



NanoCOM-MTU

COM Express Module

User's Manual 1st Ed

Copyright Notice

This document is copyrighted, 2025. 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, AAEON assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.

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

Acknowledgements

All other product names or trademarks are properties of their respective owners. No ownership is implied or assumed for products, names or trademarks not herein listed by the publisher of this document.

- Microsoft® Windows® is a registered trademark of Microsoft Corp.
- Intel® is a registered trademark of Intel Corporation
- Intel® Core™ Ultra and Intel® Arc™ 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.
- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Ubuntu and Canonical are registered trademarks of Canonical Ltd.

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
● NanoCOM-MTU		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 AAEON.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.

China RoHS Requirements (CN)

产品中有毒有害物质或元素名称及含量

AAEON 主板/子板/背板

QQ4-381 Rev.A2

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	×	○	○	○	○	○
本表格依据 SJ/T 11364 的规定编制。 ○：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GB/T 26572标准规定的限量要求以下。 ×：表示该有害物质的某一均质材料超出了GB/T 26572的限量要求，然而该部件仍符合欧盟指令2011/65/EU 的规范。 环保使用期限(EFUP (Environmental Friendly Use Period))：10年 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)

Name and content of hazardous substances in product

AAEON Main Board/Daughter Board/Backplane

QO4-381 Rev.A2

Part Name	Hazardous Substances					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
PCB Assemblies	×	○	○	○	○	○
Connector and Cable	×	○	○	○	○	○
The table is prepared in accordance with the provisions of SJ/T 11364. ○: Indicates that said hazardous substance contained in all of the homogenous materials for this product is below the limit requirement of GB/T 26572. ×: Indicates that said hazardous substance contained in at least one of the homogenous materials used for this part is above the limit requirement of GB/T 26572. But this product still be compliance with 2011/65/EU Directive (allowed with 2011/65/EU Annex III of RoHS exemption with number 6(c),7(a),7(c)-1). EFUP (Environment Friendly Use Period) value: 10 years Notes: This product defined period of use is under normal condition.						

Table of Contents

Chapter 1 - Product Specifications.....	1
1.1 Specifications	2
Chapter 2 – Hardware Information	5
2.1 Dimensions, Jumpers and Connectors	6
2.2 List of Jumpers and Connectors.....	8
2.2.1 COM Express Type 10 Connector (JCOM1)	8
2.2.2 MIPI (JMIP1).....	15
2.2.3 MIPI (JMIP2).....	16
2.3 Thermal Solution Installation.....	18
2.3.1 Fan Assembly	18
2.3.2 Heatspreader Assembly	19
Chapter 3 - AMI BIOS Setup	20
3.1 System Test and Initialization	21
3.2 AMI BIOS Setup	22
3.3 Setup Submenu: Main.....	23
3.4 Setup Submenu: Advanced.....	24
3.4.1 Video Bios Table Configuration	25
3.4.1.1 Boot Display Priority.....	26
3.4.1.2 Display Configuration	27
3.4.1.3 DDIA Configuration.....	28
3.4.2 CPU Configuration.....	29
3.4.2.1 Efficient-core Information	30
3.4.2.2 Performance-core Information	31
3.4.3 Memory Configuration	32
3.4.4 On-Module H/W Monitor	33
3.4.5 PCH-FW Configuration	35

3.4.6	On-Module Configuration	36
3.4.7	Power Management	37
3.4.8	AAEON BIOS Robot.....	38
3.4.8.1	Device Detecting Configuration.....	40
3.4.8.2	Device # Detecting Configuration.....	42
3.4.9	Smart Battery Configuration.....	49
3.5	Setup Submenu: System I/O.....	50
3.5.1	PCI Express Configuration.....	51
3.5.2	Storage Configuration.....	52
3.5.2.1	NVMe Configuration.....	53
3.5.2.2	PCIe SSD	54
3.5.2.3	SATA Configuration	55
3.5.2.3	VMD Setup Menu.....	56
3.5.3	HD Audio Configuration.....	57
3.5.4	Digital IO Port Configuration	58
3.5.5	Legacy Logical Devices Configuration.....	59
3.5.5.1	Serial Port 1 Configuration	60
3.5.5.2	Serial Port 2 Configuration.....	61
3.5.6	Serial Port Console Configuration	62
3.5.6.1	COM1 Console Redirection Settings.....	63
3.5.6.2	COM2 Console Redirection Settings	66
3.5.6.3	Console Redirection Settings	69
3.6	Setup Submenu: Security.....	71
3.6.1	Trusted Computing	72
3.6.2	Secure Boot	74
3.6.2.1	Expert Key Management.....	75
3.7	Setup Submenu: Boot	77
3.8	Setup Submenu: Save & Exit.....	78

Chapter 4 – Drivers Installation..... 79

 4.1 Driver Download and Installation..... 80

Appendix A - I/O Information..... 86

 A.1 I/O Address Map 87

 A.2 Memory Address Map 88

 A.3 Large Memory Address Map 89

 A.4 IRQ Mapping Chart..... 90

Chapter 1

Product Specifications

1.1 Specifications

System

Form Factor	COM Express Mini Size, Type 10
CPU	Intel® Core™ Ultra Processors (Series 1): Intel® Core™ Ultra 7 Processor 155H (16C/22T, up to 4.8 GHz, 28W) Intel® Core™ Ultra 5 Processor 125H (14C/18T, up to 4.5 GHz, 28W)
Chipset	Integrated with Intel ® SoC
Memory	Onboard LPDDR5(X) 6400MHz, up to 32GB
Onboard Storage	NVMe, up to 256GB
BIOS	AMI UEFI
Wake on LAN	Yes
Watchdog Timer	255 Levels
Dimension (L x W)	3.31" x 2.17" (84mm x 55mm)
Security	fTPM/dTPM (Default)

Power

Power Requirement	+9V ~ 19V and +5VSB (± 10%) for ATX, +9V ~ 19V for AT Note: +8.5V will trigger UVP & +20V will trigger OVP.
Power Type	AT/ATX, switch by BIOS
Power Consumption (Typical)	Intel® Core™ Ultra 7 Processor 155H, 2.06A @+19V

Display

Graphics Controller	Intel® Arc™ Graphics
Video Output	Dual Display: DDI x 1, up to 3840 x 2160 eDP x 1, up to 3840 x 2160 @60Hz

I/O

Ethernet	Intel® Ethernet Controller I226, 2.5GbE x 1
Audio	High Definition Audio Interface
USB Port	USB 2.0 x 8 USB 3.2 Gen 2 x 2
Serial Port	2-Wire UART x 2 (Tx/Rx)
HDD Interface	SATA 6Gb/s x 2
Expansion	PCIe 4.0 [x1] x 4 MIPI CSI x 2 LPC x 1
GPIO	8-bit
SMBus/I2C	I2C x 1, from EC (default) or CPU, switch by BIOS SMBus x 1, from CPU

Environmental

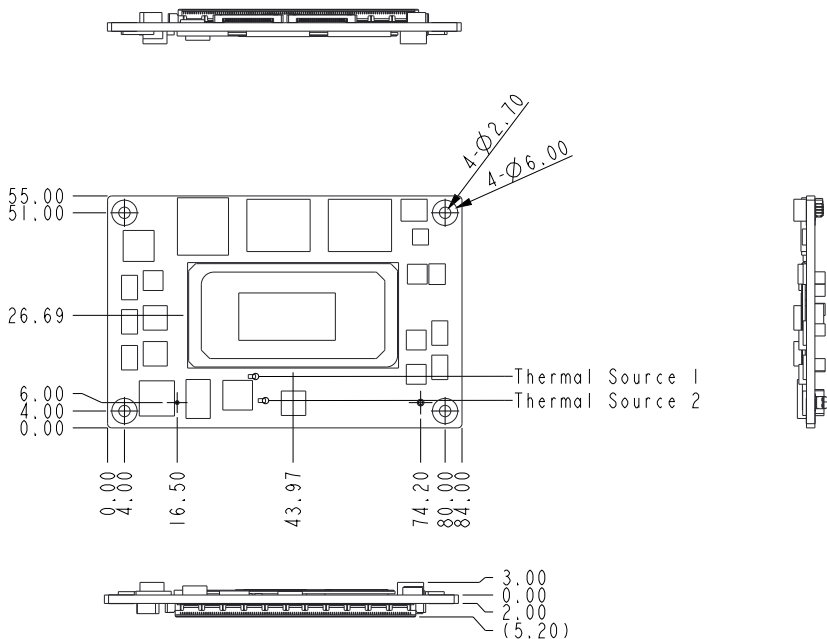
Operating Temperature	-4°F ~ 158°F (-20°C ~ 70°C)
Storage Temperature	-40°F ~ 185°F (-40°C ~ 85°C)
Operating Humidity	0% ~ 90% relative humidity, non-condensing
EMC	CE/FCC Class A
OS Support	Windows® 11 (64-bit)
	Linux Ubuntu 24.04.1/Kernel 6.8
Weight	0.15 lb. (0.07Kg)

Chapter 2

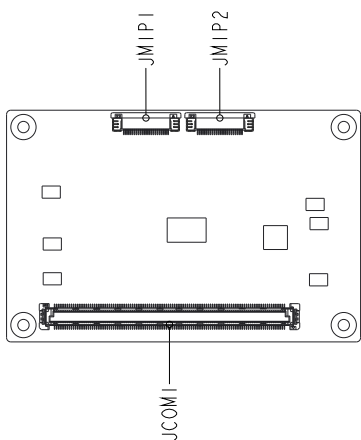
Hardware Information

2.1 Dimensions, Jumpers and Connectors

Top Side

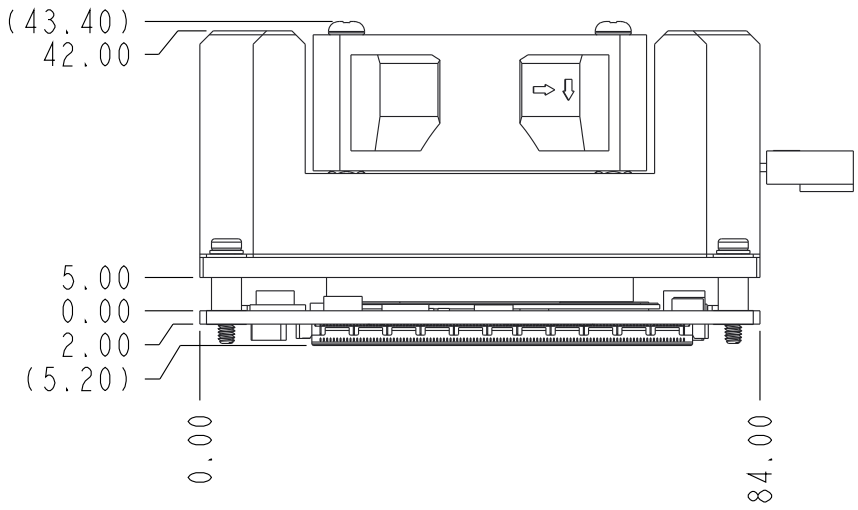


Bottom Side

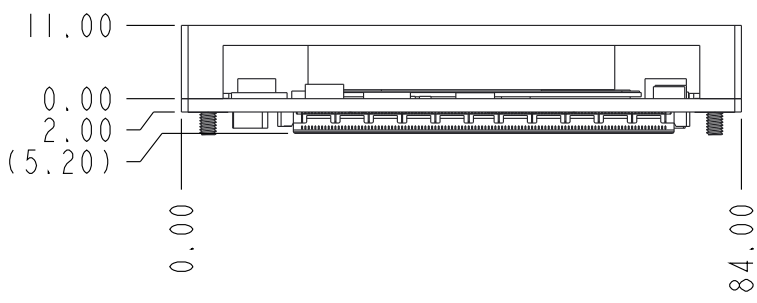


Thermal Solutions

With Active Cooler (P/N: NANOCOM-MTU-FAN01)



With Heatspreader (P/N: NANOCOM-MTU-HSP01)

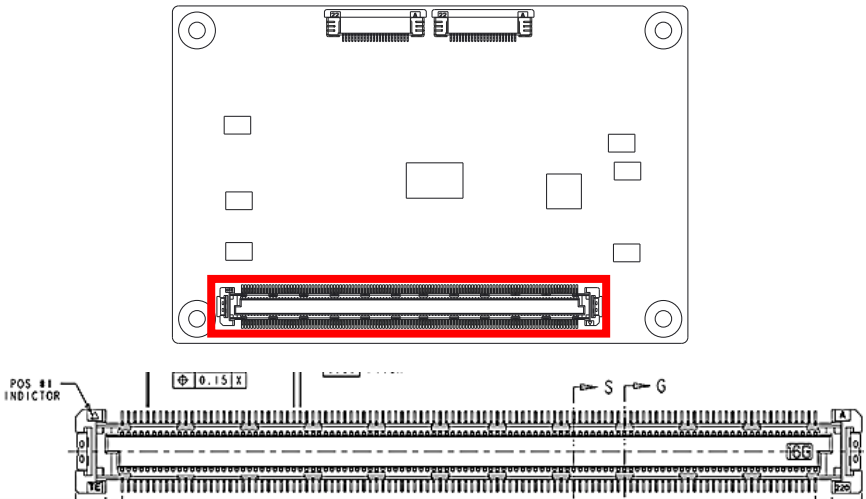


2.2 List of Jumpers and Connectors

Please refer to the table below for all of the board's jumpers that you can configure for your application

Label	Function
JCOM1	COM Express Type 10 Connector
JMIP1	MIPI
JMIP2	MIPI

2.2.1 COM Express Type 10 Connector (JCOM1)



Pin	Pin Name	Signal Type	Signal level
A1	GND(FIXED)		
A2	GBE0_MDI3-		
A3	GBE0_MDI3+		
A4	GBE0_LINK_MID#		
A5	GBE0_LINK_MAX#		
A6	GBE0_MDI2-		
A7	GBE0_MDI2+		
A8	GBE0_LINK#		
A9	GBE0_MDI1-		

Pin	Pin Name	Signal Type	Signal level
A10	GBE0_MDI1+		
A11	GND(FIXED)		
A12	GBE0_MDI0-		
A13	GBE0_MDI0+		
A14	GBE0_CTREF		
A15	SUS_S3#		
A16	SATA0_TX+		
A17	SATA0_TX-		
A18	SUS_S4#		
A19	SATA0_RX+		
A20	SATA0_RX-		
A21	GND(FIXED)		
A22	USB_SSRX0-		
A23	USB_SSRX0+		
A24	SUS_S5#		
A25	USB_SSRX1-		
A26	USB_SSRX1+		
A27	BATLOW#		
A28	(S)ATA_ACT#		
A29	HDA_SYNC		
A30	HDA_RST#		
A31	GND(FIXED)		
A32	HDA_BITCLK		
A33	HDA_SDOUT		
A34	BIOS_DIS0#		
A35	THRMTRIP#		
A36	USB6-		
A37	USB6+		
A38	USB_6_7_OC#		
A39	USB4-		
A40	USB4+		
A41	GND(FIXED)		
A42	USB2-		
A43	USB2+		
A44	USB_2_3_OC#		
A45	USB0-		
A46	USB0+		
A47	VCC_RTC		
A48	RSMRST_OUT#		

Pin	Pin Name	Signal Type	Signal level
A49	GBE0_SDP		
A50	LPC_SERIRQ		
A51	GND(FIXED)		
A52	NC		
A53	NC		
A54	GPIO		
A55	GP_SPI_CS#		
A56	GP_SPI_CK		
A57	GND		
A58	PCIE_TX3+		
A59	PCIE_TX3-		
A60	GND(FIXED)		
A61	PCIE_TX2+		
A62	PCIE_TX2-		
A63	GPIO1		
A64	PCIE_TX1+		
A65	PCIE_TX1-		
A66	GND		
A67	GPIO2		
A68	PCIE_TX0+		
A69	PCIE_TX0-		
A70	GND(FIXED)		
A71	eDP_TX2+		
A72	eDP_TX2-		
A73	eDP_TX1+		
A74	eDP_TX1-		
A75	eDP_TX0+		
A76	eDP_TX0-		
A77	eDP_VDD_EN		
A78	NC		
A79	NC		
A80	GND(FIXED)		
A81	eDP_TX3+		
A82	eDP_TX3-		
A83	eDP_AUX+		
A84	eDP_AUX-		
A85	GPIO3		
A86	NC		
A87	eDP_HPD		

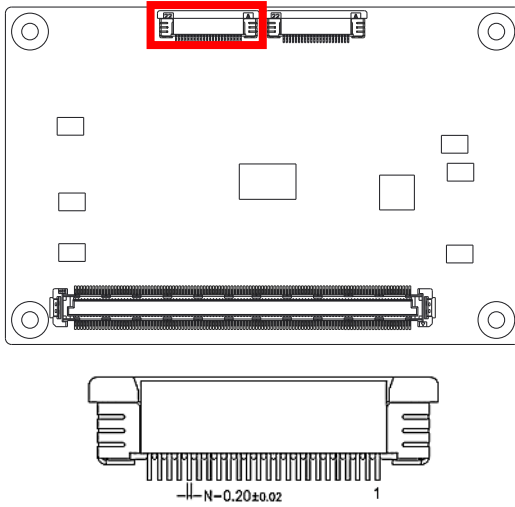
Pin	Pin Name	Signal Type	Signal level
A88	PCIE_CLK_REF+		
A89	PCIE_CLK_REF-		
A90	GND(FIXED)		
A91	SPI_POWER		
A92	SPI_MISO		
A93	GPO0		
A94	SPI_CLK		
A95	SPI_MOSI		
A96	TPM_PP		
A97	TYPE10#		
A98	SER0_TX		
A99	SER0_RX		
A100	GND(FIXED)		
A101	SER1_TX		
A102	SER1_RX		
A103	LID#		
A104	VCC_12V		
A105	VCC_12V		
A106	VCC_12V		
A107	VCC_12V		
A108	VCC_12V		
A109	VCC_12V		
A110	GND(FIXED)		
B1	GND(FIXED)		
B2	GBE0_ACT#		
B3	LPC_FRAME#		
B4	LPC_AD0		
B5	LPC_AD1		
B6	LPC_AD2		
B7	LPC_AD3		
B8	NC		
B9	NC		
B10	LPC_CLK		
B11	GND(FIXED)		
B12	PWRBTN#		
B13	SMB_CK		
B14	SMB_DAT		
B15	SMB_ALERT#		
B16	SATA1_TX+		

