CE6-6412A

COM Express Module

Copyright Notice

Acknowledgement

Packing List

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

Item	Quantity
CE6-6412A MB	1

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

About this Document

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

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

Safety Precautions

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

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

13. Watch out for high temperatures when the system is running.

14. Do not touch the heat sink or heat spreader when the system is running

15. Never pour any liquid into the openings. This could cause fire or electric shock.

16. As most electronic components are sensitive to static electrical charge, be sure to ground yourself to prevent static charge when installing the internal components. Use a grounding wrist strap and contain all electronic components in any static-shielded containers.

17. If any of the following situations arises, please the contact our service personnel:
    i. Damaged power cord or plug
    ii. Liquid intrusion to the device
    iii. Exposure to moisture
    iv. Device is not working as expected or in a manner as described in this manual
    v. The device is dropped or damaged
    vi. Any obvious signs of damage displayed on the device

18. **DO NOT LEAVE THIS DEVICE IN AN UNCONTROLLED ENVIRONMENT WITH TEMPERATURES BEYOND THE DEVICE'S PERMITTED STORAGE TEMPERATURES (SEE CHAPTER 1) TO PREVENT DAMAGE.**

FCC Statement

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

Caution:

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

Attention:

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

China RoHS Requirements (CN)

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

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板及其电子组件	○	○	○	○	○	○
外部信号连接器及线材	○	○	○	○	○	○

O : 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。
X:表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。
备注 : 此产品所标示之环保使用期限，系指在一般正常使用状况下。

China RoHS Requirement (EN)

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

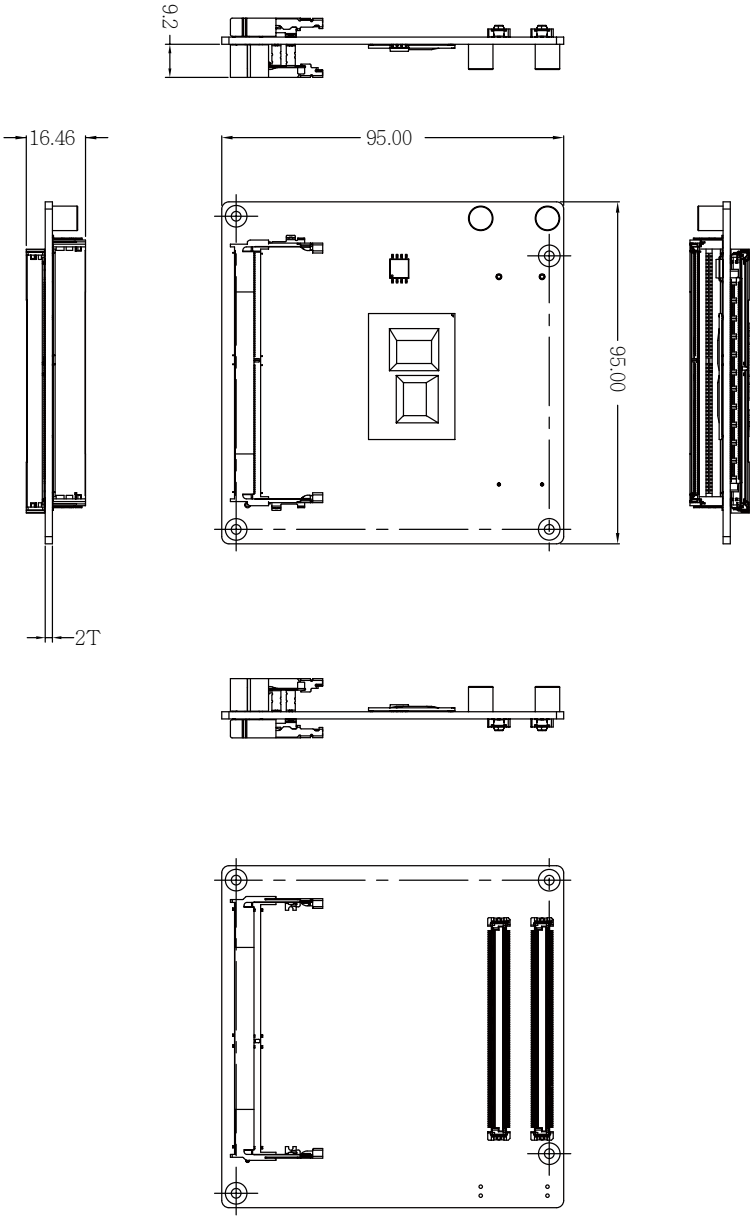
Component	Poisonous or Hazardous Substances or Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr(VI))	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
PCB & Other Components	O	O	O	O	O	○
Wires & Connectors for External Connections	O	O	O	O	O	O

O : The quantity of poisonous or hazardous substances or elements found in each of the component's parts is below the SJ/T 11363-2006-stipulated requirement.
X: The quantity of poisonous or hazardous substances or elements found in at least one of the component's parts is beyond the SJ/T 11363-2006-stipulated requirement.
Note: The Environment Friendly Use Period as labeled on this product is applicable under normal usage only

