

MF05 Series

User's Manual

NO.: G03-MF05-F

Revision: 4.0

Release date: August 2, 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	iv
USER'S NOTICE	v
MANUAL REVISION INFORMATION	v
ITEM CHECKLIST	v
CHAPTER 1 INTRODUCTION OF THE MOTHERBOARD	
1-1 FEATURE OF MOTHERBOARD	1
1-2 SPECIFICATION	2
1-3 LAYOUT DIAGRAM	4
CHAPTER 2 HARDWARE INSTALLATION	
2-1 JUMPER SETTING	9
2-2 CONNECTORS AND HEADERS	14
2-2-1 CONNECTORS	14
2-2-2 HEADERS	18
CHAPTER 3 INTRODUCING BIOS	
3-1 ENTERING SETUP	26
3-2 BIOS MENU SCREEN	27
3-3 FUNCTION KEYS	28
3-4 GETTING HELP	28
3-5 MEMU BARS	29
3-6 MAIN MENU	29
3-7 ADVANCED MENU	31
3-8 CHIPSET MENU	45
3-9 SECURITY MENU	48
3-10 BOOT MENU	51
3-11 SAVE & EXIT MENU	52



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 60 centigrade is the suitable temperature. (The figure comes from the request of the main chipset)
- Generally speaking, dramatic changes in temperature may lead to contact malfunction and crackles due to constant thermal expansion and contraction from the 'welding spots' that connect components and PCB. Computer should go through an adaptive phase before it boots when it is moved from a cold environment to a warmer one to avoid condensation phenomenon. These water drops attached on PCB or the surface of the components can bring about phenomena as minor as computer instability resulted from corrosion and oxidation from components and PCB or as major as short circuit that can burn the components. Suggest starting the computer until the temperature goes up.
- The increasing temperature of the capacitor may decrease the life of computer. Using the close case may decrease the life of other device because the higher temperature in the inner of the case.
- Attention to the heat sink when you over-clocking. The higher temperature may decrease the life of the device and burned the capacitor.

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
4.0

Revision History
Fourth Edition

Date
August 2, 2022

Item Checklist

- Motherboard
- Cable(s)

Chapter 1

Introduction of the Motherboard

1-1 Feature of Motherboard

- Onboard Intel® Tiger Lake-UP3 series processor, TDP 15 W, never denies high performance
- Support 2* DDR4 3200 MHz SO-DIMM, maximum capacity up to 64GB
- Integrated with 1* Intel® i219-LM 1.0GbE & 1* Intel® i225-LM 2.5GbE
- 2* HDMI, 2* Display Port, 1* eDP, 1* LVDS; support up to 4* independent 4K HDR Displays or 1* 8K SDR Displays
- Onboard 1* M.2 M-key slot,type-2242/2280, PCIe 4.0x4 interface supports NVMe
- Onboard 1* M.2 E-key slot,type-2230 PCIe1/USB2.0 interface supports Wi-Fi / Bluetooth with Intel CNVi technology
- Onboard TPM 2.0(Option for **MF05-22** series)
- Support 1* SATAIII device
- Support 4* USB 3.2(Gen2) + 4* USB2.0
- Support 4* COM (***COM1/2 supports RS232/422/485**)
- Support CPU Smart FAN
- Compliance with ErP standard
- Support Watchdog function
- Solution for Digital Signage, Industrial PCs, Edge Computing, Factory Automation, AI and IoT Solution applications

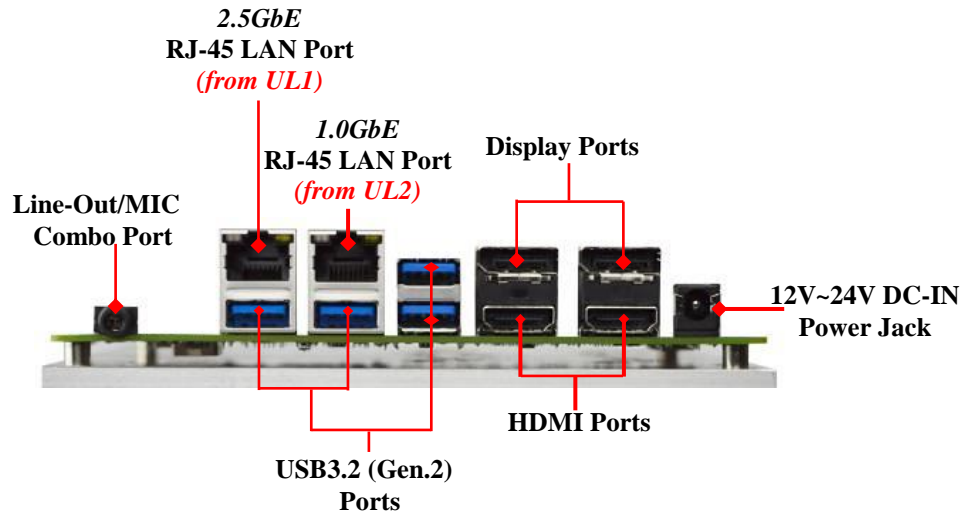
1-2 Specification

Spec	Description
Design	<ul style="list-style-type: none"> ● 3.5"SBC; 8-Layers; PCB size: 14.8x 10.2 cm
Embedded CPU	<ul style="list-style-type: none"> ● Integrated with Intel® Tiger Lake-UP3 series CPU (TDP 12~28W) <p><i>* Note: CPU model varies from different IPC options. Please consult your dealer for more information of onboard CPU.</i></p>
Memory Slot	<ul style="list-style-type: none"> ● 2* DDR4 SO-DIMM slot support 2* DDR4 3200MHz non-ECC SO-DIMM up to 64GB ● Support dual channel function <p><i>* Note: Memory clock supporting range is decided by specific CPU of the model. For more memory compatibility information please consults your local dealer.</i></p>
Expansion Slot	<ul style="list-style-type: none"> ● 1* M.2 M-key slot, type-2242/2280, PCIe4.0 x4 interface supports NVMe (M2M1) ● 1* M.2 E-key slot, type-2230, PCIe1/USB2.0 interface supports Wi-Fi / Bluetooth with Intel CNVi technology (M2E1) <p><i>*Note:M2M1 & M2E1 slot maximum current limit is 2A while using 3.3V.</i></p>
Storage	<ul style="list-style-type: none"> ● 1* SATAIII 6Gb/s port
LAN Chip	<ul style="list-style-type: none"> ● 1* Intel i219LM LAN chip supports 10/100/1000Mbps data transfer rate ● 1* Intel i225LM LAN chip supports up to 2.5Gbps data transfer rate
Audio Chip	<ul style="list-style-type: none"> ● Realtek HD audio chip
BIOS	<ul style="list-style-type: none"> ● AMI Flash ROM
Rear I/O	<ul style="list-style-type: none"> ● 1* 12V-24V DC-in power Jack (<i>*90W Power adapter is recommended for stable performance</i>) ● 2* display port (DP1.4a) ● 2* HDMI 2.0 port ● 4* USB 3.2(Gen.2) port ● 1* 2.5GbE RJ-45 LAN port (from UL1) ● 1* 1.0GbE RJ-45 LAN port (from UL2) ● 1* Audio Line Out/MIC combo port
Internal I/O	<ul style="list-style-type: none"> ● 1* 2-pin internal 12V~24V DC-in power connector ● 1* SATA Power-out connector

	<ul style="list-style-type: none"> ● 1* CPU FAN header ● 1* Front panel header ● 1* Buzzer header ● 1* PS/2 keyboard & mouse header ● 1* SMBUS header ● 2* LAN LED activity LED header ● 2* 9-pin USB 2.0 header (Expansible to 4* USB 2.0 ports) ● 4* Serial port header (COM1/2/3/4;COM1/2 supports RS232/422/485) ● 1* GPIO 8-bit/80 port header (selectable by J80PORT,default GPIO) ● 1* 3W amplifier header ● 1* EDP header ● 1* 24-bit dual channel LVDS header ● 1* LVDS inverter header
TPM 2.0	<ul style="list-style-type: none"> ● Optional for MF05-22 Series

