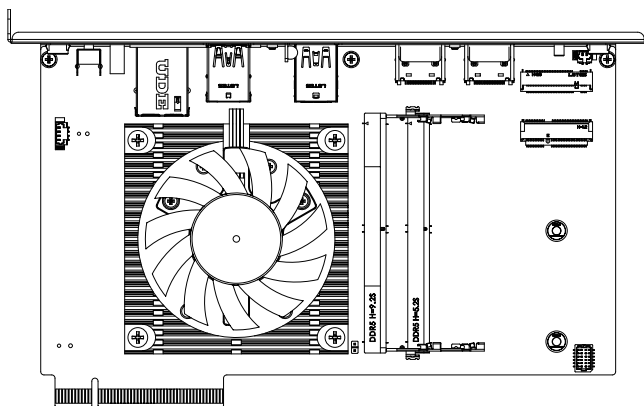


SDM-1345EAL (MRLUCAL-SI) SDM-1335AL (MRLU5AL-SI) SDM-1315AL (MRLU3AL-SI)

Smart Display Module Series
Quick Start Guide



Copyright Notice

This document is copyrighted, 2023. All rights are reserved. The original manufacturer reserves the right to make improvements to the products described in this manual at any time without notice.

No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of the original manufacturer. Information provided in this manual is intended to be accurate and reliable. However, the original manufacturer assumes no responsibility for its use, or for any infringements upon the rights of third parties that may result from its use.

The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, GIGAIPC assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.

GIGAIPC reserves the right to make changes in the product design without notice to its users.

Acknowledgement

All other products' name or trademarks are properties of their respective owners.

- Microsoft Windows is a registered trademark of Microsoft Corp.
- Intel, Pentium, Celeron, and Xeon are registered trademarks of Intel Corporation
- Core, Atom are trademarks of Intel Corporation
- ITE is a trademark of Integrated Technology Express, Inc.
- IBM, PC/AT, PS/2, and VGA are trademarks of International Business Machines Corporation.

All other product names or trademarks are properties of their respective owners.

Packing List

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

Item	Quantity
SDM-1345EAL or SDM-1335AL or SDM-1315AL	1
SCREW KIT WITH #0 ZIPLOCK BAG SCREW-BIND M3.0*L5.0 NI (P/N : 25KSD-130053-S0R)	1

- Followings are the components only when choosing M.2 NVMe SSD for SKU combination.
- To get installation instructions, please see P.31

Item	Quantity
DIMM2 PAD (P/N : 25ST3-200086-T5R)	1
M.2 Standoff (P/N : 12KSF-F10303-20R)	1
M.2 Screw (P/N: 25KSG-130048-S0R)	1
M.2 Bracket (P/N: 25ST1-1231Z0-S7R)	1

※Optional kit :

Item	Quantity
Internal Wi-Fi Cable (P/N: 25CA0-090004-A5S (90mm) + 25CA0-280003-A5S (280mm))	1
External Wi-Fi 5 Antenna (P/N: 25CA0-112001-A5S)	2
External Wi-Fi 6/6E Antenna (P/N: 25CA0-163002-A5S)	2

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

Warning!



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.

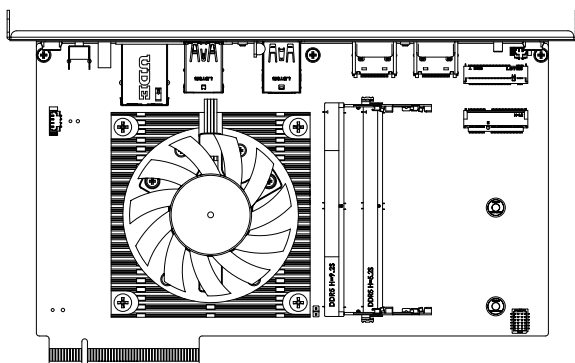
Table Contents

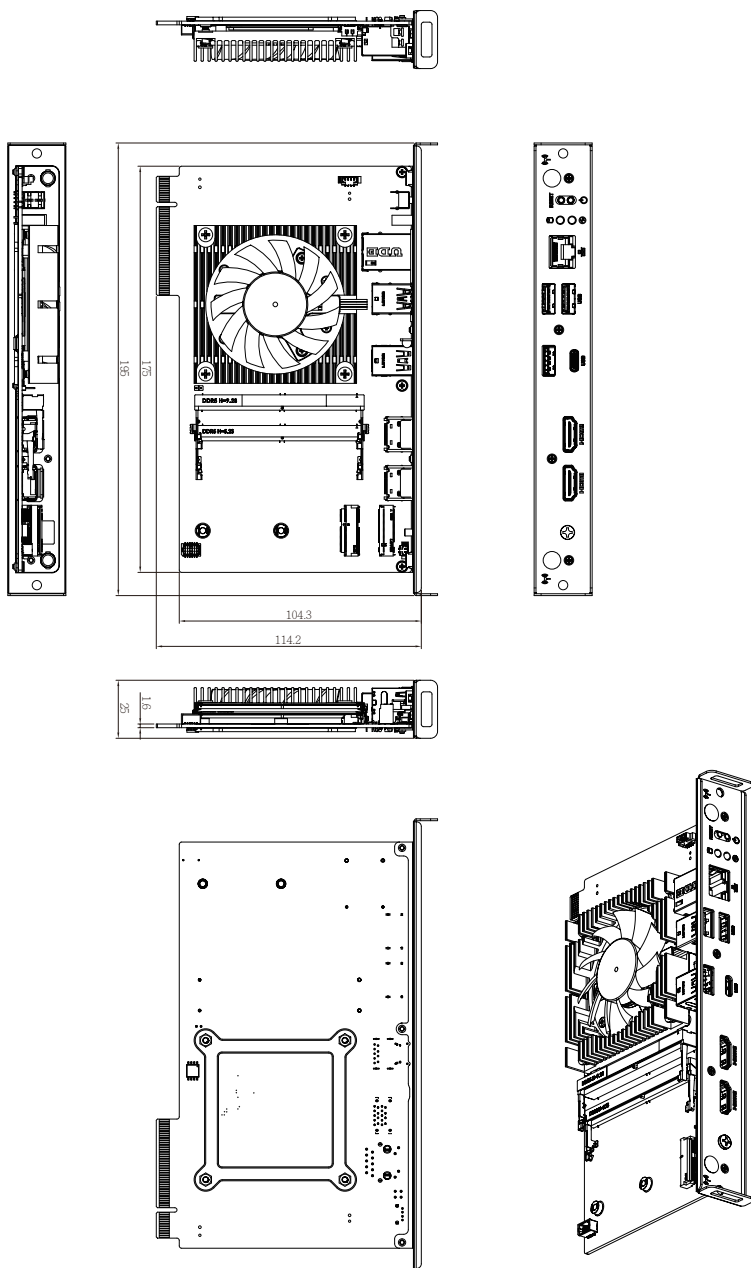
Smart Display Module Series	1
Quick Start Guide	
Copyright Notice	2
Acknowledgement	3
Packing List.....	4
About this Document	5
Safety Precautions	6
FCC Statement.....	8
 Chapter 1 - Product Specifications	 11
1.1 Specifications	13
 Chapter 2 – Hardware Information	 15
2.1 Jumpers and Connectors	16
2.2.1 HDMI_20, HDMI_21 (HDMI Connector)	18
2.2.2 USB32_2 (USB 3.2 type A Gen 2x1 connector).....	19
2.2.3 USBTC (USB 3.2 type C Gen 2x2 connector).....	20
2.2.4 USB32_1 (USB 3.2 type A Gen 2x1 connector).....	21
2.2.5 LAN (LAN connector)	22
2.2.6 SODIMMA, SODIMMB (DDR5 SO-DIMM sockets)	23
2.2.7 M2M (1 x M.2 slot, 2280 M-key)	24
2.2.8 M2E (1 x M.2 slot, 2230 E-key)	25
2.2.9 CPU_FAN (CPU Fan connector).....	26
2.2.10 BATTERY (1 x Battery cable connector)	27

Chapter 3 – SDM-L Installation	28
3.1 Dimension	29
3.2 Installation	30
 Chapter 4 – BIOS	 33
4.1 Introduction	34
4.2 The Main Menu.....	35
4.3 Advanced	36
4.3.1 AMT Configuration (For SDM-1345EAL, SDM-1335AL).	37
4.3.2 TPM Configuration.....	42
4.3.3 CPU Configuration	44
4.3.4 IT8613 Super IO Configuration	46
4.3.5 Hardware Monitor	47
4.3.6 S5 RTC Wake Settings	48
4.3.7 Intel TXT Information (For SDM-1345EAL, SDM-1335AL)	49
4.3.8 Network Stack Configuration.....	50
4.3.9 NVMe Configuration	51
4.3.10 Offboard SATA Controller Configuration	52
4.3.11 Tls Auth Configuration	53
4.3.12 Intel(R) Ethernet Controller (3) I225-LM - 74:56:3C:BB: 18:98 (MAC address may varied based on different motherboard).....	54
4.4 Chipset	55
4.5 Security	56
4.6 Boot.....	59
4.7 Save & Exit	60