Pin	Pin Name	Signal Type	Signal level
B17	SATA1_TX-		
B18	SUS_STAT#		
B19	SATA1_RX+		
B20	SATA1_RX-		
B21	GND(FIXED)		
B22	USB_SSTX0-		
B23	USB_SSTX0+		
B24	PWR_OK		
B25	USB_SSTX1-		
B26	USB_SSTX1+		
B27	WDT		
B28	SNDW0_CLK		
B29	SNDW0_DAT		
B30	HDA_SDINO		
B31	GND(FIXED)		
B32	SPKR		
B33	I2C_CK		
B34	I2C_DAT		
B35	THRM#		
B36	USB7-		
B37	USB7+		
B38	USB_4_5_OC#		
B39	USB5-		
B40	USB5+		
B41	GND(FIXED)		
B42	USB3-		
B43	USB3+		
B44	USB_0_1_OC#		
B45	USB1-		
B46	USB1+		
B47	NC		
B48	NC		
B49	SYS_RESET#		
B50	CB_RESET#		
B51	GND(FIXED)		
B52	NC		
B53	NC		
B54	GPO1		
B55	GP_SPI_MISO		

Pin	Pin Name	Signal Type	Signal level
B56	GP_SPI_MOSI		
B57	GPO2		
B58	PCIE_RX3+		
B59	PCIE_RX3-		
B60	GND(FIXED)		
B61	PCIE_RX2+		
B62	PCIE_RX2-		
B63	GPO3		
B64	PCIE_RX1+		
B65	PCIE_RX1-		
B66	WAKE0#		
B67	WAKE1#		
B68	PCIE_RX0+		
B69	PCIE_RX0-		
B70	GND(FIXED)		
B71	DDIO_PAIR0+		
B72	DDIO_PAIR0-		
B73	DDIO_PAIR1+		
B74	DDIO_PAIR1-		
B75	DDIO_PAIR2+		
B76	DDIO_PAIR2-		
B77	NC		
B78	NC		
B79	eDP_BKLT_EN		
B80	GND(FIXED)		
B81	DDIO_PAIR3+		
B82	DDIO_PAIR3-		
B83	eDP_BKLT_CTRL		
B84	VCC_5V_SBY		
B85	VCC_5V_SBY		
B86	VCC_5V_SBY		
B87	VCC_5V_SBY		
B88	BIOS_DIS1#		
B89	DDIO_HPD		
B90	GND(FIXED)		
B91	NC		
B92	NC		
B93	NC		
B94	NC		

Pin	Pin Name	Signal Type	Signal level
B95	DDIO_DDC_AUX_SEL		
B96	NC		
B97	SPI_CS#		
B98	DDIO_CTRLCLK_AUX+		
B99	DDIO_CTRLDATA_AUX-		
B100	GND(FIXED)		
B101	FAN_PWMOUT		
B102	FAN_TACHIN		
B103	SLEEP#		
B104	VCC_12V		
B105	VCC_12V		
B106	VCC_12V		
B107	VCC_12V		
B108	VCC_12V		
B109	VCC_12V		
B110	GND(FIXED)		

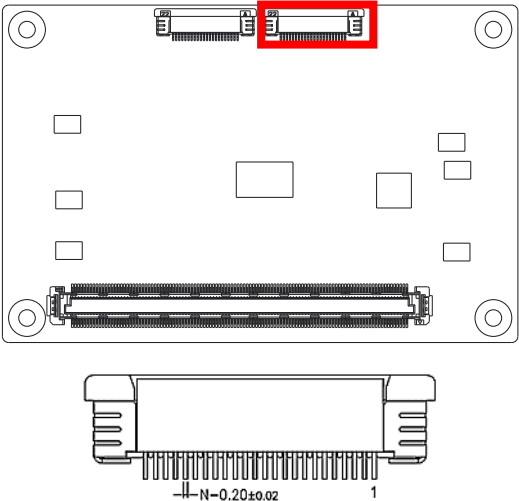
2.2.2 MIPI (JMIP1)



Pin	Pin Name	Signal Type	Signal level
1	CAM1_VCC	POWER	3.3V
2	CAM1_VCC	POWER	3.3V
3	GND		
4	CSI1_RX0+		
5	CSI1_RX0-		
6	GND		
7	CSI1_RX1+		
8	CSI1_RX1-		
9	GND		
10	CSI1_RX2+		
11	CSI1_RX2-		
12	CAM1_RST#		
13	CSI1_RX3+		
14	CSI1_RX3-		
15	GND		
16	CSI1_CK+		
17	CSI1_CK-		
18	GND		
19	I2C_CAM1_CK		
20	I2C_CAM1_DAT		

Pin	Pin Name	Signal Type	Signal level
21	CAM1_PWR#		
22	CAM1_MC		

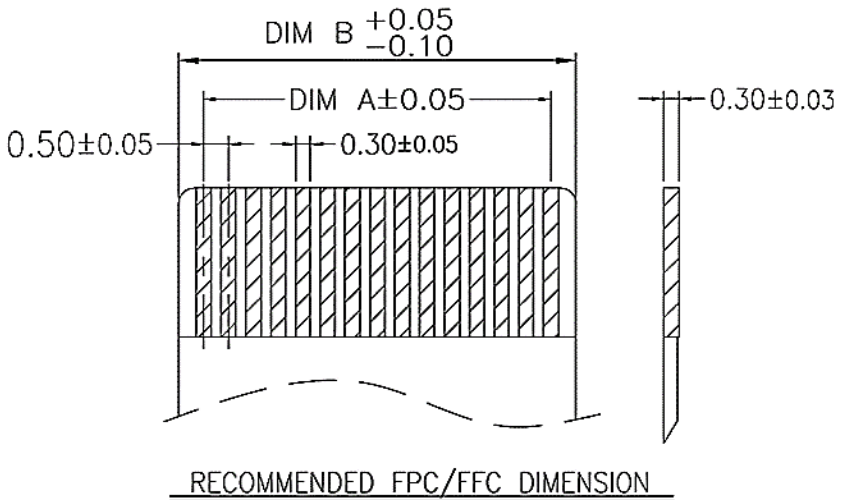
2.2.3 MIPI (JMIP2)



Pin	Pin Name	Signal Type	Signal level
1	CAM2_VCC	POWER	3.3V
2	CAM2_VCC	POWER	3.3V
3	GND		
4	CSI2_RX0+		
5	CSI2_RX0-		
6	GND		
7	CSI2_RX1+		
8	CSI2_RX1-		
9	GND		
10	CSI2_RX2+		
11	CSI2_RX2-		
12	CAM2_RST#		
13	CSI2_RX3+		
14	CSI2_RX3-		
15	GND		
16	CSI2_CK+		

Pin	Pin Name	Signal Type	Signal level
17	CSI2_CK-		
18	GND		
19	I2C_CAM2_CK		
20	I2C_CAM2_DAT		
21	CAM2_PWR#		
22	CAM2_MC		

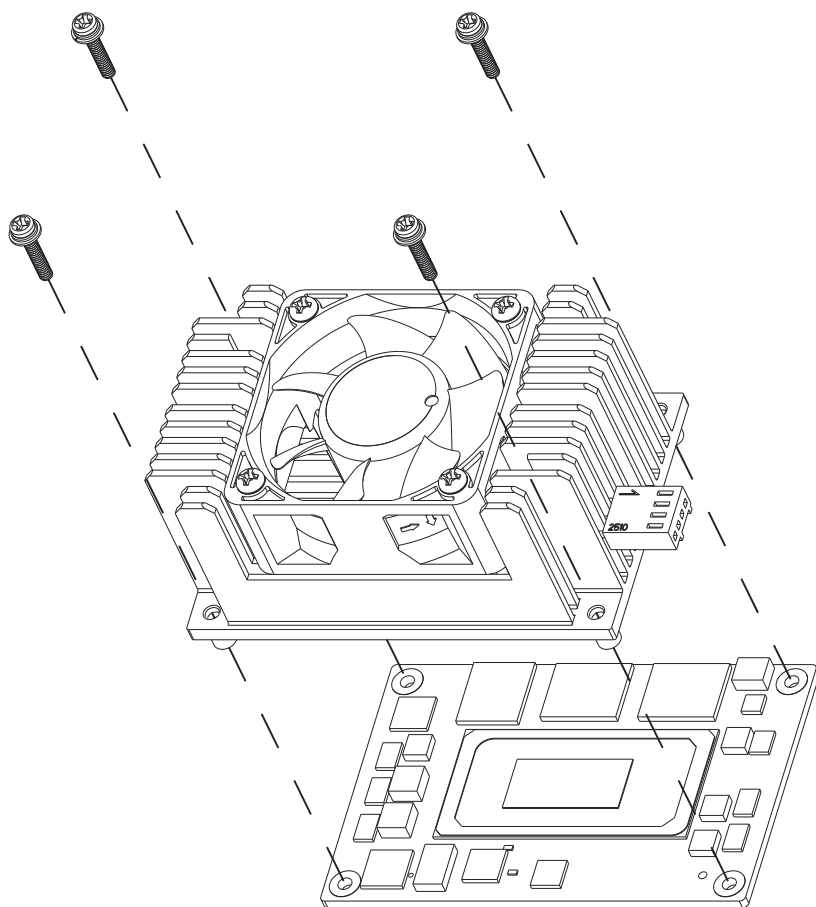
Recommended FPC/FFC cable dimensions:



2.3 Thermal Solution Installation

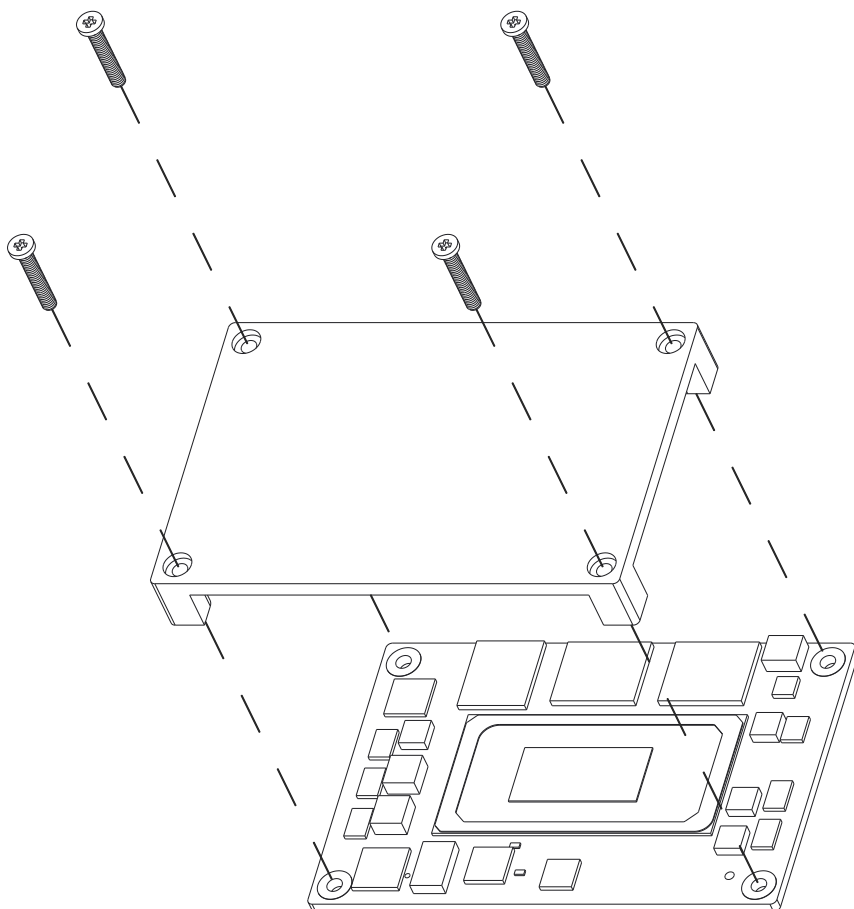
2.3.1 Fan Assembly

Tighten all four screws following the alignment shown below in order to affix the fan to the NANOCOM-MTU.



2.3.2 Heatspreader Assembly

Tighten all four screws following the alignment shown below in order to affix the heatspreader to the NANOCOM-MTU.



Chapter 3

AMI BIOS Setup

3.1 System Test and Initialization

The board uses certain routines to perform testing and initialization. If an error, fatal or non-fatal, is encountered, a few short beeps or an error message will be outputted. The board can usually continue the boot up sequence with non-fatal errors.

The system configuration verification routines check the current system configuration against the values stored in the CMOS memory. If they do not match, an error message will be outputted, in which case you will need to run the BIOS setup program to set the configuration information in memory.

There are three situations in which you will need to change the CMOS settings:

- You are starting your system for the first time
- You have changed your system's hardware
- The CMOS memory has lost power and the configuration information is erased

The system's CMOS memory uses a backup battery for data retention, which is to be replaced once emptied

3.2 AMI BIOS Setup

The AMI BIOS ROM has a pre-installed Setup program that allows users to modify basic system configurations, which is stored in the battery-backed CMOS RAM and BIOS NVRAM so that the information is retained when the power is turned off.

To enter BIOS Setup, press or <F2> immediately while your computer is powering up.

The function for each interface can be found below.

Main – Date and time can be set here. Press <Tab> to switch between date elements

Advanced – For BIOS standard features

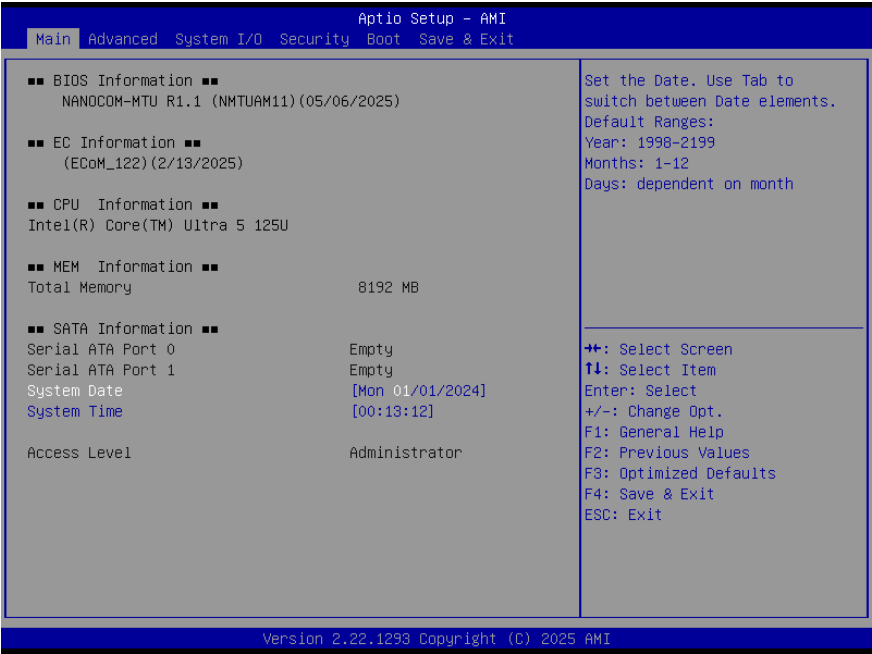
System I/O – For hosting bridge parameters

