MI225 Series

User's Manual

NO. G03-MI225-F

Revision: 1.0

Release date: June 13, 2023

Trademark:

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.

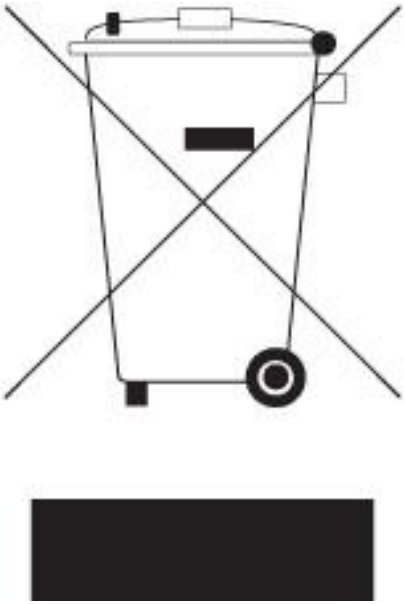


TABLE OF CONTENT

Environmental Safety Instruction

- 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

Manual Revision Information

Reversion	Revision History	Date
1.0	First Edition	June 13, 2023

Item Checklist

- ☑ Motherboard
- ☑ DVD for motherboard utilities
- ☑ User's Manual
- ☑ Cable(s)
- ☑ I/O Back panel shield

Chapter 1
Introduction of the Motherboard

1-1 Feature of Motherboard

- Intel® LGA1700 Socket supports 12th /13th Gen. Core Processor **(Max. 65W TDPs under 180A)**
- Support 2* DDR5 4800MHz SO-DIMM up to 64GB
- Integrated with 1* Intel® i219-LM GbE & 1* Intel® i225V 2.5GbE LAN chips
- Support 1* VGA, 1* HDMI, 1* DP, 1* LVDS/eDP Output
- Support 6* COM (COM1 support RS232/422/485)
- **MI225Q670X/R680X series:** total support up to 6* USB3.2 (Gen.2), 2* USB3.2 (Gen.1), 3* USB2.0 ports
- **MI225H610X series:** total support up to 2* USB3.2 (Gen.2), 2* USB3.2 (Gen.1), 5* USB2.0 ports
- **MI225Q670X/R680X series:** 4 * SATAIII (6Gb/s) ports with support for RAID 0, 1, 5, 10 mode & 2* M.2 (M-key) slots; 1* M.2 (E-key) & 1* M.2 (B-key) slot along with SIM card holder; 1* PCIE Gen.4 x16 slot
- **MI225H610X series:** 4 * SATAIII (6Gb/s) ports & 1* M.2 (M-key) slot; 1* M.2 (E-key) & 1* M.2 (B-key) slot along with SIM card holder; 1* PCIE Gen.4 x16 slot
- Support onboard TPM 2.0 **(*optional)**
- Support Smart FAN function
- Supports ACPI S3 Function
- Compliance with ErP Standard
- Support Watchdog Timer Technology

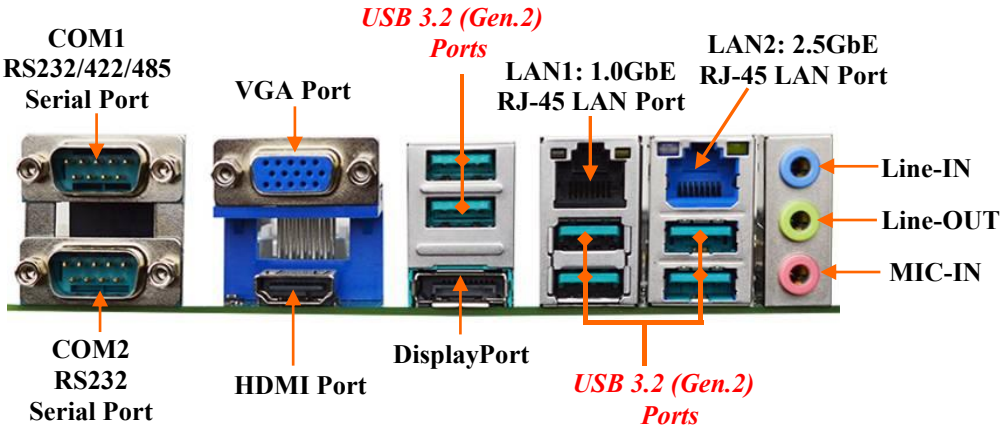
1-2 Specification

Spec	Description
Design	● Mini-ITX form factor; 10-layers; PCB size: 17.0x17.0cm
Chipset	● **MI225H610X Series**: Intel® H610E/H610 Chipset ● **MI225Q670X Series**: Intel® Q670E Chipset ● **MI225R680X Series**: Intel® R680E Chipset
CPU Socket	● Intel® LGA 1700 Socket supports 12th/13th Gen. Core™ i7/i5/i3 /Pentium™/Celeron™ processors (Max.**65W** TDPs under **180A**) **Note:* *for detailed CPU support information please visit our website.*
Memory Slot	● 2* DDR5 SO-DIMM slot ● Support 2* DDR5 4800MHz SO-DIMM up to 64GB ● Support dual channel function **Note:* ***MI225R680X*** *series support* ***ECC.***
Expansion Slot	● ***PCIE1:***1* PCIE Gen.4 x16 slot *(**PCIE1**)* ● ***M2E1:***1* M.2 E-key,type-2230 slot(USB2.0/PCIe Gen.3 x1 interface) supports CNVi ● ***M2B1:***1* M.2 B-key, type-3042 slot supports supports 4G Module *(**MI225Q670X/R680X series**: PCIe Gen.3 x1/USB3.2 Gen.2/USB2.0 interface; **MI225H610X series**: PCIe Gen.3 x1 interface **only**).* ● ***SIMCARDB1:***1* Nano-SIM card slot;co-function with **M2B1 slot**
Storage	● 4*SATAIII 6Gb/s port support **(*SATA1/2/3/4)** **Note:* ***MI225Q670X/R680X*** *series support* RAID 0/1/5/10 mode. ● ***M2M1:*** 1* M.2 M-key,type-2280 slot (PCIe Gen.3x4 interface) supports NVMe ● ****M2M2:***1* M.2 M-Key, type-2242 slot (PCIe Gen.4 x4/SATA interface) supports NVMe **Note:* ***M2M2*** *slot is only available to* ***MI225Q670X/R680X*** *series.*
Graphics	***Intel® UHD Graphics, shared memory for***: ● *1* DP 1.4a* ● *1* HDMI 2.0b* ● *1* VGA* ● *1* LVDS/eDP* ** Note:* ***MI225Q670X/R680X series*** support Quad Displays; ***MI225H610X series*** *support Triple Displays*
LAN Chips	***Integrated with:*** ● 1* Intel® **i225V 2.5GbE** PCI-E LAN chip of providing **10/100/1000/2500Mbps**

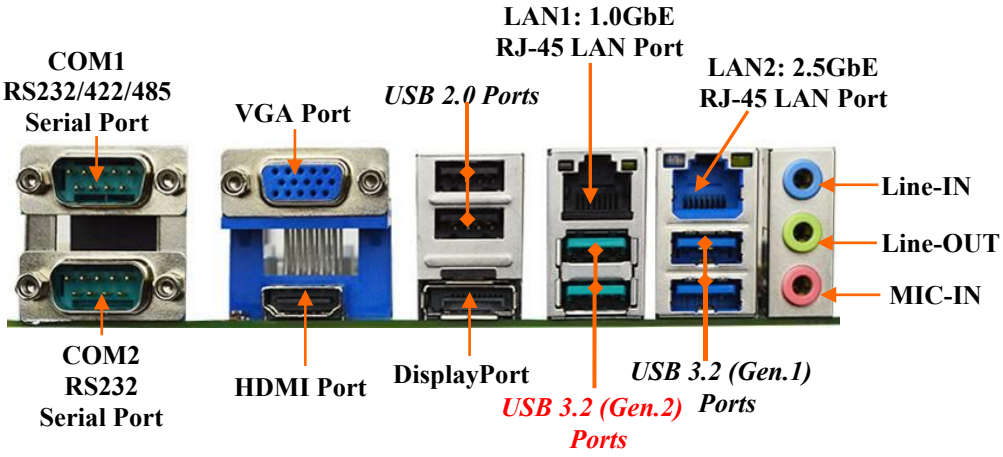
	Ethernet data transfer rate ***Note: 2500Mbps** high-speed transmission rate is **only** supported over **CAT 5e UTP cable**.* ● 1* Intel® **i219-LM** Gigabit PHY LAN chip of providing **10/100/1000Mbps** Ethernet data transfer rate ● Support Fast Ethernet LAN function
Audio Chip	● Realtek HD Audio Codec integrated ● Audio driver and utility included
BIOS	● AMI 256Mb Flash ROM
Multi I/O	***Rear Panel I/O:*** ● 2* COM port**(COM1_2; COM1: RS232/422/485 supports 5V/12V TTL)** ● 1* HDMI port, 1*VGA & 1* DP port ● ***MI225Q670X/R680X:*** 6* USB 3.2 Gen.2 port ● ***MI225H610X:*** 2* USB 3.2 Gen.2 port & 2* USB 3.2 Gen.1 port + 2* USB 2.0 port ● 1* 1.0GbE RJ-45 LAN port **(LAN1 from UL1)** ● 2.5GbE RJ-45 LAN port **(LAN2 from UL2)** ● 1* 3-jack audio connector (**Line-in, Line-out, MIC**) ***Internal I/O Connectors, Headers & Wafers:*** ● 1 *24-pin main power connector ● 1 *4-pin 12V power connector ● 1* CPUFAN1 connector & 1* SYSFAN1 connector ● 1* CMOS battery connector ● 1* Front panel header ● 1* Front panel audio header ● 1* HDMI_SPDIF header ● 4* RS232 COM port header *(**COM3/4/5/6**)* ● 1* 9-Pin USB 2.0 header for 2* USB 2.0 ports +1* 4-Pin USB 2.0 header for 1* USB 2.0 port ● ***MI225Q670X/R680X:***1*19-Pin USB 3.2 (Gen.1) header for 2* USB 3.2 (Gen.1) ports ● 1* GPIO header ● 1* PS2 Keyboard & Mouse header ● 1* SMBUS header ● 1* LVDS/EDP wafer ***(LVDS_EDP)*** & 1*Inverter wafer***(INVERTER1)***
TPM 2.0	● Optional for **MI225R6802, MI225Q6702** & **MI225H6102** Series
OS Support	● *for detailed OS support information please visit our website for latest update*

1-3 Layout Diagram

Rear IO Diagram
For MI225R680X/ MI225Q670X Series:

