

USER'S MANUAL

CEM561

**12/13th Generation Intel® Core
i7/i5/i3 and Celeron processors
COM Express Type 6 Compact
Module**

User's Manual



www.axiomtek.com

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

July 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 take care of the following jobs with 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 integrated circuit, touch an unpainted portion of the system unit chassis for a few seconds. It discharges static electricity from your body.
- Wear a wrist-grounding strap, available from most electronic component stores, when handling modules and components.

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

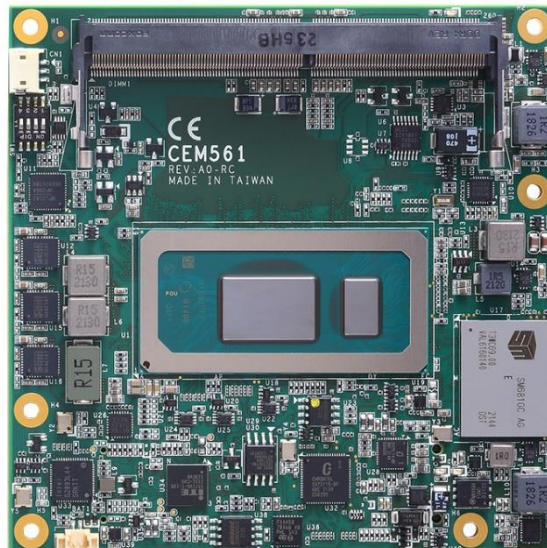
Disclaimers.....	ii
ESD Precautions	iii
Section 1 Introduction.....	1
1.1 Features	1
1.2 Specifications.....	2
1.3 Utilities Supported	3
1.4 Block diagram	4
Section 2 Module and Pin Assignments.....	5
2.1 Module Dimensions and Fixing Holes.....	5
2.2 Module Layout.....	6
2.3 Installing Thermal Solution	8
2.4 Switch Settings	10
2.4.1 Auto Power On and Restore BIOS Optimal Defaults (SW1 1 & 2)	10
2.4.2 PCI-Express Bifurcation Setting (SW1 3 & 4)	10
2.5 Connector	11
2.5.1 Fan Connector (CN1).....	11
2.5.2 CMOS Battery Connector (BAT)	11
2.5.3 COM Express™ Connector (SS1 and SS2).....	12
Section 3 Hardware Description	15
3.1 Microprocessor	15
3.2 BIOS	15
3.3 System Memory.....	15
3.4 I/O Port Address Map.....	16
3.5 Interrupt Controller (IRQ) Map	17
3.6 Memory Map	22
Section 4 AMI BIOS Setup Utility	23
4.1 Starting.....	23
4.2 Navigation Keys	23
4.3 Main Menu.....	25
4.4 Advanced Menu.....	26
4.5 Chipset Menu.....	44

4.6	Security Menu.....	49
4.7	Boot Menu.....	51
4.8	Save & Exit Menu	53
Appendix A Watchdog Timer.....		57
A.1	About Watchdog Timer	57
A.2	How to Use Watchdog Timer (C programming language)	57
Appendix B Digital I/O		59
B.1	About Digital I/O	59
B.2	How to Use Digital I/O (C programming language)	59
Appendix C iAMT Settings		61
C.1	iAMT Settings	61
C.2	iAMT Web Console.....	66

This page is intentionally left blank.

Section 1

Introduction



The CEM561 is a new COM Express™ Type 6 Compact Module supporting Intel® Core™ 12th 13th processor. It delivers outstanding system performance and support excellent multiple I/Os like LVDS, 2.5 Gigabit Ethernet, HD Audio interface, dual SATA 3.0, four USB 3.2gen2 and eight USB 2.0 ports. For extension purpose, it provides up to 12 lanes of PCI-Express by maximum Gen 4 throughput which could fulfill various applications with high computing requirement.

1.1 Features

- Intel® Core™ 12th i7-1265UE/i5-1245UE/i3-1215UE processor and Intel® Celeron® processor 7305UE
- Intel® Core™ 13th i7-1365URE/i5-1345URE/i3-1315URE processor
- Two SO-DIMMs supporting up to 64 GB memory capacity
- Support max. up to 12 lanes of PCI-Express
- 2 SATA 3.0
- 4 USB 3.2 gen2 and 8 USB 2.0 ports

1.2 Specifications

- **CPU**
 - Intel® Core™ i7-1265UE
 - Intel® Core™ i5-1245UE
 - Intel® Core™ i3-1215UE
 - Intel® Celeron® 7305UE
 - Intel® Core™ i7-1365URE
 - Intel® Core™ i5-1345URE
 - Intel® Core™ i3-1315URE

- **BIOS**
 - American Megatrends Inc. BIOS.
 - UEFI only.

- **System Memory**
 - Two 260-pin DDR4 3200MHz SO-DIMM sockets support maximum memory capacity up to 64GB.

- **Expansion Interface**
 - 1 x PCIe 4.0 x4 (PEG)
 - 5 x PCIe 3.0 x1 (maximum is up to 8x PCIe 3.0x1 by request)

- **USB Interface**
 - Four USB ports comply with USB 3.2 Gen2
 - Eight USB ports comply with USB 2.0

- **SATA Interface**
 - Dual SATA 6Gb/s ports supported through COM Express™ connector.

- **TPM**
 - Trusted Platform Module compatible with TPM2.0 Main and PC Client specification based on Intel LPC Bus Interface.

- **Graphics & Display**
 - Intel® integrated UHD Graphic.
 - Gfx - DX12.0, OCL2.0, OGL4.3.
 - 1 x LVDS; 18/24-bit single/dual channel (optional eDP 1.4b: 4096 x 2304 @60Hz).
 - 1 x VGA up to 1920 x 1200 @60Hz (default).
 - 2 x DDI (support maximum resolution up to 8K)

- **Ethernet**
 - One 2500/1000/100/10 Base-T provided by Intel® I226LM supports Wake-on-LAN, PXE Boot ROM, iAMT.

- **Audio**
 - Intel® High Definition Audio interface.

- **Operating Temperature**
 - -40°C to +85°C (-40°F to +185°F)

- **Power Input**
 - ATX: +12V, +5VSB.
 - AT: +12V.

- **Power Management**
 - ACPI (Advanced Configuration and Power Interface).
- **Form Factor**
 - Compact module 95mm x 95mm.

1.3 Utilities Supported

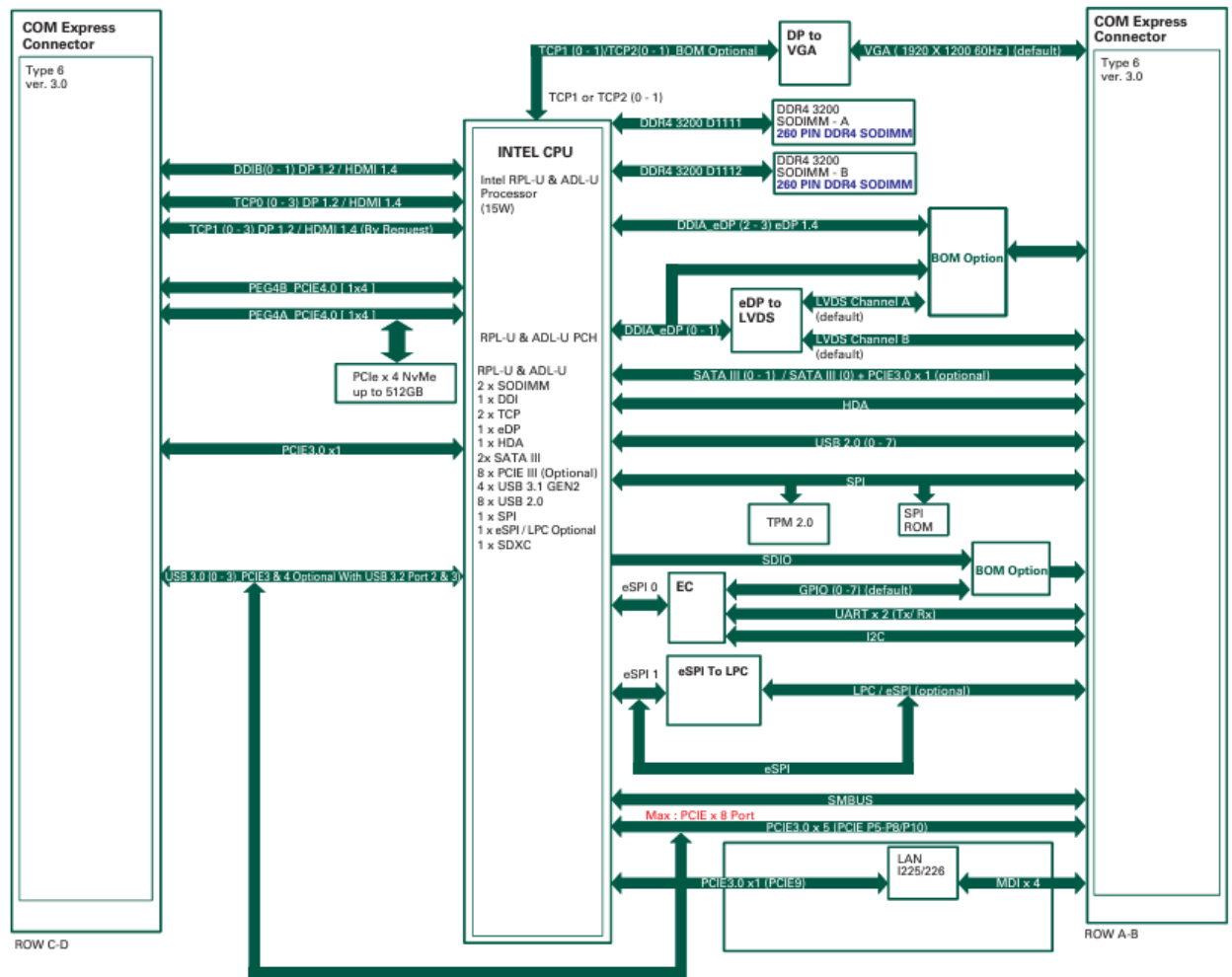
- Chipset driver
- Graphics driver
- Serial Patch_v3.0.6.7MS
- Rapid Storage Technology
- Management Engine Firmware
- Intel Network Connection



Note

All specifications and images are subject to change without notice.

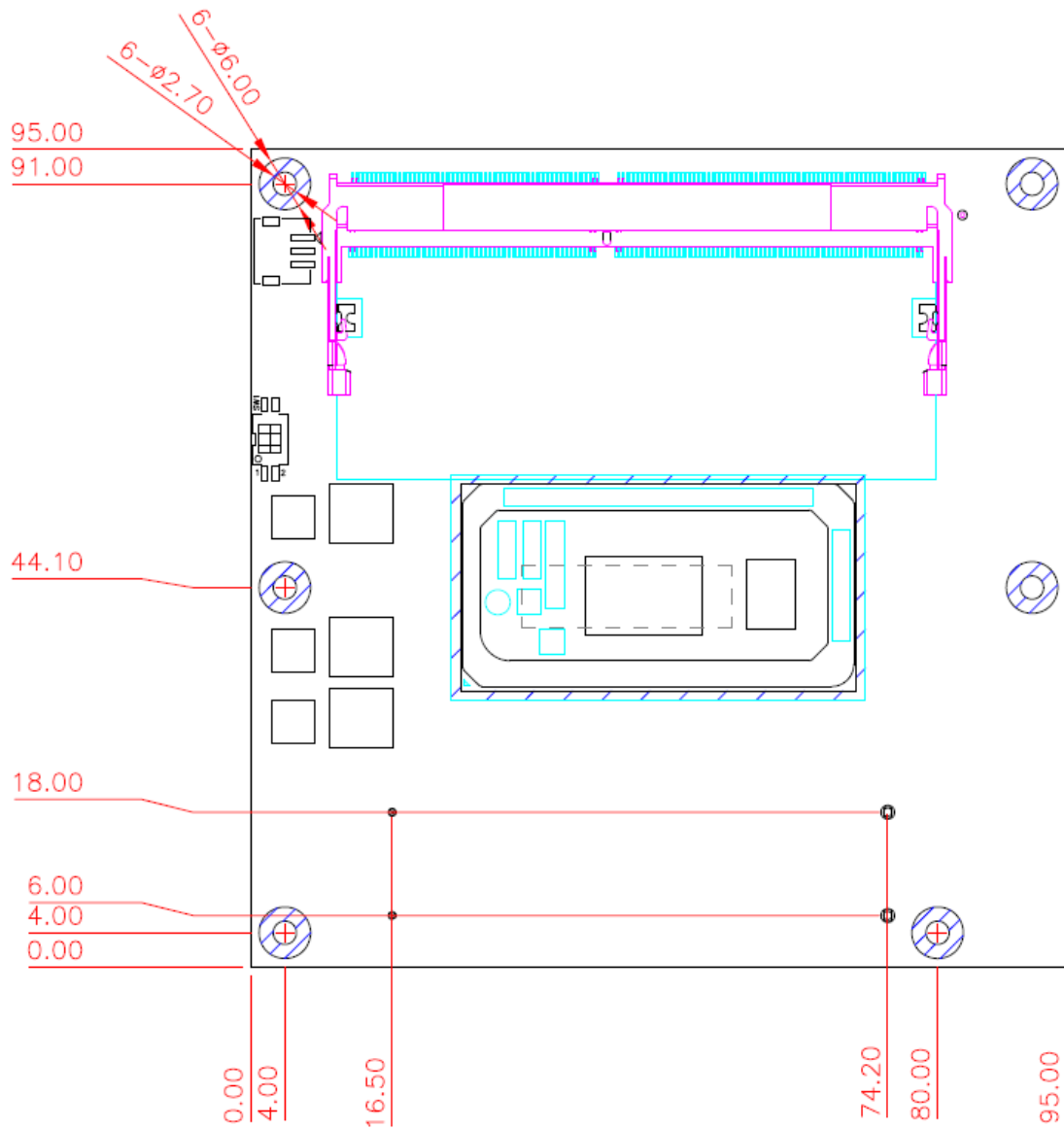
1.4 Block diagram



Section 2

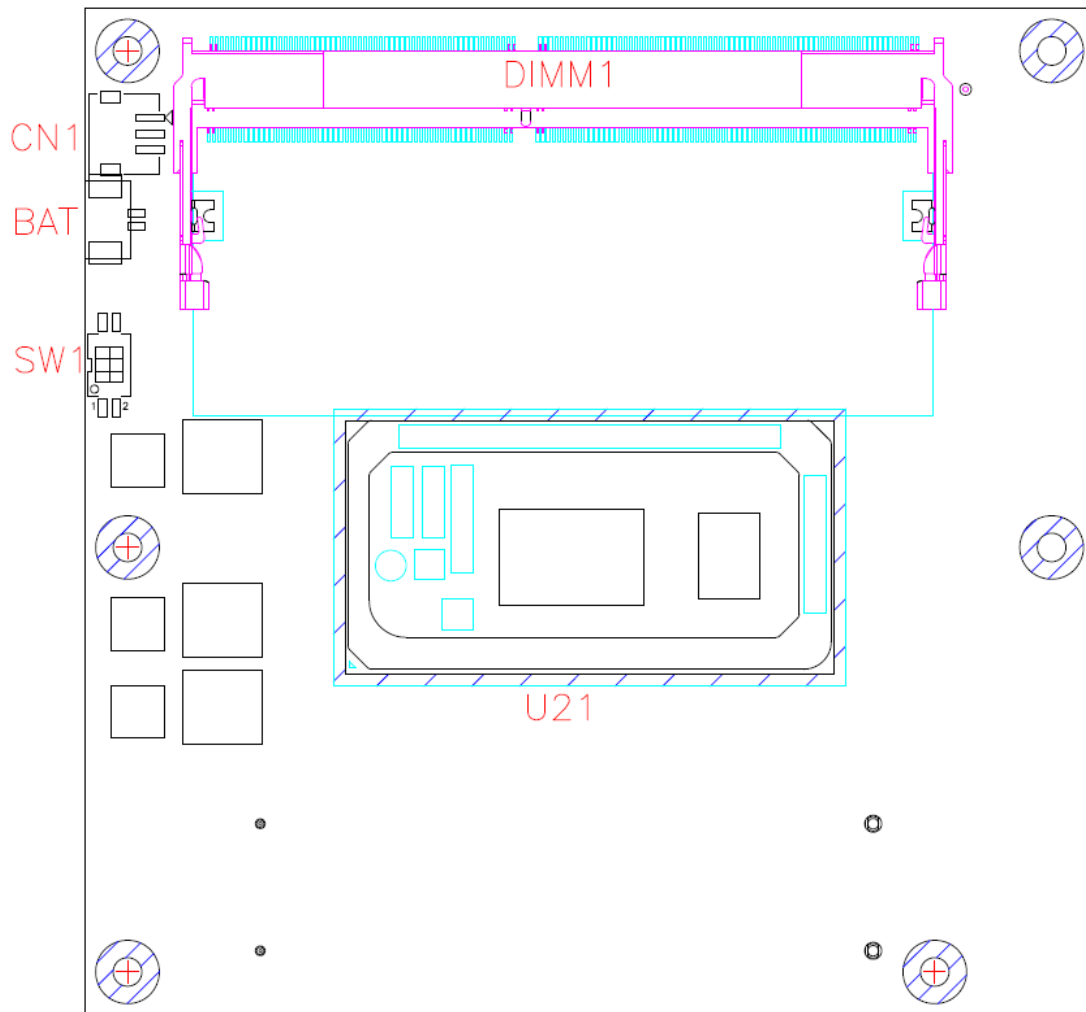
Module and Pin Assignments

2.1 Module Dimensions and Fixing Holes

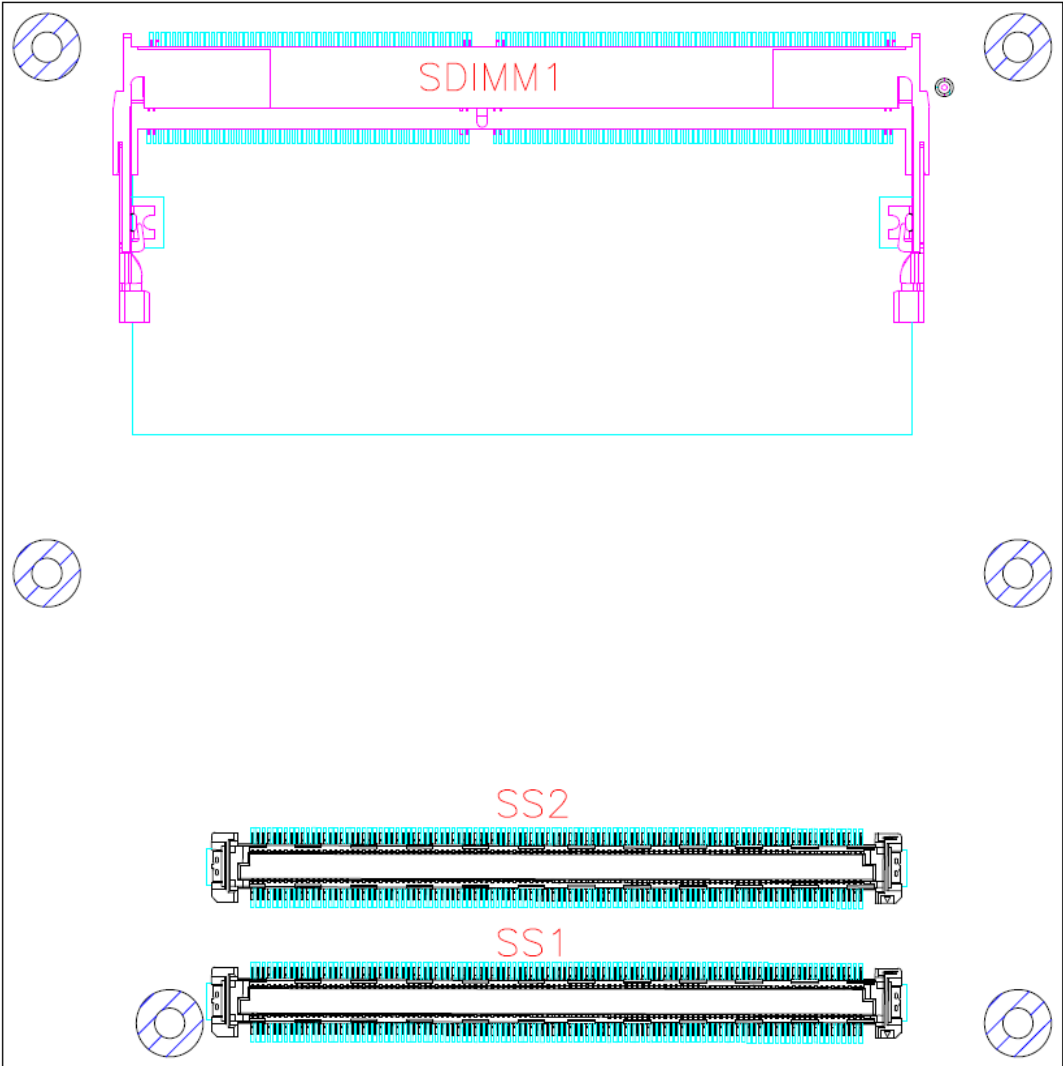


Top View

2.2 Module Layout



Top View

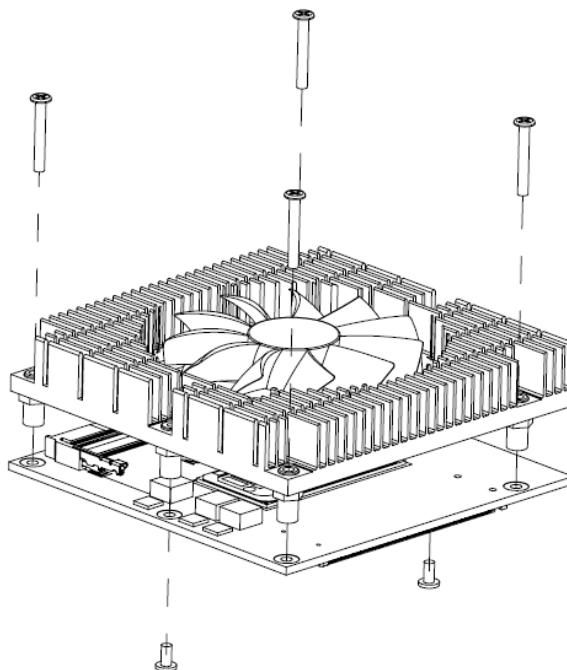


Bottom View

2.3 Installing Thermal Solution

For thermal dissipation, a thermal solution enables the CEM561's components to dissipate heat efficiently. All heat generating components are thermally conducted to the heatsink in order to avoid hot spots. Below images illustrate how to install the thermal solution.

