



SBC-371-2H

## User Manual

Version 1.0

Published July 17, 2025

Copyright©2025 ASRockInd INC. All rights reserved.

Version 1.0

Published July, 2025

Copyright©2025 ASRockInd INC. All rights reserved.

## Copyright Notice:

No part of this documentation may be reproduced, transcribed, transmitted, or translated in any language, in any form or by any means, except duplication of documentation by the purchaser for backup purpose, without written consent of ASRockInd Inc.

Products and corporate names appearing in this documentation may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

## Disclaimer:

Specifications and information contained in this documentation are furnished for informational use only and subject to change without notice, and should not be constructed as a commitment by ASRockInd. ASRockInd assumes no responsibility for any errors or omissions that may appear in this documentation.

To the extent permitted by law, with respect to the contents of this documentation, ASRockInd does not provide warranty of any kind, either expressed or implied, including but not limited to the implied warranties or conditions of merchantability or fitness for a particular purpose. In no event shall ASRockInd, its directors, officers, employees, or agents be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of data, interruption of business and the like), even if ASRockInd has been advised of the possibility of such damages arising from any defect or error in the documentation or product.



This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

The terms HDMI® and HDMI High-Definition Multimedia Interface, and the HDMI logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.





### WARNING

#### THIS PRODUCT CONTAINS A BUTTOON BATTERY

If swallowed, a button battery can cause serious injury or death.

Please keep batteries out of sight or reach of children.

### CALIFORNIA, USA ONLY

The Lithium battery adopted on this motherboard contains Perchlorate, a toxic substance controlled in Perchlorate Best Management Practices (BMP) regulations passed by the California Legislature. When you discard the Lithium battery in California, USA, please follow the related regulations in advance.

“Perchlorate Material-special handling may apply, see [www.dtsc.ca.gov/hazardouswaste/perchlorate](http://www.dtsc.ca.gov/hazardouswaste/perchlorate)”

### AUSTRALIA ONLY

Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage caused by our goods. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you require assistance please call ASRockInd Tel : +886-2-28965588 ext.123 (Standard International call charges apply)



ASRockInd follows the green design concept to design and manufacture our products, and makes sure that each stage of the product life cycle of ASRockInd product is in line with global environmental regulations. In addition, ASRockInd disclose the relevant information based on regulation requirements.



DO NOT throw the motherboard in municipal waste. This product has been designed to enable proper reuse of parts and recycling. This symbol of the crossed out wheeled bin indicates that the product (electrical and electronic equipment) should not be placed in municipal waste. Check local regulations for disposal of electronic products.

## Button Battery Safety Notice

### **WARNING**

- **INGESTION HAZARD:** This product contains a button cell or coin battery.
- **DEATH** or serious injury can occur if ingested.
- A swallowed button cell or coin battery can cause **Internal Chemical Burns** in as little as **2 hours**.
- **KEEP** new and used batteries **OUT OF REACH of CHILDREN**
- **Seek immediate medical attention** if a battery is suspected to be swallowed or inserted inside any part of the body.



- Remove and immediately recycle or dispose of used batteries according to local regulations and keep away from children. Do NOT dispose of batteries in household trash or incinerate.
- Even used batteries may cause severe injury or death.
- Call a local poison control center for treatment information.
- Battery type: CR2032
- Battery voltage: 3V
- Non-rechargeable batteries are not to be recharged.
- Do not force discharge, recharge, disassemble, heat above (manufacturer's specified temperature rating) or incinerate. Doing so may result in injury due to venting, leakage or explosion resulting in chemical burns.
- This product contains an irreplaceable battery.
- This icon indicates that a swallowed button battery can cause serious injury or death. Please keep batteries out of sight or reach of children.

## Contents

<b>Chapter 1 Introduction</b>	<b>1</b>
1.1 Package Contents	1
1.2 Specifications	2
1.3 Motherboard Layout	4
1.4 I/O Panel	7
1.5 Block Diagram	8
<b>Chapter 2 Installation</b>	<b>9</b>
2.1 Screw Holes	9
2.2 Pre-installation Precautions	9
2.3 Installation of Memory Modules (SO-DIMM)	10
2.4 Expansion Slots	11
2.5 Jumpers Setup	12
2.6 Onboard Headers and Connectors	15
<b>Chapter 3 UEFI SETUP UTILITY</b>	<b>21</b>
3.1 Introduction	21
3.1.1 Entering BIOS Setup	21
3.1.2 UEFI Menu Bar	22
3.1.3 Navigation Keys	23
3.2 Main Screen	24
3.3 Advanced Screen	25
3.3.1 CPU Configuration	26
3.3.2 Chipset Configuration	29
3.3.3 Storage Configuration	31

3.3.4	Super IO Configuration	33
3.3.5	AMT Configuration	34
3.3.6	ACPI Configuration	36
3.3.7	USB Configuration	37
3.3.8	Trusted Computing	38
3.4	Hardware Health Event Monitoring Screen	40
3.5	Security Screen	41
3.6	Boot Screen	42
3.7	Exit Screen	43

# Chapter 1 Introduction

Thank you for purchasing ASRockInd **SBC-371-2H** motherboard, a reliable motherboard produced under ASRockInd's consistently stringent quality control. It delivers excellent performance with robust design conforming to ASRockInd's commitment to quality and endurance.

In this manual, chapter 1 and 2 contain introduction of the motherboard and step-by-step guide to the hardware installation. Chapter 3 contains the configuration guide to BIOS setup.



*Because the motherboard specifications and the BIOS software might be updated, the content of this manual will be subject to change without notice. In case any modifications of this manual occur, the updated version will be available on ASRockInd website without further notice.*

ASRockInd website: <https://www.asrockind.com/SBC-371-2H>

<https://www.asrockind.com/SBC-371P-2H>

<https://www.asrockind.com/SBC-371M-2H>

<https://www.asrockind.com/SBC-371V-2H>

*If you require technical support related to this motherboard, please visit our website for specific information about the model you are using.*

<https://www.asrockind.com/technical-support>

## 1.1 Package Contents

ASRockInd **SBC-371-2H** Motherboard (3.5"SBC (5.8-in x 4-in x 0.94-in, 14.7 cm x 10.2 cm x 2.40 cm))

ASRockInd **SBC-371-2H** Jumper Setting Instruction

### **Gift Package:**

1 x Heat Spreader 102.22\*147.01mm

3 x SCREW M2\*2, D=5

2 x COM Cable

1 x SATA Data Cable

1 x SATA Power Cable

1 x DC-in Cable

### **Bulk Package:**

3 x SCREW M2\*2, D=5

## 1.2 Specifications

Form Factor	Dimensions	3.5”SBC (5.8-in x 4-in x 0.94-in, 14.7 cm x 10.2 cm x 2.40 cm)
Processor System	CPU	Intel® 13th Gen (Raptor Lake-P) Core™ Processors SBC-371P-2H (i7-1365UE, 2P+8E) SBC-371M-2H (i5-1335UE, 2P+8E) SBC-371V-2H (i3-1315UE, 2P+4E)
	BIOS	AMI SPI 256 Mbit
Memory	Technology	Dual Channel DDR4 3200 MHz
	Capacity	64GB (32GB per DIMM)
	Socket	2 x 260-pin SO-DIMM
Graphics	Controller	Intel® Iris® X <sup>c</sup> Graphics
	HDMI	HDMI 2.0b Max resolution up to 4096x2160@60Hz
	LVDS	Dual channel 24 bit up to 1920x1200@60Hz (Connector shared with eDP)
	eDP	Max resolution up to 1920x1080@60Hz (Connector shared with LVDS)
	MultiDisplay	Quad display (Included 2 output from Type-C)
Expansion Slot	PCIe	1 x PCIe Gen3 x1 (supports up to 10W)
	M.2	1 x M.2 (Key E, 2230) with PCIe Gen3 x1, USB 2.0 and CNVio/CNVio2 for Wireless 1 x M.2 (Key B, 3042/3052) with PCIe Gen3 x1 or SATA3 and USB 3.2 Gen1 and USB 2.0 and SIM for 4G/5G
	SIM Socket	1 x SIM socket connected to M.2 key B
Audio	Interface	Realtek ALC256 HD, High Definition Audio. Line-out, Mic-in
Ethernet	Controller/Speed	<b>SBC-371P-2H/SBC-371M-2H</b> LAN1: Intel® I226LM with 10/100/1000/2500 Mbps, supports vPro LAN2: Intel® I226V with 10/100/1000/2500 Mbps <b>SBC-371V-2H</b> LAN1: Intel® I226LM with 10/100/1000/2500 Mbps LAN2: Intel® I226V with 10/100/1000/2500 Mbps
	Connector	2 x RJ-45

