QBiX-EHLA6412-A1

QBiX-EHLA6412-A1 Industrial Embedded System
Quick Start Guide

Copyright Notice

Acknowledgement

Packing List

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

Item	Quantity
System kit	1
19V / 65W adapter	1
Power cord (May vary based on local distribution)	1
VESA Bracket	1
VESA screw (M4-10L x 4pcs, M3-3L x 2pcs)	1

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

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.

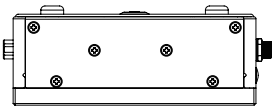
High Temperature Warning

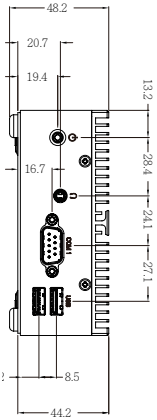
(1) This equipment is intended to be used in Restrict Access Location. The access can only be gained by Skilled person or by Instructed person who have been instructed about the metal chassis of the equipment is so hot that Skilled person have to pay special attention or take special protection. Only authorized by well trained professional person can access the restrict access location.
(2) External metal parts are hot!! Before touching it, special attention or protection is necessary

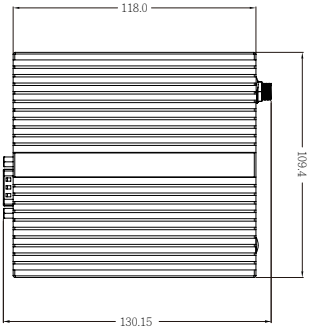
Table Contents

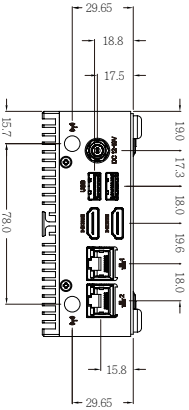
Chapter 1

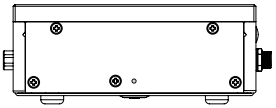
Chapter 1 - Product Specifications

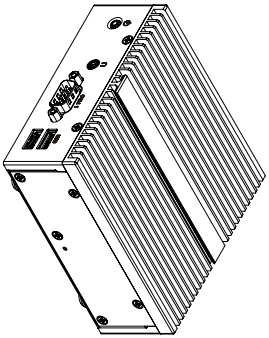


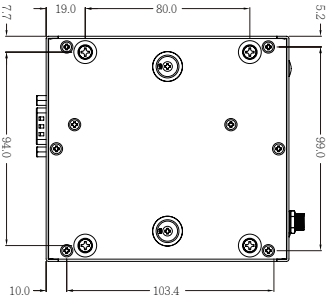

48.2
20.7
19.4
13.2
16.7
28.4
24.1
27.1
8.5
44.2


118.0
109.4
130.15


29.65
18.8
17.5
15.7
19.0
17.3
18.0
78.0
19.6
18.0
15.8
29.65






7.7
19.0
80.0
5.2
94.0
99.0
10.0
103.4

1.1 Specifications

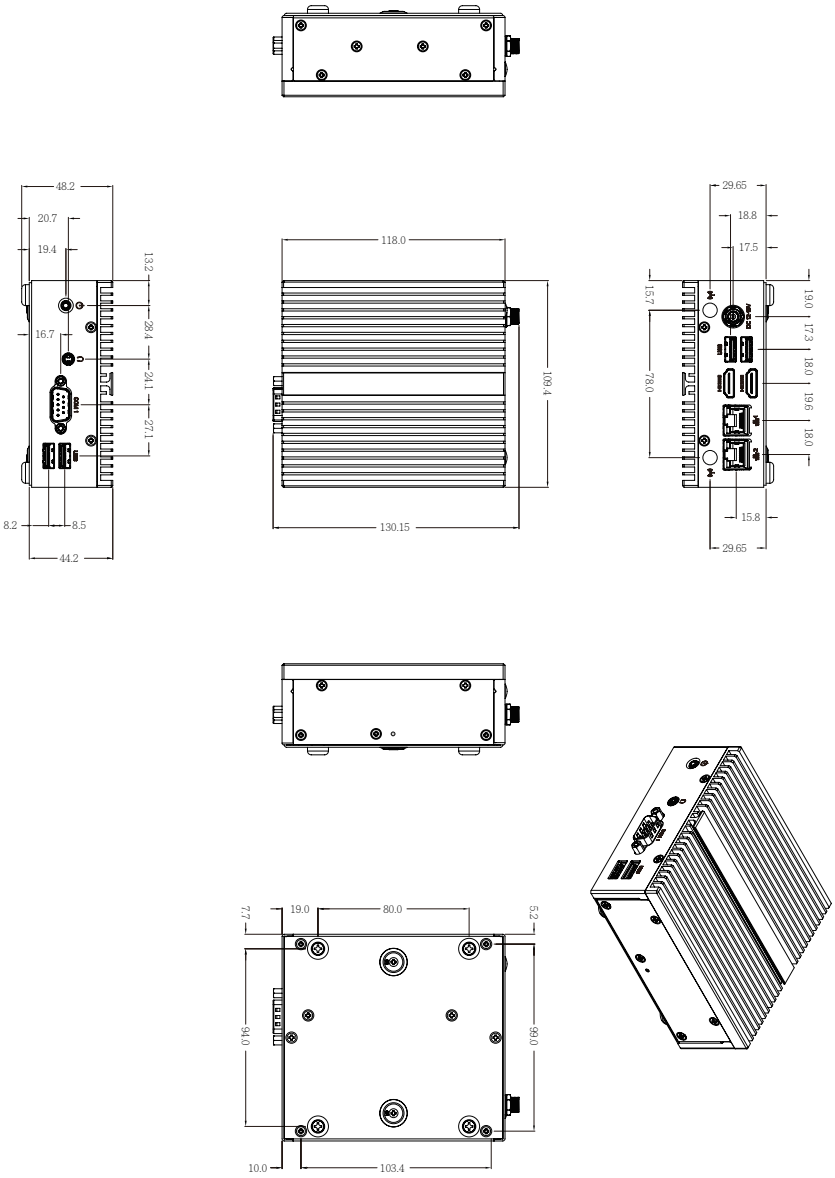
System	QBiX-EHLA6412-A1 (QB-6412A-SI)
Dimension	System Size : 118W x 109.4D x 44.4H (mm)
CPU	Intel® Celeron® J6412 Processor 10nm, 4 cores, 4 threads, up to 2.60 GHz TDP 10W
Memory	1 x DDR4 SO-DIMM socket, Max. Capacity 32 GB Support Single Channel DDR4 3200 MHz memory modules
Ethernet	2 x GbE LAN Ports (Intel® I210AT)
Graphic support	Integrated Graphics Processor - Intel® UHD Graphics for 10th Gen Intel® Processors : 2 x HDMI 2.0 port, supporting a maximum resolution of 4096x2160 @60Hz (2 independent display outputs)
Audio	Realtek® Audio Codec
Storage	—
Expansion Slots	1 x 2280 M.2 M-Key (PCIe x2, SATA 6Gb/s) 1 x 2230 M.2 E-Key (WiFi/BT)
Front I/O	2 x USB 3.2 Gen 2x1 1 x COM Port (RS-232) 1 x Combo Audio Jack (Headphone & Headset) 1 x Power button with LED
Rear I/O	2 x RJ45 LAN Ports 2 x USB 3.2 Gen 2x1 2 x HDMI 2 x External Antenna Holes (Optional) 1 x Screw Type DC Jack
Power	+12V~19VDC (Adapter 19V/65W)
Operation temperature	Operating temperature: 0°C to 50°C Operating humidity: 0-90% (non-condensing) Non-operating temperature: -40°C to 85°C Non-operating humidity: 0%-95% (non-condensing) Use wide temperature range memory and storage
Vibration During Operation	Operation: IEC 60068-2-64, 3 Grms, random, 5 ~ 500 Hz, 1 hr / Per Axis, With SSD Non-operation: IEC 60068-2-6, 2 G, Sine, 10 ~ 500 Hz, 1 Oct/ min, 1 hr / Per Axis

System	QBiX-EHLA6412-A1 (QB-6412A-SI)
Shock During Operation	Operation: IEC 60068-2-27, 50 G, half sine, 11 ms duration with SSD
Packaging Content	Carton size: 373 x 294 x 296 (mm) Packing Capacity: 8pcs Including: Power Cord : Optional (by region) PSU ADP 19V 65W 100-240VAC x 1 (P/N: 25EP0-1065W1-A3S) VESA Bracket x 1 (P/N: 25HB1-TPL021-S8R) VESA Screws x 1 (P/N: 25KSD-000001-S4R)
Order Information	System : 6BQB6412AMR-SI (Box packing)

Chapter 2

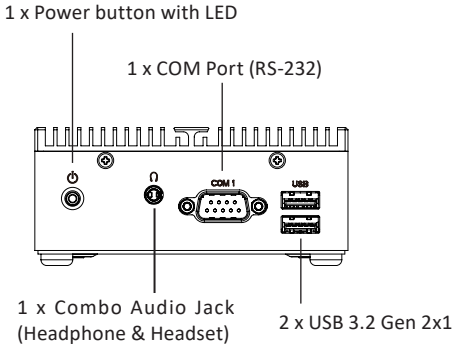
Chapter 2 – QBiX-EHLA6412-A1 Industrial Embedded System Kit