1-3 Layout Diagram

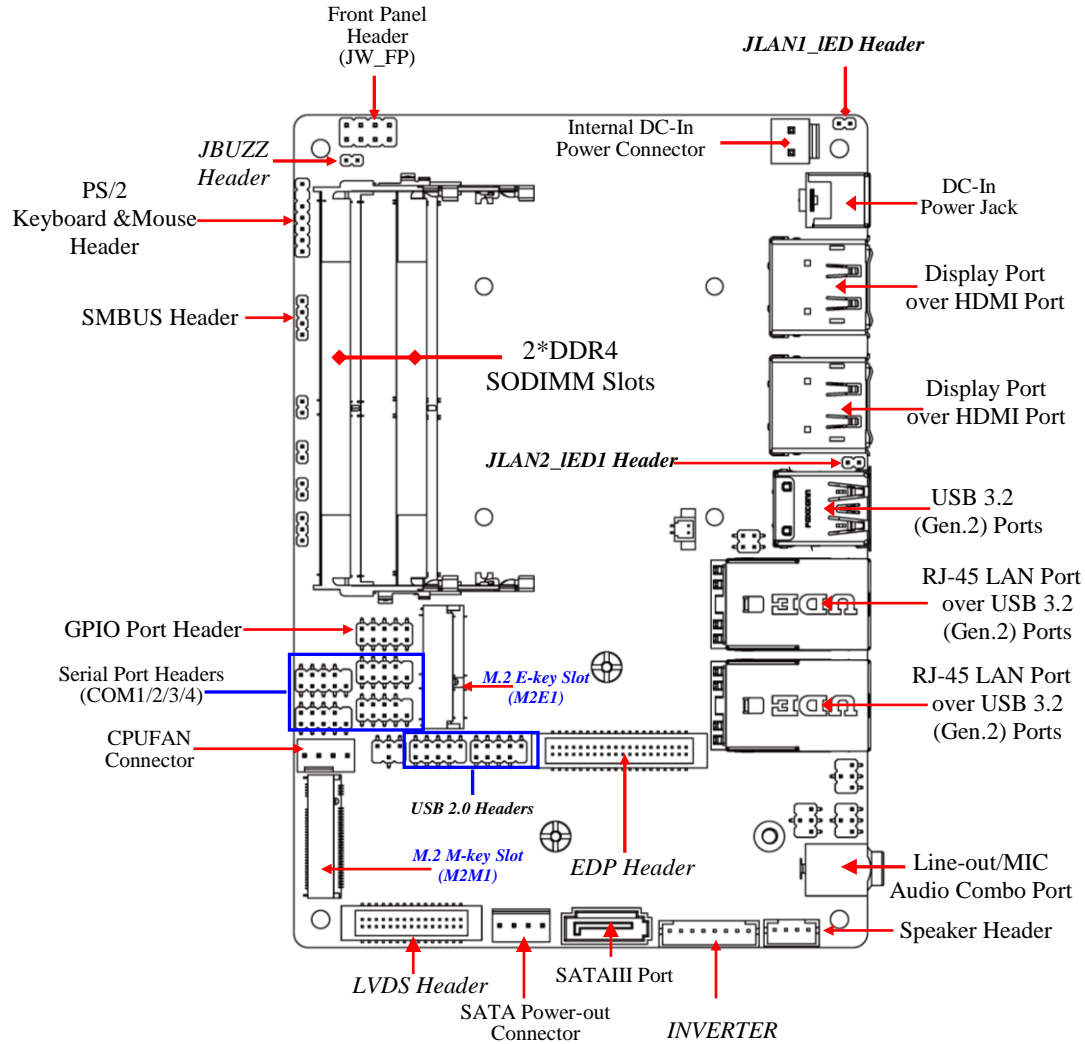
IO Panel Diagram:



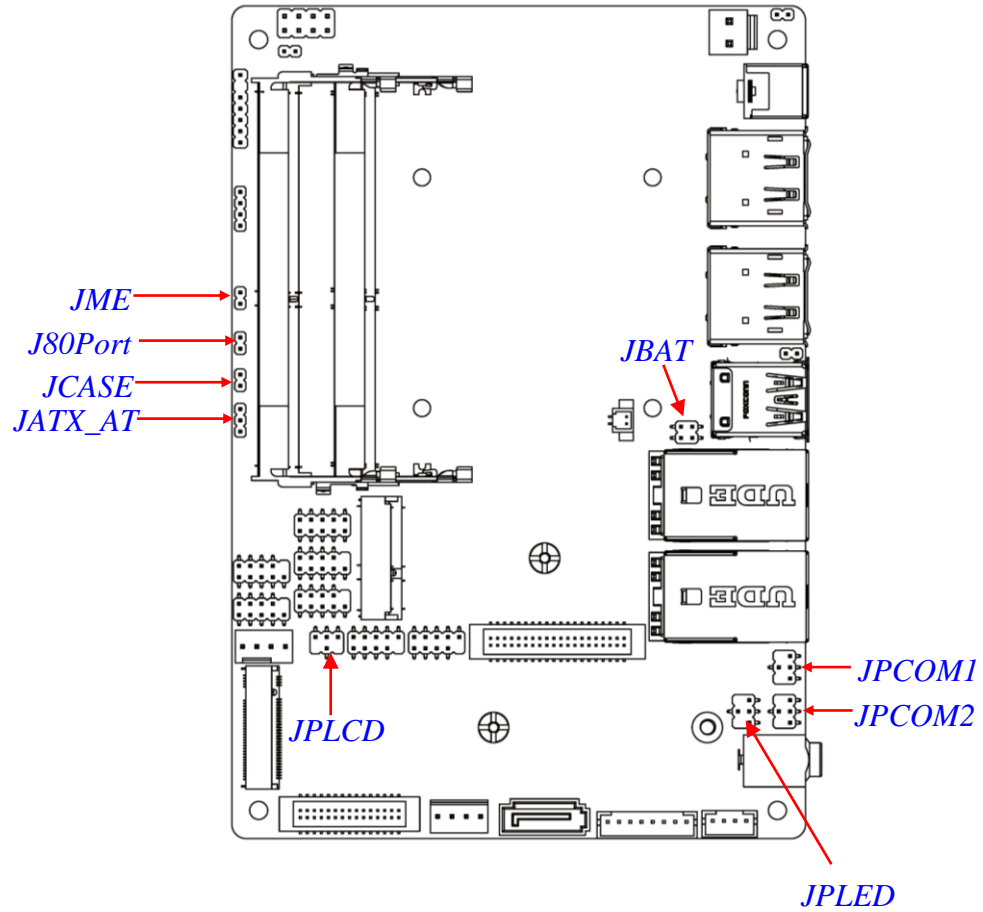
Warning!!

The board has a DC-in power connector (**DC_IN1**) in I/O back panel and an internal power connector (**DC_IN2**). User can only connect one type of compatible power supply to one of them to power the system.

Internal Diagram:



Jumper Positions:



Jumpers

Jumper	Name	Description	Pitch
JPCOM1	COM1 Header Pin-9 Function Select	4-Pin Block	2.0mm
JPCOM2	COM2 Header Pin-9 Function Select	4-Pin Block	2.0mm
JPLED	LVDS BACKLIGHT PWR Select	4-Pin Block	2.0mm
JPLCD	LVDS PANEL VCC Select	4-Pin Block	2.0mm
JME	Flash Override	2-Pin Block	2.0mm
J80PORT	For GPIO_CON 80 Port or GPIO Select	2-Pin Block	2.0mm
JCASE	Case Open Display Select	2-Pin Block	2.0mm
JATX_AT	ATX/AT Mode Select	3-Pin Block	2.0mm
JBAT	Pin (1-2): Clear CMOS Pin (3-4): Clear Mereg	4-Pin Block	2.0mm

Connectors

Connector	Name
DC_IN1	DC-in Power Jack
HDMI_DP1/ HDMI_DP2	Top: Display Port (DP 1.4a) Connector Bottom: HDMI 2.0 Port Connector
USB1	USB 3.2 (Gen.2) Port Connector X2
UL1	Top: 2.5GbE RJ-45 LAN Port Connector Bottom: USB 3.2 (Gen.2) Port Connector
UL2	Top: 1.0GbE RJ-45 LAN Port Connector Bottom: USB 3.2 (Gen.2) Port Connector
Audio	Audio Line Out /MIC Combo Connector
DC_IN2	Internal 12V~24V DC-in Power Connector
SATA	SATAIII Port Connector
SATAPWR	SATA Power out Connector
CPUFAN	CPUFAN Connector

