



S5652

Version 1.0I

Copyright

Copyright© 2023 MiTAC International Corporation. All rights reserved. No part of this manual may be reproduced or translated without prior written consent from MiTAC International Corporation.

Trademark

All registered and unregistered trademarks and company names contained in this manual are property of their respective owners including, but not limited to the following.

TYAN® is a trademark of MiTAC International Corporation.

Intel® is a trademark of Intel® Corporation.

AMI, AMI BIOS are trademarks of AMI Technologies.

Microsoft®, Windows® are trademarks of Microsoft Corporation.

Winbond® is a trademark of Winbond Electronics Corporation.

Notice

Information contained in this document is furnished by MiTAC International Corporation and has been reviewed for accuracy and reliability prior to printing. MiTAC assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of TYAN® products including liability or warranties relating to fitness for a particular purpose or merchantability. MiTAC retains the right to make changes to product descriptions and/or specifications at any time, without notice. In no event will MiTAC be held liable for any direct or indirect, incidental or consequential damage, loss of use, loss of data or other malady resulting from errors or inaccuracies of information contained in this document.

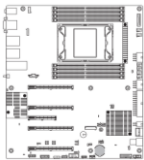
Contents

Chapter 1: Instruction	4
1.1 Congratulations	4
1.2 Hardware Specifications	4
1.3 Software Specifications	8
Chapter 2: Board Installation	9
2.1 Board Image	10
2.2 Block Diagram	11
2.3 Motherboard Mechanical Drawing	13
2.4 Board Parts, Jumpers and Connectors	14
2.5 LED Definitions	25
2.6 Installing the Processor and Heatsink	27
2.7 Thermal Interface Material	30
2.8 Tips on Installing Motherboard in Chassis	32
2.9 Installing the Memory	34
2.10 Installing the M.2 standoff and M.2 Card	38
2.11 Attaching Drive Cables	40
2.12 Installing Add-In Cards	41
2.13 Connecting External Devices	42
2.14 Installing the Power Supply	44
2.15 Finishing Up	45
Chapter 3: BIOS Setup	46
3.1 About the BIOS	46
3.2 Main Menu	48
3.3 Advanced Menu	50
3.4 CPU Configuration Subsystem	125
3.5 Chipset Menu	152
3.6 Server Management	164
3.7 Security	173
3.8 Boot	178
3.9 Save & Exit	181
Chapter 4: Diagnostics	183
4.1 Flash Utility	183
4.2 AMIBIOS Post Code (Aptio)	184
Appendix I: How to recover UEFI BIOS	191
Appendix II: Fan and Temp Sensors	193
Appendix III: PCIE Bus Number	197
Glossary	198
Technical Support	204

Before you begin...

Check the box contents!

The retail motherboard package should contain the following:

	S5652 Motherboard x 1
	XCC CPU Carrier x1
	MCC CPU Carrier x1
	SATA Single Cable x 2
	Rear IO shielding x 1
	S5652 Quick Installation Guide x 1
	M.2 Standoff & Screw x 3

IMPORTANT NOTE:

Sales samples may not come with any of the accessories listed above.

If you have ordered a sales sample and you are missing any of the above items, please contact your sales representative to help order accessories.

Chapter 1: Instruction

1.1 Congratulations

You have purchased the powerful TYAN® S5652 motherboard, based on the Intel® C741 chipset. The S5652 is designed to support Single 4th Gen. Intel Xeon Scalable Processor / 5th Gen. Intel Xeon Scalable Processor, and up to 1,024GB RDIMM/2,048GB 3DS RDIMM 5600/4800/4400 DDR5 memory. Leveraging advanced technology from Intel®, the S5652 is capable of offering scalable 64-bit computing, high-bandwidth memory design, and lightning-fast PCI-E bus implementation.

The S5652 not only empowers you in today's demanding IT environment but also offers a smooth path for future application upgradeability. All of these rich feature sets provide the S5652 with the power and flexibility to meet demanding requirements for today's IT environments.

Remember to visit the TYAN® website at <http://www.mitaccomputing.com>. There you can find all the information on all TYAN® products as well as all the supporting documentation, FAQs, Drivers and BIOS upgrades.

1.2 Hardware Specifications

S5652AGMNRE Specifications

Processor	Q'ty / Socket Type	(1) LGA4677
	Supported CPU Series	4th Gen. Intel Xeon Scalable Processors / 5th Gen. Intel Xeon Scalable Processors
	Thermal Design Power Wattage	Max up to 350W (TDP)
Chipset	PCH	Intel C741
Memory	Supported DIMM Qty	(8) DIMM slots
	DIMM Type / Speed	DDR5 4800 MHz (1DPC) / 4400MHz (2DPC) - 4th Gen. / DDR5 5600 MHz (1DPC) / 4400MHz (2DPC) - 5th Gen.
	Capacity	Up to 1,024GB RDIMM/2,048GB 3DS RDIMM 5600/4800/4400 memory *Follow latest Intel DDR5 Memory POR
	Memory channel	8 Channels per CPU
	Memory voltage	1.1V
Expansion Slots	PCIe	(1) PCIe Gen.5 x8 slot / (4) PCIe Gen.5 x16 slot
LAN	Q'ty / Port	(1) GbE port + (1) GbE dedicated for IPMI
	Controller	Intel I210
	PHY	Realtek RTL8211F
Storage SATA	Connector	(1) Mini SAS-HD connector + (2) SATA-III connectors

	Controller	Intel C741
	Speed	6Gb/s
	RAID	RAID 0/1/10/5 (Intel RSTe)
Storage NVMe	Connector (M.2)	(1) 2280 (by PCIe 4 interface)
	Connector (U.2)	(1) MCIO x8
Storage (Optional)	VROC Support	Yes
Graphic VGA	Connector type	D-Sub 15-pin
	Resolution	Up to 1920x1200 @60Hz
	Chipset	Aspeed AST2600
Input /Output	USB	(1) USB2.0 port (Type-A) / (1) USB3.2 Gen.1 header / (2) USB2.0 ports (@ rear) / (2) USB3.2 Gen.1 ports (@rear)
	COM	(1) COM port header + (1) DB-9 COM Connector (@rear)
	VGA	(1) D-Sub 15-pin VGA port (@ rear)
	RJ-45	(1) GbE port + (1) GbE dedicated for IPMI
	Front Panel	(1) 2x12-pin SSI front panel header(mini type)
	Audio	(1) 2x5-pin header / (1) 3 holes Audio Jack connector
	SATA	(1) Mini SAS-HD connector + (2) SATA-III connectors
	Power	8-pin power connectors
	Others	(1) UID button
TPM (Optional)	TPM Support	Please refer to our TPM supported list.
	Interface	SPI
System Monitoring	Chipset	Aspeed AST2600
	Fan	Total (6) 4-pin headers
	Temperature	Monitors temperature for CPU, memory & system environment
	Voltage	Monitors voltage for CPU, memory, chipset & power supply
	LED	Over temperature warning indicator / Fan & PSU fail LED indicator
	Others	Watchdog timer support
Audio	Chipset	Realtek ALC888S
	Feature	2.1 ch
Server Management	Onboard Chipset	Onboard Aspeed AST2600
	AST2600 iKVM Feature	24-bit high quality video compression / Supports storage over IP and remote platform-flash / USB 2.0 virtual hub
	AST2600 IPMI Feature	IPMI 2.0 compliant baseboard management controller (BMC) / 10/100/1000 Mb/s MAC interface
BIOS	Brand / ROM size	AMI / 32MB

	Feature	Hardware Monitor / Boot from USB device/PXE via LAN/Storage / User Configurable FAN PWM Duty Cycle / SMBIOS 3.3/PnP/Wake on LAN / ACPI sleeping states S0, S5
Physical Dimension	Form Factor	SSI CEB compatible
	Board Dimension	12" x 10.5" (305 x 267mm)
Regulation	FCC (SDoC)	Class B
	CE (DoC)	Class B
	RCM	Class B
	VCCI	Class B
Operating Environment	Operating Temp.	0° C ~ 40° C (32° F ~ 104° F)
	Non-operating Temp.	- 40° C ~ 70° C (-40° F ~ 158° F)
	In/Non-operating Humidity	90%, non-condensing at 35° C
RoHS	RoHS 6/6 Compliant	Yes
Operating System	OS supported list	Please refer to our AVL support lists.
Package Contains	Motherboard	(1) S5652 Motherboard
	Manual	(1) Quick Installation Guide
	I/O Shield	(1) I/O Shield
	Cable SATA	(2) SATA signal cables

S5652AGM3NRE-2T Specifications

Processor	Q'ty / Socket Type	(1) LGA4677
	Supported CPU Series	4th Gen. Intel Xeon Scalable Processors / 5th Gen. Intel Xeon Scalable Processors
	Thermal Design Power Wattage	Max up to 350W (TDP)
Chipset	PCH	Intel C741
Memory	Supported DIMM Qty	(8) DIMM slots
	DIMM Type / Speed	DDR5 4800 MHz (1DPC) / 4400MHz (2DPC) - 4th Gen. / DDR5 5600 MHz (1DPC) / 4400MHz (2DPC) - 5th Gen.
	Capacity	Up to 1,024GB RDIMM/2,048GB 3DS RDIMM 5600/4800/4400 memory *Follow latest Intel DDR5 Memory POR
	Memory channel	8 Channels per CPU
	Memory voltage	1.1V
Expansion Slots	PCIe	(1) PCIe Gen.5 x8 slot / (4) PCIe Gen.5 x16 slot
LAN	Q'ty / Port	(2) 10GbE ports + (1) GbE ports + (1) GbE dedicated for IPMI
	Controller	Intel I210 / Intel X550
	PHY	Realtek RTL8211F

Storage SATA	Connector	(1) Mini SAS-HD connector + (2) SATA-III connectors
	Controller	Intel C741
	Speed	6Gb/s
	RAID	RAID 0/1/10/5 (Intel RSTe)
Storage NVMe	Connector (M.2)	(1) 2280 (by PCIe 4 interface)
	Connector (U.2)	(1) MCIO x8
Storage (Optional)	VROC Support	Yes
Graphic VGA	Connector type	D-Sub 15-pin
	Resolution	Up to 1920x1200 @60Hz
	Chipset	Aspeed AST2600
Input /Output	USB	(1) USB2.0 port (Type-A) / (1) USB3.2 Gen.1 header / (2) USB2.0 ports (@ rear) / (2) USB3.2 Gen.1 ports (@rear)
	COM	(1) COM port header + (1) DB-9 COM Connector (@rear)
	VGA	(1) D-Sub 15-pin VGA port (@ rear)
	RJ-45	(2) 10GbE ports + (1) GbE ports + (1) GbE dedicated for IPMI
	Front Panel	(1) 2x12-pin SSI front panel header(mini type)
	Audio	(1) 2x5-pin header / (1) 3 holes Audio Jack connector
	SATA	(1) Mini SAS-HD connector + (2) SATA-III connectors
	Power	8-pin power connectors
	Others	(1) UID button
	TPM Support	Please refer to our TPM supported list.
TPM (Optional)	Interface	SPI
System Monitoring	Chipset	Aspeed AST2600
	Fan	Total (6) 4-pin headers
	Temperature	Monitors temperature for CPU, memory & system environment
	Voltage	Monitors voltage for CPU, memory, chipset & power supply
	LED	Over temperature warning indicator / Fan & PSU fail LED indicator
	Others	Watchdog timer support
Audio	Chipset	Realtek ALC888S
	Feature	2.1 ch
Server Management	Onboard Chipset	Onboard Aspeed AST2600
	AST2600 iKVM Feature	24-bit high quality video compression / Supports storage over IP and remote platform-flash / USB 2.0 virtual hub
	AST2600 IPMI Feature	IPMI 2.0 compliant baseboard management

		controller (BMC) / 10/100/1000 Mb/s MAC interface
BIOS	Brand / ROM size	AMI / 32MB
	Feature	Hardware Monitor / Boot from USB device/PXE via LAN/Storage / User Configurable FAN PWM Duty Cycle / SMBIOS 3.3/PnP/Wake on LAN / ACPI sleeping states S0, S5
Physical Dimension	Form Factor	SSI CEB compatible
	Board Dimension	12" x 10.5" (305 x 267mm)
Regulation	FCC (SDoC)	Class B
	CE (DoC)	Class B
	RCM	Class B
	VCCI	Class B
Operating Environment	Operating Temp.	0° C ~ 40° C (32° F ~ 104° F)
	Non-operating Temp.	- 40° C ~ 70° C (-40° F ~ 158° F)
	In/Non-operating Humidity	90%, non-condensing at 35° C
RoHS	RoHS 6/6 Compliant	Yes
Operating System	OS supported list	Please refer to our AVL support lists.
Package Contains	Motherboard	(1) S5652 Motherboard
	Manual	(1) Quick Installation Guide
	I/O Shield	(1) I/O Shield
	Cable SATA	(2) SATA signal cables

1.3 Software Specifications

For the latest AST2600 User's Guide and OS (operation system) support, please visit the Tyan's Web site at <http://www.mitaccomputing.com> for the latest information

Chapter 2: Board Installation

You are now ready to install your motherboard.

How to install our products right... the first time

The first thing you should do is read this user's manual. It contains important information that will make configuration and setup much easier. Here are some precautions you should take when installing your motherboard:

- (1) Ground yourself properly before removing your motherboard from the antistatic bag. Unplug the power from your computer power supply and then touch a safely grounded object to release static charge (i.e. power supply case). For the safest conditions, MiTAC recommends wearing a static safety wrist strap.
- (2) Hold the motherboard by its edges and do not touch the bottom of the board, or flex the board in any way.
- (3) Avoid touching the motherboard components, IC chips, connectors, memory modules, and leads.
- (4) Place the motherboard on a grounded antistatic surface or on the antistatic bag that the board was shipped in.
- (5) Inspect the board for damage.

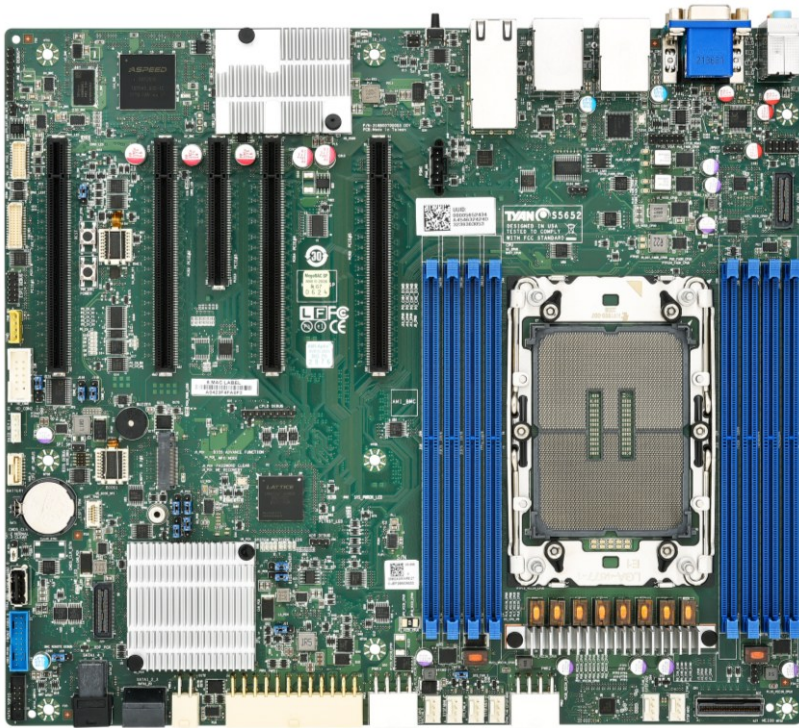
The following pages include details on how to install your motherboard into your chassis, as well as installing the processor, memory, disk drives and cables.



Caution!

1. To avoid damaging the motherboard and associated components, do not use torque force greater than **5~7kgf/cm (4.35~6.09 lb/in)** on each mounting screw for motherboard installation.
2. Do not apply power to the board if it has been damaged.

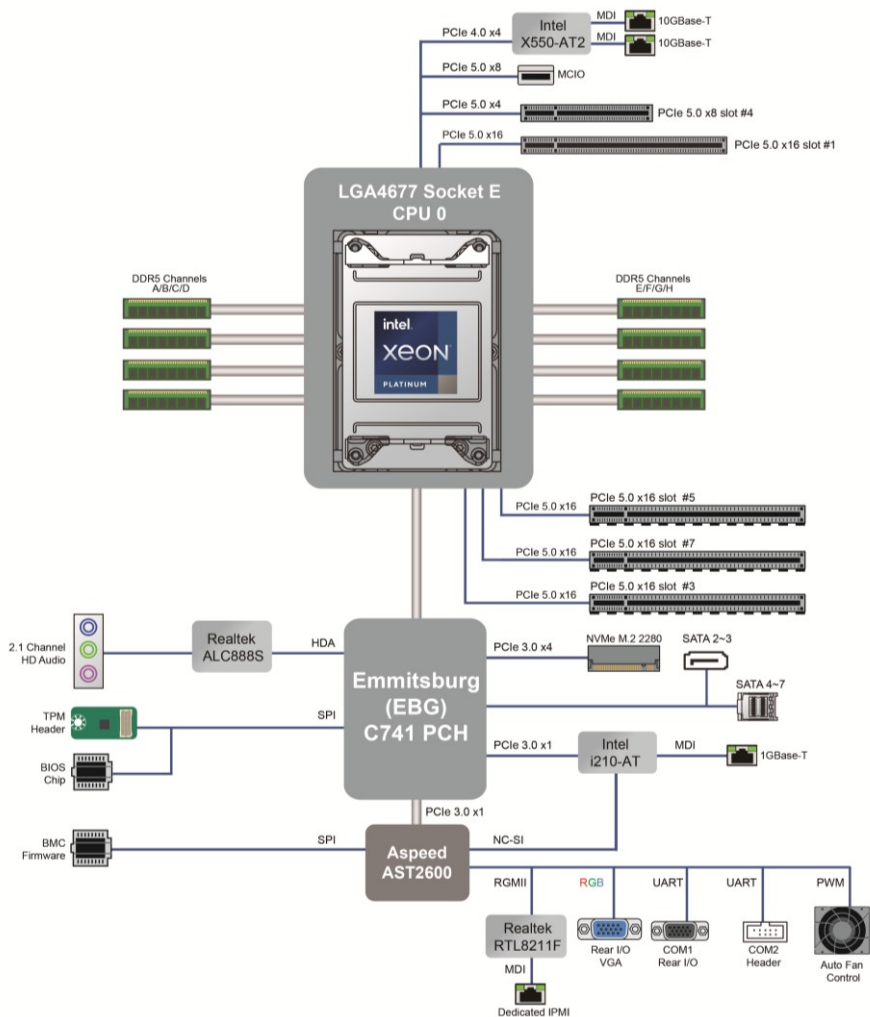
2.1 Board Image



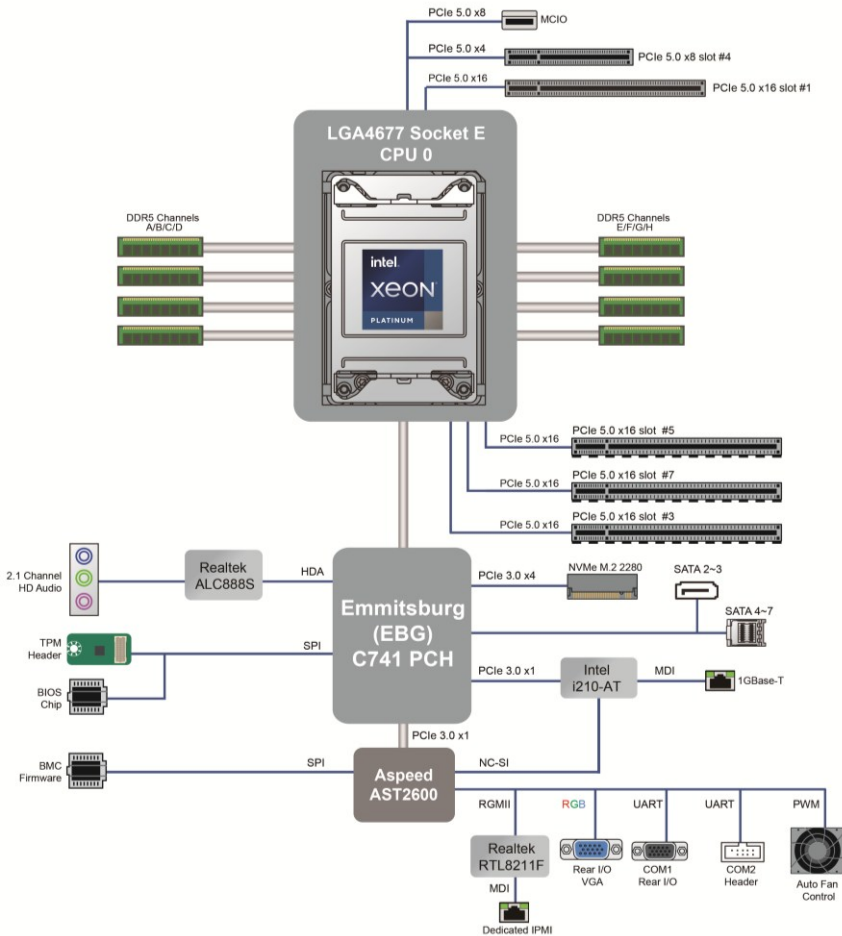
S5652AGM3NRE-2T

This picture is representative of the latest board revision available at the time of publishing. The board you receive may not look exactly like the above picture.

2.2 Block Diagram

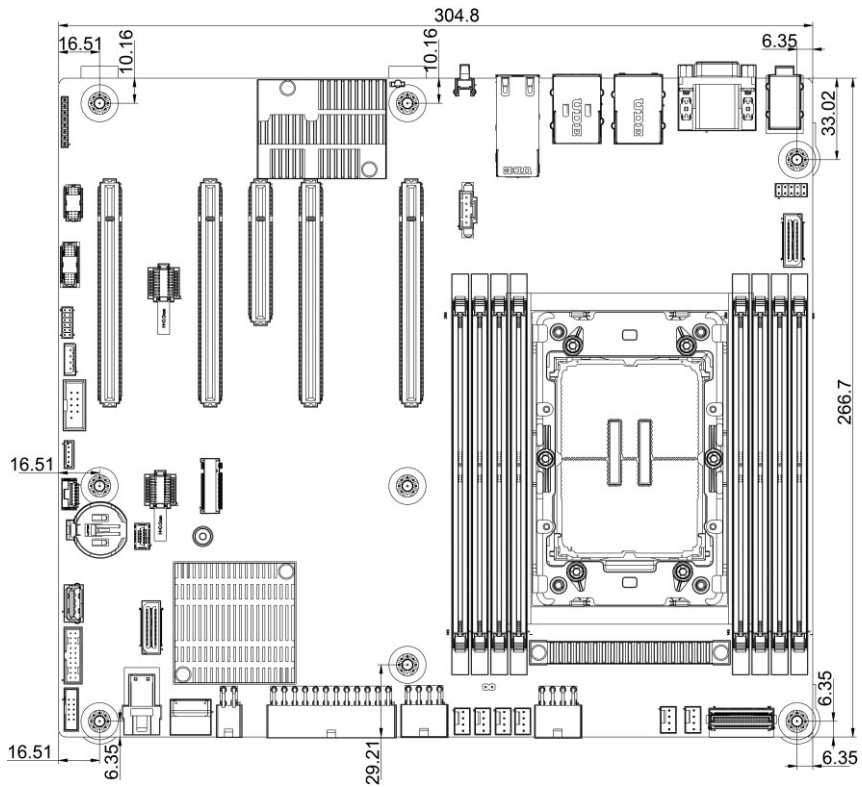


S5652AGM3NRE-2T

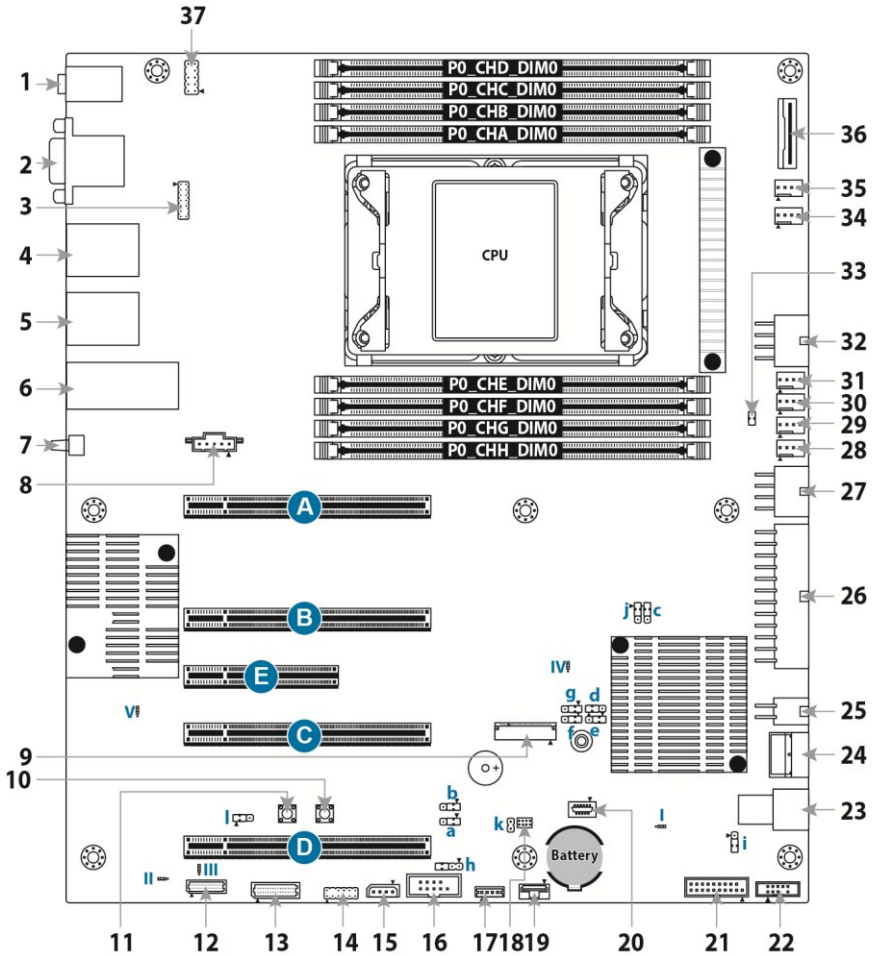


S5652AGMNRE

2.3 Motherboard Mechanical Drawing



2.4 Board Parts, Jumpers and Connectors



This diagram is representative of the latest board revision available at the time of publishing. The board you receive may not look exactly like the above diagram. The DIMM slot numbers shown above can be used as a reference when reviewing the DIMM population guidelines shown later in the manual. For the latest board revision, please visit our web site at <http://www.mitaccomputing.com>.

Motherboard Components

Connectors	
1. Audio Jack(J5)	20. SPI TPM Header (ESPI TPM1)
2. VGA+ COM PORT (VGA_COM1)	21. Front USB3.2 Gen1 Header (USB3_FPIO1)
3. VGA Header (FPIO_VGA3)	22. SGPIO Header (SATA1_SGPIO)
4. RJ45 LAN Port (LAN4)&USB2.0x2	23. SATA1-4-7
5. RJ45 LAN Port (LAN3) Dedicated IPMI &USB3.2 Gen1 x2	24. SATA1-2-3
6. RJ45 LAN Ports (LAN1&LAN2)	25. Power Connector(PWR4)
7. ID LED Button (ID BTN)	26. Power Connector(PWR1)
8. PSMI Connector (PSMI_HD1)	27. Power Connector(PWR3)
9. M.2 Socket (M.2#1)	28. 4-pin FAN Connector (SYSFAN5)
10. POWER Button (POWER)	29. 4-pin FAN Connector (SYSFAN4)
11. RESET Button (REST)	30. 4-pin FAN Connector (SYSFAN3)
12. Front Panel Connector (SSI_FP)	31. CPU0_FAN(CPUFAN1)
13. Fan Connector for BB (FAN_FP)	32. Power Connector(PWR2)
14. ESPI DEBUG Header (J4)	33. Chassis Intrusion Header(INTR)
15. IPMB Connector (IPMB_HD1)	34. 4-pin FAN Connector (SYSFAN2)
16. COM2 Header (HD_COM2)	35. 4-pin FAN Connector (SYSFAN1)
17. SATA RAID Key (RAID KEY)	36. MCIO0 Connector (MCIO0)
18. BIOS DEBUG (BIOS_DBG1)	37. Front Audio Header (J6)
19. NVMe Hot Plug Function Connector (HDR_3)	
Jumpers/ Headers	
a. COM2_RX Jumper (J118)	g. BIOS Advance Function Jumper(J5_PCH)
b. COM2_TX Jumper (J119)	h. System Buzzer Jumper (J14)
c. BIOS Recovery Jumper (J1_PCH)	i. BMC Remote Debug Jumper (J19)
d. PassWord Clear Jumper (J2_PCH)	j. CPLD setup Jumper (J7)
e. ME Recovery Jumper (J3_PCH)	k. BIOS S5 Flash Enable Jumper (J2)
f. MFG Mode Jumper (J4_PCH)	l. System Reset Mode Jumper (J136)
PCIe Slots	
A. PCI-e Gen5 x16 FH/FL (PCIe5)	D. PCI-e Gen 5 x16 FH/FL (PCIe1)
B. PCI-e Gen5 x16 FH/FL (PCIe4)	E. PCI-e Gen5 x8 FH/FL (PCIe3)
C. PCI-e Gen5 x16 FH/FL (PCIe2)	
LEDs	
i ME_LED (ME_LED)	iv PLD_HB_LED (D33)
ii HDD_LED1 (HDD_LED1)	v BMC_HB_LED (D1_BMC)
iii IPMI_LED1 (IPMI_LED)	

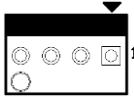
IPMB_HD1: IPMB Connector

	Signal	Pin	Pin	Signal
	IPMB_DAT	1	2	GND
	IPMB_CLK	3	4	VCC3_AUX

HD_COM2: COM2 Header

	Signal	Pin	Pin	Signal
	COM2_DCD	1	2	COM2_DSR
	COM2_RXD	3	4	COM2_RTS
	COM2_TXD	5	6	COM2_CTS
	COM2_DTR	7	8	COM2_NRI
	GND	9	10	KEY

CPUFAN1/ SYSFAN1~5: 4-pin CPU Fan Connector

	Pin	1	2	3	4
	Signal	GND	P12V	FAN_TACH	FAN_PWM
Use this header to connect the cooling fan to your motherboard to keep the system stable and reliable. Note: A 4-pin fan is required for fan support 4pin Control					

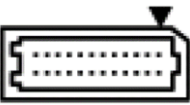
RAID KEY: SATA RAID KEY (VROC Header)

	Signal	Pin	Pin	Signal
	GND	1	2	PU_KEY_CONN_PIN2_R
	GND	3	4	FM_PCH_SATA_RAID_KEY_R

PSMI_HD1: PSMI Connector

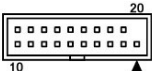
	Pin	Signal
	1	PSMI_5V_SMBCLK
	2	PSMI_5V_SMBDATA
	3	PSU_ALERT_N
	4	GND
	5	P3V3

SSI_FP: Front Panel Connector

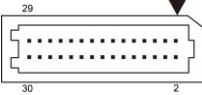
	Signal	Pin	Pin	Signal
	FP_PW_LED_PW	1	2	VCC_FPB
	NC	3	4	FP_ID_LED_PW
	FP_PW_LED_GND	5	6	FP_ID_LED_N
	HDD_LED_PW	7	8	BMC_HW_FAULT_N
	HDD_ACT_LED_N	9	10	BMC_SYS_FAULT_N
	FP_PWR_BTN_N	11	12	LAN0_LED_P
	GND	13	14	LAN0_LED_N
	FP_RST_BTN_JP_N	15	16	FP_SMB_DAT
	GND	17	18	FP_SMB_CLK
	FP_IDLE_BTN_N	19	20	FP_INTRUSION_N
	SYS_AIR_INLET	21	22	LAN1_LED_P
	FP_NMI_BTN_N	23	24	LAN1_LED_N

NOTE: Only the M.2 SSD connects the status/active LED to pins 7 and 9 of the SSI_FP connector, so HDD LED will be blinking while SSD is running I/O. In contrast, HDD LED will be off when SATA SSD or U.2 SSD is running I/O.