2.1 Dimension

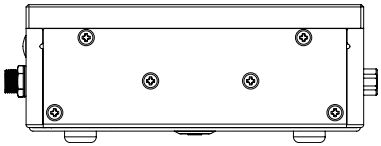


2.2 Getting Familiar with Your Unit

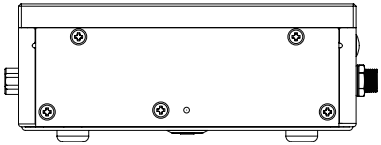
[Front Side]



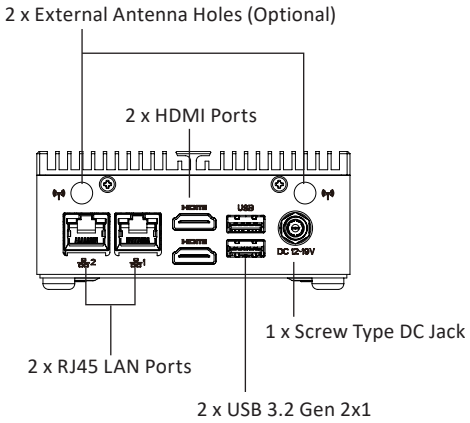
[Left Side]



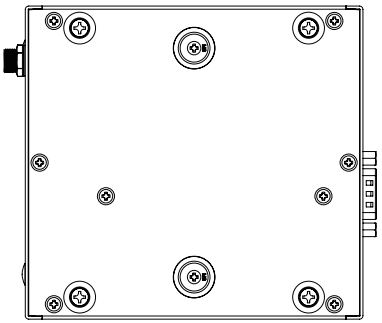
[Right Side]



[Rear Side]

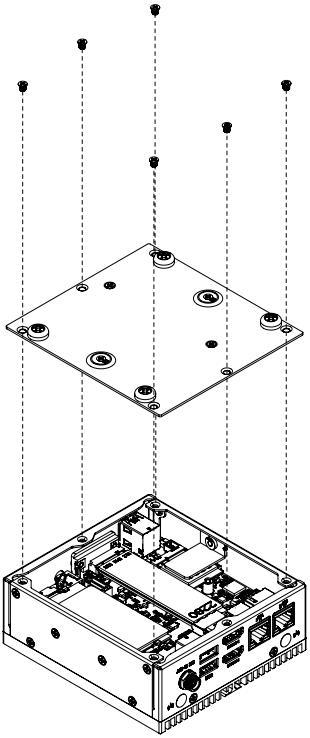


[Bottom Side]



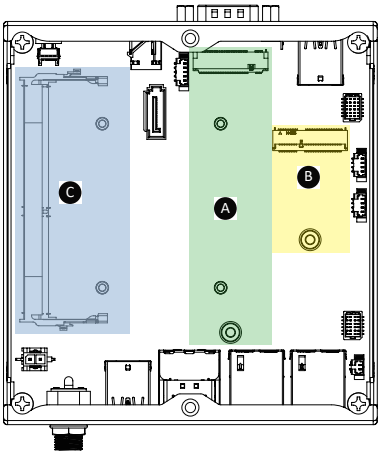
[Install]

* Before opening the case, make sure to unplug the power cord.
* 打開機殼前，請確實移除電源。
* Before Connecting the power, make sure to fasten the case securely.
* 接上電源前，請確實將機殼完整鎖附。



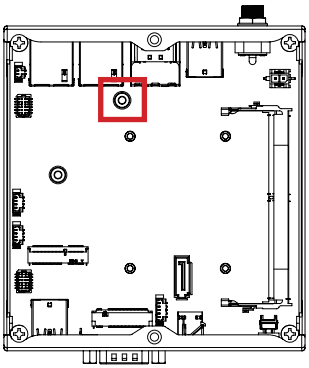
[Bottom PCB Side]

	Information
A	1 x M.2 slot, 2280 M-key
B	1 x M.2 slot, 2230 E-key
C	1 x DDR4 SO-DIMM socket

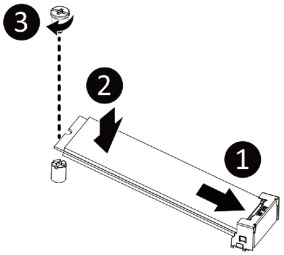


2.3 A) M.2 SSD Installation: How to safely install the M.2 2280 SSD

1. Remove the screw from the screw hole (Location : MSO1)



2. Carefully insert the M.2 SSD into the slot, and secure with the screw.

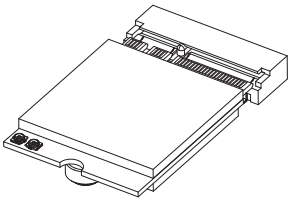


2.4 B) Wireless Module : How to safely install the Module (Wireless Module inclusion may vary based on local distribution)

1

Carefully insert the wireless module into the M.2 slot

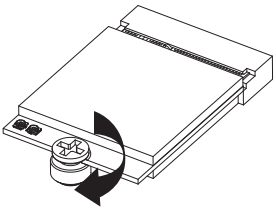
小心地將無線模組安裝於M.2插槽中。



2

Lock the screw in the middle.

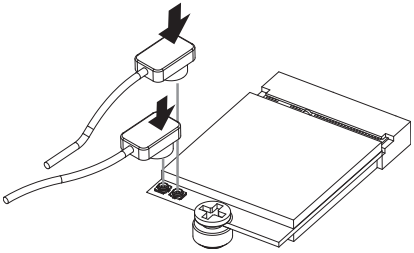
鎖入固定於無線模組中央頂端的螺絲。



3

Install the antenna on the left side of the connection wireless module down.

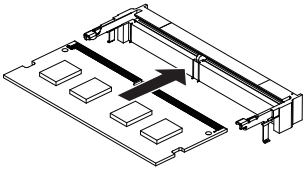
向下安裝連結於無線模組左側頂端天線。



2.5 C) Memory Installation: DDR4 SO-DIMM

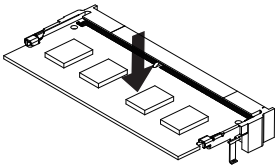
❶

Carefully insert SO-DIMM memory modules.
小心地由下至上將 SO-DIMM 記憶體安裝於記憶體插槽。



❷

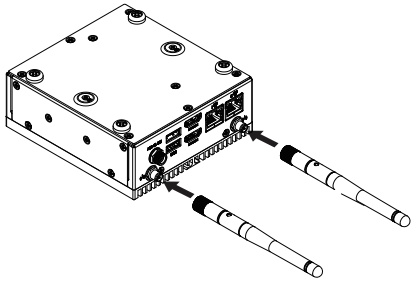
Push down until the modules click into place.
當記憶體固定於插槽後，再輕輕下壓至定點。



2.6 Antenna Installation (Antenna inclusion may vary based on local distribution)

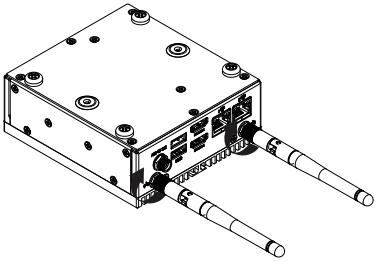
1

Carefully insert the antennas into the connectors.
小心地將天線插入天線插孔中。



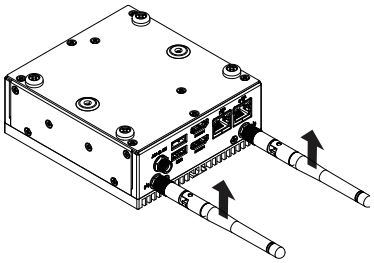
2

Turn the antennas clockwise until they are completely secure on the connectors.
握住天線接頭底端，按順時針方向將天線旋入插孔中牢牢固定。



3

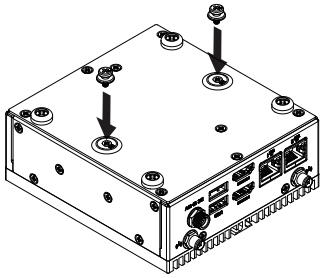
Flip up the antenna heads so that they are perpendicular to the machine.
栓緊後請將天線拉起朝上呈垂直狀。



2.7 VESA Bracket

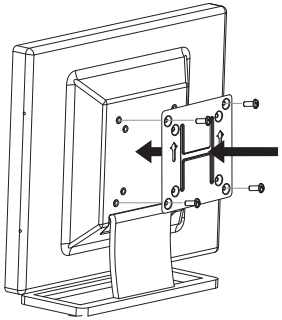
1

Attach the screws provided on the underside of the QBIX.
安裝隨附的VESA支撐架螺絲於QBiX底部。



2

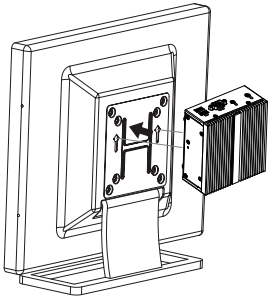
Attach the VESA mounting plate to the rear of a compatible display using the screws provided.
安裝隨附的 VESA 支撐架於支援 VESA 支撐架的電腦螢幕或電視機後背。



3

The QBiX can now be mounted by sliding the device into place.

將已安裝VESA支撐架螺絲的QBiX插入VESA支撐架的滑軌孔，向下壓至定位點後即可固定。



2.8 Support

● For a list of tested memory, M.2, wireless adapters and OS supported, go to: http://www.gigaipc.com
● To download the latest drivers and BIOS updates, go to: http://www.gigaipc.com
● For product support, go to: http://www.gigaipc.com

2.9 Safety and Regulatory Information

Risk of explosion if the battery is replaced with an incorrect type. Batteries should be recycled where possible.
Disposal of used Batteries must be in accordance with local environmental regulations.
Failure to use the included Power Adapter may violate regulatory compliance and may expose the user to safety
hazards.