Headers

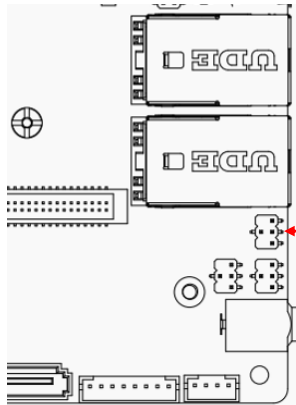
Header	Name	Description	Pitch
JW_FP	Front Panel Header(PWR LED/ HDD LED/Power Button /Reset)	8-pin Block	2.54mm
JBUZZ	Buzzer Header	2-pin Block	2.0mm
PS2KBMS	PS/2 Keyboard & Mouse Header	6-pin Block	2.0mm
SMBUS	SMBUS Header	4-pin Block	2.0mm
JLAN1_LED	UL1 2.5GbE LAN Activity LED Header	2-pin Block	2.0mm
JLAN2_LED1	UL2 1.0GbE LAN Activity LED Header	2-pin Block	2.0mm
FP_USB1/ FP_USB2	USB 2.0 Header	9-pin Block	2.0mm
COM1/COM2	RS232/422/485 Serial Port Header	9-pin Block	2.0mm
COM3/COM4	RS232 Serial Port Header	9-pin Block	2.0mm
GPIO_CON	GPIO Port Header	10-pin Block	2.0mm
SPEAK_CON	3W Amplifier Header	4-pin Block	2.0mm
EDP	EDP Port Header	40-pin Block	1.25mm
LVDS	LVDS Port Header	30-pin Block	1.25mm
INVERTER	LVDS Inverter	8-pin Block	2.0mm

Chapter 2

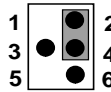
Hardware Installation

2-1 Jumper Settings

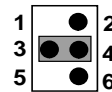
JPCOM1 (4-pin): COM1 Header Pin-9 Function Select



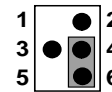
JPCOM1 → COM1 Header Pin-9 Function Select



2-4 Closed:
RI=RS232
(Default);



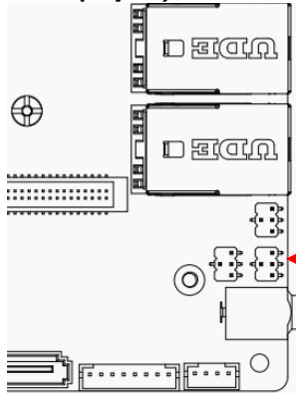
3-4 Closed:
RI=+5V;



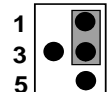
4-6 Closed:
RI=+12V.

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

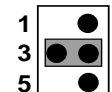
JPCOM2 (4-pin): COM2 Header Pin-9 Function Select



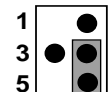
JPCOM2 → COM2 Header Pin-9 Function Select



2-4 Closed:
RI=RS232
(Default);



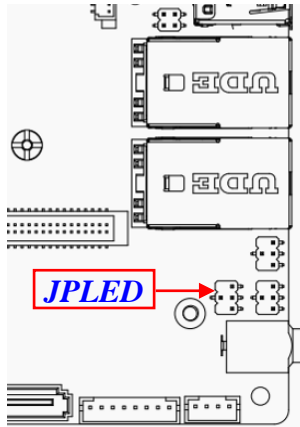
3-4 Closed:
RI=+5V;



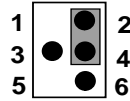
4-6 Closed:
RI=+12V.

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

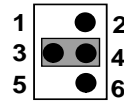
JPLED (4-pin): LVDS-BACKLIHGT-PWR Select



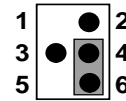
JPLED → LVDS BACKLIHGT PWR Select



2-4 Closed:
LED VCC=5V
(Default);



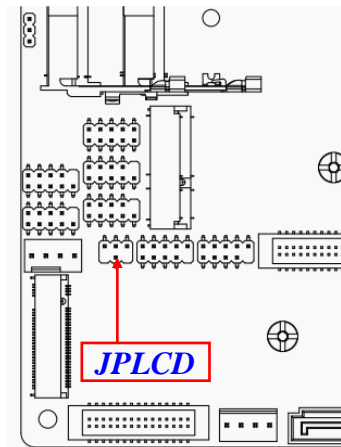
3-4 Closed:
LED VCC=+12V;



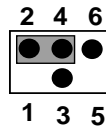
4-6 Closed:
LED VCC=ADP(12V~24V).

***Note:** Maximum current limit is 2A while using 5V or 12V.

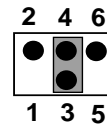
JPLCD (4-pin): LVDS PANEL VCC Select



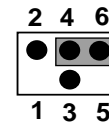
JPLCD → LVDS PANEL VCC Select



2-4 Closed:
VCC= 3.3V
(Default);



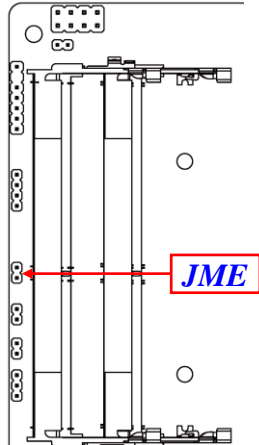
3-4 Closed:
VCC= +5V;



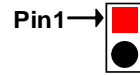
4-6 Closed:
VCC= +12V.

***Note:** Maximum current limit is 2A while using 3.3V, 5V or 12V.

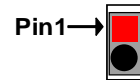
JME(2-pin): ME Flash Override Select



JME→ME Flash Override Select

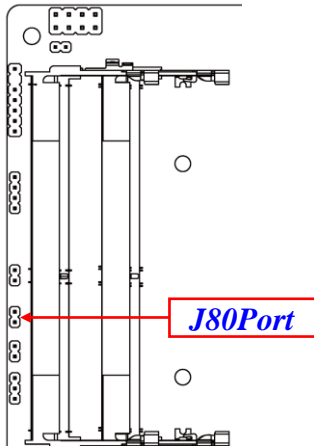


1-2 Open: Normal(Default);

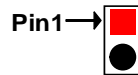


1-2 Closed: ME Flash Override.

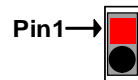
J80PORT(2-pin): GPIO_CON 80 Port/GPIO Function Select



J80PORT→GPIO_CON 80/GPIO Select



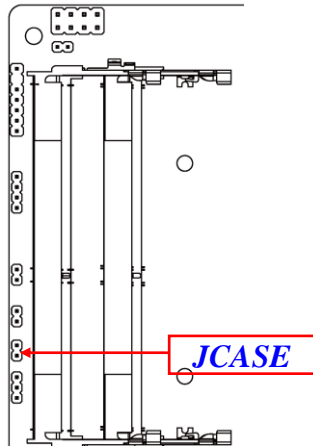
1-2 Open: GPIO_CON=80 Port;



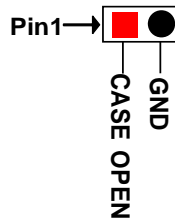
1-2 Closed: GPIO_CON=GPIO Port(Default).

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

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



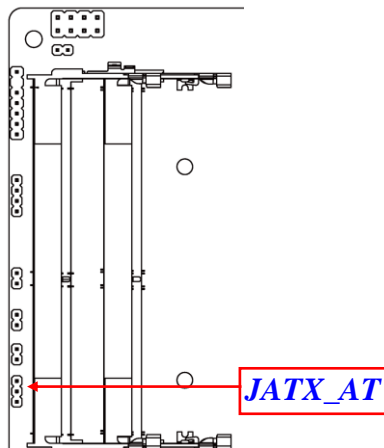
JCASE → Case Open Detection



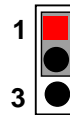
Default: Open.

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.

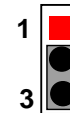
JATX_ATX (3-pin): AT Mode /ATX Mode Select



JATX_ATX → ATX/AT Mode Select



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

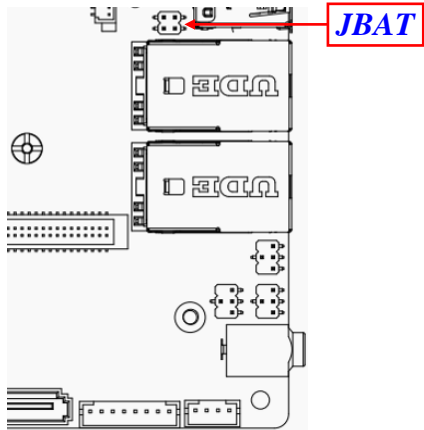


2-3 Closed: AT Mode Selected.