Chapter 1

Chapter 1 - Product Specifications





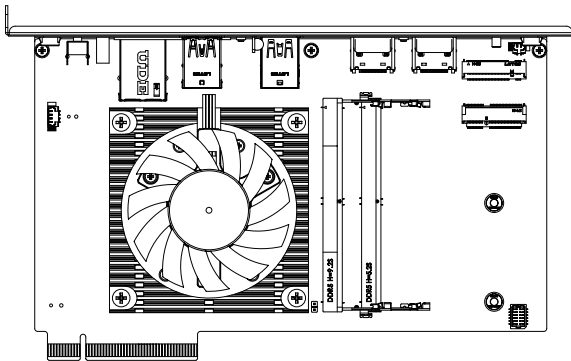
1.1 Specifications

Motherboard	SDM-1345EAL (MRLUCAL-SI)	SDM-1335AL (MRLU5AL-SI)	SDM-1315AL (MRLU3AL-SI)
Form Factor	SDM-Large 175W x 100D(mm)		
CPU	Intel® Core™ i5-1345UE Processor Intel® 7, 10 cores, 2P+8E, 12 threads, up to 4.6 GHz TDP 15W	Intel® Core™ i5-1335U Processor Intel® 7, 10 cores, 2P+8E, 12 threads, up to 4.6 GHz TDP 15W	Intel® Core™ i3-1315U Processor Intel® 7, 6 cores, 2P+4E, 8 threads, up to 4.5 GHz TDP 15W
Socket	1 x FCBGA1744		
Memory	2 x DDR5 SO-DIMM sockets, Max. Capacity 64 GB Support Dual Channel DDR5 5200 MHz memory modules		
Ethernet	1 x 2.5GbE LAN Port (Intel® I225LM)		
Video	Integrated Graphics Processor - Intel® Iris Xe Graphics: 1 x HDMI 2.1 (SDM), supporting a maximum resolution of 7680x4320 @60Hz 1 x Display Port 1.4a (SDM), supporting a maximum resolution of 7680x4320 @60Hz 1 x HDMI 2.1 (Rear), supporting a maximum resolution of 7680x4320 @60Hz 1 x HDMI 2.0 (Rear), supporting a maximum resolution of 4096x2160 @60Hz 1 x DP 1.4 through USB type C (8k), supporting a maximum resolution of 7680x4320 @60Hz (4 independent display outputs)		
		Integrated Graphics Processor - Intel® UHD Graphics for 13th Gen Intel® Processors: 1 x HDMI 2.1 (SDM), supporting a maximum resolution of 7680x4320 @60Hz 1 x Display Port 1.4a (SDM), supporting a maximum resolution of 7680x4320 @60Hz 1 x HDMI 2.1 (Rear), supporting a maximum resolution of 7680x4320 @60Hz 1 x HDMI 2.0 (Rear), supporting a maximum resolution of 7680x4320 @60Hz 1 x DP 1.4 through USB type C (8k), supporting a maximum resolution of 7680x4320 @60Hz (4 independent display outputs)	

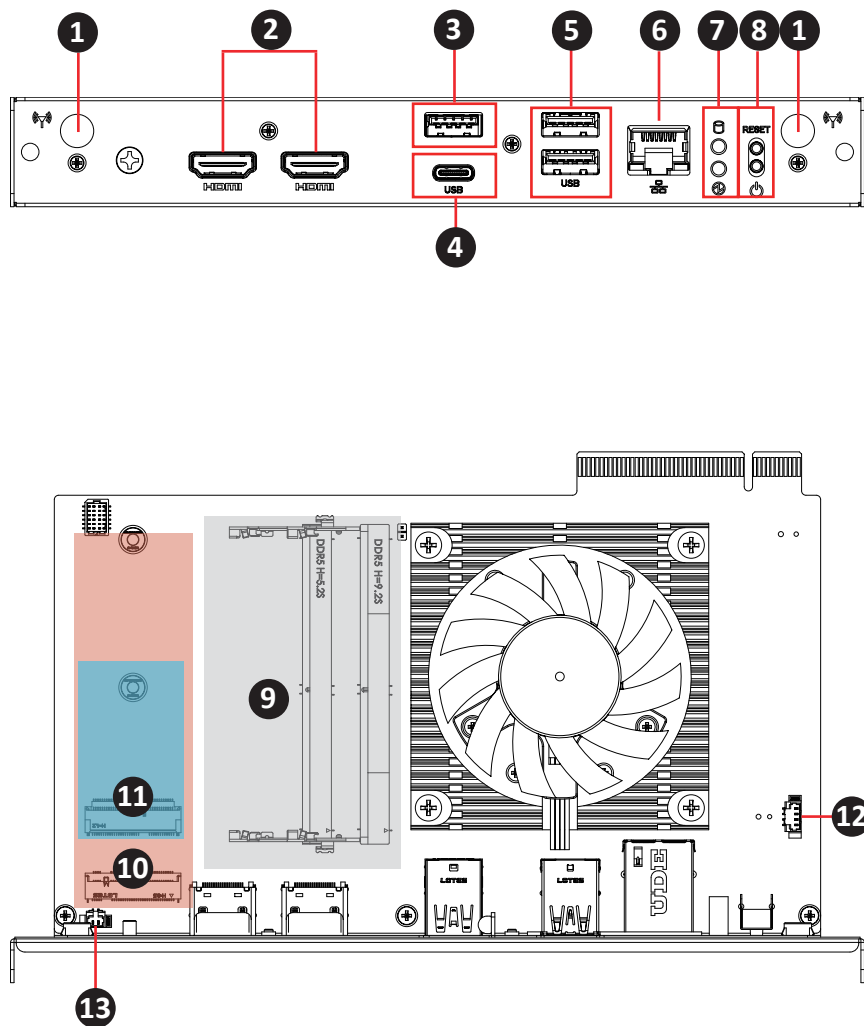
Motherboard	SDM-1345EAL (MRLUCAL-SI)	SDM-1335AL (MRLU5AL-SI)	SDM-1315AL (MRLU3AL-SI)
Audio	Intel® integrated Audio		
Expansion Slots	1 x 2280 M.2 M-Key (PCIe Gen4x4) 1 x 2230 M.2 E-Key		
Rear I/O	2 x HDMI 1 x RJ45 LAN Port 3 x USB 3.2 type A Gen 2x1 1 x USB 3.2 type C Gen 2x1 1 x PWR LED 1 x HDD LED 2 x External Antenna Holes (Optional) 1 x Reset button 1 x Power button		
TPM	Onboard TPM 2.0 security chip INFINEON SLB9670VQ2.0		
OS Compatibility	Windows® 10/11 (x64)		
Operating Properties	Operating temperature: 0°C to 55°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



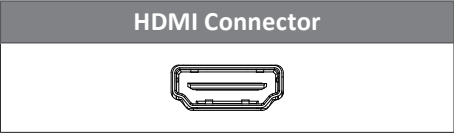
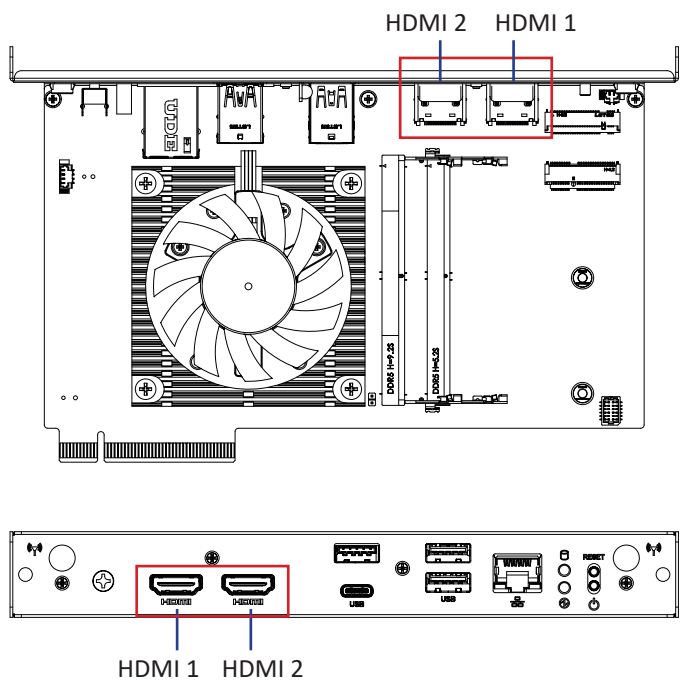
2.1 Jumpers and Connectors



No	Code	Description
1	Antenna hole	2 x Antenna (WiFi & BT) (Option)
2	HDMI_20 HDMI_21	2 x HDMI
3	USB32_2	1 x USB 3.2 type A Gen 2x1
4	USBTC	1 x USB 3.2 tyep C Gen 2x2
5	USB32_1	2 x USB 3.2 type A Gen 2x1
6	LAN	1 x RJ45
7	PS_LED	1 x HDD LED (Top) 1 x PWR LED (Bottom)
8	PSW_RST	1 x Reset button (Top) 1 x Power button (Bottom)
9	SODIMMA SODIMMB	2 x DDR5 SO-DIMM sockets
10	M2M	1 x M.2 slot, 2280 M-key
11	M2E	1 x M.2 slot, 2230 M-key
12	CPU_FAN	1 x CPU Fan connector
13	BATTERY	1 x Battery cable connector

2.2.1 HDMI_20, HDMI_21 (HDMI Connector)

2

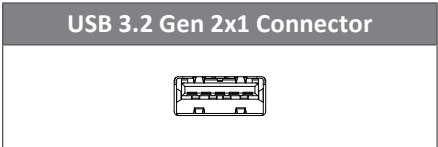
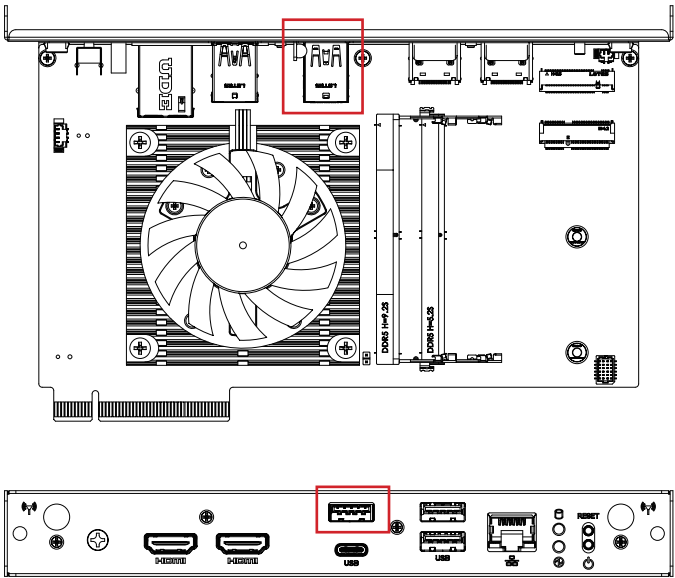


