SDM310S

Intel® Smart Display Module (SDM-S) with Intel® Celeron™ Elkhart Lake Processor

User's Manual

Disclaimers

This manual has been carefully checked and believed to contain accurate information. Axiomtek Co., Ltd. assumes no responsibility for any infringements of patents or any third party's rights, and any liability arising from such use.

Axiomtek does not warrant or assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information in this document. Axiomtek does not make any commitment to update the information in this manual.

Axiomtek reserves the right to change or revise this document and/or product at any time without notice.

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Axiomtek Co., Ltd.

CAUTION

If you replace wrong batteries, it causes the danger of explosion. It is recommended by the manufacturer that you follow the manufacturer's instructions to only replace the same or equivalent type of battery, and dispose of used ones.

©Copyright 2024 Axiomtek Co., Ltd.

All Rights Reserved

August 2024, Version A1

Printed in Taiwan

ESD Precautions

Computer boards have integrated circuits sensitive to static electricity. To prevent chipsets from electrostatic discharge damage, please observe the following precautions:

- Do not remove modules or integrated circuits from their anti-static packaging until you are ready to install them.
- Before holding the module or any integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. Doing so will help discharge static electricity from your body.
- When handling modules and components, wear a wrist-grounding strap, available from most electronic component stores.

Trademarks Acknowledgments

Axiomtek is a trademark of Axiomtek Co., Ltd.

Windows® is a trademark of Microsoft Corporation.

AMI is a trademark of American Megatrend Inc.

IBM, PC/AT, PS/2, VGA are trademarks of International Business Machines Corporation.

Intel®, Celeron® are trademarks of Intel Corporation.

Other brand names and trademarks are the properties and registered brands of their respective owners.

Table of Contents

Disclaimers ii
ESD Precautions iii

Section 1 Introduction 1

1.1 Features 1
1.2 Specifications 2
1.3 Utilities Supported 3
1.4 Block Diagram 4

Section 2 Module and Pin Assignments 5

2.1 Module Dimensions and Fixing Holes 5
2.2 Module Layout 8
2.3 Bracket Installation 10
2.3.1 Bracket Assembly 10
2.4 Jumper Settings 11
2.4.1 Auto Power on (JP1) 11
2.5 Connectors 12
2.5.1 Ethernet Port (LAN1) 12
2.5.2 Type-C Connectors (USBC1, USBC2) 13
2.5.3 Power and Reset Button (SW1) 14
2.5.4 FAN Header (FAN1) 14
2.5.5 RTC Battery Header (BAT1) 14
2.5.6 SDM Edge Connector (J1) 15

Section 3 Hardware Description 17

3.1 Microprocessor 17
3.2 BIOS 17
3.3 System Memory 17
3.4 I/O Port Address Map 18
3.5 Interrupt Controller (IRQ) Map 19
3.6 Memory Map 25

Section 4 AMI BIOS Setup Utility 27

4.1 Starting 27
4.2 Navigation Keys 27

4.3 Main Menu....29
4.4 Advanced Menu....30
4.5 Chipset Menu....39
4.6 Security Menu....40
4.7 Boot Menu....43
4.8 Save & Exit Menu....44

Appendix A Watchdog Timer....47

A.1 About Watchdog Timer....47
A.2 How to Use Watchdog Timer....47

This page is intentionally left blank.

Section 1
Introduction

The SDM310S is a new Intel® Smart Display Module (SDM-S) supporting the Intel® J6412 Elkhart Lake processor. It delivers outstanding system performance and support excellent multiple I/Os such as one Gigabyte Ethernet port and two Type C USB 3.2 ports. SDM310S measures only 100 x 60mm and delivers 4K output with streaming content thru the SDM edge connector.

The smart display module carries 4/8GB LPDDR4 onboard memory and 64/128GB eMMC onboard flash. The cost-effective SDM310S features one standard PCIe and built-in I/O such as USB 3.0, HDMI 1.4, DisplayPort 1.2, Serial TX/RX and I²C (thru SDM edge connector). In addition, SDM310S can be built in or externally plugged into a display for maximum integration flexibility to fit into the sleekest all-in-one designs.

1.1 Features

- Intel® Smart Display Module (Intel® SDM) specification
- Intel® Celeron® processor J6412 (Elkhart Lake)
- 4GB LPDDR4 memory onboard (8GB optional)
- 64GB eMMC onboard (128G optional)
- Supports two 4K 60Hz
- Two Type C (USB 3.2) and one GbE LAN
- Small design for easy integration into slim displays
- Optimized for digital signage, public kiosks, professional monitors, point-of-sale
- Projections for magic mirrors, beside terminals, hospitality and more

1.2 Specifications

- **CPU**
  - Intel® Celeron® quad core J6412 2.0~2.6GHz.
- **BIOS**
  - American Megatrends Inc. BIOS.
  - 64Mbit SPI Flash, DMI, Plug and Play.
  - PXE Ethernet Boot ROM; customized default saving features; LPC-free supported; uses SPI type Flash memory.
- **System Memory**
  - 4GB LPDDR4 3200MHz onboard memory supporting maximum capacity up to 8GB (optional).
- **eMMC**
  - Support 64/128GB eMMC 5.1 onboard flash.
- **USB Interface**
  - Two USB 3.2 Gen2 ports in Type C, one of which support DP1.2a on rear I/O.
  - One USB 3.2 Gen2 port (through SDM edge connector).
- **Graphics**
  - 1 x Type C DisplayPort 1.2a (4096x2160 @60Hz) (rear I/O)
  - 1 x HDMI 2.0b 4096x2160 @60Hz (via SDM edge connector)
  - 1 x DisplayPort 1.2a 4096x2160 @60Hz (via SDM edge connector)
- **Ethernet**
  - One 1 GbE provided by RTL8111H support Wake-on-LAN.
- **WatchDog Timer**
  - 1~65536 seconds or minutes up to 65536 levels.
- **SDM Edge Connector**
  - 98-pin golden finger, supporting DP, HDMI, PCI-Express x1, USB 3.2 Gen2, Serial TX/RX, I²C.
- **Power Management**
  - ACPI (Advanced Configuration and Power Interface).
- **Form Factor**
  - 100mm x 60mm.

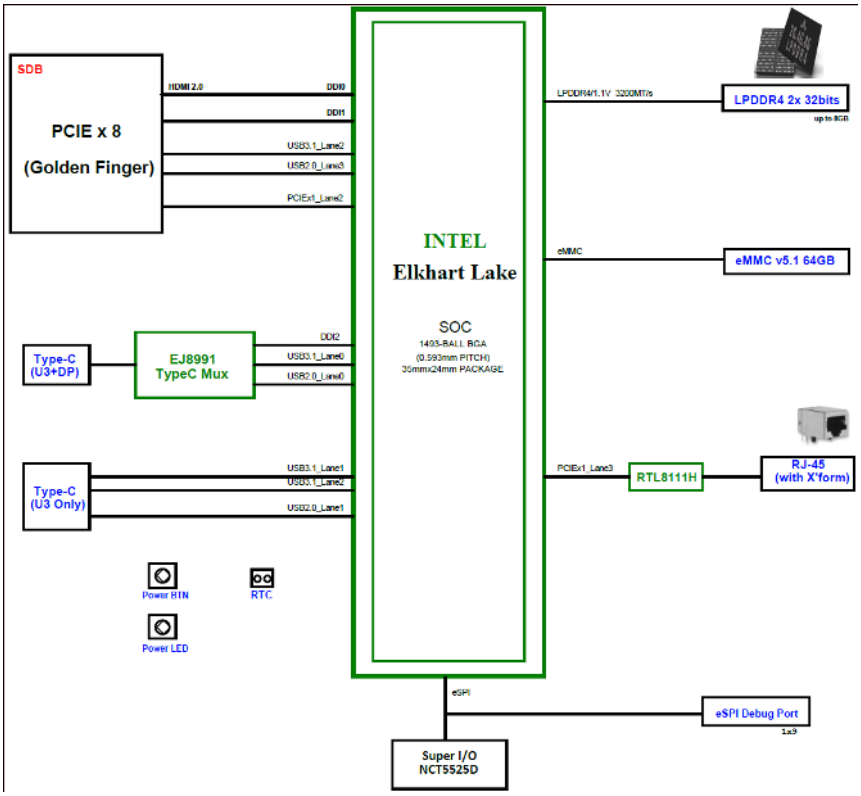
1.3 Utilities Supported

- Chipset driver
- Graphics driver
- TXE driver
- Serial IO driver
- Ethernet utility and driver

Note

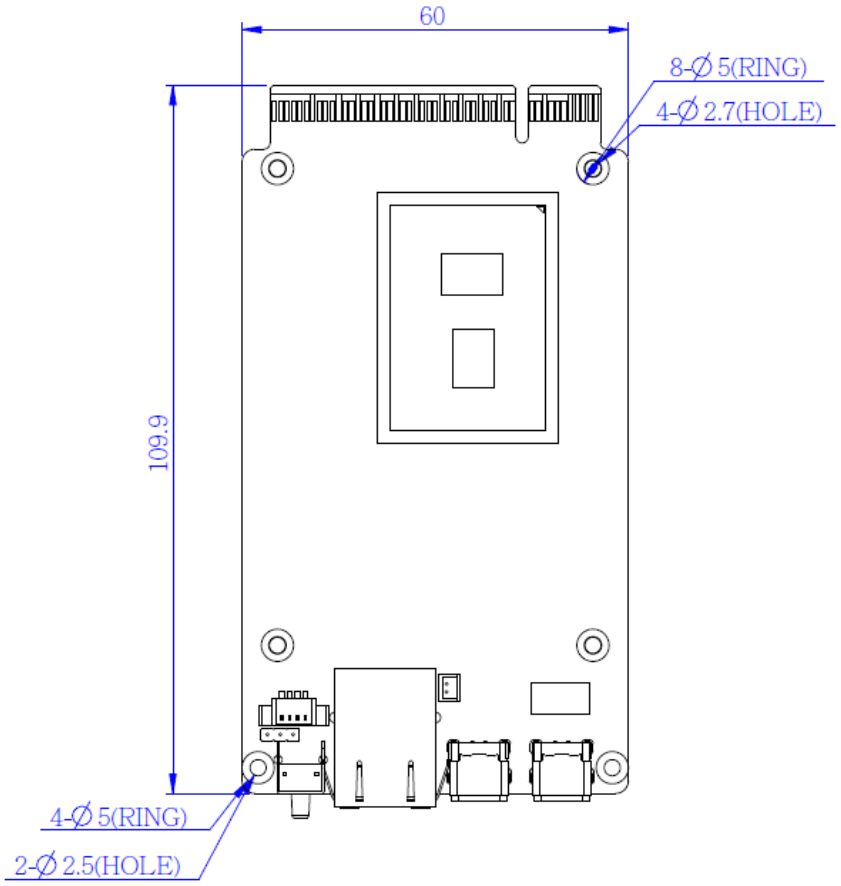
All specifications and images are subject to change without notice.

