

COM-CFHB6

COM Express Module

User's Manual 2nd 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.

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
● COM-CFHB6-A11	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 product page at 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	4
2.1 Dimensions, Jumpers and Connectors	5
2.2 Jumper: SW1 AT/ATX Mode	8
2.3 List of Connectors.....	8
2.3.1 Express ROW C/D Connector (CN1).....	9
2.3.2 Express ROW A/B Connector (CN4).....	13
2.4 Block Diagram	18
Chapter 3 - AMI BIOS Setup	19
3.1 System Test and Initialization	20
3.2 AMI BIOS Setup	21
3.3 Setup submenu: Main	22
3.4 Setup submenu: Advanced	23
3.4.1 Advanced: Graphics Configuration.....	24
3.4.2 Advanced: LVDS Panel Configuration	26
3.4.3 Advanced: CPU Configuration.....	28
3.4.4 Advanced: Memory Configuration	29
3.4.5 Advanced: On-Module H/W Monitor.....	30
3.4.5.1 Fan 1 Mode Configuration.....	31
3.4.5.2 CPU Smart Fan Control: Manual Mode by PWM.....	32
3.4.5.3 CPU Smart Fan Control: Auto Mode by PWM.....	33
3.4.6 Advanced: PCH-FW Configuration.....	34
3.4.6.1 Firmware Update Configuration	35
3.4.7 Advanced: On-Module Configuration	36
3.4.8 Advanced: Power Management.....	37

3.4.8.1	RTC Wake System from S4/S5: Fixed Time	38
3.5	Setup submenu: System I/O	39
3.5.1	System I/O: PCI Express Configuration	40
3.5.1.1	PCI Express Configuration: PEG* Hotplug Enabled	42
3.5.1.2	PCI Express Configuration: PCIE_0 – PCIE_7 Submenus	43
3.5.2	System I/O: SATA Configuration	44
3.5.3	System I/O: HD Audio Configuration	46
3.5.4	System I/O: Digital IO Port Configuration	47
3.5.5	System I/O: Legacy Logical Devices Configuration	48
3.5.5.1	[*Active*] Serial Port 1	49
3.5.5.2	[*Active*] Serial Port 2	50
3.5.6	System I/O: Serial Port Console Redirection	51
3.5.6.1	Legacy Console Redirection Settings	52
3.5.6.2	COM0 Console Redirection Settings	53
3.5.6.3	Out of Band Management	56
3.6	Setup submenu: Security	58
3.6.1	Security: Secure Boot	59
3.6.1.1	Secure Boot: Key Management	61
3.6.2	Security: Trusted Computing	65
3.7	Setup submenu: Boot	67
3.7.1	Boot: PXE Boot [UEFI] Settings	68
3.7.2	Boot: UEFI USB Key Drive BBS Priorities	69
3.8	Setup submenu: Save & Exit	70
Chapter 4 – Drivers Installation		71
4.1	Driver Download/Installation	72
Appendix A - Watchdog Timer Programming		73
A.1	Watchdog Timer Initial Program	74
Appendix B - I/O Information		79

B.1	I/O Address Map	80
B.2	Memory Address Map	81
B.3	Interrupt Request (IRQ) Mapping Chart.....	82
Appendix C – Programming Digital I/O.....		91
C.1	Digital I/O Programming	92
C.2	Digital I/O Register	92
C.2	Digital I/O Sample Program.....	94

Chapter 1

Product Specifications

1.1 Specifications

System	
FORM FACTOR	COM Express Basic Size, Type 6
CPU	8th/9th Gen Intel® Core™/ Xeon™-E Series Processor
CPU FREQUENCY	Up to E-2276ME (2.8 GHz)
CHIPSET	Intel® QM370/CM246 PCH
MEMORY TYPE	SODIMM DDR4 2666 Socket x 3 DDR4 2400 SO-DIMM x3, 2DPC DDR4 2666 SO-DIMM x2, 1DPC
MAX. MEMORY CAPACITY	up to 64 GB,ECC Support (only with CM246 PCH)
BIOS	AMI BIOS, Legacy free BIOS
WAKE ON LAN	Yes
WATCHDOG TIMER	255 Levels
POWER REQUIREMENT	Standard: +12V
POWER SUPPLY TYPE	AT/ATX Selection
POWER CONSUMPTION (TYPICAL)	Intel ® Xeon ® E-2276ME CPU , 12V@4.65A , Full load: 55.8W
DIMENSION (L X W)	4.92" x 3.75" (125mm x 95mm)
OPERATING TEMPERATURE	32°F ~ 140°F (0°C ~ 60°C) -40°F ~ 185°F (-40°C ~ 85°C) optional

STORAGE TEMPERATURE	-40°F ~ 185°F (-40°C ~ 85°C)
OPERATING HUMIDITY	0% ~ 90% relative humidity, non-condensing
MTBF (HOURS)	464,349 Hours
CERTIFICATION	CE/FCC Class A

Display

VGA/LCD CONTROLLER	Intel® GT2-P630 (Xeon series)/ GT2-630 (Core I series)
VIDEO OUTPUT	VGA, 18/24b 2ch LVDS/eDP, DDI x 2 (3rd one can be added if VGA not require)
LVDS INTERFACE	18/24b 2ch LVDS

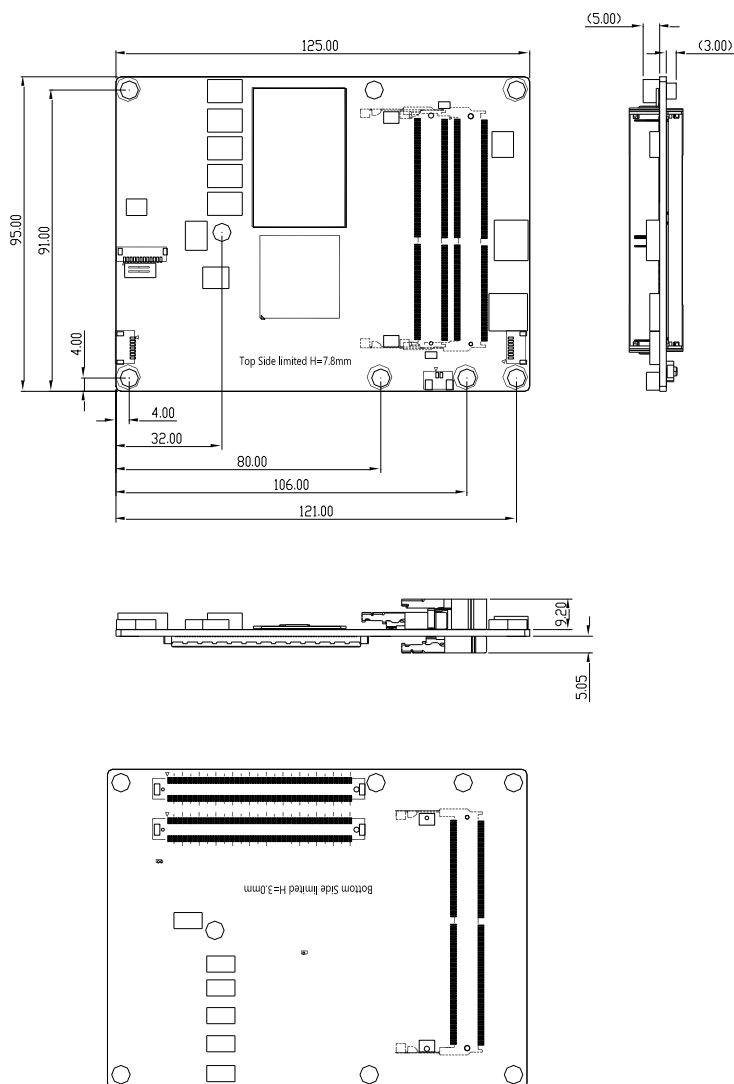
I/O

ETHERNET	Intel® Ethernet I219 GbE x1
AUDIO	HD Audio
USB PORT	USB 2.0 x 8 , USB 3.2 Gen 2 x 4
SERIAL PORT	2-wire UART(TX/RX) x 2
HDD INTERFACE	SATA3 x 4
ONBOARD STORAGE	—
EXPANSION	PCIe [x1] x8, PCIe[x16] x1, LPC, SMBUS, I2C
GPIO	8-bit
TPM	2.0(Optional)

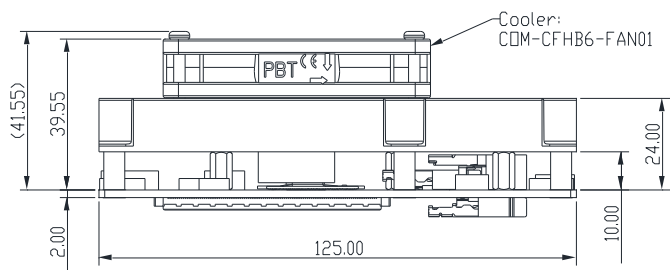
Chapter 2

Hardware Information

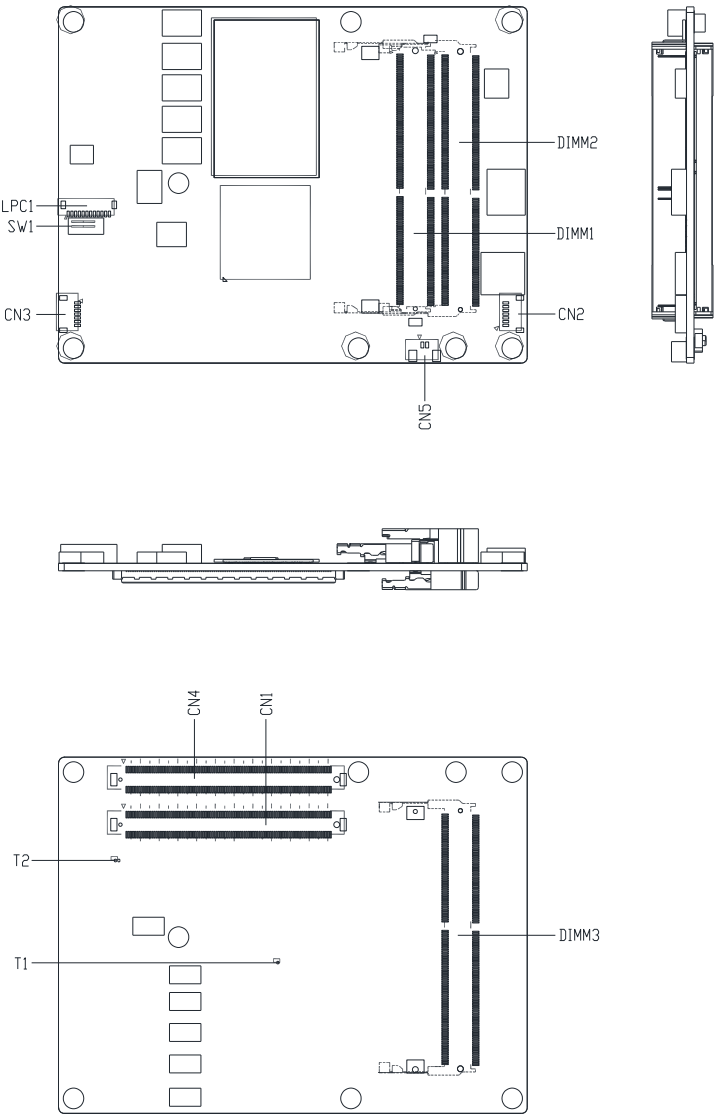
2.1 Dimensions, Jumpers and Connectors



With Fan



Jumpers, Switches and Connectors:



2.2 Jumper: SW1 AT/ATX Mode

Mode	1	2
ATX (Default)	OFF	OFF
AT Mode	ON	OFF
Clear CMOS	OFF	ON

2.3 List of Connectors

This section details the board’s connectors and their configuration. Please use this reference to determine the best setup for your application.

Label	Function
LPC1	LPC debug card Connector
DIMM1	SO-DIMMCOM Connector
DIMM2	SO-DIMMCOM Connector
DIMM3	SO-DIMMCOM Connector
CN1	Express ROW C/D Connector
CN2	SPI Flash Programming Connector
CN3	EC Flash Programming Connector
CN4	Express ROW A/B Connector
CN5	RTC Battery Connector

2.3.1 Express ROW C/D Connector (CN1)

Row C		Row D	
Pin	Signal	Pin	Signal
C1	GND (FIXED)	D1	GND (FIXED)
C2	GND (FIXED)	D2	GND (FIXED)
C3	USB_SSRX0-	D3	USB_SSTX0-
C4	USB_SSRX0+	D4	USB_SSTX0+
C5	GND (FIXED)	D5	GND (FIXED)
C6	USB_SSRX1-	D6	USB_SSTX1-
C7	USB_SSRX1+	D7	USB_SSTX1+
C8	GND (FIXED)	D8	GND (FIXED)
C9	USB_SSRX2-	D9	USB_SSTX2-
C10	USB_SSRX2+	D10	USB_SSTX2+
C11	GND (FIXED)	D11	GND (FIXED)
C12	USB_SSRX3-	D12	USB_SSTX3-
C13	USB_SSRX3+	D13	USB_SSTX3+
C14	GND (FIXED)	D14	GND (FIXED)
C15	DDI1_PAIR6+(NC)	D15	DDI1_CTRLCLK_AUX+
C16	DDI1_PAIR6-(NC)	D16	DDI1_CTRLDATA_AUX-
C17	RSVD	D17	RSVD
C18	RSVD	D18	RSVD
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND (FIXED)	D21	GND (FIXED)
C22	PCIE_RX7+	D22	PCIE_TX7+
C23	PCIE_RX7-	D23	PCIE_TX7-

Row C		Row D	
Pin	Signal	Pin	Signal
C24	DDI1_HPD	D24	RSVD
C25	DDI1_PAIR4+(NC)	D25	RSVD
C26	DDI1_PAIR4-(NC)	D26	DDI1_PAIR0+
C27	RSVD	D27	DDI1_PAIR0-
C28	RSVD	D28	RSVD
C29	DDI1_PAIR5+(NC)	D29	DDI1_PAIR1+
C30	DDI1_PAIR5-(NC)	D30	DDI1_PAIR1-
C31	GND (FIXED)	D31	GND (FIXED)
C32	DDI2_CTRLCLK_AUX+	D32	DDI1_PAIR2+
C33	DDI2_CTRLDATA_AUX-	D33	DDI1_PAIR2-
C34	DDI2_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL
C35	RSVD	D35	RSVD
C36	DDI3_CTRLCLK_AUX+	D36	DDI1_PAIR3+
C37	DDI3_CTRLDATA_AUX-	D37	DDI1_PAIR3-
C38	DDI3_DDC_AUX_SEL	D38	RSVD
C39	DDI3_PAIR0+	D39	DDI2_PAIR0+
C40	DDI3_PAIR0-	D40	DDI2_PAIR0-
C41	GND (FIXED)	D41	GND (FIXED)
C42	DDI3_PAIR1+	D42	DDI2_PAIR1+
C43	DDI3_PAIR1-	D43	DDI2_PAIR1-
C44	DDI3_HPD	D44	DDI2_HPD
C45	RSVD	D45	RSVD
C46	DDI3_PAIR2+	D46	DDI2_PAIR2+
C47	DDI3_PAIR2-	D47	DDI2_PAIR2-
C48	RSVD	D48	RSVD

Row C		Row D	
Pin	Signal	Pin	Signal
C49	DDI3_PAIR3+	D49	DDI2_PAIR3+
C50	DDI3_PAIR3-	D50	DDI2_PAIR3-
C51	GND (FIXED)	D51	GND (FIXED)
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	TYPE0#(NC)	D54	PEG_LAN_RV#
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	TYPE1#(NC)	D57	TYPE2#
C58	PEG_RX2+	D58	PEG_TX2+
C59	PEG_RX2-	D59	PEG_TX2-
C60	GND (FIXED)	D60	GND (FIXED)
C61	PEG_RX3+	D61	PEG_TX3+
C62	PEG_RX3-	D62	PEG_TX3-
C63	RSVD	D63	RSVD
C64	RSVD	D64	RSVD
C65	PEG_RX4+	D65	PEG_TX4+
C66	PEG_RX4-	D66	PEG_TX4-
C67	RSVD	D67	GND (FIXED)
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-
C70	GND (FIXED)	D70	GND (FIXED)
C71	PEG_RX6+	D71	PEG_TX6+
C72	PEG_RX6-	D72	PEG_TX6-
C73	GND (FIXED)	D73	GND (FIXED)