Pin No.	Definition	Pin No.	Definition
1	TX2p	11	GND
2	GND	12	CLKn
3	TX2n	13	NC
4	TX1p	14	NC
5	GND	15	SCL
6	TX1n	16	SDA
7	TX0p	17	GND
8	GND	18	5V
9	TX0n	19	Hot Plug Detect
10	CLKp		

Connector PN	Vendor
D13-0715-19681	WALTA

2.2.2 USB32_2 (USB 3.2 type A Gen 2x1 connector)

3

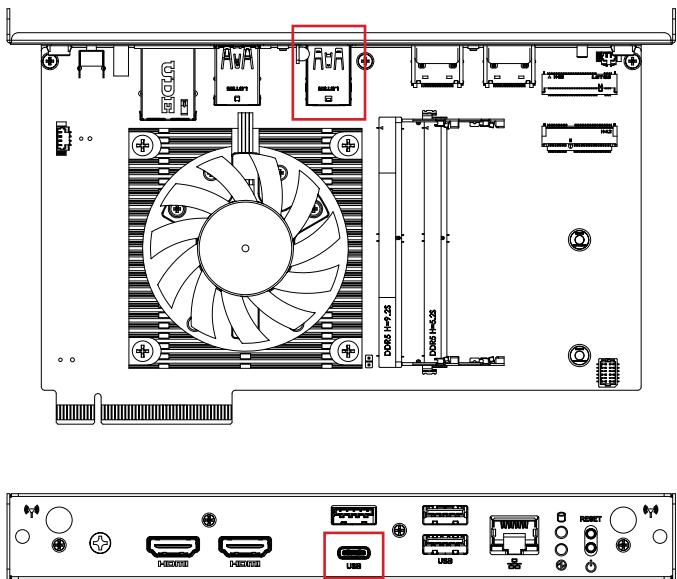


Connector PN	Vendor
AUSB0174-K005C	LOTES

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

2.2.3 USBTC (USB 3.2 type C Gen 2x2 connector)

4



USB Type C Connector

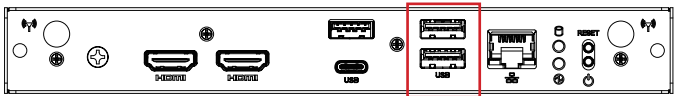
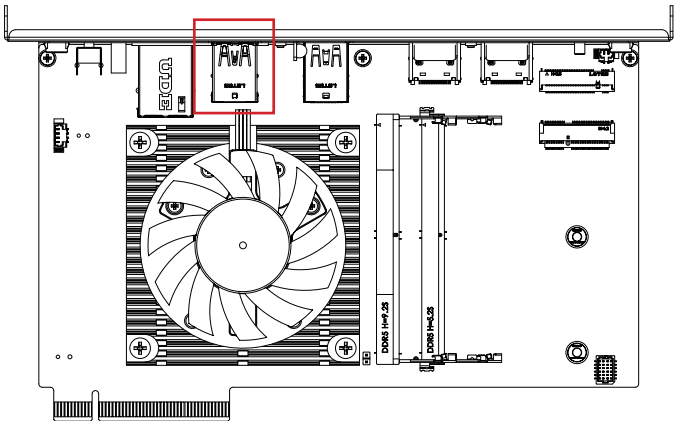

USB

Connector PN	Vendor
DX07S024JJ2	JAE

Pin No.	Definition	Pin No.	Definition
A1	GND	B1	GND
A2	TX1p	B2	TX2p
A3	TX1n	B3	TX2n
A4	VBUS	B4	VBUS
A5	CC1	B5	CC2
A6	Dp	B6	Dp
A7	Dn	B7	Dn
A8	NC	B8	NC
A9	VBUS	B9	VBUS
A10	RX2n	B10	RX1n
A11	RX2p	B11	RX1p
A12	GND	B12	GND

2.2.4 USB32_1 (USB 3.2 type A Gen 2x1 connector)

5



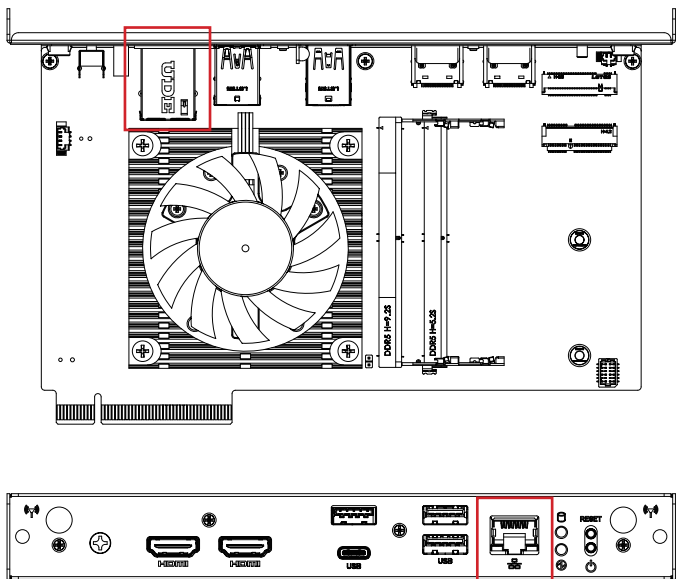
USB 3.2 Gen 2x1 Connector			
			

Connector PN	Vendor
18-A9830-6A33-A	TCONN

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

2.2.5 LAN (LAN connector)

6



LAN Connector

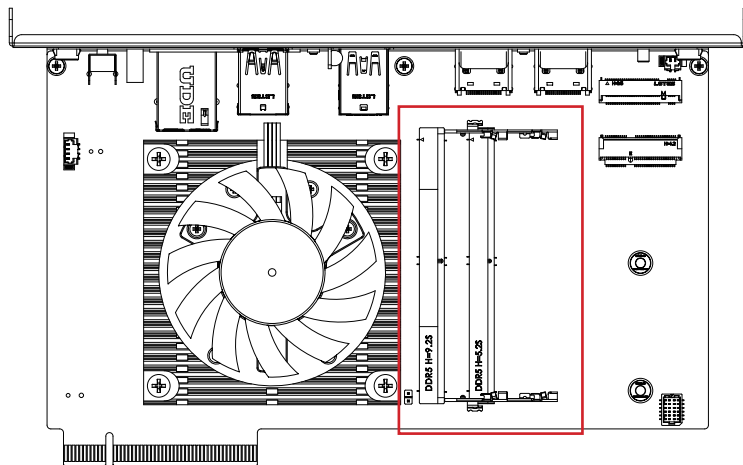
Pin No.	Definition	Pin No.	Definition
1	TX1+	4	TX3+
2	TX1-	5	TX3-
3	TX2+	7	TX4+
6	TX2-	8	TX4-

State	Description
Orange On	2.5Gbps data rate
Green On	1Gbps data rate
Off	100M&10Mbps data rate

Connector PN	Vendor
RB1-GB-0010	UDE

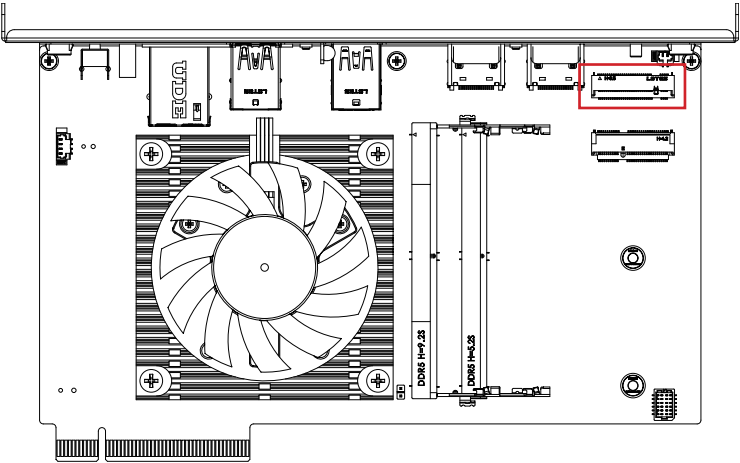
2.2.6 SODIMMA, SODIMMB (DDR5 SO-DIMM sockets)

9

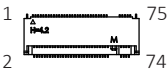


2.2.7 M2M (1 x M.2 slot, 2280 M-key)

10



M.2 M Key Connector



Pin No.	Definition	Pin No.	Definition
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE3 RXn	6	NC
7	PCIE3 RXp	8	NC
9	GND	10	SSD LED
11	PCIE3 TXn	12	3.3V
13	PCIE3 TXp	14	3.3V
15	GND	16	3.3V
17	PCIE2 RXn	18	3.3V
19	PCIE2 RXp	20	NC
21	GND	22	NC
23	PCIE2 TXn	24	NC
25	PCIE2 TXp	26	NC
27	GND	28	NC
29	PCIE1 RXn	30	NC
31	PCIE1 RXp	32	NC
33	GND	34	NC

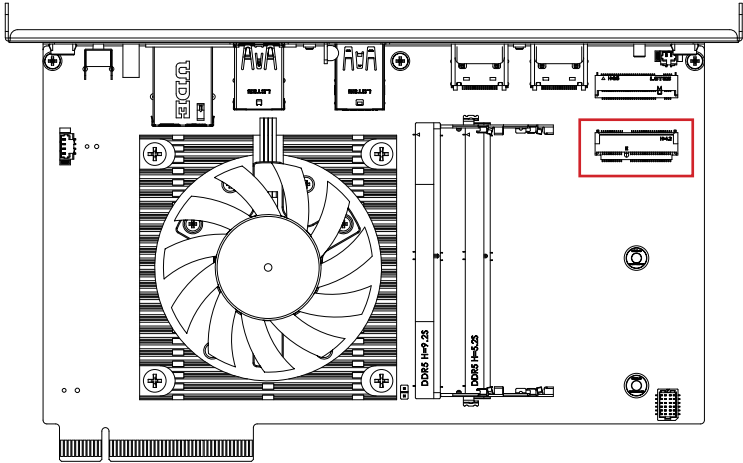
Pin No.	Definition	Pin No.	Definition
35	PCIE1 TXn	36	NC
37	PCIE1 TXp	38	Dev sleep
39	GND	40	NC
41	PCIE0 RXn	42	NC
43	PCIE0 RXp	44	NC
45	GND	46	NC
47	PCIE0 TXn	48	NC
49	PCIE0 TXp	50	PCI Reset
51	GND	52	PCIE Clock Request
53	PCIE Clockn	54	Wakeup
55	PCIE Clockp	56	NC
57	GND	58	NC

