only, not for user general purpose.

Connectors

P/N	Name
COM1/COM2	RS232/422/485 Serial Port Connector
HDMI	High-Definition Multimedia Interface Connector
USB1	USB 2.0 Connector X2
DP	DisplayPort Connector
VGA	VGA Port Connector
UL1	Top: 1.0GbE RJ-45 LAN Connector Middle & Bottom: USB 3.2 Gen.2 Port Connector X2
RJ45_USB2	Top: 2.5GbE RJ-45 LAN Connector Middle & Bottom: USB 3.2 Gen.2 Port Connector X2
AUDIO	Top: Line-in Connector Middle: Line-out Connector Bottom: MIC Connector
ATXPWR	ATX Main Power Connector
ATX12V	ATX 12V Power Connector
CPUFAN1/CPUFAN2	CPU FAN Connector X2
SYSFAN1/SYSFAN2	System FAN Connector X2
SATA_RA1/2	SATAIII Connector X4
USB30	USB 3.2 (Gen.1) type-A Port Connector

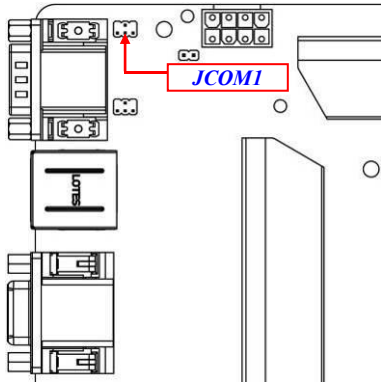
Headers & Wafers

P/N	Name	Description	Pitch
FP (Front Panel Header)	PWR LED/ HD LED/ Power Button /Reset	9-pin Block	2.54mm
FP_AUDIO	Front Panel Audio Header	9-pin Block	2.54mm
HDMI_SPDIF	HDMI_SPDIF Header	2-pin Block	2.54mm
FP_USB1/2	USB 2.0 Wafer	9-pin Block	2.54mm
COM3/4/5/6	RS232 Serial Port Wafer	9-pin Block	2.54mm
GPIO	<i>GPIO Header</i>	<i>18-pin Block</i>	2.0mm
PS2KBMS	PS/2 Keyboard & Mouse Header	6-pin Block	2.54mm
SMBUS	SMBUS Header	5-pin Block	2.0mm

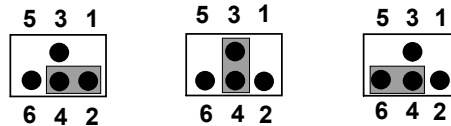
Chapter 2 Hardware Installation

2-1 Jumper Settings

JCOM1 (4-pin): COM1 Port Pin9 Function Select



JCOM1 → COM1 Port Pin-9

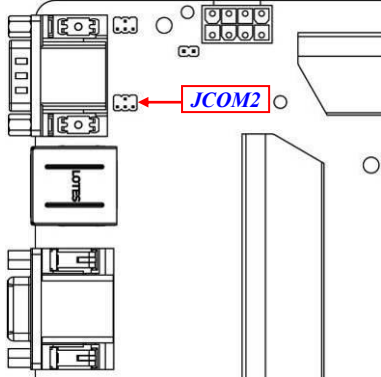


2-4 Closed:
RI=RS232;

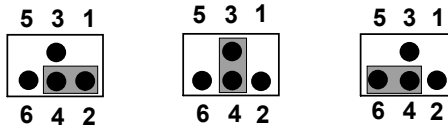
3-4 Closed:
RI= 5V;

4-6 Closed:
RI= 12V.

JCOM2 (4-pin): COM2 Port Pin9 Function Select



JCOM2 → COM2 Port Pin-9

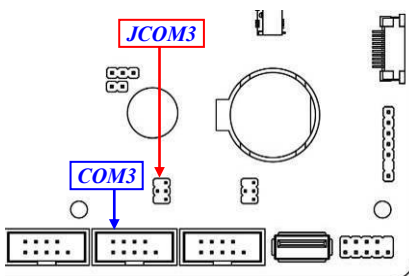


2-4 Closed:
RI=RS232;

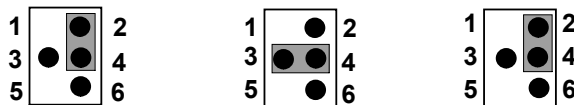
3-4 Closed:
RI= 5V;

4-6 Closed:
RI= 12V.

JCOM3 (4-pin): COM3 Header Pin9 Function Select



JCOM3 → COM3 Header Pin-9

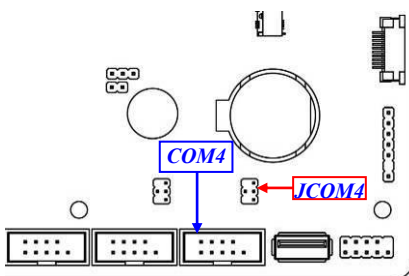


2-4 Closed:
RI=RS232;

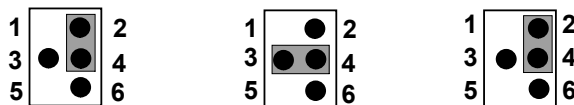
3-4 Closed:
RI= 5V;

4-6 Closed:
RI= 12V;

JCOM4 (4-pin): COM4 Header Pin9 Function Select



JCOM4 → COM4 Header Pin-9

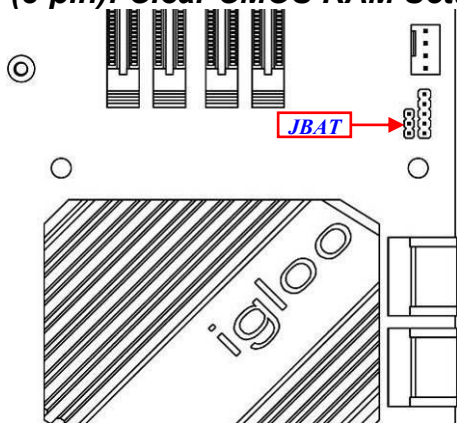


2-4 Closed:
RI=RS232;

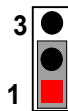
3-4 Closed:
RI= 5V;

4-6 Closed:
RI= 12V;

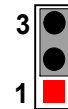
JBAT (3-pin): Clear CMOS RAM Settings



JBAT → Clear CMOS Settings

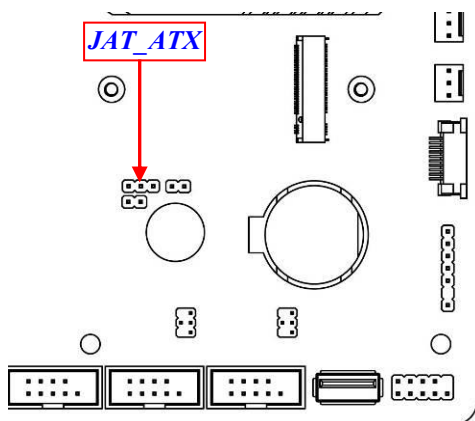


1-2 Closed: Normal;

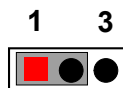


2-3 Closed: Clear CMOS.

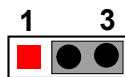
JAT_ATX (3-pin): ATX Mode/AT Mode Select



JAT_ATX → ATX/AT Mode Select



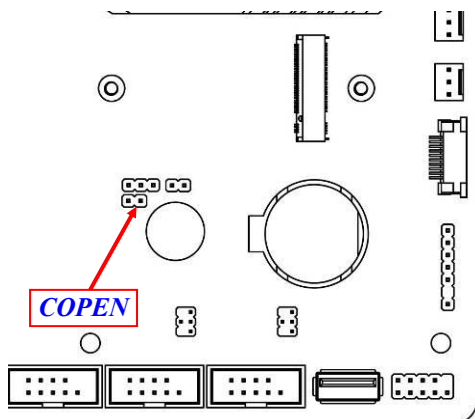
1-2 Closed: ATX Mode Selected;



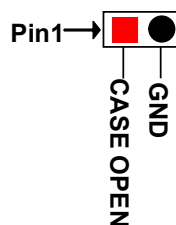
2-3 Closed: AT Mode Selected.

