GIGAIPC

QBIX-JMB-CMLA47EH-A1

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

Startup Manual

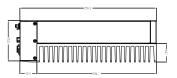
Packing List

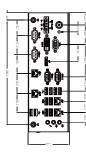
Before you begin installing your card, please make sure that the following items have been shipped:

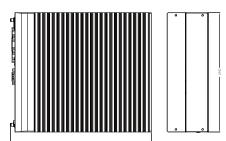
- 1. Screw HDD x 20 pcs (25984G-1C014-S00)
- 2. 4-pin Terminal Blocks Male Plug x 1 pcs (25IO0-2ESDV0-D2R)

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.

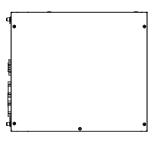
Dimension







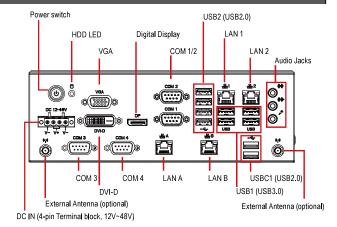
			UUU		J
E	٩	č	۲	0.	Π
đ_		•		•	Ц



Speci	fications
Dimension	System Size: 224W x 256.1D x 77.7H(mm)
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 3200 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 1920x1200 @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 (WiFi/BT) 1 x Full-size Mini PCIe with SIM slot

Front I/O	1 x DC IN (4-pin Terminal Block +12V~48V) 1 x VGA / 1 x DVI-D /1 x DP 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 3 x Audio Jacks (Line in, Line out & Mic in) 2 x External Antenna Holes (Optional)
Rear I/O	
Power	DC in +12V~48Vdc (Full Range)
Operation Temperature	Operating temperature: -20°C to 50°C (CPU 65W TDP) Operating temperature: -20°C to 60°C (CPU 35W TDP) 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/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: 300 x 315 x 166 (mm) Packing Capacity : 1 Including: Terminal Blocks Male Plug x 1pc (25IO0-2ESDV0-D2R) Screw M3x4L x 20pcs (25984G-1C014-S00)
Order Information	System : 6BQJQ47EAMR-SI (Box packing)

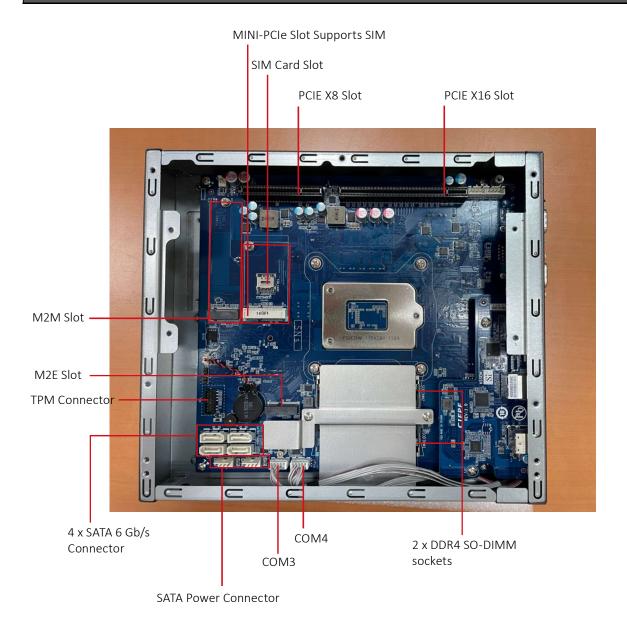
System I/O Interface



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.

Fr	ont I/O Con	nectors
No.	Code	Scription
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-12-48V	Power connector
15	Audio	Audio Jacks (Line in, Line out & Mic in)



Simple Installation Process

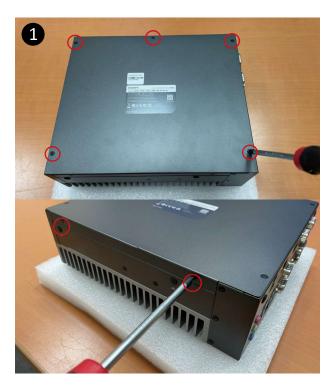
Memory Installation

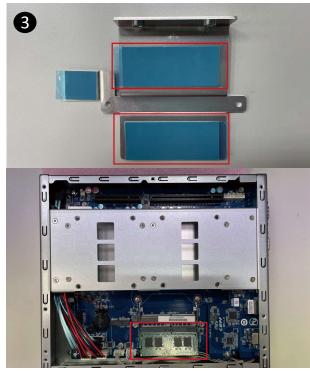
QBiX-JMB-CMLA47EH-A1 supports DDR4 SO-DIMM type memory module.