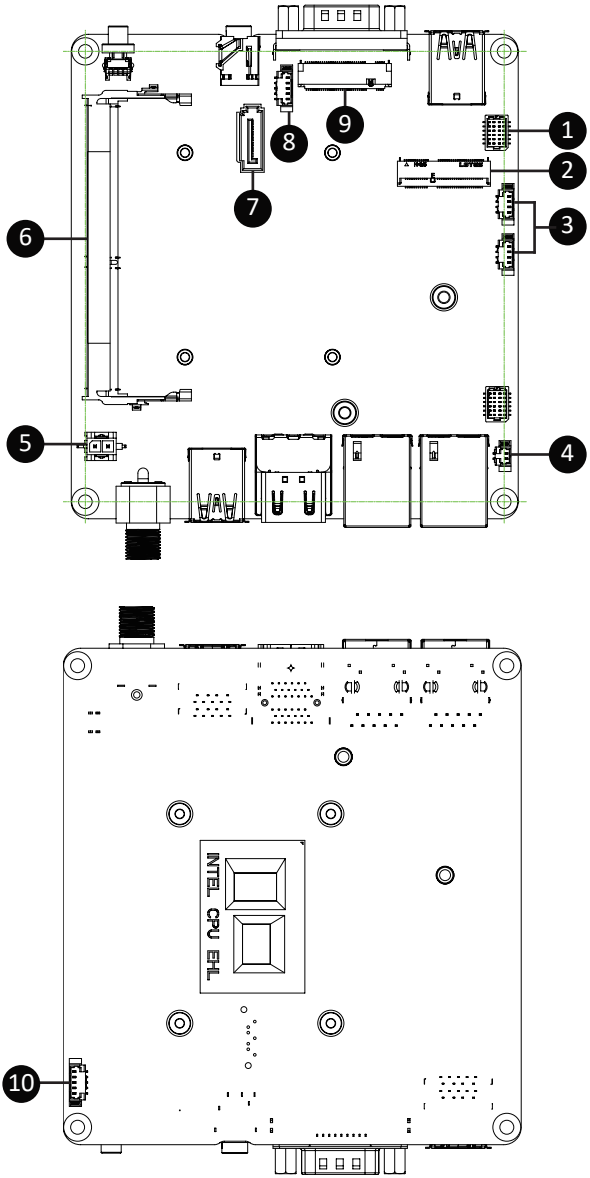
HIGH DEFINITION MULTIMEDIA INTERFACE

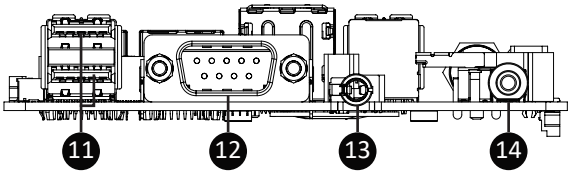
At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

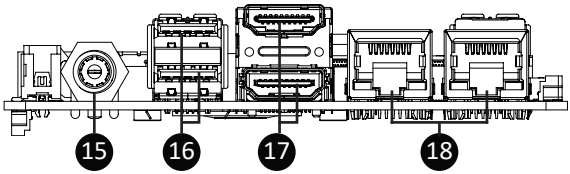
Chapter 3

Chapter 3 – Hardware Information

3.1 Jumpers and Connectors







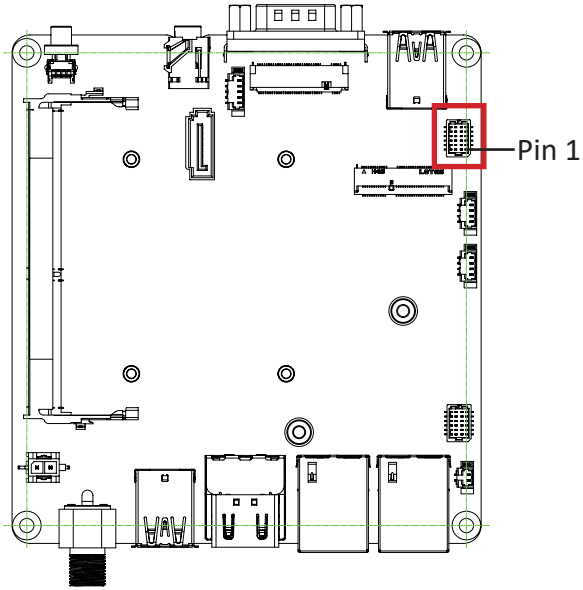
No	Code	Description
1	SYS_PANEL	Front panel header
2	M2E	M.2 Slot, E-Key NGFF 2230
3	FUSB2_1 FUSB2_2	USB 2.0 header
4	BATTERY	Battery connector
5	ATX_IN	ATX IN connector
6	SODIMM	DDR4 SO-DIMM Slot
7	SATAIII	SATA 6 Gb/s connector

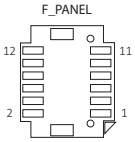
No	Code	Description
8	SATA_PWR	SATA power connector
9	M2M	M.2 Slot, M-Key NGFF 2280
10	CPU_FAN	CPU Fan connector
11	USB32_2	USB 3.2 Gen 2x1 port x 2
12	COM	Serial port connector (RS-232)
13	HP	Combo Audio Jack (Headphone & Headset)
14	PWR_BUTTON	Power button
15	DC_IN	Screw type DC Jack
16	USB32_1	USB 3.2 Gen 2x1 port x 2
17	HDMI_21	HDMI connector
18	LAN1 LAN2	LAN Connector x 2

GIGAIPC

3.2.1 SYS_PANEL (Front panel header)

1



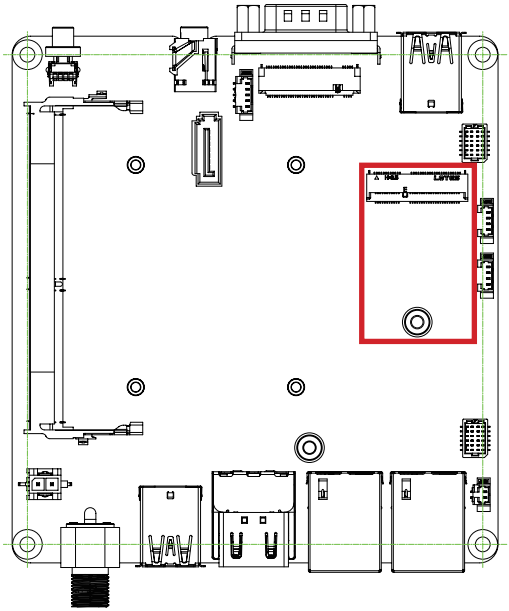
Front panel header


Connector PN	Vendor
87216-1206-06	ACES

Pin No.	Definition
1	HD-p
2	MPD-p
3	HD-n
4	MPD-n
5	GND
6	POWER-ON
7	Reset
8	GND
9	NC
10	NC
11	NC
12	NC

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

❷



M.2 E Key Connector

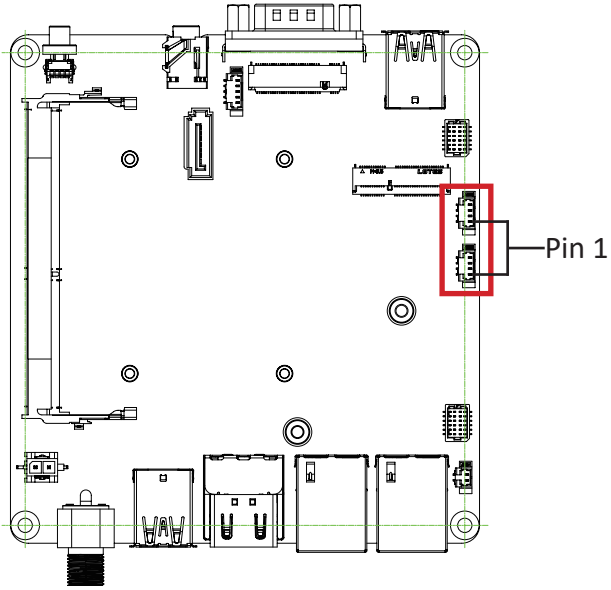
Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	D1p	4	3.3V
5	D1n	6	NC
7	GND	8	NC
9	NC	10	NC
11	NC	12	NC
13	NC	14	NC
15	NC	16	NC
17	NC	18	GND
19	NC	20	NC
21	NC	22	NC
23	NC		

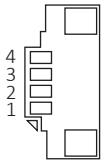
Pin No.	Definition	Pin No.	Definition
33	GND	32	NC
35	PCIE TXp	34	NC
37	PCIE TXn	36	NC
39	GND	38	NC
41	PCIE RXp	40	NC
43	PCIE RXn	42	NC
45	GND	44	NC
47	PCIE Clock p	46	NC
49	PCIE Clock n	48	NC
51	GND	50	SUSCLK
53	PCIE Clock Request	52	Reset
55	PCIE Wakeup	54	BT_Disable
57	GND	56	WLAN_Disable
59	NC	58	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
80152-8521	BELLWETHER