***ATX Mode Selected:** Press power button to power on after power input ready;
AT Mode Selected: Directly power on as power input ready.

COPEN (2-pin): Case Open Message Display Function Select

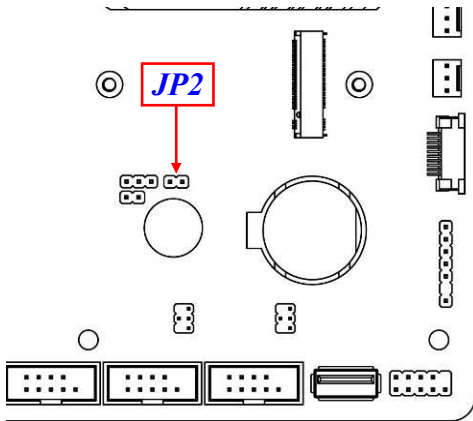


COPEN → Case Open Detection

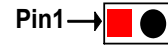


Pin 1-2 Short: When Case open function pin short to GND, the Case open function was detected. When Used, needs to enter BIOS and enable 'Case Open Detect' function. In this case if your case is removed, next time when you restart your computer, a message will be displayed on screen to inform you of this.

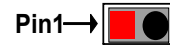
JP2(2-pin): ME Features Select



JP2 → ME Features Select



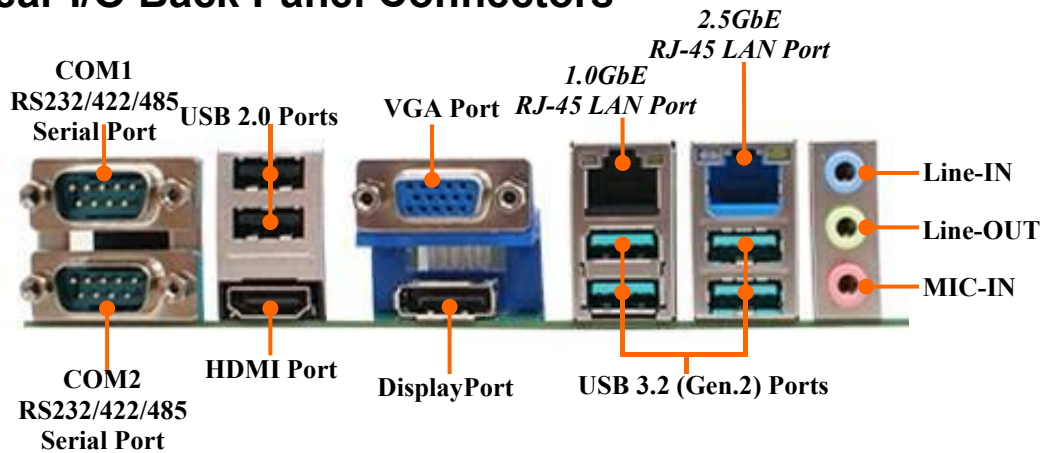
1-2 Open: Enable ME Features;












1-2 Closed: Disable ME Features.

2-2 Connectors, Headers & Wafers

2-2-1 Rear I/O Back Panel Connectors

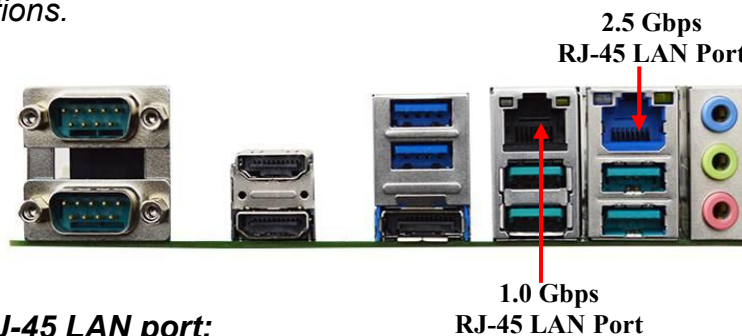


Icon	Name	Function
	RS232/422/485 Serial Port	Mainly for user to connect external MODEM or other devices that supports Serial Communications Interface.
	USB 2.0 Port	To connect USB keyboard, mouse or other devices compatible with USB specification.
	HDMI Port	To connect display device that support HDMI specification.
	Display Port	To the system to corresponding display device with compatible DP cable.
	VGA Port	To connect display device that support VGA specification.
	1.0Gbps RJ-45 LAN Port	This connector is standard RJ-45 LAN jack for Network connection which supports 10/100/1000Mbps Ethernet data transfer rate.
	2.5Gbps RJ-45 LAN Port	This connector is standard RJ-45 LAN jack for Network connection which supports 10/100/1000/2500 Mbps Ethernet data transfer rate (*Note: 2.5Gbps is only supported with CAT 5e UTP cable).

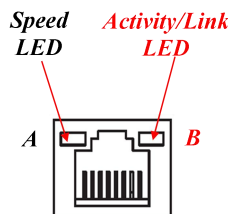
	USB 3.2 (Gen.2) Ports	To connect USB keyboard, mouse or other devices compatible with USB 3.2 (Gen.2) specification. Ports support up to 10Gbps data transfer rate.
	Audio Connectors	BLUE: Line-in Connector GREEN: Line-out Connector PINK: MIC Connector

(1) RJ-45 Ethernet Connector

** There are two LED next to the LAN port. Please refer to the table below for the LAN port LED indications.



For 1.0Gbps RJ-45 LAN port:



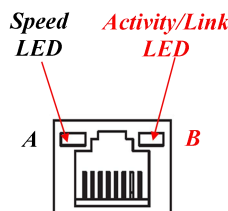
A: Speed LED

Status	Description
Off	10Mbps connection
Green	100Mbps connection
Orange	1Gbps connection

B: Activity/Link LED

Status	Description
Off	No Link
Blinking	Data Activity
On	Link

For 2.5Gbps RJ-45 LAN port:



A: Speed LED

Status	Description
Off	10/100Mbps connection
Red	1Gbps connection
Green	2.5Gbps connection

B: Activity/Link LED

Status	Description
Off	No Link
Blinking	Data Activity
On	Link

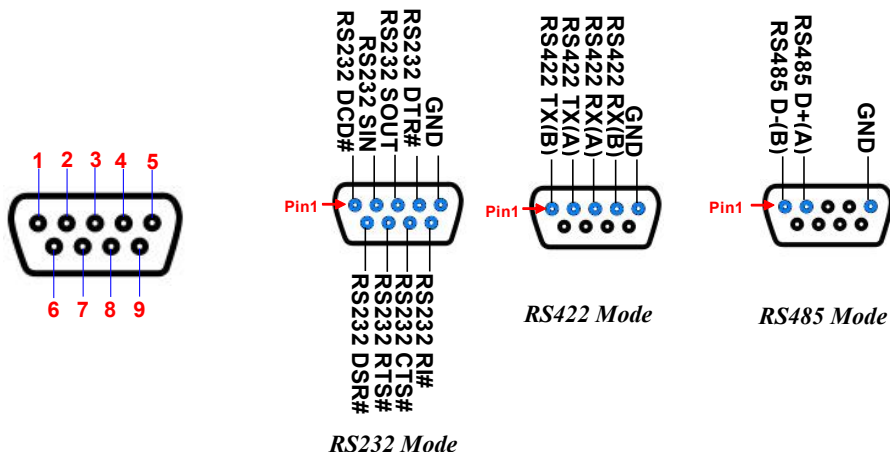
* **Note:** 2.5Gbps high-speed transmission rate is **only** supported over **CAT 5e UTP cable**.

COM1/COM2: COM1 & COM2 RS232/422/485 Port

COM1 & COM2 ports can function as RS232/422/485 port. In normal settings COM1/COM2 functions as RS232 port. With compatible COM cable they can function as RS422 or RS 485 port.

User also needs to go to BIOS to set '**Transmission Mode Select**' for COM1/COM2 (refer to Page-24) at first, before using specialized cable to connect different pins of this port.