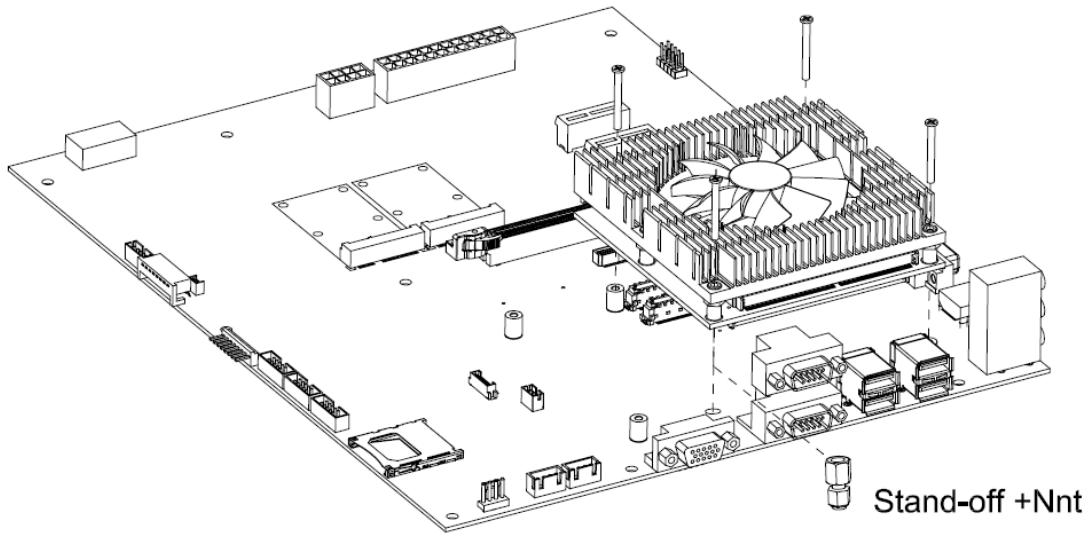
1. There is a protective plastic covering on the thermal pads. This must be removed before the heatsink can be mounted.
2. Each heatsink is designed for a specific CEM module. The thermal pads on the heatsink are designed to make contact with the necessary components on the CEM module. When mounting the heatsink you must make sure that the thermal pads on the heatsink make complete contact (no space between thermal pad and component) with the corresponding components on the CEM module. This is especially critical for CEM modules that have higher CPU speeds (for example 1.0GHz or more) to ensure that the heatsink acts as a proper thermal interface for cooling solutions.
3. This CPU module has six assembly holes for installing heatsink plate. Use the six screws to secure the heatsink plate to the CEM561. Be careful not to over-tighten the screws.





Note

When installing CEM561 on CEB94011, please add stand-off and secure with nut. Then, use the screws to secure the heatsink plate to the CEM561.



2.4 Switch Settings

Before applying power to the CEM561, please make sure onboard switches are in factory default positions.



Note

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

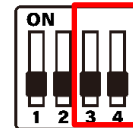
Switch	Description	Setting
SW1	Auto Power On Default: Disable	SW1-1 OFF
	Restore BIOS Optimal Defaults Default: Normal Operation	SW1-2 OFF

2.4.1 Auto Power On and Restore BIOS Optimal Defaults (SW1 1 & 2)

If dip1 of SW1 (SW1-1) is set to ON position, the system will be automatically power on without pressing soft power button. If this switch is set to OFF position, it is necessary to manually press soft power button to power on the system.

The dip2 of SW1 (SW1-2) is for restoring BIOS default status. Flip SW1-2 to ON position for a few seconds then flip it back to OFF position. Doing this procedure can restore BIOS optimal defaults.

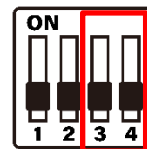
Function	Setting
Disable auto power on (Default)	SW1-1 OFF
Enable auto power on	SW1-1 ON
Normal operation (Default)	SW1-2 OFF
Restore BIOS optimal defaults	SW1-2 ON



2.4.2 PCI-Express Bifurcation Setting (SW1 3 & 4)

The SW1 is for PCI-Express bifurcation setting. See table below for detailed information.

Switch	Description	Setting
SW1	PCI-Express Bifurcation Setting 2 x4 PCI-Express (Default)	SW1-3 OFF, SW1-4 OFF
	PCI-Express Bifurcation Setting Port A (COM PEG 0~3) Reversed	SW1-3 ON, SW1-4 OFF



2.5 Connector

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 summary table which shows connectors on the hardware.

Connector	Description
CN1	Fan Connector
SS1	COM Express™ Connector
SS2	COM Express™ Connector
DIMM1	Channel 0 DDR4 SO-DIMM Socket
SDIMM1	Channel 1 DDR4 SO-DIMM Socket



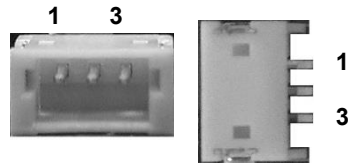
Note

- For single memory channel configuration, install memory module in channel 0 (DIMM1) DDR4 SO-DIMM socket.
- For dual memory channel configuration, install memory modules of the same size, chip width, density and rank in both channel 0 (DIMM1) and channel 1 (SDIMM1) DDR4 SO-DIMM sockets.

2.5.1 Fan Connector (CN1)

The CN1 is a 3-pin (pitch=1.5mm) connector, compliant with JST S3B-ZR-SM4A-TF, for fan interface.

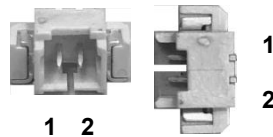
Pin	Signal
1	GND
2	+12V level
3	Fan speed feedback



2.5.2 CMOS Battery Connector (BAT)

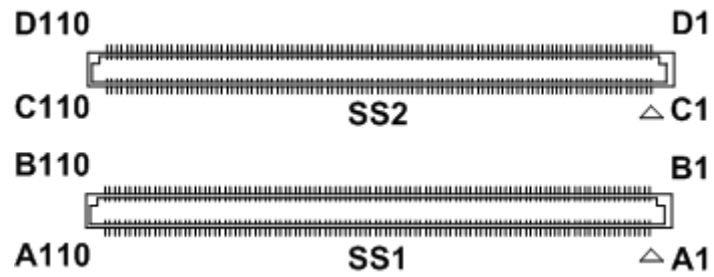
The BAT is a 2-pin (pitch=1.25mm) connector which is compliant with Molex 0532610271.

Pin	Signal
1	+3V level
2	GND



2.5.3 COM Express™ Connector (SS1 and SS2)

The following table shows pin assignments of the 220-pin COM Express™ connectors.



Bottom View

Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal
A1	GND (FIXED)	B1	GND (FIXED)	C1	GND (FIXED)	D1	GND (FIXED)
A2	LAN1_MDI3-	B2	LAN1_LED_ACT_N	C2	GND	D2	GND
A3	LAN1_MDI3+	B3	LPC_FRAME_N	C3	USB3_RX0_N	D3	USB3_TX0_N
A4	LAN1_LED_100_N	B4	LPC_AD0	C4	USB3_RX0_P	D4	USB3_TX0_P
A5	LAN1_LED_1000_N	B5	LPC_AD1	C5	GND	D5	GND
A6	LAN1_MDI2-	B6	LPC_AD2	C6	USB3_RX1_N	D6	USB3_TX1_N
A7	LAN1_MDI2+	B7	LPC_AD3	C7	USB3_RX1_P	D7	USB3_TX1_P
A8	LAN1_LINK_LED_N	B8	N.C.	C8	GND	D8	GND
A9	LAN1_MDI1-	B9	N.C.	C9	USB3_RX2_N	D9	USB3_TX2_N
A10	LAN1_MDI1+	B10	L_CLK_33M_COM	C10	USB3_RX2_P	D10	USB3_TX2_P
A11	GND (FIXED)	B11	GND (FIXED)	C11	GND (FIXED)	D11	GND (FIXED)
A12	LAN1_MDI0-	B12	PWRBTN_N_CB	C12	USB3_RX3_N	D12	USB3_TX3_N
A13	LAN1_MDI0+	B13	COM_SMB_CLK	C13	USB3_RX3_P	D13	USB3_TX3_P
A14	GBE0_CTREF	B14	COM_SMB_DAT	C14	GND	D14	GND
A15	SLP_S3_N_B	B15	SMBALERT_N	C15	N.C.	D15	DDIB_CTRLCLK_AUXP
A16	SATA0_TXP	B16	SATA1_TXP	C16	N.C.	D16	DDIB_CTRLDATA_AUXN
A17	SATA0_TXN	B17	SATA1_TXN	C17	N.C.	D17	N.C.
A18	SLP_S4_N_B	B18	SUS_STAT_N_R	C18	N.C.	D18	N.C.
A19	SATA0_RXP	B19	SATA1_RXP	C19	PCIE_RX_DP6	D19	PCIE_TX_DP6
A20	SATA0_RXN	B20	SATA1_RXN	C20	PCIE_RX_DN6	D20	PCIE_TX_DN6
A21	GND (FIXED)	B21	GND (FIXED)	C21	GND (FIXED)	D21	GND (FIXED)
A22	SATA2_TXP	B22	N.C.	C22	PCIE_RX_DP7	D22	PCIE_TX_DP7
A23	SATA2_TXN	B23	N.C.	C23	PCIE_RX_DN7	D23	PCIE_TX_DN7
A24	MCP_SLP_S5_N	B24	PWR_OK_CB	C24	DDPB_HPD	D24	N.C.
A25	SATA2_RXP	B25	N.C.	C25	N.C.	D25	N.C.
A26	SATA2_RXN	B26	N.C.	C26	N.C.	D26	DDPB_0P
A27	PM_BATLOW_N	B27	WDT_RESET_N	C27	N.C.	D27	DDPB_0N
A28	SATA_LED_N	B28	N.C.	C28	N.C.	D28	N.C.
A29	AUD_LINK_SYNC	B29	AUD_LINK_SDI1	C29	N.C.	D29	DDPB_1P
A30	AUD_LINK_RST#	B30	AUD_LINK_SDI0	C30	N.C.	D30	DDPB_1N
A31	GND (FIXED)	B31	GND (FIXED)	C31	GND (FIXED)	D31	GND (FIXED)
A32	AUD_LINK_BCLK	B32	MCP_SPKR	C32	DDIC_CTRLCLK_AUXP	D32	DDPB_2P
A33	AUD_LINK_SDO	B33	I2C_CLK_SBY	C33	DDIC_CTRLDATA_AUXN	D33	DDPB_2N
A34	BIOS_DISABLE0_N	B34	I2C_DAT_SBY	C34	DDIC_SEL	D34	DDIB_SEL
A35	THERMTRIP_N_3V3	B35	COM_THRM_N	C35	N.C.	D35	N.C.
A36	USBP_6N	B36	USBP_7N	C36	N.C.	D36	DDPB_3P
A37	USBP_6P	B37	USBP_7P	C37	N.C.	D37	DDPB_3N
A38	USB_OC3_N	B38	USB_OC2_N	C38	N.C.	D38	N.C.
A39	USBP_4N	B39	USBP_5N	C39	N.C.	D39	COM_DDPC_0P
A40	USBP_4P	B40	USBP_5P	C40	N.C.	D40	COM_DDPC_0N
A41	GND (FIXED)	B41	GND (FIXED)	C41	GND (FIXED)	D41	GND (FIXED)
A42	USBP_2N	B42	USBP_3N	C42	N.C.	D42	COM_DDPC_1P
A43	USBP_2P	B43	USBP_3P	C43	N.C.	D43	COM_DDPC_1N
A44	USB_OC1_N	B44	USB_OC0_N	C44	N.C.	D44	DDPC_HPD
A45	USBP_0N	B45	USBP_1N	C45	N.C.	D45	N.C.
A46	USBP_0P	B46	USBP_1P	C46	N.C.	D46	DDPC_2P
A47	VCC_RTC_CB	B47	N.C.	C47	N.C.	D47	DDPC_2N
A48	I2C_ALERT_N	B48	N.C.	C48	N.C.	D48	N.C.
A49	COM_GBE0_SPD	B49	RST_BTN_N	C49	N.C.	D49	DDPC_3P
A50	INT_SERIRQ_R	B50	PLTRST_2_N	C50	N.C.	D50	DDPC_3N
A51	GND (FIXED)	B51	GND (FIXED)	C51	GND (FIXED)	D51	GND (FIXED)
A52	PCIE_TX_DP5	B52	PCIE_RX_DP5	C52	N.C.	D52	N.C.
A53	PCIE_TX_DN5	B53	PCIE_RX_DN5	C53	N.C.	D53	N.C.
A54	COM_GPI0	B54	COM_GPO1	C54	N.C.	D54	N.C.
A55	PCIE_TX_DP4	B55	PCIE_RX_DP4	C55	N.C.	D55	N.C.

CEM561 COM Express™ Type 6 Module

Pin	Signal	Pin	Signal	Pin	Signal	Pin	Signal
A56	PCIE_TX_DN4	B56	PCIE_RX_DN4	C56	N.C.	D56	N.C.
A57	GND	B57	COM_GPO2	C57	N.C.	D57	TYPE2_N
A58	PCIE_TX_DP3	B58	PCIE_RX_DP3	C58	N.C.	D58	N.C.
A59	PCIE_TX_DN3	B59	PCIE_RX_DN3	C59	N.C.	D59	N.C.
A60	GND (FIXED)	B60	GND (FIXED)	C60	GND (FIXED)	D60	GND (FIXED)
A61	PCIE_TX_DP2	B61	PCIE_RX_DP2	C61	N.C.	D61	N.C.
A62	PCIE_TX_DN2	B62	PCIE_RX_DN2	C62	N.C.	D62	N.C.
A63	COM_GPI1	B63	COM_GPO3	C63	N.C.	D63	N.C.
A64	PCIE_TX_DP1	B64	PCIE_RX_DP1	C64	N.C.	D64	N.C.
A65	PCIE_TX_DN1	B65	PCIE_RX_DN1	C65	N.C.	D65	N.C.
A66	GND	B66	COM_WAKE0	C66	N.C.	D66	N.C.
A67	COM_GPI2	B67	COM_WAKE01	C67	RAPID_SHUTDOWN_R	D67	GND
A68	PCIE_TX_DP0	B68	PCIE_RX_DP0	C68	N.C.	D68	N.C.
A69	PCIE_TX_DN0	B69	PCIE_RX_DN0	C69	N.C.	D69	N.C.
A70	GND(FIXED)	B70	GND(FIXED)	C70	GND(FIXED)	D70	GND(FIXED)
A71	LVDS_A0+_R	B71	LVDS_B0+	C71	N.C.	D71	N.C.
A72	LVDS_A0-_R	B72	LVDS_B0-	C72	N.C.	D72	N.C.
A73	LVDS_A1+_R	B73	LVDS_B1+	C73	GND	D73	GND
A74	LVDS_A1-_R	B74	LVDS_B1-	C74	N.C.	D74	N.C.
A75	LVDS_A2+_R	B75	LVDS_B2+	C75	N.C.	D75	N.C.
A76	LVDS_A2-_R	B76	LVDS_B2-	C76	GND	D76	GND
A77	LVDS_VDD_EN	B77	LVDS_B3+	C77	N.C.	D77	N.C.
A78	LVDS_A3+_R	B78	LVDS_B3-	C78	N.C.	D78	N.C.
A79	LVDS_A3-_R	B79	LVDS_BKLT_EN_N	C79	N.C.	D79	N.C.
A80	GND(FIXED)	B80	GND(FIXED)	C80	GND(FIXED)	D80	GND(FIXED)
A81	LVDS_CK_A+_R	B81	LVDS_CK_B+	C81	N.C.	D81	N.C.
A82	LVDS_CK_A-_R	B82	LVDS_CK_B-	C82	N.C.	D82	N.C.
A83	LVDS_I2C_CK_R	B83	LVDS_BKLT_CTRL	C83	N.C.	D83	N.C.
A84	LVDS_I2C_DAT_R	B84	5V_SBY_CB	C84	GND	D84	GND
A85	COM_GPI3	B85	5V_SBY_CB	C85	N.C.	D85	N.C.
A86	SD_PWR_EN_N	B86	5V_SBY_CB	C86	N.C.	D86	N.C.
A87	EDP_HPD	B87	5V_SBY_CB	C87	GND	D87	GND
A88	CK_100M_COM_DP1	B88	BIOS_DISABLE1_N	C88	N.C.	D88	N.C.
A89	CK_100M_COM_DN1	B89	VGA_RED	C89	N.C.	D89	N.C.
A90	GND (FIXED)	B90	GND (FIXED)	C90	GND (FIXED)	D90	GND (FIXED)
A91	3V3_SBY	B91	VGA_GREEN	C91	N.C.	D91	N.C.
A92	SPI_MISO	B92	VGA_BLUE	C92	N.C.	D92	N.C.
A93	COM_GPO0	B93	VGA_HSYNC	C93	GND	D93	GND
A94	SPI_CLK	B94	VGA_VSYNC	C94	N.C.	D94	N.C.
A95	SPI_MOSI	B95	VGA_CH7517_DDCSCL	C95	N.C.	D95	N.C.
A96	TPM_PP	B96	VGA_CH7517_DDCSDA	C96	GND	D96	GND
A97	N.C.	B97	SPI_CS_C	C97	N.C.	D97	N.C.
A98	EC_UART1_TX	B98	N.C.	C98	N.C.	D98	N.C.
A99	EC_UART1_RX	B99	N.C.	C99	N.C.	D99	N.C.
A100	GND (FIXED)	B100	GND (FIXED)	C100	GND (FIXED)	D100	GND (FIXED)
A101	EC_UART2_TX	B101	FAN_PWMOUT	C101	N.C.	D101	N.C.
A102	EC_UART2_RX	B102	FAN_TACHIN	C102	N.C.	D102	N.C.
A103	C_LID_N	B103	C_SLEEP_N	C103	GND	D103	GND
A104	+VIN(12V)	B104	+VIN(12V)	C104	+VIN(12V)	D104	+VIN(12V)
A105	+VIN(12V)	B105	+VIN(12V)	C105	+VIN(12V)	D105	+VIN(12V)
A106	+VIN(12V)	B106	+VIN(12V)	C106	+VIN(12V)	D106	+VIN(12V)
A107	+VIN(12V)	B107	+VIN(12V)	C107	+VIN(12V)	D107	+VIN(12V)
A108	+VIN(12V)	B108	+VIN(12V)	C108	+VIN(12V)	D108	+VIN(12V)
A109	+VIN(12V)	B109	+VIN(12V)	C109	+VIN(12V)	D109	+VIN(12V)
A110	GND (FIXED)	B110	GND (FIXED)	C110	GND (FIXED)	D110	GND (FIXED)

Section 3

Hardware Description

3.1 Microprocessor

The CEM561 supports 12th/13th generation processors, which enables your system to operate under Windows® 10/11 and Linux environments. The system performance depends on the microprocessor. You must install the heatsink or cooler carefully and properly to prevent damage.