Table Contents

Chapter 1

Chapter 1 - Product Specifications


9.2
16.46
95.00
95.00
2T

1.1 Specifications

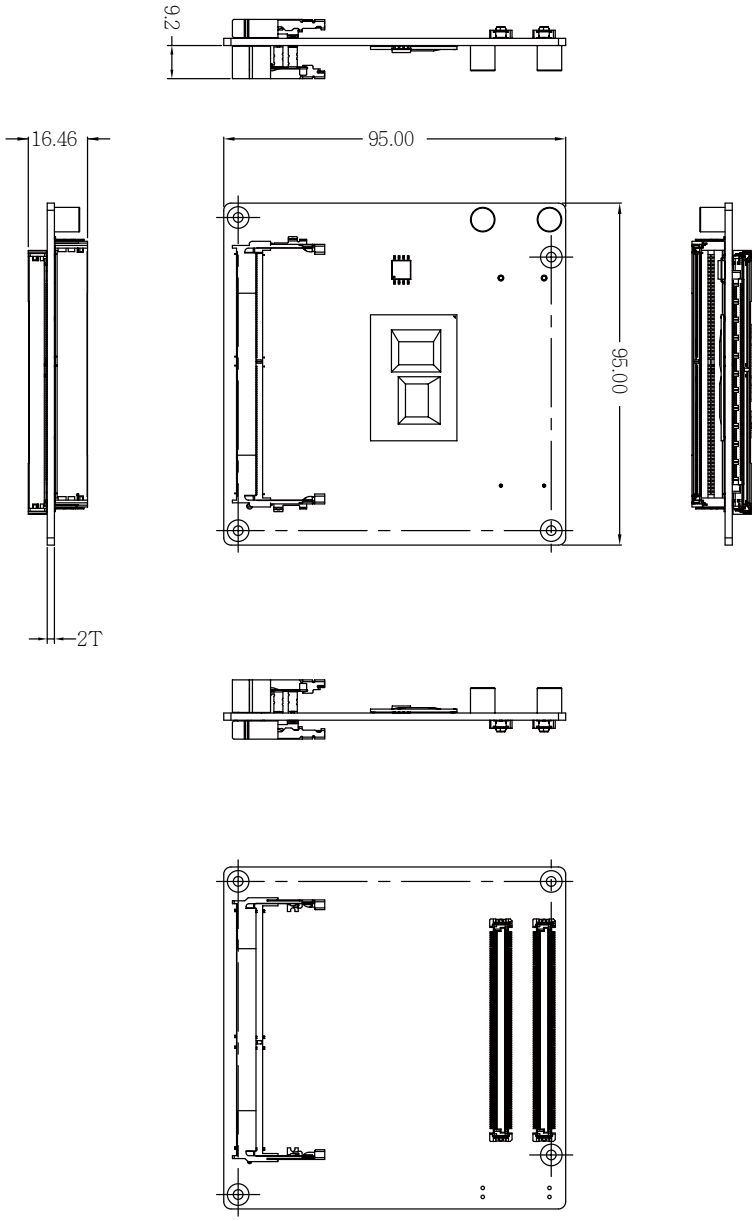
COM Express module	CE6-6412A (MEHLJAC)
Form Factor	COM Express® R3.0 Compact Module, Type 6 95W x 95D (mm)
CPU	Intel® Celeron® J6412 Processor 10nm, 4 cores, 4 threads, up to 2.60 GHz TDP 10W
Socket	1 x FCBGA 1493
Memory	2 x DDR4 SO-DIMM sockets, Max. Capacity 32 GB Support Dual Channel DDR4 3200 MHz memory modules
BIOS	AMI UEFI 256Mb
Super I/O	ITE IT8613E/NX
Video	Integrated Graphics Processor - Intel® UHD Graphics for 10th Gen Intel® Processors: - LCD : eDP 4096 x 2304 @ 60Hz - 2 x DDI ports support configurable HDMI/DisplayPort HDMI 2.0b: 4096 x 2160 @ 60Hz DisplayPort 1.4: 4096 x 2160 @ 60Hz (3 independent display outputs)
Audio	Intel® HD Audio
Storage	2 x SATA 6Gb/s Ports
Expansion Slots	6 x PCI Express x1 (Gen3)
Internal I/O	2 x USB 3.2 (Gen2)(10Gb/s) 2 x USB 3.2 (Gen2)(10Gb/s) - Optional ports by PCIe Co-lay 8 x USB 2.0 Ports (480Mbps) 1 x eSPI 1 x SMBUS 1 x I2C 1 x GPIO (8 bits) 1 x System fan
Power Requirement	Vin: 8.5V ~ 20V VSB: 4.75V ~ 5.25V RTC Battery: 2.0V ~ 3.3V
Watchdog	65536 level, 0 ~ 65535 sec
OS Compatibility	Windows 10 (x64)

COM Express module	CE6-6412A (MEHLJAC)
Operating Properties	Operating temperature: 0°C to 60°C Operating humidity: 0-90% (non-condensing) Non-operating temperature: -40°C to 85°C Non-operating humidity: 0%-95% (non-condensing)