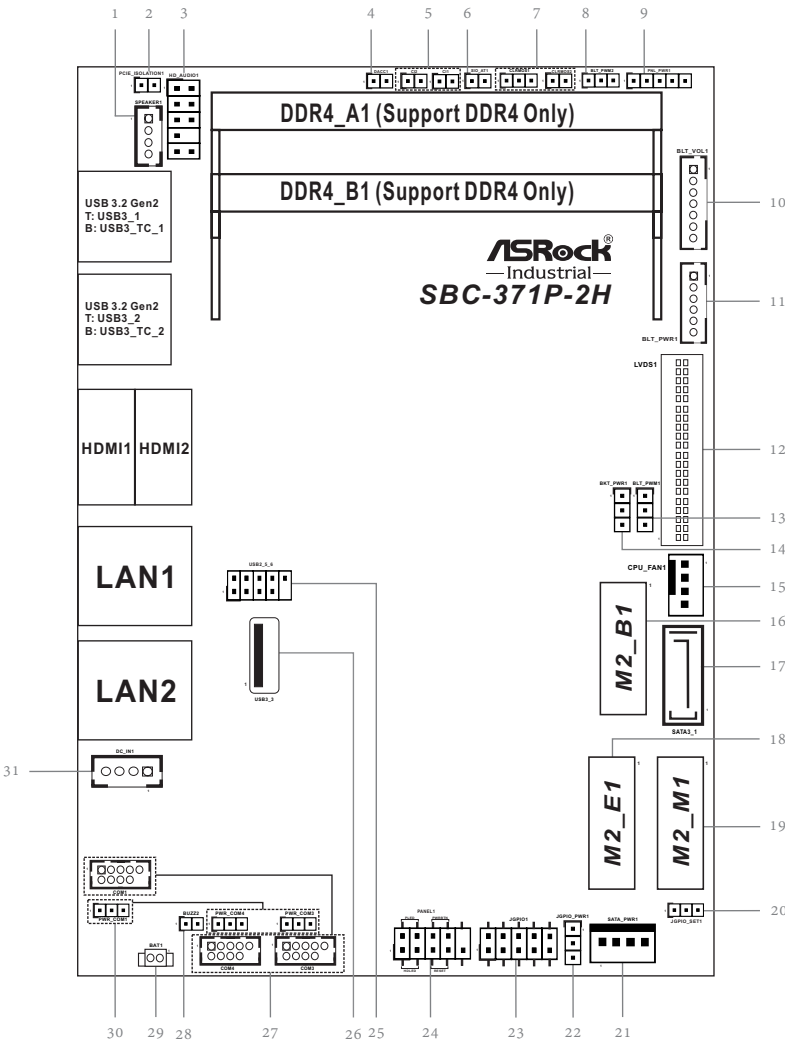


Rear I/O	HDMI	2 x HDMI 2.0b
	Ethernet	2 x 2.5 Gigabit LAN
	USB	2 x USB 3.2 Gen2 2 x USB 3.2 Gen2x2 (Type-C, 5V/3A, support DP 1.4a display output)
Internal Connector	USB	1 x USB 3.2 Gen2 2 x USB 2.0 (1 x 2.54 pitch header)
	COM	COM1, COM3, COM4 (RS-232/422/485)
	GPIO	4 x GPI, 4 x GPO
	LVDS	1 (Connector with LVDS/eDP signal, switch by BIOS)
	SATA PWR Output	1
	Speaker Header	1
Storage	M.2	1 x M.2 (Key M, 2242/2260/2280) with PCIe Gen4 x4 for SSD
	SATA	1 x SATA3 (6Gb/s)
	RAID	Intel® VMD RAID 0/1 ** supported by PCIe interface PCIe interface: M.2 Key B + M.2 Key M
Security	TPM	TPM 2.0 onboard IC
Watchdog Timer	Output	From Super I/O to drag RESETCON#
	Interval	256 Segments, 0, 1, 2, ...255 Sec
Power Requirements	Input PWR	12~36V DC-In with 4-pin wafer PWR cable 12V DC-In only (BOM option)
	Power On	AT/ATX Supported -AT: Directly PWR on as power input ready -ATX: Press button to PWR on after power input ready
Environment	Operating Temperature	-20°C ~ 70°C
	Storage Temperature	-40°C ~ 85°C
	Operating Humidity	5% ~ 90%
	Storage Humidity	5% ~ 90%

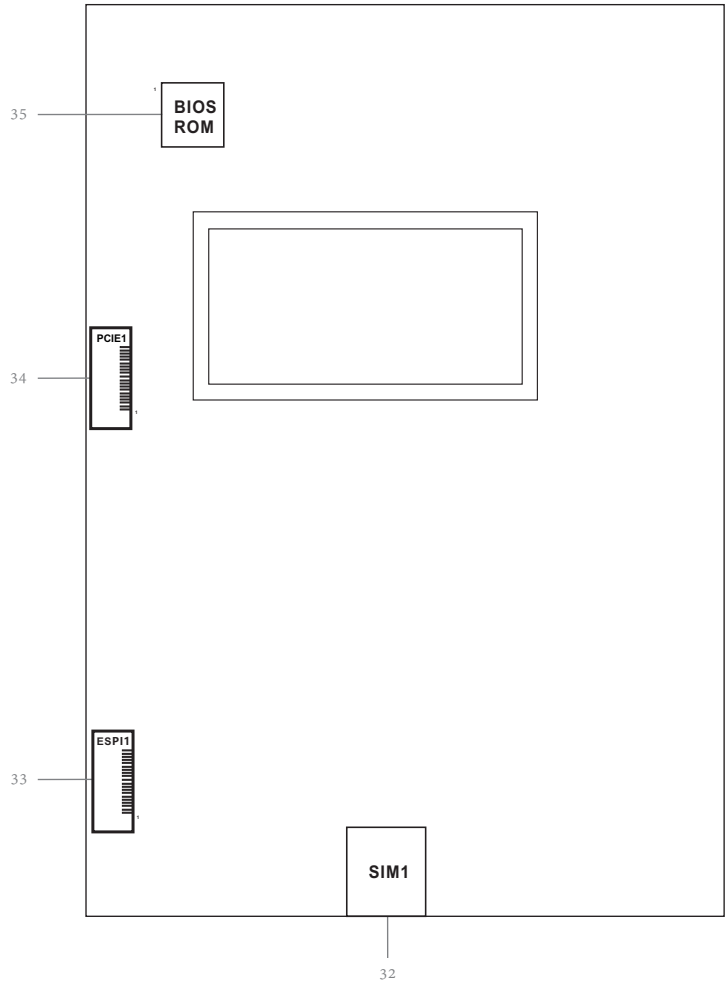
\* The thermal solution of whole system needs to be designed additionally.