3.2 BIOS

The CEM561 uses AMI Plug and Play BIOS with a single 256Mbit SPI Flash.

3.3 System Memory

The CEM561 supports two 260-pin DDR4 3200MHz SO-DIMM sockets for maximum memory capacity up to 64GB DDR4 SDRAMs. The memory module comes in sizes of 8GB, 16GB and 32GB.







































































3.4 I/O Port Address Map





















▼	Input/output (IO)
📁	[0000000000000000 - 000000000000CF7] PCI Express Root Complex
📁	[0000000000000020 - 0000000000000021] Programmable interrupt controller
📁	[0000000000000024 - 0000000000000025] Programmable interrupt controller
📁	[0000000000000028 - 0000000000000029] Programmable interrupt controller
📁	[000000000000002C - 000000000000002D] Programmable interrupt controller
📁	[000000000000002E - 000000000000002F] Motherboard resources
📁	[0000000000000030 - 0000000000000031] Programmable interrupt controller
📁	[0000000000000034 - 0000000000000035] Programmable interrupt controller
📁	[0000000000000038 - 0000000000000039] Programmable interrupt controller
📁	[000000000000003C - 000000000000003D] Programmable interrupt controller
📁	[0000000000000040 - 0000000000000043] System timer
📁	[000000000000004E - 000000000000004F] Motherboard resources
📁	[0000000000000050 - 0000000000000053] System timer
📁	[0000000000000060 - 0000000000000060] Standard PS/2 Keyboard
📁	[0000000000000061 - 0000000000000061] Motherboard resources
📁	[0000000000000062 - 0000000000000062] Microsoft ACPI-Compliant Embedded Controller
📁	[0000000000000063 - 0000000000000063] Motherboard resources
📁	[0000000000000064 - 0000000000000064] Standard PS/2 Keyboard
📁	[0000000000000065 - 0000000000000065] Motherboard resources
📁	[0000000000000066 - 0000000000000066] Microsoft ACPI-Compliant Embedded Controller
📁	[0000000000000067 - 0000000000000067] Motherboard resources
📁	[0000000000000070 - 0000000000000070] Motherboard resources
📁	[0000000000000080 - 0000000000000080] Motherboard resources
📁	[0000000000000092 - 0000000000000092] Motherboard resources
📁	[00000000000000A0 - 00000000000000A1] Programmable interrupt controller
📁	[00000000000000A4 - 00000000000000A5] Programmable interrupt controller
📁	[00000000000000A8 - 00000000000000A9] Programmable interrupt controller
📁	[00000000000000AC - 00000000000000AD] Programmable interrupt controller
📁	[00000000000000B0 - 00000000000000B1] Programmable interrupt controller
📁	[00000000000000B2 - 00000000000000B3] Motherboard resources
📁	[00000000000000B4 - 00000000000000B5] Programmable interrupt controller
📁	[00000000000000B8 - 00000000000000B9] Programmable interrupt controller
📁	[00000000000000BC - 00000000000000BD] Programmable interrupt controller
📁	[0000000000000248 - 000000000000024F] Communications Port (COM1)
📁	[0000000000000258 - 000000000000025F] Communications Port (COM2)
📁	[00000000000002F8 - 00000000000002FF] Communications Port (COM4)
📁	[00000000000003F8 - 00000000000003FF] Communications Port (COM3)
📁	[00000000000004D0 - 00000000000004D1] Programmable interrupt controller
📁	[0000000000000680 - 000000000000069F] Motherboard resources
📁	[0000000000000D00 - 000000000000FFFF] PCI Express Root Complex
📁	[000000000000164E - 000000000000164F] Motherboard resources
📁	[0000000000001800 - 00000000000018FE] Motherboard resources
📁	[0000000000001854 - 0000000000001857] Motherboard resources
📁	[0000000000002000 - 00000000000020FE] Motherboard resources
📁	[0000000000003000 - 000000000000303F] Intel(R) UHD Graphics 610
📁	[0000000000003060 - 000000000000307F] Standard SATA AHCI Controller
📁	[0000000000003080 - 0000000000003083] Standard SATA AHCI Controller
📁	[0000000000003090 - 0000000000003097] Standard SATA AHCI Controller
📁	[000000000000EFA0 - 000000000000EFBF] Intel(R) SMBus - 9DA3

3.5 Interrupt Controller (IRQ) Map

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

IRQ	Device
(ISA) 0x00000000 (00)	System timer
(ISA) 0x00000001 (01)	Standard PS/2 Keyboard
(ISA) 0x00000003 (03)	Communications Port (COM4)
(ISA) 0x00000004 (04)	Communications Port (COM3)
(ISA) 0x00000006 (06)	Communications Port (COM2)
(ISA) 0x00000007 (07)	Communications Port (COM1)
(ISA) 0x0000000E (14)	Intel(R) Serial IO GPIO Host Controller - INT34BB
(ISA) 0x0000001F (31)	Trusted Platform Module 2.0
(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) 0x000001AE (430)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D1 (465)	Microsoft ACPI-Compliant System
 (ISA) 0x000001AF (431)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D2 (466)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B0 (432)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D3 (467)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B1 (433)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D4 (468)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B2 (434)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D5 (469)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B3 (435)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D6 (470)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B4 (436)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D7 (471)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B5 (437)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D8 (472)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B6 (438)	Microsoft ACPI-Compliant System	 (ISA) 0x000001D9 (473)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B7 (439)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DA (474)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B8 (440)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DB (475)	Microsoft ACPI-Compliant System
 (ISA) 0x000001B9 (441)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DC (476)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BA (442)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DD (477)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BB (443)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DE (478)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BC (444)	Microsoft ACPI-Compliant System	 (ISA) 0x000001DF (479)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BD (445)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E0 (480)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BE (446)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E1 (481)	Microsoft ACPI-Compliant System
 (ISA) 0x000001BF (447)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E2 (482)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C0 (448)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E3 (483)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C1 (449)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E4 (484)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C2 (450)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E5 (485)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C3 (451)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E6 (486)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C4 (452)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E7 (487)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C5 (453)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E8 (488)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C6 (454)	Microsoft ACPI-Compliant System	 (ISA) 0x000001E9 (489)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C7 (455)	Microsoft ACPI-Compliant System	 (ISA) 0x000001EA (490)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C8 (456)	Microsoft ACPI-Compliant System	 (ISA) 0x000001EB (491)	Microsoft ACPI-Compliant System
 (ISA) 0x000001C9 (457)	Microsoft ACPI-Compliant System	 (ISA) 0x000001EC (492)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CA (458)	Microsoft ACPI-Compliant System	 (ISA) 0x000001ED (493)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CB (459)	Microsoft ACPI-Compliant System	 (ISA) 0x000001EE (494)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CC (460)	Microsoft ACPI-Compliant System	 (ISA) 0x000001EF (495)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CD (461)	Microsoft ACPI-Compliant System	 (ISA) 0x000001F0 (496)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CE (462)	Microsoft ACPI-Compliant System	 (ISA) 0x000001F1 (497)	Microsoft ACPI-Compliant System
 (ISA) 0x000001CF (463)	Microsoft ACPI-Compliant System	 (ISA) 0x000001F2 (498)	Microsoft ACPI-Compliant System
 (ISA) 0x000001D0 (464)	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) 0x00000013 (19)	Intel SD Host Controller
	(PCI) 0x00000400 (1024)	Intel SD Host Controller
	(PCI) 0xFFFFF0FA (-6)	Intel(R) Ethernet Connection (6) I219-LM
	(PCI) 0xFFFFF0FB (-5)	Intel(R) Management Engine Interface
	(PCI) 0xFFFFF0FC (-4)	Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
	(PCI) 0xFFFFF0FD (-3)	Intel(R) UHD Graphics 610
	(PCI) 0xFFFFF0FE (-2)	Standard SATA AHCI Controller

3.6 Memory Map

The memory mapping list is shown as follows:

▼	Memory
▶	[00000000000A0000 - 00000000000BFFFF] PCI Express Root Complex
▶	[00000000000E0000 - 00000000000E3FFF] PCI Express Root Complex
▶	[00000000000E4000 - 00000000000E7FFF] PCI Express Root Complex
▶	[00000000000E8000 - 00000000000EBFFF] PCI Express Root Complex
▶	[00000000000EC000 - 00000000000EFFFF] PCI Express Root Complex
▶	[00000000000F0000 - 00000000000FFFFF] PCI Express Root Complex
▶	[0000000400000000 - 0000000403FFFFF] Motherboard resources
▶	[0000000090000000 - 000000099FFFFF] Intel(R) UHD Graphics 610
▶	[0000000090000000 - 0000000DFFFFFFF] PCI Express Root Complex
▶	[00000000A0000000 - 0000000A0FFFFFFF] Intel(R) UHD Graphics 610
▶	[00000000A1120000 - 0000000A112FFFFF] Intel(R) USB 3.1 eXtensible Host Controller - 1.10 (Microsoft)
▶	[00000000A113C000 - 0000000A113DFFF] Standard SATA AHCI Controller
▶	[00000000A1140000 - 0000000A1140FFF] Intel(R) SMBus - 9DA3
▶	[00000000A1141000 - 0000000A11417FF] Standard SATA AHCI Controller
▶	[00000000A1142000 - 0000000A11420FFF] Standard SATA AHCI Controller
▶	[00000000A1144000 - 0000000A1144FFF] Intel SD Host Controller
▶	[00000000E0000000 - 0000000EFFFFFFF] Motherboard resources
▶	[00000000FC800000 - 0000000FE7FFFFF] PCI Express Root Complex
▶	[00000000FCF00000 - 0000000FCFFFFFFF] High Definition Audio Controller
▶	[00000000FD000000 - 0000000FD69FFFFF] Motherboard resources
▶	[00000000FD6A0000 - 0000000FD6AFFFFF] Intel(R) Serial IO GPIO Host Controller - INT34BB
▶	[00000000FD6B0000 - 0000000FD6CFFFFF] Motherboard resources
▶	[00000000FD6D0000 - 0000000FD6DFFFFF] Intel(R) Serial IO GPIO Host Controller - INT34BB
▶	[00000000FD6E0000 - 0000000FD6EFFFFF] Intel(R) Serial IO GPIO Host Controller - INT34BB
▶	[00000000FD6F0000 - 0000000FD6FFFFFFF] Motherboard resources
▶	[00000000FE000000 - 0000000FE01FFFFF] Motherboard resources
▶	[00000000FE010000 - 0000000FE010FFFFF] Intel(R) SPI (flash) Controller - 9DA4
▶	[00000000FE1DB000 - 0000000FE1DBFFF] Intel(R) Management Engine Interface
▶	[00000000FE1DC000 - 0000000FE1DFFFFF] High Definition Audio Controller
▶	[00000000FE1E0000 - 0000000FE1FFFFFFF] Intel(R) Ethernet Connection (6) I219-LM
▶	[00000000FE200000 - 0000000FE7FFFFFFF] Motherboard resources
▶	[00000000FED00000 - 0000000FED003FFF] High precision event timer
▶	[00000000FED10000 - 0000000FED17FFF] Motherboard resources
▶	[00000000FED18000 - 0000000FED18FFF] Motherboard resources
▶	[00000000FED19000 - 0000000FED19FFF] Motherboard resources
▶	[00000000FED20000 - 0000000FED3FFFFF] Motherboard resources
▶	[00000000FED40000 - 0000000FED44FFF] Trusted Platform Module 2.0
▶	[00000000FED45000 - 0000000FED8FFFFF] Motherboard resources
▶	[00000000FED90000 - 0000000FED93FFF] Motherboard resources
▶	[00000000FEE00000 - 0000000FEEFFFFFFF] Motherboard resources
▶	[00000000FF000000 - 0000000FFFFFFFFF] Motherboard resources

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 chapter 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 key immediately.
2. After you press the key, the main BIOS setup menu displays. You can access the other setup screens from the main BIOS setup menu, such as the Advanced and Chipset menus.



Note

If your computer cannot boot after making and saving system changes with BIOS setup, you can restore BIOS optimal defaults by setting SW1-2 (see section 2.4.1).

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.



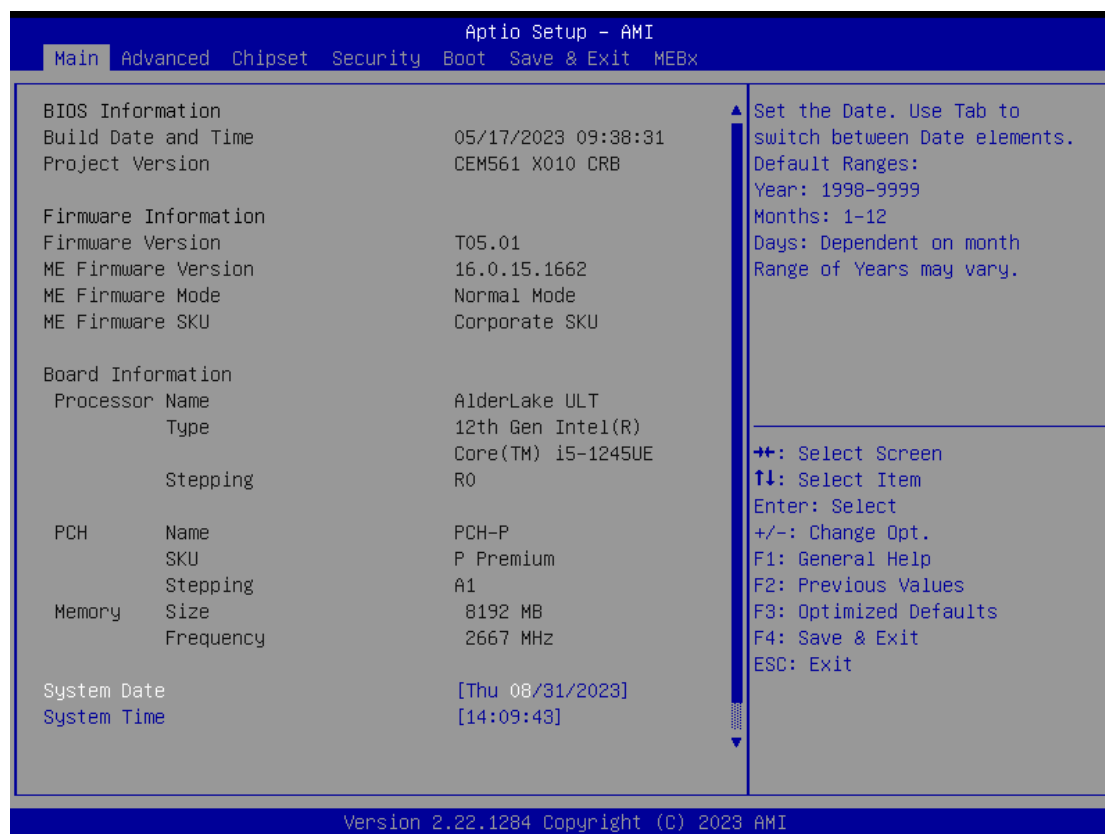
Note

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

When you first enter the setup utility, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab. System Time/Date can be set up as described below. The Main BIOS setup screen is shown below.



BIOS and EC Information

Display BIOS and EC 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.

Access Level

Display the access level of current user.

Board Information

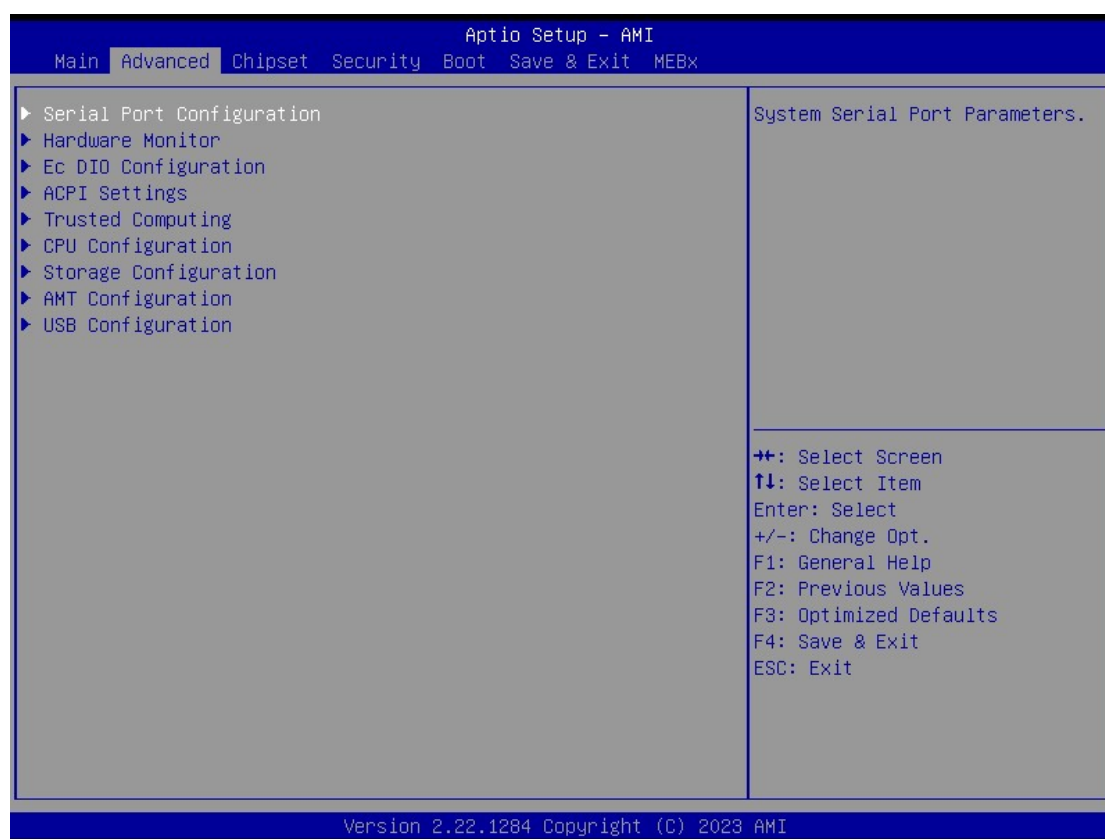
Display board related information.

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:

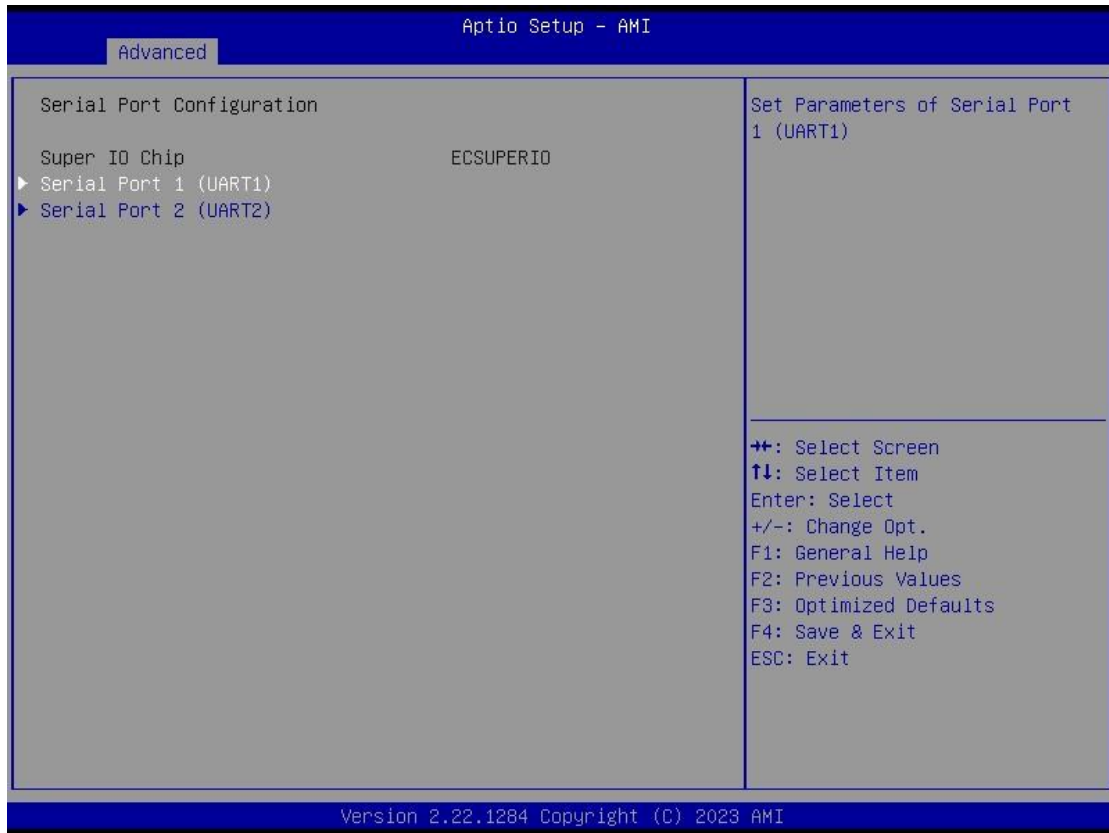
- ▶ Serial Port Configuration
- ▶ Hardware Monitor
- ▶ Ec DIO Configuration
- ▶ ACPI Settings
- ▶ Trusted Computing
- ▶ CPU Configuration
- ▶ Storage Configuration
- ▶ USB Configuration

For items marked with “▶”, please press <Enter> for more options.