- 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.









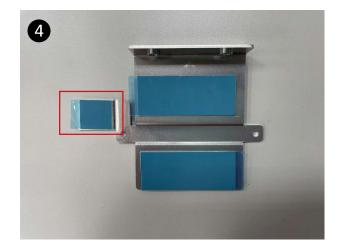
M2E (Support NGFF-2230 Wifi/BT) Installation

- 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.



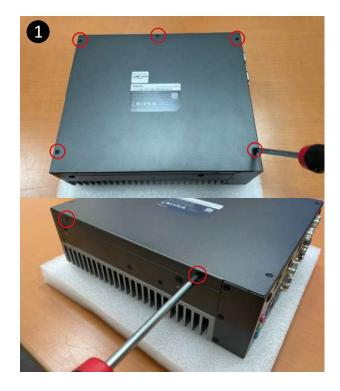


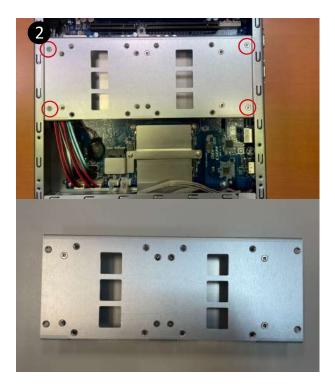


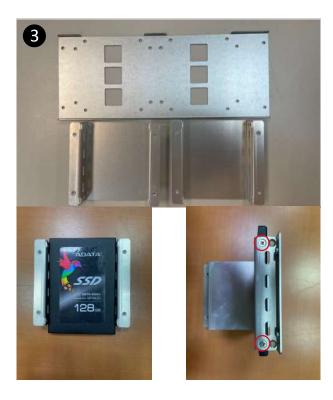


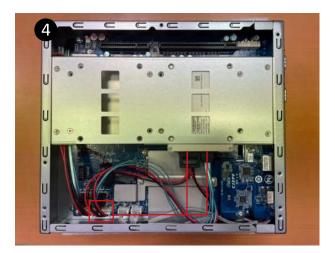
Storage Installation 1 (2.5" HDD/SSD)

- 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.



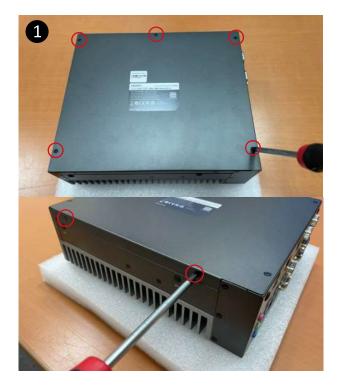






Storage Installation 2 (M2M Storeage)

- 1. Loosen 7 screws, and then remove the bottom cover
- 2. Loosen 4 screws to remove the hard disk storage aluminum sheet
- 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 the hard disk storage aluminum sheet
- 7. Replace the bottom cover and secure with screws.









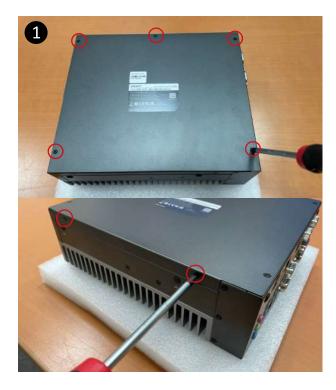




Mini-PCIe Slot (PCIex1 + USB2.0) and SIM Card Slot Installation

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

- 1. Loosen 7 screws, and then remove the bottom cover
- 2. Loosen 4 screws to remove the hard disk storage aluminum sheet
- 3. Assemble the Mini-PCIe expansion Card (Mini-PCIex1 + USB2.0) or 3G/4G SIM Card in SIM Slot.
- 4. Install 4 screws to firmly install the hard disk storage aluminum sheet
- 5. Replace the bottom cover and secure with screws.







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-CMLA47EH-A1

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 bootup 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		
$\uparrow \downarrow$	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	C 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.