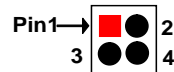
***ATX Mode Selected:** Press power button to power on after power input ready;

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

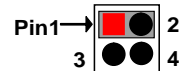
Pin (1-2) of JBAT (4-pin): Clear CMOS Settings



Pin 1&2 of JBAT → Clear CMOS

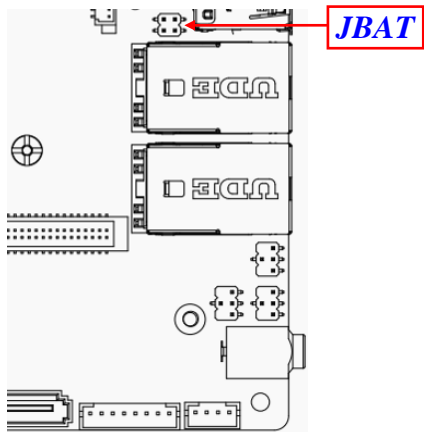


1-2 Open: Normal(Default);

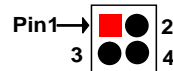


1-2 Closed: Clear CMOS(One Touch).

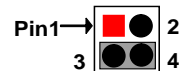
Pin (3-4) of JBAT (4-pin): Clear MEREg



Pin 3&4 of JBAT → Clear MEREg



3-4 Open: Normal(Default);

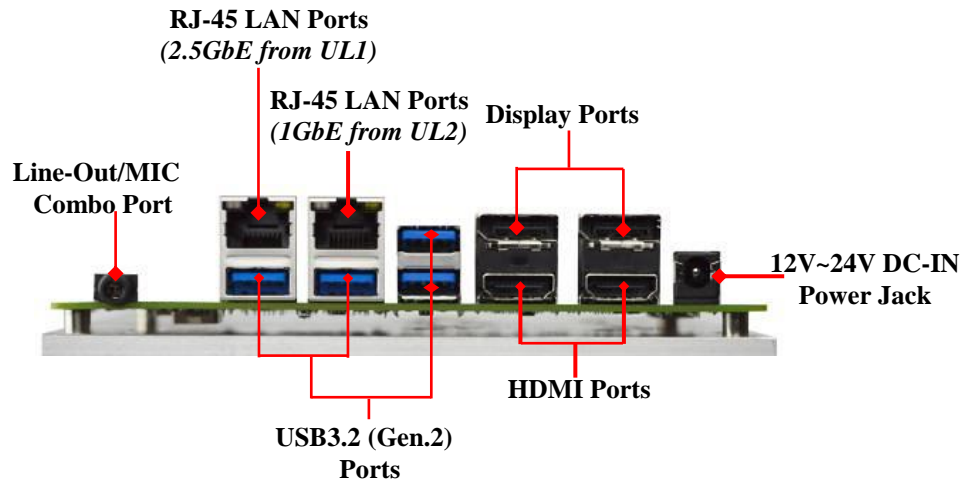







3-4 Closed: Clear MEREg.

2-2 Connectors and Headers

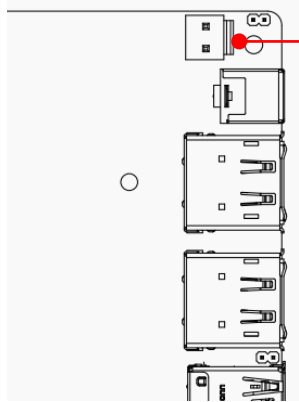
2-2-1 Connectors

(1) Rear I/O Connectors



Icon	Name	Function
	12V~24V DC-in Power Jack	For user to connect compatible power adapter to provide power supply for the system.
	Top: Display Port Bottom: HDMI Port	Display port: to the system to corresponding display device with compatible DP cable. HDMI port: to connect display device that support HDMI specification.
	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. <i>*Note: Maximum current limit is 1.5A while using 5V working voltage</i>
	RJ-45 LAN Port	This connector is standard RJ-45 LAN jack for Network connection (<i>LAN port from UL1 Intel® i225-LM supports up to 2.5Gbps transfer rate; PHY LAN port from UL2 Intel® i219-LM supports up to 1.0Gbps transfer rate</i>).
	Audio Line Out /MIC Combo Connector	This audio jack can function as audio Line-out & MIC-in combo connector with compatible cable connection.

(2) DC_IN2(2-pin) : Internal 12V~24V DC-in Power Connector



DC_IN2

Pin 1

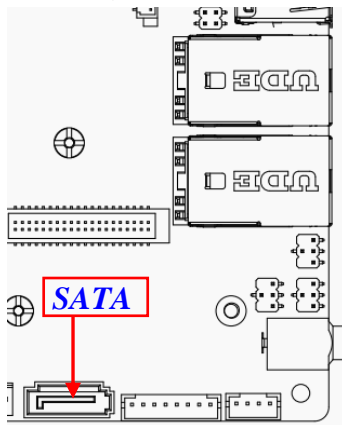


Pin No.	Definition
1	+12V~24VC DC-In
2	GND

Warning: Find Pin-1 position before connecting power cable to this 2-pin power connector. **WRONG INSTALLATION DIRECTION WILL DAMAGE THE BOARD!!**

(3) SATA(7-pin): SATAIII Port connector

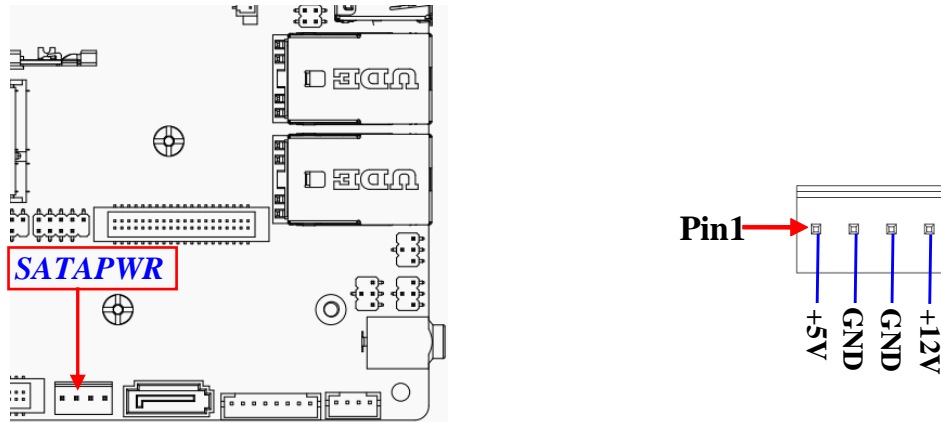
This is a high-speed SATAIII port that supports 6GB/s transfer rate.



SATA

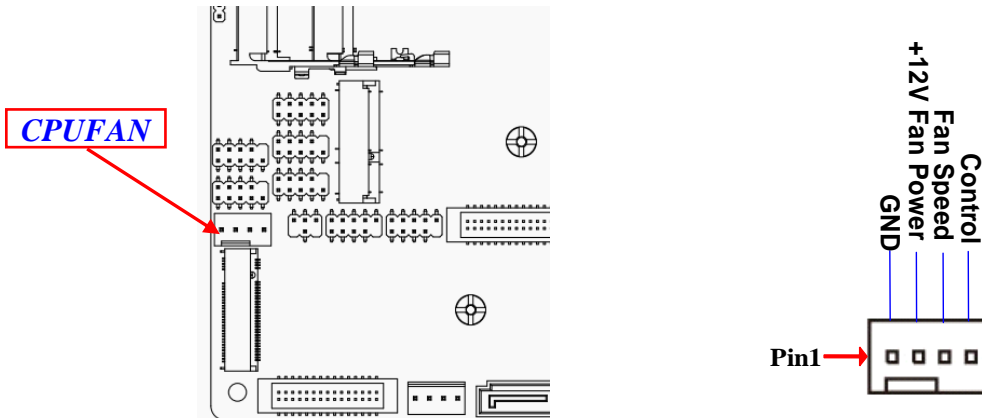
Pin No.	Definition
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND

(4) SATAPWR (4-pin): SATA HDD Power-Out Connector



Warning: Make sure that Pin-1 of compatible SATA Power out connector is inserted into corresponding Pin-1 of **SATAPWR** connector to avoid possible damage to the board and hard disk driver!