Security – The setup administrator password can be set here

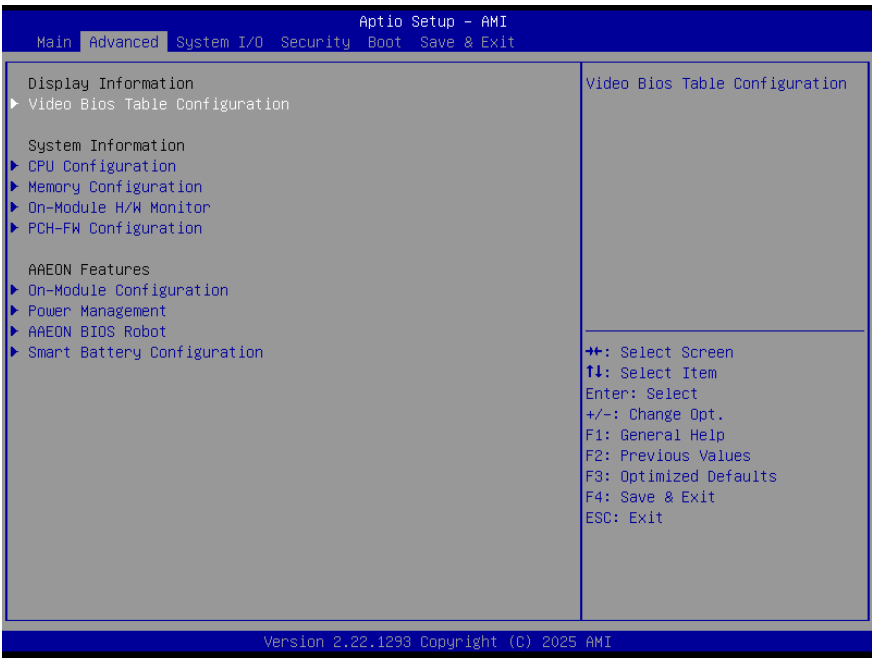
Boot – Enable/ Disable Boot Option

Save & Exit – Save your changes and exit the program

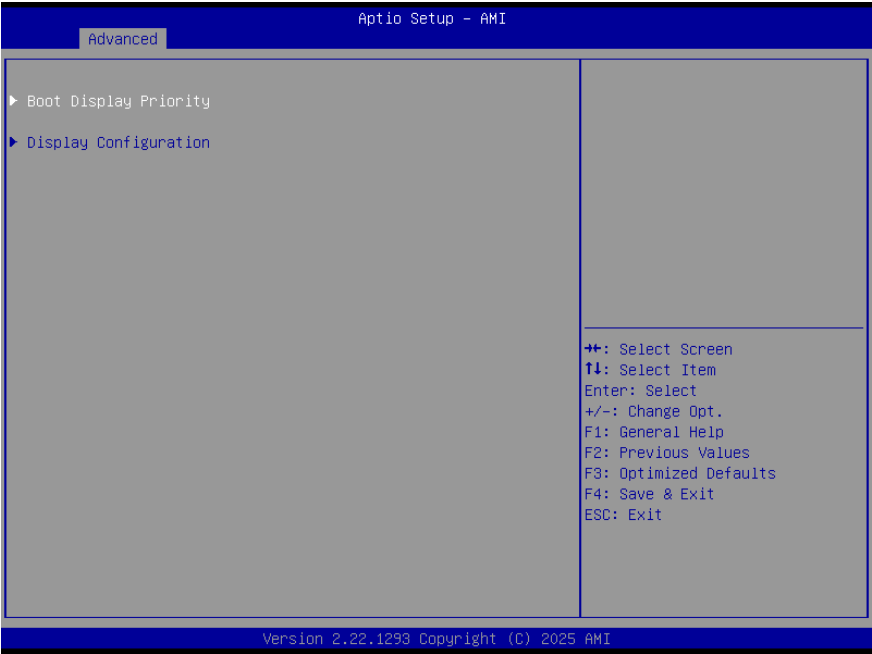
3.3 Setup Submenu: Main



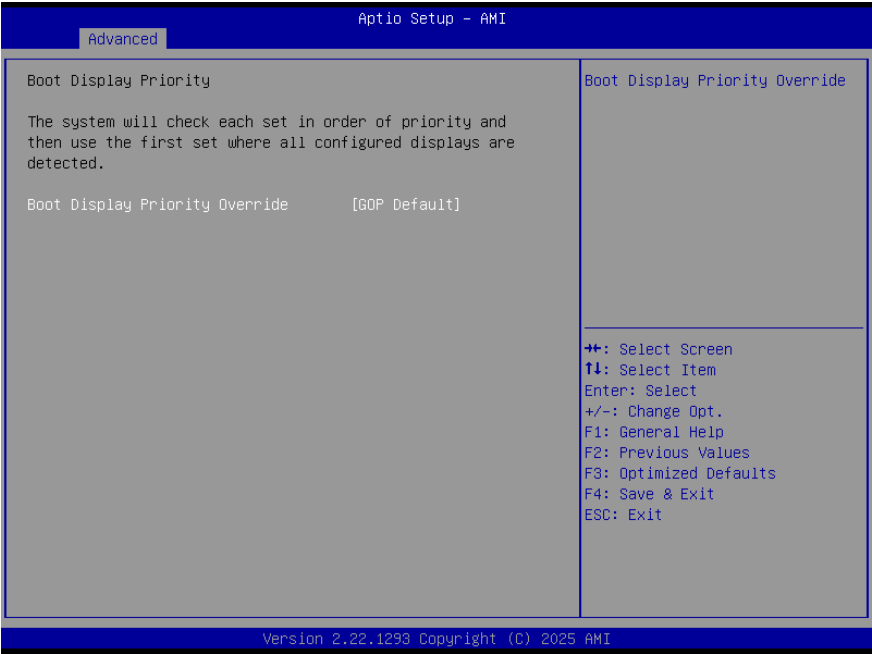
3.4 Setup Submenu: Advanced



3.4.1 Video Bios Table Configuration

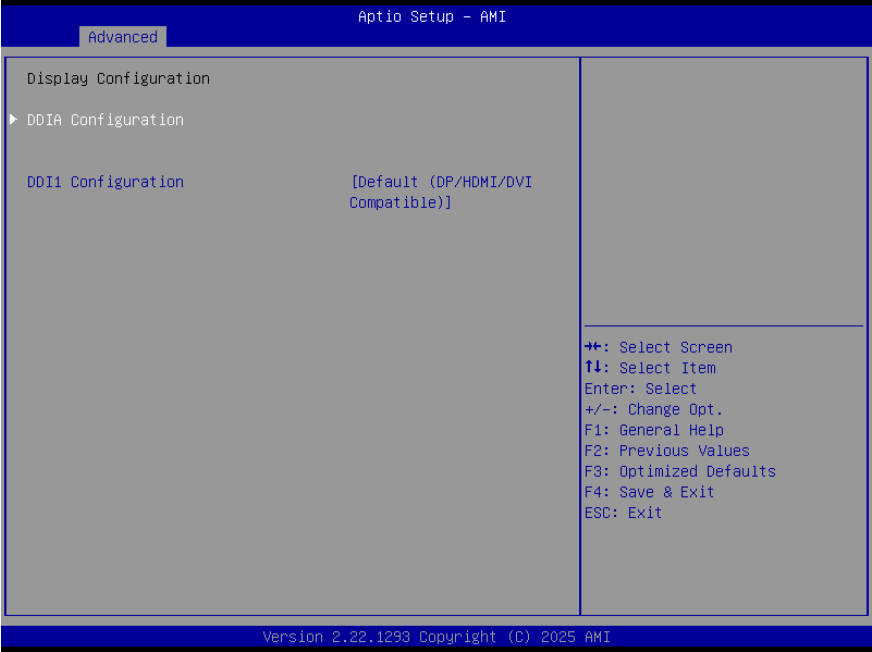


3.4.1.1 Boot Display Priority



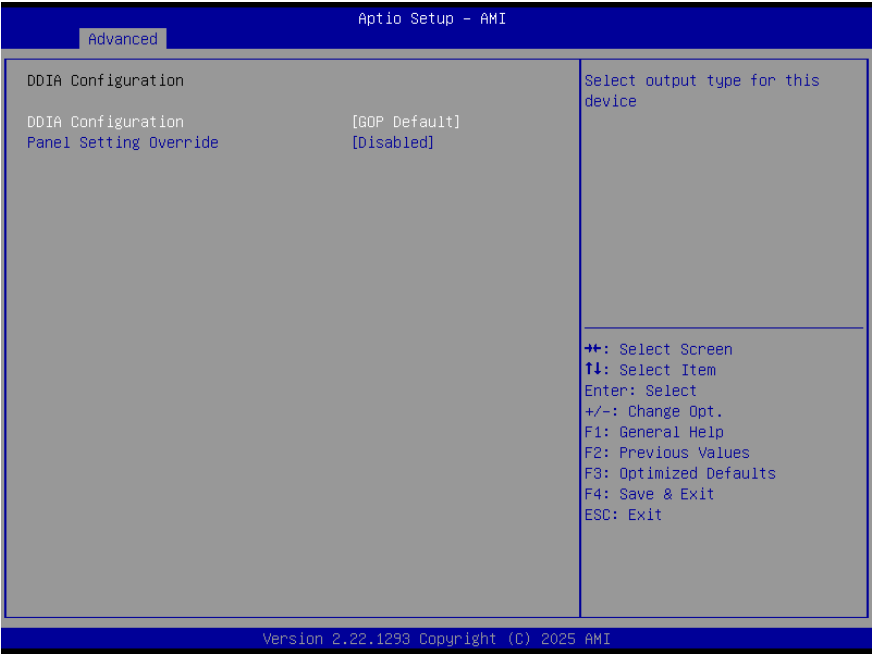
Options Summary		
Boot Display Priority	Enabled	
Override	GOP Default	Optimal Default, Failsafe Default
Boot Display Priority Override.		

3.4.1.2 Display Configuration



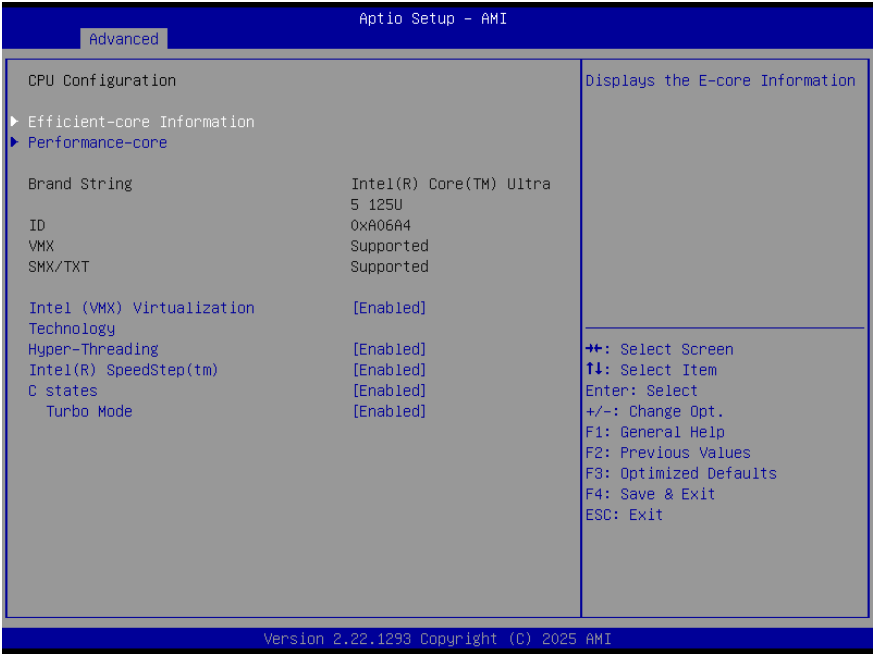
Options Summary		
DDI1 Configuration	No Device	
	DP	
	DP/HDMI/DVI Compatible	
	HDMI/DVI	
	Default (DP/HDMI/DVI Compatible)	Optimal Default, Failsafe Default
Select output type for this device.		

3.4.1.3 DDIA Configuration



Options Summary		
DDIA Configuration	No Device	
	DDIA	
	GOP Default	Optimal Default, Failsafe Default
Select output type for this device.		
Panel Setting Override	Enable	
	Disable	Optimal Default, Failsafe Default
Panel Setting Override.		

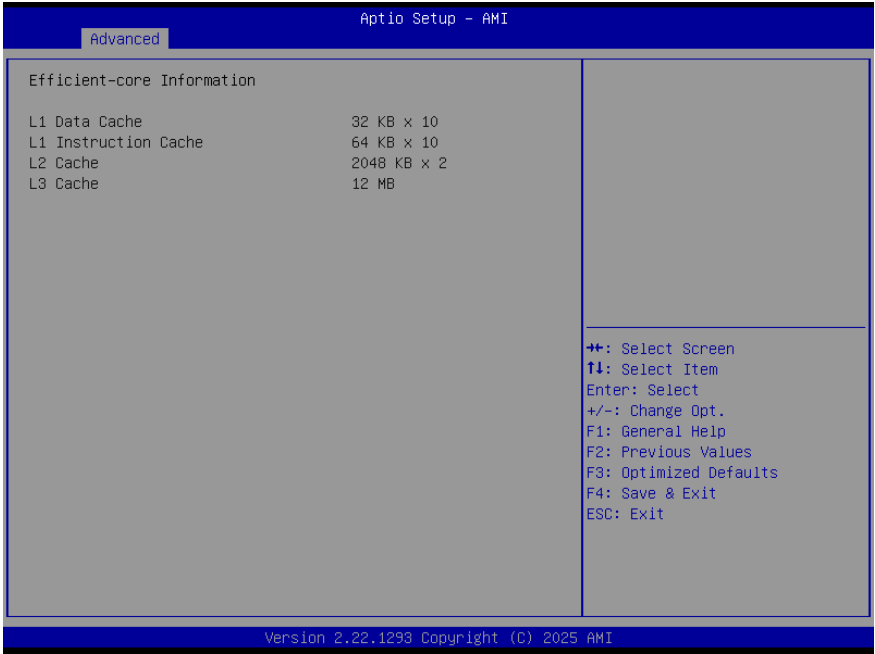
3.4.2 CPU Configuration



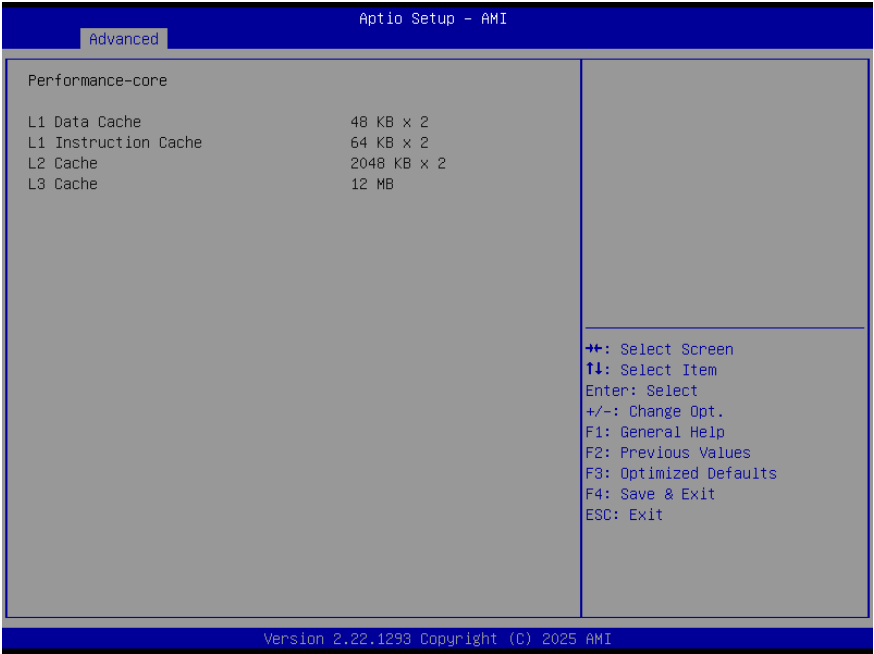
Options Summary		
Intel (VMX) Virtualization Technology	Disabled	
	Enabled	Optimal Default, Failsafe Default
When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.		
Hyper-Threading	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable Hyper-Threading Technology.		
Intel® SpeedStep™	Disabled	
	Enabled	Optimal Default, Failsafe Default
Allows more than two frequency ranges to be supported.		
C states	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable/Disable CPU Power Management.		
Allows CPU to go to C states when it's not 100% utilized.		

Options Summary		
Turbo Mode	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable/Disable processor Turbo Mode.		

