OPS-H610B

Open Pluggable Specification (OPS)
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	10
External Antenna (25CA0-112001-A5S)	20
Exsiccator (25g)	10

※The ratio of OPS system to antennas is 1:2

Quantity of above items by varied based on the actual packing.
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.

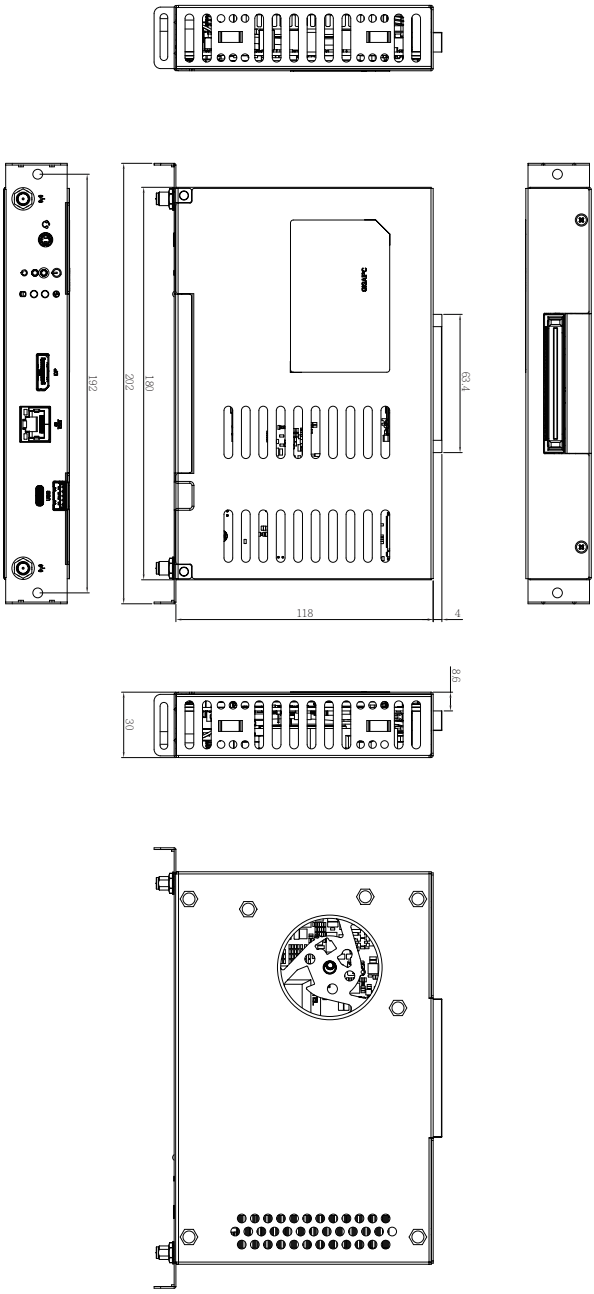
High Temperature Warning

(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


192
202
180
63.4
118
4
8.6
30

1.1 Specifications

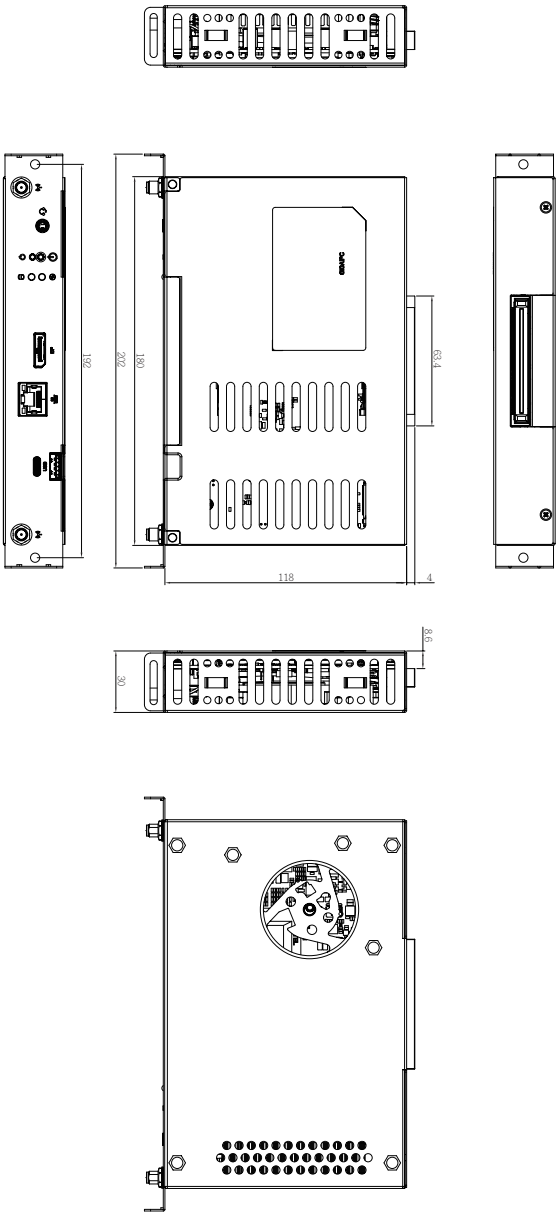
System	OPS-H610B (OP-H610B-SI)
Dimension	System Size : 180W x 120D x 30H (mm)
CPU	Support for 13th/12th Generation Intel Core i7/i5/i3, Pentium & Celeron processors in the LGA1700 package TDP under 35W ※ Please refer to CPU Support list for more information.
Chipset	Intel® H610 Chipset
Memory	1 x DDR4 SO-DIMM socket, Max. Capacity 16 GB Support Single channel DDR4 3200 MHz memory module
Ethernet	1 x GbE LAN Port (Realtek® RTL8111H)
Graphics support	Integrated Graphics Processor - depends on CPU: 1 x DP port, supporting a maximum resolution of 3840x2160 @60Hz (1 independent display outputs)
Audio	Realtek® ALC897
Expansion Slots	1 x 2280 M.2 M-Key (PCIe Gen 3x4) 1 x 2230 M.2 E-Key
Front I/O	1 x Display port 1 x RJ45 LAN Port 1 x USB 3.2 Type A Gen 1 1 x USB 3.2 Type C Gen 1 1 x Combo Audio Jack (Headphone & Headset) 2 x External Antenna Holes 1 x Reset button 1 x Power button 1 x PWR LED 1 x HDD LED
Rear I/O	1 x 80-pin JAE Tx25 OPS connector
TPM	Onboard TPM 2.0 security chip INFINEON SLB9670VQ2.0
OS Compatibility	Windows 10/11 (x64)