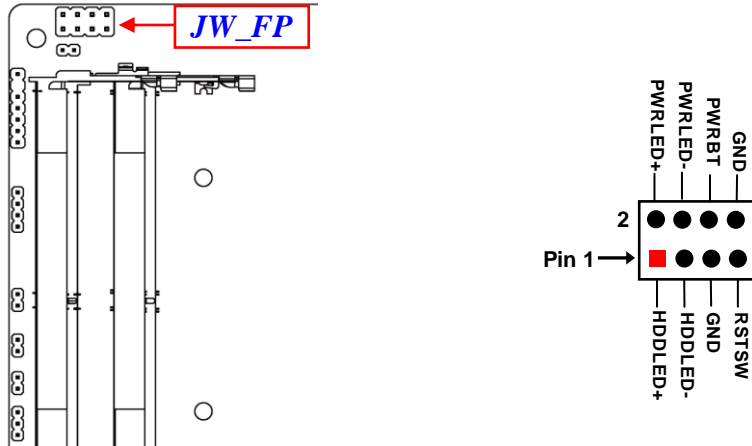
(5) CPUFAN (4-pin): CPU FAN Connector



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

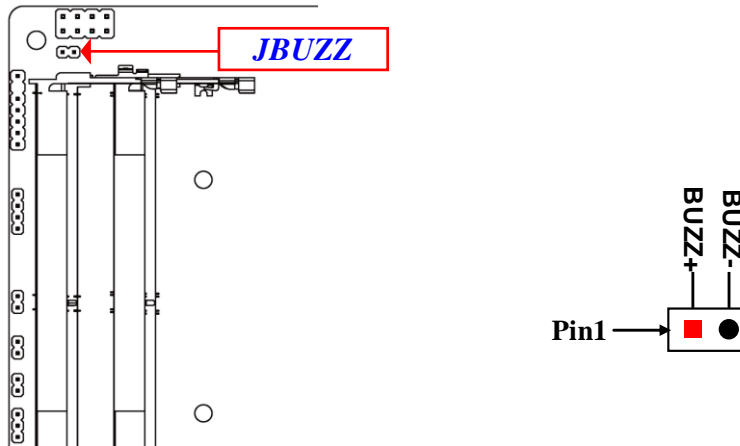
2-2-2 Headers

JW_FP (8-pin): Front Panel Header



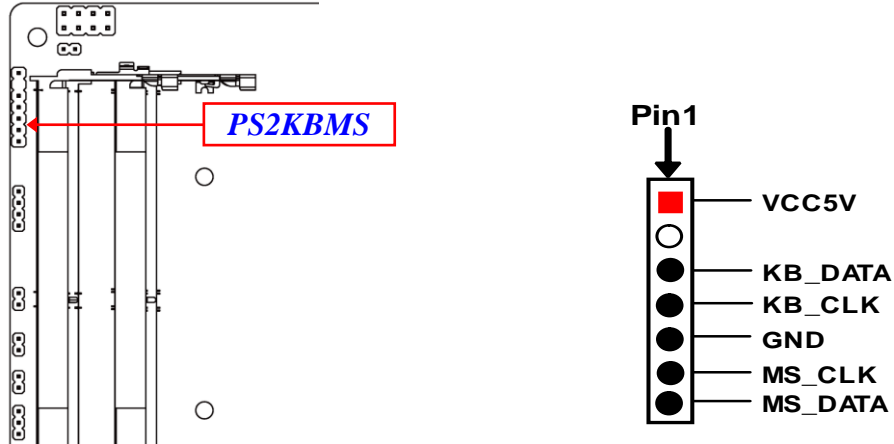
***Note:** Maximum current limit is **1A** while using 5V working voltage.

JBUZZ (2-pin): Buzzer Header



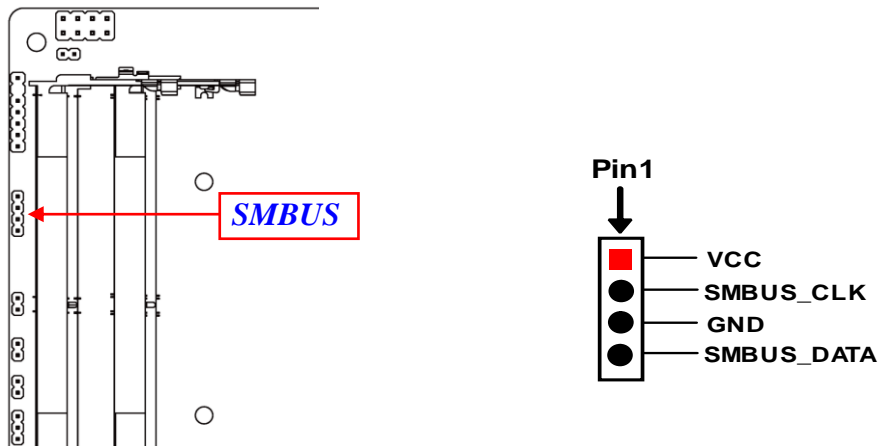
***Note:** Maximum current limit is **60mA** while using 5V working voltage.

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



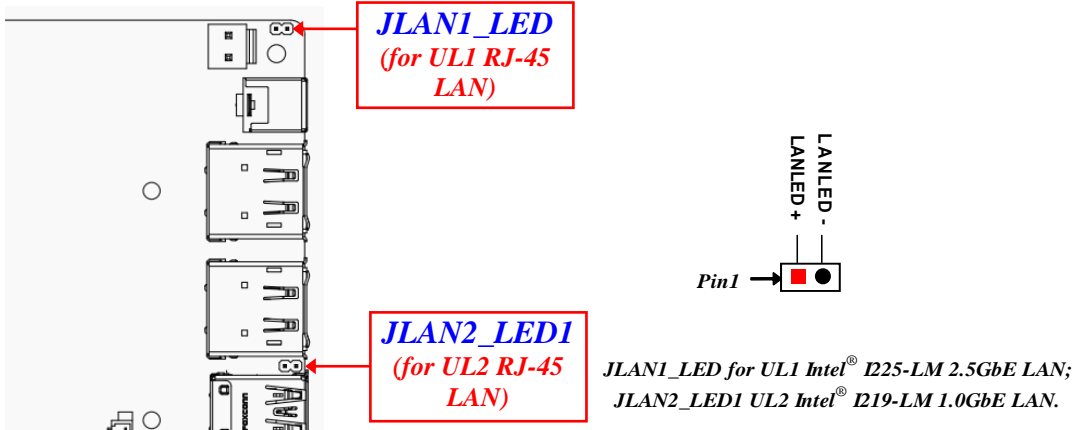
***Note:** Maximum current limit is **500mA** while using 5V working voltage.

SMBUS (4-Pin): SMBUS Header



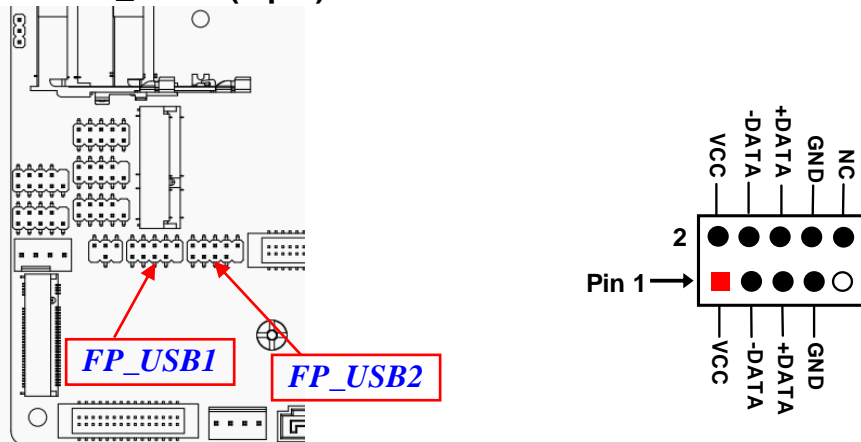
***Note:** Maximum current limit is **300mA** while using 5V working voltage.