Main Advanced Chipset S	Aptio Setup – AMI ecurity Boot Save & Exit	
BIOS Information Project Name BIOS Version Build Date and Time	QBiX-JMB-CMLA47EH-A1 F2 05/27/2022 14:11:28	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 1998–9999 Months: 1–12
LAN1 MAC Address LAN2 MAC Address LANA MAC Address LANB MAC Address	D8-5E-D3-0F-43-77 D8-5E-D3-0F-43-78 D8-5E-D3-06-55-23 D8-5E-D3-06-55-24	Days: Dependent on month Range of Years may vary.
Total Memory	4096 MB	
ME FW Version	14.0.48.1605	↔: Select Screen ↑↓: Select Item
System Date System Time	[Tue 06/07/2022] [11:05:21]	Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.21.1278 Copyright (C) 20	22 AMI

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
Jystem Date	(Format : Week - Month - Day - Year)
System Time	Set the time for the system
System Time	(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.

Main Advanced Chipset Security Boot Sa	ve & Exit
 TPM Configuration IT0786 Super IO Configuration Hardware Monitor SS RTC Wake Settings CPU Configuration SATA And RST Configuration Network Stack Configuration NVMe Configuration Offboard SATA Controller Configuration 	TPM Configuration ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.21.1278	Copyright (C) 2022 AMI

2.1 TPM configuration

Use TPM Configuration submenu to choose TPM interface.

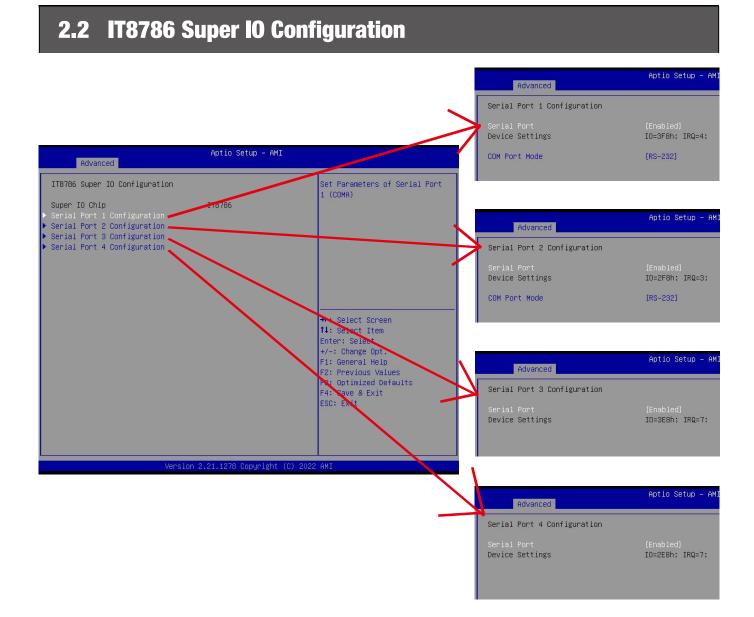


ltem	Description		
	PTT : Internal TPM (Default setting) dTPM : External TPM (When using External TPM module or having TPM chip on MB)		

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

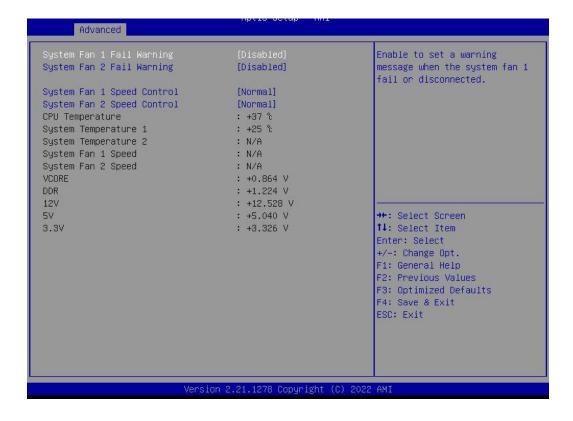
Advanced	nprio octop Ini.	
TPM 2.0 Device Found		Enables or Disables BIOS support for security device.
Security Device Support Pending operation	[Enable] [None]	<pre>support for security device. 0.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Vers	ion 2.21.1278 Copyright	(C) 2022 AMI

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	



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

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

Advanced	Aptio Setup - AMI	
Wake system from S5	[Disabled]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time + Increase minute(s) ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.21.1278 Copyright (C) 2	2022 AMI

ltem	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)