System	OPS-H610B (OP-H610B-SI)
Operation Temperature	Operating temperature: 0°C to 45°C Operating humidity: 0-90% (non-condensing) Non-operating temperature: -20°C to 70°C Non-operating humidity: 0%-95% (non-condensing) Use wide temperature range memory and storage
Vibration During Operation	Operation: IEC 60068-2-64, 1 Grms, random, 5 ~ 500 Hz, 1 hr / Per Axis, with SSD/M.2 2280 Non-operation: IEC 60068-2-6, 2 G, Sine, 10 ~ 500 Hz, 1 Oct/min, 1 hr / Per Axis
Shock During Operation	Operation: IEC 60068-2-27, 50 G, half sine, 11 ms duration, With SSD
Packaging Content	Carton size: 505 x 333 x 231 (mm) Packing Capacity: 10pcs Including: External Antenna x 20 (P/N: 25CA0-112001-A5S) ※ The ratio of OPS system to antennas is 1:2
Order Information	System: 6BOPH610BNR-SI (Bulk Packing)

Chapter 2

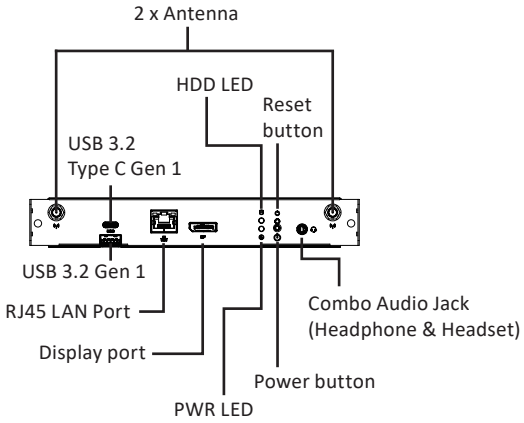
Chapter 2 – OPS-H610B (OP-H610B-SI)
Open Pluggable Specification System Kit

2.1 Dimension

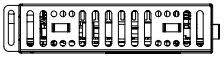


2.2 Getting Familiar with Your Unit

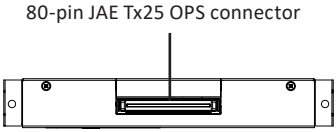
[Front Side]



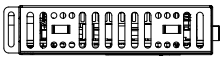
[Left Side]



[Rear Side]

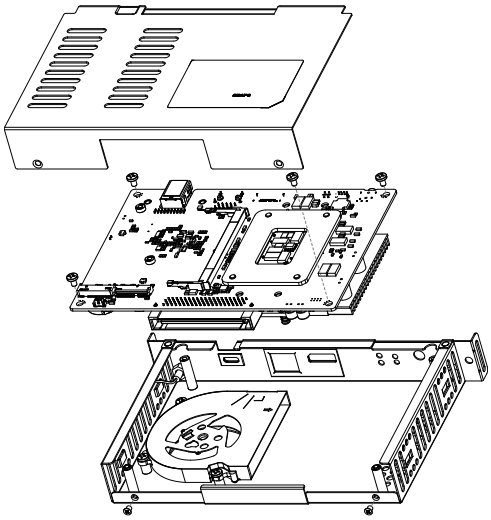


[Right Side]



[Install]

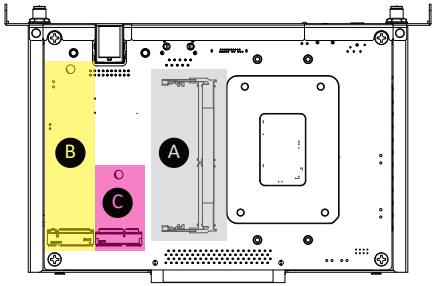
* Before opening the case, make sure to unplug the power cord.
* Before Connecting the power, make sure to fasten the case securely.



[Bottom PCB Side]

	Information
A	1 x DDR4 SO-DIMM socket

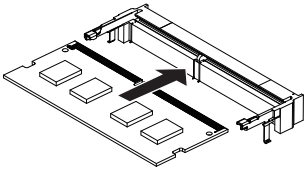
	Information
B	1 x M.2 slot 2280 M-key
C	1 x M.2 slot 2230 E-key



2.3 A) Memory Installation: DDR4 SO-DIMM

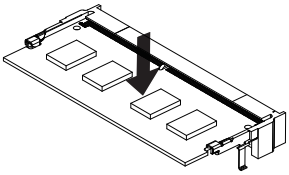
1

Carefully insert SO-DIMM memory modules.



2

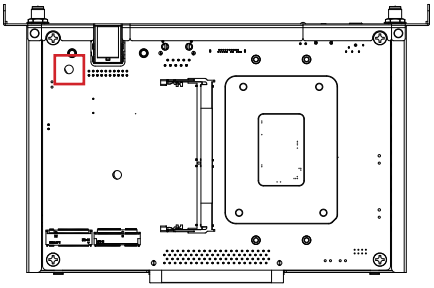
Push down until the modules click into place.



2.4 B) M.2 SSD Installation: How to safely install the M.2 2280 SSD

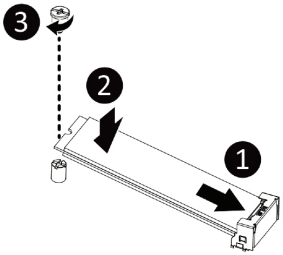
❶

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



❷

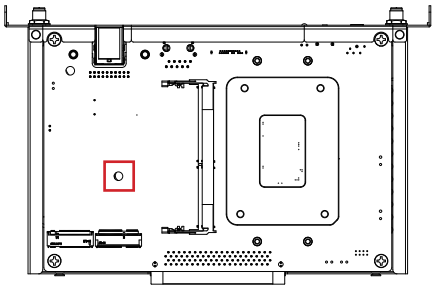
Carefully insert the M.2 SSD into the slot, and secure with the screw.



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

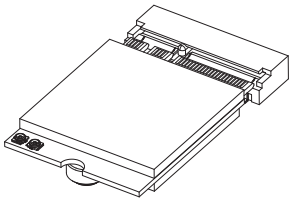
1

Remove the screw from the screw hole
(Location : MSO2)



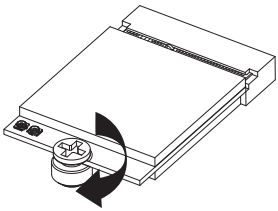
2

Carefully insert the wireless module into
the M.2 slot



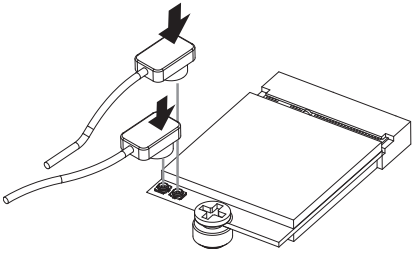
3

Lock the screw in the middle.