The pin assignment for RS-232/ 422/ 485 is listed as follows:

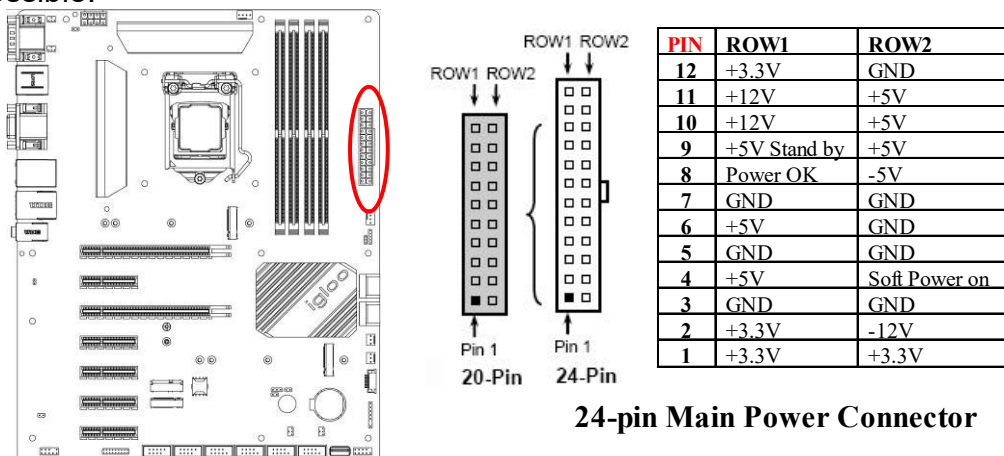


2-2-2 Motherboard Internal Connectors

(1) ATXPWR (24-pin block): Main Power Connector

ATX Power Supply connector: This is a new defined 24-pins connector that usually comes with ATX case. The ATX Power Supply allows using soft power on momentary switch that connect from the front panel switch to 2-pins Power On jumper pole on the motherboard. When the power switch on the back of the ATX power supply turned on, the full power will not come into the system board until the front panel switch is momentarily pressed. Press this switch again will turn off the power to the system board.

- ** We recommend that you use an ATX 12V Specification 2.0-compliant power supply unit (PSU) with a minimum of 350W power rating. This type has 24-pin and 4-pin power plugs.
- ** If you intend to use a PSU with 20-pin and 4-pin power plugs, make sure that the 20-pin power plug can provide at least 15A on +12V and the power supply unit has a minimum power rating of 350W. The system may become unstable or may not boot up if the power is inadequate.
- ** If you are using a 20-pin power plug, please refer to Figure1 for power supply connection. Power plug form power supply and power connectors from motherboard both adopt key design to avoid mistake installation. You can insert the power plug into the connector with ease only in the right direction. If the direction is wrong it is hard to fit in and if you make the connection by force it is possible.



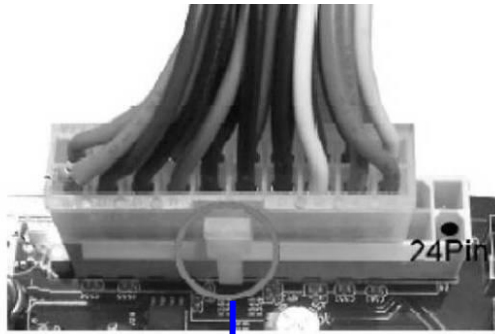


Figure 1: 20-pin power plug

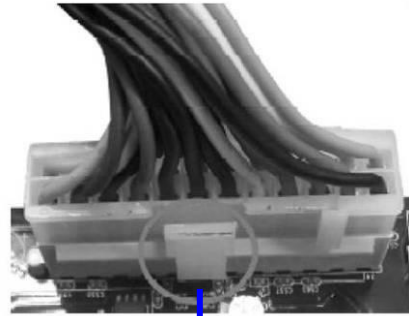
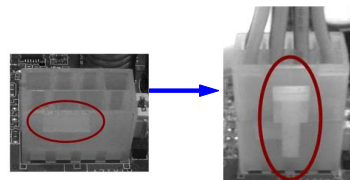
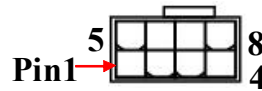
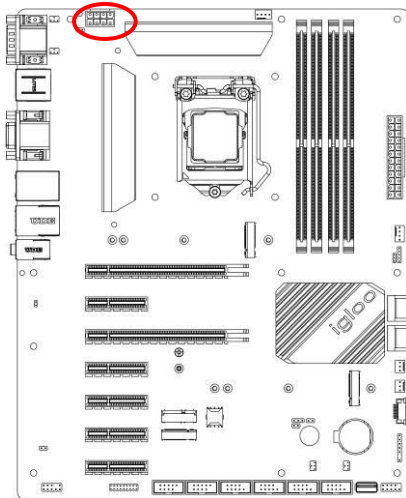


Figure 2: 24-pin power plug

(2) ATX12V (8-pin block): ATX12V Type Power Connector

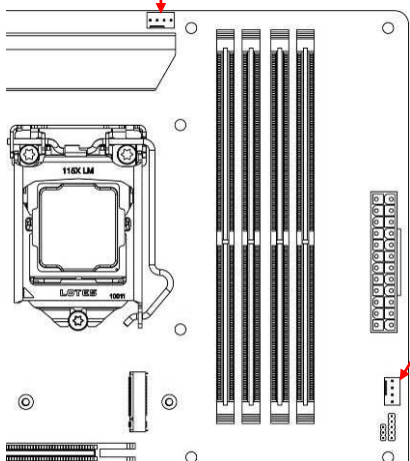
This is a new defined 8-pin connector that usually comes with ATX Power Supply that supports extra 12V voltage to maintain system power consumption. Without this connector might cause system unstable because the power supply can not provide sufficient current for system.



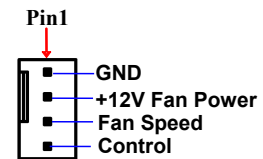
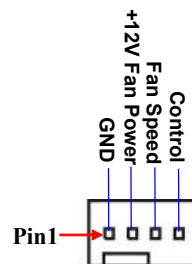
Pin No.	1	2	3	4
Definition	GND	GND	GND	GND
Pin No.	5	6	7	8
Definition	+12V	+12V	+12V	+12V

