

TECHNICAL MANUAL

of

Intel Q470E Express Chipset

Based Mini-ITX M/B

NO. G03-MI92V-F

Revision: 2.0

Release date: December 8, 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.

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.



TABLE OF CONTENT

ENVIRONMENTAL SAFETY INSTRUCTION.....	iii
USER'S NOTICE	iv
MANUAL REVISION INFORMATION	iv
ITEM CHECKLIST	iv
CHAPTER 1 INTRODUCTION OF THE MOTHERBOARD	
1-1 FEATURE OF MOTHERBOARD	1
1-2 SPECIFICATION	2
1-3 LAYOUT DIAGRAM	3
CHAPTER 2 HARDWARE INSTALLATION	
2-1 JUMPER SETTING.....	7
2-2 CONNECTORS AND HEADERS	11
2-2-1 CONNECTORS	11
2-2-2 HEADERS	17
CHAPTER 3 INTRODUCING BIOS	
3-1 ENTERING SETUP	21
3-2 BIOS MENU SCREEN	22
3-3 FUNCTION KEYS.....	23
3-4 GETTING HELP.....	23
3-5 MENU BARS	24
3-6 MAIN MENU	24
3-7 ADVANCED MENU	25
3-8 CHIPSET MENU	40
3-9 SECURITY MENU	44
3-10 BOOT MENU	47
3-11 SAVE & EXIT MENU	48



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 THE OWNER'S BENEFIT, WITHOUT INTENT TO INFRINGE.

Manual Revision Information

Reversion	Revision History	Date
2.0	Second Edition	December 8, 2022

Item Checklist

- ☒ Motherboard
- ☒ Cable(s)

Chapter 1

Introduction of the Motherboard

1-1 Feature of Motherboard

- Intel® Q470E express chipset
- LGA 1200 CPU socket for the 10th Intel® Core™ i7/ i5 /i3, Celeron & Pentium® processors (TDP Max support 65W)
- Support 2* DDR4 Max 2933MHz SO-DIMM up to 64GB and dual channel function
- 2* HDMI port, DP port & eDP with support for 3 independent displays
- Integrated with 1* Intel® i219-LM GbE & 1* Intel® i225V 2.5GbE LAN chips
- Support 2 * COM port (COM1/2 support RS232/422/485)
- Support up to **4 * USB 3.2 (Gen.2) port, 2 * USB 3.2 (Gen.1) port & 2 * USB 2.0 port**
- Support 4 * **SATAIII** (6Gb/s) Devices with RAID 0, 1, 5, 10 mode
- Support 1* PCIE 3.0 x16 slot, 1 * M.2 M-key 2280 slot (SATA/PClex4) support NVMe, 1* M.2 E-key 2230 slot (PClex1/USB2.0) support CNVi
- Support onboard TPM 2.0 (option)
- Support Smart FAN function
- Supports ACPI S3 Function
- Compliance with ErP Standard
- Support Watchdog Timer Technology
- Solution for Edge Computing / Digital Signage/Industrial PCs/Factory Automation/Public Sector/Digital Security/Surveillance

1-2 Specification

Spec	Description
Design	<ul style="list-style-type: none"> ● Mini-ITX form factor; PCB size:17.0x17.0cm
Chipset	<ul style="list-style-type: none"> ● Intel Q470E Express Chipset
CPU Socket	<ul style="list-style-type: none"> ● Intel LGA 1200 Socket supports 10th Core i7/i5/i3/Pentium/Celeron processors (Max. 65W TDP) * Note: for detailed CPU support information please visit our website
Memory Slot	<ul style="list-style-type: none"> ● 2*DDR4 SO-DIMM slot support 2* DDR4 SDRAM ● Maximum frequency: 2933MHz ● Maximum capacity: up to 64GB ● Support dual channel function * Note:Memory frequency range also depends on CPU support
Expansion Slot	<ul style="list-style-type: none"> ● 1* PCIE x16 slot (PCIE2) ● 1* M.2 E-key 2230 PCIe1/USB2.0 slot support CNVi (M2E) * Note:M2E slot maximum current limit is 2A while using 3.3V.
Storage	<ul style="list-style-type: none"> ● 4*SATAIII 6G/s ports with support for RAID 0/1/5/10 mode ● 1*M.2 M-key 2280 SATA/PCIex4 slot support NVMe(M2M) * Note:M2M slot maximum current limit is 2A while using 3.3V.
LAN Chip	<ul style="list-style-type: none"> ● Integrated with: ● 1* Intel i225V 2.5GbE PCI-E LAN chip of providing 10/100/1000/2500Mbps Ethernet data transfer rate * Note: 2500Mbps high-speed transmission rate is only supported over CAT 5e UTP cable. ● 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"> ● 128Mb AMI Flash ROM
Multi I/O	<p>Rear Panel I/O:</p> <ul style="list-style-type: none"> ● 2* RS232/422/485 COM port (COM1-2) ● 2* HDMI port & 1* DP port

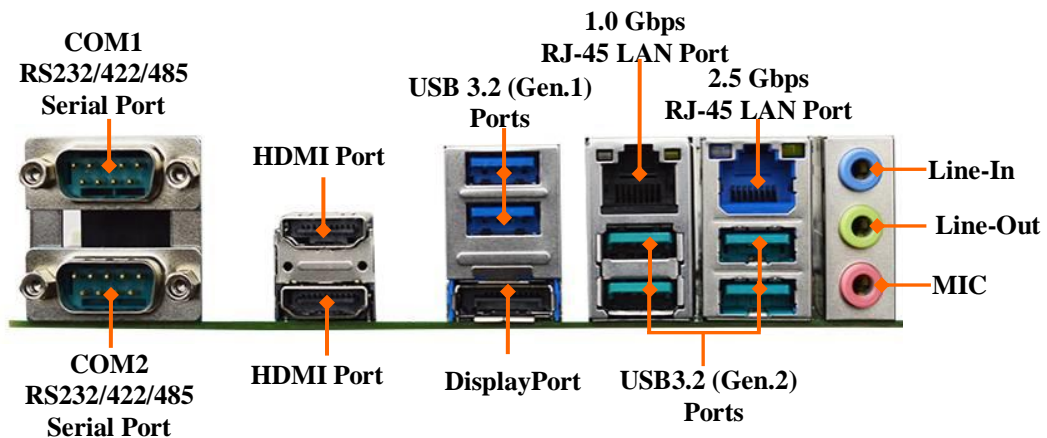
- 4* USB 3.2 (Gen.2) 10Gbps port
- 2* USB 3.2 (Gen.1) 5Gbps port
- 1* 1.0GbE RJ-45 LAN port & 2.5GbE RJ-45 LAN port
- 1* 3-jack audio connector (Line-in, Line-out, MIC)

Internal I/O Connectors & Headers:

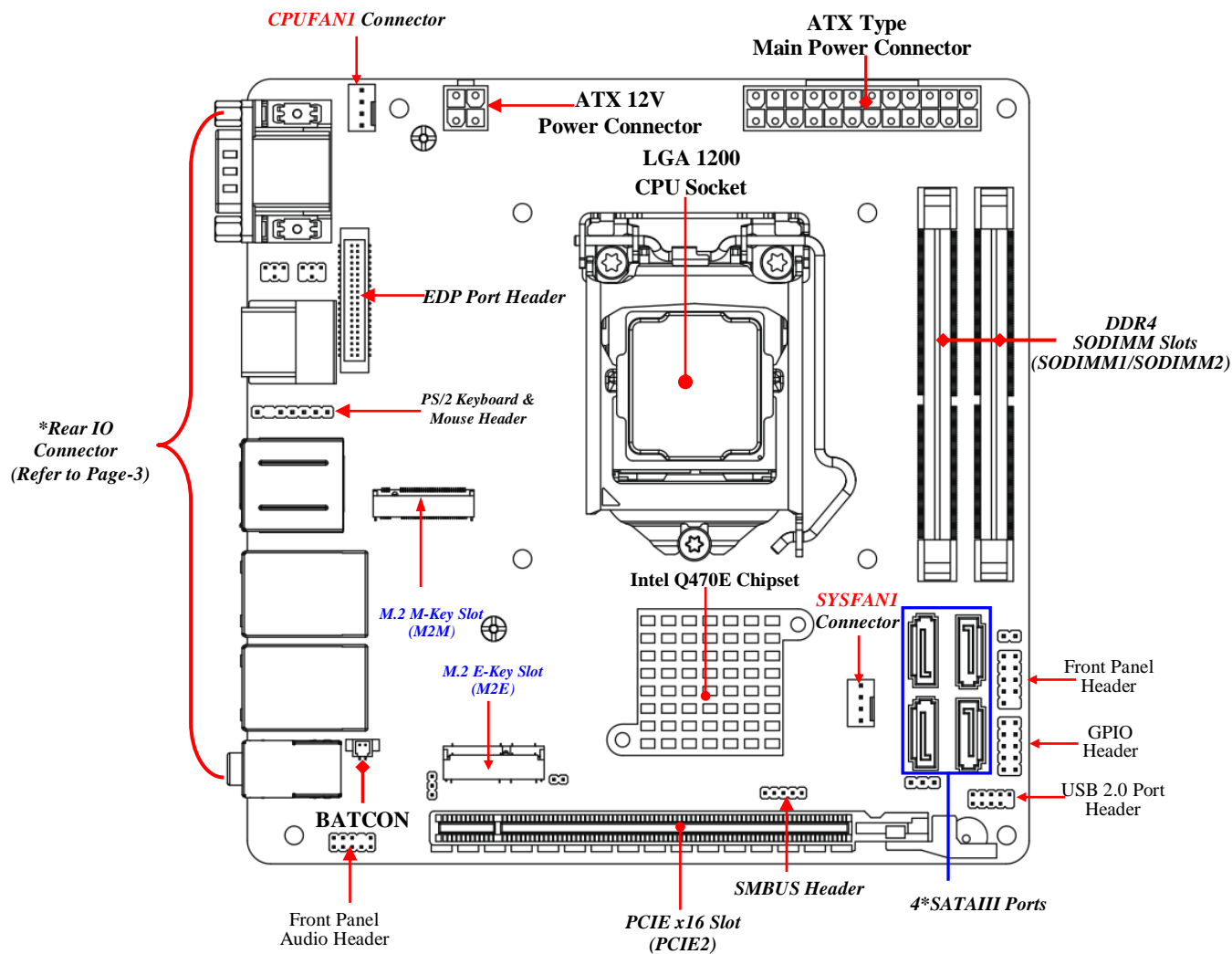
- 1* 24-pin main power connector
- 1* 4-pin 12V power connector
- 1* CPUFAN connector & 1* SYSFAN connector
- 1* Front panel header
- 1* 9-Pin USB 2.0 header for 2* USB 2.0 ports
- 1* GPIO header
- 1* SMBUS header
- 1* PS2 Keyboard & Mouse header
- 1* Front panel audio header
- 1* EDP header

