

QBiX-JMB-CMLA47EHG-B1

Industrial System with Intel® Q470E Chipset,
Support for Intel® 10th Gen. Core™ i Processor

Startup Manual

Packing List

Before you begin installing your card, please make sure that the following items have been shipped:

For Main system : 9BQJQ47EAMR-SI

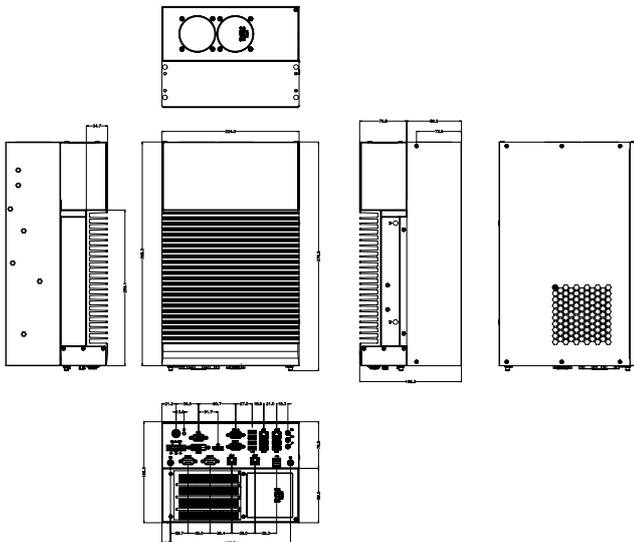
1. Terminal Blocks Male Plug x 1 (P/N: 25IO0-2ESDVO-D2R)
2. Screw M3x4L x 16 (P/N : 25984G-1C014-S00)

*Quantity of the HDD screws in the accessory kit may decreased based on actual HDD assemble quantity.

For Expansion slot kit : 6BQJH310BPR-SI

1. Power Cable #18 350mm x 2 (P/N: 25CRI-35030I-S9R)
2. Screw #6-32x4L x16 (P/N: 25KS2-13004F-S0R)

Dimension



Caution: DANGER OF EXPLOSION

IF BATTERY IS INCORRECTLY

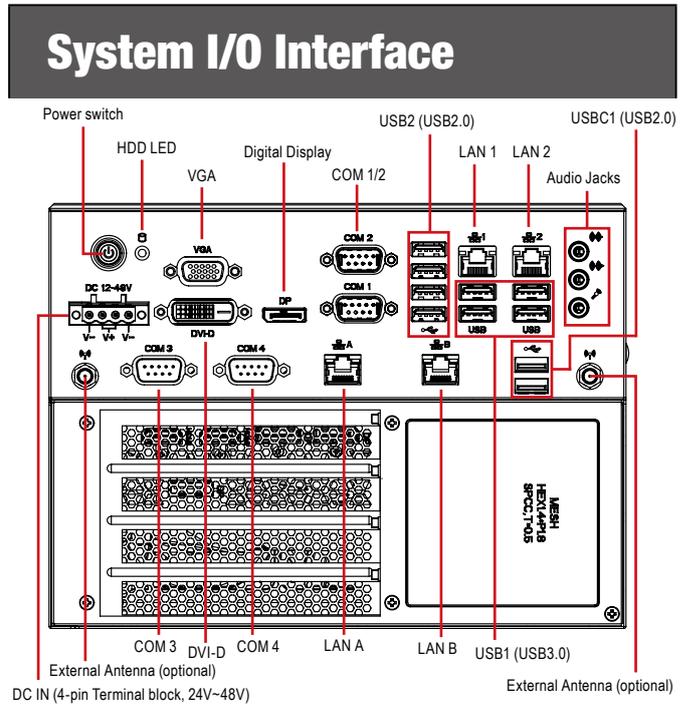
REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED

BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

Specifications

Dimension	System Size: 224W x 368D x 166.3H(mm) - Discrete GFX support (Optional)
CPU	Support for 10th Generation Intel® Core™ i9/i7/i5/i3, Pentium® and Celeron® processors in the LGA1200 package, TDP under 65W
Chipset	Intel® Q470E Express Chipset
Memory	2 x DDR4 SO-DIMM sockets supporting up to 64 GB, Dual channel DDR4 2933/2666 MHz
Ethernet	1 x GbE LAN Port (Intel® I219V) 3 x GbE LAN Ports (Intel® I211AT)
Graphic support	Integrated Graphics Processor - Intel® HD Graphics support: 1 x DVI-D port, supporting a maximum resolution of 1920x1080 @60Hz 1 x D-Sub port, supporting a maximum resolution of 1920x1080 @60Hz 1 x DP port, supporting a maximum resolution of 4096x2160 @60Hz (3 independent displays output)
Audio	Realtek® Audio Codec
Storage	4 x 2.5" HDD/SSD (SATA 6Gb/s)
Expansion Slots	1 x 2280 M.2 M-Key (PCIe x4 & SATA 6Gb/s) 1 x 2230 M.2 E-Key 1 x Full-size mini PCIe with SIM slot 1 x PCIe slot -- Discrete riser card support

Front I/O	1 x Power Switch/Power/HDD LED 3 x Audio Jacks (Line in, Line out, Mic in) 1 x Display Port/1 x DVI-D/1 x VGA 2 x COM Ports (RS-232/422/485 & RI/5V/12V) 2 x COM Ports (RS-232) 4 x RJ45 LAN Ports 4 x USB 3.2 Gen 1 6 x USB 2.0 1 x 4-pin Terminal Block 2 x External Antenna Holes (Optional)
Riser Card (Optional)	1 x PCIe x4 (Gen3 x4) 2 x PCIe x16 — Single at Gen3 x16 only or — Dual at Gen3 x8 + Gen3 x8
Power	+24V~48VDC (Full Range) -- Support discrete GFX card
Operation Temperature	For Main system : Operating temperature: -20°C to 50°C (CPU 65W TDP) Operating temperature: -20°C to 60°C (CPU 35W TDP) For Full system : Depends on the Graphic cards installed in the system 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, 1 Grms, random, 5 ~ 500 Hz, 1 hr / Per Axis, with SSD/M.2 2280 & Without Graphics Cards 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	For Main system : 9BQJQ47EAMR-SI Carton size: 351 x 300 x 166 (mm) Packing Capacity: 1pc Including: Terminal Blocks Male Plug x 1 (P/N: 25I00-2ESDV0-D2R) Screw M3x4L x 16 (P/N : 25984G-1C014-S00) *Quantity of the HDD screws in the accessory kit may decreased based on actual HDD assemble quantity. For Expansion slot kit : 6BQJH310BPR-SI Carton size: 460 x 315 x 279 (mm) Packing Capacity: 1pc Including: Power Cable #18 350mm x 2 (P/N: 25CRI-35030I-S9R) Screw #6-32x4L x16 (P/N: 25KS2-13004F-S0R)
Order Information	System : 9BQJQ47EAMR-SI & 6BQJH310BPR-SI (Built in Components: Please contact with your sales representative for more information or e-mailed to : sales@gigaipc.com)

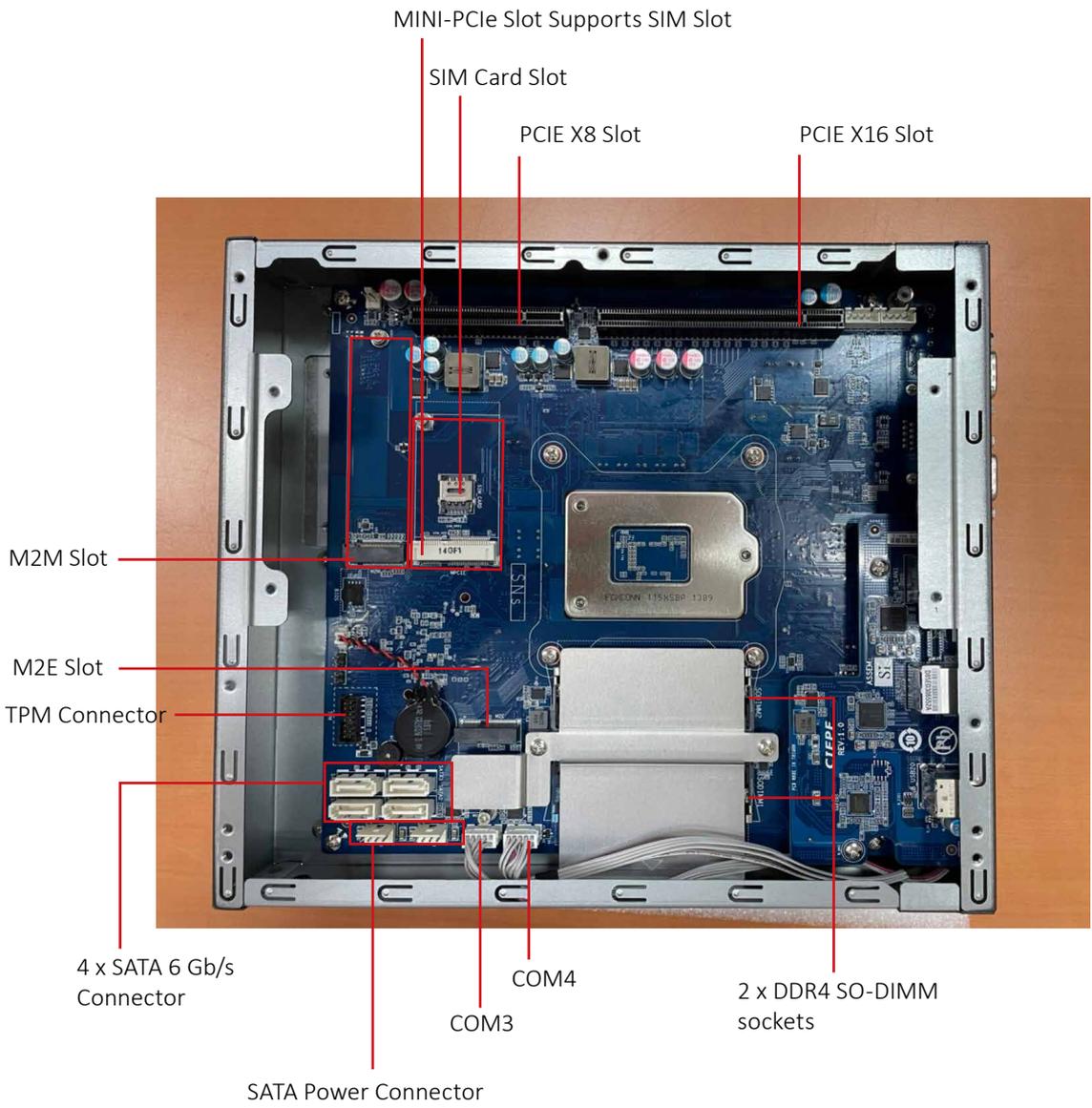


Jumpers and Connectors

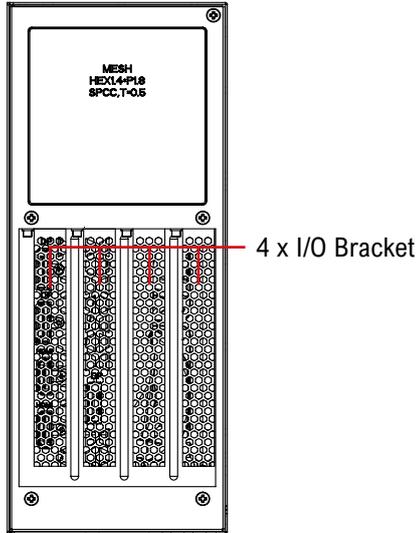
The board has a number of jumpers that allow you to configure your system to suit your application. The table below lists the function of each of the jumpers and connectors.