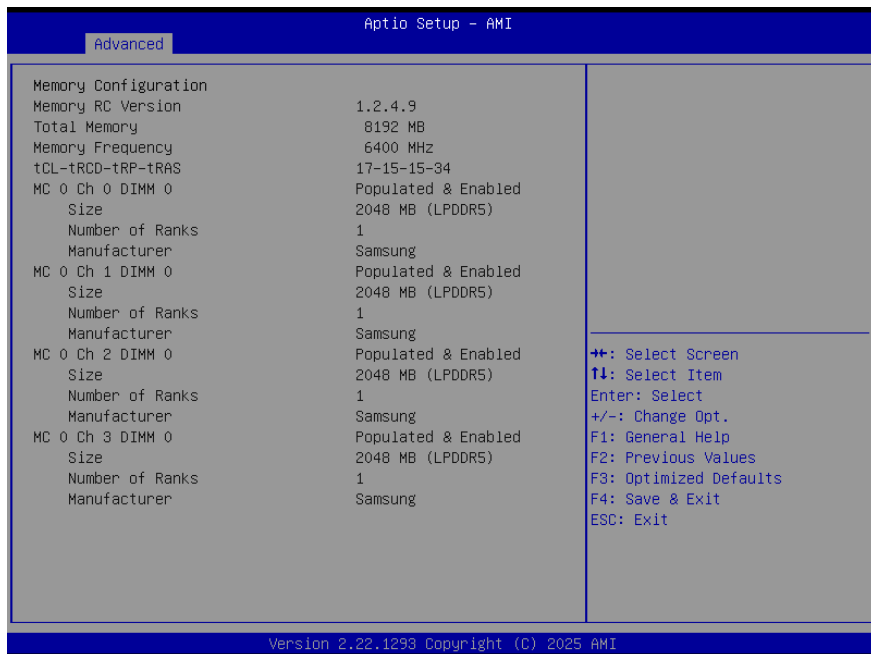
3.4.2.1 Efficient-core Information



3.4.2.2 Performance-core Information

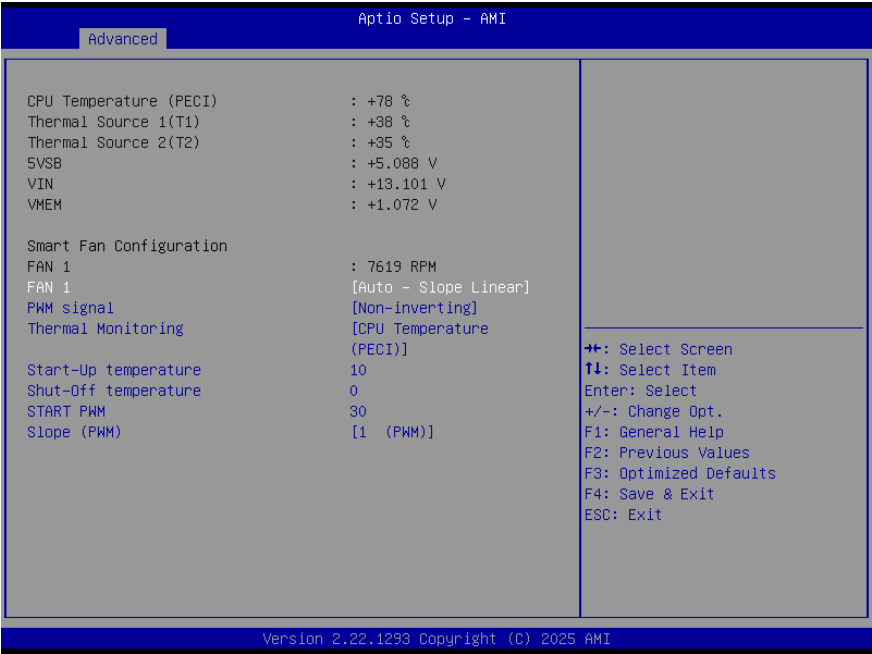


3.4.3 Memory Configuration



3.4.4 On-Module H/W Monitor

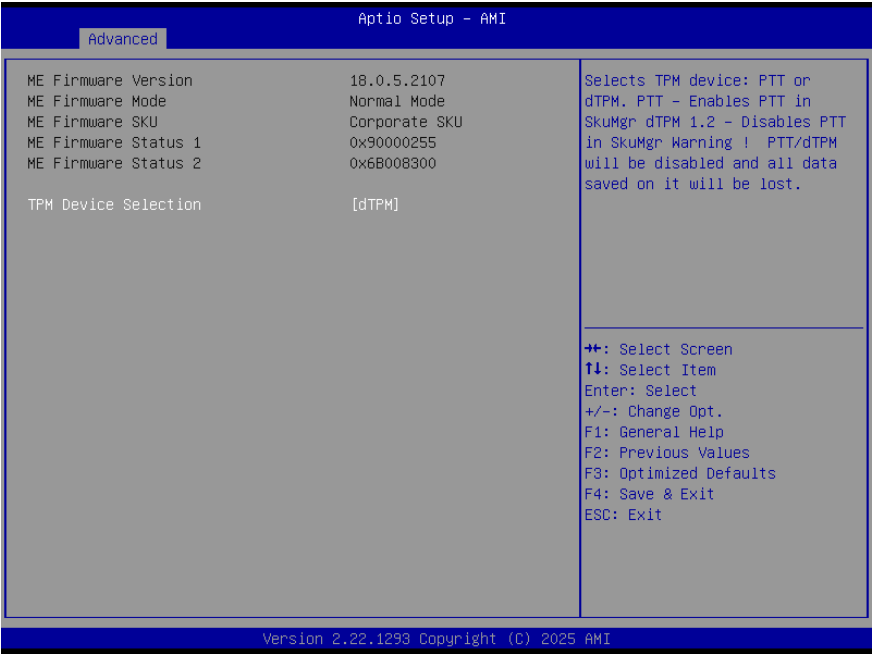
Fan Mode: Auto – Slope Linear



Options Summary		
Smart Fan	Full Mode	
	Manual Mode	
	Auto – Slope Linear	Optimal Default, Failsafe Default
Fan Mode select.		
PWM signal	Non-inverting	Optimal Default, Failsafe Default
	inverting	
Select output PWM of inverting or non-inverting signal.		
Thermal Monitoring	CPU Temperature (PECI)	Optimal Default, Failsafe Default
	Thermal Source 1 (T1)	
	Thermal Source 2 (T2)	
Monitoring thermal sensor select.		
Start-Up temperature	10	

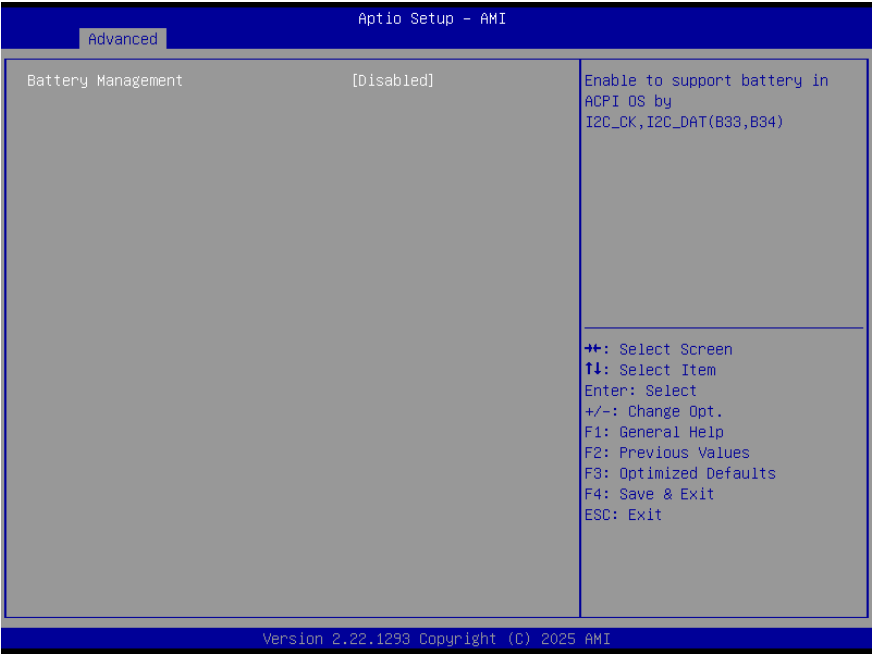
Options Summary		
PWM output when monitoring thermal sensor is exceeded. Range: 0 – 100		
Start-Off temperature	0	
PWM turns off when monitored thermal sensor is less or equal to. Range: 0- 100		
START PWM	30	
The beginning PWM output value when Start-Up temperature is triggered.		
Slope (PWM)	0 (PWM)	
	1 (PWM)	Optimal Default, Failsafe Default
	2 (PWM)	
	4 (PWM)	
	8 (PWM)	
	16 (PWM)	
	32 (PWM)	
	64 (PWM)	
When the monitored temperature is higher than the Start-Up temperature, the PWM output increases per degree.		

3.4.5 PCH-FW Configuration



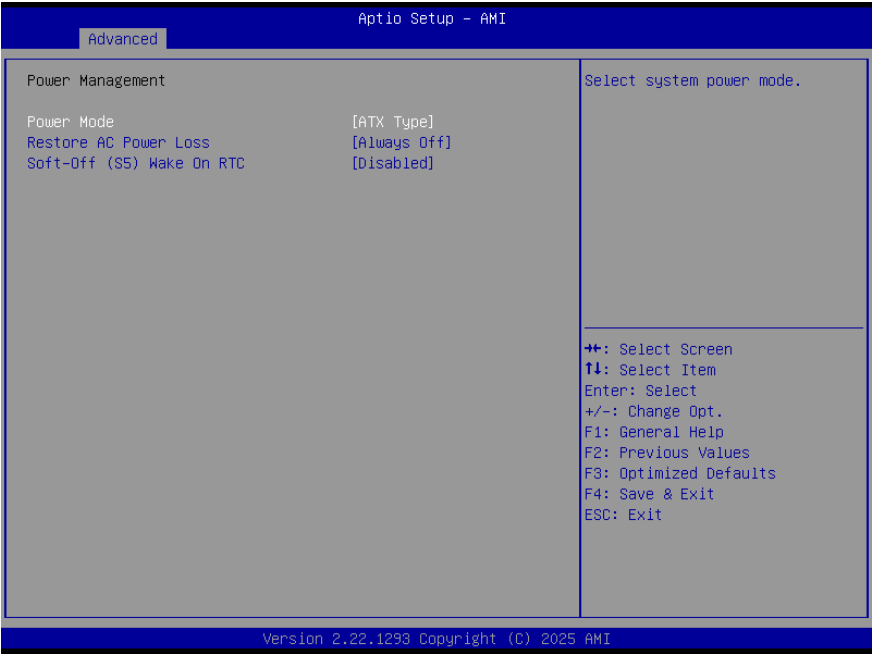
Options Summary		
TPM Device Section	dTPM	Optimal Default, Failsafe Default
	PTT	
Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr. dTPM 1.2 - Disables PTT in SkuMgr. Warning! PTT/dTPM will be disabled and all data saved on it will be lost.		

3.4.6 On-Module Configuration



Options Summary		
Battery Management	Disabled	Optimal Default, Failsafe Default
	One Battery	
Enable to support battery in ACPI OS by I2C_CK, I2C_DAT(B33, B34).		

3.4.7 Power Management



Options Summary		
Power Mode	ATX Type	Optimal Default, Failsafe Default
	AT Type	
Select system power mode.		
Restore AC Power Loss	Last State	
	Always On	
	Always Off	Optimal Default, Failsafe Default
Restore AC Power Loss.		
Soft-Off (S5) Wake On RTC	Disable	Optimal Default, Failsafe Default
	By Date	
	By Weekday	
	Bypass	
By Date: System will wake on the day with hr::min::sec specified.		
By Weekday: System will wake on the enabled weekday with hr::min::sec specified.		
Bypass: BIOS will not control RTC wake function.		

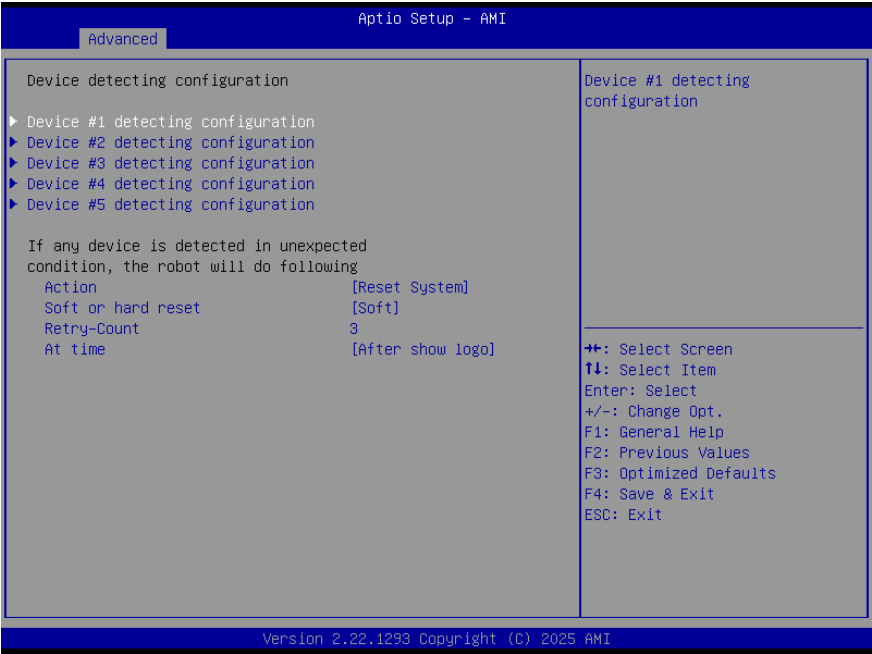
3.4.8 AAEON BIOS Robot



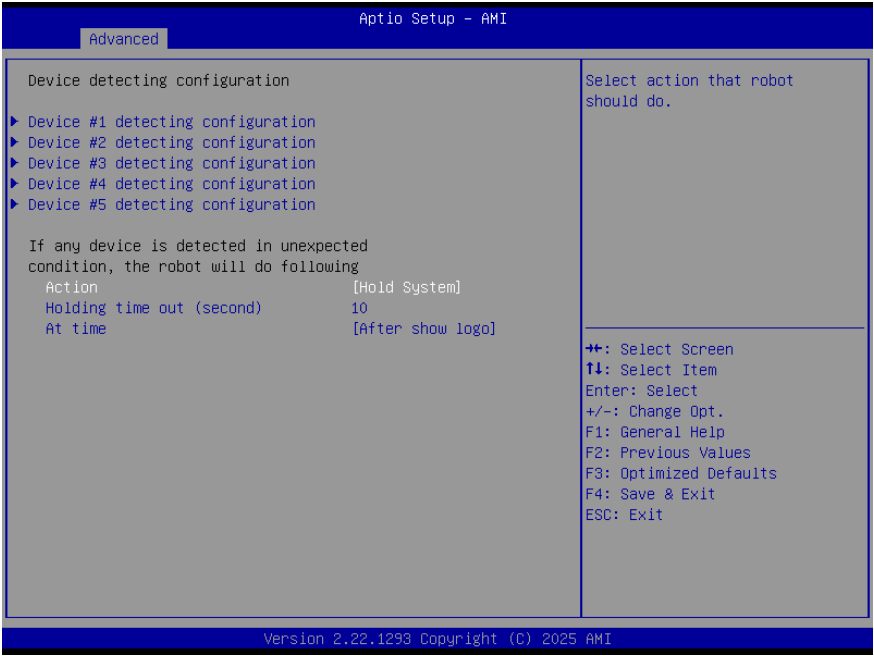
Options Summary		
Send watch dog before BIOS POST	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled - Robot set Watch Dog Timer (WDT) right after power on, before BIOS start POST process. And then Robot will clear WDT on completion of POST. WDT will reset system automatically if it is not cleared before its timer counts down to zero.		
POST Timer (second)	30	Optimal Default, Failsafe Default
Timer count set to Watch Dog Timer for POST. WARNING: Do not set to a value equal or shorter than normal POST time, otherwise system may never complete POST unless clearing BIOS settings. More than 2 x normal POST time is suggested.		

Options Summary		
Send watch dog before booting OS	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled - Robot set Watch Dog Timer (WDT) after POST completion, before BIOS transfer control to OS. WARNING: Before enabling this function, a program in OS must be responsible for clearing WDT. Also, this function should be disabled if OS is going to update itself.		
OS Timer (minute)	3	Optimal Default, Failsafe Default
Timer count set to Watch Dog Timer for OS loading.		
Delayed POST (PEI phase)	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled - Robot holds BIOS from starting POST, right after power on. This allows BIOS POST to start with stable power or start after system is physically warmed-up. Note: Robot does this before 'Sends watch dog'.		
Delayed time (second)	10	Optimal Default, Failsafe Default
Period of time for Robot to hold BIOS from POST.		
Delayed POST (DXE phase)	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled - Robot holds BIOS before POST completion. This allows BIOS POST to start with stable power or start after system is physically warmed-up. Note: Robot does this after 'Sends watch dog before BIOS POST'.		
Delayed time (second)	10	Optimal Default, Failsafe Default
Period of time for Robot to hold BIOS from POST.		
Reset system once	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled - Robot resets system for one time on each boot. This will send a soft or hard reset to onboard devices, thus puts devices to more stable state.		
Soft or hard reset	Soft reset	Optimal Default, Failsafe Default
	Hard reset	
Select reset type robot should send on each boot.		

3.4.8.1 Device Detecting Configuration

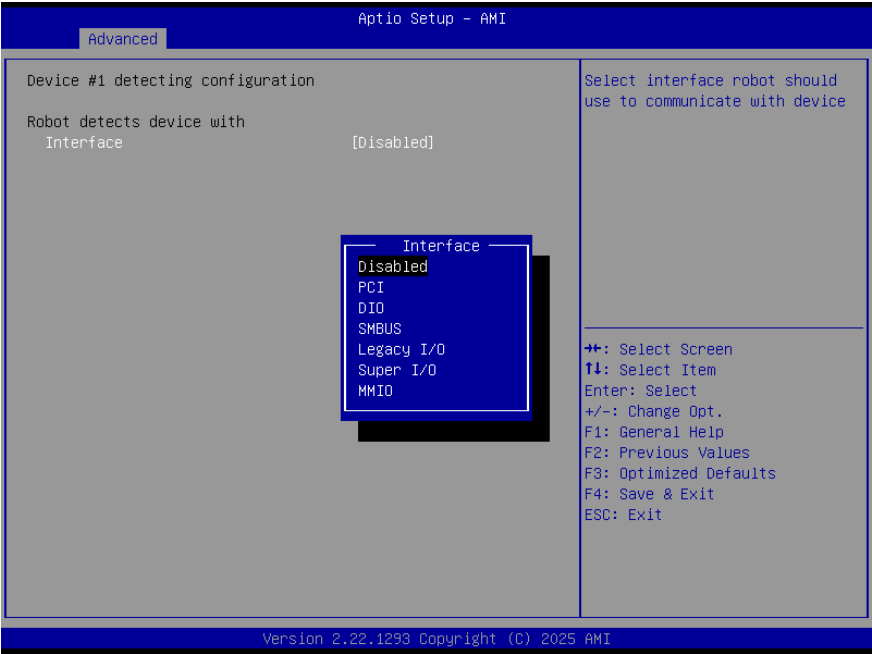


Options Summary		
Action	Reset System	Optimal Default, Failsafe Default
	Hold System	
Select action that robot should do.		
Soft or hard reset	Soft	Optimal Default, Failsafe Default
	Hard	
Select reset type robot should send on each boot.		
Retry-Count	3	Optimal Default, Failsafe Default
Fill retry counter here. Robot will reset system at most counter times, and then let system continue its POST.		
At time	After show logo	Optimal Default, Failsafe Default
	Before show logo	
Select robot action time: After show logo - Robot will do action after logo is displayed. System devices are almost ready. Before show logo - Robot will do action earlier before logo, but some devices may not be ready.		