Chapter 2

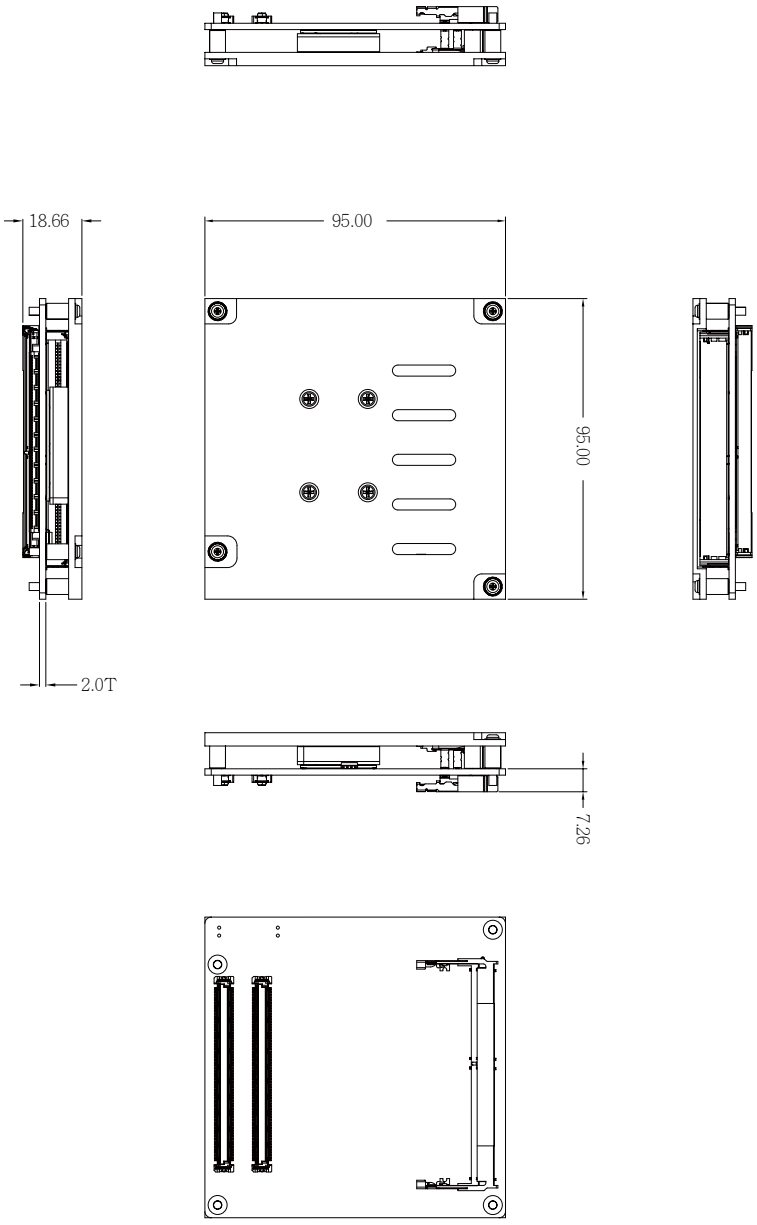
Chapter 2 – Hardware Information

2.1 Dimensions

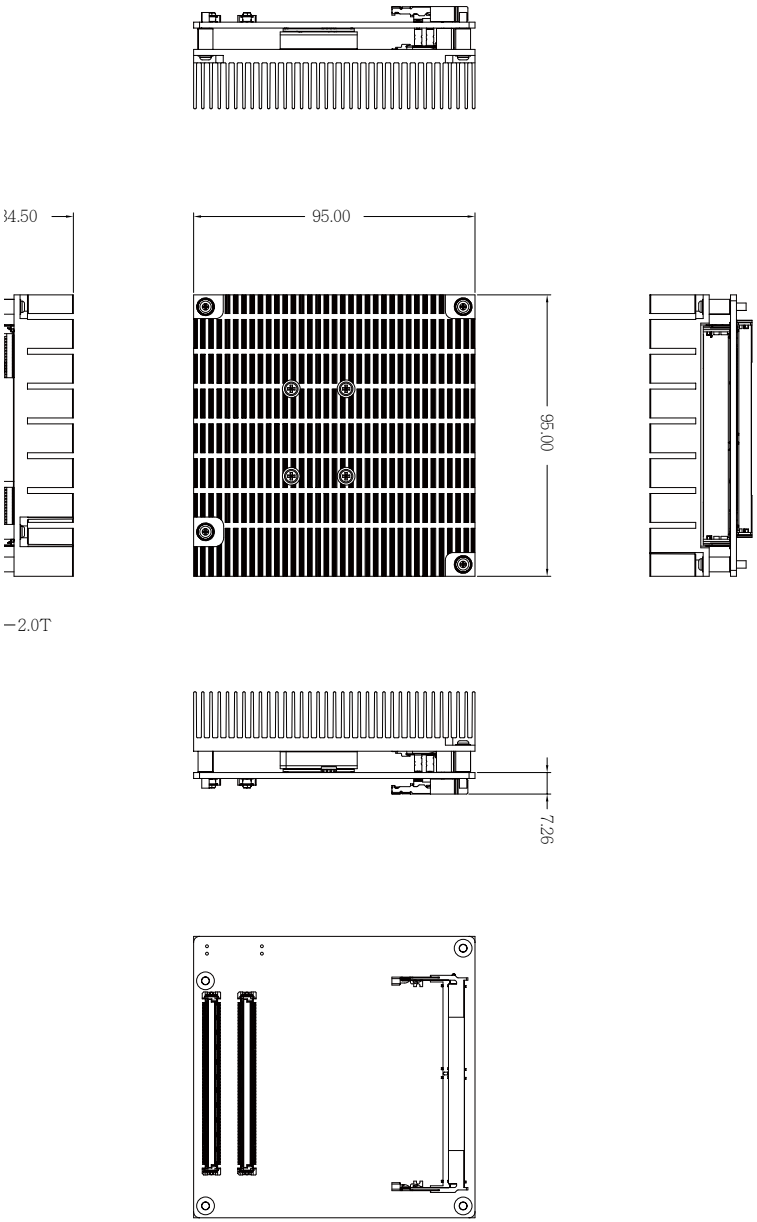


GIGAIPC

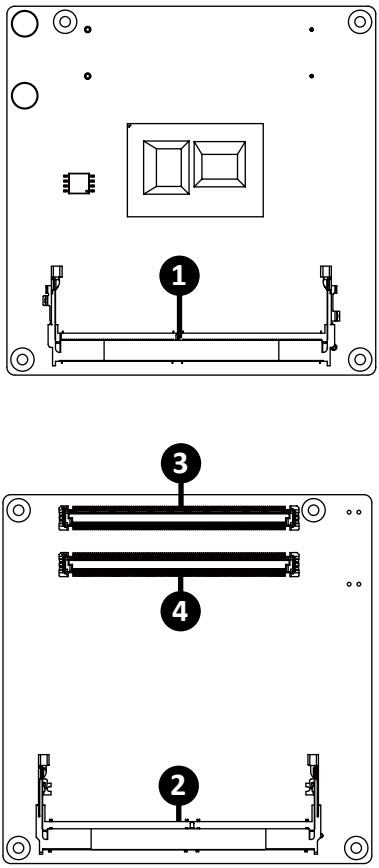
COM Express module with Heat spreader



COM Express module with Heat sink



2.2 Jumpers and Connectors

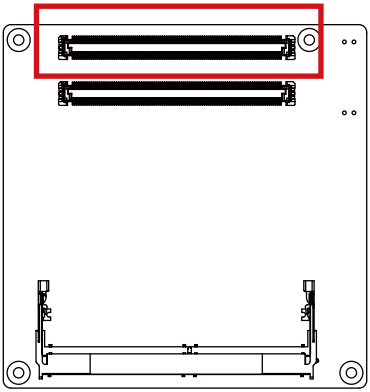


No	Code	Description
1	SODIMMA	DDR4 SO-DIMM Socket
2	SODIMMB	DDR4 SO-DIMM Socket
3	CEP_M	COM Express connector ROW A/B
4		COM Express connector ROW C/D

www.gigaipc.com

2.2.1 COM Express connector ROW A/B

1



Pin No.	Definition	Pin No.	Definition
A1	GND (FIXED)	B1	GND (FIXED)
A2	NC	B2	NC
A3	NC	B3	ESPI_CS#_R
A4	NC	B4	ESPI_IO0_R
A5	NC	B5	ESPI_IO1_R
A6	NC	B6	ESPI_IO2_R
A7	NC	B7	ESPI_IO3_R
A8	NC	B8	NC
A9	NC	B9	NC
A10	NC	B10	ESPI_CLK_R
A11	GND (FIXED)	B11	GND (FIXED)
A12	NC	B12	PANSHW
A13	NC	B13	SMB_CK
A14	NC	B14	SMB_DATA
A15	PCH_SLP_S3#	B15	SMB_ALERT_n
A16	SATAIII_TX0p	B16	SATA_M.2_SSD_SLOT1_TX_Dp
A17	SATAIII_TX0n	B17	SATA_M.2_SSD_SLOT1_TX_Dn
A18	PCH_SLP_S4#	B18	ESPI_RST#_R
A19	SATAIII_RX0p	B19	SATA_M.2_SSD_SLOT1_RX_Dp
A20	SATAIII_RX0n	B20	SATA_M.2_SSD_SLOT1_RX_Dn
A21	GND (FIXED)	B21	GND (FIXED)
A22	NC	B22	NC
A23	NC	B23	NC