Row C		Row D	
Pin	Signal	Pin	Signal
C74	PEG_RX7+	D74	PEG_TX7+
C75	PEG_RX7-	D75	PEG_TX7-
C76	GND (FIXED)	D76	GND (FIXED)
C77	RSVD	D77	RSVD
C78	PEG_RX8+	D78	PEG_TX8+
C79	PEG_RX8-	D79	PEG_TX8-
C80	GND (FIXED)	D80	GND (FIXED)
C81	PEG_RX9+	D81	PEG_TX9+
C82	PEG_RX9-	D82	PEG_TX9-
C83	RSVD	D83	RSVD
C84	GND (FIXED)	D84	GND (FIXED)
C85	PEG_RX10+	D85	PEG_TX10+
C86	PEG_RX10-	D86	PEG_TX10-
C87	GND (FIXED)	D87	GND (FIXED)
C88	PEG_RX11+	D88	PEG_TX11+
C89	PEG_RX11-	D89	PEG_TX11-
C90	GND (FIXED)	D90	GND (FIXED)
C91	PEG_RX12+	D91	PEG_TX12+
C92	PEG_RX12-	D92	PEG_TX12-
C93	GND	D93	GND
C94	PEG_RX13+	D94	PEG_TX13+
C95	PEG_RX13-	D95	PEG_TX13-
C96	GND (FIXED)	D96	GND (FIXED)
C97	RSVD	D97	RSVD
C98	PEG_RX14+	D98	PEG_TX14+

Row C		Row D	
Pin	Signal	Pin	Signal
C99	PEG_RX14-	D99	PEG_TX14-
C100	GND (FIXED)	D100	GND (FIXED)
C101	PEG_RX15+	D101	PEG_TX15+
C102	PEG_RX15-	D102	PEG_TX15-
C103	GND (FIXED)	D103	GND
C104	VCC_12V	D104	VCC_12V
C105	VCC_12V	D105	VCC_12V
C106	VCC_12V	D106	VCC_12V
C107	VCC_12V	D107	VCC_12V
C108	VCC_12V	D108	VCC_12V
C109	VCC_12V	D109	VCC_12V
C110	GND (FIXED)	D110	GND (FIXED)

2.3.2 Express ROW A/B Connector (CN4)

Row A		Row B	
Pin	Signal	Pin	Signal
A1	GND (FIXED)	B1	GND (FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#
A4	GBE0_LINK100#	B4	LPC_AD0
A5	GBE0_LINK1000#	B5	LPC_AD1
A6	GBE0_MDI2-	B6	LPC_AD2
A7	GBE0_MDI2+	B7	LPC_AD3
A8	GBE0_LINK	B8	LPC_DRQ0#(NC)

Row A		Row B	
Pin	Signal	Pin	Signal
A9	GBE0_MDI1-	B9	LPC_DRQ1#(NC)
A10	GBE0_MDI1+	B10	LPC_CLK
A11	GND (FIXED)	B11	GND (FIXED)
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	GBE0_CTREF	B14	SMB_DAT
A15	SUS_S3#	B15	SMB_ALERT#
A16	SATA0_TX+	B16	SATA1_TX+
A17	SATA0_TX-	B17	SATA1_TX-
A18	SUS_S4#	B18	SUS_STAT#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND (FIXED)	B21	GND (FIXED)
A22	SATA2_TX+	B22	SATA3_TX+
A23	SATA2_TX-	B23	SATA3_TX-
A24	SUS_S5#	B24	PWR_OK
A25	SATA2_RX+	B25	SATA3_RX+
A26	SATA2_RX-	B26	SATA3_RX-
A27	BATLOW#	B27	WDT
A28	ATA_ACT#	B28	AC_SDIN2(NC)
A29	AC_SYNC	B29	AC_SDIN1
A30	AC_RST#	B30	AC_SDIN0
A31	GND (FIXED)	B31	GND (FIXED)
A32	AC_BITCLK	B32	SPKR
A33	AC_SDOOUT	B33	I2C_CK

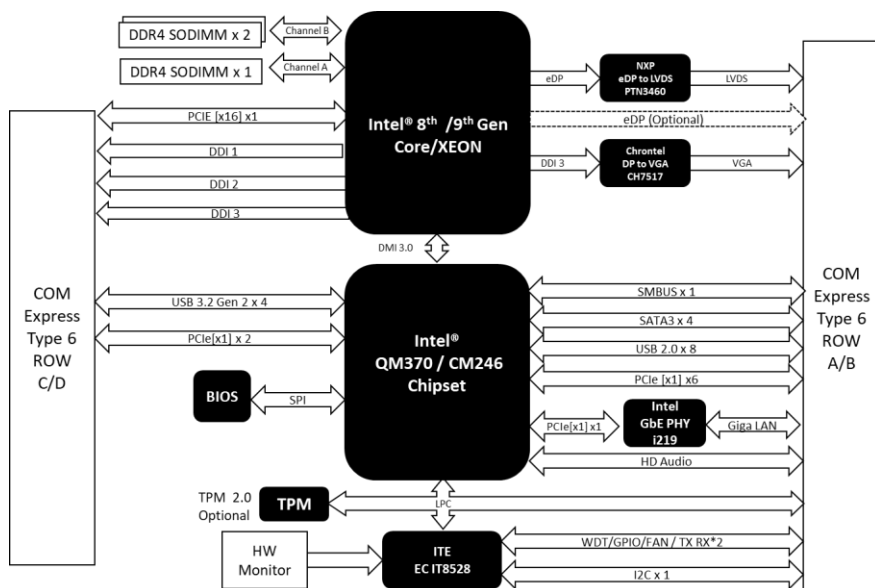
Row A		Row B	
Pin	Signal	Pin	Signal
A34	BIOS_DIS0#	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	USB6-	B36	USB7-
A37	USB6+	B37	USB7+
A38	USB_6_7_OC#	B38	USB_4_5_OC#
A39	USB4-	B39	USB5-
A40	USB4+	B40	USB5+
A41	GND (FIXED)	B41	GND (FIXED)
A42	USB2-	B42	USB3-
A43	USB2+	B43	USB3+
A44	USB_2_3_OC#	B44	USB_0_1_OC#
A45	USB0-	B45	USB1-
A46	USB0+	B46	USB1+
A47	VCC_RTC	B47	EXCD1_PERST#
A48	EXCD0_PERST#	B48	EXCD1_CPPE#
A49	EXCD0_CPPE#	B49	SYS_RESET#
A50	LPC_SERIRQ	B50	CB_RESET#
A51	GND (FIXED)	B51	GND (FIXED)
A52	PCIE_TX5+	B52	PCIE_RX5+
A53	PCIE_TX5-	B53	PCIE_RX5-
A54	GPIO	B54	GPO1
A55	PCIE_TX4+	B55	PCIE_RX4+
A56	PCIE_TX4-	B56	PCIE_RX4-
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+

Row A		Row B	
Pin	Signal	Pin	Signal
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND (FIXED)	B60	GND (FIXED)
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND (FIXED)	B70	GND (FIXED)
A71	LVDS_A0+	B71	LVDS_B0+
A72	LVDS_A0-	B72	LVDS_B0-
A73	LVDS_A1+	B73	LVDS_B1+
A74	LVDS_A1-	B74	LVDS_B1-
A75	LVDS_A2+	B75	LVDS_B2+
A76	LVDS_A2-	B76	LVDS_B2-
A77	LVDS_VDD_EN	B77	LVDS_B3+
A78	LVDS_A3+	B78	LVDS_B3-
A79	LVDS_A3-	B79	LVDS_BKLT_EN
A80	GND (FIXED)	B80	GND (FIXED)
A81	LVDS_A_CK+	B81	LVDS_B_CK+
A82	LVDS_A_CK-	B82	LVDS_B_CK-
A83	LVDS_I2C_CK	B83	LVDS_BKLT_CTRL

Row A		Row B	
Pin	Signal	Pin	Signal
A84	LVDS_I2C_DAT	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	RSVD	B86	VCC_5V_SBY
A87	RSVD	B87	VCC_5V_SBY
A88	PCIE0_CK_REF+	B88	BISO_DIS1#
A89	PCIE0_CK_REF-	B89	VGA_RED
A90	GND (FIXED)	B90	GND (FIXED)
A91	SPI_POWER	B91	VGA_GRN
A92	SPI_MISO	B92	VGA_BLU
A93	GPO0	B93	VGA_HSYNC
A94	SPI_CLK	B94	VGA_VSYNC
A95	SPI_MOSI	B95	VGA_I2C_CK
A96	TPM_PP	B96	VGA_I2C_DAT
A97	TYPE10#(NC)	B97	SPI_CS#
A98	SER0_TX	B98	RSVD
A99	SER0_RX	B99	RSVD
A100	GND (FIXED)	B100	GND (FIXED)
A101	SER1_TX	B101	FAN_PWNOUT
A102	SER1_RX	B102	FAN_TACHIN
A103	LID#	B103	SLEEP#
A104	VCC_12V	B104	VCC_12V
A105	VCC_12V	B105	VCC_12V
A106	VCC_12V	B106	VCC_12V
A107	VCC_12V	B107	VCC_12V
A108	VCC_12V	B108	VCC_12V

Row A		Row B	
Pin	Signal	Pin	Signal
A109	VCC_12V	B109	VCC_12V
A110	GND (FIXED)	B110	GND (FIXED)

2.4 Block Diagram



Chapter 3

AMI BIOS Setup

3.1 System Test and Initialization

The board uses certain routines to test and initialize board hardware. If the routines encounter an error during the tests, you will either hear a few short beeps or see an error message on the screen. There are two kinds of errors: fatal and non-fatal. The system can usually continue the boot up sequence with non-fatal errors.

System configuration verification routines check the current system configuration stored in the CMOS memory and BIOS NVRAM. If a system configuration is not found or a system configuration data error is detected, the system will load the optimized default and re-boot with this default system configuration automatically.

There are four situations in which you will need to setup system configuration:

- You are starting your system for the first time.
- You have changed the hardware attached to your system.
- The system configuration is reset by Clear-CMOS jumper.
- The CMOS memory has lost power and the configuration information has been erased.

The COM-CFHB6 CMOS memory has an integral lithium battery backup for data retention. You will need to replace the complete unit when it runs down.

3.2 AMI BIOS Setup

The AMI BIOS ROM has a built-in Setup program that allows users to modify the basic system configuration. This information is stored in the battery-backed CMOS RAM and BIOS NVRAM so it retains the Setup information when the power is turned off.

To enter Setup, power on the computer and press or <ESC> immediately.

The function of each interface is as follows:

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

Advanced – Advanced configuration options including display, system, and AAEON features.

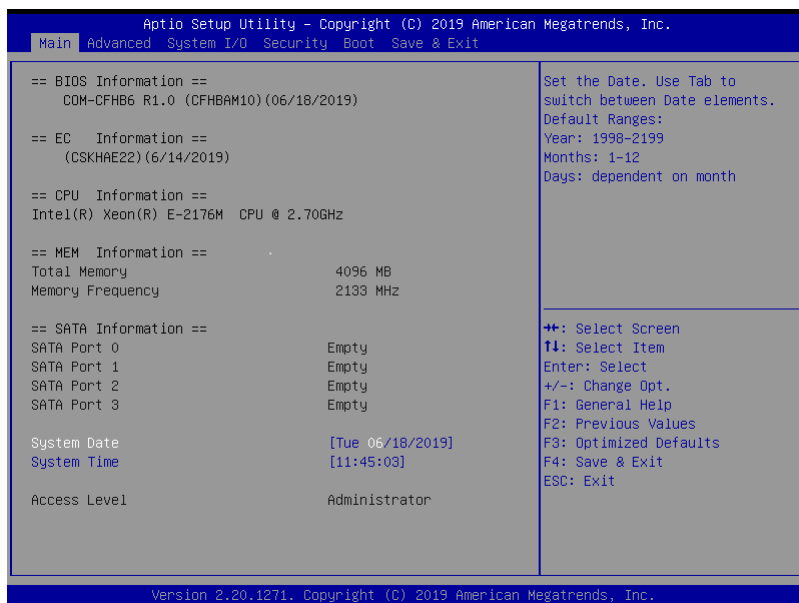
System I/O – Manage I/O port settings and configurations.

Security – Administrator password, Trusted Computing, and Secure Boot can be setup and configured here.

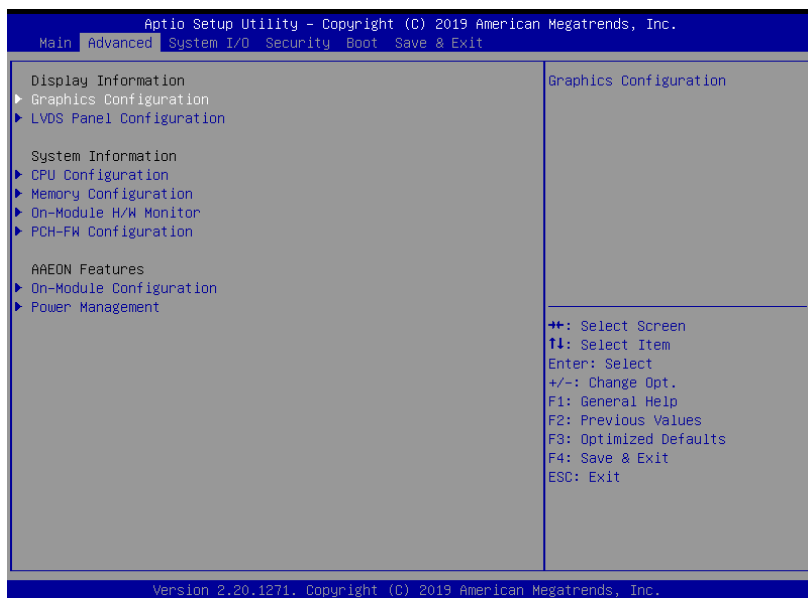
Boot – Boot options including Quiet Boot, PXE Boot, and Boot Priority.

Save & Exit – Save changes and exit Setup.

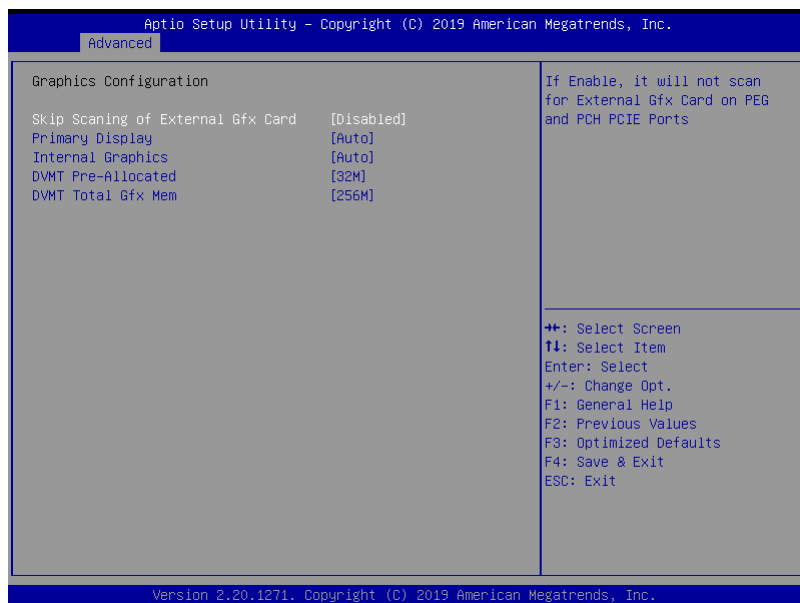
3.3 Setup submenu: Main



3.4 Setup submenu: Advanced



3.4.1 Advanced: Graphics Configuration

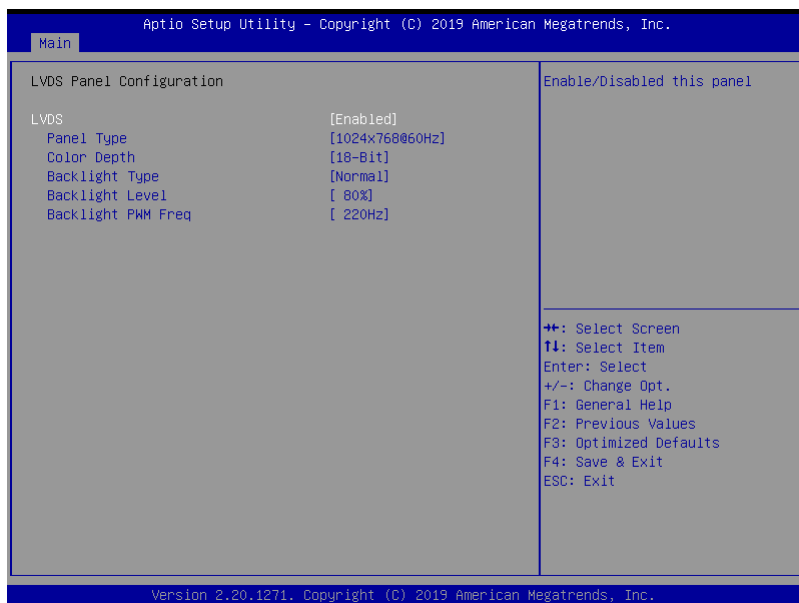


Options Summary		
Skip Scanning of External Gfx Card	Disabled	Optimal Default, Failsafe Default
	Enabled	
If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports		
Primary Display	Auto	Optimal Default, Failsafe Default
	IGFX	
	PEG	
	PCI	
Select which of IGFX/ PEG/ PCI Graphics device should be Primary Display Or select SG for Switchable Gfx.		
Internal Graphics	Auto	Optimal Default, Failsafe Default
	Disabled	
	Enabled	

Table Continues on Next Page

Options Summary		
DVMT Pre-Allocated	0M	
	32M	Optimal Default, Failsafe Default
	64M	
	4M	
	8M	
	12M	
	16M	
	20M	
	24M	
	28M	
	32M/F7	
	36M	
	40M	
	44M	
	48M	
	52M	
	56M	
	60M	
Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.		
DVMT Total Gfx Mem	128M	
	256M	Optimal Default, Failsafe Default
	MAX	
Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.		