# 1.3 Motherboard Layout

Top:



**Bottom:**

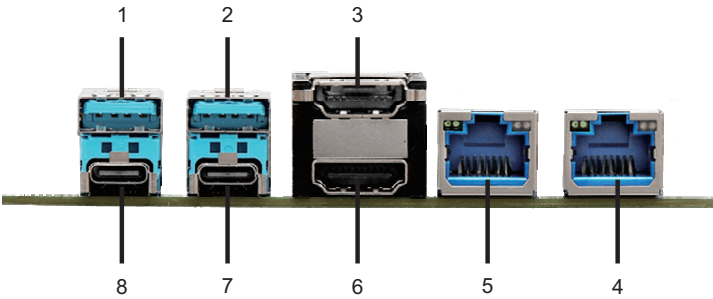


- 1 : 3W Audio AMP Output Wafer (SPEAKER1)
- 2 : PCIE\_ISOLATION1
- 3 : Front Panel Audio Header (HD\_AUDIO1)
- 4 : DACC Jumper (DACC1)
- 5 : Chassis Intrusion Headers (CI1, CI2)
- 6 : ATX/AT Mode Jumper (SIO\_AT1)
- 7 : Clear CMOS Headers (CLRMOS1, CLRMOS2)
- 8 : CON\_LBKLT\_CTL Voltage Level (BLT\_PWM2)
- 9 : Panel Power Select (LCD\_VCC) (PNL\_PWR1)
- 10 : Backlight & Amp Volume Control (BLT\_VOL1)
- 11 : Inverter Power Control Wafer (BLT\_PWR1)
- 12 : LVDS Panel Connector (LVDS1)
- 13 : Brightness Control Mode (BLT\_PWM1)
- 14 : Backlight Power Select (LCD\_BLT\_VCC) (BKT\_PWR1)
- 15 : 4-Pin CPU FAN Connector (+12V) (CPU\_FAN1)
- 16 : M.2 Key-B Socket (M2\_B1)
- 17 : SATA3 Connector (SATA3\_1)
- 18 : M.2 Key-E Socket (M2\_E1)
- 19 : M.2 Key-M Socket (M2\_M1)
- 20 : GPIO Default Setting (JGPIO\_SET1)
- 21 : SATA Power Output Connector (SATA\_PWR1)
- 22 : Digital Input/Output Power Select (JGPIO\_PWR1)
- 23 : Digital Input/Output Pin Header (JGPIO1)
- 24 : System Panel Header (PANEL1)
- 25 : USB 2.0 Connector (USB2\_5\_6)
- 26 : USB 3.2 Gen2 Port (USB3\_3)
- 27 : COM1, 3, 4 Headers (COM1, 3, 4) (RS232/422/485)
- 28 : Buzzer (BUZZ2)
- 29 : Battery Connector (BAT1)
- 30 : COM Port Pin9 PWR Setting Jumpers
  - PWR\_COM1 (For COM Port1)
  - PWR\_COM3 (For COM Port3)
  - PWR\_COM4 (For COM Port4)
- 31 : ATX Power Connector (DC\_IN1) (Input 12V-36V (Default); 12V only (by BOM option))

Back Side:

- 32 : SIM Card Socket (SIM1)
- 33 : ESPI Connector (ESPI1)
- 34 : PCIE Connector (PCIE1)
- 35 : BIOS ROM Socket

1.4 I/O Panel



- 1

USB 3.2 Gen2 Port (USB3\_1)
- 2

USB 3.2 Gen2 Port (USB3\_2)
- 3

HDMI Port (HDMI2)
- 4

RJ45 LAN Port (LAN2)\*
- 5

RJ45 LAN Port (LAN1)\*  
(Only SBC-371P-2H and SBC-371M-2H  
support vPro.)
- 6

HDMI Port (HDMI1)
- 7

USB 3.2 Gen2x2 Type-C Port (USB3\_TC\_2)
- 8

USB 3.2 Gen2x2 Type-C Port (USB3\_TC\_1)


\* There are two LEDs next to the LAN port. Please refer to the table below for the LAN ports LED indications.

LAN Ports LED Indications

Activity/Link LED		SPEED LED	
Status	Description	Status	Description
Off	No Link	Off	10Mbps/100Mbps connection
Blinking	Data Activity	Orange	1Gbps connection
On	Link	Green	2.5Gbps connection

ACT/LINK LED

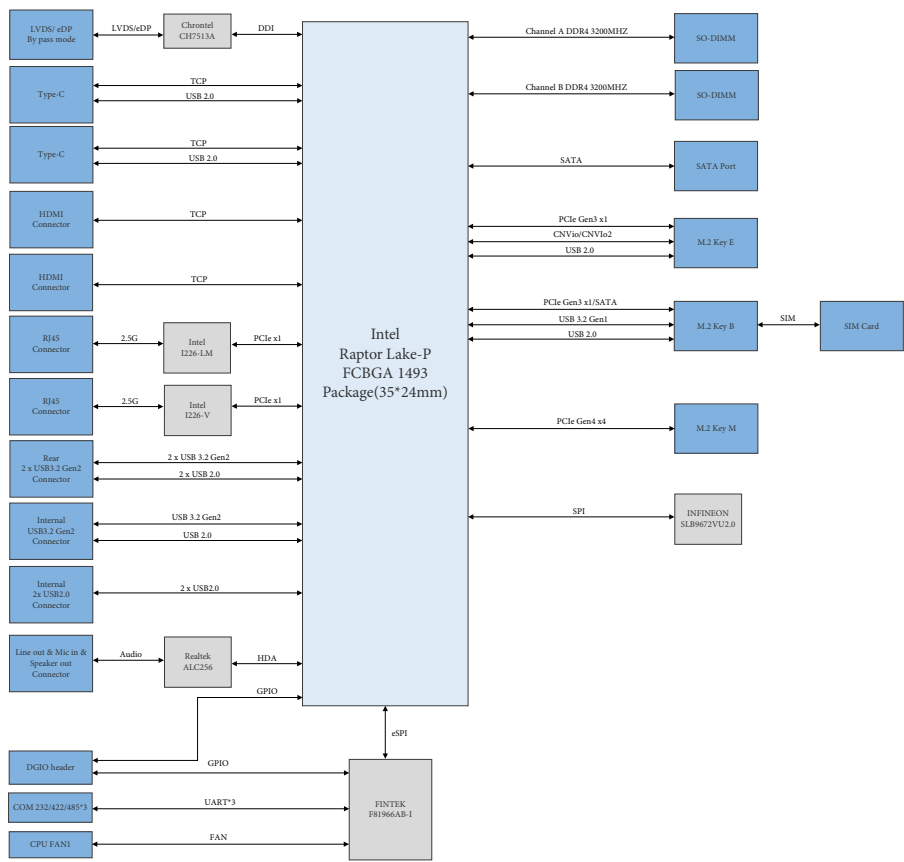
SPEED LED



LAN Port

# 1.5 Block Diagram

## SBC-371-2H



## Chapter 2 Installation

This is a 3.5" SBC (5.8-in x 4-in x 0.94-in, 14.7 cm x 10.2 cm x 2.40 cm) form factor motherboard. Before you install the motherboard, study the configuration of your chassis to ensure that the motherboard fits into it.



*Make sure to unplug the power cord before installing or removing the motherboard. Failure to do so may cause physical injuries to you and damages to motherboard components.*

### 2.1 Screw Holes

Place screws into the holes to secure the motherboard to the chassis.



*Do not over-tighten the screws! Doing so may damage the motherboard.*

### 2.2 Pre-installation Precautions

Take note of the following precautions before you install motherboard components or change any motherboard settings.

1. Unplug the power cord from the wall socket before touching any component.
2. To avoid damaging the motherboard components due to static electricity, NEVER place your motherboard directly on the carpet or the like. Also remember to use a grounded wrist strap or touch a safety grounded object before you handle components.
3. Hold components by the edges and do not touch the ICs.
4. Whenever you uninstall any component, place it on a grounded antistatic pad or in the bag that comes with the component.
5. Heatsink (The thermal solution of whole system needs to be designed additionally.)