(3) CPUFAN1/ CPUFAN2 (4-pin): CPUFAN Connectors

CPUFAN1

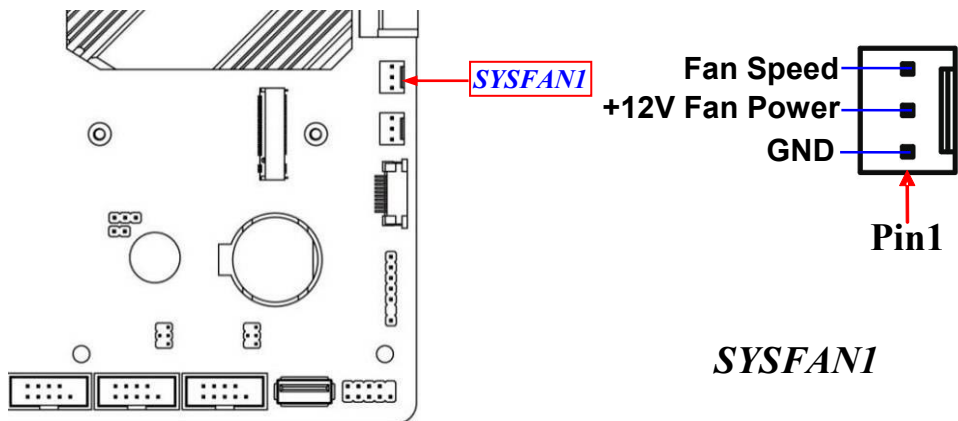


CPUFAN1

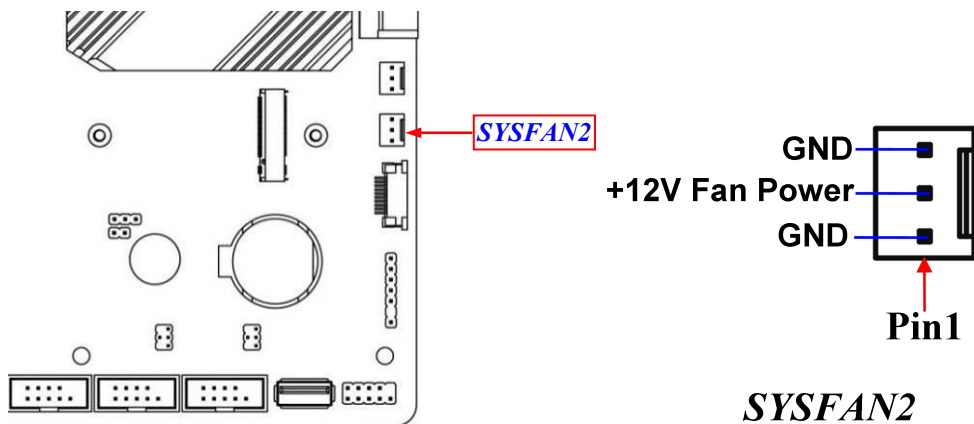


CPUFAN2

(4) SYSFAN1 (3-pin): System Fan Connector

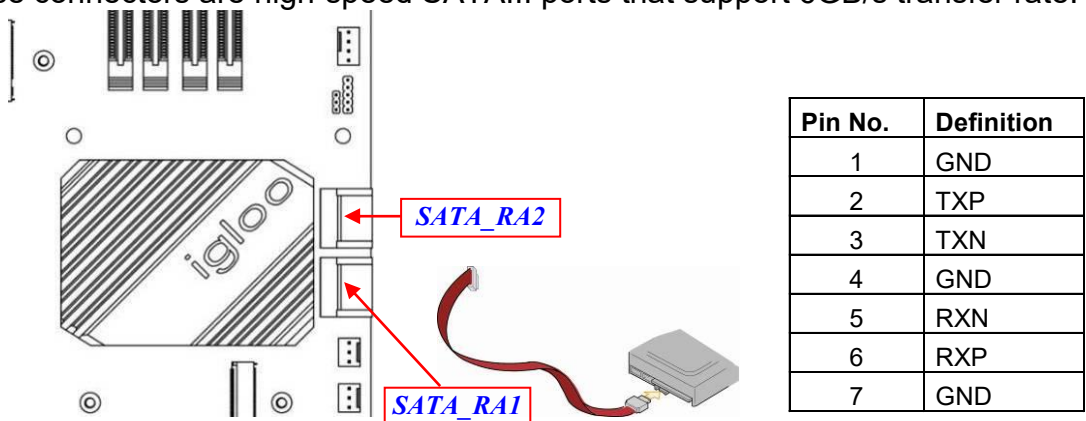


(5) SYSFAN2(3-pin): System Fan Connector



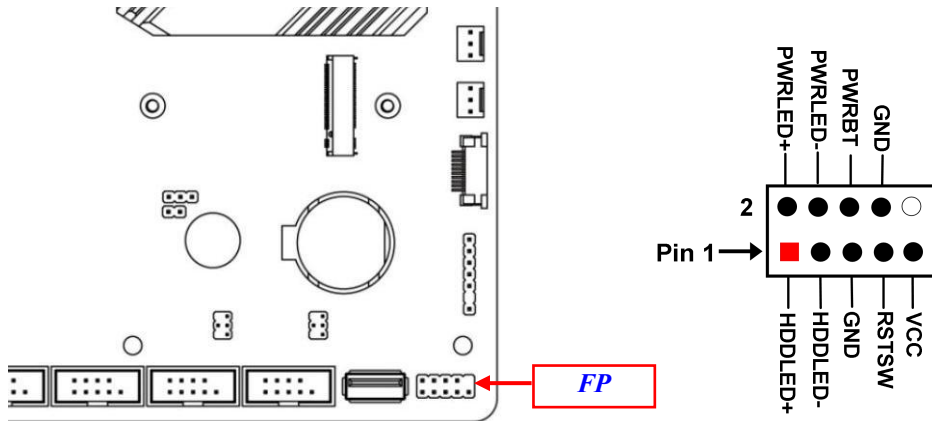
(6) SATA_RA1/2: SATAIII Port Connector

These connectors are high-speed SATAIII ports that support 6GB/s transfer rate.



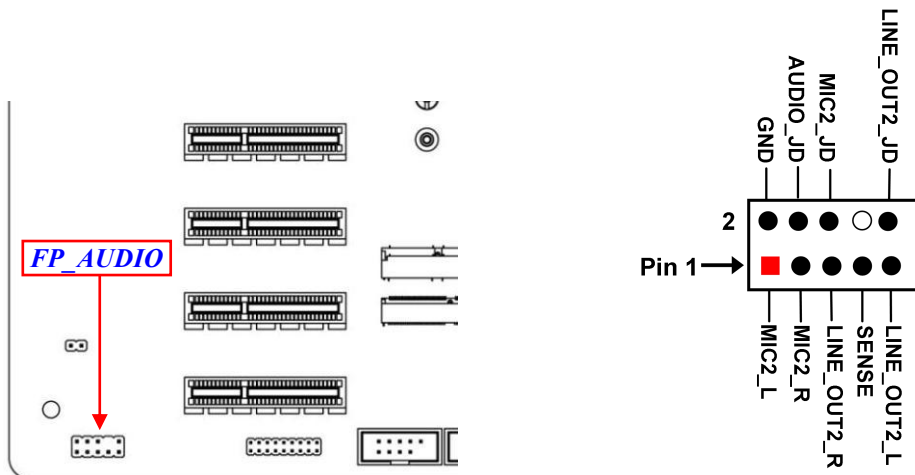
2-2-3 Pin Definition for Headers & Wafers

(1) FP (9-pin): Front Panel Header

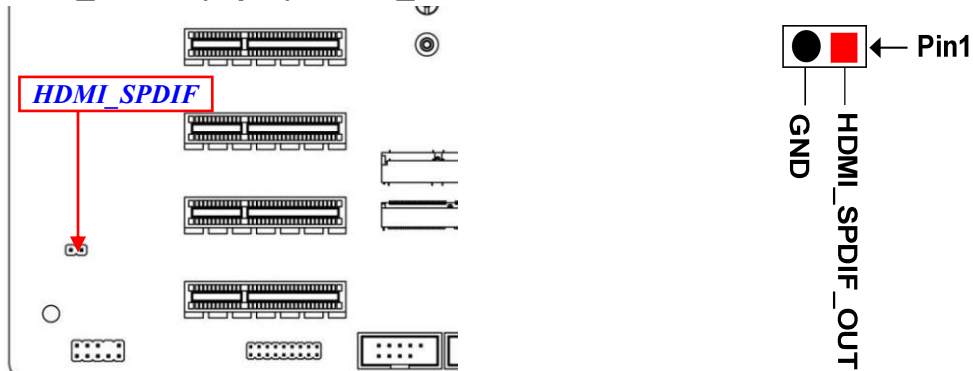


(2) FP_AUDIO (9-pin): Line-Out, MIC-In Header

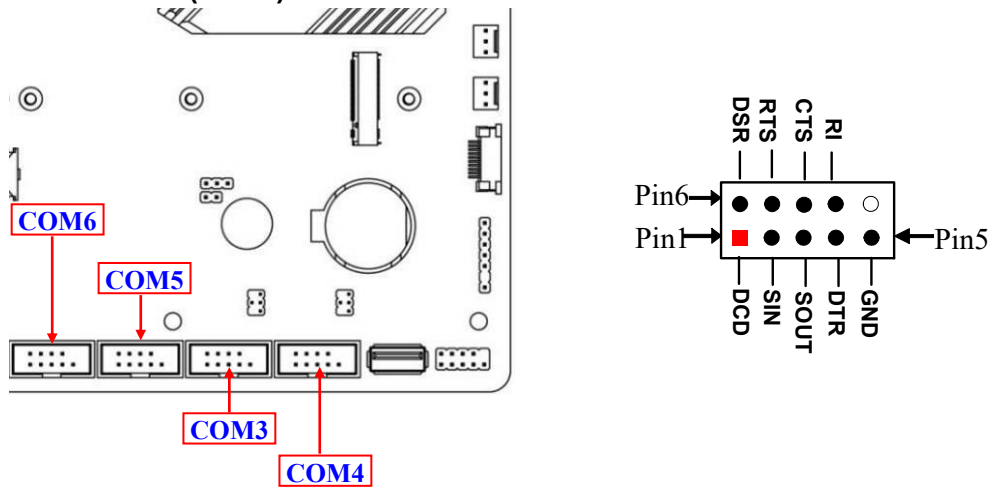
This header is connected to Front Panel Line-out, MIC connector with cable.