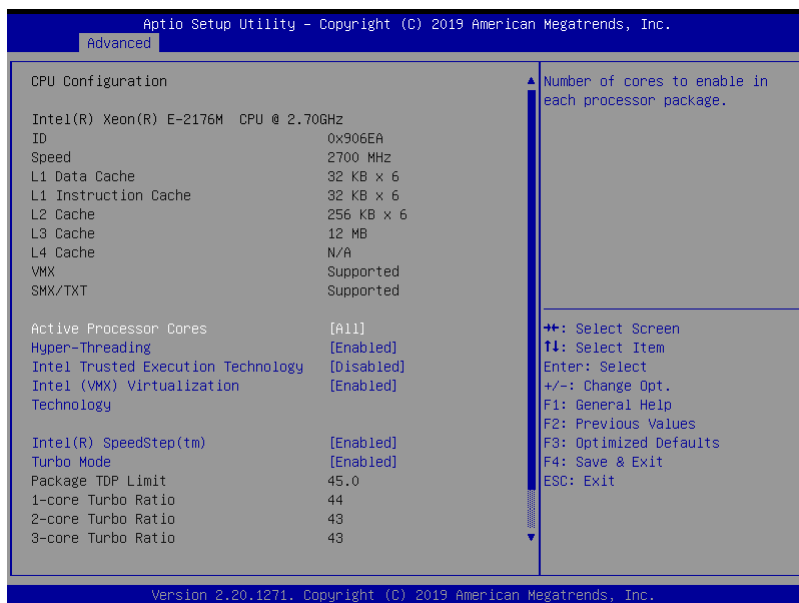
3.4.2 Advanced: LVDS Panel Configuration



Options Summary		
LVDS	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enabled/ Disabled this panel		
Panel Type	640x480@60Hz	
	800x480@60Hz	
	800x600@60Hz	
	1024x600@60Hz	
	1024x768@60Hz	Optimal Default, Failsafe Default
	1280x768@60Hz	
	1280x800@60Hz	
	1280x1024@60Hz	
	1366x768@60Hz	
	1440x900@60Hz	
	1600x1200@60Hz	
	1920x1080@60Hz	
	1920x1200@60Hz	
Select panel type		

Options Summary		
Color Depth	18-bit	Optimal Default, Failsafe Default
	24-bit	
Select Color Depth		
Backlight Type	Normal	Optimal Default, Failsafe Default
	Inverted	
Select backlight control signal type		
Backlight Level	0%	
	10%	
	20%	
	30%	
	40%	
	50%	
	60%	
	70%	
	80%	Optimal Default, Failsafe Default
	90%	
	100%	
Select backlight control level		
Backlight PWM Freq	100Hz	
	200Hz	
	220Hz	Optimal Default, Failsafe Default
	500Hz	
	1KHz	
	2.2KHz	
	6.5KHz	
Select PWM frequency of backlight control signal		

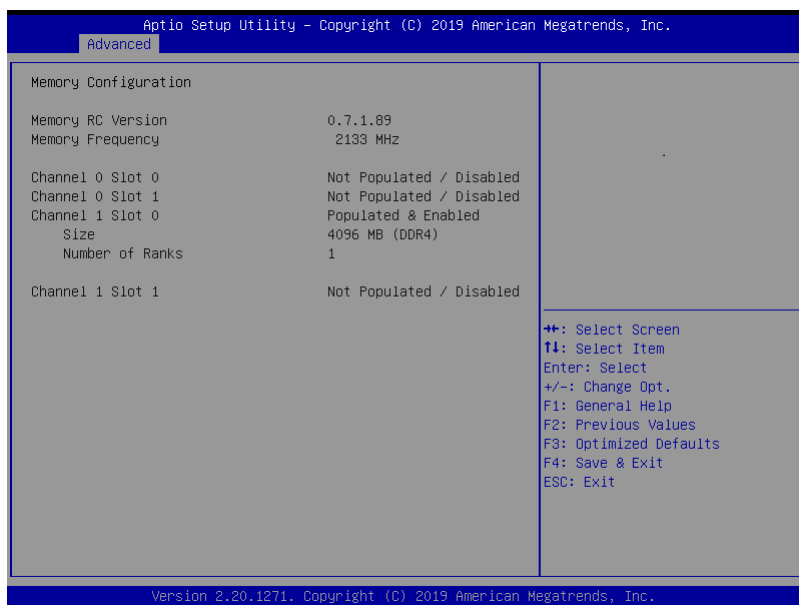
3.4.3 Advanced: CPU Configuration



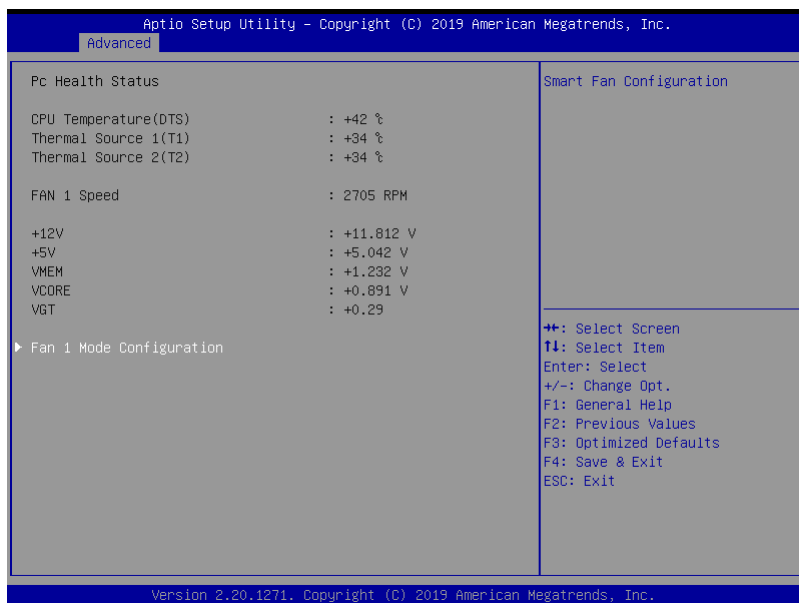
Options Summary		
Active Processor Cores	ALL	Optimal Default, Failsafe Default
	1	
	2	
	3	
	4	
	5	
Number of cores to enable in each processor package.		
Hyper-Threading	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enabled for Windows XP and Linux (OS optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology).		
Intel Trusted Execution Technology	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enable utilization of additional hardware capabilities provided by Intel Trusted Execution Technology.		
Changes require a full power cycle to take effect.		

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.		
Intel(R) SpeedStep(tm)	Disabled	
	Enabled	Optimal Default, Failsafe Default
Allows more than two frequency ranges to be supported.		
Turbo Mode	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable/ Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).		

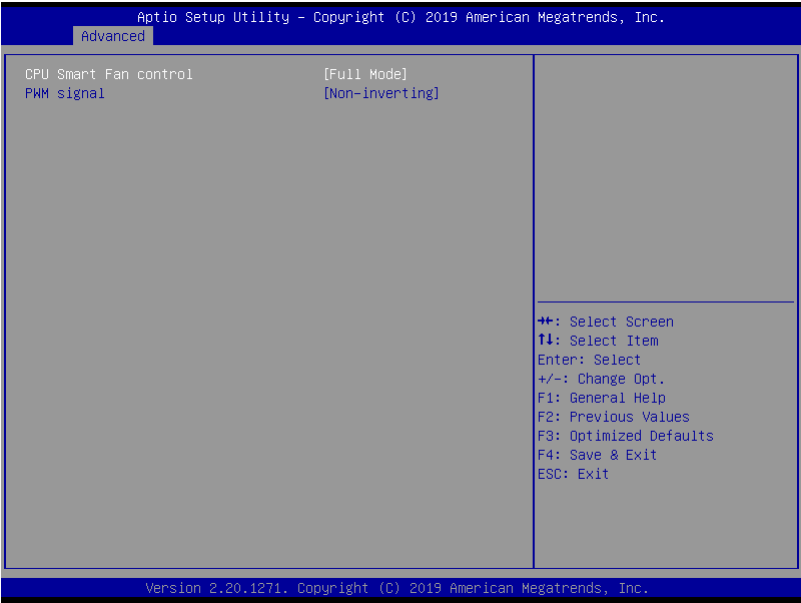
3.4.4 Advanced: Memory Configuration



3.4.5 Advanced: On-Module H/W Monitor



3.4.5.1 Fan 1 Mode Configuration



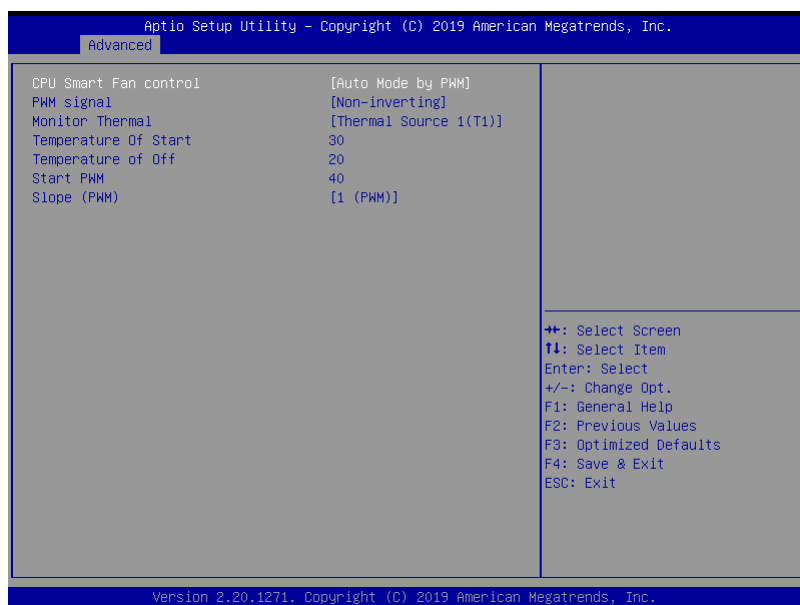
Options Summary		
CPU Smart Fan control	Full Mode	Optimal Default, Failsafe Default
	Manual Mode by PWM	
	Auto Mode by PWM	
PWM signal	Non-inverting	Optimal Default, Failsafe Default
	Inverting	
Select output PWM of inverting or non-uninverting signal		

3.4.5.2 CPU Smart Fan Control: Manual Mode by PWM



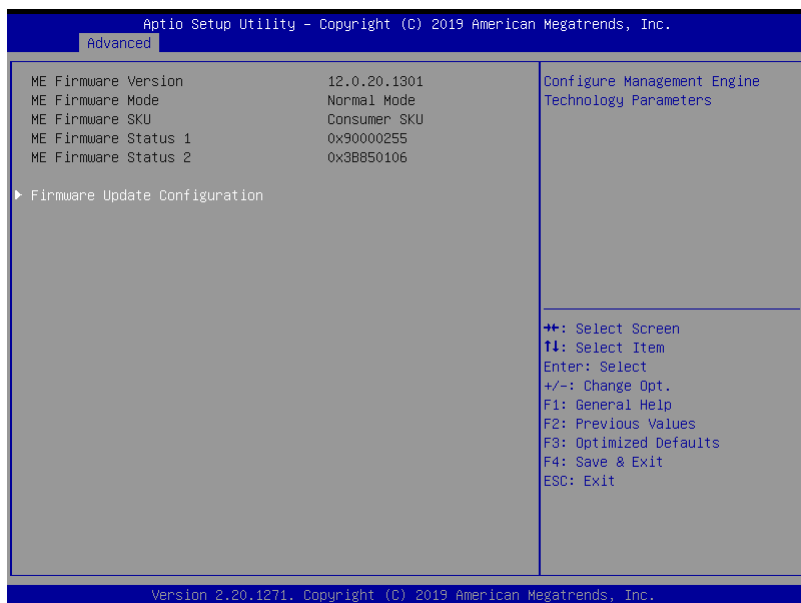
Options Summary		
Manual Setting	70	Optimal Default, Failsafe Default
Set Fan at fixed Duty-Cycle Min=0 Max=100 Please input Dec number:		

3.4.5.3 CPU Smart Fan Control: Auto Mode by PWM



Options Summary		
Monitor Thermal	Thermal Source 1(T1)	Optimal Default, Failsafe Default
	Thermal Source 2(T2)	
Select monitor thermal source		
Temperature of Start	30	Optimal Default, Failsafe Default
Temperature Of Start		
Temperature Of Off	20	Optimal Default, Failsafe Default
Temperature Of Off		
Start PWM	40	Optimal Default, Failsafe Default
Start PWM		
Slope (PWM)	0 (PWM)	
	1 (PWM)	Optimal Default, Failsafe Default
	2 (PWM)	
	4 (PWM)	
	8 (PWM)	
	16 (PWM)	
	32 (PWM)	
	64 (PWM)	
Slope (PWM)		

3.4.6 Advanced: PCH-FW Configuration



3.4.6.1 Firmware Update Configuration



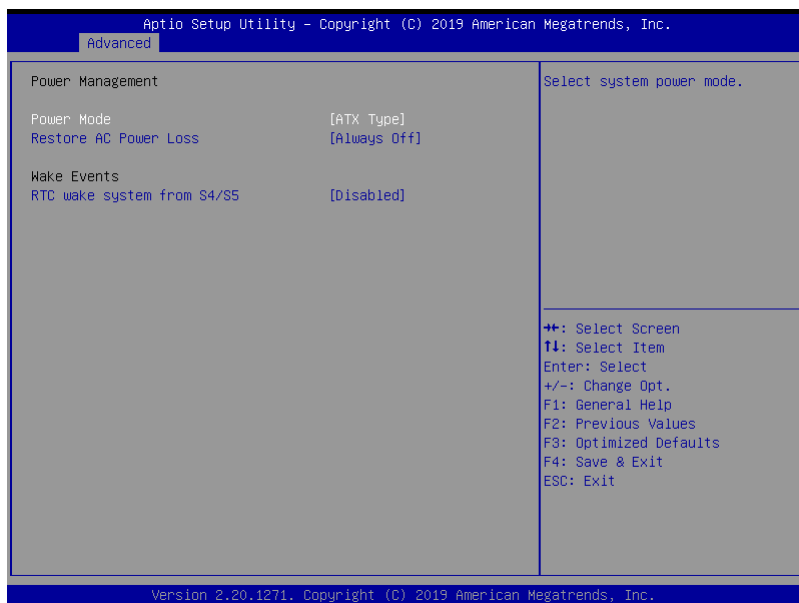
Options Summary		
Me FW Image Re-Flash	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled /Disabled Me FW Image Re-Flash function.		
Local FW Update	Disabled	
	Enabled	Optimal Default, Failsafe Default
Options for Local FW Update function.		