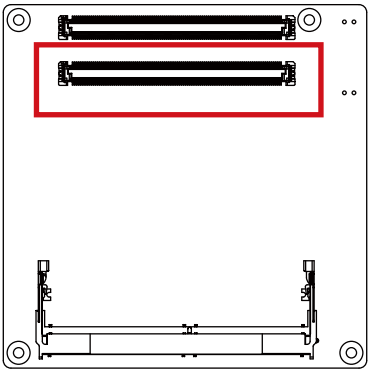
Pin No.	Definition	Pin No.	Definition
A24	NC	B24	ATXPWOK
A25	NC	B25	NC
A26	NC	B26	NC
A27	BATLOW#	B27	TP
A28	SATA LED	B28	NC
A29	ACZ_SYNC	B29	NC
A30	ACZ_RST	B30	ACZ_SDIN0
A31	GND (FIXED)	B31	GND (FIXED)
A32	ACZ_BITCLK	B32	SPKR
A33	ACZ_SDOUT	B33	NC
A34	NC	B34	NC
A35	THRMTRIP#	B35	NC
A36	USBP6n	B36	USBP7n
A37	USBP6p	B37	USBP7p
A38	NC	B38	USB_OC3
A39	USBP4n	B39	USBP5n
A40	USBP4p	B40	USBP5p
A41	GND (FIXED)	B41	GND (FIXED)
A42	USBP2n	B42	USBP3n
A43	USBP2p	B43	USBP3p
A44	USB_OC2	B44	USB_OC0
A45	USBP0n	B45	USBP1n
A46	USBP0p	B46	USBP1p
A47	3.3A_RTC	B47	NC
A48	NC	B48	NC
A49	NC	B49	SYS_RESET#
A50	NC	B50	PCIRST1#
A51	GND (FIXED)	B51	GND (FIXED)
A52	NC	B52	NC
A53	NC	B53	NC
A54	PWR LED	B54	M2E_WIFI_RF_KILL_R_N
A55	M.2_WLAN_TX_Dp	B55	M.2_LAN_RX_Dp
A56	M.2_WLAN_TX_Dn	B56	M.2_LAN_RX_Dn
A57	GND	B57	MPCIE_W_DISABLE
A58	LAN2_TXp_S	B58	LAN2_RXp_H
A59	LAN2_TXn_S	B59	LAN2_RXn_H
A60	GND (FIXED)	B60	GND (FIXED)
A61	LAN1_TXp_S	B61	LAN1_RXp_H
A62	LAN1_TXn_S	B62	LAN1_RXn_H
A63	PS_ON	B63	5VSB_CTRL
A64	PCIE1_TX_Dp	B64	PCIE1_RX_Dp

Pin No.	Definition	Pin No.	Definition
A65	PCIE1_TX_Dn	B65	PCIE1_RX_Dn
A66	GND	B66	PCIE_WAKE#
A67	FANPWM5	B67	NC
A68	NC	B68	NC
A69	NC	B69	NC
A70	GND (FIXED)	B70	GND (FIXED)
A71	NC	B71	NC
A72	NC	B72	NC
A73	NC	B73	NC
A74	NC	B74	NC
A75	NC	B75	LNC
A76	NC	B76	NC
A77	LVDS_eDP_VDD_EN	B77	NC
A78	NC	B78	NC
A79	NC	B79	eDP_BKLEN
A80	GND (FIXED)	B80	GND (FIXED)
A81	NC	B81	NC
A82	NC	B82	NC
A83	NC	B83	eDP_BKLTCTL
A84	NC	B84	5VSB
A85	LVDS_RST	B85	5VSB
A86	SPI_TPM_PIRQ_LT_R	B86	5VSB
A87	eDP_HPD	B87	5VSB
A88	CLK_100M_9ZXL831_Dp	B88	NC
A89	CLK_100M_9ZXL831_Dn	B89	NC
A90	GND (FIXED)	B90	GND (FIXED)
A91	NC	B91	NC
A92	SPI_SO_OUT	B92	NC
A93	M2E_BT_RF_KILL_N	B93	NC
A94	SPI_CLK_OUT	B94	NC
A95	SPI_SI_IN	B95	NC
A96	TP	B96	NC
A97	NC	B97	SPI_CS#2_OUT
A98	NC	B98	NC
A99	NC	B99	NC
A100	GND (FIXED)	B100	GND (FIXED)
A101	NC	B101	FAN_PWM4
A102	NC	B102	FANIO4
A103	NC	B103	NC
A104	ATX_12V	B104	ATX_12V
A105	ATX_12V	B105	ATX_12V

Pin No.	Definition	Pin No.	Definition
A106	ATX_12V	B106	ATX_12V
A107	ATX_12V	B107	ATX_12V
A108	ATC_12V	B108	ATX_12V
A109	ATX_12V	B109	ATX_12V
A110	GND (FIXED)	B110	GND (FIXED)

2.2.2 COM Express connector ROW C/D

❷



Pin No.	Definition	Pin No.	Definition
C1	GND (FIXED)	D1	GND (FIXED)
C2	GND	D2	GND
C3	USB3_RN0	D3	USB3_TN0
C4	USB3_RP0	D4	USB3_TP0
C5	GND	D5	GND
C6	USB3_RN1	D6	USB3_TN1
C7	USB3_RP1	D7	USB3_TP1
C8	GND	D8	GND
C9	USB3_RN2	D9	USB3_TN2
C10	USB3_RP2	D10	USB3_TP2
C11	GND (FIXED)	D11	GND (FIXED)
C12	NC	D12	NC
C13	NC	D13	NC
C14	GND	D14	GND
C15	NC	D15	DDI0_AUXP
C16	NC	D16	DDI0_AUXN
C17	NC	D17	NC
C18	NC	D18	NC
C19	PCIE6_MPCIE_RX_DP	D19	PCIE6_MPCIE_TX_DP
C20	PCIE6_MPCIE_RX_DN	D20	PCIE6_MPCIE_TX_DN
C21	GND (FIXED)	D21	GND (FIXED)
C22	NC	D22	NC
C23	NC	D23	NC