- **Serial Port Configuration**

You can use this screen to select options for Serial Port 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 1~2 (UART1~2)

Set parameters related to serial port 1~2.

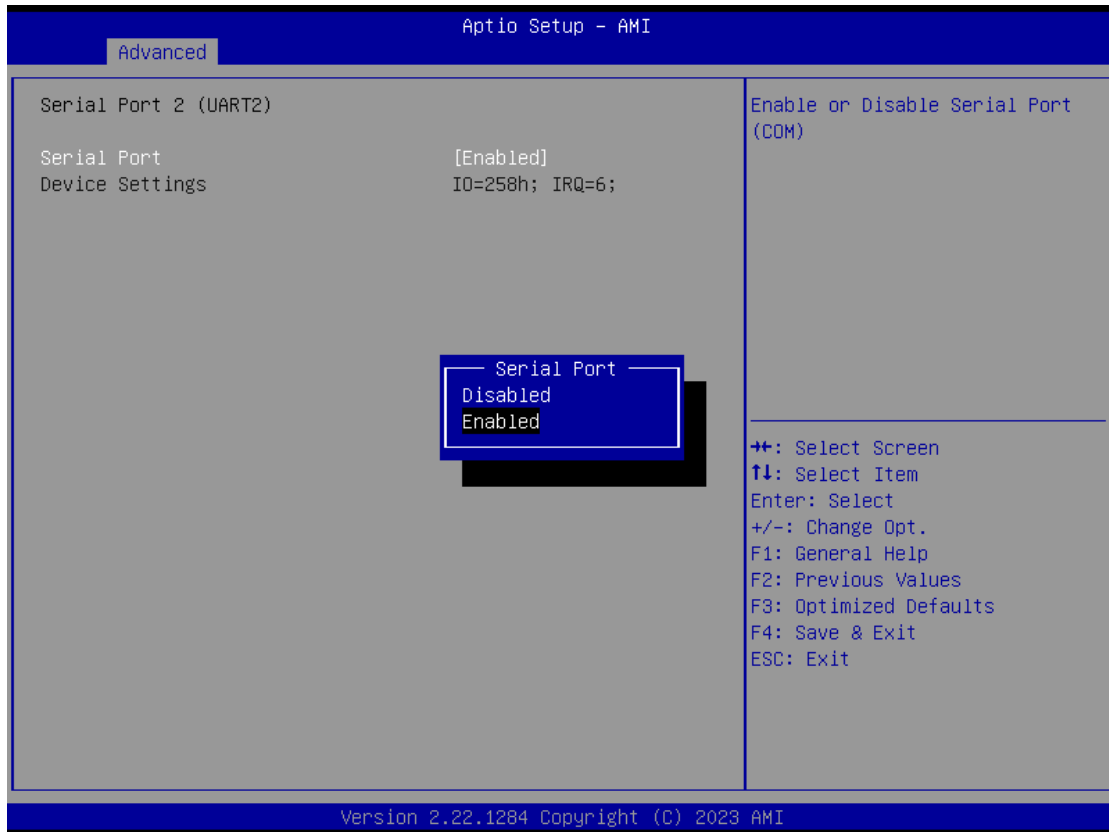
- **Serial Port 1 (UART1)**



Serial Port

Enable or disable serial port 1. The optimal setting for base I/O address is 248h and for interrupt request address is IRQ7.

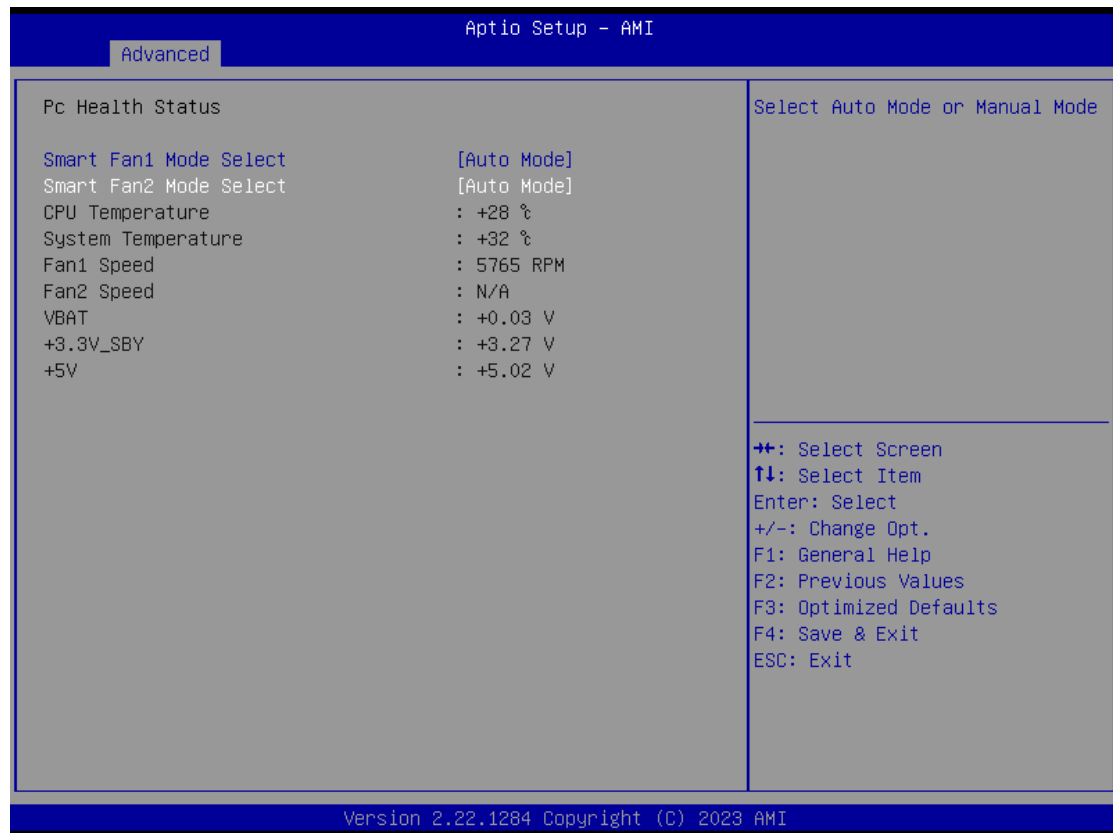
- **Serial Port 2 (UART2)**

**Serial Port**

Enable or disable serial port 2. The optimal setting for base I/O address is 258h and for interrupt request address is IRQ6.

- **Hardware Monitor**

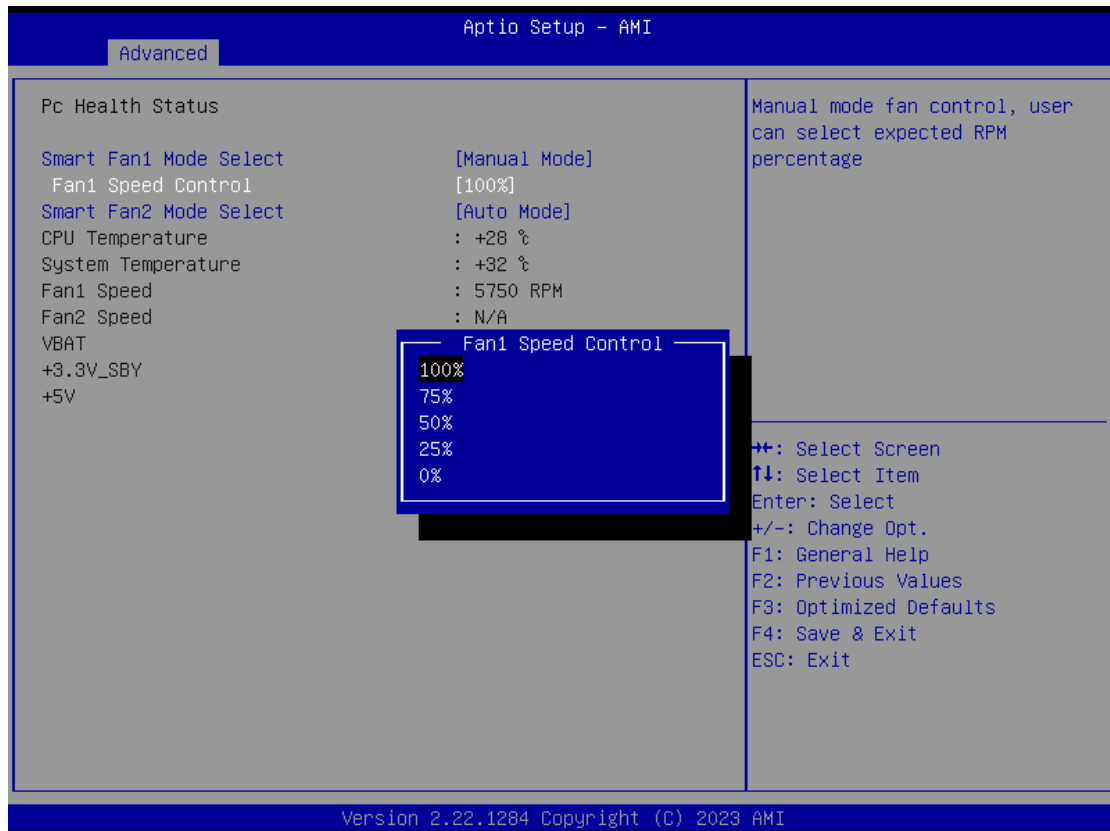
This screen is for fan speed control and hardware health status monitoring.



This screen displays the temperature of system and CPU, cooling fans speed in RPM and system voltages (+3.3V, +3.3V standby and +5V).

Smart Fan1/2 Mode Select

Set Smart Fan 1/2 mode. The default is Auto Mode. If Smart Fan is in Auto Mode, the system fan spins at different speed depending on system temperature; the higher the temperature, the faster the system fan spins. If Smart Fan is in Manual Mode, user can manually change system fan speed to 100%, 75%, 50%, 25% or 0% (see image below).



● **Ec DIO Configuration**

You can use this screen to select options for DIO configuration. A description of selected item appears on the right side of the screen. For more details, see Appendix B.



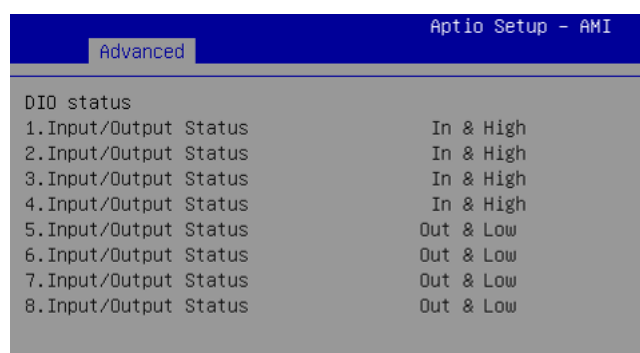
DIO Modification

Enable or disable digital I/O modification. The default is Disabled.

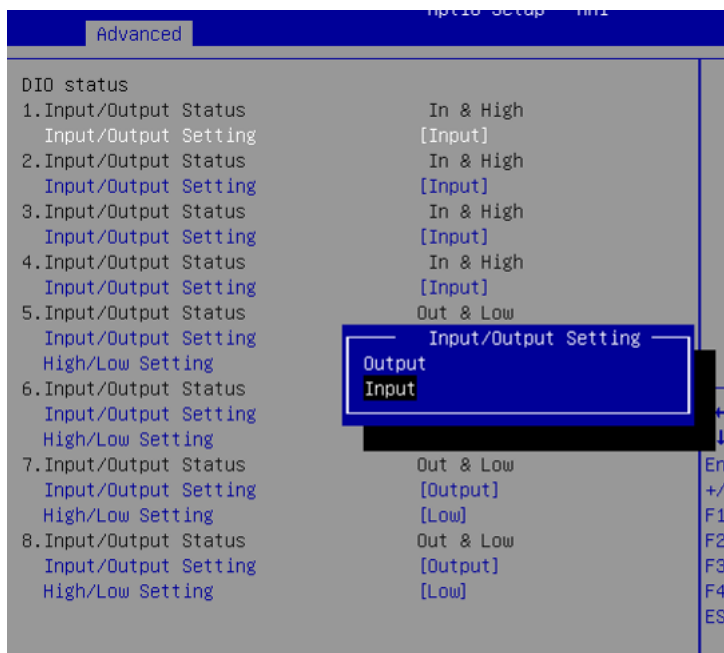
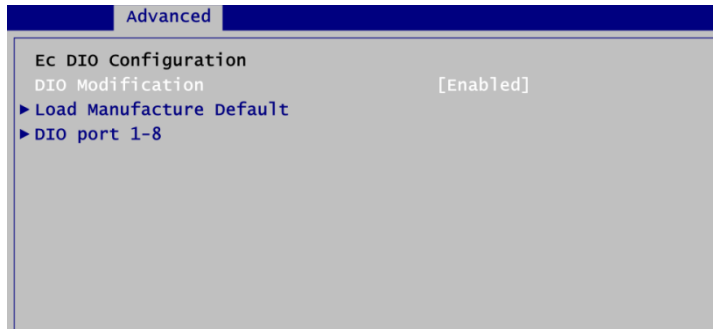
DIO port 1-8

Select this option to open DIO status sub screen.

If DIO Modification is disabled, you are not allowed to change inputs/outputs setting. The DIO status sub screen is as follows:

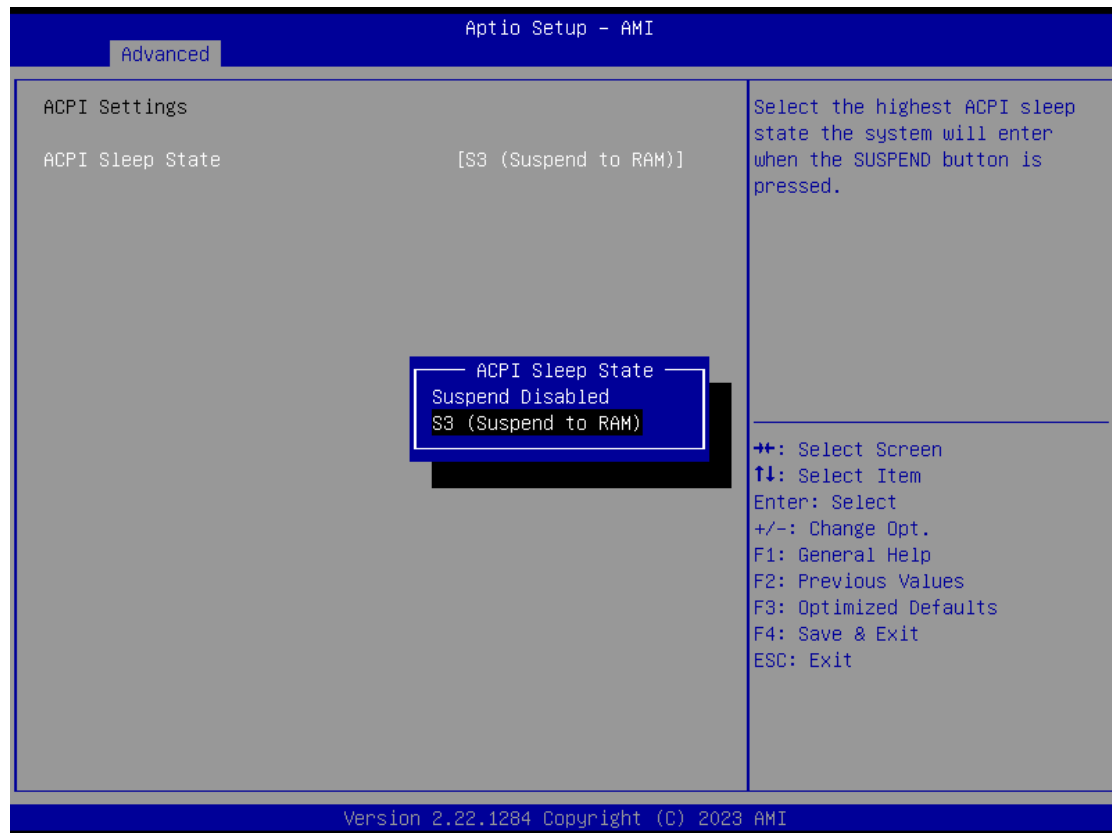


If DIO Modification is enabled, you can load manufacture default and access to the DIO status sub screen to change inputs/outputs setting, see images below.



- **ACPI Settings**

You can use this screen to select options for the ACPI configuration, and change the value of the selected option. A description of the selected item appears on the right side of the screen.

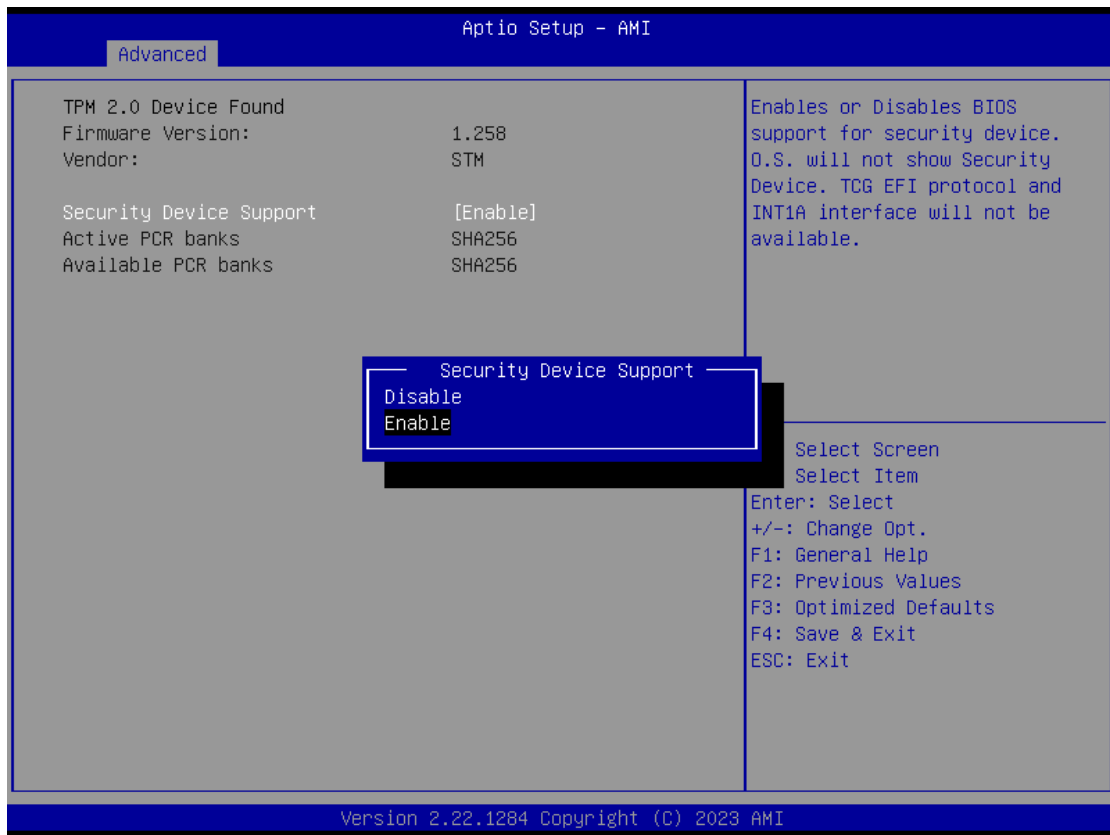


ACPI Sleep State

Select the ACPI (Advanced Configuration and Power Interface) sleep state. Configuration options are Suspend Disabled and S3 (Suspend to RAM). The default is S3 (Suspend to RAM); this option selects ACPI sleep state the system will enter when suspend button is pressed.

- **Trusted Computing**

You can use this screen for TPM (Trusted Platform Module) configuration. It also shows current TPM status information.



Security Device Support

Enable or disable BIOS support for security device.