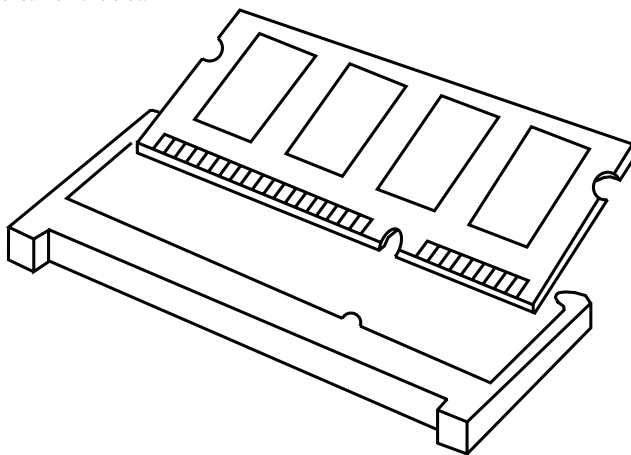


*Before you install or remove any component, ensure that the power is switched off or the power cord is detached from the power supply. Failure to do so may cause severe damage to the motherboard, peripherals, and/or components.*

## 2.3 Installation of Memory Modules (SO-DIMM)

**SBC-371-2H** provides two 260-pin DDR4 (Double Data Rate 4) SO-DIMM slots, and supports Dual Channel Memory Technology.

- Step 1. Align a SO-DIMM on the slot such that the notch on the SO-DIMM matches the break on the slot.



1. *The SO-DIMM only fits in one correct orientation. It will cause permanent damage to the motherboard and the SO-DIMM if you force the SO-DIMM into the slot at incorrect orientation.*
2. *Please do not intermix different voltage SO-DIMMs on this motherboard.*

- Step 2. Firmly insert the SO-DIMM into the slot until the retaining clips at both ends fully snap back in place and the SO-DIMM is properly seated.



## 2.4 Expansion Slots

There are one PCI Express slot, three M.2 sockets and one SIM socket on this motherboard.

**PCIE slot:** PCIE1 (PCIe 3.0 x1 slot) is used for PCI Express x1 lane width cards and supports up to 10W.

**SIM socket:** 1 x SIM socket connected to M.2 key B.

### M.2 sockets:

1 x M.2 (Key E, 2230) with PCIe Gen3 x1, USB 2.0 and CNVio/CNVio2 for Wireless.

1 x M.2 (Key B, 3042/3052) with PCIe Gen3 x1, SATA3, USB 3.2 Gen1, USB 2.0 and SIM for 4G/5G.

1 x M.2 (Key M, 2242/2260/2280) with PCIe Gen4 x4 for SSD

M.2 Key-E Socket  
(M2\_E1)

Pin	Signal Name	Signal Name	Pin
2	+3VSB	GND	1
4	+3VSB	LP+10	3
6	NC	LP-10	5
8	M2_BT_PCMCLK	GND	7
10	M2_BT_PCMFRM_CRF_RST_N	CNV_WR_D1#	9
12	M2_BT_PCMIN	CNV_WR_D1	11
14	MODEM_CLKREQ_R	NC	13
16	NC	CNV_WR_D0#	15
18	GND	CNV_WR_D0	17
20	VBALERT#	NC	19
22	CNV_BBI_RSP	CNV_WR_CLK#	21
		CNV_WR_CLK	23
32	CNV_BGL_DT		
34	CNV_BGL_RSP	GND	33
36	CNV_BBL_DT	PCH_PLE_TXP6	35
38	CL_RST#	PCH_PLE_TXN6	37
40	CL_DATA	GND	39
42	CL_CLK	PCH_PLE_RXP6	41
44	CNV_PA_BLANKING	PCH_PLE_RXN6	43
46	CNV_MFUART2_RXD	GND	45
48	CNV_MFUART2_RXD	PCH_ECLK_WLAN1	47
50	SUS_CLK	PCH_ECLK_WLAN1#	49
52	BUF_PIT_RST_N	GND	51
54	BT_RF_KILL_N	CLKREQ1_WLAN_N	53
56	WiFi_RF_KILL_N	NA	55
58	NA	GND	57
60	NA	CNV_WT_D1#	59
62	NC	CNV_WT_D1	61
64	NC	GND	63
66	NC	CNV_WT_D0#	65
68	NC	CNV_WT_D0	67
70	NC	GND	69
72	+3VSB	CNV_WT_CLK#	71
74	+3VSB	CNV_WT_CLK	73
76	NC	GND	75
78	NC	NC	77
78	NC	NC	79
78	N/C	N/C	77
		N/C	79

M.2 Key-B Socket  
(M2\_B1)

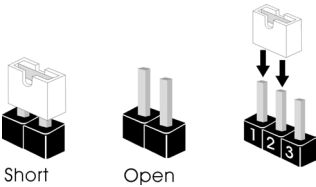
Pin	SIGNAL	SIGNAL	Pin
2	+3V_M2B	CONFIG_J	1
4	+3V_M2B	GND	3
6	Pull_Card_Power_Off#	GND	5
8	W_DISABLE1_B#	LP+4	7
10	WWAN_LED#	LP-4	9
		GND	11
20	NC		
22	NC	NC	21
24	NC	WAKE_ON_WAN#	23
26	W_DISABLE2_B#	DPR	25
28	NC	GND	27
30	UIM1_RESET	USB3_RX4_N	29
32	UIM1_CLK	USB3_RX4_P	31
34	UIM1_DATA	GND	33
36	+UIM1_PWR	USB3_TX4_N	35
38	NA	USB3_TX4_P	37
40	NA	GND	39
42	NA	PER0/SATA-B+	41
44	NC	PER0/SATA-B-	43
46	NC	GND	45
48	NC	PET0/SATA-A+	47
50	BUF_PIT_RST#	PET0/SATA-A-	49
52	PCIECLKREQ#	GND	51
54	NA	M2B_CLKIN	53
56	NA	M2B_CLKAP	55
58	NA	GND	57
60	NC	NC	59
62	NC	NC	61
64	NC	NC	63
66	SIM_DETECT_1	NC	65
68	SUS_CLK	BUF_PIT_RST_N	67
70	+3V_M2B	CONFIG_J	69
72	+3V_M2B	GND	71
74	+3V_M2B	GND	73
76	NC	NC	75
78	NC	NC	77
		NC	79
78	N/C	N/C	77
		N/C	79




M.2 Key-M Socket  
(M2\_M1)

Pin	Signal Name	Signal Name	Pin
2	+3V	GND	1
4	+3V	GND	3
6	NC	M2M_RXN3	5
8	NC	M2M_RXN3	7
10	M2_LED	GND	9
12	+3V	M2M_TXN3	11
14	+3V	M2M_TXP3	13
16	+3V	GND	15
18	+3V	M2M_RXN2	17
20	NC	M2M_RXP2	19
22	NC	GND	21
24	NC	M2M_TXN2	23
26	NC	M2M_TXP2	25
28	NC	GND	27
30	NC	M2M_RXN1	29
32	NC	M2M_RXP1	31
34	NC	GND	33
36	NC	M2M_TXN1	35
38	NC	M2M_TXP1	37
40	NA	GND	39
42	NA	M2M_RXN0	41
44	NC	M2M_RXP0	43
46	NC	GND	45
48	NC	M2M_TXN0	47
50	BUF_PIT_RST_N	M2M_TXP0	49
52	CLKREQ0_M2M	GND	51
54	NA	M2M_CLKIN	53
56	NC	M2M_CLKAP	55
58	NC	GND	57
68	SUS_CLK	NC	67
70	+3V	+3V	69
72	+3V	GND	71
74	+3V	GND	73
76	NC	GND	75
78	NC	NC	77
		NC	79
78	N/C	N/C	77
		N/C	79

## 2.5 Jumpers Setup

The illustration shows how jumpers are setup. When the jumper cap is placed on pins, the jumper is “Short.” If no jumper cap is placed on pins, the jumper is “Open.” The illustration shows a 3-pin jumper whose pin1 and pin2 are “Short” when jumper cap is placed on these 2 pins.