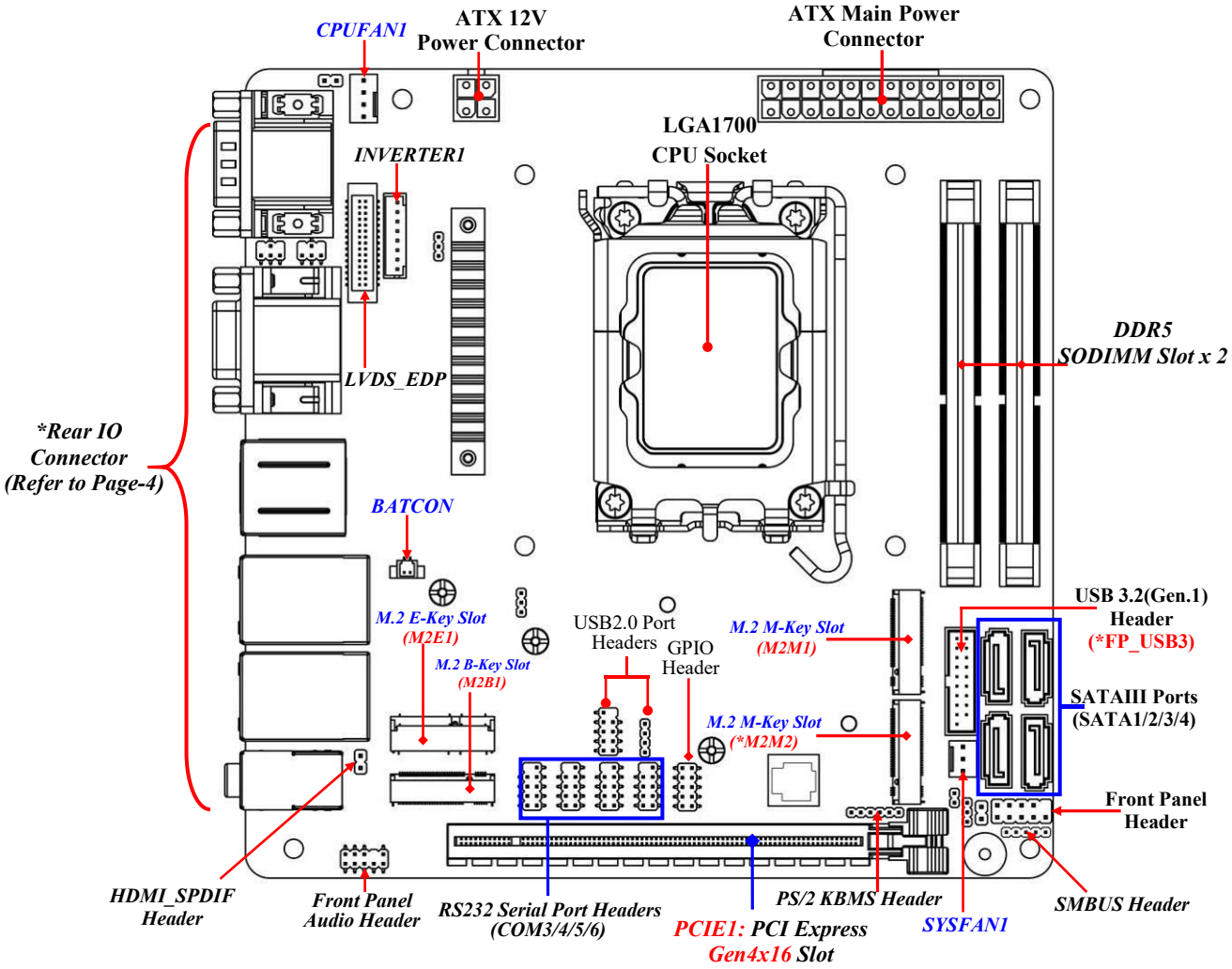


For MI225H610X Series:

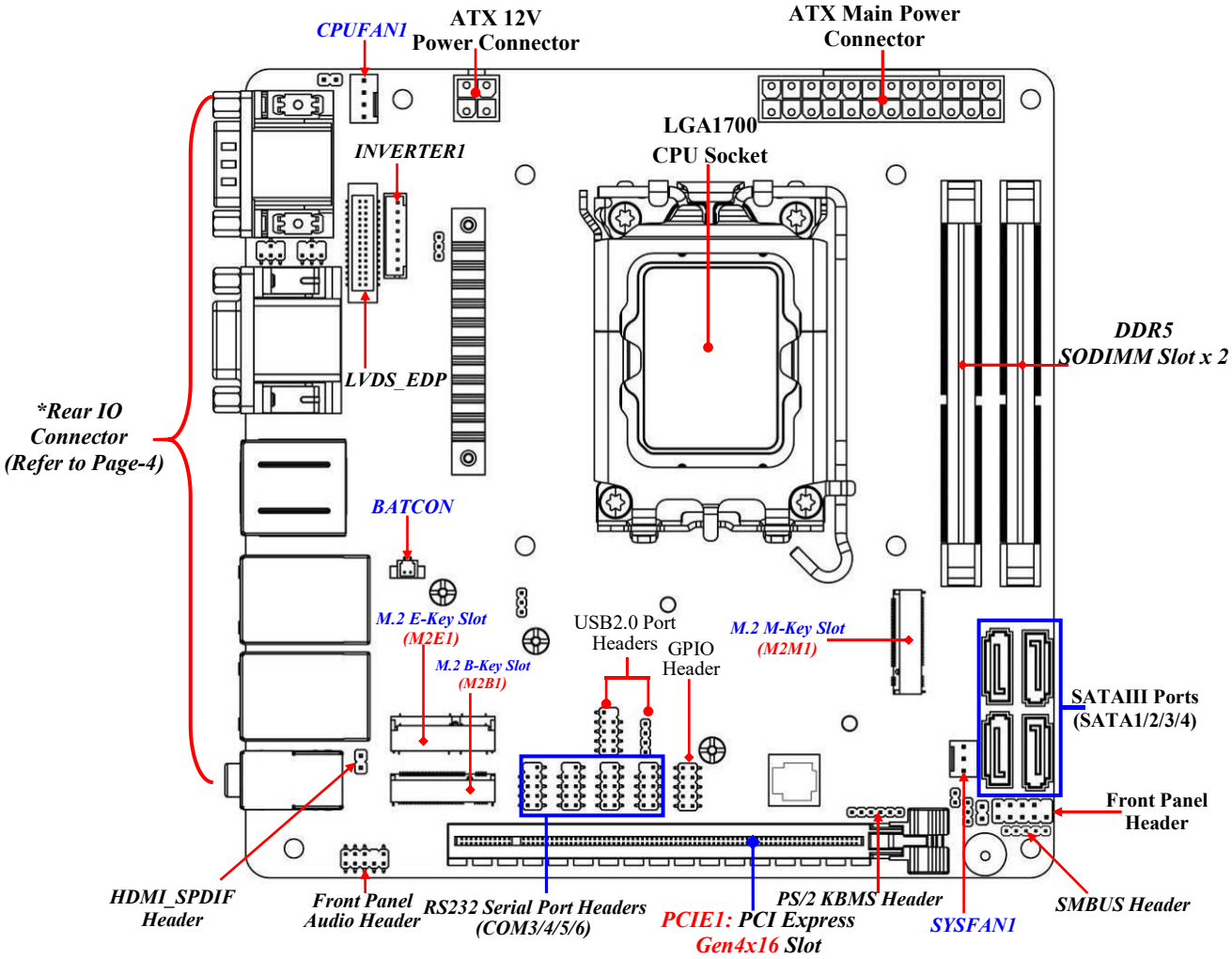


Motherboard Internal Diagram-Front

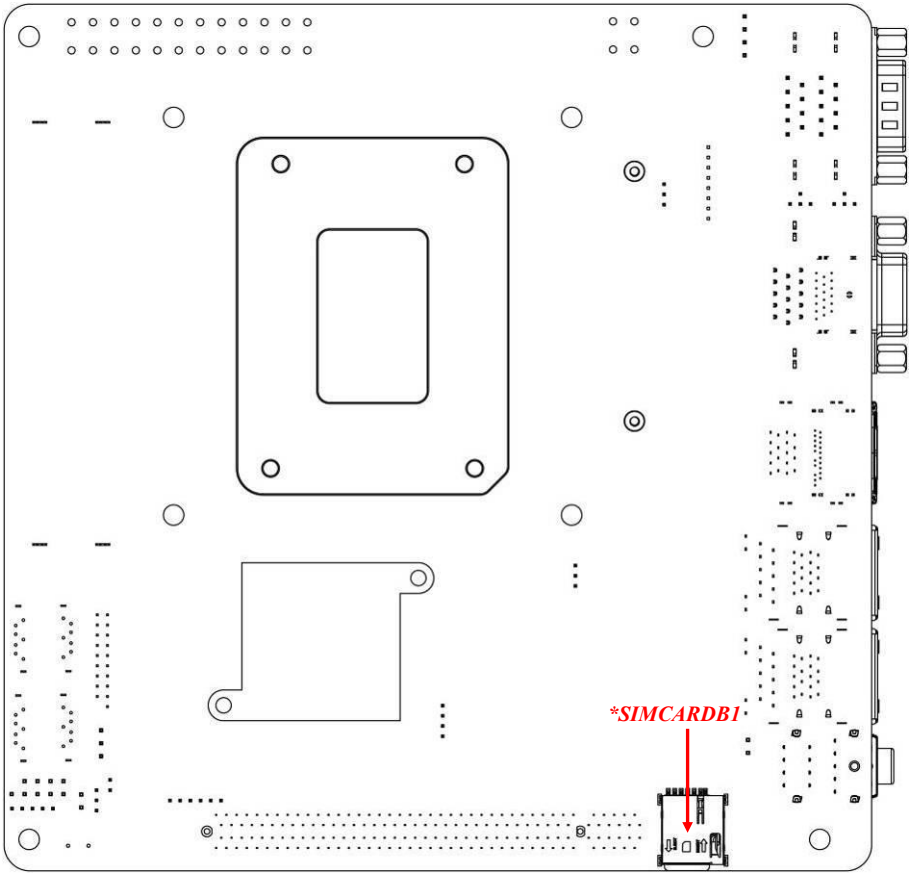
MI225Q670X/R680X Series:



MI225H610X Series:

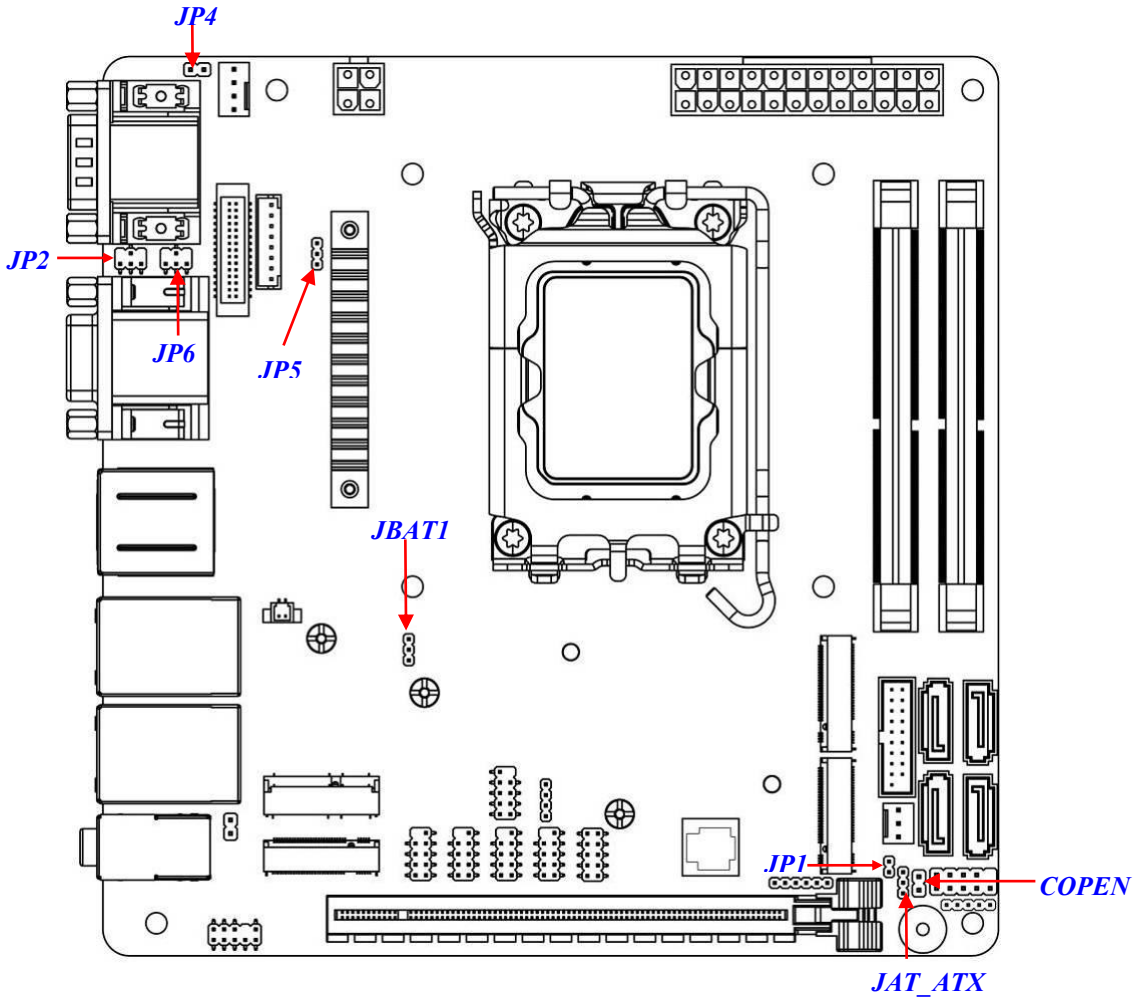


Motherboard Internal Diagram-Back



***Note:** **1.** SIM card slot only workable along with M.2 B-key slot; **2. M2M2** Slot & **FP_USB3** header are only available to **MI225Q670X/R680X series**).*

Motherboard Jumper Position



***Note:**The diagrams in the manual are mostly taken from **MI225Q670X/R680X** series for illustration purpose,unless otherwise stated.*

Jumper

P/N	Name	Description	Pitch
JBAT1	Clear CMOS RAM Settings	3-pin Block	2.0mm
JP1	Flash Descriptor Security Override	2-pin Block	2.0mm
JAT_ATX	ATX Mode / AT Mode Select	3-pin Block	2.0mm
COPEN	Case Open Message Display Function	2-pin Block	2.54mm
JP4	GPIO Header Function Select	2-pin Block	2.0mm
JP6	COM1 Port Pin9 Function Select	4-pin Block	2.0mm
JP2	LVDS_EDP PANEL VCC Select	4-pin Block	2.0mm
JP5	INVERTER1 Backlight VCC Select	3-pin Block	2.0mm

Connectors

P/N	Name
COM1_2	***Top(COM1):*** RS232/422/485 Serial Port ***Bottom(COM2):*** RS232 Serial Port
VGA	VGA Port
HDMI	HDMI Port
USB3	***MI225Q670X/R680X:*** ***Top & Middle:*** USB 3.2(Gen.2) Port X2 ***MI225H610X:*** ***Top & Middle:*** USB 2.0 Port X2
DP	***Bottom:*** DisplayPort
UL1	**Top:** 1.0 GbE RJ-45 LAN Port **Middle & Bottom**: USB 3.2 (Gen.2) Port X2
UL2	***MI225Q670X/R680X:*** **Top:** 2.5 GbE RJ-45 LAN Port **Middle & Bottom**: USB 3.2 (Gen.2) Port X2 ***MI225H610X:*** **Top:** 2.5 GbE RJ-45 LAN Port **Middle & Bottom**: USB 3.2 (Gen.1) Port X2
AUDIO	**Top:** Line-in Connector **Middle:** Line-out Connector **Bottom:** MIC Connector
ATXPWR1	24-Pin ATX Main Power Connector

ATX12V	Internal 12V Power Connector
SATA1/2/3/4	SATAIII Connector
CPUFAN1	CPU Fan Connector
SYSFAN1	System Fan Connector
BATCON	CMOS Battery Connector

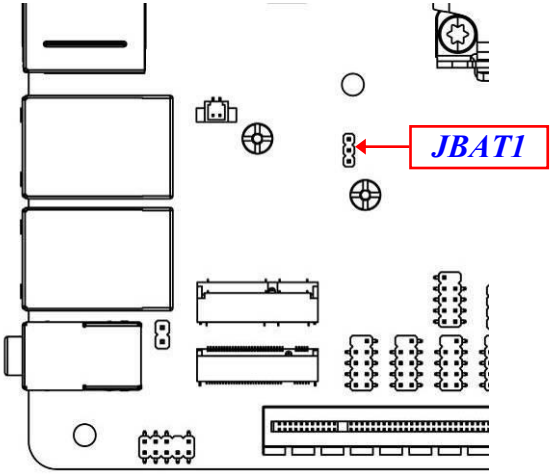
Headers & Wafers

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	2.0mm
HDMI_SPDIF	HDMI_SPDIF Header	2-pin Block	2.54mm
COM3/4/5/6	RS232 Serial Port Header	9-pin Block	2.0mm
FP_USB1/2	USB2.0 Port Header	9-pin Block	2.0mm
MI225Q670X/R680X: FP_USB3	USB 3.2 (Gen.1) Port Header	19-pin Block	2.0mm
GPIO	GPIO Port Header	10-pin Block	2.0mm
PS2KBMS	PS2 Keyboard & Mouse Header	6-pin Block	2.0mm
SMBUS1	SMBUS Header	5-pin Block	2.0mm
LVDS_EDP	*LVDS/EDP Wafer*	*30-pin Block*	*1.25mm*
INVERTER1	*Inverter Wafer*	*8-pin Block*	*2.0mm*

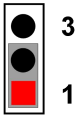
Chapter 2
Hardware Installation

2-1 Jumper Setting

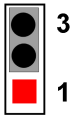
JBAT1 (3-pin): Clear CMOS RAM Settings



JBAT1→Clear CMOS Settings

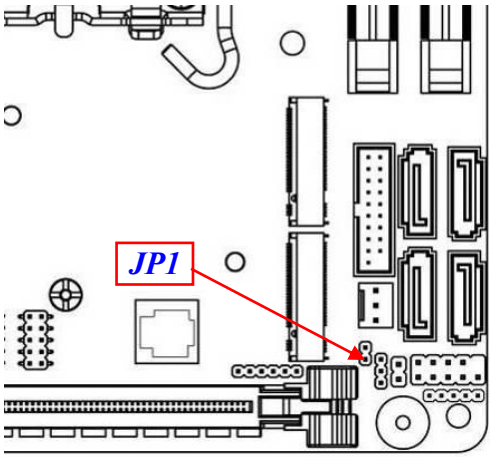


1-2 Closed: Normal(Default);

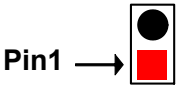


2-3 Closed: Clear CMOS.

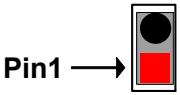
JP1 (2-pin): Flash Descriptor Security Override



JP1→ Flash Override

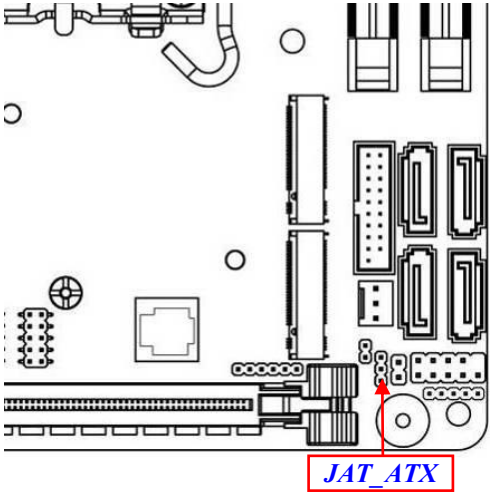


1-2 Open: Enable Security Measures in the Flash Descriptor(Default);

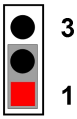


1-2 Closed: Disable Security Measures in the Flash Descriptor(Override).

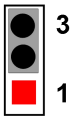
JAT_ATX (3-pin): AT Mode /ATX Mode Select



JAT_ATX→ATX/AT Mode Select



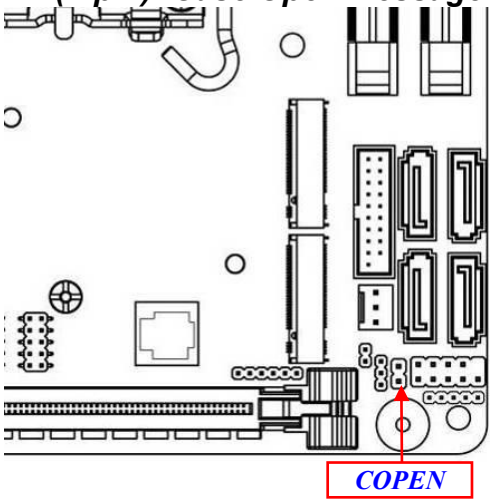
1-2 Closed: ATX Mode Selected;



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.*

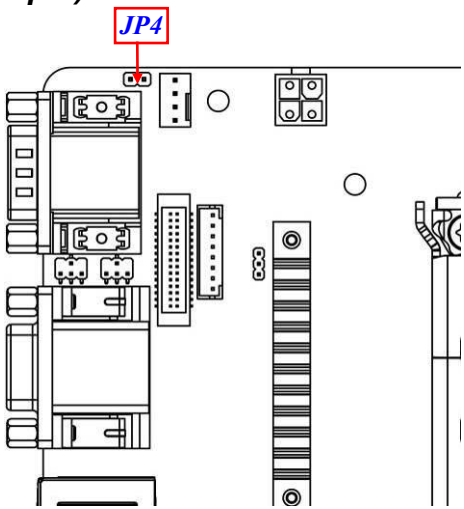
COPEN (2-pin): Case Open Message Display Function



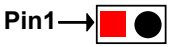
COPEN→ Case Open Detection

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.*

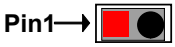
JP4(2-pin): GPIO Header Function Select



JP4→GPIO Function Select

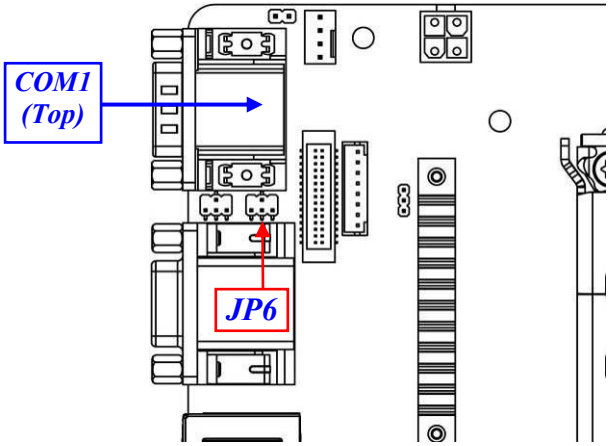


1-2 Open: Function as 80 Port;

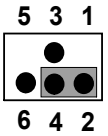


1-2 Closed: Function as GPIO Port.

