

ATX-Q670B (MQ670BX)

ATX Motherboard

Copyright Notice

This document is copyrighted, 2024. All rights are reserved. The original manufacturer reserves the right to make improvements to the products described in this manual at any time without notice.

No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of the original manufacturer. Information provided in this manual is intended to be accurate and reliable. However, the original manufacturer assumes no responsibility for its use, or for any infringements upon the rights of third parties that may result from its use.

The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, GIGAIPC assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.

GIGAIPC reserves the right to make changes in the product design without notice to its users.

Acknowledgement

All other products' name or trademarks are properties of their respective owners.

- Microsoft Windows is a registered trademark of Microsoft Corp.
- Intel, Pentium, Celeron, and Xeon are registered trademarks of Intel Corporation
- Core, Atom are trademarks of Intel Corporation
- ITE is a trademark of Integrated Technology Express, Inc.
- IBM, PC/AT, PS/2, and VGA are trademarks of International Business Machines Corporation.

All other product names or trademarks are properties of their respective owners.

Packing List

Before setting up your product, please make sure the following items have been shipped:

Item	Quantity
ATX-Q670B (MQ670BX)	1
IO Shield	1
SATA cable	2

If any of these items are missing or damaged, please contact your distributor or sales representative immediately.

About this Document

This User's Manual contains all the essential information, such as detailed descriptions and explanations on the product's hardware and software features (if any), its specifications, dimensions, jumper/connector settings/definitions, and driver installation instructions (if any), to facilitate users in setting up their product.

Users may refer to the GIGAIPC.com for the latest version of this document.

Safety Precautions

Please read the following safety instructions carefully. It is advised that you keep this manual for future references

1. All cautions and warnings on the device should be noted.
2. Make sure the power source matches the power rating of the device.
3. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
4. Always completely disconnect the power before working on the system's hardware.
5. No connections should be made when the system is powered as a sudden rush of power may damage sensitive electronic components.
6. If the device is not to be used for a long time, disconnect it from the power supply to avoid damage by transient over-voltage.
7. Always disconnect this device from any AC supply before cleaning.
8. While cleaning, use a damp cloth instead of liquid or spray detergents.
9. Make sure the device is installed near a power outlet and is easily accessible.
10. Keep this device away from humidity.
11. Place the device on a solid surface during installation to prevent falls
12. Do not cover the openings on the device to ensure optimal heat

dissipation.

13. Watch out for high temperatures when the system is running.
14. Do not touch the heat sink or heat spreader when the system is running
15. Never pour any liquid into the openings. This could cause fire or electric shock.
16. As most electronic components are sensitive to static electrical charge, be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and contain all electronic components in any static-shielded containers.
17. If any of the following situations arises, please the contact our service personnel:
 - i. Damaged power cord or plug
 - ii. Liquid intrusion to the device
 - iii. Exposure to moisture
 - iv. Device is not working as expected or in a manner as described in this manual
 - v. The device is dropped or damaged
 - vi. Any obvious signs of damage displayed on the device
18. **DO NOT LEAVE THIS DEVICE IN AN UNCONTROLLED ENVIRONMENT WITH TEMPERATURES BEYOND THE DEVICE'S PERMITTED STORAGE TEMPERATURES (SEE CHAPTER 1) TO PREVENT DAMAGE.**

FCC Statement

Warning!



This device complies with Part 15 FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

Caution:

There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions and your local government's recycling or disposal directives.

Attention:

Il y a un risque d'explosion si la batterie est remplacée de façon incorrecte. Ne la remplacer qu'avec le même modèle ou équivalent recommandé par le constructeur. Recycler les batteries usées en accord avec les instructions du fabricant et les directives gouvernementales de recyclage.

China RoHS Requirements (CN)

产品中有毒有害物质或元素名称及含量
GIGAIPC Main Board/ Daughter Board/ Backplane

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯 醚 (PBDE)
印刷电路板 及其电子组件	○	○	○	○	○	○
外部信号 连接器及线材	○	○	○	○	○	○
○: 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。 X: 表示该有毒有害物质至少在该部件的 某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。 备注: 此产品所标示之环保使用期限, 系指在一般正常使用状况下。						

China RoHS Requirement (EN)

Poisonous or Hazardous Substances or Elements in Products
GIGAIPC Main Board/ Daughter Board/ Backplane

Component	Poisonous or Hazardous Substances or Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr(VI))	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB & Other Components	O	O	O	O	O	O
Wires & Connectors for External Connections	O	O	O	O	O	O
O : The quantity of poisonous or hazardous substances or elements found in each of the component's parts is below the SJ/T 11363-2006-stipulated requirement. X: The quantity of poisonous or hazardous substances or elements found in at least one of the component's parts is beyond the SJ/T 11363-2006-stipulated requirement. Note: The Environment Friendly Use Period as labeled on this product is applicable under normal usage only						

Table Contents

ATX Motherboard	1
Copyright Notice	2
Acknowledgement	3
Packing List	4
About this Document	5
Safety Precautions	6
FCC Statement.....	8
China RoHS Requirements (CN).....	9
China RoHS Requirement (EN)	10
Chapter 1 - Product Specifications	15
1.1 Specifications	17
Chapter 2 – Hardware Information	19
2.1 Jumpers and Connectors	20
2.2.1 Rear I/O Connector	23
2.2.2 AUDIO (Line in, Line out, Mic in)	24
2.2.3 USB3_LAN1, USB3_LAN2 (USB 3.2 Gen 1 + 2.5GbE LAN Connector)	25
2.2.4 DP (Display Port Connector)	26
2.2.5 HDMI_1 & 2 (HDMI Connector).....	27
2.2.6 VGA (VGA Port)	28
2.2.7 COM1 (COM1 Port (RS-232/422/485 & RI/5V/12V))	29
2.2.8 JCOM1 (RI pin RI/5V/12V Select jumper for COM1 Port)	30

2.2.9	P12V_CPU (8-pin ATX 12V power connector (for CPU))	31
2.2.10	SYS_FAN2 (System Fan connector)	32
2.2.11	CPU_FAN (CPU Fan connector)	33
2.2.12	DIMM_A1, DIMM_A2, DIMM_B1, DIMM_B2 (DDR5 DIMM Sockets)	34
2.2.13	ATX (24-pin ATX main power connector)	35
2.2.14	SATA4, SATA5, SATA6, SATA7 (SATA 6Gb/s Connector)	36
2.2.15	CLR_CMOS (Clear CMOS jumper)	37
2.2.16	F_PANEL (Front panel header)	38
2.2.17	SYS_FAN1 (System Fan connector)	39
2.2.18	FUSB2_1, FUSB2_2 (USB 2.0 header)	40
2.2.19	FUSB30 (USB 3.2 Gen 1 header)	41
2.2.20	COM2, COM3, COM4, COM5, COM6 (Serial Port header)	42
2.2.21	JCOM2 (RJ pin RI/5V/12V Select jumper for COM2 Port)	43
2.2.22	GPIO_CNT (General Purpose input/output header)	44
2.2.23	F_AUDIO (Front panel audio header)	45
2.2.24	PCIEX4_2 (PCIe x4 (Gen3 x4) Slot)	46
2.2.25	PCIEX1_3 (PCIe x1 (Gen3 x1) Slot)	47
2.2.26	PCIEX16_2 (PCIe x16 (Gen4 x16) Slot)	48
2.2.27	PCIEX4_1 (PCIe x4 (Gen3 x4) Slot)	49
2.2.28	PCIEX1_2 (PCIe x1 (Gen3 x1) Slot)	50
2.2.29	PCIEX1_1 (PCIe x1 (Gen3 x1) Slot)	51
2.2.30	PCIEX16_1 (PCIe x16 (Gen4 x16) Slot)	52
2.2.31	AT_CN (AT/ATX mode select jumper)	53
2.2.32	M2M_1 (M.2 Slot, 2242/2280 M-Key)	54

2.2.33	M2M_2 (M.2 Slot, 2242/2280 M-Key)	55
2.2.34	M2E (M.2 Slot, 2230 E-Key)	56

Chapter 3 – BIOS 57

3.1	Introduction	58
3.2	The Main Menu.....	59
3.3	Advanced	60
3.3.1	AMT Configuration	61
3.3.2	TPM Configuration.....	65
3.3.3	CPU Configuration	67
3.3.4	SATA Configuration	68
3.3.5	IT8786 Super IO Configuration	69
3.3.6	Hardware Monitor	70
3.3.7	S5 RTC Wake Settings	71
3.3.8	Network Stack Configuration.....	72
3.3.9	NVMe Configuration.....	73
3.3.10	Offboard SATA Controller Configuration	74
3.3.11	Digital IO Port Configuration	75
3.3.12	Tls Auth Configuration	76
3.3.13	Intel(R) Ethernet Controller I226-LM - (MAC:10:FF:E0:39:4D:5C) (MAC address may varied based on different motherboard).....	77
3.3.14	Intel(R) Ethernet Controller I226-V - (MAC:10:FF:E0:39:4D:5D) (MAC address may varied based on different motherboard).....	78
3.4	Chipset	79
3.5	Security	81

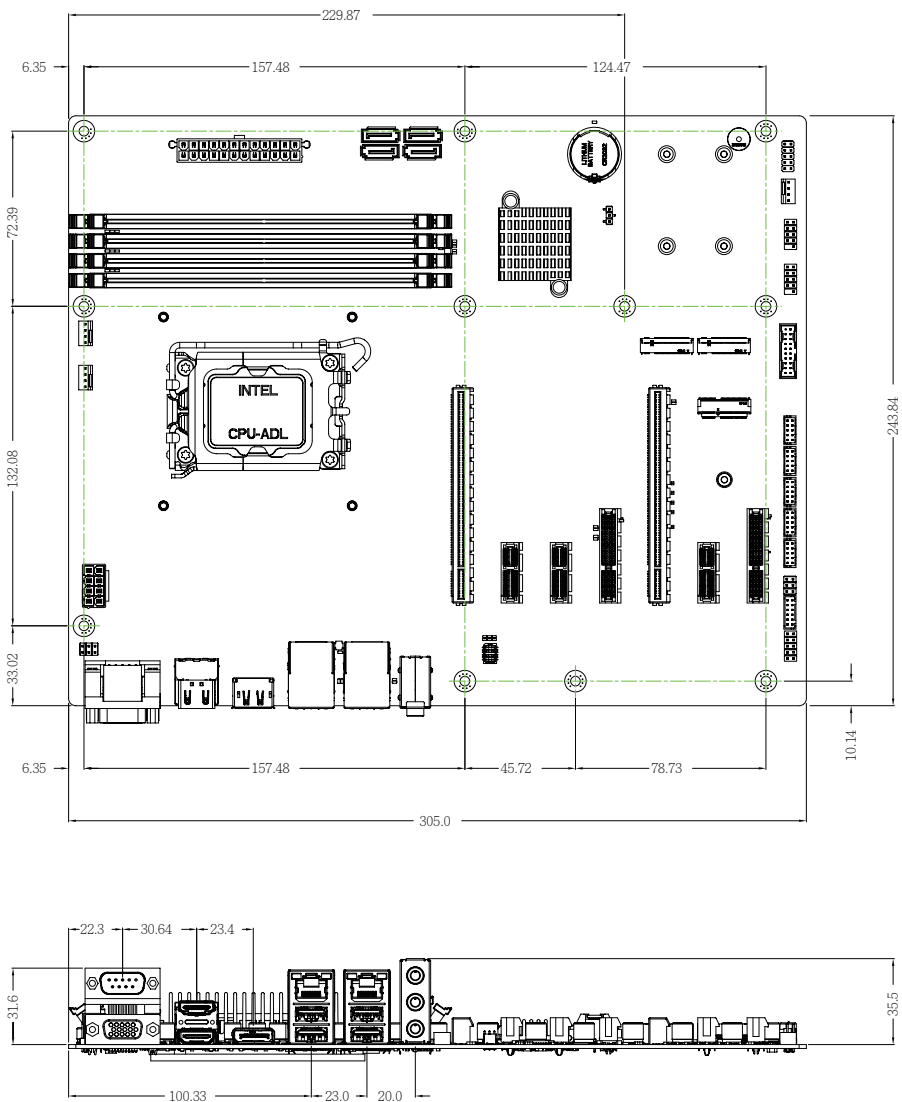
3.6 Boot..... 84

3.7 Save & Exit 85

3.8 MEBx 86

Chapter 1

Chapter1 - Product Specifications



1.1 Specifications

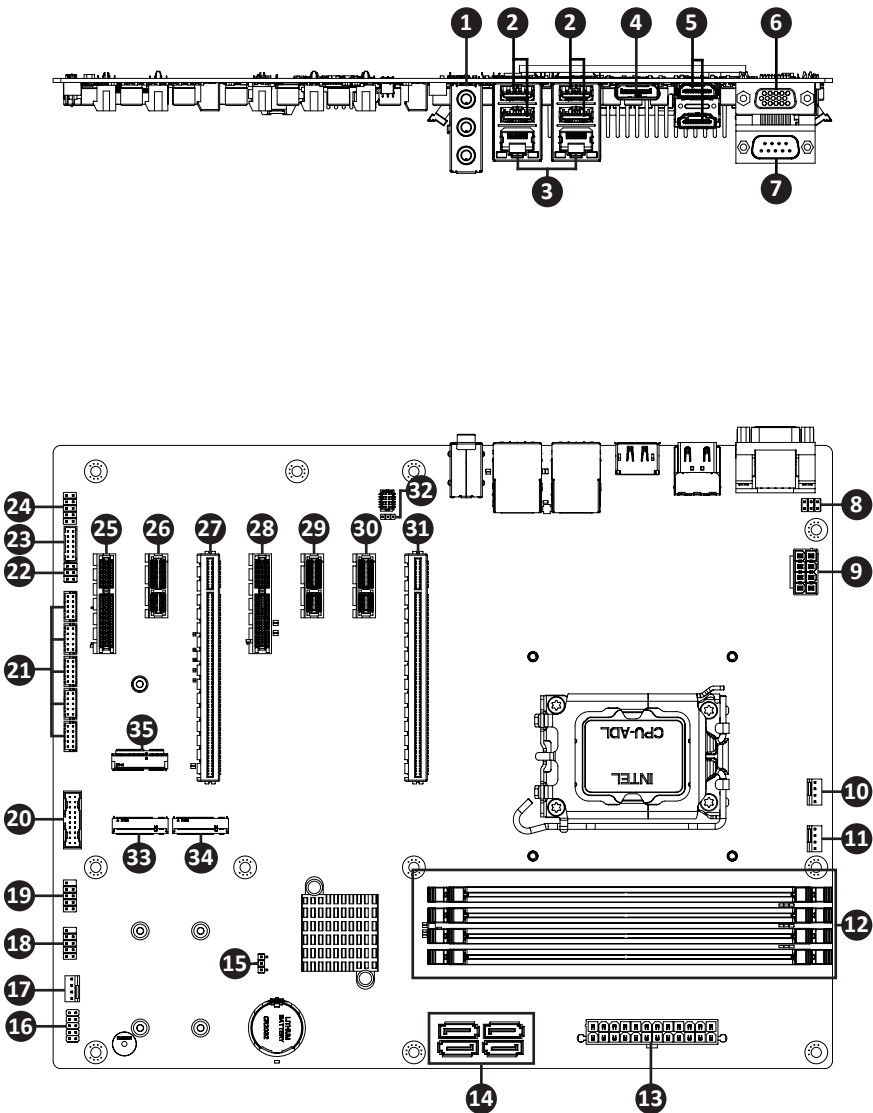
Motherboard	ATX-Q670B (MQ670BX)
Form Factor	ATX 305W x 244D (mm)
CPU	Support for 14th/13th/12th Generation Intel® Core™ i9/i7/i5/i3, Pentium® & Celeron® processors in the LGA1700 package TDP under 125W
Socket	1 x LGA 1700
Chipset	Intel® Q670 Chipset
Memory	4 x DDR5 DIMM sockets, Max. Capacity 128 GB Support Dual channel DDR5 4800 MHz memory modules
Ethernet	2 x 2.5GbE LAN Ports (Intel® I226V & I226LM)
Video	Integrated Graphics Processor – depends on CPU: 2 x HDMI 2.0 port, supporting a maximum resolution of 4096x2160 @60Hz 1 x DP port, supporting a maximum resolution of 4096x2160 @60Hz 1 x D-sub port, supporting a maximum resolution of 1920x1080 @60Hz (4 independent display outputs)
Audio	Realtek® ALC897
Storage	4 x SATA 6Gb/s Ports
RAID	RAID 0/1/5/10
Expansion Slots	1 x PCIe x16 (Gen 4x16)(PCIEX16_1) * The PCIEX16_1 slot shares bandwidth with the PCIEX16_2 slot. * The PCIEX16_1 slot operates at up to x8 mode when a device is installed in the PCIEX16_2 slot. 1 x PCIe x16 (Gen 4x8)(PCIEX16_2) 2 x PCIe x4 (Gen 3x4) 3 x PCIe x1 (Gen 3x1) 1 x 2280/2242 M.2 M-Key (PCIe Gen4x4, SATA 6Gb/s)(M2M_1) 1 x 2280/2242 M.2 M-Key (PCIe Gen4x4)(M2M_2) 1 x 2230 M.2 E-Key