Advanced		
CPU Configuration		Enable/Disable Software Guard Extensions (SGX)
Type ID L1 Data Cache L1 Instruction Cache L2 Cache L3 Cache VMX Software Guard Extensions (SGX) Intel Virtualization Technology EIST Turbo Mode CPU C states CPU P states Optimize Performance	Intel(R) Core(TM) i3-10100T CPU @ 3.00GHz 0xA0653 32 KB x 4 32 KB x 4 256 KB x 4 6 MB Supported [Disabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled] [Disabled]	<pre>++: Select Screen ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version	2.21.1278 Copyright (C) 202	2 AMI

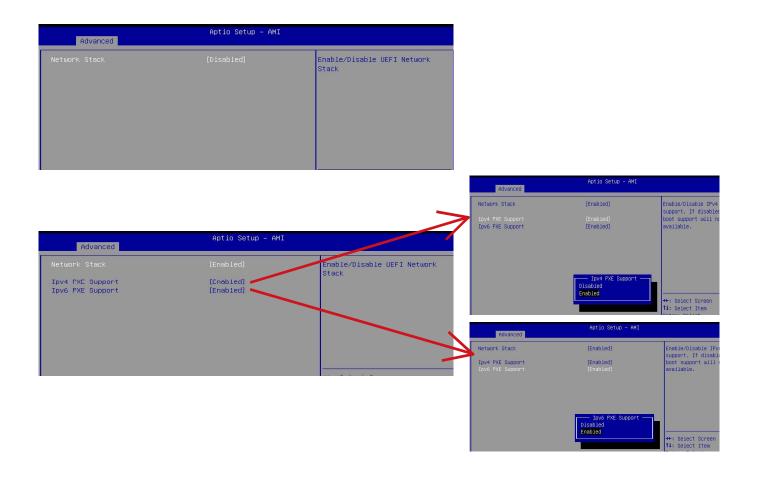
Item	Description		
Software Guard Extensions (SGX)	Disabled : Disables Software Guard Extensions (SGX) (Default seeting) Enabled : Enables Software Guard Extensions (SGX) Software Controlled : If this item is selected, SGX will be controlled by SGX application for UEFI boot OS		
Intel Virtualization 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

Advanced	Aptio Setup – AMI	
SATA And RST Configuration		Determines how SATA controller(s) operate.
SATA Mode Selection	[AHCI]	controller (3) operate.
M.2 SATA Port Serial ATA Port O Serial ATA Port 1 Serial ATA Port 3 Serial ATA Port 4	Empty Empty Empty Empty Empty	
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.21.1278 Copyright (C) 2022 AMI		

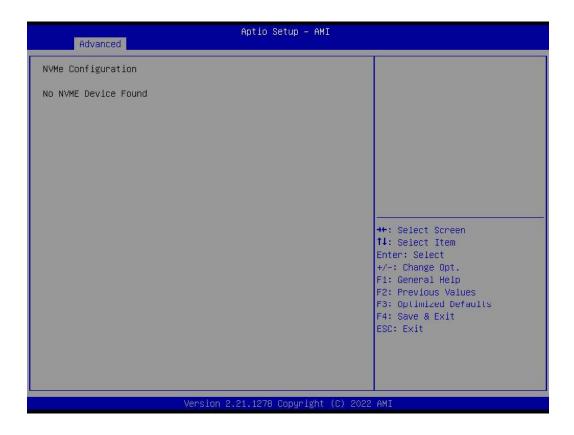
Item	Description	
SATA Mode Selection	Set SATA controller to AHCI mode	
M.2 SATA Port	shows M.2 SSD information	
Serial ATA Port 0		
Serial ATA Port 1	shows 2.5" SATA HDD/SSD information	
Serial ATA Port 3		
Serial ATA Port 4		

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	
lpv4 PXE Support	When Network stack is enabled : Disabled : Disables Ipv4 PXE Support Enabled : Enables Ipv4 PXE Support	
When Network stack is enabled : Ipv6 PXE Support Disabled : Disables Ipv6 PXE Support Enabled : Enables Ipv6 PXE Support		

2.8 NVMe Configuration



2.9 Offboard SATA Controller Configuration

Aptio Setup – AMI Advanced		
No PCIe SATA Controllers / PCIe SSDs are Present	<pre>++: Select Screen f1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>	
Version 2.21.1278 Copyright (C) 2022 AMI		