1-3 Layout Diagram

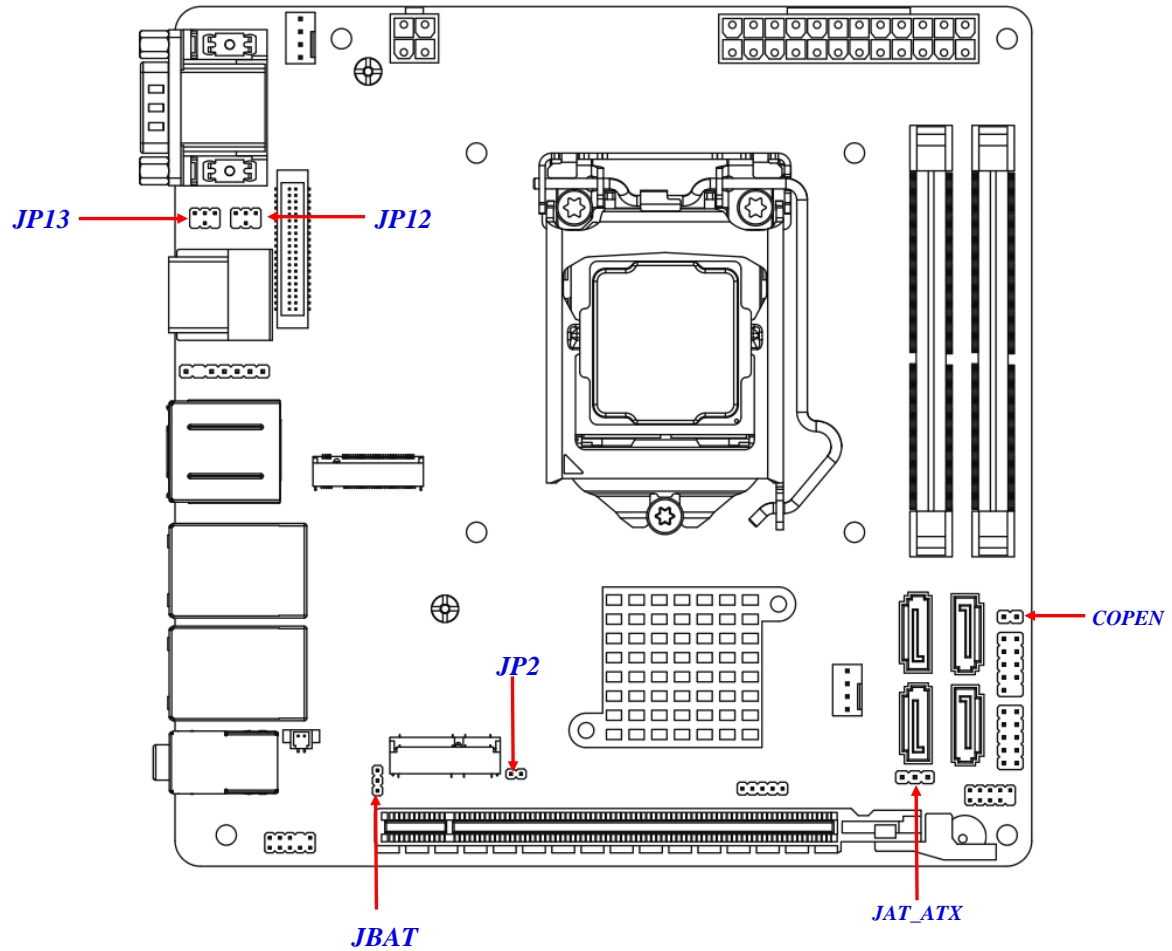
Rear IO Diagram



Motherboard Internal Diagram



Motherboard Jumper Positions



Jumper

P/N	Name	Description	Pitch
JP12	COM1 Port Pin9 Function Select	4-pin Block	2.0mm
JP13	COM2 Port Pin9 Function Select	4-pin Block	2.0mm
JBAT	Clear CMOS RAM Settings	3-pin Block	2.0mm
JP2	Flash Descriptor Override	2-pin Block	2.0mm
JAT_ ATX	ATX Mode / AT Mode Select	3-pin Block	2.0mm
COPEN	Case Open Display Select	2-pin Block	2.0mm

Connectors

P/N	Name
COM1-2	RS232/422/485 Serial COM Port Connector X2
HDMI1_2	HDMI Port Connector X2
DP	Display Port Connector
USB3	USB 3.2 (Gen.1) Port Connector X2
UL1	Top: 1.0GbE RJ-45 LAN Connector Mid. & Bottom: USB 3.2 (Gen.2) Port Connector X2
UL2	Top: 2.5GbE RJ-45 LAN Connector Mid. & Bottom: USB 3.2 (Gen.2) Port Connector X2
AUDIO	Top: Line-in Connector Middle: Line-out Connector Bottom: MIC Connector
ATXPWR	ATX Type Main Power Connector
ATX12V	12V Power Connector
SATA1/2/3/4	SATAIII Port Connector
CPUFAN1	CPU FAN Connector
SYSFAN	System FAN Connector

Headers

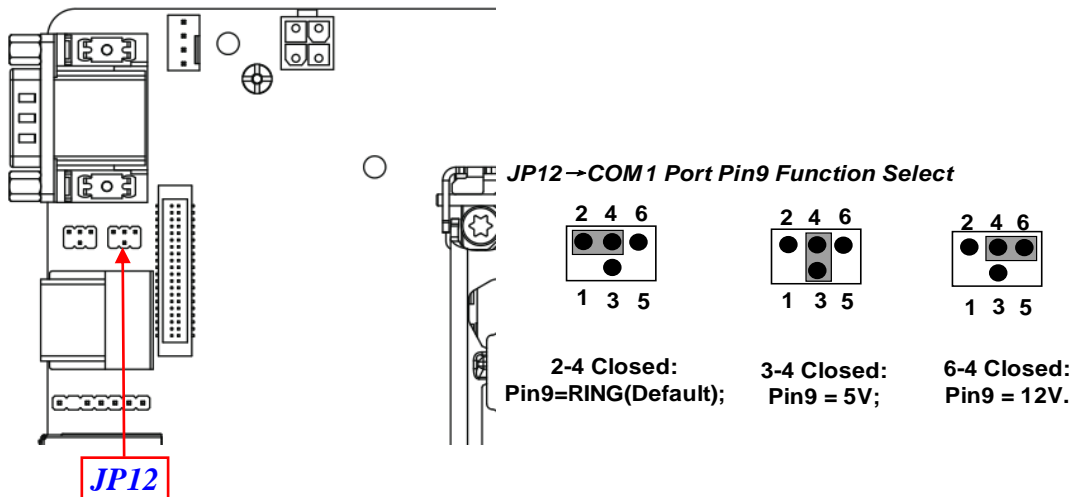
P/N	Name	Description	Pitch
FP	Front Panel Header(PWR LED/ HD LED/Power Button /Reset)	9-pin Block	2.54mm
GPIO	GPIO Port Header	10-pin Block	2.0mm
FP_USB1	USB 2.0 Port Header	9-pin Block	2.0mm
SMBUS	SMBUS Header	5-pin Block	2.0mm
FP_AUDIO	Front Panel Audio Header	9-pin Block	2.0mm
PS2KBMS1	PS2 Keyboard & Mouse Header	6-pin Block	2.54mm
EDP	EDP Header	40-pin Block	1.25mm