Motherboard	ATX-Q670B (MQ670BX)
Internal I/O	1 x 24-pin ATX main power connector 1 x 8-pin ATX 12V power connector 1 x CPU fan header 2 x System fan headers 1 x Front panel header 1 x Front panel audio header 4 x USB 2.0 headers 2 x USB 3.2 Gen 1 headers 1 x COM header (RS-232/422/485 & RI/5V/12V) 4 x COM headers (RS-232) 1 x GPIO (8 bits) & SMBus header 1 x Clear CMOS jumper 1 x Buzzer 1 x AT/ATX mode select jumper
Rear I/O	3 x Audio Jacks (Line in, Line out, Mic in) 1 x COM Port (RS-232/422/485 & RI/5V/12V) 2 x HDMI 1 x Display Port 1 x VGA 2 x RJ45 LAN Ports 4 x USB 3.2 Gen 1
TPM	Onboard TPM 2.0 security chip INFINEON SLB9670VQ2.0
OS Compatibility	Windows 10/11 (x64)
Operating Properties	Operating temperature: 0°C to 60°C Operating humidity: 0-90% (non-condensing) Non-operating temperature: -40°C to 85°C Non-operating humidity: 0%-95% (non-condensing)

Chapter 2

Chapter 2 – Hardware Information

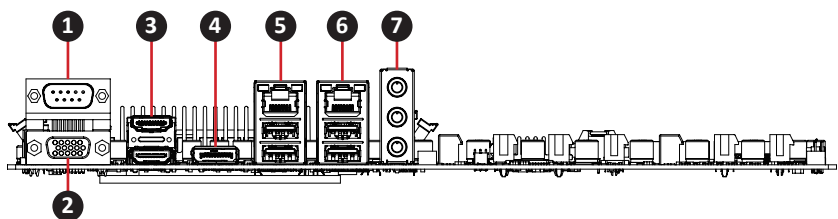
2.1 Jumpers and Connectors



No	Code	Description
1	AUDIO	3 x Audio Jacks (Line in, Line out, Mic in)
2	USB3_LAN1	USB 3.2 Gen 1 Connector
3	USB3_LAN2	2.5GbE LAN Port
4	DP	Display Port Connector
5	HDMI_1 & 2	HDMI Connector
6	VGA	VGA Port
7	COM1	COM1 Port (RS-232/422/485 & RI/5V/12V)
8	JCOM1	RI pin RI/5V/12V Select jumper for COM1 Port
9	P12V_CPU	8-pin ATX 12V power connector (for CPU)
10	SYS_FAN2	System fan connector
11	CPU_FAN	CPU fan connector
12	DIMM_A1, DIMM_A2 DIMM_B1, DIMM_B2	DDR5 DIMM Sockets x 4
13	ATX	24-pin ATX main power connector
14	SATA4, SATA5 SATA6, SATA7	SATA 6Gb/s Connector x 4
15	CLR_CMOS	Clear CMOS jumper
16	F_PANEL	Front panel header
17	SYS_FAN1	System Fan connector
18	FUSB2_2	USB 2.0 header
19	FUSB2_1	USB 2.0 header
20	FUSB30	USB 3.2 Gen 1 header
21	COM2, COM3, COM4, COM5, COM6	Serial Port header COM2 : RS-232/422/485 & RI/5V/12V COM3, COM4, COM5, COM6 : RS-232
22	JCOM2	RI pin RI/5V/12V Select jumper for COM2 Port

No	Code	Description
23	GPIO_CNT	General Purpose input/output header
24	F_AUDIO	Front panel audio header
25	PCIEX4_2	PCIe x4 (Gen3 x4) slot
26	PCIEX1_3	PCIe x1 (Gen3 x1) slot
27	PCIEX16_2	PCIe x16 (Gen4 x16) Slot
28	PCIEX4_1	PCIe x4 (Gen3 x4) Slot
29	PCIEX1_2	PCIe x1 (Gen3 x1) Slot
30	PCIEX1_1	PCIe x1 (Gen3 x1) Slot
31	PCIEX16_1	PCIe x16 (Gen4 x16) Slot
32	AT_CN	AT/ATX mode select jumper
33	M2M_1	M.2 slot, 2242/2280 M-key
34	M2M_2	M.2 slot, 2242/2280 M-key
35	M2E	M.2 slot, 2230 E-key

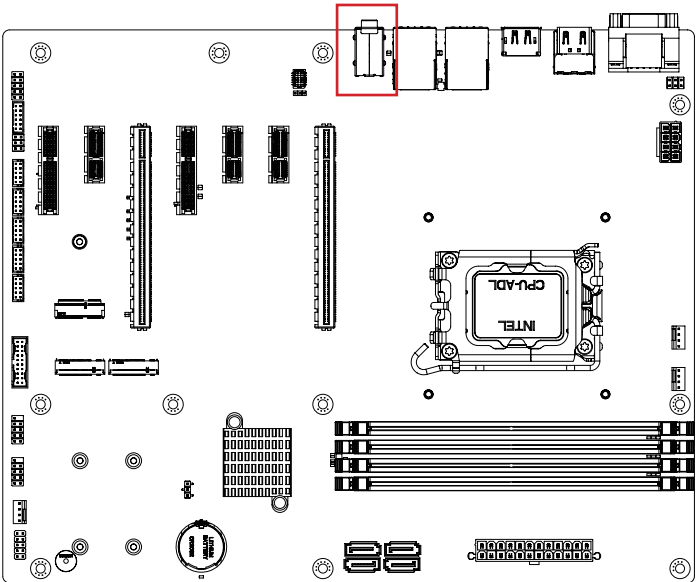
2.2.1 Rear I/O Connector



No	Code	Description
1	COM1	COM1 Port (RS-232/422/485 & RI/5V/12V)
2	VGA	VGA Port
3	HDMI_1 & 2	HDMI connector
4	DP	Display port
5	USB3_LAN1	1 x 2.5GbE LAN Port (top) 2 x USB 3.2 Gen 1 (bottom)
6	USB3_LAN2	1 x 2.5GbE LAN Port (top) 2 x USB 3.2 Gen 1 (bottom)
7	AUDIO	3 x Audio Jacks (Line in, Line out, Mic in)

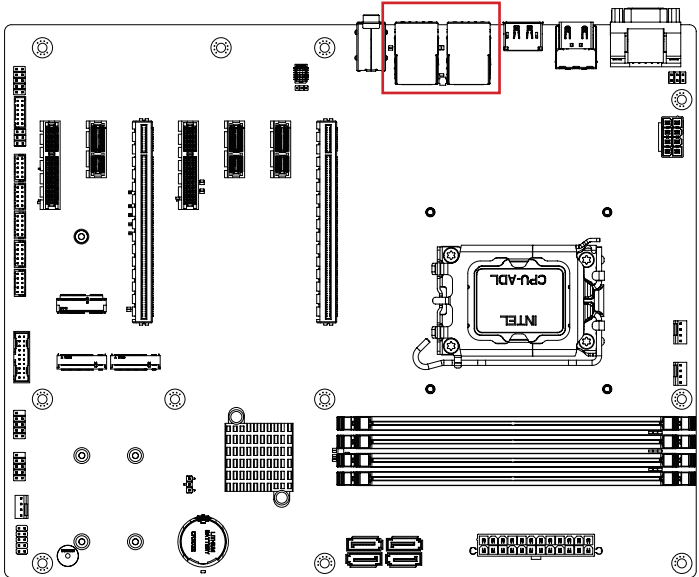
2.2.2 AUDIO (Line in, Line out, Mic in)

1

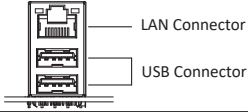


2.2.3 USB3_LAN1, USB3_LAN2 (USB 3.2 Gen 1 + 2.5GbE LAN Connector)

2 3



USB & LAN Connector



USB Connector			
Pin No.	Definition	Pin No.	Definition
1	5V	10	5V
2	D1n	11	D0n
3	D1p	12	D0p
4	GND	13	GND
5	USB3_RX1n	14	USB3_RX2n
6	USB3_RX1p	15	USB3_RX2p
7	GND	16	GND
8	USB3_TX1n	17	USB3_TX2n
9	USB3_TX1p	18	USB3_TX2p

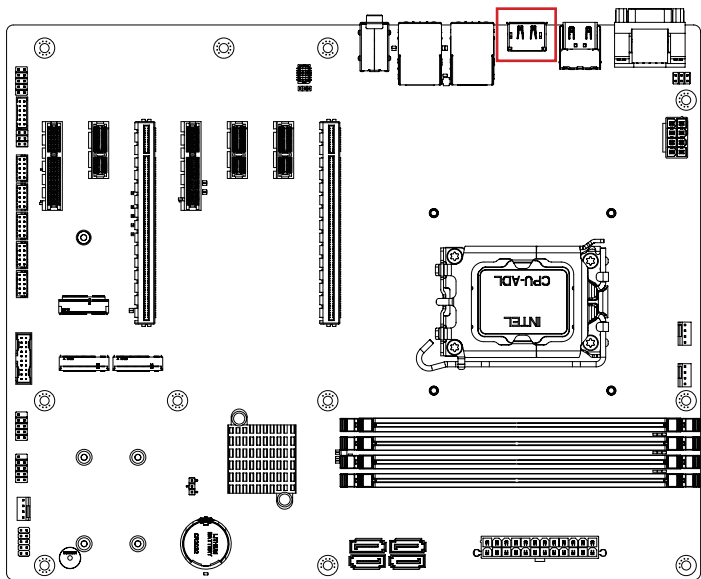
LAN Connector			
Pin No.	Definition	Pin No.	Definition
1	TX1+	4	TX3+
2	TX1-	5	TX3-
3	TX2+	7	TX4+
6	TX2-	8	TX4-
State		Description	
Orange On		2.5Gbps data rate	
Green On		1Gbps data rate	
Off		100M&10Mbps data rate	

ATX Motherboard

ATX-Q670B (MQ670BX)

2.2.4 DP (Display Port Connector)

4



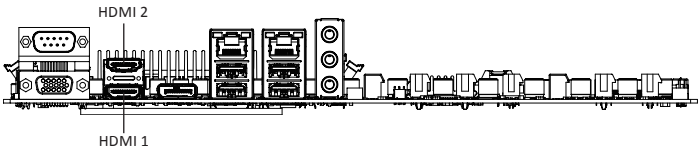
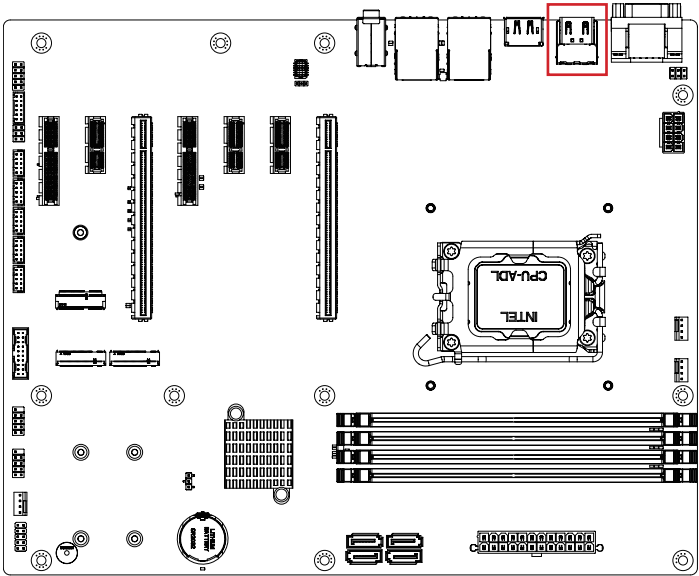
DP Connector



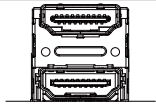
Pin No.	Definition	Pin No.	Definition
1	TX0p	11	GND
2	GND	12	TX3n
3	TX0n	13	GND
4	TX1p	14	GND
5	GND	15	AUXp
6	TX1n	16	GND
7	TX2p	17	AUXn
8	GND	18	Hot Plug Detect
9	TX2n	19	3.3V
10	TX3p	20	3.3V

2.2.5 HDMI_1 & 2 (HDMI Connector)

5



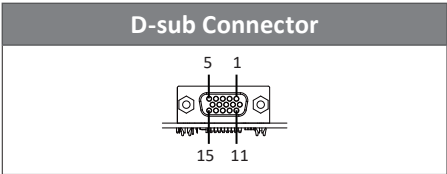
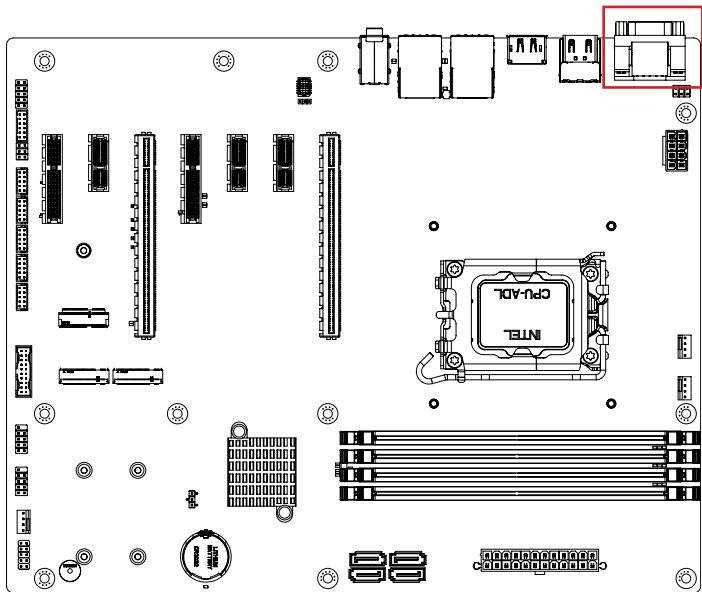
HDMI Connector



Pin No.	Definition	Pin No.	Definition
1	TX2p	11	GND
2	GND	12	CLKn
3	TX2n	13	NC
4	TX1p	14	NC
5	GND	15	SCL
6	TX1n	16	SDA
7	TX0p	17	GND
8	GND	18	5V
9	TX0n	19	Hot Plug Detect
10	CLKp		