USB3_FPIO1: Front USB3.2 Gen1 Header

	Signal	Pin	Pin	Signal
	P5V_USB3_FRONT_HEAD	1	20	KEY
	USB3_N1_RX_FPB	2	19	P5V_USB3_FRONT_HEAD
	USB3_P1_RX_FPB	3	18	USB3_N0_RX_FPB
	GND	4	17	USB3_P0_RX_FPB
	USB3_N1_TX_FPB	5	16	GND
	USB3_P1_TX_FPB	6	15	USB3_N0_TX_FPB
	GND	7	14	USB3_P0_TX_FPB
	USB2_N1_FPB_R	8	13	GND
	USB2_P1_FPB_R	9	12	USB2_N0_FPB_R
	NC	10	11	USB2_P0_FPB_R

FAN_FP: Fan Connector (Reserved for Barebone)

	Signal	Pin	Pin	Signal
	FAN_T1	1	2	FAN_T6
	FAN_T2	3	4	FAN_T7
	FAN_T3	5	6	FAN_T8
	FAN_T4	7	8	FAN_T8
	FAN_T5	9	10	FAN_T10
	GND	11	12	GND
	PWM_FRONT3	13	14	PWM_FRONT12
	FAN_T11	15	16	FAN_SDA
	FAN_T12	17	18	FAN_SCL
	P3V3_AUX	19	20	PWM_REAR12
	P3V3_AUX	21	22	GND
	FAN_T13	23	24	FAN_T15
	FAN_T14	25	26	FAN_T16

	PWM_BB3	27	28	PWM_6
	PWM_CPU0	29	30	GND

ID BTN: Rear IDLED Button

	Signal	Pin	Pin	Signal
	FP_IDLE_BTN_N	1	2	GND

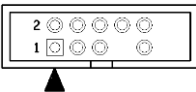
REST: Reset Button

 Normal (Default)	Pin	1	2	3	4
	Signal	FP_RST_BTN_N	FP_RST_BTN_N	GND	GND

POWER: POWER Button

 Normal (Default)	Pin	1	2	3	4
	Signal	FP_PWR_BTN_N	FP_PWR_BTN_N	GND	GND

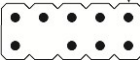
SATA1_SGPIO: SGPIO Header

	Signal	Pin	Pin	Signal
	SGIO_HDR_SM_CLK	1	2	NC
	SGIO_HDR_SM_DAT	3	4	SGPIO_SATA1_DATAOUT_R
	GND	5	6	SGPIO_SATA1_LOAD_R
	KEY	7	8	SGPIO_SATA1_CLOCK_R
	DBG_LPC3	9	10	NC

HDR_3: 7-pin NVMe Hot Plug Function Connector

	Signal	Pin	Pin	Signal
	VCC3_AUX	1	2	HP0_SCK
	HP0_SDA	3	4	CPU01_SMBALERT_N_C
	NC	5	6	NC
	VCC3	7		

J6: Front Audio Header

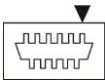
	Signal	Pin	Pin	Signal
	MIC2-L_R	1	2	AGND_P5V
	MIC2-R_R	3	4	FP_AUD_DETECT_N
	LINE2-R_R	5	6	MIC2-JD
	FIO_SENSE	7	8	KEY

MCIO0: MCIO0 Connector

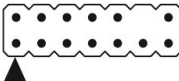

Signal Name	Pin	Pin	Signal Name
GND	A1	B1	GND
CPU0_PE4_RX_DN<7>	A2	B2	CPU0_PE4_TX_DN<7>
CPU0_PE4_RX_DP<7>	A3	B3	CPU0_PE4_TX_DP<7>
GND	A4	B4	GND
CPU0_PE4_RX_DN<6>	A5	B5	CPU0_PE4_TX_DN<6>
CPU0_PE4_RX_DP<6>	A6	B6	CPU0_PE4_TX_DP<6>
GND	A7	B7	GND
PE4_TYPEA	A8	B8	CPU0_PE4_HDD0_SCL0
WAKE_NVME_N0	A9	B9	CPU0_PE4_HDD0_SDA0
GND	A10	B10	GND
CLK_100M_DB2000_CPU0_N VME1_DP	A11	B11	RST_NVME0_CPU0_PERST_N
CLK_100M_DB2000_CPU0_N VME1_DN	A12	B12	FM_CPU0_PE4_PRSTNA_N
GND	A13	B13	GND
CPU0_PE4_RX_DN<5>	A14	B14	CPU0_PE4_TX_DN<5>
CPU0_PE4_RX_DP<5>	A15	B15	CPU0_PE4_TX_DP<5>
GND	A16	B16	GND
CPU0_PE4_RX_DN<4>	A17	B17	CPU0_PE4_TX_DN<4>
CPU0_PE4_RX_DP<4>	A18	B18	CPU0_PE4_TX_DP<4>
GND	A19	B19	GND
CPU0_PE4_RX_DN<3>	A20	B20	CPU0_PE4_TX_DN<3>
CPU0_PE4_RX_DP<3>	A21	B21	CPU0_PE4_TX_DP<3>
GND	A22	B22	GND
CPU0_PE4_RX_DN<2>	A23	B23	CPU0_PE4_TX_DN<2>
CPU0_PE4_RX_DP<2>	A24	B24	CPU0_PE4_TX_DP<2>
GND	A25	B25	GND
PE4_TYPEB	A26	B26	CPU0_PE4_HDD0_SCL1
WAKE_NVME_N1	A27	B27	CPU0_PE4_HDD0_SDA1
GND	A28	B28	GND
CLK_100M_DB2000_CPU0_N VME2_DP	A29	B29	RST_NVME1_CPU0_PERST_N
CLK_100M_DB2000_CPU0_N VME2_DN	A30	B30	FM_CPU0_PE4_PRSTNB_N
GND	A31	B31	GND
CPU0_PE4_RX_DN<1>	A32	B32	CPU0_PE4_TX_DN<1>
CPU0_PE4_RX_DP<1>	A33	B33	CPU0_PE4_TX_DP<1>
GND	A34	B34	GND
CPU0_PE4_RX_DN<0>	A35	B35	CPU0_PE4_TX_DN<0>
CPU0_PE4_RX_DP<0>	A36	B36	CPU0_PE4_TX_DP<0>

	GND	A37	B37	GND
--	-----	-----	-----	-----

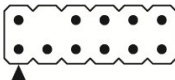
ESPI_TPM1: SPI TPM Header

	Signal	Pin	Pin	Signal
	SPI_TPM_CONN_CLK	1	7	P3V3_AUX
	RST_PLTRST_TPM_CONN_N	2	8	FM_TPM_CONN_PRSENT_R_N
	SPI_TPM_CONN_MOSI	3	9	IRQ_TPM_CONN_PIRQ_N
	SPI_TPM_CONN_MISO	4	10	P3V3
	SPI_PCH_TPM_CONN_CS_N	5	11	GND
	NC_TPM_PIN6	6		

FPIO_VGA3: VGA Header

	Signal	Pin	Pin	Signal
	GND	1	2	VGA2_5V
	GND	3	4	HD_VGA_R
	GND	5	6	HD_VGA_G
	GND	7	8	HD_VGA_B
	GND	9	10	HD_VGA_DAT
	HD_VGA_HS	11	12	KEY
	HD_VGA_CLK	13	14	HD_VGA_VS

J4: ESPI Debug Header

	Signal	Pin	Pin	Signal
	P3V3_AUX	1	2	DBG_ESPI_CS1_N
	LAD0_ESPI_DBG_IO0	3	4	KEY
	LAD1_ESPI_DBG_IO1	5	6	DBG_ESPI_RESET_N
	LAD2_ESPI_DBG_IO2	7	8	GND
	LAD3_ESPI_DBG_IO3	9	10	CLK_DBG_ESPI
	DBG_ESPI_ALERT1_N	11	12	GND

M.2#1: M.2 Socket

	Signal	Pin	Pin	Signal
	GND	1	2	P3V3
	GND	3	4	P3V3
	PERN3	5	6	NC2
	PERP3	7	8	NC3
	GND	9	10	I/O/LED
	PETN3	11	12	P3V3
	PETP3	13	14	P3V3
	GND	15	16	P3V3
	PERN2	17	18	P3V3
	PERP2	19	20	NC
	GND	21	22	NC
	PETN2	23	24	NC
	PETP2	25	26	NC
	GND	27	28	NC
	PERN1	29	30	NC
	PERP1	31	32	NC
	GND	33	34	NC
	PETN1	35	36	NC
	PETP1	37	38	NC
	GND	39	40	M2_SMB_CLK2
	PERP0/SATA+	41	42	M2_SMB_DAT2
	PERN0/SATA-	43	44	NC
	GND	45	46	NC
	PETN0/SATA-	47	48	NC
	PETP0/SATA+	49	50	M2_PERST_N
	GND	51	52	NC
	REFCLKN	53	54	NC
	REFCLKP	55	56	NC21
	GND	57	58	NC
	KEY	59	60	KEY
	KEY	61	62	KEY
	KEY	63	64	KEY
	KEY	65	66	KEY
	NC	67	68	NC
	PEDET-NC-PCIE GND-SATA	69	70	3.3V
	GND	71	72	3.3V
	GND	73	74	3.3V

	GND	75		
--	-----	----	--	--

J118: BMC COM Port Jumper (RX)

	Signal	Pin	Pin	Signal
 1 - 2	BMC_COM2_RXD	1	2	RXD_2
 2 - 3	SP_BMC_UART5_RXD	3		
	Pin1-2 closed: BMC COM PORT2 (Default) Pin2-3 closed: BMC CONSOLE PORT5			

J119: BMC COM Port Jumper (TX)

	Signal	Pin	Pin	Signal
 1 - 2	BMC_COM2_TXD	1	2	TXD_2
 2 - 3	SP_BMC_UART5_TXD	3		
	Pin1-2 closed: BMC COM PORT2 (Default) Pin2-3 closed: BMC CONSOLE PORT5			

J1_PCH: BIOS Recovery Jumper

	Signal	Pin	Pin	Signal
 1 - 2	TP_BIOS_RCVR_BOOT	1	2	FM_PCH_BIOS_RCVR_MODE
 2 - 3	PU_BIOS_RCVR_BOOT	3		
	Pin1-2 closed: Normal Mode (Default) Pin2-3 closed: Recovery BIOS			

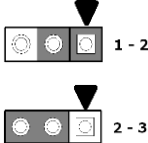
J2_PCH: Password Clear Jumper

	Signal	Pin	Pin	Signal
 1 - 2	NC	1	2	FM_PASSWORD_CLEAR_N
 2 - 3	PD_PASSWORD_CLEAR	3		
	Pin1-2 closed: Normal Mode (Default) Pin2-3 closed: PASSWORD CLEAR			

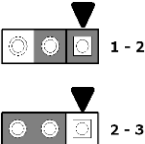
J3_PCH: ME Recovery Jumper

	Signal	Pin	Pin	Signal
 1 - 2	PU_ME_RCVR_BOOT	1	2	FM_ME_RCVR_N
 2 - 3	PD_ME_RCVR_N	3		
	Pin1-2 closed: Normal Mode (Default) Pin2-3 closed: RECOVER ME			

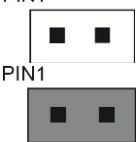
J4_PCH: MFG Mode Jumper

	Signal	Pin	Pin	Signal
	PU_MFG_MODE	1	2	FM_MFG_MODE
	PD_MFG_MODE	3		
	Pin1-2 closed: MFG DISABLE Pin2-3 closed: MFG ENABLE (Default)			

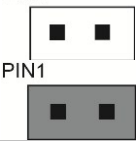
J5_PCH: BIOS Advance Function Jumper

	Signal	Pin	Pin	Signal
	PD_BIOS_ADV_FUNCT	1	2	FM_BIOS_ADV_FUNCTIONS
	PU_BIOS_ADV_FUNCT	3		
	Pin1-2 closed: NORMAL OPERATION (Default) Pin2-3 closed: MFG BIOS CORE EXECUTION TREE			

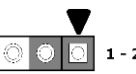
J2: BIOS S5 Flash Enable Jumper

	Signal	Pin	Pin	Signal
	P5V_AUX	1	2	SPI_SW_EN_N
	1-2: Place J2_1-2 to isolate SPI (Support BIOS SPI S5 Flash Mode)			

INTR: Chassis Intrusion Header

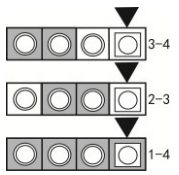
	Signal	Pin	Pin	Signal
	FP_CHASSIS_INTRUSION	1	2	GND
	1-2: Chassis Cover Is Closed (Default) Empty Chassis Cover Is Closed Removed			

J7: CPLD setup Jumper

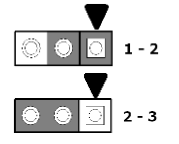
	Signal	Pin	Pin	Signal
	NC	1	2	FM_FORCE_PWRON_LVC3R
	PU_FORCE_PWRON_LVC3	3		

 2 - 3	1-2: BMC Remote debug 2-3: Disable Remote Debug (Default)
---	---

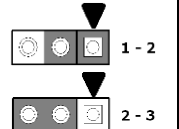
J14: System Buzzer Jumper

 3-4 2-3 1-4	Signal	Pin	Pin	Signal
	VCC5_BZ	1	2	NC
	BUZ_1	3	4	BUZ_2
Pin3-4 closed: Normal Mode (Default) Pin2-3 closed: Disable PC Beep Pin1-4 closed: Use the external speaker				

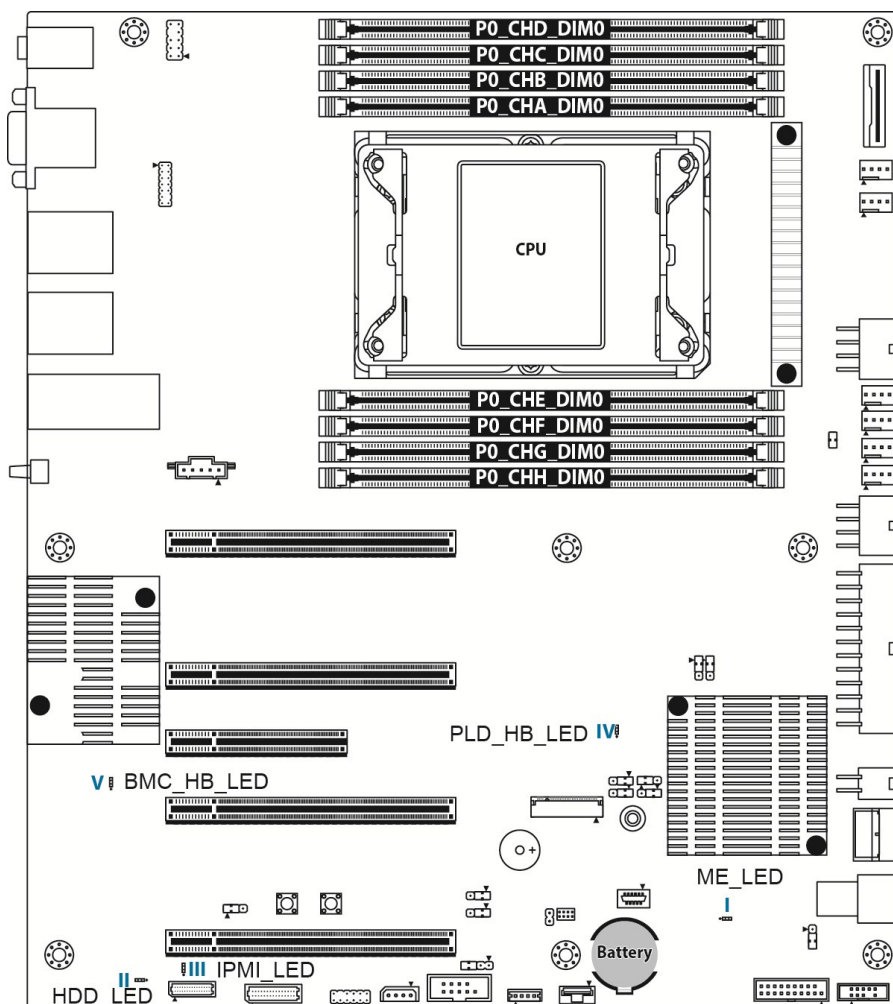
J19: BMC Remote Debug Jumper

 1 - 2 2 - 3	Signal	Pin	Pin	Signal
	P3V3_AUX	1	2	FM_REMOTE_DEBUG_EN_DET_R2
	NC	3		
1-2: Disable (Default) 2-3: Enable				

J136: System Reset Mode Jumper

 1 - 2 2 - 3	Signal	Pin	Pin	Signal
	FP_RST_BTN_N	1	2	FP_RST_BTN_JP_N
	FP_BMC_RST_BTN_N	3		
1-2: System Reset (Default) 2-3: BMC Reset				

2.5 LED Definitions



i. ME_LED	PCH ME Heartbeat LED	Pin	Signal	
		+	P3V3_AUX	
		-	ME Heartbeat LED	
		State	Description	
		OFF	OFF	ME cannot properly initiated.
ii.HDD_LED1	On board HDD active LED (SATA by SGPIO, M.2 By ACT pin, MCIO No support.)	Blinking	Green	ME is working normally
		Pin	Signal	
			P3V3	
			HDD ACT LED	
		State	Description	
iii.IPMI_LED1	On Board BMC IPMI(HW Fault) Alert LED	OFF	OFF	None
		Blinking	Blue	HDD work
		Pin	Signal	
		+	P3V3_AUX	
		-	BMC HW Fault	
iv. D33 (PLD_HB_LED)	CPLD Heartbeat LED	State	Description	
		ON	Red	IPMI (HW Fault) alert.
		Pin	Signal	
		+	P3V3_AUX	
		-	CPLD Heartbeat LED	
v. D1_BMC (MC_HB_LED)	BMC Heart beat LED	State	Description	
		OFF	OFF	CPLD cannot properly initiated.
		Blinking	Green	CPLD is working normally
		Pin	Signal	
		+	VCC3_SB	
		-	BMC Heartbeat LED	
		State	Description	
		OFF	OFF	BMC cannot properly initiated.
		Blinking	Green	BMC is working normally

2.6 Installing the Processor and Heatsink

The types of processors supported by the S5652 are listed in the [1.3 Hardware Specifications](#) on page 16. Check our website at <http://www.mitaccomputing.com> for the latest list of validated **Intel®** processors for this specific motherboard.

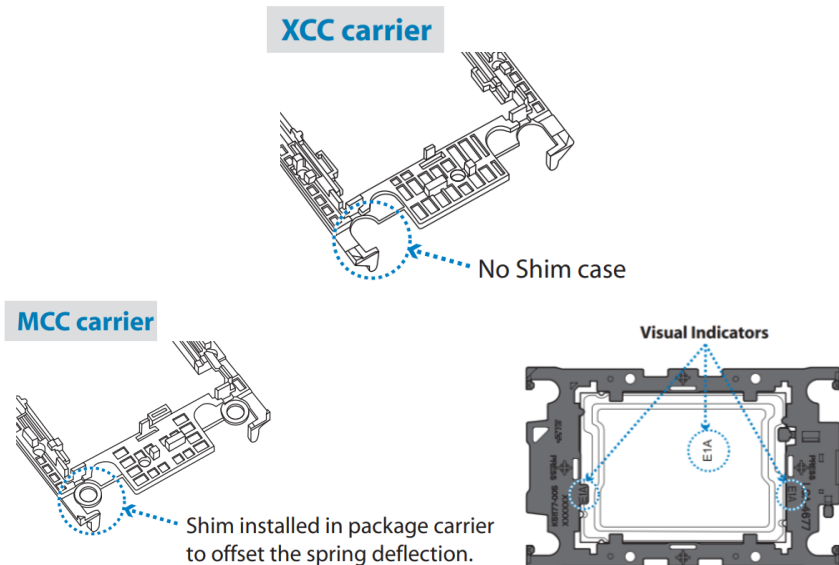
NOTE: MiTAC is not liable for damage as a result of operating an unsupported configuration.

Processor Installation (Single Socket LGA4677 for 4th Gen. Intel Xeon Scalable Processor / 5th Gen. Intel Xeon Scalable Processor)

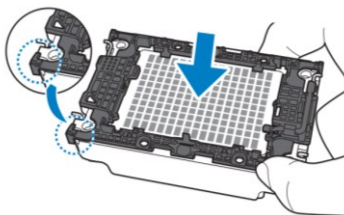
Follow the steps below to install the processors and heat sinks. Please note that the illustrations are based on LGA4677 socket which may not look exactly like the motherboard you purchased. Therefore, the illustrations should be held for your reference only.

NOTE: Please save and replace the flip CPU protection cap when returning for service.

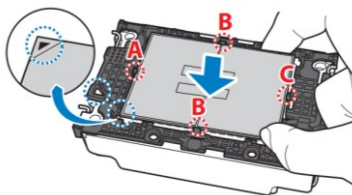
Shim concept



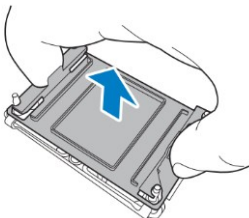
1. Align the triangle edge of the carrier with the notch on the edge of the heatsink. Then install the carrier on the bottom of the heatsink and make sure the latches are snapped under the edge of the heatsink.



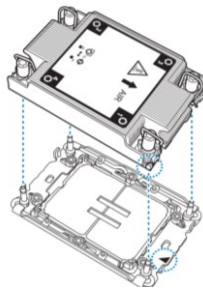
2. Align and install the processor on the carrier. Make sure the gold arrow is located in the correct direction. NOTE: When installing the processor, secure the front side (A) first, and following with the middle and rear sides (B→C).



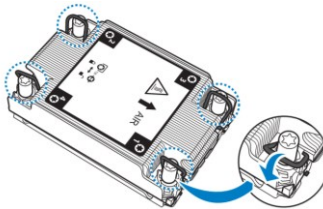
3. Remove the CPU cover.



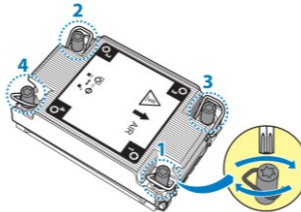
4. Carefully flip the heatsink assembly. Align the heatsink with the CPU socket by the guide pins. Make also sure that the triangle edge of the carrier is aligned correctly with the triangle mark on the CPU socket. Then place the heatsink assembly onto the top of the CPU socket.



5. Press down on the retention clips to fix the heatsink assembly to the CPU socket.

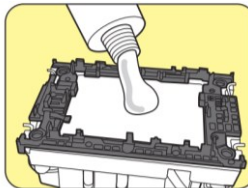


6. To secure the heatsink assembly, use a T30 Security Torx to tighten the screws in a sequential order (1→2→3→4). NOTE: When disassembling the heatsink, loosen the screws in reverse order (4→3→2→1).

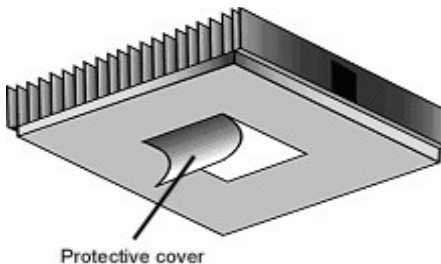


NOTE: A new heatsink comes with pre-applied thermal grease.

Once the heatsink has been removed from the processor, you need to clean the processor and heatsink using an alcohol solvent. Then apply new thermal grease before reinstalling the heatsink.

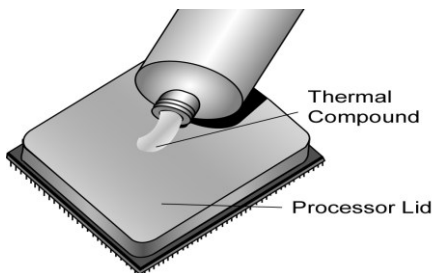


2.7 Thermal Interface Material



There are two types of thermal interface materials designed for use with the processors.

The most common material comes as a small pad attached to the heat sink at the time of purchase. There should be a protective cover over the material. Take care not to touch this material. Simply remove the protective cover and place the heat sink on the processor.

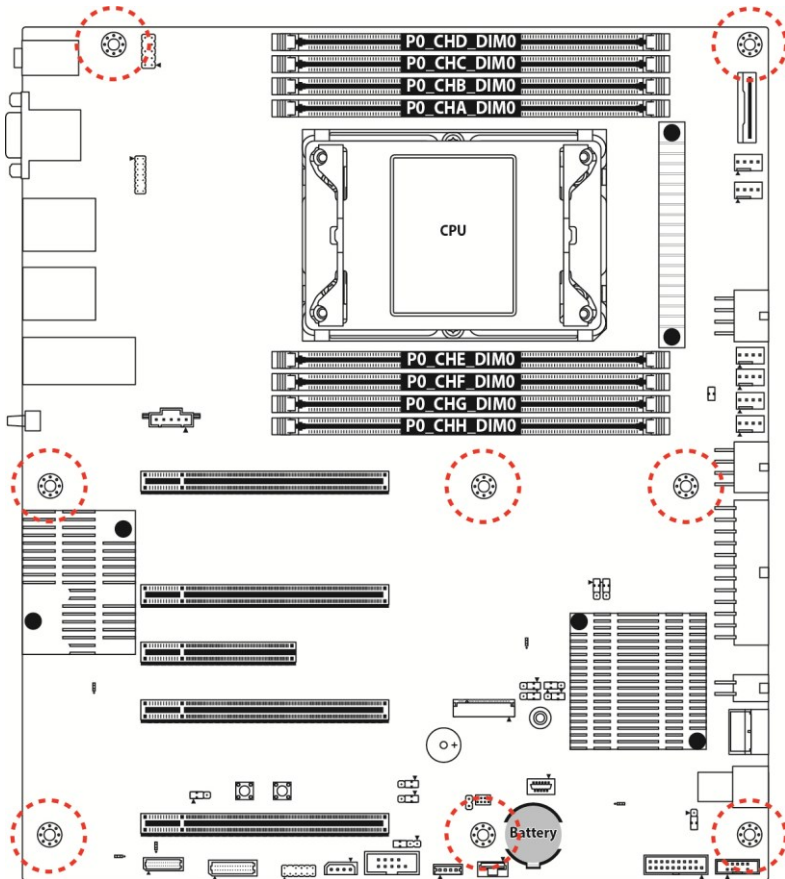


The second type of interface material is usually packaged separately. It is commonly referred to as 'thermal compound'. Simply apply a thin layer on to the CPU lid (applying too much will actually reduce the cooling).

NOTE: Always check with the manufacturer of the heat sink & processor to ensure that the thermal interface material is compatible with the processor and meets the manufacturer's warranty requirements.

2.8 Tips on Installing Motherboard in Chassis

Before installing your motherboard, make sure your chassis has the necessary motherboard support studs installed. These studs are usually metal and are gold in color. Usually, the chassis manufacturer will pre-install the support studs. If you are unsure of stud placement, simply lay the motherboard inside the chassis and align the screw holes of the motherboard to the studs inside the case. If there are any studs missing, you will know right away since the motherboard will not be able to be securely installed.

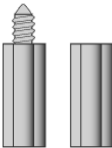
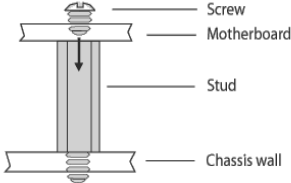
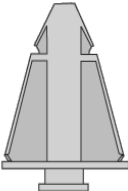
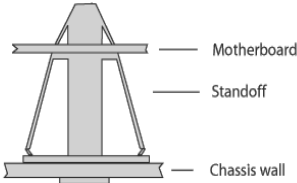
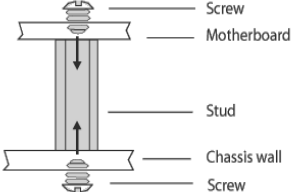
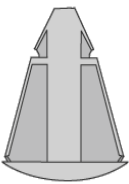
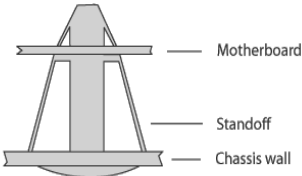
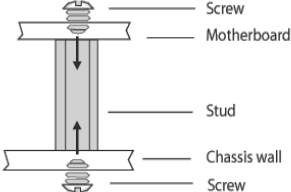


Note: Be especially careful to look for extra stand-offs. If there are any stand-offs present that are not aligned with a mounting hole on the motherboard, it will likely short components on the back of the motherboard when installed. This will cause malfunction and/or damage to your motherboard.

Some chassis include plastic studs instead of metal. Although the plastic studs are usable, MiTAC recommends using metal studs with screws that will fasten the motherboard more securely in place.

Below is a chart detailing what the most common motherboard studs look like and how they should be installed.

Mounting the Motherboard

Type	Solutions for installing	
		
		
		

2.9 Installing the Memory

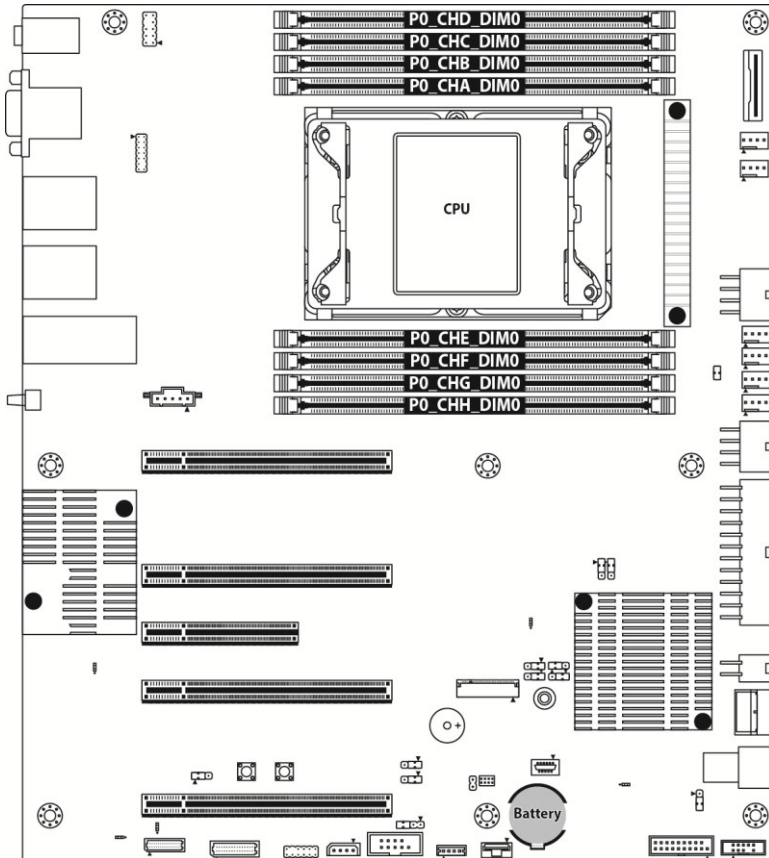
Before installing memory, ensure that the memory you have is compatible with the motherboard and processor. Check the TYAN Web site at <http://www.mitacomputing.com> for details of the type of memory recommended for your motherboard.

Processor level & features

8xxxx(Platinum)	6xxxx(Gold)	5xxxx(Gold)
•2S Scalability*^s •4 UPI @16GT/s* •8-ch DDR5@4800 1DPC and 4400 2DPC •Intel® Optane Persistent Memory Module •80 lanes PCIe 5.0/CXL •Intel® Turbo Boost •Intel® Hyper-Threading •Intel®AVX-512(2FMAs) •Advanced RAS	•2S Scalability*^s •3UPI@16GT/s* •8-ch DDR5 @4800 •1DPC and 4400 2DPC •Intel® Optane Persistent Memory Module •80 lanes PCIe 5.0/CXL •Intel® Turbo Boost •Intel® Hyper-Threading •Intel®AVX-512(2FMAs) •Advanced RAS	•2S Scalability*^s •3UPI@16GT/s* •8-ch DDR5 @4400 1DPC/2DPC •Intel® Optane Persistent Memory Module* •80 lanes PCIe 5.0/CXL •Intel® Turbo Boost •Intel® Hyper-Threading •Intel®AVX-512(2FMAs) •Advanced RAS
4xxxx(Silver)	3xxxx(Bronze)	
•2S Scalability*^s •3UPI@16GT/s* •DDR5 @4400 •1DPC/2DPC •80 lanes PCIe 5.0/CXL •Intel® Turbo Boost •Intel® Hyper-Threading •Intel®AVX-512(2FMAs) •Standard RAS	•1S Scalability •DDR5 @4000 •1DPC/2DPC •80 lanes PCIe 4.0 •Intel®AVX-512(1 FMA) •Standard RAS	

Type	Ranks Per DIMM and Data Width	DIMM Capacity(GB)	Speed (MT/s); Voltage(V); DIMM Per Channel (DPC)	
			1DPC*	2DPC
		16Gb	1.1V	
RDIMM	SRx8(RC D)	16Gb	4800	4400
	SRx4(RC C)	32Gb		
	SRx4(RC F) 9x4	32Gb		
	DRx8 (RC E)	32Gb		
	DRx4 (RC A)	64Gb		
	DRx4 (RC B) 9x4	64Gb		
RDIMM-3DS	(4R/8R)x4	2H-128 GB		
	(RC A)	4H- 256GB		

DIMM Location



- (8) DDR5 DIMM slots supports
- (1) DIMM slots per channel
- (8) memory channels per CPU
- DDR5 4800 MHz (1DPC) / 4400MHz (2DPC) - 4th Gen. / DDR5 5600 MHz (1DPC) / 4400MHz (2DPC) - 5th Gen.
- All installed memory will be automatically detected. No jumpers or settings need to be changed for memory detection.
- All memory must be of the same type and density. **Different memory types can NOT be mixed and matched on the same motherboard.**

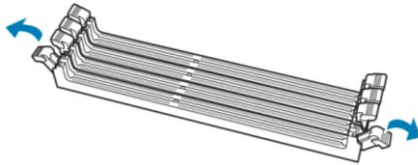
Recommended Memory Population Table

DDR5	Quantity of memory installed											
	1DDRS			2DDRS		4DDRS	6DDRS				8DDRS	
1 DIMM at DIMM A0	✓				✓		✓	✓	✓		✓	✓
1 DIMM at DIMM B0		✓						✓	✓	✓	✓	✓
1 DIMM at DIMM C1					✓	✓	✓	✓	✓	✓	✓	✓
1 DIMM at DIMM D0							✓		✓			✓
1 DIMM at DIMM E0			✓		✓	✓	✓	✓	✓			✓
1 DIMM at DIMM F0				✓			✓		✓	✓	✓	✓
1 DIMM at DIMM G1					✓		✓	✓	✓		✓	✓
1 DIMM at DIMM H0								✓	✓	✓	✓	✓

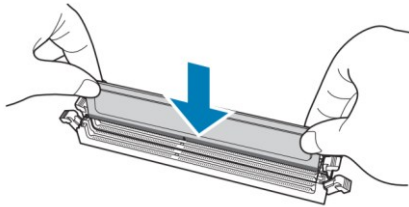
Memory Installation Procedure

Follow these instructions to install memory modules into the S5652.

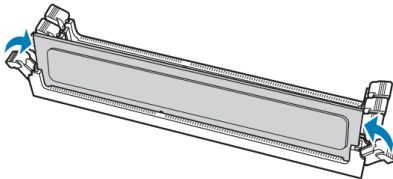
1. Unlock a DIMM socket by Press the retaining clip outwardly in the following illustration.



2. Align the memory module with the socket, such that the DIMM NOTCH match the KEY SLOT on the socket.



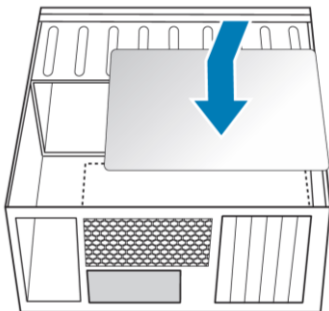
3. Seat the module firmly into the socket by gently pressing down until it sits flush with the socket. The locking levers pop up into place.



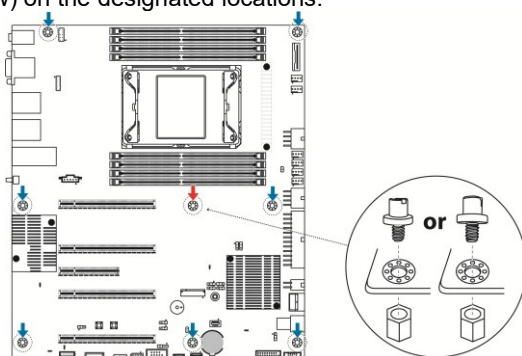
2.10 Installing the M.2 standoff and M.2 Card

Follow these instructions to install standoff onto the S5652.

1. Insert the server board into the chassis.



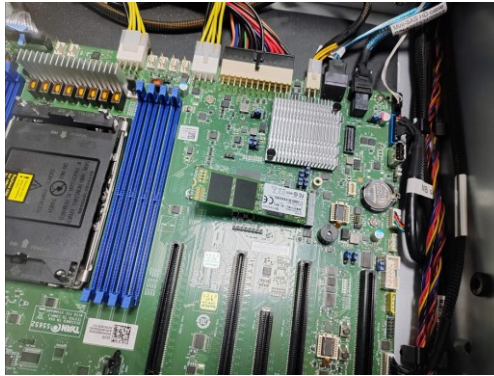
2. Attach the server board to the chassis by securing the standoff (marked with the red arrow) on the designated locations.



NOTE: The standoff depends on the chassis type.



3. Insert appropriate M.2 card into the slot.



4. Use one M.2 screw to secure the M.2 Card.



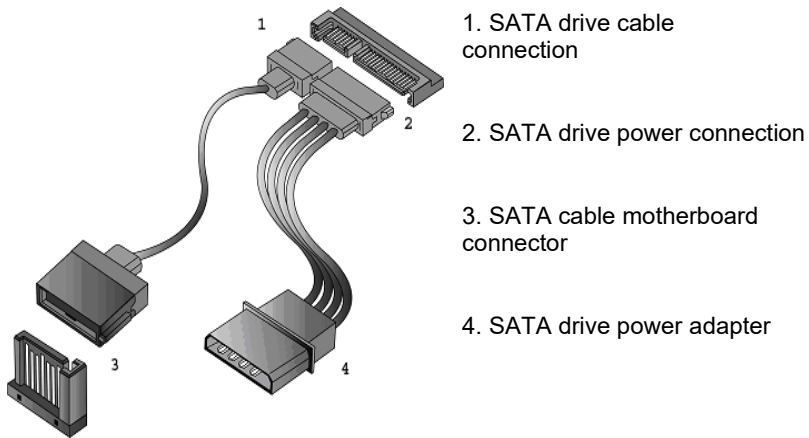
2.11 Attaching Drive Cables

Attaching SATA Cables

S5652 is equipped with **two (2)** Serial ATA (SATA) channel. Connections for the drives are very simple.