4

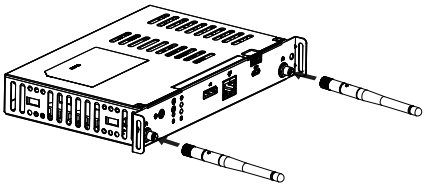
Install the antenna on the left side of the connection wireless module down.



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

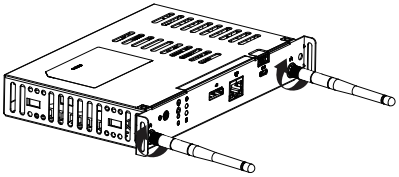
1

Carefully insert the antennas into the connectors.



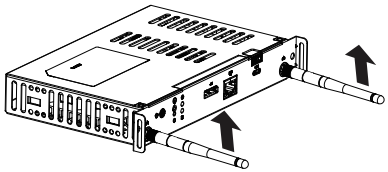
2

Turn the antennas clockwise until they are completely secure on the connectors.



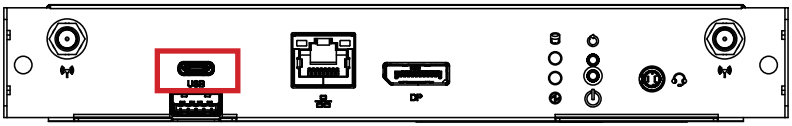
3

Flip up the antenna heads so that they are perpendicular to the machine.



2.7 I/O Pin-define

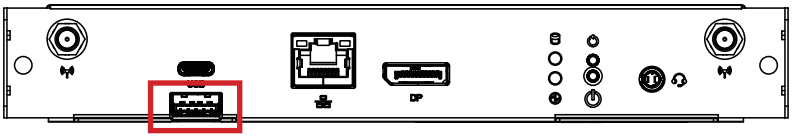
1. USB Type C Gen 1 port

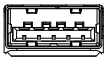


USB Type C Connector


Pin No.	Definition	Pin No.	Definition
A1	GND	B1	GND
A2	TX1+	B2	TX2+
A3	TX1-	B3	TX2-
A4	VBUS	B4	VBUS
A5	CC1	B5	CC2
A6	D+	B6	D+
A7	D-	B7	D-
A8	NC	B8	NC
A9	VBUS	B9	VBUS
A10	RX2-	B10	RX1-
A11	RX2+	B11	RX1+
A12	GND	B12	GND

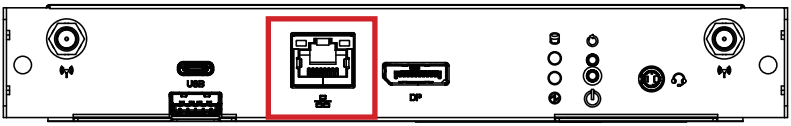
2. USB 3.2 Type A Gen 1 port



USB Connector


Pin No.	Definition
1	5V
2	D1n
3	D1p
4	GND
5	USB3_RX1n
6	USB3_RX1p
7	GND
8	USB3_TX1n
9	USB3_TX1p

3. RJ45 LAN Port

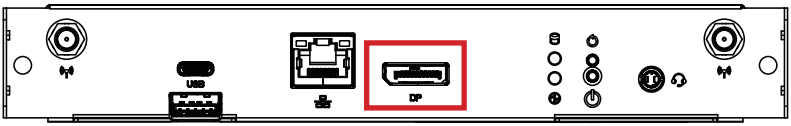


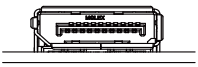
LAN Connector


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	1Gbps data rate
Green On	100Mbps data rate
Off	10Mbps data rate

4. Display port



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

2.8 Support

- For AVL list, go to: http://www.gigaipc.com
- To download the latest drivers, 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.