2.2.6 VGA (VGA Port)

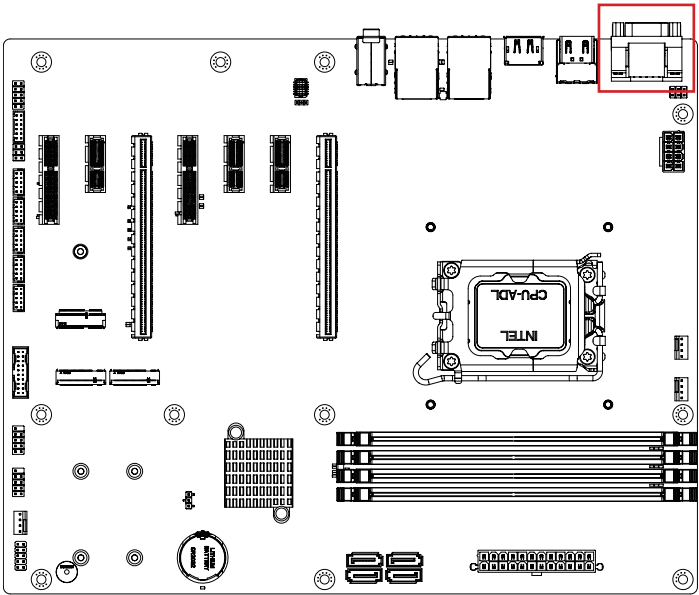
6



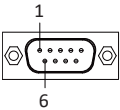
Pin No.	Definition	Pin No.	Definition
1	Red	9	5V
2	Green	10	GND
3	Blue	11	NC
4	NC	12	DDCSDA
5	GND	13	HSYNC
6	GND	14	VSYNC
7	GND	15	DDCSCL
8	GND		

2.2.7 COM1 (COM1 Port (RS-232/422/485 & RI/5V/12V))

7



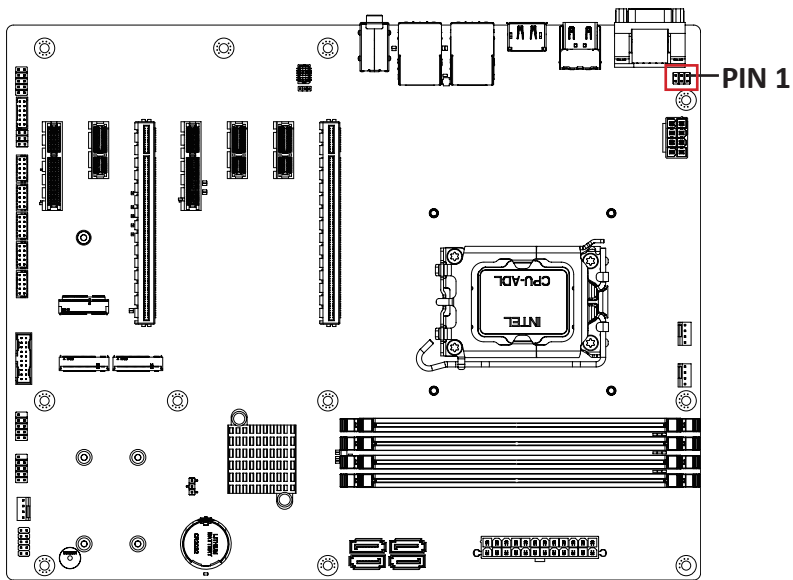
Serial Port Connector



Pin No.	RS-232	RS-422 Full Duplex	RS-485 Half Duplex
1	DCD	TXD-	D-
2	RXD	TXD+	D+
3	TXD	RXD+	—
4	DTR	RXD-	—
5	GND		
6	DSR	—	—
7	RTS	—	—
8	CTS	—	—
9	RI	—	—

2.2.8 JCOM1 (RI pin RI/5V/12V Select jumper for COM1 Port)

8

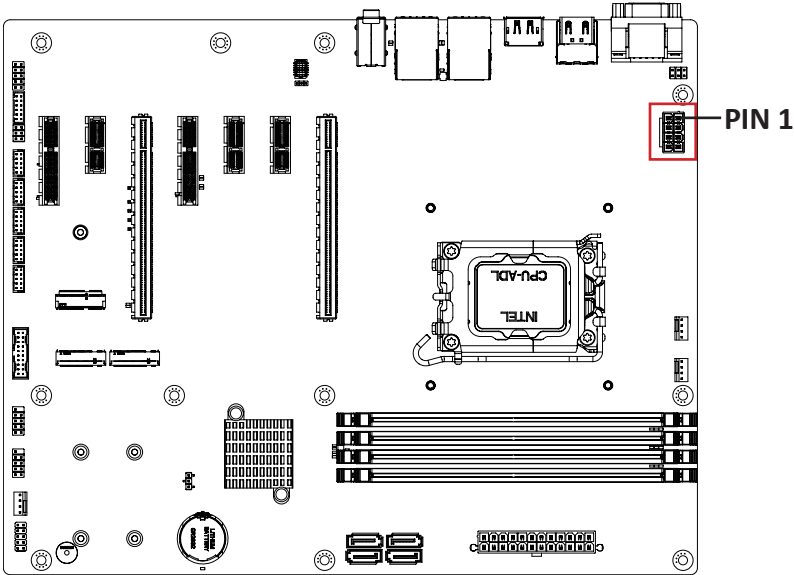


JCOM1 header	
JCOM1 Jumper	
	1-2 Close: 5V (Power COM)
	3-4 Close: RI (Stand COM)
	5-6 Close: 12V (Power COM)

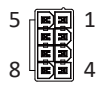
Connector PN	Vendor
210-92-03GB01	PINREX
PH06R53BAZ000	HORNGTONG
Connector type	
2x3pin header, pitch 2.54mm	

2.2.9 P12V_CPU (8-pin ATX 12V power connector (for CPU))

9



ATX 12V Connector



Connector PN

740-96-085B61

Vendor

PINREX

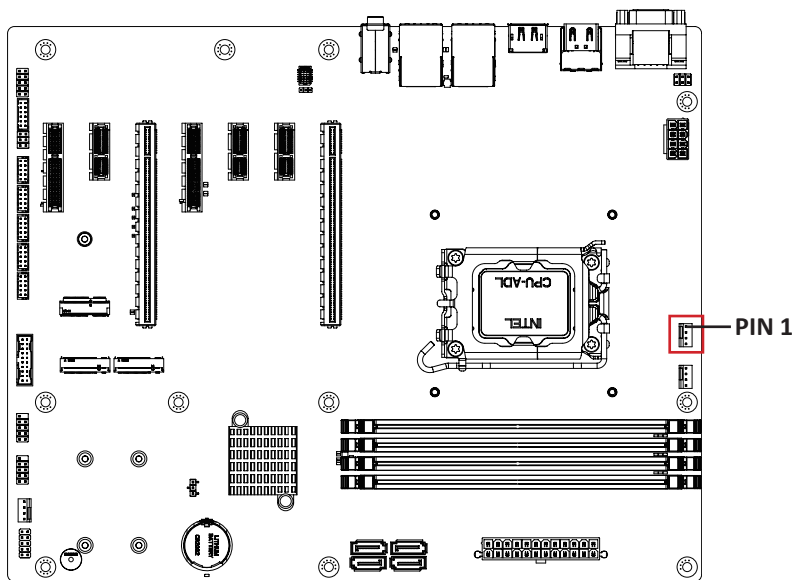
Connector type

2x4pin header, pitch 4.2mm

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

2.2.10 SYS_FAN2 (System Fan connector)

10



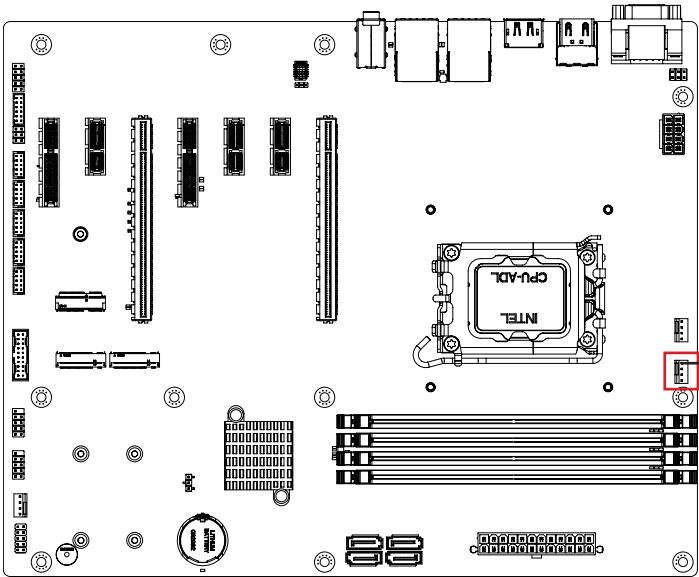
System FAN Connector	
	1 4

Connector PN	Vendor
744-81-045R11	PINREX
Connector type	
1x4pin header, pitch 2.54mm	

Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed Control

2.2.11 CPU_FAN (CPU Fan connector)

11



PIN 1

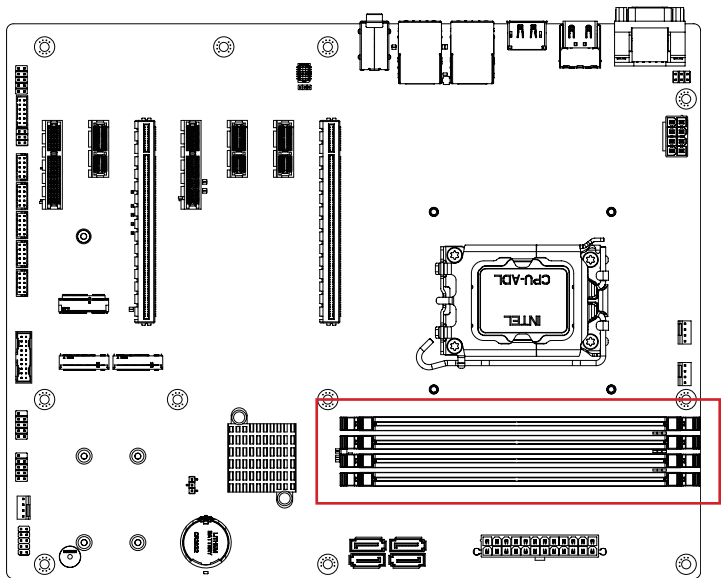
CPU FAN Connector	
	1 4

Connector PN	Vendor
744-81-045W11	PINREX
Connector type	
1x4pin header, pitch 2.54mm	

Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed Control

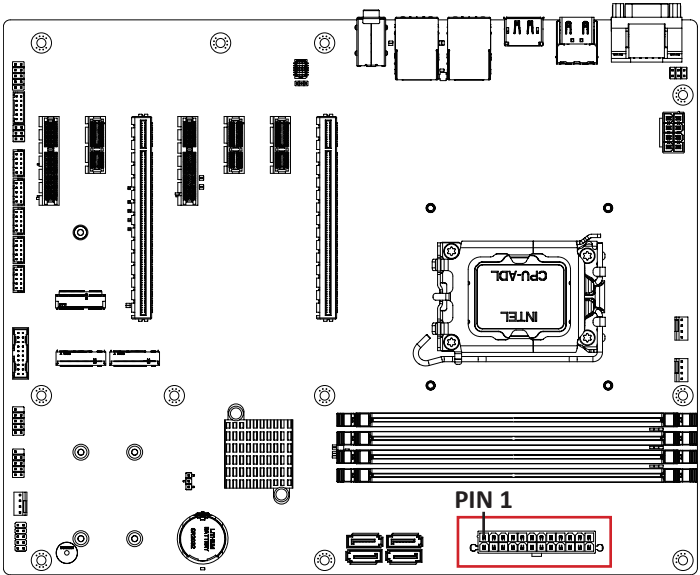
2.2.12 DIMM_A1, DIMM_A2, DIMM_B1, DIMM_B2 (DDR5 DIMM Sockets)

12



2.2.13 ATX (24-pin ATX main power connector)

13



ATX power Connector			
1			23
2			24

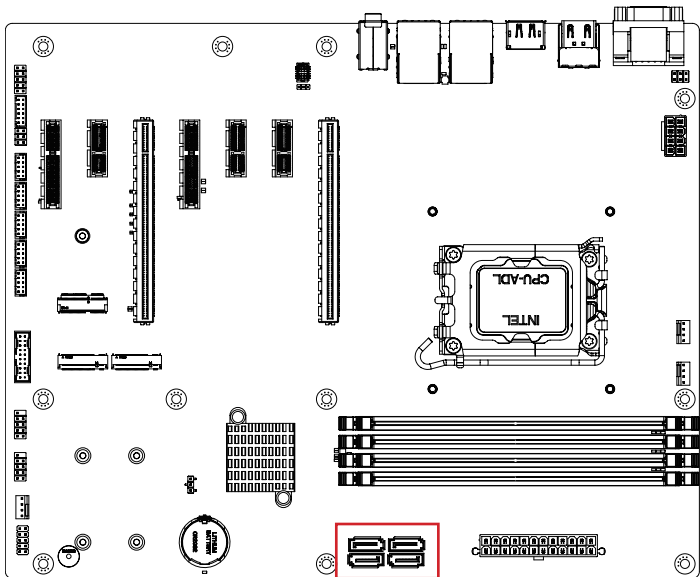
Pin No.	Definition	Pin No.	Definition
1	3.3V	13	3.3V
2	3.3V	14	-12V
3	GND	15	GND
4	5V	16	PS_ON
5	GND	17	GND
6	5V	18	GND
7	GND	19	GND
8	Power Good	20	NC
9	5VSB	21	5V
10	12V	22	5V
11	12V	23	5V
12	3.3V	24	GND

Connector PN	Vendor
740-96-245B70	PINREX

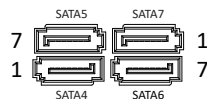
Connector type
2x12pin header, pitch 4.2mm

2.2.14 SATA4, SATA5, SATA6, SATA7 (SATA 6Gb/s Connector)

14



SATA 6Gb/s Connector

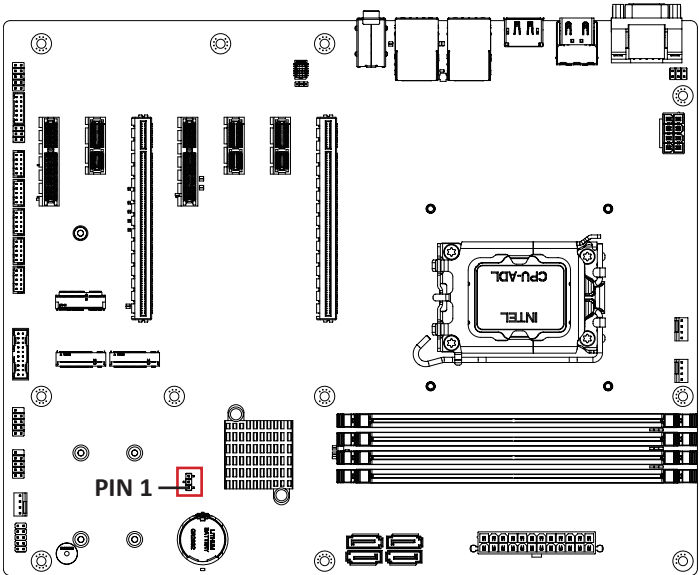


Connector PN	Vendor
WATM-07ABNB2BAUW3	WINWIN
770-83-07SW19	PINREX

Pin No.	Definition
1	GND
2	TXp
3	TXn
4	GND
5	RXn
6	RXp
7	GND

2.2.15 CLR_CMOS (Clear CMOS jumper)

15



Clear CMOS jumper

The diagram shows a 3-pin header with pins numbered 1, 2, and 3. Pin 1 is the leftmost pin, pin 2 is the middle pin, and pin 3 is the rightmost pin.