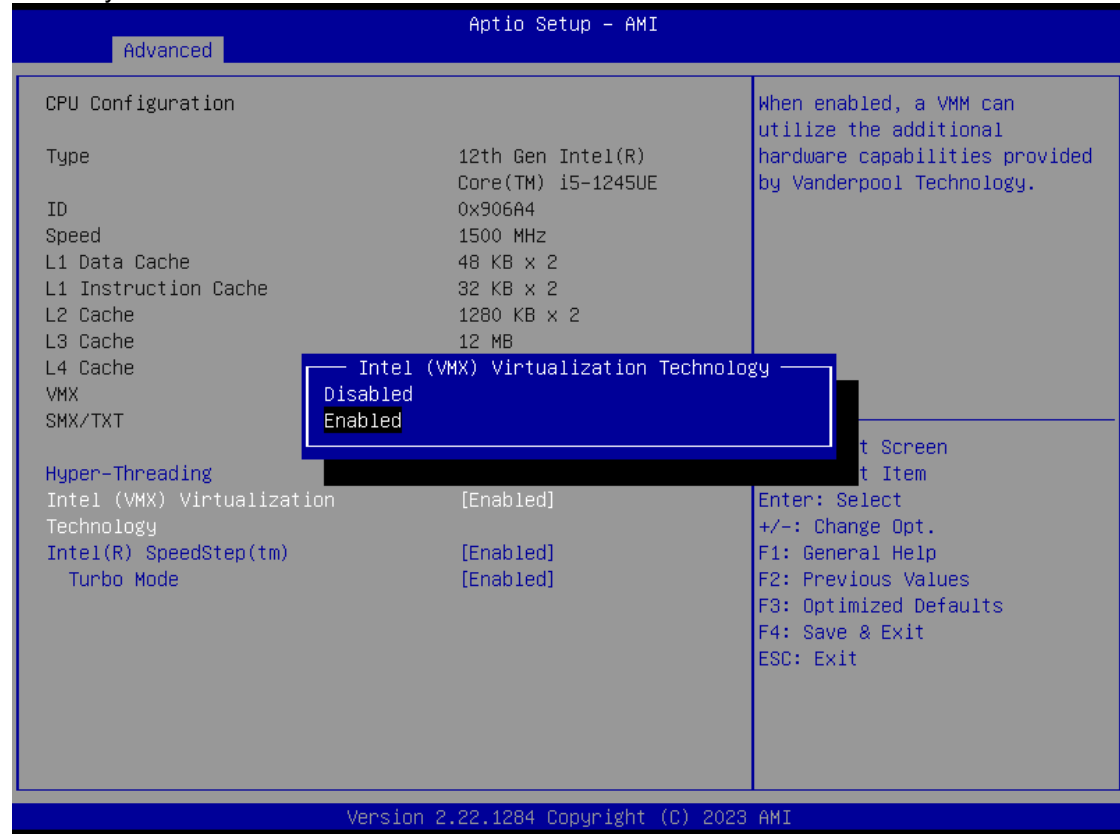
● **CPU Configuration**

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



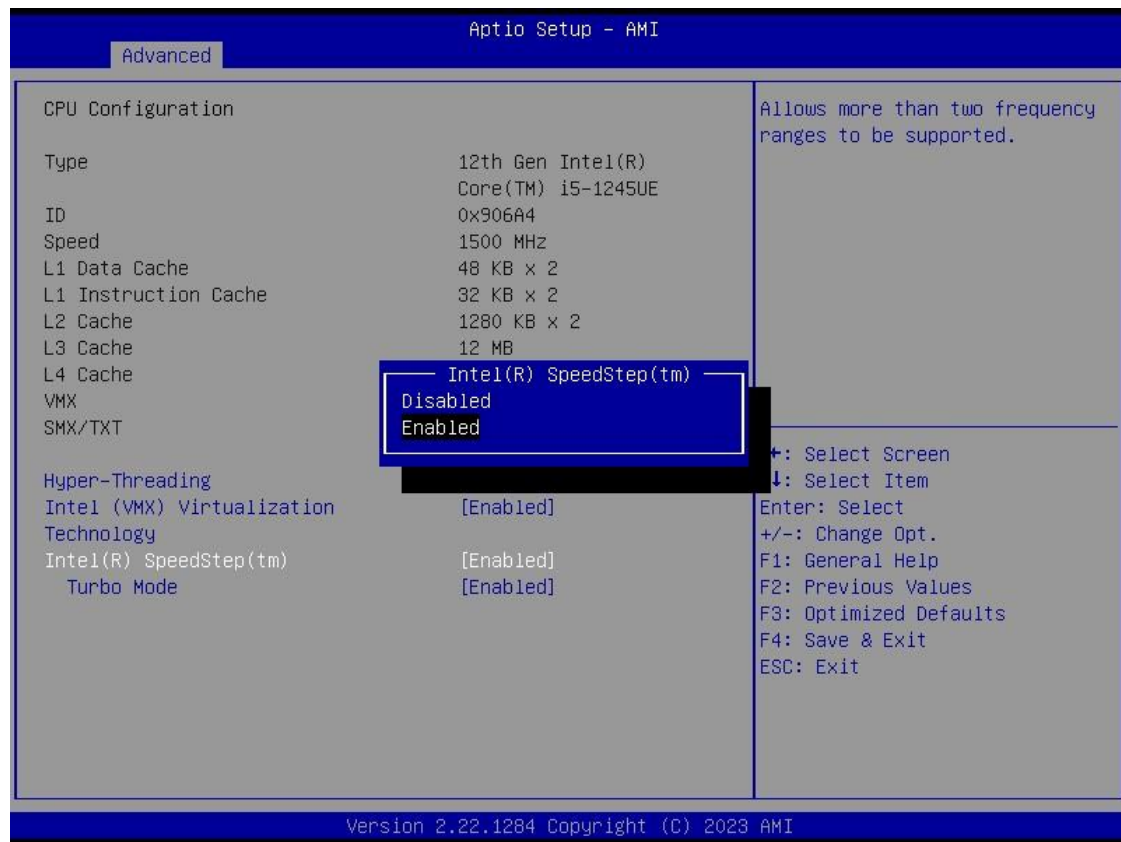
Intel (VMX) Virtualization Technology

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 computer system to work as several virtual systems.



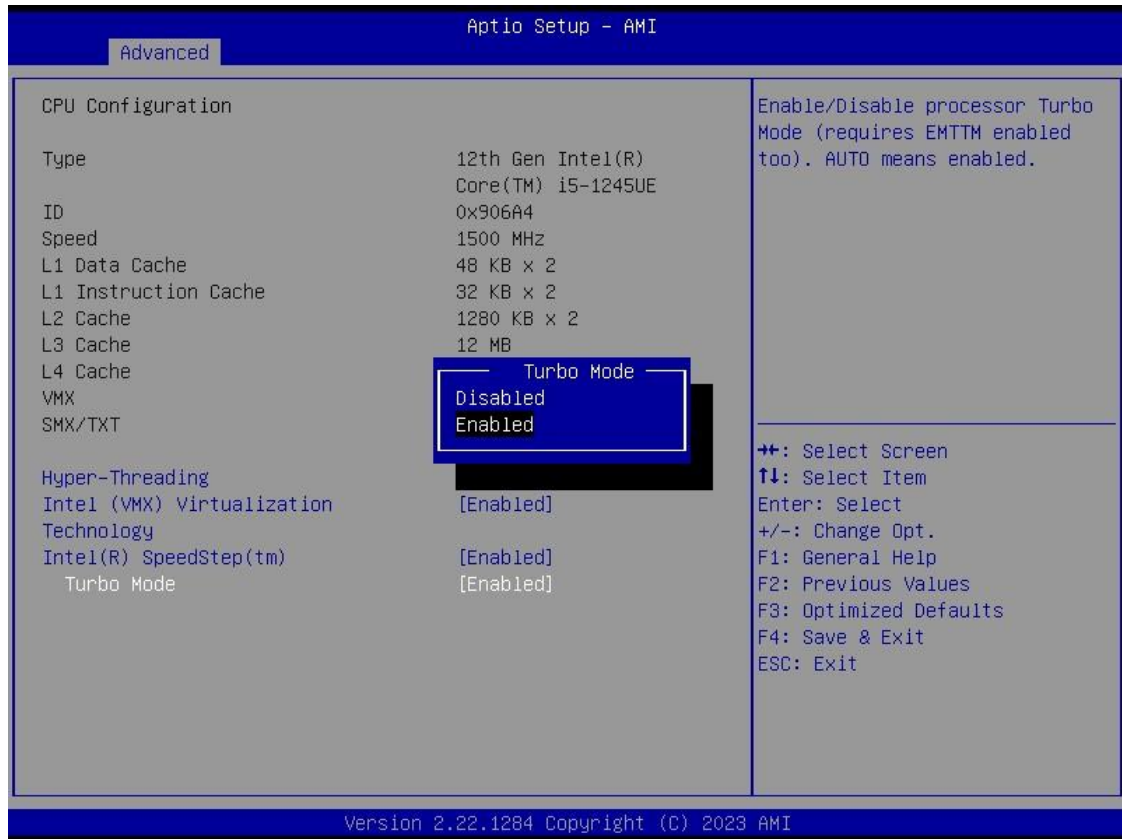
Intel(R) SpeedStep(tm)

Enable or disable Intel® SpeedStep. When disabled, CPU runs at its default speed. When enabled, the CPU speed is controlled by the operating system.



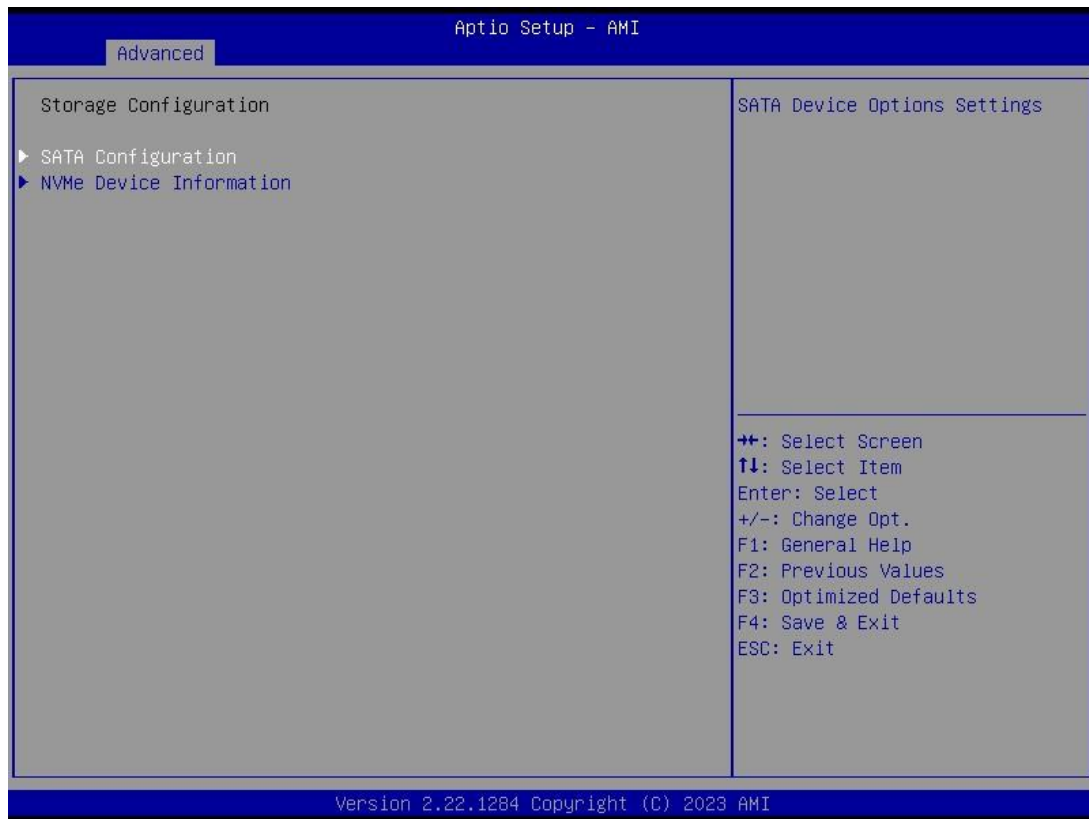
Turbo Mode

Enable or disable processor Turbo Mode. The processor can run up to maximum turbo frequency when the system loading becomes higher.



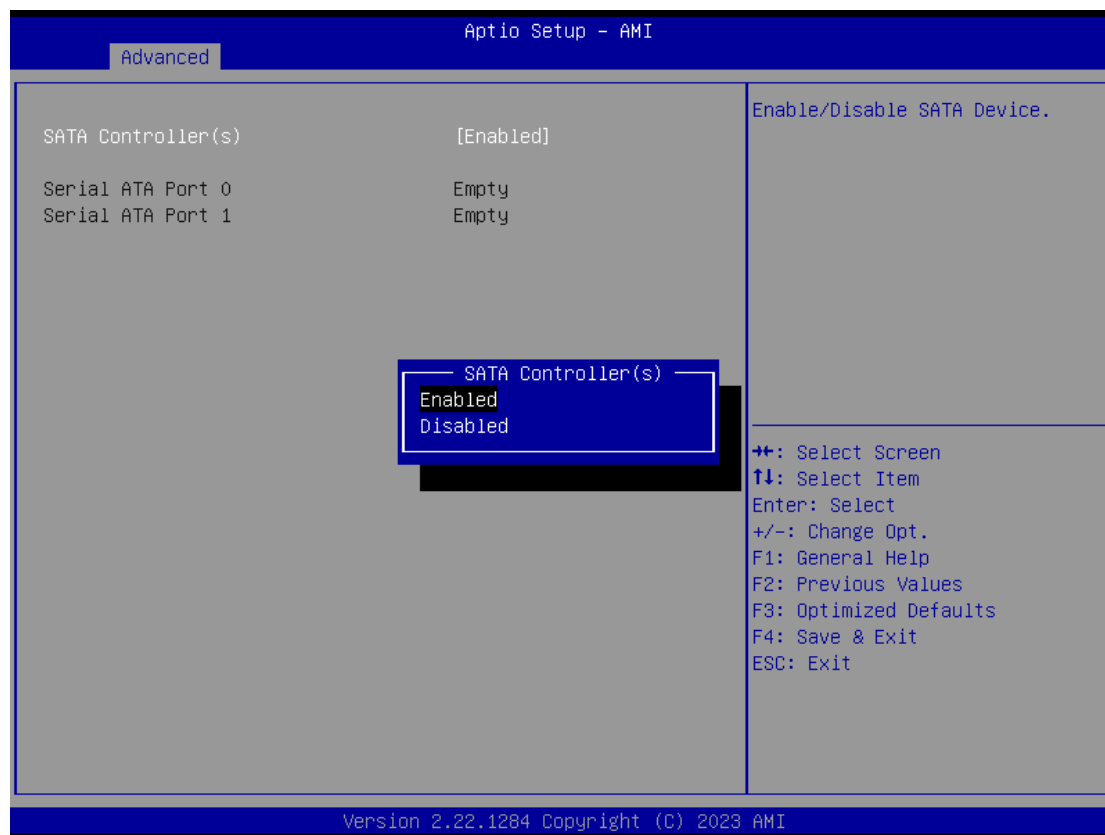
- **Storage Configuration**

In the Storage Configuration menu, you can see the currently installed hardware in the SATA/NVME ports. During system boot up, the BIOS automatically detects the presence of installed devices.



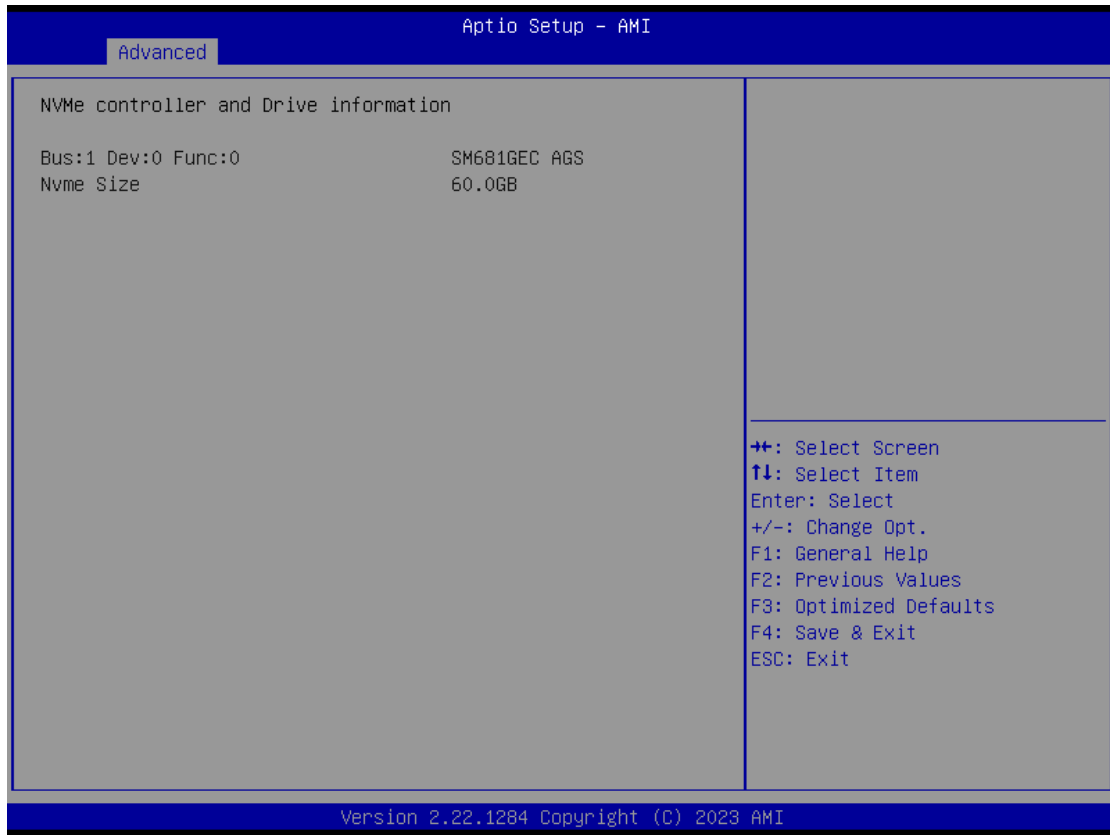
SATA Controller(s)

Enable or disable the SATA Controller feature.

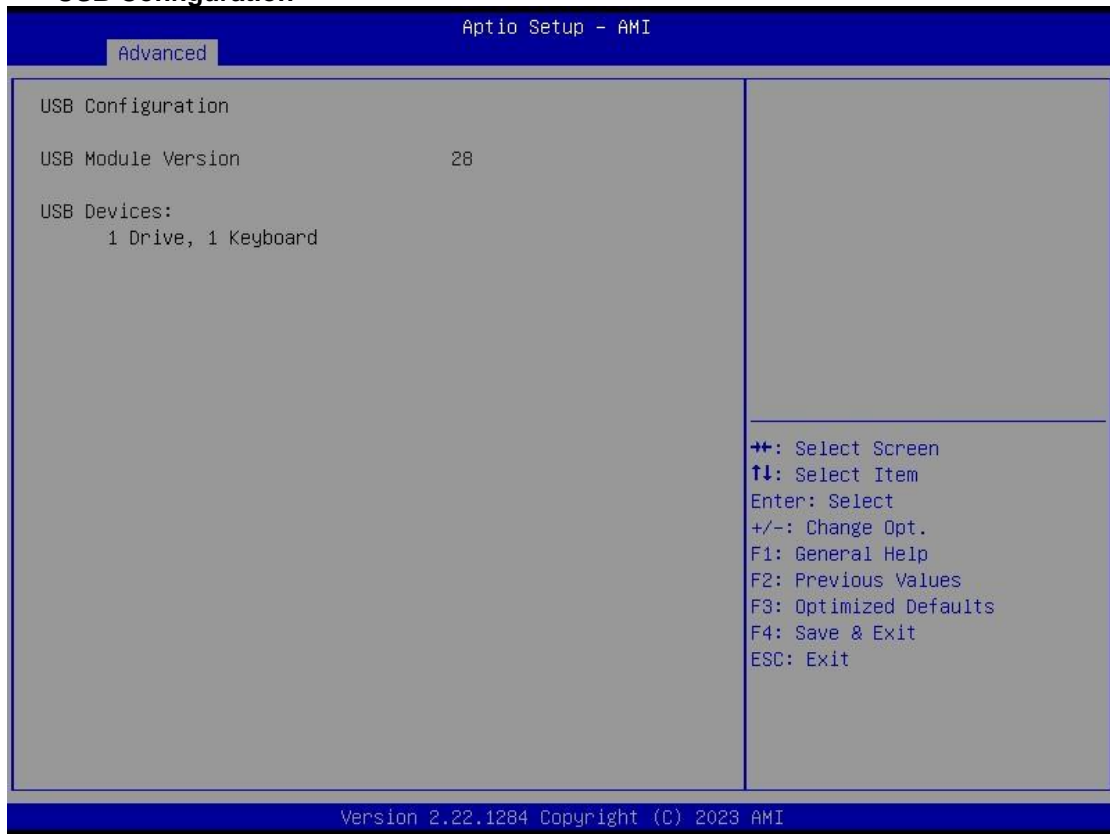


NVME controller(S)

Showing the information of installed NVME devices.