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

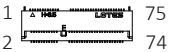
Connector PN	Vendor
80159-8523	BELLWETHER

2.2.8 M2E (1 x M.2 slot, 2230 E-key)

11



M.2 E Key Connector



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

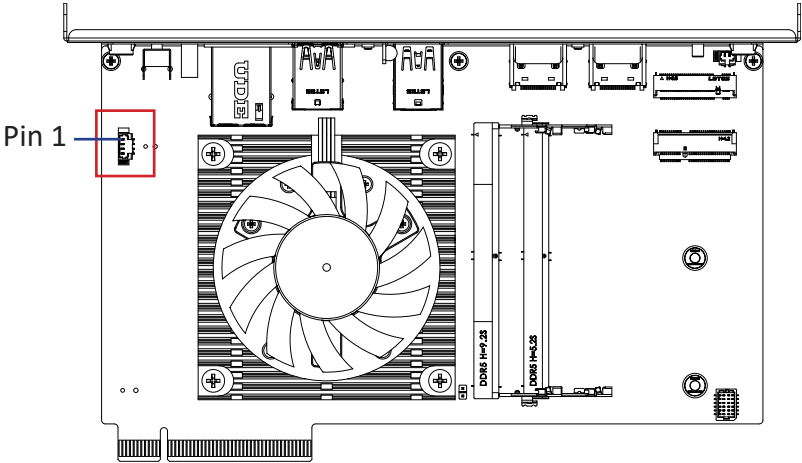
Pin No.	Definition	Pin No.	Definition
33	GND	32	NC
35	PCIE_TXp	34	NC
37	PCIE_TXn	36	NC

39	GND	38	CL_Reset
41	PCIE_RXp	40	CL_DATA
43	PCIE_RXn	42	CL_Clock
45	GND	44	NC
47	PCIE_CLOCKp	46	NC
49	PCIE_CLOCKn	48	NC
51	GND	50	SUSCLK
53	PCIE Clock Request	52	PCIRST
55	PCIE wake up	54	BT_Disable
57	GND	56	WLAN_DISABLE
59	NC	58	NC
61	NC	60	NC
63	GND	62	NC
65	NC	64	NC
67	NC	66	NC
69	GND	68	NC
71	NC	70	NC
73	NC	72	3.3V
75	GND	74	3.3V

Connector PN	Vendor
APCI0076-P002A	LOTES

2.2.9 CPU_FAN (CPU Fan connector)

12

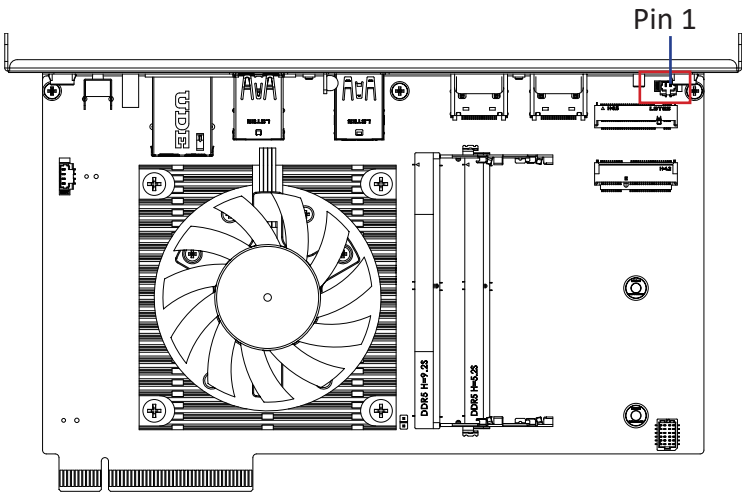


CPU FAN Connector	
	
Pin No.	Definition
1	GND
2	12V
3	Detect
4	Speed control

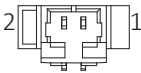
Connector PN	Vendor
85205-0470N	ACES
A1250WV-S-04PC	JOINT-TECH
Connector type	
1x4pin header, pitch 1.25mm	

2.2.10 BATTERY (1 x Battery cable connector)

13



Battery Connector

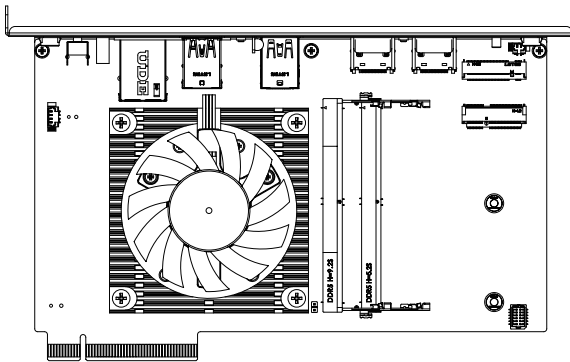


Pin No.	Definition
1	3.3V RTC
2	GND

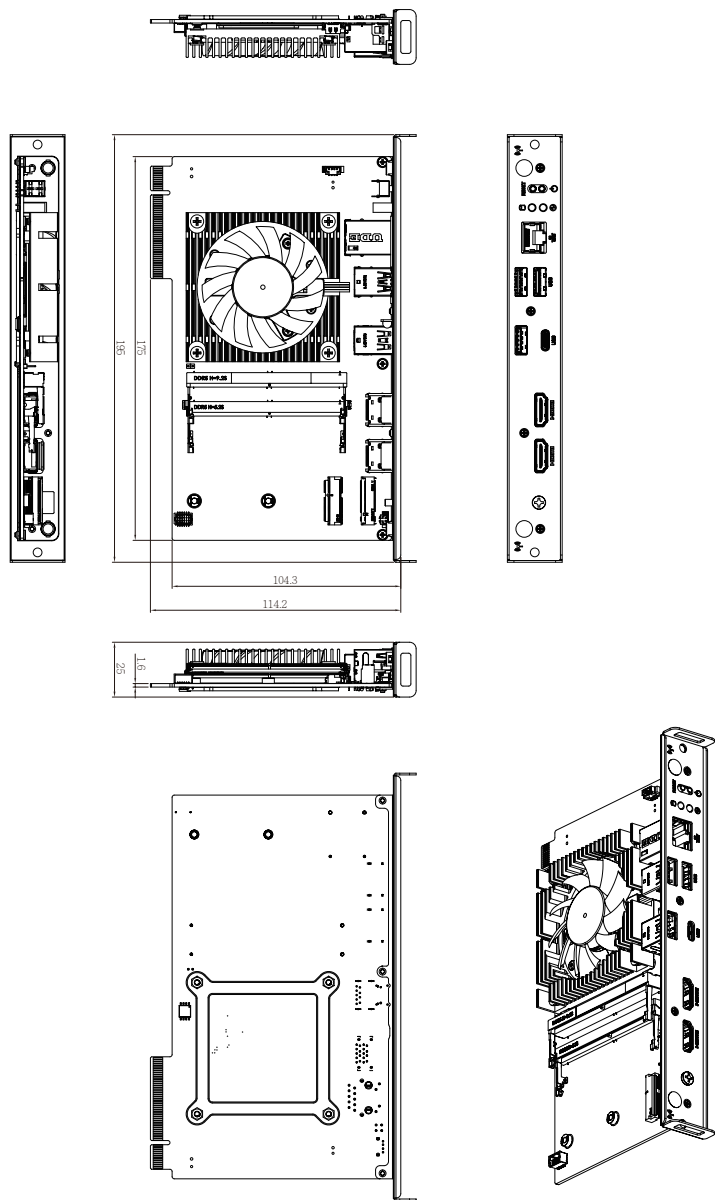
Connector type
1x2pin connector, pitch 1.25mm

Chapter 3

Chapter 3 – SDM-L Installation

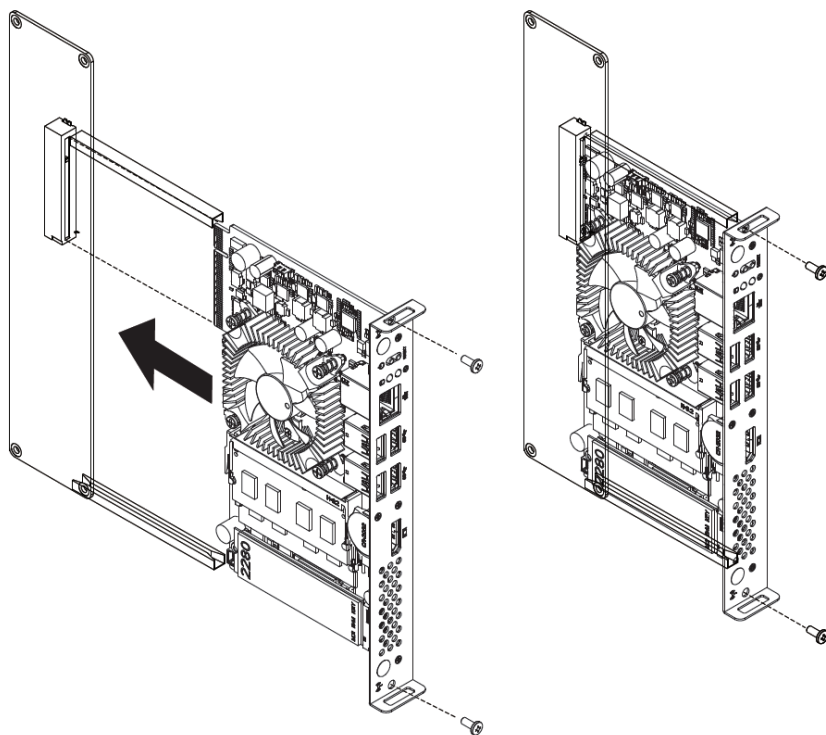


3.1 Dimension



3.2 Installation

[SDM Install]



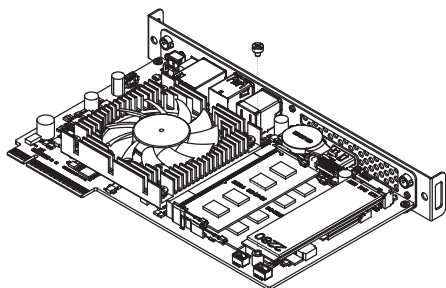
* The image is for reference only.
The actual product could be slightly different.