Jumper	Setting	Description
DACC1 (2-pin DACC1) (see p. 4, No. 4)		Open : No ACC ACC Short : ACC (Default)
Auto clear CMOS when system boot improperly.		
Chassis Intrusion Jumpers (CI1, CI2) (2-pin CI1, CI2) (see p. 4, No. 5)		CI1 : Open : Normal (Default) Short : Active Case Open  CI2 : Open : Active Case Open Short : Normal (Default)
This motherboard supports CASE OPEN detection feature that detects if the chassis cover has been removed. This feature requires a chassis with chassis intrusion detection design.		
ATX/AT Mode Jumper (2-pin SIO_AT1) (see p. 4, No. 6)		Open : ATX Mode (Default) Short : AT Mode

## Clear CMOS Jumpers

(3-pin CLRMOS1)

(see p. 4, No. 7)



## CLRMOS1 :

1-2 : Normal (Default)

2-3 : Clear CMOS

NOTE: CLRMOS1 allows you to clear the data in CMOS. To clear and reset the system parameters to default setup, please turn off the computer and unplug the power cord from the power supply. After waiting for 15 seconds, use a jumper cap to short pin2 and pin3 on CLRMOS1 for 5 seconds. However, please do not clear the CMOS right after you update the BIOS. If you need to clear the CMOS when you just finish updating the BIOS, you must boot up the system first, and then shut it down before you do the clear-CMOS action. Please be noted that the password, date, and time will be cleared only if the CMOS battery is removed.

(2-pin CLRMOS2)

(see p. 4, No. 7)



## CLRMOS2 :

Open : Normal (Default)

Short : Auto Clear CMOS  
(Power Off)

NOTE: CLRMOS2 allows you to clear the data in CMOS automatically when AC power on. The data in CMOS includes system setup information such as system password, date, time, and system setup parameters. To clear and reset the system parameters to default setup, please turn off the computer and unplug the power cord, then use a jumper cap to short the pins on CLRMOS2.

## CON\_LBKLT\_CTL Voltage Level

(3-pin BLT\_PWM2)

(see p. 4, No. 8)



1-2 : 3V Level (Default)

2-3 : 5V Level

## Panel Power Select (LCD\_VCC)

(5-pin PNL\_PWR1)

(see p. 4, No. 9)



1-2: +3V (Default)

2-3: +5V

3-4: +5V

4-5: +12V

Use this to set up the VDD power of the LVDS connector.

Brightness Control Mode

(3-pin BLT\_PWM1)

(see p. 4, No. 13)



1-2 : From eDP PWM to

CON\_LBKLT\_CTL

2-3 : From LVDS PWM to

CON\_LBKLT\_CTL (Default)

Please set to 1-2 when adjusting brightness by Brightness Control bar under OS.

Please set to 2-3 when adjusting brightness by BLT\_VOL1.

---

Backlight Power Select (LCD\_BLT\_VCC)

(3-pin BKT\_PWR1)

(see p. 4, No. 14)



1-2 : +5V (Default)

2-3 : +12V

Use this to set up the backlight power of the LVDS connector.

---

GPIO Default Setting

(3-pin JGPIO\_SET1)

(see p. 4, No. 20)



1-2: Pull-High (Default)

2-3: Pull-Low

---

Digital Input/Output Power Select

(3-pin JGPIO\_PWR1)

(see p. 4, No. 22)



1-2 : +12V

2-3 : +5V (Default)

---

COM Port Pin9 PWR Setting Jumpers

(3-pin PWR\_COM1, 4, 3)

(see p. 4, No. 30)



1-2 : +5V (Default)

2-3 : +12V

2.6 Onboard Headers and Connectors



Onboard headers and connectors are NOT jumpers. Do NOT place jumper caps over these headers and connectors. Placing jumper caps over the headers and connectors will cause permanent damage of the motherboard!

3W Audio AMP Output Wafer  
(4-pin SPEAKER1)  
(see p. 4, No. 1)



Pin	Signal Name
1	SPK L-
2	SPK L+
3	SPK R+
4	SPK R-

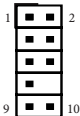
PCIE\_ISOLATION1  
(2-pin PCIE\_ISOLATION1)  
(see p. 4, No. 2)



Pin	Signal Name
1	PSON#
2	GND

Connect to PCIE\_ISOLATION\_1 header on VGA-PWR card.

Front Panel Audio Header  
(9-pin HD\_AUDIO1)  
(see p. 4, No. 3)



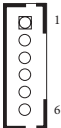
Pin	Signal Name	Signal Name	Pin
1	MIC1_L	AGND_A	2
3	MIC1_R	NA	4
5	LINE2_R_OUT	MIC1_JD	6
7	AGND_A		8
9	LINE2_L_OUT	LINE2_JD	10

Backlight & Amp Volume Control  
(7-pin BLT\_VOL1)  
(see p. 4, No. 10)



Pin	Signal Name
1	NA
2	NA
3	PWRDN
4	GPIO_BLT_UP
5	GPIO_BLT_DW
6	GND
7	GND

Inverter Power Control Wafer  
(6-pin BLT\_PWR1)  
(see p. 4, No. 11)

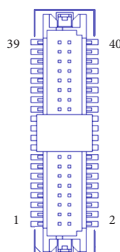


Pin	Signal Name
1	GND
2	GND
3	CON_LBKLT_CTL
4	CON_LBKLT_EN
5	LCD_BLT_VCC
6	LCD_BLT_VCC

## LVDS Panel Connector

(40-pin LVDS1)

(see p. 4, No. 12)



Pin	Signal Name	Signal Name	Pin
1	LCD_VCC	LCD_VCC	2
3	+3.3V	NA	4
5	NA	LVDS_A_DATA0#	6
7	LVDS_A_DATA0	GND	8
9	LVDS_A_DATA1#	LVDS_A_DATA1	10
11	GND	LVDS_A_DATA2#	12
13	LVDS_A_DATA2	GND	14
15	LVDS_A_DATA3#	LVDS_A_DATA3	16
17	GND	LVDS_A_CLK#	18
19	LVDS_A_CLK	GND	20
21	LVDS_B_DATA0#	LVDS_B_DATA0	22
23	GND	LVDS_B_DATA1#	24
25	LVDS_B_DATA1	GND	26
27	LVDS_B_DATA2#	LVDS_B_DATA2	28
29	DPLVDD_EN	LVDS_B_DATA3#	30
31	LVDS_B_DATA3	GND	32
33	LVDS_B_CLK#	LVDS_B_CLK	34
35	GND	CON_LBKLT_EN	36
37	CON_LBKLT_CTL	LCD_BLT_VCC	38
39	LCD_BLT_VCC	LCD_BLT_VCC	40

\* eDP by pass mode pin

definition (switch by BIOS)

Pin	Signal Name	Signal Name	Pin
1	LCD_VCC	LCD_VCC	2
3	NA	NA	4
5	NA	NA	6
7	NA	GND	8
9	EDP_TX1#	EDP_TX1	10
11	GND	EDP_TX0#	12
13	EDP_TX0	GND	14
15	NA	NA	16
17	GND	EDP_AUXN	18
19	EDP_AUXP	GND	20
21	NA	NA	22
23	GND	NA	24
25	NA	GND	26
27	NA	NA	28
29	DPLVDD_EN	NA	30
31	NA	GND	32
33	NA	NA	34
35	GND	CON_LBKLT_EN	36
37	CON_LBKLT_CTL	LCD_BLT_VCC	38
39	LCD_BLT_VCC	LCD_BLT_VCC	40

## 4-pin CPU Fan Connector (+12V)

(4-pin CPU\_FAN1)

(see p. 4, No. 15)



Pin	Signal Name
1	GND
2	+12V
3	CPU_FAN_SPEED
4	FAN_SPEED_CONTROL

Please connect the CPU fan cable to the connector and match the black wire to the ground pin.