3.2.3 FUSB2_1, FUSB2_2 (USB 2.0 header)

3



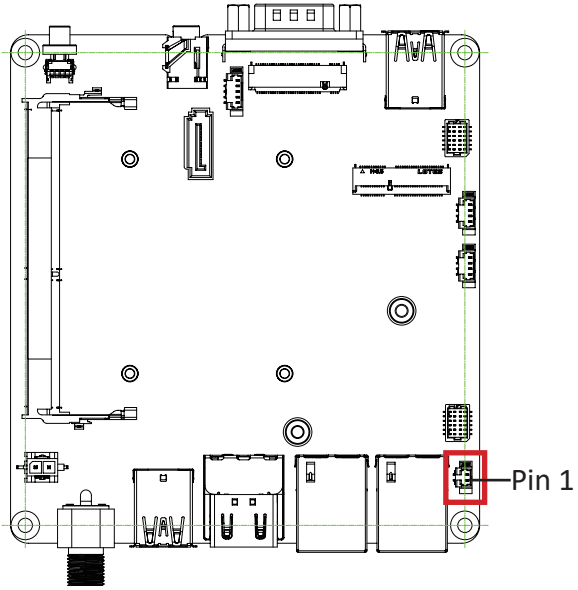
USB 2.0 header

F_USB2.0

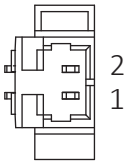
Pin No.	Definition
1	5V
2	D1n
3	D1p
4	GND

Connector PN	Vendor
A1250WV-S-04PNLBT1T00L	JOINT-TECH
50273-0047N-001	ACES

3.2.4 BATTERY (Battery connector)

4

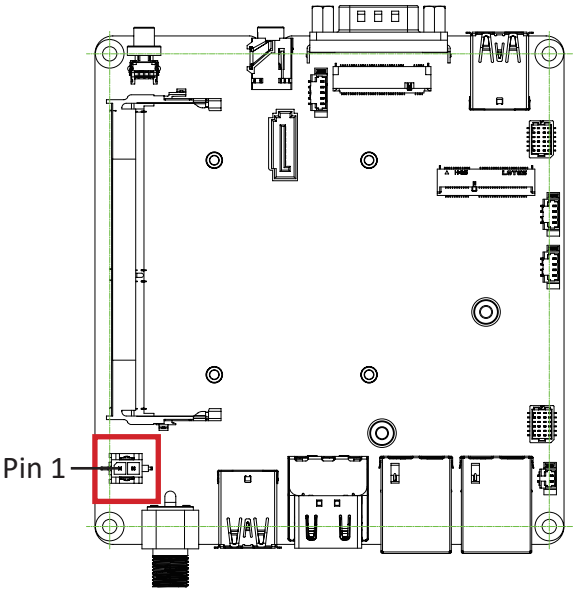


Battery Connector


Pin No.	Definition
1	3V
2	GND

3.2.5 ATX_IN (ATX IN Connector)

5



ATX_IN Connector

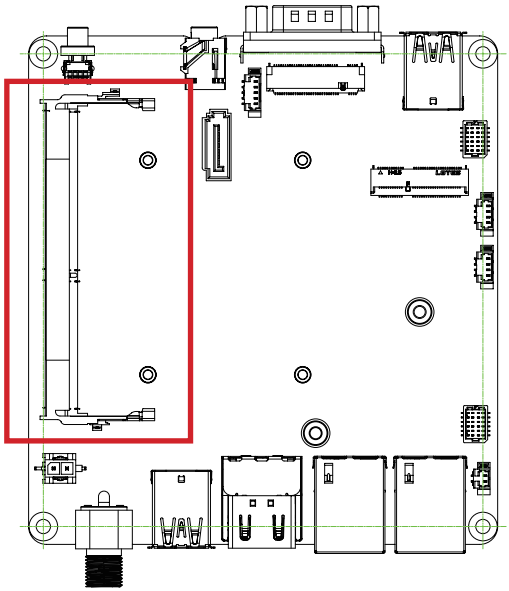
1

Connector PN	Vendor
99-01740-B004-A	TCONN

Pin No.	Definition
1	GND
2	DC IN

3.2.6 SODIMM (DDR4 SO-DIMM Slot)

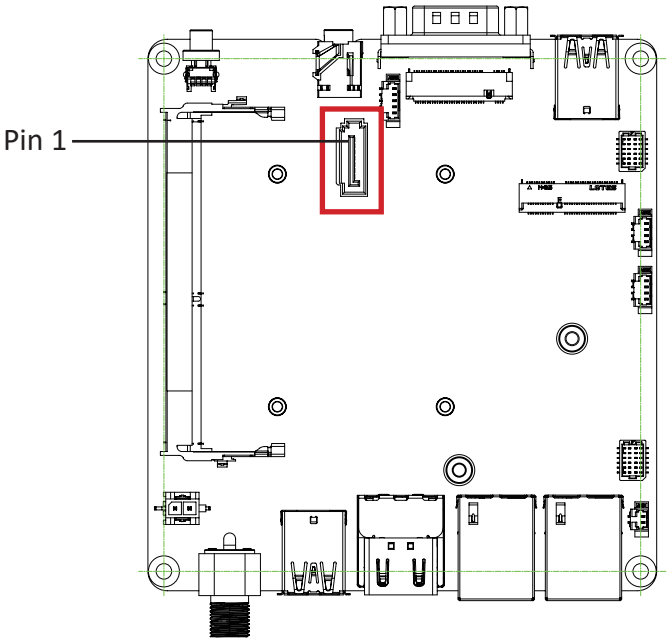
6



GIGAIPC

3.2.7 SATAIII (SATA 6 Gb/s connector)

7

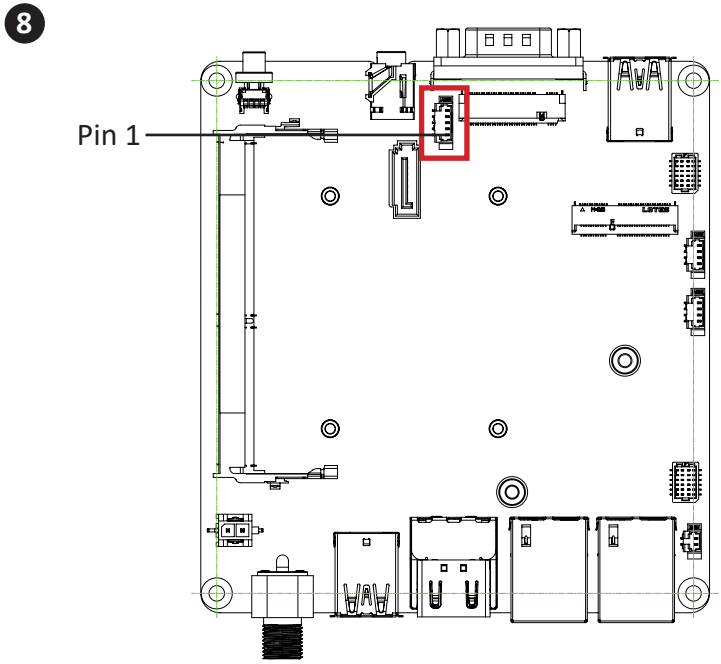


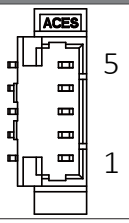
SATA 6 Gb/s connector


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

3.2.8 SATA_PWR (SATA power connector)



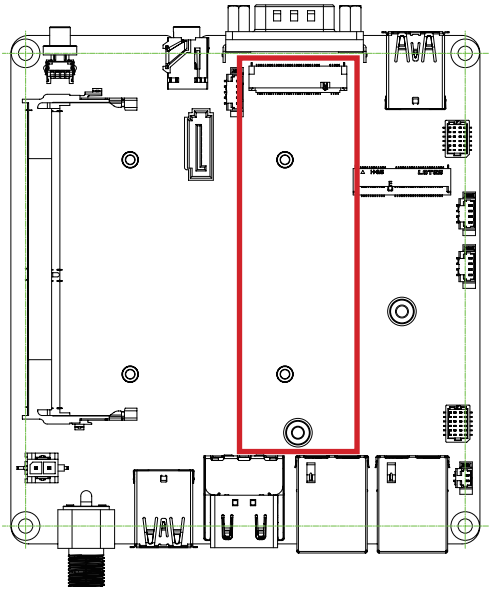
SATA power connector


Connector PN	Vendor
85205-0570N	ACES

Pin No.	Definition
1	5V
2	5V
3	3.3V
4	GND
5	GND

3.2.9 M2M (M.2 Slot, M-Key NGFF 2280)

9



M.2 M Key Connector	
1	75
2	74

Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	NC	6	NC
7	NC	8	NC
9	GND	10	SSD LED
11	NC	12	3.3V
13	NC	14	3.3V
15	GND	16	3.3V
17	NC	18	3.3V
19	NC	20	NC
21	GND	22	NC
23	NC	24	NC
25	NC	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
37	PCIE1 TXp	38	NC