There is no need to set Master/Slave jumpers on SATA drives. If you are in need of SATA/SAS cables or power adapters please contact your place of purchase.

The following pictures illustrate how to connect an SATA drive.



2.12 Installing Add-In Cards

Before installing add-in cards, it's helpful to know if they are fully compatible with your motherboard. For this reason, we've provided the diagrams below, showing the slots that may appear on your motherboard.

Slot	Support spec	Card install notes
	Standard PCIe x16 slot FH/FL, support PCIe Gen5 16 lanes (PCIe#5)	(IOU2, Port 3A)
	Standard PCIe x16 slot FH/FL, support PCIe Gen5 16 lanes (PCIe#4)	Double wide FH/FL GPGPU Limit (IOU1, Port 2A)
	Standard PCIe x8 slot FH/FL, support PCIe Gen5 8 lanes (PCIe#3)	(IOU4, Port 5G)
	Standard PCIe x16 slot FH/FL, support PCIe Gen5 16 lanes (PCIe#2)	Double wide FH/FL GPGPU Limit (IOU0, Port 1A)
	Standard PCIe x8 slot FH/FL, support PCIe Gen5 16 lanes(PCIe#1)	(IOU3, Port 4A)

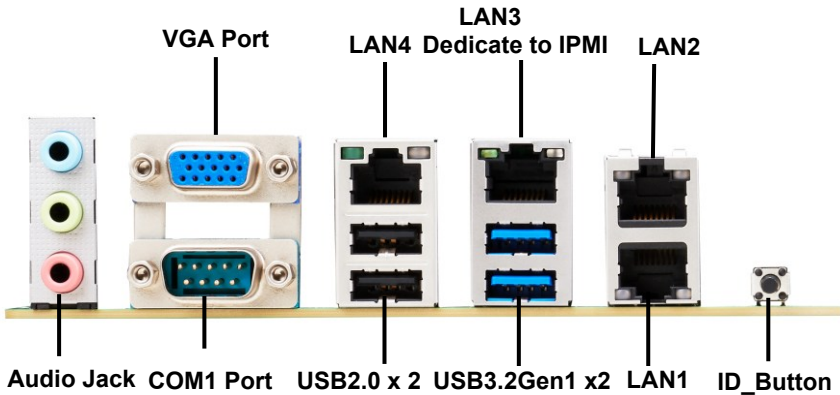
Simply find the appropriate slot for your add-in card and insert the card firmly. Do not force any add-in cards into any slots if they do not seat in place. It is better to try another slot or return the faulty card rather than damaging both the motherboard and the add-in card.

TIP: It's a good practice to install add-in cards in a staggered manner rather than making them directly adjacent to each other. Doing so allows air to circulate within the chassis more easily, thus improving cooling for all installed devices.

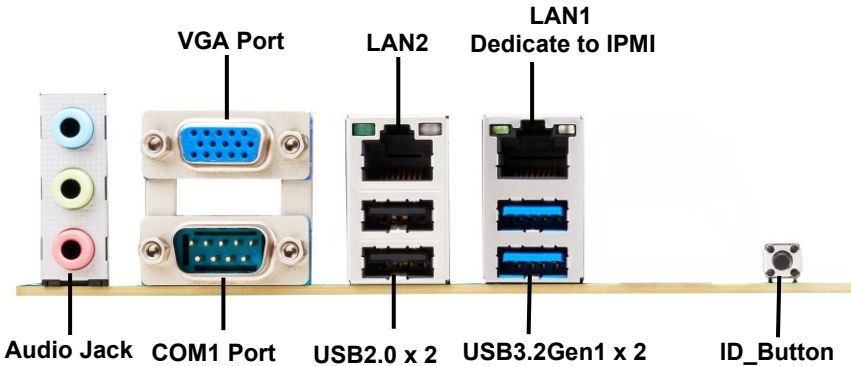
NOTE: You must always unplug the power connector from the motherboard before performing system hardware changes to avoid damaging the board or expansion device.

2.13 Connecting External Devices

Connecting external devices to the motherboard is an easy task. The motherboard supports a number of different interfaces through connecting peripherals. See the following diagrams for the details.



S5652AGM3NRE-2T



S5652AGMNRE

Onboard LAN LED Color Definition

he **four (4)** onboard Ethernet ports have green and Amber LEDs to indicate LAN status. The chart below illustrates the different LED states.

I210 10 Mbps /100 Mbps /1Gbps Link/Activity LED Scheme			
		Left LED	Right LED
No Link		OFF	OFF
10 Mbps	Link	Green Solid On	OFF
	Active	Green Blinking	OFF
100 Mbps	Link	Green Solid On	Green Solid On
	Active	Green Blinking	Green Solid On
1Gbps	Link	Green Solid On	Amber Solid On
	Active	Green Blinking	Amber Solid On

X550 100 Mbps /1000 Mbps /10Gbps LAN Link/Activity LED Scheme			
		Left LED (Link/Activity)	Right LED (Speed)
No Link		OFF	OFF
100 Mbps	Link	Solid Green	Solid Green
	Active	Blinking Green	Solid Green
1000 Mbps	Link	Solid Green	Solid Yellow
	Active	Blinking Green	Solid Yellow
(10Gbps)	Link	Solid Yellow	Solid Yellow
	Active	Blinking Yellow	Solid Yellow

S5652AGM3NRE-2T

- (2) 10GbE LAN from Intel X550 (LAN1, LAN2)
- (1) 1GbE LAN from Intel I210 (LAN4)
- (1) IPMI port from Realtek RTL8211F for server management (LAN3).

S5652AGMNRE

- (1) 1GbE LAN from Intel I210 (LAN2)
- (1) IPMI port from Realtek RTL8211F for server management (LAN1).

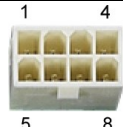
2.14 Installing the Power Supply

There are **Four (4)** power connectors on your S5652 motherboard. The S5652 supports EPS 12V power supply.

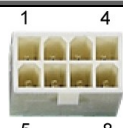
PWR1: ATX 24-Pin Power Connector

	Signal	Pin	Pin	Signal
	P3V3	1	13	P3V3
	P3V3	2	14	NC
	GND	3	15	GND
	P5V	4	16	FM_PS_EN_PSU_N
	GND	5	17	GND
	P5V	6	18	GND
	GND	7	19	GND
	PWRGD_PS_PWROK	8	20	NC
	P5V_STBY_PSU	9	21	GND
	P12V_IN	10	22	P5V
	P12V_IN	11	23	P5V
	P3V3	12	24	P5V

PWR2: 8-pin CPU Power Connector

	Signal	Pin	Pin	Signal
	GND	1	5	VCC12_P0_CPU
	GND	2	6	VCC12_P0_CPU
	GND	3	7	VCC12_P0_CPU
	GND	4	8	VCC12_P0_CPU

PWR3: 8-pin DIMM/PCIE Power Connector

	Signal	Pin	Pin	Signal
	GND	1	5	DIMM_12V_IN
	GND	2	6	DIMM_12V_IN
	GND	3	7	P12V_4
	GND	4	8	P12V_4

PWR4: 4-pin PCIE Power Connector

	Signal	Pin	Pin	Signal
	GND	1	3	P12V_IN
	GND	2	4	P12V_IN

2.15 Finishing Up

Congratulations on making it this far! You have finished setting up the hardware aspect of your computer. Before closing up your chassis, make sure that all cables and wires are connected properly, especially SATA cables and most importantly, jumpers. You may have difficulty powering on your system if the motherboard jumpers are not set correctly.

In the rare circumstance that you have experienced difficulty, you can find help by asking your vendor for assistance. If they are not available for assistance, please find setup information and documentation online at our website or by calling your vendor's support line.

Chapter 3: BIOS Setup

3.1 About the BIOS

The BIOS is the basic input/output system, the firmware on the motherboard that enables your hardware to interface with your software. The BIOS determines what a computer can do without accessing programs from a disk. The BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. This chapter describes the various BIOS settings that can be used to configure your system.

The BIOS section of this manual is subject to change without notice and is provided for reference purposes only. The settings and configurations of the BIOS are current at the time of print and are subject to change, and therefore may not match exactly what is displayed on screen.

This section describes the BIOS setup program. The setup program lets you modify basic configuration settings. The settings are then stored in a dedicated, battery-backed memory (called NVRAM) that retains the information even when the power is turned off.

To start the BIOS setup utility:

1. Turn on or reboot your system.
2. Press **<F2>** or **<Del>** during POST (**<Tab>** on remote console) to start the BIOS setup utility.

3.1.1 Setup Basics

The table below shows how to navigate in the setup program using the keyboard.

Key	Function
↑ ↓ → ←	Move cursor
<Enter>	Execute command or select submenu
<->/<+>	Select the previous or next value/setting of the field
<ESC>	Exit current menu
<F1>	General help
<F2>	Previous values
<F3>	Load the Optimal default configuration values of the menu
<F4>	Save and exit
<K>	Scroll help area upwards
<M>	Scroll help area downwards
<PgUp> / <PgDn>	Move cursor to next/previous page

3.1.2 Getting Help

Pressing [**F1**] will display a small help window that describes the appropriate keys to use and the possible selections for the highlighted item. To exit the Help Window, press [**ESC**] or the [**Enter**] key again.

3.1.3 In Case of Problems

If you have trouble booting your computer after making and saving the changes with the BIOS setup program, you can restart the computer by holding the power button down until the computer shuts off (usually within 4 seconds); resetting by pressing CTRL-ALT-DEL; or clearing the CMOS.

The best advice is to only alter settings that you thoroughly understand. In particular, do not change settings in the Chipset section unless you are absolutely sure of what you are doing. The Chipset defaults have been carefully chosen either by MiTAC or your system manufacturer for best performance and reliability. Even a seemingly small change to the Chipset setup options may cause the system to become unstable or unusable.

3.1.4 Setup Variations

Not all systems have the same BIOS setup layout or options. While the basic look and function of the BIOS setup remains more or less the same for most systems, the appearance of your Setup screen may differ from the charts shown in this section. Each system design and chipset combination requires a custom configuration. In addition, the final appearance of the Setup program depends on the system designer. Your system designer may decide that certain items should not be available for user configuration, and remove them from the BIOS setup program.

NOTE: The following pages provide the details of BIOS menu. Please be aware that the BIOS menus are continually changing due to continual BIOS updates over the product lifespan of the motherboard. The BIOS menus provided are current as of the date when this manual was written. Please visit TYAN's website at <http://www.mitaccomputing.com> for information on BIOS updates available for this specific motherboard.

3.2 Main Menu

In this section, you can alter general features such as the date and time.
Note that the options listed below are for options that can directly be changed within the Main Setup screen.



BIOS Information

It displays BIOS related information.

Product Name

It displays Product information.

BIOS Version

It displays BIOS version information

Build Date and Time

It displays the time when built

Access Level

Administrator

Platform Information

It displays the processor and PCH information

Memory Information

Total Memory

It displays the total memory size.

Memory Frequency

It displays Memory frequency

System Language

Choose the system default language.

English / Simplified Chinese / Japanese

System Date

Set the Date. Use Tab to switch between Date elements. Default Ranges:

Year: 1998-9999

Months: 1-12

Days: dependent on month

Range of Years may vary

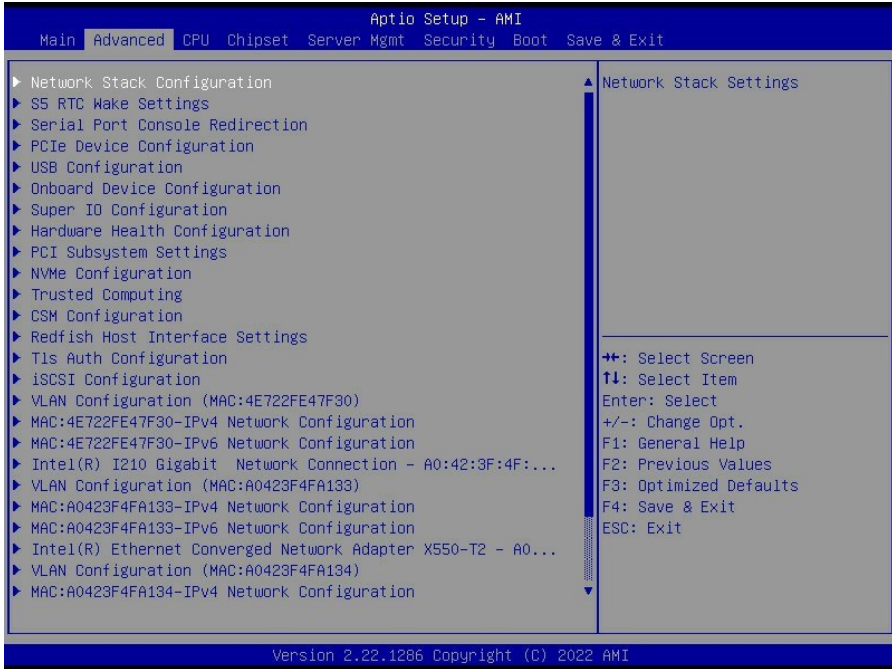
System Time

Adjust the system clock.

HH (24 hours format): MM (Minutes): SS (Seconds)

3.3 Advanced Menu

This section facilitates configuring advanced BIOS options for your system.



NOTE: This is a sample screenshot of the Advanced Menu. The HII network drivers displayed here depend on the card(s) you installed and the functions you enabled.

Network Stack Configuration

Network Stack Settings

S5 RTC Wake Settings

Enable system to wake from S5 using RTC alarm

Serial Port Console Redirection

Serial Port Console Redirection

PCIe Device Configuration

Onboard PCIe Slot Configuration

USB Configuration

USB Configuration Parameters

Onboard Device Configuration

Onboard Device and Function Configuration.

Super IO Configuration

System Super IO Chip Parameters.

Hardware Health Configuration

Hardware Health Configuration

PCI Subsystem Settings

PCI, PCI-X and PCI Express Settings

NVMe Configuration

NVMe Device information

Trusted Computing

Trusted Computing settings.

CSM Configuration

CSM Configuration, Enable/Disable Option ROM execution setting, etc

Redfish Host Interface Settings

Redfish Host Interface Parameters

Tls Auth Configuration

Press<Enter> to select Tls Auth configuration.

iSCSI Configuration

Configure the iSCSI parameters

VLAN Configuration(MAC: 4E722FE47F30)

VLAN Configuration(MAC: 4E722FE47F30)

MAC: 4E722FE47F30-IPv4 Network Configuration

Configure IPv4 network parameters.(MAC: 4E722FE47F30)

MAC: 4E722FE47F30-IPv6 Network Configuration

Configure IPv6 network parameters.(MAC: 4E722FE47F30)

Intel ® I210 Gigabit Network Connection

Configure Gigabit Ethernet device parameters.

VLAN Configuration (MAC:A0423F4FA133)

VLAN Configuration (MAC:A0423F4FA133)

MAC: A0423F4FA133-IPv4 Network Configuration

Configure IPv4 network parameters.(MAC: A0423F4FA133)

MAC: A0423F4FA133-IPv6 Network Configuration

Configure IPv6 network parameters.(MAC: A0423F4FA133)

Intel® Ethernet Converged Network Adapter X550-T2-A0

Configure 10 Gigabit Ethernet device parameters.

VLAN Configuration (MAC:A0423F4FA134)

VLAN Configuration MAC:A0423F4FA134

MAC: A0423F4FA134-IPv4 Network Configuration

Configure IPv4 network parameters.(MAC: A0423F4FA134)

MAC: A0423F4FA134-IPv6 Network Configuration

Configure IPv6 network parameters.(MAC: A0423F4FA134)

Intel® Ethernet Converged Network Adapter X550-T2-A0

Configure 10 Gigabit Ethernet device parameters.

VLAN Configuration (MAC:A0423F4FA135)

VLAN Configuration MAC:A0423F4FA135

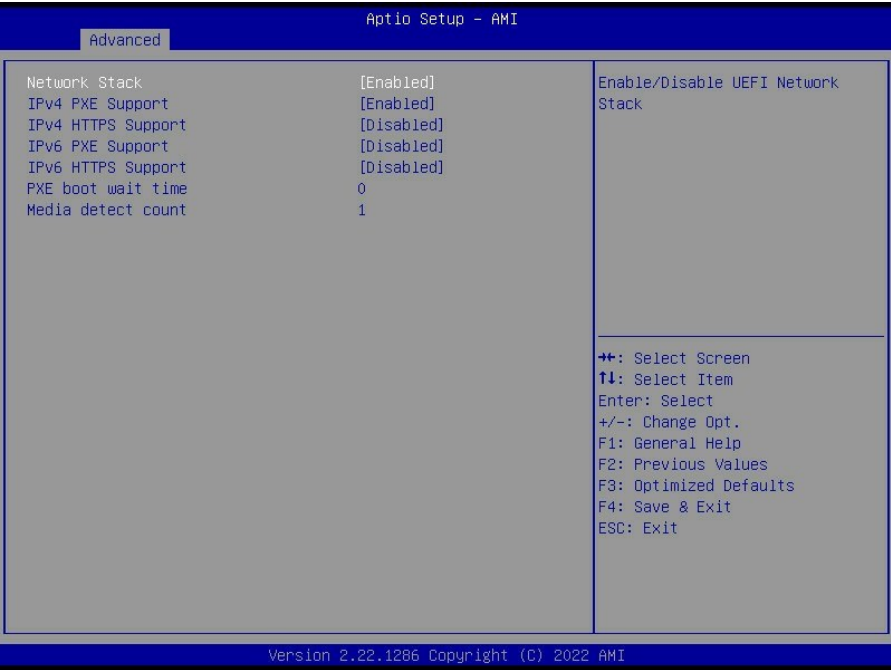
MAC: A0423F4FA135-IPv4 Network Configuration

Configure IPv4 network parameters.(MAC: A0423F4FA135)

MAC: A0423F4FA135-IPv6 Network Configuration

Configure IPv6 network parameters.(MAC: A0423F4FA135)

3.3.1 Network Stack Configuration



Network Stack

Enable/Disable UEFI Network Stack

Disabled / **Enabled**

NOTE: When Network Stack was set to **Enabled**, the following item will appear.

IPv4 PXE Support.

Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

Disabled / **Enabled**

IPv4 HTTPs Support

Enable/Disable IPv4 HTTPs boot support. If disabled, IPv4 HTTPs boot support will not be available.

Disabled / Enabled

IPv6 PXE Support

Enable/Disable IPv6 HTTPs boot support. If disabled, IPv6 HTTPs boot support will not be available.

Disabled / Enabled

IPv6 HTTPs Support

Enable/Disable IPv6 HTTPs boot support. If disabled, IPv6 HTTPS boot support will not be available.

Disabled / Enabled

PXE boot wait time

Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.

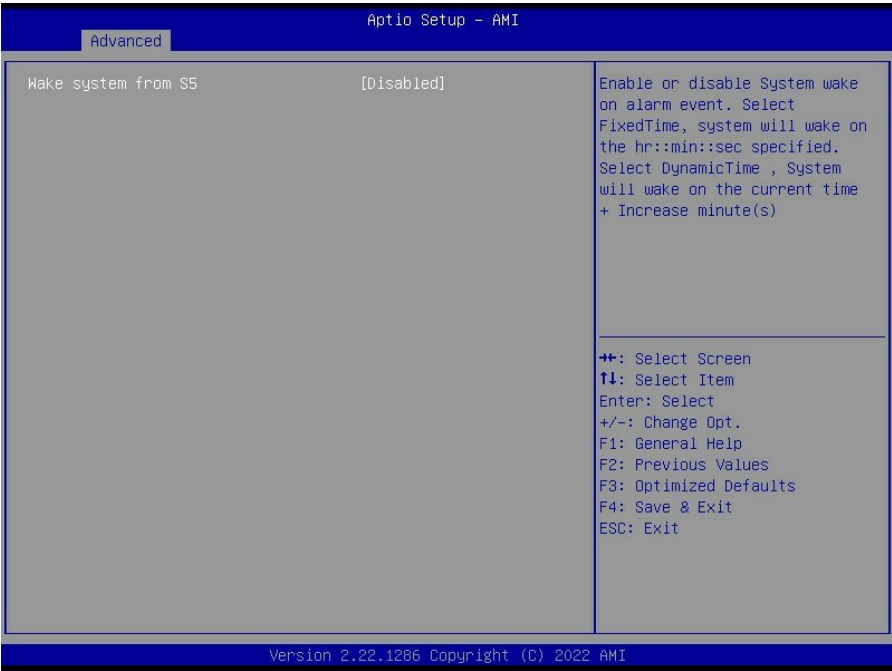
0

Media detect count

Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

1

3.3.2 S5 RTC Wake Settings



Wake system from S5

Enable or disable System wake on alarm event. Select Fixed Time, system will wake on the hr::min::sec specified. Select dynamic Time, system will wake on the current time+ increase minute(s)

Disabled / Fixed Time / Dynamic Time

3.3.3 Serial Port Console Redirection



COM1/COM2

Console Redirection

Console redirection enable or disable.

Disabled / Enabled

Legacy Console Redirection

Legacy Console Redirection Settings

Serial Port for Out-Of-Band Management/Windows Emergency Services (EMS)

Console Redirection

Console redirection enable or disable.

Disabled / Enabled

Console Redirection Settings

The settings specify how the host computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

NOTE: Console Redirection Settings menu only be available to set up when Console Redirection was set to [Enabled].

3.3.3.1 COM1 Console Redirection Settings

Aptio Setup - AMI	
Advanced	
COM1 Console Redirection Settings	
Terminal Type	[VT100+]
Bits per second	[115200]
Data Bits	[8]
Parity	[None]
Stop Bits	[1]
Flow Control	[None]
VT-UTF8 Combo Key Support	[Enabled]
Recorder Mode	[Disabled]
Resolution 100x31	[Enabled]
Putty KeyPad	[VT100]
Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.	
++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1286 Copyright (C) 2022 AMI	

Terminal Type

Emulation: ANSI: Extended ASCII char set.

VT100: ASCII char set.

VT100+: Extends VT100 to support color function keys, etc.

VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.

VT100 / **VT100+** / VT-UTF8 / ANSI

Bits per Second

Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

9600 / 19200 / 38400 / 57600 / **115200**

Data Bits

8 / 7

Parity

A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if the num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space parity do not allow for error detection.

None / Even / Odd / Mark / Space

Stop Bits

Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.

1 / 2

Flow Control

Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signal.

None / Hardware RTS/CTS

VT-UTF8 Combo Key Support

Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.

Enabled / Disabled

Recorder Mode

With this mode enabled only text will be sent. This is to capture Terminal data.

Disabled / Enabled

Resolution 100x31

Enable or disable extended terminal resolution.

Disabled / **Enabled**

Putty KeyPad

Select FunctionKey and KeyPad on Putty.

VT100 / LINUX / XTERMR6 / SCO / ESCN / VT400

3.3.3.2 COM2 Console Redirection Settings

Aptio Setup - AMI	
Advanced	
COM2	
Console Redirection Settings	
Terminal Type	[VT100+]
Bits per second	[115200]
Data Bits	[8]
Parity	[None]
Stop Bits	[1]
Flow Control	[None]
VT-UTF8 Combo Key Support	[Enabled]
Recorder Mode	[Disabled]
Resolution 100x31	[Enabled]
Putty KeyPad	[VT100]
Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.	
++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Version 2.22.1285 Copyright (C) 2022 AMI

Terminal Type

Emulation: ANSI: Extended ASCII char set.

VT100: ASCII char set.

VT100+: Extends VT100 to support color function keys, etc.

VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.

VT100 / **VT100+** / VT-UTF8 / ANSI

Bits per Second

Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

9600 / 19200 / 38400 / 57600 / **115200**

Data Bits

8 / 7

Parity

A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if the num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: parity bit is always 0. Mark and Space parity do not allow for error detection.

None / Even / Odd / Mark / Space

Stop Bits

Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.

1 / 2

Flow Control

Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

None / Hardware RTS/CTS

VT-UTF8 Combo Key Support

Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.

Enabled / Disabled

Recorder Mode

With this mode enabled only text will be sent. This is to capture Terminal data.

Disabled / Enabled

Resolution 100x31

Enable or disable extended terminal resolution.

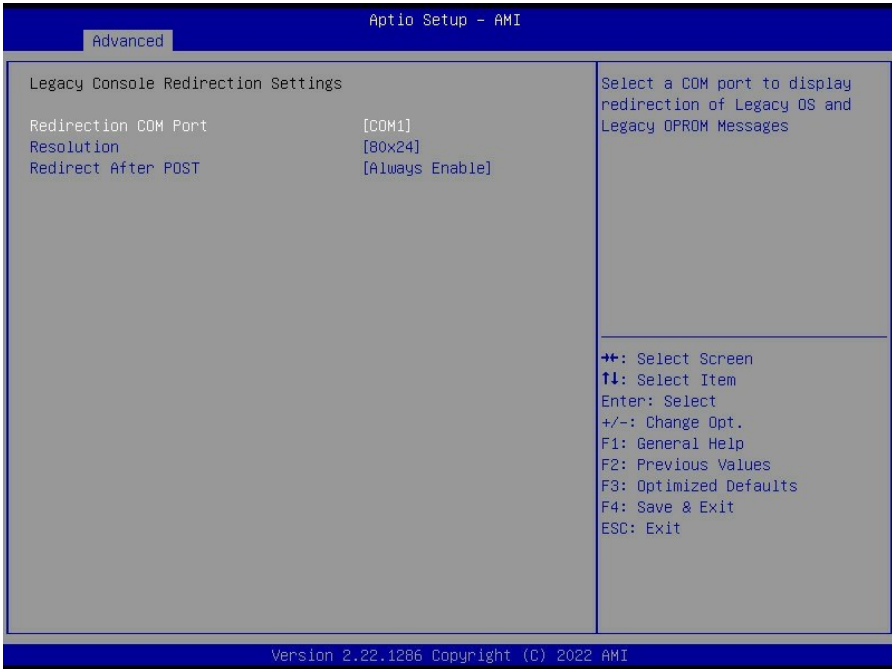
Disabled / **Enabled**

Putty KeyPad

Select FunctionKey and KeyPad on Putty.

VT100 / LINUX / XTERMR6 / SCO / ESCN / VT400

3.3.3.3 Legacy Console Redirection Settings



Redirection COM Port

Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages

COM1 / COM2

Resolution

On Legacy OS, the Number of Rows and Columns supported redirection

80x24 / 80x25

Redirect After POST

when Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS, when Always Enable is selected, then Legacy Console Redirection is enabled for Legacy OS. Default setting for this option is set to Always Enable.

Always Enable / BootLoader

3.3.3.4 Serial Port for Out-Of-Band Management/Windows Emergency Services (EMS) Console Redirection Settings

Aptio Setup - AMI		
Advanced		
Out-of-Band Mgmt Port	[COM1]	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.
Terminal Type	[VT-UTF8]	
Bits per second	[115200]	
Flow Control	[None]	
Data Bits EMS	8	
Parity EMS	None	
Stop Bits EMS	1	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1286 Copyright (C) 2022 AMI		

Out-of Band Mgmt Port

Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.

COM1 / COM2

Terminal Type

VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.

VT-UTF8 / VT100 / VT100+ / ANSI

Bits per Second

Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

9600 / 19200 / 57600 / **115200**

Flow Control

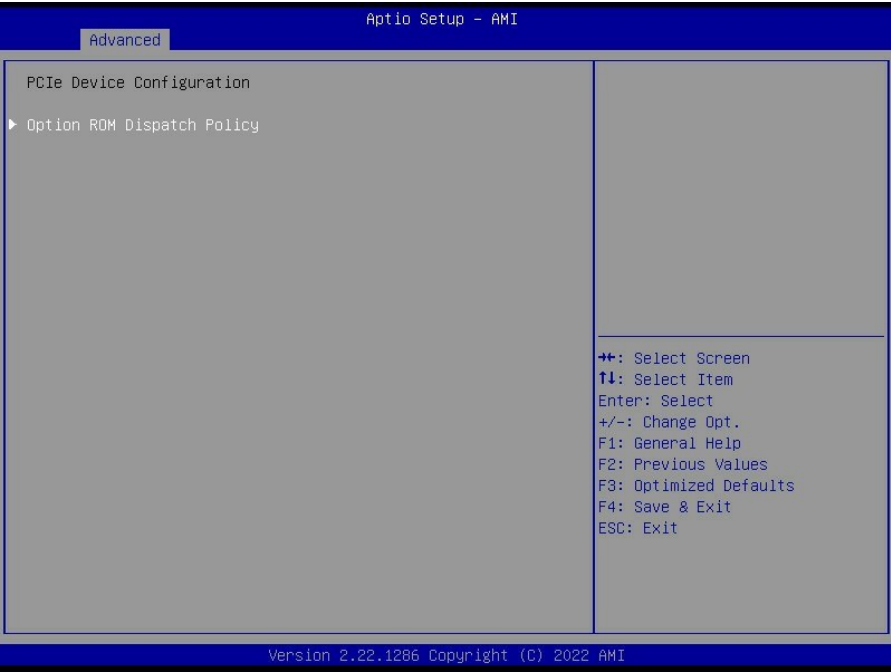
Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signal.

None / Hardware RTS/CTS / Software Xon/Xoff

Data Bits EMS / Parity EMS / Stop Bits EMS

Read only.

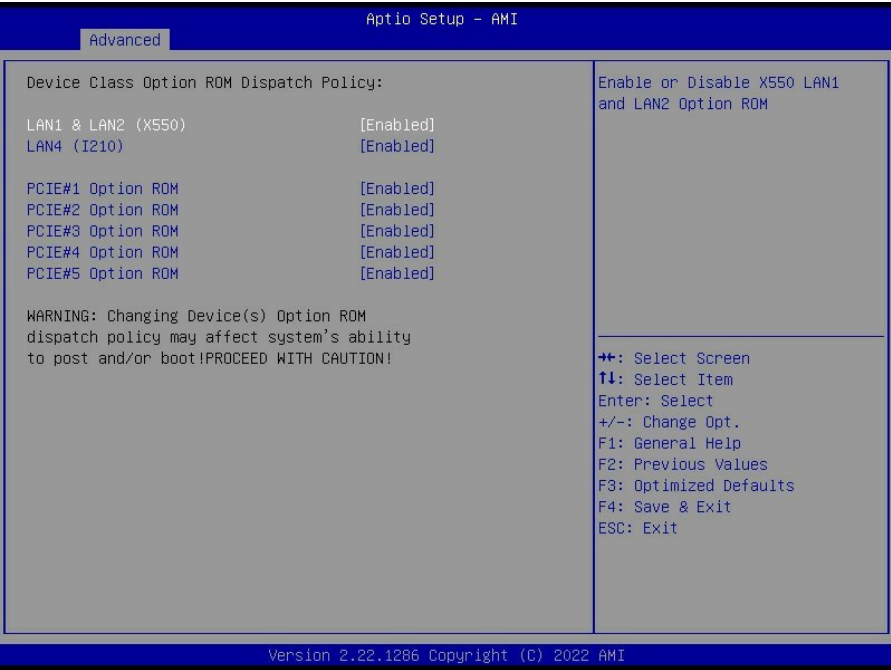
3.3.4 PCIe Device Configuration



Option ROM Dispatch Policy

Option ROM Dispatch Policy settings.

3.3.4.1 Device Class Option ROM Dispatch Policy:



LAN1&LAN2 (X550)

Enable or Disable X550 LAN1 and LAN2 Option ROM

Enabled / Disabled

LAN4 (I210)

Enable or Disable LAN2 Option Rom

Enabled / Disabled

PCIE#1 Option ROM

Enable or Disable Option ROM execution for selected Slot.

Enabled / Disabled

PCIE#2 Option ROM

Enable or Disable Option ROM execution for selected Slot.

Enabled / Disabled

PCIE#3 Option ROM

Enable or Disable Option ROM execution for selected Slot.

Enabled / Disabled

PCIe#4 Option ROM

Enable or Disable Option ROM execution for selected Slot.

Enabled / Disabled

PCIe#5 Option ROM

Enable or Disable Option ROM execution for selected Slot.

Enabled / Disabled

3.3.5 USB Configuration



Legacy USB Support

Enables legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.

Enabled / Disabled / Auto

XHCI Hand-off

This is a workaround for OSeS without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

Enabled / Disabled

USB Mass Storage Driver Support

Enable/Disable USB Mass Storage Driver Support.

Disabled / **Enabled**

Port 60/64 Emulation

Enable I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSeS.

Disabled / **Enabled**

USB transfer time-out

The time-out value for Control, Bulk and Interrupt transfers.

1 sec / 5 sec / 10 sec / **20 sec**

Device reset time-out

USB mass storage device Start Unit command time-out.

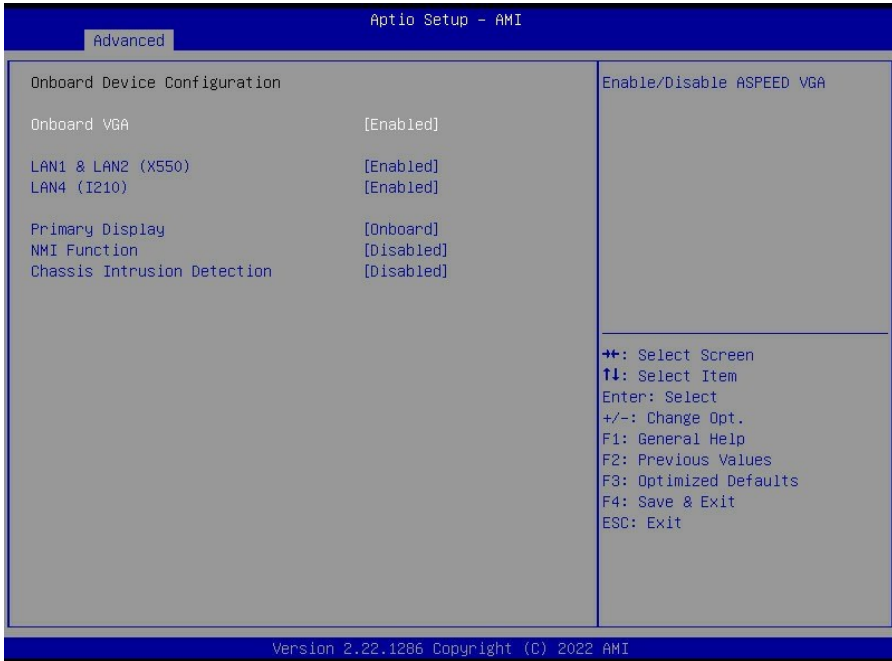
10 sec / **20 sec** / 30 sec / 40 sec

Device power-up delay

Maximum time the device will take before it properly reports itself to the Host Controller. 'AUTO' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Auto / Manual

3.3.6 Onboard Device Configuration



Onboard VGA

Enable/Disable ASPEED VGA
Disabled / **Enabled**

LAN1& LAN2 (X550)

LAN Enable/Disable control function.
Disabled / **Enabled**

LAN4 (I210)

LAN4 Enable/Disable control function.
Disabled / **Enabled**

Primary Display

Select active Video type.
Onboard / External

NMI Button

Enable or disable NMI button.
Disabled / Enabled

Chassis Intrusion Detection

Enabled: When a chassis open event is detected, the BIOS will display the event.
Disabled / Enabled

3.3.7 Super IO Configuration



Serial Port 1 Configuration

Set Parameters of serial Port 1 (COMA)

Serial Port 2 Configuration

Set Parameters of serial Port 2 (COMB)

3.3.7.1 Serial Port 1 Configuration



Serial Port

Select an optimal settings for Super IO Device.

Disabled / **Enabled**

NOTE: Serial Port has set to **Enabled**, the following items will be appear.

Change Settings

Select an optimal settings for Super IO device.