1.4 Block Diagram

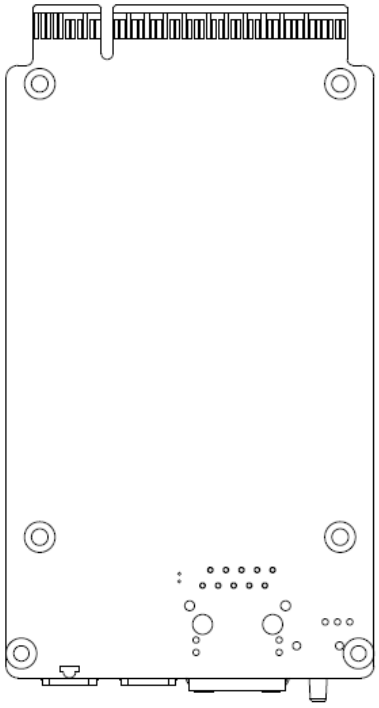


Section 2
Module and Pin Assignments

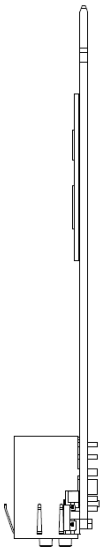
2.1 Module Dimensions and Fixing Holes



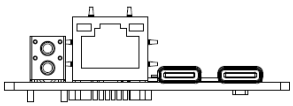
Top View



Bottom View

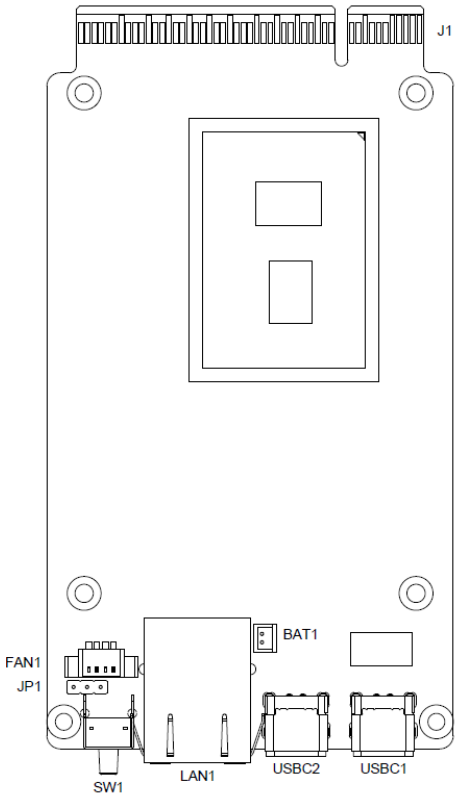


Side View

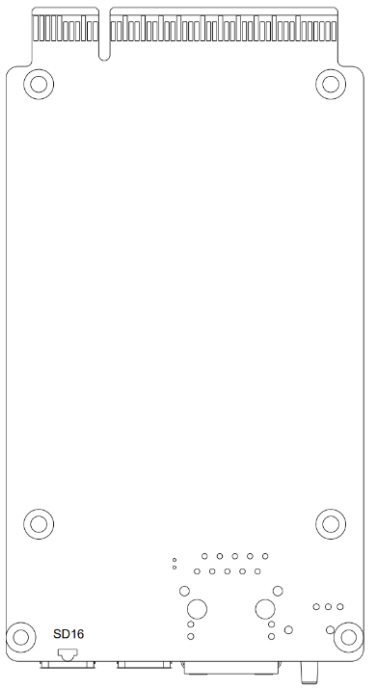


Front View

2.2 Module Layout



Top View

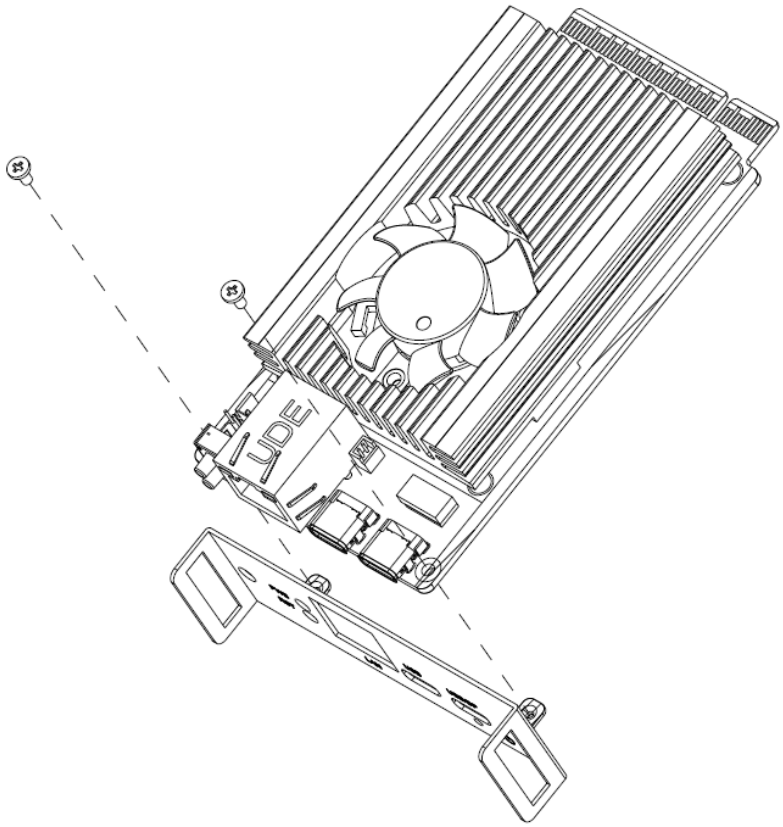


Bottom View

2.3 Bracket Installation

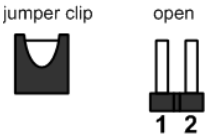
2.3.1 Bracket Assembly

SDM310S bracket assembly.



2.4 Jumper Settings

A jumper is a small component consisting of a set of jumper pins with a jumper clip. Place a jumper clip on two jumper pins to close; remove a jumper clip from two jumper pins to open. The following illustration shows how to set up a jumper.



Properly configure jumper settings on the SDM310S to meet your application purpose. Below you can find a summary table of jumpers and their default onboard settings.

Note

Once the default jumper setting needs to be changed, please do it under power-off condition.

2.4.1 Auto Power on (JP1)

If JP1 is enabled for power input, the system will be automatically power on without the need to press the soft power button. If JP1 is disabled for power input, it is necessary to manually press the soft power button to power on the system.

已註解 **[jeremy1]:** Should it be "JP2"?

Function	Setting
Enable auto power on (Default)	1-2 close
Disable auto power on	2-3 close

2.5 Connectors

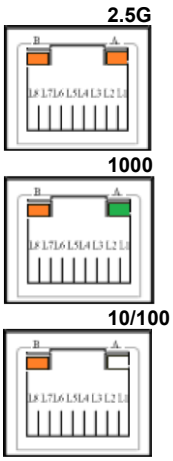
Signals go to the other parts of the system through connectors. Loose or improper connection might cause problems. Please make sure all connectors are properly and firmly connected. Here is a table summarizing the connectors on the hardware.

Connector	Description
LAN1	2.5G Ethernet Port
USBC1	Type-C w/ DP Alt
USBC2	Type-C w/o DP Alt
SW1	Power and Reset Button
FAN1	Fan Header
BAT1	Battery Header
J1	SDM Edge Connector

2.5.1 Ethernet Port (LAN1)

The board has one RJ-45 Ethernet connector (LAN1). Connection can be established by plugging one end of the Ethernet cable into this connector and the other end (phone jack) to a 2500/1000/100/10-Base-T hub.

Pin	2500 Base-T
L1	MDI0+
L2	MDI0-
L3	MDI1+
L4	MDI1-
L5	MDI2+
L6	MDI2-
L7	MDI3+
L8	MDI3-
B	Active Link LED (Orange) Off: No link Blinking: Data activity detected
A	Speed LED 2.5G: Orange 1000: Green 100/10: OFF

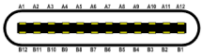


2.5.2 Type-C Connectors (USBC1, USBC2)

The Universal Serial Bus (compliant with USB 3.2 Gen2 (10Gb/s)) connectors are on the rear I/O side. They are both commonly used for installing USB peripherals such as keyboard, mouse, scanner, etc. Only USBC1 also supports 4K display.

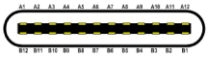
Pin	Signal	Pin	Signal
A1	GND	B1	GND
A2	SSTXP1	B2	SSTXP2
A3	SSTXN1	B3	SSTXN2
A4	+5V_VBUS	B4	+5V_VBUS
A5	CC1	B5	CC2
A6	USB_DP0	B6	USB_DP0
A7	USB_DN0	B7	USB_DN0
A8	CSBU1	B8	CSBU2
A9	+5V_VBUS	B9	+5V_VBUS
A10	SSRXN2	B10	SSRXN1
A11	SSRXP2	B11	SSRXP1
A12	GND	B12	GND

USBC1



Pin	Signal	Pin	Signal
A1	GND	B1	GND
A2	U3_TXP1	B2	U3_TXP2
A3	U3_TXN1	B3	U3_TXN2
A4	+5V_USBC2	B4	+5V_USBC2
A5	A_CC1	B5	A_CC2
A6	USB_DP1	B6	USB_DP1
A7	USB_DN1	B7	USB_DN1
A8	NC	B8	NC
A9	+5V_USBC2	B9	+5V_USBC2
A10	U3_RXN2	B10	U3_RXN1
A11	U3_RXP2	B11	U3_RXP1
A12	GND	B12	GND

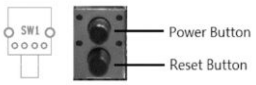
USBC2



2.5.3 Power and Reset Button (SW1)

The upper power button allows users to control the power on/off of the SDM300S. The lower reset button allows users to reset the SDM300S during abnormal system situations.

Power Button	Description
Press	Turn on/off system
Release	Keep system status



Reset Button	Description
Press	Reset system
Release	Keep system status

2.5.4 FAN Header (FAN1)

You can find fan speed option within BIOS Setup Utility if fan is installed. For further information, see BIOS Setup Utility: Advanced\Hardware Monitor\PC Health Status in section 4.4.

Pin	Signal
1	GND
2	FAN_DCVOUT
3	SIO_FANIN
4	FAN_PWMOUT

2.5.5 RTC Battery Header (BAT1)

This is a header for RTC battery interface.

Pin	Signal
1	VBAT
2	GND

2.5.6 SDM Edge Connector (J1)

The following table shows the pin assignments for the 98-pin SDM PCIe x8 edge connector.

Pin	Side B (Top)	Pin	Side A (Bottom)
1	+12V	1	+12V
2	+12V	2	+12V
3	+3.3VSB	3	+12V
4	GND	4	GND
5	GND	5	GND
6	PWRBTN#	6	PWRGD#
7	RESET#	7	SLP_S4
8	SYSFAN#	8	SDM_DET#
9	GND	9	CEC/NC
10	I2C1_SDA	10	I2C0_SDA
11	I2C1_SCL	11	I2C0_SCL
12	GSPI_MOSI	12	GSPI_CLK
13	GSPI_MISO	13	GSPI_CS0#
14	GND	14	GND
15	UART_TXD	15	PCIe_TX+
16	UART_RXD	16	PCIe_TX-
17	GND	17	GND
18	USB_SSTX+	18	PCIe_RX+
19	USB_SSTX-	19	PCIe_RX-
20	GND	20	GND
21	USB_SSRX+	21	PCIe_Clk+
22	USB_SSRX-	22	PCIe_Clk-
23	GND	23	GND
24	USB+	24	PCIE_WAKE#
25	USB-	25	PCIE_CLKREQ#
26	USB_OC#	26	PCIE_RST#
27	GND	27	GND
28	DP3-	28	TMDS_CLK-
29	DP3+	29	TMDS_CLK+
30	GND	30	GND
31	DP2-	31	TMDS0-
32	DP+	32	TMDS0+
33	GND	33	GND
34	DP1-	34	TMDS1-
35	DP1+	35	TMDS1+
36	GND	36	GND
37	DP0-	37	TMDS2-
38	DP0+	38	TMDS2+
39	GND	39	GND
40	DP_AUX-	40	DDC_DATA
41	DP_AUX+	41	DDC_CLK
42	DP_HPD	42	TMDS_HPD
43	GND	43	GND
44	RSVD	44	RSVD
45	RSVD	45	RSVD
46	RSVD	46	RSVD
47	RSVD	47	RSVD
48	RSVD	48	RSVD
49	RSVD	49	RSVD

This page is intentionally left blank.