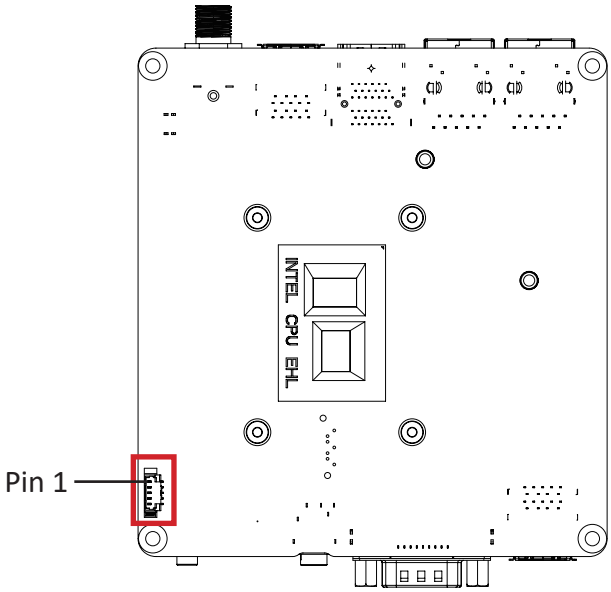
Pin No.	Definition	Pin No.	Definition
39	GND	40	NC
41	PCIE0 RXn/ SATA RXp	42	NC
43	PCIE0 RXp/ SATA RXn	44	NC
45	GND	46	NC
47	PCIE0 TXn/ SATA TXn	48	NC
49	PCIE0 TXp/ SATA TXp	50	PCI Reset
51	GND	52	PCIE Clock Request
53	PCIE Clock n	54	NC
55	PCIE Clock p	56	NC
57	GND	58	NC

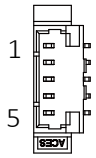
Pin No.	Definition	Pin No.	Definition
67	NC	68	NC
69	Detect	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

Connector PN	Vendor
80159-8521	BELLWETHER

3.2.10 CPU FAN (CPU Fan connector)

10



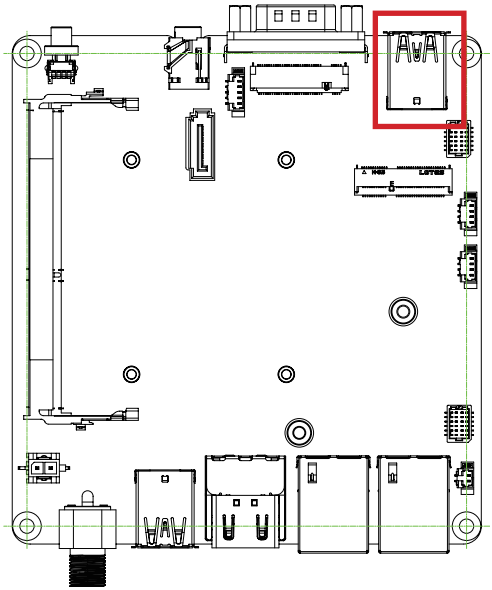
CPU FAN connector


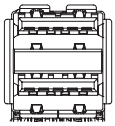
Connector PN	Vendor
85205-0570N	ACES

Pin No.	Definition
1	GND
2	5V
3	Detect
4	PWM
5	NC

3.2.11 USB32_2 (USB 3.2 Gen 2x1 connector)

11



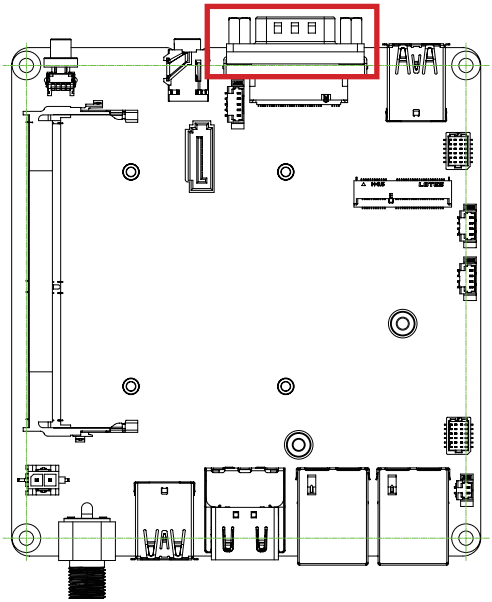
USB 3.2 Gen 2x1 connector


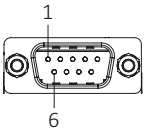
Pin No.	Definition	Pin No.	Definition
1	5V	10	5V
2	D1n	11	D0n
3	D1p	12	D0p
4	GND	13	GND
5	USB3_RX1n	14	USB3_RX2n
6	USB3_RX1p	15	USB3_RX2p
7	GND	16	GND
8	USB3_TX1n	17	USB3_TX2n
9	USB3_TX1p	18	USB3_TX2p

Connector PN	Vendor
18-A5950-6A33-A	TCONN

3.2.12 COM (Serial port connector, RS-232)

12



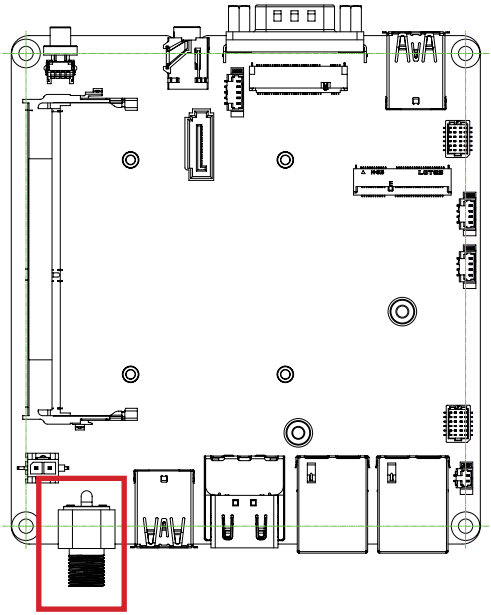
Serial port Connector


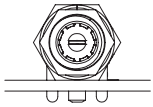
Pin No.	Definition
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

Connector PN	Vendor
SM41D1P1122N33N1	FENYING

3.2.13 DC_IN (Screw type DC Jack connector)

15

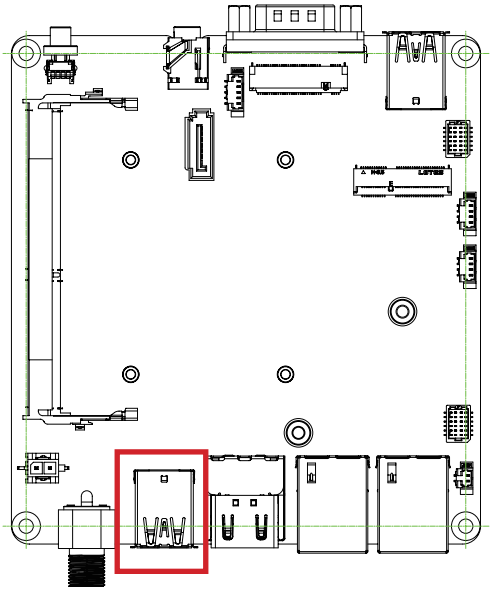


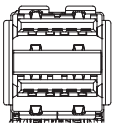
Screw Type DC Jack Connector


Connector PN	Vendor
655-360-000	SHEN-MING

3.2.14 USB32_1 (USB 3.2 Gen 2x1 connector)

16



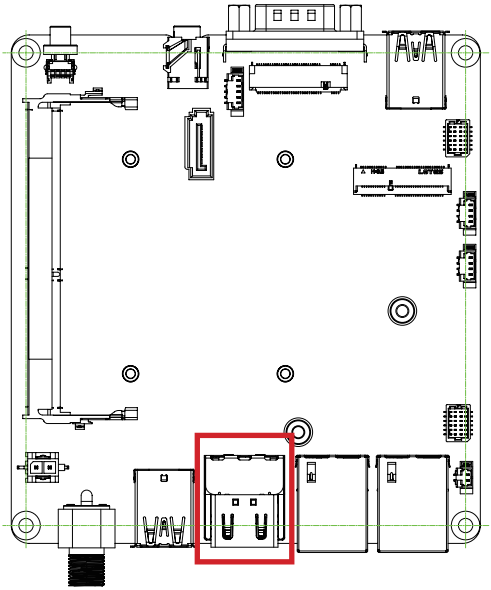
USB 3.2 Gen 2x1 connector


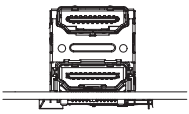
Pin No.	Definition	Pin No.	Definition
1	5V	10	5V
2	D1n	11	D0n
3	D1p	12	D0p
4	GND	13	GND
5	USB3_RX1n	14	USB3_RX2n
6	USB3_RX1p	15	USB3_RX2p
7	GND	16	GND
8	USB3_TX1n	17	USB3_TX2n
9	USB3_TX1p	18	USB3_TX2p

Connector PN	Vendor
18-A5950-6A33-A	TCONN

3.2.15 HDMI_21 (HDMI connector)

17



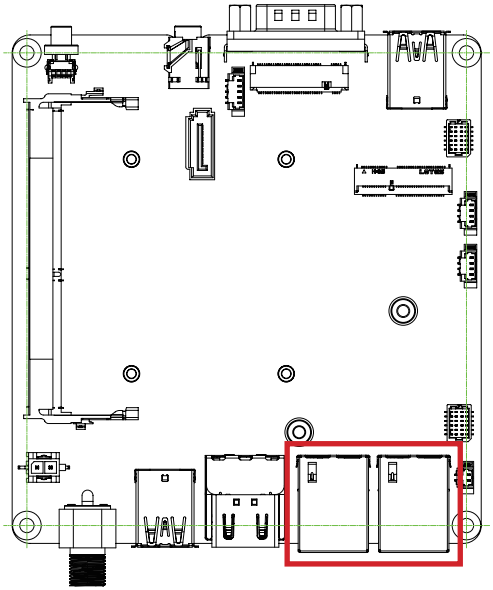
HDMI Connector


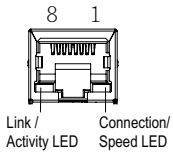
Pin No.	Definition	Pin No.	Definition
1	TX2p	11	GND
2	GND	12	CLKn
3	TX2n	13	NC
4	TX1p	14	NA
5	GND	15	DDC Clock
6	TX1n	16	DDC Data
7	TX0p	17	GND
8	GND	18	5V
9	TX0n	19	Hot Plug Detect
10	CLKp		

Connector PN	Vendor
QJ11191-DFB1-4F	FOXCONN

3.2.16 LAN1, LAN2 (LAN connector)

18



LAN Connector


Pin No.	Definition
1	TX1+
2	TX1-
3	TX2+
6	TX2-
4	TX3+
5	TX3-
7	TX4+
8	TX4-

State	Description
Orange On	1Gbps data rate
Green On	100Mbps data rate
Off	10Mbps data rate

Connector PN	Vendor
RB1-13NB5N5A	UDE

Chapter 4

Chapter 4 – BIOS

4.1 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.