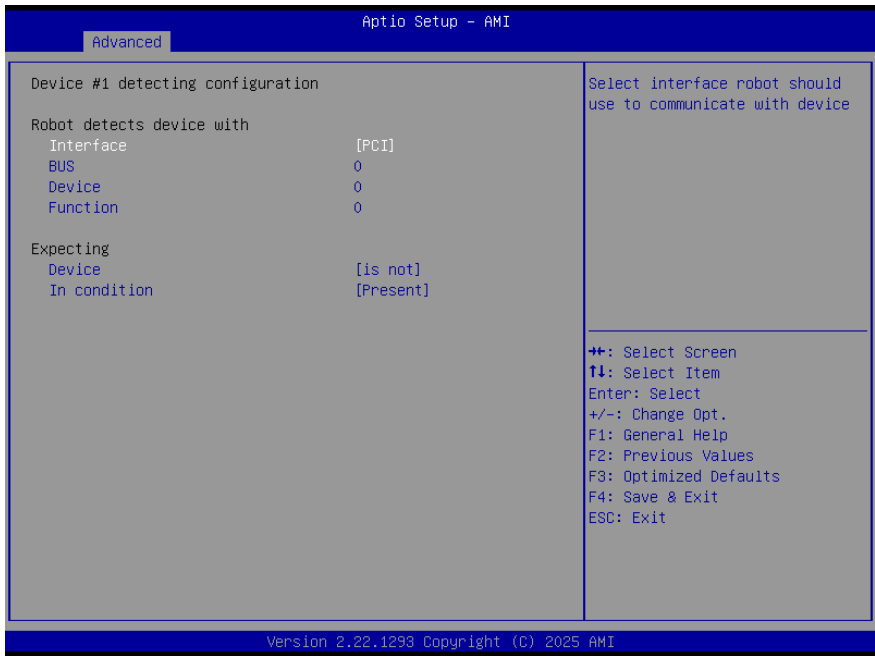


Options Summary		
Action	Reset System	
	Hold System	Optimal Default, Failsafe Default
Select action that robot should do.		
Holding time out (second)	10	Optimal Default, Failsafe Default
Fill hold time out here. Robot will hold system no longer than time-out value, and then let system continue its POST.		
At time	After show logo	Optimal Default, Failsafe Default
	Before show logo	
Select robot action time: After show logo - Robot will do action after logo is displayed. System devices are almost ready. Before show logo - Robot will do action earlier before logo, but some devices may not be ready.		

3.4.8.2 Device # Detecting Configuration



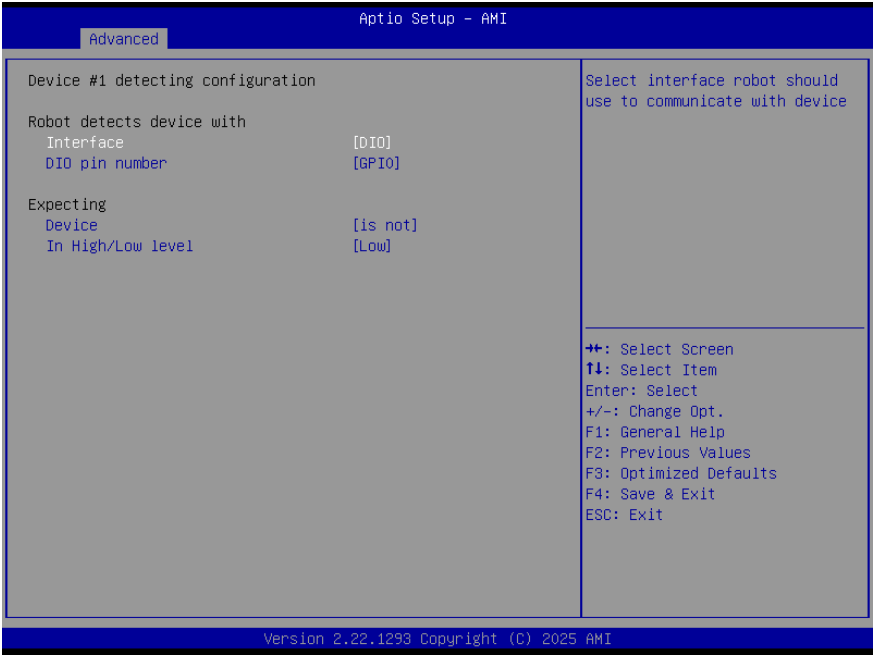
Options Summary		
Interface	Disabled	Optimal Default, Failsafe Default
	PCI	
	DIO	
	SMBUS	
	Legacy I/O	
	Super I/O	
	MMIO	
Select interface robot should use to communicate with device.		



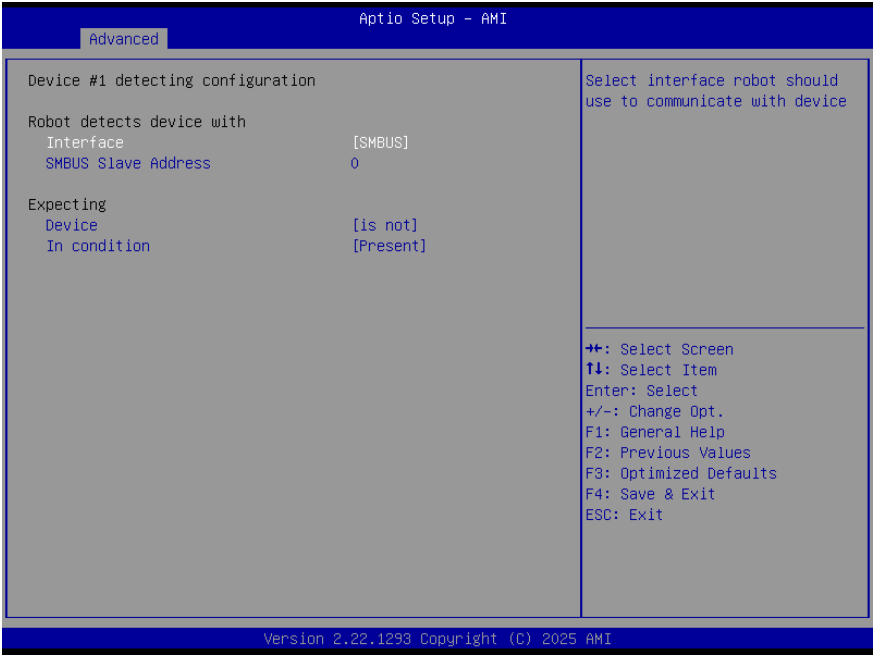
Options Summary

When interface item set to "PCI" will show below items

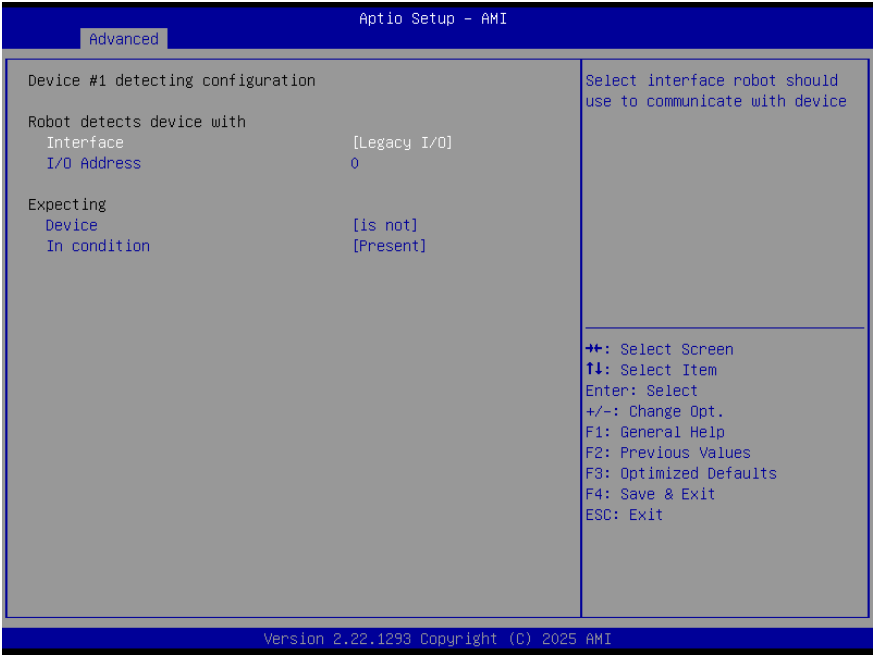
BUS	0	Optimal Default, Failsafe Default
Fill BUS number to a PCI device, in hexadecimal. Range: 0 – FF.		
Device	0	Optimal Default, Failsafe Default
Fill DEVICE number to a PCI device, in hexadecimal. Range: 0 – FF.		
Function	0	Optimal Default, Failsafe Default
Fill FUNCTION number to a PCI device, in hexadecimal. Range: 0 – FF.		
Device	is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In condition	Present	Optimal Default, Failsafe Default
	Specified register data	
Select the condition that robot should check for device. Present - device is detected. According to register - Robot read register according to configuration. Note: Device will be considered 'Present' by Robot, when data read from device is not 0xFF.		



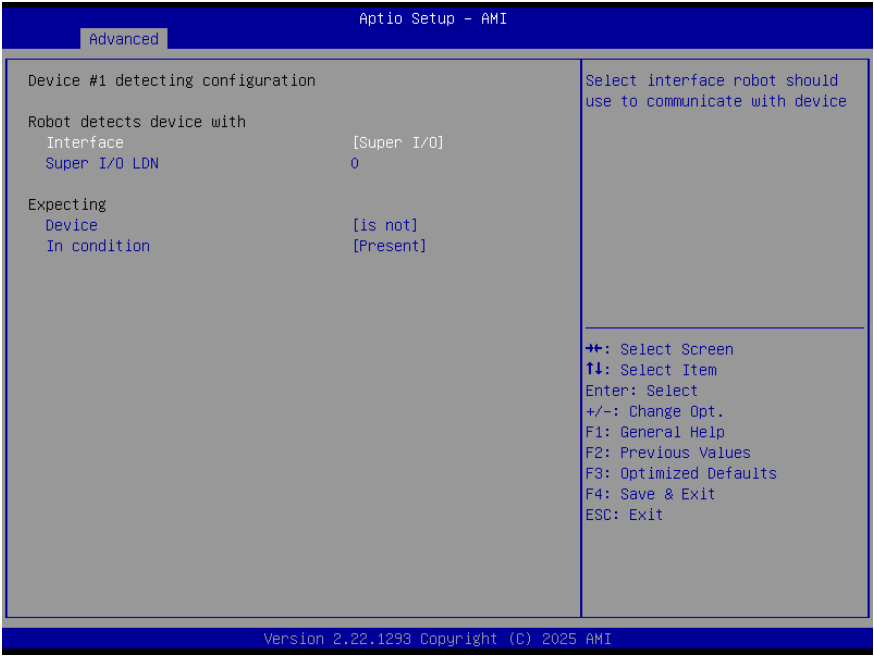
Options Summary		
When interface item set to "DIO" will show below items		
DIO pin number	GPIO 0	Optimal Default, Failsafe Default
	GPIO *	
Fill DIO pin number, 0 - DIO, 1 - DIO1, and so on. For COM express product: 0-3 - GPIO-3 4-7 - GPO0-3		
Device	is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In High/Low level	Low	Optimal Default, Failsafe Default
	High	
Select High/Low level of the DIO pin that robot should do action.		



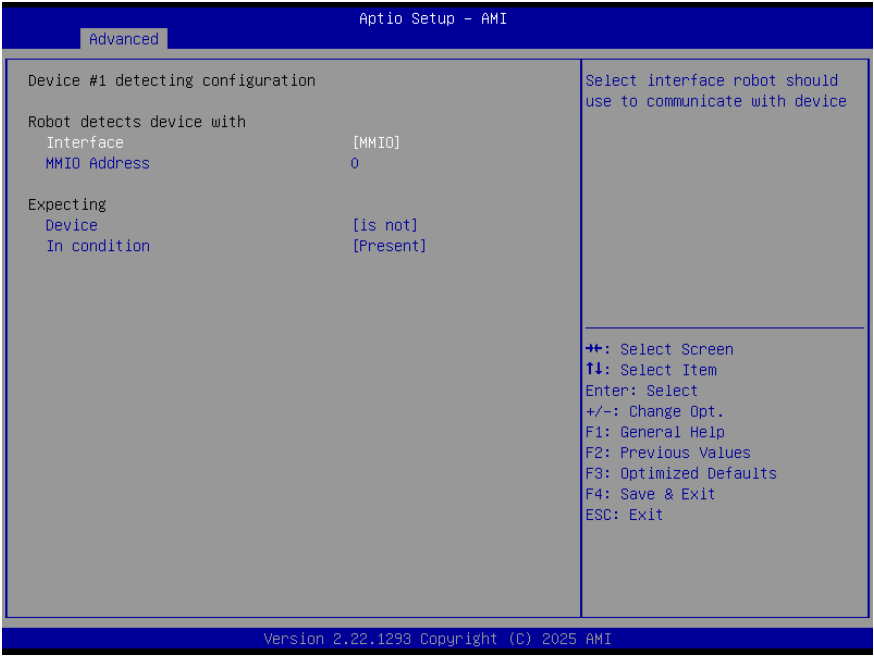
Options Summary		
When interface item set to "SMBUS" will show below items		
SMBUS Slave Address	0	Optimal Default, Failsafe Default
Fill slave address to a SMBUS device, in hexadecimal. Range: 0 - FF		
Device	is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In condition	Present	Optimal Default, Failsafe Default
	Specified register data	
Select the condition that robot should check for device. Present - device is detected According to register - Robot read register according to configuration. Note: Device will be considered 'Present' by Robot, when data read from device is not 0xFF.		



Options Summary		
When interface item set to "Legacy I/O" will show below items		
I/O Address	0	Optimal Default, Failsafe Default
Fill I/O address device is responding to. Range: 0~FFFF.		
Device	is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In condition	Present	Optimal Default, Failsafe Default
	Specified register data	
Select the condition that robot should check for device. Present - device is detected. According to register - Robot read register according to configuration. Note: Device will be considered 'Present' by Robot, when data read from device is not 0xFF.		

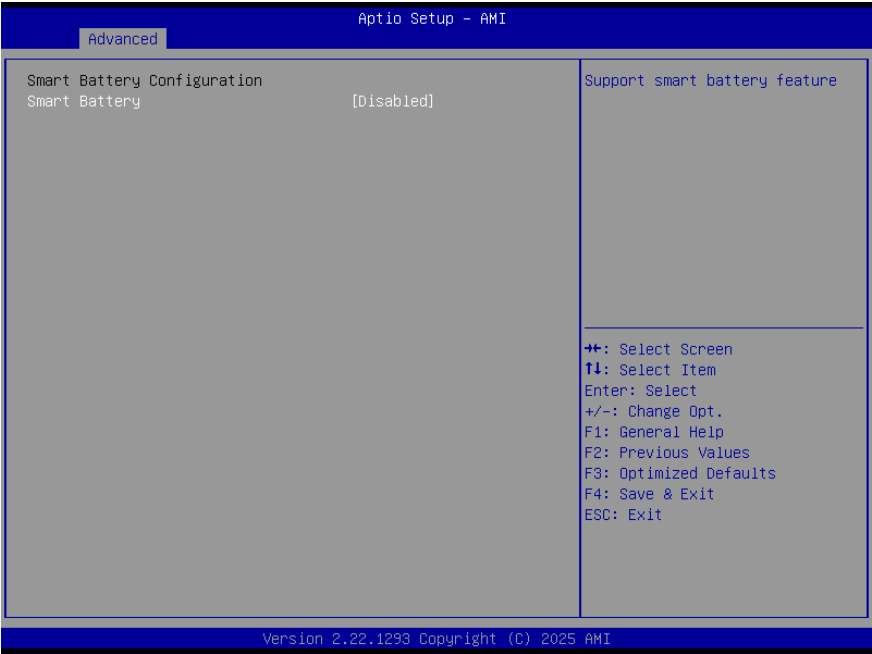


Options Summary		
When interface item set to "Super I/O" will show below items		
Super I/O LDN	0	Optimal Default, Failsafe Default
Fill LDN number to a Super I/O device. Range: 0~FF.		
Device	Is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In condition	Present	Optimal Default, Failsafe Default
	Specified register data	
Select the condition that robot should check for device. Present - device is detected. According to register - Robot read register according to configuration. Note: Device will be considered 'Present' by Robot, when data read from device is not 0xFF.		