Chapter 2

Hardware Installation

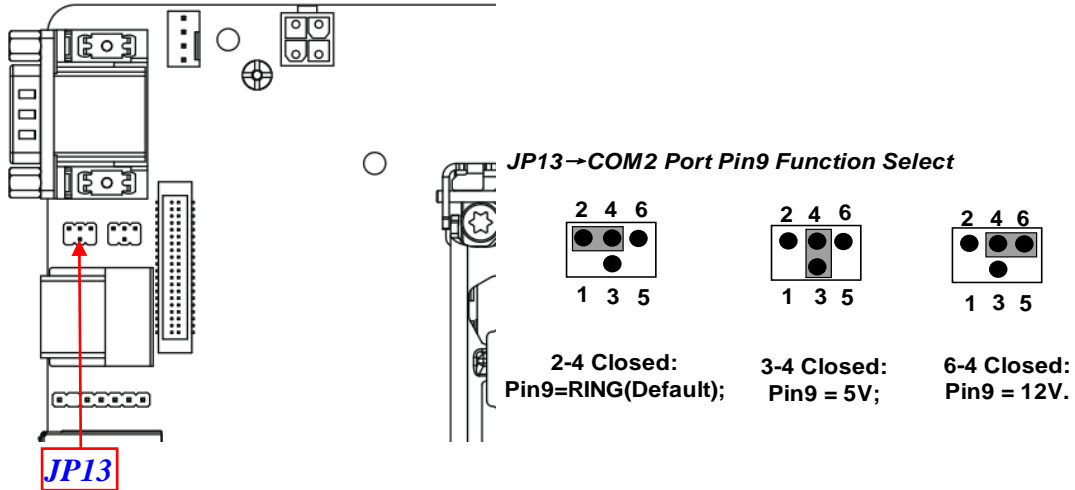
2-1 Jumper Setting

JP12 (4-pin): COM1 Port Pin9 Function Select



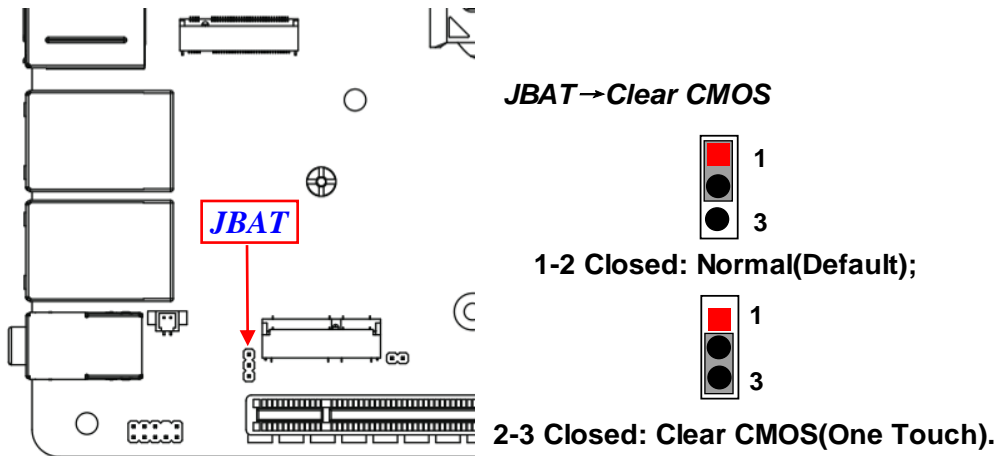
***Note:** Maximum current limit is 500mA while using 5V or 12V.

JP13 (4-pin): COM2 Port Pin9 Function Select

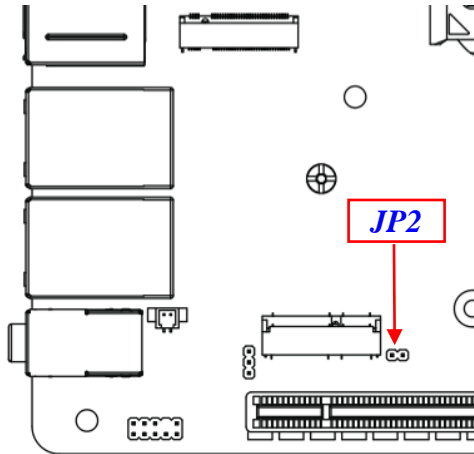


***Note:**Maximum current limit is 500mA while using 5V or 12V.

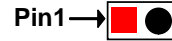
JBAT (3-pin): Clear CMOS RAM Settings



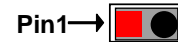
JP2(2-pin): Flash Descriptor Override Select



JP2 → Flash Descriptor Override

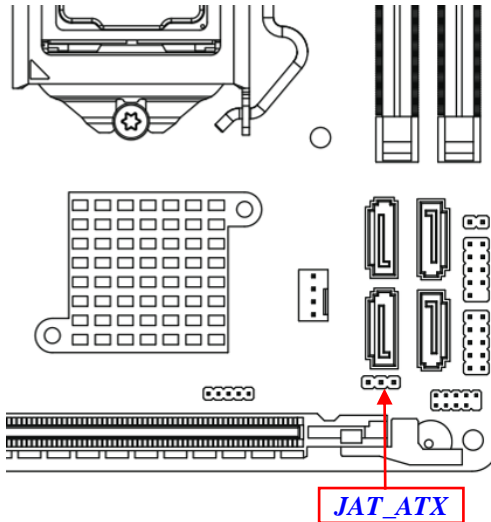


**1-2 Open: Enable Security Measures
in the Flash Descriptor(Default);**

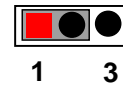


**1-2 Closed: Disable Flash
Descriptor Security (override).**

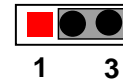
JAT_ATX (3-pin): ATX Mode/AT Mode Select



JAT_ATX → ATX/AT Mode Select



1-2 Closed: ATX Mode Selected(Default);

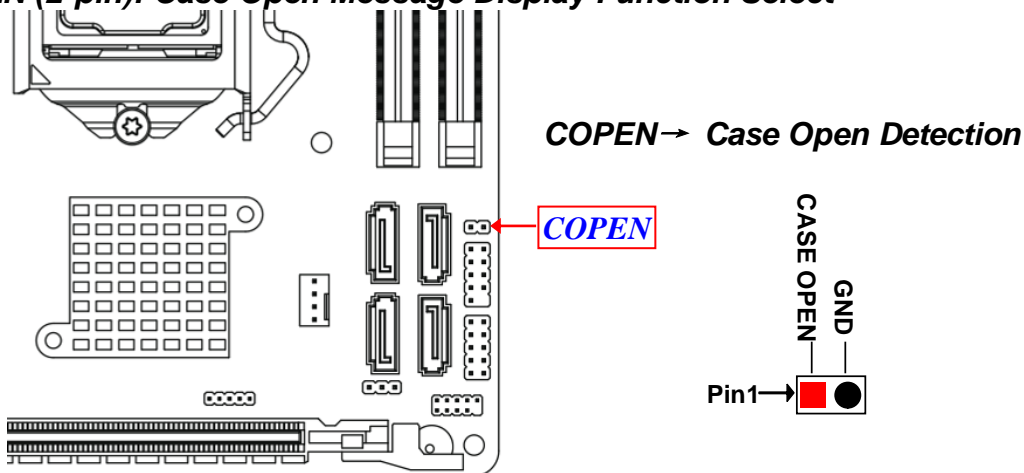


2-3 Closed: AT Mode Selected.

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

AT Mode Selected: Directly power on as power input ready.
User needs to restart the system for the settings to take effect.

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





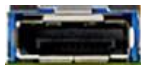





Pin (1&2) Closed: When Case open function pin short to GND, the Case open function was detected. When used, needs to enter BIOS and enable 'Case Open Detect' function. In this case if your case is removed, next time when you restart your computer, a message will be displayed on screen to inform you of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

2-2 Connectors and Headers

2-2-1 Connectors

Rear Panel Connectors

**Refer to Page-3 Rear IO Diagram*

<i>Icon</i>	<i>Name</i>	<i>Function</i>
	RS232/422/485 Serial Port	Mainly for user to connect external MODEM or other devices that supports Serial Communications Interface.
	HDMI Port	To connect display device that support HDMI specification.
	Display Port	To the system to corresponding display device with compatible DP cable.
	USB 3.2 (Gen.1) Port	To connect USB keyboard, mouse or other devices compatible with USB 3.2 (Gen.1) specification. Ports support up to 5Gbps data transfer rate.
	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) Port	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

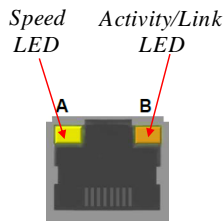
***Note:** Maximum current limit for USB ports from **UL1/UL2/USB3** is **1.5A** while using **5V** working voltage.