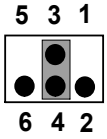
JP6(4-pin): COM1 Port Pin9 Function Select



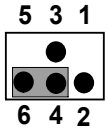
JP6→COM1 Port Pin-9



2-4 Closed: RI=RS232;

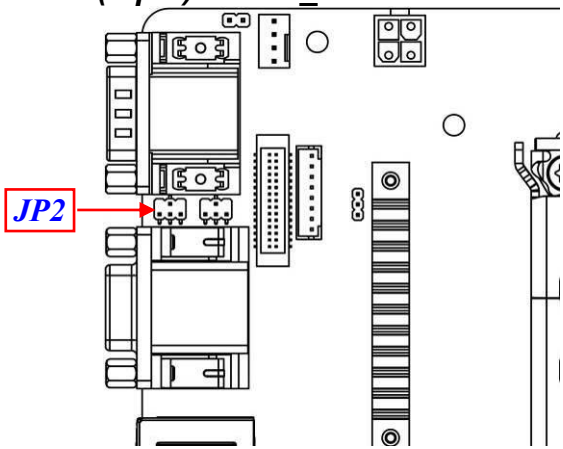


3-4 Closed: RI= 5V;

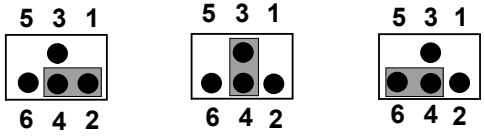


4-6 Closed: RI= 12V.

JP2 (4-pin): LVDS_EDP Power VCC Select



JP2→LVDS_EDP Power VCC Select



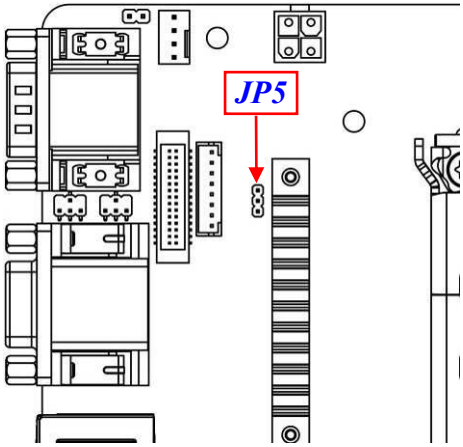
2-4 Closed: VCC=3.3V;

3-4 Closed: VCC=5V;

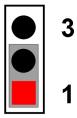
4-6 Closed: VCC= 12V.

***Warning!** Wrong voltage setting will result in screen burn out.*

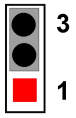
JP5(3-pin):INVERTER1 Backlight VCC Select



JP5→INVERTER1 Backlight VCC Select



1-2 Closed: VCC=5V;



2-3 Closed: VCC=12V.

***Warning!** Wrong voltage setting will result in screen burn out.*

2-2 Connectors, Headers & Wafers
2-2-1 Rear I/O Back Panel Connectors

Refer to Page-4 Rear IO Diagram

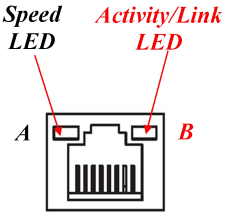
Icon	*Name*	*Function*
	**Serial Port**	Mainly for user to connect external MODEM or other devices that supports Serial Communications Interface. ***Note: COM1 (Top) supports RS232/422/485 function.**
	**VGA Port**	To connect display device that support VGA specification.
	**HDMI Port**	To connect display device that support HDMI specification.
	**Display Port**	To the system to corresponding display device with compatible DP cable.
	**1.0Gbps RJ-45 LAN Port**	This connector is standard RJ-45 LAN jack for Network connection which supports10/100/1000Mbps Ethernet data transfer rate.
	**2.5Gbps RJ-45 LAN Port**	This connector is standard RJ-45 LAN jack for Network connection which supports10/100/1000/2500 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.

	**USB 3.2 (Gen.1) Port**	To connect USB keyboard, mouse or other devices compatible with USB 3.2 (Gen.1) specification.
	**USB 2.0 Port**	To connect USB keyboard, mouse or other devices compatible with USB 2.0 specification.
	**Audio Connectors**	**Blue:** Line-in Connector **Green:** Line-out Connector **Pink:** MIC Connector

(1) RJ-45 Ethernet Connectors

*** There are two LED next to the RJ-45 LAN port. Please refer to the table below for LAN port LED indications.*

For UL1 (I219-LM) 1.0Gbps RJ-45 LAN port LED Signals:



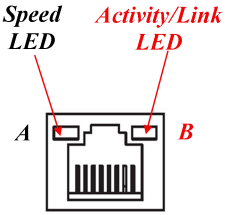
A: Speed LED

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 UL2 (I225-V) 2.5Gbps RJ-45 LAN port LED Signals:



A: Speed LED

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

B: Activity/Link LED

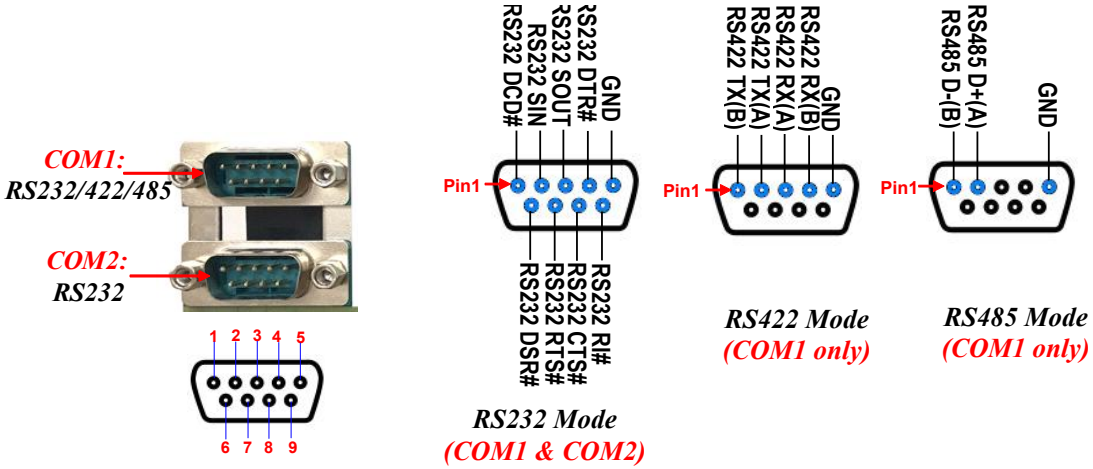
Status	Description
Off	No Link
Blinking	Data Activity
On	Link

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

(2) COM1_2 (9-pin Block): COM1 & COM2 Serial Port

***COM1**: RS232/422/485 Serial Port; **COM2:** RS232 Serial Port.*

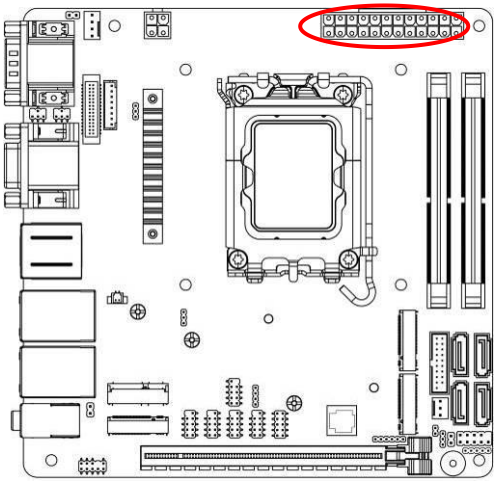
The pin assignment for RS-232/ 422/ 485 is listed as follows:

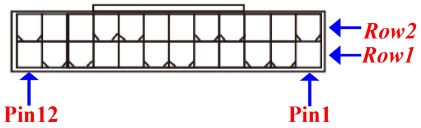


COM1 port can function as RS232/422/485 port. In normal settings COM1 functions as RS232 port. With compatible COM cable COM1 can function as RS422 or RS 485 port. User also needs to go to BIOS to set **'Transmission Mode Select'** for COM1 at first, before using specialized cable to connect different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

2-2-2 Motherboard Internal Connectors

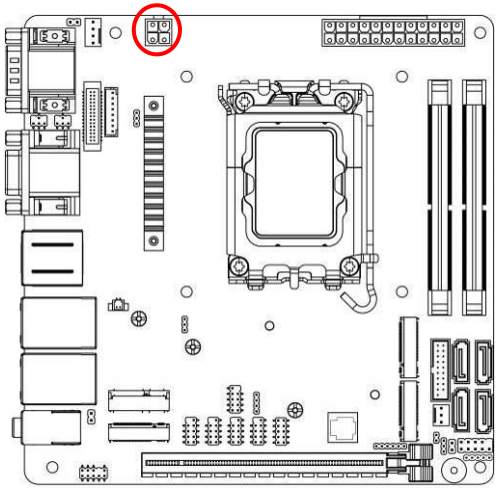
(1) ATXPWR(24-pin block): Main Power Connector

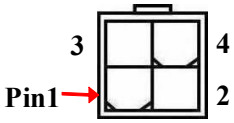




PIN	ROW1	ROW2
1	+3.3V	+3.3V
2	+3.3V	-12V
3	GND	GND
4	+5V	Soft Power on
5	GND	GND
6	+5V	GND
7	GND	GND
8	Power OK	-5V
9	+5V Stand by	+5V
10	+12V	+5V
11	+12V	+5V
12	+3.3V	GND

(2) ATX12V (4-pin block): 12V Internal Power Connector

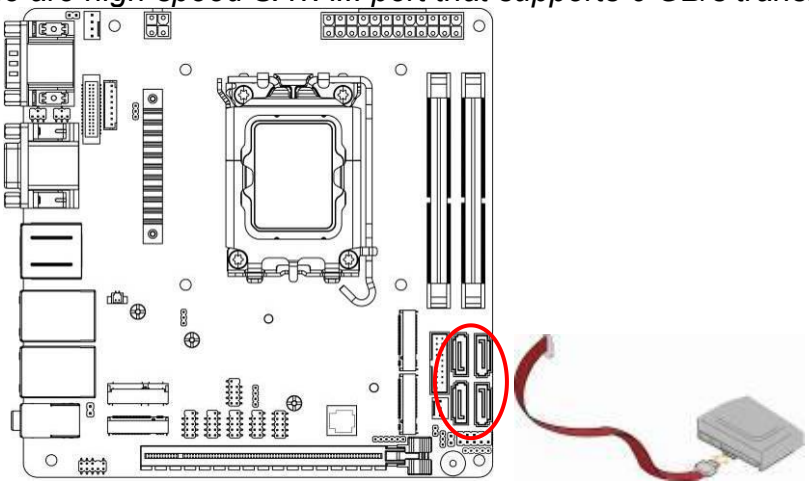




Pin No.	Definition
1	GND
2	GND
3	+12V
4	+12V

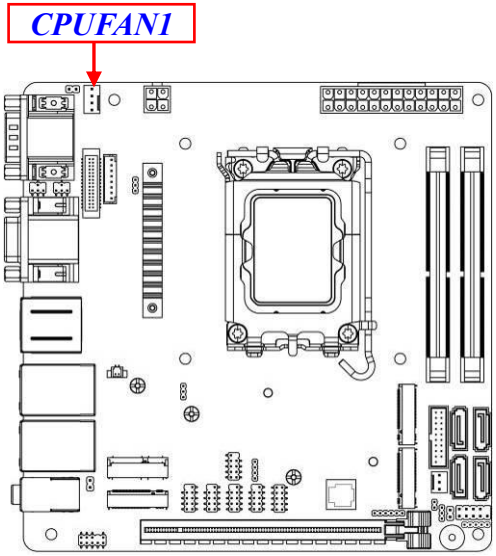
(3) SATA1/2/3/4 (7-pin): SATA III Port connector

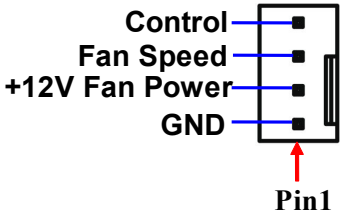
These are high-speed SATAIII port that supports 6 GB/s transfer rate.