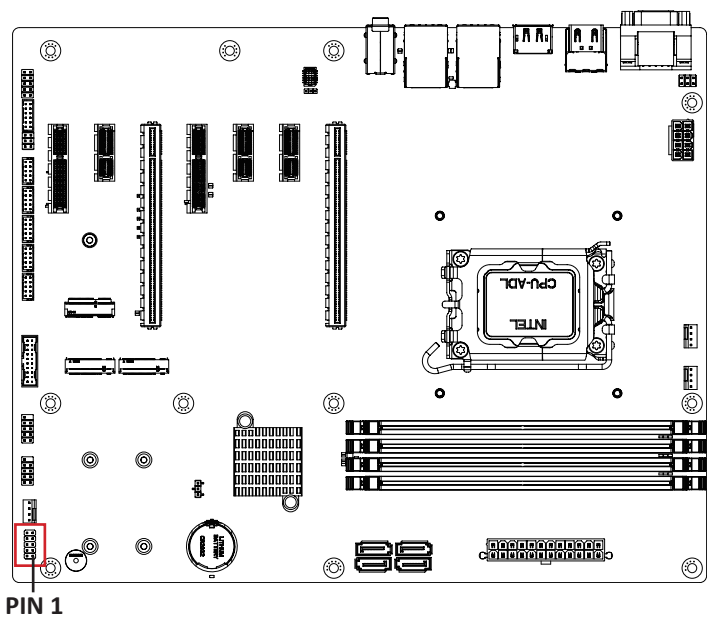
Connector PN	Vendor
212-91-03GBE00K	PINREX

Connector type
1x3pin header, pitch 2.54mm

Pin No.	Definition
1	NC
2	GND
3	Clear CMOS
1-2 Close: Normal Operator (Default setting)	
2-3 Close: Clear CMOS data	

2.2.16 F_PANEL (Front panel header)

16



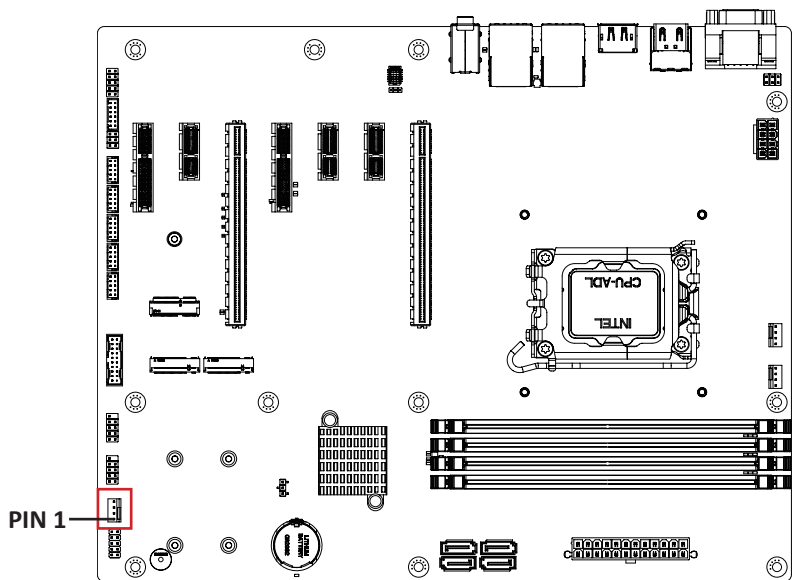
Front panel header	
10	9
2	1

Connector PN	Vendor
210-92-05GW5W	PINREX
Connector type	
2x5pin header, pitch 2.54mm	

Pin No.	Definition
1	HDD LED+
2	Power LED+
3	HDD LED-
4	Power LED-
5	GND
6	Power button+
7	Reset button
8	Power button-
9	No connect
10	No pin

2.2.17 SYS_FAN1 (System Fan connector)

17



System FAN Connector



Connector PN

744-81-045R11

Vendor

PINREX

Connector type

1x4pin header, pitch 2.54mm

Pin No.

Definition

1

GND

2

12V

3

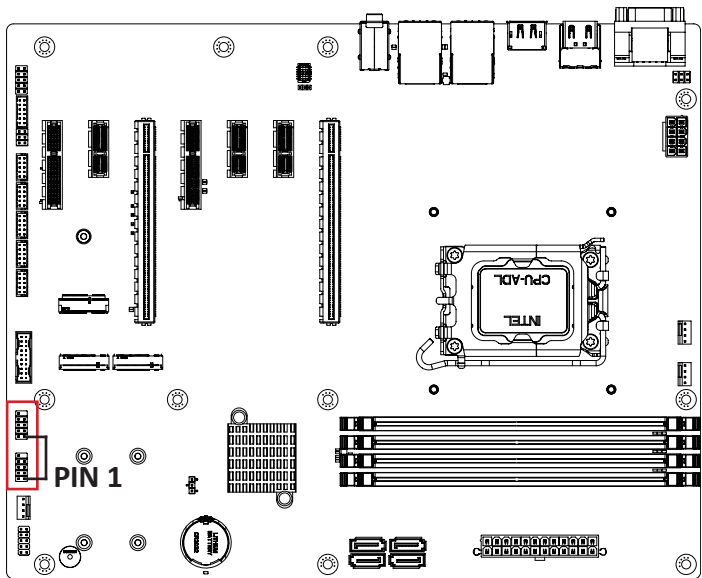
Detect

4

Speed Control

2.2.18 FUSB2_1, FUSB2_2 (USB 2.0 header)

18 19



USB 2.0 Header		
10		9
		
		
		
2		1

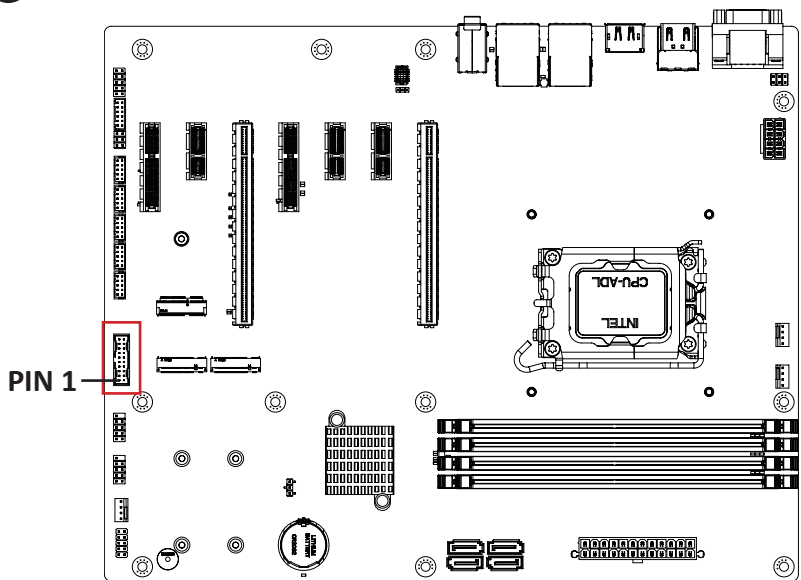
Connector PN	Vendor
210-92-05GB04	PINREX
PH10R53BAZ009	HORNGTONG

Connector type
2x5pin header, pitch 2.54mm

Pin No.	Definition
1	5V
2	5V
3	D2n
4	D1n
5	D2p
6	D1p
7	GND
8	GND
9	No Pin
10	No Connect

2.2.19 FUSB30 (USB 3.2 Gen 1 header)

20



USB 3.2 Gen 1 header



Pin No.	Definition
1	5V
2	RX1n
3	RX1p
4	GND
5	TX1n
6	TX1p
7	GND
8	D1n
9	D1p
10	OC
11	D2p
12	D2n
13	GND

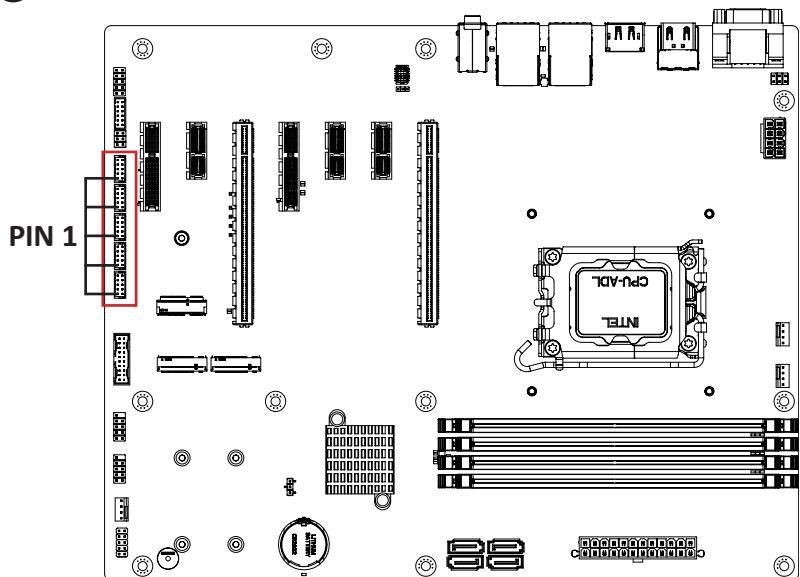
Pin No.	Definition
14	TX2p
15	TX2n
16	GND
17	RX2p
18	RX2n
19	5V
20	NC

Connector PN	Vendor
52X-80-20GU65	PINREX
WUIR-19A9N4BU3W	WINWIN

Connector type
2x10pin header, pitch 2.0mm

2.2.20 COM2, COM3, COM4, COM5, COM6 (Serial Port header)

21



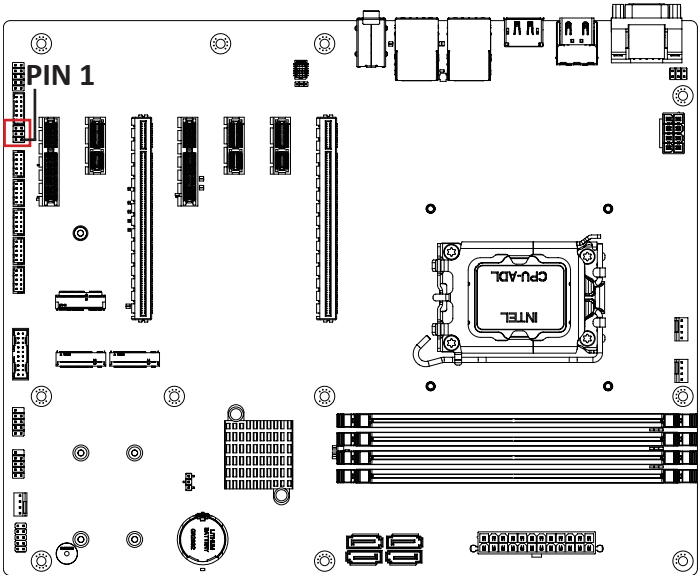
Serial port Header			
Pin No.	RS-232	RS-422 Full Duplex	RS-485 Half Duplex
1	RXD	TXD+	D+
2	DCD	TXD-	D-
3	DTR	RXD-	—
4	TXD	RXD+	—
5	DSR	—	—
6	GND	—	—
7	CTS	—	—
8	RTS	—	—
9	No Connect	—	—
10	RI/5V/12V	—	—

Connector PN	Vendor
725-81-10TW00	PINREX
A2004WV-2X05P46	JOINT-TECH
Connector type	
2x5pin header, pitch 2.0mm	

Note :
COM2 : Support RS-232/422/485 & RI/5V/12V
For RI/5V/12V jumper setting, please see P. 43
COM3, COM4, COM5, COM6 : Support RS-232 only

2.2.21 JCOM2 (RI pin RI/5V/12V Select jumper for COM2 Port)

22



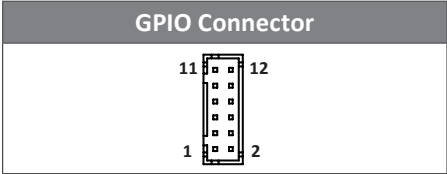
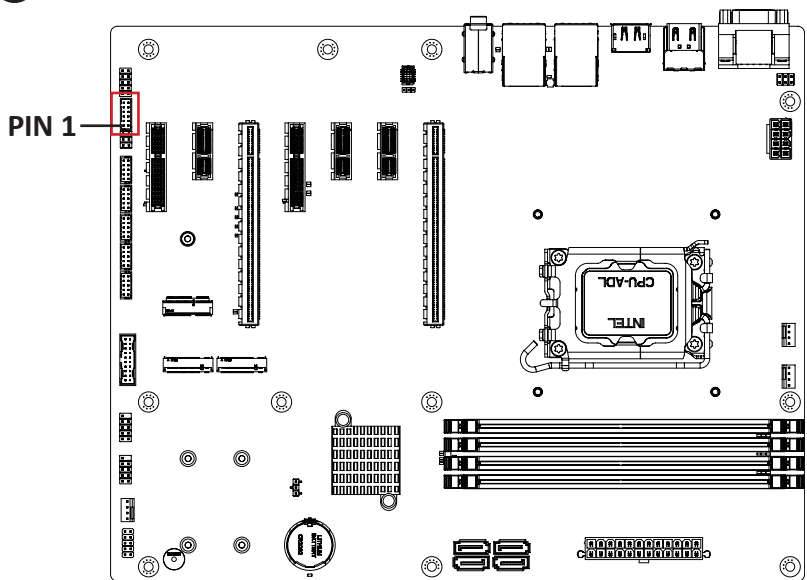
JCOM2 Jumper Select	
	1-2 Close: 5V (Power COM)
	3-4 Close: RI (Stand COM)
	5-6 Close: 12V (Power COM)

Connector PN	Vendor
210-92-03GB01	PINREX
PH06R53BAZ000	HORNGTONG

Connector type
2x3pin header, pitch 2.54mm

2.2.22 GPIO_CNT (General Purpose input/output header)

23



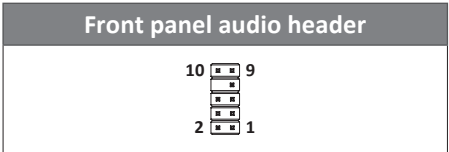
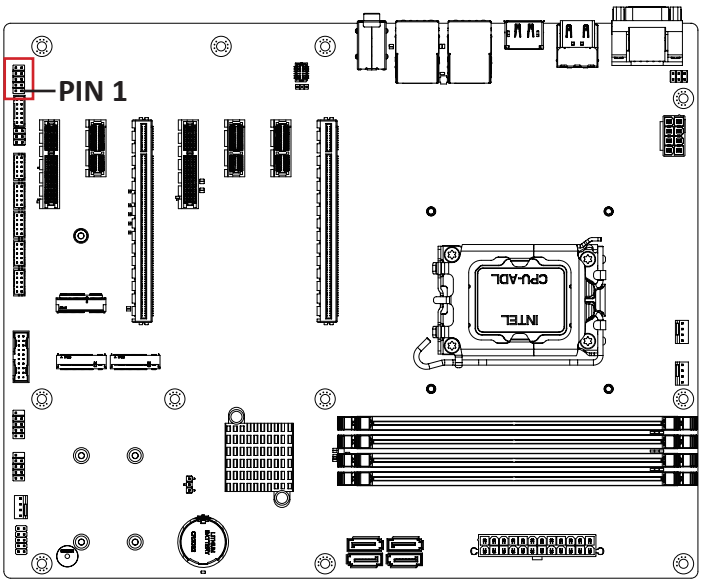
Connector PN	Vendor
725-81-12TW00	PINREX
A2004WV-2X06P46	JOINT-TECH

Connector type
2x6pin header, pitch 2.0mm

Pin No.	Definition
1	GPIO-output_1
2	GPIO-input_1
3	GPIO-output_2
4	GPIO-input_2
5	GPIO-output_3
6	GPIO-input_3
7	GPIO-output_4
8	GPIO-input_4
9	SMBus Clock
10	SMBus DATA
11	5V
12	GND