Front I/O Connectors		
No.	Code	Scripton
1	VGA	VGA Connector
2	DVI-D	DVI-D Connector
3	DP	Digital Display Port
4	COM 1/2	RS-232/422/485
5	COM 3/4	RS-232
6	USB 1	4 x USB 3.2 Gen 1
7	USB 2	4 x USB 2.0
8	USB C1	2 x USB 2.0
9	LAN 1	Intel® I219V
10	LAN 2	Intel® I211AT
11	LAN A	Intel® I211AT
12	LAN B	Intel® I211AT
13	LED	Power and Storage Device Status LED
14	DC-24-48V	Power connector
15	Audio	Audio Jacks (Line in, Line out & Mic in)

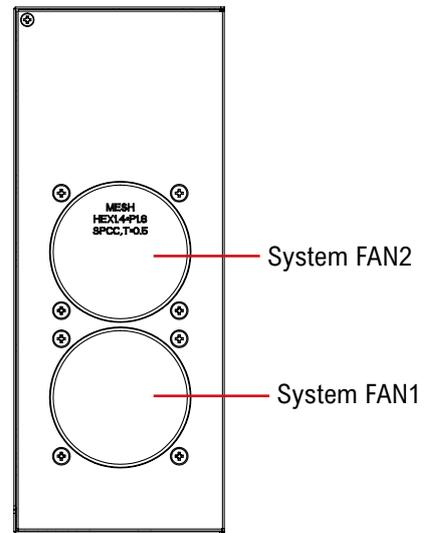
Internal I/O Connectors



Expansion Front View

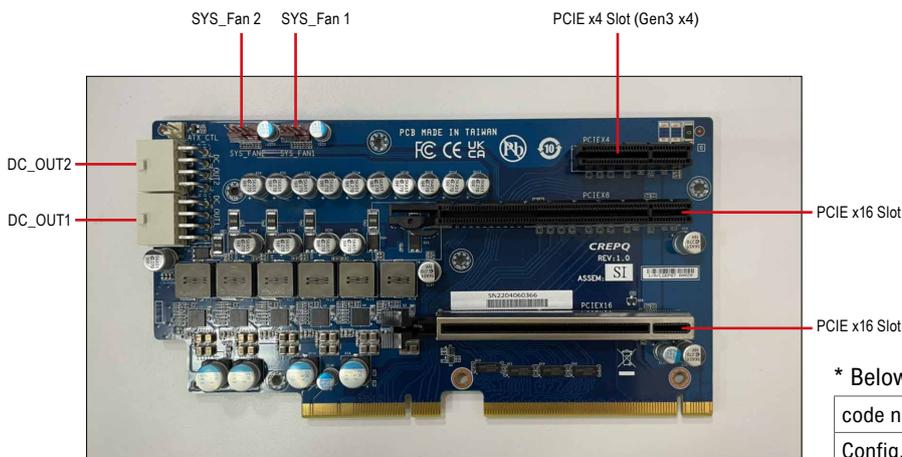


Expansion Rear View



Expansion I/O Connectors

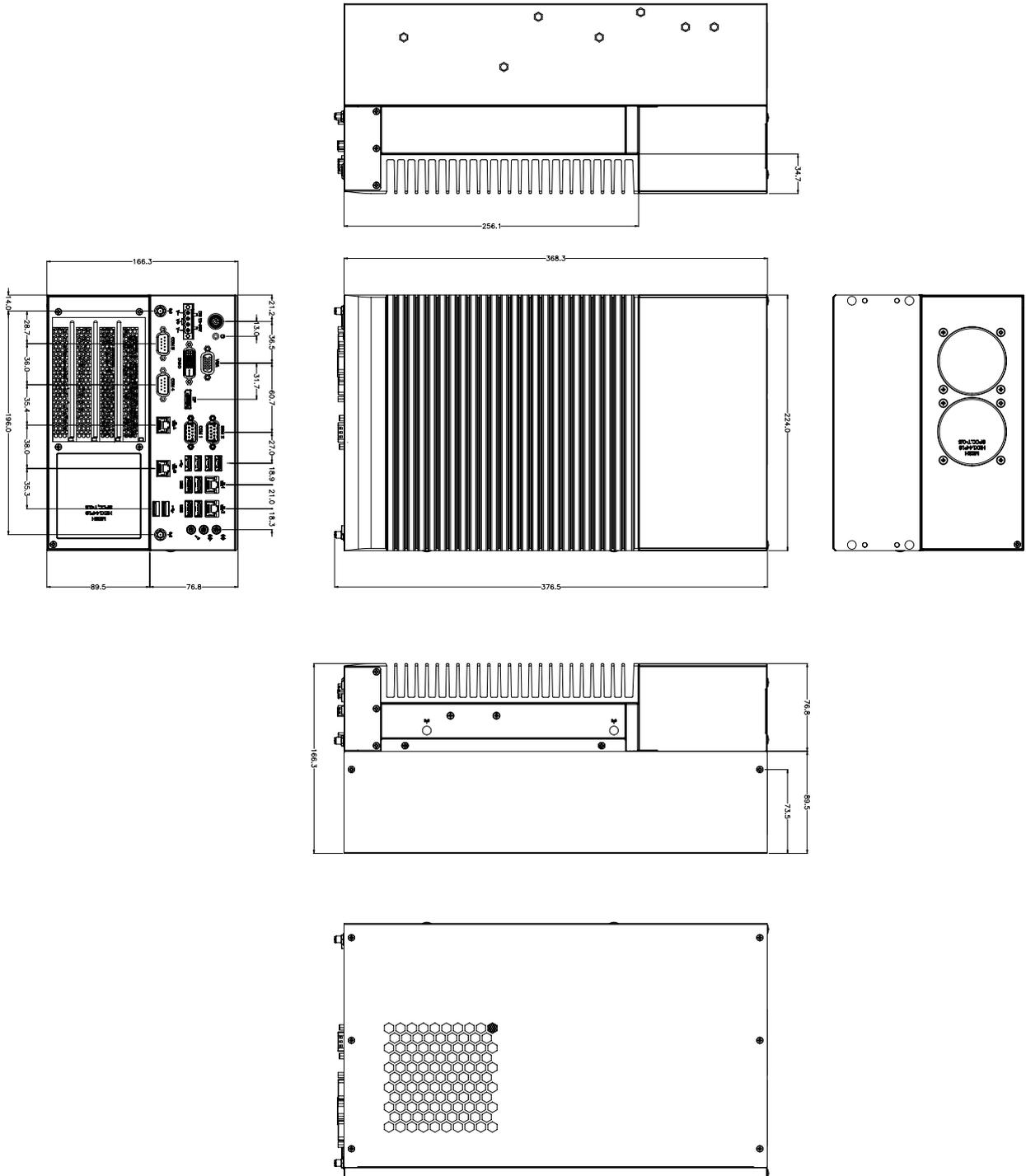
No.	Code	Scripton
1	DC_OUT1	GPU Power Supply Connector DC Output 1
2	DC_OUT2	GPU Power Supply Connector DC Output 2
3	SYS_FAN1	Fan1 Power Connector
4	SYS_FAN2	Fan2 Power Connector
5	PCIEX4	PCIE x4 Slot (Gen3 x4)
6	PCIEX8	PCIE x16 Slot*
7	PCIEX16	PCIE x16 Slot*



* Below are the possible configurations :

code name	PCIEX8	PCIEX16	
Config. 1	0	Signal at x16	
Config. 2	Signal at x8	Signal at x8	By auto switch

System Dimensions



Simple Installation Process

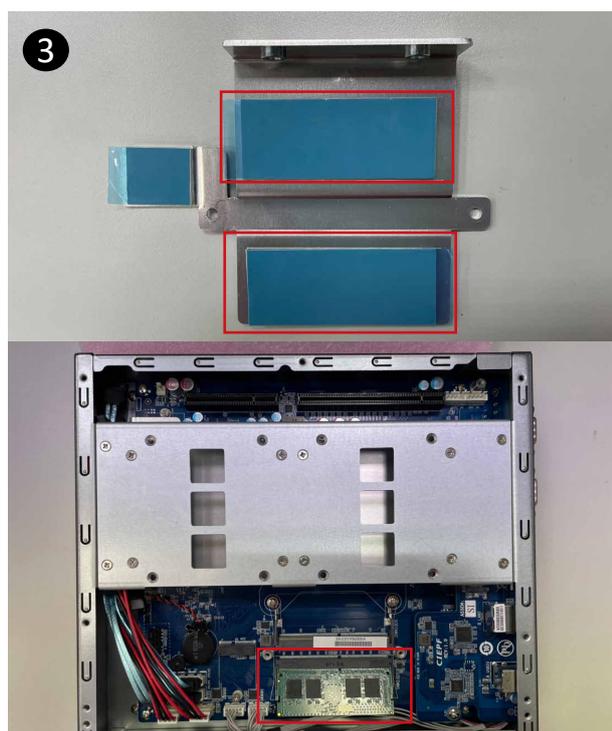
Memory Installation

QBiX-JMB-CMLA47EH-A1 supports DDR4 SO-DIMM type memory module.

1. Loosen 7 screws and remove the bottom cover.
2. Loosen 4 screws to remove memory thermal cover.
3. Remove the release paper, and assemble memory.
4. Install 4 screws and memory thermal cover.

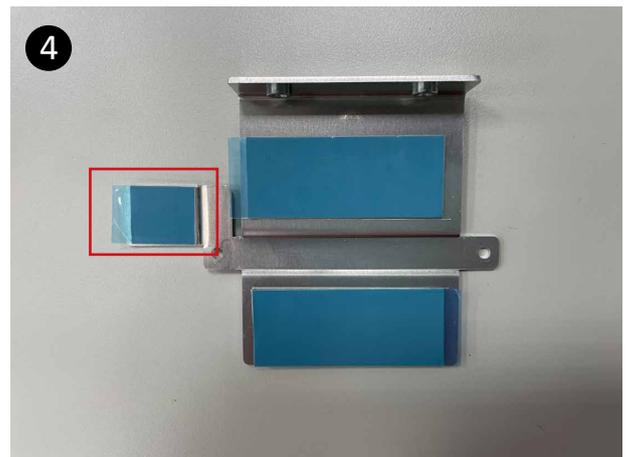
Note : Thermal pad and memory thermal cover must be fully mated and compacted.