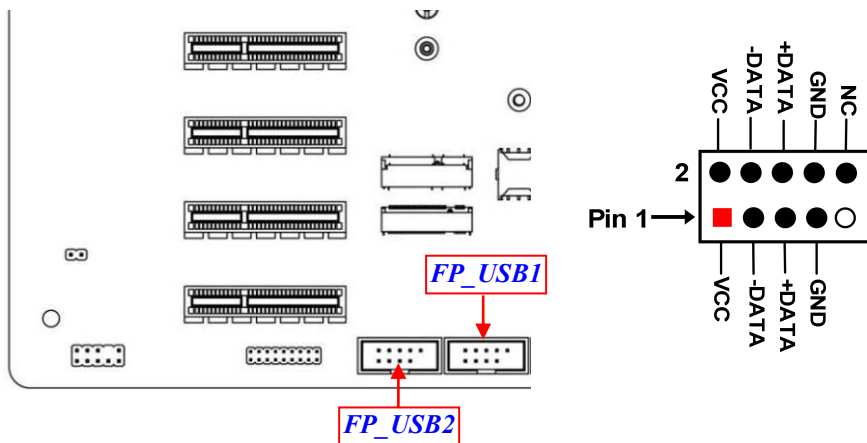
(3) HDMI_SPDIF (2-pin): HDMI_SPDIF Out Header



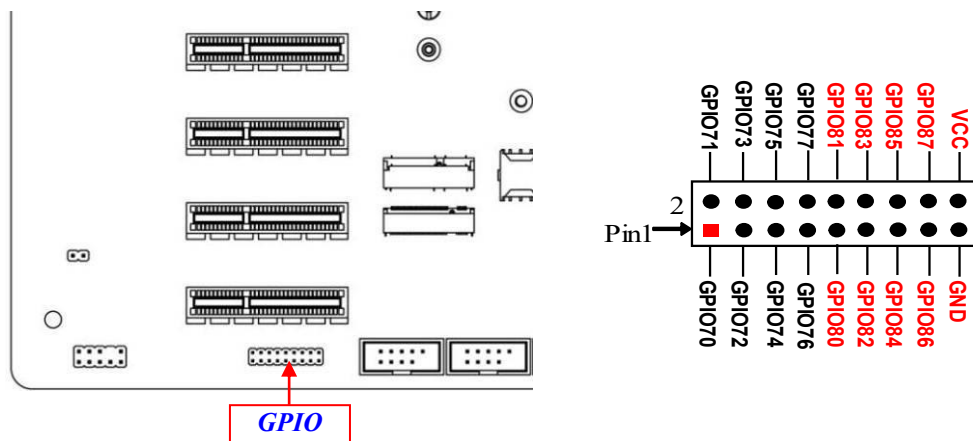
(4) COM3/4/5/6 (9-Pin): RS232 Serial Port Header



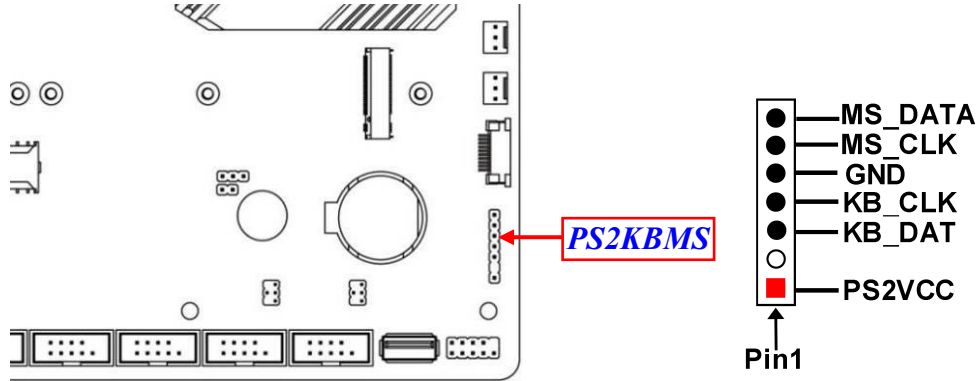
(5) FP_USB2/FP_USB1(9-pin): USB 2.0 Port Header



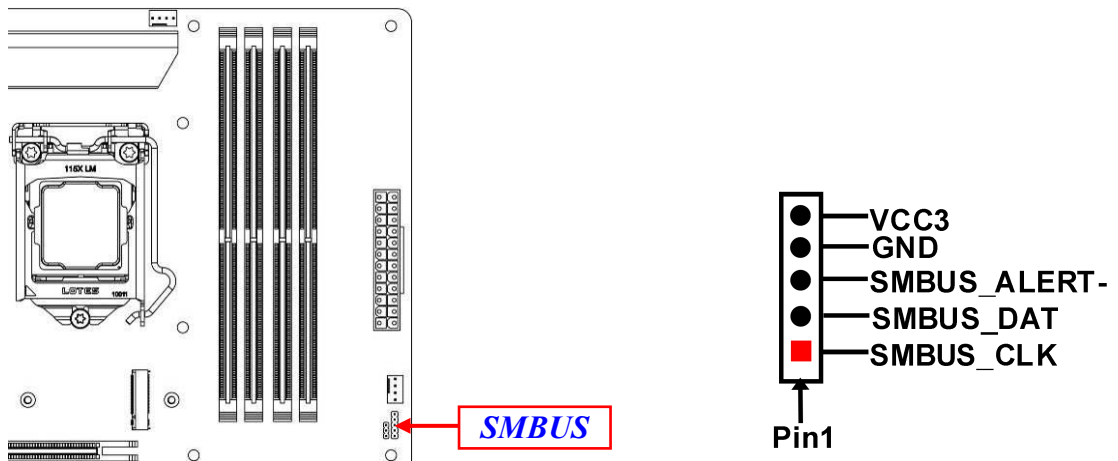
(6) GPIO (18-pin): 16-Bit GPIO Header



(7) PS2KBMS (6-pin): PS/2 Keyboard & Mouse Header



(8) SMBUS (5-pin): SM BUS Header



2-2-4 Maximum Voltage & Current Limit

Below is a list of maximum voltage & Current Limit specification for motherboard interface (including but not limited to slots, connectors and headers) for setup reference:

Parts		Working Voltage	Current Support
USB Ports from	USB1	5V	1.5A
	UL1	5V	1.5A
	RJ45-USB2	5V	1.5A
	USB30	5V	1.5A
	FP_USB1	5V	1.5A
	FP_USB2	5V	1.5A
COM1(JCOM1)		5V/12V	0.5A
COM2(JCOM2)		5V/12V	0.5A
COM3(JCOM3)		5V/12V	0.5A
COM4(JCOM4)		5V/12V	0.5A
FP		5V	1A
GPIO		5V	1A
PS2KBMS		5V	0.5A
SMBUS		5V	0.5A
CPUFAN1/CPUFAN2		12V	1.5A
SYSFAN1/ SYSFAN2		12V	1.5A
M2M/M2M1		3.3V	2A
M2E		3.3V	2A
M2B		3.3V	2A