2.2.23 F_AUDIO (Front panel audio header)

24



Connector PN	Vendor
210-92-05GE05	PINREX

Connector type
2x5pin header, pitch 2.54mm

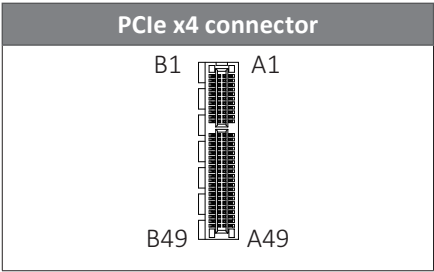
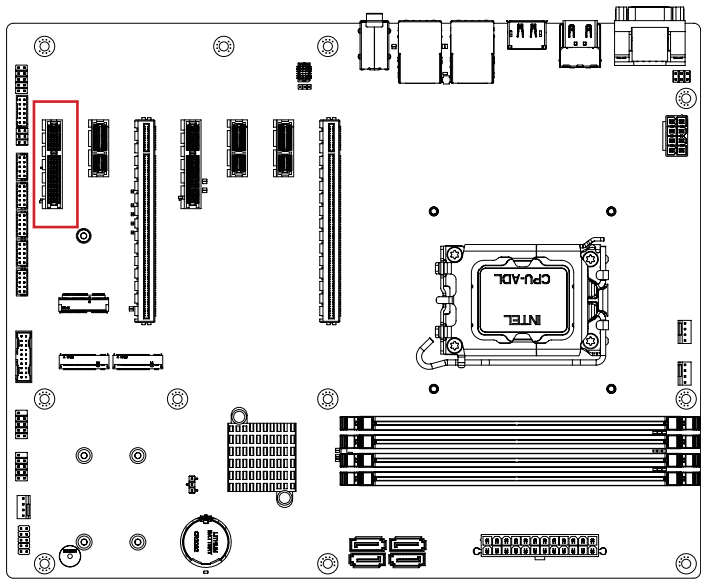
Pin No.	Definition
1	MIC_LEFT
2	GND
3	MIC_RIGHT
4	Detect
5	LINE_RIGHT
6	GND
7	JACKSENSE Detect
8	No connect
9	LINE_LEFT
10	GND

ATX Motherboard

ATX-Q670B (MQ670BX)

2.2.24 PCIEX4_2 (PCIe x4 (Gen3 x4) Slot)

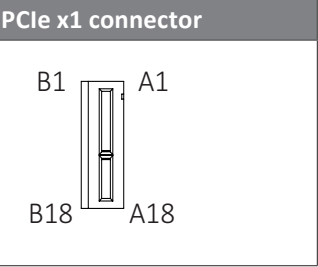
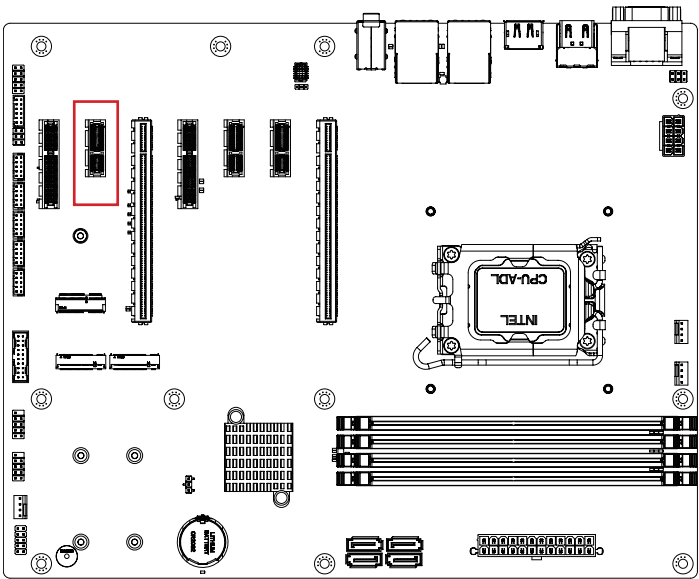
25



Connector PN	Vendor
WPES-064AN41B22UWS	WINWIN

2.2.25 PCIEX1_3 (PCIe x1 (Gen3 x1) Slot)

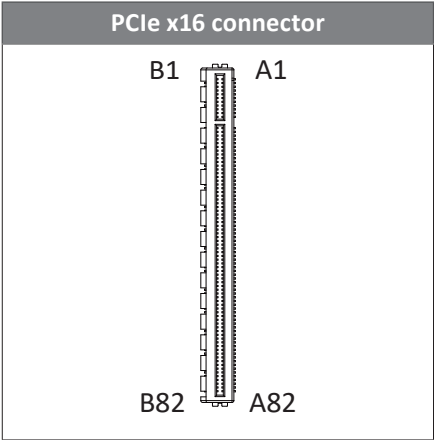
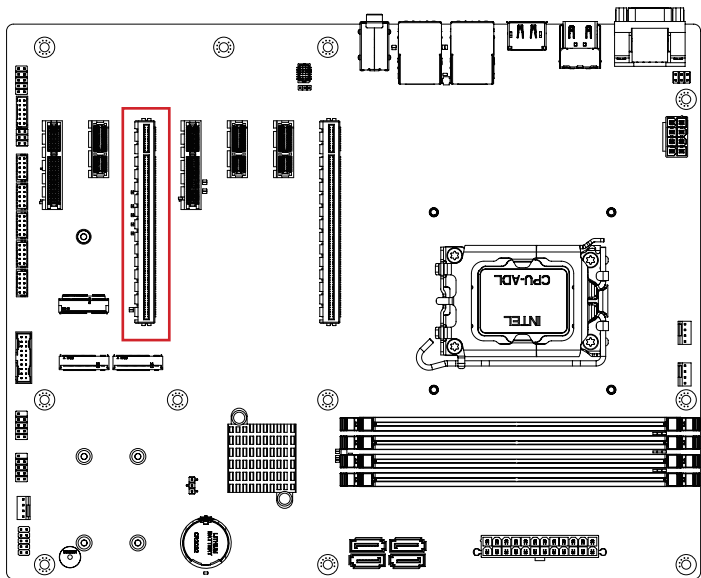
26



Connector PN	Vendor
2EG01817-D2D-DF	FOXCONN
AAA-PCI-003-K01	LOTES

2.2.26 PCIEX16_2 (PCIe x16 (Gen4 x16) Slot)

27



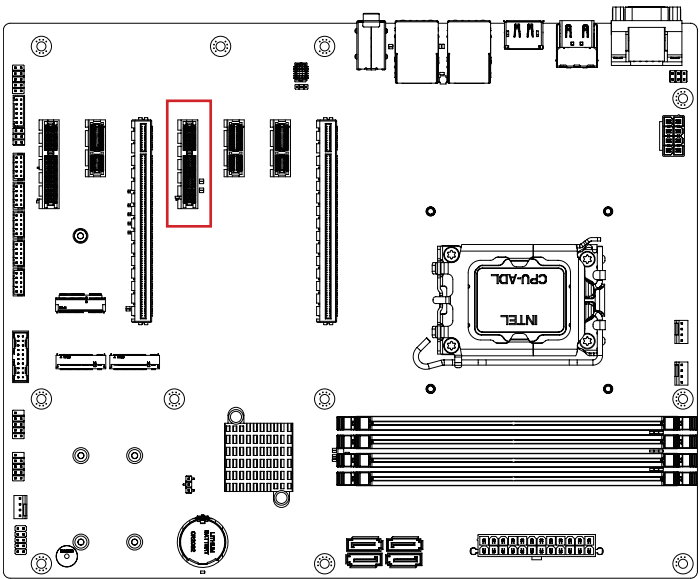
Connector PN	Vendor
10144667-123ZOLF	FCI

* Below are the possible configurations :

code name	PCIEX16_1	PCIEX16_2
Config. 1	Signal at x16	0
Config. 2	Signal at x8	Signal at x8

2.2.27 PCIEX4_1 (PCIe x4 (Gen3 x4) Slot)

28



PCIe x4 connector

B1 A1

B49 A49



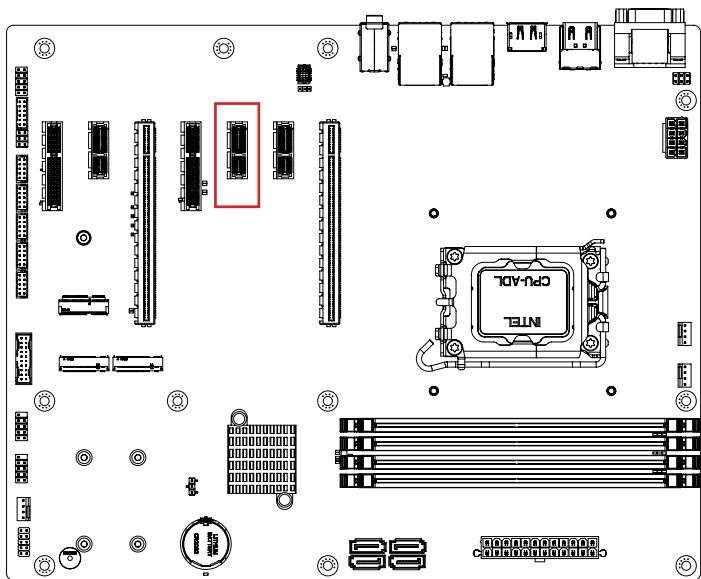
Connector PN	Vendor
WPES-064AN41B22UWS	WINWIN

ATX Motherboard

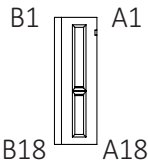
ATX-Q670B (MQ670BX)

2.2.28 PCIEX1_2 (PCIe x1 (Gen3 x1) Slot)

29



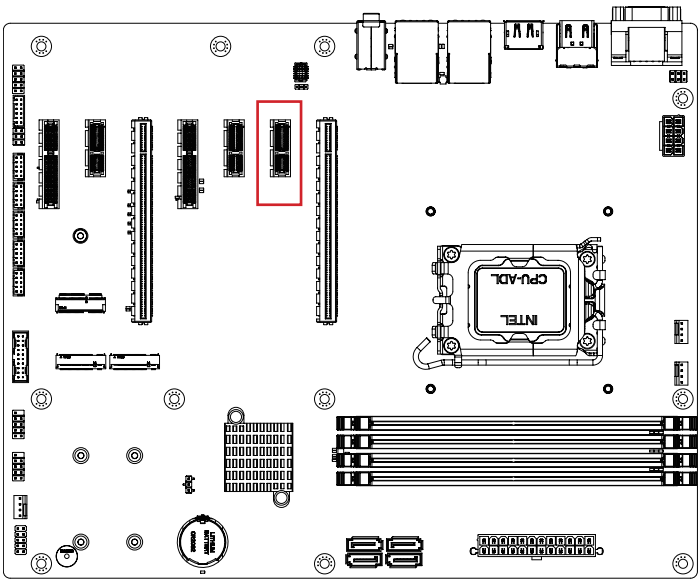
PCIe x1 connector



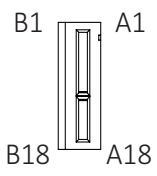
Connector PN	Vendor
2EG01817-D2D-DF	FOXCONN
AAA-PCI-003-K01	LOTES

2.2.29 PCIEX1_1 (PCIe x1 (Gen3 x1) Slot)

30



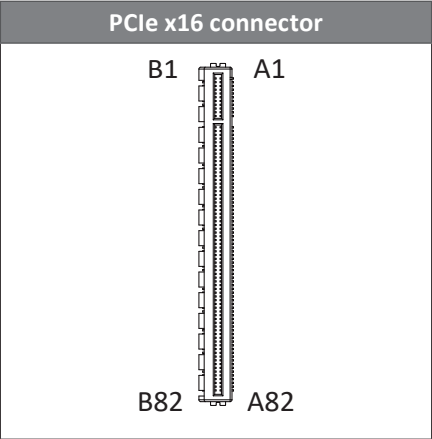
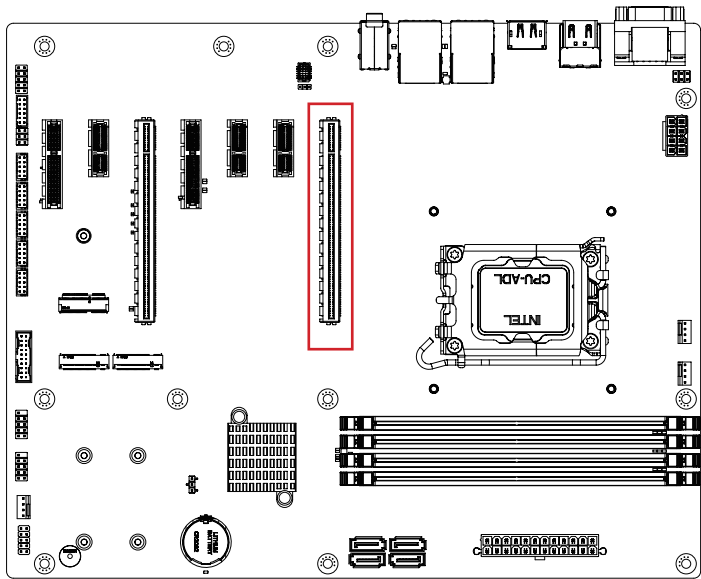
PCIe x1 connector



Connector PN	Vendor
2EG01817-D2D-DF	FOXCONN
AAA-PCI-003-K01	LOTES

2.2.30 PCIEX16_1 (PCIe x16 (Gen4 x16) Slot)

31



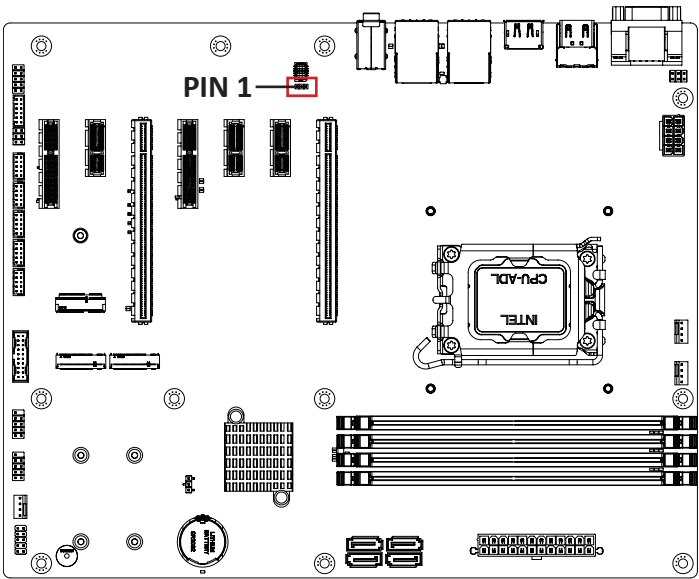
Connector PN	Vendor
10144667-123Z0LF	FCI

* Below are the possible configurations :

code name	PCIEX16_1	PCIEX16_2
Config. 1	Signal at x16	0
Config. 2	Signal at x8	Signal at x8

2.2.31 AT_CN (AT/ATX mode select jumper)

32



AT/ATX mode select jumper



1

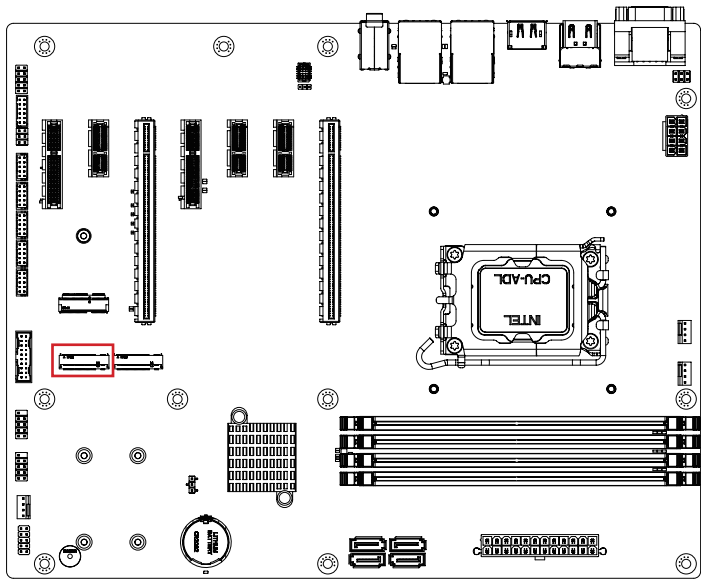
Pin No.	Definition
1	AT MODE
2	Detect
3	ATX MODE
Jumper setting	
1-2 Close : AT mode.	
2-3 Close : ATX mode.(Default setting)	