4.1.1 How to Entering into BIOS menu

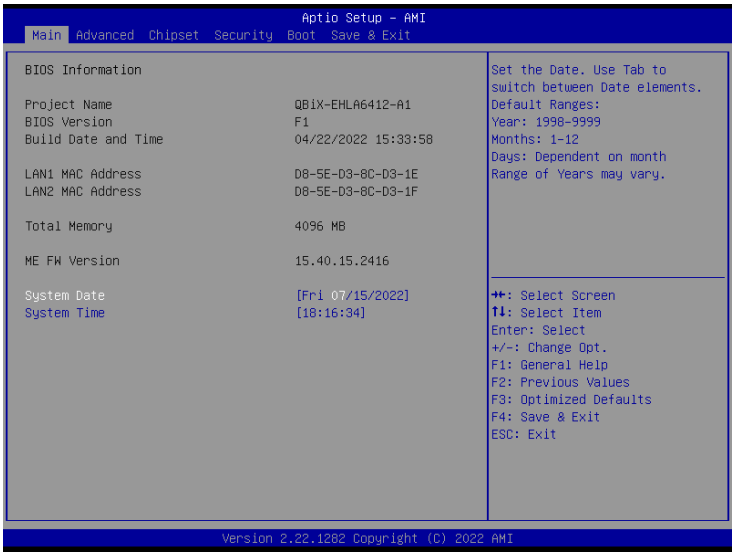
Once the system is power on, press the <DEL> key as soon as possible to access into BIOS Setup program.

4.1.2 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

4.2 The Main Menu

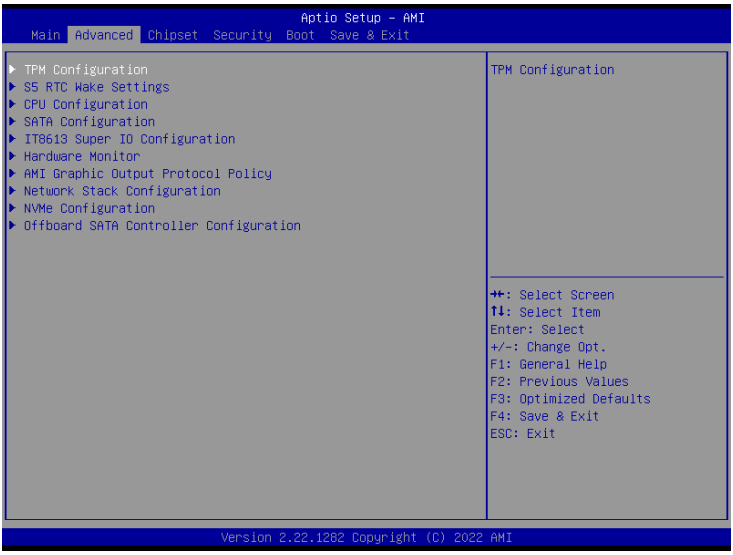
The main menu shows the basic system information.
Use arrow keys to move among the items.



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 LAN1 MAC Address information
LAN2 MAC Address	Shows LAN2 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)

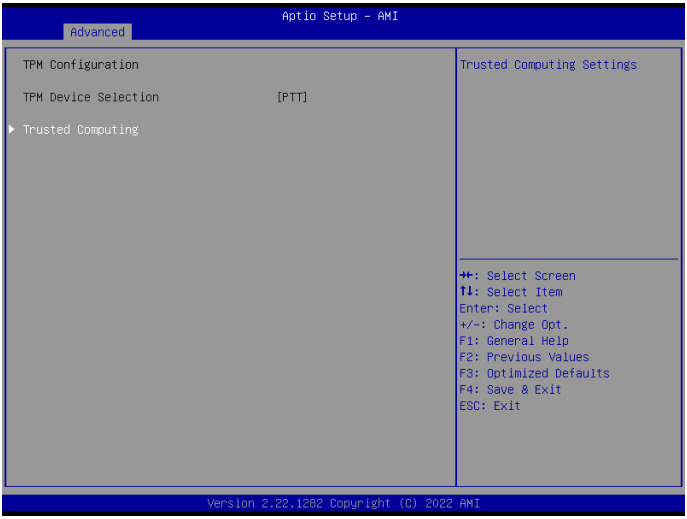
4.3 Advanced

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.



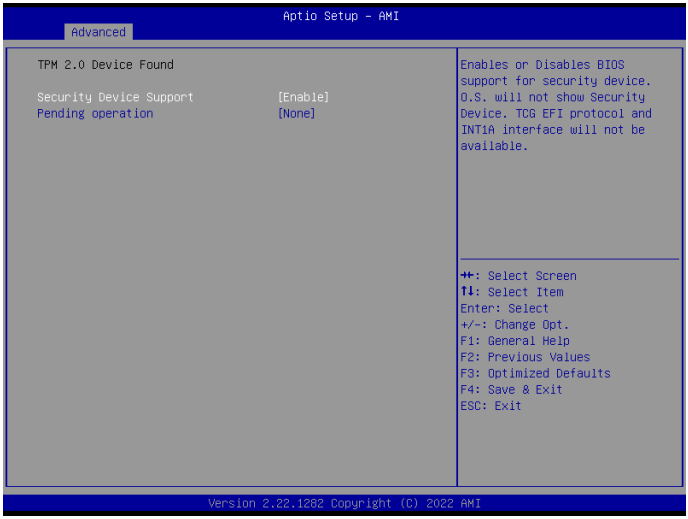
4.3.1 TPM Configuration

Use TPM Configuration submenu to choose TPM interface.



Item	Description
TPM Device Selection	**PTT : Internal TPM (Default setting)**

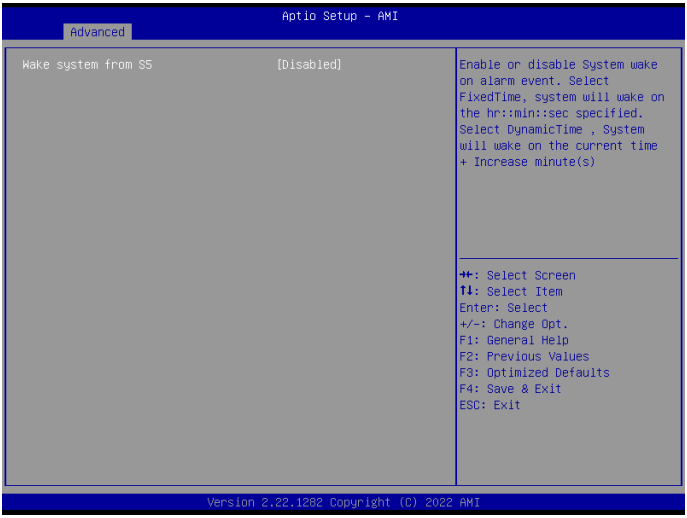
Trusted Computing : Shows TPM information, and TPM module configuration setting.



Item	Description
Security Device support	**Enabled : Enables TPM feature (Default setting)** **Disabled : Disables TPM feature**

Item	Description
Pending operation	**None : No execution will be conducted (Default setting)** **TPM clear : Set to clear data on TPM**

4.3.2 S5 RTC Wake Settings



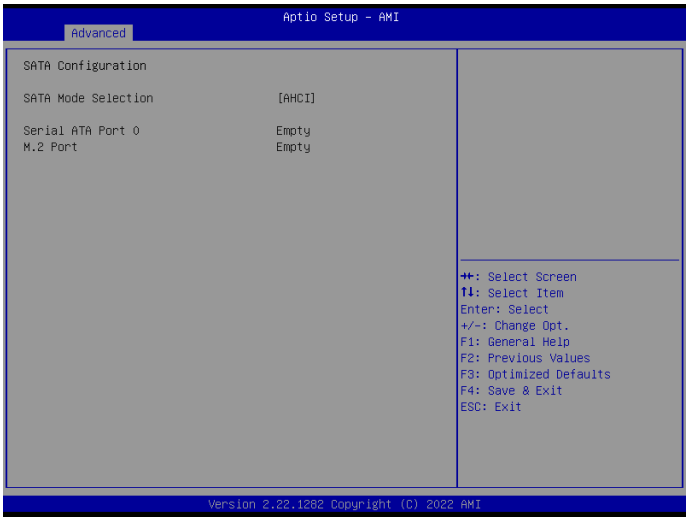
Item	Description
Wake system from S5	Enable or Disable System to wake on a specific time. **Disabled : Disables system to wake on a specific time (Default setting)** **Fixed Time : Enables system to wake on a specific time** **(Format : hr : min : sec)**

4.3.3 CPU Configuration

This submenu shows detailed CPU informations.