Chapter 3

Introducing BIOS

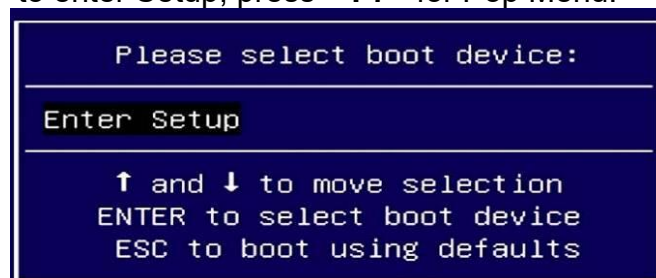
Notice! The BIOS options in this manual are for reference only. Different configurations may lead to difference in BIOS screen and BIOS screens in manuals are usually the first BIOS version when the board is released and may be different from your purchased motherboard. Users are welcome to download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

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

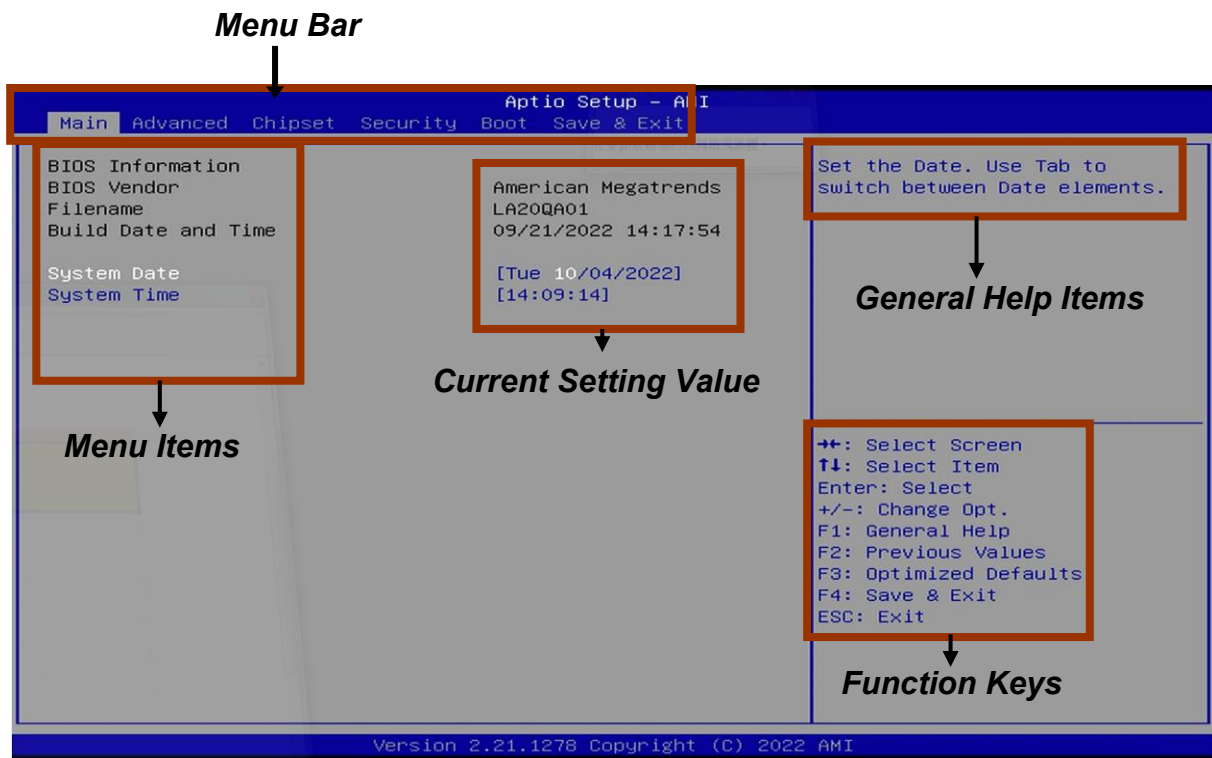
Power on the computer and by pressing immediately allows you to enter Setup. If the message disappears before your respond and you still wish to enter Setup, restart the system to try again by turning it OFF then ON or pressing the “RESET” button on the system case. You may also restart by simultaneously 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

Press **** to enter Setup; press **< F7>** for Pop Menu.



3-2 BIOS Menu Screen

The following diagram show a general BIOS menu screen:



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 value.
- [F3]: Optimized defaults.
- [F4]: Save & Exit.
- Press <Esc> to quit the 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

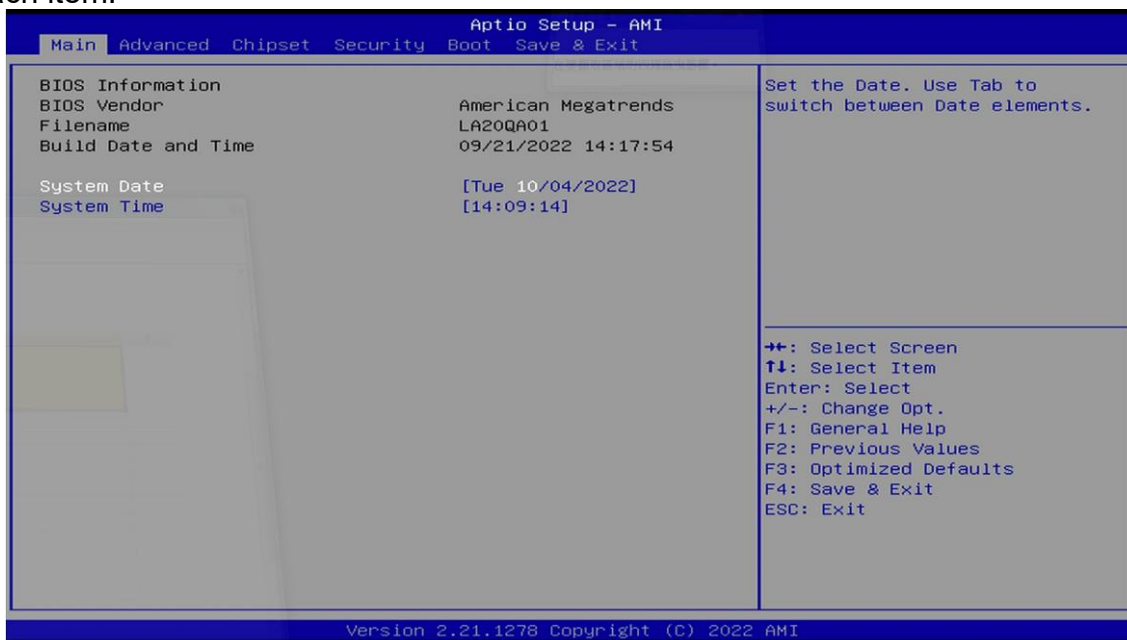
There are seven menu bars on top of BIOS screen:

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.



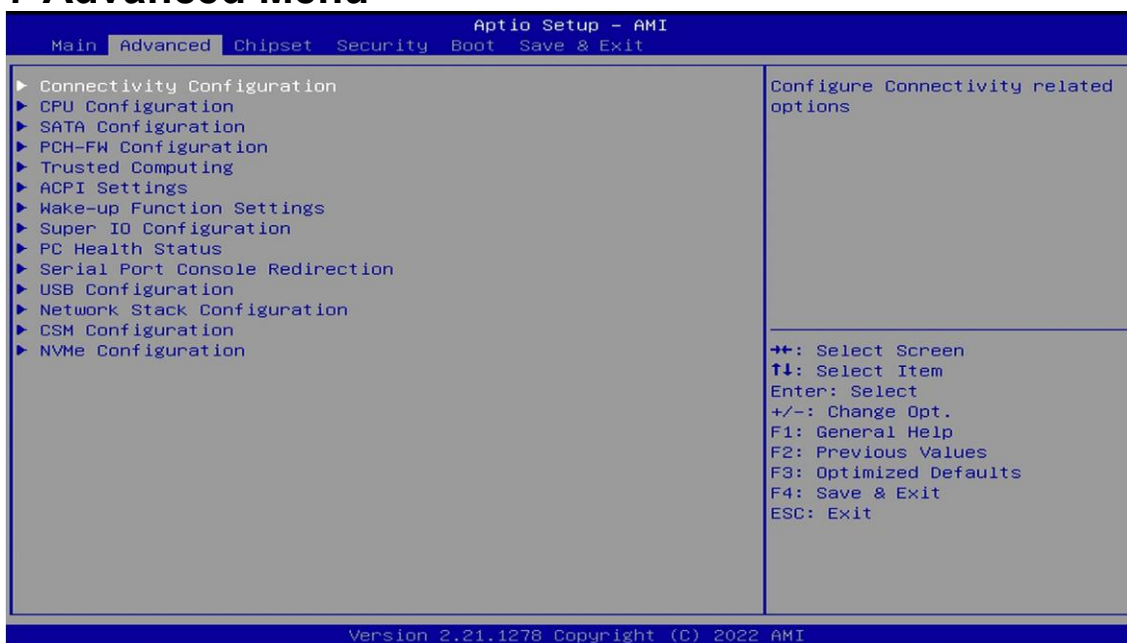
System Date

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



▶ **Connectivity Configuration**

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

CNVi present

CNVi Configurayion

CNVi Mode

Use this item to option configures connectivity.