*Though this motherboard provides 4-Pin CPU fan (Quiet Fan) support, the 3-Pin CPU fan still can work successfully even without the fan speed control function. If you plan to connect the 3-Pin CPU fan to the CPU fan connector on this motherboard, please connect it to Pin 1-3.*

## SATA3 Connector

(SATA3\_1)

(see p. 4, No. 17)



Pin	Signal Name
1	GND
2	SATA-A+
3	SATA-A-
4	GND
5	SATA-B-
6	SATA-B+
7	GND

The Serial ATA3 (SATA3) connector supports SATA data cables for internal storage devices. The current SATA3 interface allows up to 6.0 Gb/s data transfer rate.

SATA Power Output Connector

(4-pin SATA\_PWR1)

(see p. 4, No. 21)

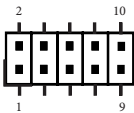


Pin	Signal Name
1	+5V
2	GND
3	GND
4	+12V

Digital Input/Output Pin Header

(10-pin JGPIO1)

(see p. 4, No. 23)



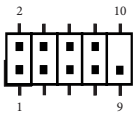
Pin	Signal Name	Signal Name	Pin
1	SIO_GP71	GPP_B15	2
3	SIO_GP72	GPP_E1	4
5	SIO_GP73	GPP_E2	6
7	SIO_GP74	GPP_E13	8
9	JGPIOPWR	GND	10

Parameter	Range
GPIO input Low voltage	Max: 0.8V
GPIO input High voltage	Low: 2V
GPIO output Low voltage	Max: 0.4V
GPIO output High voltage	Low: 2.4V
Note: Max. load per GPI/O pin: 12mA Current Max. 1A per power pin.	

System Panel Header

(9-pin PANEL1)

(see p. 4, No. 24)



Pin	Signal Name	Signal Name	Pin
1	HDLED+	PLED+	2
3	HDLED-	PLED-	4
5	GND	PWRBTN#	6
7	RESET#	GND	8
9	GND		10

This header accommodates several system front panel functions.



Connect the power switch, reset switch and system status indicator on the chassis to this header according to the pin assignments below. Note the positive and negative pins before connecting the cables.

**PWRBTN (Power Switch):**

Connect to the power switch on the chassis front panel. You may configure the way to turn off your system using the power switch.

**RESET (Reset Switch):**

Connect to the reset switch on the chassis front panel. Press the reset switch to restart the computer if the computer freezes and fails to perform a normal restart.

**PLED (System Power LED):**

Connect to the power status indicator on the chassis front panel. The LED is on when the system is operating. The LED keeps blinking when the sys-tem is in S1 sleep state. The LED is off when the system is in S3/S4 sleep state or powered off (S5).

**HDLED (Hard Drive Activity LED):**

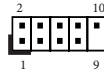
Connect to the hard drive activity LED on the chassis front panel. The LED is on when the hard drive is reading or writing data.

The front panel design may differ by chassis. A front panel module mainly consists of power switch, reset switch, power LED, hard drive activity LED, speaker and etc. When connecting your chassis front panel module to this header, make sure the wire assignments and the pin assign-ments are matched correctly.

### USB 2.0 Header

(9-pin USB2\_5\_6)

(see p. 4, No. 25)



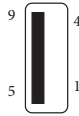
Pin	Signal Name	Signal Name	Pin
1	USB_PWR	USB_PWR	2
3	P-	P-	4
5	P+	P+	6
7	GND	GND	8
9		DUMMY	10

There is one USB 2.0 header on this motherboard.  
This USB 2.0 header can support two USB 2.0 Ports.

### USB3.2 Gen2 Port

(USB3\_3)

(see p. 4, No. 26)

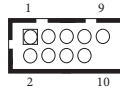


Pin	Signal Name
1	USB_PWR
2	USB_D-
3	USB_D+
4	GND
5	SSRX-
6	SSRX+
7	GND
8	SSTX-
9	SSTX+

### COM Port Headers

(9-pin COM1, 3, 4)

(see p. 4, No. 27)



Pin	Signal Name	Signal Name	Pin
1	DDCD#	RRXD	2
3	TTXD	DDTR#	4
5	GND	DDSR#	6
7	RRTS#	CCTS#	8
9	PWR		10



This motherboard supports RS232/422/485 on COM1, 3, 4 ports. Please refer to below table for the pin definition. In addition, COM1, 3, 4 ports (RS232/422/485) can be adjusted in BIOS setup utility > Advanced Screen > Super IO Configuration. You may refer to page 32 for details.

#### COM1, 3, 4 Port Pin Definition

Pin	RS232	RS422	RS485
1	DCD	TX-	RTX-
2	RXD	TX+	RTX+
3	TXD	RX+	NA
4	DTR	RX-	NA
5	GND	GND	GND
6	DSR	NA	NA
7	RTS	NA	NA
8	CTS	NA	NA
9	PWR	PWR	PWR



Buzzer Header

(2-pin BUZZ2)

(see p. 4, No. 28)



Pin	Signal Name
1	+5V
2	SPKR

Battery Connector

(BAT1)

(see p. 4 No. 29)



Pin	Signal Name
1	+BAT
2	GND

ATX Power Connector

(Input 12V-36V (Default); 12V only (by BOM option))

(4-pin DC\_IN1)

(see p. 4, No. 31)



Pin	Signal Name
1	GND
2	DC Input
3	DC Input
4	GND

Please connect a DC power supply to this connector.

\*+12V PWR in—system loading under 65W

+19V PWR in—system loading under 95W

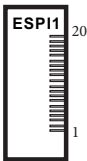
PWR in ≥ +24V for system loading over 95W

Back Side:

ESPI Header

(20-pin ESPI1)

(see p. 5, No. 33)

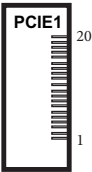


Pin	Signal Name
20	GND
19	ESPI_ALERT#
18	Internal use
17	Internal use
16	+3VSB
15	GND
14	ESPI_IO3
13	ESPI_IO2
12	ESPI_IO1
11	ESPI_IO0
10	SMB_DATA
9	SMB_CLK
8	GND
7	+3V
6	GND
5	ESPI_RESET#
4	ESPI_CS#
3	GND
2	ESPI_CLK
1	GND

PCIE Connector

(20-pin PCIE)

(see p. 5, No. 34)



\* Supports PCIE devices up to 10W.

Pin	Signal Name
20	+12V
19	+12V
18	+12V
17	+12V
16	+12V
15	GND
14	CLKREQ#
13	GND
12	PCIE_RXN
11	PCIE_RXP
10	GND
9	PCIE_TXN
8	PCIE_TXP
7	GND
6	CLKN
5	CLKP
4	GND
3	PLT_RST#
2	+12V
1	+12V

## Chapter 3 UEFI SETUP UTILITY

### 3.1 Introduction

ASRock Industrial UEFI (Unified Extensible Firmware Interface) is a BIOS utility which offers tweak-friendly options in an advanced viewing interface. The UEFI system works with a USB mouse and offers users a faster, sleeker experience.

This BIOS utility can perform the Power-On Self-Test (POST) during system startup, record hardware parameters of the system, load operating system, and so on. The battery on the motherboard supplies the power needed to the CMOS when the system power is turned off, and the values configured in the UEFI utility are kept in the CMOS.

Please note that inadequate BIOS settings may cause system instability, malfunction or boot failure. We strongly recommend that you do not alter the UEFI default configurations or change the settings only with the assistance of a trained service person.

If the system becomes unstable or fails to boot after you change the setting, try to clear the CMOS values and reset the board to default values. See your motherboard manual for instructions.

#### 3.1.1 Entering BIOS Setup

You may run the UEFI SETUP UTILITY by pressing <F2> or <Delete> right after you power on the computer; otherwise, the Power-On-Self-Test (POST) will continue with its test routines. If you wish to enter the UEFI SETUP UTILITY after POST, restart the system by pressing <Ctl> + <Alt> + <Delete>, or by pressing the reset button on the system chassis. You may also restart by turning the system off and then back on.