5. Replace the bottom cover and secure with screws.



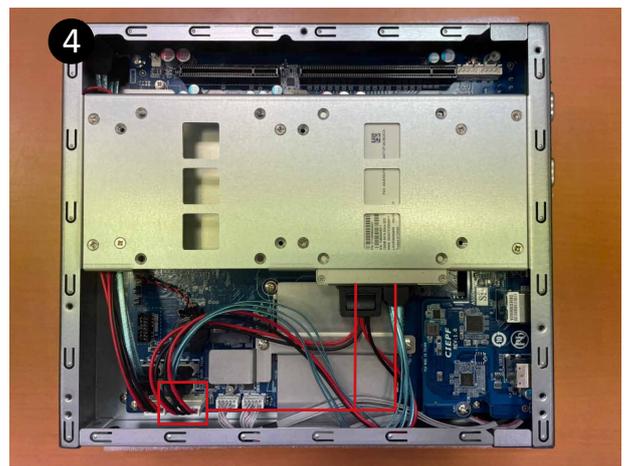
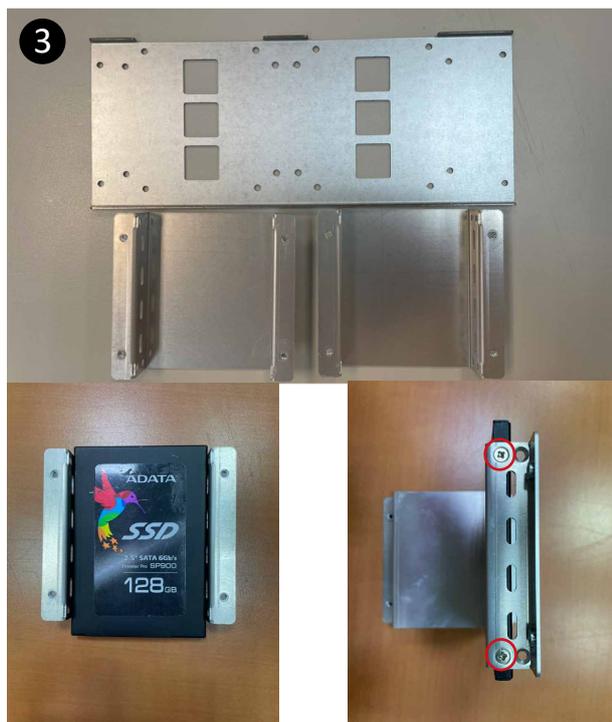
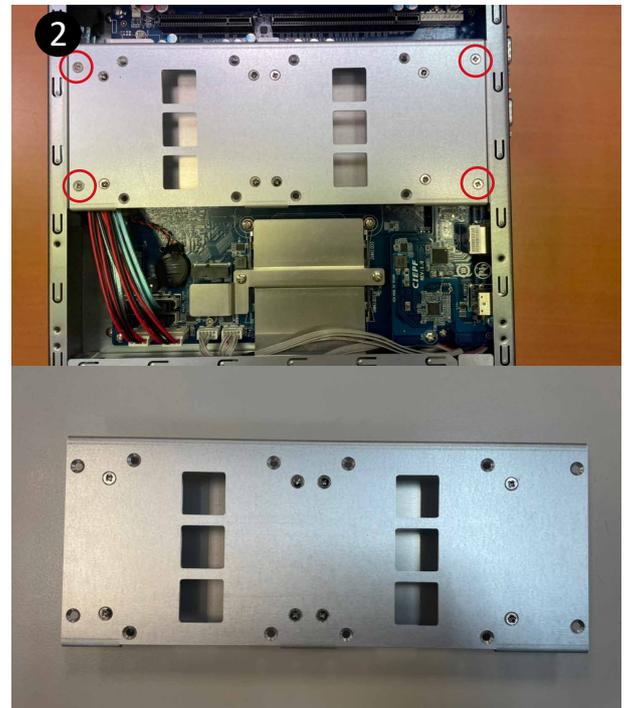
M2E (Support NGFF-2230 Wifi/BT) Installation

1. Loosen 7 screws and remove the bottom cover.
2. Loosen 4 screws to remove M2E thermal cover.
3. Install the module in the M2E (Support NGFF-2230 Wifi/BT) slot and secure with screws.
4. Remove the release paper on the thermal pad.
5. Install 4 screws and M2E thermal cover.
6. Replace the bottom cover and secure with screws.



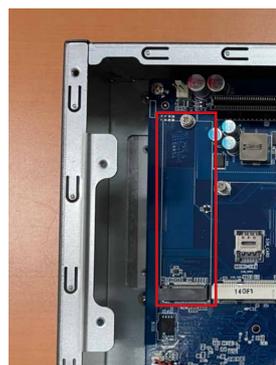
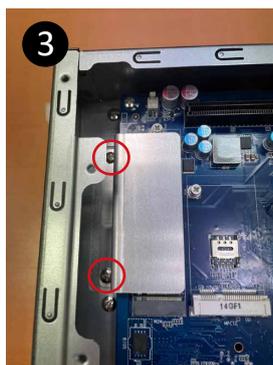
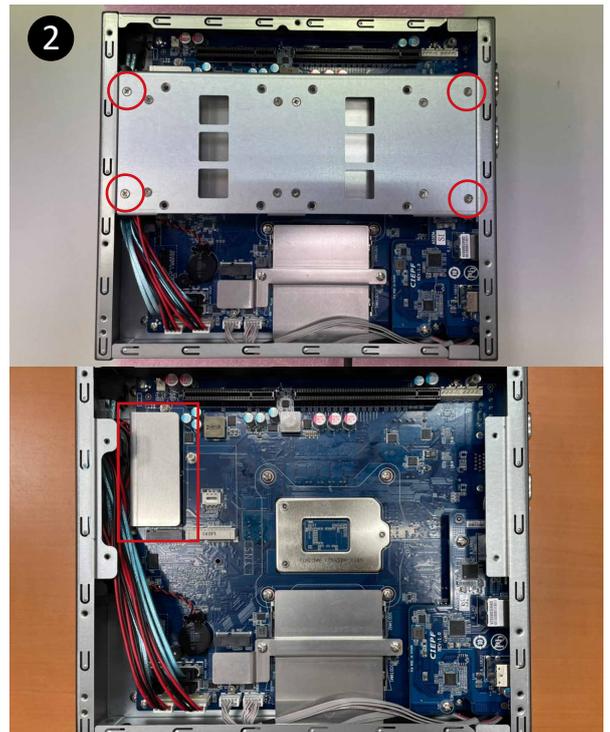
Storage Installation 1 (2.5" HDD/SSD)

1. Loosen 7 screws and remove the bottom cover
2. Loosen 4 screws to remove storage tray.
3. Secure storage with 4 x screws.
4. Assemble SATA cable/power cable and replace storage tray securely with 4 x screws.
5. Replace the bottom cover and secure with screws.



Storage Installation 2 (M2M Storage)

1. Loosen 7 screws, and then remove the bottom cover
2. Loosen 4 screws to remove storage tray.
3. Loosen the 2 screws to remove the aluminum heat sink.
4. Assemble the M2M (NGFF-2280 SATA) storage hard drive, and remove the release paper which is on the aluminum heat sink.
5. Install the 2 screws to securely replace the aluminum heat sink and heat sink paste.
6. Install 4 screws to firmly install storage tray.
7. Replace the bottom cover and secure with screws.



Mini-PCle Slot (PClex1 + USB2.0) and SIM Card Slot Installation

QBiX-JMB-CMLA47EH-A1 supports one full size Mini-PCle.

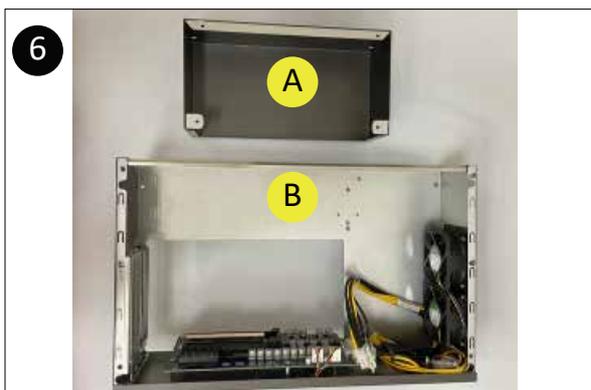
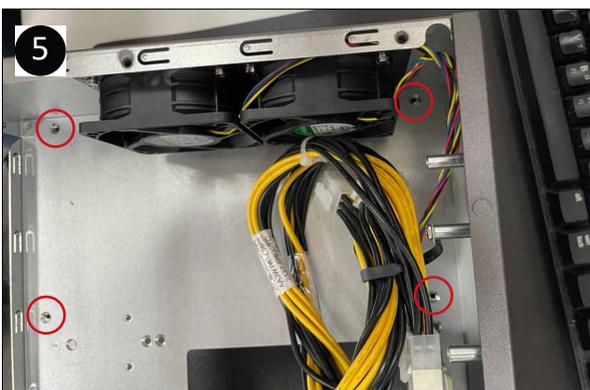
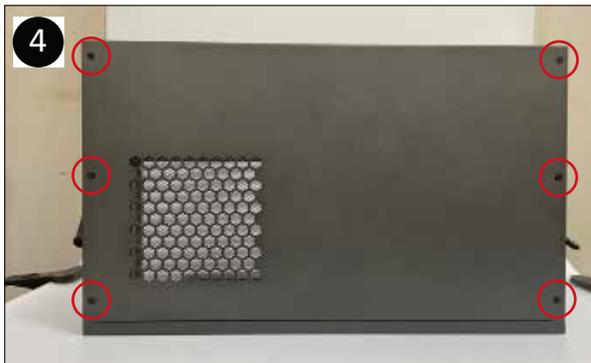
1. Loosen 7 screws, and then remove the bottom cover.
2. Loosen 4 screws to remove storage tray.
3. Assemble the Mini-PCle expansion Card (Mini-PClex1 + USB2.0) or 3G/4G SIM Card in SIM Slot.
4. Install 4 screws to firmly install storage tray.
5. Replace the bottom cover and secure with screws.