Connector PN	Vendor
220-96-03GB01	PINREX
220-96-03GB001K	PINREX

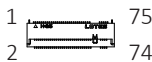
Connector type
1x3pin header, pitch 2.0mm

2.2.32 M2M_1 (M.2 Slot, 2242/2280 M-Key)

33



M.2 M Key Connector



Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE3 RXn	6	NC
7	PCIE3 RXp	8	NC
9	GND	10	SSD LED
11	PCIE3 TXn	12	3.3V
13	PCIE3 TXp	14	3.3V
15	GND	16	3.3V
17	PCIE2 RXn	18	3.3V
19	PCIE2 RXp	20	NC
21	GND	22	NC
23	PCIE2 TXn	24	NC
25	PCIE2 TXp	26	NC
27	GND	28	NC
29	PCIE1 RXn	30	NC
31	PCIE1 RXp	32	NC
33	GND	34	NC
35	PCIE1 TXn	36	NC

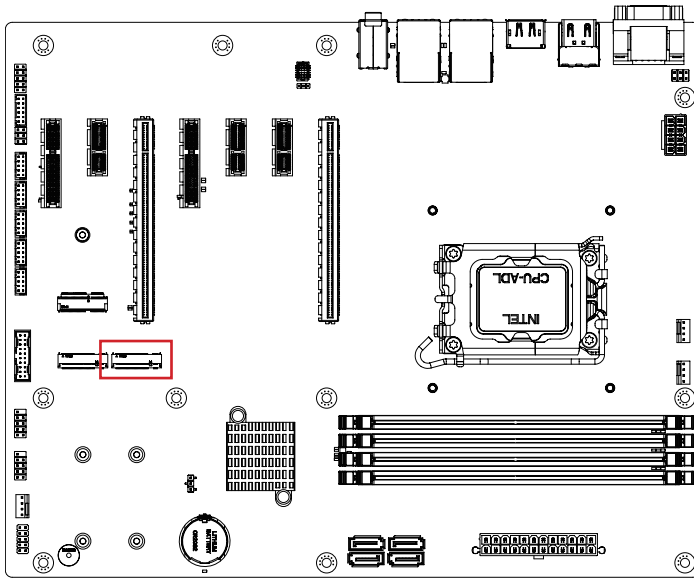
Pin No.	Definition	Pin No.	Definition
37	PCIE1 TXp	38	NC
39	GND	40	NC
41	SATA0/PCIE0 RXp	42	NC
43	SATA0/PCIE0 RXn	44	NC
45	GND	46	NC
47	SATA0/PCIE0 TXn	48	NC
49	SATA0/PCIE0 TXp	50	Reset
51	GND	52	Clock Request
53	Clockp	54	Wakeup
55	Clockn	56	NC
57	GND	58	NC

Pin No.	Definition	Pin No.	Definition
67	NC	68	SUSCLK
69	Detect	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

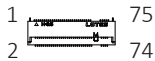
Connector PN	Vendor
80159-8521	BELLWETHER
APCI0096-P002A	LOTES

2.2.33 M2M_2 (M.2 Slot, 2242/2280 M-Key)

34



M.2 M Key Connector



Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE3 RXn	6	NC
7	PCIE3 RXp	8	NC
9	GND	10	SSD LED
11	PCIE3 TXn	12	3.3V
13	PCIE3 TXp	14	3.3V
15	GND	16	3.3V
17	PCIE2 RXn	18	3.3V
19	PCIE2 RXp	20	NC
21	GND	22	NC
23	PCIE2 TXn	24	NC
25	PCIE2 TXp	26	NC
27	GND	28	NC
29	PCIE1 RXn	30	NC
31	PCIE1 RXp	32	NC
33	GND	34	NC
35	PCIE1 TXn	36	NC

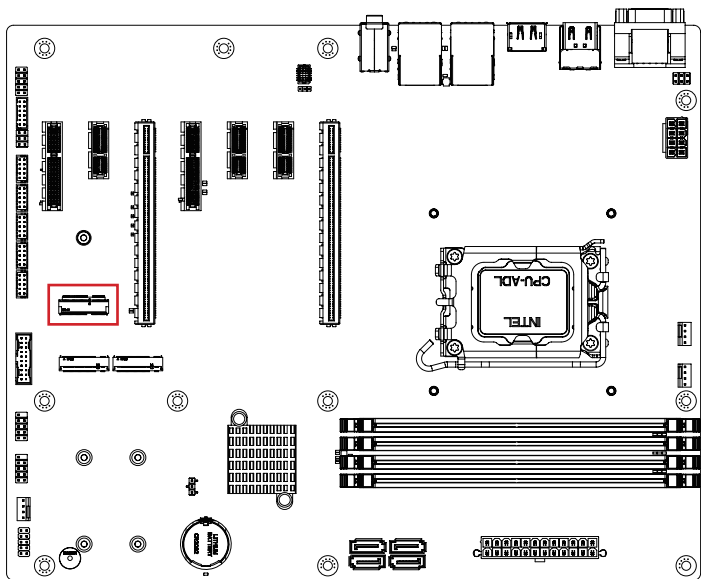
Pin No.	Definition	Pin No.	Definition
37	PCIE1 TXp	38	NC
39	GND	40	NC
41	PCIE0 RXp	42	NC
43	PCIE0 RXn	44	NC
45	GND	46	NC
47	PCIE0 TXn	48	NC
49	PCIE0 TXp	50	Reset
51	GND	52	Clock Request
53	Clockp	54	Wakeup
55	Clockn	56	NC
57	GND	58	NC

Pin No.	Definition	Pin No.	Definition
67	NC	68	SUSCLK
69	Detect	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

Connector PN	Vendor
80159-8521	BELLWETHER
APCI0096-P002A	LOTES

2.2.34 M2E (M.2 Slot, 2230 E-Key)

35



M.2 E Key Connector



Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	D1p	4	3.3V
5	D1n	6	NC
7	GND	8	NC
9	NC	10	NC
11	NC	12	NC
13	GND	14	NC
15	NC	16	NC
17	NC	18	GND
19	GND	20	NC
21	NC	22	NC
23	NC		
33	GND	32	NC
35	PCIE_TXp	34	NC
37	PCIE_TXn	36	NC

39	GND	38	CL_Reset
41	PCIE_RXp	40	CL_DATA
43	PCIE_RXn	42	CL_Clock
45	GND	44	NC
47	PCIE_CLOCKp	46	NC
49	PCIE_CLOCKn	48	NC
51	GND	50	SUSCLK
53	PCIE Clock Request	52	Reset
55	PCIE wake up	54	BT_Disable
57	GND	56	WLAN_Disable
59	NC	58	NC
61	NC	60	NC
63	GND	62	NC
65	NC	64	NC
67	NC	66	NC
69	GND	68	NC
71	NC	70	NC
73	NC	72	3.3V
75	GND	74	3.3V

Connector PN	Vendor
AS0BC21-S40BE-7H	FOXCONN
80152-4221	BELLWETHER

Chapter 3

Chapter 3 – BIOS

3.1 Introduction

BIOS (Basic input/output system) provides hardware detailed information and boot-up options, which include firmware to control, set-up and test all hardware settings. Therefore, BIOS is the communication bridge between OS/application software and hardware.

3.1.1 How to Entering into BIOS menu

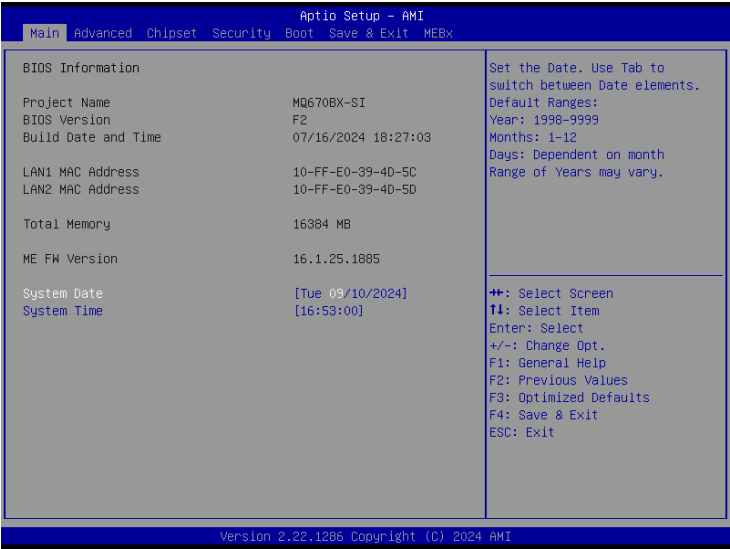
Once the system is power on, press the key as soon as possible to access into BIOS Setup program.

3.1.2 Function Keys to setup in BIOS Setup program

Function keys	Description
→←	Select Screen
↑↓	Select Item
Enter	Execute command or enter the submenu
+	Increase the numeric value or make changes
—	Decrease the numeric value or make changes
F1	General Help
F2	Previous Values
F3	Load Optimized Defaults Settings
F4	Save changes & Exit the BIOS Setup program
ESC	Exit the BIOS Setup program

3.2 The Main Menu

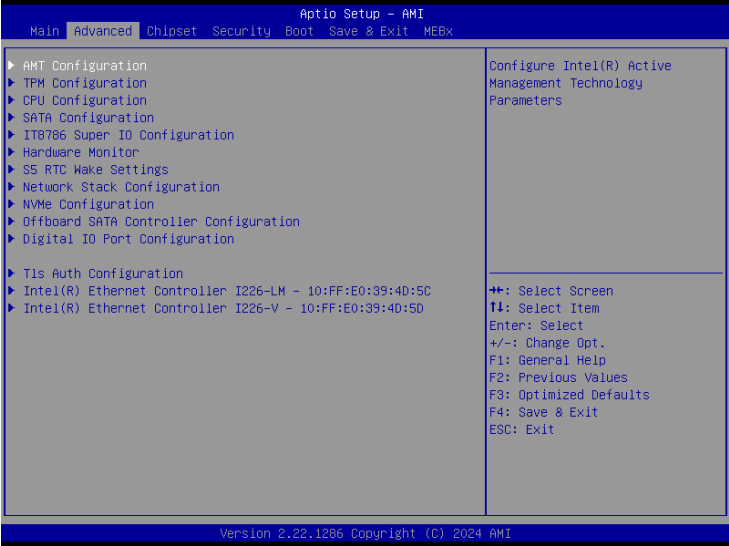
The main menu shows the basic system information.
Use arrow keys to move among the items.



Items	Description
Project Name	Shows Project name information
BIOS Version	Shows the BIOS version of the system
Build Date and Time	Shows the Build Date and Time when the BIOS was created.
LAN1 MAC Address	Shows LAN 1 MAC Address information
LAN2 MAC Address	Shows LAN 2 MAC Address information
Total Memory	Shows the total memory size of the installed memory
ME FW version	Shows ME firmware version
System Date	Set the Date for the system (Format : Week - Month - Day - Year)
System Time	Set the time for the system (Format : Hour - Minute - Second)

3.3 Advanced

The Advanced menu is to configure the functions of hardware settings through submenu. Use arrow keys to move among the items, and press <Enter> to access into the related submenu.



3.3.1 AMT Configuration



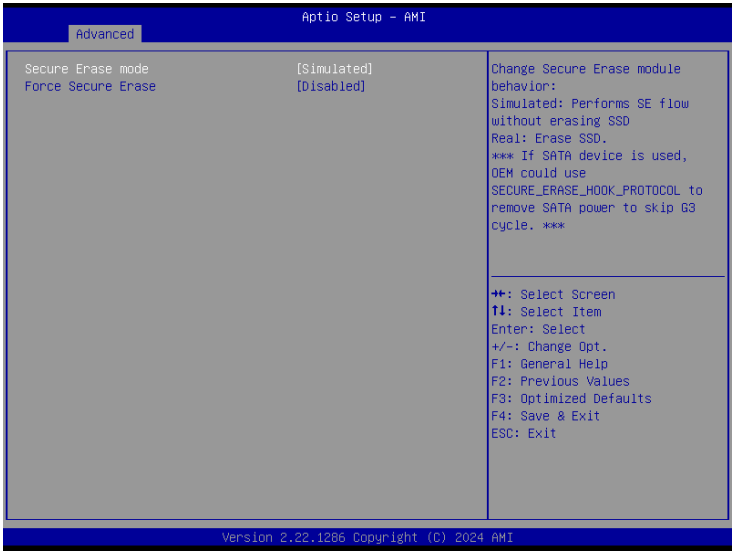
Item	Description
USB Provisioning of AMT	Inserting a specially formatted USB drive into a system, to let the other system remotely control. Disabled : Disables USB Provisioning of AMT Enabled : Enables USB Provisioning of AMT (Default setting)
MAC Pass Through	Disabled : Disables MAC Pass Through function (Default setting) Enabled : Enables MAC Pass Through function
Activate Remote Assistance Process	Trigger CIRA boot Disabled : Disables TPM feature (Default setting) Enabled : Enables TPM feature
Unconfigure ME	To Un-configure ME without password. Disabled : Disables Unconfigure ME (Default settings) Enabled : Enables Unconfigure ME

ASF Congifuration



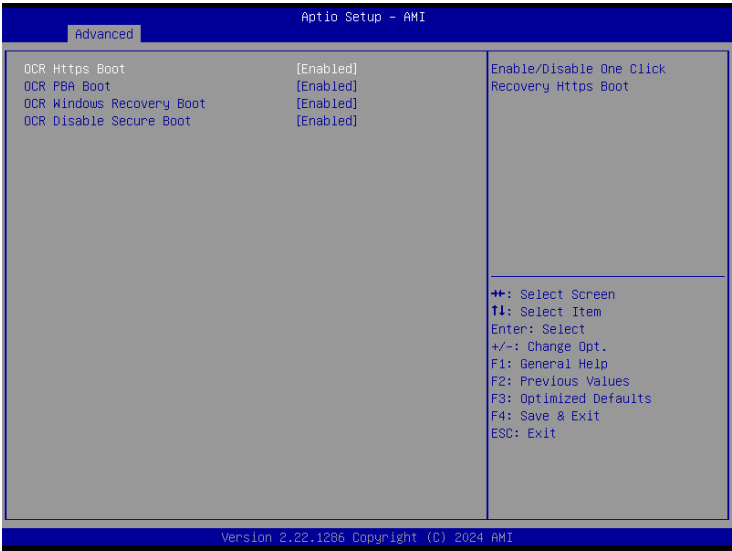
Item	Description
PET Progress	Choose to receive PET events or not Disabled : Disables PET Progress Enabled : Enables PET Progress (Default setting)
WatchDog	Choose to enables watchdog timer or not Disabled : Disables watchdog Timer (Default setting) Enabled : Enables watchdog Timer
OS Timer	Sets OS Watchdog Timer.
BIOS Timer	Sets BIOS Timer.
ASF Sensors Table	Disabled : Disables ASF Sensors Table (Default setting) Enabled : Enables ASF Sensors Table

Secure Erase Configuration



Item	Description
Secure Erase mode	Choose to enables secure erase mode or not. Simulated : Performs SE flow without erasing SSD (Default setting) Real : Erase SSD
Force Secure Erase	Force Secure Erase on next boot. Disabled : Disables Force Secure Erase (Default setting) Enabled : Enables Force Secure Erase

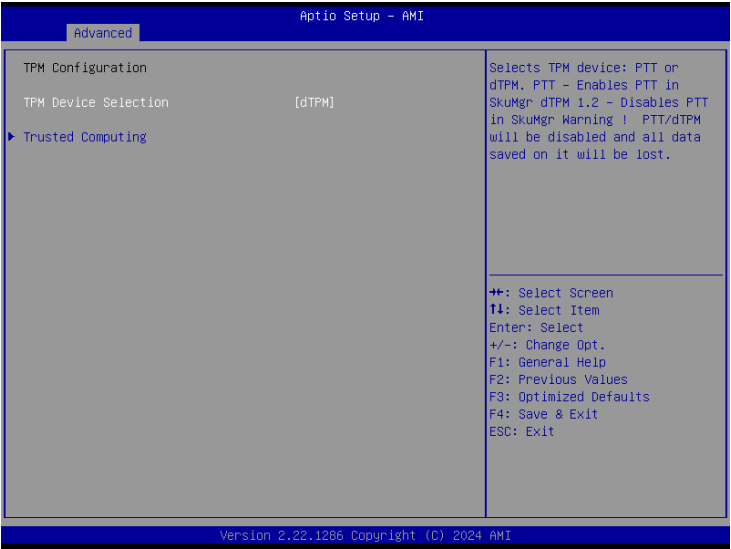
One Click Recovery (OCR) Configuration



Item	Description
OCR Https Boot	Enabled : Enables One Click Recovery Https Boot. (Default setting) Disabled : Disables One Click Recovery Https Boot.
OCR PBA Boot	Enabled : Enables One Click Recovery PBA Boot. (Default setting) Disabled : Disables One Click Recovery PBA Boot.
OCR Windows Recovery Boot	Enabled : Enables One Click Recovery Windows recovery boot. (Default setting) Disabled : Disables One Click Recovery Windows recovery boot.
OCR Disable Secure Boot	Allows CSME to request Secureboot to be disabled for One Click Recovery. Enabled : Enables One Click Recovery disable Secure Boot function. (Default setting) Disabled : Disables One Click Recovery disable Secure Boot function.