[Auto Detection]: means that if discrete solution is discovered it will be enabled by default. Otherwise integrated solution (CNVi) will be enabled ;

[Disable Integrated]: Disables integrated solution.

***NOTE:** When CNVi is present, the GPIO pins that are used for radio interface cannot be assigned to the other native function.

The optional settings: [Disable Integrated]; [Auto Detection]

▶ **CPU Configuration**

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

Hyper-Threading

Use this item to enable or disable Hyper-Threading Technology.

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

Intel (VMX) Virtualization Technology

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

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

Intel® 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. This item allows CPU to go to C states when it's not 100% utilized.

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

Turbo Mode

Use this item to enable or disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).

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

▶ **SATA Configuration**

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

SATA Controller(s)

Use this item to enable or disable SATA device.

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

When set as [Enabled], user can make more settings for the following sub-items:

SATA Mode Selection

Use this item to determine how SATA controller(s) operate.

The optional settings: [AHCI]; [RAID]

M.2

Port

Use this item to enable or disable SATA Port

The optional settings: [Disabled]; [Enabled]

SATA Port 1/ SATA Port 2/ SATA 3/ SATA 4

Port

Use this item to enable or disable each SATA port.

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

Hot Plug

Use this item to designate this port as Hot Pluggable.

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

▶ **PCH-FW Configuration**

Press [Enter] to view current Management Engine Technology Parameters and make more settings for the following sub-item:

TPM Device Selection

Use this item to select TPM device: PTT or dTPM. When set as PTT, user can enable PTT in SkuMgr. When set as dTPM 1.2, user can disable 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**

Press [Enter] to go to 'ME FW Image Re-Flash' to enable or disable ME FW Image Re-Flash function.

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:

TPM 2.0 Device Found

Security Device Support

Use this item to Enables or Disables BIOS support for security device.

***Note:** O.S. will not show security Device. TCG EFI protocol and INTIA interface will not be available.

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

When set as [Enabled], user can make more settings for the following sub-items:

Pending operation

Use this item to schedule an operation for the security device.

***Note:** your computer will reboot during restart in order to change state of security device.

The optional settings: [None]; [TPM Clear].

▶ **ACPI Settings**

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

ACPI Settings

ACPI Sleep State

Use this item to select 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 System with Fixed Time

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

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

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

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.

When **Wake System with Fixed Time** set as [Disabled], the following items shall appear:

Wake-up system With Dynamic Time

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

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

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

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

Wake-up Minute Increase

Use this item to 1-60

PS2 KB/MS Wake-up

Use this item to enable or disable PS2 KB/MS wakeup from S3/S4/S5 state. This function is only supported when ERP function is disabled.

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

USB S3/S4 Wake-up

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

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

USB S5 Power

Use this item to enable or disable USB S5 state after System Shutdown. This function is only supported when ERP function is disabled.

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

▶ **Super I/O Configuration**

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

Super IO Configuration

ERP Support

Use this item to set Energy-Related Products function. When set as [Disabled], user can active all wake-up function.

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

▶ **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].

When set as [Enabled], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

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].

Transmission Mode Select

The optional settings are: [RS422]; [RS232]; [RS485].

Mode Speed Select

Use this item to select RS232/RS422/RS485 speed.

The optional settings: [RS232/RS422/RS485=250Kbps]; [RS232=1Mbps, RS422/RS485=10Mbps].

▶ **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].

When set as [Enabled], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

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].

Transmission Mode Select

The optional settings are: [RS422]; [RS232]; [RS485].

Mode Speed Select

Use this item to select RS232/RS422/RS485 speed.

The optional settings: [RS232/RS422/RS485=250Kbps]; [RS232=1Mbps, RS422/RS485=10Mbps].

▶ **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].

When set as [Enable], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

The optional settings: [IO=3E8h; 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].

▶ **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].

When set as [Enabled], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

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].

▶ **Serial Port 5 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].

When set as [Enabled], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

The optional settings: [IO=3E0h; 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 6 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].

When set as [Enabled], user can make more settings for the following sub-items:

Device Settings

Change Settings

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

The optional settings: [IO=2E0h; 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].

WatchDog Reset Timer

Use this item to support WDT reset function

The optional settings: [Disabled]; [Enabled]

When set as [Enabled], user can make more settings for the following sub-items:

WatchDog Reset Timer Value

Use this item to range 4~255.

WatchDog Reset Timer Unit

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

ATX Power Emulate AT Power

This item support Emulate AT power function, MB power On/Off control by power supply. Use needs to select 'AT or ATX Mode' on MB jumper at first (refer to JAT_ATX jumper setting for Pin1&2 of ATX Mode & Pin2&3 of AT Mode Select)

Case Open Detect

Use this item to detect Case has already open or not. Show message in POST.

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

When set as **[Enabled]**, system will detect if COPEN has been short or not (refer to COPEN jumper setting for Case Open Detection); if Pin 1&2 of COPEN are short, system will show Case Open Message during POST.

▶ **PC Health Status**

Press [Enter] to view current hardware health status, and make settings for the following sub-items:

▶ **SmartFan Configuration**

Press [Enter] to make settings for SmartFan Configuration:

CPUFAN1/ CPUFAN2 Smart Mode

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

CPUFAN1/ CPUFAN2 Full-Speed Temperature

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

CPUFAN1/ CPUFAN2 Full-Speed Duty

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

CPUFAN1/ CPUFAN2 Idle-Speed Temperature

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

CPUFAN1/ CPUFAN2 Idle-Speed Duty

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

▶ **Serial Port Console Redirection**

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

COM1

Console Redirection

Use this item to enable or disable Console Redirection.

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

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

▶ **Console Redirection Settings**

Use this item to 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 sub-items:

Terminal Type

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

Data Bits

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

Parity

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

The optional settings are: [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. They can be used as an additional data bit.

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 are: [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 are: [None]; [Hardware RTS/CTS].

VT-UT F8 Combo Key Support

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

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

Recorder Mode

With this mode enable only text will be sent. This is to capture Terminal data. The optional settings are: [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 are: [VT100]; [LINUX]; [XTERMR6]; [SCO]; [ESCN]; [VT400].

Serial Port for Out-of-Band Management / Windows Emergency

Management Services (EMS)

Console Redirection EMS

Use this item to enable or disable Console Redirection.

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

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

▶ **Console Redirection Settings**

Use this item to the settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both compatible settings.

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

Terminal Type EMS

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

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

Bits per second EMS

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 are: [9600]; [19200]; [57600]; [115200].

Flow Control EMS

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].

▶ **USB Configuration**

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

USB Configuration

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 or Disable USB Mass Storage Driver Support.

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

USB hardware delays and time-outs

USB Transfer Timer-out

The time-out value for Control, Bulk, and Interrupt transfers.
The optional settings: [1 sec]; [5 sec]; [10sec]; [20 sec].

Device Reset Timer-out

USB mass storage device Start Unit command timer-out.
The optional settings: [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].

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 are: [Disabled]; [Enabled].

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

Ipv4 PXE Support

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

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

Ipv6 PXE Support

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

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

PXE boot wait time

Use this item to set wait time in second 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 the presence of media will be check.
Use either +/- or numeric keys to set the value.