How to combine the QBiX-JMB-CMLA47EH-A1 system & PCI-E extension chassis

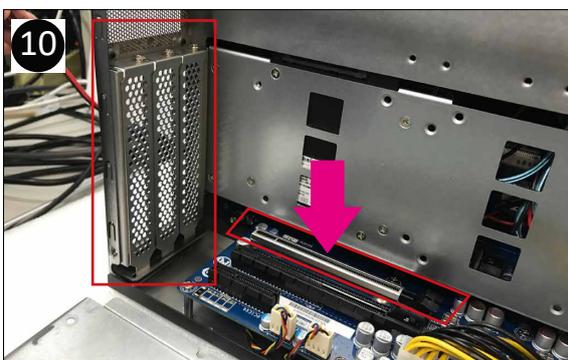
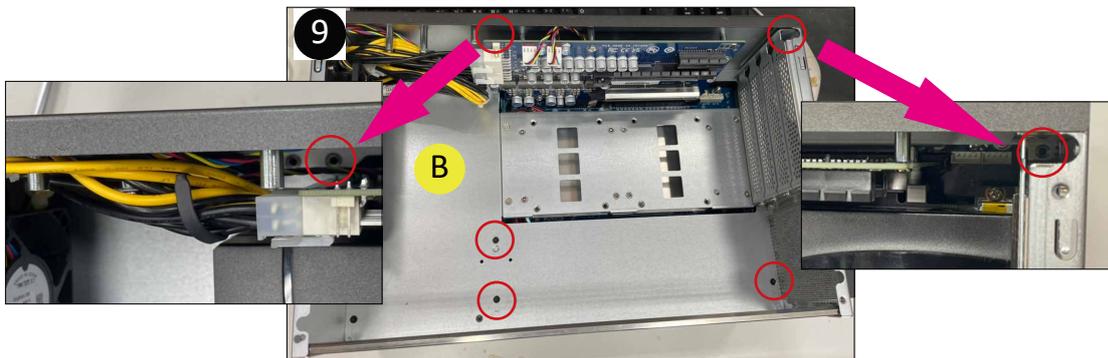
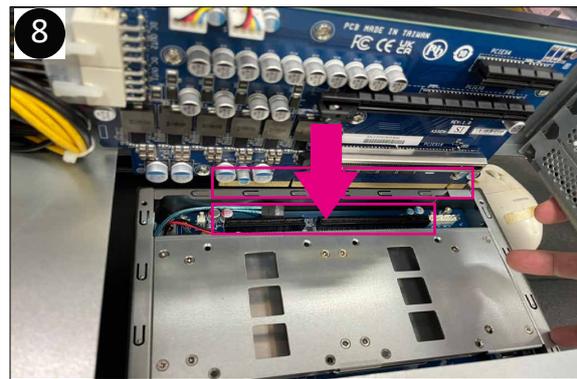
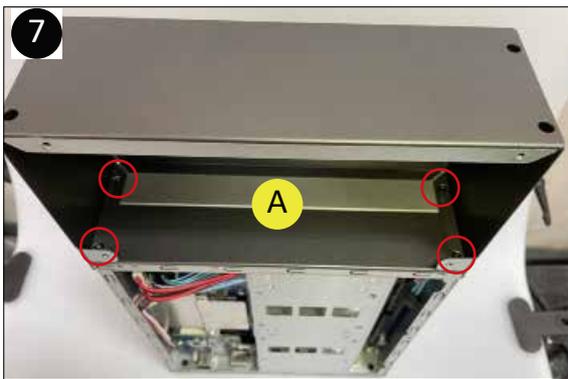
QBiX-JMB-CMLA47EHG-B1 is combined with QBiX-JMB-CMLA47EH-A1 and Expansion PCIE Slot Chassis.

1. Loosen 7 screws and remove the bottom cover of QBiX-JMB-CMLA47EH-A1. (refer Figure 1 and 2)
2. Loosen 8 screws and remove the cover of Expansion PCIE Slot Chassis. (refer Figure 3 and 4)
3. Loosen 4 screws on the system fan side of Expansion PCIE Slot Chassis to separate into 2 parts as below A & B parts. (refer Figure 5 and 6)



How to combine the QBiX-JMB-CMLA47EH-A1 system & PCI-E extension chassis (Cont.)

4. Assemble 4 screws (Torsion : 4- 5 kgf.cm) to fix A parts on the QBiX-JMB-CMLA47EH-A1 system (refer Figure 7)
※ Recommend to use at least 15cm length screwdriver.
5. Insert the PCIe riser card into PCI-E slot of QBiX-JMB-CMLA47EH-A1 system from Top to Bottom. (refer Figure 8)
6. Assemble 5 screws (Torsion : 4- 5 kgf.cm) to fix B parts on the QBiX-JMB-CMLA47EH-A1 system. (refer Figure 9)
7. Remove the screws on the IO Bracket, and then insert the graphic card into the PCI-E slot of PCI-E extension chassis from top to bottom. Connect the power cord in the extension card to the power connector of the graphics card (refer Figure 10 and 11)



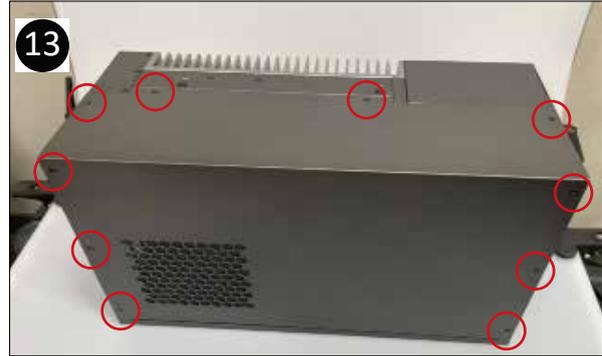
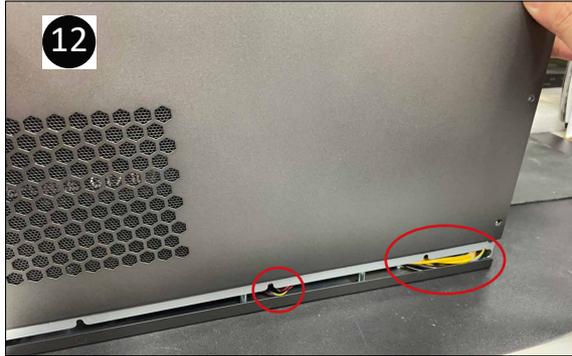
NOTE 1 : To connect 1 or 2 power cables on the graphic cards is depends on different graphic card spec.

NOTE 2 : If only 1 power connector on the graphic card, you can choose any one of two power cables for connection.

NOTE 3 : The graphic card model uses on above picture (refer Figure 11) is for reference only.

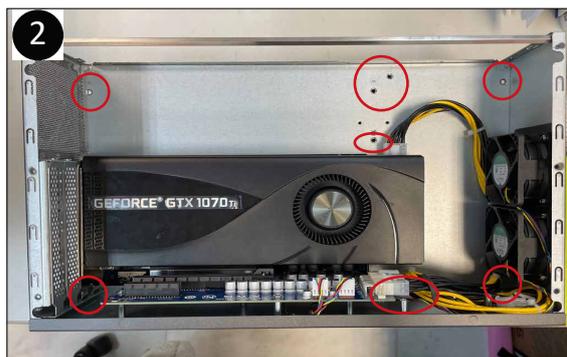
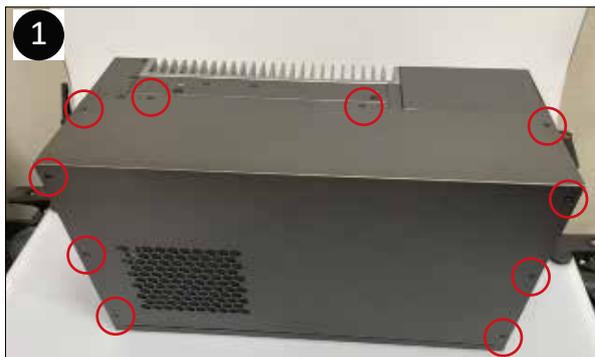
How to combine the QBiX-JMB-CMLA47EH-A1 system & PCI-E extension chassis (Cont.)

8. Reinstall the cover back, and please be careful for the cables that may be harmed by the cover. (refer Figure 12)
9. Assemble 10 screws (Torsion : 4- 5 kgf.cm). (refer Figure 13)



How to disassemble the graphic card

1. Remove 10 screws to open the bottom cover. (refer Figure 1)
2. Remove 9 screws to separate the QBiX-JMB-CMLA47EH-A1 system and PCI-E extension chassis. (refer Figure 2, or please refer to page 11/Figure 5 and page 12/Figure 9)
3. Push the lock on the PCIe slot down to easily disassemble the graphic card. (refer Figure 3)
4. Disassemble the graphic card from the PCIe slot. (refer Figure 4)



NOTE 1 : The graphic card model in this page is for reference only.

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this Startup Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. **DO NOT COVER THE OPENINGS.**
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
 - The power cord or plug is damaged.
 - Liquid has penetrated into the equipment.
 - The equipment has been exposed to moisture.
 - The equipment does not work well, or you cannot get it to work according to the user's manual.
 - The equipment has been dropped and damaged.
 - The equipment has obvious signs of breakage.
15. **DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40°C (-40°F) OR ABOVE 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.**
16. **CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.**
17. **RESTRICTED ACCESS AREA:** The equipment should only be installed in a Restricted Access Area.
18. **DISCLAIMER:** This set of instructions is given according to IEC 704-1. GIGAIPC disclaims all responsibility for the accuracy of any statements contained here in.

QBiX-JMB-CMLA47EHG-B1

Industrial Fanless System with Intel® Q470E Chipset,
Support for Intel® 10th Gen. Core™ i Processor

BIOS Manual

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.

How to Entering into BIOS menu

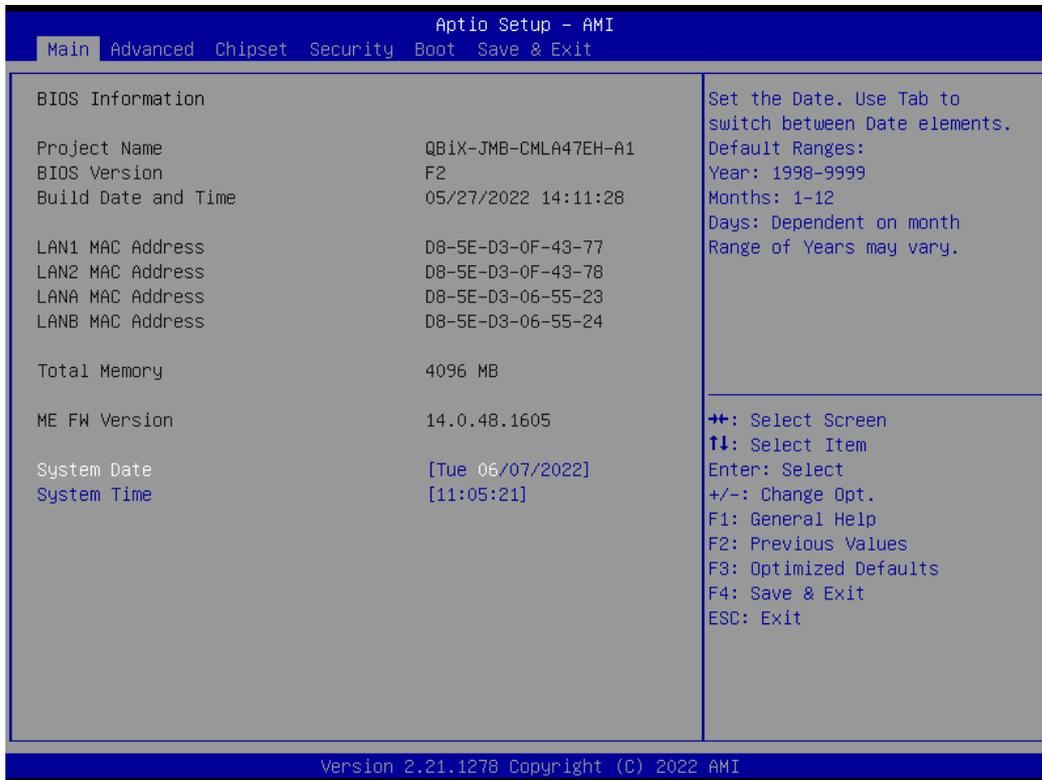
Once the system is power on, press the key as soon as possible to access into BIOS Setup program.