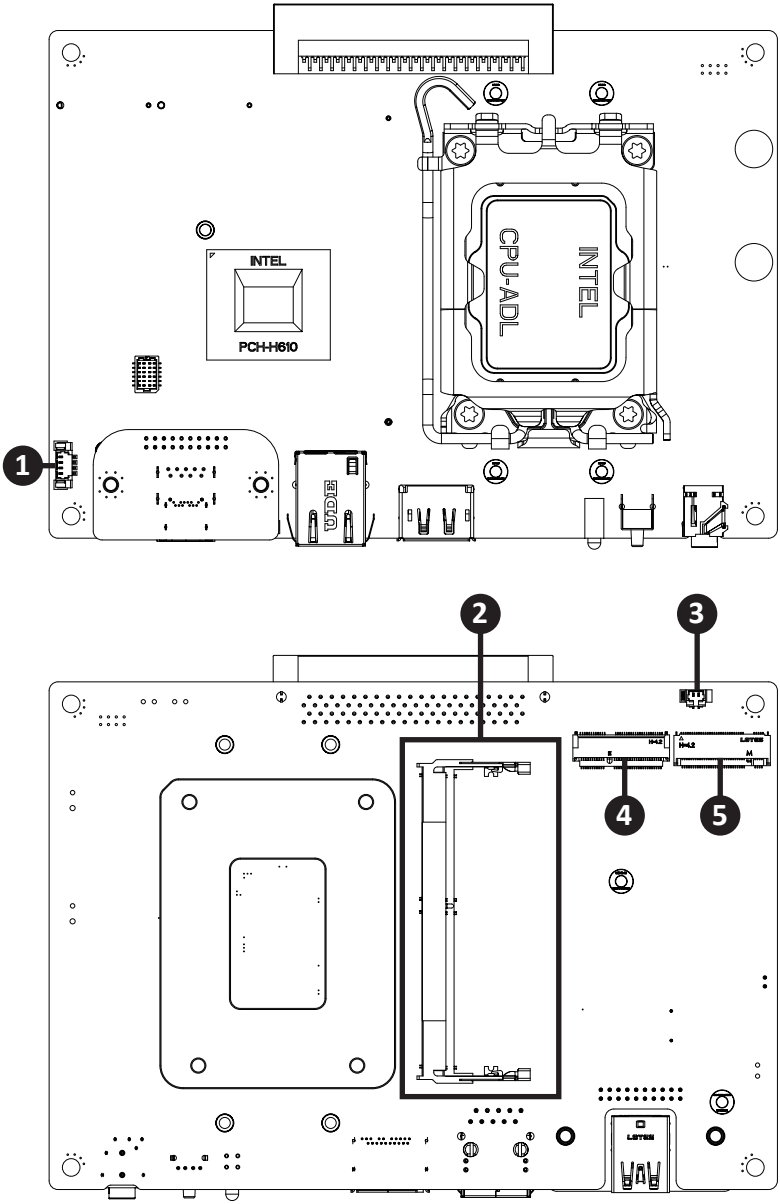
HIGH DEFINITION MULTIMEDIA INTERFACE

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

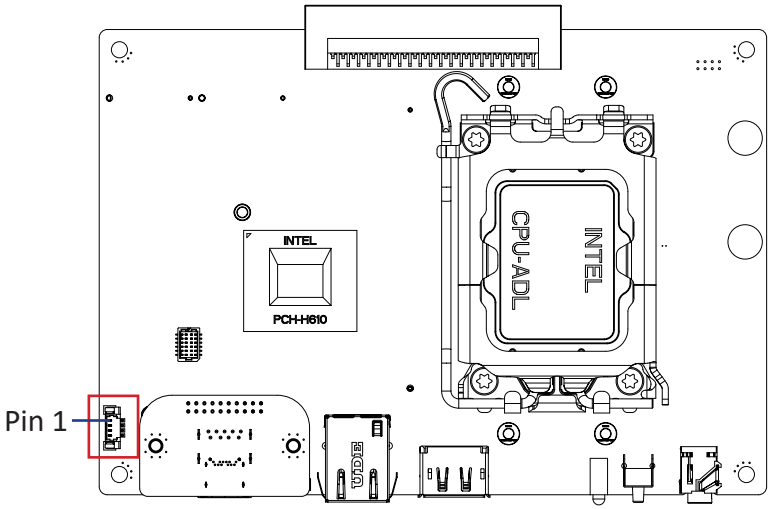
3.1 Jumpers and Connectors

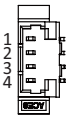


No	Code	Description
1	CPU_FAN	CPU fan connector
2	SODIMM	DDR4 SO-DIMM Slot
3	BATTERY	Battery cable connector
4	M2E	M.2 Slot, 2230 E-key
5	M2M	M.2 Slot, 2280 M-key

3.2.1 CPU_FAN (CPU fan connector)

1



CPU fan Connector


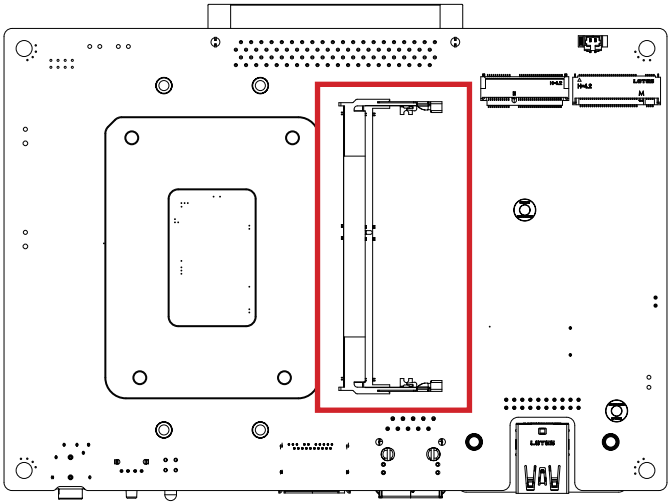
Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed control

Connector PN	Vendor
85205-0470N	ACES
A1250WV-S-04PC	JOINT-TECH

Connector type
1x4pin header, pitch 1.25mm

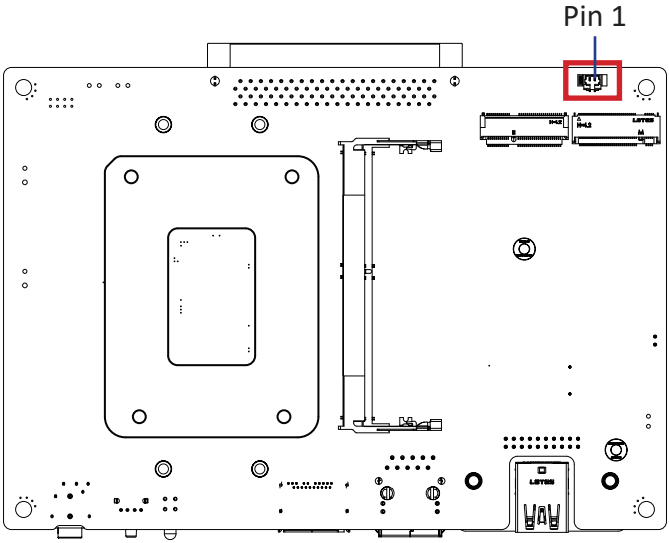
3.2.2 SODIMM (DDR4 SO-DIMM Slot)

❷



3.2.3 BATTERY (Battery cable Connector)

❸



Battery cable Connector
2 1 

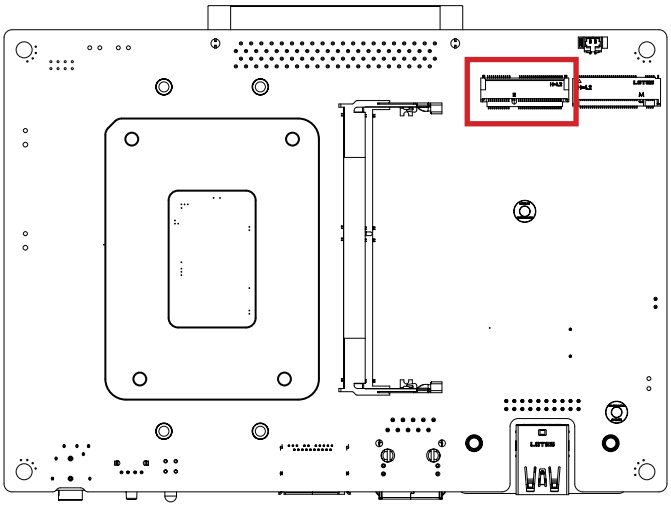
Pin No.	Definition
1	3V
2	GND

Connector PN	Vendor
85205-0270L	ACES
A1250WV-S-02PC	JOINT-TECH

Connector type
1x2pin header, pitch 1.25mm

3.2.4 M2E (M.2 Slot, 2230 E-key)

4



M.2 E Key Connector			
1			75
2			74

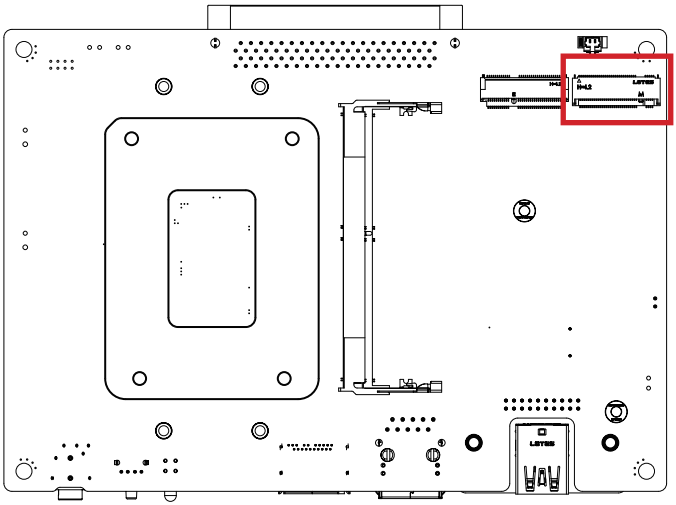
Pin No.	Definition	Pin No.	Definition
1	GND	2	3V
3	USB_Dp	4	3V
5	USB_Dn	6	NC
7	GND	8	NC
9	NC	10	NC
11	NC	12	NC
13	NC	14	NC
15	NC	16	NC
17	NC	18	GND
19	NC	20	NC
21	NC	22	NC
23	NC		