● **USB Configuration**



USB Devices

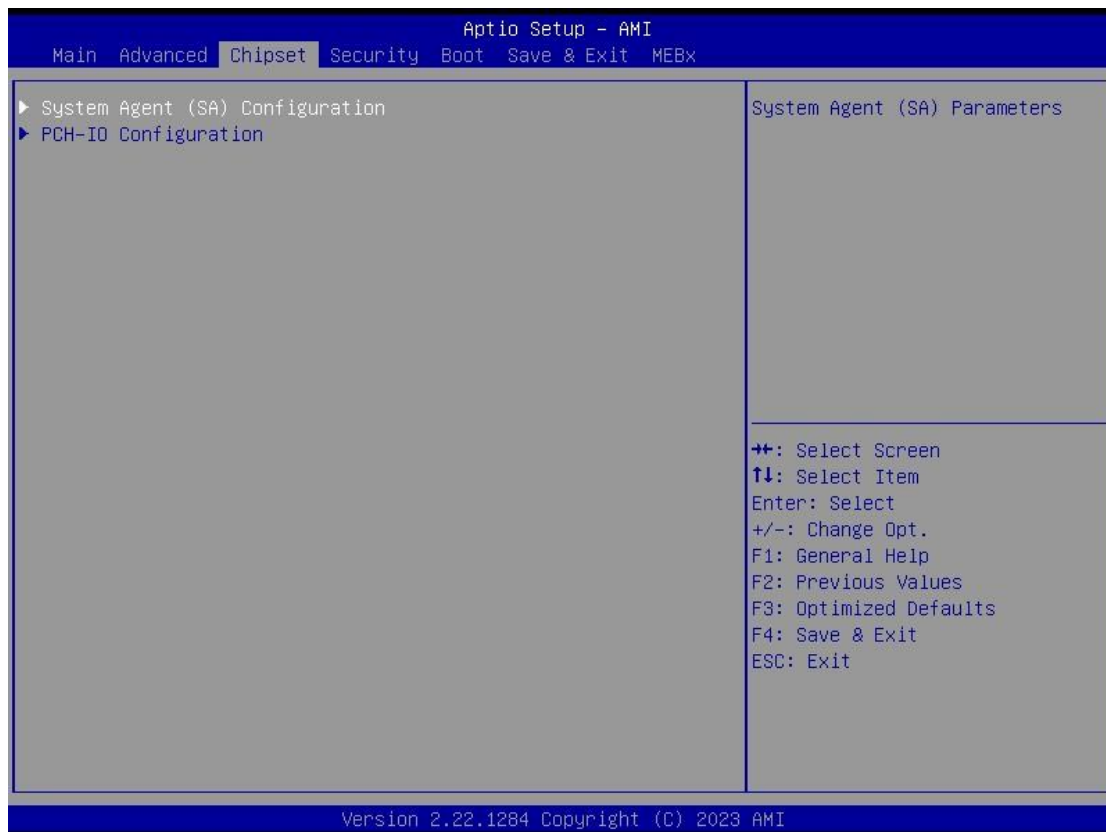
Display all detected USB devices.

4.5 Chipset Menu

The Chipset menu allows users to change the advanced chipset settings. You can select any of the items in the left frame of the screen to go to the sub menus:

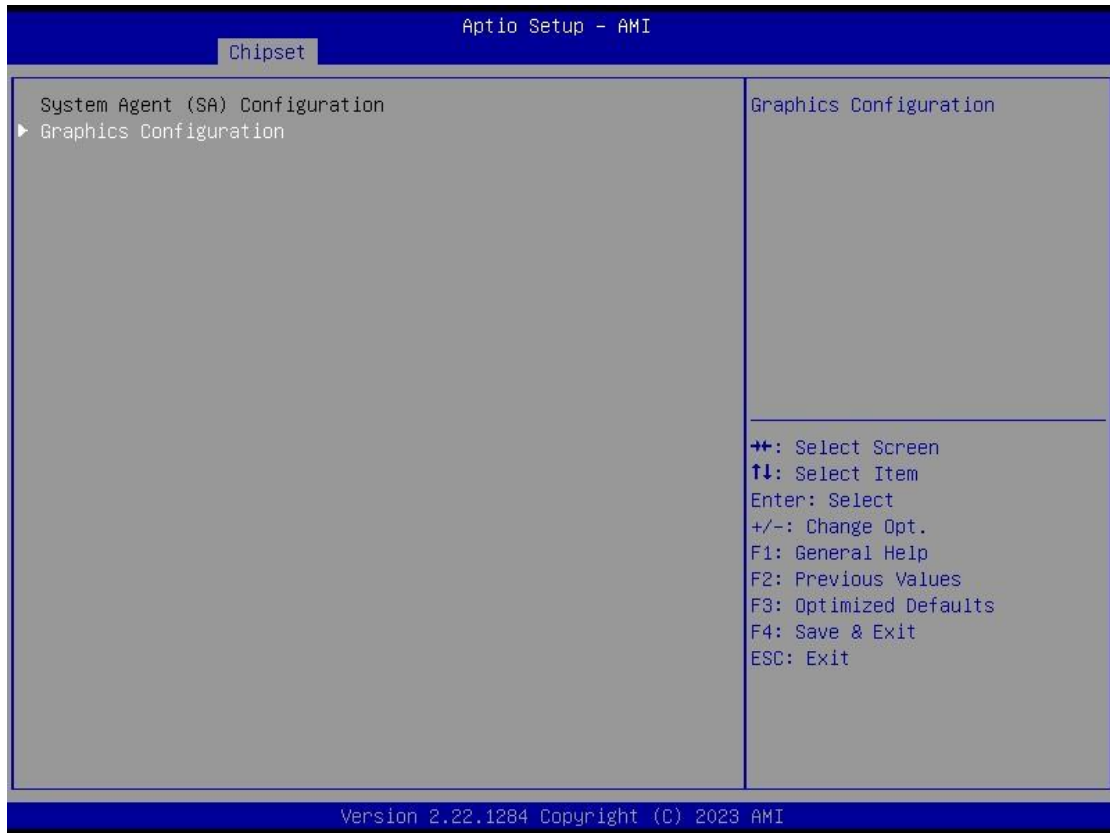
- ▶ System Agent (SA) Configuration
- ▶ PCH-IO Configuration

For items marked with “▶”, please press <Enter> for more options.



- **System Agent (SA) Configuration**

This screen shows System Agent version information and provides function for specifying related parameters.



Graphics Configuration

Open sub menu for parameters related to graphics configuration.

● **Graphics Configuration**



DDI1 Signal Select

Select the DDI1 signal output to DisplayPort or HDMI.

DDI2 Signal Select

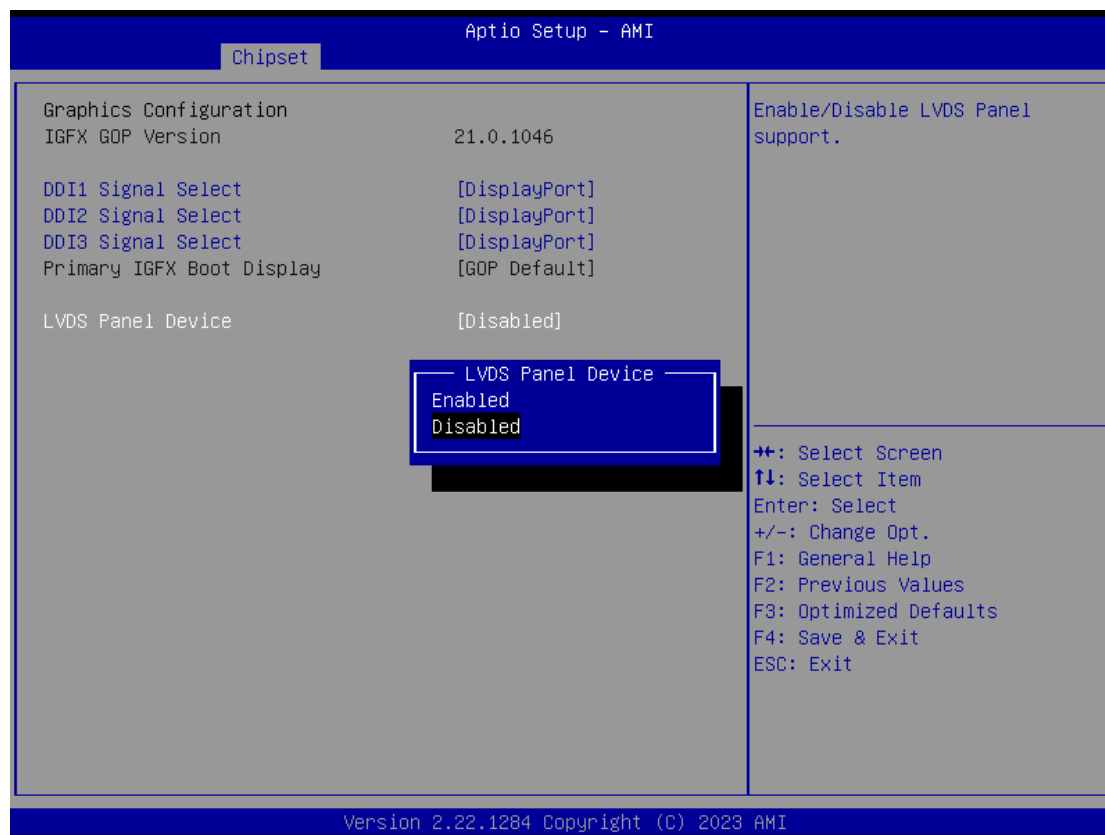
Select the DDI2 signal output to DisplayPort or HDMI.

DDI3 Signal Select

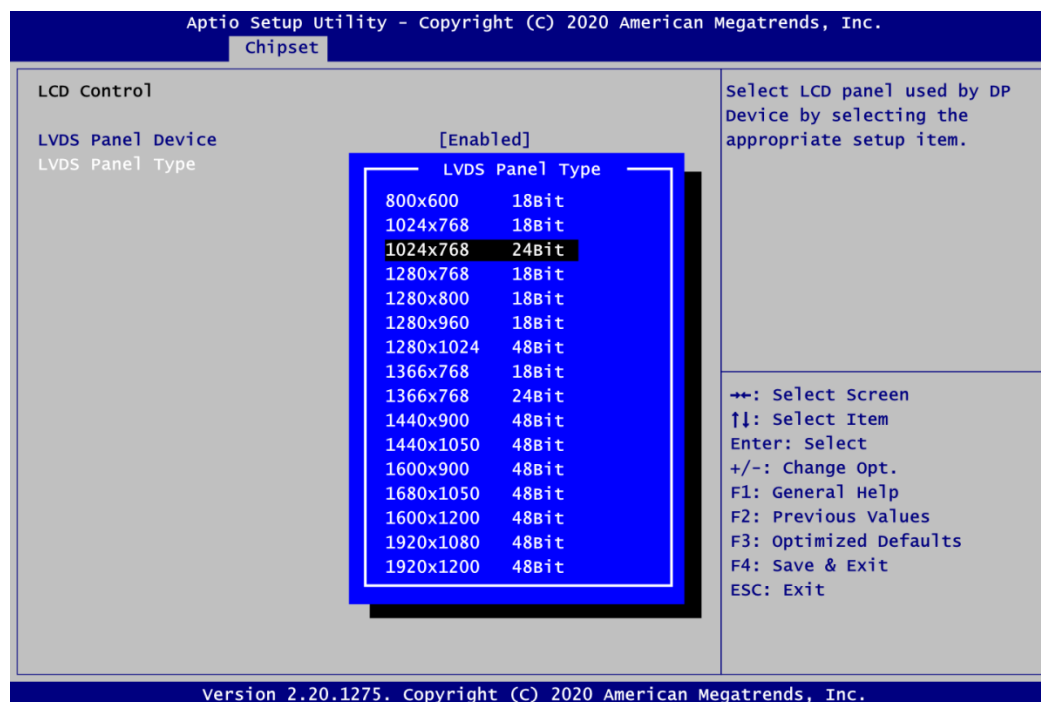
Select the DDI2\3 signal output to DisplayPort or HDMI.

LVDS Panel Device

Enable or disable LVDS panel depend on application.



- **LCD Control**

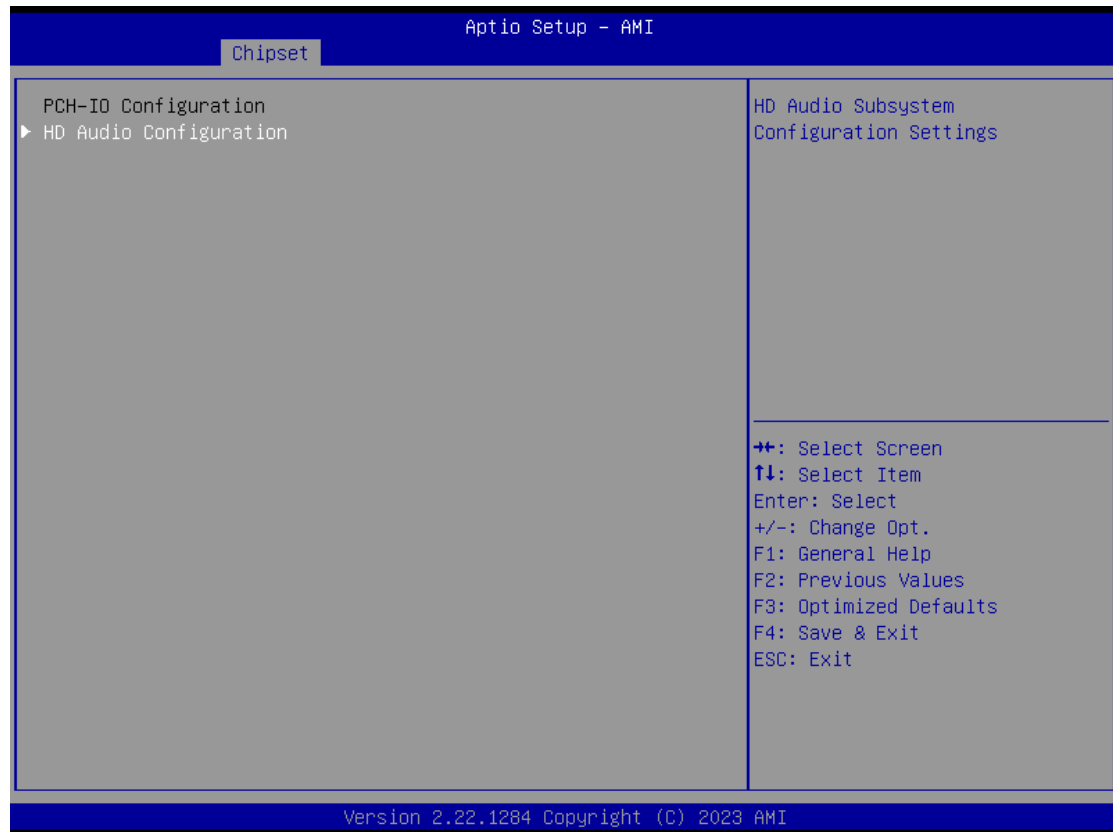


LVDS Panel Type

After LVDS Panel Device is enabled, the LVDS Panel Type is showed for selection. Select the appropriate LVDS panel resolution by options in image above.

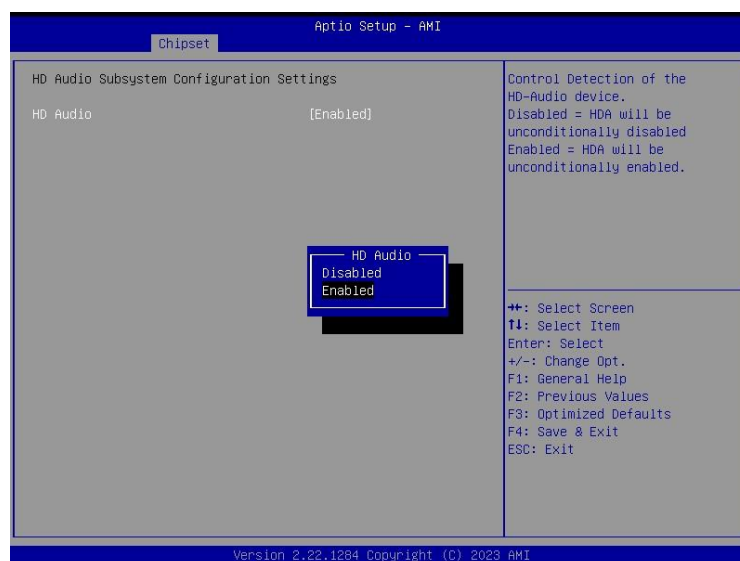
- **PCH-IO Configuration**

This screen shows PCH-IO information.



HD Audio Configuration

Enable or disable onboard Audio controller.



4.6 Security Menu

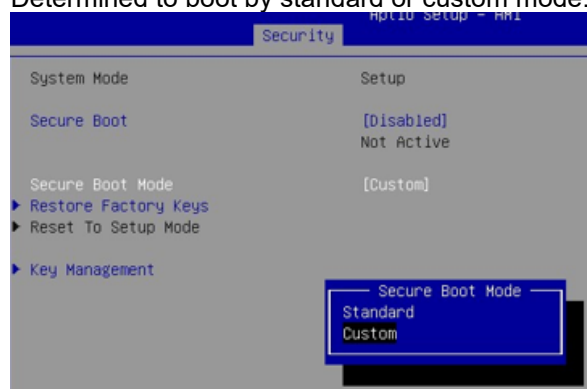
The Security menu allows users to change the security settings for the system.



- **Administrator Password.**
Set administrator password.
- **User Password**
Set user password.
- **Secure Boot**
Enable and disable secure boot and determined boot mode.

Secure Boot mode

Determined to boot by standard or custom mode.



Key management

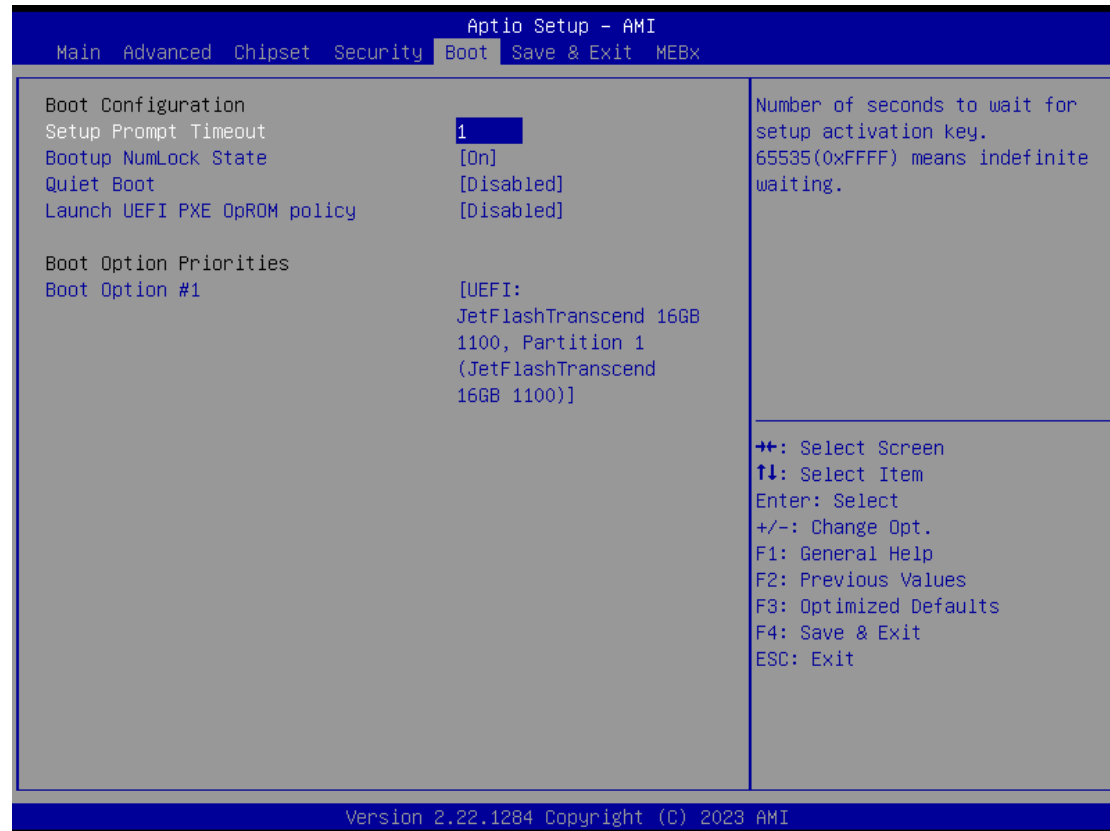
Enable or disable factory key provision

The screenshot displays the BIOS Key management menu. At the top, 'Vendor Keys' is listed as 'Valid'. Below it, 'Factory Key Provision' is listed as '[Disabled]'. A list of options follows: 'Restore Factory Keys', 'Reset To Setup Mode', 'Export Secure Boot variables', and 'Enroll Efi Image'. A table of Secure Boot variables is shown below, with columns for 'Secure Boot variable', 'Size', 'Keys', and 'Key Source'. The table lists Platform Key (PK), Key Exchange Keys (KEK), Authorized Signatures (db), Forbidden Signatures (dbx), Authorized TimeStamps (dbt), and OsRecovery Signatures (dhr). A context menu is open over the 'Factory Key Provision' entry, showing 'Disabled' (highlighted) and 'Enabled' options.