Section 3
Hardware Description

3.1 Microprocessor

The SMD310S supports Intel® Celeron® J6412 processors, which enable your system to operate under Windows® 10, Windows® 11 and Linux environments. The system performance depends on the microprocessor. Make sure all correct settings are arranged for the installed microprocessor to prevent the CPU from damage.

3.2 BIOS

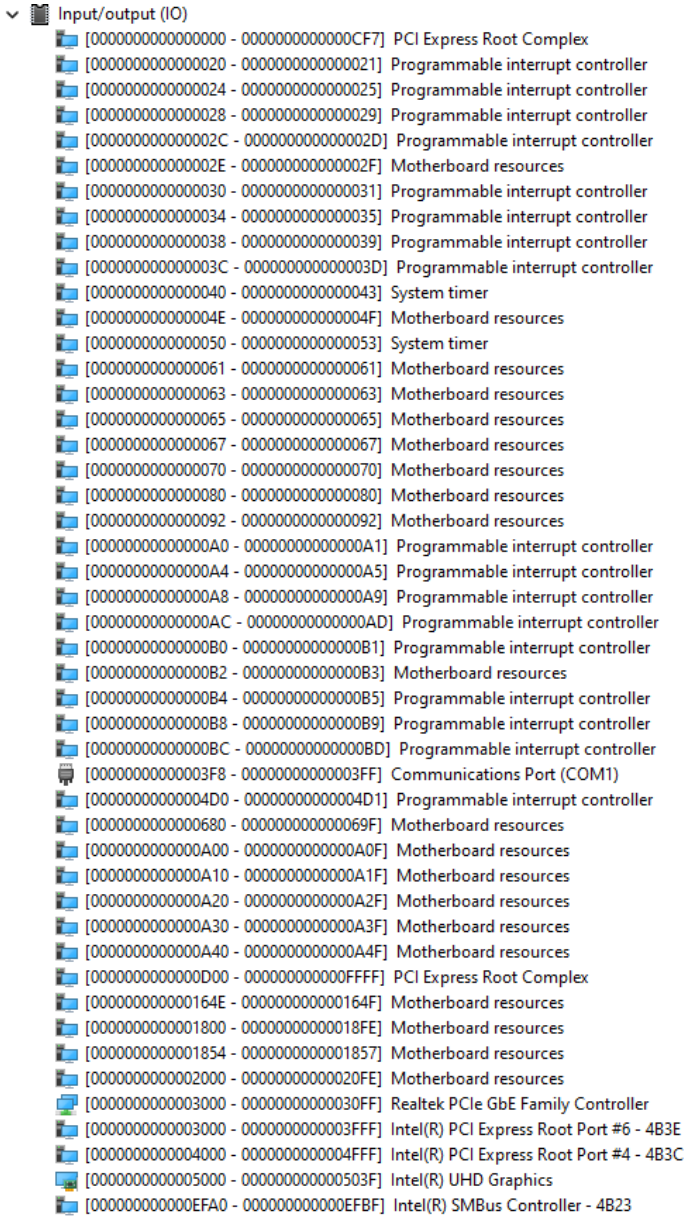
The SDM310S uses AMI Plug and Play BIOS with a single 256Mbit SPI Flash.

3.3 System Memory

4GB LPDDR4 3200MHz onboard memory supporting maximum capacity up to 8GB.

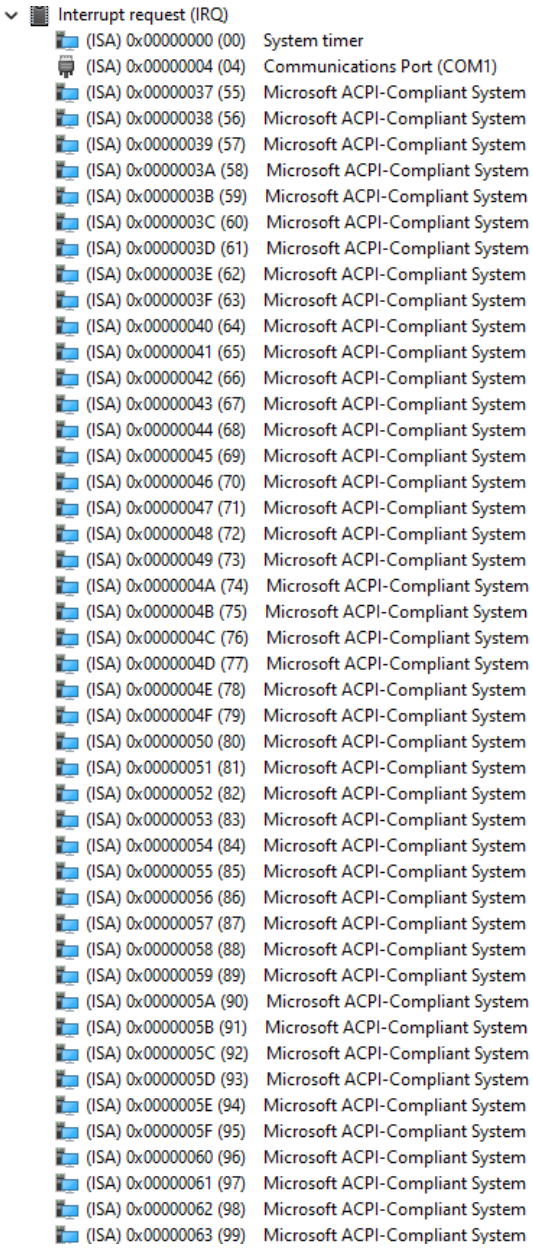
3.4 I/O Port Address Map

The I/O port address mapping list is shown as follows:



3.5 Interrupt Controller (IRQ) Map

The interrupt controller (IRQ) mapping list is shown as follows:



(ISA) 0x00000064 (100) Microsoft ACPI-Compliant System
(ISA) 0x00000065 (101) Microsoft ACPI-Compliant System
(ISA) 0x00000066 (102) Microsoft ACPI-Compliant System
(ISA) 0x00000067 (103) Microsoft ACPI-Compliant System
(ISA) 0x00000068 (104) Microsoft ACPI-Compliant System
(ISA) 0x00000069 (105) Microsoft ACPI-Compliant System
(ISA) 0x0000006A (106) Microsoft ACPI-Compliant System
(ISA) 0x0000006B (107) Microsoft ACPI-Compliant System
(ISA) 0x0000006C (108) Microsoft ACPI-Compliant System
(ISA) 0x0000006D (109) Microsoft ACPI-Compliant System
(ISA) 0x0000006E (110) Microsoft ACPI-Compliant System
(ISA) 0x0000006F (111) Microsoft ACPI-Compliant System
(ISA) 0x00000070 (112) Microsoft ACPI-Compliant System
(ISA) 0x00000071 (113) Microsoft ACPI-Compliant System
(ISA) 0x00000072 (114) Microsoft ACPI-Compliant System
(ISA) 0x00000073 (115) Microsoft ACPI-Compliant System
(ISA) 0x00000074 (116) Microsoft ACPI-Compliant System
(ISA) 0x00000075 (117) Microsoft ACPI-Compliant System
(ISA) 0x00000076 (118) Microsoft ACPI-Compliant System
(ISA) 0x00000077 (119) Microsoft ACPI-Compliant System
(ISA) 0x00000078 (120) Microsoft ACPI-Compliant System
(ISA) 0x00000079 (121) Microsoft ACPI-Compliant System
(ISA) 0x0000007A (122) Microsoft ACPI-Compliant System
(ISA) 0x0000007B (123) Microsoft ACPI-Compliant System
(ISA) 0x0000007C (124) Microsoft ACPI-Compliant System
(ISA) 0x0000007D (125) Microsoft ACPI-Compliant System
(ISA) 0x0000007E (126) Microsoft ACPI-Compliant System
(ISA) 0x0000007F (127) Microsoft ACPI-Compliant System
(ISA) 0x00000080 (128) Microsoft ACPI-Compliant System
(ISA) 0x00000081 (129) Microsoft ACPI-Compliant System
(ISA) 0x00000082 (130) Microsoft ACPI-Compliant System
(ISA) 0x00000083 (131) Microsoft ACPI-Compliant System
(ISA) 0x00000084 (132) Microsoft ACPI-Compliant System
(ISA) 0x00000085 (133) Microsoft ACPI-Compliant System
(ISA) 0x00000086 (134) Microsoft ACPI-Compliant System
(ISA) 0x00000087 (135) Microsoft ACPI-Compliant System
(ISA) 0x00000088 (136) Microsoft ACPI-Compliant System
(ISA) 0x00000089 (137) Microsoft ACPI-Compliant System
(ISA) 0x0000008A (138) Microsoft ACPI-Compliant System
(ISA) 0x0000008B (139) Microsoft ACPI-Compliant System
(ISA) 0x0000008C (140) Microsoft ACPI-Compliant System
(ISA) 0x0000008D (141) Microsoft ACPI-Compliant System
(ISA) 0x0000008E (142) Microsoft ACPI-Compliant System
(ISA) 0x0000008F (143) Microsoft ACPI-Compliant System
(ISA) 0x00000090 (144) Microsoft ACPI-Compliant System
(ISA) 0x00000091 (145) Microsoft ACPI-Compliant System
(ISA) 0x00000092 (146) Microsoft ACPI-Compliant System
(ISA) 0x00000093 (147) Microsoft ACPI-Compliant System
(ISA) 0x00000094 (148) Microsoft ACPI-Compliant System
(ISA) 0x00000095 (149) Microsoft ACPI-Compliant System
(ISA) 0x00000096 (150) Microsoft ACPI-Compliant System
(ISA) 0x00000097 (151) Microsoft ACPI-Compliant System
(ISA) 0x00000098 (152) Microsoft ACPI-Compliant System
(ISA) 0x00000099 (153) Microsoft ACPI-Compliant System
(ISA) 0x0000009A (154) Microsoft ACPI-Compliant System
(ISA) 0x0000009B (155) Microsoft ACPI-Compliant System
(ISA) 0x0000009C (156) Microsoft ACPI-Compliant System
(ISA) 0x0000009D (157) Microsoft ACPI-Compliant System
(ISA) 0x0000009E (158) Microsoft ACPI-Compliant System
(ISA) 0x0000009F (159) Microsoft ACPI-Compliant System
(ISA) 0x000000A0 (160) Microsoft ACPI-Compliant System
(ISA) 0x000000A1 (161) Microsoft ACPI-Compliant System
(ISA) 0x000000A2 (162) Microsoft ACPI-Compliant System
(ISA) 0x000000A3 (163) Microsoft ACPI-Compliant System
(ISA) 0x000000A4 (164) Microsoft ACPI-Compliant System
(ISA) 0x000000A5 (165) Microsoft ACPI-Compliant System
(ISA) 0x000000A6 (166) Microsoft ACPI-Compliant System
(ISA) 0x000000A7 (167) Microsoft ACPI-Compliant System
(ISA) 0x000000A8 (168) Microsoft ACPI-Compliant System
(ISA) 0x000000A9 (169) Microsoft ACPI-Compliant System
(ISA) 0x000000AA (170) Microsoft ACPI-Compliant System
(ISA) 0x000000AB (171) Microsoft ACPI-Compliant System
(ISA) 0x000000AC (172) Microsoft ACPI-Compliant System
(ISA) 0x000000AD (173) Microsoft ACPI-Compliant System
(ISA) 0x000000AE (174) Microsoft ACPI-Compliant System
(ISA) 0x000000AF (175) Microsoft ACPI-Compliant System
(ISA) 0x000000B0 (176) Microsoft ACPI-Compliant System
(ISA) 0x000000B1 (177) Microsoft ACPI-Compliant System
(ISA) 0x000000B2 (178) Microsoft ACPI-Compliant System
(ISA) 0x000000B3 (179) Microsoft ACPI-Compliant System
(ISA) 0x000000B4 (180) Microsoft ACPI-Compliant System
(ISA) 0x000000B5 (181) Microsoft ACPI-Compliant System
(ISA) 0x000000B6 (182) Microsoft ACPI-Compliant System
(ISA) 0x000000B7 (183) Microsoft ACPI-Compliant System
(ISA) 0x000000B8 (184) Microsoft ACPI-Compliant System
(ISA) 0x000000B9 (185) Microsoft ACPI-Compliant System
(ISA) 0x000000BA (186) Microsoft ACPI-Compliant System
(ISA) 0x000000BB (187) Microsoft ACPI-Compliant System
(ISA) 0x000000BC (188) Microsoft ACPI-Compliant System
(ISA) 0x000000BD (189) Microsoft ACPI-Compliant System
(ISA) 0x000000BE (190) Microsoft ACPI-Compliant System
(ISA) 0x000000BF (191) Microsoft ACPI-Compliant System
(ISA) 0x000000C0 (192) Microsoft ACPI-Compliant System
(ISA) 0x000000C1 (193) Microsoft ACPI-Compliant System
(ISA) 0x000000C2 (194) Microsoft ACPI-Compliant System
(ISA) 0x000000C3 (195) Microsoft ACPI-Compliant System
(ISA) 0x000000C4 (196) Microsoft ACPI-Compliant System
(ISA) 0x000000C5 (197) Microsoft ACPI-Compliant System
(ISA) 0x000000C6 (198) Microsoft ACPI-Compliant System
(ISA) 0x000000C7 (199) Microsoft ACPI-Compliant System
(ISA) 0x000000C8 (200) Microsoft ACPI-Compliant System