Pin No.	Definition	Pin No.	Definition
33	GND	32	NC
35	PCIe_TXp	34	NC
37	PCIe_TXn	36	NC
39	GND	38	CL_RST#
41	PCIe_RXp	40	CL_DATA
43	PCIe_RXn	42	CL_CLK
45	GND	44	NC
47	CLK_Dp	46	NC
49	CLK_Dn	48	NC
51	GND	50	SUSCLK
53	CLK_REQ	52	PCIe_RST
55	PCIe_WAKE	54	BT_Disable#
57	GND	56	PCIe_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	3V
75	GND	74	3V

Connector PN	Vendor
APCI0076-P001A	LOTES
AS0BC21-S40BE-7H	FOXCONN

3.2.5 M2M (M.2 Slot, 2280 M-key)

5



M.2 M Key Connector			
1			75
	M.2		
2			74

Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE_RXn3	6	NC
7	PCIE_RXp3	8	NC
9	GND	10	NC
11	PCIE_TXn3	12	3.3V
13	PCIE_TXp3	14	3.3V
15	GND	16	3.3V
17	PCIE_RXn2	18	3.3V
19	PCIE_RXp2	20	NC
21	GND	22	NC
23	PCIE_TXn2	24	NC
25	PCIE_TXp2	26	NC
27	GND	28	NC
29	PCIE_RXn1	30	NC
31	PCIE_RXp1	32	NC
33	GND	34	NC

Pin No.	Definition	Pin No.	Definition
35	PCIE_TXn1	36	NC
37	PCIE_ TXp1	38	DEVSLP
39	GND	40	NC
41	PCIE_RXp	42	NC
43	PCIE_RXn	44	NC
45	GND	46	NC
47	PCIE_TXn	48	NC
49	PCIE_TXp	50	PLT_RST
51	GND	52	CK_REQ
53	CLK_n	54	PCIE_WAKE#
55	CLK_p	56	NC
57	GND	58	NC

Pin No.	Definition	Pin No.	Definition
67	NC	68	SUSCLK
69	M2_SSD_ Detect	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

Connector PN	Vendor
APCI0073-P001A	LOTES
AS0BC21-S40BM-7H	FOXCONN

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

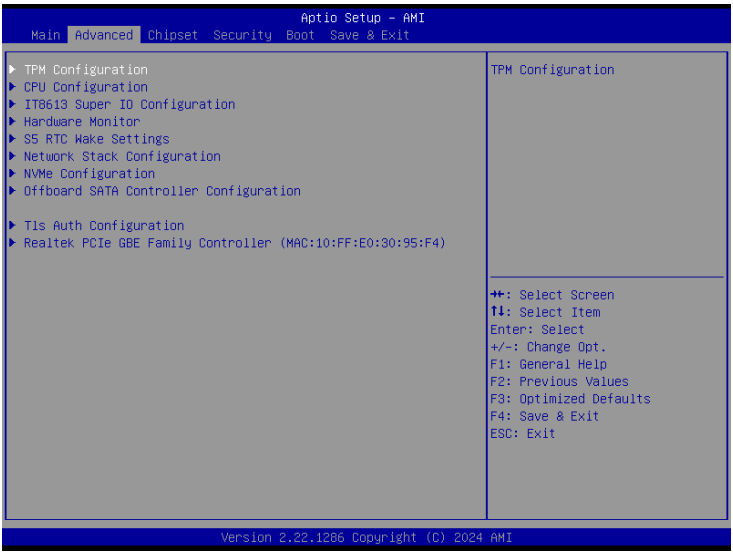
4.2 The Main Menu

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.
LAN MAC Address	Shows LAN1 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)

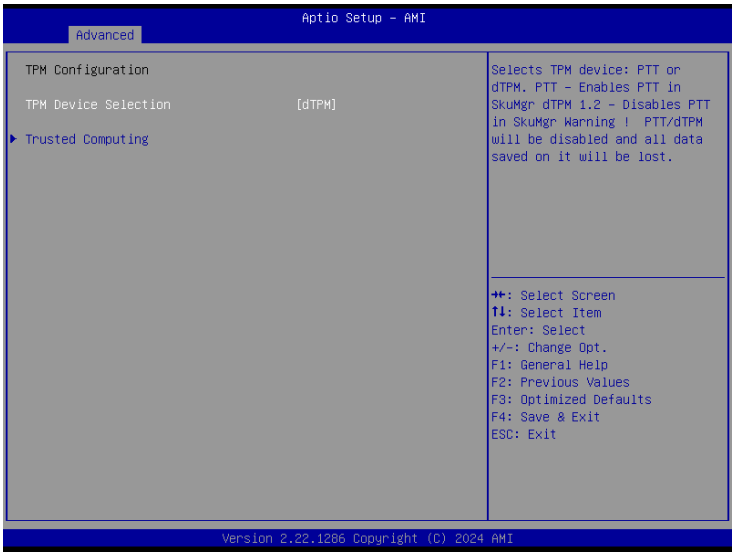
4.3 Advanced

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.



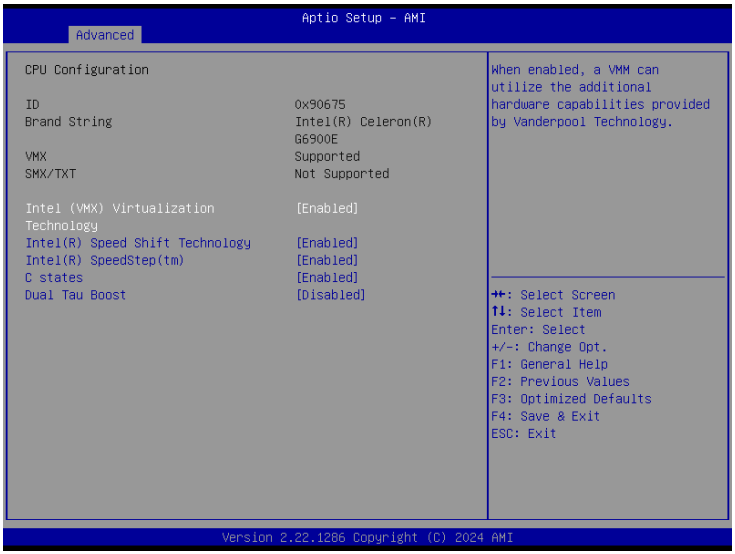
Item	Description
TPM Device Selection	**PTT : Internal TPM** **dTPM : External TPM (When using External TPM module or having TPM chip on MB)(Default setting)**