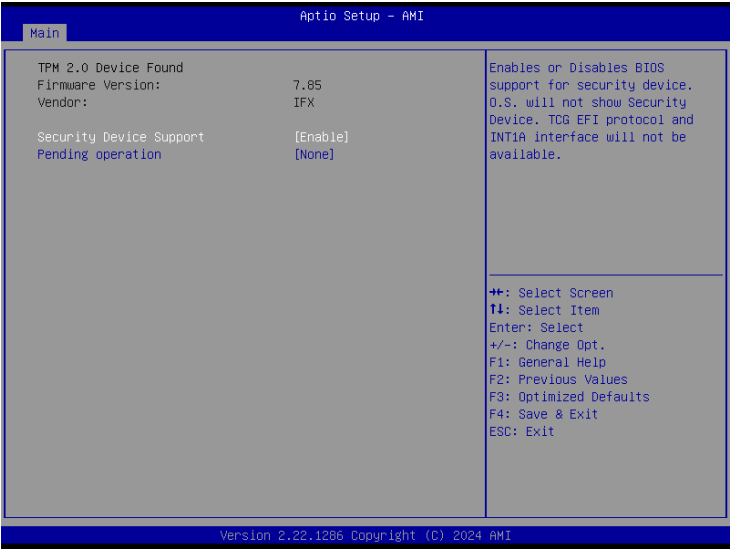
3.3.2 TPM Configuration

Use TPM Configuration submenu to choose TPM interface.



Item	Description
TPM Device Selection	PTT : Internal TPM dTPM : External TPM (When using External TPM module or having TPM chip on MB) (Default setting)

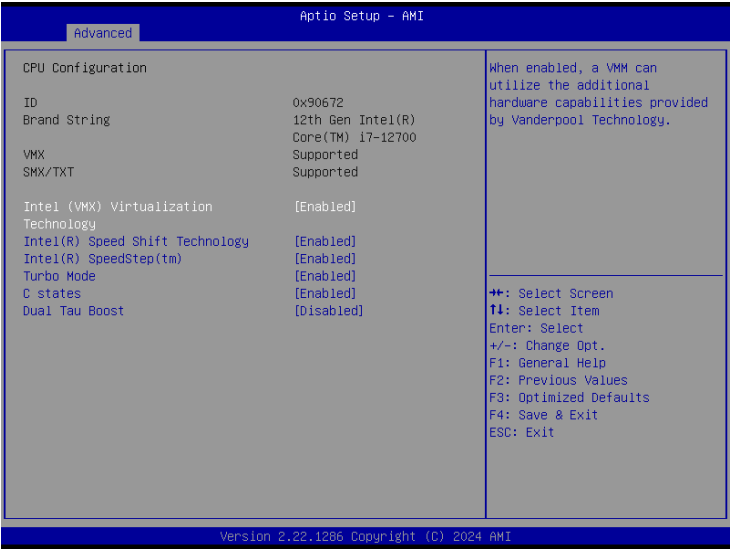
Trusted Computing : Shows TPM information, and TPM module configuration setting.



Item	Description
Security Device Support	Enabled : Enables TPM feature (Default setting) Disabled : Disables TPM feature
Pending operation	None : No execution will be conducted (Default setting) TPM clear : Set to clear data on TPM

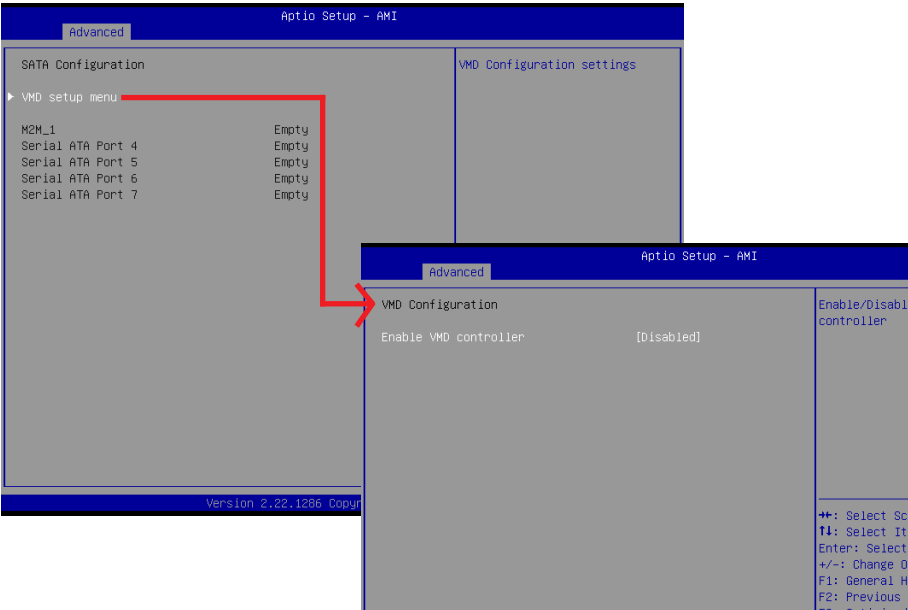
3.3.3 CPU Configuration

This submenu shows detailed CPU informations.



Item	Description
Intel (VMX) Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. Enabled : Enables Intel Virtualization Technology (Default setting) Disabled : Disables Intel Virtualization Technology
Intel(R) Speed Shift Technology	To speed up CPU frequency transition time from basic frequency to maximum frequency. Enabled : Enables Intel(R) Speed Shift Technology Interrupt control (Default setting) Disabled : Disables Intel(R) Speed Shift Technology Interrupt control
Intel(R) SpeedStep(tm)	According to Intel CPU loading, Intel SpeedStep Technology will automatically adjust the CPU voltage and core frequency to decrease heat and power consumption for power saving. Enabled : Enables Intel SpeedStep Technology (Default setting) Disabled : Disables Intel SpeedStep Technology
Turbo Mode	Enabled : Enables Turbo Mode (Default setting) Disabled : Disables Turbo Mode
C states	Command CPU to enter into low power consumption mode when CPU is under idle mode. Enabled : Enables CPU C states function (Default setting) Disabled : Disables CPU C states function
Dual Tau Boost	To optimize CPU performance. Enabled : Enables Dual Tau Boost function Disabled : Disables Dual Tau Boost function (Default setting)

3.3.4 SATA Configuration



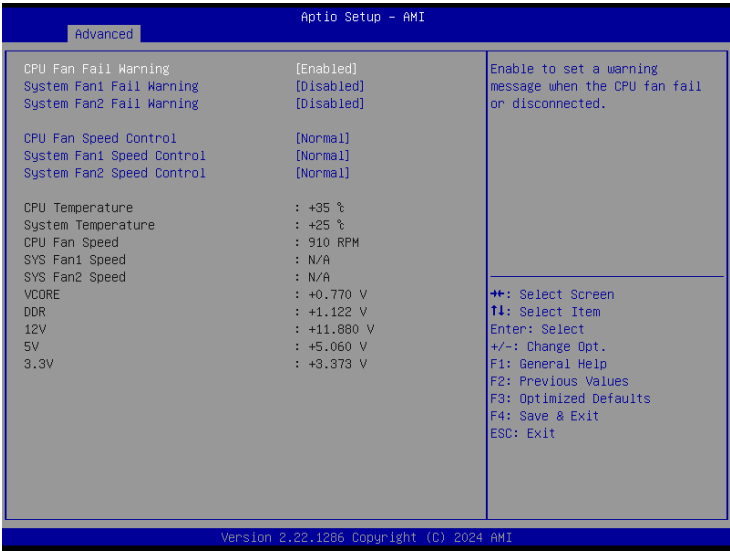
Item	Description
VMD setup menu / Enable VMD controller	Intel VMD feature helps you to control and manage NVMe PCIe SSD. Enabled : Enables Intel VMD feature Disabled : Disables Intel VMD feature (Default setting)
M2M_1	shows M.2 SSD information
Serial ATA Port 4	shows SATA HDD/SSD information
Serial ATA Port 5	shows SATA HDD/SSD information
Serial ATA Port 6	shows SATA HDD/SSD information
Serial ATA Port 7	shows SATA HDD/SSD information

3.3.5 IT8786 Super IO Configuration



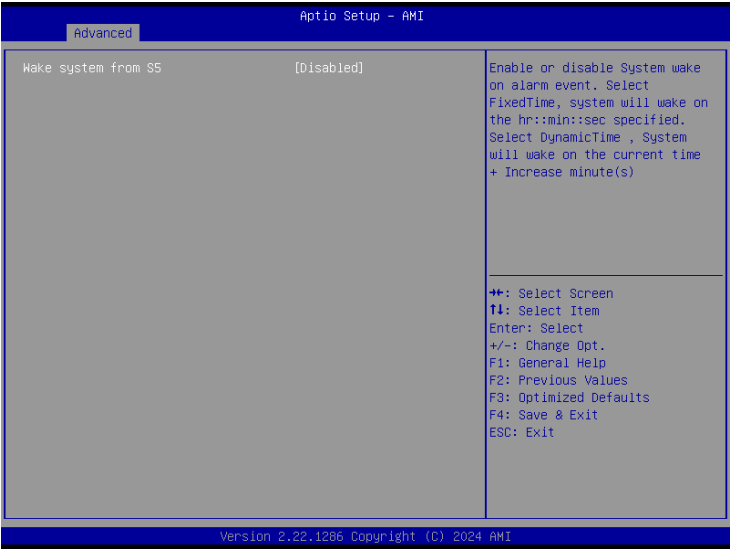
Item	Description
Serial Port 1 Configuration Serial Port 2 Configuration	Press [Enter] to configure advanced items : Serial Port : Enabled : Enables allows you to configure the serial port settings Disabled : if Disabled, displays no configuration for the serial port Device settings : Display the specified Serial Port base I/O address and IRQ COM Port Mode : Choose RS-232, RS-422, or RS-485 feature
Serial Port 3 Configuration Serial Port 4 Configuration Serial Port 5 Configuration Serial Port 6 Configuration	Press [Enter] to configure advanced items : Serial Port : Enabled : Enables allows you to configure the serial port settings Disabled : if Disabled, displays no configuration for the serial port Device settings : Display the specified Serial Port base I/O address and IRQ

3.3.6 Hardware Monitor



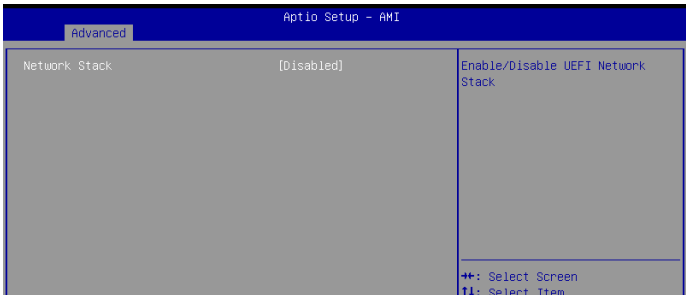
Item	Description
CPU Fan Fail Warning	Enabled : Enables CPU FAN Fail warning alert function (Default setting) Disabled : Disables CPU FAN Fail warning alert function
System Fan1 Fail Warning	Enabled : Enables System FAN Fail warning alert function Disabled : Disables System FAN Fail warning alert function (Default setting)
System Fan2 Fail Warning	Enabled : Enables System FAN Fail warning alert function Disabled : Disables System FAN Fail warning alert function (Default setting)
CPU Fan Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed
System Fan1 Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed
System Fan2 Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed
CPU Temperature	Shows current CPU temperature
System Temperature	Shows current system temperature
CPU Fan Speed	Shows current CPU fan Speed
SYS Fan1 Speed	Shows current System fan 1 Speed
SYS Fan2 Speed	Shows current System fan 2 Speed

3.3.7 S5 RTC Wake Settings

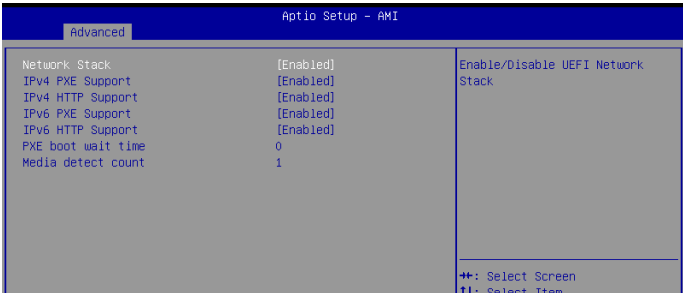


Item	Description
Wake system from S5	Enable or Disable System to wake on a specific time. Disabled : Disables system to wake on a specific time (Default setting) Fixed Time : Enables system to wake on a specific time (Format : hr : min : sec)

3.3.8 Network Stack Configuration



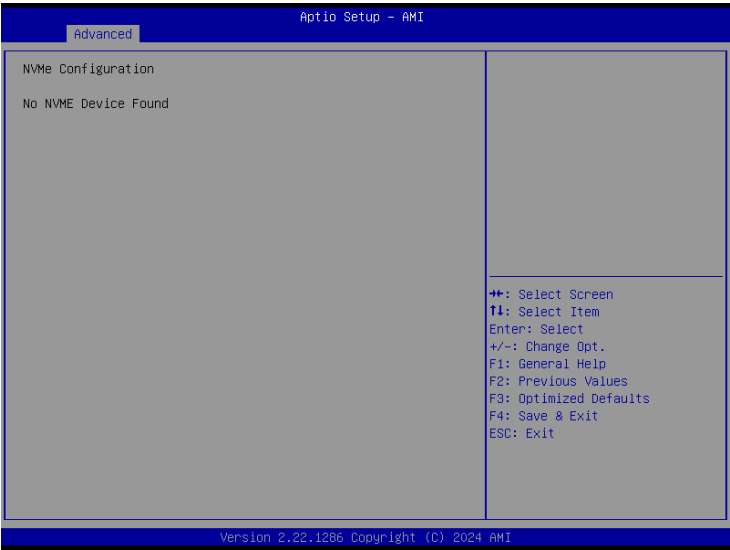
When Network stack is enabled :



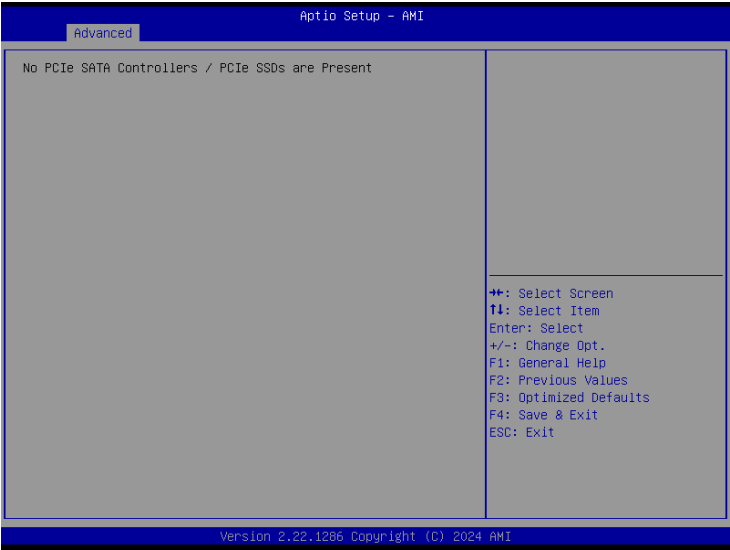
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode Disabled : Disables UEFI Network Stack (Default setting) Enabled : Enables UEFI Network Stack
IPv4 PXE Support	When Network stack is enabled : Disabled : Disables IPv4 PXE Support Enabled : Enables IPv4 PXE Support
IPv4 HTTP Support	When Network stack is enabled : Disabled : Disables IPv4 HTTP Support Enabled : Enables IPv4 HTTP Support
IPv6 PXE Support	When Network stack is enabled : Disabled : Disables IPv6 PXE Support Enabled : Enables IPv6 PXE Support
IPv6 HTTP Support	When Network stack is enabled : Disabled : Disables IPv6 HTTP Support Enabled : Enables IPv6 HTTP Support
PXE boot wait time	Wait time in seconds, or use ESC key to abort the PXE boot.
Media detect count	Number of times the presence of media will be checked.