3.4.7 Advanced: On-Module Configuration



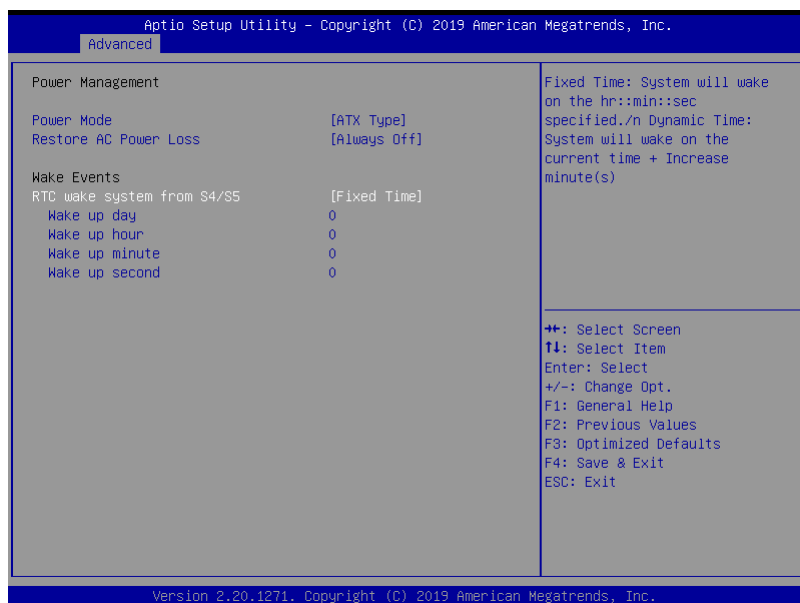
Options Summary		
Battery Management	Disabled	Optimal Default, Failsafe Default
	One Battery	
Enabled to support battery in ACPI OS by I2C_CK , I2C_DAT (B33,B34)		
EC-SMB-HC Support	Disabled	Optimal Default, Failsafe Default
	Enabled	
SMBus Host Controller Interface via Embedded Controller.		

3.4.8 Advanced: 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
IO Restore AC Power Loss		
RTC wake system from S4/S5	Disabled	Optimal Default, Failsafe Default
	Fixed Time	
Fixed Time: System will wake on the hr::min::sec specified.		
Dynamic time: System will wake on the current time + Increase minute(s)		

3.4.8.1 RTC Wake System from S4/S5: Fixed Time

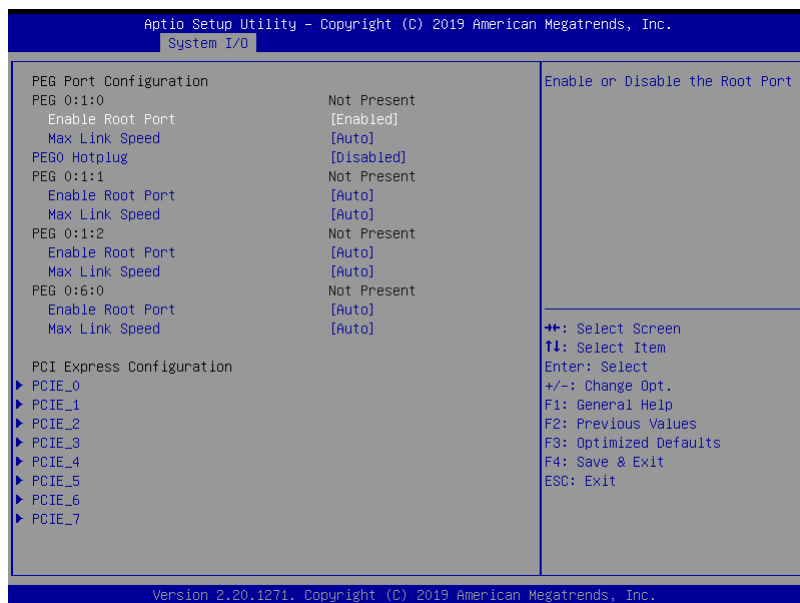


Options Summary		
Wake up day	0	Optimal Default, Failsafe Default
Select 0 for daily system wake up ,1-31 for which day of the month that you would like the system to work up		
Wake up hour	0	Optimal Default, Failsafe Default
Select 0-23 For example enter 3 for 3am and 15 for 3pm		
Wake up minute	0	Optimal Default, Failsafe Default
Select minute: 0-59		
Wake up second	0	Optimal Default, Failsafe Default
Select second: 0-59		

3.5 Setup submenu: System I/O



3.5.1 System I/O: PCI Express Configuration

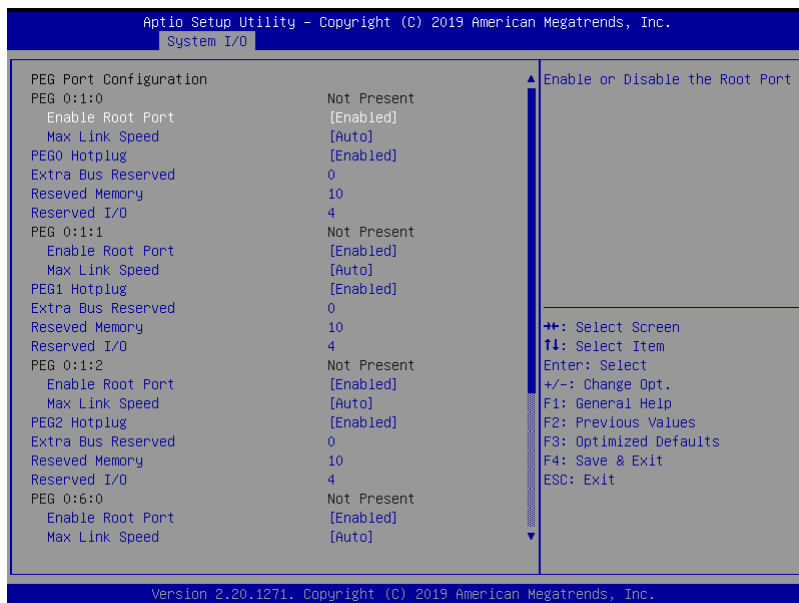


Options Summary		
PEG 0:1:0 Enable Root Port	Disabled	
	Enabled	Optimal Default, Failsafe Default
	Auto	
Enabled or Disabled the Root Port		
PEG 0:1:0 Max Link Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
Configure PEG 0:1:0 Max Speed		
PEG 0:1:0 - PEG0 Hotplug	Disabled	Optimal Default, Failsafe Default
	Enabled	
PCI Express Hot Plug Enabled/ Disabled		
PEG 0:1:1 Enable Root Port	Disabled	
	Enabled	
	Auto	Optimal Default, Failsafe Default
Enabled or Disabled the Root Port		

Options Summary		
PEG 0:1:1 Max Link Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
Configure PEG 0:1:1 Max Speed		
PEG 0:1:2 Enable Root Port	Disabled	
	Enabled	
	Auto	Optimal Default, Failsafe Default
Enabled or Disabled the Root Port		
PEG 0:1:2 Max Link Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
Configure PEG 0:1:2 Max Speed		
PEG 0:6:0 Enable Root Port	Disabled	
	Enabled	
	Auto	Optimal Default, Failsafe Default
Enabled or Disabled the Root Port		
PEG 0:6:0 Max Link Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
Configure PEG 0:6:0 Max Speed		

3.5.1.1 PCI Express Configuration: PEG* Hotplug Enabled

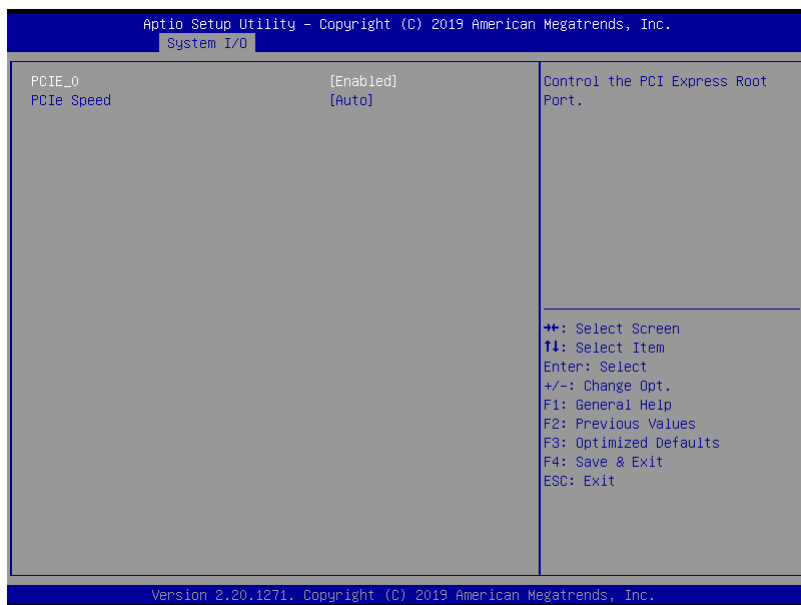
This is the menu and options available if both “Enable Root Port” and “PEG* Hotplug” options are both set to “Enabled”



Options Summary

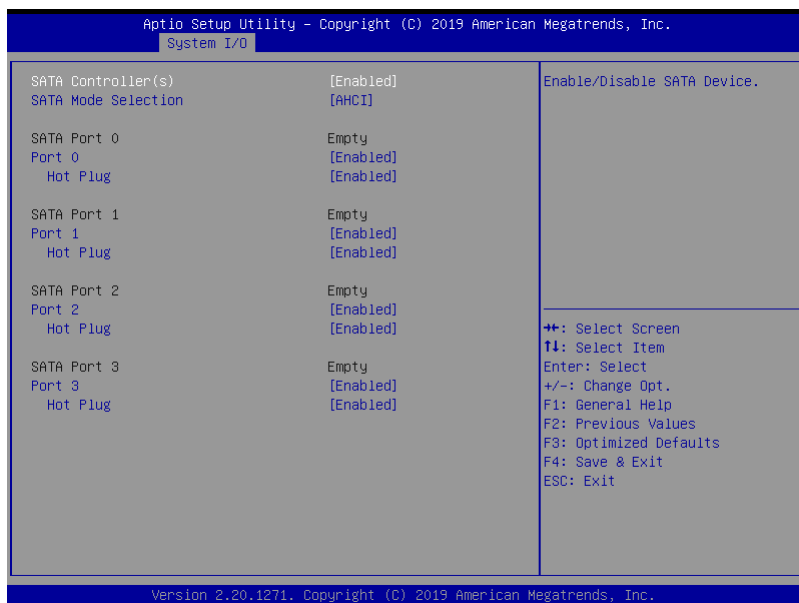
Extra Bus Reserved	0	Optimal Default, Failsafe Default
Extra Bus Reserved (0-7) for bridges behind this Root Bridge.		
Reserved Memory	10	Optimal Default, Failsafe Default
Reserved Memory for this Root Bridge (1-4096) MB		
Reserved I/O	4	Optimal Default, Failsafe Default
Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.		

3.5.1.2 PCI Express Configuration: PCIE_0 – PCIE_7 Submenus



Options Summary		
PCIE_0~PCIE_7	Disabled	
	Enabled	Optimal Default, Failsafe Default
Control the PCI Express Root Port.		
PCle Speed	Auto	Optimal Default, Failsafe Default
	Gen1	
	Gen2	
	Gen3	
Configure PCIe Speed		

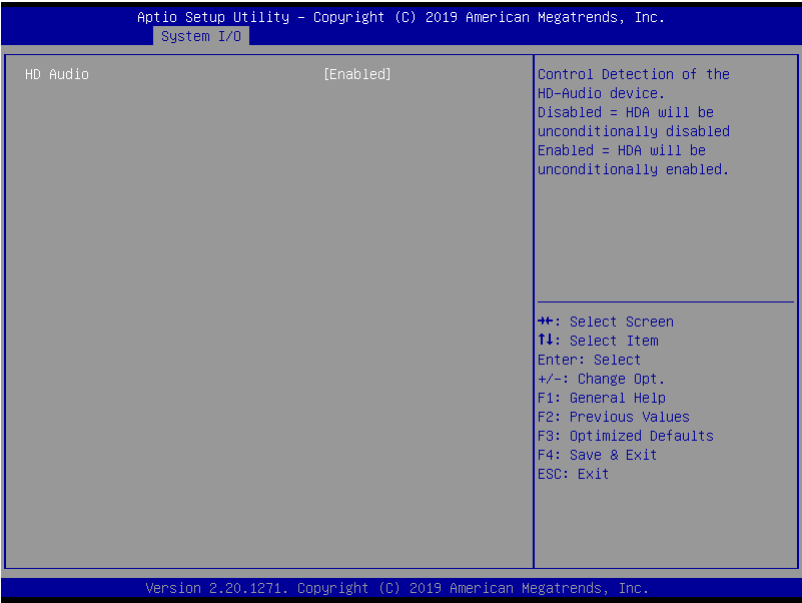
3.5.2 System I/O: SATA Configuration



Options Summary		
SATA Controller(s)	Enabled	Optimal Default, Failsafe Default
	Disabled	
Enable/Disable SATA Device.		
SATA Mode Selection	AHCI	Optimal Default, Failsafe Default
	Intel RST Premium with Intel Option System Acceleration	
Determines how SATA controller(s) operate.		
Port 0	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable SATA Port.		
Hot Plug	Disabled	
	Enabled	Optimal Default, Failsafe Default
Designates this port as Hot Pluggable.		
Port 1	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable SATA Port.		

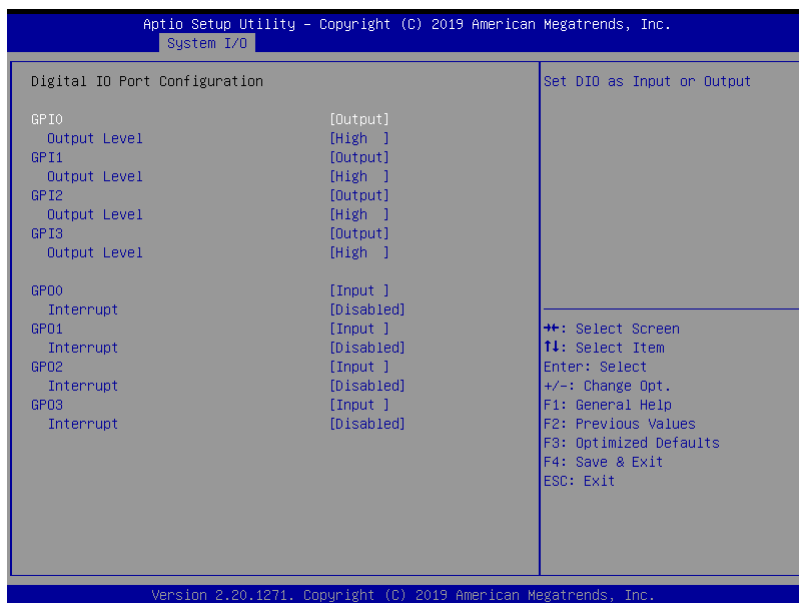
Options Summary		
Hot Plug	Disabled	
	Enabled	Optimal Default, Failsafe Default
Designates this port as Hot Pluggable.		
Port 2	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable SATA Port.		
Hot Plug	Disabled	
	Enabled	Optimal Default, Failsafe Default
Designates this port as Hot Pluggable.		
Port 3	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enable or Disable SATA Port.		
Hot Plug	Disabled	
	Enabled	Optimal Default, Failsafe Default
Designates this port as Hot Pluggable.		

3.5.3 System I/O: HD Audio Configuration



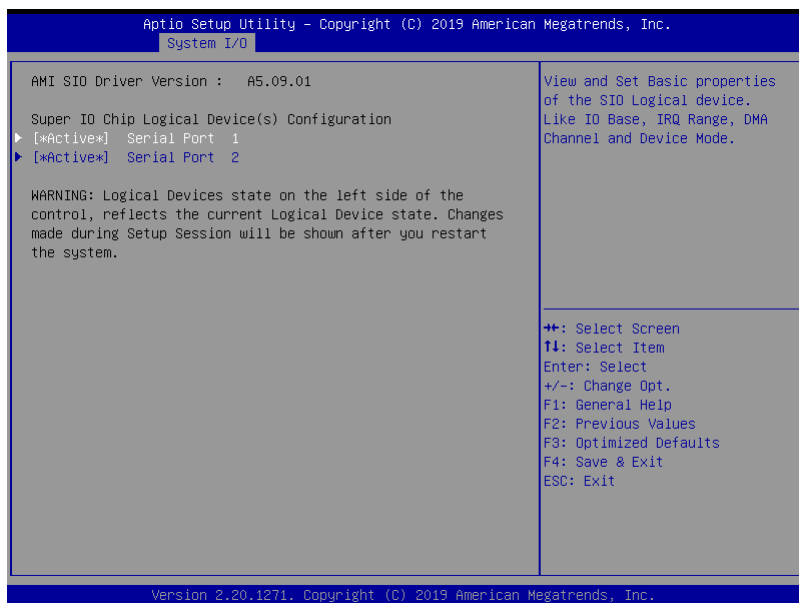
Options Summary		
HD Audio	Disabled	
	Enabled	Optimal Default, Failsafe Default
Control Detection of the HD-Audio device. Disabled = HAD will be unconditionally disable Enabled = HAD will be unconditionally enable.		