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

1. The Main Menu

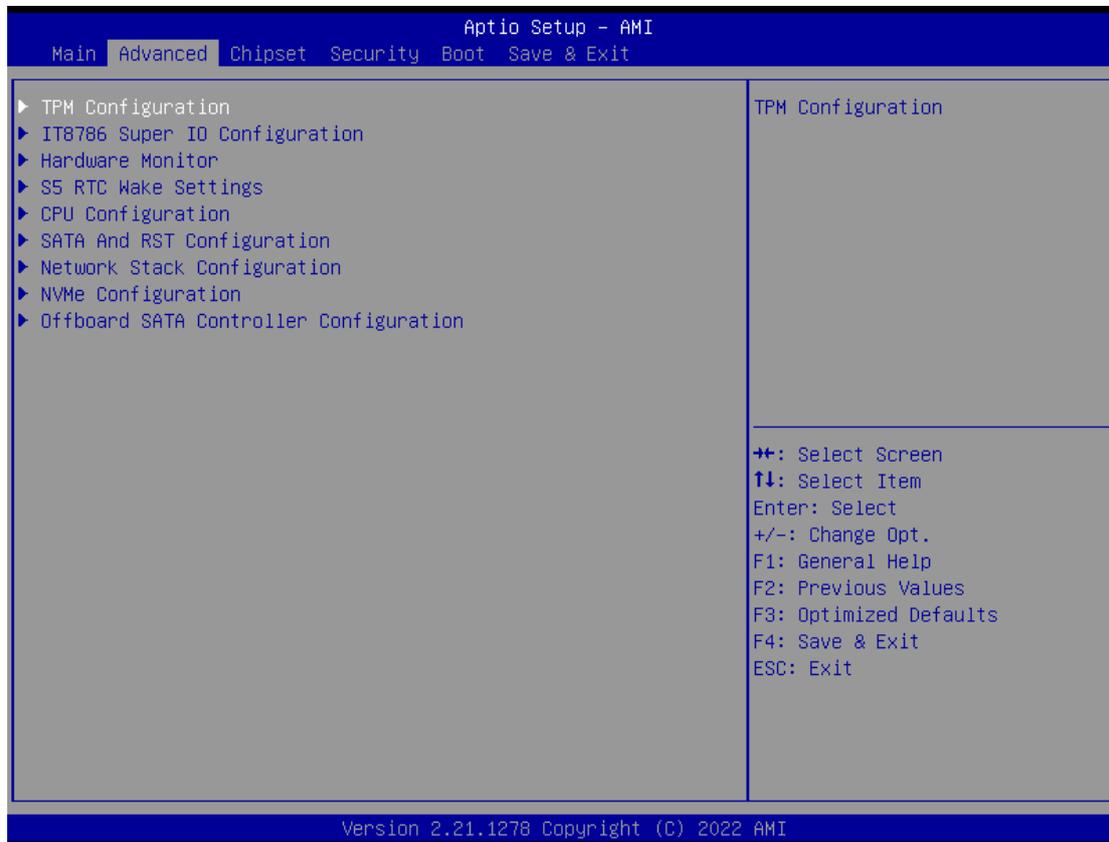
The main menu shows the basic system information. Use arrow keys to move among the items.



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
LANA MAC Address	Shows LANA MAC Address information
LANB MAC Address	Shows LANB 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)

2. 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.



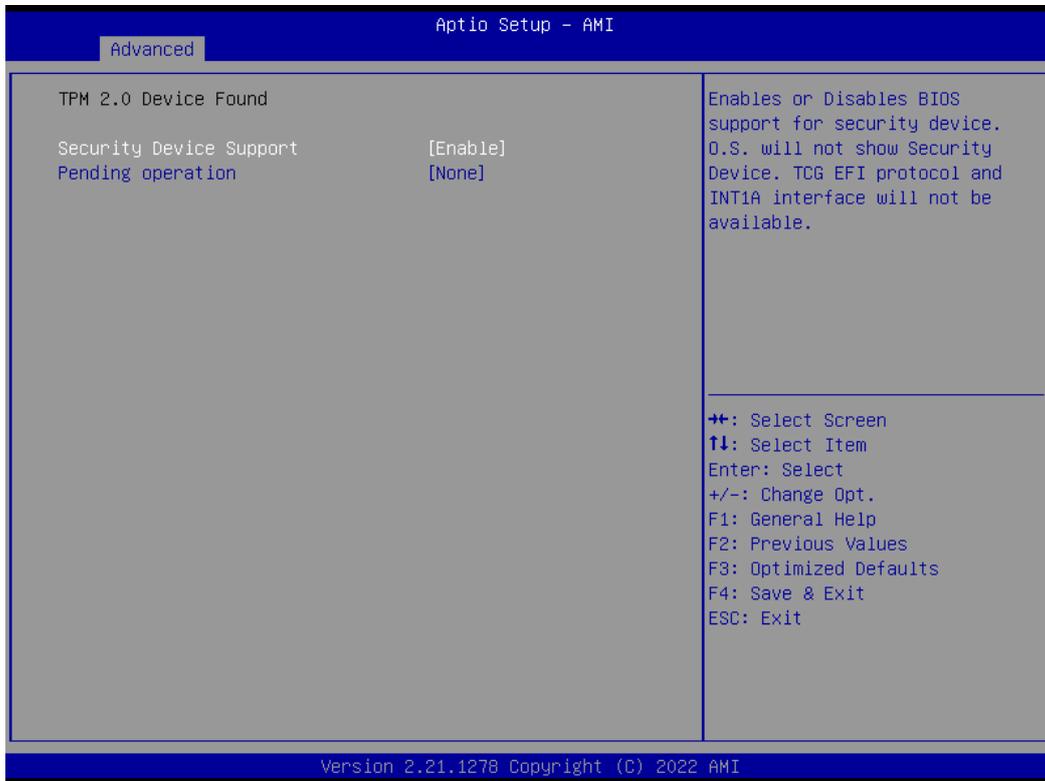
2.1 TPM configuration

Use TPM Configuration submenu to choose TPM interface.



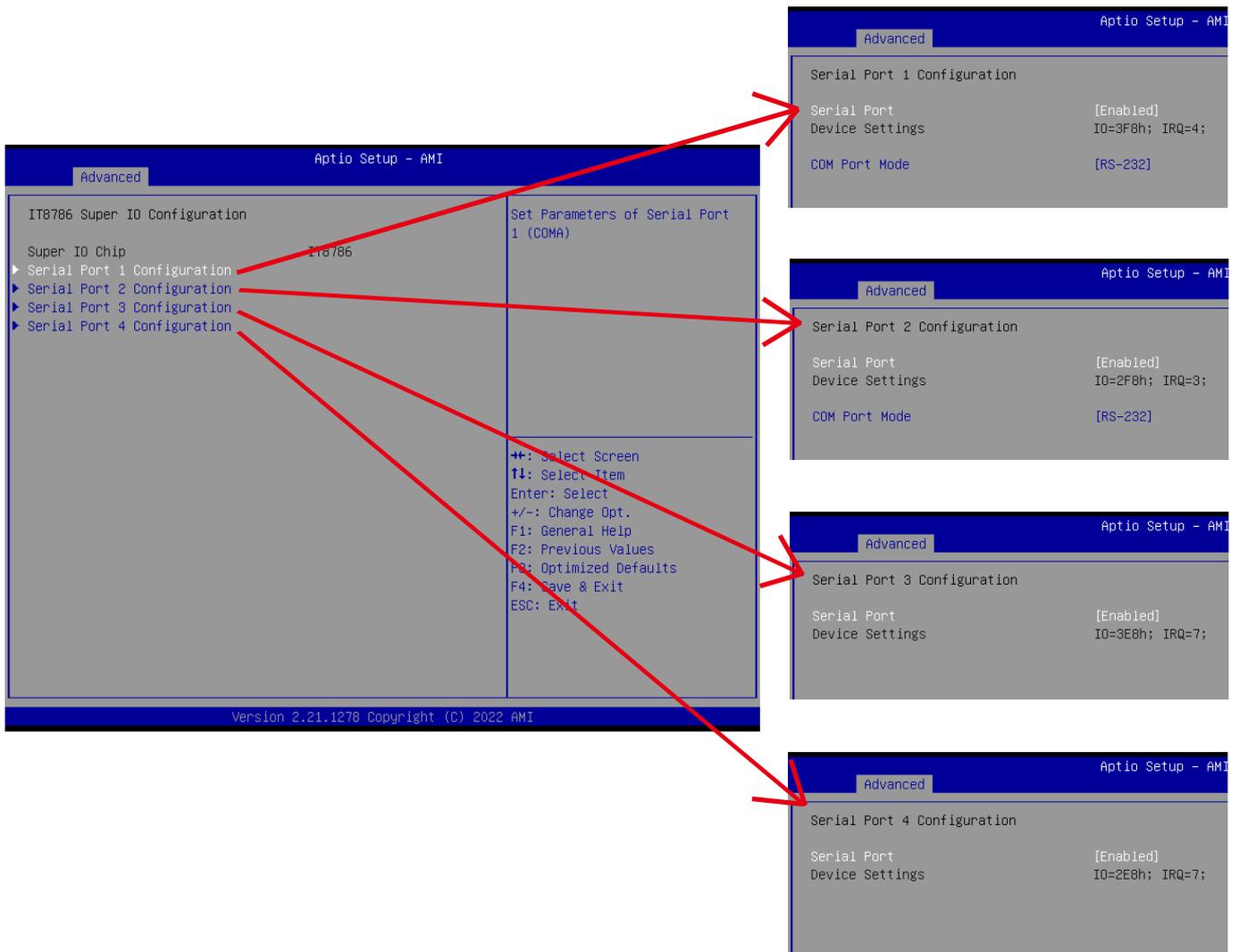
Item	Description
TPM Device Selection	PTT : Internal TPM (Default setting) dTPM : External TPM (When using External TPM module or having TPM chip on MB)