(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:



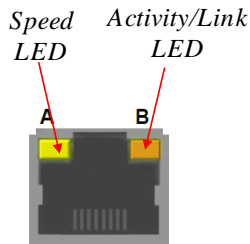
A: Speed LED

Status	Description
Off	10Mbps connection
Orange	100Mbps connection
Green	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

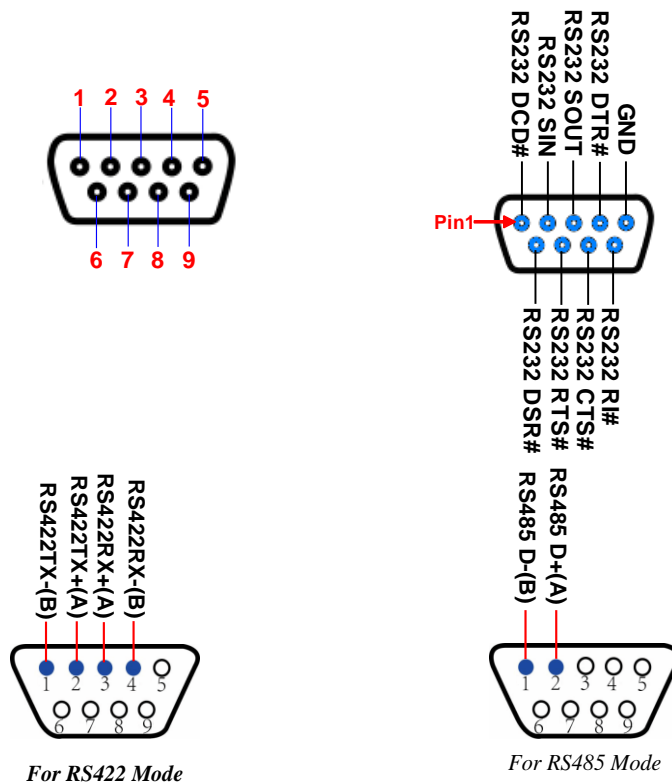
B: Activity/Link LED

Status	Description
Off	No Link
Blinking	Data Activity
On	Link

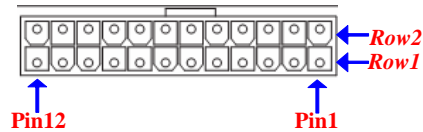
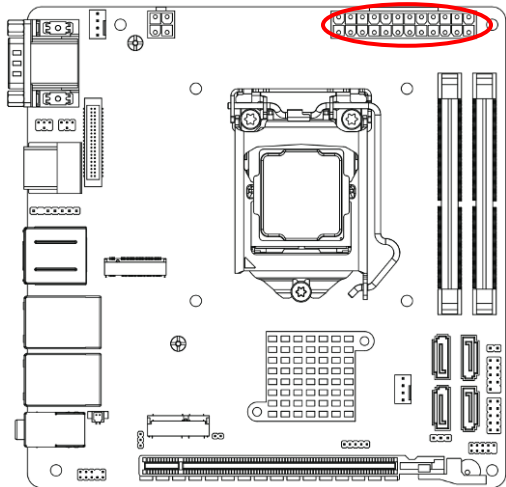
*** Note:** **2.5Gbps** high-speed transmission rate is **only** supported over **CAT 5e UTP** cable.

(2) COM1-2: RS232/422/485 Ports

COM1/COM2 port can function as RS232/422/485 port. In normal settings COM1/COM2 functions as RS232 port. With compatible COM cable COM1/COM2 can function as RS422 or RS 485 port. User also needs to go to BIOS to set '**Transmission Mode Select**' for COM1/COM2 at first, before using specialized cable to connect different pins of this port.

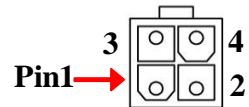
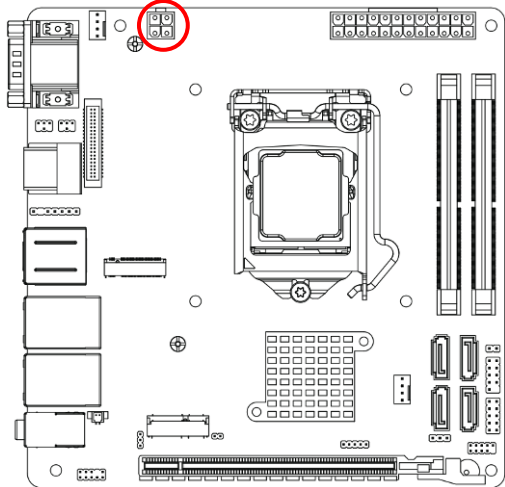


(3) ATXPWR(24-pin block): Main Power Connector



PIN	ROW1	ROW2
1	+3.3V	+3.3V
2	+3.3V	-12V
3	GND	GND
4	+5V	Soft Power on
5	GND	GND
6	+5V	GND
7	GND	GND
8	Power OK	-5V
9	+5V Stand by	+5V
10	+12V	+5V
11	+12V	+5V
12	+3.3V	GND

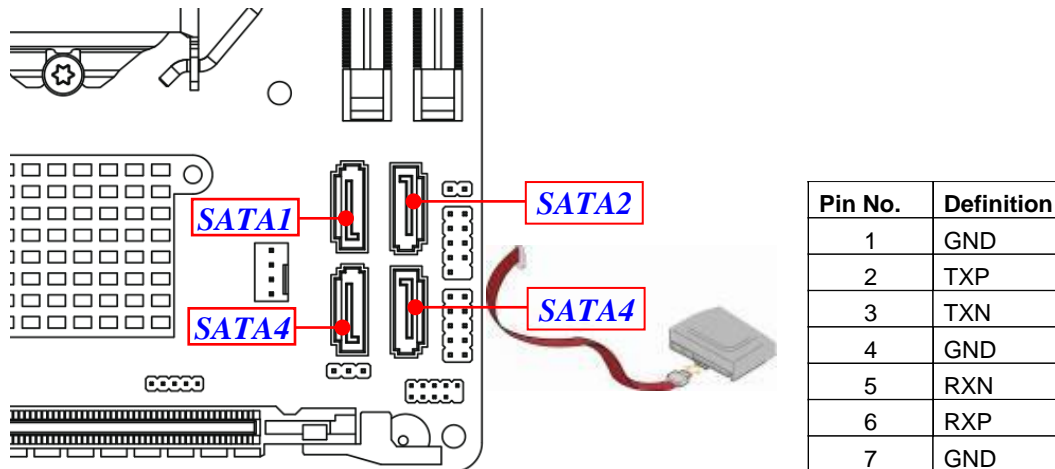
(4) ATX12V (4-pin block): ATX-Type 12V Power Connector



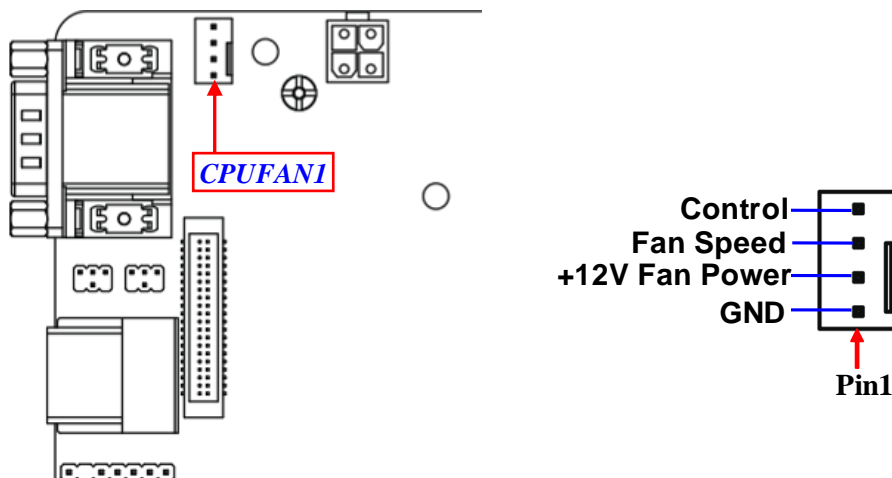
Pin No.	Definition
1	GND
2	GND
3	+12V
4	+12V

(5) SATA1/2/3/4 (7-pin): SATAIII Port connector

These are high-speed SATAIII port that supports 6GB/s transfer rate.

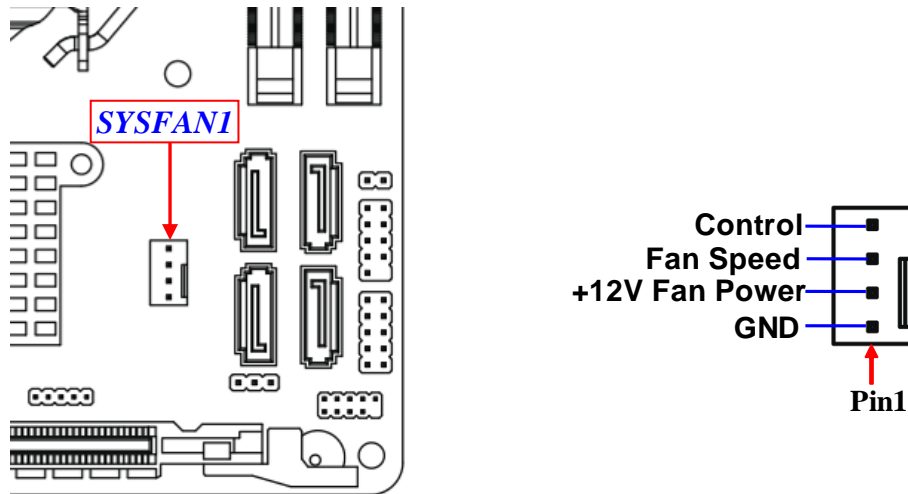


(6) CPUFAN1 (4-pin): CPU Fan Connector



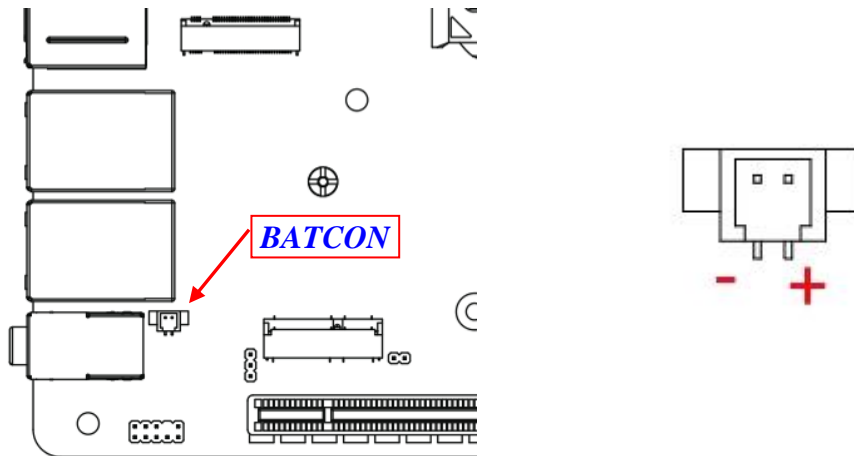
***Note:** Maximum current limit is **1.5A** while using 12V working voltage.