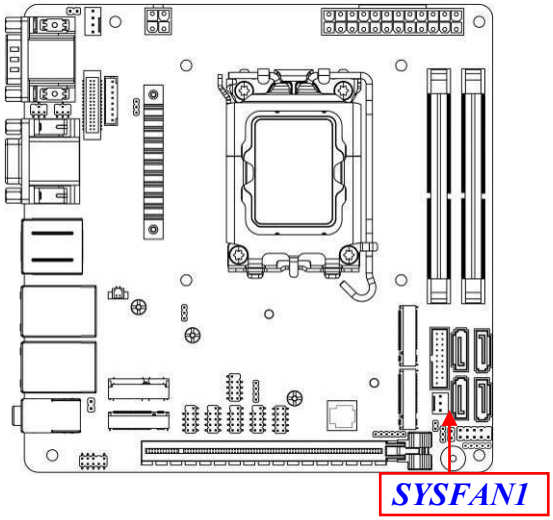
Pin No.	Defnition
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND

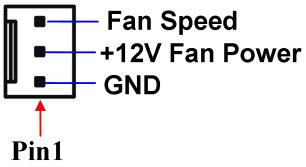
(4) CPUFAN1 (4-pin): CPU FAN Connector



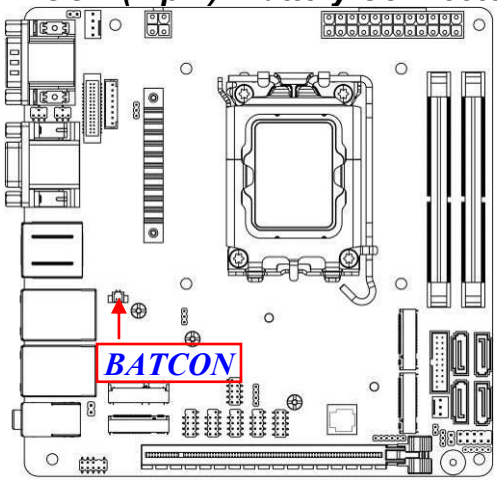


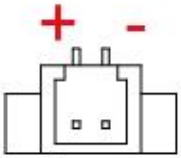
(5) SYSFAN1 (3-pin): System FAN Connector





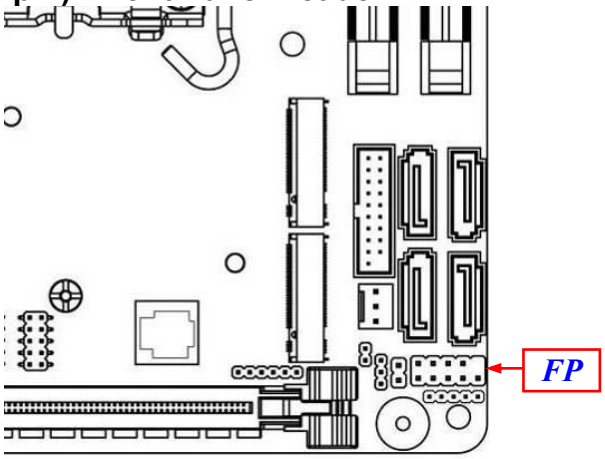
(6) BATCON (2-pin): Battery Connector

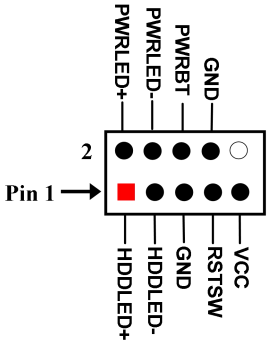




2-2-3 Pin Definition for Headers & Wafers

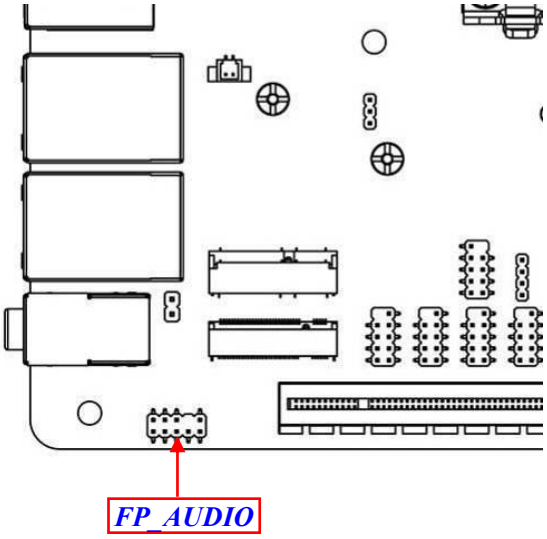
FP (9-pin): Front Panel Header

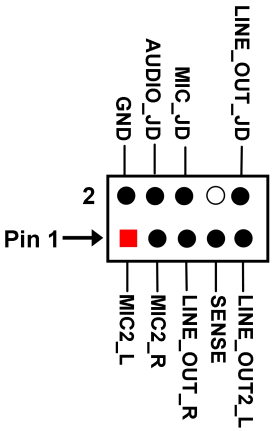




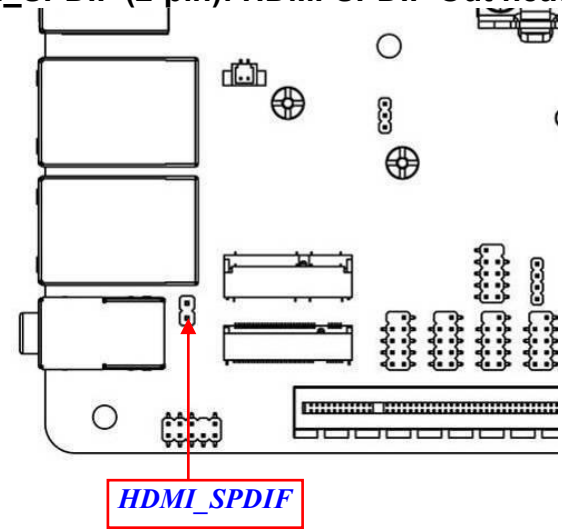
FP_AUDIO (9-pin): Line-Out, MIC-In Header

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

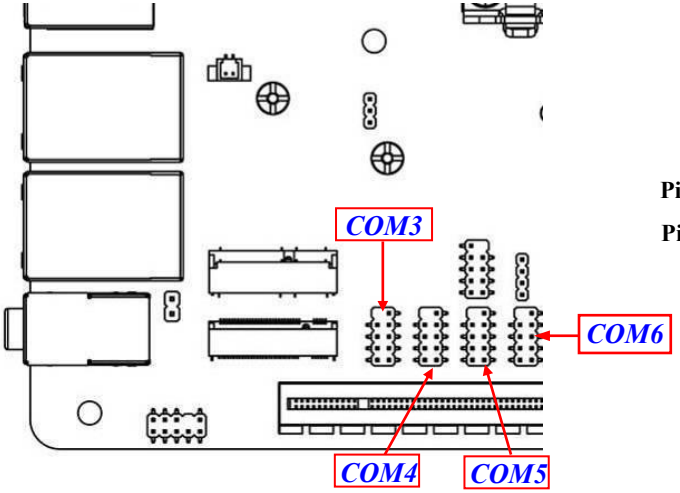


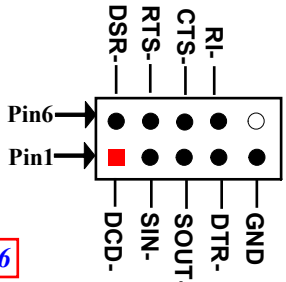


HDMI_SPDIF (2-pin): HDMI-SPDIF Out header

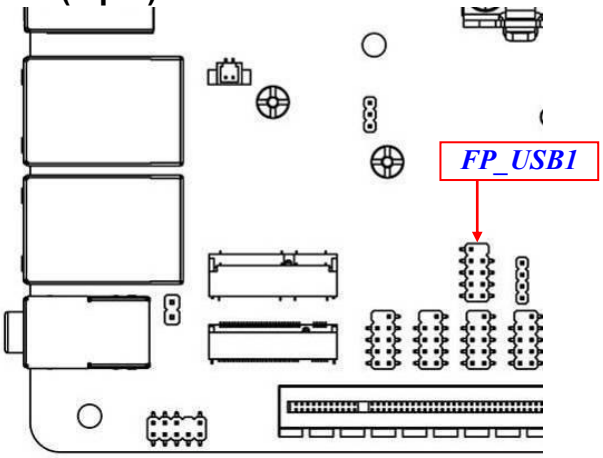


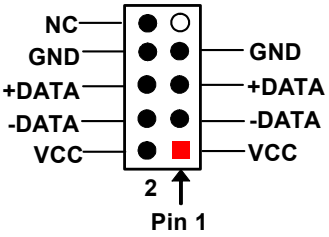
COM3/4/5/6 (9-pin): RS232 Serial Port Header



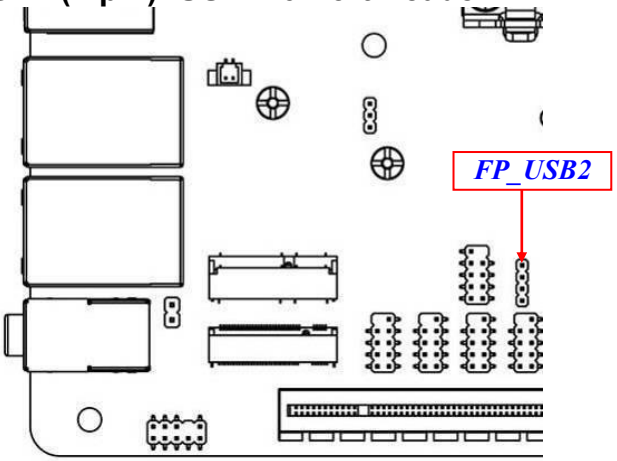


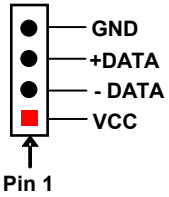
FP_USB1 (9-pin): USB 2.0 Port Header



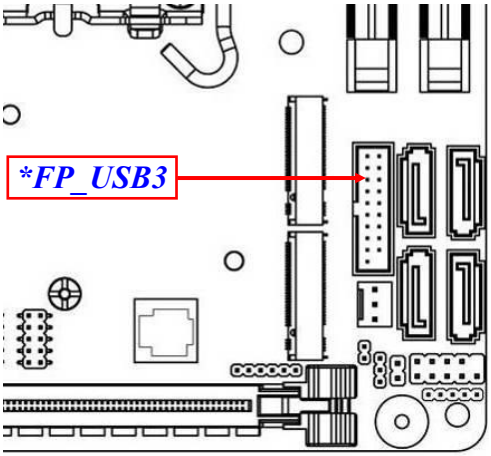


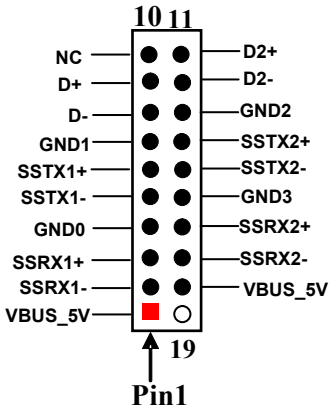
FP_USB2 (4-pin): USB 2.0 Port Header





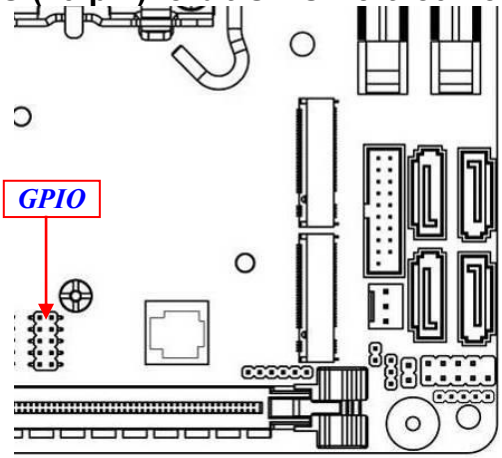
***FP_USB3 (19-pin): USB 3.2(Gen.1) Port Header**