Auto /

IO=3F8h; IRQ=4; /

IO=2F8h; IRQ=4; /

IO=3E8h; IRQ=4; /

IO=2E8h, IRQ=4;

3.3.7.2 Serial Port 2 Configuration



Serial Port

Enable or Disable Serial Port (COM).

Disabled / **Enabled**

NOTE: Serial Port has set to **Enabled**, the following items will be appear.

Change Settings

Select an optimal settings for Super IO device.

Auto /

IO=3F8h; IRQ=3; /

IO=2F8h; IRQ=3; /

IO=3E8h; IRQ=3; /

IO=2E8h; IRQ=3;

3.3.8 Hardware Health Configuration



Auto Fan Control

Auto Fan Control help.

Manual / Full Speed

PWM Minimal Duty Cycle

PWM Minimal Duty Cycle (%). This item is available when **Fan Speed Control** is set to [Manual].

30

BMC Alert Beep

Enable/Disable BMC Alert Beep.

On / Off

PMBus support

PMBus Support.

Disabled / Enabled

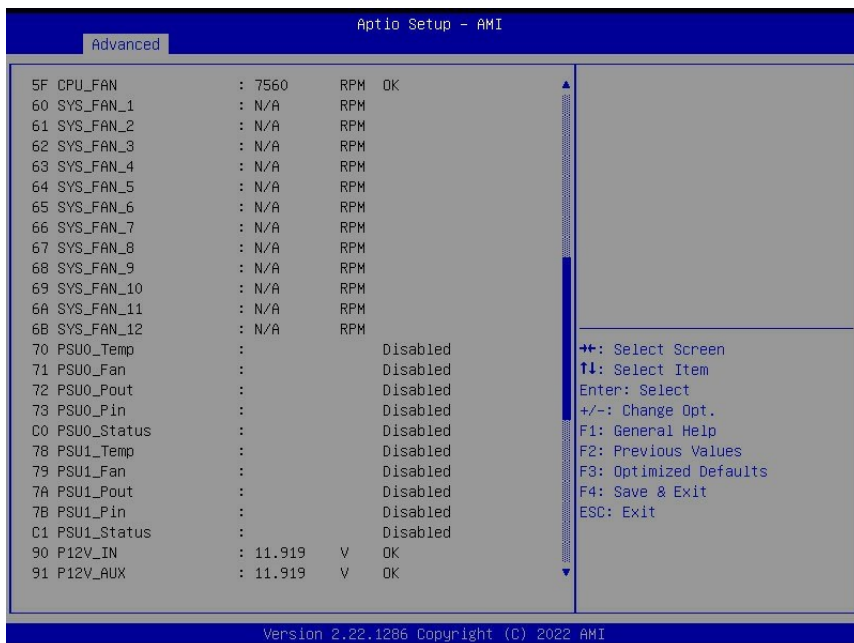
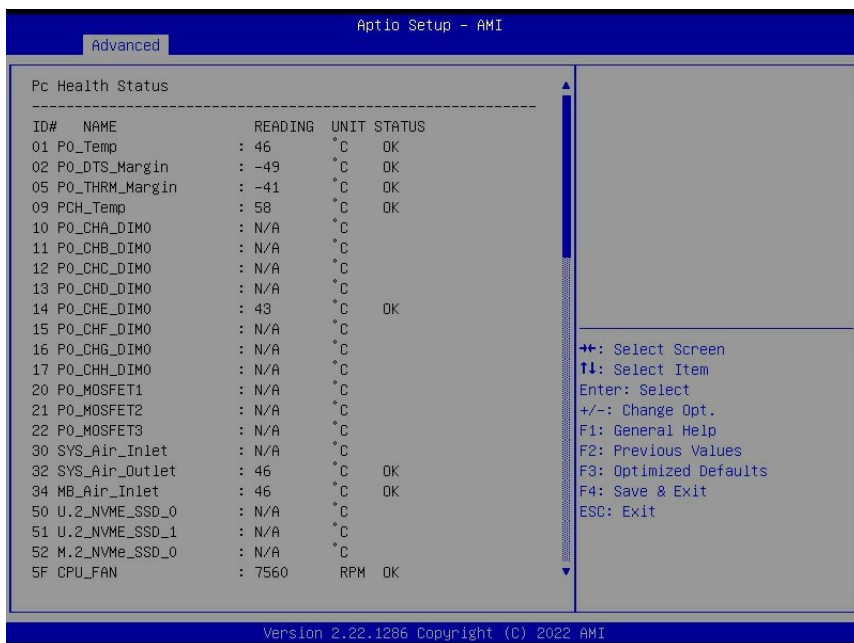
3.3.8.1 Sensor Data Register Monitoring

When you enter the **Sensor Data Register Monitoring** submenu, you will see the following dialog window pop out. Please wait 8~10 seconds.

PC Health Status			
ID#	NAME	READING	Unit STATUS

Sensor Data are reading now,			
Please wait a moment!!			

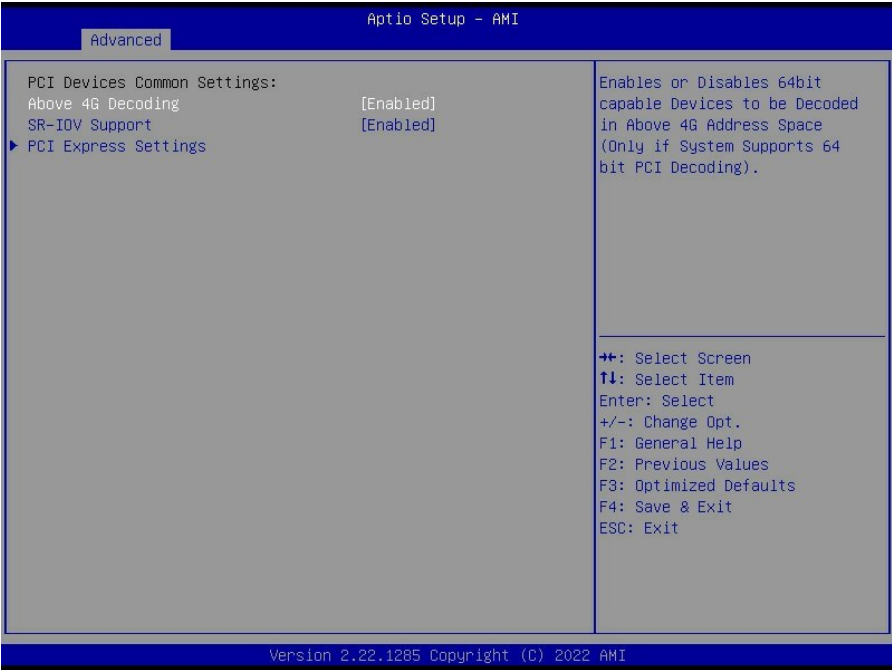
NOTE 1: SDR can not be modified. Read only.



71	PSU0_Fan	:		Disabled
72	PSU0_Pout	:		Disabled
73	PSU0_Pin	:		Disabled
00	PSU0_Status	:		Disabled
78	PSU1_Temp	:		Disabled
79	PSU1_Fan	:		Disabled
7A	PSU1_Pout	:		Disabled
7B	PSU1_Pin	:		Disabled
C1	PSU1_Status	:		Disabled
90	P12V_IN	:	11.919	V OK
91	P12V_AUX	:	11.919	V OK
92	P3V3	:	3.3082	V OK
93	P5V	:	5.0260	V OK
94	PVNN_PCH_AUX	:	0.9016	V OK
95	P1V05_PCH_AUX	:	1.0500	V OK
96	P1V8_AUX	:	1.7902	V OK
97	P3V_BAT	:	3.2705	V OK
98	PU1_VCCIN_CPU0	:	1.8098	V OK
9A	PU1_FAQN_CPU0	:	1.0882	V OK
9E	PU2VCCD_CPU0	:	1.1490	V OK
A1	CPU_Power	:	96	W OK
BA	Chassis_Status	:		Disabled

⇐: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

3.3.9 PCI Device Common Settings



Above 4G Decoding

Enables or Disables 64bit capable Devices to be decoded in Above 4G Address Space(Only if System supports 64 bit PCI Decoding).

Enabled / Disabled

SR-IOV Support

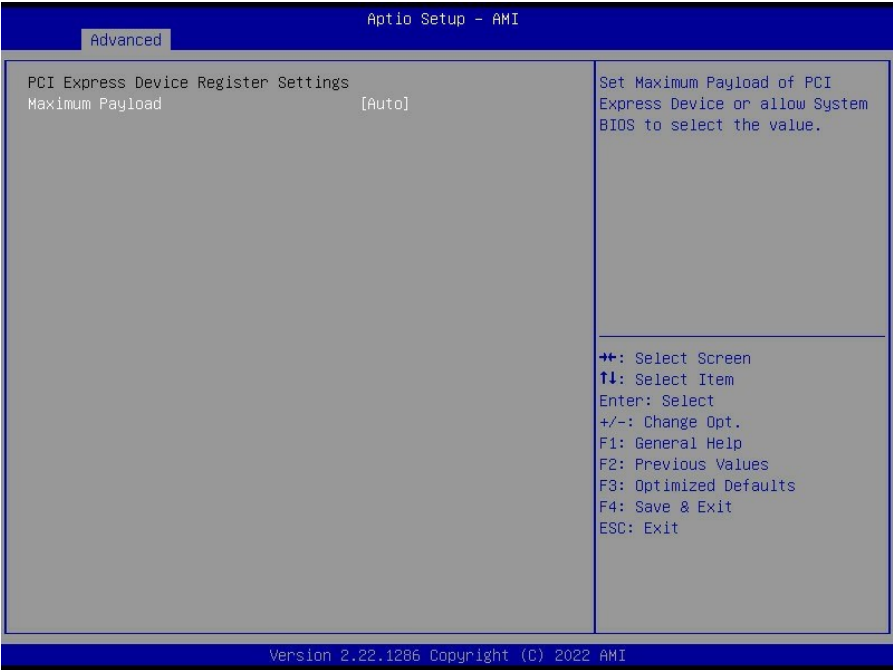
If system has SR-IOV capable PCIe devices, this option Enables or Disables Single Root IO virtualization Support

Enabled / Disabled

PCI Express Settings

Change PCI Express Devices Settings

3.3.9.1 PCI Express Subsystem

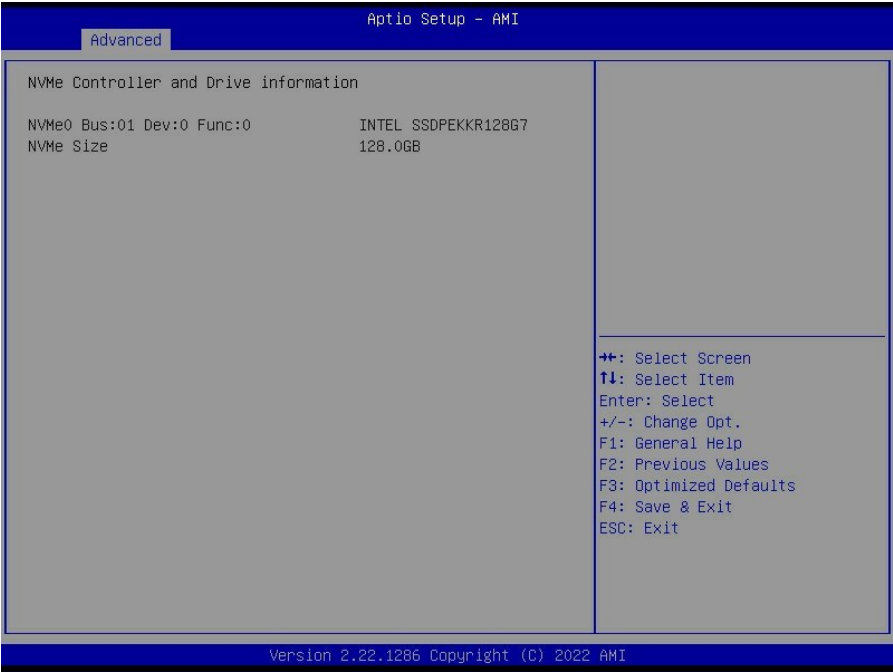


Maximum Payload

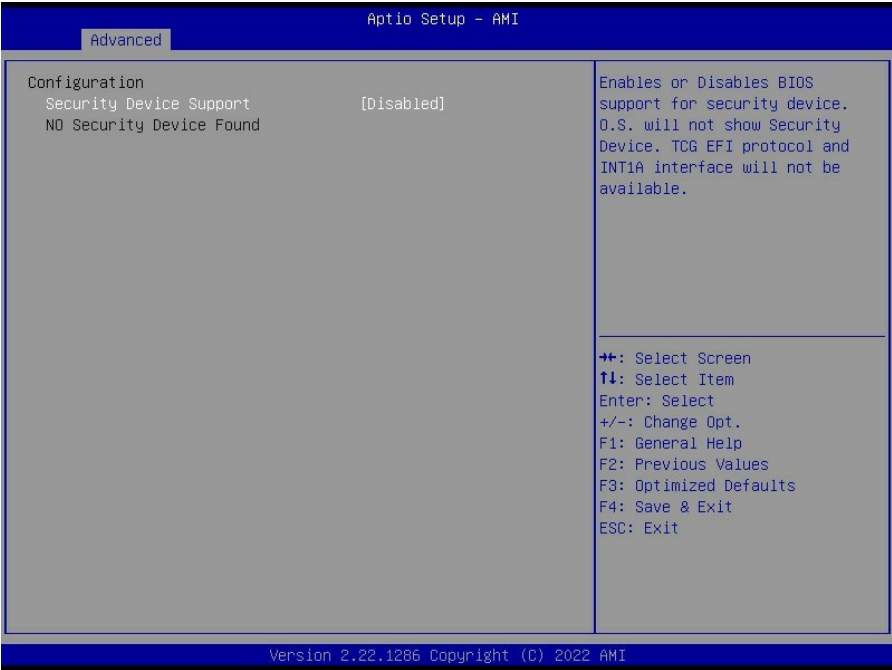
Set Maximum Payload of PCI Express Device or allow System BIOS to select the value.

Auto / 128 Bytes / 256 Bytes / 512 Bytes / 1024 Bytes / 2048 Bytes / 4096 Bytes

3.3.10 NVMe Configuration



3.3.11 Trusted Computing



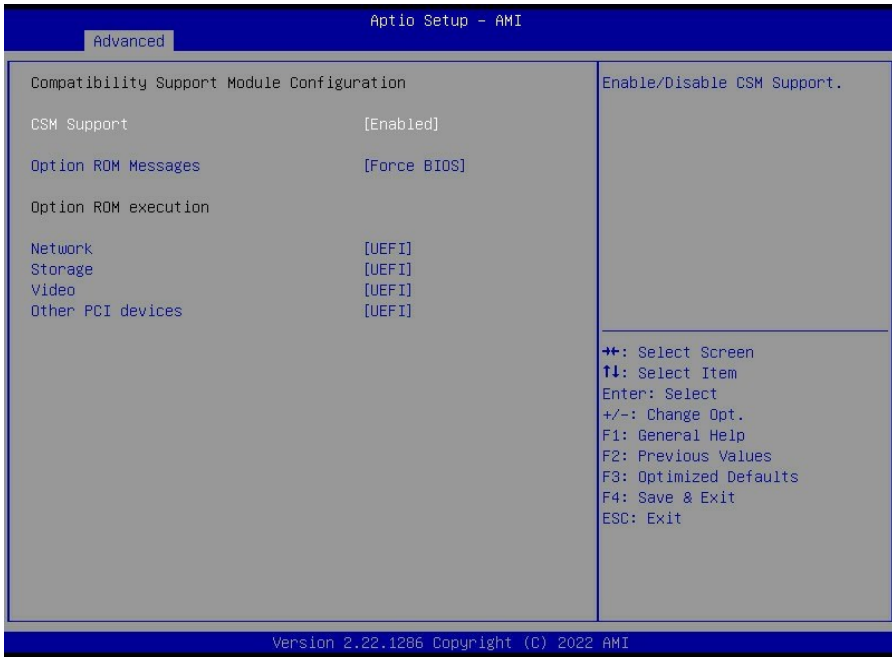
Security Device Support

Enables or disables BIOS support for security device. O.S. will not show Security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Enabled / **Disabled**

.

3.3.12 CSM Configuration



CSM support

Enable/Disable CSM Support

Enabled / **Disabled**

NOTE: When the CSM support set to **Enabled**, the following items will appear.

Option ROM Messages

Set display mode for Option ROM

Force BIOS / Keep Current

Network

Controls the execution of UEFI and legacy PXE OpROM

UEFI / legacy

Storage

Controls the execution of UEFI and legacy PXE OpROM

UEFI / legacy

Video

Controls the execution of UEFI and legacy Video OpROM

UEFI / legacy

Other PCI devices

Determines OpRom execution policy for devices other than network, storage, or video

UEFI / legacy

3.3.13 Redfish Host Interface Settings

Advanced

Aptio Setup - AMI

Redfish Host Interface Settings		Enable/Disable AMI Redfish
Redfish	[Enabled]	
BMC Redfish Version	1.11.0	
BIOS Redfish Version	1.11.0	
Redfish BMC Settings		
IP address	169.254.0.17	
IP Mask address	255.255.0.0	
IP Port	443	
		←+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

Redfish

Enable/Disable AMI Redfish.

Disabled / **Enabled**

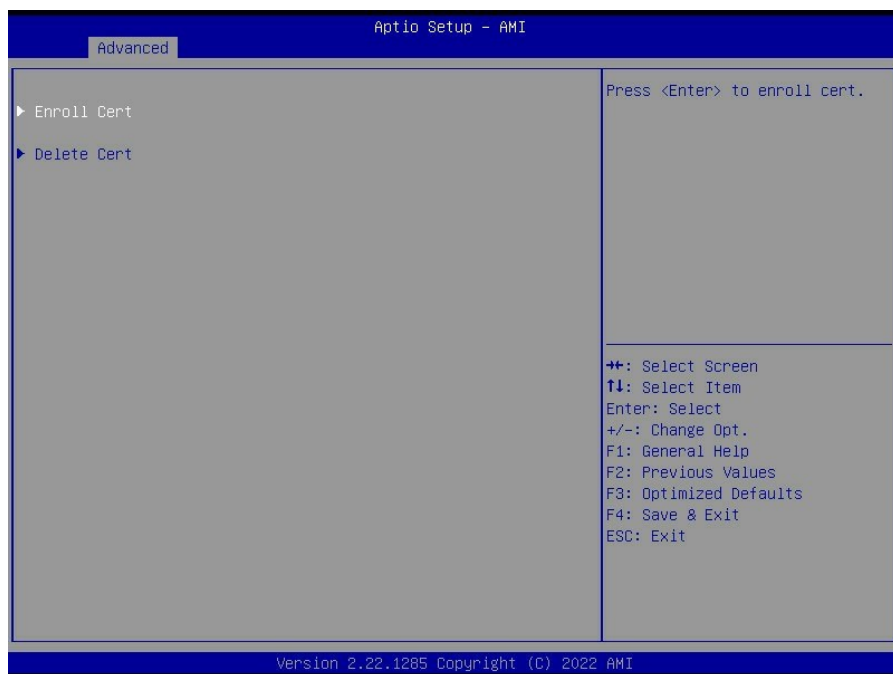
3.3.14 Tls Auth Configuration



Server CA Configuration

Press <Enter> to configure Server CA.

3.3.14.1 Tls Auth Configuration



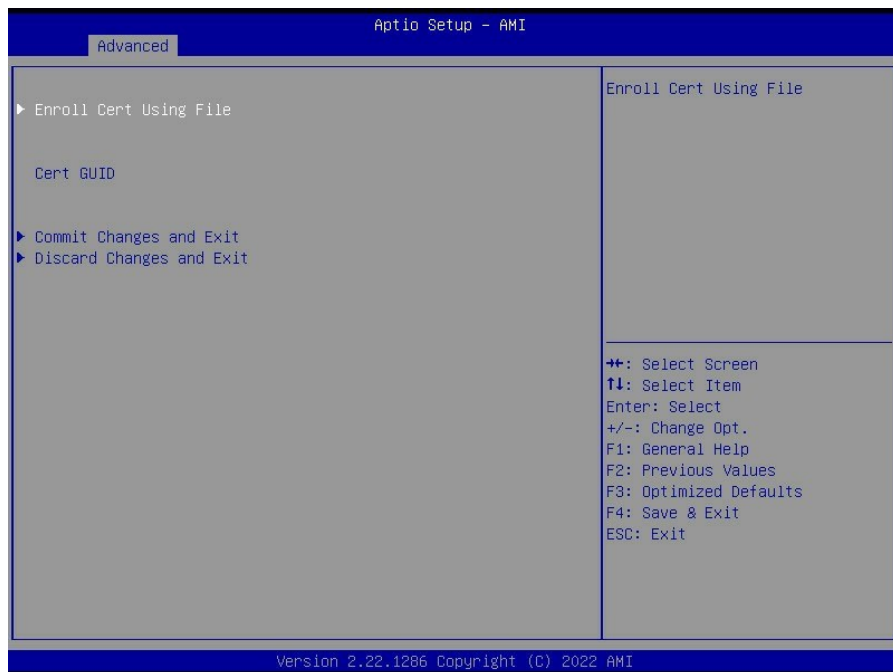
Enroll Cert

Press <Enter> to enroll cert.

Delete Cert

Press <Enter> to delete cert.

3.3.14.1.1 Enroll Cert Configuration



Enroll Cert Using File

Enroll Cert Using File

Cert GUID

Input digit character in 11111111-2222-3333-4444-1234567890ab format.

Commit Changes and Exit

Commit Changes and Exit

Discard Changes and Exit

Discard Changes and Exit

3.3.14.1.2 Delete Cert Configuration



FEXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

GUID for CERT
Disabled / Enabled

3.3.15 iSCSI Initiator Configuration



Host iSCSI Configuration

Host iSCSI Configuration settings

3.3.15.1 Host iSCSI Configuration

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.		
Advanced		
iSCSI Initiator Name	iqn.dqa	Delete one or more attempts
▶ Add an Attempt		
▶ Attempt 1		
▶ Attempt 2		
▶ Attempt 3		
▶ Delete Attempts		
▶ Change Attempt Order		
		↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.20.1275, Copyright (C) 2020 American Megatrends, Inc.		

Please follow the instructions to initiate the iSCSI function.

Step 1.

Select **Advanced** → **CSM Configuration** → **Network** → [UEFI].

Step 2.

Select **Advanced** → **Network Stack Configuration** → **Network Stack** → [Enabled]

Step 3.

Save changes and reboot.

iSCSI Initiator Name

The worldwide unique name of iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 223.

Add an Attempt

Add one or more attempts

Attempt 1

Attempt 2

Attempt 3

Delete Attempts

Delete one or more attempts

Change Attempt Order

Change attempt sequence

3.3.15.2 Add an Attempt



Read only.

3.3.15.2.1 MAC 36:02:0B:83:D7:63

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.		
Advanced		
iSCSI Attempt Name	Attempt 2	▲ The human name defined for this attempt.
iSCSI Mode	[Disabled]	
Internet Protocol	[IPv4]	
Connection Retry Count	0	
Connection Establishing Timeout	1000	
OUI-format ISID	36020B83D763	
Configure ISID	83D763	
Enable DHCP	[Disabled]	
Initiator IP Address	0.0.0.0	↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Initiator Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Target Name		
Target Address		
Target Port	3260	
Boot LUN	0	
Authentication Type	[None]	
Save Changes		

Version 2.20.1275, Copyright (C) 2020 American Megatrends, Inc.

iSCSI Mode

Disabled, Enabled, Enabled for MPIO.

Disabled / Enabled / Enabled for MPIO

Internet Protocol

Initiator IP address is system assigned in IP6 mode. In Autoconfigure mode, iSCSI driver will attempt to connect iSCSI target via IPv4 stack, if failed then attempt IPv6 stack.

IPv4 / IPv6 / Autoconfigure

Connection Retry Count

The minimum value is 0 and the maximum is 16. 0 means no retry.

Connection Establishing Timeout

The timeout value in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds.

Configure ISID

OUI-format ISID in 6 bytes, default value is derived from MAC address. Only last 3 bytes are configurable. Example: update 0ABBCCDDEEFF to 0ABBCCF07901 by input F07901.

Enable DHCP

Enable DHCP.

Disabled / Enabled

Initiator IP Address

Enter IP address in dotted-decimal notation.

Initiator Subnet Mask

Enter IP address in dotted-decimal notation.

Gateway

Enter IP address in dotted-decimal notation.

Target Name

The worldwide unique name of the target. Only iqn. format is accepted. Range is from 4 to 223

iqu. xxx

Target Address

Enter Target address in IPv4, IPv6 or URL format. You need to configure DNS server address in advance if input a URL string.

Target Port

Target Port.

Boot LUN

Hexadecimal representation of the LU number. Examples are: 4752-3A4F-6b7e-3F99, 6734-9-156f-127, 4186-9.

Authentication Type

Authentication method: CHAP, Kerberos, or None.

CHAP / **None**

Save Changes

Must reboot system manually for changes to take place.

3.3.15.2.2 MAC A0:42:3F:37:EA:08

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

ISCSI Attempt Name	Attempt 4	▲ The human name defined for this attempt.
ISCSI Mode	[Disabled]	
Internet Protocol	[IPv4]	
Connection Retry Count	0	
Connection Establishing Timeout	1000	
OUI-format ISID	20423F37EA08	
Configure ISID	37EA08	
Enable DHCP	[Disabled]	
Initiator IP Address	0.0.0.0	↔: Select Screen
Initiator Subnet Mask	0.0.0.0	↑↓: Select Item
Gateway	0.0.0.0	Enter: Select
		+/-: Change Opt.
Target Name		F1: General Help
Target Address		F2: Previous Values
Target Port	3260	F3: Optimized Defaults
Boot LUN	0	F4: Save & Exit
		ESC: Exit
Authentication Type	[None]	
Save Changes		

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

iSCSI Mode

Disabled, Enabled, Enabled for MPIO.

Disabled / Enabled / Enabled for MPIO

Internet Protocol

Initiator IP address is system assigned in IP6 mode. In Autoconfigure mode, iSCSI driver will attempt to connect iSCSI target via IPv4 stack, if failed then attempt IPv6 stack.

IPv4 / IPv6 / Autoconfigure

Connection Retry Count

The minimum value is 0 and the maximum is 16. 0 means no retry.

Connection Establishing Timeout

The timeout value in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds.

Configure ISID

OUI-format ISID in 6 bytes, default value is derived from MAC address. Only last 3 bytes are configurable. Example: update 0ABBCCDDEEFF to 0ABBCCF07901 by input F07901.

Enable DHCP

Enable DHCP.

Disabled / Enabled

Initiator IP Address

Enter IP address in dotted-decimal notation.

Initiator Subnet Mask

Enter IP address in dotted-decimal notation.

Gateway

Enter IP address in dotted-decimal notation.

Target Name

The worldwide unique name of the target. Only iqn. format is accepted. Range is from 4 to 223

iqu. xxx

Target Address

Enter Target address in IPv4, IPv6 or URL format. You need to configure DNS server address in advance if input a URL string.

Target Port

Target Port.

Boot LUN

Hexadecimal representation of the LU number. Examples are: 4752-3A4F-6b7e-3F99, 6734-9-156f-127, 4186-9.

Authentication Type

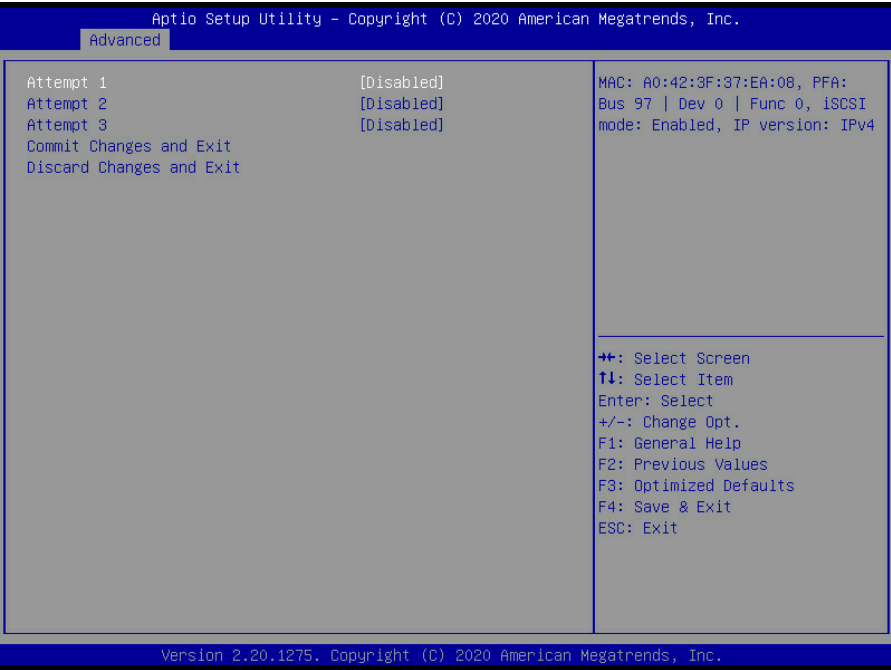
Authentication method: CHAP, Kerberos, or None.

CHAP / **None**

Save Changes

Must reboot system manually for changes to take place.

3.3.15.3 Delete Attempts



Attempt 1

MAC: A0:42:3F:37:EA:08, PFA: Bus 97/ Dev 0 / Func 0, iSCSI mode: Enabled, IP version: IPv4.

Disabled / Enabled

Attempt 2

MAC: 36:02:0B:83:D7:63, PFA: Bus 35 / Dev 0 / Func 3, iSCSI mode: Disabled, IP version: IPv4.

Disabled / Enabled

Attempt 3

MAC: 36:02:0B:83:D7:63, PFA: Bus 35 / Dev 0 / Func 3, iSCSI mode: Disabled, IP version: IPv4.

Disabled / Enabled

Commit Changes and Exit

Commit Changes and Exit.

Discard Changes and Exit

Discard Changes and Exit.

3.3.15.4 Change Attempt Order



Change Attempt Order

Change the order of Attempts using +/- keys. Use arrow keys to select the attempt then press +/- to move the attempt up/down in the attempt order list.

Attempt 1 / Attempt 2 / Attempt 3

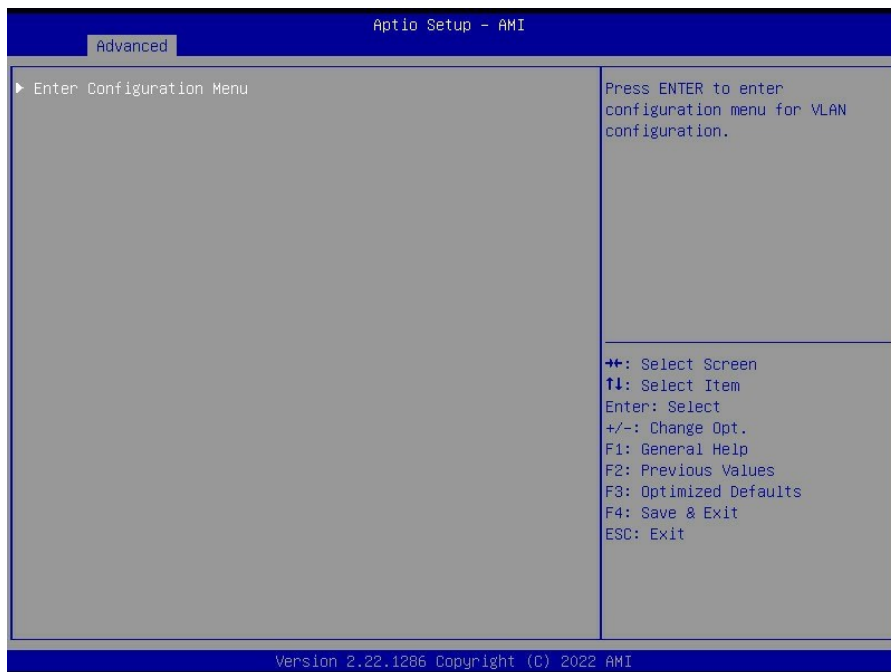
Commit Changes and Exit

Commit Changes and Exit.

Discard Changes and Exit

Discard Changes and Exit.

3.3.16 VLAN Configuration



Enter Configuration

Press ENTER to enter configuration menu for VLAN configuration.

3.3.16.1 Enter Configuration

Aptio Setup - AMI	
Advanced	
Create new VLAN VLAN ID 0 Priority 0 Add VLAN Configured VLAN List Remove VLAN	VLAN ID of new VLAN or existing VLAN, valid value is 0~4094 ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1286 Copyright (C) 2022 AMI	

VLAN ID

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

Priority

802.1Q Priority, valid value is 0~7

Add VLAN

Create a new VLAN or update existing VLAN

Remove VLAN

Remove selected VLANs

3.3.17 MAC: 4E722FER47F30-IPv4 Network Menu

Aptio Setup - AMI		
Advanced		
Configured	[Disabled]	Indicate whether network address configured successfully or not.
Save Changes and Exit		
		→+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1286 Copyright (C) 2022 AMI		

Configured

Indicate whether network address configured successfully or not.

Disabled / Enabled

NOTE: When Configured was set to **Enabled**, the following items will be available to set up.

Enable DHCP

Indicate whether network address configured successfully or not.

Disabled / Enabled

Local IP Address

Enter IP address in dotted-decimal notation. Example: 162.168.10.12

Local NetMask

Enter Netmask in dotted-decimal notation. Example: 255.255.255.0

Local Gateway

Enter Gateway in dotted-decimal notation. Example: 192.168.10.1

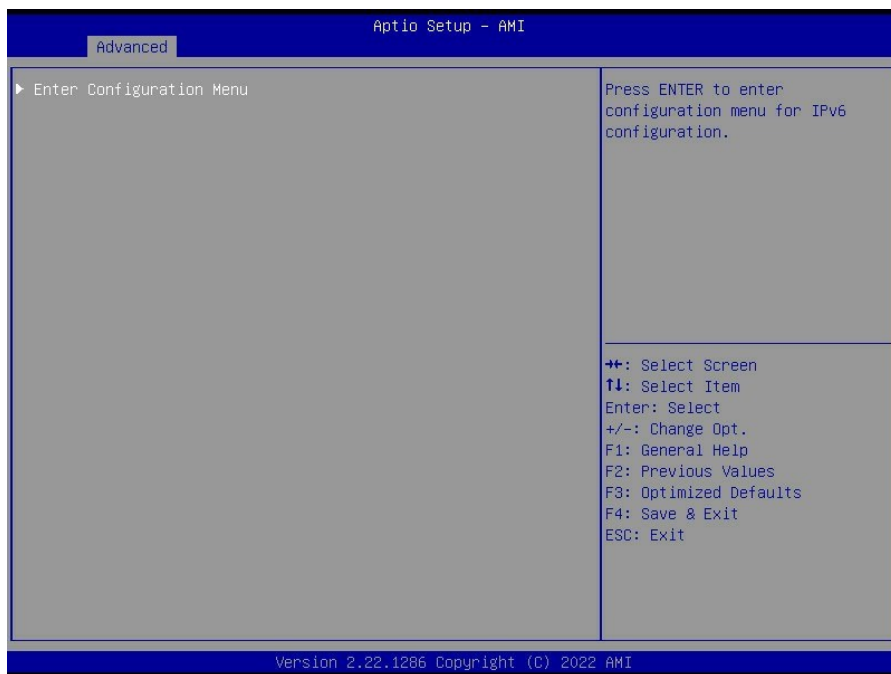
Local DNS Servers

Enter DNS Servers in dotted-decimal notation. Example: 192.168.10.8
192.168.10.9

Save Changes and Exit

Save Changes and Exit

3.3.18 MAC: 4E722FER47F30-IPv6 Network Menu



Enter Configuration Menu

Press ENTER to enter configuration menu for IPv6 configuration.