JLAN1_LED/ JLAN2_LED1 (2-pin): LAN Activity LED Header



***Note:** Maximum current limit is **300uA** while using **3.3V** working voltage.

FP_USB1/FP_USB2 (9-pin): USB2.0 Header

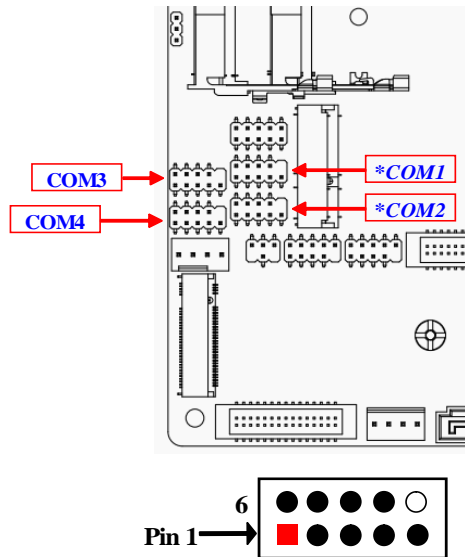


***Note:** Maximum current limit is **1.5A** in total while using **5V** working voltage.

COM1/2/3/4(9-pin): Serial Port Headers

COM1/2: RS232/422/485 Serial Port Header.

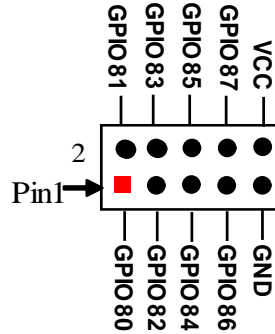
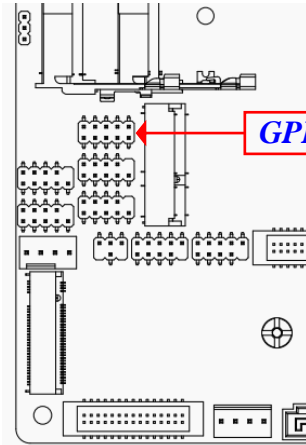
COM3/4: RS232 Serial Port Header.



Pin NO.	RS232	*RS422 <i>(optional)</i>	*RS485 <i>(optional)</i>
Pin 1	DCD	TX-	DATA-
Pin 2	RXD	TX+	DATA+
Pin 3	TXD	RX+	NC
Pin 4	DTR	RX-	NC
Pin 5	GND	GND	GND
Pin 6	DSR	NC	NC
Pin 7	RTS	NC	NC
Pin 8	CTS	NC	NC
Pin 9	RI	NC	NC

***Note:** COM1 & COM2 header can function as RS232/422/485 port header. In normal settings COM1 & COM2 function as RS232 header. With compatible COM cable connection COM1 & COM2 can function as RS422 or RS 485 header. User also needs to go to BIOS to set 'Transmission Mode Select' for COM1 or COM2 header (refer to Page-36/37) at first, before using specialized cable to connect different pins of this port.

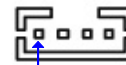
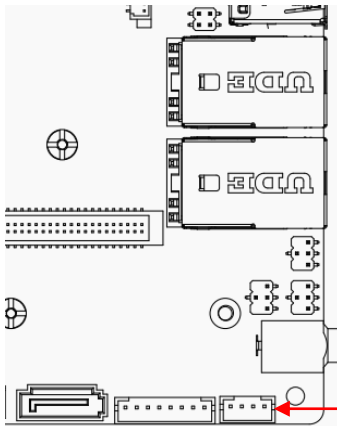
GPIO_CON (10-pin): GPIO 8-bit Port or 80 Port Header



***J80PORT Closed: Normal 8-bit GPIO;
J80PORT Open: For 80Port Function.***

***Note:** 1. Maximum current limit is 1A while using 5V working voltage; 2. Please refer to **Page-11** **J80PORT** jumper settings for GPIO_CON 80Port or GPIO Port function select.

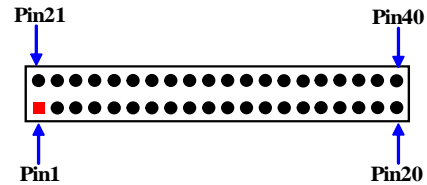
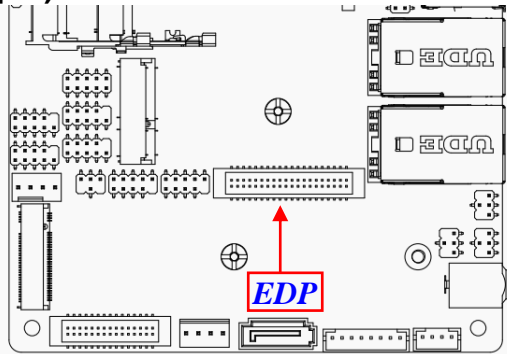
SPEAK_CON (4-pin): 3W Amplifier Header



Pin1

Pin No.	Definition
1	L-
2	L+
3	R+
4	R-

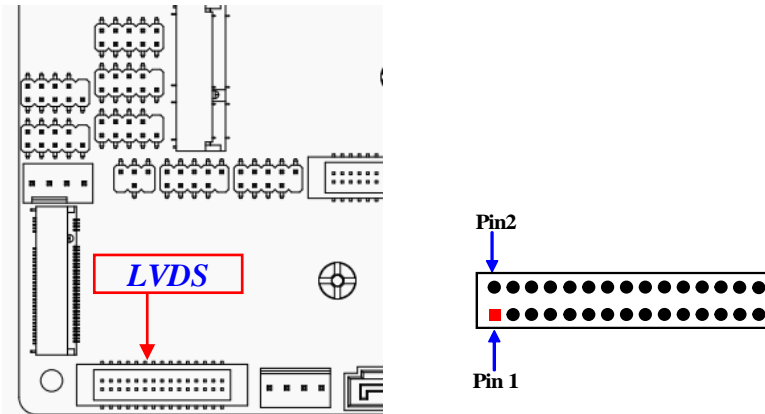
EDP (40-pin): 4-lane eDP Header



Pin Define	Pin NO.	Pin NO.	Pin Define
NC	Pin 1	Pin 21	NC
GND	Pin 2	Pin 22	NC
Lane3_N	Pin 3	Pin 23	GND
Lane3_P	Pin 4	Pin 24	GND
GND	Pin 5	Pin 25	GND
Lane2_N	Pin 6	Pin 26	GND
Lane2_P	Pin 7	Pin 27	HPD
GND	Pin 8	Pin 28	GND
Lane1_N	Pin 9	Pin 29	GND
Lane1_P	Pin 10	Pin 30	GND
GND	Pin 11	Pin 31	EDP_DET
Lane0_N	Pin 12	Pin 32	BL_ENABLE
Lane0_P	Pin 13	Pin 33	BL_CTRL
GND	Pin 14	Pin 34	NC
AUX_CH_P	Pin 15	Pin 35	NC
AUX_CH_N	Pin 16	Pin 36	BL_PWR
GND	Pin 17	Pin 37	BL_PWR
LCD_VCC	Pin 18	Pin 38	BL_PWR
LCD_VCC	Pin 19	Pin 39	BL_PWR
LCD_VCC	Pin 20	Pin 40	NC

***Note:** Maximum current limit is 2A while EDP backlight =12V & EDP PANEL VCC =3.3V.

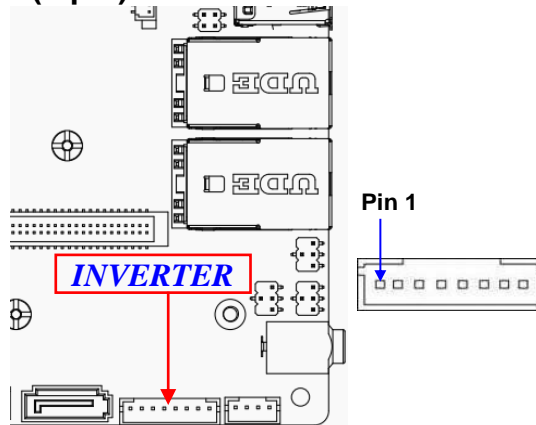
LVDS (30-pin): 24-bit Dual Channel LVDS Header



Pin Define	Pin NO.	Pin NO.	Pin Define
LVDSB_DATAP3	Pin 1	Pin 2	LVDSB_DATAP3
LVDS_CLKBN	Pin 3	Pin 4	LVDS_CLKBP
LVDSB_DATAP2	Pin 5	Pin 6	LVDSB_DATAP2
LVDSB_DATAP1	Pin 7	Pin 8	LVDSB_DATAP1
LVDSB_DATAP0	Pin 9	Pin 10	LVDSB_DATAP0
NC	Pin 11	Pin 12	NC
GND	Pin 13	Pin 14	LVDS_DET
GND	Pin 15	Pin 16	GND
LVDSA_DATAP3	Pin 17	Pin 18	LVDSA_DATAN3
LVDS_CLKAP	Pin 19	Pin 20	LVDS_CLKAN
LVDSA_DATAP2	Pin 21	Pin 22	LVDSA_DATAN2
LVDSA_DATAP1	Pin 23	Pin 24	LVDSA_DATAN1
LVDSA_DATAP0	Pin 25	Pin 26	LVDSA_DATAN0
LCD VCC	Pin 27	Pin 28	LCD VCC
LCD VCC	Pin 29	Pin 30	LCD VCC

***Note:** Maximum current limit is 2A while using 3.3V, 5V or 12V.

INVERTER (8-pin): LVDS Inverter Connector



Pin No.	Definition
1	Backlight Enable
2	Backlight PWM
3	Back Light LED VCC
4	Back Light LED VCC
5	GND
6	GND
7	Backlight Up SW
8	Backlight Down SW

***Note:** Maximum current limit is 2A while using 5V or 12V or adapter DCIN Voltage(12V~24V).

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!!