(ISA) 0x000000C9 (201) Microsoft ACPI-Compliant System
(ISA) 0x000000CA (202) Microsoft ACPI-Compliant System
(ISA) 0x000000CB (203) Microsoft ACPI-Compliant System
(ISA) 0x000000CC (204) Microsoft ACPI-Compliant System
(ISA) 0x00000100 (256) Microsoft ACPI-Compliant System
(ISA) 0x00000101 (257) Microsoft ACPI-Compliant System
(ISA) 0x00000102 (258) Microsoft ACPI-Compliant System
(ISA) 0x00000103 (259) Microsoft ACPI-Compliant System
(ISA) 0x00000104 (260) Microsoft ACPI-Compliant System
(ISA) 0x00000105 (261) Microsoft ACPI-Compliant System
(ISA) 0x00000106 (262) Microsoft ACPI-Compliant System
(ISA) 0x00000107 (263) Microsoft ACPI-Compliant System
(ISA) 0x00000108 (264) Microsoft ACPI-Compliant System
(ISA) 0x00000109 (265) Microsoft ACPI-Compliant System
(ISA) 0x0000010A (266) Microsoft ACPI-Compliant System
(ISA) 0x0000010B (267) Microsoft ACPI-Compliant System
(ISA) 0x0000010C (268) Microsoft ACPI-Compliant System
(ISA) 0x0000010D (269) Microsoft ACPI-Compliant System
(ISA) 0x0000010E (270) Microsoft ACPI-Compliant System
(ISA) 0x0000010F (271) Microsoft ACPI-Compliant System
(ISA) 0x00000110 (272) Microsoft ACPI-Compliant System
(ISA) 0x00000111 (273) Microsoft ACPI-Compliant System
(ISA) 0x00000112 (274) Microsoft ACPI-Compliant System
(ISA) 0x00000113 (275) Microsoft ACPI-Compliant System
(ISA) 0x00000114 (276) Microsoft ACPI-Compliant System
(ISA) 0x00000115 (277) Microsoft ACPI-Compliant System
(ISA) 0x00000116 (278) Microsoft ACPI-Compliant System
(ISA) 0x00000117 (279) Microsoft ACPI-Compliant System
(ISA) 0x00000118 (280) Microsoft ACPI-Compliant System
(ISA) 0x00000119 (281) Microsoft ACPI-Compliant System
(ISA) 0x0000011A (282) Microsoft ACPI-Compliant System
(ISA) 0x0000011B (283) Microsoft ACPI-Compliant System
(ISA) 0x0000011C (284) Microsoft ACPI-Compliant System
(ISA) 0x0000011D (285) Microsoft ACPI-Compliant System
(ISA) 0x0000011E (286) Microsoft ACPI-Compliant System
(ISA) 0x0000011F (287) Microsoft ACPI-Compliant System
(ISA) 0x00000120 (288) Microsoft ACPI-Compliant System
(ISA) 0x00000121 (289) Microsoft ACPI-Compliant System
(ISA) 0x00000122 (290) Microsoft ACPI-Compliant System
(ISA) 0x00000123 (291) Microsoft ACPI-Compliant System
(ISA) 0x00000124 (292) Microsoft ACPI-Compliant System
(ISA) 0x00000125 (293) Microsoft ACPI-Compliant System
(ISA) 0x00000126 (294) Microsoft ACPI-Compliant System
(ISA) 0x00000127 (295) Microsoft ACPI-Compliant System
(ISA) 0x00000128 (296) Microsoft ACPI-Compliant System
(ISA) 0x00000129 (297) Microsoft ACPI-Compliant System
(ISA) 0x0000012A (298) Microsoft ACPI-Compliant System
(ISA) 0x0000012B (299) Microsoft ACPI-Compliant System
(ISA) 0x0000012C (300) Microsoft ACPI-Compliant System
(ISA) 0x0000012D (301) Microsoft ACPI-Compliant System
(ISA) 0x0000012E (302) Microsoft ACPI-Compliant System
(ISA) 0x0000012F (303) Microsoft ACPI-Compliant System
(ISA) 0x00000130 (304) Microsoft ACPI-Compliant System
(ISA) 0x00000131 (305) Microsoft ACPI-Compliant System
(ISA) 0x00000132 (306) Microsoft ACPI-Compliant System
(ISA) 0x00000133 (307) Microsoft ACPI-Compliant System
(ISA) 0x00000134 (308) Microsoft ACPI-Compliant System
(ISA) 0x00000135 (309) Microsoft ACPI-Compliant System
(ISA) 0x00000136 (310) Microsoft ACPI-Compliant System
(ISA) 0x00000137 (311) Microsoft ACPI-Compliant System
(ISA) 0x00000138 (312) Microsoft ACPI-Compliant System
(ISA) 0x00000139 (313) Microsoft ACPI-Compliant System
(ISA) 0x0000013A (314) Microsoft ACPI-Compliant System
(ISA) 0x0000013B (315) Microsoft ACPI-Compliant System
(ISA) 0x0000013C (316) Microsoft ACPI-Compliant System
(ISA) 0x0000013D (317) Microsoft ACPI-Compliant System
(ISA) 0x0000013E (318) Microsoft ACPI-Compliant System
(ISA) 0x0000013F (319) Microsoft ACPI-Compliant System
(ISA) 0x00000140 (320) Microsoft ACPI-Compliant System
(ISA) 0x00000141 (321) Microsoft ACPI-Compliant System
(ISA) 0x00000142 (322) Microsoft ACPI-Compliant System
(ISA) 0x00000143 (323) Microsoft ACPI-Compliant System
(ISA) 0x00000144 (324) Microsoft ACPI-Compliant System
(ISA) 0x00000145 (325) Microsoft ACPI-Compliant System
(ISA) 0x00000146 (326) Microsoft ACPI-Compliant System
(ISA) 0x00000147 (327) Microsoft ACPI-Compliant System
(ISA) 0x00000148 (328) Microsoft ACPI-Compliant System
(ISA) 0x00000149 (329) Microsoft ACPI-Compliant System
(ISA) 0x0000014A (330) Microsoft ACPI-Compliant System
(ISA) 0x0000014B (331) Microsoft ACPI-Compliant System
(ISA) 0x0000014C (332) Microsoft ACPI-Compliant System
(ISA) 0x0000014D (333) Microsoft ACPI-Compliant System
(ISA) 0x0000014E (334) Microsoft ACPI-Compliant System
(ISA) 0x0000014F (335) Microsoft ACPI-Compliant System
(ISA) 0x00000150 (336) Microsoft ACPI-Compliant System
(ISA) 0x00000151 (337) Microsoft ACPI-Compliant System
(ISA) 0x00000152 (338) Microsoft ACPI-Compliant System
(ISA) 0x00000153 (339) Microsoft ACPI-Compliant System
(ISA) 0x00000154 (340) Microsoft ACPI-Compliant System
(ISA) 0x00000155 (341) Microsoft ACPI-Compliant System
(ISA) 0x00000156 (342) Microsoft ACPI-Compliant System
(ISA) 0x00000157 (343) Microsoft ACPI-Compliant System
(ISA) 0x00000158 (344) Microsoft ACPI-Compliant System
(ISA) 0x00000159 (345) Microsoft ACPI-Compliant System
(ISA) 0x0000015A (346) Microsoft ACPI-Compliant System
(ISA) 0x0000015B (347) Microsoft ACPI-Compliant System
(ISA) 0x0000015C (348) Microsoft ACPI-Compliant System
(ISA) 0x0000015D (349) Microsoft ACPI-Compliant System
(ISA) 0x0000015E (350) Microsoft ACPI-Compliant System