Pin No.	Definition	Pin No.	Definition
C24	eDP_HPD	D24	NC
C25	NC	D25	NC
C26	NC	D26	DDI0_TX0_DP
C27	NC	D27	DDI0_TX0_DN
C28	NC	D28	NC
C29	NC	D29	DDI0_TX1_DP
C30	NC	D30	DDI0_TX1_DN
C31	GND (FIXED)	D31	GND (FIXED)
C32	DDI1_DDC_SCL	D32	DDI0_TX2_DP
C33	DDI1_DDC_SDA	D33	DDI0_TX2_DN
C34	NC	D34	NC
C35	NC	D35	NC
C36	DDI2_DDC_SCL	D36	DDI0_TX3_DP
C37	DDI2_DDC_SDA	D37	DDI0_TX3_DN
C38	NC	D38	NC
C39	DDI2_TX0_DP	D39	DDI1_TX0_DP
C40	DDI2_TX0_DN	D40	DDI1_TX0_DN
C41	GND (FIXED)	D41	GND (FIXED)
C42	DDI2_TX1_DP	D42	DDI1_TX1_DP
C43	DDI2_TX1_DN	D43	DDI1_TX1_DN
C44	DDI2_HPD	D44	DDI1_HPD
C45	NC	D45	NC
C46	DDI2_TX2_DP	D46	DDI1_TX2_DP
C47	DDI2_TX2_DN	D47	DDI1_TX2_DN
C48	NC	D48	NC
C49	DDI2_TX3_DP	D49	DDI1_TX3_DP
C50	DDI2_TX3_DN	D50	DDI1_TX3_DN
C51	GND (FIXED)	D51	GND (FIXED)
C52	NC	D52	NC
C53	NC	D53	NC
C54	NC	D54	NC
C55	NC	D55	NC
C56	NC	D56	NC
C57	NC	D57	GND
C58	NC	D58	NC
C59	NC	D59	NC
C60	GND (FIXED)	D60	GND (FIXED)
C61	NC	D61	NC
C62	NC	D62	NC
C63	NC	D63	NC
C64	NC	D64	NC

Pin No.	Definition	Pin No.	Definition
C65	NC	D65	NC
C66	NC	D66	NC
C67	NC	D67	GND
C68	NC	D68	NC
C69	NC	D69	NC
C70	GND (FIXED)	D70	GND (FIXED)
C71	NC	D71	NC
C72	NC	D72	NC
C73	GND	D73	GND
C74	NC	D74	NC
C75	NC	D75	NC
C76	GND	D76	GND
C77	NC	D77	NC
C78	NC	D78	NC
C79	NC	D79	NC
C80	GND (FIXED)	D80	GND (FIXED)
C81	NC	D81	NC
C82	NC	D82	NC
C83	NC	D83	NC
C84	GND	D84	GND
C85	NC	D85	NC
C86	NC	D86	NC
C87	GND	D87	GND
C88	NC	D88	NC
C89	NC	D89	NC
C90	GND (FIXED)	D90	GND (FIXED)
C91	NC	D91	NC
C92	NC	D92	NC
C93	GND	D93	GND
C94	NC	D94	NC
C95	NC	D95	NC
C96	GND	D96	GND
C97	NC	D97	NC
C98	NC	D98	NC
C99	NC	D99	NC
C100	GND (FIXED)	D100	GND (FIXED)
C101	NC	D101	NC
C102	NC	D102	NC
C103	GND	D103	GND
C104	ATX_12V	D104	ATX_12V
C105	ATX_12V	D105	ATX_12V

Pin No.	Definition	Pin No.	Definition
C106	ATX_12V	D106	ATX_12V
C107	ATX_12V	D107	ATX_12V
C108	ATX_12V	D108	ATX_12V
C109	ATX_12V	D109	ATX_12V
C110	GND (FIXED)	D110	GND (FIXED)

Chapter 3

Chapter 3 – BIOS

3.1 Introduction

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

3.1.1 How to Entering into BIOS menu

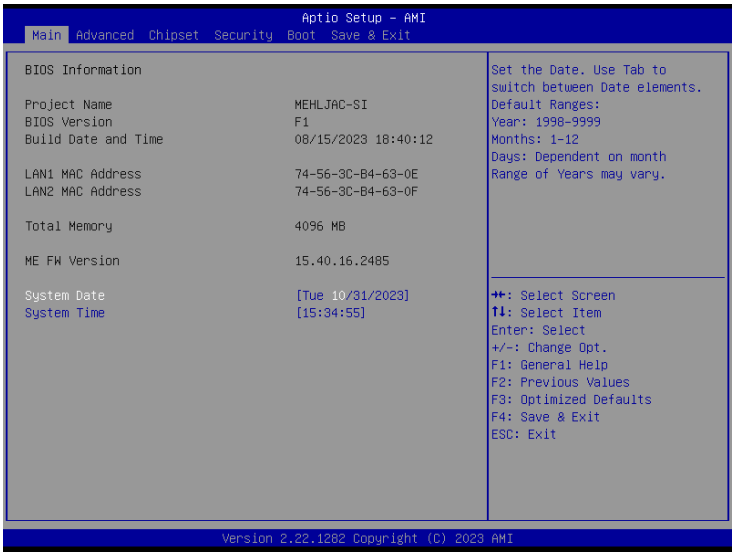
Once the system is power on, press the <DEL> key as soon as possible to access into BIOS Setup program.

3.1.2 Function Keys to setup in BIOS Setup program

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

3.2 The Main Menu

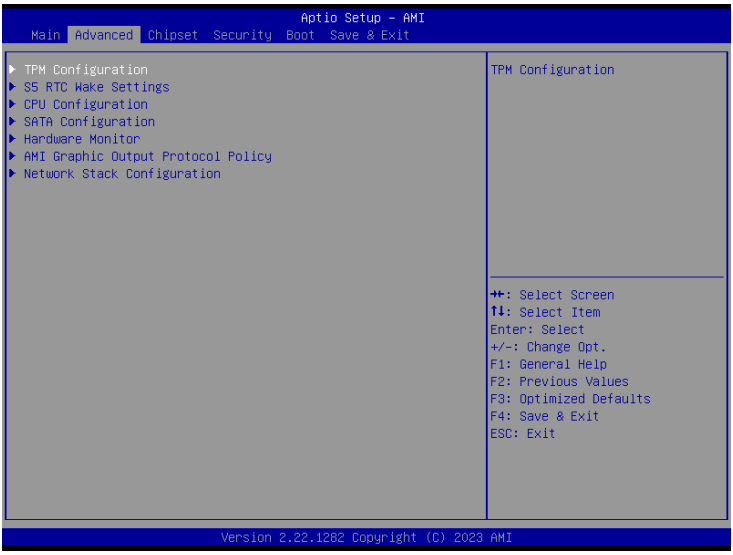
The main menu shows the basic system information.
Use arrow keys to move among the items.