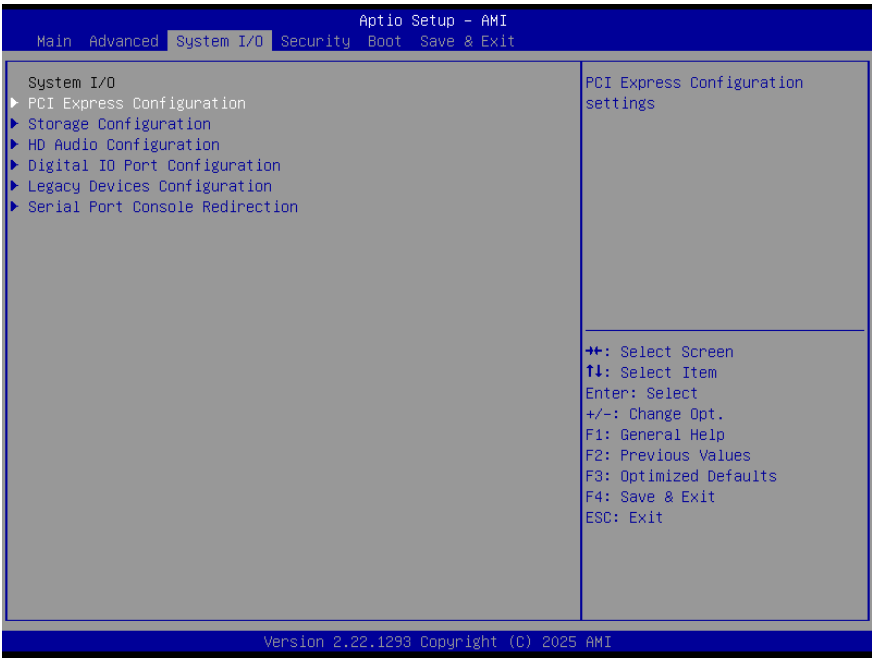
Options Summary		
When interface item set to "MMIO" will show below items		
MMIO Address	0	Optimal Default, Failsafe Default
Fill Memory Mapped I/O address device is responding to. Range: 0~FFFFFFFF.		
Device	is	
	Is not	Optimal Default, Failsafe Default
Select that robot should or should not do action if condition met.		
In condition	Present	Optimal Default, Failsafe Default
	Specified register data	
Select the condition that robot should check for device. Present - device is detected. According to register - Robot read register according to configuration. Note: Device will be considered 'Present' by Robot, when data read from device is not 0xFF.		

3.4.9 Smart Battery Configuration

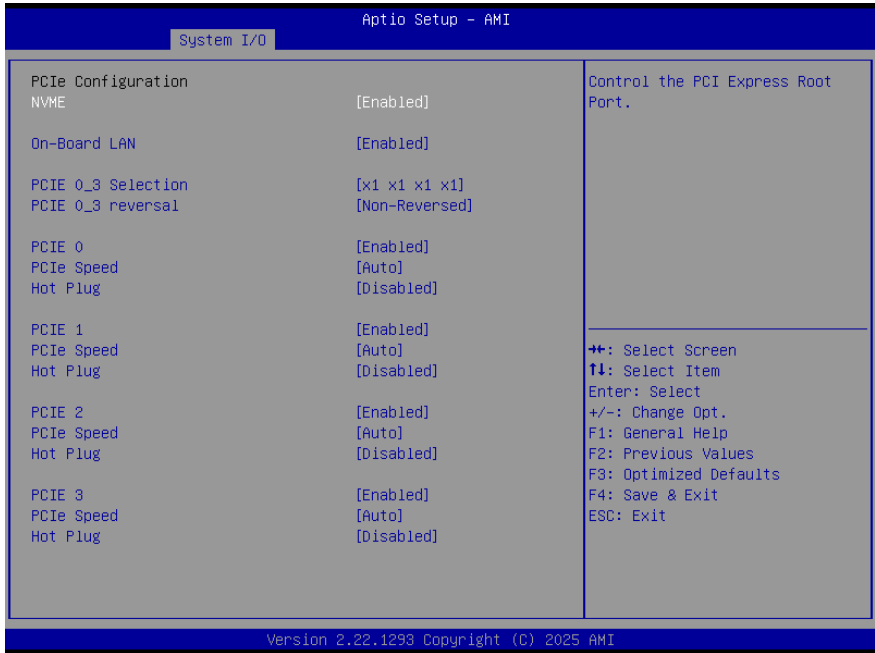


Options Summary		
Smart Battery	Disable	Optimal Default, Failsafe Default
	Enable	
Support smart battery feature.		

3.5 Setup Submenu: System I/O



3.5.1 PCI Express Configuration



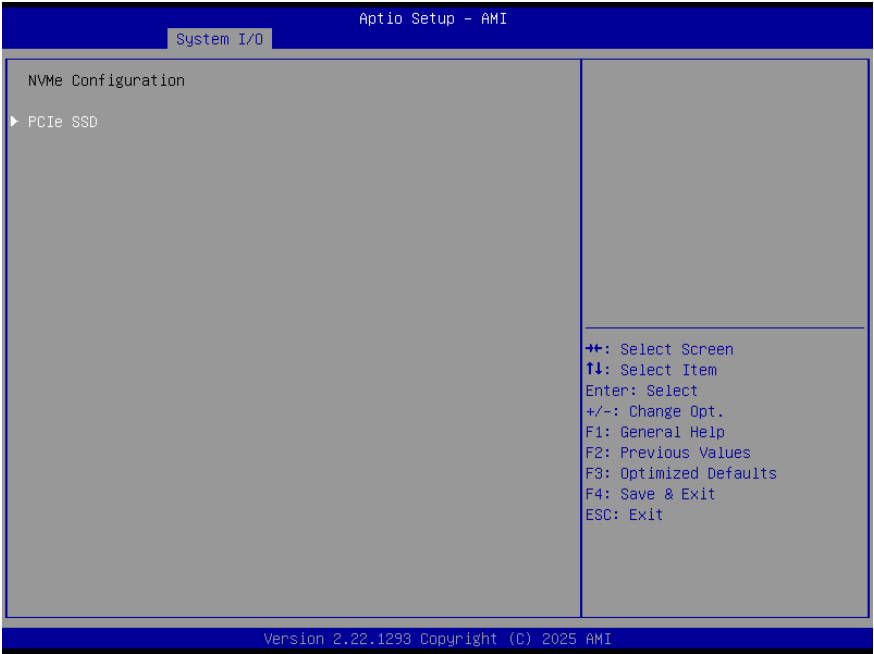
Options Summary		
NVME	Disable	
	Enable	Optimal Default, Failsafe Default
Control the PCI Express Root Port.		
On-Board LAN	Disable	
	Enable	Optimal Default, Failsafe Default
Control the PCI Express Root Port.		
PCIe 0_3 Selection	x1 x1 x1 x1	Optimal Default, Failsafe Default
	x2 x1 x1	
	x2 x2	
	x4	
PCIe Controller Setting.		
PCIe 0_3 reversal	Non-Reversed	Optimal Default, Failsafe Default
	Reversed	
PCIe LANE REVERSAL.		

Options Summary		
PCIe 0 ~ 3	Disable	
	Enable	Optimal Default, Failsafe Default
Control the PCI Express Root Port.		
PCIe Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
	Gen4	
Configure PCIe Speed.		
Hot Plug	Disable	Optimal Default, Failsafe Default
	Enable	
PCI Express Hot Plug Enable/Disable.		

3.5.2 Storage Configuration



3.5.2.1 NVMe Configuration

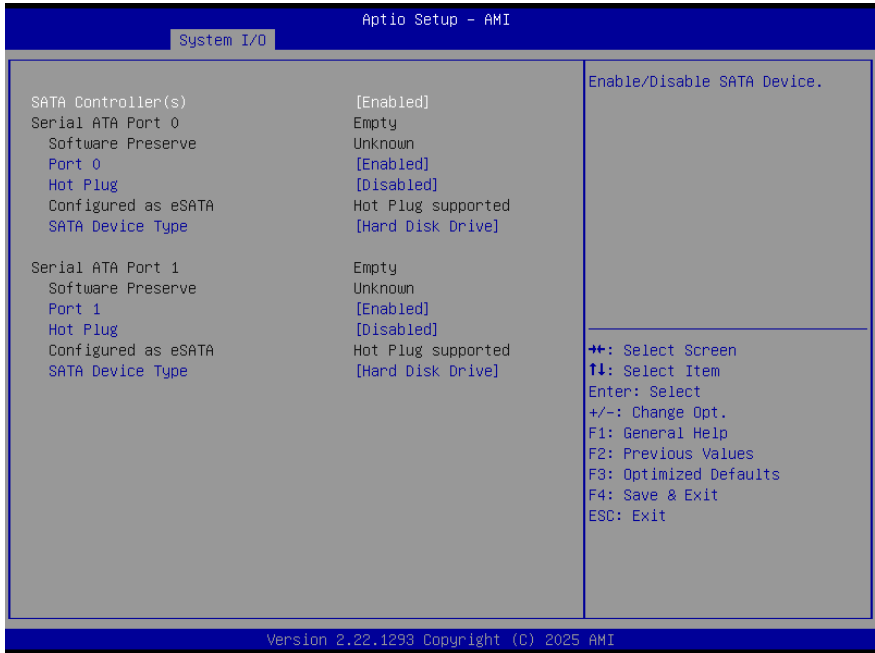


3.5.2.2 PCIe SSD



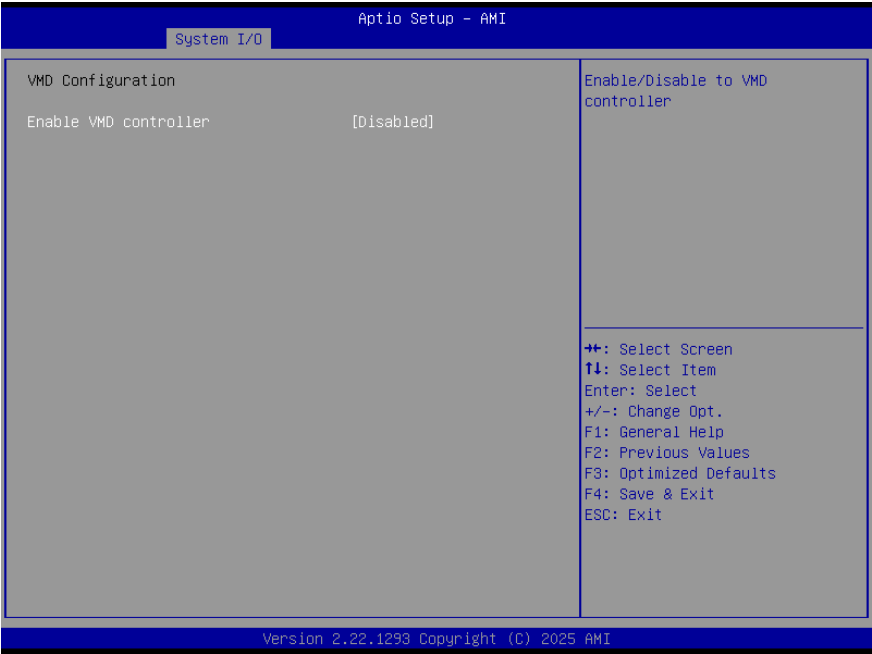
Options Summary		
Self Test Option	Short	Optimal Default, Failsafe Default
	Extended	
Select either Short or Extended Self Test Option. Short option will take a couple of minutes and extended option will take several minutes to complete.		
Self Test Action	Controller only test	Optimal Default, Failsafe Default
	Controller and NameSpace test	
Select either to test Controller alone or Controller and NameSpace. Select Controller and NameSpace option will take a lot longer to complete the test.		

3.5.2.3 SATA Configuration



Options Summary		
SATA Controller(s)	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable/Disable SATA Device.		
Port 0 ~ 1	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable SATA Port.		
Hot Plug	Disabled	Optimal Default, Failsafe Default
	Enabled	
Designates this port as Hot Pluggable.		
SATA Device Type	Hard Disk Drive	Optimal Default, Failsafe Default
	Solid State Drive	
Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.		

3.5.2.3 VMD Setup Menu



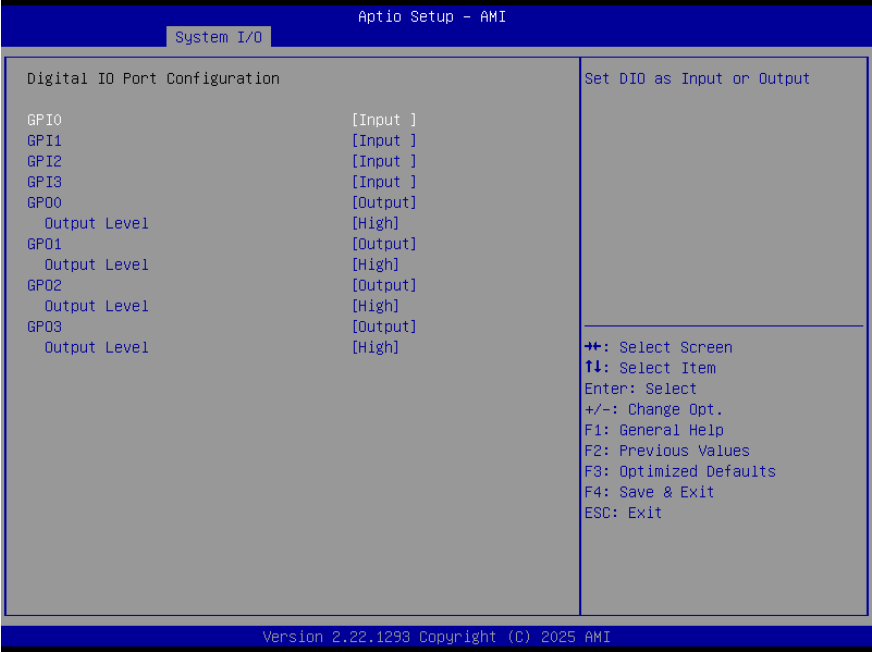
Options Summary		
Enable VMD controller	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enable/Disable to VMD controller.		

3.5.3 HD Audio Configuration



Options Summary		
HD Audio	Disabled	
	Enabled	Optimal Default, Failsafe Default
Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled. Enabled = HDA will be unconditionally enabled.		

3.5.4 Digital IO Port Configuration

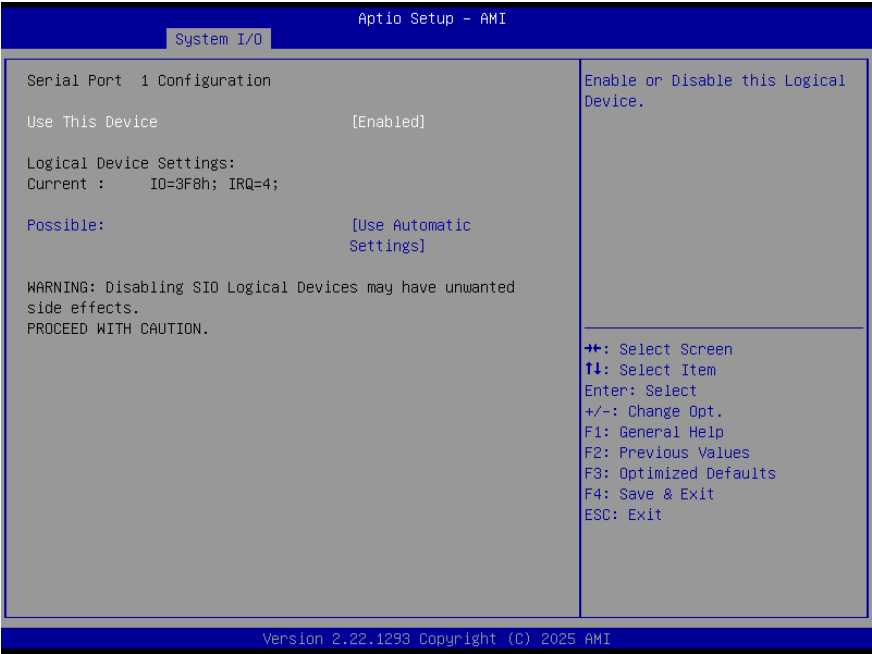


Options Summary		
GPI 0 - 3	Input	Optimal Default, Failsafe Default
	Output	
Set DIO as Input or Output.		
GPO 0 - 3	Input	
	Output	Optimal Default, Failsafe Default
Set DIO as Input or Output.		
Output Level	High	Optimal Default, Failsafe Default
	Low	
Set output level when DIO pin is output.		