3.3.18.1 Enter Configuration Menu

Aptio Setup - AMI		
Advanced		
Interface Name :	eth0	The 64 bit alternative interface ID for the device.
Interface Type :	Ethernet	The string is colon separated.
MAC address :	4E-72-2F-E4-7F-30	e.g. ff:dd:88:66:cc:1:2:3
Host addresses :	FE80::4C72:2FFF:FEE4:...	
Route Table :	FE80::/64 >>::	
Gateway addresses :		
DNS addresses :		
Interface ID :	4C:72:2F:FF:FE:E4:7F:30	
DAD Transmit Count :	1	
Policy :	[automatic]	
Save Changes and Exit		←→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

Interface ID

The 64 bit alternative interface ID for the device. The string is colon separated.
e.g. ff:dd:88:66:cc:1:2:3

DAD Transmit Count

The number of consecutive Neighbor Solicitation message sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that duplicate address detection is not performed.

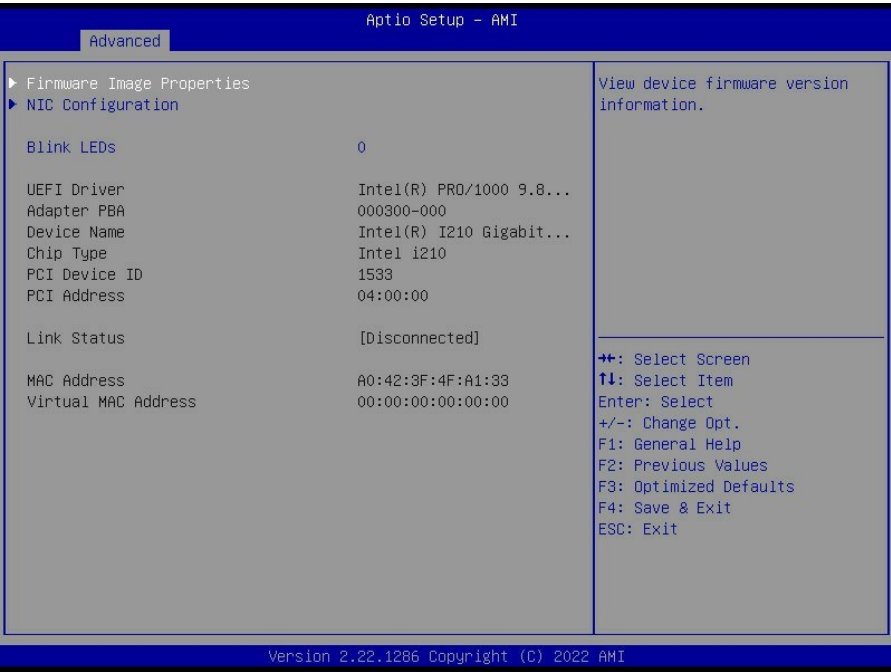
Policy

Automatic or manual
Automatic / manual

Save Changes and Exit

Save changes for interface ID, DAD transmit count, policy, and data in advanced configuration.

3.3.19 Intel® I210 Gigabit Network Connection Settings



Firmware Image Properties

View device firmware version information.

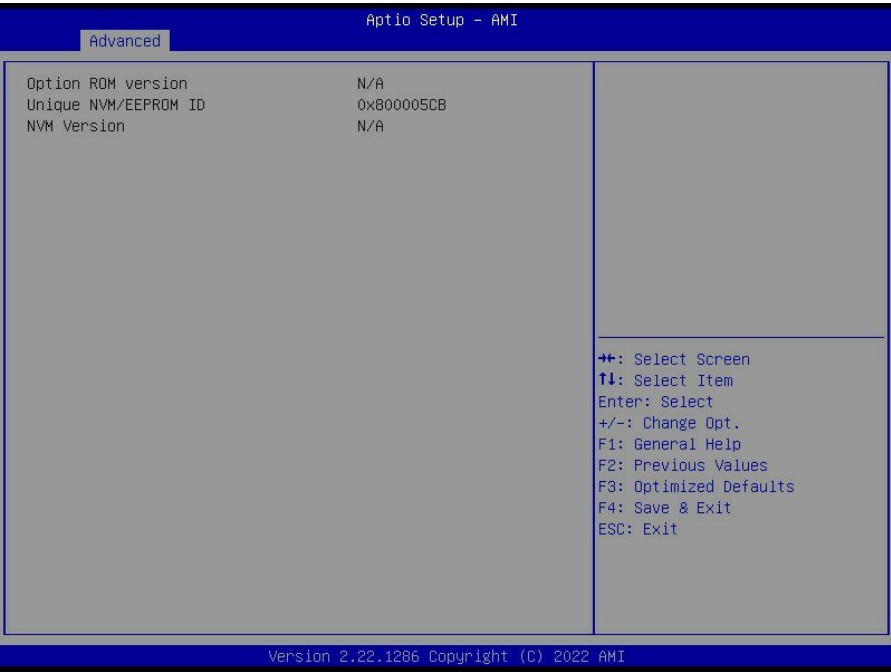
NIC Configuration

Click to configure the network device port.

Blink LEDs

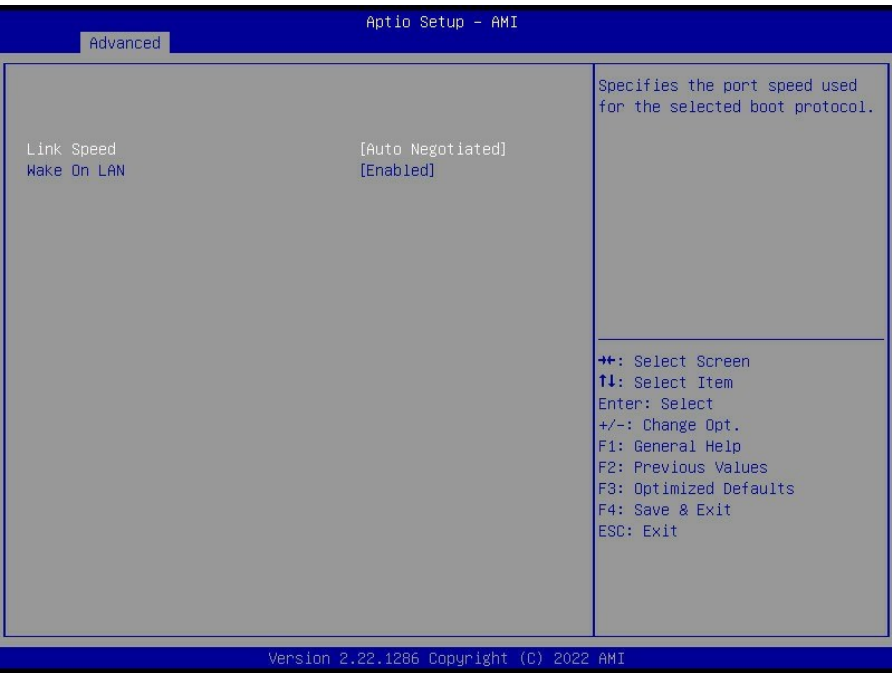
Blink LEDs for a duration up to 15 seconds.

3.3.19.1 Firmware Image Properties Settings



Only Read

3.3.19.2 NIC Configuration Settings



Link Speed

Specifies the port speed used for the selected boot protocol

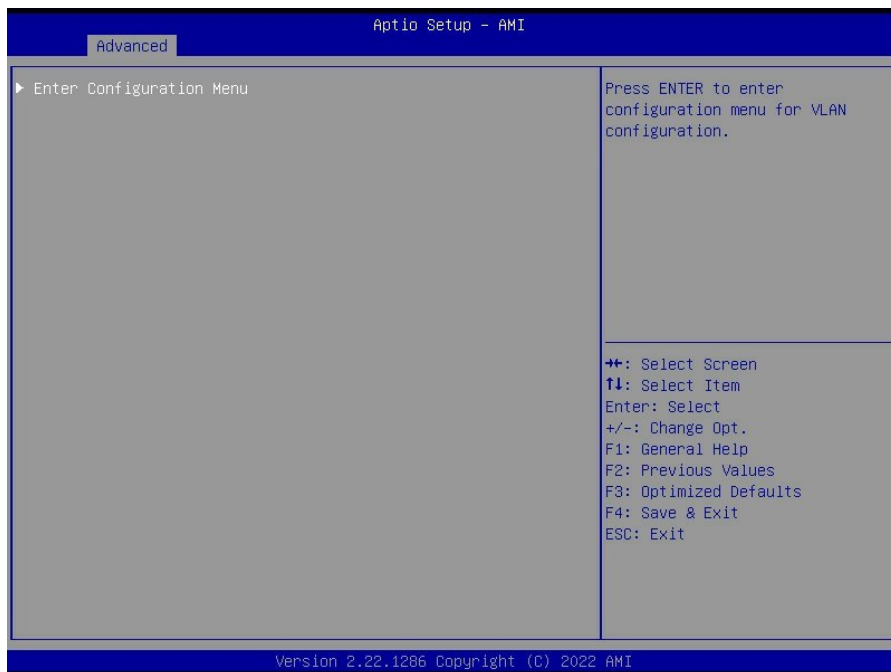
Auto Negotiated / 10 Mbps Half / 10 Mbps Full / 100 Mbps Half / 100 Mbps Full

Wake On LAN

Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.

Disabled / **Enabled**

3.3.20 VLAN Configuration (MAC: A0423F4FA133)



Enter Configuration Menu

Press ENTER to enter configuration menu for VLAN configuration.

3.3.20.1 Enter Configuration Settings

Aptio Setup - AMI	
Advanced	
Create new VLAN	
VLAN ID	0
Priority	0
Add VLAN	
Configured VLAN List	
Remove VLAN	
VLAN ID of new VLAN or existing VLAN, valid value is 0~4094	
++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1286 Copyright (C) 2022 AMI	

VLAN ID

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

Priority

802.1Q Priority, valid value is 0~7

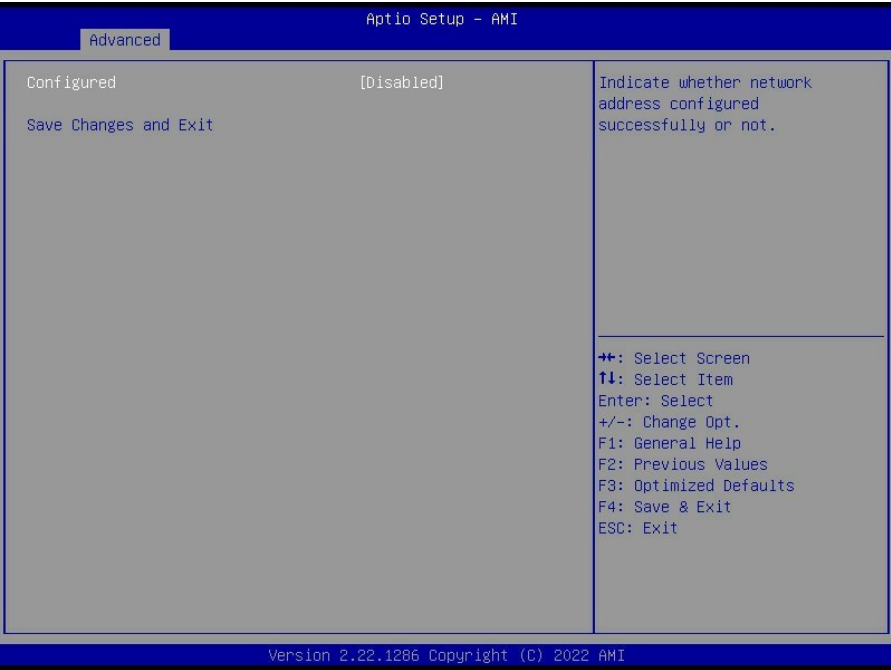
Add VLAN

Create a new VLAN or update existing VLAN

Remove VLAN

Remove selected VLANs

3.3.21 MAC: A0423F4FA133-IPv4 Network Menu



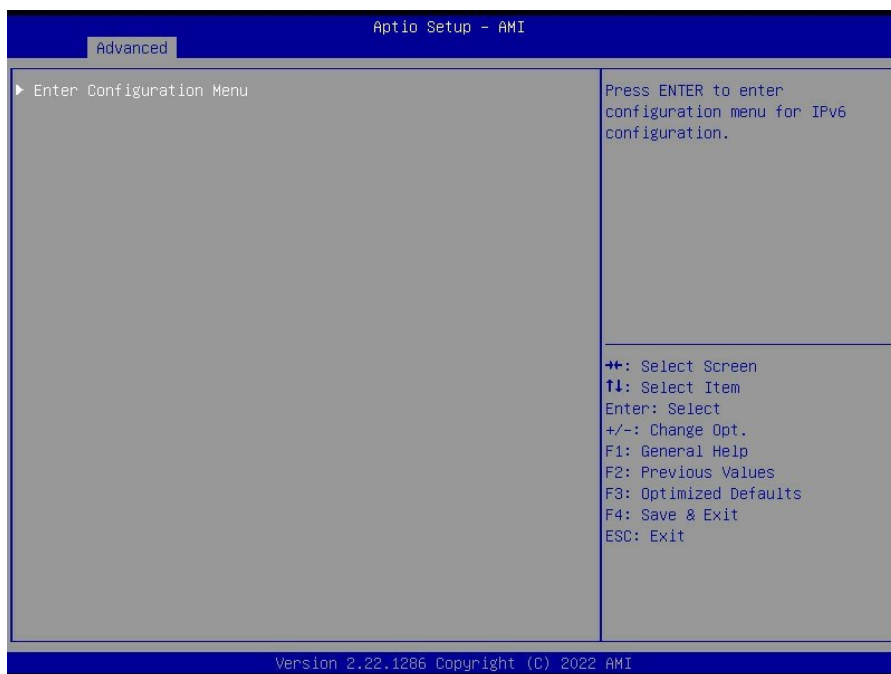
Configured

Indicated whether network address configured successfully.

Save Changes and Exit

Save changes and exit.

3.3.22 MAC: A0423F4FA133-IPv6 Network Menu



Enter Configuration Menu

Press ENTER to enter configuration menu for IPv6 configuration.

3.3.22.1 Enter Configuration Menu

Aptio Setup - AMI		
Advanced		
Interface Name :	eth1	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3
Interface Type :	Ethernet	
MAC address :	A0-42-3F-4F-A1-33	
Host addresses :	FE80::A242:3FFF:FE4F:...	
Route Table :	FE80::/64 >>::	
Gateway addresses :		
DNS addresses :		
Interface ID :	A2:42:3F:FF:FE:4F:A1:33	
DAD Transmit Count :	1	
Policy :	[automatic]	
Save Changes and Exit		↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

Interface ID

The 64 bit alternative interface ID for the device. The string is colon separated. E.g. ff:dd:88:66:cc:1:2:3

DAD Transmit Count

The number of consecutive Neighbor Solicitation message sent while performing duplicate address detection on a tentative address. A value of zero indicates that duplicate address detection is not performed.

1

Policy

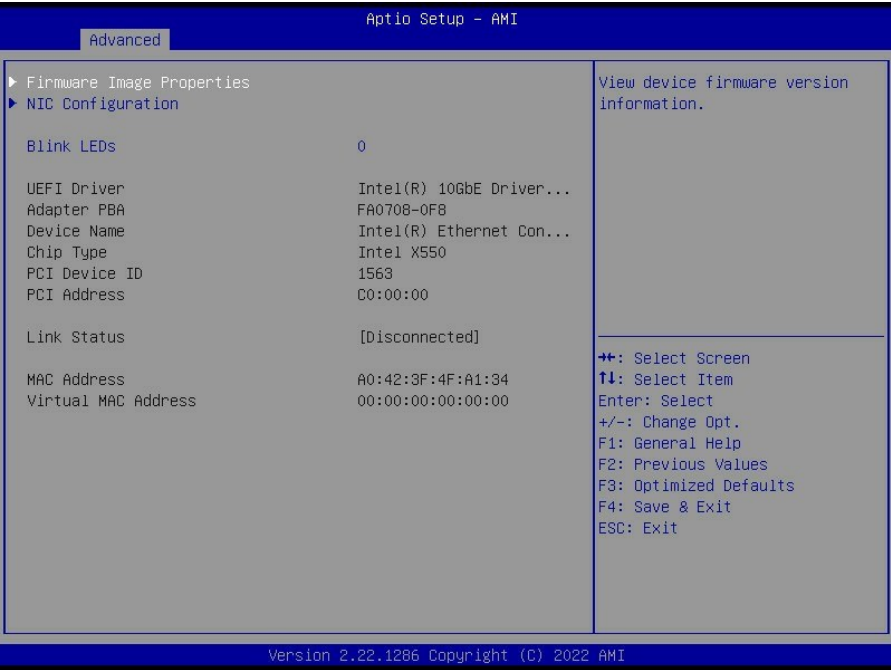
Automatic or manual

Automatic / manual

Save Changes and Exit

Save Changes for interface ID, DAD transmit count, policy, and data in advanced configuration.

3.3.23 Intel® Ethernet Converged Network Adapter X550-T2-A0



Firmware Image Properties

View device firmware version information.

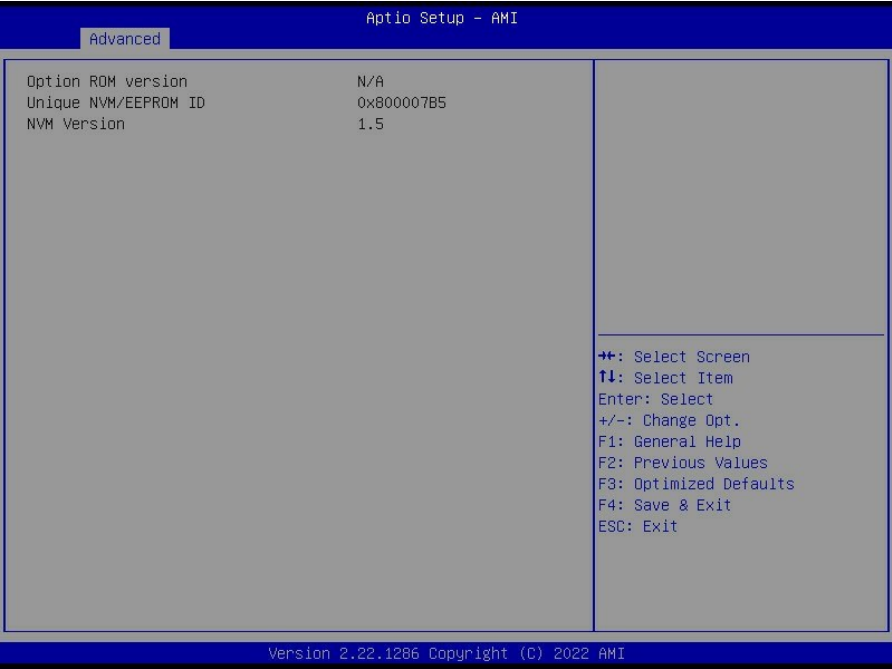
NIC Configuration

Click to configure the network device port.

Blink LEDs

Blink LEDs for a duration up to 15 seconds.

3.3.23.1 Firmware Image Properties



Only Read

3.3.23.2 NIC Configuration

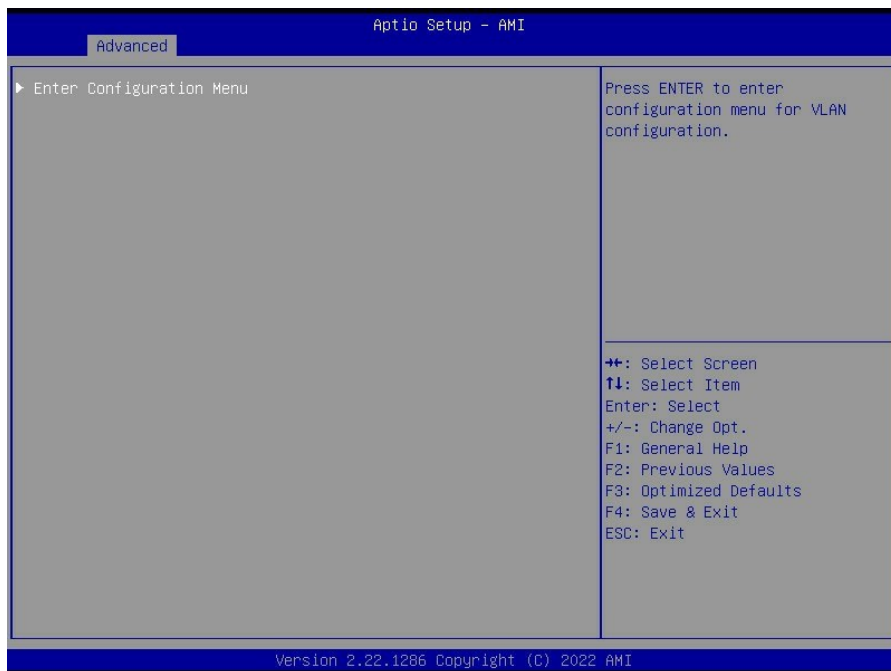


Wake On LAN

Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.

Enabled / Disabled

3.3.24 VLAN Configuration (MAC: A0423F4FA134)



Enter Configuration Menu

Press Enter to enter configuration menu for VLAN configuration

3.3.24.1 Enter Configuration Menu

Aptio Setup - AMI	
Advanced	
Create new VLAN	
VLAN ID	0
Priority	0
Add VLAN	
Configured VLAN List	
Remove VLAN	
VLAN ID of new VLAN or existing VLAN, valid value is 0~4094	
↑↑: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1286 Copyright (C) 2022 AMI	

VLAN ID

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

Priority

802.1Q Priority, valid value is 0~7

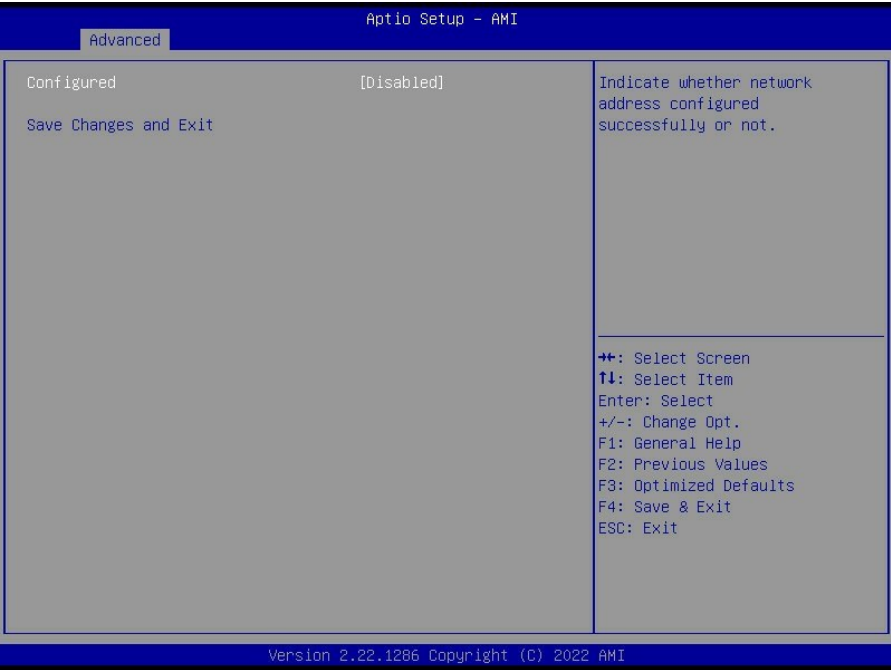
Add VLAN

Create a new VLAN or update existing VLAN

Remove VLAN

Remove selected VLANs

3.3.25 MAC: A0423F4FA134-IPv4 Network Menu



Configured

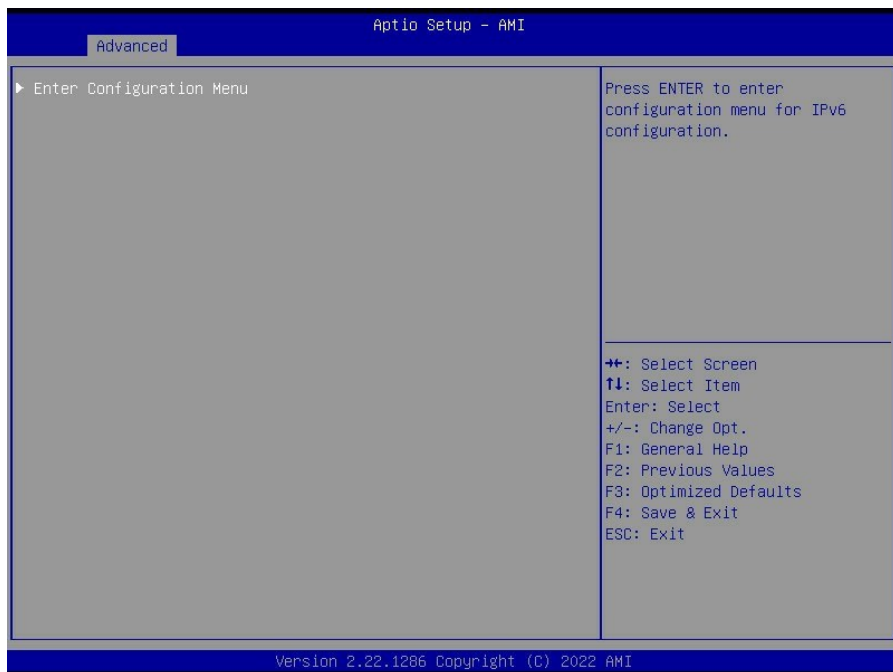
Indicate whether network address configured sucessfully or not.

Enabled / **Disabled**

Save Changes and Exit

Save Changes and exit

3.3.26 MAC: A0423F4FA134-IPv6 Network Menu



Enter Configuration Menu

Press ENTER to enter configuration menu for IPv6 configuration.

3.3.26.1 Enter Configuration Menu

Aptio Setup - AMI		
Advanced		
Interface Name :	eth2	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3
Interface Type :	Ethernet	
MAC address :	A0-42-3F-4F-A1-34	
Host addresses :	FE80::A242:3FFF:FE4F:...	
Route Table :	FE80::/64 >>::	
Gateway addresses :		
DNS addresses :		
Interface ID :	A2:42:3F:FF:FE:4F:A1:34	
DAD Transmit Count :	1	
Policy :	[automatic]	
Save Changes and Exit		↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

Interface ID

The 64 bit alternative interface ID for the device. The string is colon separated. E.g. ff:dd:88:66:cc:1:2:3

DAD Transmit Count

The number of consecutive Neighbor Solicitation message sent while performing duplicate address detection on a tentative address. A value of zero indicates that duplicate address detection is not performed.

1

Policy

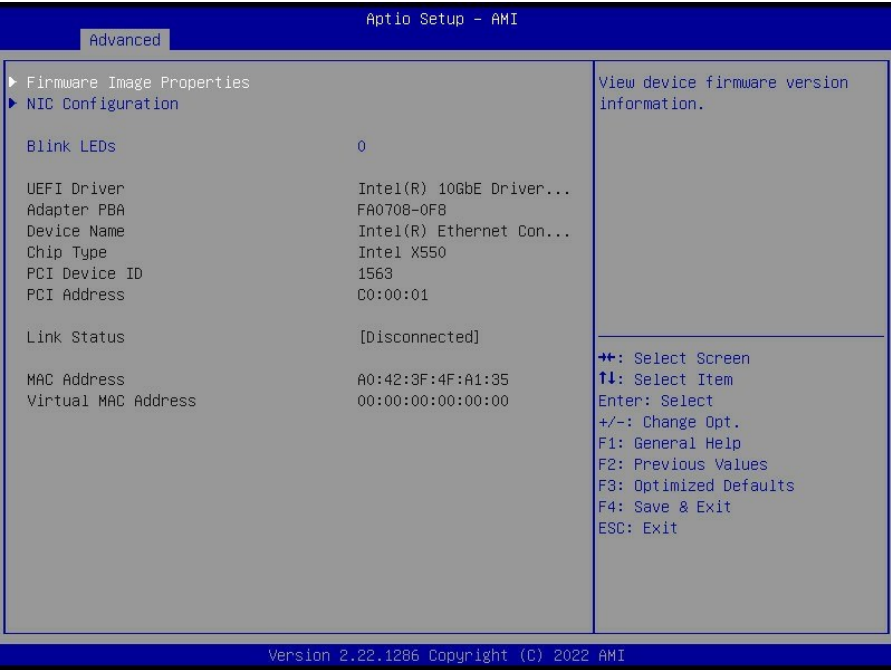
Automatic or manual

Automatic / manual

Save Changes and Exit

Save Changes for interface ID, DAD transmit count, policy, and data in advanced configuration.

3.3.27 Intel® Ethernet Converged Network Adapter X550-T2-A0



Firmware Image Properties

View device firmware version information.

NIC Configuration

Click to configure the network device port.

Blink LEDs

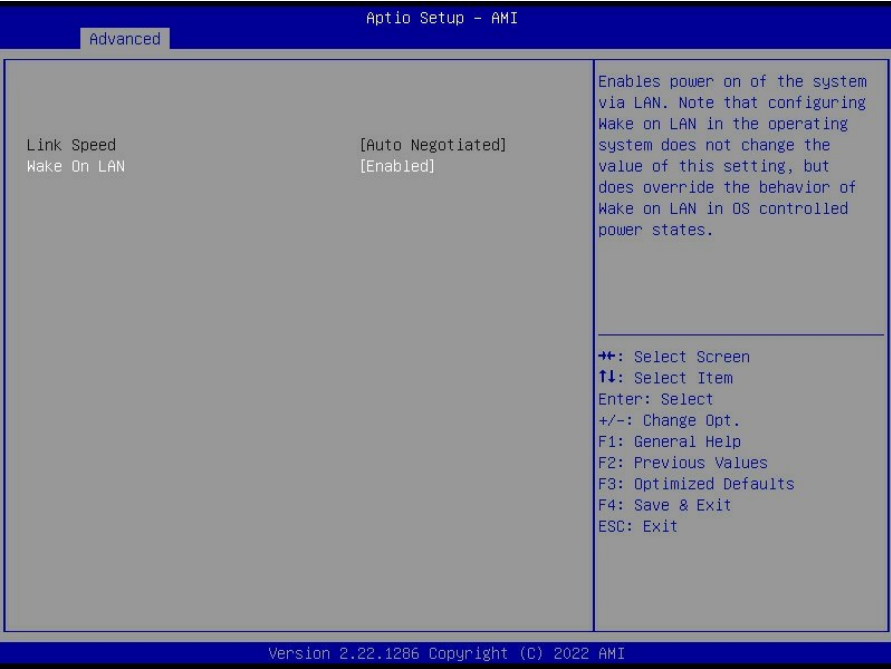
Blink LEDs for a duration up to 15 seconds.

3.3.27.1 Firmware Image Properties



Only Read

3.3.27.2 NIC Configuration

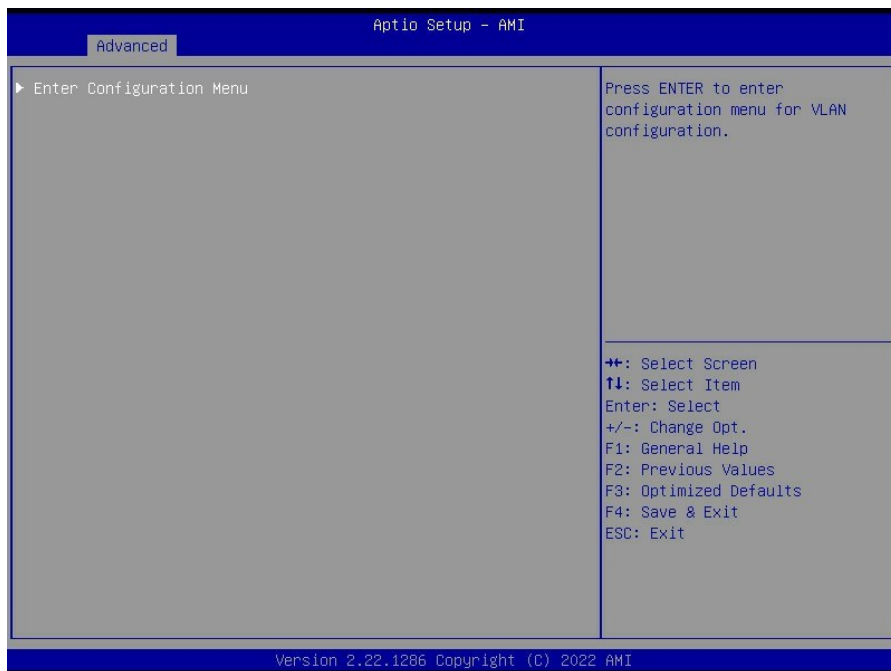


Wake On LAN

Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.

Enabled / Disabled

3.3.28 VLAN Configuration (MAC: A0423F4FA135)



Enter Configuration Menu

Press Enter to enter configuration menu for VLAN configuration

3.3.28.1 Enter Configuration Menu

Advanced

Aptio Setup - AMI

Create new VLAN

VLAN ID0

Priority0

Add VLAN

Configured VLAN List

Remove VLAN

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

↕: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous Values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

VLAN ID

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

Priority

802.1Q Priority, valid value is 0~7

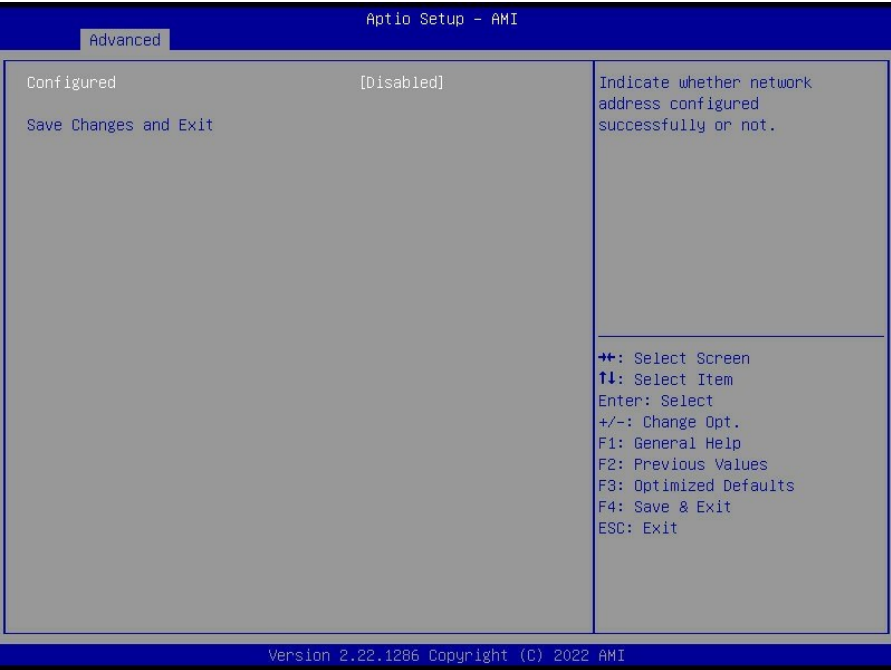
Add VLAN

Create a new VLAN or update existing VLAN

Remove VLAN

Remove selected VLANs

3.3.29 MAC: A0423F4FA135-IPv4 Network Menu



Configured

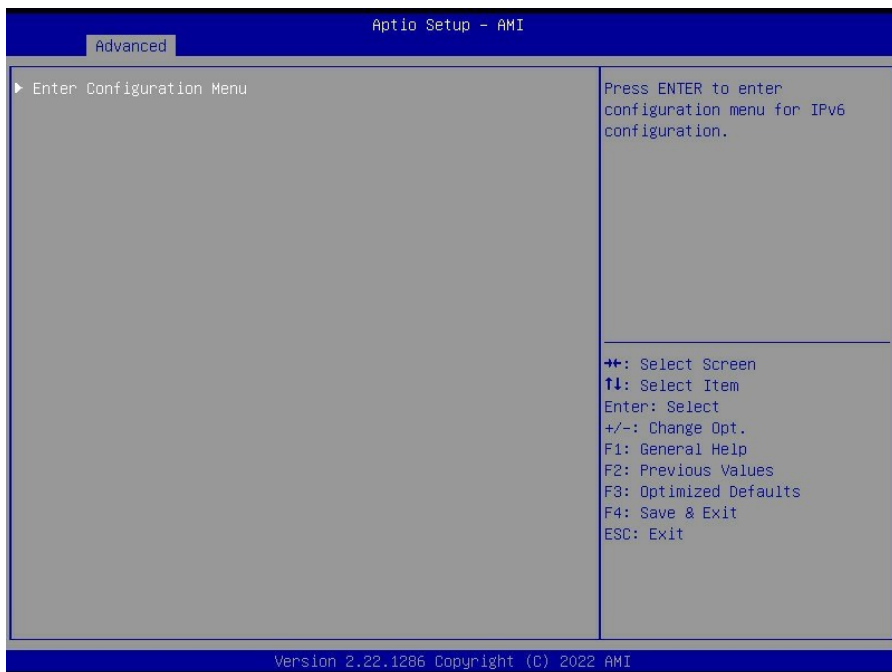
Indicate whether network address configured sucessfully or not.