Chapter 3

Introducing BIOS

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

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

3-1 Entering Setup

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

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

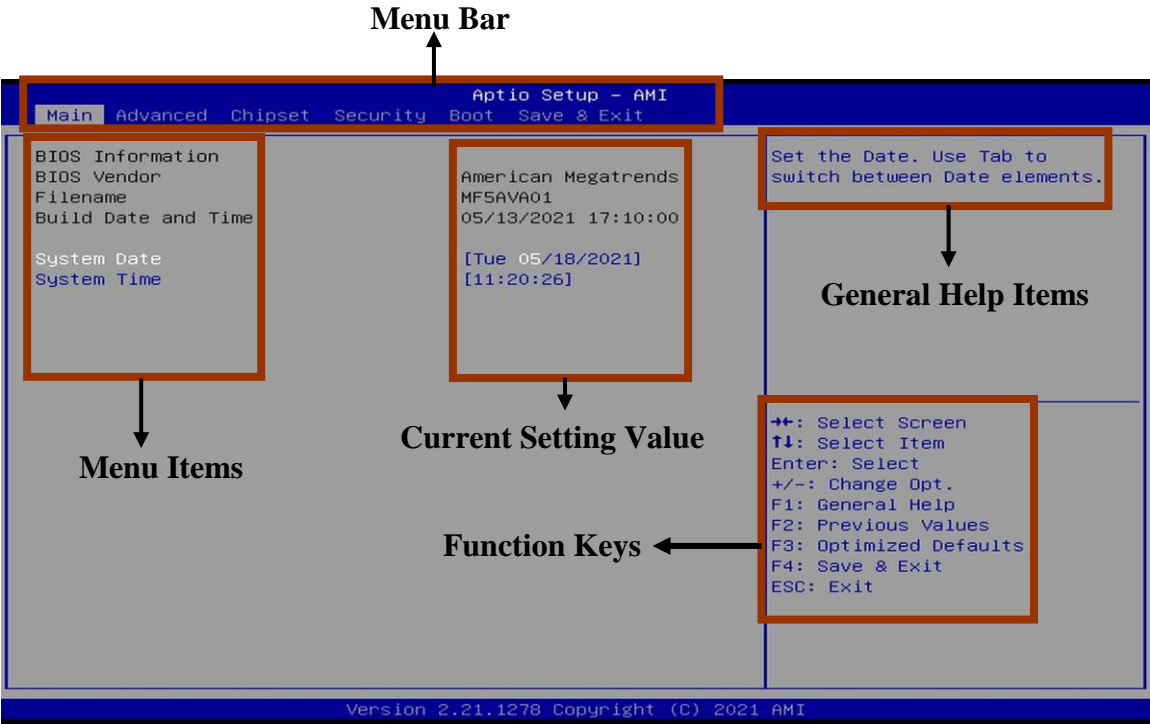
```
Please select boot device:
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

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

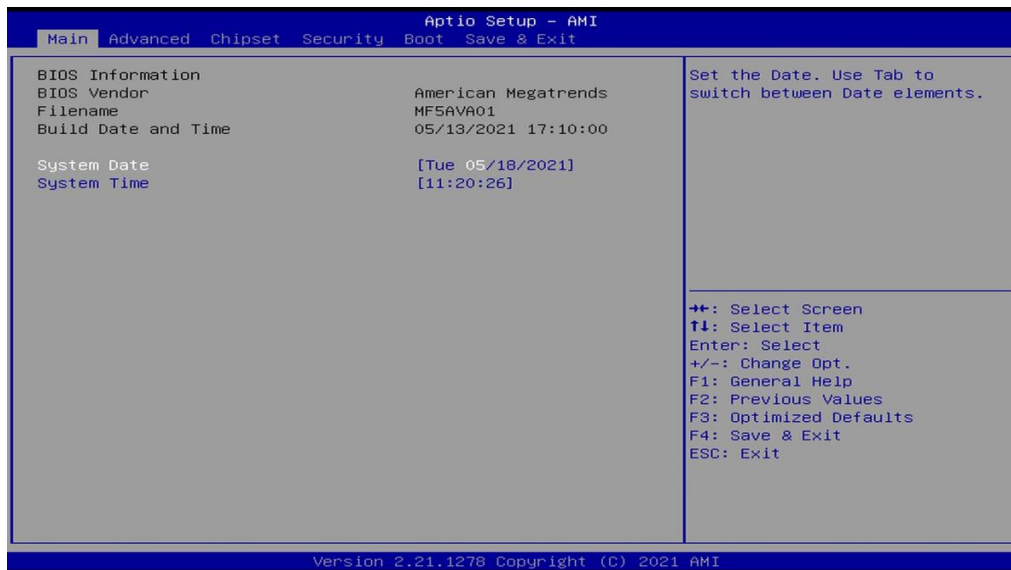
There are six menu bars on top of BIOS screen:

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.



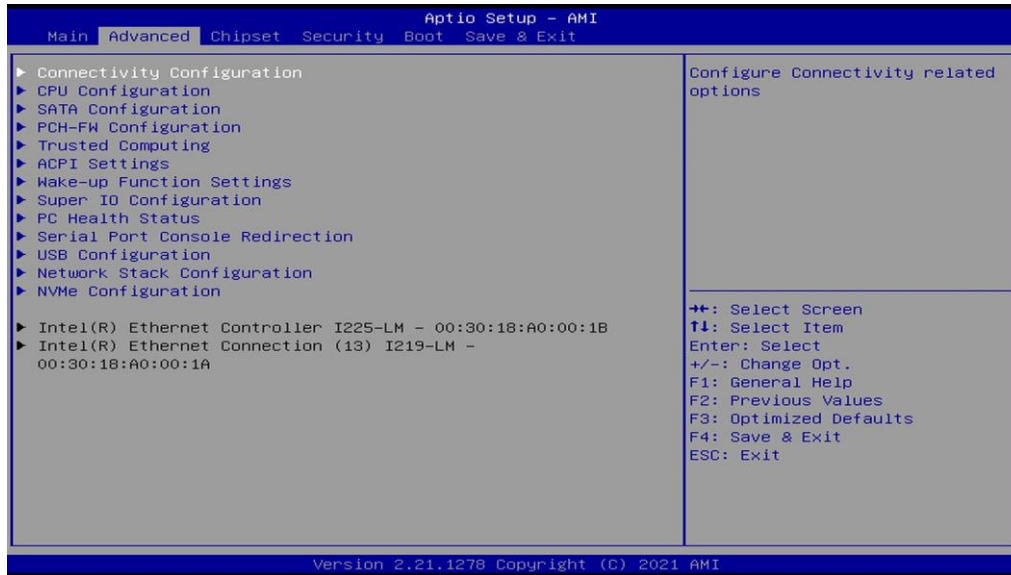
System Date

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].

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

Turbo Mode

Use this item to enable or disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.

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].

Hardware Prefetcher

Use this item to turn on/off the MLC streamer prefetcher.

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

Adjacent Cache Line Prefetch

Use this item to turn on/off prefetching of adjacent cache lines.

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

▶ **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

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].

▶ **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

▶ **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.*

▶ **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, MM05-22 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].

TPM 2.0 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 wake-up from S3/S4 state.

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

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

USB S5 Power

Use this item to enable or disable USB Power after System Shutdown.

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

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

Internal USB Port 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].

► Serial Port 3 Configuration

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

Serial Port 3 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=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 4 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=2E8h; IRQ=10;]; [IO=3F8h; IRQ=3,4,5,7,10,11;];

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

IRQ=3,4,5,7,10,11;]; [IO=3E0h; IRQ=3,4,5,7,10,11;]; [IO=2E0h;

IRQ=3,4,5,7,10,11;].

WatchDog Reset Timer

Use this item to enable or disable WDT reset function. 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 **JATX_AT** jumper setting for ATX Mode & 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 **JCASE** jumper setting for Case Open Detection*); if Pin 1&2 of **JCASE** 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

CPUFAN Smart Mode

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

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

CPUFAN Full-Speed Temperature

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

CPUFAN Full-Speed Duty

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

CPUFAN Idle-Speed Temperature

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

CPUFAN Idle-Speed Duty

Use this item to set CPUFAN 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

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.