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



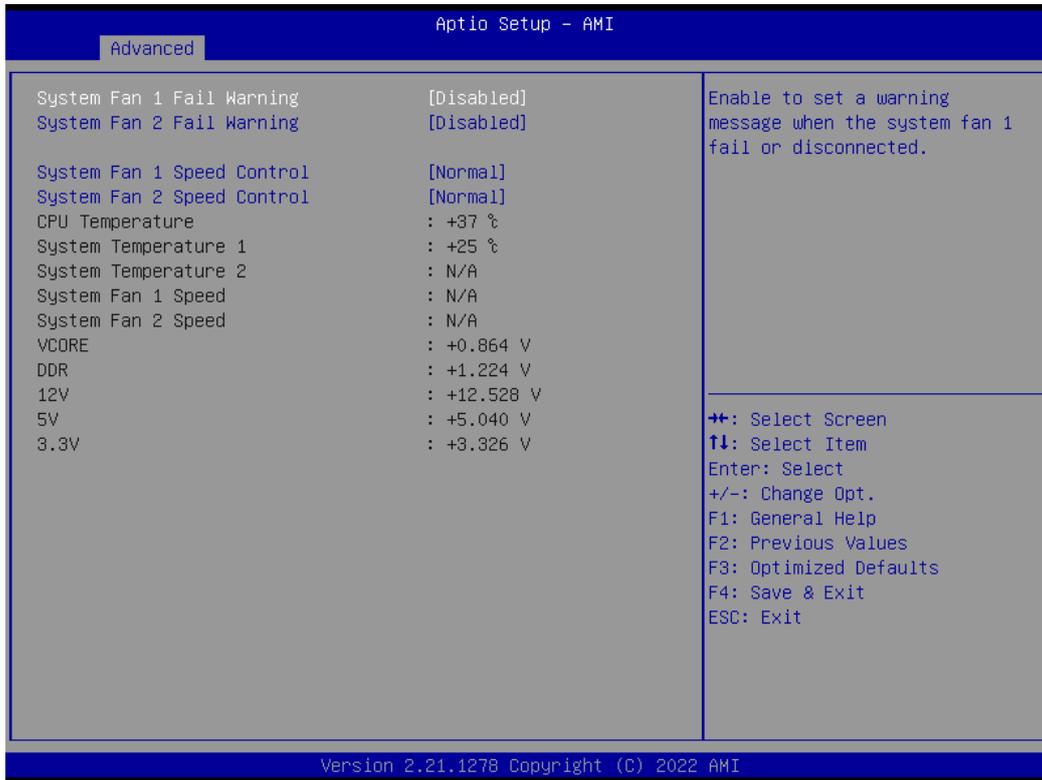
Item	Description
Security Device Support	Enabled : Enables TPM feature (Default setting) Disabled : Disables TPM feature
Pending operation	None : No execution will be conducted (Default setting) TPM clear : Set to clear data on TPM

2.2 IT8786 Super IO Configuration



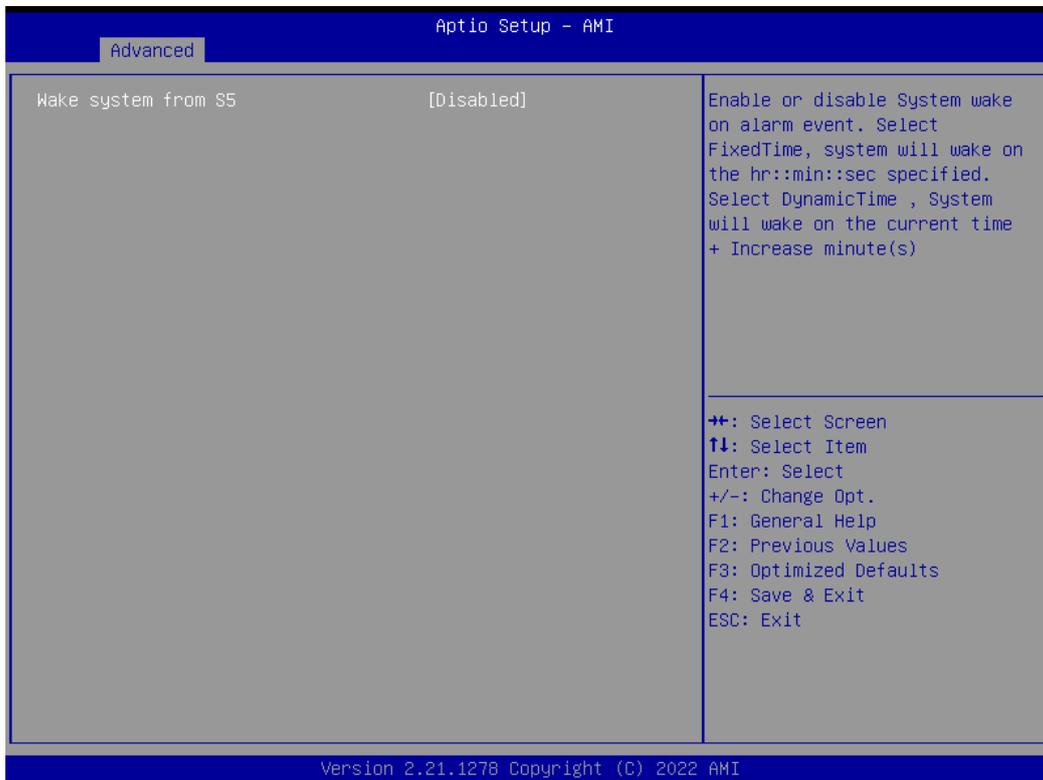
Item	Description
Super IO Chip	Shows Super I/O chip model
Serial Port 1 Configuration Serial Port 2 Configuration	<p>Press [Enter] to configure advanced items :</p> <p>Serial Port : Enabled : Enables allows you to configure the serial port settings Disabled : if Disabled, displays no configuration for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

2.3 Hardware Monitor



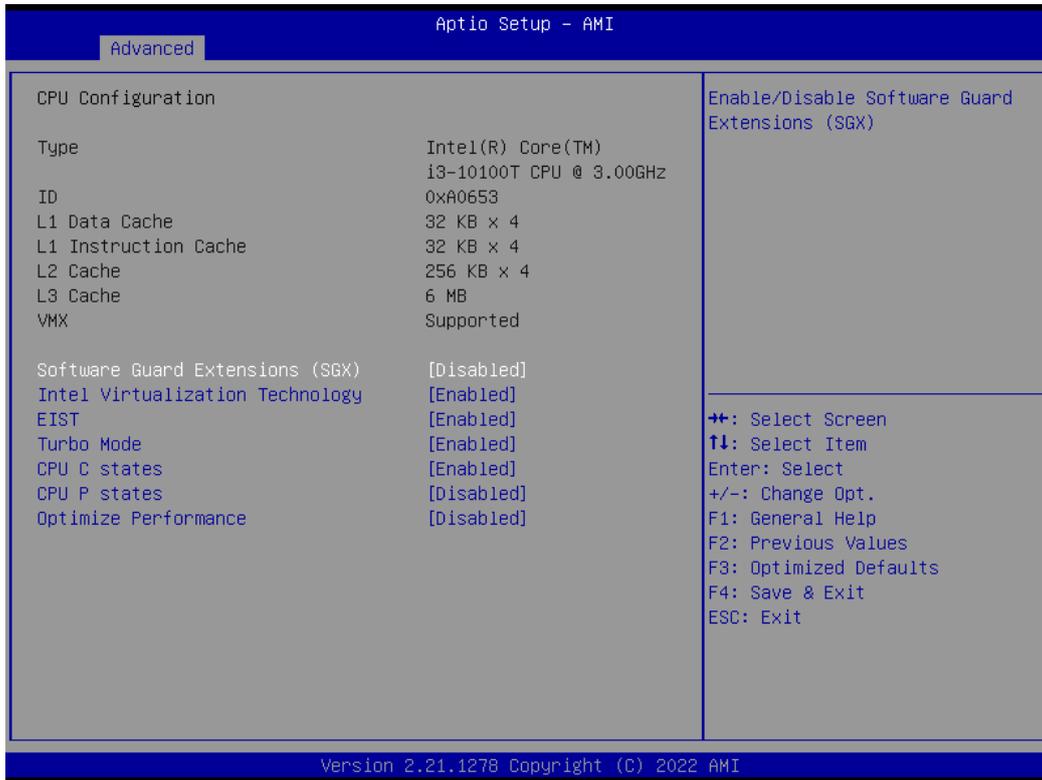
Item	Description
System Fan 1 Fail Warning	Enabled : Enables System FAN 1 Fail warning alert function Disabled : Disables System FAN 1 Fail warning alert function (Default setting) (This setting will effect only if you add the extend kit on the system)
System Fan 2 Fail Warning	Enabled : Enables System FAN 2 Fail warning alert function Disabled : Disables System FAN 2 Fail warning alert function (Default setting) (This setting will effect only if you add the extend kit on the system)
System Fan 1 Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed (This setting will effect only if you add the extend kit on the system)
System Fan 2 Speed Control	Normal : Fan speed set by BIOS default (Default setting) Full Speed : Set Fan operates at full speed (This setting will effect only if you add the extend kit on the system)
CPU Temperature	Shows current CPU temperature
System Temperature 1	Shows current System temperature
System Temperature 2	Shows current System temperature for the extend kit of the system (This numerical value will shows only if you add the extend kit on the system)
System Fan 1 Speed	Shows current System fan 1 Speed for the extend kit of the system (This numerical value will shows only if you add the extend kit on the system)
System Fan 2 Speed	Shows current System fan 2 Speed for the extend kit of the system (This numerical value will shows only if you add the extend kit on the system)

2.4 S5 RTC Wake Settings



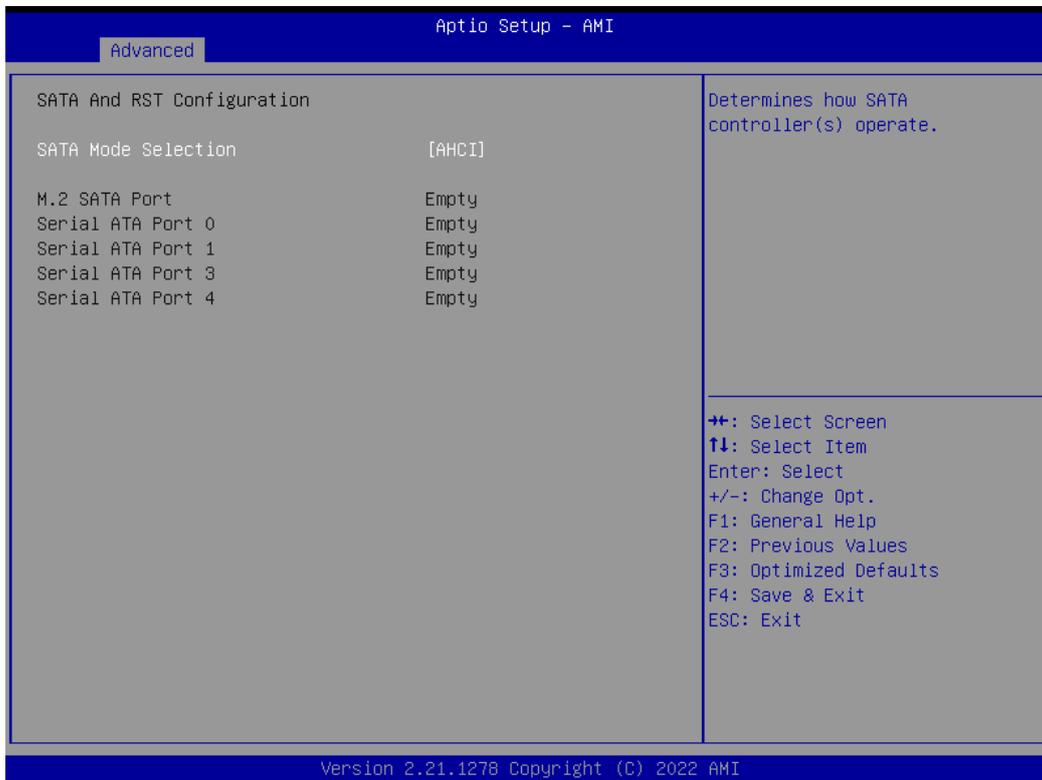
Item	Description
Wake system from S5	Enable or Disable System to wake on a specific time. Disabled : Disables system to wake on a specific time (Default setting) Fixed Time : Enables system to wake on a specific time (Format : hr : min : sec)