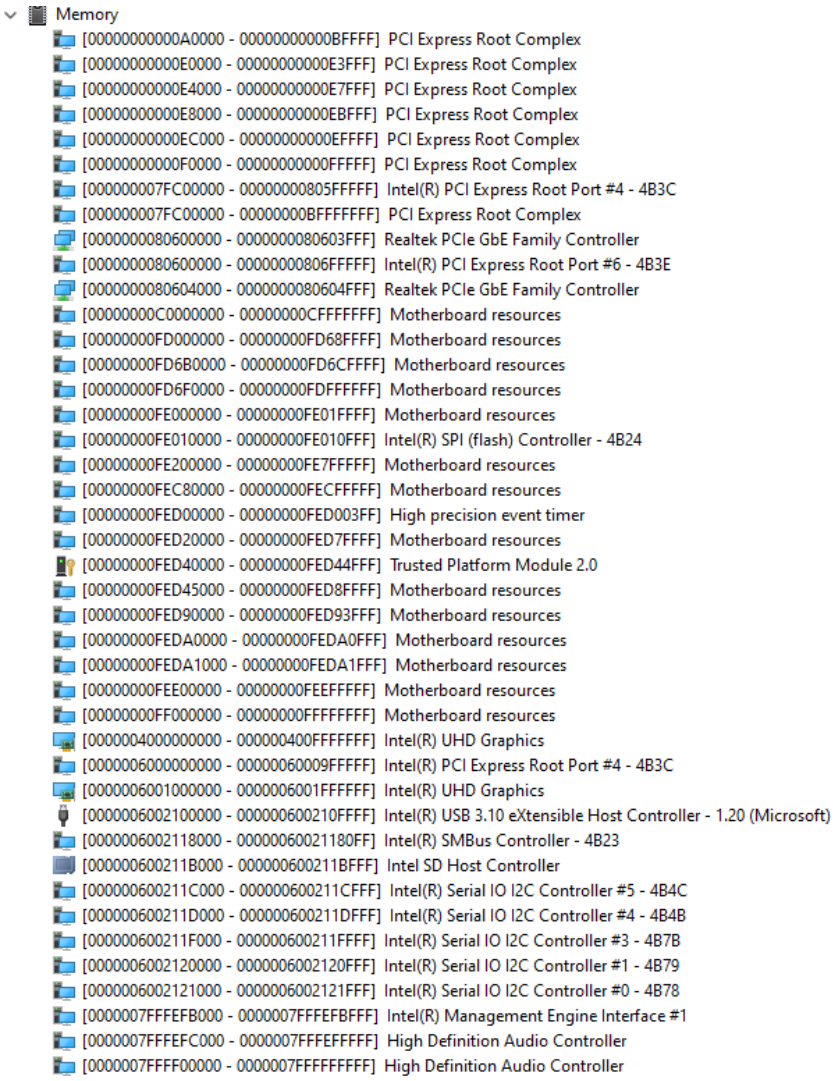
(ISA) 0x0000015F (351) Microsoft ACPI-Compliant System
(ISA) 0x00000160 (352) Microsoft ACPI-Compliant System
(ISA) 0x00000161 (353) Microsoft ACPI-Compliant System
(ISA) 0x00000162 (354) Microsoft ACPI-Compliant System
(ISA) 0x00000163 (355) Microsoft ACPI-Compliant System
(ISA) 0x00000164 (356) Microsoft ACPI-Compliant System
(ISA) 0x00000165 (357) Microsoft ACPI-Compliant System
(ISA) 0x00000166 (358) Microsoft ACPI-Compliant System
(ISA) 0x00000167 (359) Microsoft ACPI-Compliant System
(ISA) 0x00000168 (360) Microsoft ACPI-Compliant System
(ISA) 0x00000169 (361) Microsoft ACPI-Compliant System
(ISA) 0x0000016A (362) Microsoft ACPI-Compliant System
(ISA) 0x0000016B (363) Microsoft ACPI-Compliant System
(ISA) 0x0000016C (364) Microsoft ACPI-Compliant System
(ISA) 0x0000016D (365) Microsoft ACPI-Compliant System
(ISA) 0x0000016E (366) Microsoft ACPI-Compliant System
(ISA) 0x0000016F (367) Microsoft ACPI-Compliant System
(ISA) 0x00000170 (368) Microsoft ACPI-Compliant System
(ISA) 0x00000171 (369) Microsoft ACPI-Compliant System
(ISA) 0x00000172 (370) Microsoft ACPI-Compliant System
(ISA) 0x00000173 (371) Microsoft ACPI-Compliant System
(ISA) 0x00000174 (372) Microsoft ACPI-Compliant System
(ISA) 0x00000175 (373) Microsoft ACPI-Compliant System
(ISA) 0x00000176 (374) Microsoft ACPI-Compliant System
(ISA) 0x00000177 (375) Microsoft ACPI-Compliant System
(ISA) 0x00000178 (376) Microsoft ACPI-Compliant System
(ISA) 0x00000179 (377) Microsoft ACPI-Compliant System
(ISA) 0x0000017A (378) Microsoft ACPI-Compliant System
(ISA) 0x0000017B (379) Microsoft ACPI-Compliant System
(ISA) 0x0000017C (380) Microsoft ACPI-Compliant System
(ISA) 0x0000017D (381) Microsoft ACPI-Compliant System
(ISA) 0x0000017E (382) Microsoft ACPI-Compliant System
(ISA) 0x0000017F (383) Microsoft ACPI-Compliant System
(ISA) 0x00000180 (384) Microsoft ACPI-Compliant System
(ISA) 0x00000181 (385) Microsoft ACPI-Compliant System
(ISA) 0x00000182 (386) Microsoft ACPI-Compliant System
(ISA) 0x00000183 (387) Microsoft ACPI-Compliant System
(ISA) 0x00000184 (388) Microsoft ACPI-Compliant System
(ISA) 0x00000185 (389) Microsoft ACPI-Compliant System
(ISA) 0x00000186 (390) Microsoft ACPI-Compliant System
(ISA) 0x00000187 (391) Microsoft ACPI-Compliant System
(ISA) 0x00000188 (392) Microsoft ACPI-Compliant System
(ISA) 0x00000189 (393) Microsoft ACPI-Compliant System
(ISA) 0x0000018A (394) Microsoft ACPI-Compliant System
(ISA) 0x0000018B (395) Microsoft ACPI-Compliant System
(ISA) 0x0000018C (396) Microsoft ACPI-Compliant System
(ISA) 0x0000018D (397) Microsoft ACPI-Compliant System
(ISA) 0x0000018E (398) Microsoft ACPI-Compliant System
(ISA) 0x0000018F (399) Microsoft ACPI-Compliant System
(ISA) 0x00000190 (400) Microsoft ACPI-Compliant System
(ISA) 0x00000191 (401) Microsoft ACPI-Compliant System
(ISA) 0x00000192 (402) Microsoft ACPI-Compliant System
(ISA) 0x00000193 (403) Microsoft ACPI-Compliant System
(ISA) 0x00000194 (404) Microsoft ACPI-Compliant System
(ISA) 0x00000195 (405) Microsoft ACPI-Compliant System
(ISA) 0x00000196 (406) Microsoft ACPI-Compliant System
(ISA) 0x00000197 (407) Microsoft ACPI-Compliant System
(ISA) 0x00000198 (408) Microsoft ACPI-Compliant System
(ISA) 0x00000199 (409) Microsoft ACPI-Compliant System
(ISA) 0x0000019A (410) Microsoft ACPI-Compliant System
(ISA) 0x0000019B (411) Microsoft ACPI-Compliant System
(ISA) 0x0000019C (412) Microsoft ACPI-Compliant System
(ISA) 0x0000019D (413) Microsoft ACPI-Compliant System
(ISA) 0x0000019E (414) Microsoft ACPI-Compliant System
(ISA) 0x0000019F (415) Microsoft ACPI-Compliant System
(ISA) 0x000001A0 (416) Microsoft ACPI-Compliant System
(ISA) 0x000001A1 (417) Microsoft ACPI-Compliant System
(ISA) 0x000001A2 (418) Microsoft ACPI-Compliant System
(ISA) 0x000001A3 (419) Microsoft ACPI-Compliant System
(ISA) 0x000001A4 (420) Microsoft ACPI-Compliant System
(ISA) 0x000001A5 (421) Microsoft ACPI-Compliant System
(ISA) 0x000001A6 (422) Microsoft ACPI-Compliant System
(ISA) 0x000001A7 (423) Microsoft ACPI-Compliant System
(ISA) 0x000001A8 (424) Microsoft ACPI-Compliant System
(ISA) 0x000001A9 (425) Microsoft ACPI-Compliant System
(ISA) 0x000001AA (426) Microsoft ACPI-Compliant System
(ISA) 0x000001AB (427) Microsoft ACPI-Compliant System
(ISA) 0x000001AC (428) Microsoft ACPI-Compliant System
(ISA) 0x000001AD (429) Microsoft ACPI-Compliant System
(ISA) 0x000001AE (430) Microsoft ACPI-Compliant System
(ISA) 0x000001AF (431) Microsoft ACPI-Compliant System
(ISA) 0x000001B0 (432) Microsoft ACPI-Compliant System
(ISA) 0x000001B1 (433) Microsoft ACPI-Compliant System
(ISA) 0x000001B2 (434) Microsoft ACPI-Compliant System
(ISA) 0x000001B3 (435) Microsoft ACPI-Compliant System
(ISA) 0x000001B4 (436) Microsoft ACPI-Compliant System
(ISA) 0x000001B5 (437) Microsoft ACPI-Compliant System
(ISA) 0x000001B6 (438) Microsoft ACPI-Compliant System
(ISA) 0x000001B7 (439) Microsoft ACPI-Compliant System
(ISA) 0x000001B8 (440) Microsoft ACPI-Compliant System
(ISA) 0x000001B9 (441) Microsoft ACPI-Compliant System
(ISA) 0x000001BA (442) Microsoft ACPI-Compliant System
(ISA) 0x000001BB (443) Microsoft ACPI-Compliant System
(ISA) 0x000001BC (444) Microsoft ACPI-Compliant System
(ISA) 0x000001BD (445) Microsoft ACPI-Compliant System
(ISA) 0x000001BE (446) Microsoft ACPI-Compliant System
(ISA) 0x000001BF (447) Microsoft ACPI-Compliant System
(ISA) 0x000001C0 (448) Microsoft ACPI-Compliant System
(ISA) 0x000001C1 (449) Microsoft ACPI-Compliant System
(ISA) 0x000001C2 (450) Microsoft ACPI-Compliant System

(ISA) 0x000001C3 (451) Microsoft ACPI-Compliant System
(ISA) 0x000001C4 (452) Microsoft ACPI-Compliant System
(ISA) 0x000001C5 (453) Microsoft ACPI-Compliant System
(ISA) 0x000001C6 (454) Microsoft ACPI-Compliant System
(ISA) 0x000001C7 (455) Microsoft ACPI-Compliant System
(ISA) 0x000001C8 (456) Microsoft ACPI-Compliant System
(ISA) 0x000001C9 (457) Microsoft ACPI-Compliant System
(ISA) 0x000001CA (458) Microsoft ACPI-Compliant System
(ISA) 0x000001CB (459) Microsoft ACPI-Compliant System
(ISA) 0x000001CC (460) Microsoft ACPI-Compliant System
(ISA) 0x000001CD (461) Microsoft ACPI-Compliant System
(ISA) 0x000001CE (462) Microsoft ACPI-Compliant System
(ISA) 0x000001CF (463) Microsoft ACPI-Compliant System
(ISA) 0x000001D0 (464) Microsoft ACPI-Compliant System
(ISA) 0x000001D1 (465) Microsoft ACPI-Compliant System
(ISA) 0x000001D2 (466) Microsoft ACPI-Compliant System
(ISA) 0x000001D3 (467) Microsoft ACPI-Compliant System
(ISA) 0x000001D4 (468) Microsoft ACPI-Compliant System
(ISA) 0x000001D5 (469) Microsoft ACPI-Compliant System
(ISA) 0x000001D6 (470) Microsoft ACPI-Compliant System
(ISA) 0x000001D7 (471) Microsoft ACPI-Compliant System
(ISA) 0x000001D8 (472) Microsoft ACPI-Compliant System
(ISA) 0x000001D9 (473) Microsoft ACPI-Compliant System
(ISA) 0x000001DA (474) Microsoft ACPI-Compliant System
(ISA) 0x000001DB (475) Microsoft ACPI-Compliant System
(ISA) 0x000001DC (476) Microsoft ACPI-Compliant System
(ISA) 0x000001DD (477) Microsoft ACPI-Compliant System
(ISA) 0x000001DE (478) Microsoft ACPI-Compliant System
(ISA) 0x000001DF (479) Microsoft ACPI-Compliant System
(ISA) 0x000001E0 (480) Microsoft ACPI-Compliant System
(ISA) 0x000001E1 (481) Microsoft ACPI-Compliant System
(ISA) 0x000001E2 (482) Microsoft ACPI-Compliant System
(ISA) 0x000001E3 (483) Microsoft ACPI-Compliant System
(ISA) 0x000001E4 (484) Microsoft ACPI-Compliant System
(ISA) 0x000001E5 (485) Microsoft ACPI-Compliant System
(ISA) 0x000001E6 (486) Microsoft ACPI-Compliant System
(ISA) 0x000001E7 (487) Microsoft ACPI-Compliant System
(ISA) 0x000001E8 (488) Microsoft ACPI-Compliant System
(ISA) 0x000001E9 (489) Microsoft ACPI-Compliant System
(ISA) 0x000001EA (490) Microsoft ACPI-Compliant System
(ISA) 0x000001EB (491) Microsoft ACPI-Compliant System
(ISA) 0x000001EC (492) Microsoft ACPI-Compliant System
(ISA) 0x000001ED (493) Microsoft ACPI-Compliant System
(ISA) 0x000001EE (494) Microsoft ACPI-Compliant System
(ISA) 0x000001EF (495) Microsoft ACPI-Compliant System
(ISA) 0x000001F0 (496) Microsoft ACPI-Compliant System
(ISA) 0x000001F1 (497) Microsoft ACPI-Compliant System
(ISA) 0x000001F2 (498) Microsoft ACPI-Compliant System
(ISA) 0x000001F3 (499) Microsoft ACPI-Compliant System
(ISA) 0x000001F4 (500) Microsoft ACPI-Compliant System

(ISA) 0x000001F5 (501) Microsoft ACPI-Compliant System
(ISA) 0x000001F6 (502) Microsoft ACPI-Compliant System
(ISA) 0x000001F7 (503) Microsoft ACPI-Compliant System
(ISA) 0x000001F8 (504) Microsoft ACPI-Compliant System
(ISA) 0x000001F9 (505) 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) 0x00000010 (16) Intel SD Host Controller
(PCI) 0xFFFFFFF9 (-7) Intel(R) Management Engine Interface #1
(PCI) 0xFFFFFFFA (-6) Intel(R) UHD Graphics
(PCI) 0xFFFFFFFB (-5) Intel(R) USB 3.10 eXtensible Host Controller - 1.20 (Microsoft)
(PCI) 0xFFFFFFFC (-4) Realtek PCIe GbE Family Controller
(PCI) 0xFFFFFFFD (-3) Intel(R) PCI Express Root Port #6 - 4B3E
(PCI) 0xFFFFFFFE (-2) Intel(R) PCI Express Root Port #4 - 4B3C

3.6 Memory Map

The memory mapping list is shown as follows:



This page is intentionally left blank.