3.5.5 Legacy Logical Devices Configuration

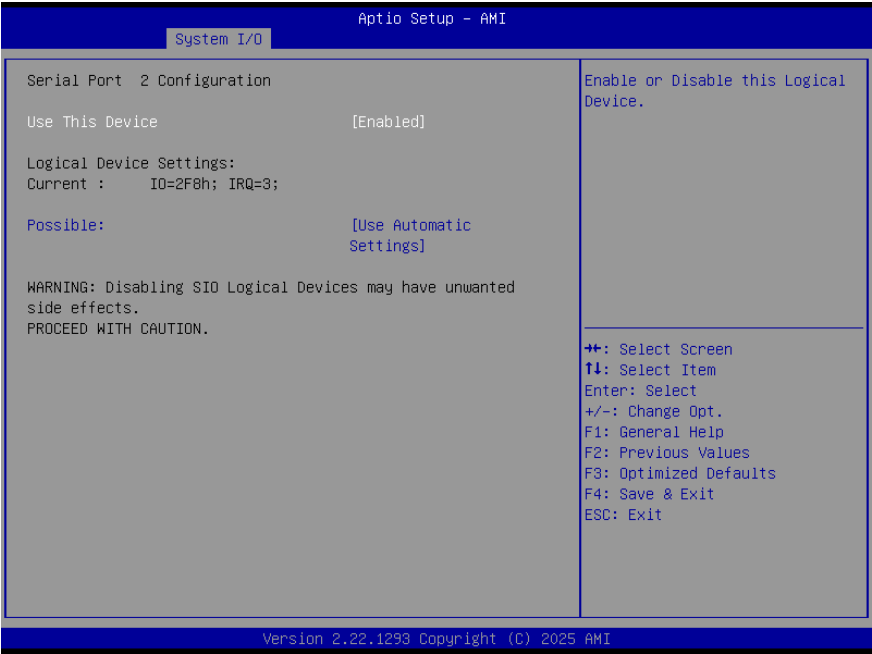


3.5.5.1 Serial Port 1 Configuration



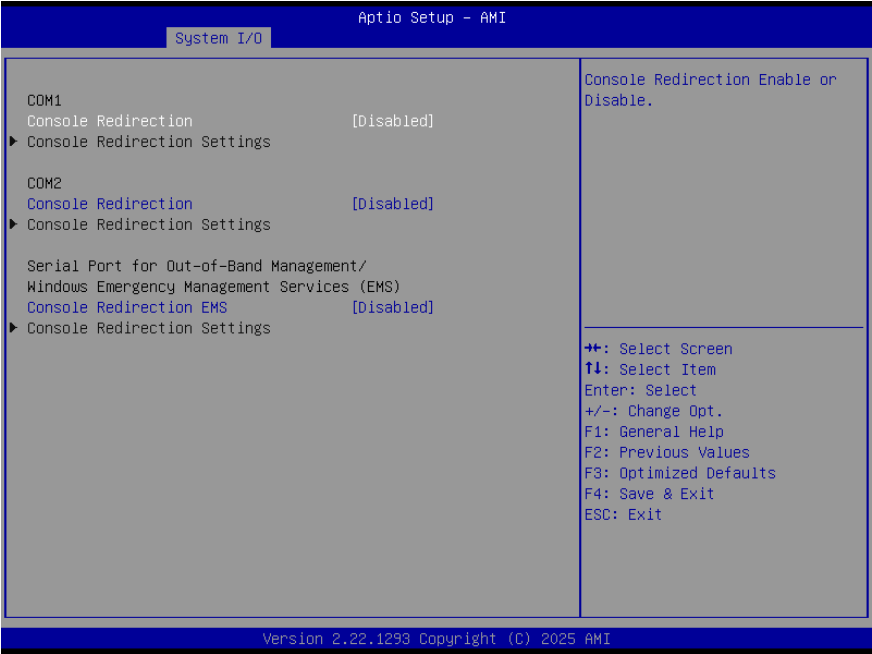
Options Summary		
Use This Device	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable this Logical Device.		
Possible:	Use Automatic Settings	Optimal Default, Failsafe Default
	IO=3F8h; IRQ=4; DMA;	
	IO=2C8h; IRQ=11; DMA;	
Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		

3.5.5.2 Serial Port 2 Configuration



Options Summary		
Use This Device	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable this Logical Device.		
Possible:	Use Automatic Settings	Optimal Default, Failsafe Default
	IO=2F8h; IRQ=3; DMA;	
	IO=2d8h; IRQ=10; DMA;	
Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		

3.5.6 Serial Port Console Configuration



Options Summary		
COM1 Console Redirection	Disabled	Optimal Default, Failsafe Default
	Enabled	
Console Redirection Enable or Disable.		
COM2 Console Redirection	Disabled	Optimal Default, Failsafe Default
	Enabled	
Console Redirection Enable or Disable.		
Console Redirection EMS	Disabled	Optimal Default, Failsafe Default
	Enabled	
Console Redirection Enable or Disable.		

3.5.6.1 COM1 Console Redirection Settings



Options Summary		
Terminal Type	VT100	
	VT100Plus	
	VT-UTF8	
	ANSI	Optimal Default, Failsafe Default
Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.		

Options Summary		
Bits per second	9600	
	19200	
	38400	
	57600	
	115200	Optimal Default, Failsafe Default
	230400	
	460800	
	921600	
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.		
Data Bits	7	
	8	Optimal Default, Failsafe Default
Data Bits		
Parity	None	Optimal Default, Failsafe Default
	Even	
	Odd	
	Mark	
	Space	
A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.		
Stop Bits	1	Optimal Default, Failsafe Default
	2	
Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.		
Flow Control	None	Optimal Default, Failsafe Default
	Hardware RTS/CTS	
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.		
VT-UTF8 Combo Key	Disabled	
Support	Enabled	Optimal Default, Failsafe Default

Options Summary		
Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals		
Recorder Mode	Disabled	Optimal Default, Failsafe Default
	Enabled	
With this mode enabled only text will be sent. This is to capture Terminal data.		
Resolution 100x31	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enables or disables extended terminal resolution.		
Putty KeyPad	VT100	Optimal Default, Failsafe Default
	LINUX	
	XTERMR6	
	SCO	
	ESCN	
	VT400	
Select FunctionKey and KeyPad on Putty		

3.5.6.2 COM2 Console Redirection Settings

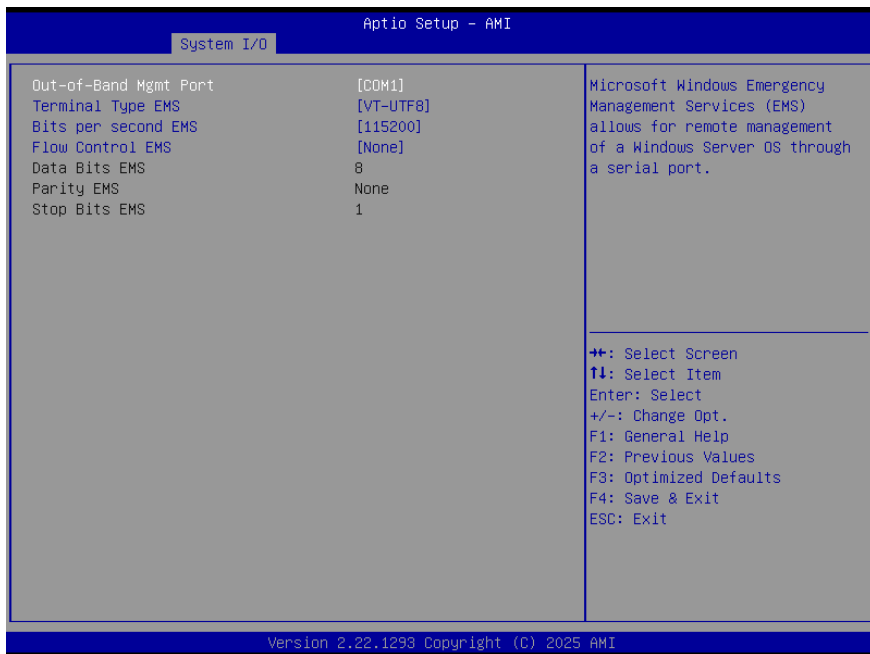


Options Summary		
Terminal Type	VT100	
	VT100Plus	
	VT-UTF8	
	ANSI	Optimal Default, Failsafe Default
Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.		

Options Summary		
Bits per second	9600	
	19200	
	38400	
	57600	
	115200	Optimal Default, Failsafe Default
	230400	
	460800	
	921600	
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.		
Data Bits	7	
	8	Optimal Default, Failsafe Default
Data Bits		
Parity	None	Optimal Default, Failsafe Default
	Even	
	Odd	
	Mark	
	Space	
A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.		
Stop Bits	1	Optimal Default, Failsafe Default
	2	
Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.		
Flow Control	None	Optimal Default, Failsafe Default
	Hardware RTS/CTS	
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.		
VT-UTF8 Combo Key	Disabled	
Support	Enabled	Optimal Default, Failsafe Default

Options Summary		
Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals		
Recorder Mode	Disabled	Optimal Default, Failsafe Default
	Enabled	
With this mode enabled only text will be sent. This is to capture Terminal data.		
Resolution 100x31	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enables or disables extended terminal resolution.		
Putty KeyPad	VT100	Optimal Default, Failsafe Default
	LINUX	
	XTERMR6	
	SCO	
	ESCN	
	VT400	
Select FunctionKey and KeyPad on Putty		

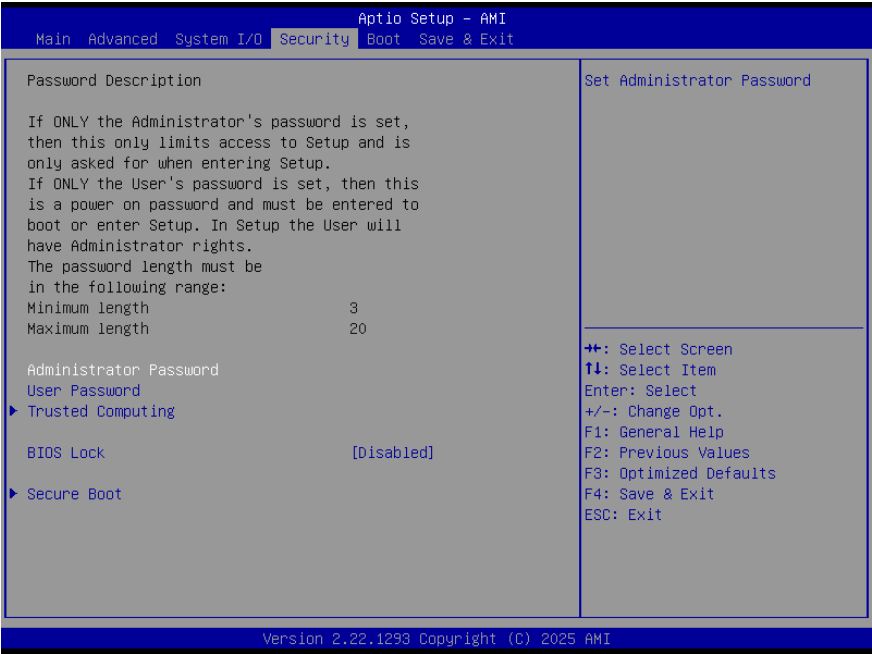
3.5.6.3 Console Redirection Settings



Options Summary		
Out-of-Band Mgmt Port	COM1	
	COM2	Optimal Default, Failsafe Default
Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port		
Terminal Type EMS	VT100	
	VT100Plus	
	VT-UTF8	Optimal Default, Failsafe Default
	ANSI	
VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.		
Bits per second EMS	9600	
	19200	
	57600	
	115200	Optimal Default, Failsafe Default

Options Summary		
	230400	
	460800	
	921600	
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.		
Flow Control EMS	None	Optimal Default, Failsafe Default
	Hardware RTS/CTS	
	Software Xon/Xoff	
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.		

3.6 Setup Submenu: Security



Change User/Administrator Password

You can set a User Password once an Administrator Password is set. The password will be required during boot up, or when the user enters the Setup utility. Please Note that a User Password does not provide access to many of the features in the Setup utility. Select the password you wish to set, press Enter to open a dialog box to enter your password (you can enter no more than six letters or numbers). Press Enter to confirm your entry, after which you will be prompted to retype your password for a final confirmation. Press Enter again after you have retyped it correctly.

Removing the Password

Select the password you want to remove and enter the current password. At the next dialog box press Enter to disable password protection.

Options Summary		
BIOS Lock	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.		

3.6.1 Trusted Computing

Aprio Setup - AMI		
Security		
TPM 2.0 Device Found		Enables or Disables BIOS support for security device. U.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Firmware Version:	7.2	
Vendor:	NTC	
Security Device Support	[Enable]	
Active PCR banks	SHA256	
Available PCR banks	SHA256,SHA384	
SHA256 PCR Bank	[Enabled]	
SHA384 PCR Bank	[Disabled]	
Pending operation	[None]	
Platform Hierarchy	[Enabled]	
Storage Hierarchy	[Enabled]	
Endorsement Hierarchy	[Enabled]	
Physical Presence Spec Version	[1.3]	
TPM 2.0 InterfaceType	[TIS]	
Device Select	[Auto]	
		++: Select Screen tl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1293 Copyright (C) 2025 AMI		

Options Summary		
Security Device Support	Disable	
	Enable	Optimal Default, Failsafe Default

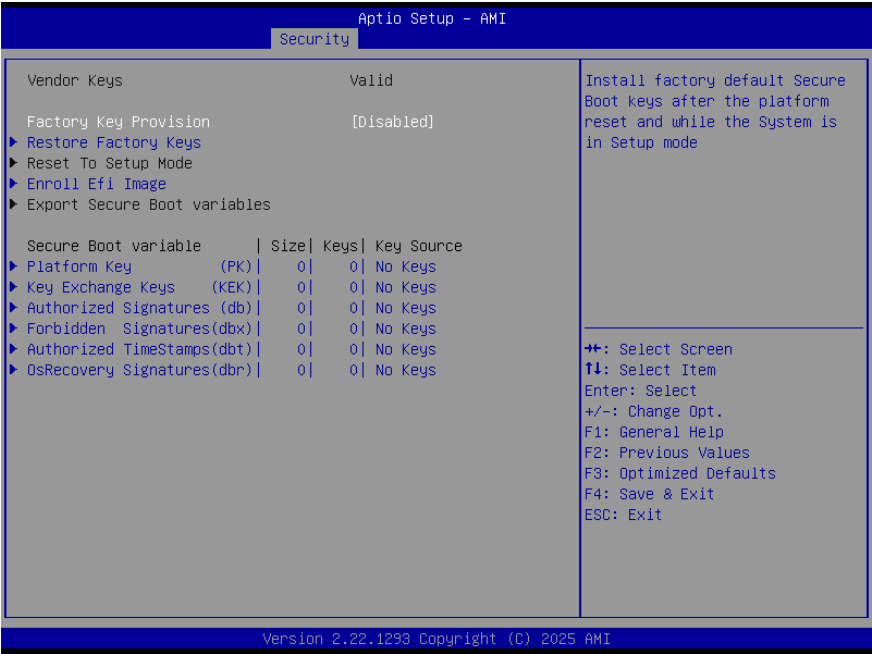
Options Summary		
Enables or Disables BIOS support for the security device. OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.		
SHA256 PCR Bank	Disable	
	Enable	Optimal Default, Failsafe Default
Enable or Disable SHA256 PCR Bank.		
SHA384 PCR Bank	Disable	Optimal Default, Failsafe Default
	Enable	
Enable or Disable SHA384 PCR Bank.		
Pending Operation	None	Optimal Default, Failsafe Default
	TPM Clear	
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.		
Platform Hierarchy	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or disable Platform Hierarchy.		
Storage Hierarchy	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable Storage Hierarchy.		
Endorsement Hierarchy	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable Endorsement Hierarchy.		
Physical Presence Spec Version	1.2	
	1.3	Optimal Default, Failsafe Default
Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.		
Device Select	TPM 1.2	
	TPM 2.0	
	Auto	Optimal Default, Failsafe Default
TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.		

3.6.2 Secure Boot



Options Summary		
Secure Boot	Disabled	Optimal Default, Failsafe Default
	Enabled	
Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset.		
Secure Boot Mode	Custom	Optimal Default, Failsafe Default
	Standard	
Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.		
Restore Factory Keys		
Force System to User Mode. Install factory default Secure Boot key databases.		
Restore To Setup Mode		
Force System Delete all Secure Boot key databases from NVRAM.		

3.6.2.1 Expert Key Management

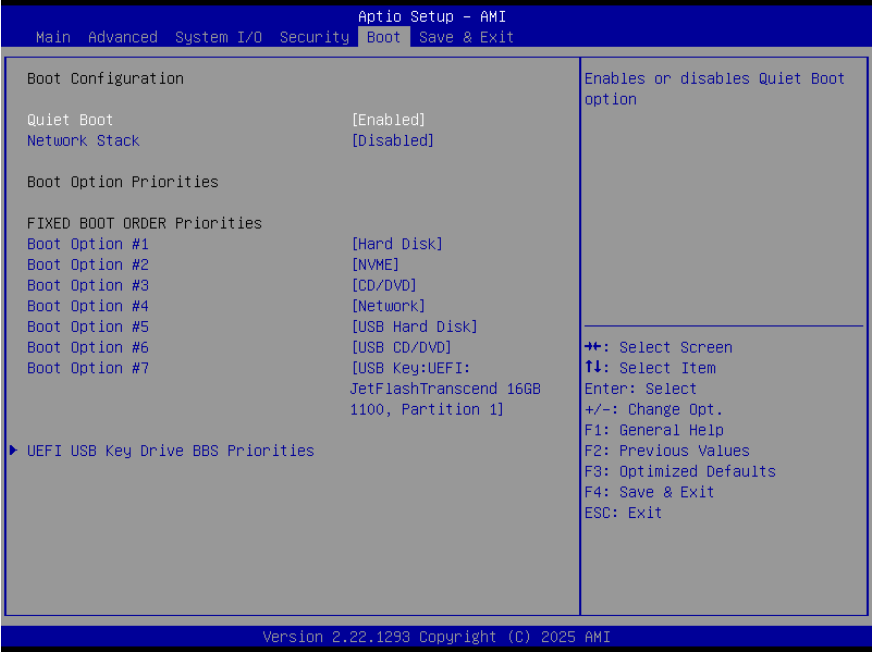


Options Summary		
Factory Key Provision	Disabled	Optimal Default, Failsafe Default
	Enabled	
Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.		
Restore Factory Keys		
Force System to User Mode. Install factory default Secure Boot key databases.		
Reset to Setup Mode		
Delete all Secure Boot key databases from NVRAM.		
Export Secure Boot variables		
Save NVRAM content of Secure Boot variable to a file.		
Enroll Efi Image		
Allow the image to run in Secure Boot mode.		
Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).		