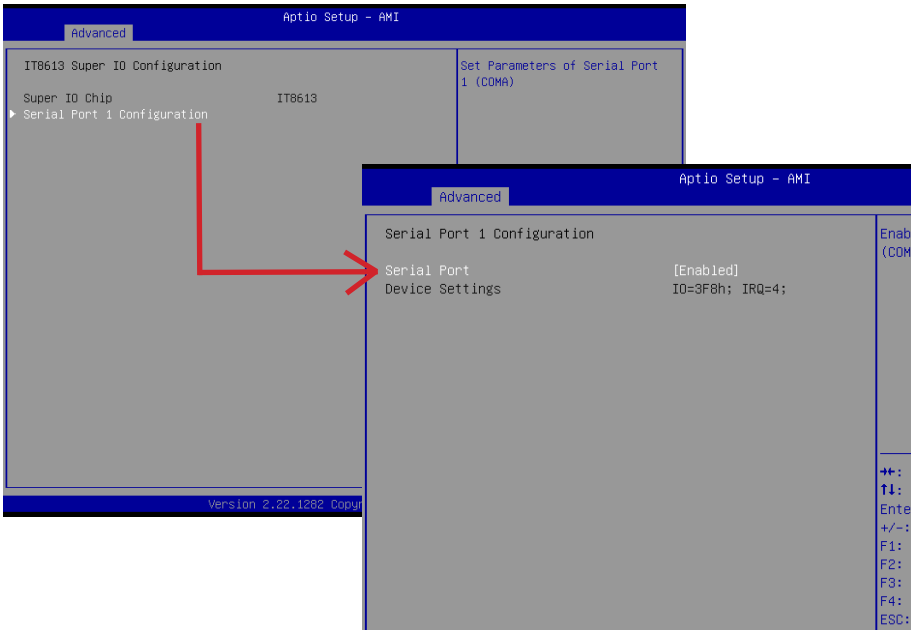
Item	Description
Intel Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. **Enabled : Enables Intel Virtualization Technology (Default setting)** **Disabled : Disables Intel Virtualization Technology**
EIST	According to System loading, Enhanced Intel SpeedStep Technology (EIST)will automatically adjust the CPU voltage and core frequency to decrease heat and power consumption for power saving. **Enabled : Enables EIST Technology (Default setting)** **Disabled : Disables EIST Technology**
Turbo Mode	**Enabled : Enables Turbo Mode (Default setting)** **Disabled : Disables Turbo Mode**
CPU 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**
CPU P states	CPU will adjust frequency depends on it's loading. **Enabled : Enables CPU P states function (Default setting)** **Disabled : Disables CPU P states function**

4.3.4 SATA Configuration



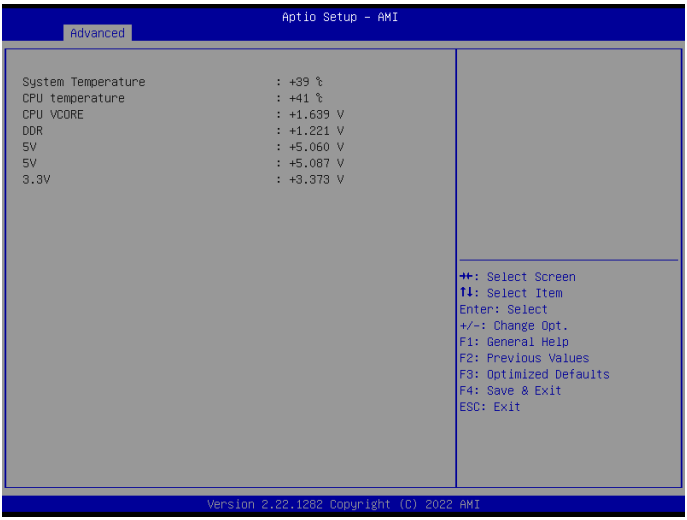
Item	Description
SATA Mode Selection	**AHCI : Configures the SATA controllers to AHCI mode. (Default setting)**
Serial ATA Port 0	shows 2.5" SATA HDD/SSD information
M.2 Port	shows M.2 SATA interface SSD information

4.3.5 IT8613 Super IO Configuration



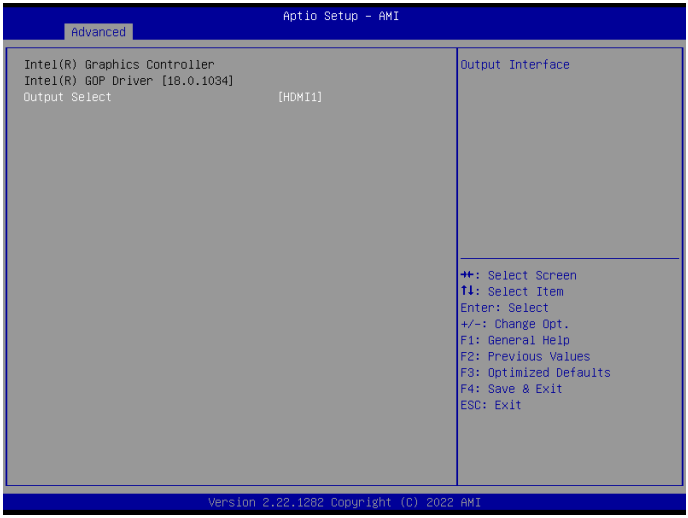
Item	Description
Super IO Chip	Shows Super I/O chip model
Serial Port 1 Configuration	Press [Enter] to configure advanced items : Enable or Disable Serial Port **Enabled : Enables Serial Port function (Default setting)** **Disabled : Disables Serial Port function** Device settings : Display the specified Serial Port base I/O address and IRQ

4.3.6 Hardware Monitor



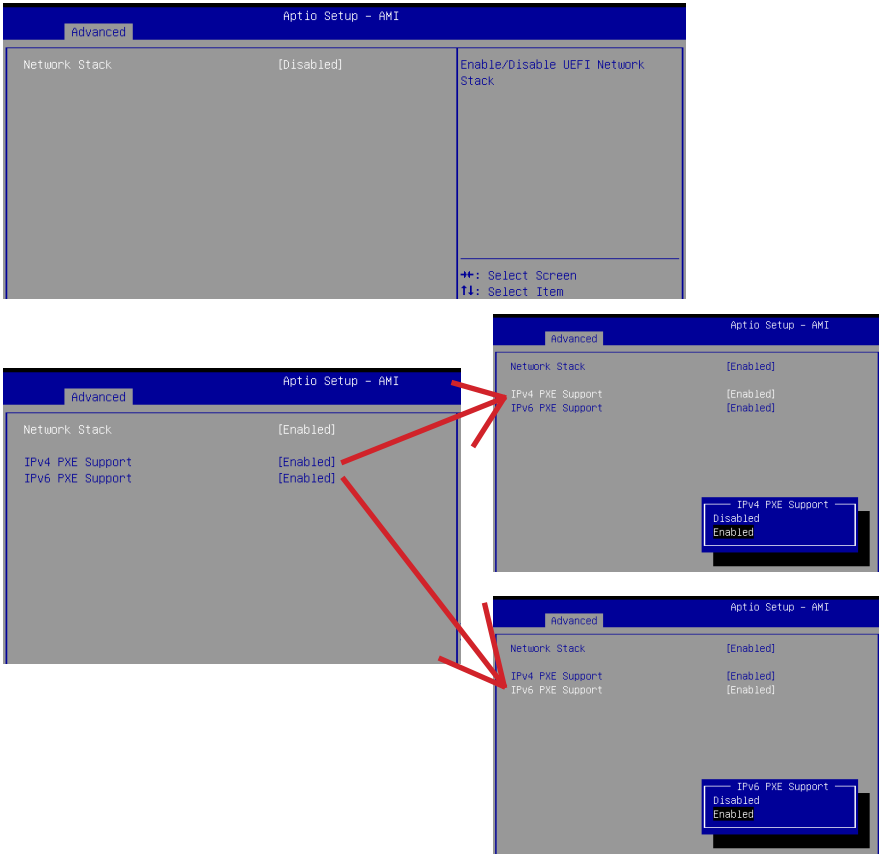
Item	Description
System Temperature	Shows current system temperature
CPU Temperature	Shows current CPU temperature

4.3.7 AMI Graphic Output Protocol Policy



Item	Description
Output Select	Choose default monitor output when there are more than one monitor plugged on the motherboard.