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

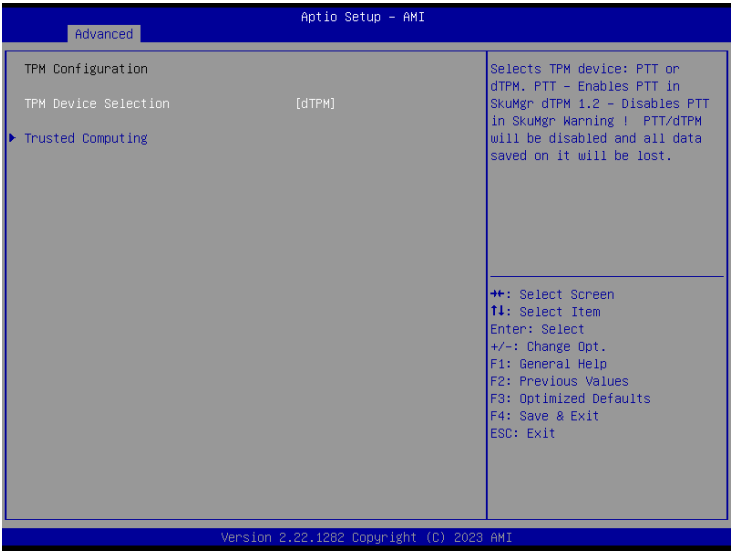
3.3 Advanced

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



3.3.1 TPM Configuration

Use TPM Configuration submenu to choose TPM interface.

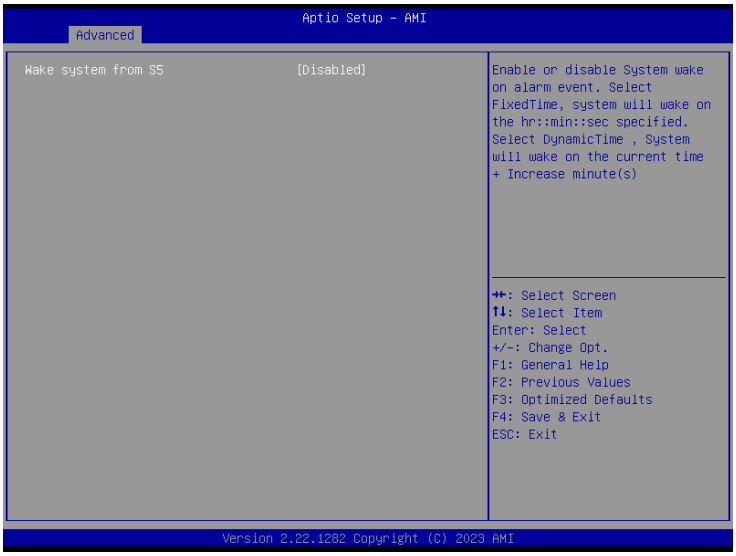


Item	Description
TPM Device Selection	**PTT : Internal TPM** **dTPM : External TPM (When using External TPM module or having TPM chip on MB) (Default setting)**

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

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

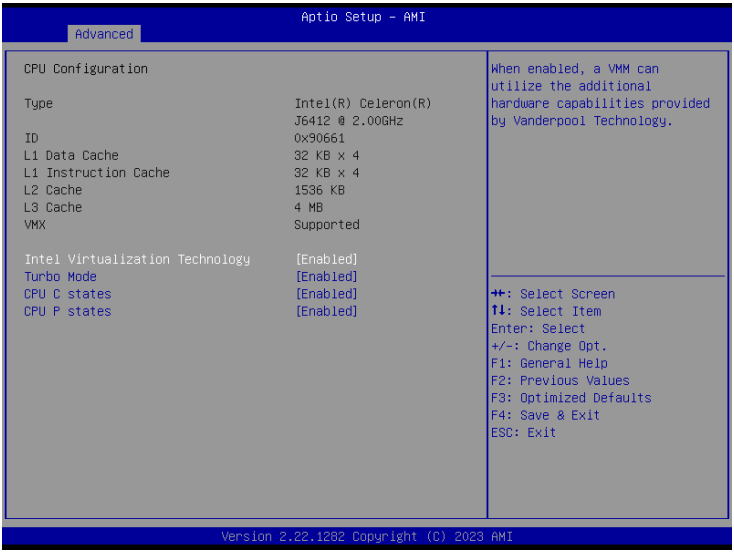
3.3.2 S5 RTC Wake Settings



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

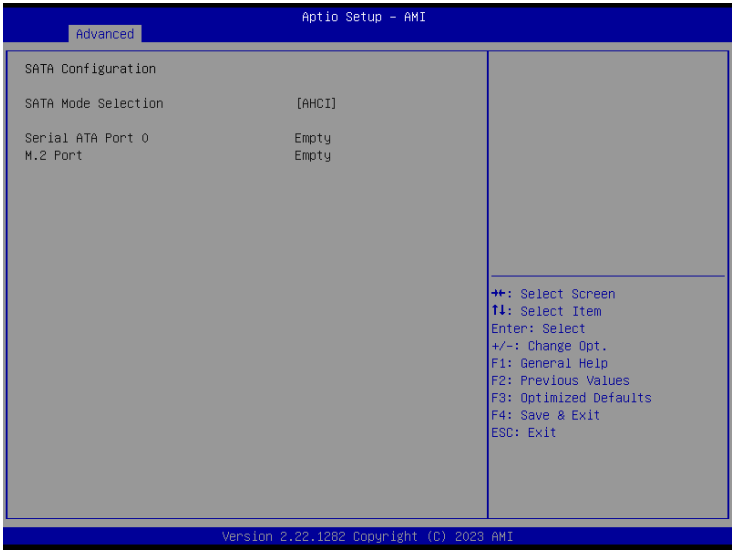
3.3.3 CPU Configuration

This submenu shows detailed CPU informations.



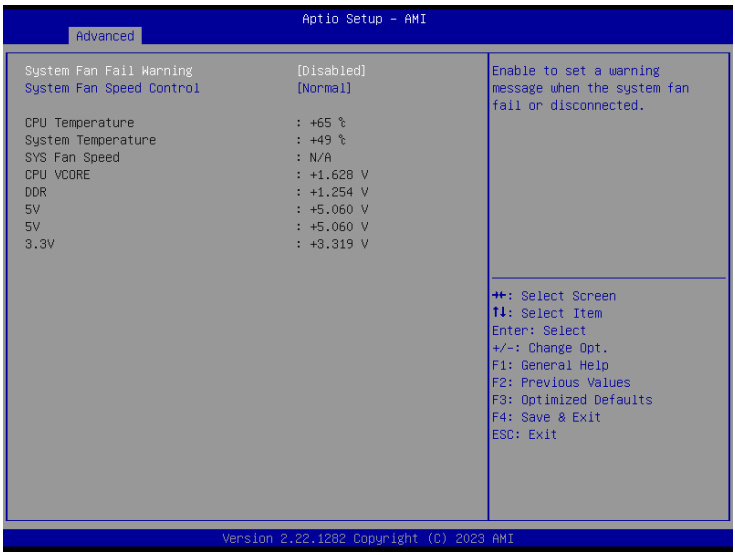
Item	Description
Intel Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. **Enabled : Enables Intel Virtualization Technology (Default setting)** **Disabled : Disables Intel Virtualization Technology**
Turbo Mode	**Enabled : Enables Turbo Mode (Default setting)** **Disabled : Disables Turbo Mode**
CPU C states	Command CPU to enter into low power consumption mode when CPU is under idle mode. **Enabled : Enables C states (Default setting)** **Disabled : Disables C states**
CPU P states	CPU will adjust frequency depends on it's loading. **Enabled : Enables CPU P states function (Default setting)** **Disabled : Disables CPU P states function**