2.5 CPU Configuration



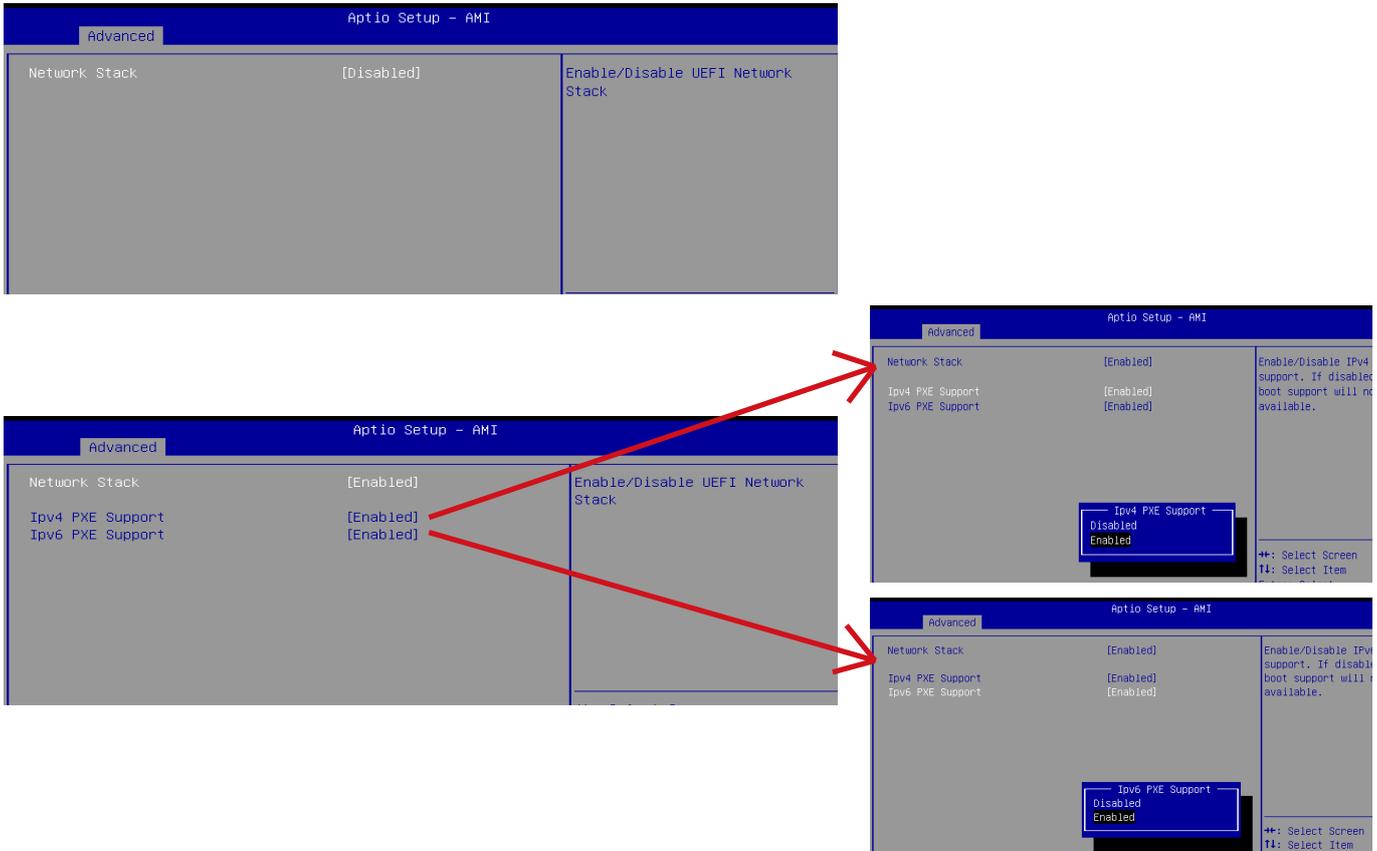
Item	Description
Software Guard Extensions (SGX)	Disabled : Disables Software Guard Extensions (SGX) (Default setting) Enabled : Enables Software Guard Extensions (SGX) Software Controlled : If this item is selected, SGX will be controlled by SGX application for UEFI boot OS
Intel Virtualization Technology	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
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 Disabled : Disables CPU P states function (Default setting)
Optimize Performance	To optimize CPU performance. Enabled : Enables optimize performance function Disabled : Disables optimize performance function (Default setting)

2.6 SATA And RST Configuration



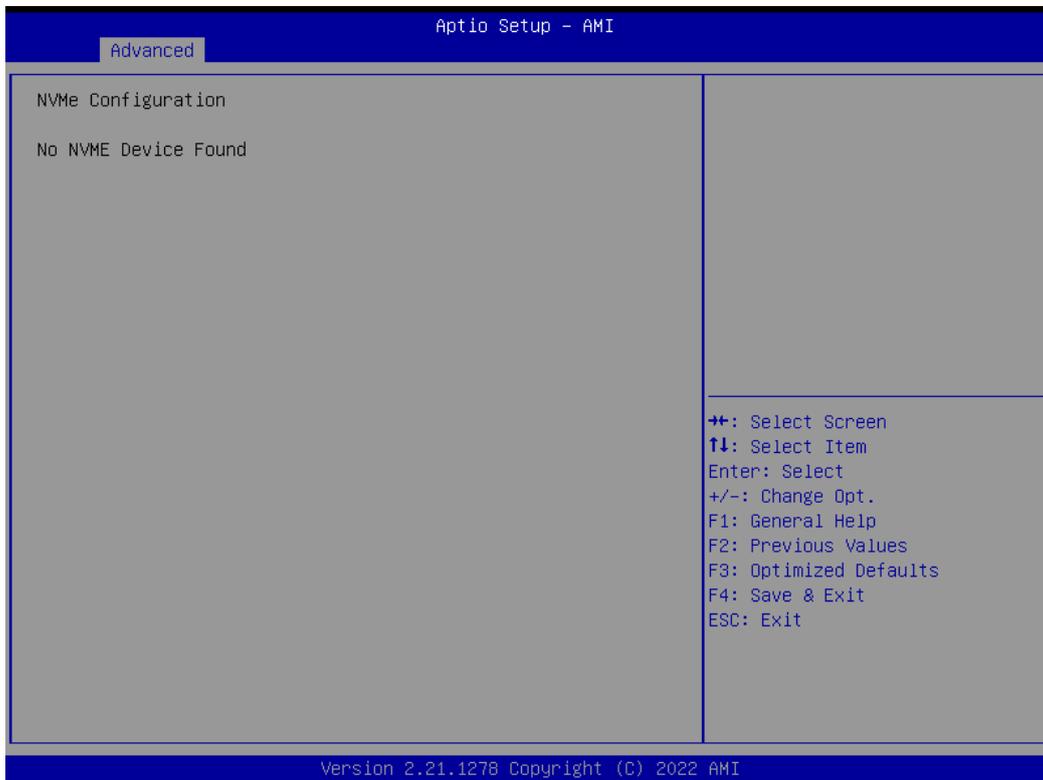
Item	Description
SATA Mode Selection	Set SATA controller to AHCI mode
M.2 SATA Port	shows M.2 SSD information
Serial ATA Port 0	shows 2.5" SATA HDD/SSD information
Serial ATA Port 1	
Serial ATA Port 3	
Serial ATA Port 4	

2.7 Network Stack Configuration

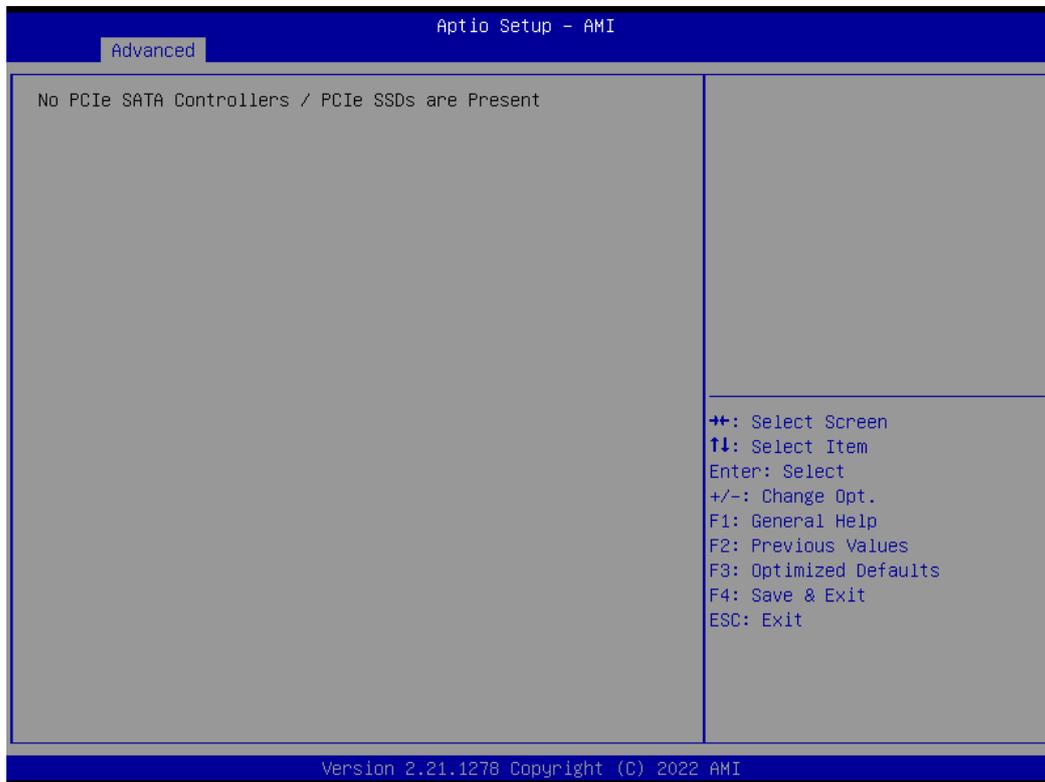


Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode Disabled : Disables UEFI Network Stack (Default setting) Enabled : Enables UEFI Network Stack
Ipv4 PXE Support	When Network stack is enabled : Disabled : Disables Ipv4 PXE Support Enabled : Enables Ipv4 PXE Support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