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



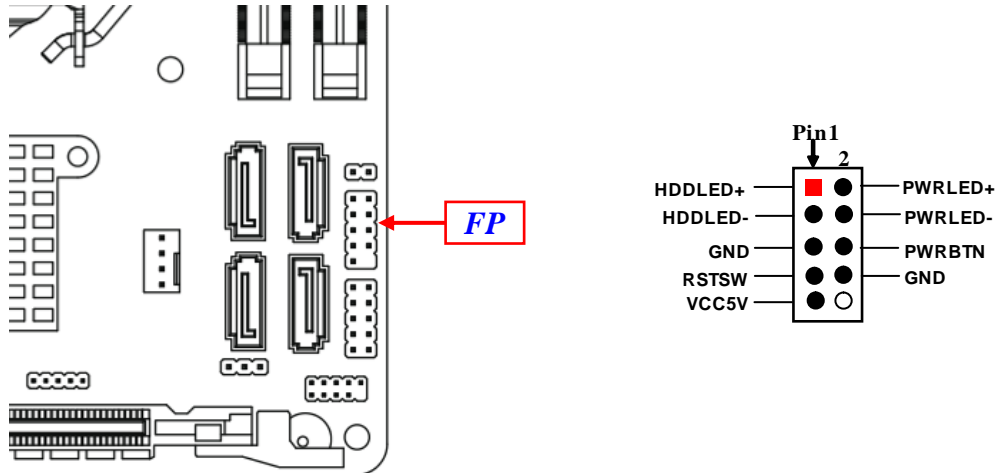
***Note:** Maximum current limit is **1.5A** while using 12V working voltage.

(8) BATCON (2-pin): Battery Connector



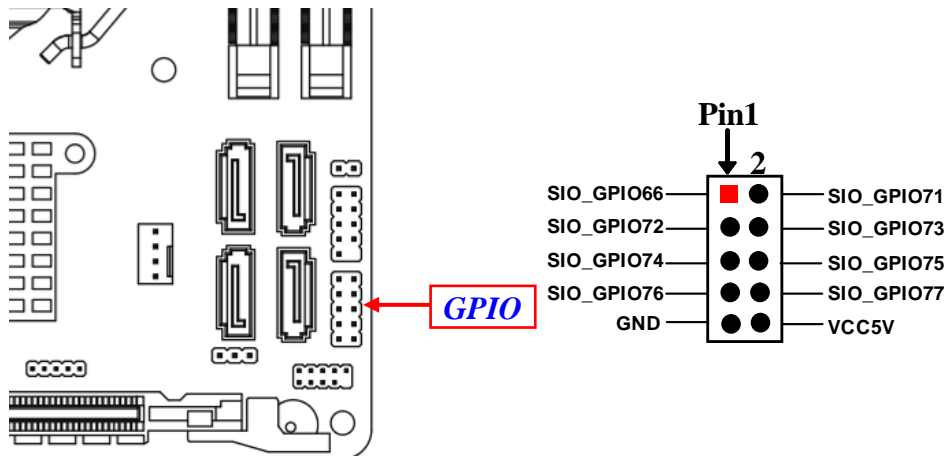
2-2-2 Headers

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



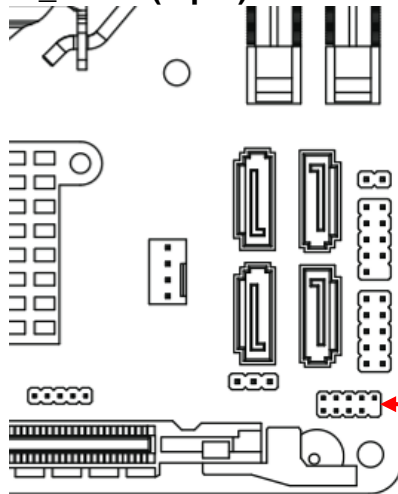
***Note:** Maximum current limit is **1A** while using 5V working voltage.