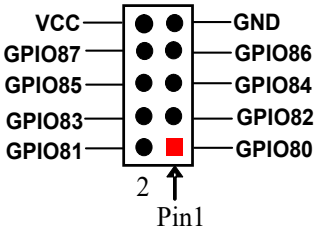




***Note:FP_USB3** is only optional to **MI225Q670X/R680X** series.*

GPIO (10-pin): 8-bit GPIO Port /80 Port Header

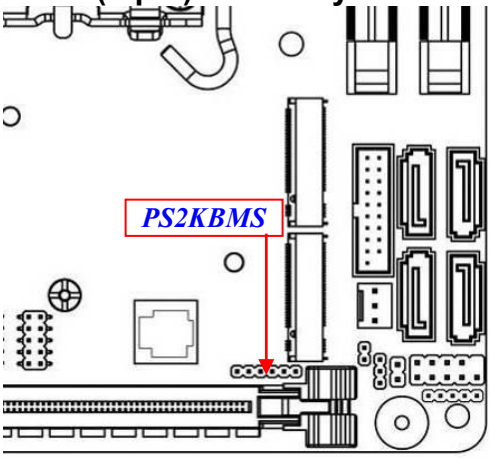


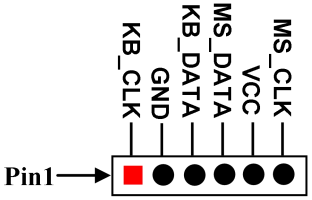


JP4 Open: For 80Port Function;
JP4 Closed: Normal 8-bit GPIO.

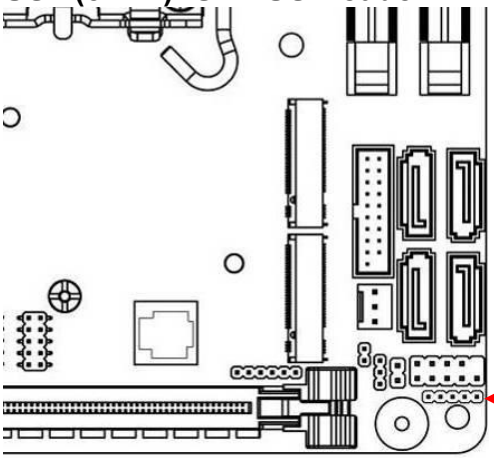
***Note:** **GPIO** can function as Debug display port or GPIO port via **JP4** jumper setting (refer to **Page-13** for JP4 description).*

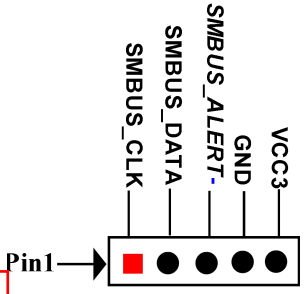
PS2KBMS (6-pin): PS/2 Keyboard & Mouse Header



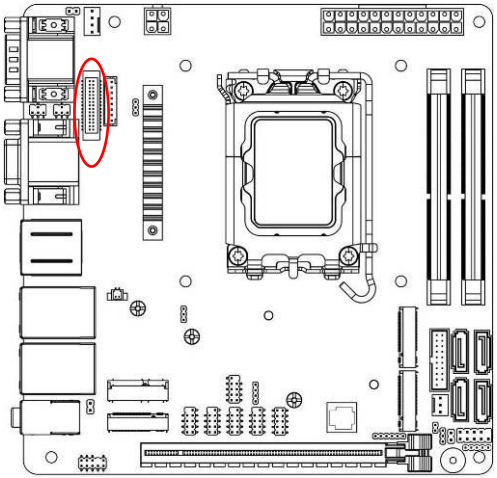


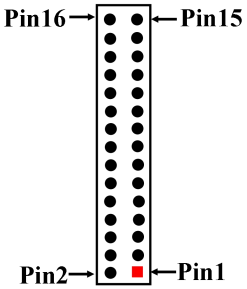
SMBUS1 (5-Pin): SMBUS Header





LVDS_EDP (30-Pin): LVDS/EDP LCD Panel Wafer



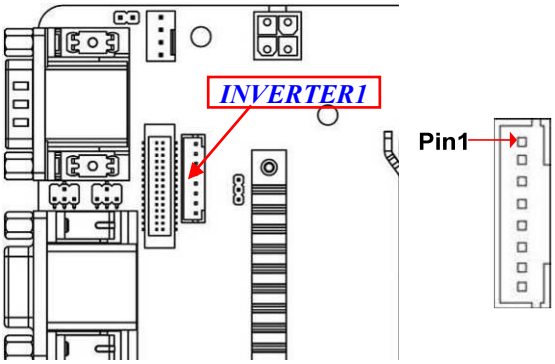


Pin Define	Pin NO.	Pin NO.	Pin Define
LCD_VCC	Pin 30	Pin 29	LCD_VCC
LCD_VCC	Pin 28	Pin 27	LCD_VCC
LVDSA_DATAN0	Pin 26	Pin 25	LVDSA_DATAP0
LVDSA_DATAN1_eDP_TX1N	Pin 24	Pin 23	LVDSA_DATAP1_eDP_TX1P
LVDSA_DATAN2_eDP_TX0N	Pin 22	Pin 21	LVDSA_DATAP2_eDP_TX0P
LVDS_CLKAN_eDP_AUXN	Pin 20	Pin 19	LVDS_CLKAP_eDP_AUXP
LVDSA_DATAN3	Pin 18	Pin 17	LVDSA_DATAP3
GND	Pin 16	Pin 15	GND
GND	Pin 14	Pin 13	GND
LVDS_DDC_SCL	Pin 12	Pin 11	LVDS_DDC_SDA
LVDSB_DATAP0	Pin 10	Pin 9	LVDSB_DATAN0
LVDSB_DATAP1	Pin 8	Pin 7	LVDSB_DATAN1
LVDSB_DATAP2	Pin 6	Pin 5	LVDSB_DATAN2
LVDS_CLKBP	Pin 4	Pin 3	LVDS_CLKBN
LVDSB_DATAP3	Pin 2	Pin 1	LVDSB_DATAN3

***Note:** 1.Maximum current limit is **2A** while using **5V/12V** backlight power working voltage (refer to **P-10 JPLVDS settings**);2.Maximum current limit is **2A** while using **3.3V/5V/12V LCD_VCC** working voltage (refer to **P-10 JP2 settings**).*

***Warning!** Wrong voltage setting will result in screen burn out.*

INVERTER1 (8-pin): LVDS/eDP Inverter Connector



Pin No.	Definition
1	Backlight Enable
2	Backlight PWM
3	PVCC
4	PVCC
5	GND
6	GND
7	Backlight Up SW
8	Backlight Down SW

Warning! *Find Pin-1 location of the inverter and make sure that the installation direction is correct! Otherwise serious harm will occur to the board/display panel!!*

2-3 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	***USB3***	5V	2A
	UL1	5V	2A
	UL2	5V	2A
	FP_USB1	5V	1.5A
	FP_USB2	5V	1.5A
	****FP_USB3***	5V	1.5A
COM1(JP6)		5V/12V	0.5A
FP		5V	1A
GPIO		5V	1A
PS2KBMS		5V	0.5A
SMBUS1		5V	0.5A
LVDS_EDP(JP2)		3.3V/5V/12V(via jumper setting)	**2A**
INVERTER1 (JP5)		5V/12V(via jumper setting)	**2A**
CPUFAN1/ SYSFAN1		12V	1.5A

****Note:FP_USB3** is only optional to **MI225Q670X/R680X** series.*

Chapter 3
Introducing BIOS

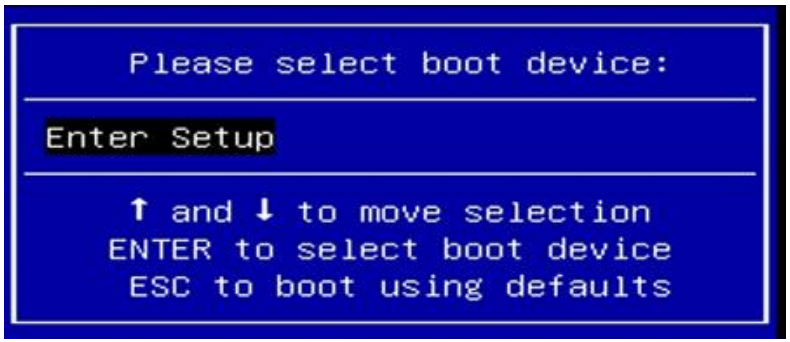
Notice!	The BIOS options in this manual are for reference only. Different configurations may lead to difference in BIOS screen and BIOS screens in manuals are usually the first BIOS version when the board is released and may be different from your purchased motherboard. Users are welcome to download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

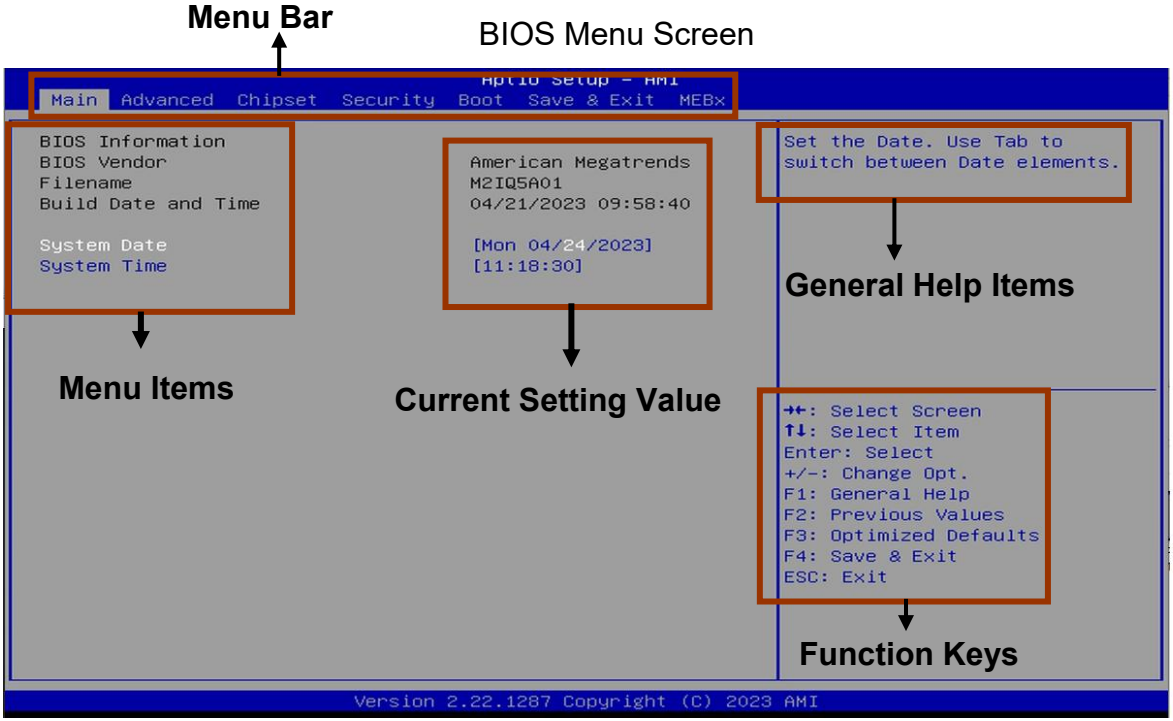
Power on the computer and by pressing <Del> immediately allows you to enter Setup.
If the message disappears before your respond and you still wish to enter Setup, restart the system to try again by turning it OFF then ON or pressing the “RESET” button on the system case. You may also restart by simultaneously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