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**

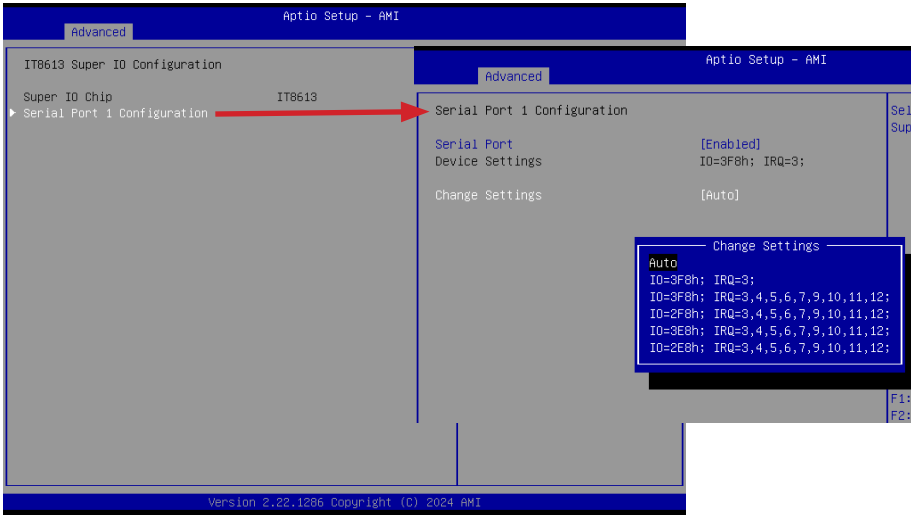
4.3.2 CPU Configuration

This submenu shows detailed CPU informations.



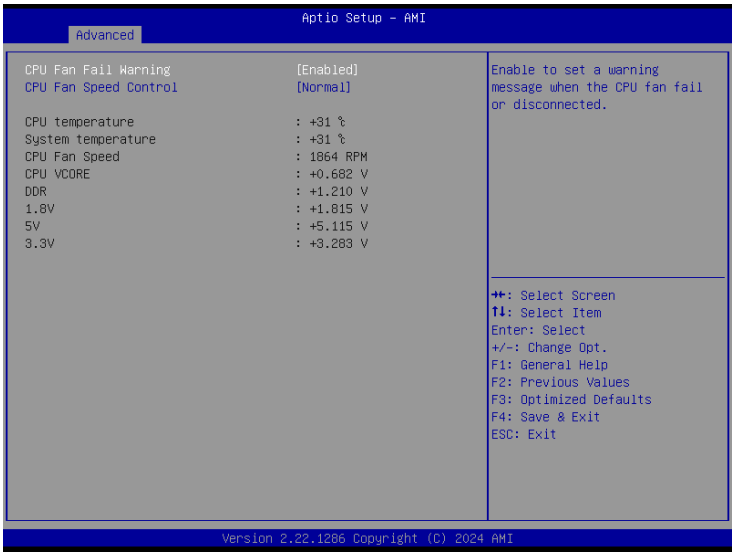
Item	Description
Intel (VMX) Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. **Enabled : 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**
C states	Command CPU to enter into low power consumption mode when CPU is under idle mode. **Enabled : Enables C states (Default setting)** **Disabled : Disables C states**
Dual Tau Boost	To optimize CPU performance. **Enabled : Enables Dual Tau Boost function** **Disabled : Disables Dual Tau Boost function (Default setting)**

4.3.3 IT8613 Super IO Configuration



Item	Description
Serial Port 1 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 Change settings : Auto (Default setting) IO=3F8h; IRQ=3; IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;

4.3.4 Hardware Monitor

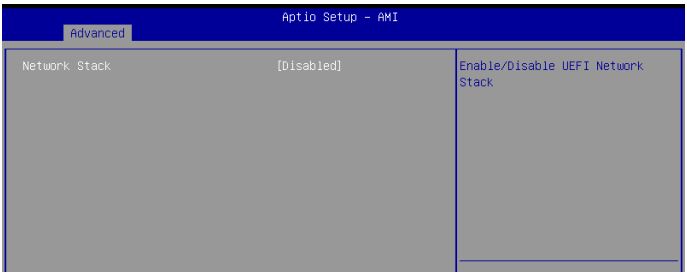


Item	Description
CPU Fan Fail Warning	**Enabled : Enables CPU FAN Fail warning alert function (Default setting)** **Disabled : Disables CPU FAN Fail warning alert function**
CPU Fan Speed Control	**Normal : Fan speed set by BIOS default(Default setting)** **Full Speed : Set Fan operates at full speed**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

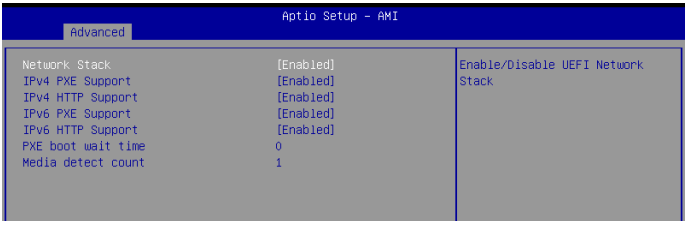
4.3.5 S5 RTC Wake Settings

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)**

4.3.6 Network Stack Configuration



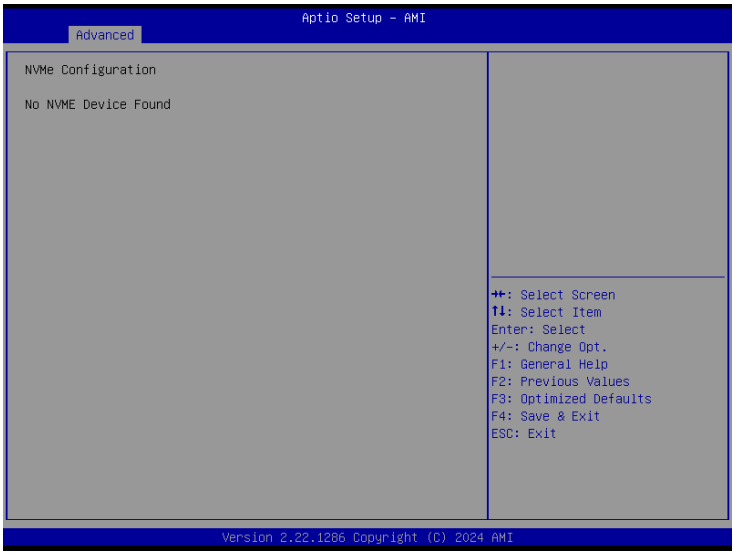
When Network stack is enabled :