Secure Boot variable	Size	Keys	Key Source
▶ Platform Key (PK)		0	0 No Keys
▶ Key Exchange Keys (KEK)			
▶ Authorized Signatures (db)			
▶ Forbidden Signatures (dbx)			
▶ Authorized TimeStamps (dbt)			
▶ OsRecovery Signatures (dhr)		0	

4.7 Boot Menu

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



- **Setup Prompt Timeout**

Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.

- **Bootup NumLock State**

Use this item to select the power-on state for the keyboard NumLock.

- **Quiet Boot**

Select to display either POST output messages or a splash screen during boot-up.

- **Launch UEFI PXE OpROM policy**

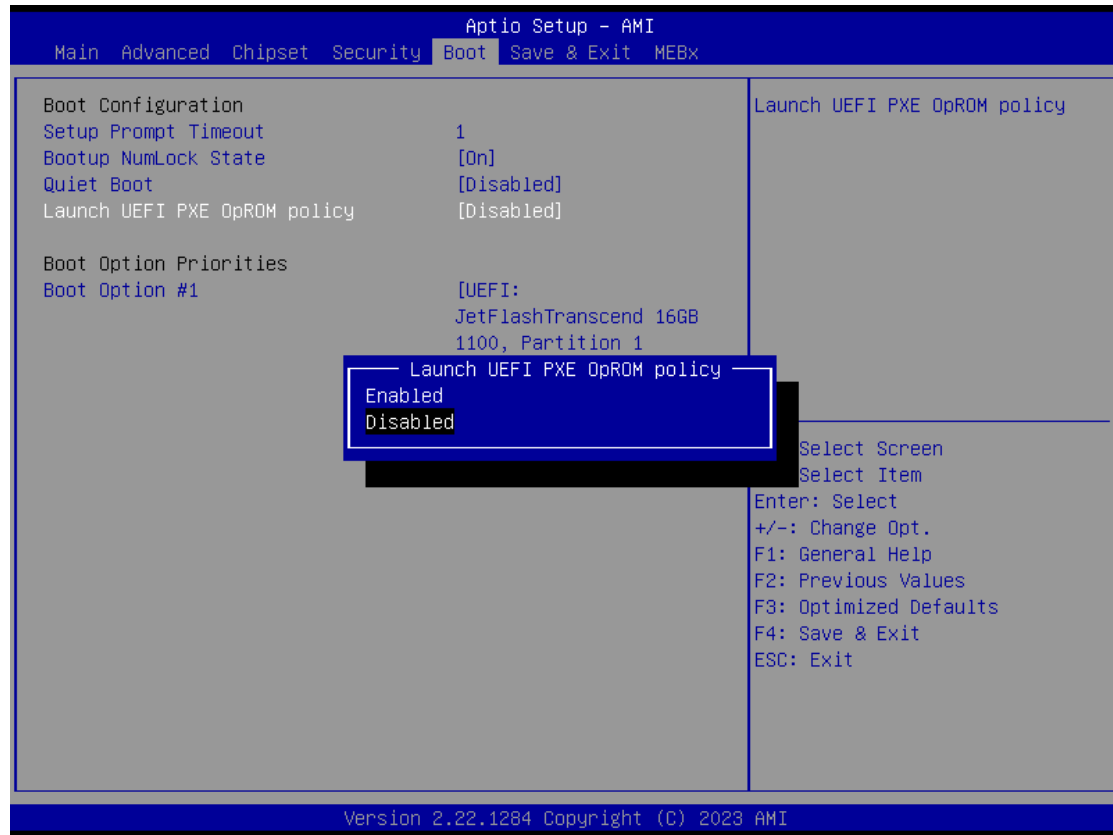
Use this item to enable or disable the boot ROM function of the onboard LAN chip when the system boots up.

- **Boot Option Priorities**

These are settings for boot priority. Specify the boot device priority sequence from the available devices.

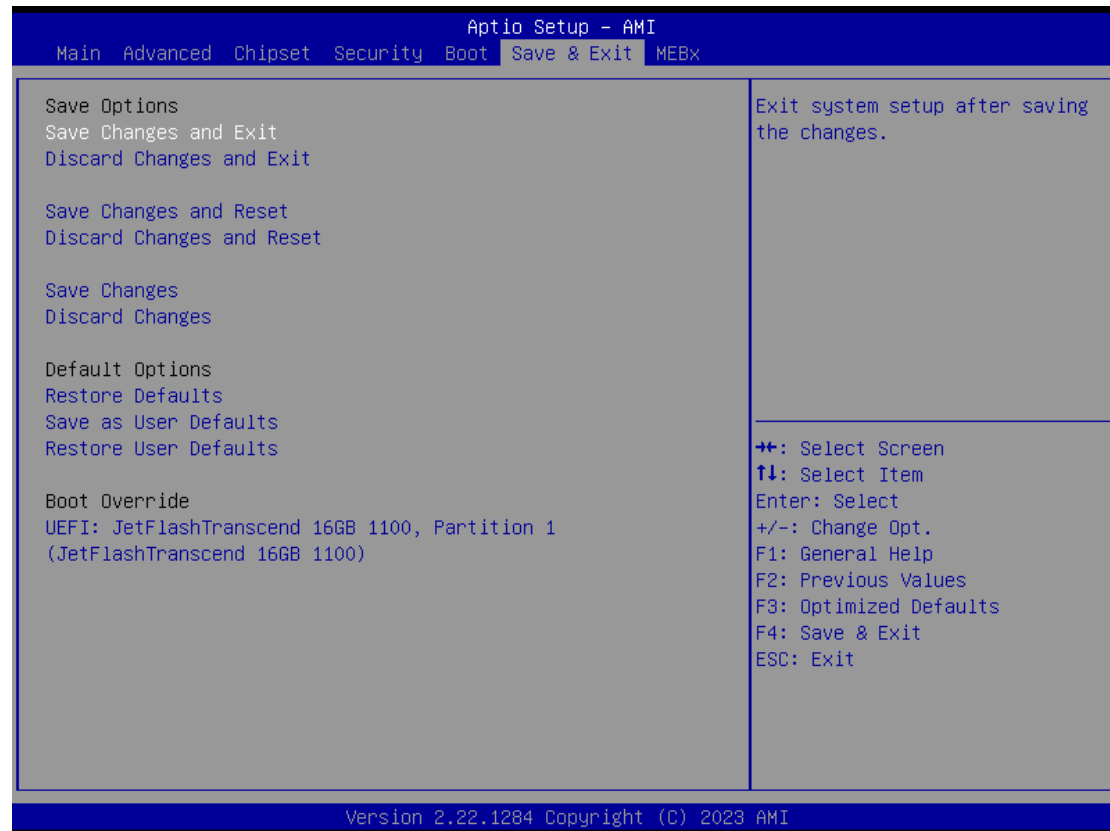
- **Launch UEFI PXE OpROM policy**

Enable or disable UEFI PXE OpROM policy



4.8 Save & Exit Menu

The Save & Exit menu allows users to load your system configuration 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 return to Main Menu. 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 return to Main Menu. 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.

- **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 boot device regardless of the current boot priority order.

4.9 MEBx

The page is for enable and optimize AMT function.

*SOP of enabling MEBx page.

1. Boot system to OS
2. Reboot system and enter BIOS
3. See the MEBx page and enter ME password

Intel® ME Password

To enable ME function, user can enter MEBx page and fill in native password" admin " to unlock AMT setting and create new password. (See detail in Appendix C iAMT Settings)



This page is intentionally left blank.

Appendix A

Watchdog Timer

A.1 About Watchdog Timer

After the system stops working for a while, it can be auto-reset by the watchdog timer. The integrated watchdog timer can be set up in the system reset mode by program.

A.2 How to Use Watchdog Timer (C programming language)

```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

```
#include <stdio.h>
#include <conio.h>
#include <stdlib.h>
#include <dos.h>
```

```
#define AXIOM_WDT_TIMER    0xFA10
#define AXIOM_WDT_TRIGGER  0xFA12
```

```
void main()
```

```
{
```

```
    unsigned long int  DefaultTimer = 0xFFFF; // 65535 Seconds
    unsigned long int  CurrentWdtTimer = 0;
```

```
    clrscr();
```

```
    // Set WDT Timer, maximum is 65535 seconds
```

```
    outportw(AXIOM_WDT_TIMER, DefaultTimer);
```

```
    printf("Set WDT Timer to: %ld Seconds\n", DefaultTimer);
```

```
    // 0x01: Enabled WDT, 0x00: Disabled WDT
```

```
    outportb(AXIOM_WDT_TRIGGER, 0x01);
```

```
    printf("Enabled WDT Timer\n");
```

```
    while(1)
```

```
    {
```

```
        clrscr();
```

```
        // Get current WDT Timer
```

```
        CurrentWdtTimer = inportw(AXIOM_WDT_TIMER);
```

```
        printf("Set WDT Timer to: %ld Seconds\n", DefaultTimer);
```

```
        printf("Current WDT Timer: %ld Seconds\n", CurrentWdtTimer);
```

```
        delay(1000);
```

```
    }
```

```
}
```

```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

This page is intentionally left blank.

Appendix B

Digital I/O

B.1 About Digital I/O

The onboard GPIO or digital I/O has 8 bits (DIO0~7). Each bit can be set to function as input or output by software programming. In default, all pins are pulled high with +3.3V level (according to main power). The BIOS default settings are 4 inputs and 4 outputs where all of these pins are set to 1.

B.2 How to Use Digital I/O (C programming language)

```

////////////////////////////////////
#include <stdio.h>
#include <conio.h>
#include <stdlib.h>
#include <dos.h>

#define AXIOM_DIO_IN_OUT_ADDR          0xFA31
#define AXIOM_DIO_HIGH_LOW_ADDR       0xFA32

#define DIO_PIN1 BIT0 //correspondence to HW pin is GPIO
#define DIO_PIN2 BIT1 //correspondence to HW pin is GPI1
#define DIO_PIN3 BIT2 //correspondence to HW pin is GPI2
#define DIO_PIN4 BIT3 //correspondence to HW pin is GPI3
#define DIO_PIN5 BIT4 //correspondence to HW pin is GPO0
#define DIO_PIN6 BIT5 //correspondence to HW pin is GPO1
#define DIO_PIN7 BIT6 //correspondence to HW pin is GPO2
#define DIO_PIN8 BIT7 //correspondence to HW pin is GPO3

void main()
{
    // BIT0-BIT3 is input,BIT4-BIT7 is output
    unsigned char DIO_DefaultInOutSetting = 0x0F;
    // BIT0-BIT3 is input so do not care,BIT4-BIT7 is High
    unsigned char DIO_DefaultHighLowSetting = 0xF0;

    clrscr();
    // Set DIO input/output,1:input,0:output,BIT0-BIT3 is input,BIT4-BIT7 is output
    outportb(AXIOM_DIO_IN_OUT_ADDR, DIO_DefaultInOutSetting);
    printf("DIO input/output set to 0x%X \n", DIO_DefaultInOutSetting);
    printf("BIT0-BIT3 is setting to input,BIT4-BIT7 is setting to output\n");
}