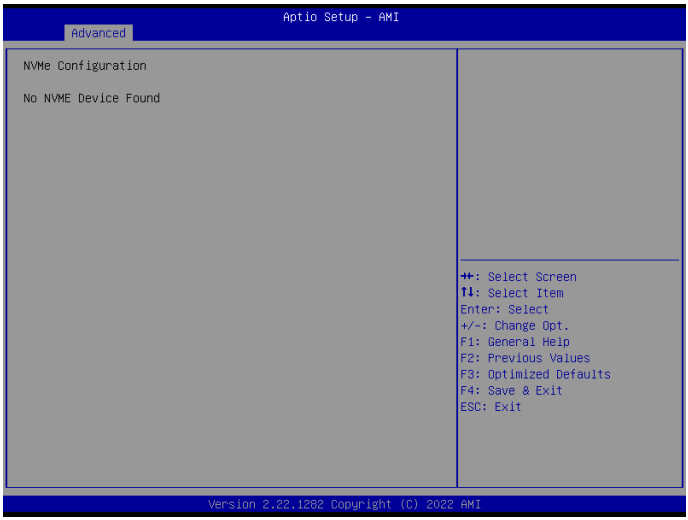
4.3.8 Network Stack Configuration



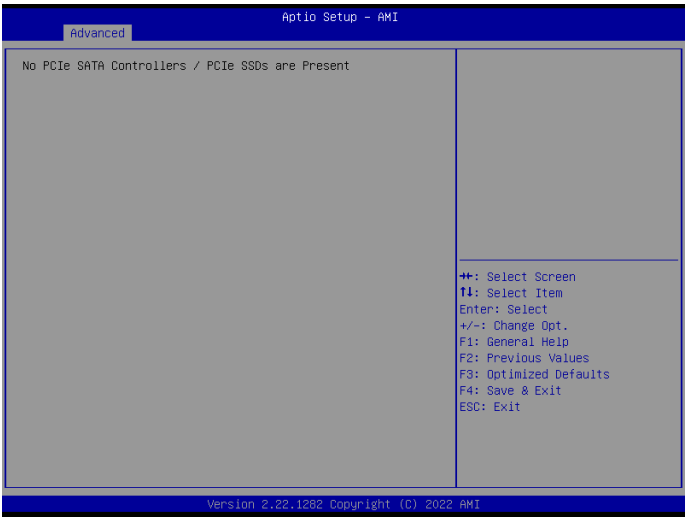
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode **Disabled : Disables UEFI Network Stack (Default setting)** **Enabled : Enables UEFI Network Stack**
Ipv4 PXE Support	When Network stack is enabled : **Disabled : Disables Ipv4 PXE Support** **Enabled : Enables Ipv4 PXE Support**
Ipv6 PXE Support	When Network stack is enabled : **Disabled : Disables Ipv6 PXE Support** **Enabled : Enables Ipv6 PXE Support**

4.3.9 NVMe Configuration

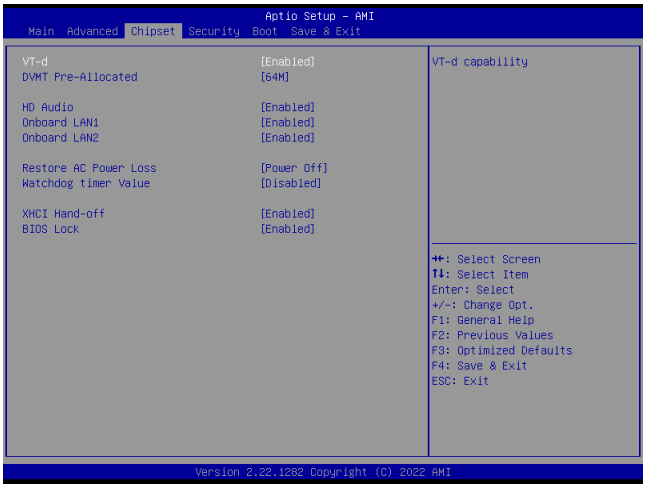
NVMe Configuration shows information when your M.2 NVMe PCIe SSD is installed.



4.3.10 Offboard SATA Controller Configuration

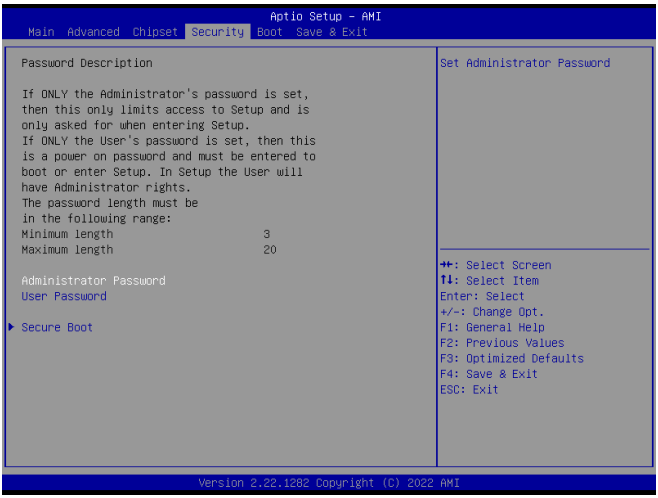


4.4 Chipset

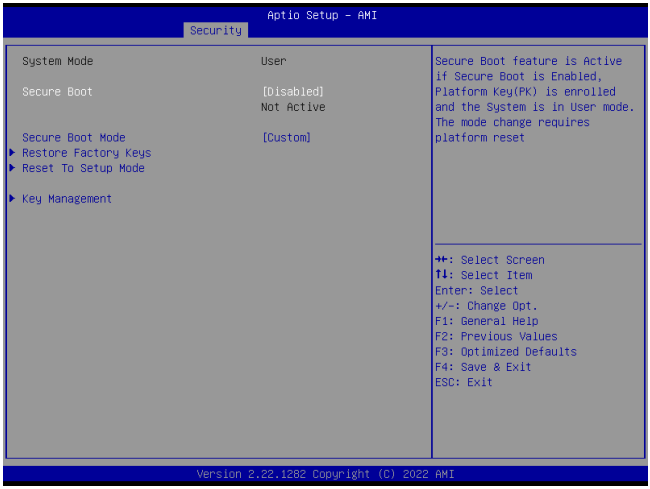


Item	Description
VT-d	**Enabled : Enables VT-d function (Default setting)** **Disabled : Disables VT-d function**
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor **Option items : 32M , 64M(Default setting), 128M, 256M**
HD Audio	Enable/Disable onboard audio controller **Enabled : Enables onboard audio controller (Default setting)** **Disabled : Disables onboard audio controller**
Onboard LAN1 **Onboard LAN2**	Enable/Disable onboard LAN controller **Enabled : Enables onboard LAN controller (Default setting)** **Disabled : Disables onboard LAN controller**
Restore AC Power Loss	To set which option the system should returns if a sudden power loss occured **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 occures**
Watchdog Timer Value	Enable/Disable Watchdog Timer function **Enabled : Enables Watchdog Timer function** **Disabled : Disabled Watchdog Timer function (Default setting)**
XHCI Hand-off	Enable/Disable XHCI Hand-off function **Enabled : Enables XHCI Hand-off function (Default setting)** **Disabled : Disables XHCI Hand-off function**
BIOS Lock	Enable/Disable BIOS Lock function **Enabled : Enables BIOS Lock function (Default setting)** **Disabled : Disabled BIOS Lock funtion**

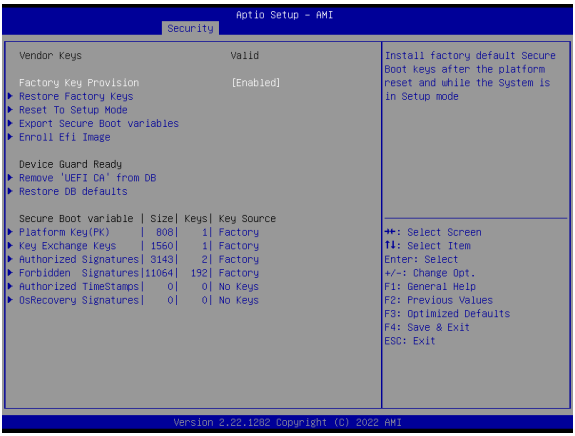
4.5 Security



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

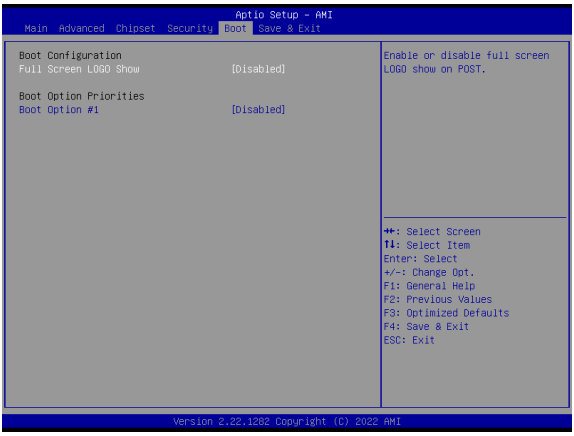


Item	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode **Enabled : Enables Factory Key Provision (Default setting)** **Disabled : Disables Factory Key Provision**
Restore Factory Keys	To restore factory settings
Reset To Setup Mode	Delete all Secure boot key databases from NVRAM
Export Secure Boot variables	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device
Enroll Efi Image	Allow the image to run in Secure Boot mode
Remove 'UEFI CA' from DB	To remove 'UEFI CA' from database
Restore DB defaults	Restore DB variables to factory defaults **Yes : Agree to restore DB defaults** **No : Cancel to restore DB defaults**

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	

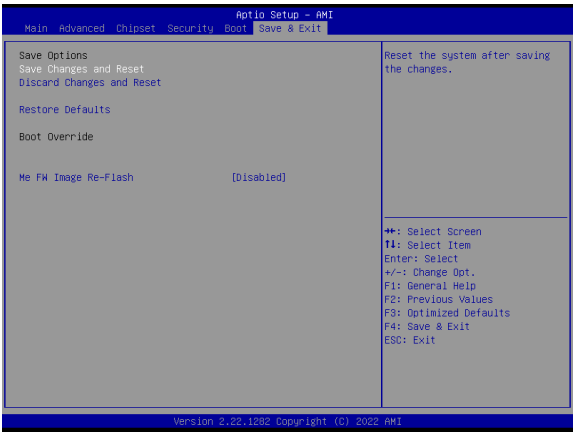
4.6 Boot

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)**
Boot Option #1	Shows the information of the storage that be installed in the system **Choose/set the boot priority**

4.7 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)**