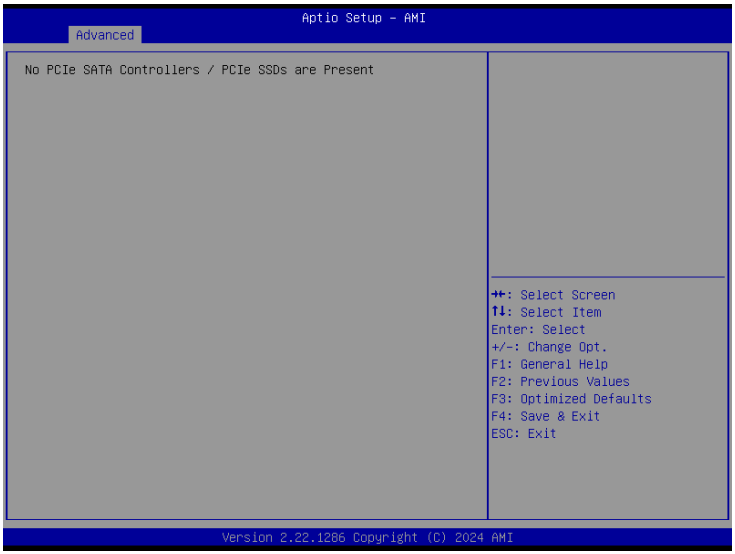
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode **Disabled : Disables UEFI Network Stack (Default setting)** **Enabled : Enables UEFI Network Stack**
IPv4 PXE Support	When Network stack is enabled : **Disabled : Disables IPv4 PXE Support** **Enabled : Enables 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.

4.3.7 NVMe Configuration

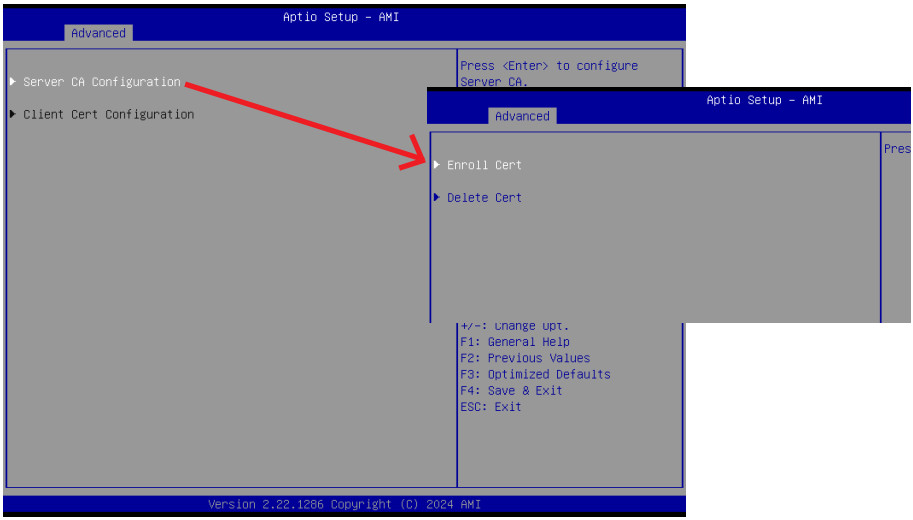
NVMe Configuration shows information when your M.2 NVMe PCIe SSD is installed.



4.3.8 Offboard SATA Controller Configuration



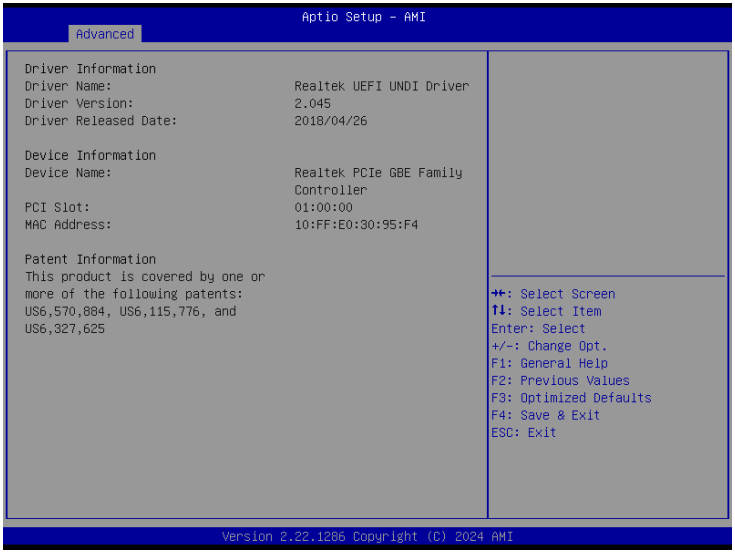
4.3.9 Tls Auth Configuration



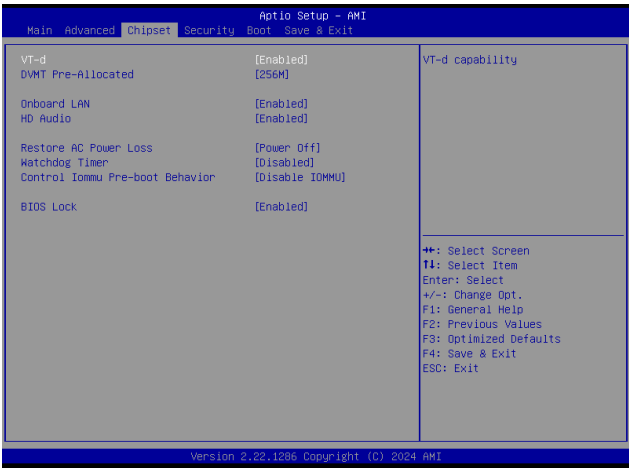
Item	Description
Enroll Cert	Press [Enter] to configure advanced items : **Server CA Configuration :** Enroll Cert : 1. Enroll Cert Using File 2. Cert GUID : Input digit character in 11111111-2222-3333-4444-1234567 890ab format. 3. Commit Changes and Exit 4. Discard Changes and Exit

4.3.10 Realtek PCIe GBE Family Controller (MAC:10:FF:E0:30:95:F4) (MAC address may varied based on different motherboard)