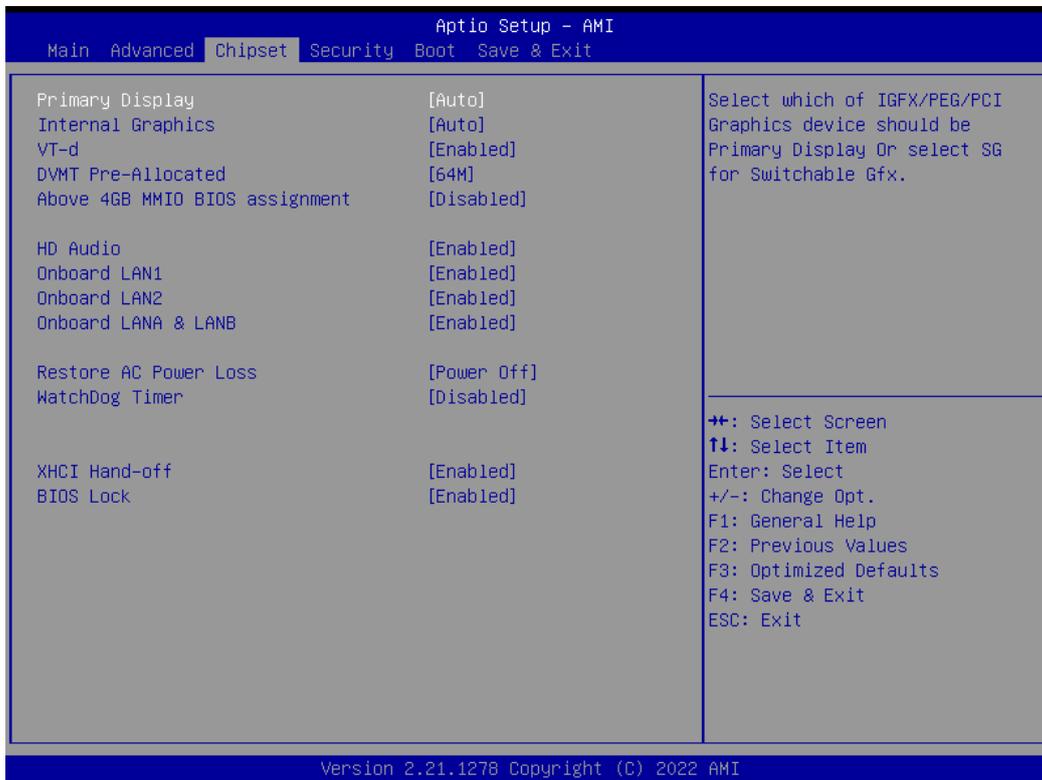
2.8 NVMe Configuration



2.9 Offboard SATA Controller Configuration

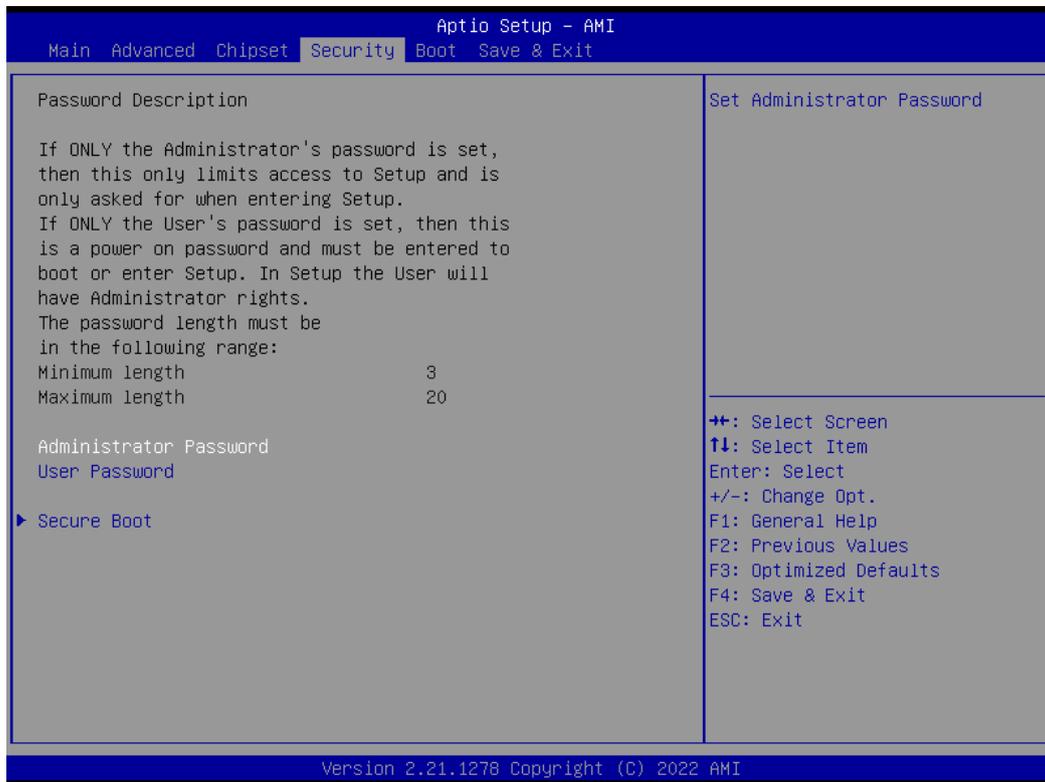


3 Chipset



Item	Description
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
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
Above 4GB MMIO BIOS assignment	Enable or disable to re-allocate memory space for device cards when more than one external graphic cards installed. (This function could be only used under 64 bit operating system with above 4 GB address space) Enabled : Enables Above 4GB MMIO BIOS assignment function Disabled : Disables Above 4GB MMIO BIOS assignment function (Default setting)
HD Audio	Enable/Disable onboard audio controller Enabled : Enables onboard audio controller (Default setting) Disabled : Disables onboard audio controller
Onboard LAN1 Onboard LAN2 Onboard LANA & LANB	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 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 : Disabled Watchdog Timer function (Default setting) 30s : delay watchdog for 30 seconds. 60s : delay watchdog for 60 seconds.
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 function

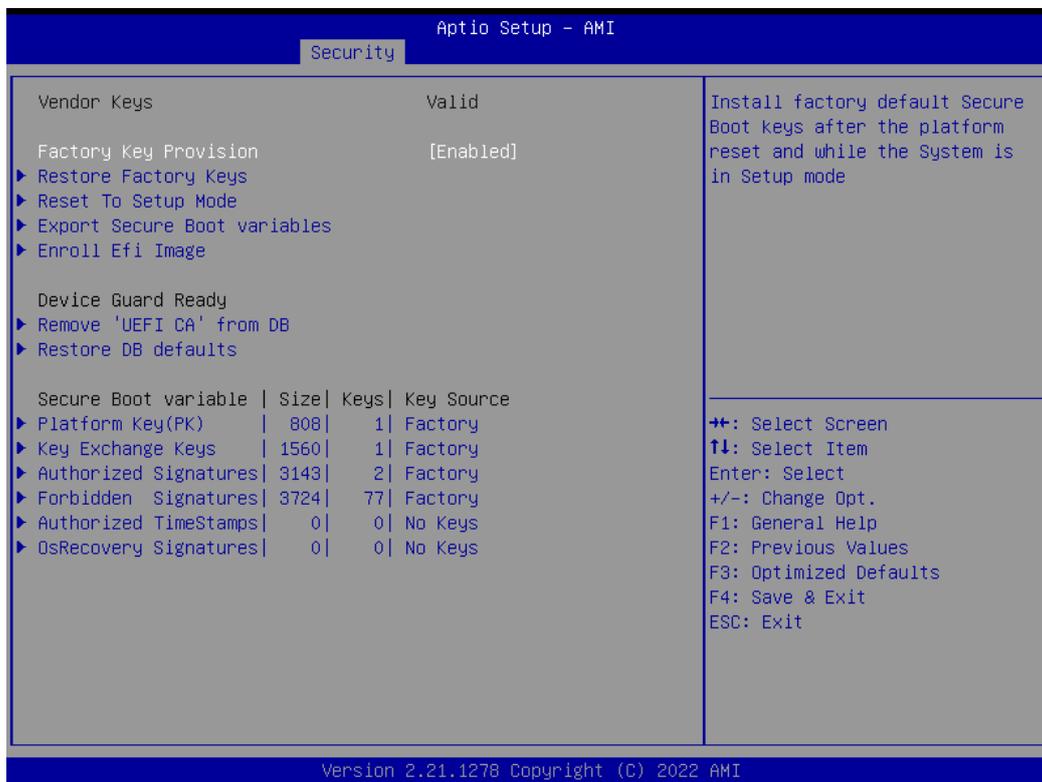
4 Security



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



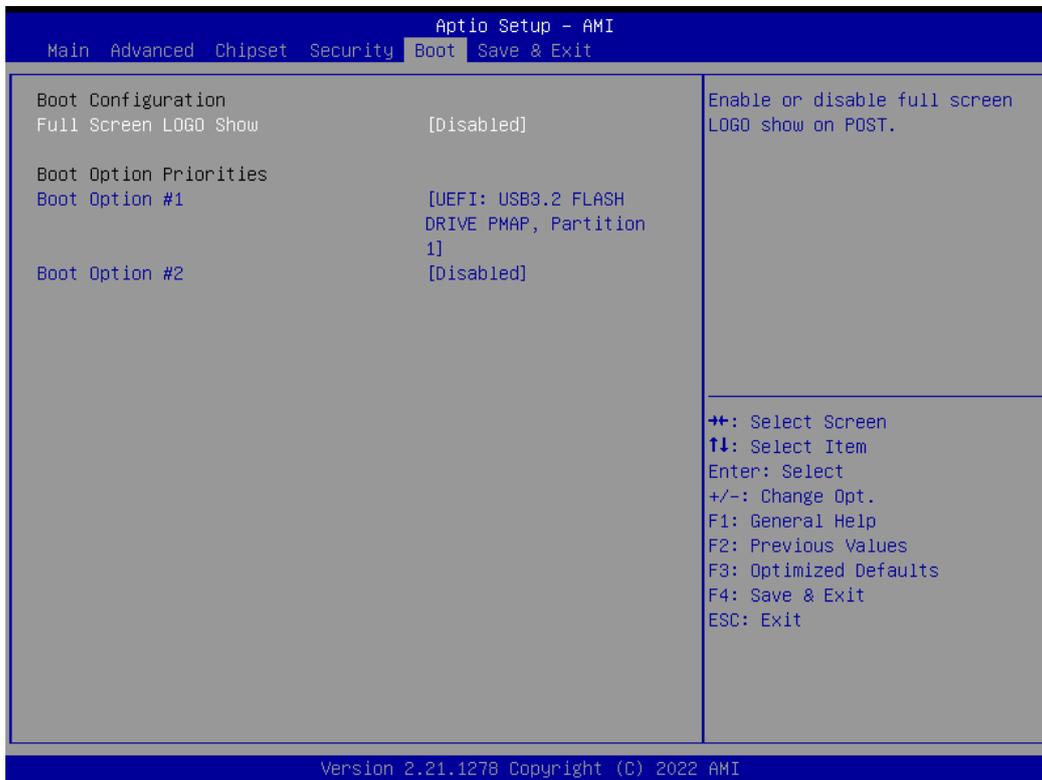
Item	Description
Secure Boot	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates Enabled : Enables Secure Boot function Disabled : Disables Secure Boot function (Default setting)
Secure Boot Mode	Standard : Standard mode 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
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 Yes : Agree to remove 'UEFI CA' from database No : Cancel 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	

5 Boot



Item	Description
Full Screen LOGO Show	Enable/Disable full screen LOGO show on POST screen Enabled : Enables Full screen LOGO Show on POST screen (Default setting) Disabled : Disables Full screen LOGO Show on POST screen
Boot Option #1 Boot Option #2	Shows the information of the storage that be installed in the system Choose/set the boot priority

6 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)