Press **<Del>** to enter Setup



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 value.
- **[F3]:** Optimized defaults.
- **[F4]:** Save & Reset.
- 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

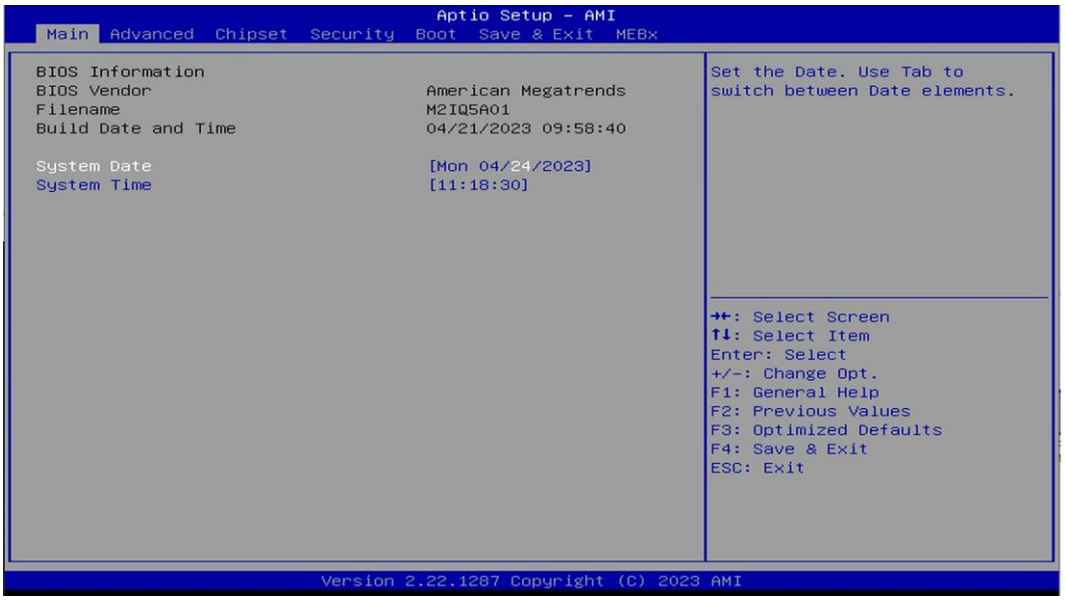
There are six menu bars on top of BIOS screen:

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.

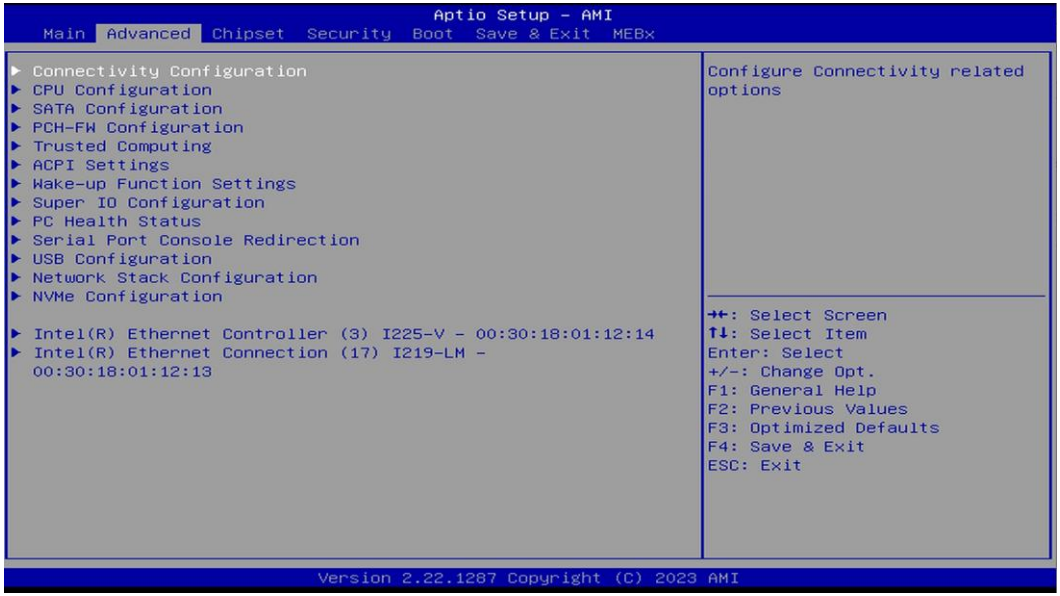
3-6 Main Menu

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**
  Press [Enter] to make settings for the following sub-item:
  CNVi Mode
  This 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
  The optional settings are: [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 enabled, a VHM can utilize the additional hardware capabilities provided by Vanderpool Technology.

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

  Intel (R) SpeedStep ™

  Use this item to Allows more than two frequency ranges to be supported.

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

  C states

  Use this item to enable/disable CPU Power management. 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/disable processor turbo mode (requires EMTTM enabled too). AUTO means enabled.

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

- **SATA Configuration**

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

  SATA Controller(s)

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

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

  M.2

  Port

  Use this item to enable or disable SATA Port

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

  SATA1/2/3/4

  Port

  Use this item to enable or disable SATA Port

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

Hot Plug

Use this item to designates this port as Hot Pluggable.

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

- **PCH-FW Configuration**

  Use this item to configure Management engine technology parameters

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

  TPM Device Selection

  Use this item to selects 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 are: [dTPM]; [PTT].

  I219 Lan MAC address Override

  Use this item to enable for override MAC Address

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

- **Firmware Update Configuration**

  Use this item to configure management engine technology parameters.

  Me FW Image Re-Flash

  Use this item to enable/disable Me FW Image Re-Flash function

  The optional settings: [Disabled]; [Enabled]

- **Trusted Computing**

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

  Security Device Support

  Use this item to enables or disables 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 settings in the following items that appear:

  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].

  TPM Device Selection

  Use this item to selects 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].

- **ACPI Settings**

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

ACPI Settings

ACPI Sleep State

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

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

► **Wake-up Function Settings**

Wake-up System With Fixed Time

Use this item to enable or disable system wake on alarm event. When enabled, system will wake on the hr: min: sec specified

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

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

This item will only show when* *'Wake-up System With Fixed Time'*** *is set as [Disabled].*

Use this item to enable or disable system wake on alarm event. When enabled, system will wake on the current time + Increase minute(s)

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

Wake-up Minute Increase

Use this item to select 1-60

PS2 KB/MS Wake-up

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

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

PCIE Wake-up from S3-S5

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

USB S3/S4 Wake-up

Use this item to enable or disable USB S3/S4 Wake-up Support only disable ERP function

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

USB S5 Power

Use this item to USB Power after system shutdown support only disable ERP function

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

- **Super IO Configuration**

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

Super IO Configuration

ERP Support

Use this item to energy-related products function. Disable ERP to active all wake-up functions.

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].

Change Settings

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

The optional settings are: [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 RS232/RS422/RS485 Speed Select

The optional settings are: [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].
  Change Settings
  Use this item to select an optimal setting for super IO device.
  The optional settings are: [IO=2F8h; IRQ=3]; [IO=3F8h; IRQ=3,4,5,7,10,11]; [IO=2F8h; IRQ=3,4,5,7,10,11]; [IO=3E8h; IRQ=3,4,5,7,10,11]; [IO=2E8h; IRQ=3,4,5,7,10,11];
- **Serial Port 3 Configuration**
  Press [Enter] to make settings for the following items:
  Serial Port
  Use this item to enable or disable serial port (COM).
  The optional settings: [Disabled]; [Enabled].
  Change Settings
  Use this item to select an optimal setting for super IO device.
  The optional settings are: [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].
  Change Settings
  Use this item to select an optimal setting for super IO device.
  The optional settings are: [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].
Change Settings
Use this item to select an optimal setting for super IO device.
The optional settings are: [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].
Change Settings
Use this item to select an optimal setting for super IO device.
The optional settings are: [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], the following sub-items shall appear:

WatchDog Reset Timer Value
User can set a value in the range of [4] to [255].

WatchDog Reset Timer Unit
The optional settings are: [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 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 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**

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

COM1

Console Redirection
Use this item to Console Redirection enable or disable.
The optional settings: [Disabled]; [Enabled].
When set as **[Enabled**], user can make further settings in the '**Console Redirection**

Settings' screen:

- **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：

Terminal Type

The optional settings: [VT100]; [VT100Plus]; [VT-UTF8]; [ANSI].

[ANSI]: Extended ASCII char set;

[VT100]: ASCII char set;

[VT100Plus]: 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 Function Key and KeyPad on Putty.
The optional settings: [VT100]; [LINUX]; [XTERMR6]; [SCO]; [ESCN]; [VT400].

- **Legacy Console Redirection Settings**

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

  Redirection COM Port

  Use this item to select a COM port to display redirection of Legacy OS and Legacy OPROM Messages
  The optional settings: [COM1]

  Resolution

  Use this item to on legacy OS, the number of rows and columns supported redirection
  The optional settings: [80x24]; [80x25]

  Redirect After POST

  When bootloader is selected, then legacy console redirection is disabled before booting to legacy OS. When always enable is selected, the legacy console redirection is enabled for legacy OS. Default setting for this option is set to always enable.

The optional settings: [Always Enable]; [BootLoader]

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

Console Redirection EMS

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

When set as **[Enabled]**, user can make further settings in '**Console Redirection Settings**' screen:

- **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.

Terminal Type EMS

The optional settings: [VT100]; [VT100Plus]; [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

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

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

Flow Control

Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

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

Data Bits 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

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].