Section 4
AMI BIOS Setup Utility

The AMI UEFI BIOS provides users with a built-in setup program to modify basic system configuration. All configured parameters are stored in a flash chip to save the setup information whenever the power is turned off. This section provides users with detailed description about how to set up basic system configuration through the AMI BIOS setup utility.

4.1 Starting

To enter the setup screens, follow the steps below:

1. Turn on the computer and press the <Del> key immediately.
2. After you press the <Del> key, the main BIOS setup menu displays. You can access the other setup screens, such as the Advanced and Chipset menus, from the main BIOS setup menu.

It is strongly recommended that you should avoid changing the chipset's defaults. Both AMI and your system manufacturer have carefully set up these defaults that provide the best performance and reliability.

4.2 Navigation Keys

The BIOS setup/utility uses a key-based navigation system called hot keys. Most of the BIOS setup utility hot keys can be used at any time during the setup navigation process. These keys include <F1>, <F2>, <Enter>, <ESC>, <Arrow> keys, and so on.

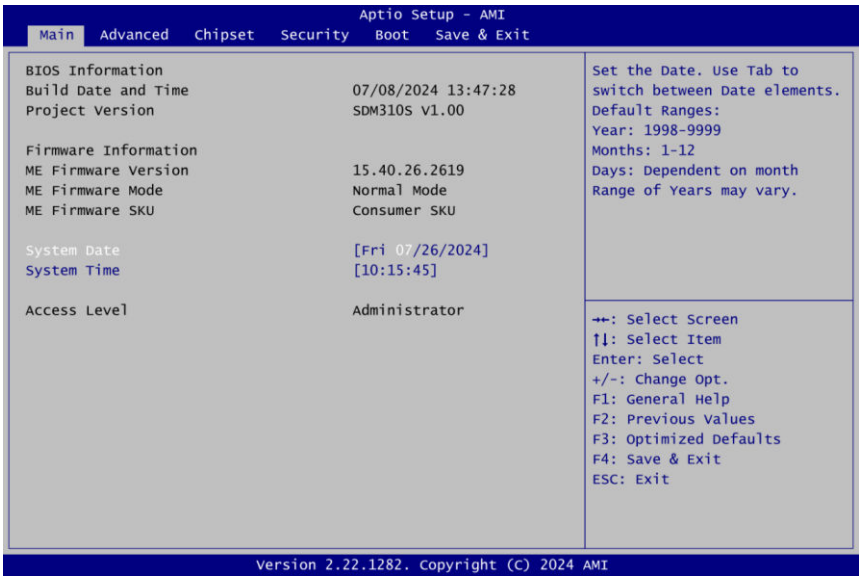
Note

Some of the navigation keys differ from one screen to another.

Hot Keys	Description
→← **Left/Right**	The Left and Right <Arrow> keys allow you to select a setup screen.
↑↓ **Up/Down**	The Up and Down <Arrow> keys allow you to select a setup screen or sub-screen.
+– Plus/Minus	The Plus and Minus <Arrow> keys allow you to change the field value of a particular setup item.
Tab	The <Tab> key allows you to select setup fields.
F1	The <F1> key allows you to display the General Help screen.
F2	The <F2> key allows you to load previous values.
F3	The <F3> key allows you to load optimized defaults.
F4	The <F4> key allows you to save any changes you have made and exit Setup. Press the <F4> key to save your changes.
Esc	The <Esc> key allows you to discard any changes you have made and exit the Setup. Press the <Esc> key to exit the setup without saving your changes.
Enter	The <Enter> key allows you to display or change the setup option listed for a particular setup item. The <Enter> key can also allow you to display the setup sub-screens.

4.3 Main Menu

The Main BIOS setup screen is the first screen you see when entering the setup utility. You can always return to the Main BIOS setup screen by selecting the Main tab. System Time/Date can be set up as described below. The Main BIOS setup screen is also shown below.



BIOS Information
Display BIOS and ME firmware information.

System Date/Time
Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time is entered in HH:MM:SS format.

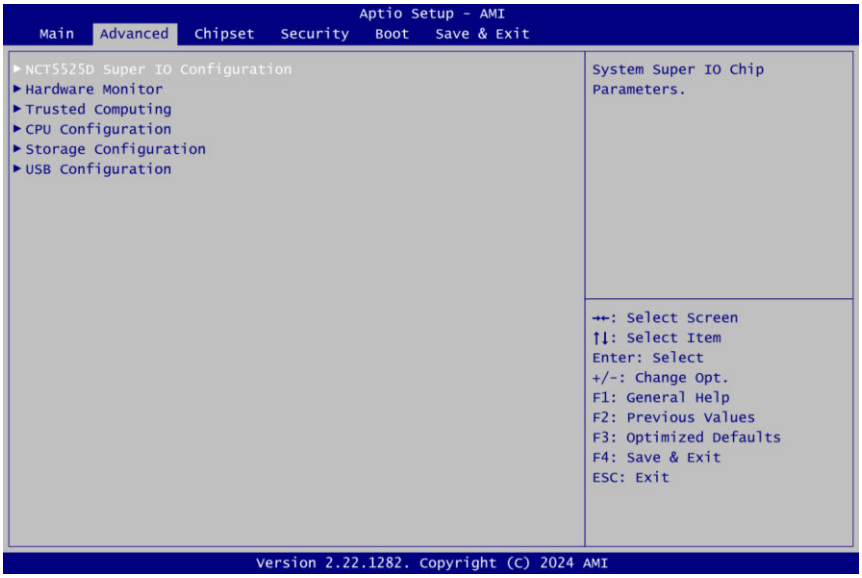
4.4 Advanced Menu

The Advanced menu also allows users to set configuration of the CPU and other system devices. You can select any of the items in the left frame of the screen to go to the sub menus:

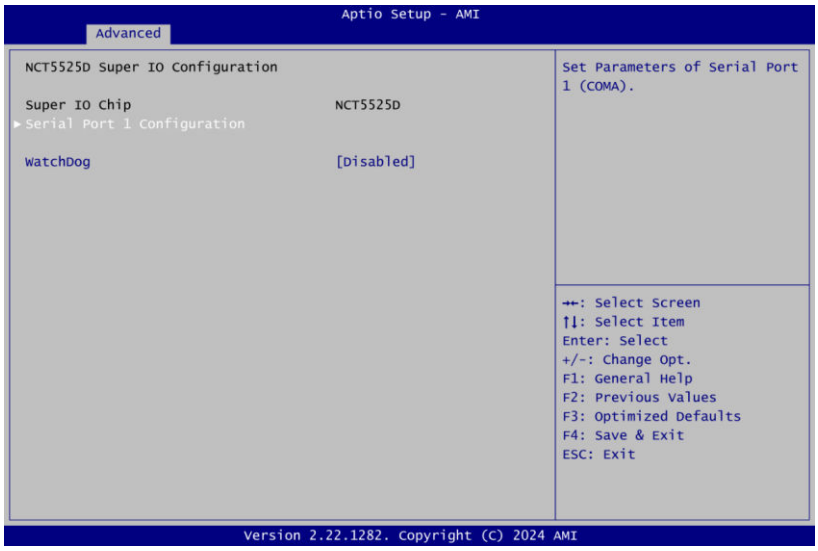
- ► NCT5525D Super IO Configuration
- ► Hardware Monitor
- ► Trusted Computing
- ► CPU Configuration
- ► Storage Configuration
- ► USB Configuration

已註解 **[jeremy2]:** The menu item order appears inconsistent with the screenshot below.

For items marked with "►", please press <Enter> for more options.

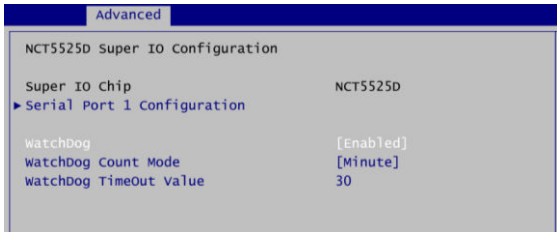


- **NCT5525D Super IO Configuration**
  You can use this screen to select options for the Super IO Configuration, and change the value of the selected option. A description of the selected item appears on the right side of the screen. For items marked with "►", please press <Enter> for more options.



Serial Port 1 Configuration
Use this item to set parameters related to serial port 1.

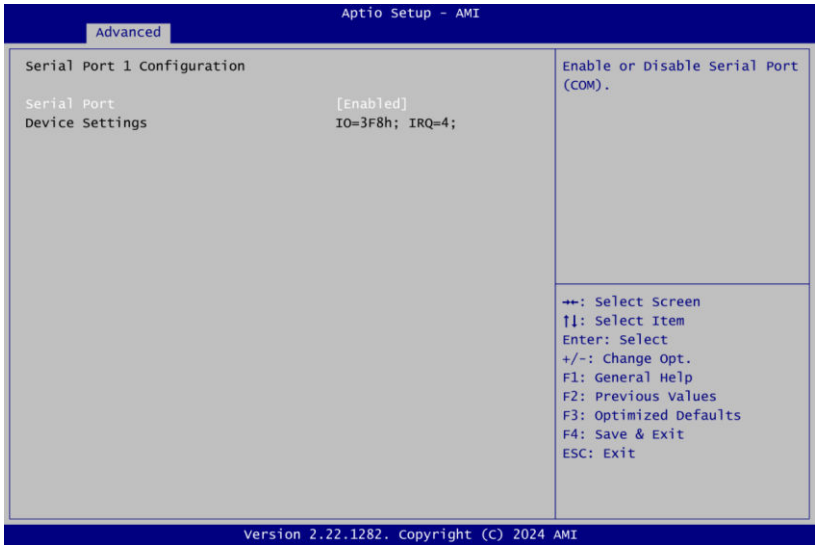
WatchDog
Enable or disable WatchDog.



When WatchDog is enabled, the following items will appear:
WatchDog Count Mode
Use this item to select WatchDog count mode.

WatchDog TimeOut Value
Fill in with WatchDog timeout value, where 0 means disabled.