(2) GPIO (10-pin): GPIO Port Header

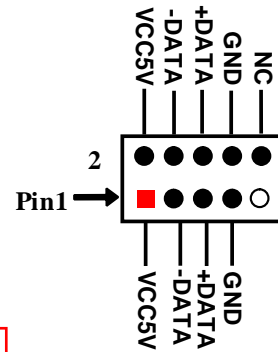


***Note:** Maximum current limit is **1A** while using 5V working voltage.

(3) **FP_USB1 (9-pin): USB 2.0 Port Header**

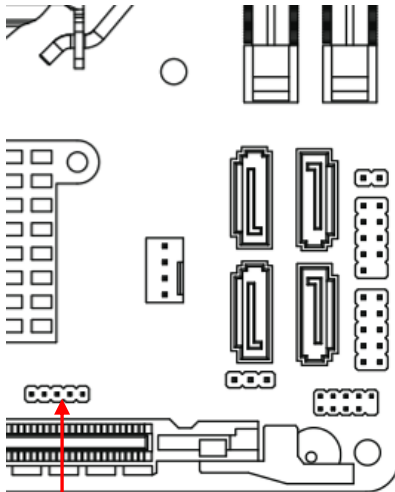


FP_USB1

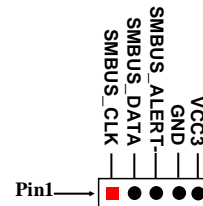


***Note:** Maximum current limit is **1.5A** in total while using 5V working voltage.

(4) **SMBUS (5-pin): SMBUS Header**

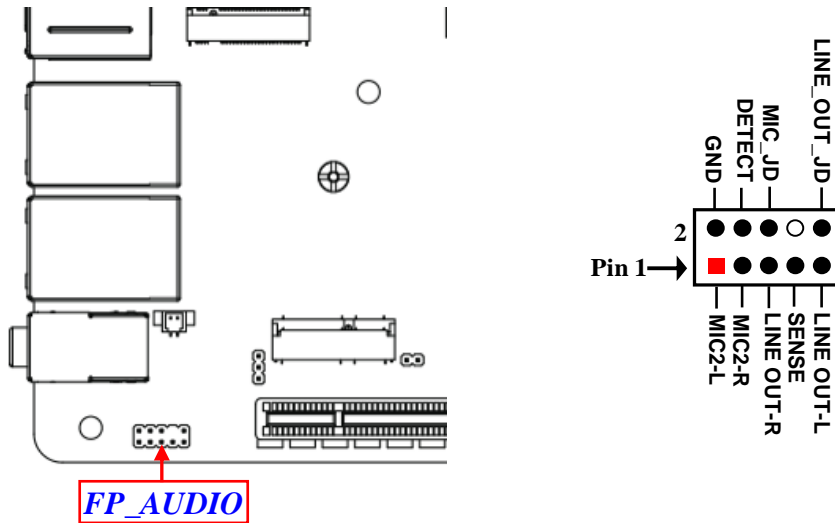


SMBUS

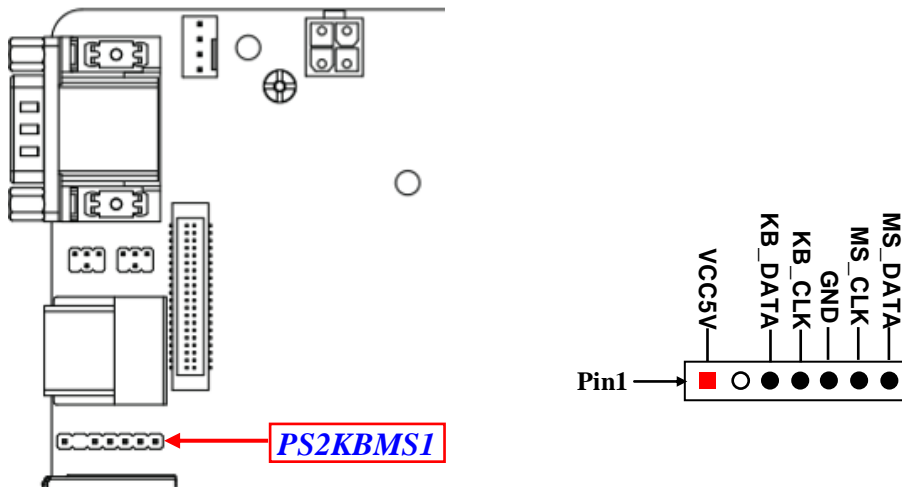


(5) FP_AUDIO (9-pin): Line-Out, MIC-In Header

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

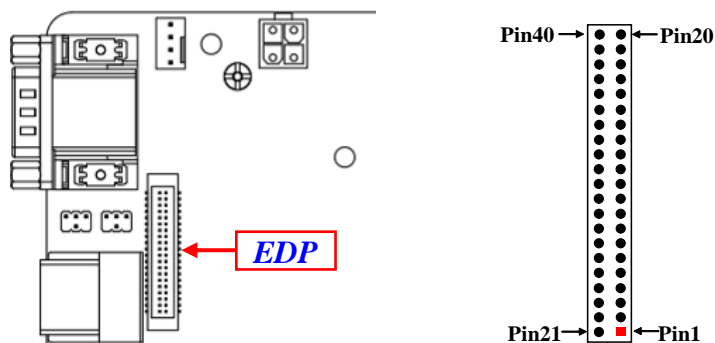


(6) PS2KBMS1 (6-pin): PS/2 Keyboard & Mouse Header



***Note:** Maximum current limit is **500mA** while using 12V working voltage.

(7) EDP (40-Pin): EDP wafer



Pin Define	Pin NO.	Pin NO.	Pin Define
XX	Pin 40	Pin 20	LCD_VCC
Backlight power	Pin 39	Pin 19	LCD_VCC
Backlight power	Pin 38	Pin 18	LCD_VCC
Backlight power	Pin 37	Pin 17	GND
Backlight power	Pin 36	Pin 16	EDP_AUXN
XX	Pin 35	Pin 15	EDP_AUXP
XX	Pin 34	Pin 14	GND
EDP_Backlight PWM	Pin 33	Pin 13	EDP_TXP0
EDP_Backlight Enable	Pin 32	Pin 12	EDP_TXN0
GND	Pin 31	Pin 11	GND
GND	Pin 30	Pin 10	EDP_TXP1
GND	Pin 29	Pin 9	EDP_TXN1
GND	Pin 28	Pin 8	GND
EDP_HPDP	Pin 27	Pin 7	EDP_TXP2
GND	Pin 26	Pin 6	EDP_TXN2
GND	Pin 25	Pin 5	GND
GND	Pin 24	Pin 4	EDP_TXP3
GND	Pin 23	Pin 3	EDP_TXN3
XX	Pin 22	Pin 2	GND
XX	Pin 21	Pin 1	XX

***Note:** 1. Maximum current limit is **2A** while using 12V backlight power working voltage;
2. Maximum current limit is **3A** while using 3V LCD_VCC working voltage

Chapter 3

Introducing BIOS

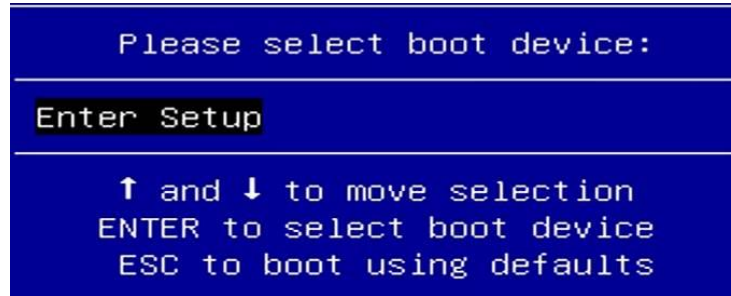
Notice! The BIOS options in this manual are for reference only. Different configurations may lead to difference in BIOS screen and BIOS screens in manuals are usually the first BIOS version when the board is released and may be different from your purchased motherboard. Users are welcome to download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

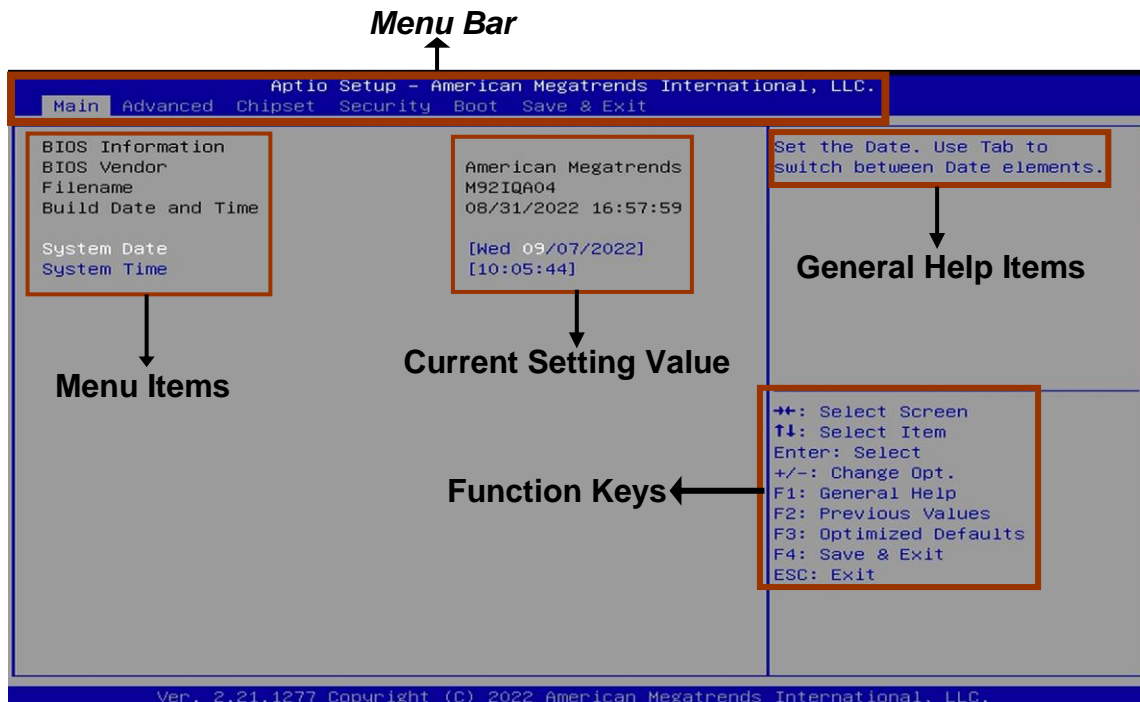
Press **** to enter Setup; press **< F7>** to enter pop-up Boot menu.



BIOS Boot Menu Screen (boot device options please refer to actual configuration)

3-2 BIOS Menu Screen

The following diagram show a general 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

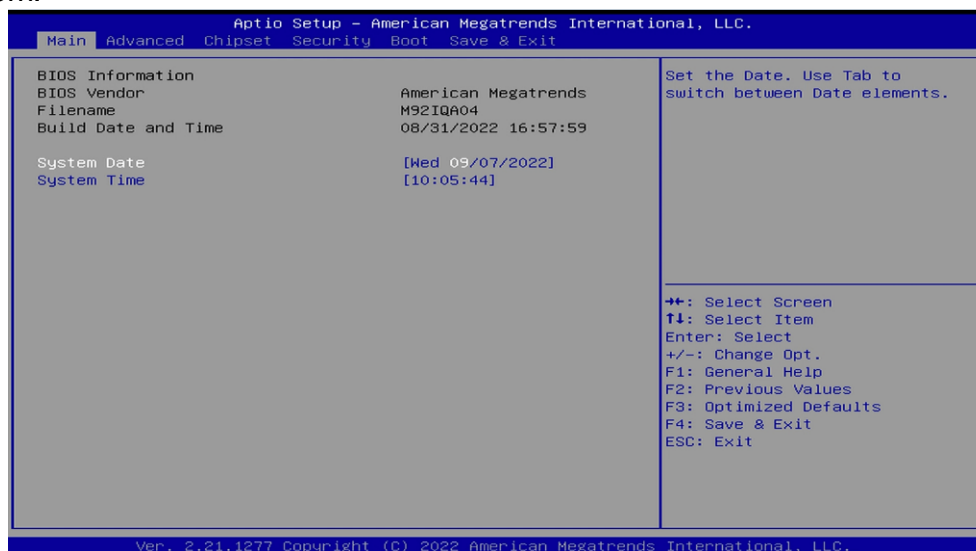
There are six menu bars on top of BIOS screen:

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.



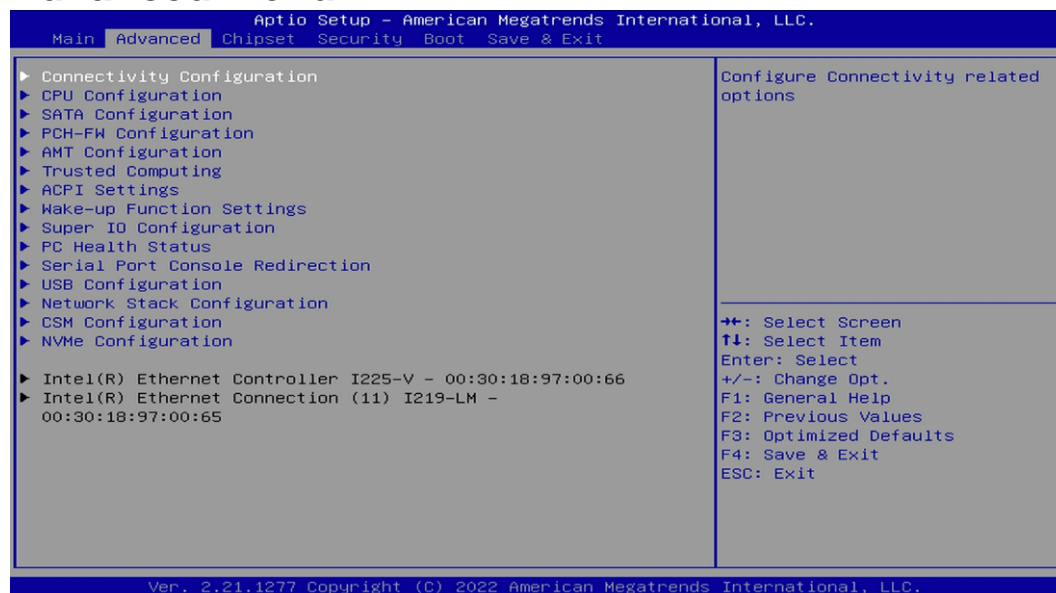
System Date

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

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:

Hyper-Threading

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

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

Intel (VMX) Virtualization Technology

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

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. When set as [Enabled], it 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].