3.3.9 NVMe Configuration

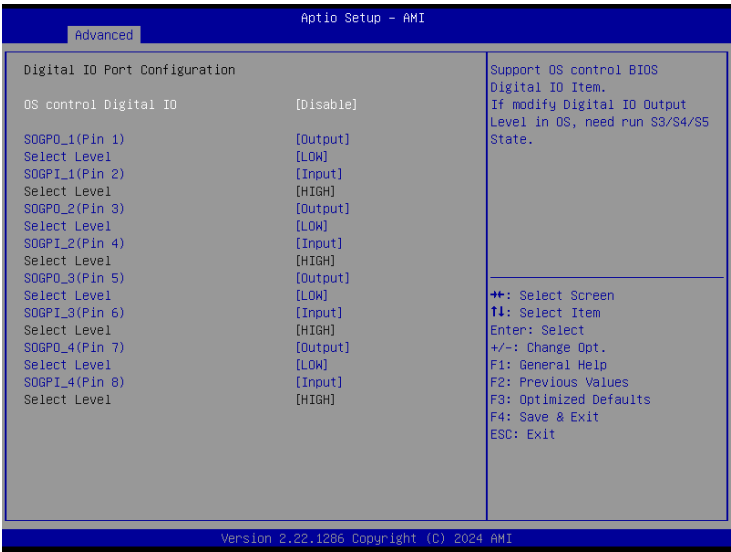
NVMe Configuration shows information when your M.2 NVMe PCIe SSD is installed.



3.3.10 Offboard SATA Controller Configuration

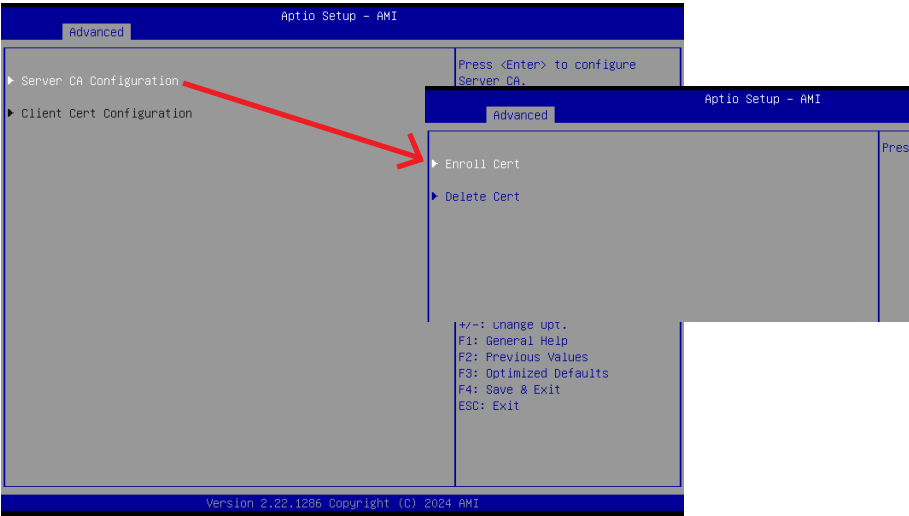


3.3.11 Digital IO Port Configuration



Item	Description
OS control Digital IO	Disabled : If Digital IO Output value/level is modified in OS, they will not be memorized and kept. (Default setting) Enabled : If Digital IO Output value/level is modified in OS, they will be memorized and kept.
SOGPO_1 (Pin 1) SOGPI_1 (Pin 2) SOGPO_2 (Pin 3) SOGPI_2 (Pin 4) SOGPO_3 (Pin 5) SOGPI_3 (Pin 6) SOGPO_4 (Pin 7) SOGPI_4 (Pin 8)	Configure Digital IO Input or Output values for each pin.

3.3.12 Tls Auth Configuration



Item	Description
Enroll Cert	Press [Enter] to configure advanced items : Server CA Configuration : Enroll Cert : 1. Enroll Cert Using File 2. Cert GUID : Input digit character in 11111111-2222-3333-4444-1234567 890ab format. 3. Commit Changes and Exit 4. Discard Changes and Exit

3.3.13 Intel(R) Ethernet Controller I226-LM - (MAC:10:FF:E0:39:4D:5C) (MAC address may varied based on different motherboard)

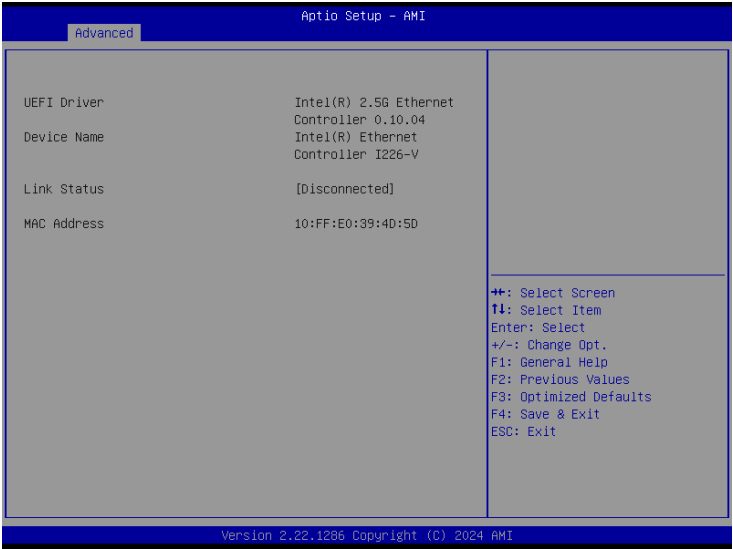
Shows Intel Ethernet controller information



NOTE : MAC address may varied based on different motherboard

3.3.14 Intel(R) Ethernet Controller I226-V - (MAC:10:FF:E0:39:4D:5D) (MAC address may varied based on different motherboard)

Shows Intel Ethernet controller information



NOTE : MAC address may varied based on different motherboard

3.4 Chipset



Item	Description
VT-d	Enabled : Enables VT-d function (Default setting) Disabled : Disables VT-d function
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor Option items : 32M , 64M, 128M, 256M (Default setting)
Primary Display	Auto : When detects PCIe Graphic card, primary display will set to PCIe (Default setting) IGFX : Force IGFX Graphic card as the primary display device PEG : Force PEG Graphic card as the primary display device
Internal Graphics	Enables or disables the onboard graphics function Auto : Detects display device automatically (Default setting) Enabled : Enables onboard graphics Disabled : Disables onboard graphics
Onboard LAN1 Onboard LAN2	Enable/Disable onboard LAN controller Enabled : Enables onboard LAN controller (Default setting) Disabled : Disables onboard LAN controller

HD Audio	Enable/Disable onboard audio controller Enabled : Enables onboard audio controller (Default setting) Disabled : Disables onboard audio controller
Restore AC Power Loss	To set which option the system should returns if a sudden power loss occurred Power off : Do not power on when the power is back (Default setting) Power on : System power on when the power is back Last state : Restore the system to the state before power loss occurs
Watchdog Timer	Enable/Disable Watchdog Timer function Disabled : Disables Watchdog Timer function (Default setting) Enabled : Enables Watchdog Timer function
Chassis Opened Warning	Enable/Disable to set a warning message when the system chassis opened. Disabled : Disables Warning message (Default setting) Enabled : Enables Warning message Clear : Clear the chassis intrusion status record
Control Iommu Pre-boot Behavior	Enable/Disable Control Iommu Pre-boot behavior Disabled : Disables IOMMU during boot (Default setting) Enabled : Enables IOMMU during boot
BIOS Lock	Enable/Disable BIOS Lock function Enabled : Enables BIOS Lock function (Default setting) Disabled : Disabled BIOS Lock funtion

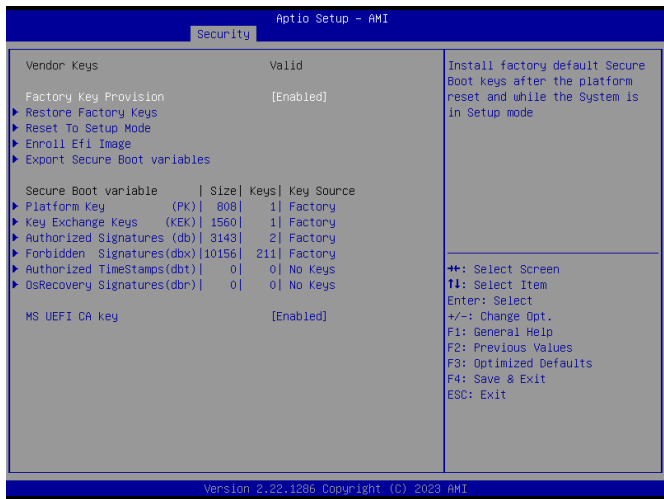
3.5 Security



Item	Description
Administrator Password	To set up Administrator's password Minimum length : 3 Maximum length : 20
User Password	To set up User's password Minimum length : 3 Maximum length : 20
Secure Boot	Press <Enter> to configure the advanced items



Item	Description
Secure Boot	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates Enabled : Enables Secure Boot function Disabled : Disables Secure Boot function (Default setting)
Secure Boot Mode	Standard : Standard mode Custom : Custom mode (Default setting)
Restore Factory Keys	To restore factory settings Yes : Agree to restore factory settings No : Cancel to restore factory settings
Reset To Setup Mode	Yes : Agree to setup mode No : Cancel to setup mode
Key Management	Enables expert users to modify Secure boot policy variables without full authentication Press <Enter> to configure the advanced items

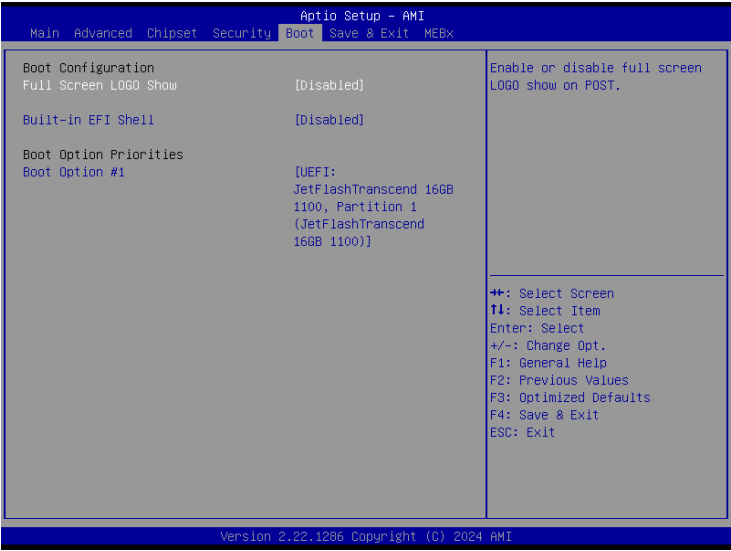


Item	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode Enabled : Enables Factory Key Provision (Default setting) Disabled : Disables Factory Key Provision
Restore Factory Keys	To restore factory settings Yes : Agree to restore factory settings No : Cancel to restore factory settings
Reset To Setup Mode	Yes : Agree to setup mode No : Cancel to setup mode
Enroll Efi Image	Allow the image to run in Secure Boot mode
Export Secure Boot variables	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device

Item	Description
Platform Key (PK)	These items allows you to enroll factory defaults or load Certificates from a file.
Key Exchange Keys	
Authorized Signatures	
Forbidden Signatures	
Authorized TimeStamps	
OsRecovery Signatures	Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database(db)
MS UEFI CA Key	

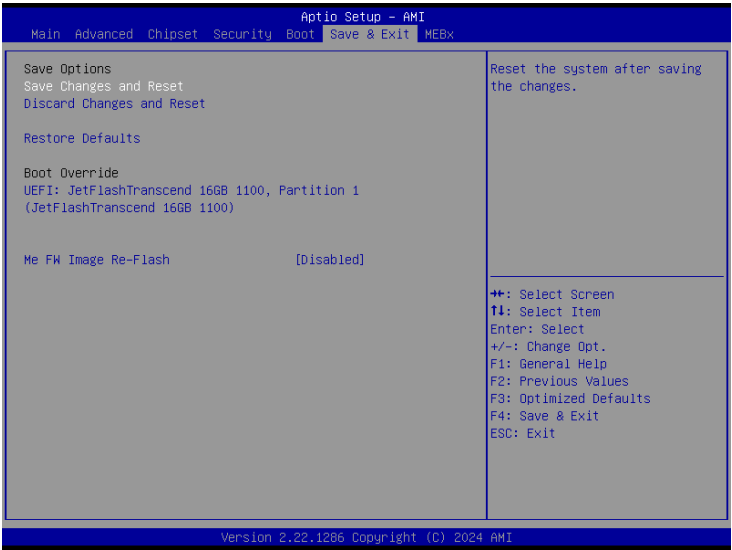
3.6 Boot

This Boot menu allows you to set/change system boot options



Item	Description
Full Screen LOGO Show	Enable/Disable full screen LOGO show on POST screen Enabled : Enables Full screen LOGO Show on POST screen Disabled : Disables Full screen LOGO Show on POST screen (Default setting)
Built-in EFI Shell	Enable/Disable Built-in EFI Shell Enabled : Enables Built-in EFI Shell Disabled : Disables Built-in EFI Shell (Default setting)
Boot Option #1	Shows the information of the storage that be installed in the system Choose/set the boot priority

3.7 Save & Exit



Item	Description
Save Changes and Reset	After configuring all the options that you wish to change, choose this option to save all the changes and reboot the system Yes : Agree to save and reset No : Cancel to save and reset
Discard Changes and Reset	Choose this option to reboot the system without saving any changes Yes : Agree to discard changes and reset No : Cancel to discard changes and reset
Restore Defaults	Restore/Load default values for all the setup options Yes : Agree to load optimized defaults No : Cancel to load optimized defaults
Me FW Image Re-Flash	Enable/Disable Me FW image re-flash function Enabled : Enables Me FW image re-flash function Disabled : Disables Me FW image re-flash function (Default setting)

3.8 MEBx



Item	Description
Intel(R) ME Password	For MEBx Login