Port 60/64 Emulation

Use this item to enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes

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

USB hardware delay and time-out

USB Transfer time-out

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

The optional settings: [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

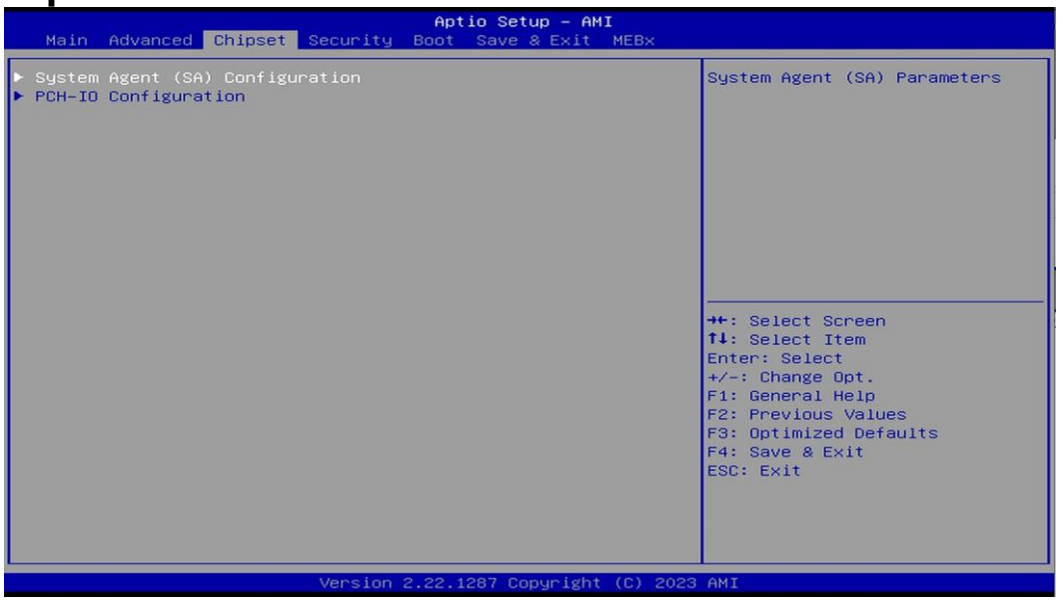
Use this item to set maximum time the device will take before it properly reports itself to the host controller. 'Auto' uses default value: for a root port it is 100 ms, for a hub port the delay is taken from hub descriptor.

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 PXE boot option will not be created.
  The optional settings: [Disabled]; [Enabled].
  Ipv6 PXE Support
  Use this item to enable IPv6 PXE Boot Support. When set as [Disabled], IPv6 PXE boot option will not be created.
  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.
  Media detect count
  Use this item to set number of times presence of media will be checked.
- **NVMe Configuration**
  Use this item to NVMe Device options settings
- **Intel(R) Ethernet Controller(3) I225-V - XX:XX:XX:XX:XX:XX**
  This item shows current network brief information.
- **Intel(R) Ethernet Connection(17) 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:
- **Memory Configuration**
  Maximum Memory Frequency
  Use this item to maximum memory frequency selections in Mhz
  The optional settings are: [Auto]; [4000]; [4400]; [4800]; [5000]; [5200]; [5400]; [5600]
- **Graphics Configuration**
  Press [Enter] to make settings for the following sub-items:
  PCIE1 Slot
  Use this item to control the PCI Express root port
  The optional settings: [Disabled]; [Enabled].
  PCIE Slot Lane Select
  The optional settings: [X16]; [X8/X8].
  eDP /LVDS
  Use this item to select the active configuration

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

Panel Type

The optional settings: [800x480 18bit Single]; [800x600 18bit Single]; [800x600 24bit Single]; [1024x600 18bit Single]; [1024x768 18bit Single]; [1024x768 24bit Single]; [1280x800 18bit Single]; [1280x800 24bit Single]; [1366x768 18bit Single]; [1366x768 24bit Single]; [1440x900 18bit Dual]; [1440x900 24bit Dual]; [1280x1024 24bit Dual]; [1680x1050 24bit Dual]; [19200x1080 24bit Dual]; [eDP].

Backlight Control

Use this item to back light control setting

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

Primary Display

Use this item to select which graphics device should be primary display

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

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]

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]; [128M]

DVMT Total Gfx Mem

Use this item to select DVMT 5.0 total graphic memory size used by the internal graphics device

The optional settings: [128M]; [256M]; [Max]

- **VMD setup menu**

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

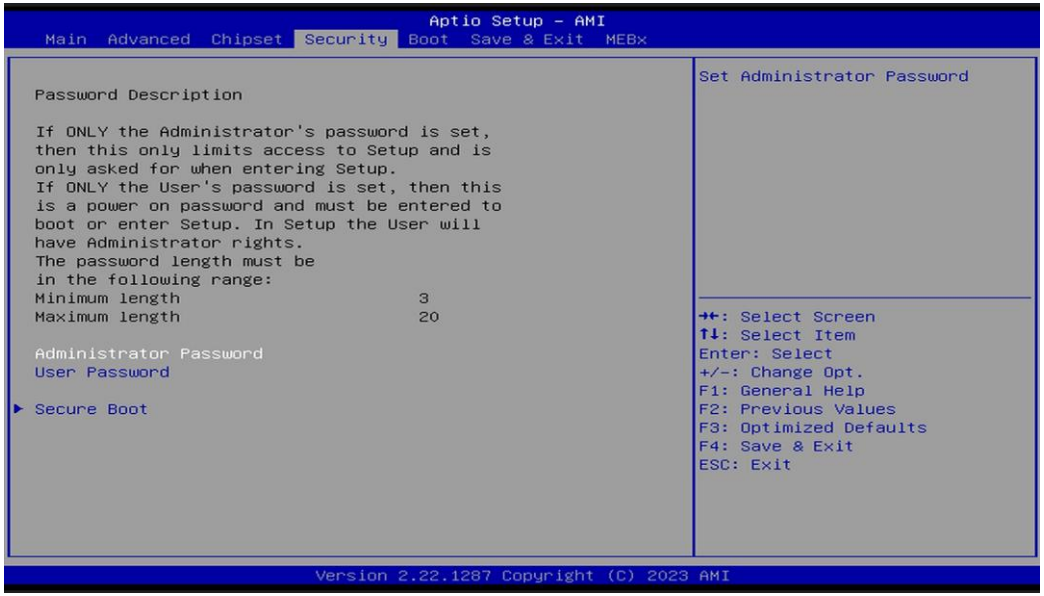
  Enable VMD controller

Use this item to enable/disable to VMD controller
The optional settings: [Disabled]; [Enabled].
When set as [Enabled], the following sub-items shall appear:
Enable VMD Global Mapping
Use this item to enable/disable to VMD global mapping
The optional settings: [Disabled]; [Enabled].
When set as [Disabled], the following sub-items shall appear:
Map this Root Port under VMD
Use this item to Map/UnMap this root port to VMD
The optional settings: [Disabled]; [Enabled].
Root Port BDF details

- **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.
Disabled= HAD will be unconditionally disabled
Enabled= HAD will be unconditionally enabled
The optional settings: [Disabled]; [Enabled].
Onboard Lan1 Controller
Use this item to enable or disable onboard NIC.
The optional settings: [Enabled]; [Disabled].
Wake on LAN Enable
Use this item to enable/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].
System State after Power Failure
Use this item to specify what state to go to when power re-applied after a power failure (G3 state).
The optional settings: [Always Off]; [Always On]; [Former State].

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:

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: [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).

- **Export Secure Boot variables**

Use this item to save NVRAM content of secure boot variable to a file.

Secure Boot variable/Size/Keys/Key Source

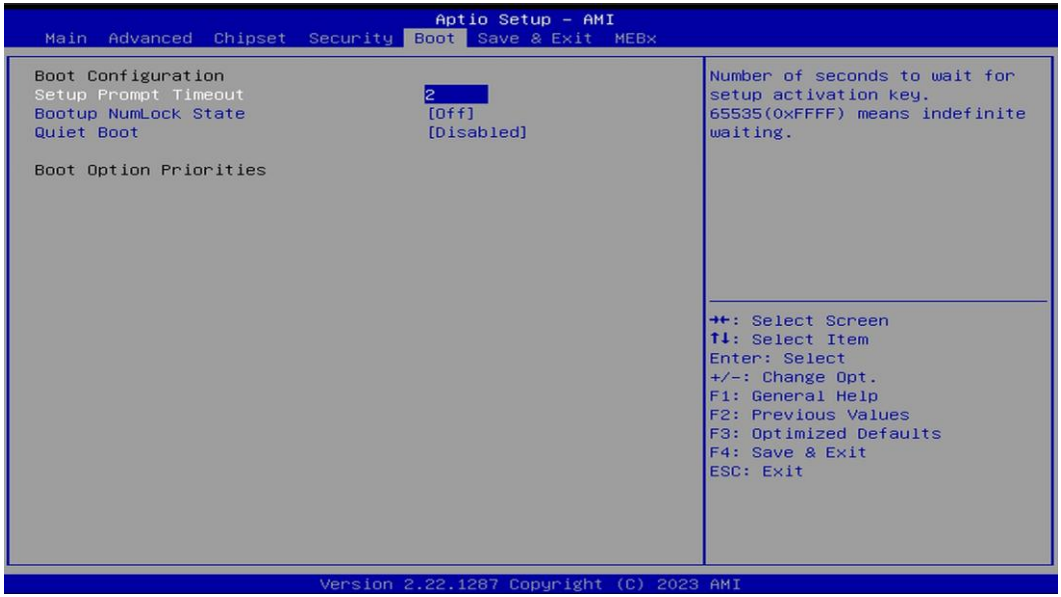
- **Platform Key(PK)/Key Exchange Keys/Authorized Signatures/Forbidden Signatures/ Authorized TimeStamps/OsRecovery Signatures**

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

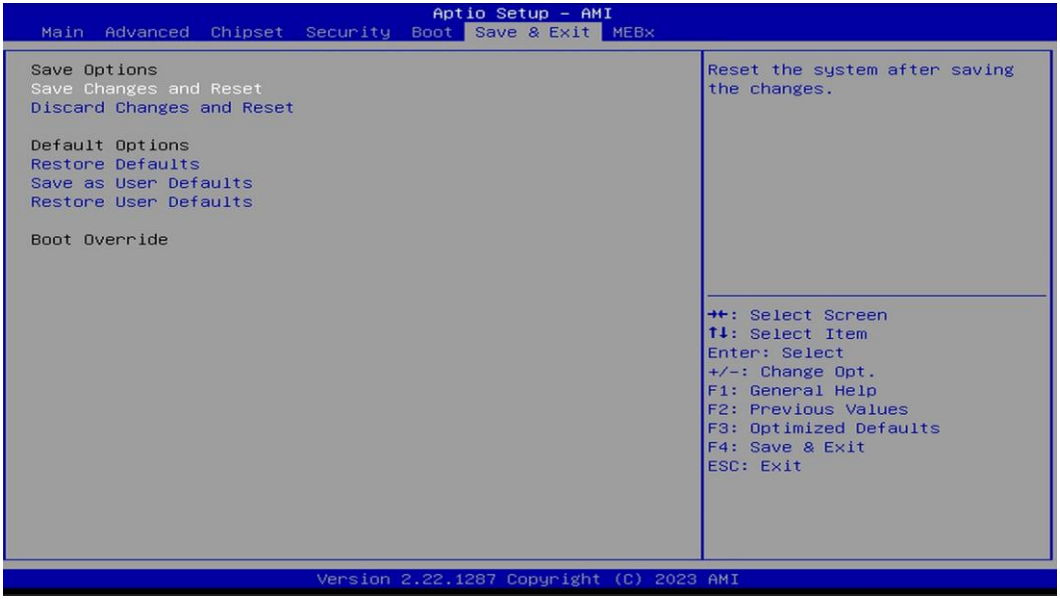


Boot Configuration

- **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].
  When set as [Enabled], user can make settings in the following items that appear:

Boot Option Priorities

3-11 Save & Exit Menu



- **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.
- **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

3-12 MEBx

- **Intel(R) ME Password**
  Use this item to MEBx Login.