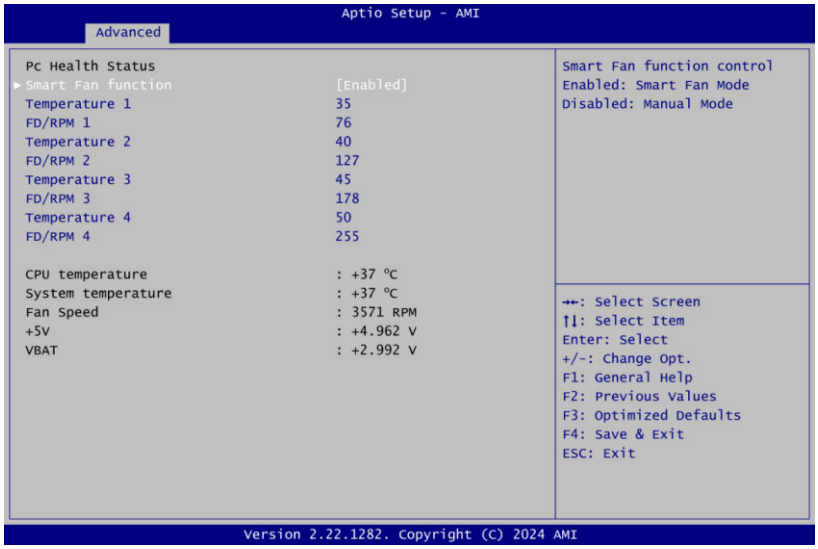
- **Serial Port 1 Configuration**



Serial Port
Enable or disable serial port 1. The optimal setting for base I/O address is 3F8h and for interrupt request line is IRQ4. The default setting is Enabled.

- **Hardware Monitor**
  This menu allows the user to monitor hardware health status as well as enable or disable the Smart Fan function.

已註解 **[jeremy3]:** Please check the accuracy of this description.



This screen displays the temperature of system and CPU, fan speed, system voltages (+5V and VBAT).

Smart Fan function
Enable or disable Smart Fan function.
- Enabled: Select Smart Fan mode.
- Disable: Select manual mode.
- The default setting is Enabled.

Temperature 1/2/3/4
When system temperature is higher than threshold of Temperature 1/2/3/4, the system fan will spin faster according to FD/RPM 1/2/3/4 setting.

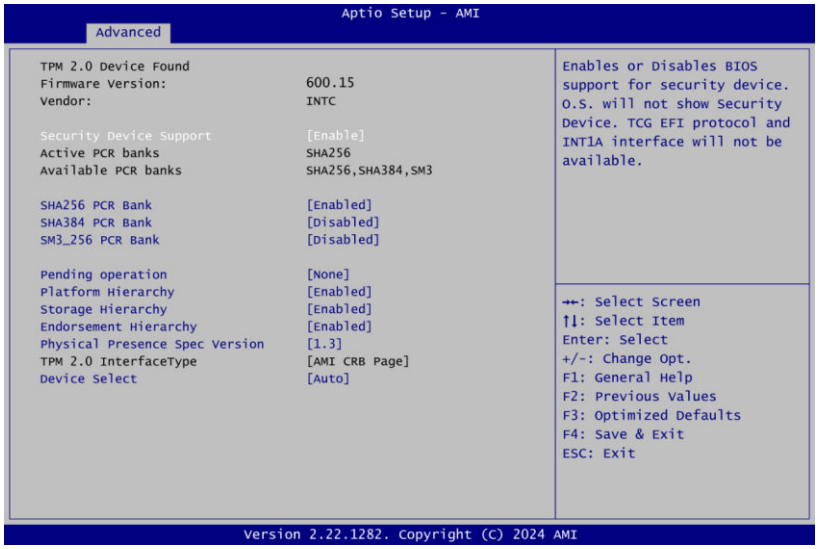
FD/RPM 1
Default is 76, which means 76/255 = 30% of PWM.

FD/RPM 2
Default is 127, which means 127/255 = 50% of PWM.

FD/RPM 3
Default is 178, which means 178/255 = 70% of PWM.

FD/RPM 4
Default is 255, which means 255/255 = 100% of PWM.

- **Trusted Computing**
  This menu contains settings related to the Trusted Platform Module (TPM) and other security features.



Security Device Support
Enable or disable BIOS support for security device, typically a TPM. When enabled (default setting), the BIOS initializes and makes the TPM available for use by the operating system and other system components. When disabled, the TPM is effectively hidden from the OS, and critical security functions, such as secure boot and disk encryption, may not function. Additionally, TCG EFI protocols and the INT1A interface, which are used for secure boot and other trusted computing tasks, will not be available.

SHA256 PCR Bank
Enable or disable SHA256 hashing algorithm for PCR (Platform Configuration Register) Bank within the TPM.

SHA384 PCR Bank
Enable or disable SHA384 hashing algorithm for PCR Bank within the TPM.

SM3_256 PCR Bank
Enable or disable SM3_256 cryptographic hash algorithm for PCR Bank.

Pending operation
Schedule an operation for the security device.
- None
- TPM Clear: Clear all data secured by TPM.

Note that your computer will reboot during restart in order to change State of Security Device.

Platform Hierarchy
Enable or disable platform hierarchy, used to manage keys and operations related to the entire platform.

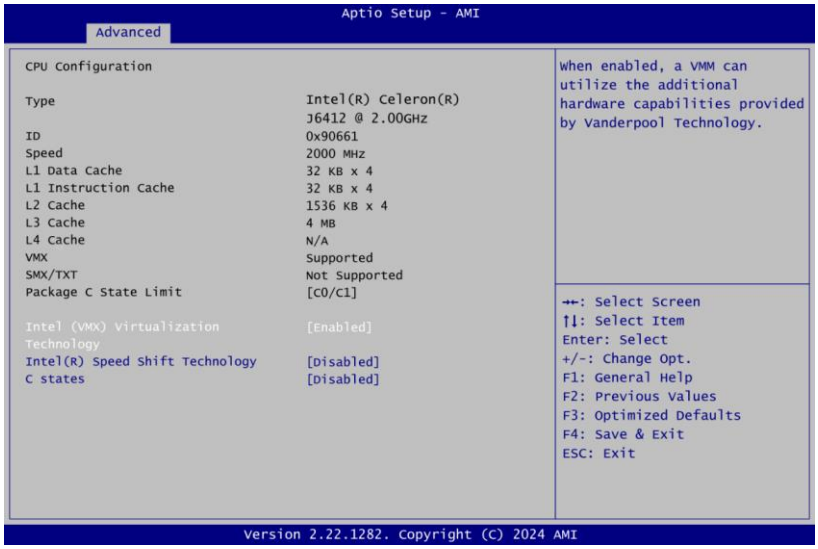
Storage Hierarchy
Enable or disable storage hierarchy, used to manage keys and operations related to data storage.

Endorsement Hierarchy
Enable or disable endorsement hierarchy, used to manage keys and operations related to the TPM's endorsement keys.

Physical Presence Spec Version
This setting allows you to select the version of the Physical Presence Interface (PPI) Specification: Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.

Device Select
This setting determines which version of the TPM is supported and active on your system
- TPM 1.2: Restrict support to only TPM 1.2 devices.
- TPM 2.0: Restrict support to only TPM 2.0 devices.
- Auto: This option provides flexibility by supporting both TPM 1.2 and TPM 2.0 devices. The system will default to TPM 2.0 if it is available, and will fall back to TPM 1.2 if TPM 2.0 is not found.

- **CPU Configuration**
  This screen shows the CPU Configuration, and you can change the value of the selected option.



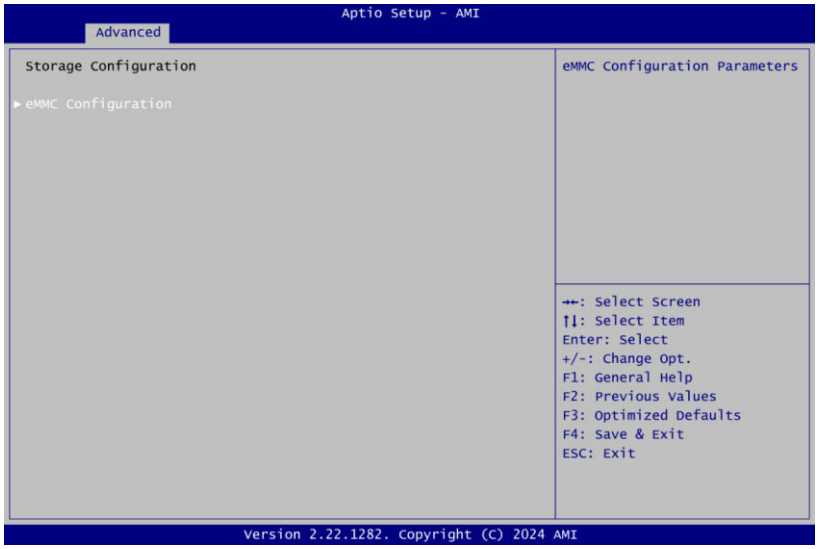
Intel (VMX) Virtualization Technology
Enable or disable Intel Virtualization Technology. When enabled, a VMM (Virtual Machine Mode) can utilize the additional hardware capabilities. It allows a platform to run multiple operating systems and applications independently, hence enabling a single computer system to work as several virtual systems. The default setting is Enabled.

Intel(R) Speed Shift Technology
Enable or disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.

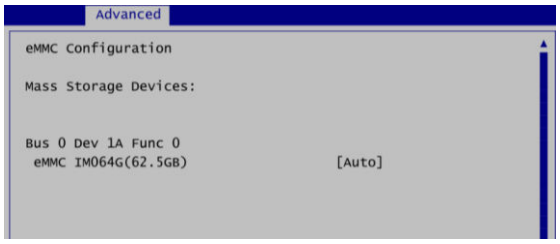
Turbo Mode
Enable or disable processor Turbo Mode. The processor can be up to maximum turbo frequency when the system loading becomes higher. The default setting is Enabled.

C states
Enable or disable CPU power management. Allows CPU to go to C states when it's not 100% utilized.

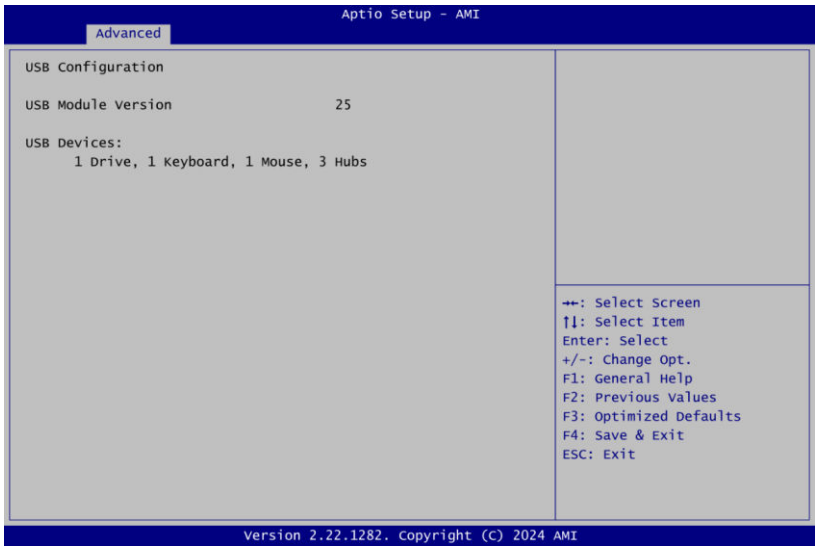
- **Storage Configuration**
  This screen specifies storage information. For items marked with "▸", please press <Enter> for more options.