This setup guide explains how to use the UEFI SETUP UTILITY to configure all the supported system. The screenshots in this manual are for reference only. UEFI Settings and options may vary owing to different BIOS release versions or CPU installed. Please refer to the actual BIOS version of the motherboard you purchased for detailed screens, settings and options.

### 3.1.2 UEFI Menu Bar

The top of the screen has a menu bar with the following selections:

<b>Main</b>	For setting system time/date information
<b>Advanced</b>	For advanced system configurations
<b>H/W Monitor</b>	Displays current hardware status
<b>Security</b>	For security settings
<b>Boot</b>	For configuring boot settings and boot priority
<b>Exit</b>	Exit the current screen or the UEFI Setup Utility



*Because the UEFI software is constantly being updated, the following UEFI setup screens and descriptions for reference purpose only, and may vary from the latest BIOS and do not exactly match what you see on your screen.*

### 3.1.3 Navigation Keys

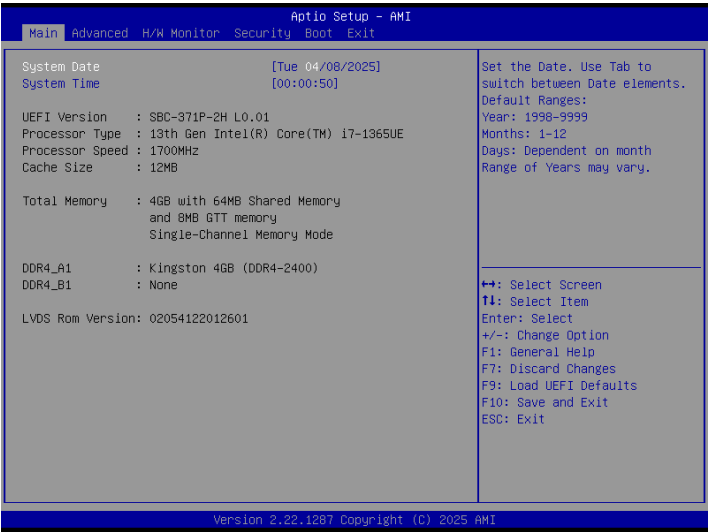
Use < ← > key or < → > key to choose among the selections on the menu bar, and use < ↑ > key or < ↓ > key to move the cursor up or down to select items, then press <Enter> to get into the sub screen. You can also use the mouse to click your required item.

Please check the following table for the descriptions of each navigation key.

Navigation Key(s)	Description
+ / -	To change option for the selected items
<Tab>	Switch to next function
<PGUP>	Go to the previous page
<PGDN>	Go to the next page
<HOME>	Go to the top of the screen
<END>	Go to the bottom of the screen
<F1>	To display the General Help Screen
<F7>	Discard changes and exit the SETUP UTILITY
<F9>	Load optimal default values for all the settings
<F10>	Save changes and exit the SETUP UTILITY
<F12>	Print screen
<ESC>	Jump to the Exit Screen or exit the current screen

### 3.2 Main Screen

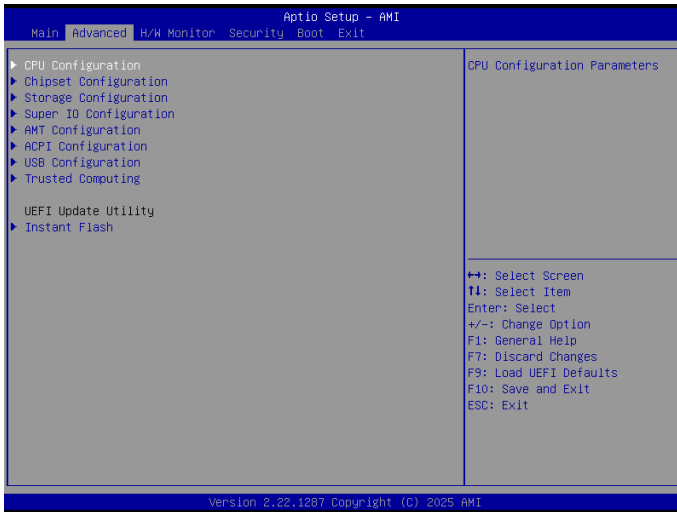
When you enter the UEFI SETUP UTILITY, the Main screen will appear and display the system overview.



*Because the UEFI software is constantly being updated, the following UEFI setup screens and descriptions are for reference purpose only, and they may not exactly match what you see on your screen. Options may also vary depending on the features of your motherboard.*

### 3.3 Advanced Screen

In this section, you may set the configurations for the following items: CPU Configuration, Chipset Configuration, Storage Configuration, Super IO Configuration, AMT Configuration, ACPI Configuration, USB Configuration and Trusted Computing.

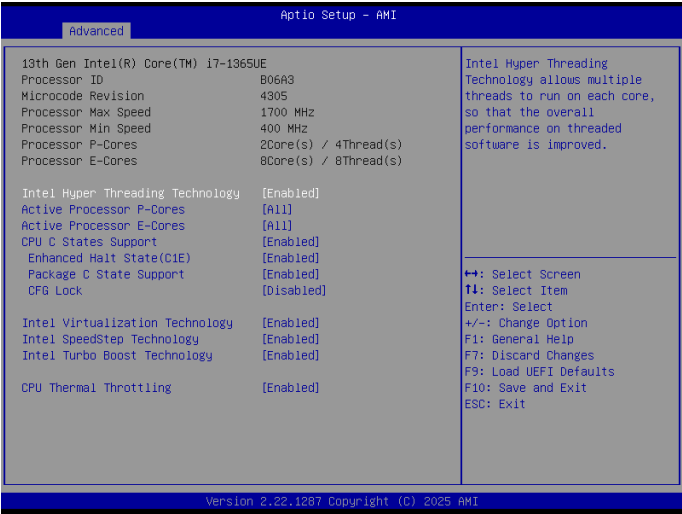


*Setting wrong values in this section may cause the system to malfunction.*

#### Instant Flash

Instant Flash is a UEFI flash utility embedded in Flash ROM. This convenient UEFI update tool allows you to update system UEFI without entering operating systems first like MS-DOS or Windows®. Just launch this tool and save the new UEFI file to your USB flash drive, floppy disk or hard drive, and then you can update your UEFI in only a few clicks without preparing an additional floppy diskette or other complicated flash utility. Please be noted that the USB flash drive or hard drive must use FAT32/16/12 file system. If you execute Instant Flash utility, the utility will show the UEFI files and their respective information. Select the proper UEFI file to update your UEFI, and reboot your system after UEFI update process completes.

### 3.3.1 CPU Configuration



#### Intel Hyper Threading Technology

Intel Hyper Threading Technology allows multiple threads to run on each core, so that the overall performance on threaded software is improved.

Configuration options: [Enabled] [Disabled]

#### Active Processor P-Cores

Allows you to select the number of cores to enable in each processor package.

#### Active Processor E-Cores

Allows you to select the number of E-Cores to enable in each processor package. NOTE: Number of P-Cores and E-Cores are looked at together. When both are {0,0}, Pcore will enable all cores.

#### CPU C States Support

Allows you to enable CPU C States Support for power saving. It is recommended to keep C3, C6 and C7 all enabled for better power saving.

Configuration options: [Enabled] [Disabled]



## Enhanced Halt State (C1E)

The option allows you to enable Enhanced Halt State (C1E) for lower power consumption.

Configuration options: [Enabled] [Disabled]

## Package C State Support

The option allows you to enable CPU, PCIe, Memory, Graphics C State Support for power saving.

## CFG Lock

The option allows you to enable or disable the CFG Lock.

Configuration options: [Enabled] [Disabled]

## Intel Virtualization Technology

Intel Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions, so that one computer system can function as multiple virtual systems.

Configuration options: [Enabled] [Disabled]

## Intel SpeedStep Technology

Intel SpeedStep technology allows processors to switch between multiple frequencies and voltage points for better power saving and heat dissipation. CPU turbo ratio can be fixed when Intel SpeedStep Technology is set to [Disabled] and Intel Turbo Boost Technology is set to [Enabled].