3.5.4 System I/O: Digital IO Port Configuration

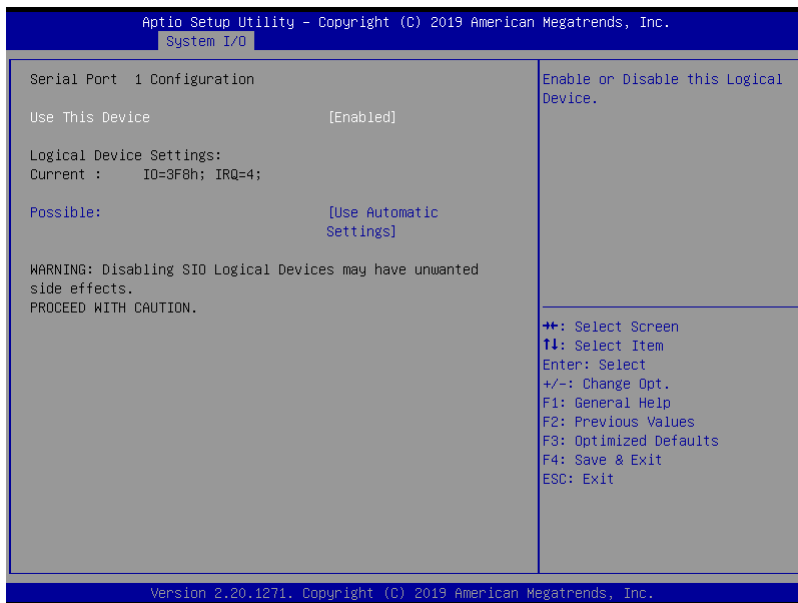


Options Summary		
GPI *	Input	
	Output	Optimal Default, Failsafe Default
Set DIO as Input or Output		
Output Level	High	Optimal Default, Failsafe Default
	Low	
Set output level when DIO pin is output		
GPO *	Input	Optimal Default, Failsafe Default
	Output	
Set DIO as Input or Output		
Interrupt	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enabled interrupt function with low pulse mode. This triggered pulse needs more than 10ms.		

3.5.5 System I/O: Legacy Logical Devices Configuration

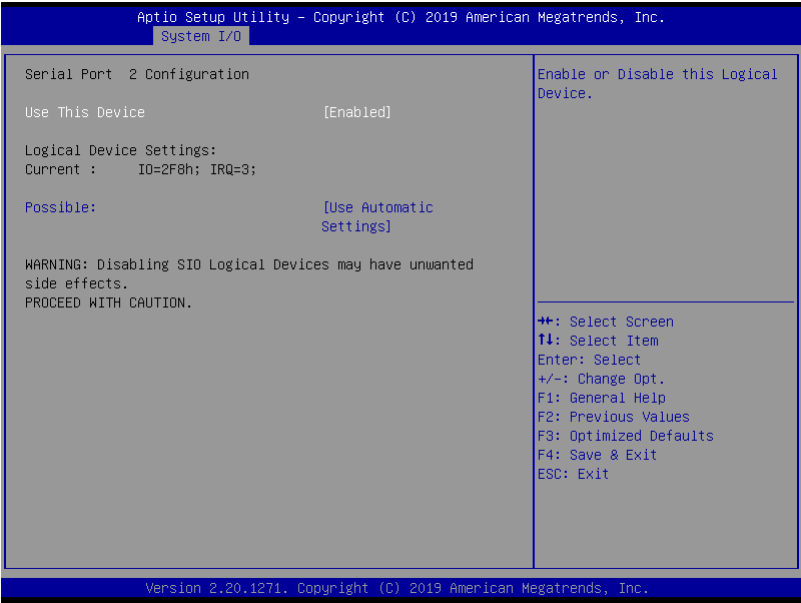


3.5.5.1 [*Active*] Serial Port 1



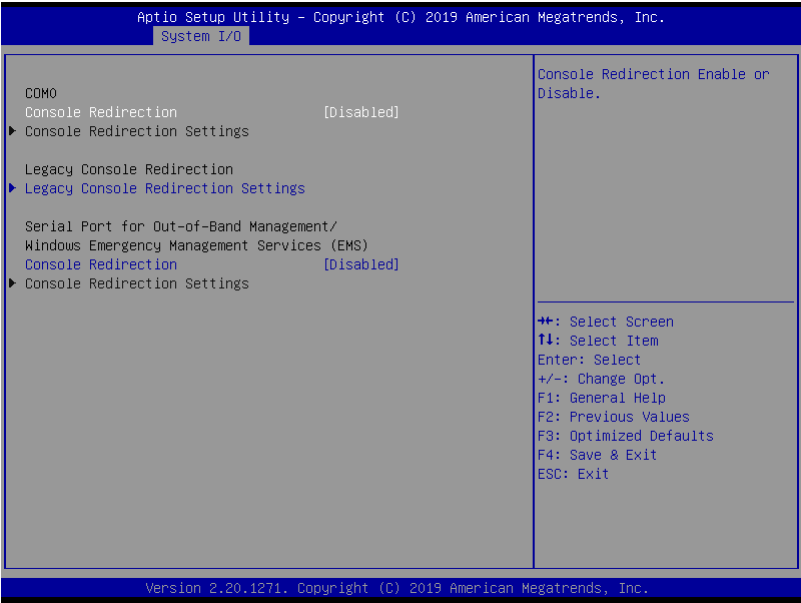
Options Summary		
Use This Device	Disable	
	Enable	Optimal Default, Failsafe Default
Enable or Disable this Logical Device.		
Possible	Use Automatic Setting	Optimal Default, Failsafe Default
	IO=3F8h; IRQ=4 ; DMA;	
	IO=2C8h; IRQ=11 ; DMA;	
Allows the user to change the device resource settings. New settings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

3.5.5.2 [*Active*] Serial Port 2



Options Summary		
Use This Device	Disable	
	Enable	Optimal Default, Failsafe Default
Enable or Disable this Logical Device.		
Possible	Use Automatic Setting	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 System I/O: Serial Port Console Redirection



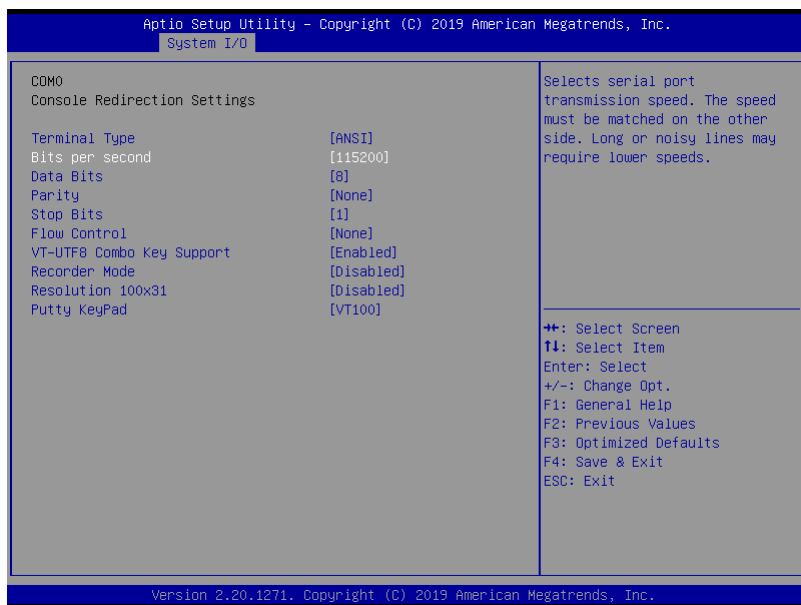
Options Summary		
COM0 : Console Redirection	Disable	Optimal Default, Failsafe Default
	Enable	
Console Redirection Enable or Disable		
Out-of-Band Management: Console Redirection	Disable	Optimal Default, Failsafe Default
	Enable	
Console Redirection Enable or Disable		

3.5.6.1 Legacy Console Redirection Settings



Options Summary		
Redirection COM Port	COM0	Optimal Default, Failsafe Default
Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages		
Resolution	80x24	Optimal Default, Failsafe Default
	80x25	
On Legacy OS, the Number of Rows and Columns supported redirection		
Redirect After POST	Always Enable	Optimal Default, Failsafe Default
	BootLoader	
When Boot Loader is selected, then Legacy Console Redirection is disable before booting to legacy OS , When Always Enable is selected, then Legacy Console Redirection is enables for legacy OS. Default setting for this option is set to Always Enable.		

3.5.6.2 COM0 Console Redirection Settings



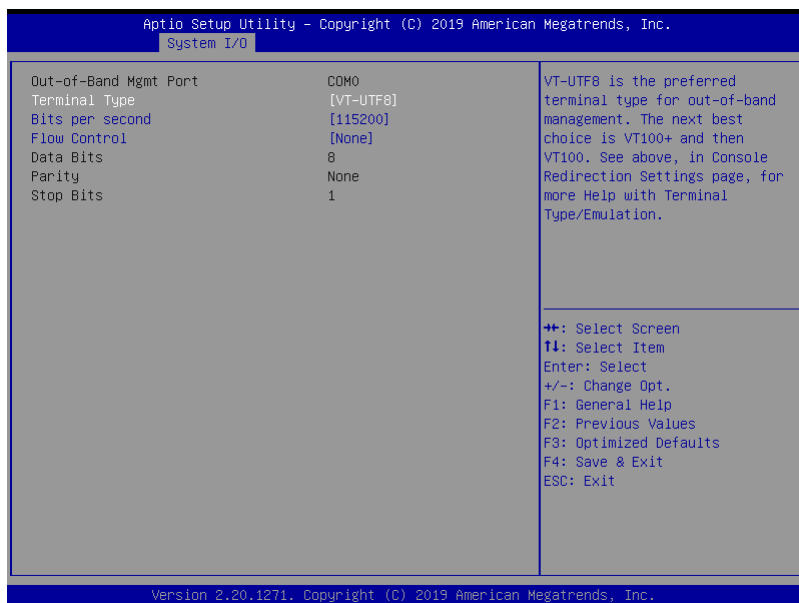
Options Summary		
Terminal Type	VT100	
	VT100+	
	VT-UTF8	
	ANSI	Optimal Default, Failsafe Default
Emulation:		
ANSI: Extended ASCII char set.		
VT100: ASCII char set.		
VT100+: Extends VT100 to support color, function keys, etc.		
VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.		
Bits per second	9600	
	19200	
	38400	
	57600	
	115200	Optimal Default, Failsafe Default
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.		

Options Summary		
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.		
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 form 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	Disable	
Key Support	Enable	Optimal Default, Failsafe Default
Enable VT-UTF8 Combo Key Support for ANSI/VT100 terminals.		
Recorder Mode	Disable	Optimal Default, Failsafe Default
	Enable	
With the mode enabled only text will be sent. This is to capture Terminal data.		
Resolution 100x31	Disable	Optimal Default, Failsafe Default
	Enable	
Enable or Disable extended terminal resolution.		

Table Continues on Next Page

Options Summary		
Putty KeyPad	VT100	Optimal Default, Failsafe Default
	LINUX	
	XTERMR6	
	SC0	
	ESCN	
	VT400	
Select FunctionKey and KeyPad on Putty.		

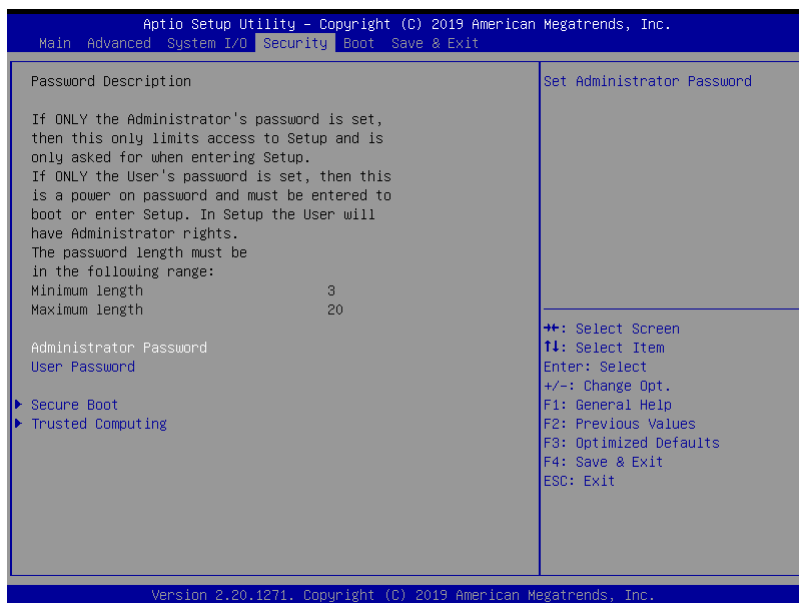
3.5.6.3 Out of Band Management



Options Summary		
Terminal Type	VT100	
	VT100+	
	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	9600	
	19200	
	38400	
	57600	
	115200	Optimal Default, Failsafe Default
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.		

Options Summary		
Flow Control	None	Optimal Default, Failsafe Default
	Hardware RTS/CTS	
	Software Xon/Xoff	
Flow Control can prevent data loss form 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 Administrator/User Password

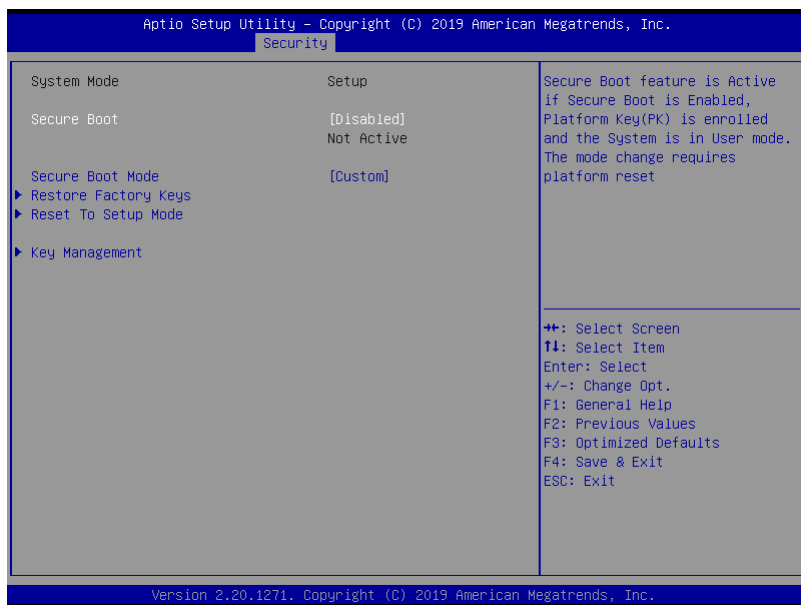
You can set an Administrator password. If you set an Administrator password, you can then set a User password. User passwords do not have access to many of the features in the Setup utility.

Select the password you want to set and press <Enter>. A dialog box will appear which lets you set the password. Passwords must be between 3 and 20 letters or numbers. Press <Enter> and re-enter the password into the next dialog box that appears. Press <Enter> after you have retyped it correctly. The password is required at boot time, or when the user enters the Setup utility.