▶ **CSM Configuration**

Use this item to Enable or Disable Option ROM execution settings, etc.

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

Compatibility Support Module Configuration

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

Use this item to control the execution of Network OpROM.

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

Storage

Use this item to control the execution of UEFI and Legacy Storage OpROM.

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

Video

Use this item to controls the execution of UEFI and Legacy Video OpROM.
The optional settings: [Do not launch]; [UEFI]; [Legacy].

Other PCI devices

This item determines OpROM execution policy for devices other than Network, Storage, or Video.

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

▶ **NVMe Configuration**

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

3-8 Chipset Menu



▶ **System Agent (SA) Configuration**

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

▶ **Memory Configuration**

Use this item to see Memory Configuration Parameters.

▶ **Graphics Configuration**

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

Primary Display

Use this item to select which IGFX/PEG Graphics device should be Primary Display.

The optional settings: [Auto]; [IGFX]; [PEG].

Internal Graphics

Use this item to keep IGFX enabled based on the setup options.

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

Aperture Size

Use this item to select the Aperture Size.

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

***Note:** Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. Please disable CSM Support to use this feature.

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 graphics memory size used by the internal graphics device.

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

▶ **PEG Slot Configuration**

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

PEG Port Configuration

PCIE1/ PCIE3/ PCIE2 Slot

Enable Root Port

Use this item to enable or disable the root port.

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

Max Link Speed

Use this item to configure PEG 0: 1: 0 Max Speed.

The optional settings: [Auto]; [Gen1]; [Gen2]; [Gen3].

Detect Non-Compliance Device

Use this item to detect Non-Compliance PCI Express Device in PEG.

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

▶ **PCH-IO Configuration**

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

▶ **HD Audio**

Use this item to control detection of the HD-Audio device.

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

[Disabled]: HDA will be unconditionally disabled;

[Enabled]: HDA will be unconditionally enabled;

▶ **Onboard Lan1 Controller**

Use this item to enable or disable onboard NIC.

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

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: [Enabled]; [Disabled].

Onboard Lan2 Controller

Use this item to control the PCI Express Root port.

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

PCIE4 Slot

Use this item to control the PCI Express Root port.

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

PCIE5 Slot

Use this item to control the PCI Express Root port.

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

PCIE6 Slot

Use this item to control the PCI Express Root port.

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

PCIE7 Slot

Use this item to control the PCI Express Root port.

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

M2M Slot

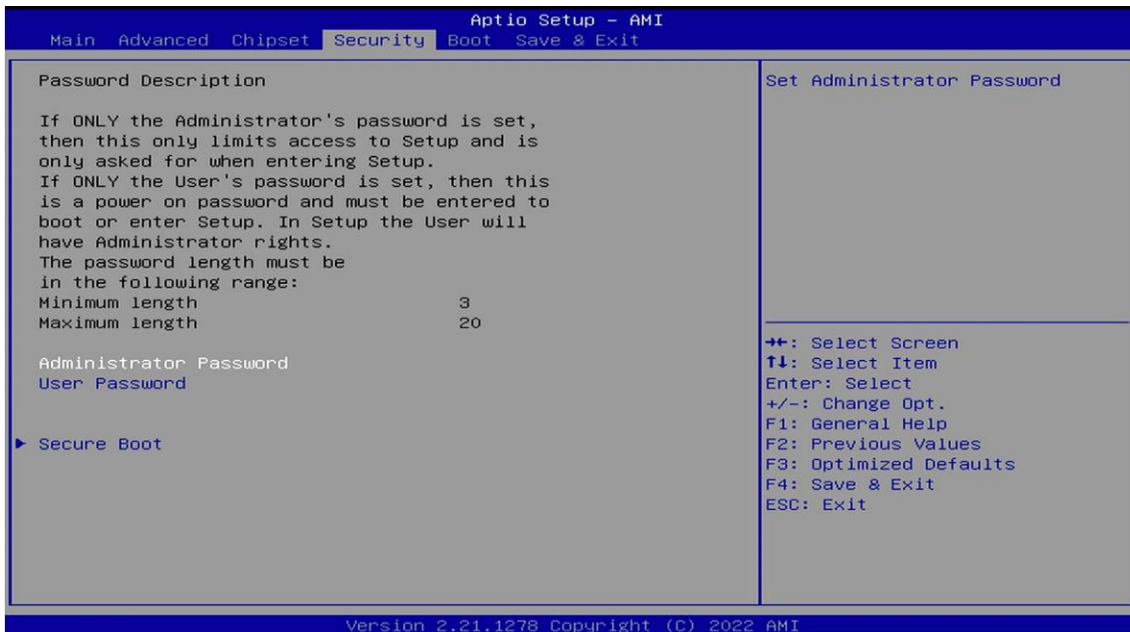
Use this item to control the PCI Express Root port.
The optional settings: [Disabled]; [Enabled].

System State After Power Failure

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

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

3-9 Security Menu



Administrator Password

This item allows user to set administrator password.

User Password

This item allows user to set user password.

▶ Secure Boot

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

Secure Boot

Secure boot feature is active if secure boot is enabled, platform key (PK) enrolled and the system is in user mode. The mode change requires platform reset.

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

Secure Boot Mode

Use this item to select secure boot mode options: standard or custom. In custom mode, secure boot policy variables can be configured by a physically present user without full authentication.

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

**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. 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:

Vendor Keys

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 'URFI 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/OsRecovery 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.

65535(0xFFFF) means indefinite waiting.

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

Bootup Numlock State

Use this item to select keyboard NumLock state.

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

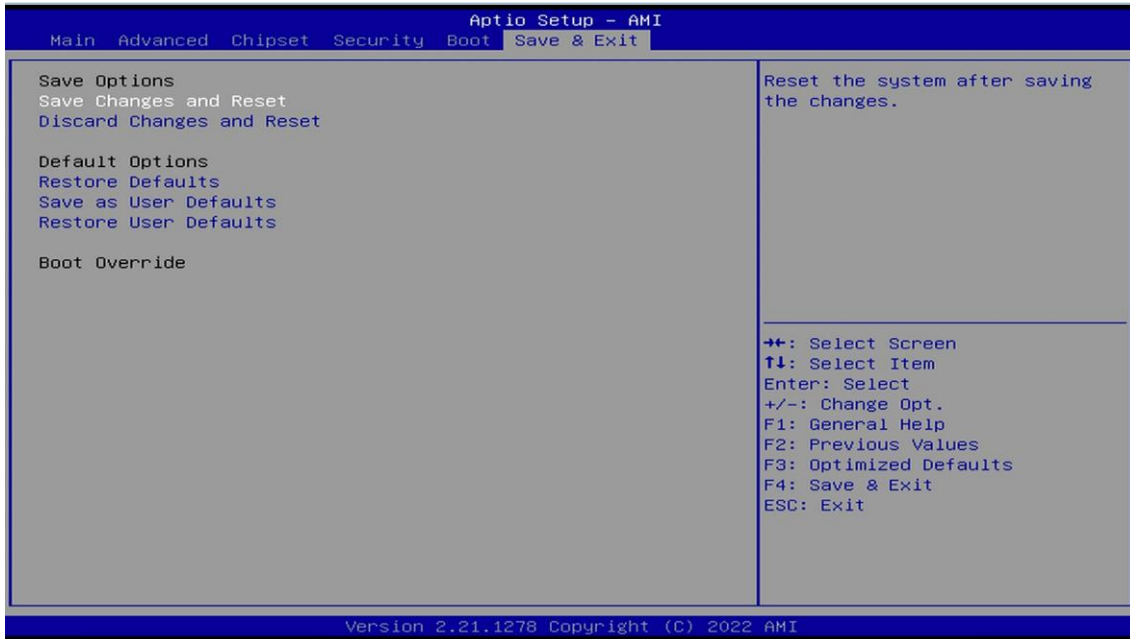
Quiet Boot

Use this item to Enable or Disable Quiet Boot option.

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

Boot Option Priorities

3-11 Save & Exit Menu



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 defaults to all the setup options.

Boot Override