[M.2 SSD Heatplate module Install]

Following instructions are only for using M.2 NVMe SSD and the kit listed on P.4

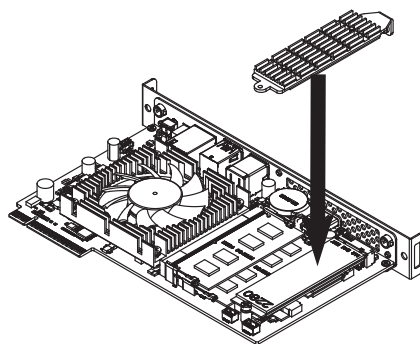
Step 1.

Remove the on-board screw
(Location : MSO1).
Carefully insert M.2 2280 SSD into
the M.2 slot, and use the standoff
which provided in the accessory kits
to secure the M.2 SSD.



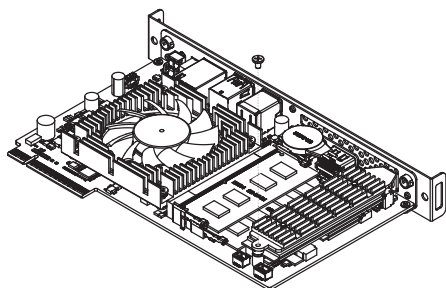
Step 2.

Remove the release paper on M.2
SSD Heatplate, and attach M.2 SSD
Heatplate module to the M.2 SSD.



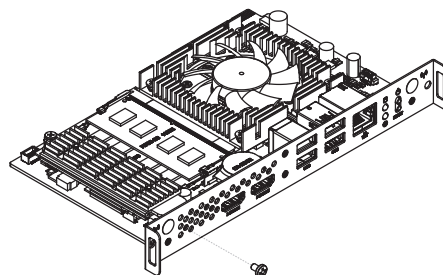
Step 3.

Tighten up the screw which was
previously removed.



Step 4.

Tighten up the screw which was
provided in the accessory kits on the
bracket.

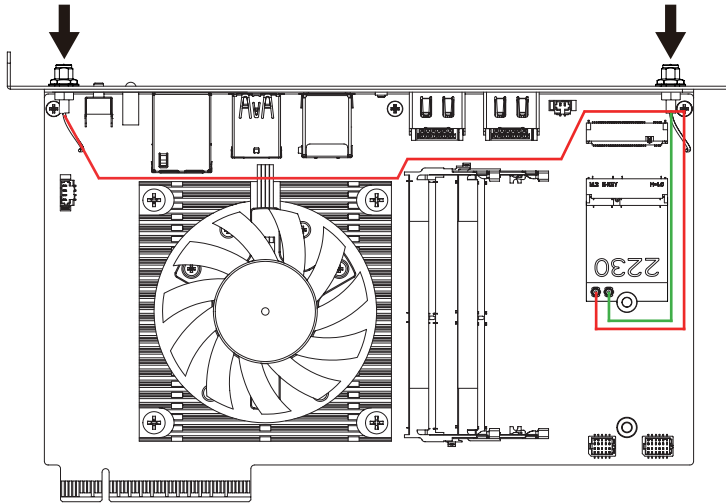


* The image is for reference only.
The actual product could be slightly different.

[Internal WiFi cable Install & Routing]

Using 280mm
Internal WiFi cable

Using 90mm
Internal WiFi cable



* The image is for reference only.
The actual product could be slightly different.

Chapter 4

Chapter 4 – BIOS

4.1 Introduction

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

4.1.1 How to Entering into BIOS menu

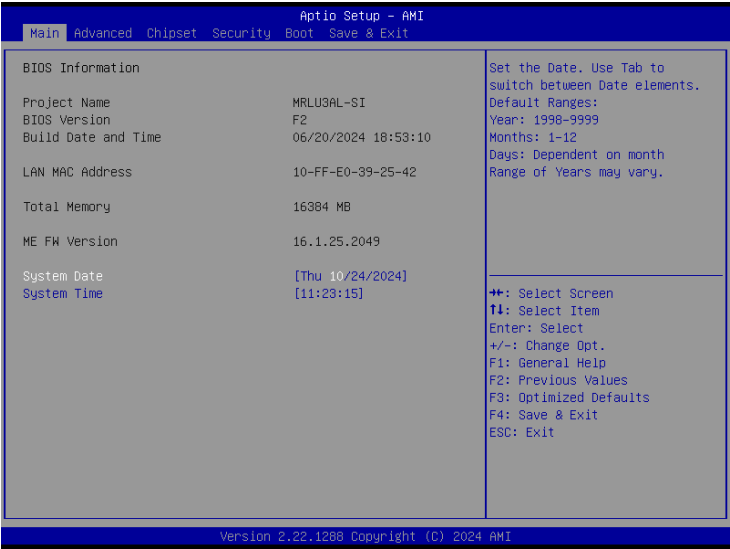
Once the system is power on, press the key as soon as possible to access into BIOS Setup program.

4.1.2 Function Keys to setup in BIOS Setup program

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

4.2 The Main Menu

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

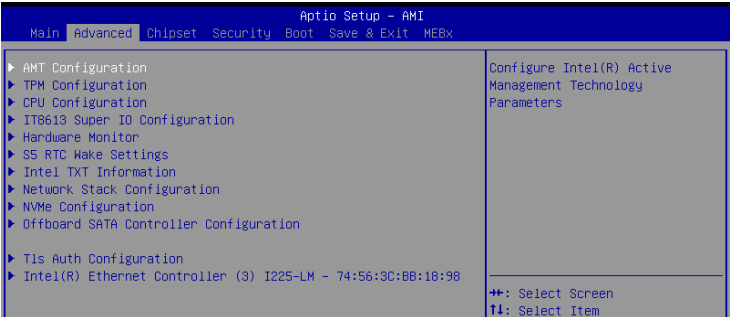


Items	Description
Project Name	Shows Project name information
BIOS Version	Shows the BIOS version of the system
Build Date and Time	Shows the Build Date and Time when the BIOS was created.
LAN MAC Address	Shows LAN MAC Address information
Total Memory	Shows the total memory size of the installed memory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