Shows Realtek Ethernet controller information

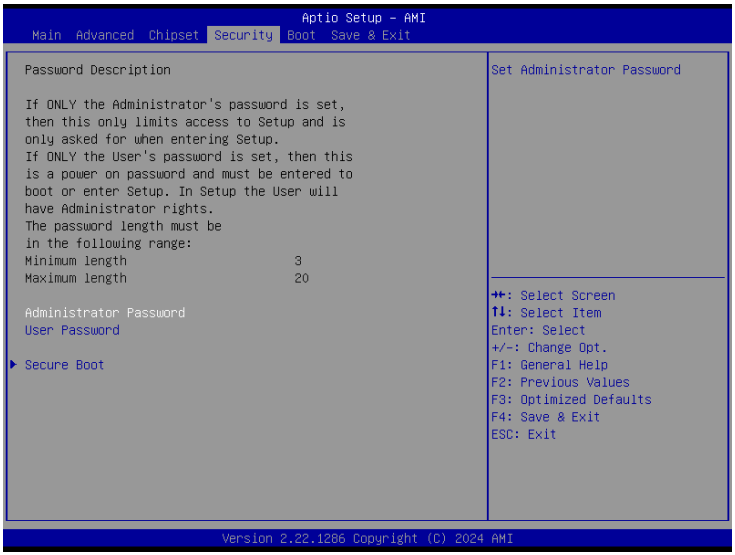


4.4 Chipset

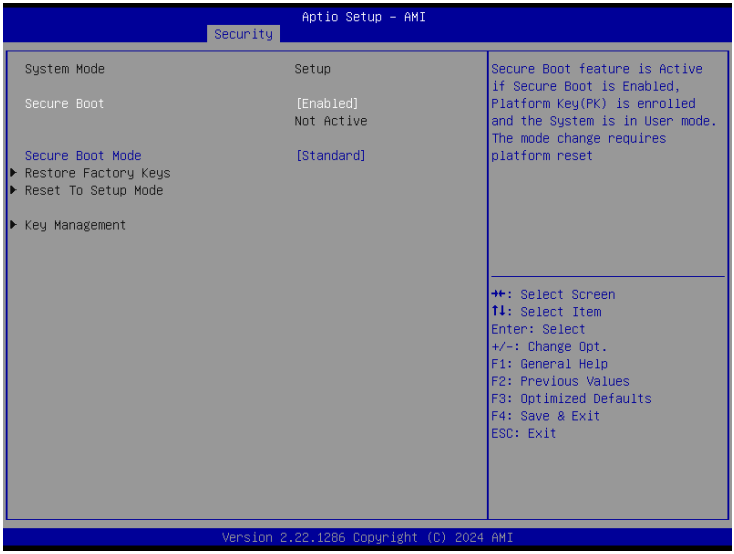


Item	Description
VT-d	**Enabled : Enables VT-d function (Default setting)** **Disabled : Disables VT-d function**
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor **Option items : 32M , 64M, 128M, 256M (Default setting)**
Onboard LAN	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 occured **Power on : System power on when the power is back** **Power off : Do not power on when the power is back (Default setting)** **Last state : Restore the system to the state before power loss occures**
Watchdog Timer	Enable/Disable Watchdog Timer function **Enabled : Enables Watchdog Timer function** **Disabled : Disabled Watchdog Timer function (Default setting)**
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**

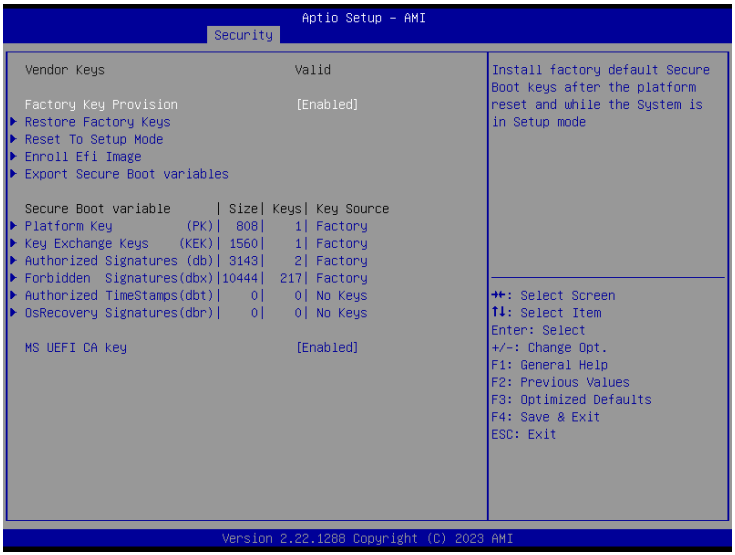
4.5 Security



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 (Default setting)** **Disabled : Disables Secure Boot function**
Secure Boot Mode	**Standard : Standard mode (Default setting)** **Custom : Custom mode**
Restore Factory Keys	When Secure Boot mode is set to Custom : To restore factory settings **Yes : Agree to restore factory settings** **No : Cancel to restore factory settings**
Reset To Setup Mode	When Secure Boot mode is set to Custom : **Yes : Agree to setup mode** **No : Cancel to setup mode**
Key Management	When Secure Boot mode is set to Custom : 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

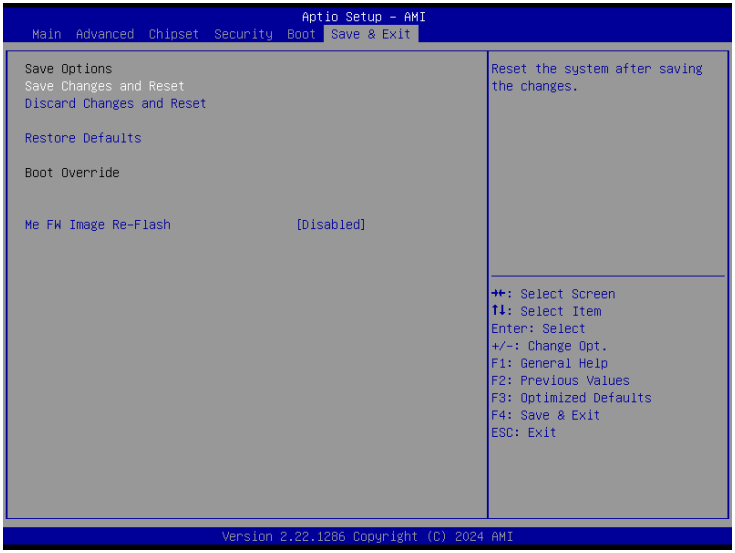
Item	Description
Platform Key (PK)	These items allows you to enroll factory defaults or load Certificates from a file.
Key Exchange Keys (KEK)	
Authorized Signatures (db)	
Forbidden Signatures (dbx)	
Authorized TimeStamps (dbt)	
OsRecovery Signatures (dbr)	
MS UEFI CA Key	Device Guard ready system must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

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)**
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 Priorites	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)**