****Note:** 'Turbo Mode' item may or may not show up, depending on different CPU.*

► SATA Configuration

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

SATA Configuration

SATA Controller(s)

Use this item to enable or disable SATA Device.

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

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

SATA Mode Selection

This item determines how SATA controller(s) operate.

The optional settings: [AHCI]; [RAID].

SATA1/SATA2/SATA3/SATA4

Port

Use this item to enable or disable SATA Port.

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

Hot Plug

Use this item to designate this port as Hot Pluggable.

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

M.2

Port

Use this item to Enable or Disable SATA Port.

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

▶ **PCH-FW Configuration**

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

ME Firmware Version

ME Firmware Mode

TPM Device Selection

Use this item to select TPM device: PTT or dTPM. PTT-Enables PTT in SkuMgr
dTPM 1.2-Disables PTT in SkuMgr

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

The optional settings: [dTPM]; [PTT]

▶ **Firmware Update Configuration**

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].

** **Note:** 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.*

▶ **AMT Configuration**

Use this item to configure Intel(R) Active Management Technology Parameters.

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

USB Provisioning of AMT

Use this item to enable or disable AMT USB Provisioning.

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

▶ **CIRA Configuration**

This item is for user to configure Remote Assistance Process parameters.

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

Activate Remote Assistance Process

Use this item to trigger CIRA boot.

***Note:** *Network Access must be activated first from MEBx Setup.*

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

When set as [Enabled], user can make further settings in ‘CIRA Timeout**’.*

CIRA Timeout

OEM defined timeout for MPS connection to be established.

The setting range is from [0] to [255].

[0]: use the default timeout value of 60 seconds;

[255]: MEBx waits until the connection succeeds.

▶ **ASF Configuration**

This item is for user to configure Alert Standard Format parameters.

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

PET Progress

Use this item to enable or disable PET Events Progress to receive PET Events.

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

WatchDog

Use this item to enable or disable WatchDog Timer.

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

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

OS Timer

Use this item to set OS watchdog timer.

BIOS Timer

Use this item to set BIOS watchdog timer.

ASF Sensors Table

Use this item to add ASF Sensor Table into ASF ! ACPI Table.

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

‣ **Secure Erase Configuration**

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

Secure Erase Mode

Use this item to change Secure Erase module behavior.

The optional settings: [Simulated]; [Real].

[Simulated]: Performs SE flow without erasing SSD.

[Real]: Erase SSD.

Force Secure Erase

This item is for user to force Secure Erase on next boot.

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

‣ **OEM Flags Settings**

Use this item to configure OEM flags.

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

Hide Unconfigure ME Confirmation Prompt

Use this function to enable or disable Hide Unconfigure ME confirmation prompt when attempting ME unconfiguration.

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

MEBx OEM Debug Menu Enable

Use this function to enable or disable OEM debug menu in MEBx.

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

Unconfigure ME

Use this function to enable or disable Unconfigure ME with resetting MEBx password to default.

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

‣ **MEBx Resolution Settings**

Use this item to configure resolution settings for MEBx display modes.

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

Non-UI Mode Resolution

Use this item to set resolution for non-UI text mode.

The optional settings: [Auto]; [80x25]; [100x31].

UI Mode Resolution

Use this item to set resolution for UI text mode.

The optional settings: [Auto]; [80x25]; [100x31].

Graphics Mode Resolution

Use this item to set resolution for graphics mode.

The optional settings: [Auto]; [640x480]; [800x600]; [1024x768].

► **Trusted Computing**

Press [Enter] to view current status information, or make further settings in the following sub-items:

TPM 2.0 Device Found

****Note:** TPM function is optional, **MI92V12** model supports TPM2.0.*

Security Device Support

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

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

When set as **[Enabled]**, user can make further settings in the following 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].

TPM2.0 UEFI Spec Version

Use this item to select the TCG2 Spec Version Support.

The optional settings: [TCG_1_2]; [TCG_2].

[TCG_1_2]: The Compatible mode for Win8/Win10.

[TCG_2]: Support new TCG2 protocol and event format for Win10 or later.

► **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: [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], 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.

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).

PS2 KB/MS Wake-up

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

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

***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 Wake-up.

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

***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 System Shutdown.

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

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

► **Super IO Configuration**

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

Super IO Configuration

ERP Support

Use this item to select Energy-Related Products function. This item should be set as [Disabled] if you wish to have all active wake-up functions.

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

► **Serial Port 1 Configuration**

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

Serial Port 1 Configuration

Serial Port

Use this item to enable or disable Serial Port (COM).

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

When set as [Enabled], user can make further settings in the following 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: [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 2 Configuration

Serial Port

Use this item to enable or disable Serial Port (COM).

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

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

WatchDog Reset Timer

Use this item to enable or disable WDT reset function. When set as [Enabled], the following sub-items shall appear:

WatchDog Reset Timer Value

User can select a value in the range of [4] to [255] seconds when 'WatchDog Reset Timer Unit' set as [Sec]; or in the range of [4] to [255] minutes when 'WatchDog Reset Timer Unit' set as [Min].

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 Pin 1&2 of for ATX Mode & Pin 2&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: [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, make further settings in 'SmartFAN Configuration' and set value in 'Shutdown Temperature'.

▶ **SmartFAN Configuration**

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

SmartFAN Configuration

CPUFAN1 / SYSFAN1 Smart Mode

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

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

CPUFAN1 / SYSFAN1 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.

CPUFAN1 / SYSFAN1 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.

CPUFAN1 / SYSFAN1 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.

CPUFAN1 / SYSFAN1 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

Use this item to enable or disable COM1 Console Redirection.

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

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

► **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 sub-items.

COM1

Console Redirection Settings

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].

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

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

Terminal Type EMS

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 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: [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].

Data Bits EMS

The default setting is: [8].

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

Parity EMS

The default setting is: [None].

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

Stop Bits EMS

The default setting is: [1].

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

► **USB Configuration**

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

USB Configuration

Legacy USB Support

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

USB Mass Storage Driver Support

Use this item to enable or disable USB mass storage driver support.

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

USB hardware delays and time-outs:

USB transfer time-out

Use this item to set the time-out value for Control, Bulk, and Interrupt transfers.

The optional settings: [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: [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. 'Auto' uses default value: for a root port it is 100 ms, for a hub port the delay is taken from hub descriptor.

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: [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 support will not be available.

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

Ipv6 PXE Support

Use this item to enable IPv6 PXE boot support. When set as [Disabled], IPv6 boot support will not be available.

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

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:

Compatibility Support Module Configuration

CSM Support

Use this item enable or disable CSM support.

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

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

Option ROM execution

Network

This option controls the execution of Network OpROM.

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

Storage

This option controls the execution of UEFI and Legacy Storage OpROM.

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

Other PCI devices

This item is for system to determine OpROM execution policy for devices other than Network, Storage or Video.

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

▶ **NVMe Configuration**

Press [Enter] to view current NVMe Configuration.

****Note**: options only when NVME device is available.*

****Note**: When ‘**CSM Support**’ set as **[Disabled]** and ‘**SATA Mode Selection**’ set as **[RAID]**, the following sub-items shall appear:*

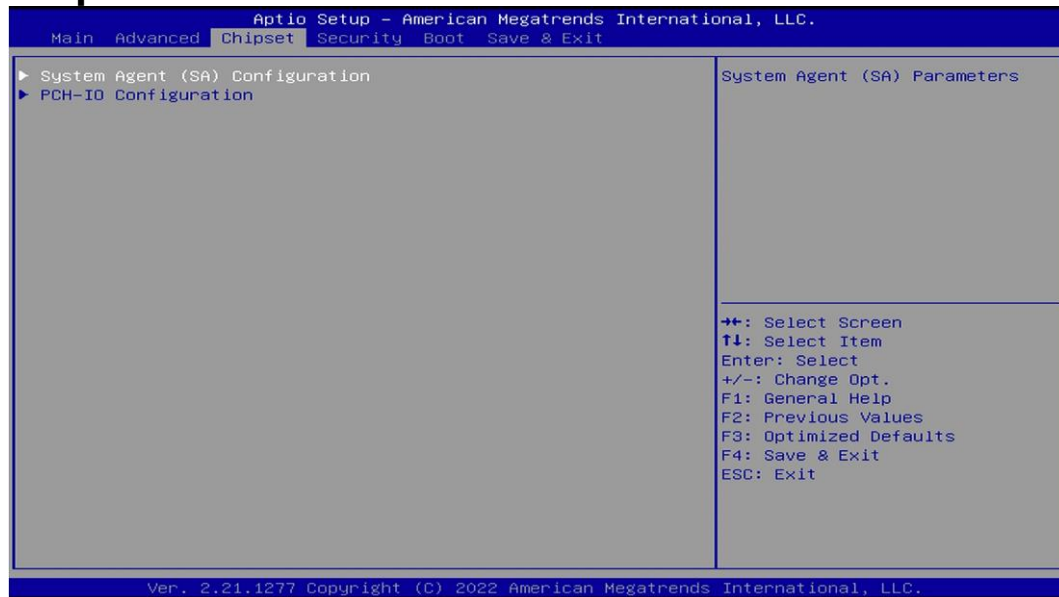
▶ **Intel(R) Ethernet Controller I225-V - XX:XX:XX:XX:XX:XX**

This item shows current network brief information.