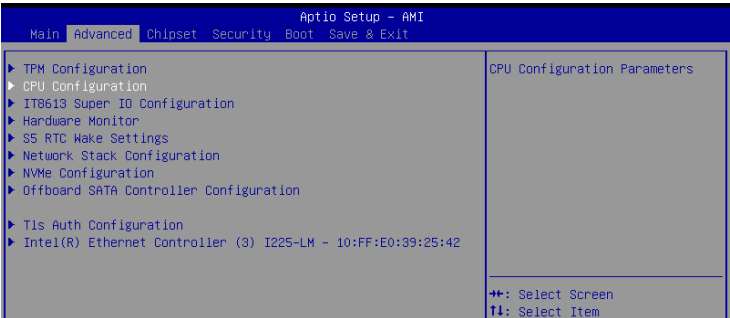
4.3 Advanced

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

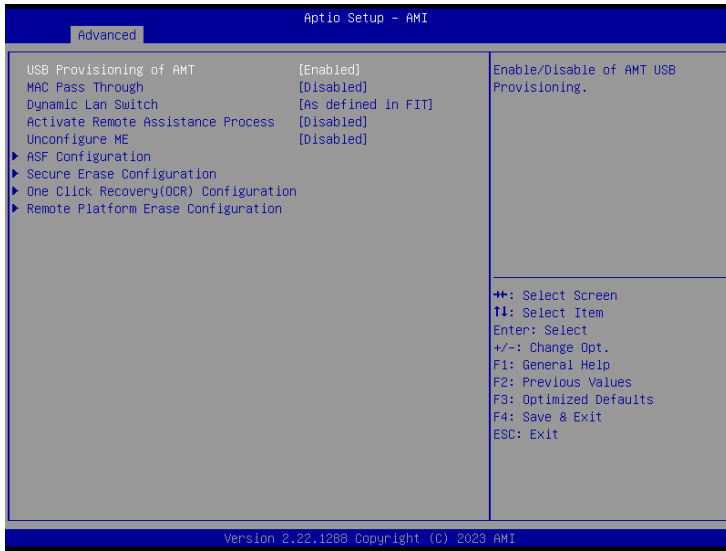
Items for SDM-1345EAL, SDM-1335AL



Items for SDM-1315AL



4.3.1 AMT Configuration (For SDM-1345EAL, SDM-1335AL)



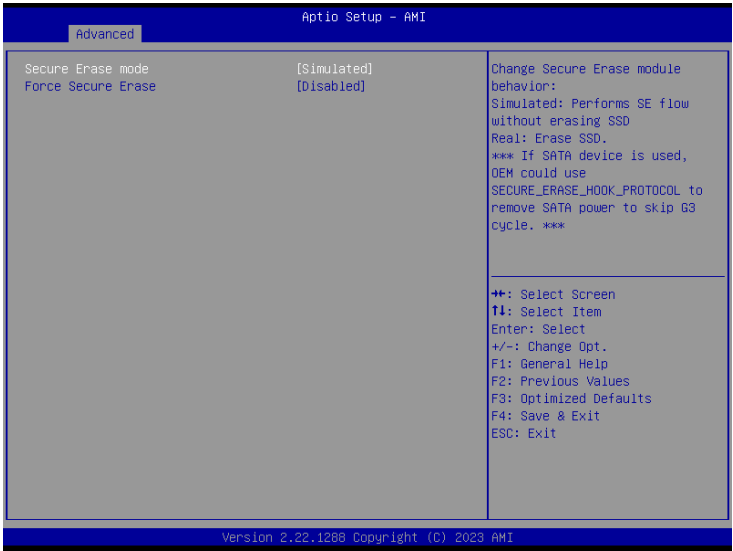
Item	Description
USB Provisioning of AMT	Inserting a specially formatted USB drive into a system, to let the other system remotely control. Disabled : Disables USB Provisioning of AMT Enabled : Enables USB Provisioning of AMT (Default setting)
MAC Pass Through	Disabled : Disables MAC Pass Through function (Default setting) Enabled : Enables MAC Pass Through function
Dynamic Lan Switch	Allow switching AMT support from Integrated LAN to Discrete LAN. Option items : As defined in FIT (Default setting), Integrated LAN, Discrete LAN.
Activate Remote Assistance Process	Trigger CIRA boot Disabled : Disables TPM feature (Default setting) Enabled : Enables TPM feature
Unconfigure ME	To Un-configure ME without password. Disabled : Disables Unconfigure ME (Default settings) Enabled : Enables Unconfigure ME

ASF Configuration



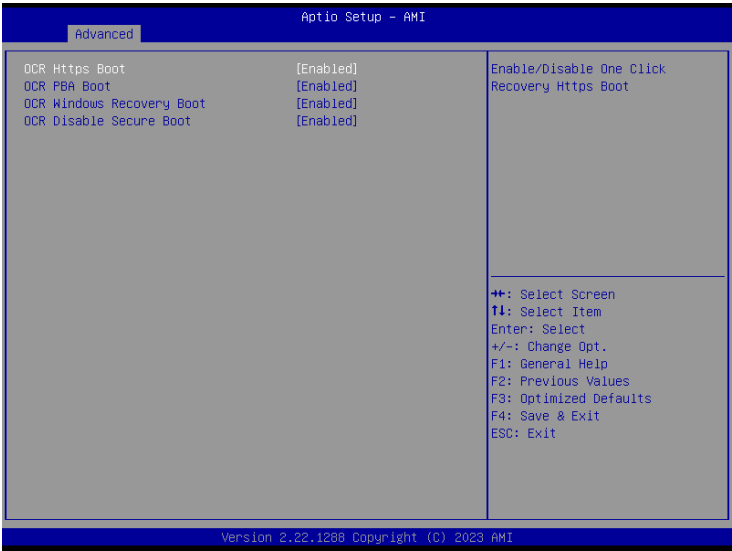
Item	Description
PET Progress	Choose to receive PET events or not Disabled : Disables PET Progress Enabled : Enables PET Progress (Default setting)
WatchDog	Choose to enables watchdog timer or not Disabled : Disables watchdog Timer (Default setting) Enabled : Enables watchdog Timer
OS Timer	Sets OS Watchdog Timer.
BIOS Timer	Sets BIOS Timer.
ASF Sensors Table	Disabled : Disables ASF Sensors Table (Default setting) Enabled : Enables ASF Sensors Table

Secure Erase Configuration



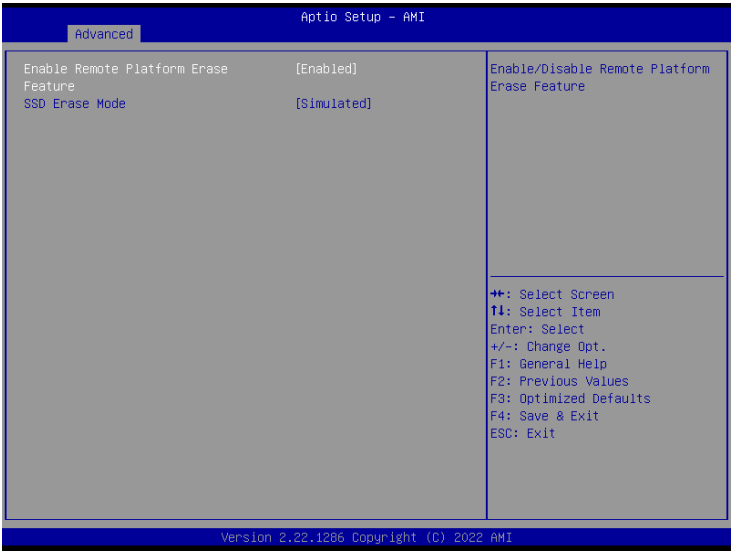
Item	Description
Secure Erase mode	Choose to enables secure erase mode or not. Simulated : Performs SE flow without erasing SSD (Default setting) Real : Erase SSD
Force Secure Erase	Force Secure Erase on next boot. Disabled : Disables Force Secure Erase (Default setting) Enabled : Enables Force Secure Erase

One Click Recovery (OCR) Configuration



Item	Description
OCR Https Boot	Enabled : Enables One Click Recovery Https Boot. (Default setting) Disabled : Disables One Click Recovery Https Boot.
OCR PBA Boot	Enabled : Enables One Click Recovery PBA Boot. (Default setting) Disabled : Disables One Click Recovery PBA Boot.
OCR Windows Recovery Boot	Enabled : Enables One Click Recovery Windows recovery boot. (Default setting) Disabled : Disables One Click Recovery Windows recovery boot.
OCR Disable Secure Boot	Allows CSME to request Secureboot to be disabled for One Click Recovery. Enabled : Enables One Click Recovery disable Secure Boot function. (Default setting) Disabled : Disables One Click Recovery disable Secure Boot function.

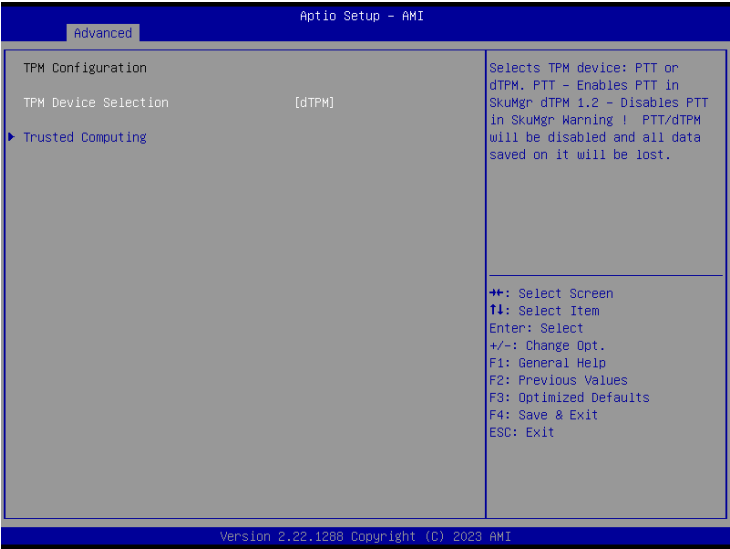
Remote Platform Erase Configuration



Item	Description
Enable Remote Platform Erase Feature	Disabled : Disables remote platform erase feature. Enabled : Enables remote platform erase feature. (Default setting)
SSD Erase Mode	Change RPE SSD Erase Action behavior Simulated : performs RPE SSD Erase flow without erasing SSD. (Default setting) Real : Erase SSD.

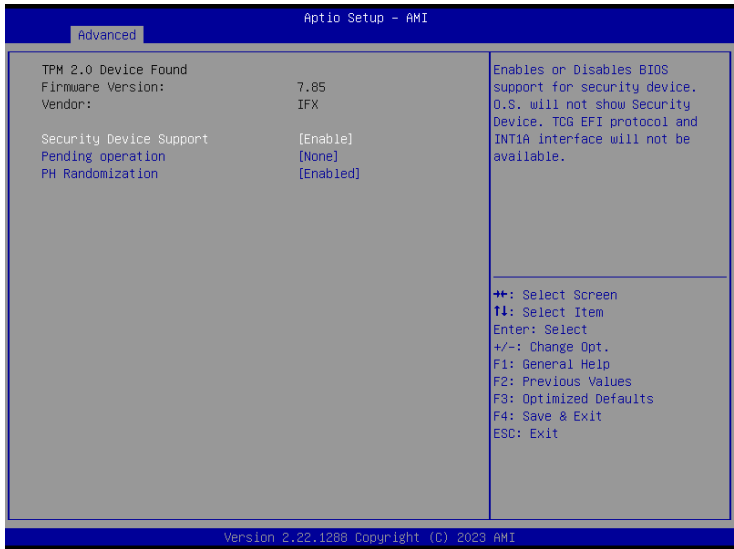
4.3.2 TPM Configuration

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
PH Randomization	Enabled : Enables Platform Hierarchy (PH) Randomization. (Default setting) Disabled : Disables Platform Hierarchy (PH) Randomization.

4.3.3 CPU Configuration

This submenu shows detailed CPU informations.