▶ **NVMe Configuration**

Press [Enter] to view current NVMe Configuration.

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

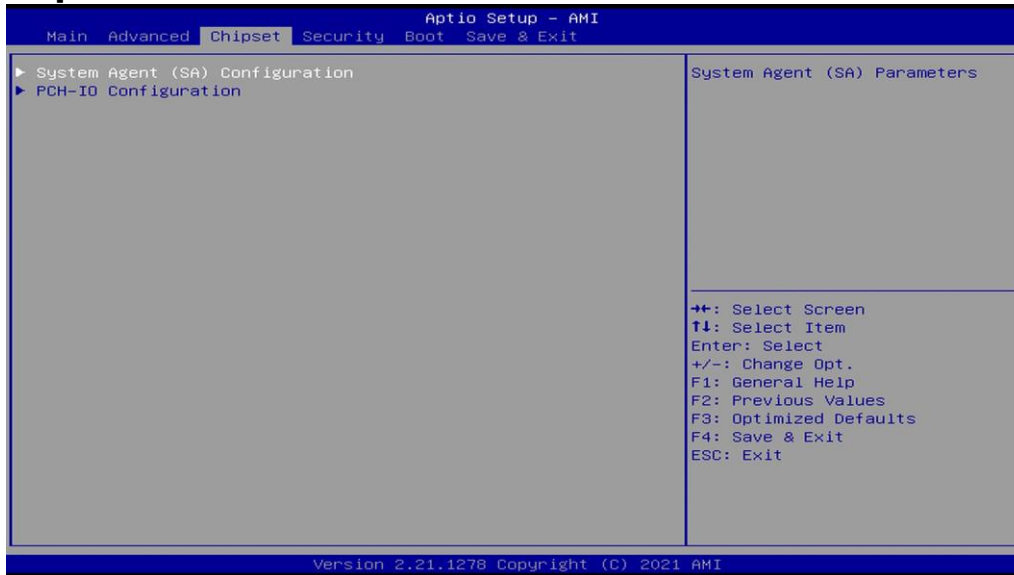
▶ **Intel(R) Ethernet Connection I225-LM - XX:XX:XX:XX:XX:XX**

This item shows current network brief information.

▶ **Intel(R) Ethernet Connection (13) 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

Active LVDS

Use this item to select the Active Configuration.

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

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

Panel Type

Use this item to select panel type.

The optional settings: [800x 480 18bit Single]; [800x 600 18bit Single]; [800x 600 24bit Single]; [1024 x 600 18bit Single]; [1024 x 768 18bit Single]; [1024 x 768 24bit Single]; [1280 x 768 24bit Single]; [1280 x 800 18bit Single]; [1280 x 800 24bit Single]; [1366 x 768 18bit Single]; [1366 x 768 24bit Single]; [1440 x 900 18bit Dual]; [1440 x 900 24bit Dual]; [1280 x 1024 24bit Dual]; [1680 x 1050 24bit Dual]; [1920 x 1080 24bit Dual].

LVDS FW Write Protect

Use this item to enable or disable LVDS FW Update/Protect.

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

► **PCH-IO Configuration**

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

PCH-IO Configuration

USB Controller

Use this item to enable or disable USB Physical Connector (physical port). Once **[Disabled]**, any USB devices plug into the connector will not be detected by BIOS or OS.

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

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.

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.*

Onboard Lan1 Controller

Use this item to control the PCI Express Root Port.

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

Onboard Lan2 Controller

Use this item to enable or disable onboard NIC.

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

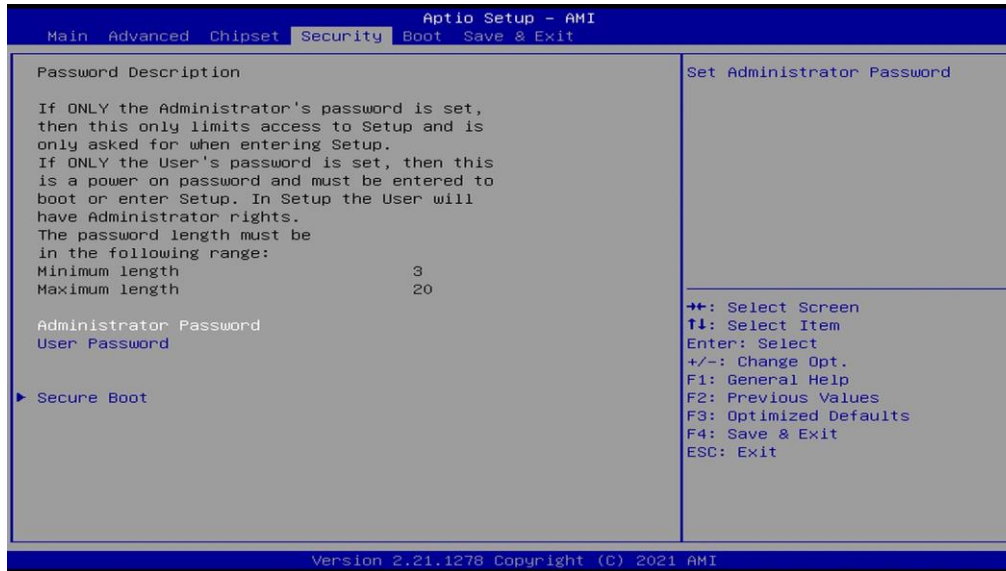
When set as [Enabled], the following sub-items shall appear:

Wake on LAN Enable

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

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

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 administrator password. If password is present on system, please press [Enter] to verify old password then to clear/change password. Press again to confirm the new administrator password.

▶ Secure Boot

Press [Enter] to make customized secure settings:

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**

- ▶ **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**
- ▶ **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. 65535 (0xFFFF) means indefinite waiting.

Bootup NumLock State

Use this item to select keyboard NumLock state.

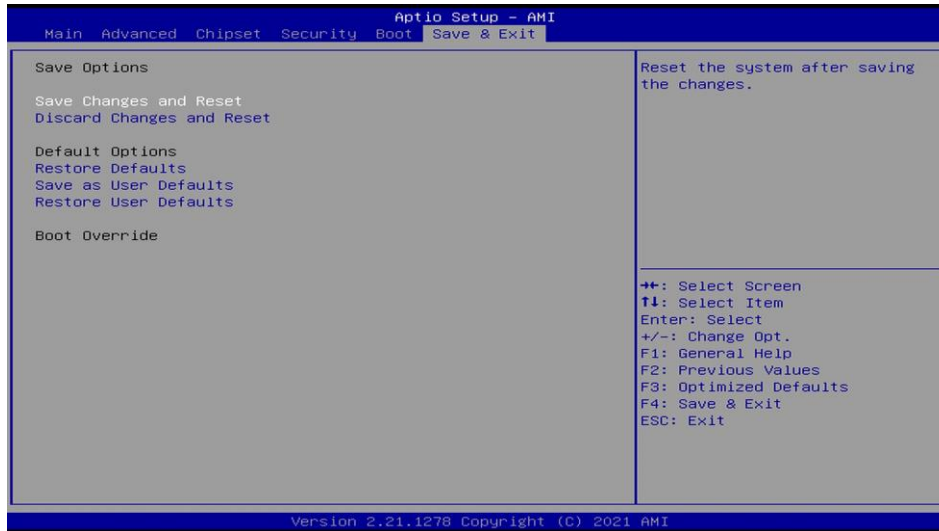
The optional settings: [On]; [Off].

Quiet Boot

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

Boot Option Priorities

3-11 Save & Exit Menu



Save Options

Save Changes and Reset

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

Discard Changes and Reset

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

Default Options

Restore Defaults

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

Save as User Defaults

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

Restore User Defaults

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

Boot Override