Primary Display[Auto]Internal Graphics[Auto]VT-d[Enabled]DVMT Pre-Allocated[64M]Above 4GB MMID BIOS assignment[Disabled]HD Audio[Enabled]Onboard LAN1[Enabled]Onboard LAN2[Enabled]Onboard LAN3 & LANB[Enabled]Restore AC Power Loss[Power Off]WatchDog Timer[Disabled]XHCI Hand-off[Enabled]BIOS Lock[Enabled]F1 Select ItemEnabled]F2: Previous ValuesF3: Optimized DefaultsF4: Save & ExitESC: Exit	Aptio Setup – AMI Main Advanced <mark>Chipset</mark> Security Boot Save & Exit			
WatchDog Timer [Disabled] ++: Select Screen tl: Select Item XHCI Hand-off [Enabled] BIOS Lock [Enabled] +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit	Internal Graphics VT-d DVMT Pre-Allocated Above 4GB MMIO BIOS assignment HD Audio Onboard LAN1 Onboard LAN2	[Auto] [Enabled] [64M] [Disabled] [Enabled] [Enabled] [Enabled]	Graphics device should be Primary Display Or select SG	
XHCI Hand-off [Enabled] Enter: Select BIOS Lock [Enabled] +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit				
			Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit	

ltem	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 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	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 funtion	

Aptio Setup – AMI Main Advanced Chipset <mark>Security</mark> Boot Save & Exit		
Password Description If ONLY the Administrator's passw then this only limits access to S only asked for when entering Setu If ONLY the User's password is se is a power on password and must b boot or enter Setup. In Setup the have Administrator rights. The password length must be in the following range: Minimum length Maximum length Administrator Password User Password	etup and is p. t, then this e entered to	Set Administrator Password ++: Select Screen 11: Select Item Enter: Select
▶ Secure Boot		+/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

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</enter>

Se	Aptio Setup – AMI curity	
System Mode	User	Secure Boot feature is Active if Secure Boot is Enabled,
Secure Boot	[Disabled] Not Active	Platform Key(PK) is enrolled and the System is in User mode.
Secure Boot Mode ▶ Restore Factory Keys ▶ Reset To Setup Mode	[Custom]	The mode change requires platform reset
▶ Key Management		
		++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	/ersion 2.21.1278 Copyright (C) 2022 AMI

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	Standard : Standard mode
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	Yes : Agree to setup mode
Mode	No : Cancel to setup mode
Key	Enables expert users to modify Secure boot policy variables without full authentication
Management	Press <enter> to configure the advanced items</enter>

Securi	Aptio Setup – AMI ty	
Vendor Keys	Valid	Install factory default Secure Boot keys after the platform
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image Device Guard Ready Remove 'UEFI CA' from DB Restore DB defaults	[Enabled]	reset and while the System is in Setup mode
Secure Boot variable Size Key Platform Key(PK) 808 Key Exchange Keys 1560 Authorized Signatures 3143 Forbidden Signatures 3724 7 Authorized TimeStamps 0	ys Key Source 1 Factory 2 Factory 2 Factory 7 Factory 0 No Keys 0 No Keys	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Vensi	on 2.21.1278 Copyright	(C) 2022 AMT

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)		
Key Exchange Keys		
Authorized Signatures		
Forbidden Signatures	These items allows you to enroll factory defaults or load Certificates from a file.	
Authorized TimeStamps		
OsRecovery Signatures		

Main Advanced Chipset S	Aptio Setup – AMI ecurity <mark>Boot</mark> Save & Exit	
Boot Configuration Full Screen LOGO Show	[Disabled]	Enable or disable full screen LOGO show on POST.
Boot Option Priorities Boot Option #1	[UEFI: USB3.2 FLASH DRIVE PMAP, Partition 1]	
Boot Option #2	[Disabled]	
		++: Select Screen ↑↓: Select Item Enter: Select
		+/−: Change Opt. F1: General Help F2: Previous Values
		F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.21.1278 Copyright (C) 200	22 AMI

ltem	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

Main Advanced Chipset Security B	Aptio Setup – AMI oot Save & Exit	
Save Options Save Changes and Reset Discard Changes and Reset		Reset the system after saving the changes.
Restore Defaults		
Boot Override UEFI: USB3.2 FLASH DRIVE PMAP, Partit	ion 1	
Me FW Image Re-Flash	[Disabled]	
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>
Version 2.	21.1278 Copyright (C) 2022	AMI

ltem	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)