Remove Password

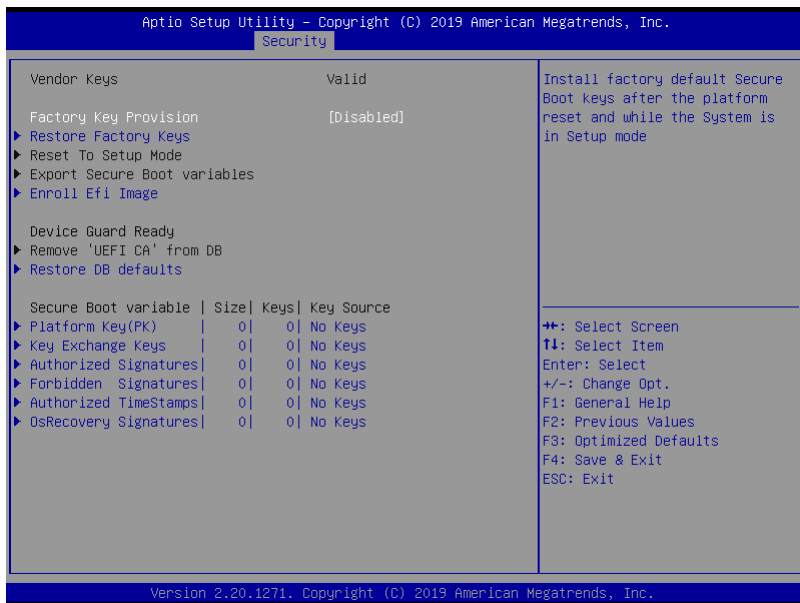
Highlight this item and type in the current password. At the next dialog box press <Enter> to disable password protection.

3.6.1 Security: 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	Standard	
	Custom	Optimal Default, Failsafe Default
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 database		
Reset To Setup Mode		
Delete all Secure Boot key database form NVRAM		

3.6.1.1 Secure Boot: Key Management



Options Summary		
Factory Key Provision	Disabled	Optimal Default, Failsafe Default
	Enabled	
Install factory default Secure Boot key 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 database		
Reset To Setup Mode		
Delete all Secure Boot key database form NVRAM		
Export Secure Boot variables		
Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device		
Enroll Efi Image		
Allow the image to run in Secure Boot mode.		
Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)		

Options Summary		
Remove 'UEFI CA' from DB		
Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature Database (db)		
Restore DB defaults		
Restore DB variable to factory defaults		
Platform Key(PK)	Details	
	Export	
	Update	
	Delete	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		
Key Exchange Keys	Details	
	Export	
	Update	
	Append	
	Delete	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		

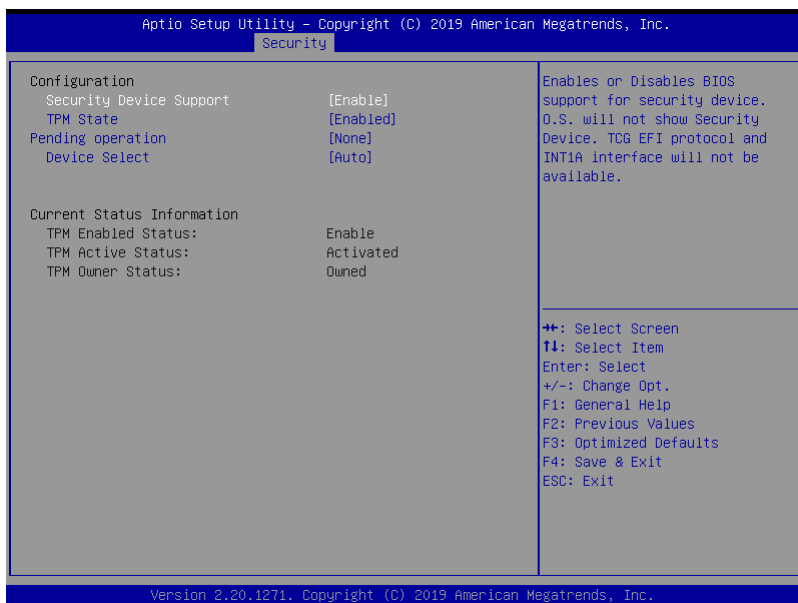
Table Continues on Next Page

Options Summary		
Authorized Signatures	Details	
	Export	
	Update	
	Append	
	Delete	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		
Forbidden Signatures	Details	
	Export	
	Update	
	Append	
	Delete	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		

Table Continues on Next Page

Options Summary		
Authorized TimeStamps	Update	
	Append	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		
OsRecovery Signatures	Update	
	Append	
Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate : a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed		

3.6.2 Security: Trusted Computing

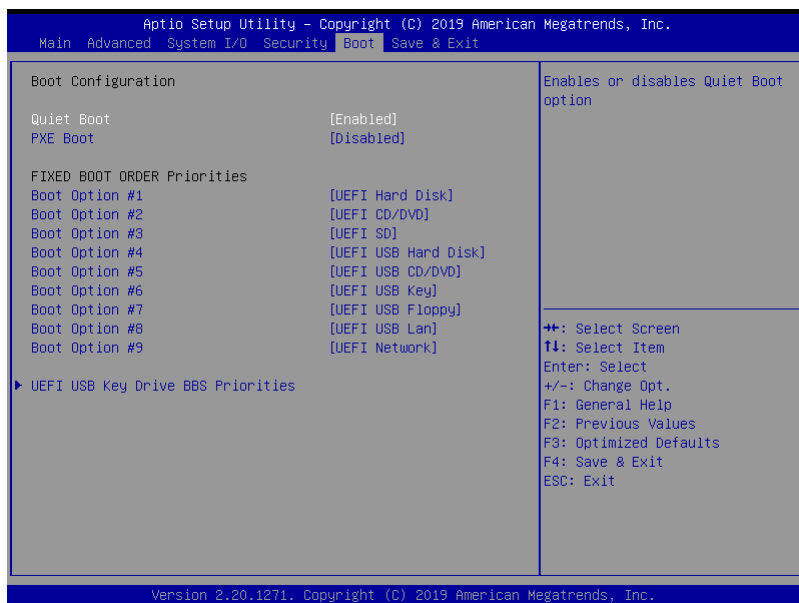


Options Summary		
Security Device Support	Disable	
	Enable	Optimal Default, Failsafe Default
Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.		
TPM State	Disable	
	Enable	Optimal Default, Failsafe Default
Enables/Disables Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.		
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.		

Table Continues on Next Page

Options Summary		
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 device will be enumerated.		

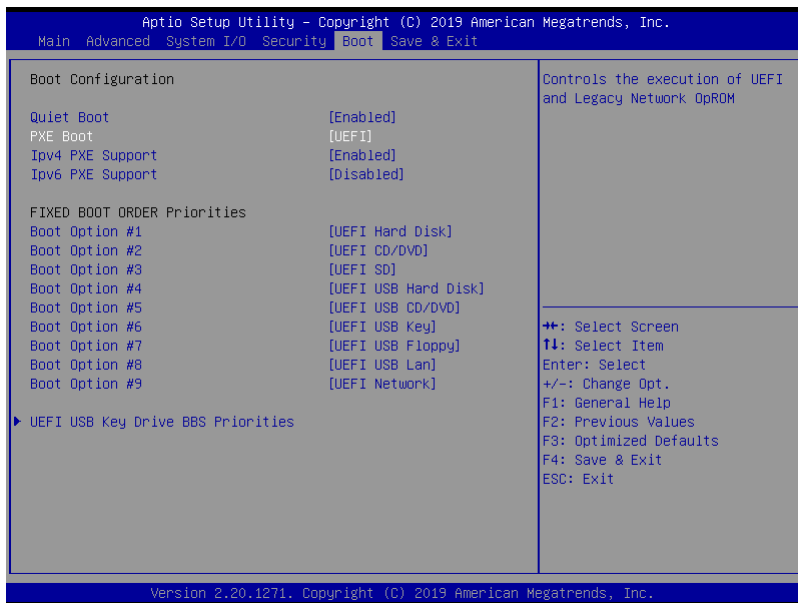
3.7 Setup submenu: Boot



Options Summary		
Quiet Boot	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enables or Disables Quiet Boot option.		
PXE Boot	Disabled	Optimal Default, Failsafe Default
	UEFI	
Controls the execution of UEFI and Legacy PXE OpROM.		

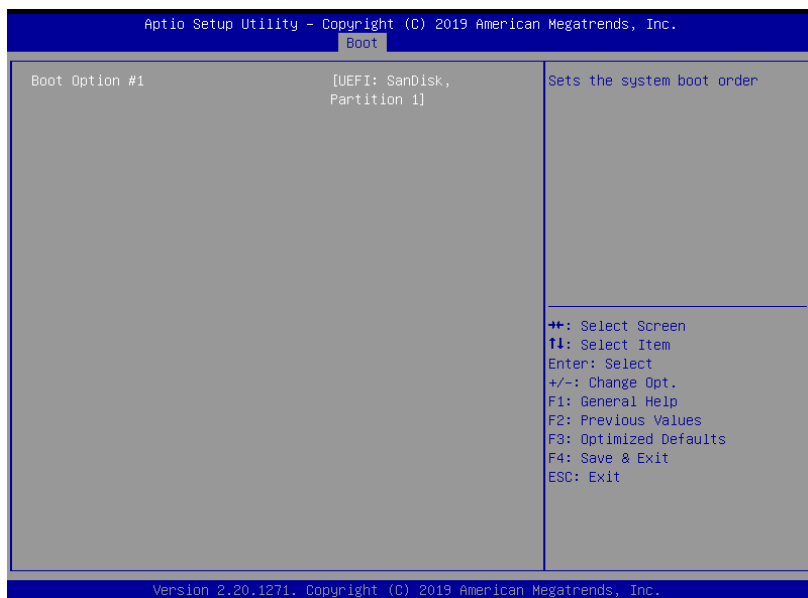
3.7.1 Boot: PXE Boot [UEFI] Settings

This is how the Boot submenu appears when PXE Boot is set to “[UEFI]”.

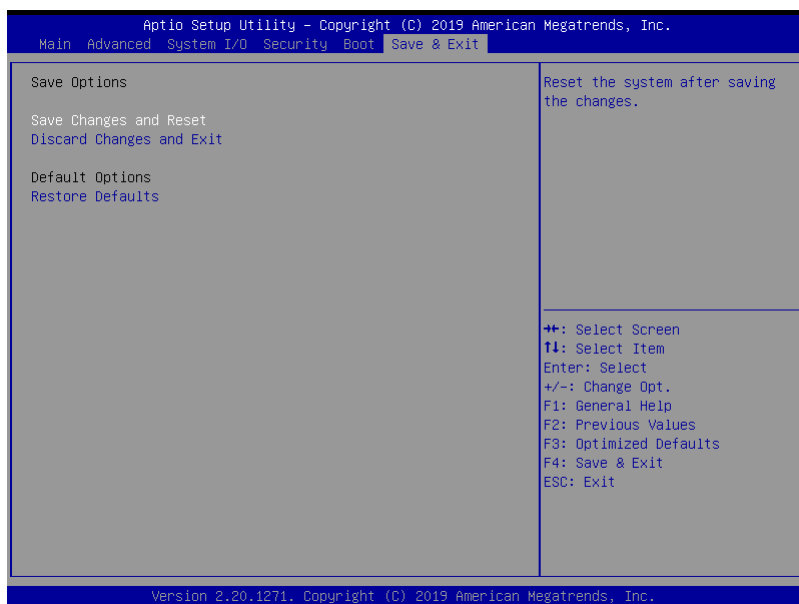


Options Summary		
Ipv4 PXE Support	Disabled	
	Enabled	Optimal Default, Failsafe Default
Enables / Disables Ipv4 PXE support. If disabled, Ipv4 PXE boot support will not be available.		
Ipv6 PXE Support	Disabled	Optimal Default, Failsafe Default
	Enabled	
Enables / Disables Ipv6 PXE support. If disabled, Ipv6 PXE boot support will not be available.		

3.7.2 Boot: UEFI USB Key Drive BBS Priorities



3.8 Setup submenu: Save & Exit



Chapter 4

Drivers Installation

4.1 Driver Download/Installation

Drivers for the COM-CFHB6 can be downloaded from the product page on the AAEON website by following this link:

<https://www.aaeon.com/en/p/com-express-modules-com-cfhb6>

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

Step 1 – Install Chipset Driver

1. Click the **Step1 - Chipset** folder followed by **SetupChipset.exe**
2. Follow the instructions
3. Drivers will be installed automatically

Step 2 – Install Graphics Driver

1. Click the **Step2 - Graphic** folder
2. Click the **igxpin.exe** file in the folder
3. Follow the instructions
4. Drivers will be installed automatically

Step 3 – Install LAN Driver

1. Click the **Step3 - Network** folder.
2. Click the **ProWinx64.exe** file in the folder.
3. Follow the instructions
4. Drivers will be installed automatically

Step 4 – Install Audio Driver

1. Click the **STEP4 - Audio** folder followed by **0006-64bit_Win7_Win8_Win81_Win10_R279.exe**
2. Follow the instructions
3. Drivers will be installed automatically

Appendix A

Watchdog Timer Programming

A.1 Watchdog Timer Initial Program

Table 1 : Embedded BRAM relative register table

	Default Value	Note
Index	0x284(Note1)	BRAM Index Register
Data	0x285(Note2)	BRAM Data Register
Logical Device Number	0xA8(Note3)	Watch dog Logical Device Number
Function and Device Number	0x00(Note4)	Watch dog Function/Device Number

Table 2 : Watchdog relative register table

	Option Register	BitNum	Value	Note
Timer Counter	0x00(Note5)		(Note10)	Time of watchdog timer (0~255)
Counting Unit	0x01(Note6)	0(Note7)	0(Note11)	Select time unit. 0: second 1: minute
Watchdog RST pulse width	0x01(Note8)	[3:2](Note9)	0(Note12)	0: 20ms 1: 60ms 2: 100ms 3: 250ms

```

*****
// Embedded BRAM relative definition (Please reference to Table 1)
#define byte EcBRAMIndex //This parameter is represented from Note1
#define byte EcBRAMData //This parameter is represented from Note2
#define byte BRAMLDRReg //This parameter is represented from Note3
#define byte BRAMFnDataReg //This parameter is represented from Note4
#define void EcBRAMWriteByte(byte Offset, byte Value);
#define byte EcBRAMReadByte(byte Offset);
#define void IOWriteByte(byte Offset, byte Value);
#define byte IOReadByte(byte Offset);
// Watch Dog relative definition (Please reference to Table 2)
#define byte TimerReg //This parameter is represented from Note5
#define byte TimerVal // This parameter is represented from Note10
#define byte UnitReg //This parameter is represented from Note6
#define byte UnitBit //This parameter is represented from Note7
#define byte UnitVal //This parameter is represented from Note11
#define byte RSTReg //This parameter is represented from Note8
#define byte RSTBit //This parameter is represented from Note9
#define byte RSTVal //This parameter is represented from Note12
*****

```

```
*****
VOID  Main(){
    // Procedure : AaeonWDTConfig
    // (byte)Timer : Time of WDT timer.(0x00~0xFF)
    // (boolean)Unit : Select time unit(0: second, 1: minute).
    AaeonWDTConfig();

    // Procedure : AaeonWDTEnable
    // This procedure will enable the WDT counting.
    AaeonWDTEnable();
}
*****
```

```

*****
// Procedure : AaeonWDTEnable
VOID  AaeonWDTEnable 0{
    WDTEnableDisable(1);
}

// Procedure : AaeonWDTConfig
VOID  AaeonWDTConfig 0{
    // Disable WDT counting
    WDTEnableDisable(0);
    // WDT relative parameter setting
    WDTParameterSetting();
}

VOID  WDTEnableDisable(byte Value){
    ECBRAMWriteByte(TimerReg , Value);
}

VOID  WDTParameterSetting0{
    Byte TempByte;

    // Watchdog Timer counter setting
    ECBRAMWriteByte(TimerReg , TimerVal);
    // WDT counting unit setting
    TempByte = ECBRAMReadByte(UnitReg);
    TempByte |= (UnitVal << UnitBit);
    ECBRAMWriteByte(UnitReg , TempByte);
    // WDT RST pulse width setting
    TempByte = ECBRAMReadByte(RSTReg);
    TempByte |= (RSTVal << RSTBit);
    ECBRAMWriteByte(RSTReg , TempByte);
}
*****