▶ **Intel(R) Ethernet Connection (11) I219-LM - XX:XX:XX:XX:XX:XX**

This item shows current network brief information.

3-8 Chipset Menu



► **System Agent (SA) Configuration**

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

System Agent (SA) Configuration

VT-d

► **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 Display

Use this item to select which Graphics device should be primary display.

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

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.

eDP will be supported only on primary display.

The optional setting: [VBIOS Default]; [HDMI1]; [HDMI2]; [DP]; [eDP].

***Note:** Only when ‘**CSM Support**’ is select as [Enabled], user can make further settings in the following sub-items.

***Note:** In the case that the ‘**Primary IGFX Boot Display**’ is select as [HDMI1], [HDMI2], [DP] 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: [Disabled]; [HDMI1]; [HDMI2]; [DP].

Internal Graphics

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

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

Aperture Size

Use this item to select the Aperture Size.

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

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

DVMT Total Gfx Mem

Use this item to select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

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

► PEG Port Configuration

Press [Enter] to make further settings for PEG port options.

PEG Port Configuration

PEG Lane Select

Use this item to select X16 or X8/X8.

The optional settings: [X16]; [X8/X8].

When set as [X8/X8], the PCIE2 Slot (Bifurcation) items shall appear:

PCIE2 Slot

Enable Root Port

Use this item to enable or disable the Root Port. Root Port will Always Enable if set x8 Bifurcation.

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].

Max Link Width

This item is for user to force PEG link to retrain to X1/2/4/8.

The optional settings are: [Auto]; [Force X1]; [Force X2]; [Force X4]; [Force X 8].

PCIE2 Slot (Bifurcation)

Max Link Speed

Use this item to configure PEG 0:1:1 Max Speed.
The optional settings: [Auto]; [Gen1]; [Gen2]; [Gen3].

Max Link Width

This item is for user to force PEG link to retrain to X1/2/4/8.
The optional settings are: [Auto]; [Force X1]; [Force X2]; [Force X4].

Detect Non-Compliance Device

This item is for user to detect Non-Compliance PCI Express Device in PEG.
The optional settings: [Disabled]; [Enabled].

► **PCH-IO Configuration**

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

PCH-IO Configuration

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]: HAD will be unconditionally enabled.

Onboard Lan1 Controller/2 Controller

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

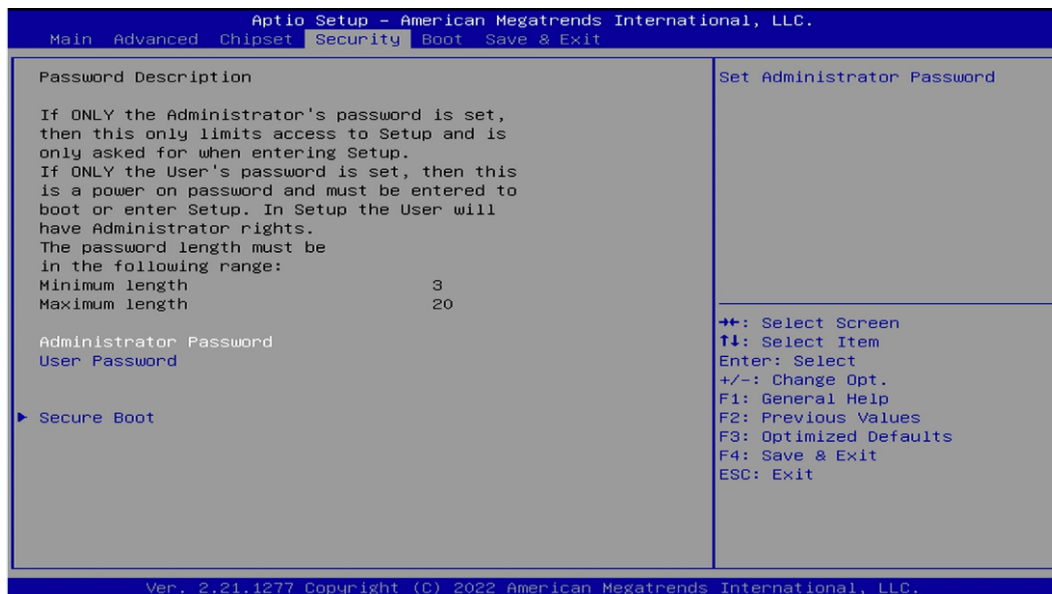
System State After Power Failure

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].

***Note:** The option [Always On] and [Former State] are affected by ‘**ERP Support**’ function. Please disable ERP to support [Always On] and [Former State] function.

3-9 Security Menu



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 user 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 user password.

► Secure Boot

Press [Enter] to make customized secure settings:

System Mode

Secure Boot

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.

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

Secure Boot Mode

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

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, 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 expert users to modify Secure Boot Policy variables without full authentication, 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: [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**

- ▶ **Export Secure Boot variables**

▶ **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**

▶ **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 Signatures/Forbidden Signatures/ Authorized TimeStamps/OsRecovery Signatures**

Use this item to enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:

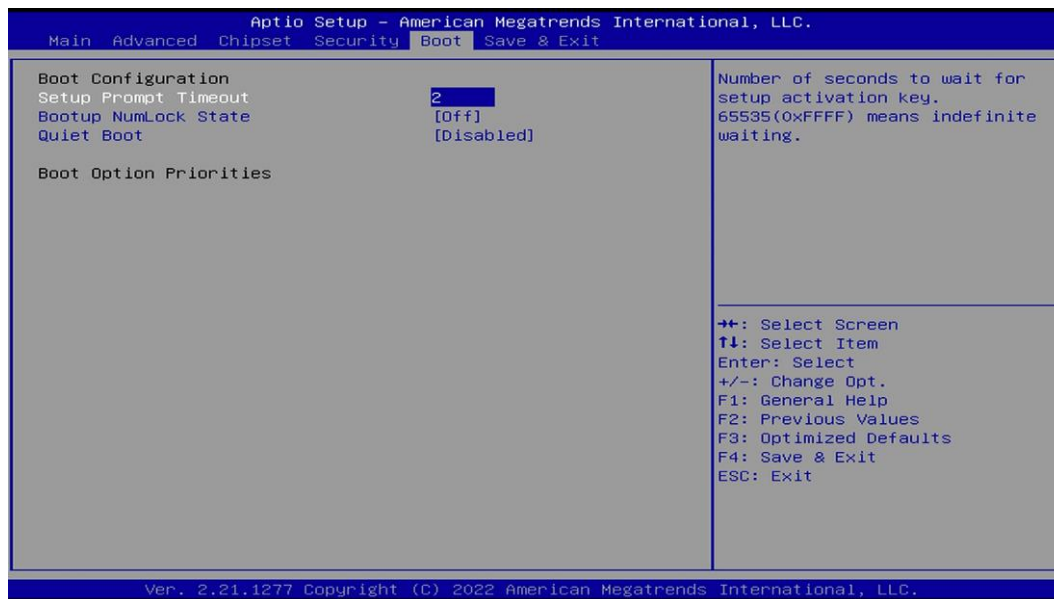
- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

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.

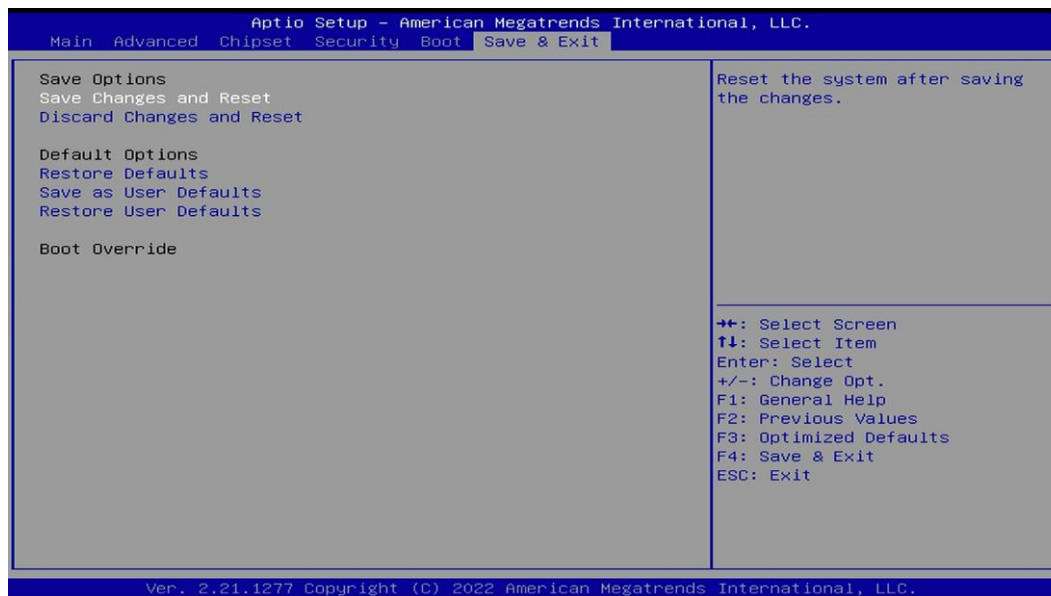
The optional settings are: [On]; [Off].

Quiet Boot

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

Boot Option Priorities

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 the user defaults to all the setup options.

Boot Override