Items for SDM-1345EAL, SDM-1335AL

Advanced Aptio Setup - AMI		
CPU Configuration		
ID	0xB06A3	When enabled, a VMX can utilize the additional hardware capabilities provided by Vanderpool Technology.
Brand String	13th Gen Intel(R) Core(TM) i5-1335U	
VMX	Supported	
SMX/TXT	Supported	
Intel (VMX) Virtualization Technology	[Enabled]	++: Select Screen T1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values
Intel Trusted Execution Technology	[Disabled]	
Intel(R) Speed Shift Technology	[Enabled]	
Intel(R) SpeedStep(tm)	[Enabled]	
Turbo Mode	[Enabled]	
C states	[Enabled]	

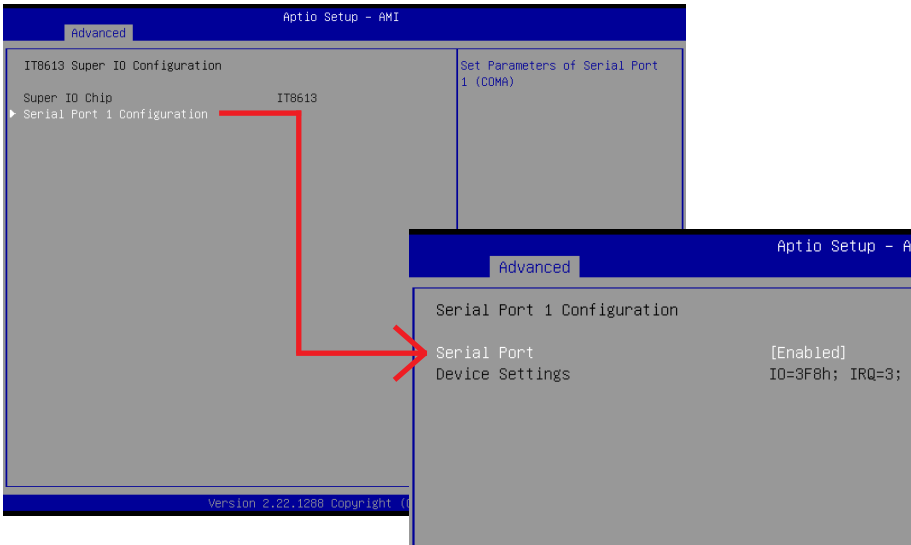
Items for SDM-1315AL

Advanced Aptio Setup - AMI		
CPU Configuration		
ID	0xB06A3	When enabled, a VMX can utilize the additional hardware capabilities provided by Vanderpool Technology.
Brand String	13th Gen Intel(R) Core(TM) i3-1315U	
VMX	Supported	
SMX/TXT	Not Supported	
Intel (VMX) Virtualization Technology	[Enabled]	++: Select Screen T1: Select Item Enter: Select +/-: Change Opt. F1: General Help
Intel(R) Speed Shift Technology	[Enabled]	
Intel(R) SpeedStep(tm)	[Enabled]	
Turbo Mode	[Enabled]	
C states	[Enabled]	

Item	Description
Intel (VMX) Virtualization Technology	Virtualization enhanced by Intel® Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple virtual systems. Enabled : Enables Intel Virtualization Technology (Default setting) Disabled : Disables Intel Virtualization Technology
Intel Trusted Execution Technology	Disabled : Disables Intel Trusted Execution Technology (Intel® TXT) (Default setting) Enabled : Enables Intel Trusted Execution Technology (Intel® TXT)

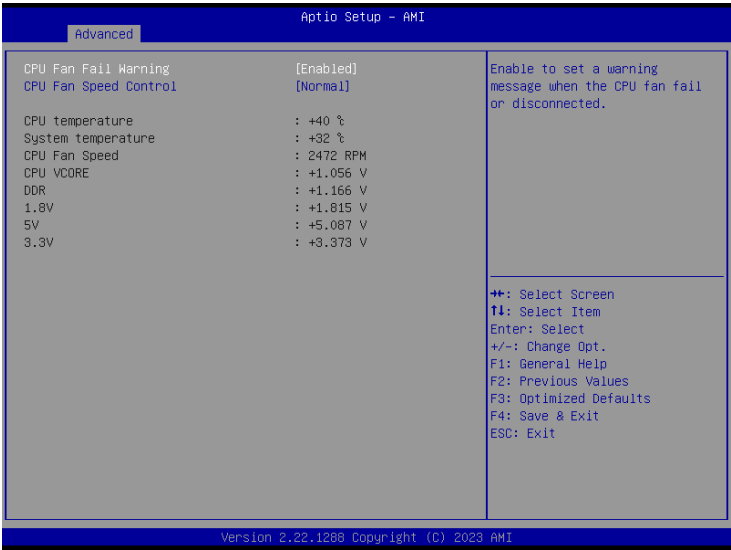
Intel(R) Speed Shift Technology	To speed up CPU frequency transition time from basic frequency to maximum frequency. Enabled : Enables Intel(R) Speed Shift Technology Interrupt control (Default setting) Disabled : Disables Intel(R) Speed Shift Technology Interrupt control
Intel(R) SpeedStep(tm)	According to Intel CPU loading, Intel SpeedStep Technology will automatically adjust the CPU voltage and core frequency to decrease heat and power consumption for power saving. Enabled : Enables Intel SpeedStep Technology (Default setting) Disabled : Disables Intel SpeedStep Technology
Turbo Mode	Enabled : Enables Turbo Mode (Default setting) Disabled : Disables Turbo Mode
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

4.3.4 IT8613 Super IO Configuration



Item	Description
Super IO Chip	Shows Super I/O chip model
Serial Port 1 Configuration	Press [Enter] to configure advanced items : 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

4.3.5 Hardware Monitor



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

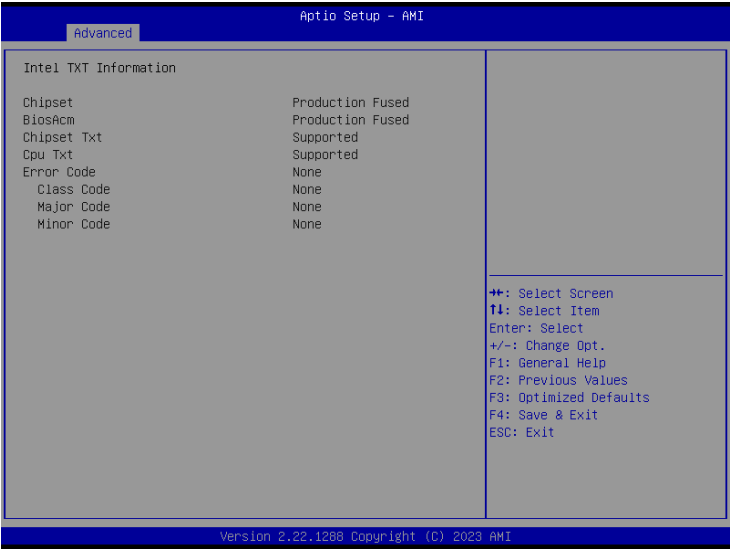
4.3.6 S5 RTC Wake Settings



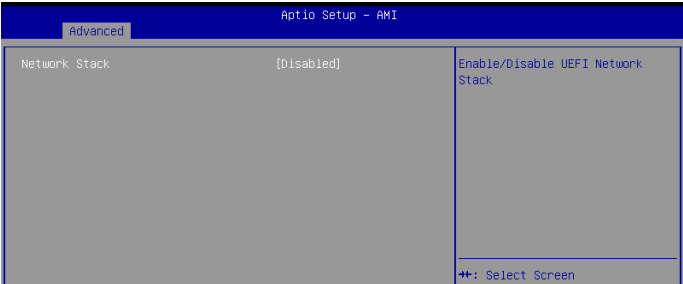
Item	Description
Wake system from S5	Enable or Disable System to wake on a specific time. Disabled : Disables system to wake on a specific time (Default setting) Fixed Time : Enables system to wake on a specific time (Format : hr : min : sec)

4.3.7 Intel TXT Information (For SDM-1345EAL, SDM-1335AL)

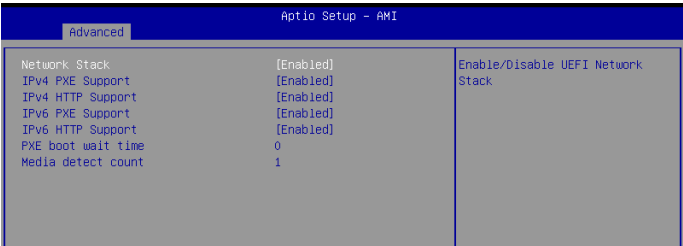
This submenu shows detailed Intel TXT informations.



4.3.8 Network Stack Configuration



When Network stack is enabled :



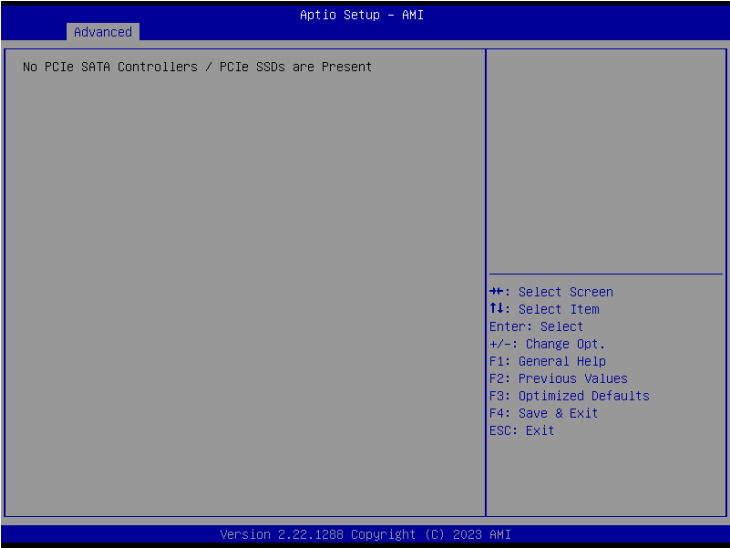
Item	Description
Network Stack	When system is power on, install LAN driver under UEFI mode Disabled : Disables UEFI Network Stack (Default setting) Enabled : Enables UEFI Network Stack
IPv4 PXE Support	When Network stack is enabled : Disabled : Disables IPv4 PXE Support Enabled : Enables IPv4 PXE Support
IPv4 HTTP Support	When Network stack is enabled : Disabled : Disables IPv4 HTTP Support Enabled : Enables IPv4 HTTP Support
IPv6 PXE Support	When Network stack is enabled : Disabled : Disables IPv6 PXE Support Enabled : Enables IPv6 PXE Support
IPv6 HTTP Support	When Network stack is enabled : Disabled : Disables IPv6 HTTP Support Enabled : Enables IPv6 HTTP Support
PXE boot wait time	Wait time in seconds, or use ESC key to abort the PXE boot.
Media detect count	Number of times the presence of media will be checked.