3.3.4 SATA Configuration



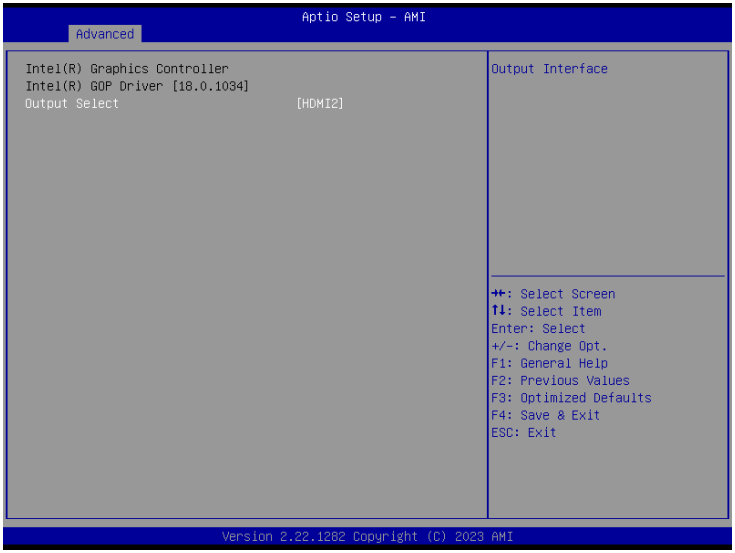
Item	Description
SATA Mode Selection	AHCI : Configures the SATA controllers to AHCI mode. (Default setting)
Serial ATA Port 0	shows 2.5" SATA HDD/SSD information
M.2 Port	shows M.2 SATA interface SSD information

3.3.5 Hardware Monitor



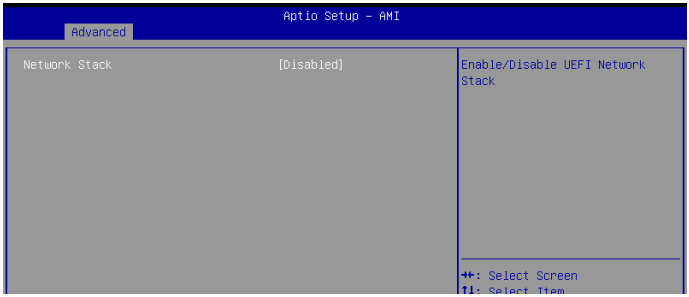
Item	Description
System Fan Fail Warning	**Enabled : Enables System FAN Fail warning alert function** **Disabled : Disables System FAN Fail warning alert function (Default setting)**
System Fan Speed Control	**Normal : Fan speed set by BIOS default (Default setting)** **Full Speed : Set Fan operates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

3.3.6 AMI Graphic Output Protocol Policy

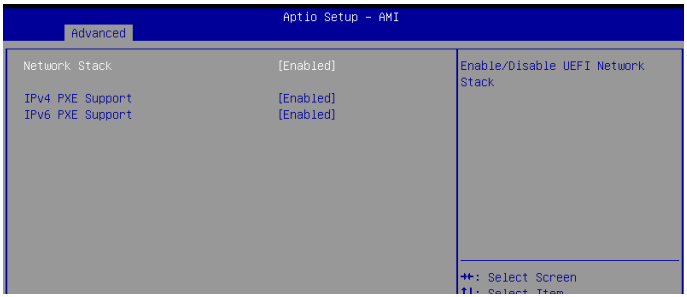


Item	Description
Output Select	Choose default monitor output when there are more than one monitor plugged on the motherboard.

3.3.7 Network Stack Configuration

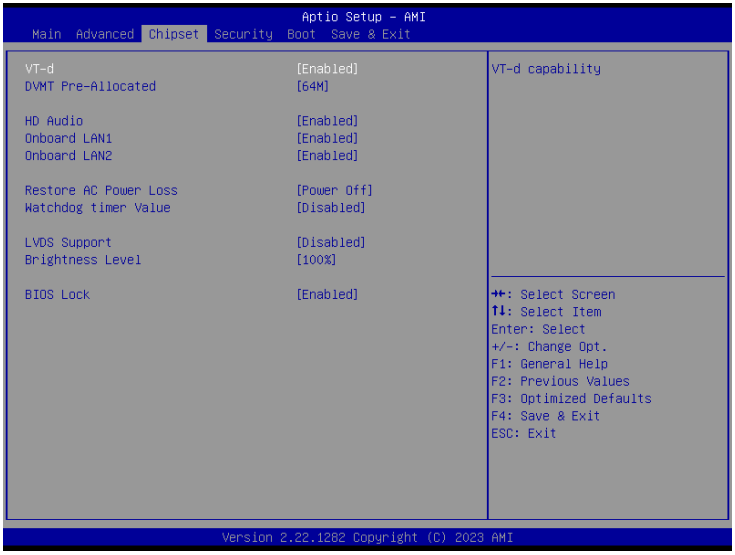


When Network stack is enabled :