Options Summary

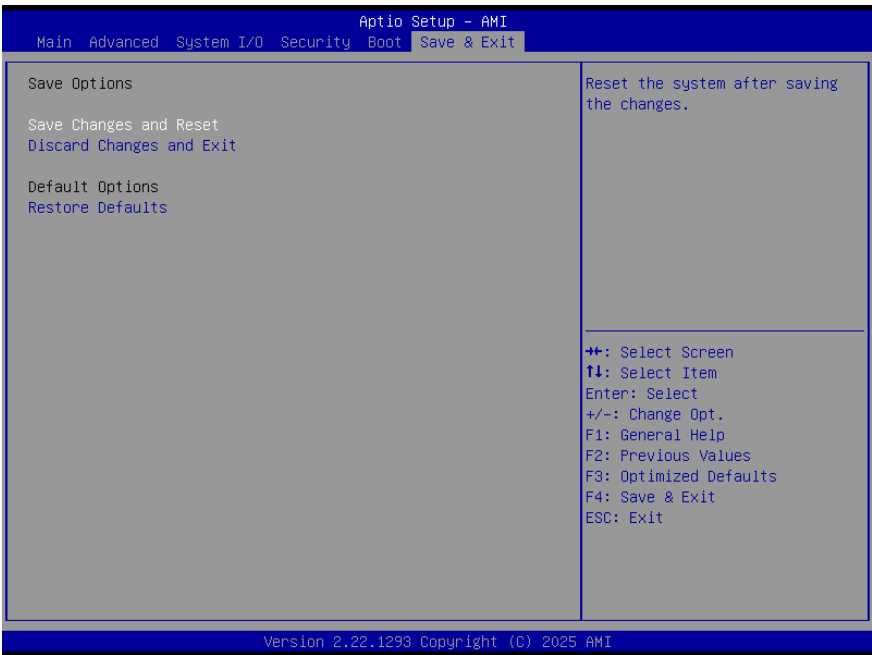
Platform Key (PK)	Details
	Export
	Update
	Delete
Key Exchange Keys (KEK)	Details
	Export
	Update
	Append
	Delete
Authorized Signatures (db)	Details
	Export
	Update
	Append
	Delete
Forbidden Signatures (dbx)	Details
	Export
	Update
	Append
	Delete
Authorized TimeStamps (dbt)	Update
	Append
OsRecovery Signatures (dbr)	Update
	Append
Enroll Factory Defaults or load certificates from a file: Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX Authenticated UEFI Variable EFI PE/COFF Image (SHA256) Key Source: Factory, Modified, Mixed	

3.7 Setup Submenu: Boot



Options Summary		
Quiet Boot	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enables or disables Quiet Boot option.		
Network Stack	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enable/Disable UEFI Network Stack.		

3.8 Setup Submenu: Save & Exit



Chapter 4

Drivers Installation

4.1 Driver Download and Installation

Drivers for the NANOCOM-MTU can be downloaded from the product page on the AAEON website by following this link:

<https://www.aaeon.com/en/>

Download the driver(s) you need and follow the steps below to install them.

Chipset Driver

1. Open the folder where you unzipped the **Chipset Drivers**.
2. Run the **SetupChipset.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

Graphics Driver

1. Open the folder where you unzipped the **Graphics Drivers**.
2. Run the **gfx_win_101.5762.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

LAN Drivers

1. Open the folder where you unzipped the **LAN Drivers**.
2. Press Windows + X, then click Device Manager, Expand Network adapters.
3. If the device is not yet installed, look under Other devices (it may appear as Ethernet Controller).
4. Right-click the Intel® Ethernet device (or unknown Ethernet Controller), then click Update driver.
5. Choose Browse my computer for drivers.

6. Click Browse... and select the folder containing the driver files (e.g., C:\LAN_Driver).
7. Click Next to begin installation.
8. Windows will install the driver using the e2f.inf file.
9. Once complete, the device will appear as Intel(R) Ethernet Controller I225-V or I226-V, depending on your hardware.
10. Click Close to finish.

ME & TXE Drivers

1. Open the folder where you unzipped the **ME & TXE Drivers**.
2. Run the **SetupME.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

Serial I/O Driver

1. Open the folder where you unzipped the **Serial I/O Driver**.
2. Run the **SetupSerialIO.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

Intel NPU Driver

1. Open the folder where you unzipped the **Intel NPU Driver**.
2. Open Device Manager
3. Press Windows + X → Select Device Manager.
4. Locate the NPU device: It may appear under System Devices, Processors, or Other devices as Intel® NPU, AI Processor, or Unknown device.
5. Right-click the NPU device and choose Update driver.
6. Click Browse, then navigate to your driver folder (e.g., C:\IntelNPU_Driver).

7. Click Next. Windows will search for and install the driver using the .inf file (likely named npu.inf if present in the full package).
8. Finish Installation
9. Once finished, the NPU device should be correctly named and functional.
10. If prompted, restart your computer.

Intel Platform Monitoring Technology Driver

1. Open the folder where you unzipped the **Intel Platform Monitoring Technology Driver**.
2. Extract or copy the folder containing intcpmt.inf, intcpmt.sys, and intcpmt.cat to a location like C:\Intel_PMT_Driver.
3. Press Windows + X → Select Device Manager.
4. Locate the Platform Monitoring Technology device
5. Manually Install the Driver
 - i. Right-click the device, then choose Update driver.
 - ii. Click Browse my computer for drivers.
 - iii. Select the folder containing the driver files (C:\Intel_PMT_Driver).
 - iv. Click Next to begin installation.
6. Windows will install the driver using the intcpmt.inf file.
7. When complete, the device will appear as Intel(R) Platform Monitoring Technology Driver or similar.
8. Click Close, then restart your computer if prompted.

Audio Drivers

Intel® ADSP (Audio DSP) Driver

1. **Open Device Manager**
 - a. Press Windows + X, then select **Device Manager**.
2. **Locate the Target Device**

- Expand categories like **Sound, video and game controllers**, **System devices**, **Audio inputs and outputs**, or **Other devices**.
 - Devices may appear as unknown (e.g., "Audio DSP" or "Multimedia Controller").
3. **Update the Driver**
 - Right-click the device → **Update driver**.
 - Choose **Browse my computer for drivers**.
 - Click **Browse**, and navigate to the folder for the correct driver component (e.g., C:\Intel_ADSP\IntcSST).
 - Click **Next** to install the driver.
 4. **Repeat for All Components**
 - Install each component in the suggested order.
 - Restart the system after completing all installations.

Recommended Installation Order

1. IntcAudioBus
2. IntcSDW / IntcSdwBus
3. IntcSST
4. IntcDMic
5. IntcOED
6. IntcUSB
7. IntcBTau
8. IntcBtLE
9. IntcAudioSensors
10. IntcStreaming
11. WoV (Wake-on-Voice)
12. DetectionVerificationDrv

If any driver fails to install, verify that the .inf file is in the folder and that your hardware supports the feature.

Realtek Audio Driver

1. Open the folder where you unzipped the **Realtek Audio Driver**.
2. Run the **Setup.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

RAID Driver

1. Open the folder where you unzipped the **RAID Driver**.
2. Run the **SetupRST.exe** file in the folder.
3. Follow the instructions.
4. Drivers will be installed automatically.

Intel Camera Driver

1. Open the folder where you unzipped the **Intel Camera Driver**.
2. Extract the driver package to a folder such as: C:\Intel_Camera_Driver\
3. **Open Device Manager**
 1. Press Windows + X → **Device Manager**.
 2. Expand **Imaging Devices, Cameras, or Other devices**.
 3. Look for:
 4. "Intel AVStream Camera"
 5. "Unknown Device"
 6. "OV01A1S" / "OV13858" (depending on camera module)
4. Manually Install Drivers.

Right-click → Update driver

Select "Browse my computer for drivers"

Browse to the extracted folder, and let Windows search subfolders

Click Next to install

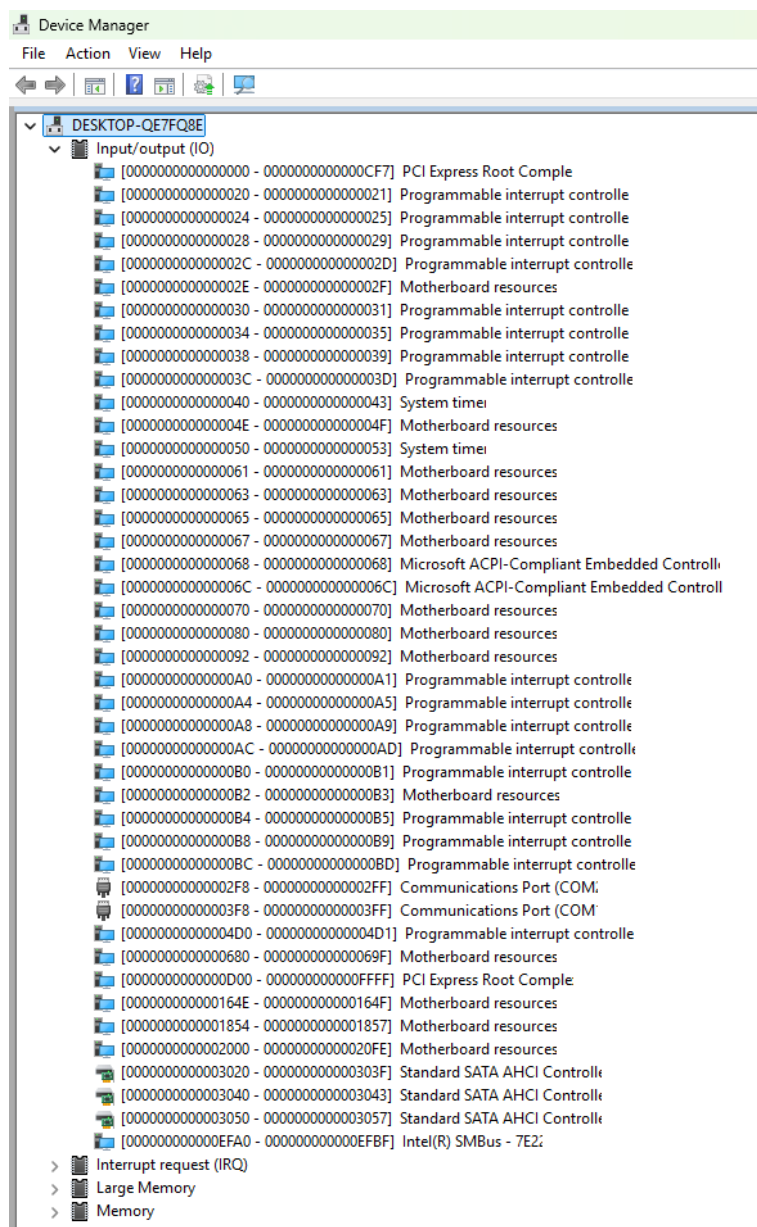
Repeat for:

- Main camera (iacamera64.sys)
- Sensor modules (e.g., ov01a1s.sys, ov13858.sys)
- ISP driver (iaisp64.sys)
- Control logic (iactrllogic64.sys)
- Sub-drivers like IntcOED, Im3643, lt6911uxc, etc.

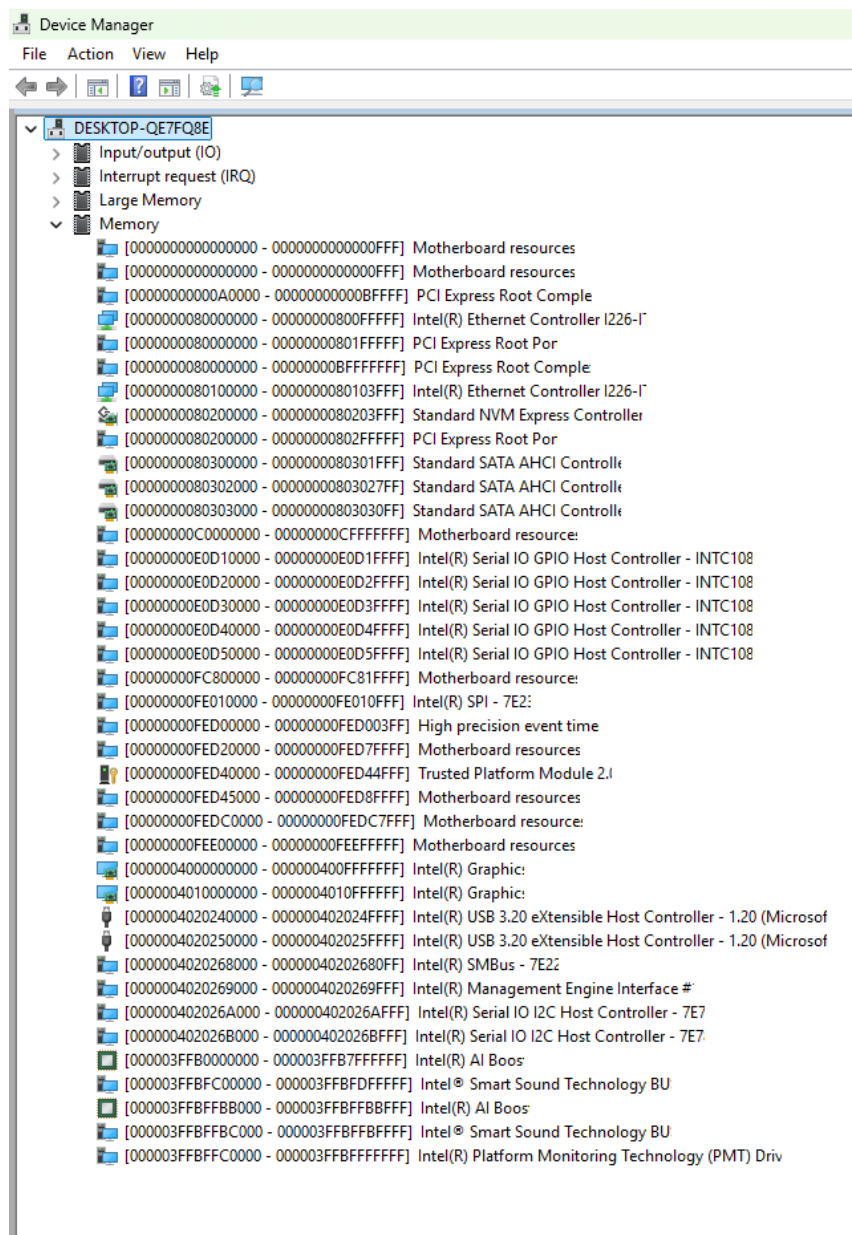
Appendix A

I/O Information

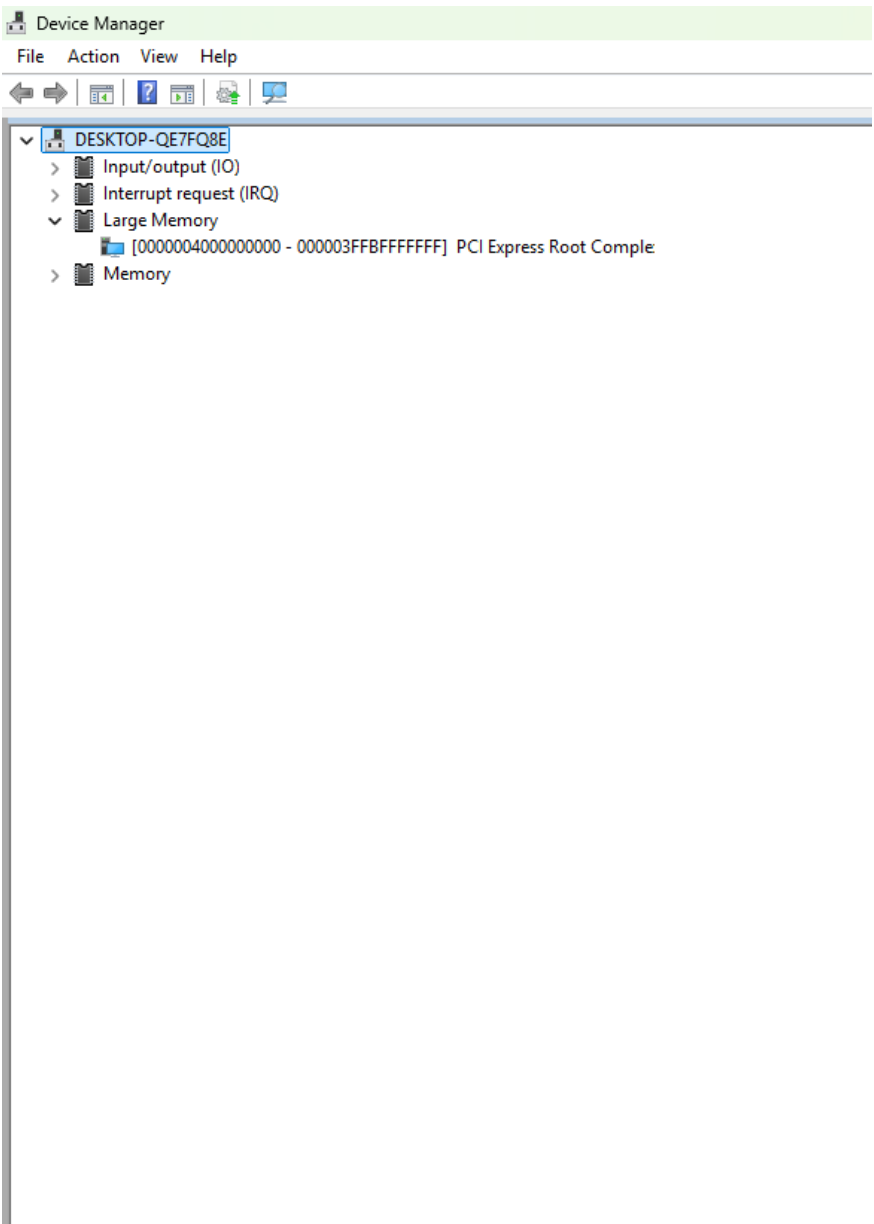
A.1 I/O Address Map



A.2 Memory Address Map



A.3 Large Memory Address Map



A.4 IRQ Mapping Chart