Enabled / **Disabled**

Save Changes and Exit

Save Changes and exit

3.3.30 MAC: A0423F4FA134-IPv6 Network Menu



Enter Configuration Menu

Press ENTER to enter configuration menu for IPv6 configuration.

3.3.30.1 Enter Configuration Menu

Aptio Setup - AMI		
Advanced		
Interface Name :	eth3	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3
Interface Type :	Ethernet	
MAC address :	A0-42-3F-4F-A1-35	
Host addresses :	FE80::A242:3FFF:FE4F:...	
Route Table :	FE80::/64 >>::	
Gateway addresses :		
DNS addresses :		
Interface ID :	A2:42:3F:FF:FE:4F:A1:35	
DAD Transmit Count :	1	
Policy :	[automatic]	
Save Changes and Exit		↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

Interface ID

The 64 bit alternative interface ID for the device. The string is colon separated. E.g. ff:dd:88:66:cc:1:2:3

DAD Transmit Count

The number of consecutive Neighbor Solicitation message sent while performing duplicate address detection on a tentative address. A value of zero indicates that duplicate address detection is not performed.

1

Policy

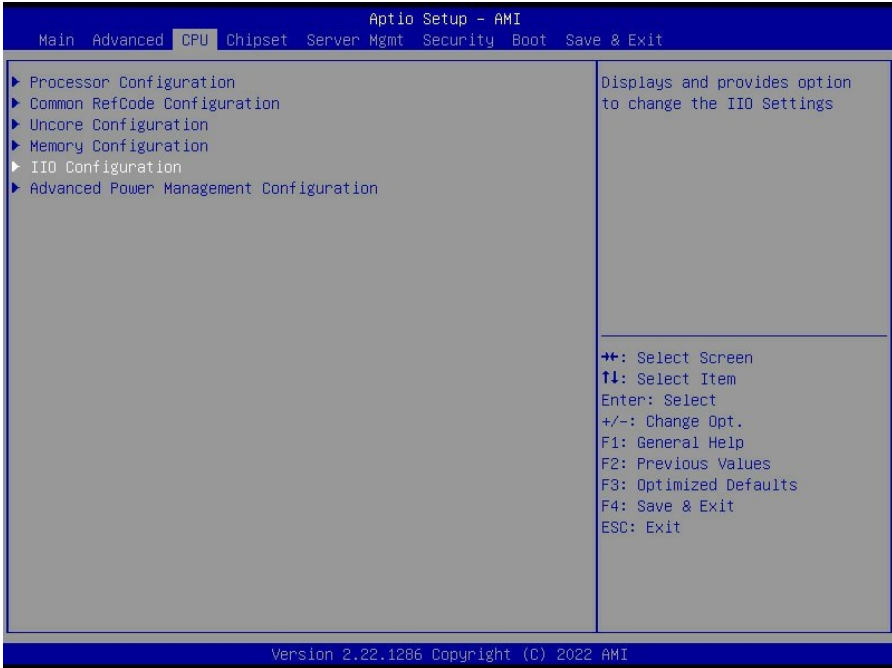
Automatic or manual

Automatic / manual

Save Changes and Exit

Save Changes for interface ID, DAD transmit count, policy, and data in advanced configuration.

3.4 CPU Configuration Subsystem



Processor Configuration

Displays and provides option to change the Processor Settings.

Common RefCode Configuration

Displays and provides option to change the Common RefCode Settings.

Uncore Configuration

Displays and provides option to change the Uncore Settings

Memory Configuration

Displays and provides option to change the Memory Settings.

IIO Configuration

Displays and provides option to change the IIO Settings.

Advanced Power Management Configuration

Displays and provides option to change the Power Management Settings.

3.4.1 Processor Configuration

CPU		Aptio Setup - AMI
Processor Configuration		Enabledsd Logical processor (Software Method to Enabled/Disabled Logical Processor threads) (Hyper-Threading)
Processor BSP Revision	806F6 - Unknown	
Processor Socket	Socket 0	
Processor ID	000806F6*	
Processor Frequency	2.200GHz	
Processor Max Ratio	16H	
Processor Min Ratio	08H	
Microcode Revision	2B000021	
L1 Cache RAM(Per Core)	80KB	
L2 Cache RAM(Per Core)	2048KB	
L3 Cache RAM(Per Package)	99840KB	
Processor 0 Version	Intel(R) Xeon(R) Pla tinum 8461V	
Enabled LP [Global]	[ALL LPs]	↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Enabled Intel® TXT	[Disabled]	
Hardware Prefetcher	[Enabled]	
Adjacent Cache Prefetch	[Enabled]	
Extended APIC	[Disabled]	
AES-NI	[Enabled]	

Version 2.22.1286 Copyright (C) 2022 AMI

Enabled LP [Global]

Enabled sd Logical processor (software method to Enabled/Disabled logical processor threads) (Hyper-Threading).

ALL LPs / Single LP

Enable Intel® TXT

Enable Intel® TXT.

Disabled / Enabled

Hardware Prefetcher

=MLC Streamer Prefetcher (MSR 1A4h Bit [0]).

Disabled / **Enabled**

Adjacent Cache Prefetch

=MLC Spatial Prefetcher (MSR 1A4h Bit [1]).

Disabled / **Enabled**

Extended APIC

Enabled/Disabled extended APIC support

Note: This will Enabled VT-d automatically if x2APIC is Enabled.

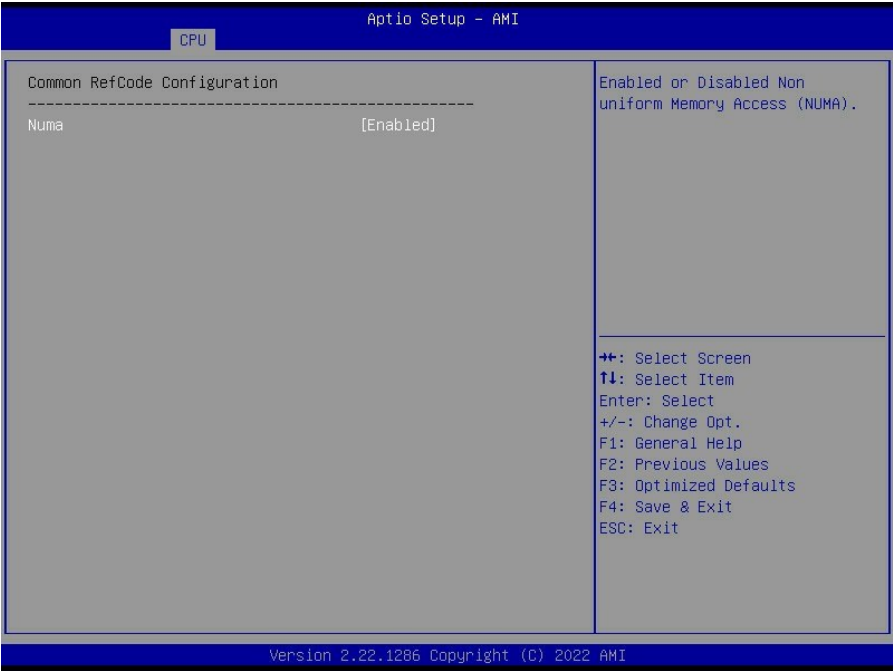
Disabled / Enabled

AES-NI

Enabled/Disabled AES-NI support.

Disabled / **Enabled**

6.4.2 Common RefCode Configuration



Numa

Enabled or Disabled Non uniform Memory Access(NUMA).

Disabled / **Enabled**

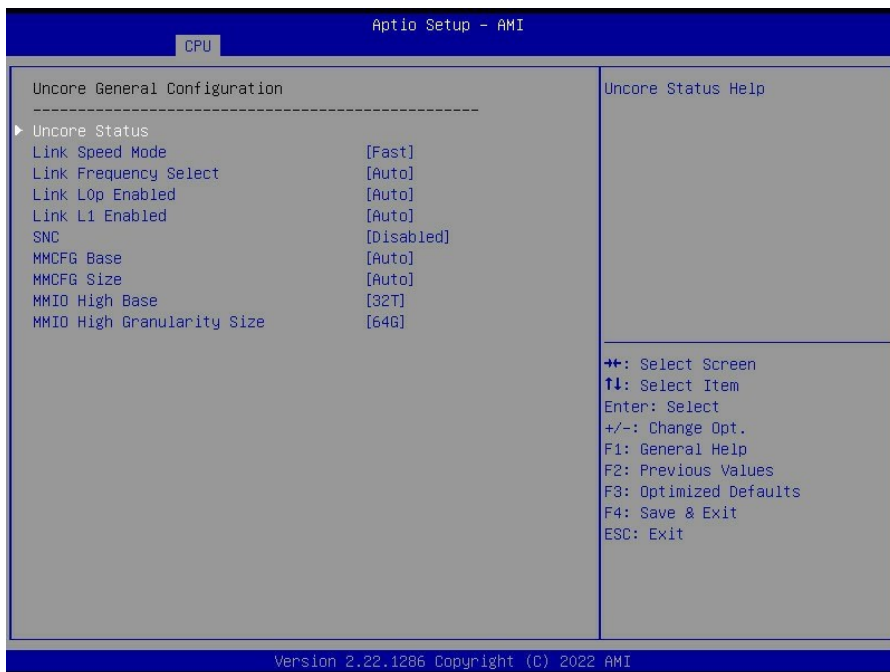
3.4.3 Uncore Configuration



Uncore General Configuration

Displays and provides option to change the uncore General settings.

3.4.3.1 Uncore General Configuration



Uncore Status

Uncore Status Help

Link Speed Mode

Select the UPI link speed as either the POR speed (fast) default speed (slow)

Slow / **Fast**

Link Frequency Select

Allows for selecting the UPI Link frequency

12.8GT/s / 14.4 GT/s / 16.0 GT/s / **Auto** / Use Per Link Setting

Link L0p Enabled

Enabled – Set the c_10p_en,

Disabled – Reset it,

Auto – Auto decides based on Si Compatibility.

Disabled / Enabled / **Auto**

Link L1 Enabled

Enabled – Set the c_l1_en,

Disabled – Reset it,

Auto – Auto decides based on Si Compatibility.

Disabled / Enabled / **Auto**

SNC

Disabled supports 1-cluster and 4-IMC way interleave. Enabled SNC2 supports 2-clusters SNC and 2- way IMC interleave. Enabled SNC4 supports 4-cluster and 1-IMC way interleave.

Disabled / Enabled SNC2 (2-clusters) / Enabled SNC4 (4-clusters)

MMCFG Base

Select MMCFG Base,

Auto – Auto decides based on Si Compatibility

1G / 1.5G / 1.75G / 2G / 2.25G / 3G / **Auto**

MMCFG Size

Select MMCFG Size,

Auto – Auto decides based on Si Compatibility.

64M / 128M / 256M / 512M / 1G / 2G / **Auto**

MMIO High Base

Select MMIO High Base

56T / 40T / **32T** / 24T / 16T / 4T / 2T / 1T / 512G / 3584T

MMIO High Granularity Size

Selects the allocation size used to assign mmioh resources. Total mmioh space can be up to 32x granularity. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.

1G / 4G / 16G / **64G** / 256G / 1024G

3.4.3.1.1 Uncore General Configuration



3.4.4 Memory Configuration



Memory Frequency

Maximum Memory Frequency Selections in MT/s. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.

Auto / 4000 / 4400 / 4800

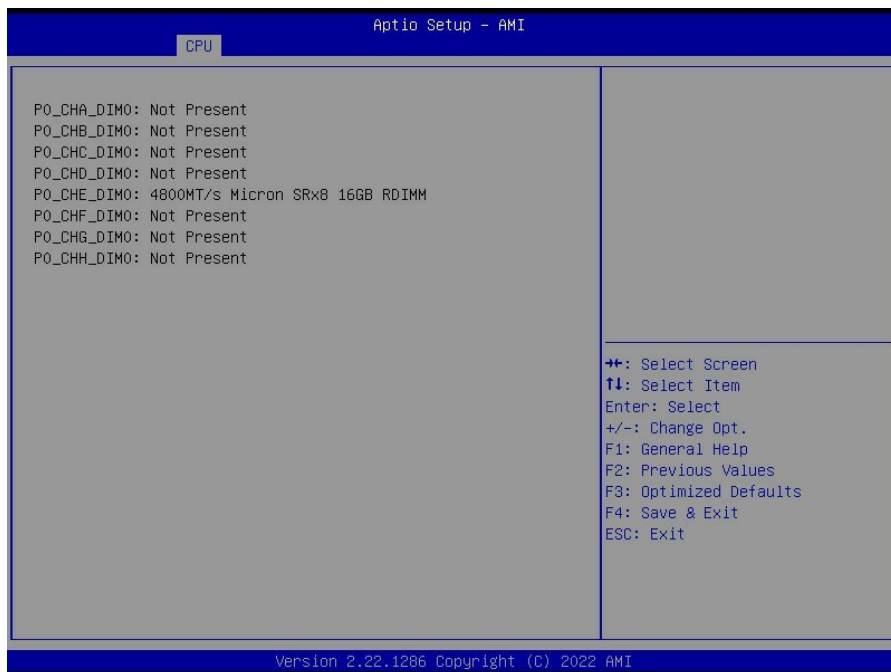
Memory Topology

Displays memory topology with Dimm population information

Memory RAS Configuration

Displays and provides option to change the Memory RAS Settings

3.4.4.1 Memory Topology



3.4.4.2 Memory RAS Configuration



Dynamic ECC Mode Selection

Enabled/Disabled Dynamic ECC Mode selection

Disabled / **Enabled**

Mirror Mode

Full Mirror mode will set entire 1LM memory in system to be mirrored , consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable.

Disabled / Enabled

Mirror TAD0

Enabled Mirror on entire memory for TAD0

Disabled / Enabled

Correctable Error Threshold

Correctable Error Threshold (1-32767) used for sparing, and leaky bucket.

10

Patrol Scrub

Enabled/Disabled Patrol Scrub

Disabled / **Enabled**

Patrol Scrub Interval

Enabled/Disabled Patrol Scrub

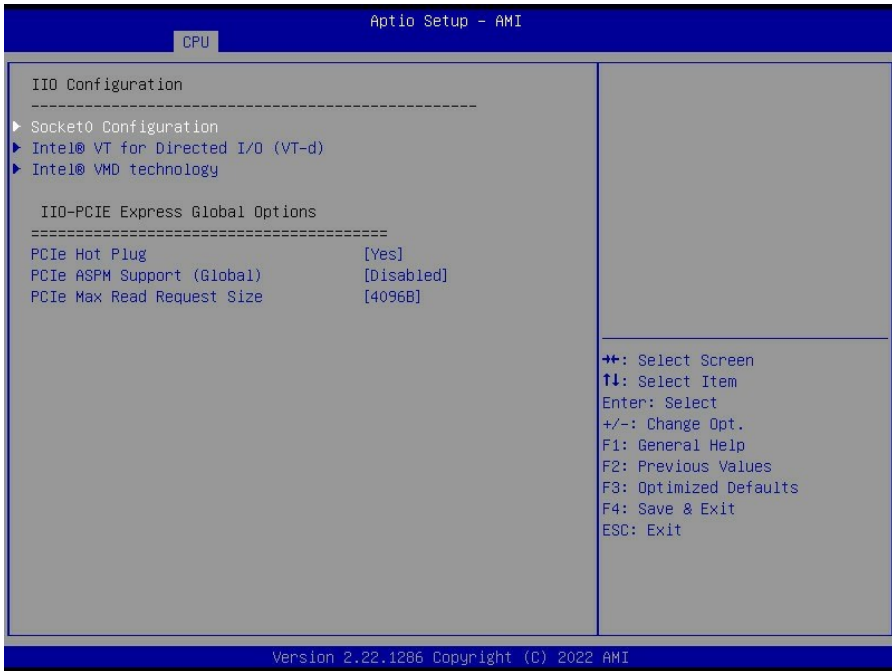
Disabled / **Enabled**

Patrol Scrub Interval

Select the number of hours (1-24) required to complete full scrub. A value of zero means auto!

24

3.4.5 IIO Configuration



Socket0 Configuration

Press <Enter> to bring up the Socket0 Configuration

Intel® VT for Directed I/O (VT-d)

Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.

Intel® VMD Technology

Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.

PCIe Hot Plug

Enabled/Disabled PCIe Hot Plug globally.

No / **Yes**

PCIe ASPM Support (Global)

This option can disable ASPM support in all PCIe root ports.

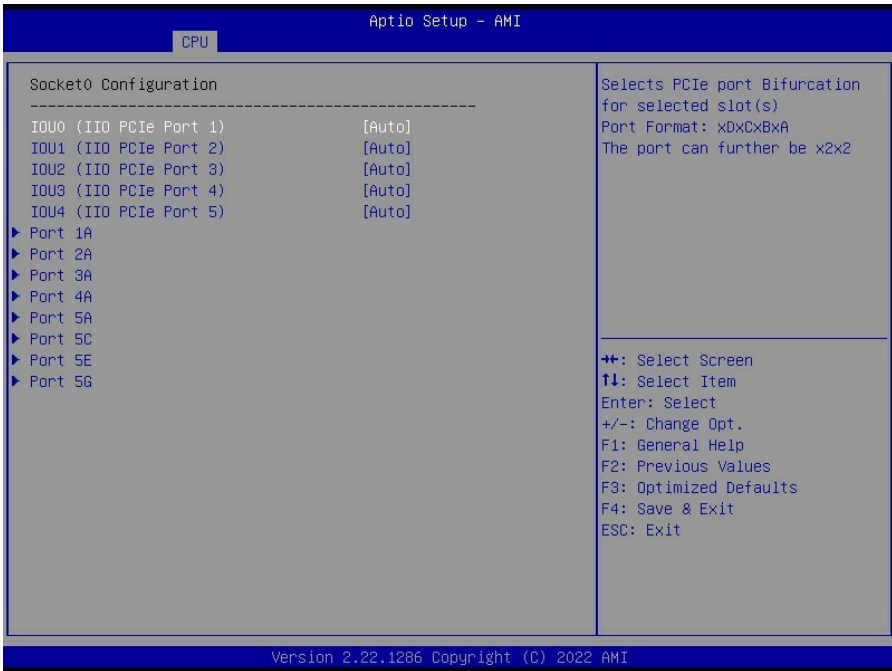
Disabled / Per Port

PCIe Max Read Request Size

This option can set requested Max Read Request Size in PCI Hierarchy. 'Default' keeps hardware default.

Auto / 128B / 256B / 512B / 1024B / 2048B / **4096B**

3.4.5.1 Socket0 Configuration



IOU0 (IIO PCIe Port 1)

Selects PCIe port Bifurcation for selected slot(s)

Port Format:xDxCxBxA.

The port can further be x2x2

Auto / x4x4x4x4 / x4x4_x8 / x_x8x4x4 / x_x8x_x8 / x_x_x_x16

IOU1 (IIO PCIe Port 2)

Selects PCIe port Bifurcation for selected slot(s)

Port Format: xDxCxBxA.

The port can further be x2x2

Auto / x4x4x4x4 / x4x4_x8 / x_x8x4x4 / x_x8x_x8 / x_x_x_x16

IOU2 (IIO PCIe Port 3)

Selects PCIe port Bifurcation for selected slot(s)

Port Format: xDxCxBxA.

The port can further be x2x2

Auto / x4x4x4x4 / x4x4_x8 / x_x8x4x4 / x_x8x_x8 / x_x_x_x16

IOU3 (IIO PCIe Port 4)

Selects PCIe port Bifurcation for selected slot(s)

Port Format: xDxCxBxA.

The port can further be x2x2

Auto / x4x4x4x4 / x4x4_x8 / x_x8x4x4 / x_x8x_x8 / x_x_x_x16

IOU4 (IIO PCIe Port 5)

Selects PCIe port Bifurcation for selected slot(s).

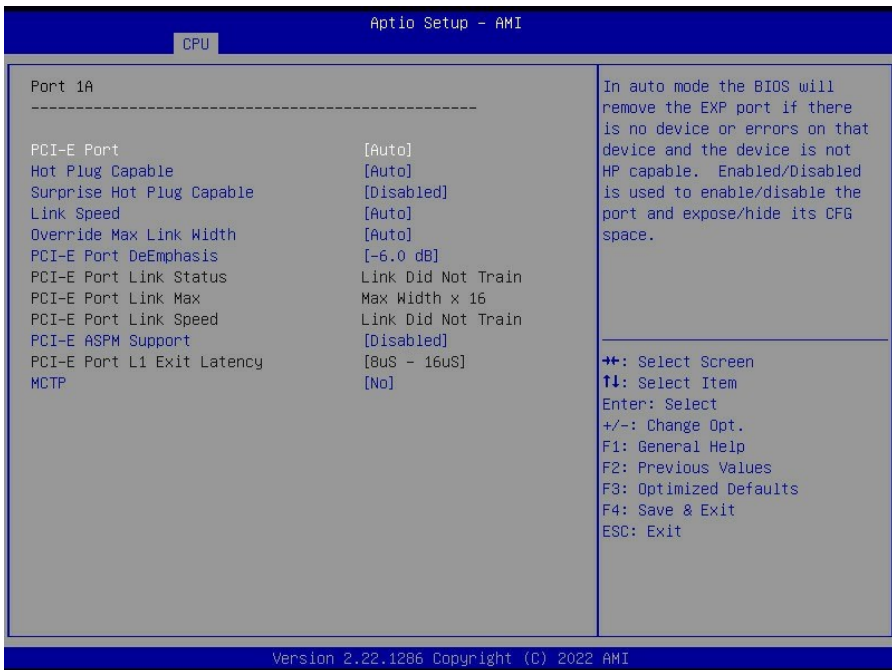
Auto / x4x4x4x4 / x4x4_x8 / x_x8x4x4 / x_x8x_x8 / x_x_x_x16

Port 1A/2A/3A/4A/5A/5C/5E/5G

Settings related to PCI Express Ports

(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).

3.4.5.1.1 Port 1A/2A/3A/4A/5A/5C/5E/5G



PCI-E Port

In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enabled/Disabled is used to enable/disable the port and expose/hide its CFG space.

Auto / No / Yes

Hot Plug Capable

This option specifies if the link is considered Hot Plug capable.

Auto / Disabled / Enabled

Surprise Hot Plug Capable

This option specifies if the link is considered Hot Plug capable.

Disabled / Enabled

Link Speed

Choose Link Speed for this PCIe port.

Auto / Gen1 (2.5 GT/s) / Gen2 (5 GT/s) / Gen3 (8 GT/s) / Gen4 (16 GT/s) / Gen 5 (32 GT/s)

Override Max Link Width

Override the max link width that was set by bifurcation.

Auto / x1 / x2 / x4 / x8 / x16

PCI-E Port DeEmphasis

De-Emphasis control (LNKCON2[6]) for this PCIe port.

-6.0 dB / -3.5 dB

PCI-E ASPM Support

This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.

Disabled / Auto

Hide Port?

User can force to hide this root port from OS.

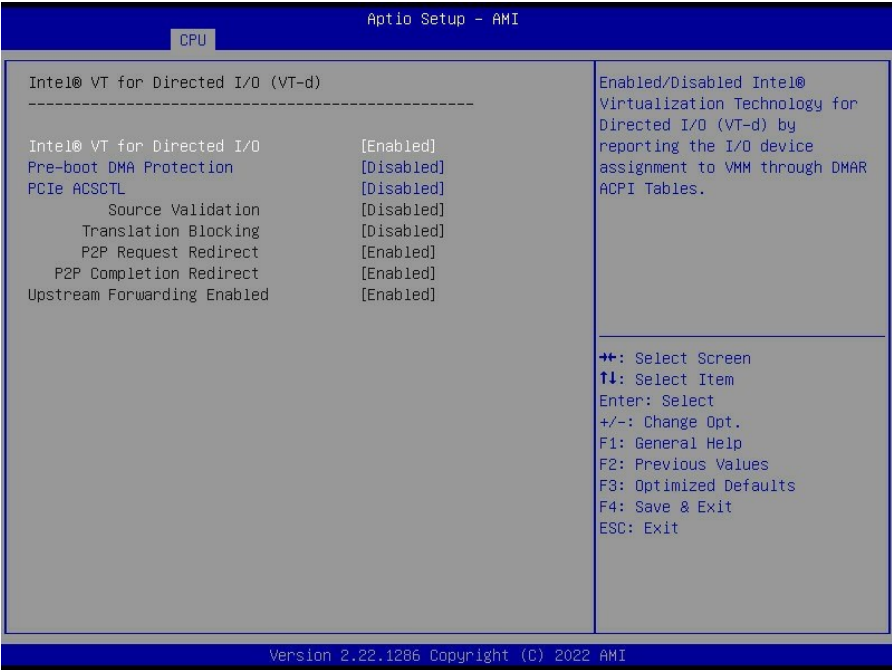
no / yes

MCTP

Enabled/Disabled MCTP

No / Yes

3.4.5.2 Intel® VT for Directed I/O (VT-d)



Intel® VT for Directed I/O

Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.

Enabled / Disabled

Pre-boot DMA Protection

Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

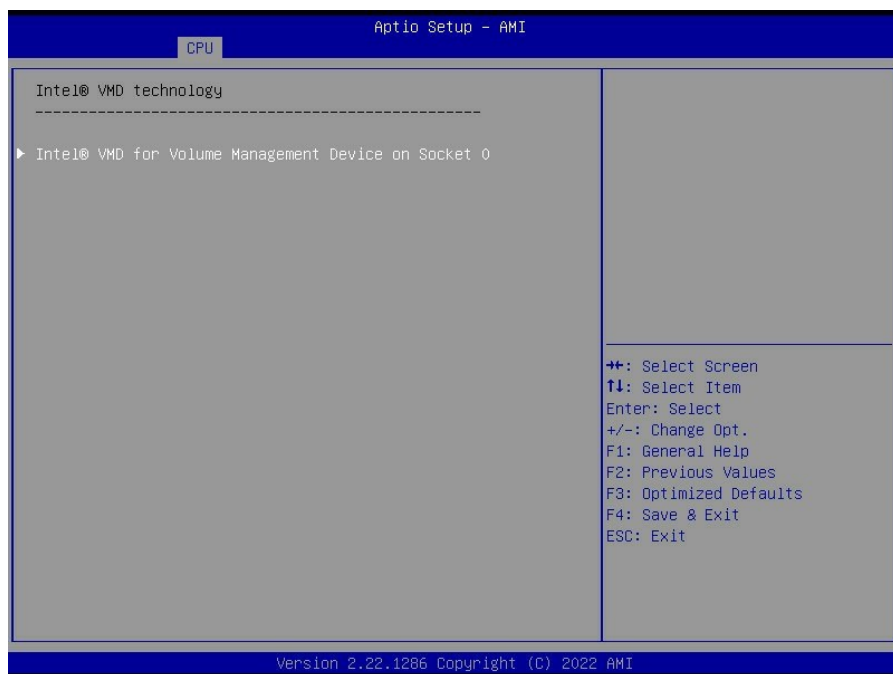
Enabled / **Disabled**

PCIe ACSCTL

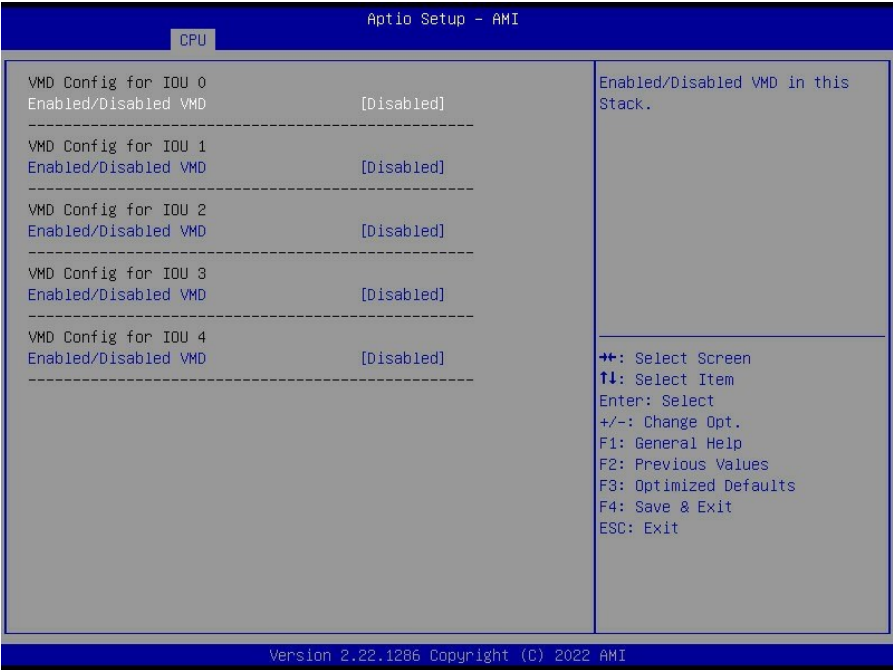
Enabled/Disabled overwrite of PCI Access Control Services Control register in PCI root ports.

Enabled / **Disabled**

3.4.5.3 Intel® VMD Technology



3.4.5.3.1 Intel VMD for Volume Management for Socket 0



VMD Config for IOU0

Enable/Disable VMD in this Stack.

Disabled / Enabled

VMD Config for IOU1

Enable/Disable VMD in this Stack.

Disabled / Enabled

VMD Config for IOU2

Enable/Disable VMD in this Stack.

Disabled / Enabled

VMD Config for IOU3

Enable/Disable VMD in this Stack.

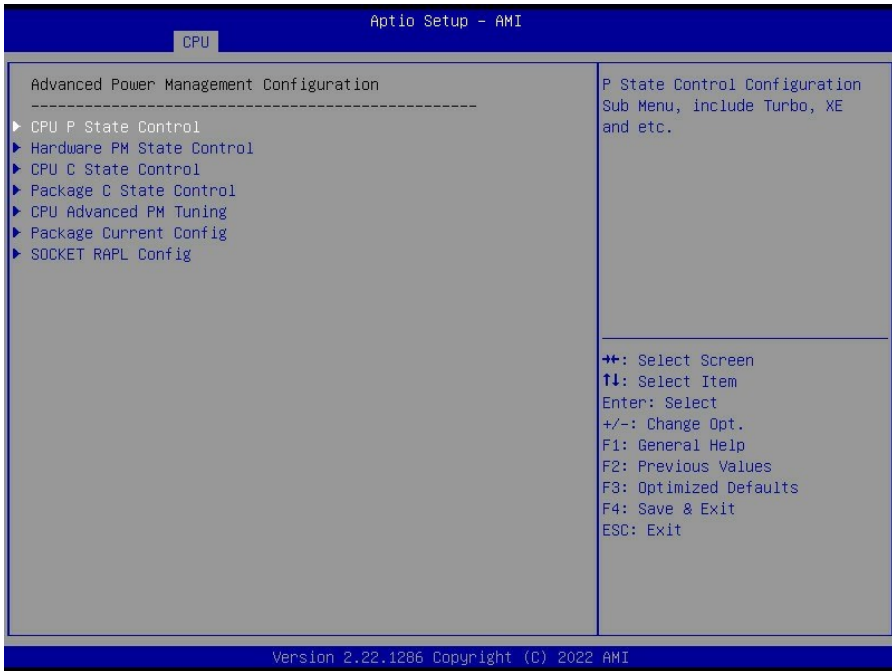
Disabled / Enabled

VMD Config for IOU4

Enable/Disable VMD in this Stack.

Disabled / Enabled

3.4.6 Advanced Power Management Configuration



CPU P State Control

P State Control Configuration Sub Menu, include Turbo, XE and etc.

Hardware PM State Control

Hardware P-State setting

CPU C State Control

CPU C State setting.

Package C State Control

Package C State setting

CPU Advanced PM Tuning

Setting Energy Per Bias, Pwr_Ctl, PP0 Current SWLTD, SAPM etc

Package Current Config

Program

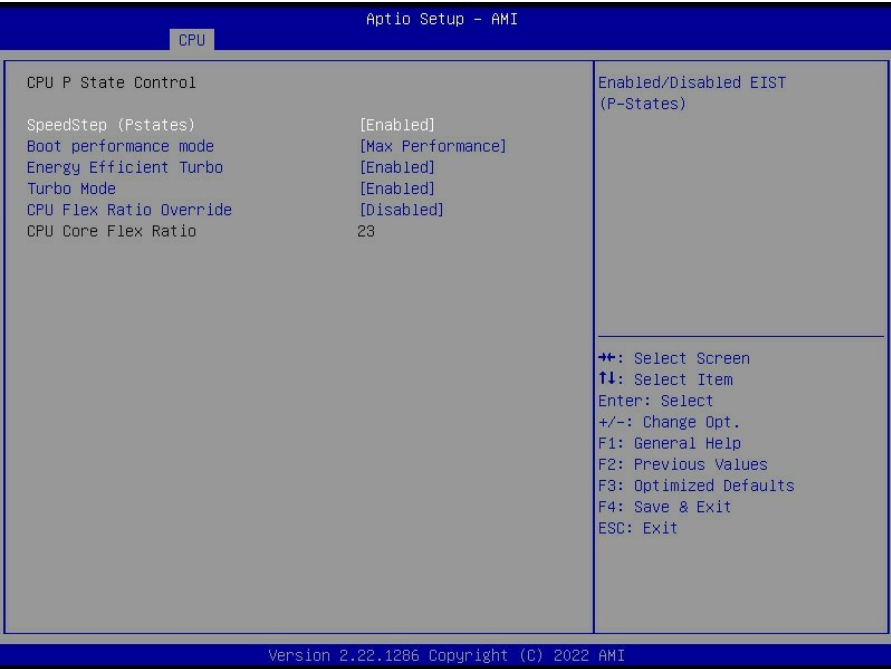
PRI_PLANE_CURT_CFG_CTRI_MSR

0x601 Sub Menu

SOCKET RAPL Config

SOCKET RAPL Configuration Sub Menu – TURBO_POWER_LIMIT CSR & MSR

3.4.6.1 CPU P State Control Configuration



SpeedStep (Pstates)

Enable/Disable EIST (P-States).