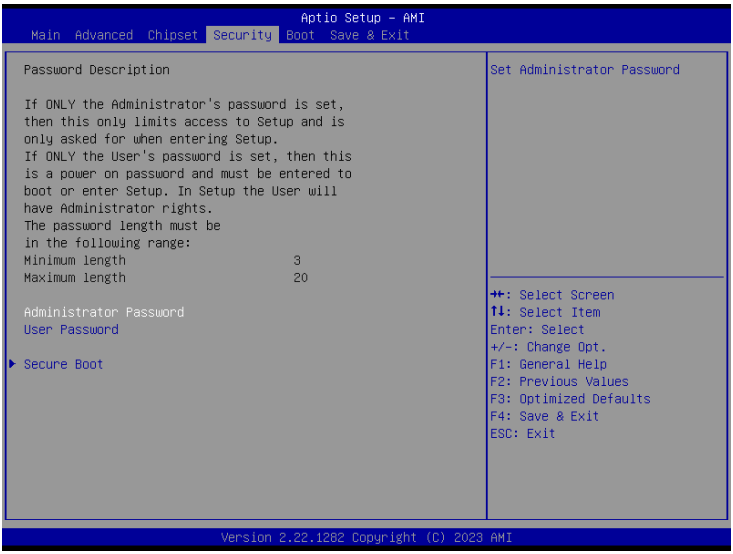
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode **Disabled : Disables UEFI Network Stack (Default setting)** **Enabled : Enables UEFI Network Stack**
IPv4 PXE Support	When Network stack is enabled : **Disabled : Disables IPv4 PXE Support** **Enabled : Enables IPv4 PXE Support (Default setting)**
IPv6 PXE Support	When Network stack is enabled : **Disabled : Disables IPv6 PXE Support** **Enabled : Enables IPv6 PXE Support (Default setting)**

3.4 Chipset

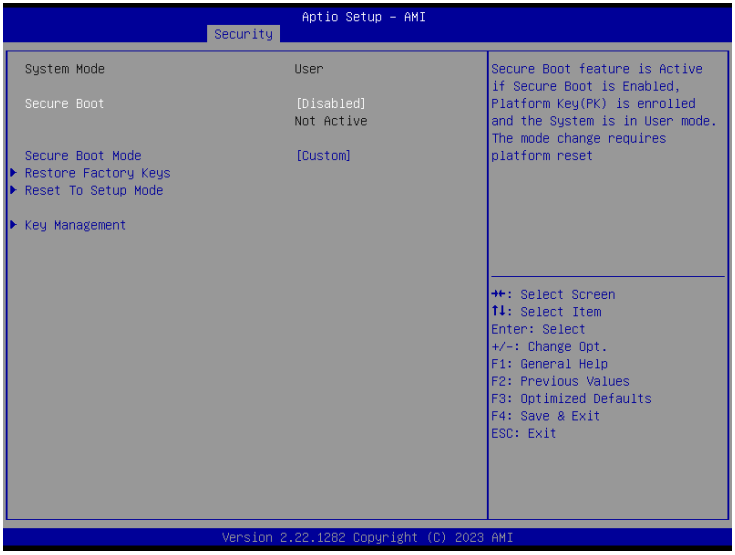


Item	Description
VT-d	**Enabled : Enables VT-d function (Default setting)** **Disabled : Disables VT-d function**
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor **Option items : 32M , 64M(Default setting) , 128M , 256M**
HD Audio	Enable/Disable onboard audio controller **Enabled : Enables onboard audio controller (Default setting)** **Disabled : Disables onboard audio controller**
Onboard LAN1 **Onboard LAN2**	Enable/Disable onboard LAN controller **Enabled : Enables onboard LAN controller (Default setting)** **Disabled : Disables onboard LAN controller**
Restore AC Power Loss	To set which option the system should returns if a sudden power loss occured **Power off : Do not power on when the power is back (Default setting)** **Power on : System power on when the power is back** **Last state : Restore the system to the state before power loss occures**
Watchdog timer Value	Enable/Disable Watchdog Timer function **Enabled : Enables Watchdog Timer function** **Disabled : Disabled Watchdog Timer function (Default setting)**
LVDS Support	**Disabled : Disables LVDS Support (Default setting)** **Enabled : Enables LVDS Support**
Brightness Level	To modified the backlight brightness of the LVDS panel **Option items : 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100% (Default Setting)**
BIOS Lock	Enable/Disable BIOS Lock function **Enabled : Enables BIOS Lock function (Default setting)** **Disabled : Disabled BIOS Lock funtion**

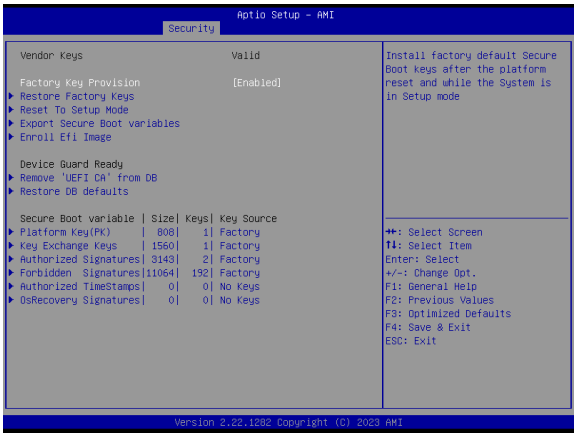
3.5 Security



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



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



Item	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode **Enabled : Enables Factory Key Provision (Default setting)** **Disabled : Disables Factory Key Provision**
Restore Factory Keys	To restore factory settings **Yes : Agree to restore factory settings** **No : Cancel to restore factory settings**
Reset To Setup Mode	**Yes : Agree to setup mode** **No : Cancel to setup mode**
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**

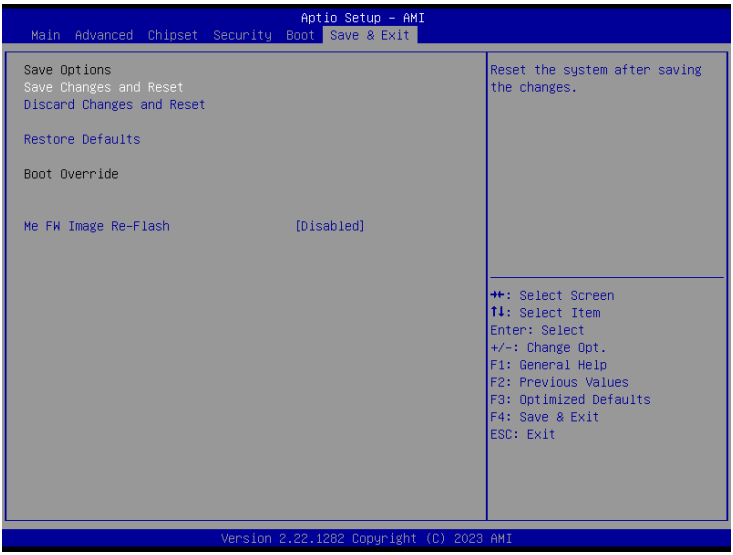
Item	Description
Platform Key (PK)	These items allows you to enroll factory defaults or load Certificates from a file.
Key Exchange Keys	
Authorized Signatures	
Forbidden Signatures	
Authorized TimeStamps	
OsRecovery Signatures	

3.6 Boot

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

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

3.7 Save & Exit



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