Specifies eMMC storage information as follows:



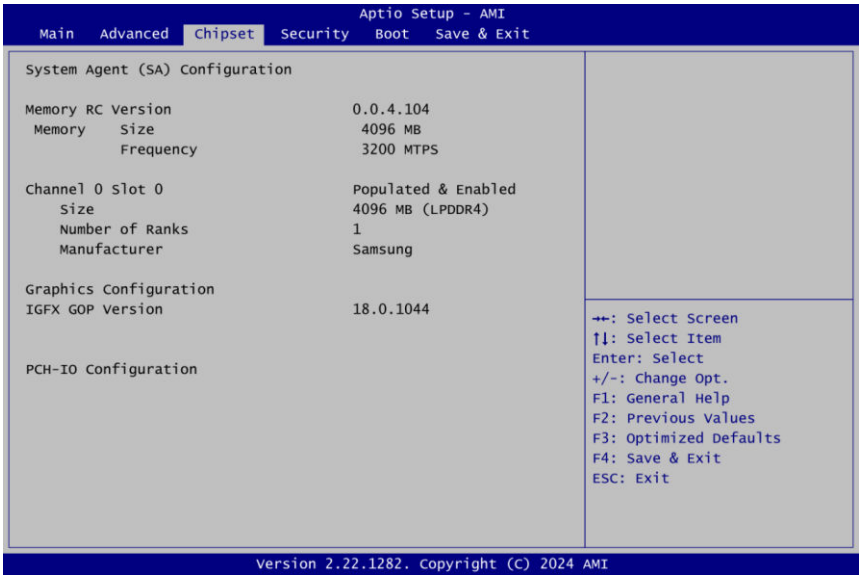
- **USB Configuration**
  This screen specifies USB settings.



USB Devices
Display all detected USB devices.

4.5 Chipset Menu

The Chipset menu shows memory configuration parameters dan graphics configuration version.



4.6 Security Menu

The Security menu allows users to enhance system security by creating an administrator password to limit system access.

Administrator Password
This item indicates whether an administrator password has been set (installed or uninstalled).

User Password
This item indicates whether a user password has been set (installed or uninstalled).

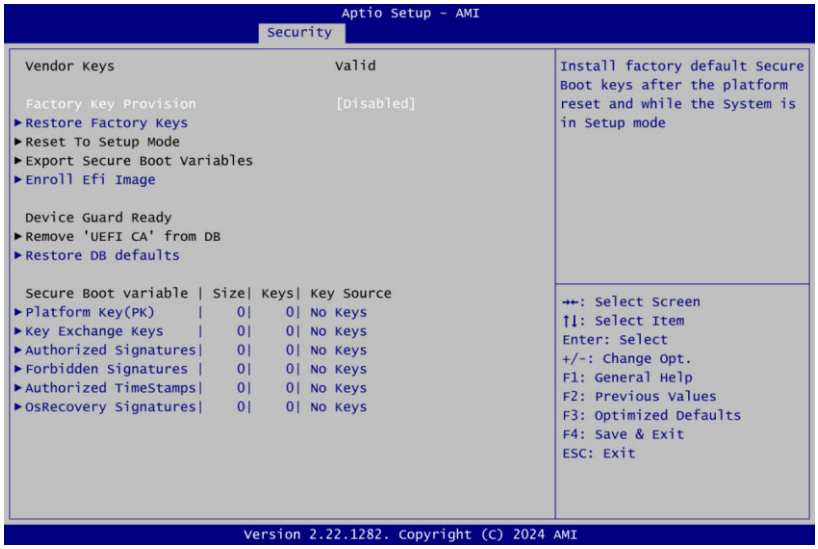
- **Secure Boot**

Secure Boot
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 ensures that the system only boots from trusted software, preventing malicious software from loading and compromising the device. It checks the digital signatures of boot loaders, firmware, and operating systems to verify that they are from trusted sources and have not been tampered with. Users can choose to enable it or not, between standard and custom mode. The default setting is secure boot.

Secure Boot Mode
Secure Boot mode options: Standard or Custom. In Custom mode, the policy of Secure Boot variables can be configured by a physically present user without full authentication. The default setting is custom.

Restore Factory Keys
Force system to user mode. Install factory default secure boot key databases.

Key Management
Enables expert users to modify secure boot policy variables without full authentication.

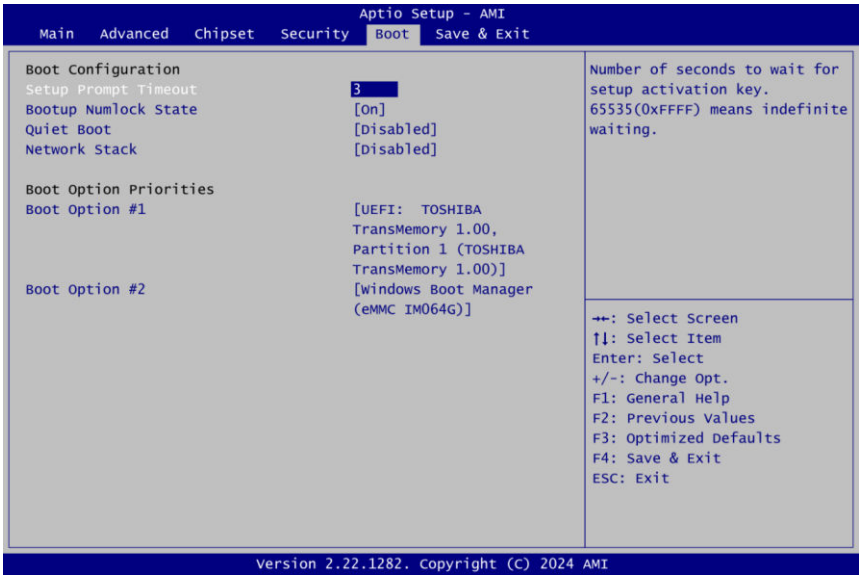


Factory Key Provision

The Factory Key Provision ensures that the device has secure access to encrypted resources, such as data storage or communication. The keys are often unique to each device and can be used to secure firmware updates, secure boot processes, and to encrypt data at rest. The factory key provisioning process is an important step in securing devices and maintaining the confidentiality of sensitive information.

4.7 Boot Menu

The Boot menu allows users to change boot options of the system.



- **Setup Prompt Timeout**
  Setup Prompt Timeout is to delay the BIOS post before entering the operating system for a period of seconds according to user's setting. The default setting is 1.

- **Bootup NumLock State**
  Use this item to select the power-on state for the keyboard NumLock. The default setting is On.

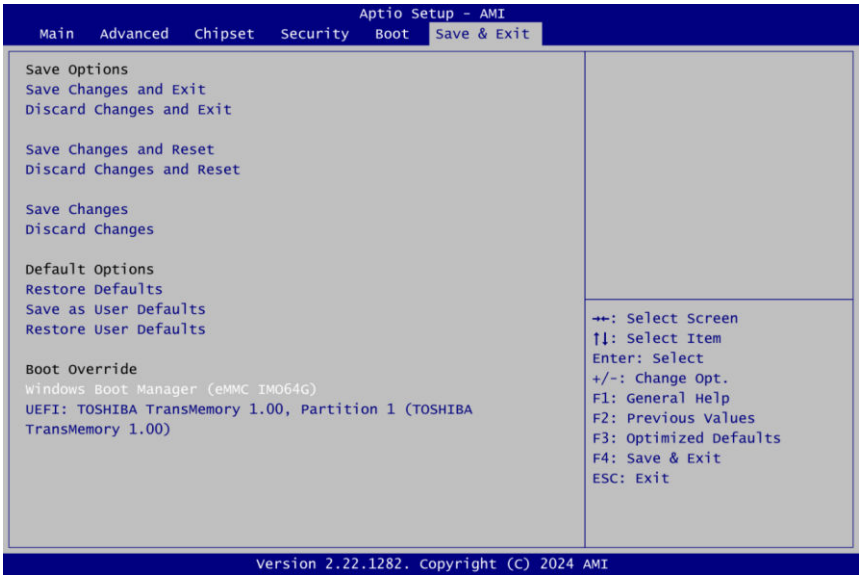
- **Quiet Boot**
  Quiet boot is a boot process that is performed without displaying diagnostic or status information on the screen. The default setting is On. The default setting is disable.

- **Network Stack**
  Enable or disable UEFI Network stack.

- **Boot Option Priorities [Boot Option #1, Boot Option #2]**
  These are settings for boot priority. Specify the boot device priority sequence from the available devices.

4.8 Save & Exit Menu

The Save & Exit menu allows users to load system configurations with optimal or fail-safe default values.



- **Save Changes and Exit**
  When you have completed the system configuration changes, select this option to leave Setup and continue to boot to operating system. Select Save Changes and Exit from the Save & Exit menu and press <Enter>. Select Yes to save changes and exit.

- **Discard Changes and Exit**
  Select this option to quit Setup without making any permanent changes to the system configuration and continue to boot to operating system. Select Discard Changes and Exit from the Save & Exit menu and press <Enter>. Select Yes to discard changes and exit.

- **Save Changes and Reset**
  When you have completed the system configuration changes, select this option to leave Setup and reboot the computer so the new system configuration parameters can take effect. Select Save Changes and Reset from the Save & Exit menu and press <Enter>. Select Yes to save changes and reset.

- **Discard Changes and Reset**
  Select this option to quit Setup without making any permanent changes to the system configuration and reboot the computer. Select Discard Changes and Reset from the Save & Exit menu and press <Enter>. Select Yes to discard changes and reset.

- **Save Changes**
  When you have completed the system configuration changes, select this option to save changes. Select Save Changes from the Save & Exit menu and press <Enter>. Select Yes to save changes.

已註解 [jeremy4]: 其他手冊如 DSP 寫 “return to Main Menu”，請再確認

已註解 [jeremy5]: 其他手冊如 DSP 寫 “return to Main Menu”，請再確認

- **Discard Changes**
  Select this option to quit Setup without making any permanent changes to the system configuration. Select Discard Changes from the Save & Exit menu and press <Enter>. Select Yes to discard changes.

- **Restore Defaults**
  It automatically sets all Setup options to a complete set of default settings when you select this option. Select Restore Defaults from the Save & Exit menu and press <Enter>.

- **Save as User Defaults**
  Select this option to save system configuration changes done so far as User Defaults. Select Save as User Defaults from the Save & Exit menu and press <Enter>.

- **Restore User Defaults**
  It automatically sets all Setup options to a complete set of User Defaults when you select this option. Select Restore User Defaults from the Save & Exit menu and press <Enter>.

- **Boot Override**
  Select a drive to immediately boot that device regardless of the current boot order.

This page is intentionally left blank.

Appendix A
Watchdog Timer

A.1 About Watchdog Timer

Software stability is a major issue in most application. Some embedded systems are not watched by human for 24 hours. It is usually too slow to wait for someone to reboot when computer hangs. The systems need to be able to reset automatically when things go wrong. The watchdog timer gives us solutions in this regard.

The watchdog timer is a counter that triggers a system reset when it counts down to zero from a preset value. The software starts the counter with an initial value and must reset it periodically. If the counter ever reaches zero which means the software has crashed, the system will reboot.

A.2 How to Use Watchdog Timer

```
#include <stdio.h>
#include <conio.h>
#include <bios.h>

#define UINT unsigned int
#define NCT5104IO           0x2E

int main()
{
    UINT WDT_mode = 0;        // 00H for second, 08h for minute
    UINT WDT_Count = 0;       // Range from 00 to FF

    //Un-lock super I/O
    outp( NCT5104IO, 0x87 );
    outp( NCT5104IO, 0x87 );

    //Select Logic device
    outp( NCT5104IO, 0x07 );
    outp( NCT5104IO+1, 0x08 );

    //Enable WDT
    outp( NCT5104IO, 0x30 );
    outp( NCT5104IO+1, 0x01 );

    //Set Count mode
    outp( NCT5104IO, 0xF0 );
    outp( NCT5104IO+1, WDT_mode );
```

```
    //WDT counting re-set timer
    outp( NCT5104IO, 0xF1 );
    outp( NCT5104IO+1, WDT_Count );

    // IF to disable WDT:
    //outp( NCT5104IO, 0x30 );
    //outp( NCT5104IO+1, 0x00 );

    return 0;
}
```