Disabled / **Enabled**

Boot performance mode

Select the performance state that the BIOS will set before OS hand off.

Max Performance / Max Efficient / Set by Intel Node Manager

Energy Efficient Turbo

Energy Efficient Turbo Disable, MSR 0x1FC [19].

Enabled / Disabled

Turbo Mode

Enable/Disable processor Turbo Mode (requires EMTTM enabled too).

Disabled / **Enabled**

CPU Flex Ratio Override

Enable/Disable CPU Flex Ratio Programming

Disabled / Enabled

3.4.6.2 Hardware PM State Control



Hardware P-States

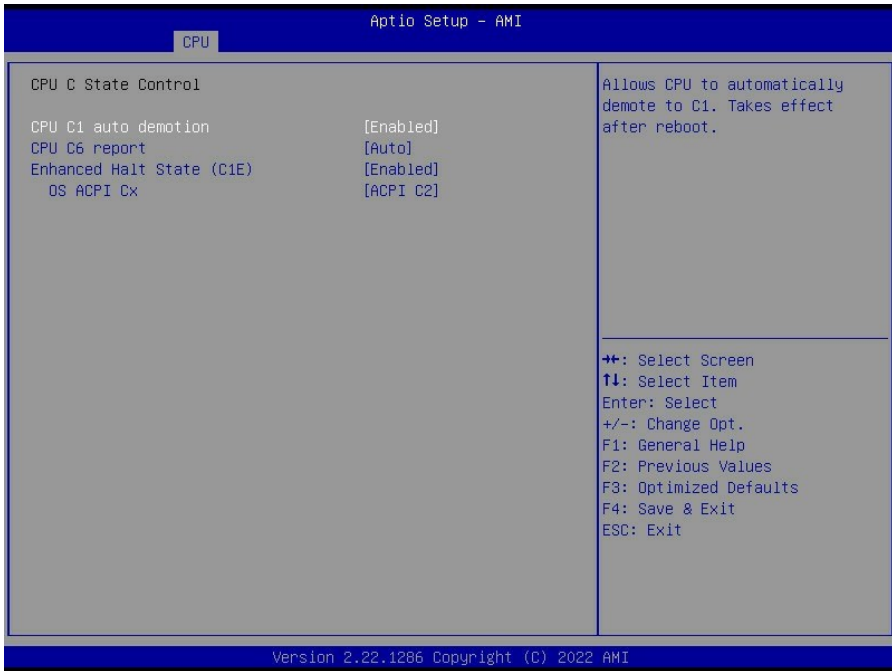
Disabled: Hardware choose a P-state based on OS Request (Legacy P-States)

Native Mode: Hardware choose a P-state based on OS guidance

Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance)

Disabled / **Native Mode** / Out of Band Mode / Native Mode with No Legacy Support

3.4.6.3 CPU C State Control



CPU C1 auto demotion

Allows CPU to automatically demote to C1. Takes effect after reboot.

Disabled / **Enabled**

CPU C6 report

Enable/Disable CPU C6 (ACPI C3) report to OS.

Disabled / Enabled / **Auto**

Enhanced Halt State (C1E)

Core C1E auto promotion Control. Take effect after reboot.

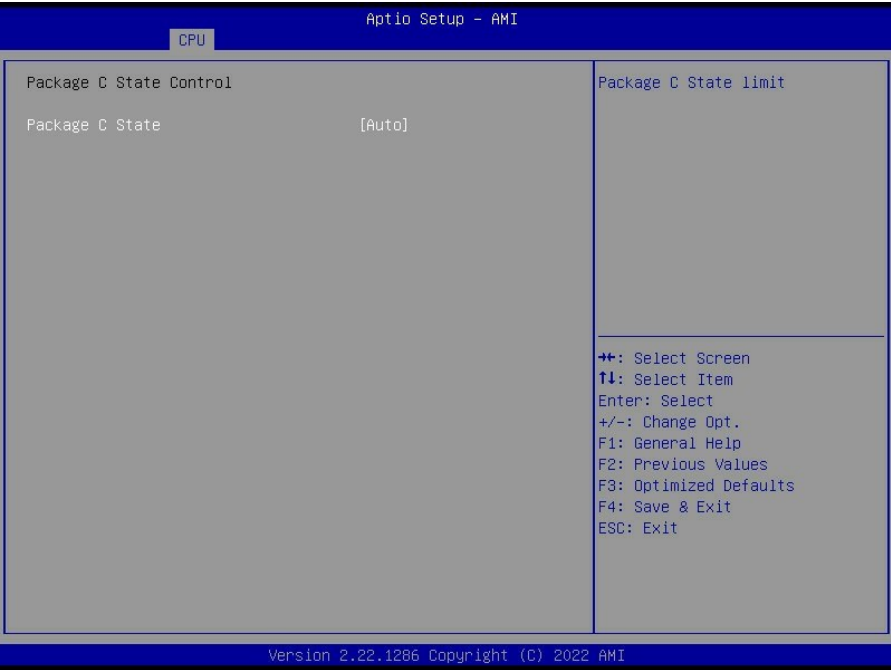
Disabled / **Enabled**

OS ACPI Cx

Report CC3/CC6 to OS ACPI C2 or ACPI C3

ACPI C2 / ACPI C3

3.4.6.4 Package C State Control



Package C State

Package C State limit

C0/C1 state / C2 state / C6(non Retention) state / C6(Retention) state / No
Limit / **Auto**

3.4.6.5 CPU Advanced PM Tuning



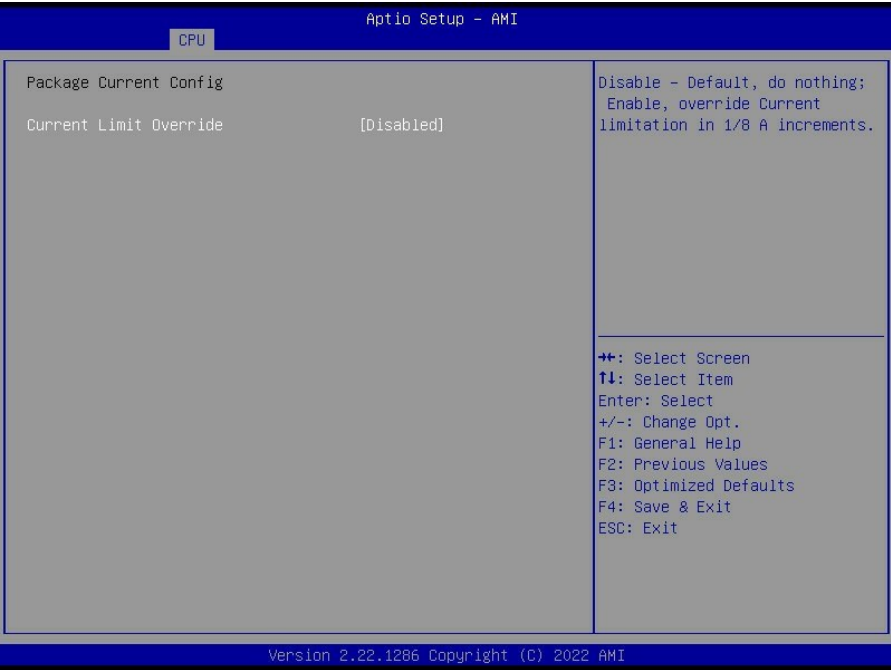
Power Performance Tuning

Options decide who Controls EPB. In OS mode: IA32_ENERGY_PERF_BIAS is used In BIOS mode:

ENERGY_PERF_BIAS_CONFIG is used In PECI mode: PCS53 is used

OS Controls EPB / BIOS Controls EPB / PECI Controls EPB

3.4.6.6 Package Current Config



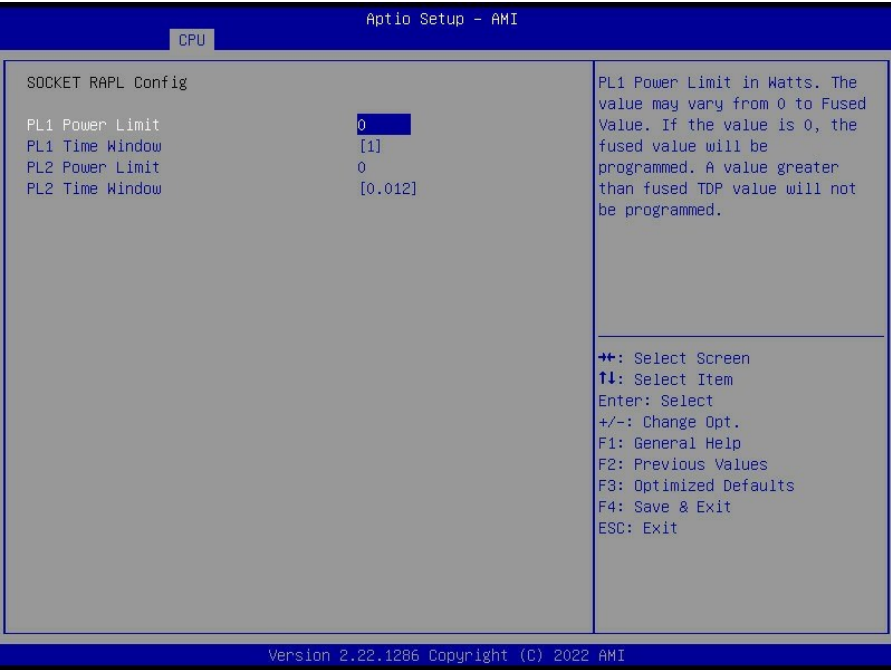
Current Limit Override

Disable – Default, do nothing;

Enable, override Current limitation in 1/8 A increments.

Disabled / Enabled

3.4.6.7 SOCKET RAPL Configuration



PL1 Power Limit

PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.

0

PL1 Time Window

PL1 value in seconds. The value may vary from 0 to 448. Indicates the time window over which TDP value should be maintained.

1

PL2 Power Limit

PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 120%*TDP

0

PL2 Time Window

PL2 value in seconds. The value may vary from 0 to 438. Indicates the time window over which TDP value should be maintained.

0.001 / 0.0012 / 0.0015 / 0.0017 / 0.002 / 0.0024 / 0.003 / 0.0034 / 0.004 / 0.005 / 0.006 / 0.007 / 0.008 / 0.01 / 0.012 / 0.014 / 0.016 / 0.02 / 0.023

3.5 Chipset Menu



PCH-IO Configuration

PCH Parameters

Server ME Configuration

Configure Server ME Technology Parameters

3.5.1 PCH-IO Configuration



PCI Express Configuration

PCI Express Configuration settings

SATA And RST Configuration

Device Options Settings

Deep Sx Configuration

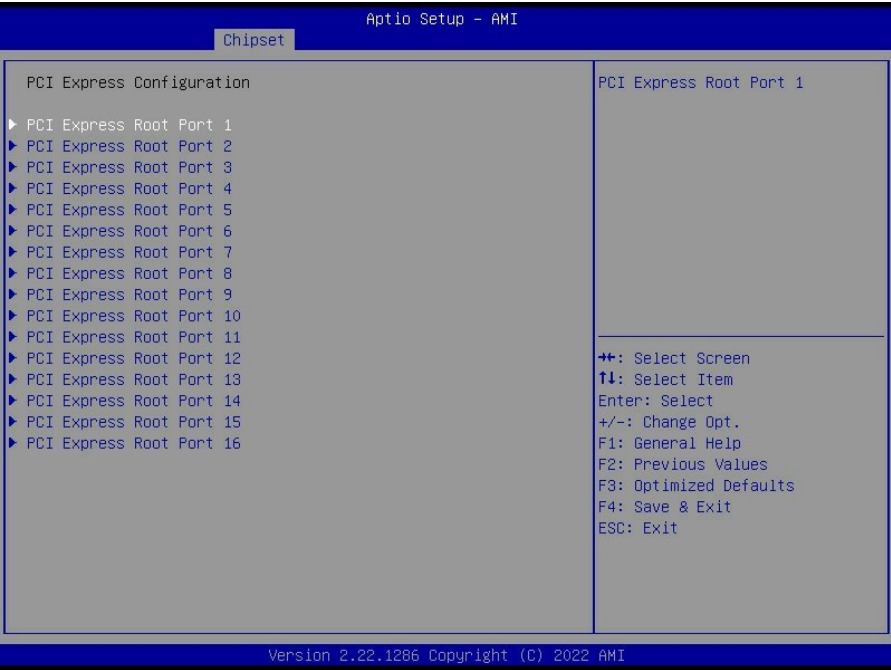
Deep Sx Option Settings

Restore AC Power Loss

Specify what state to go to when power is re-applied after a power failure (G3 state).

Power On / Power Off / **Last State**

3.5.1.1 PCI Express Configuration



PCI Express Root Port 1~16

3.5.1.1.1 PCI Express Root Configuration1~16



PCI Express Root Port 1

Control the PCI Express Root Port.

Disabled / **Enabled**

ASPM

PCI Express Active State Power Management Settings.

Disabled / L1

L1 Substates

PCI Express L1 Substates settings.

Disabled / L1.1 / L1.2 / L1.1 & L1.2

PCIe Speed

Configure PCIe Speed

Auto / Gen1 / Gen2 / Gen3

Max Payload Size

Set Maximum TLP payload size

128 bytes / 256 bytes

3.5.1.2 SATA And RST Configuration



Controller 0 SATA And RST Configuration

SATA Controller 0 Device Options Settings

Controller 1 SATA And RST Configuration

SATA Controller 1 Device Options Settings

3.5.1.2.1 Controller 0 SATA And RST Configuration



SATA Controller(S)

Enabled/Disabled SATA Device.

Enabled / Disabled

SATA Mode Selection

Determines how SATA controllers operate.

AHCI / RAID

Port 4

Enabled or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

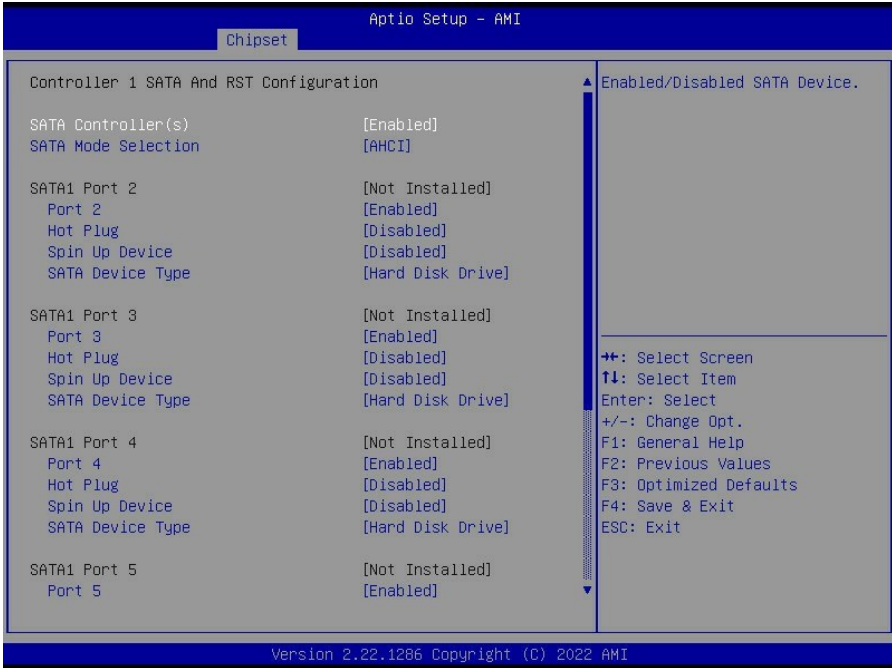
If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
Hard Disk Drive / Solid State Drive

3.5.1.2.2 Controller 1 SATA And RST Configuration



SATA Controller(s)

Enabled/Disabled SATA Device.

Enabled / Disabled

SATA Mode Selection

Determines how SATA controllers operate.

AHCI / RAID

SATA1 Port 2

Port 2

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

SATA1 Port 3

Port 3

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

SATA1 Port 4

Port 4

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

SATA1 Port 5

Port 5

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

SATA1 Port 6

Port 6

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

SATA1 Port 7

Port 7

Enable or Disabled SATA Port

Enabled / Disabled

Hot Plug

Designates this port as Hot Pluggable.

Enabled / **Disabled**

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enabled / **Disabled**

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive / Solid State Drive

3.5.1.3 Deep Sx Configuration

Aptio Setup - AMI	
Chipset	
Deep Sx Configuration	
DeepSx Power Policies	[Disabled]
Platform Deep S5 Mode	[Hardware]
Platform Deep S5 Delay Time	[3s]
configure the DeepSx Mode configuration.	
 ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1286 Copyright (C) 2022 AMI	

DeepSx Power Policies

Configure the DeepSx Mode configuration.

Disabled / Enabled in S5 / Enabled in S4-S5 / Enabled in S3-S4-S5

NOTE: When the DeepSx Power Policies is set to **Enabled in S5/S4-S5/S3-S4-S5**, the following items will be available to set up.

Platform Deep S5 Mode

Enabled – Enabled Platform Deep S5 mode,

Disable – Disable Platform Deep S5 mode,

Hardware– No support Platform Deep S5 mode

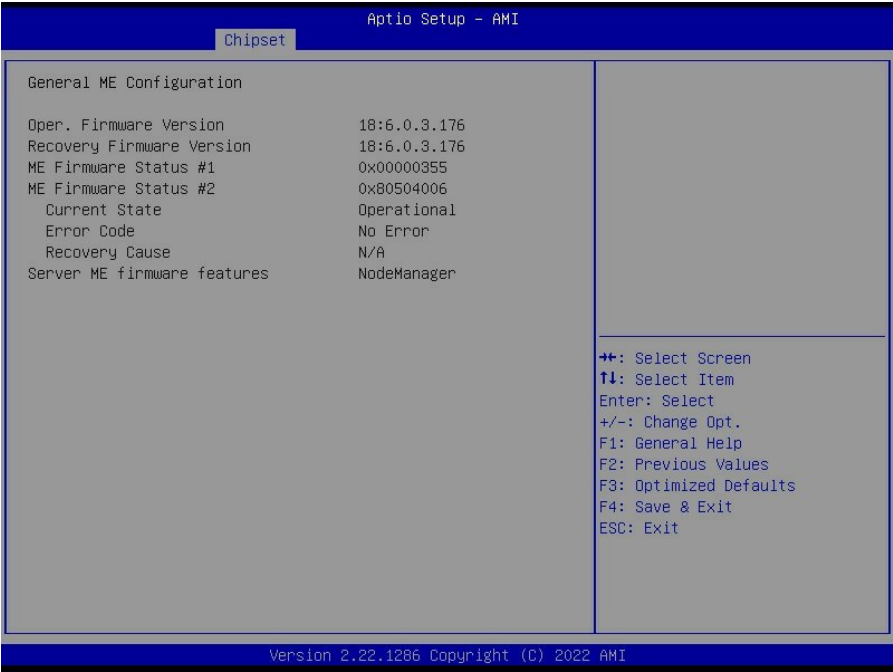
Disabled / Enabled / **Hardware**

Platform Deep S5 Delay Time

Delay (0/3/6/10) seconds to enter deep S5 state

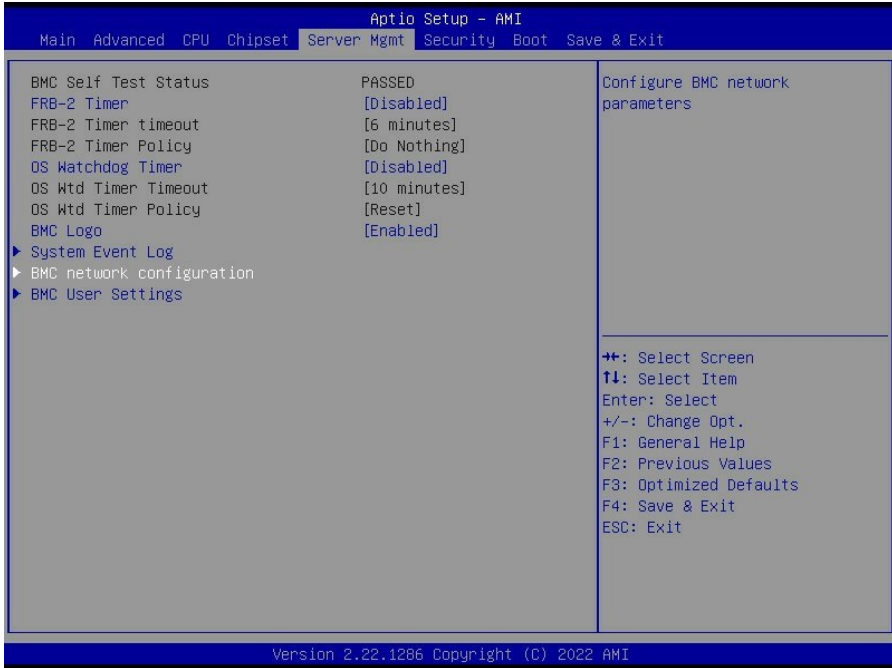
0S/**3S**/6S/10S

3.5.2 Server ME Configuration



Only Read

3.6 Server Management



FRB-2 Timer

Enable or Disable FRB-2 timer (POST timer).

Enabled / **Disabled**

NOTE: When FRB-2 Timer was set to **Enabled**, the following 3 items will be available.

FRB-2 Timer timeout

Enter value Between 3 to 6 min for FRB-2 Timer Expiration value.

3 minutes / 4 minutes / 5 minutes / **6 minutes** / 12 minutes

FRB-2 Timer Policy

Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.

Do Nothing / Reset / Power Down / Power Cycle

OS Watchdog Timer

If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.

Enabled / **Disabled**

NOTE: When OS Watchdog Timer was set to **Enabled**, the following 2 items will be available.

OS Wtd Timer timeout

Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog timer is disabled.

5 minutes / **10 minutes** / 15 minutes / 20 minutes

OS Wtd Timer Policy

Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog timer is disabled.

Do Nothing / **Reset** / Power Down / Power Cycle

BMC Logo

Enable or Disable BMC Logo

Disabled / **Enabled**

System Event Log

Press<Enter> to change the SEL event log configuration.

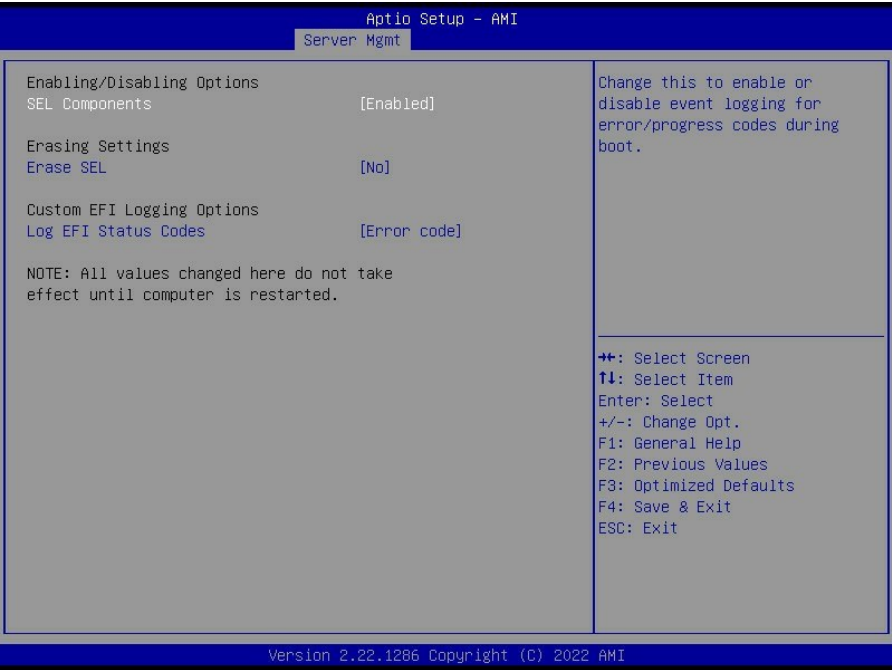
BMC network configuration

Configure BMC network parameters

BMC User Settings

Press<Enter> to Add, Delete and Set Privilege level for user.

3.6.1 System Event Log Configuration



SEL Components

Change this to enable or disable event logging for error/progress codes during boot.

Disabled / **Enabled**

Erase SEL

Choose options for erasing SEL.

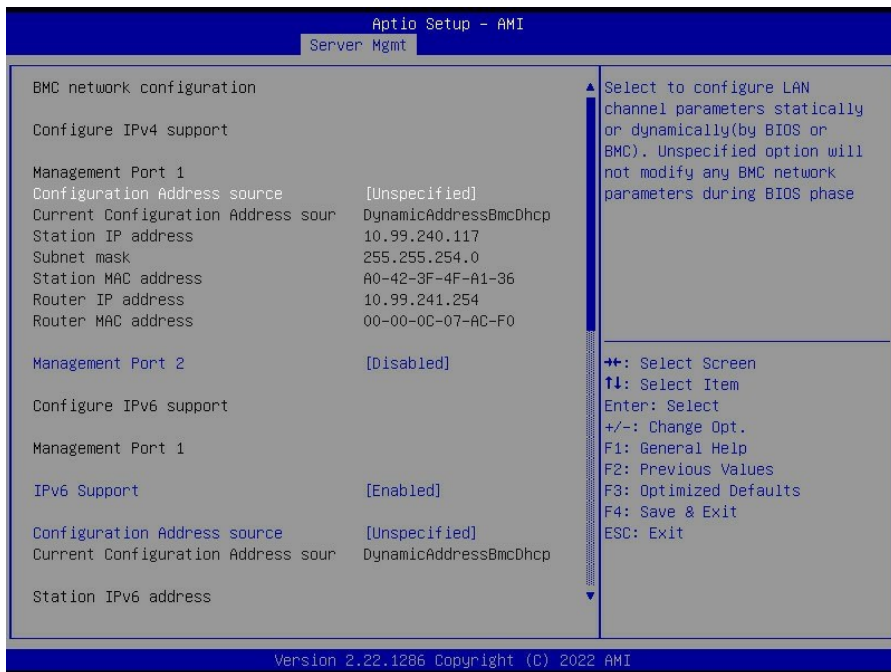
No / Yes, On next reset / Yes, On every reset

Log EFI Status Codes

Disable the logging of EFI Status Codes or log only error code or only progress code or both.

Disabled / Both / **Error code** / Progress code

3.6.2 BMC Network Configuration



Configure IPV4 Support

Management Port 1

Configuration Address Source

Select the configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.

Unspecified / Static / DynamicBmcDhcp / DynamicBmcNonDhcp

Management Port 2

Enable/Disable BMC Share Nic.

Enabled / **Disabled**

Configure IPV6 Support

Server Management Port 1

IPV6 Support

Enable or Disable LAN1 IPV6 Support.

Enabled / Disabled

Configuration Address Source

Select the configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.

Unspecified / Static / DynamicBmcDhcp

Server Management Port 2

IPV6 Support

Enable or Disable LAN1 IPV6 Support.

Enabled / **Disabled**

IPv6 Support

Enable or Disable LAN2 IPv6 Support.

Enabled / Disabled

Configuration Address source

Enable or Disable LAN2 IPv6 Support.

Unspecified / Static / DynamicBmcDhcp

3.6.3 BMC User Setting Configuration



Add User

Press< Enter> to Add a User

Delete User

Press<Enter> to Delete a User

Change User Settings

Press<Enter> to Change User settings

3.6.3.1 BMC Add User Configuration

Main

Aptio Setup - AMI

BMC Add User Details

User Name

User Password

User Access

[Disabled]

Channel No

[N/A]

User Privilege Limit

[User]

Enter BMC User Name

↔: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous Values

F3: Optimized Defaults

F4: Save & Exit

ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

User Name
Enter BMC User Name

3.6.3.2 BMC Delete User Configuration

Main

Aptio Setup - AMI

BMC Delete User Details User Name User Password	Enter BMC User Name ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
--	--

Version 2.22.1286 Copyright (C) 2022 AMI

User Name

Enter BMC User Name

3.6.3.3 BMC Change User Configuration

Main

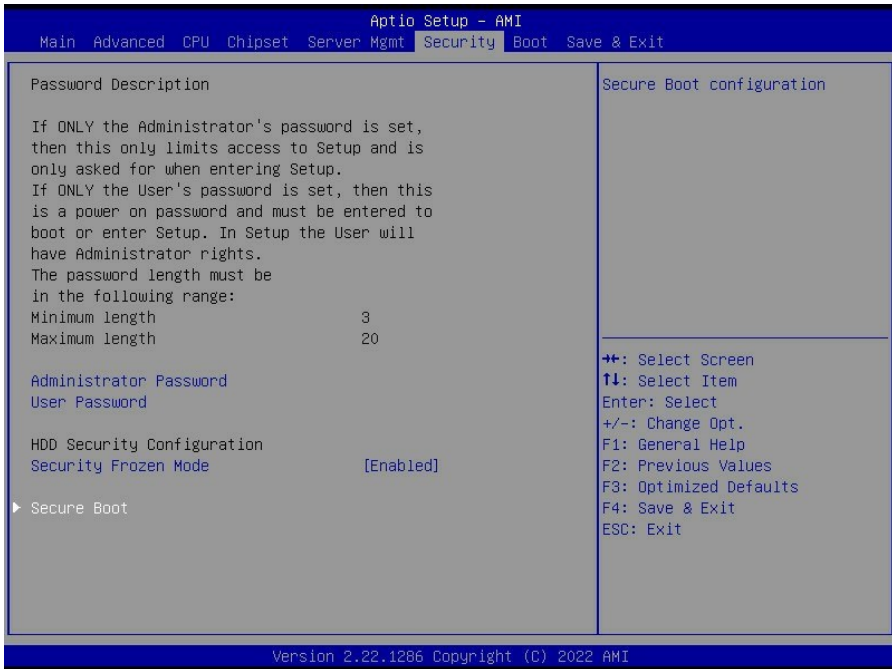
Aptio Setup - AMI

BMC Change User Settings User Name User Password Change User Password User Access Channel No User Privilege Limit [Disabled] [N/A] [None]	Enter BMC User Name ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
---	--

Version 2.22.1286 Copyright (C) 2022 AMI

User Name
Enter BMC User Name

3.7 Security



Password Description

Read only.

Administrator Password

Set administrator password in the **Create New Password** window. After you key in the password, the **Confirm New Password** window will pop out to ask for confirmation.

User Password

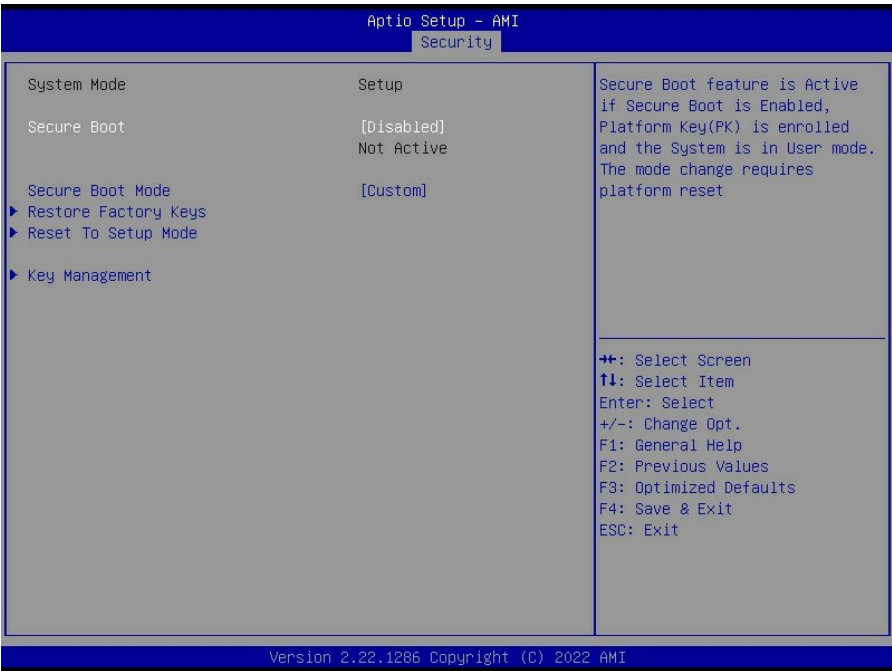
Set user password in the **Create New Password** window. After you key in the password, the **Confirm New Password** window will pop out to ask for confirmation.

Security Frozen Mode

Enable or disable HDD security freeze lock. Disable to support secure erase function. For AHCI SATA ports only.

Enabled / Disabled

3.7.1 Secure Boot



Secure Boot

Secure boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and System is in User mode. The mode change requires platform reset.

Disabled / Enabled

Secure Boot Mode

Secure Boot mode selector: Standard/Custom. In Custom mode Secure Boot Variables can be configured without authentication.

Standard / **Custom**

NOTE: When Secure Boot Mode was set to [Custom], the following items will be available to change.

Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot Key databases

Reset To Setup Mode

Delete all Secure Boot Key databases from NVRAM

Key Management

Enables expert users to modify Secure Boot Policy variables without full authentication.

3.7.1.1 Key Management



Factory keys Provision

Allow to provision factory default Secure Boot keys when System is in Setup Mode.

Disabled / Enabled

Restore Factory Keys

Force System to User Mode. Install Factory Default Secure Boot key databases.

Reset To Setup Mode

Delete all Secure Boot key database from NVRAM

Enroll Efi Image

Allow the image to run in Secure Boot mode. Enroll SHA256 has of the binary into Authorized signature Database (db).

Export Secure Boot variables

Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device

Platform Key (PK)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
 - a) EFI_SIGNATURE_LIST
 - b) EFI_CERT_X509 (DER)
 - c) EFI_CERT_RSA2048 (bin)
 - d) EFI_CERT_SHAXXX
 2. Authenticated UEFI Variable
 3. EFI PE/COFF Image (SHA256)
- Key source: Default, External, Mixed

Update

Key Exchange Keys

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate :
 - a) EFI_SIGNATURE_LIST
 - b) EFI_CERT_X509 (DER)
 - c) EFI_CERT_RSA2048 (bin)
 - d) EFI_CERT_SHAXXX
 2. Authenticated UEFI Variable
 3. EFI PE/COFF Image (SHA256)
- Key source: Default, External, Mixed

Update / Append

Authorized Signatures

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
 - a) EFI_SIGNATURE_LIST
 - b) EFI_CERT_X509 (DER)
 - c) EFI_CERT_RSA2048 (bin)
 - d) EFI_CERT_SHAXXX
 2. Authenticated UEFI Variable
 3. EFI PE/COFF Image (SHA256)
- Key source: Default, External, Mixed

Update / Append

Forbidden Signatures

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
 - a) EFI_SIGNATURE_LIST
 - b) EFI_CERT_X509 (DER)
 - c) EFI_CERT_RSA2048 (bin)
 - d) EFI_CERT_SHAXXX
 2. Authenticated UEFI Variable
 3. EFI PE/COFF Image (SHA256)
- Key source: Default, External, Mixed

Update / Append

Authorized TimeStamps

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image (SHA256)

Key source: Factory, External, Mixed

Update / Append

OsRecovery Signatures

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

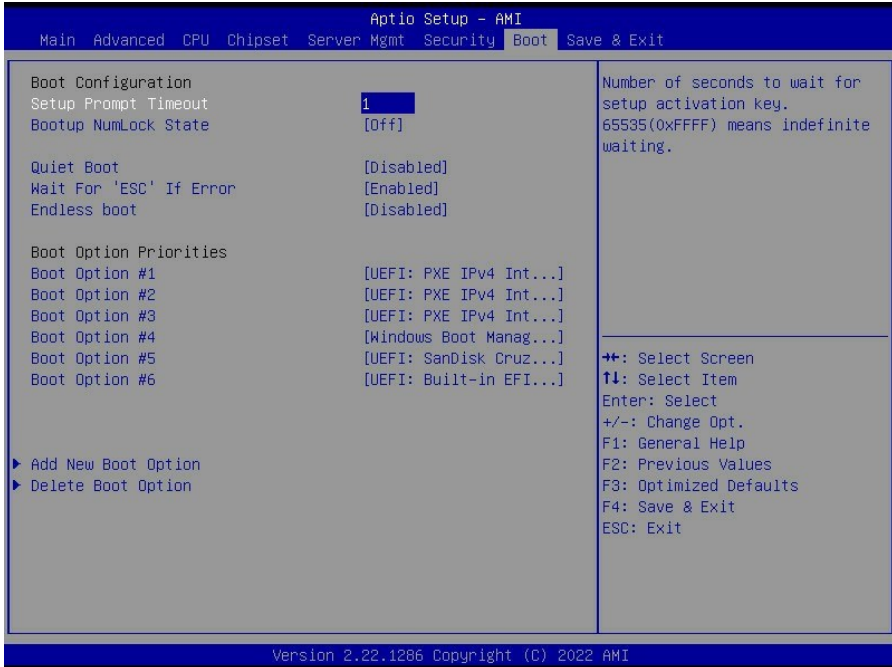
2. Authenticated UEFI Variable

3. EFI PE/COFF Image (SHA256)

Key source: Default, External, Mixed

Update / Append

3.8 Boot



Setup Prompt Timeout

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

1

Bootup NumLock State

Select the keyboard NumLock state.