```

```
*****
```

```
VOID ECBRAMWriteByte(byte OPReg, byte OPBit, byte Value){
```

```
    IOWriteByte(EcBRAMIndex, 0x10);
```

```
    IOWriteByte(EcBRAMData, BRAMLDNReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x11);
```

```
    IOWriteByte(EcBRAMData, BRAMFnDataReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x13 + OPReg);
```

```
    IOWriteByte(EcBRAMData, Value);
```

```
    IOWriteByte(EcBRAMIndex, 0x12);
```

```
    IOWriteByte(EcBRAMData, 0x30);          //Write start
```

```
}
```

```
Byte ECBRAMReadByte(byte OPReg){
```

```
    IOWriteByte(EcBRAMIndex, 0x10);
```

```
    IOWriteByte(EcBRAMData, BRAMLDNReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x11);
```

```
    IOWriteByte(EcBRAMData, BRAMFnDataReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x12);
```

```
    IOWriteByte(EcBRAMData, 0x10);          //Read start
```

```
    IOWriteByte(EcBRAMIndex, 0x13 + OPReg);
```

```
    Return      IOReadByte(EcBRAMData, Value);
```

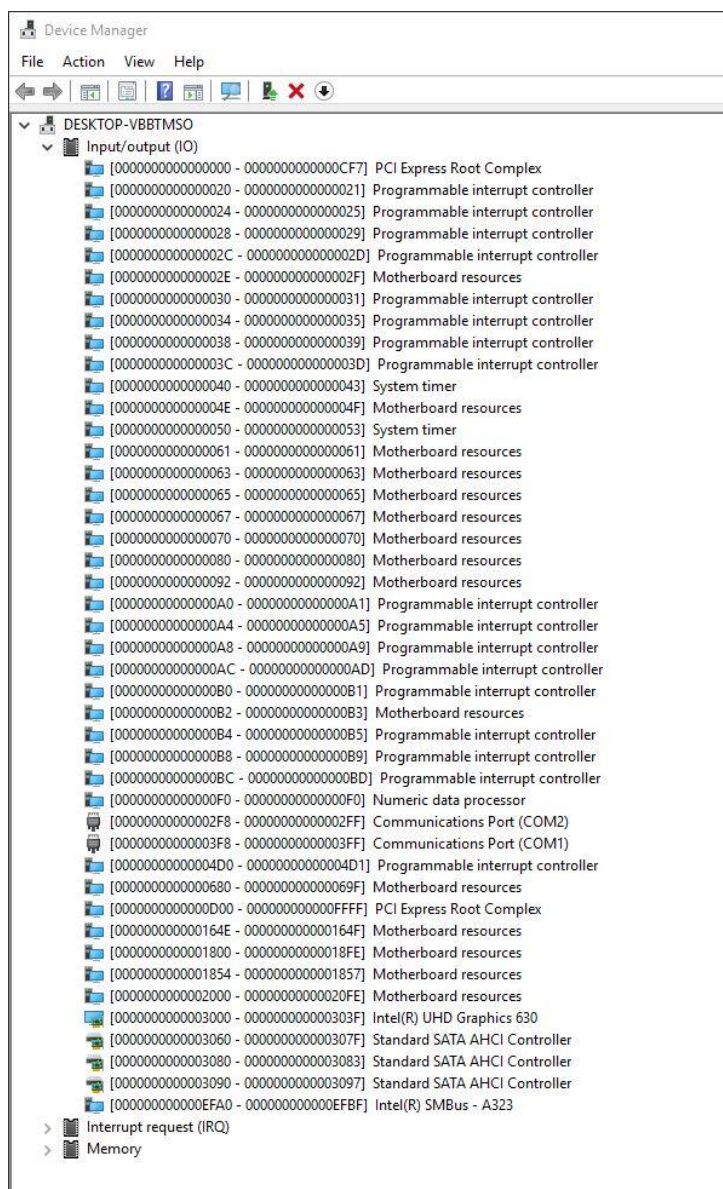
```
}
```

```
*****
```

Appendix B

I/O Information

B.1 I/O Address Map

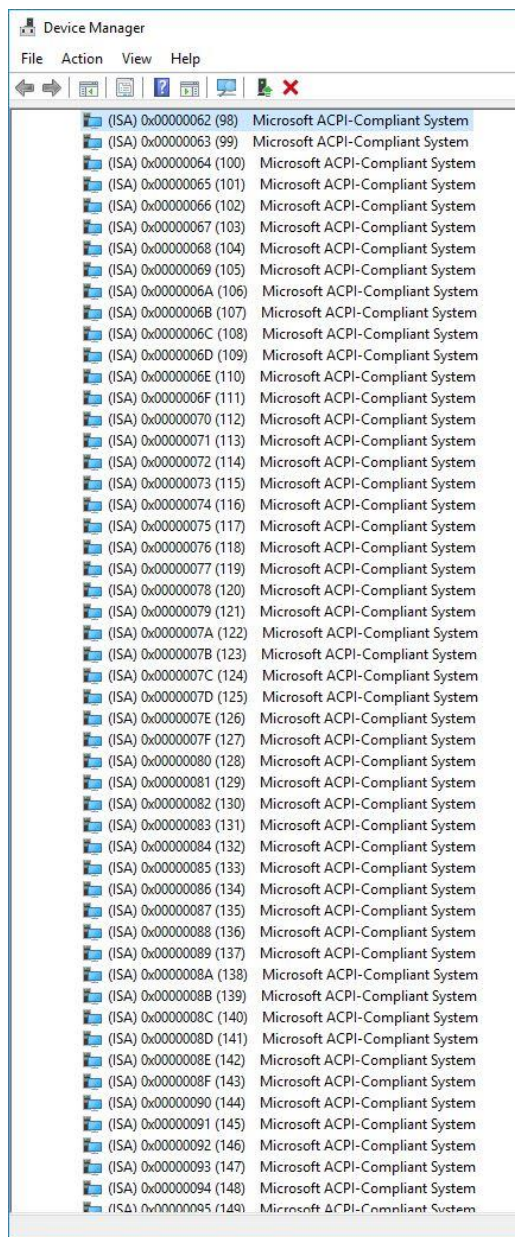


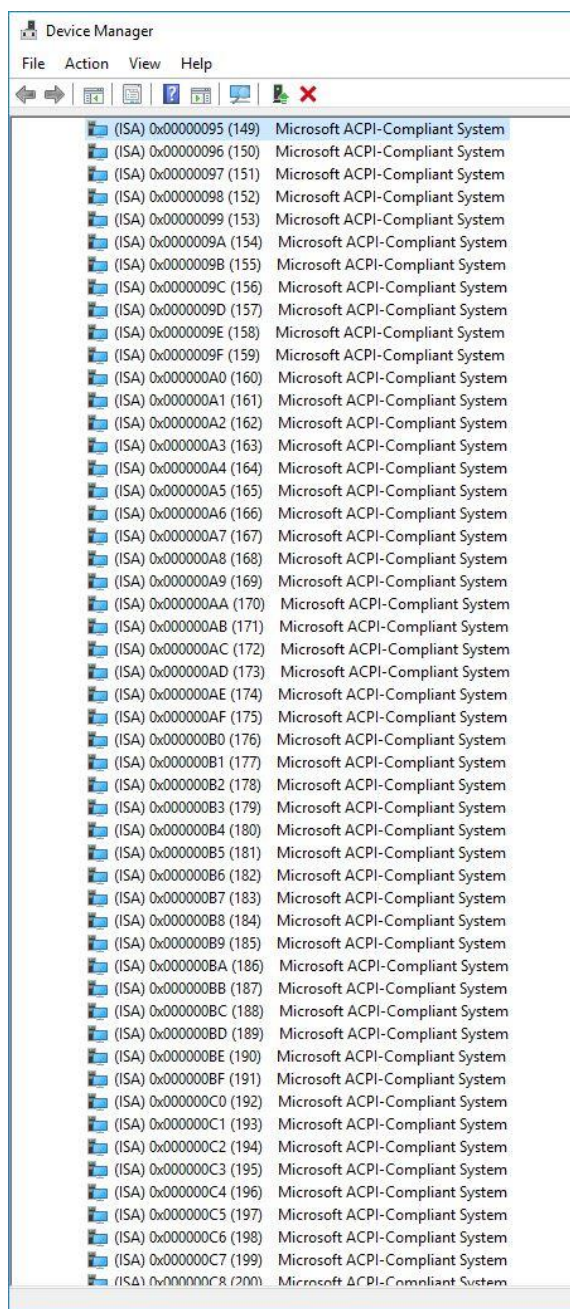
B.2 Memory Address Map

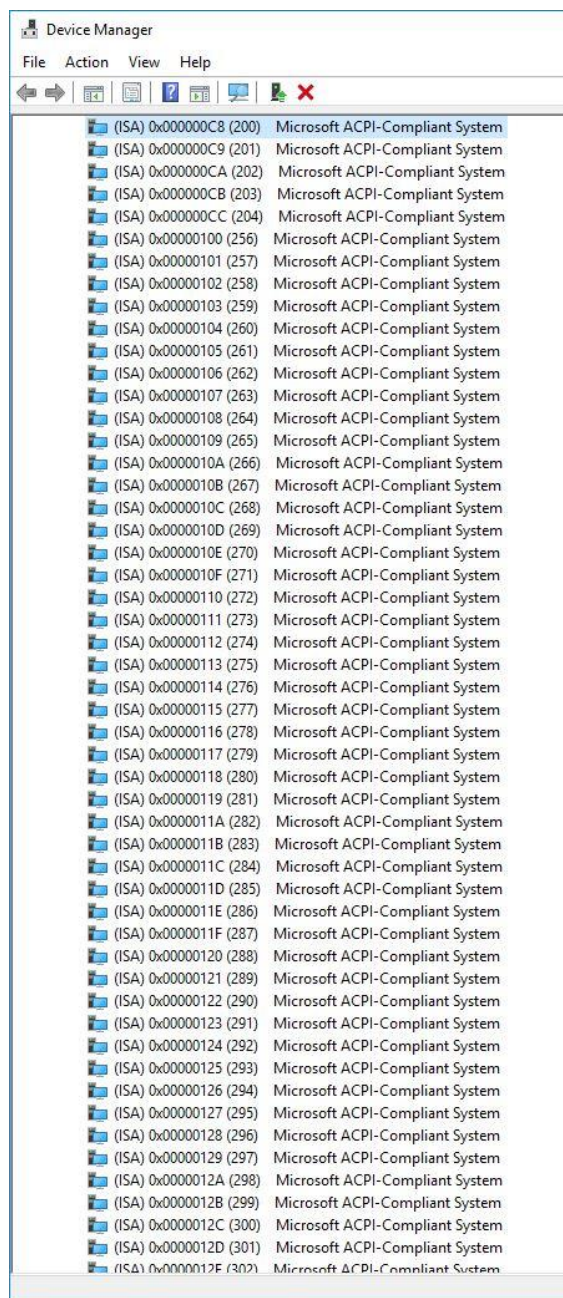
Memory	
[000000000A0000 - 0000000000BFFFF]	PCI Express Root Complex
[0000000040000000 - 00000000403FFFF]	Motherboard resources
[0000000090000000 - 000000009FFFFFF]	Intel(R) UHD Graphics 630
[0000000090000000 - 00000000DFFFFFF]	PCI Express Root Complex
[00000000A0000000 - 00000000A0FFFFFF]	Intel(R) UHD Graphics 630
[00000000A1120000 - 00000000A112FFFF]	Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
[00000000A1134000 - 00000000A1135FFF]	Standard SATA AHCI Controller
[00000000A1138000 - 00000000A11380FF]	Intel(R) SMBus - A323
[00000000A1139000 - 00000000A11397FF]	Standard SATA AHCI Controller
[00000000A113A000 - 00000000A113A0FF]	Standard SATA AHCI Controller
[00000000A113E000 - 00000000A113EFFF]	Intel(R) Thermal Subsystem - A379
[00000000E0000000 - 00000000EFFFFFF]	Motherboard resources
[00000000FC800000 - 00000000FE7FFFF]	PCI Express Root Complex
[00000000FCF00000 - 00000000FCFFFFFF]	High Definition Audio Controller
[00000000FD000000 - 00000000FD69FFF]	Motherboard resources
[00000000FD6A0000 - 00000000FD6AFFFF]	Intel(R) Serial IO GPIO Host Controller - 3450
[00000000FD6B0000 - 00000000FD6BFFFF]	Intel(R) Serial IO GPIO Host Controller - 3450
[00000000FD6C0000 - 00000000FD6CFFF]	Motherboard resources
[00000000FD6D0000 - 00000000FD6DFFF]	Intel(R) Serial IO GPIO Host Controller - 3450
[00000000FD6E0000 - 00000000FD6EFFF]	Intel(R) Serial IO GPIO Host Controller - 3450
[00000000FD6F0000 - 00000000FDFFFF]	Motherboard resources
[00000000FE000000 - 00000000FE01FFF]	Motherboard resources
[00000000FE010000 - 00000000FE01FFF]	Intel(R) SPI (flash) Controller - A324
[00000000FE1DC000 - 00000000FE1DFFF]	High Definition Audio Controller
[00000000FE1E0000 - 00000000FE1FFFF]	Intel(R) Ethernet Connection (7) I219-LM
[00000000FE200000 - 00000000FE7FFFF]	Motherboard resources
[00000000FED00000 - 00000000FED003FF]	High precision event timer
[00000000FED10000 - 00000000FED17FFF]	Motherboard resources
[00000000FED18000 - 00000000FED18FFF]	Motherboard resources
[00000000FED19000 - 00000000FED19FFF]	Motherboard resources
[00000000FED20000 - 00000000FED3FFFF]	Motherboard resources
[00000000FED45000 - 00000000FED8FFFF]	Motherboard resources
[00000000FED90000 - 00000000FED93FFF]	Motherboard resources
[00000000FEE00000 - 00000000FEEFFFF]	Motherboard resources
[00000000FF000000 - 00000000FFFFFFFF]	Motherboard resources

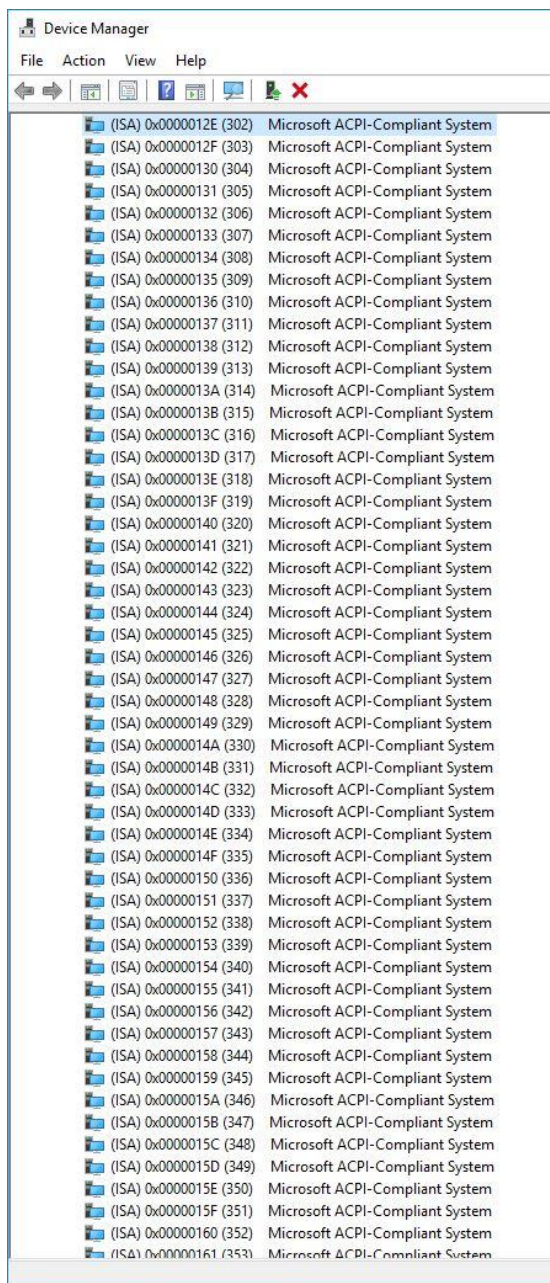
B.3 Interrupt Request (IRQ) Mapping Chart