4.3.9 NVMe Configuration

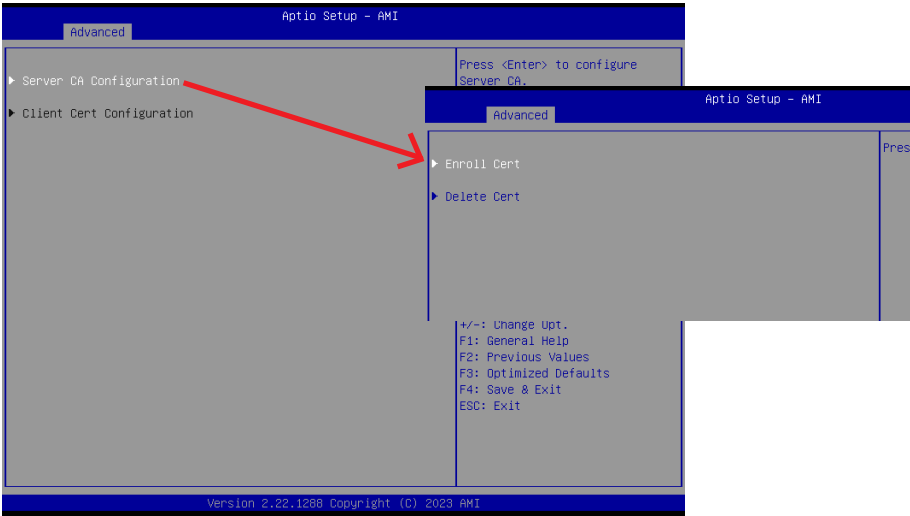
NVMe Configuration shows information when your M.2 NVMe PCIe SSD is installed.



4.3.10 Offboard SATA Controller Configuration



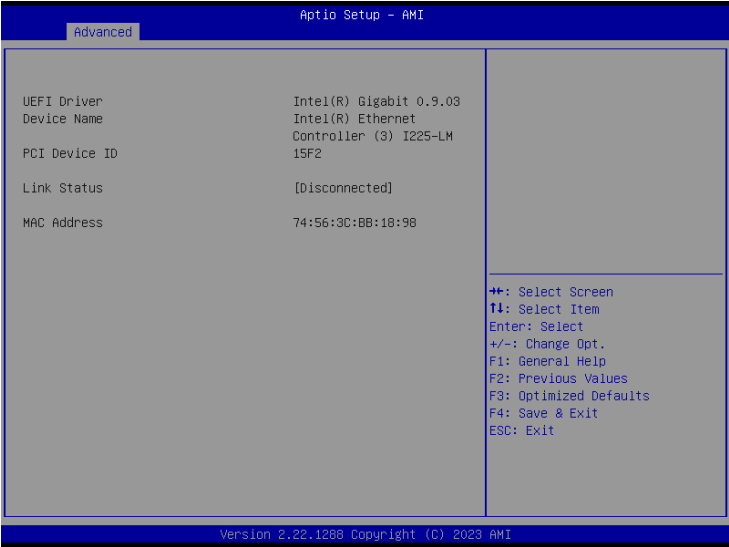
4.3.11 Tls Auth Configuration



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

4.3.12 Intel(R) Ethernet Controller (3) I225-LM - 74:56:3C:BB:18:98 (MAC address may varied based on different motherboard)

Shows Intel Ethernet controller information



4.4 Chipset



Item	Description
VT-d	Enabled : Enables VT-d function (Default setting) Disabled : Disables VT-d function
DVMT Pre-Allocated	Use DVMT Pre-Allocated to set the amount of system memory which is installed to the integrated graphics processor Option items : 32M , 64M, 128M, 256M (Default setting)
Onboard LAN	Enable/Disable onboard LAN controller Enabled : Enables onboard LAN controller (Default setting) Disabled : Disables onboard LAN controller
Watchdog Timer	Enable/Disable Watchdog Timer function Enabled : Enables Watchdog Timer function Disabled : Disabled Watchdog Timer function (Default setting)
I2C0 Controller	Enable/Disable I2C0 controller function Enabled : Enables I2C0 controller function (Default setting)
I2C1 Controller	Enable/Disable I2C1 controller function Enabled : Enables I2C1 controller function Disabled : Disables I2C1 controller function (Default setting)
SDM Display Maximum Data Rate	Select SDM Display Maximum Data Rate Options : Default Gbps , Lower Gbps (Default setting)
BIOS Lock	Enable/Disable BIOS Lock function Enabled : Enables BIOS Lock function (Default setting) Disabled : Disabled BIOS Lock funtion

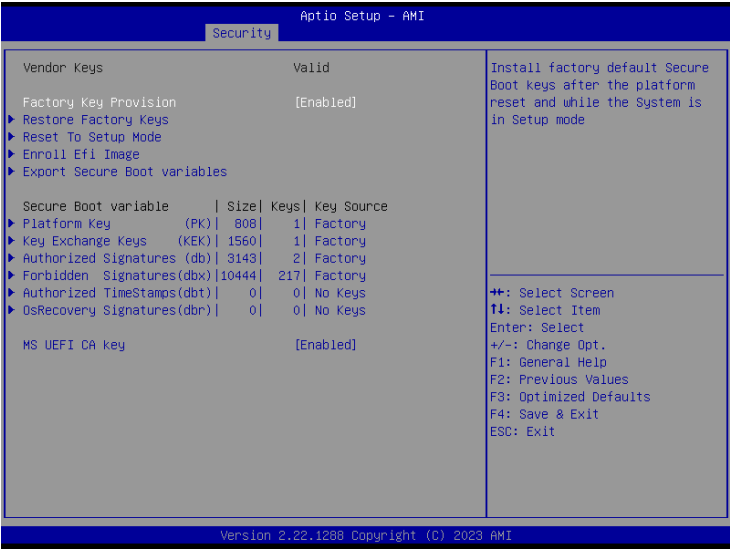
4.5 Security



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



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

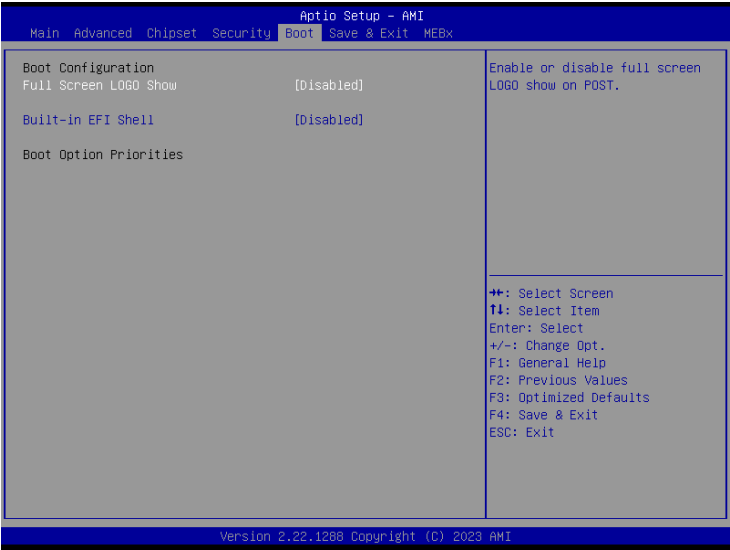


Item	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in Setup mode Enabled : Enables Factory Key Provision (Default setting) Disabled : Disables Factory Key Provision
Restore Factory Keys	To restore factory settings Yes : Agree to restore factory settings No : Cancel to restore factory settings
Reset To Setup Mode	Yes : Agree to setup mode No : Cancel to setup mode
Enroll Efi Image	Allow the image to run in Secure Boot mode
Export Secure Boot variables	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device

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

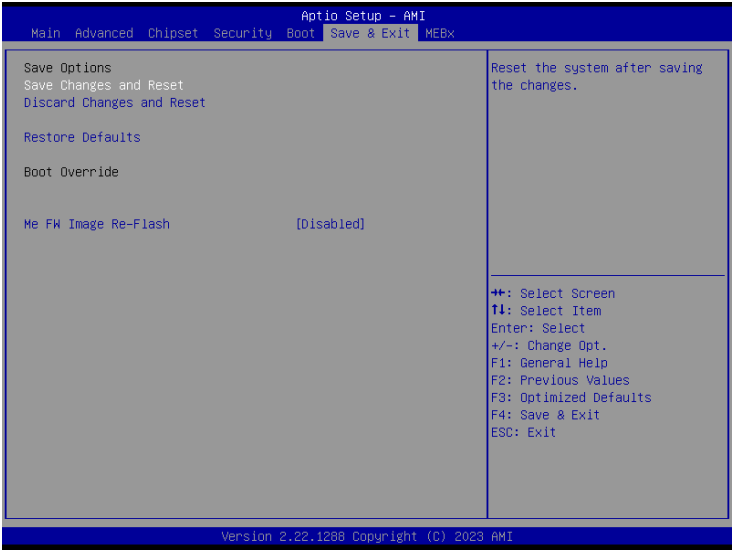
4.6 Boot

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



Item	Description
Full Screen LOGO Show	Enable/Disable full screen LOGO show on POST screen Enabled : Enables Full screen LOGO Show on POST screen Disabled : Disables Full screen LOGO Show on POST screen (Default setting)
Built-in EFI Shell	Enable/Disable Built-in EFI Shell Enabled : Enables Built-in EFI Shell Disabled : Disables Built-in EFI Shell (Default setting)
Boot Option Priorities	Choose/set the boot priority

4.7 Save & Exit



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