Off / On

Quiet Boot

Enable or disable Quiet Boot option.

Disabled / Enabled

Wait for 'ESC' If Error

Wait for 'ESC' key to be pressed if error occurs.

Disabled / **Enabled**

Endless Boot

Enabled: BIOS try bootable devices constantly in loop until finding a bootable device (Excluding Built – in EFI Shell)

Disabled / Enabled

Boot Option Priorities

Boot Option #1~#6

Select the first/second boot device.

Device Name / Disabled

Add New Boot Option

Add a new EFI boot option to the boot order

Delete Boot Option

Remove an EFI boot option from the boot order

3.8.1 Add New Boot Management



Add boot option

Create new boot option

Path for boot option

Enter the path to the boot option in the format

Fs0:\path\filename.efi

Create

Create the newly formed boot option

3.8.2 Delete Boot Option

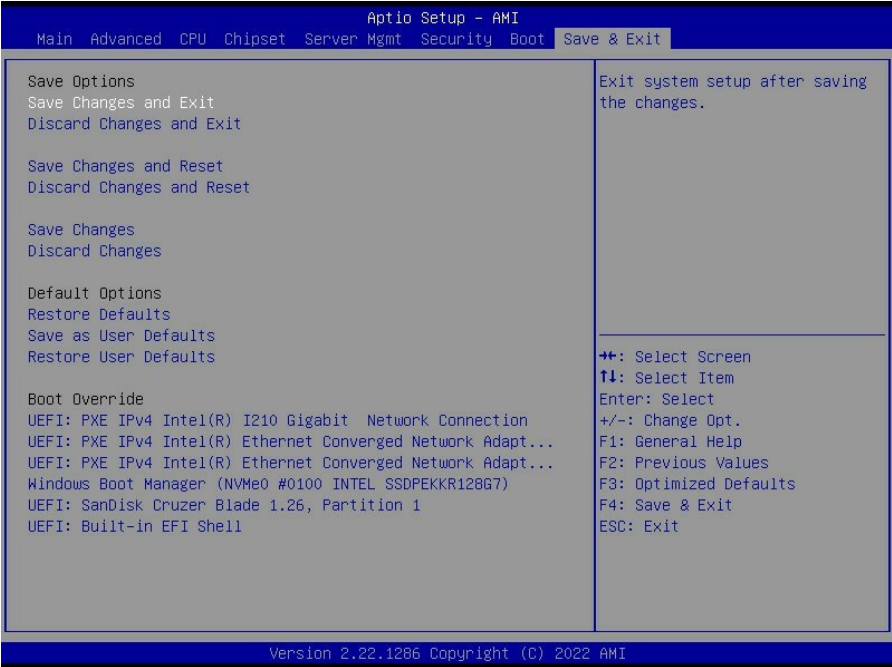


Delete Boot Option

Remove an EFI boot option from the boot order

Select one to Delete / Device Name

3.9 Save & Exit



Save Changes and Exit

Exit system setup after saving the changes.

Discard Changes and Exit

Exit system setup without saving any changes.

Save Changes and Reset

Reset the system after saving the changes.

Discard Changes and Reset

Reset system setup without saving any changes.

Save Changes

Save changes done so far to any of the setup options.

Discard Changes

Discard changes done so far to any of the setup options.

Restore Defaults

Restore/Load Default values for all the setup options.

Save as User Defaults

Save the changes done so far as User Defaults.

Restore User Defaults

Restore the User Defaults to all the setup options.

Boot Override

Read only.

Chapter 4: Diagnostics

NOTE: if you experience problems with setting up your system, always check the following things in the following order:

Memory, Video, CPU

By checking these items, you will most likely find out what the problem might have been when setting up your system. For more information on troubleshooting, check the TYAN website at <http://www.mitacomputing.com>.

4.1 Flash Utility

Every BIOS file is unique for the motherboard it was designed for. For Flash Utilities, BIOS downloads, and information on how to properly use the Flash Utility with your motherboard, please check the TYAN web site at <http://www.mitacomputing.com>

NOTE: Please be aware that by flashing your BIOS, you agree that in the event of a BIOS flash failure, you must contact your dealer for a replacement BIOS. There are no exceptions. TYAN does not have a policy for replacing BIOS chips directly with end users. In no event will TYAN be held responsible for damages done by the end user.

4.2 AMIBIOS Post Code (Aptio)

The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following table describes the type of checkpoints that may occur during the POST portion of the BIOS:

Checkpoint Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

Standard Checkpoints

SEC Phase

Status Code	Description
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not found

SEC Beep Codes

None

PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-Memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-Memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other)
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode(SMM) initialization
0x37	Post-Memory North Bridge initialization is started

Status Code	Description
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F – 0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU microcode is not found or microcode update is failed
0x5A	Internal CPU error
0x5B	Reset PPI is not available
0x5C – 0x5F	Reserved for future AMI error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4 – 0xE7	Reserved for future AMI progress codes
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC – 0xEF	Reserved for future AMI error codes

Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5 – 0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE initialization (South Bridge module specific)
0x74	South Bridge DXE initialization (South Bridge module specific)
0x75	South Bridge DXE initialization (South Bridge module specific)

Status Code	Description
0x76	South Bridge DXE initialization (South Bridge module specific)
0x77	South Bridge DXE initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller initialization
0x94	PCI Bus Enumeration
0x95	PCI BUS Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console Input devices connect
0x99	Super IO initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E -0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event

Status Code	Description
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

ACPI/ASL Checkpoints

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state

Status Code	Description
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

Appendix I: How to recover UEFI BIOS

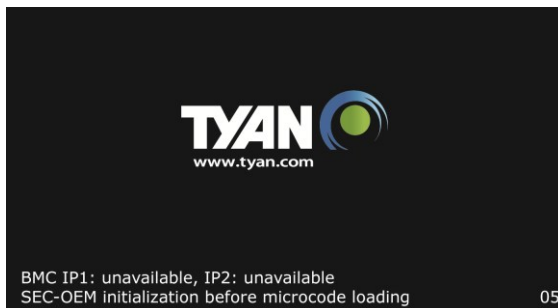
Important Notes:

The emergency UEFI BIOS Recovery process is only used to rescue a system with a failed or corrupted BIOS image that fails to boot to an OS. It is not intended to be used as a general purpose BIOS flashing procedure and should not be used as such. Please do not shutdown or reset the system while the BIOS recovery process is underway or there is risk of damage to the UEFI recovery bootloader that would prevent the recovery process itself from working. In no event shall Tyan be liable for direct, indirect, incidental, special or consequential damages arising from the BIOS update or recovery.

The BIOS Recovery file is named xxxx.cap, where the 'xxxx' portion is the motherboard model number. Examples: 5630.cap, 7106.cap, 7109.cap, etc. Please make sure that you are using the correct BIOS Recovery file from Tyan's web site.

BIOS Recovery Process

- 1.Place the recovery BIOS file (xxxx.cap) in the root directory of a USB disk.
- 2.Ensure that the system is powered off.
- 3.Insert the USB disk to any USB port on the motherboard or chassis.
- 4.Power the system on while pressing “Ctrl” and “Home” simultaneously on the keyboard. Continue to hold these keys down until the following Tyan screen is displayed on the monitor:



```

Apptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
Main Advanced Platform Configuration Socket Configuration Recovery >
-----
Please select blocks you want to update
Reset NVRAM [Enabled]
Boot Block Update [Enabled]
> Proceed with flash update

-----
|<: Select Screen
|v: Select Item
|Enter: Select
|+/-: Change Opt.
|F1: General Help
|F2: Previous Values
|F3: Optimized Defaults
|F4: Save & Exit
|ESC: Exit
-----
DXE-USB hot plug 2.19.1268. Copyright (C) 2017 American Megatrends, Inc. B4

```

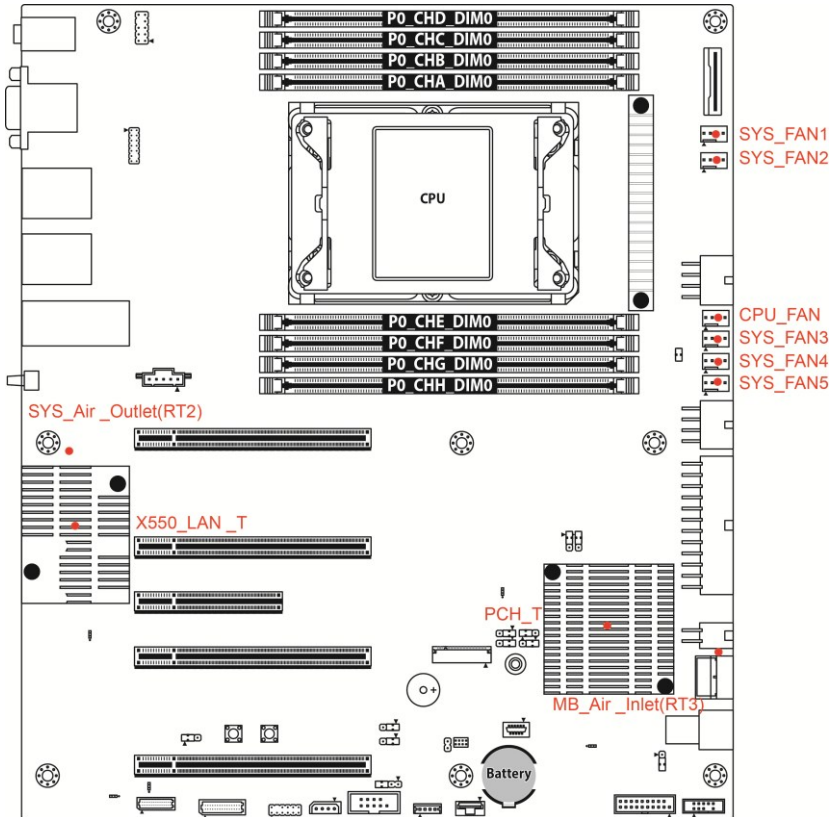
7.Wait for the BIOS recovery procedure to complete. Completion is signified with the message “Flash update completed. Press any key to reset the system” displayed on screen.

If your system does not have video output or the POST code halts at “FF” on the right-lower portion of the screen, please contact Tyan representatives for RMA service.

Appendix II: Fan and Temp Sensors

This section aims to help readers identify the locations of some specific FAN and Temp Sensors on the motherboard. A table of BIOS Temp sensor name explanation is also included for readers' reference.

Figure 1: Sensor Location



NOTE: The red spot indicates the sensor.

Fan and Temp Sensor Location:

1. Fan Sensor: It is located in the **third** pin of the fan connector, which detects the fan speed (rpm)
2. Temp Sensor: **SYS_Air_Outlet(RT2)** , **MB_Air_Inlet(RT3)** and **SYS_FAN1~5/CPU_FAN** etc. They detect the system temperature around.

NOTE: The system temperature is measured in a scale defined by **Intel**, not in Fahrenheit or Celsius.

BIOS Temp Sensor Name Explanation:

Advanced

Aptio Setup - AMI

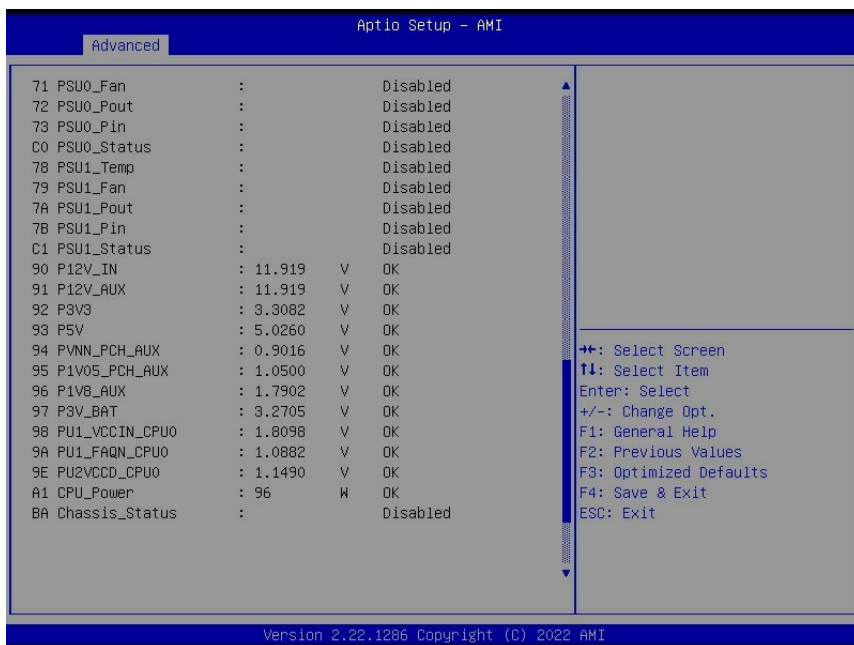
Pc Health Status

ID#	NAME	READING	UNIT	STATUS
01	P0_Temp	: 46	°C	OK
02	P0_DTS_Margin	: -49	°C	OK
05	P0_THRM_Margin	: -41	°C	OK
09	PCH_Temp	: 58	°C	OK
10	P0_CHA_DIMO	: N/A	°C	
11	P0_CHB_DIMO	: N/A	°C	
12	P0_CHC_DIMO	: N/A	°C	
13	P0_CHD_DIMO	: N/A	°C	
14	P0_CHE_DIMO	: 43	°C	OK
15	P0_CHF_DIMO	: N/A	°C	
16	P0_CHG_DIMO	: N/A	°C	
17	P0_CHH_DIMO	: N/A	°C	
20	P0_MOSFET1	: N/A	°C	
21	P0_MOSFET2	: N/A	°C	
22	P0_MOSFET3	: N/A	°C	
30	SYS_Air_Inlet	: N/A	°C	
32	SYS_Air_Outlet	: 46	°C	OK
34	MB_Air_Inlet	: 46	°C	OK
50	U.2_NVME_SSD_0	: N/A	°C	
51	U.2_NVME_SSD_1	: N/A	°C	
52	M.2_NVME_SSD_0	: N/A	°C	
5F	CPU_FAN	: 7560	RPM	OK

++: Select Screen
F1: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1286 Copyright (C) 2022 AMI

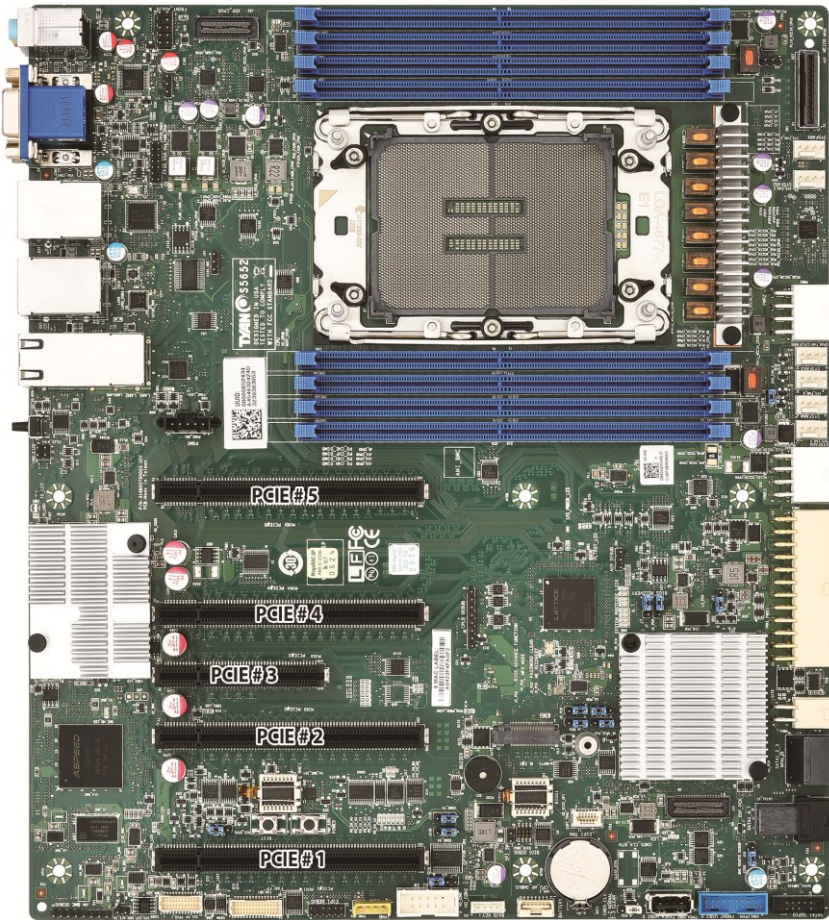
Advanced				Aptio Setup - AMI	
5F	CPU_FAN	: 7560	RPM	OK	↑ ++: Select Screen F1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
60	SYS_FAN_1	: N/A	RPM		
61	SYS_FAN_2	: N/A	RPM		
62	SYS_FAN_3	: N/A	RPM		
63	SYS_FAN_4	: N/A	RPM		
64	SYS_FAN_5	: N/A	RPM		
65	SYS_FAN_6	: N/A	RPM		
66	SYS_FAN_7	: N/A	RPM		
67	SYS_FAN_8	: N/A	RPM		
68	SYS_FAN_9	: N/A	RPM		
69	SYS_FAN_10	: N/A	RPM		
6A	SYS_FAN_11	: N/A	RPM		
6B	SYS_FAN_12	: N/A	RPM		
70	PSU0_Temp	:		Disabled	
71	PSU0_Fan	:		Disabled	
72	PSU0_Pout	:		Disabled	
73	PSU0_Pin	:		Disabled	
C0	PSU0_Status	:		Disabled	
78	PSU1_Temp	:		Disabled	
79	PSU1_Fan	:		Disabled	
7A	PSU1_Pout	:		Disabled	
7B	PSU1_Pin	:		Disabled	
C1	PSU1_Status	:		Disabled	
90	P12V_IN	: 11.919	V	OK	
91	P12V_AUX	: 11.919	V	OK	
Version 2.22.1286 Copyright (C) 2022 AMI					



BIOS Temp Sensor	Name Explanation
P0 Temp	P0 Temperature
PCH Temp	Temperature of PCH
P0_CHA_DIM0	Temperature of CPU0 DIMM Channel A
P0_CHB_DIM0	Temperature of CPU0 DIMM Channel B
P0_CHC_DIM0	Temperature of CPU0 DIMM Channel C
P0_CHD_DIM0	Temperature of CPU0 DIMM Channel D
P0_CHE_DIM0	Temperature of CPU0 DIMM Channel E
P0_CHF_DIM0	Temperature of CPU0 DIMM Channel F
P0_CHG_DIM0	Temperature of CPU0 DIMM Channel G
P0_CHH_DIM0	Temperature of CPU0 DIMM Channel H
SYS Air Inlet	Temperature of the System Air Inlet Area
SYS Air Outlet	Temperature of the System Air Outlet Area
U.2 NVME SSD 0	Temperature of the U.2 NVME SSD 0
U.2 NVME SSD 1	Temperature of the U.2 NVME SSD 1
M.2 NVME SSD 0	Temperature of the M.2 NVME SSD 0
CPU_FAN	Fan Speed of CPU_FAN
SYS_FAN_1	Fan Speed of SYS_FAN_1
SYS_FAN_2	Fan Speed of SYS_FAN_2
SYS_FAN_3	Fan Speed of SYS_FAN_3
SYS_FAN_4	Fan Speed of SYS_FAN_4
SYS_FAN_5	Fan Speed of SYS_FAN_5
SYS_FAN_6	Fan Speed of SYS_FAN_6
SYS_FAN_7	Fan Speed of SYS_FAN_7

SYS_FAN_8	Fan Speed of SYS_FAN_8
SYS_FAN_9	Fan Speed of SYS_FAN_9
SYS_FAN_10	Fan Speed of SYS_FAN_10
SYS_FAN_11	Fan Speed of SYS_FAN_11
SYS_FAN_12	Fan Speed of SYS_FAN_12
PSU0_Status	Current status of PSU0
PSU0_Temp	Temperature of PSU0
PSU0_FAN	Fan Speed of PSU0
PSU1_Status	Current status of PSU1
PSU1_Temp	Temperature of PSU1
PSU1_FAN	Fan Speed of PSU1

Appendix III: PCIe Bus Number



If PCIe#3 is not inserted, only PCIe#1, #2, #4, and #5 are inserted, check the table below for the PCIe Bus Number and its corresponding PCIe Slot.

	PCIe#1	PCIe#2	PCIe#3	PCIe#4	PCIe#5
CPU IOU	4A	1A	5G	2A	3A
PE	PE3	PE0	PE4	PE1	PE2
PCIe Bus Number	94h	16h	X	40h	6Ah

Glossary

ACPI (Advanced Configuration and Power Interface): a power management specification that allows the operating system to control the amount of power distributed to the computer's devices. Devices not in use can be turned off, reducing unnecessary power expenditure.

AGP (Accelerated Graphics Port): a PCI-based interface which was designed specifically for demands of 3D graphics applications. The 32-bit AGP channel directly links the graphics controller to the main memory. While the channel runs only at 66 MHz, it supports data transmission during both the rising and falling ends of the clock cycle, yielding an effective speed of 133 MHz.

ATAPI (AT Attachment Packet Interface): also known as IDE or ATA; a drive implementation that includes the disk controller on the device itself. It allows CD-ROMs and tape drives to be configured as master or slave devices, just like HDDs.

ATX: the form factor designed to replace the AT form factor. It improves on the AT design by rotating the board 90 degrees, so that the IDE connectors are closer to the drive bays, and the CPU is closer to the power supply and cooling fan. The keyboard, mouse, USB, serial, and parallel ports are built-in.

Bandwidth: refers to carrying capacity. The greater the bandwidth, the more data the bus, phone line, or other electrical path can carry. Greater bandwidth results in greater speed.

BBS (BIOS Boot Specification): a feature within the BIOS that creates, prioritizes, and maintains a list of all Initial Program Load (IPL) devices, and then stores that list in NVRAM. IPL devices have the ability to load and execute an OS, as well as provide the ability to return to the BIOS if the OS load process fails. At that point, the next IPL device is called upon to attempt loading of the OS.

BIOS (Basic Input/Output System): the program that resides in the ROM chip, which provides the basic instructions for controlling your computer's hardware. Both the operating system and application software use BIOS routines to ensure compatibility.

Buffer: a portion of RAM which is used to temporarily store data; usually from an application though it is also used when printing and in most keyboard drivers. The CPU can manipulate data in a buffer before copying it to a disk drive. While this improves system performance (reading to or writing from a disk drive a single time is much faster than doing so repeatedly) there is the possibility of losing your data should the system crash. Information in a buffer is temporarily stored, not permanently saved.

Bus: a data pathway. The term is used especially to refer to the connection between the processor and system memory, and between the processor and PCI or ISA local buses.

Bus mastering: allows peripheral devices and IDEs to access the system memory without going through the CPU (similar to DMA channels).

Cache: a temporary storage area for data that will be needed often by an application. Using a cache lowers data access times since the information is stored in SRAM instead of slower DRAM. Note that the cache is also much smaller than your regular memory: a typical cache size is 512KB, while you may have as much as 4GB of regular memory.

Closed and open jumpers: jumpers and jumper pins are active when they are “on” or “closed”, and inactive when they are “off” or “open”.

CMOS (Complementary Metal-Oxide Semiconductors): chips that hold the basic startup information for the BIOS.

COM port: another name for the serial port, which is called as such because it transmits the eight bits of a byte of data along one wire, and receives data on another single wire (that is, the data is transmitted in serial form, one bit after another). Parallel ports transmit the bits of a byte on eight different wires at the same time (that is, in parallel form, eight bits at the same time).

DDR (Double Data Rate): a technology designed to double the clock speed of the memory. It activates output on both the rising and falling edge of the system clock rather than on just the rising edge, potentially doubling output.

DIMM (Dual In-line Memory Module): faster and more capacious form of RAM than SIMMs, and do not need to be installed in pairs.

DIMM bank: sometimes called DIMM socket because the physical slot and the logical unit are the same. That is, one DIMM module fits into one DIMM socket, which is capable of acting as a memory bank.

DMA (Direct Memory Access): channels that are similar to IRQs. DMA channels allow hardware devices (like soundcards or keyboards) to access the main memory without involving the CPU. This frees up CPU resources for other tasks. As with IRQs, it is vital that you do not double up devices on a single line. Plug-n-Play devices will take care of this for you.

DRAM (Dynamic RAM): widely available, very affordable form of RAM which loses data if it is not recharged regularly (every few milliseconds). This refresh requirement makes DRAM three to ten times slower than non-recharged RAM such as SRAM.

ECC (Error Correction Code or Error Checking and Correcting): allows data to be checked for errors during run-time. Errors can subsequently be corrected at the same time that they're found.

EEPROM (Electrically Erasable Programmable ROM): also called Flash BIOS, it is a ROM chip which can, unlike normal ROM, be updated. This allows you to keep up with changes in the BIOS programs without having to buy a new chip. TYAN®'s BIOS updates can be found at <http://www.mitacomputing.com>

ESCD (Extended System Configuration Data): a format for storing information about Plug-n-Play devices in the system BIOS. This information helps properly configure the system each time it boots.

Firmware: low-level software that controls the system hardware.

Form factor: an industry term for the size, shape, power supply type, and external connector type of the Personal Computer Board (PCB) or motherboard. The standard form factors are the AT and ATX.

Global timer: onboard hardware timer, such as the Real-Time Clock (RTC).

HDD: stands for Hard Disk Drive, a type of fixed drive.

H-SYNC: controls the horizontal synchronization/properties of the monitor.

HyperTransport™: a high speed, low latency, scalable point-to-point link for interconnecting ICs on boards. It can be significantly faster than a PCI bus for an equivalent number of pins. It provides the bandwidth and flexibility critical for today's networking and computing platforms while retaining the fundamental programming model of PCI.

IC (Integrated Circuit): the formal name for the computer chip.

IDE (Integrated Device/Drive Electronics): a simple, self-contained HDD interface. It can handle drives up to 8.4 GB in size. Almost all IDEs sold now are in fact Enhanced IDEs (EIDEs), with maximum capacity determined by the hardware controller.

IDE INT (IDE Interrupt): Hardware interrupt signal that goes to the IDE.

I/O (Input/Output): the connection between your computer and another piece of hardware (mouse, keyboard, etc.)

IRQ (Interrupt Request): an electronic request that runs from a hardware device to the CPU. The interrupt controller assigns priorities to incoming requests and delivers them to the CPU. It is important that there is only one device hooked up to each IRQ line; doubling up devices on IRQ lines can lock up your system. Plug-n-Play operating systems can take care of these details for you.

Latency: the amount of time that one part of a system spends waiting for another part to catch up. This occurs most commonly when the system sends data out to a peripheral device and has to wait for the peripheral to spread (peripherals tend to be slower than onboard system components).

NVRAM: ROM and EEPROM are both examples of Non-Volatile RAM, memory that holds its data without power. DRAM, in contrast, is volatile.

Parallel port: transmits the bits of a byte on eight different wires at the same time.

PCI (Peripheral Component Interconnect): a 32 or 64-bit local bus (data pathway) which is faster than the ISA bus. Local buses are those which operate within a single system (as opposed to a network bus, which connects multiple systems).

PCI PIO (PCI Programmable Input/Output) modes: the data transfer modes used by IDE drives. These modes use the CPU for data transfer (in contrast, DMA channels do not). PCI refers to the type of bus used by these modes to communicate with the CPU.

PCI-to-PCI Bridge: allows you to connect multiple PCI devices onto one PCI slot.

Pipeline burst SRAM: a fast secondary cache. It is used as a secondary cache because SRAM is slower than SDRAM, but usually larger. Data is cached first to the faster primary cache, and then, when the primary cache is full, to the slower secondary cache.

PnP (Plug-n-Play): a design standard that has become ascendant in the industry. Plug-n-Play devices require little set-up to use. Devices and operating systems that are not Plug-n-Play require you to reconfigure your system each time you add or change any part of your hardware.

PXE (Preboot Execution Environment): one of four components that together make up the Wired for Management 2.0 baseline specification. PXE was designed to define a standard set of preboot protocol services within a client with the goal of allowing networked-based booting to boot using industry standard protocols.

RAID (Redundant Array of Independent Disks): a way for the same data to be stored in different places on many hard drives. By using this method, the data is stored redundantly and multiple hard drives will appear as a single drive to the operating system. RAID level 0 is known as striping, where data is striped (or overlapped) across multiple hard drives, but offers no fault-tolerance. RAID level 1 is known as mirroring, which stores the data within at least two hard drives, but does not stripe. RAID level 10 also allows for faster access time and fault-tolerance, since either hard drive can be read at the same time. RAID level 0+1 is striping and mirroring, providing fault-tolerance, striping, and faster access all at the same time.

RAIDIOS: RAID I/O Steering (Intel)

RAM (Random Access Memory): technically refers to a type of memory where any byte can be accessed without touching the adjacent data and is often referred to the system's main memory. This memory is available to any program running on the computer.

ROM (Read-Only Memory): a storage chip which contains the BIOS; the basic instructions required to boot the computer and start up the operating system.

SDRAM (Synchronous Dynamic RAM): called as such because it can keep two sets of memory addresses open simultaneously. By transferring data alternately from one set of addresses and then the other, SDRAM cuts down on the delays associated with non-synchronous RAM, which must close one address bank before opening the next.

Serial port: called as such because it transmits the eight bits of a byte of data along one wire, and receives data on another single wire (that is, the data is transmitted in serial form, one bit after another).

SCSI Interrupt Steering Logic (SISL): Architecture that allows a RAID controller, such as AcceleRAID 150, 200 or 250, to implement RAID on a system board-embedded SCSI bus or a set of SCSI busses. SISL: SCSI Interrupt Steering Logic (LSI) (only on LSI SCSI boards)

Sleep/Suspend mode: in this mode, all devices except the CPU shut down.

SDRAM (Static RAM): unlike DRAM, this type of RAM does not need to be refreshed in order to prevent data loss. Thus, it is faster and more expensive.

SLI (Scalable Link Interface): NVIDIA SLI technology links two graphics cards together to provide scalability and increased performance. NVIDIA SLI takes advantage of the increased bandwidth of the PCI Express bus architecture, and features hardware and software innovations within NVIDIA GPUs (graphics processing units) and NVIDIA MCPs (media and communications processors). Depending on the application, NVIDIA SLI can deliver as much as two times the performance of a single GPU configuration.

Standby mode: in this mode, the video and hard drives shut down; all other devices continue to operate normally.

UltraDMA-33/66/100: a fast version of the old DMA channel. UltraDMA is also called UltraATA. Without a proper UltraDMA controller, your system cannot take advantage of higher data transfer rates of the new UltraDMA/UltraATA hard drives.

USB (Universal Serial Bus): a versatile port. This one port type can function as a serial, parallel, mouse, keyboard or joystick port. It is fast enough to support video transfer, and is capable of supporting up to 127 daisy-chained peripheral devices.

VGA (Video Graphics Array): the PC video display standard

V-SYNC: controls the vertical scanning properties of the monitor.

ZCR (Zero Channel RAID): PCI card that allows a RAID card to use the onboard SCSI chip, thus lowering cost of RAID solution

ZIF Socket (Zero Insertion Force socket): these sockets make it possible to insert CPUs without damaging the sensitive CPU pins. The CPU is lightly placed in an open ZIF socket, and a lever is pulled down. This shifts the processor over and down, guiding it into the board and locking it into place.

Technical Support

If a problem arises with your system, you should first turn to your dealer for direct support. Your system has most likely been configured or designed by them and they should have the best idea of what hardware and software your system contains. Hence, they should be of the most assistance for you. Furthermore, if you purchased your system from a dealer near you, take the system to them directly to have it serviced instead of attempting to do so yourself (which can have expensive consequences).

If these options are not available for you then TYAN® Computer Corporation can help. Besides designing innovative and quality products for over a decade, TYAN has continuously offered customers service beyond their expectations. TYAN®'s website (<http://www.mitacomputing.com>) provides easy-to-access FAQ searches and online Trouble Ticket creation as well as Instant Chat capabilities with our Support Agents. TYAN® also provides easy-to-access resources such as in-depth Linux Online Support sections with downloadable Linux drivers and comprehensive compatibility reports for chassis, memory and much more. With all these convenient resources just a few keystrokes away, users can easily find the latest software and operating system components to keep their systems running as powerful and productive as possible. TYAN® also ranks high for its commitment to fast and friendly customer support through email. By offering plenty of options for users, TYAN® serves multiple market segments with the industry's most competitive services to support them.

Please feel free to contact us directly for this service at tech-support@tyan.com

Help Resources:

1. See the beep codes section of this manual.
2. See the TYAN® website for FAQ's, bulletins, driver updates, and other information: <http://www.mitacomputing.com>
3. Contact your dealer for help BEFORE calling TYAN®.

Returning Merchandise for Service

During the warranty period, contact your distributor or system vendor FIRST for any product problems. This warranty only covers normal customer use and does not cover damages incurred during shipping or failure due to the alteration, misuse, abuse, or improper maintenance of products.

NOTE:

A receipt or copy of your invoice marked with the date of purchase is required before any warranty service can be rendered. You may obtain service by calling the manufacturer for a Return Merchandise Authorization (RMA) number. The RMA number Should be prominently displayed on the outside of the shipping carton and the package should be mailed prepaid. TYAN® will pay to have the board shipped back to you.

**Notice for the USA**

Compliance Information Statement (Declaration of Conformity Procedure) DoC

FCC Part 15: This device complies with part 15 of the FCC Rules

Operation is subject to the following conditions:

This device may not cause harmful interference, and this device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Plug the equipment into an outlet on a circuit different from that of the receiver.

Consult the dealer on an experienced radio/television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communications Radio Interference Regulations. (Cet appareil est conforme aux normes de Classe B d'interférence radio tel que spécifié par le Ministère Canadien des Communications dans les règlements d'interférence radio.)

CAUTION: Lithium battery included with this board. Do not puncture, mutilate, or dispose of battery in fire. There is danger of an explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacturer. Dispose of used battery according to manufacturer instructions and in accordance with your local regulations.

Document #: D2560 - 100