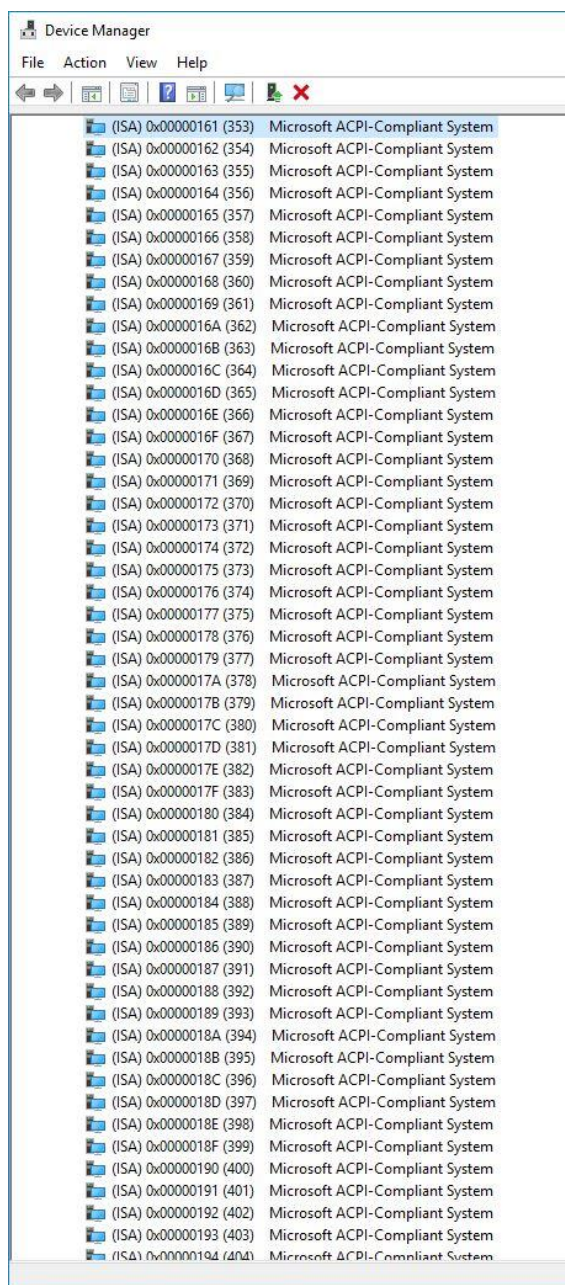
Device Manager		
File Action View Help		
Interrupt request (IRQ)		
	(ISA) 0x00000000 (00)	System timer
	(ISA) 0x00000003 (03)	Communications Port (COM2)
	(ISA) 0x00000004 (04)	Communications Port (COM1)
	(ISA) 0x0000000D (13)	Numeric data processor
	(ISA) 0x0000000E (14)	Intel(R) Serial IO GPIO Host Controller - 3450
	(ISA) 0x00000036 (54)	Microsoft ACPI-Compliant System
	(ISA) 0x00000037 (55)	Microsoft ACPI-Compliant System
	(ISA) 0x00000038 (56)	Microsoft ACPI-Compliant System
	(ISA) 0x00000039 (57)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003A (58)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003B (59)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003C (60)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003D (61)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003E (62)	Microsoft ACPI-Compliant System
	(ISA) 0x0000003F (63)	Microsoft ACPI-Compliant System
	(ISA) 0x00000040 (64)	Microsoft ACPI-Compliant System
	(ISA) 0x00000041 (65)	Microsoft ACPI-Compliant System
	(ISA) 0x00000042 (66)	Microsoft ACPI-Compliant System
	(ISA) 0x00000043 (67)	Microsoft ACPI-Compliant System
	(ISA) 0x00000044 (68)	Microsoft ACPI-Compliant System
	(ISA) 0x00000045 (69)	Microsoft ACPI-Compliant System
	(ISA) 0x00000046 (70)	Microsoft ACPI-Compliant System
	(ISA) 0x00000047 (71)	Microsoft ACPI-Compliant System
	(ISA) 0x00000048 (72)	Microsoft ACPI-Compliant System
	(ISA) 0x00000049 (73)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004A (74)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004B (75)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004C (76)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004D (77)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004E (78)	Microsoft ACPI-Compliant System
	(ISA) 0x0000004F (79)	Microsoft ACPI-Compliant System
	(ISA) 0x00000050 (80)	Microsoft ACPI-Compliant System
	(ISA) 0x00000051 (81)	Microsoft ACPI-Compliant System
	(ISA) 0x00000052 (82)	Microsoft ACPI-Compliant System
	(ISA) 0x00000053 (83)	Microsoft ACPI-Compliant System
	(ISA) 0x00000054 (84)	Microsoft ACPI-Compliant System
	(ISA) 0x00000055 (85)	Microsoft ACPI-Compliant System
	(ISA) 0x00000056 (86)	Microsoft ACPI-Compliant System
	(ISA) 0x00000057 (87)	Microsoft ACPI-Compliant System
	(ISA) 0x00000058 (88)	Microsoft ACPI-Compliant System
	(ISA) 0x00000059 (89)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005A (90)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005B (91)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005C (92)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005D (93)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005E (94)	Microsoft ACPI-Compliant System
	(ISA) 0x0000005F (95)	Microsoft ACPI-Compliant System
	(ISA) 0x00000060 (96)	Microsoft ACPI-Compliant System
	(ISA) 0x00000061 (97)	Microsoft ACPI-Compliant System
	(ISA) 0x00000062 (98)	Microsoft ACPI-Compliant System
	(ISA) 0x00000063 (99)	Microsoft ACPI-Compliant System

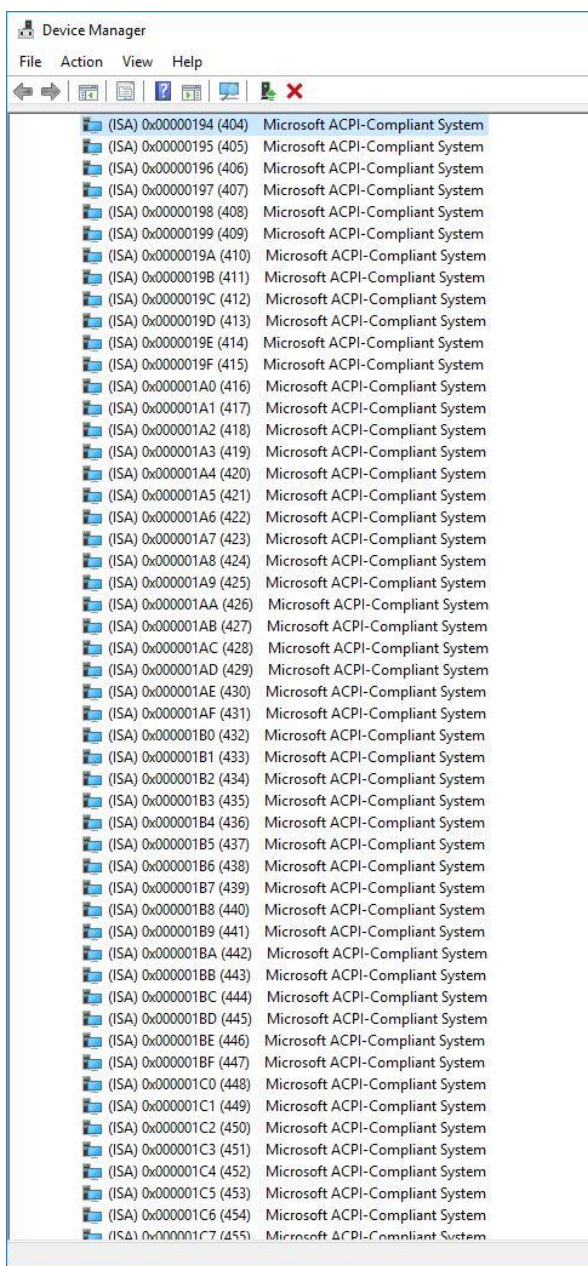


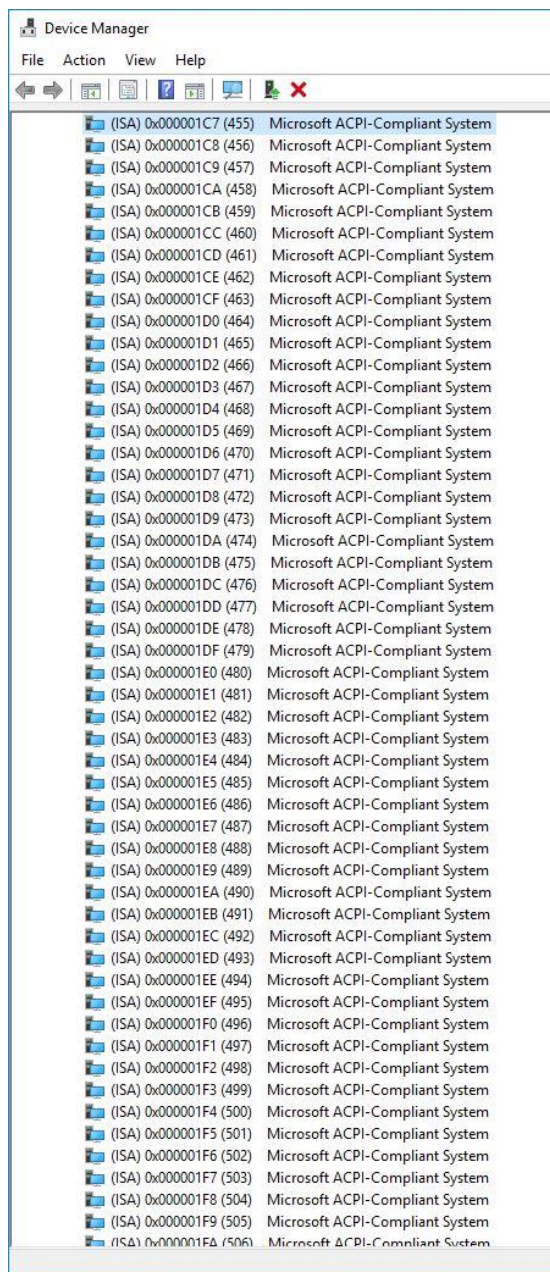












	(ISA) 0x000001FA (506)	Microsoft ACPI-Compliant System
	(ISA) 0x000001FB (507)	Microsoft ACPI-Compliant System
	(ISA) 0x000001FC (508)	Microsoft ACPI-Compliant System
	(ISA) 0x000001FD (509)	Microsoft ACPI-Compliant System
	(ISA) 0x000001FE (510)	Microsoft ACPI-Compliant System
	(ISA) 0x000001FF (511)	Microsoft ACPI-Compliant System
	(PCI) 0x00000010 (16)	High Definition Audio Controller
	(PCI) 0xFFFFFFFF (-6)	Intel(R) Ethernet Connection (7) I219-LM
	(PCI) 0xFFFFFFFFB (-5)	Intel(R) UHD Graphics 630
	(PCI) 0xFFFFFFFFC (-4)	Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
	(PCI) 0xFFFFFFFFD (-3)	Standard SATA AHCI Controller
	(PCI) 0xFFFFFFFFE (-2)	Intel(R) PCIe Controller (x16) - 1901

Appendix C

Programming Digital I/O

C.1 Digital I/O Programming

The COM-CFHB6 utilizes an AAEON chipset as its Digital I/O controller.

Below are the procedures to complete its configuration, which you can use to develop a customized program to fit your application.

C.2 Digital I/O Register

Table 1 : Embedded BRAM relative register table

	Default Value	Note
Index	0x284(Note1)	BRAM Index Register
Data	0x285(Note2)	BRAM Data Register
Logical Device Number	0xA2(Note3)	Watchdog Logical Device Number
IO Direction Function and Device Number	0x00(Note4)	DIO Input/Output Function/Device Number
IO Vaule/Status Function and Device Number	0x01(Note5)	DIO Output Data Function/Device Number

Table 2 : Digital I/O relative register table

	Register			
	Option Register	BitNum	Value	Note
GPI0 Pin Status	0x00(Note6)	0(Note7)	(Note15)	GPA2
GPI1 Pin Status	0x00(Note6)	1(Note8)	(Note16)	GPA3
GPI2 Pin Status	0x00(Note6)	2(Note9)	(Note17)	GPA4
GPI3 Pin Status	0x00(Note6)	3(Note10)	(Note18)	GPA5
GPO0 Pin Status	0x00(Note6)	4(Note11)	(Note19)	GPJ0
GPO1 Pin Status	0x00(Note6)	5(Note12)	(Note20)	GPJ1
GPO2 Pin Status	0x00(Note6)	6(Note13)	(Note21)	GPJ2
GPO3 Pin Status	0x00(Note6)	7(Note14)	(Note22)	GPJ3

C.2 Digital I/O Sample Program

```

*****
// Embedded BRAM relative definition (Please reference to Table 1)
#define byte EcBRAMIndex //This parameter is represented from Note1
#define byte EcBRAMData //This parameter is represented from Note2
#define byte BRAMLDNReg //This parameter is represented from Note3
#define byte BRAMFnData0Reg //This parameter is represented from Note4
#define byte BRAMFnData1Reg //This parameter is represented from Note5
#define void EcBRAMWriteByte(byte Offset, byte Value);
#define byte EcBRAMReadByte(byte Offset);
#define void IOWriteByte(byte Offset, byte Value);
#define byte IOReadByte(byte Offset);
// Digital Input Status relative definition (Please reference to Table 2)
#define byte DIO0ToDIO7Reg // This parameter is represented from Note6
#define byte DIO0Bit // This parameter is represented from Note7
#define byte DIO1Bit // This parameter is represented from Note8
#define byte DIO2Bit // This parameter is represented from Note9
#define byte DIO3Bit // This parameter is represented from Note10
#define byte DIO4Bit // This parameter is represented from Note11
#define byte DIO5Bit // This parameter is represented from Note12
#define byte DIO6Bit // This parameter is represented from Note13
#define byte DIO7Bit // This parameter is represented from Note14
#define byte DIO0Val // This parameter is represented from Note15
#define byte DIO1Val // This parameter is represented from Note16
#define byte DIO2Val // This parameter is represented from Note17
#define byte DIO3Val // This parameter is represented from Note18
#define byte DIO4Val // This parameter is represented from Note19
#define byte DIO5Val // This parameter is represented from Note20
#define byte DIO6Val // This parameter is represented from Note21
#define byte DIO7Val // This parameter is represented from Note22
*****

```

```

*****
VOID  Main() {
    Boolean PinStatus ;

    // Procedure : AaeonReadPinStatus
    // Input :
    //     Example, Read Digital I/O Pin 3 status
    // Output :
    //     InputStatus :
    //         0: Digital I/O Pin level is low
    //         1: Digital I/O Pin level is High
    PinStatus = AaeonReadPinStatus(DIO0ToDIO7Reg, DIO3Bit);

    // Procedure : AaeonSetOutputLevel
    // Input :
    //     Example, Set Digital I/O Pin 6 level
    AaeonSetOutputLevel(DIO0ToDIO7Reg, DIO6Bit, DIO6Val);
}
*****

```

```
*****
```

```
Boolean  AaeonReadPinStatus(byte OptionReg, byte BitNum){
```

```
    Byte TempByte;
```

```
    TempByte = ECBRAMReadByte(BRAMFnData1Reg, OptionReg);
```

```
    If (TempByte & BitNum == 0)
```

```
        Return 0;
```

```
    Return 1;
```

```
}
```

```
VOID  AaeonSetOutputLevel(byte OptionReg, byte BitNum, byte Value){
```

```
    Byte TempByte;
```

```
    TempByte = ECBRAMReadByte(BRAMFnData1Reg, OptionReg);
```

```
    TempByte |= (Value << BitNum);
```

```
    ECBRAMWriteByte(OptionReg, BitNum, Value);
```

```
}
```

```
*****
```

```
*****
```

```
VOID ECBRAMWriteByte(byte OPReg, byte OPBit, byte Value){
```

```
    IOWriteByte(EcBRAMIndex, 0x10);
```

```
    IOWriteByte(EcBRAMData, BRAMLDNReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x11);
```

```
    IOWriteByte(EcBRAMData, BRAMFnDataReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x13 + OPReg);
```

```
    IOWriteByte(EcBRAMData, Value);
```

```
    IOWriteByte(EcBRAMIndex, 0x12);
```

```
    IOWriteByte(EcBRAMData, 0x30);           //Write start
```

```
}
```

```
Byte ECBRAMReadByte(byte FnDataReg, byte OPReg){
```

```
    IOWriteByte(EcBRAMIndex, 0x10);
```

```
    IOWriteByte(EcBRAMData, BRAMLDNReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x11);
```

```
    IOWriteByte(EcBRAMData, FnDataReg);
```

```
    IOWriteByte(EcBRAMIndex, 0x12);
```

```
    IOWriteByte(EcBRAMData, 0x10);           //Read start
```

```
    IOWriteByte(EcBRAMIndex, 0x13 + OPReg);
```

```
    Return      IOReadByte(EcBRAMData, Value);
```

```
}
```

```
*****
```