```

```
// Set DIO High/Low,1:High,0:Low,now is set to BIT0-BIT3 is Low,BIT4-BIT7 is
// High
outportb(AXIOM_DIO_HIGH_LOW_ADDR, DIO_DefaultHighLowSetting);
printf("DIO High/Low set to 0x%X \n", DIO_DefaultHighLowSetting);
printf("BIT0-BIT3 is set to input so do not care,BIT4-BIT7 is setting to High");

while(1);
}
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

Appendix C

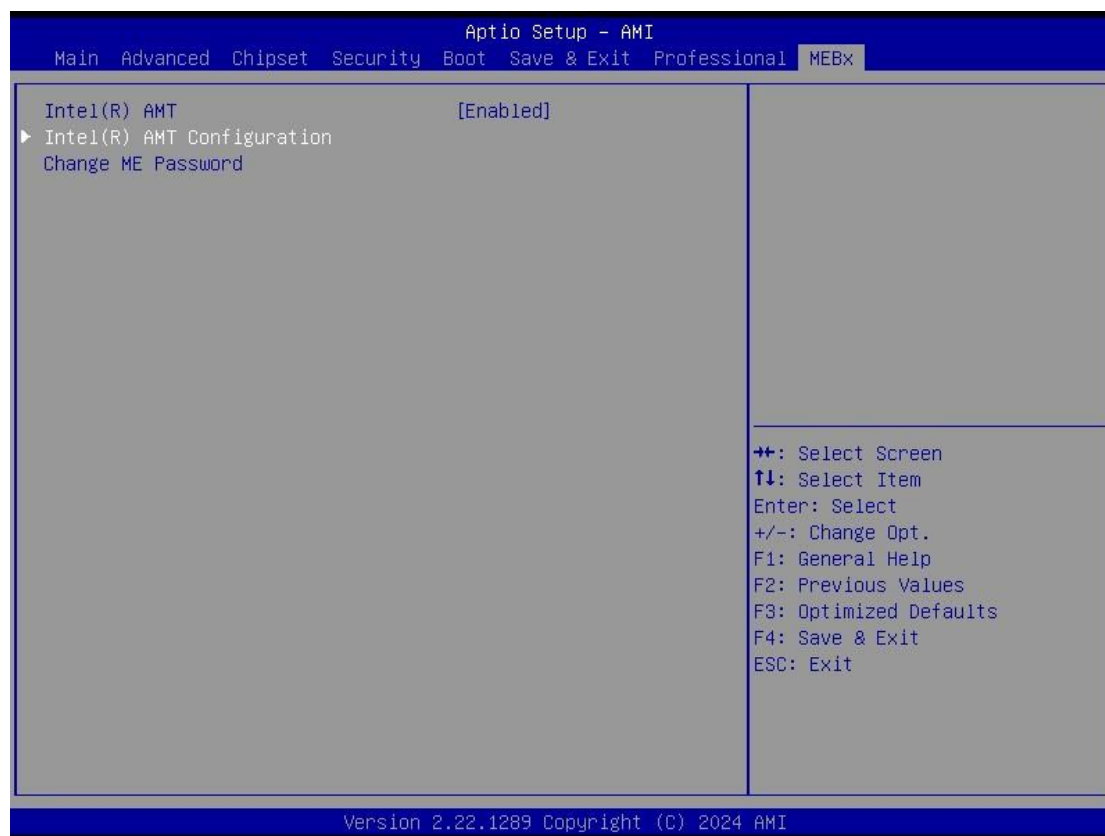
iAMT Settings

The Intel® Active Management Technology (Intel® iAMT) has decreased a major barrier to IT efficiency that uses built-in platform capabilities and popular third-party management and security applications to allow IT a better discovering, healing, and protection their networked computing assets.

In order to utilize Intel® iAMT you must enter the ME BIOS (<Ctrl + P> during system startup), change the ME BIOS password, and then select “Intel® iAMT” as the manageability feature.

C.1 iAMT Settings

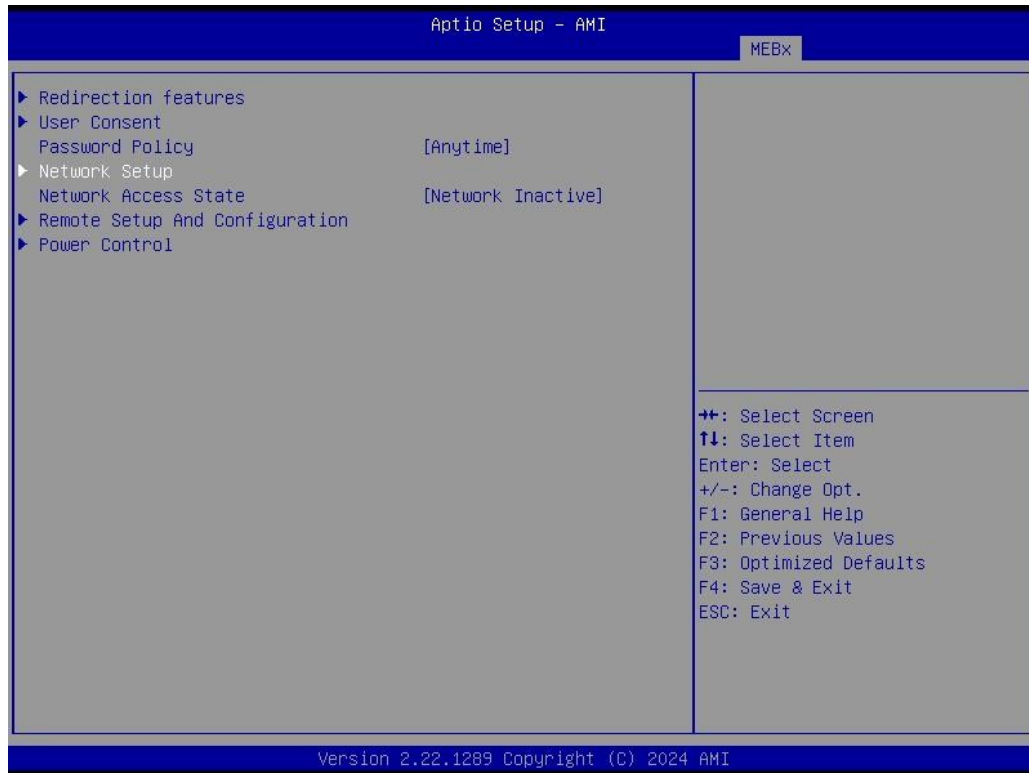
Select Intel® AMT configuration and press <Enter>.



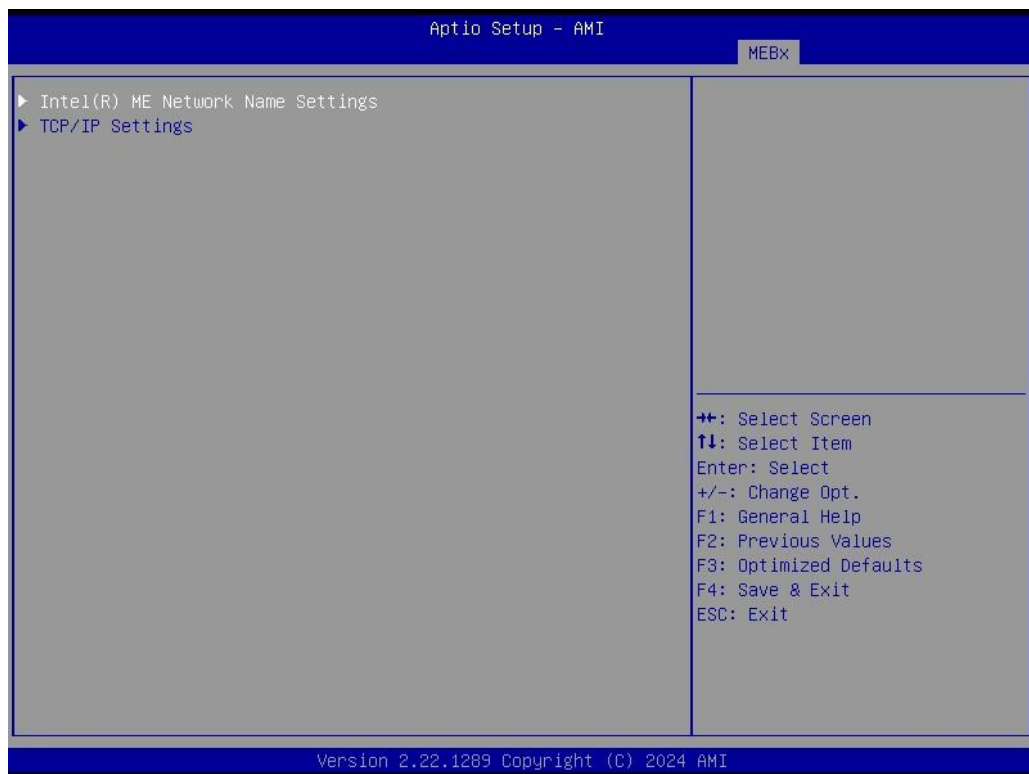
From AMT Configuration menu, select Manageability Feature Selection and set it to Enabled. This item allows you to enable or disable Intel® AMT feature.

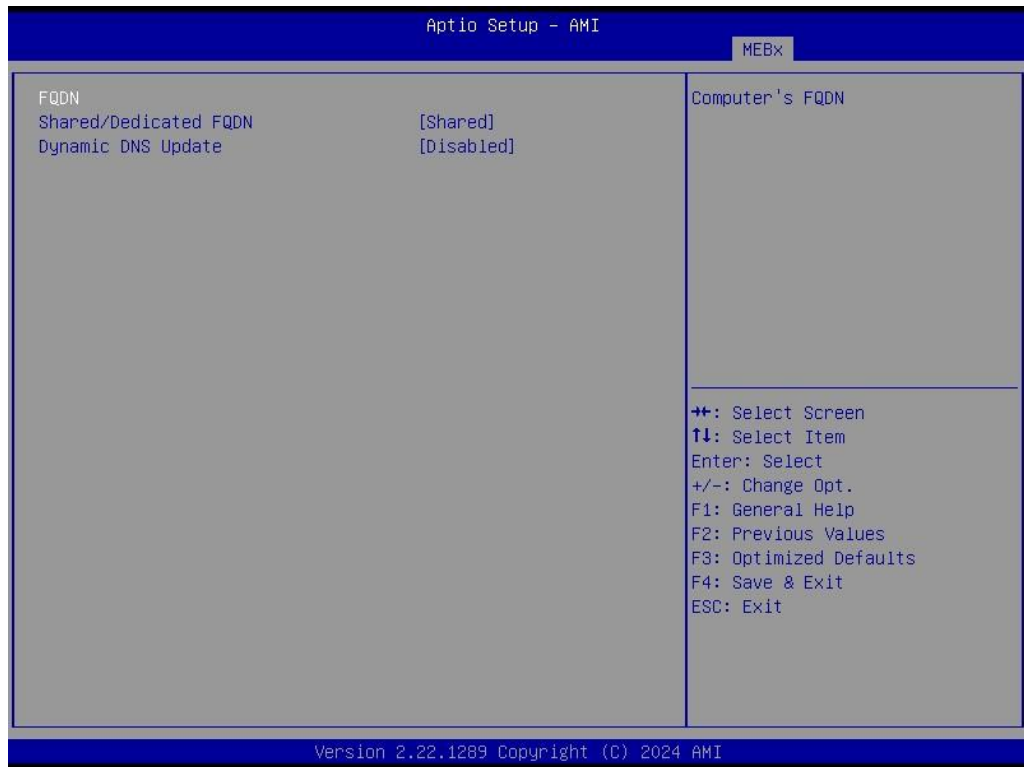
- **Network Setup**

1. Select Network Setup to configure iAMT.



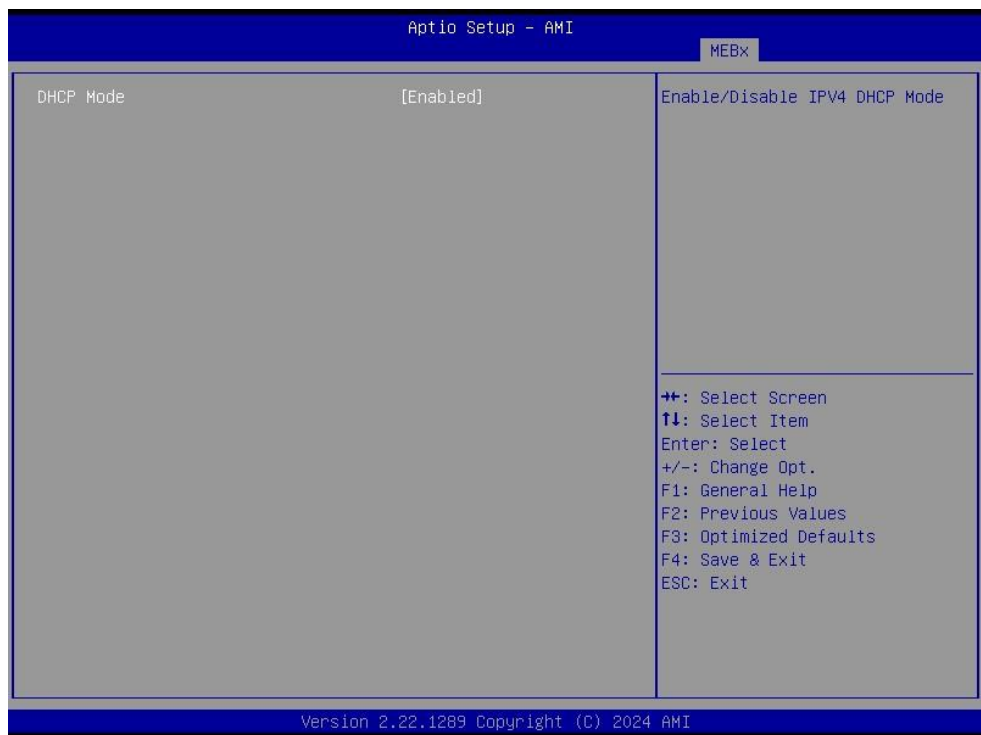
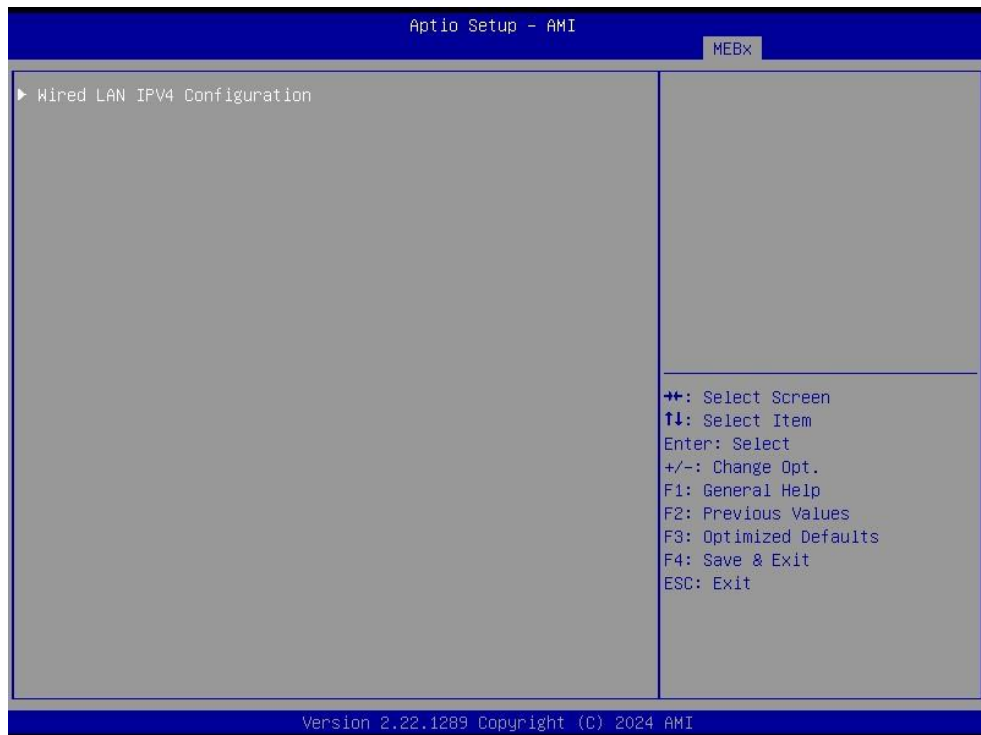
2. Select ME Network Name Settings to set computer host and domain name.





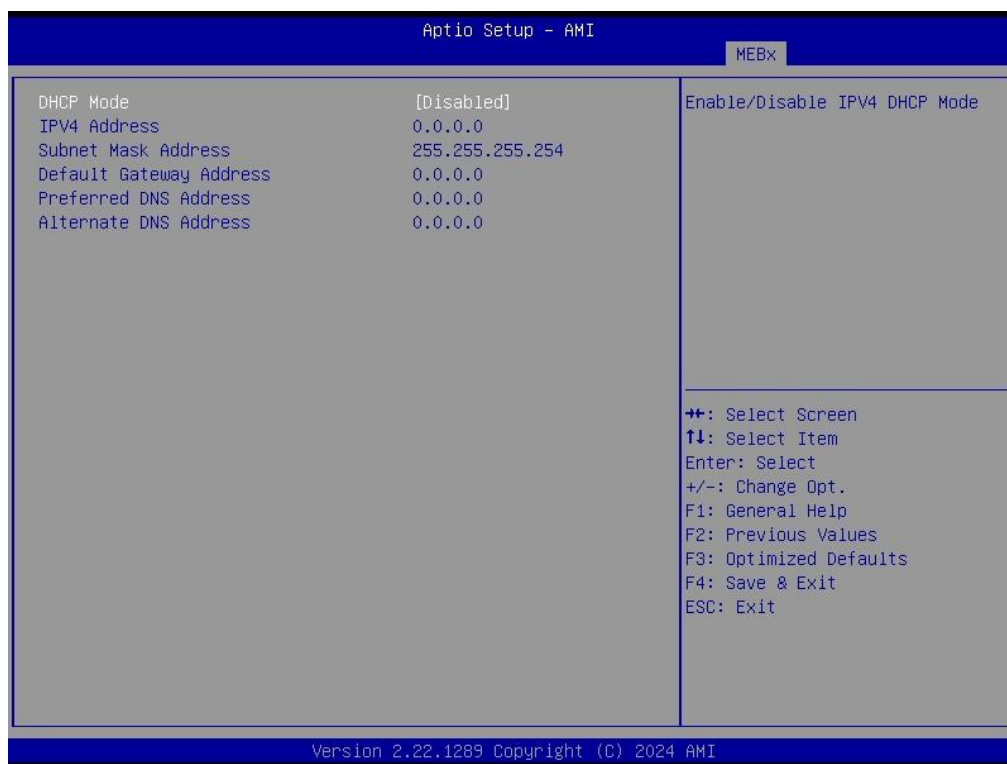
3. Select TCP/IP to get into Network interface and set it to Enabled. Get into DHCP Mode and set it to Disabled.



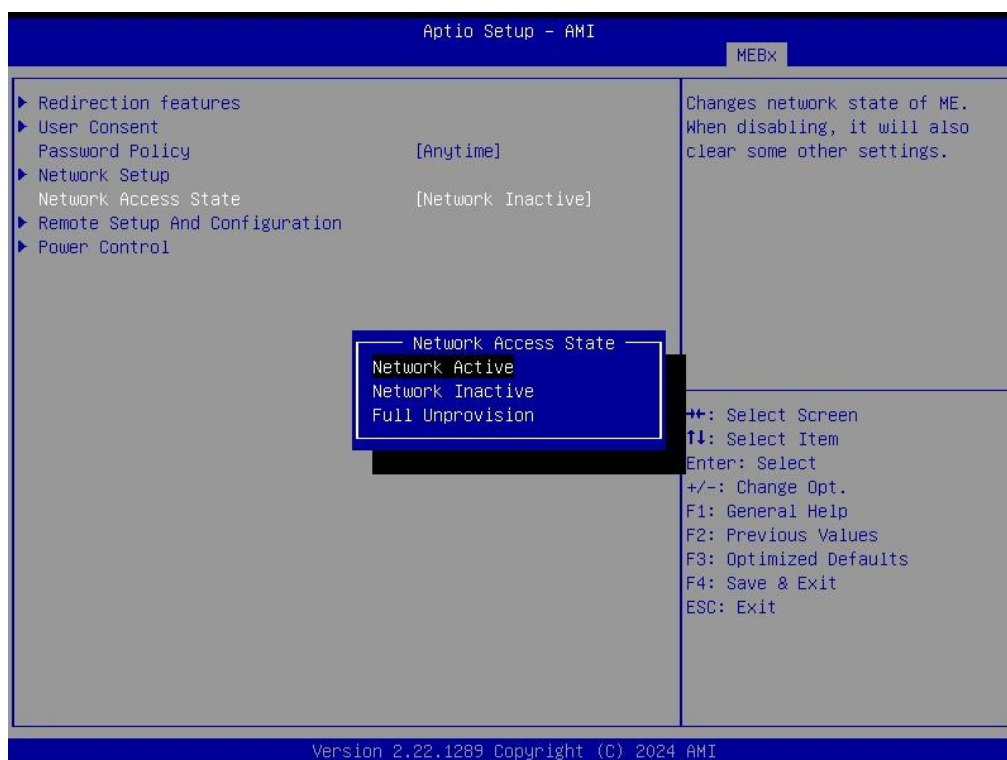


4. If DHCP Mode is disabled, set the following settings:

- IP address
- Subnet mask



5. Go back to Intel® iAMT Configuration, then select Activate Network Access and press <Enter>.

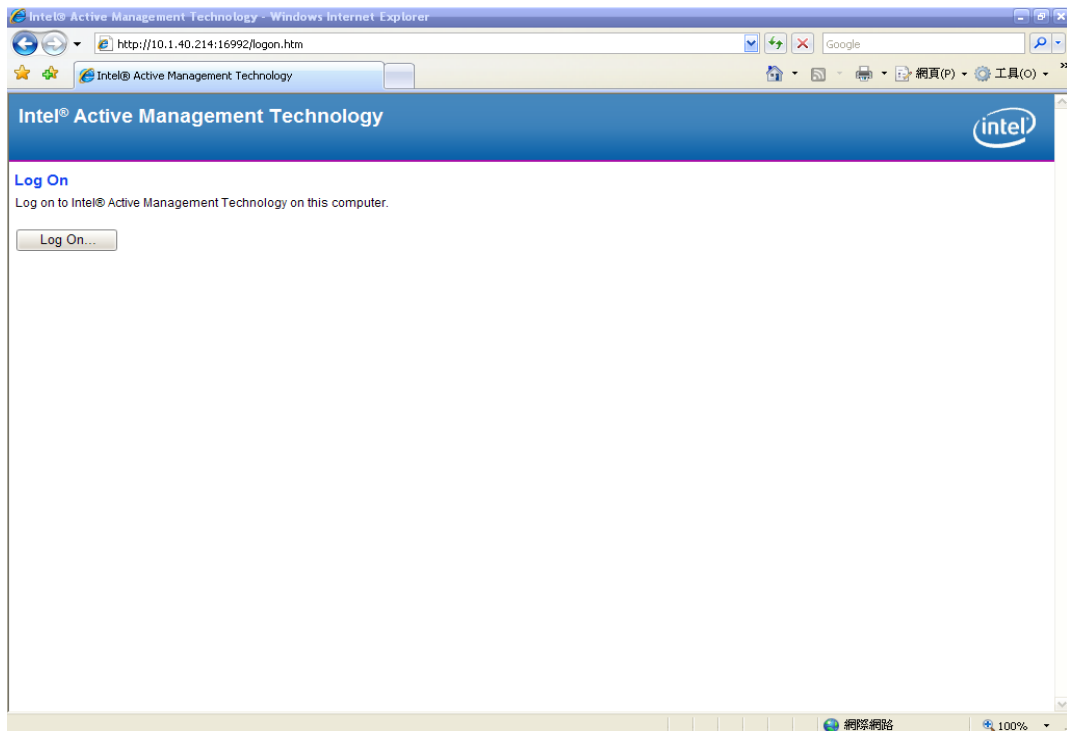


6. Exit from MEBx after completing the iAMT settings.

C.2 iAMT Web Console

1. From a web browser, please type [http://\(IP ADDRESS\):16992](http://(IP ADDRESS):16992), which connects to iAMT Web.

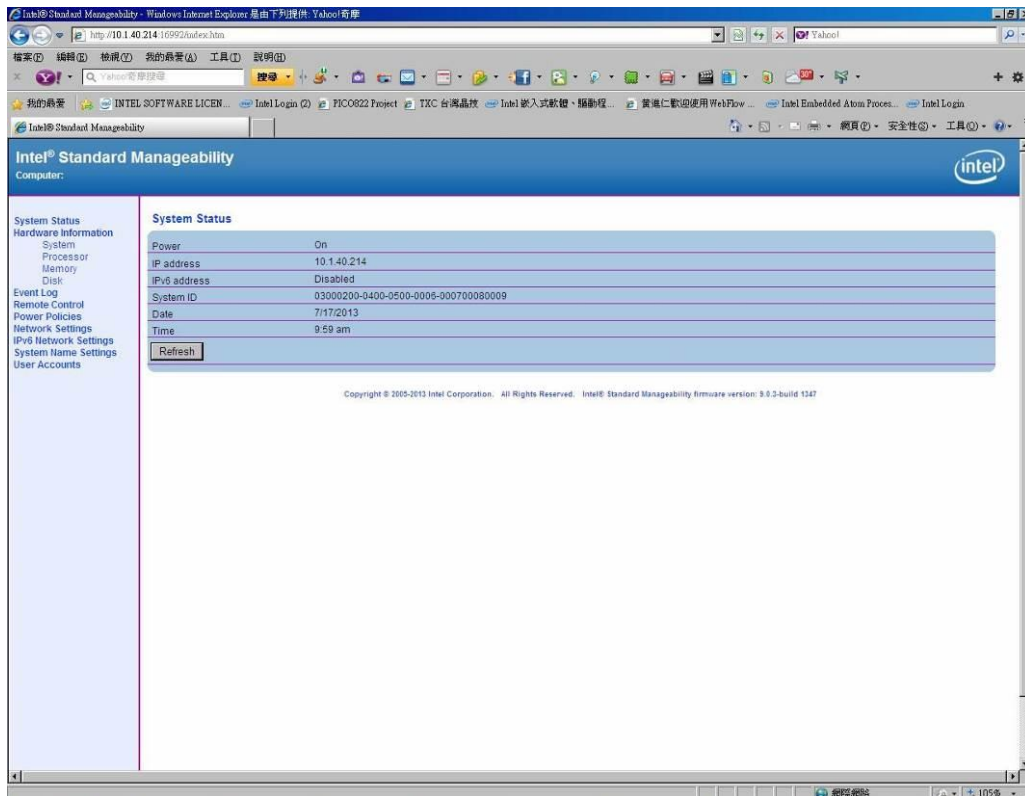
Example: <http://10.1.40.214:16992>



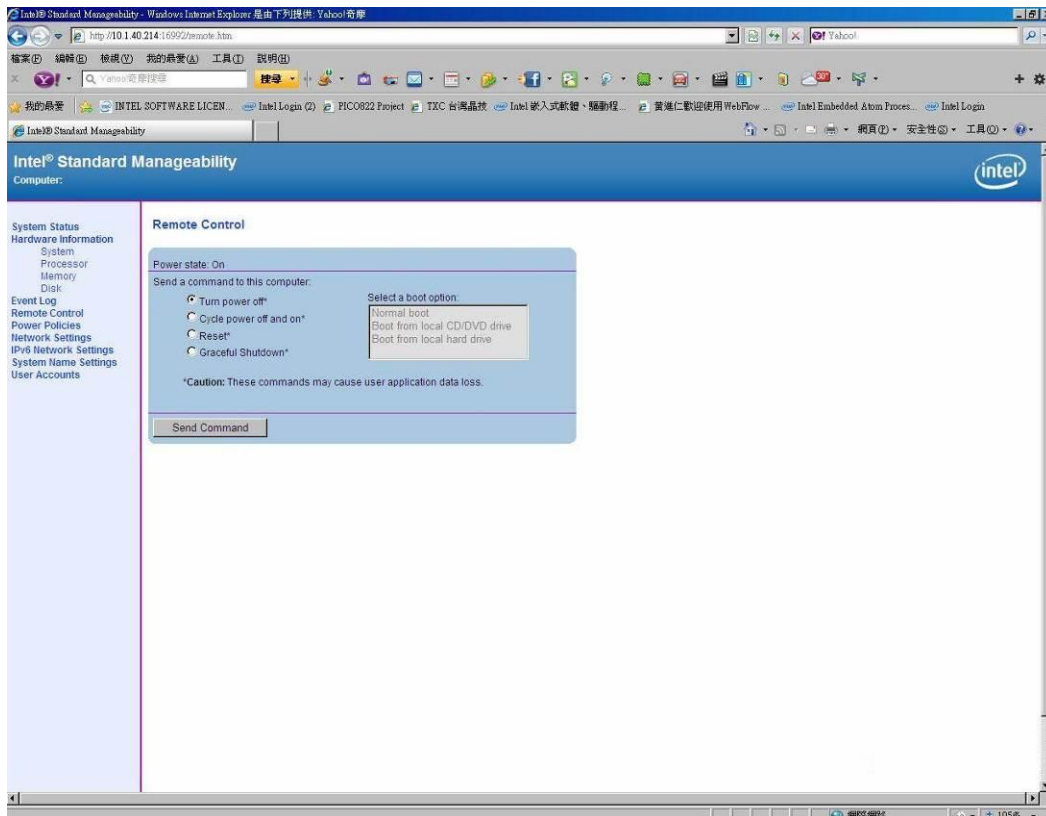
2. To log on, you will be required to type in username and password for access to the Web.

USER: admin (default value)
PASS: (MEBx password)

3. Enter the iAMT Web.



- Click Remote Control, and select commands on the right side.



- When you have finished using the iAMT Web console, close the Web browser.