Configuration options: [Enabled] [Disabled].

If you install Windows® 10 and want to enable this function, please set this item to [Enabled]. This item will be hidden if the current CPU does not support Intel SpeedStep technology.



*Please note that enabling this function may reduce CPU voltage and lead to system stability or compatibility issues with some power supplies. Please set this item to [Disabled] if above issues occur.*

---

## Intel Turbo Boost Technology

Intel Turbo Boost Technology enables the processor to run above its base operating frequency when the operating system requests the highest performance state. The default value is [Enabled].

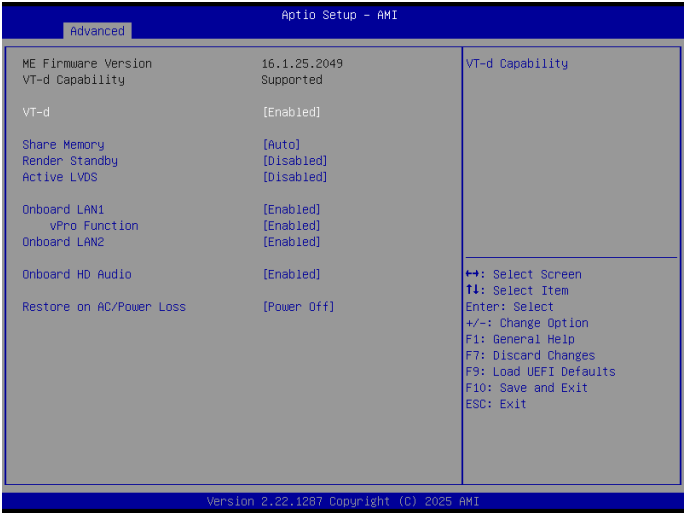
Configuration options: [Enabled] [Disabled]

## CPU Thermal Throttling

CPU Thermal Throttling allows you to enable CPU internal thermal control mechanisms to keep the CPU from overheating.

Configuration options: [Enabled] [Disabled]

### 3.3.2 Chipset Configuration



#### VT-d

Intel® Virtualization Technology for Directed I/O helps your virtual machine monitor better utilize hardware by improving application compatibility and reliability, and providing additional levels of manageability, security, isolation, and I/O performance.

Configuration options: [Enabled] [Disabled]

#### Share Memory

Share memory allows you to configure the size of memory that is allocated to the integrated graphics processor when the system boots up.

Configuration options: [Auto] [32M] [64M] [128M] [256M] [512M] [1024M]

Options vary depending on the memory you use on your motherboard.

#### Render Standby

Power down the render unit when the GPU is idle for lower power consumption.

#### Active LVDS

Use this to enable or disable the LVDS. The default value is [Disabled]. Set the item to [Enabled]. Then press <F10> to save the setting and restart the system. Now the default value of Active LVDS is changed to [Enabled] (F9 load default is also set to [Enabled]).

---

Change the setting from [Enabled] to [Disabled], and then press <F10> to save the setting and restart the system. Likewise, the default value of Active LVDS is changed to [Disabled] (F9 load default is also set to [Disabled]).

## Onboard LAN1

This allows you to enable or disable the Onboard LAN1 feature.

## vPro Function

Enable/Disable vPro SMLink of LAN port. Select Enabled if you would like to utilize LAN port with vPro. Select Disabled if you would like to utilize LAN port as DHCP Server. Please turn off the computer and unplug the power cord from the power supply after the setting has been changed.

## Onboard LAN2

This allows you to enable or disable the Onboard LAN2 feature.

## Onboard HD Audio

Onboard HD Audio allows you to enable or disable the onboard HD audio controller. Set this item to [Auto] to enable the onboard HD and automatically disable it when a sound card is installed.

Configuration options: [Auto] [Enabled] [Disabled]

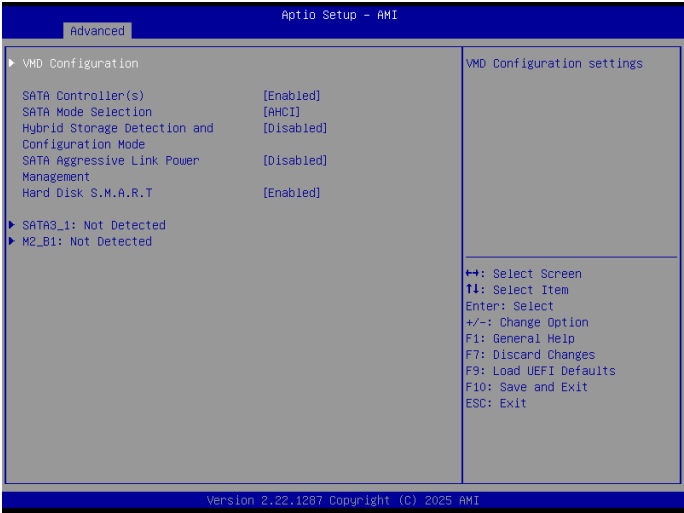
## Restore on AC/Power Loss

Allows you to select the power state after a power failure.

[Power Off] sets the power to remain off when the power recovers.

[Power On] sets the system to start to boot up when the power recovers.

### 3.3.3 Storage Configuration



#### VMD Configuration

Press [Enter] to view the followings items for VMD configurations.

#### SATA Controller(s)

Allows you to enable or disable the SATA controllers.

Configuration options: [Enabled] [Disabled]

#### SATA Mode Selection

AHCI: Supports new features that improve performance.

Configuration option: [AHCI]

#### Hybrid Storage Detection and Configuration Mode

Hybrid Storage Detection and Configuration Mode allows you to select Hybrid Storage Detection and Configuration Mode.

Configuration options: [Dynamic Configuration for Hybrid Storage Enable] [Disabled]

---

## SATA Aggressive Link Power Management

SATA Aggressive Link Power Management allows SATA devices to enter a low power state during periods of inactivity to save power. It is supported only by AHCI mode.

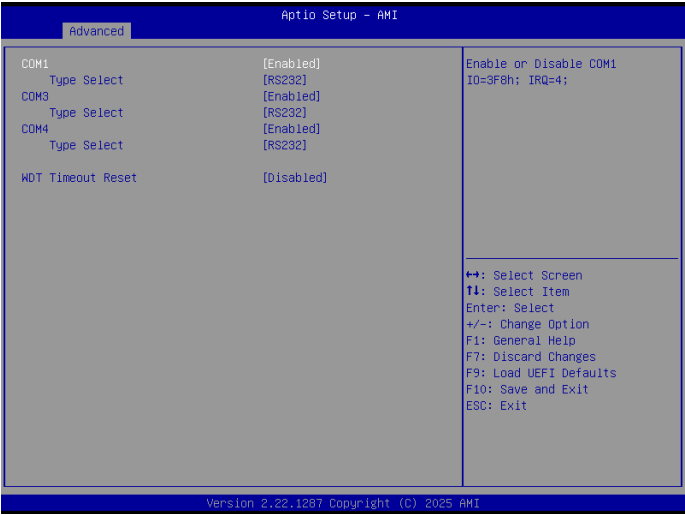
Configuration options: [Enabled] [Disabled]

## Hard Disk S.M.A.R.T.

S.M.A.R.T stands for Self-Monitoring, Analysis, and Reporting Technology. It is a monitoring system for computer hard disk drives to detect and report on various indicators of reliability.

Configuration options: [Enabled] [Disabled]

### 3.3.4 Super IO Configuration



#### COM1 Configuration

Use this to set parameters of COM1.

##### Type Select

Use this to select COM1 port type: [RS232], [RS422] or [RS485].

#### COM3 Configuration

Use this to set parameters of COM3.

##### Type Select

Use this to select COM1 port type: [RS232], [RS422] or [RS485].

#### COM4 Configuration

Use this to set parameters of COM4.

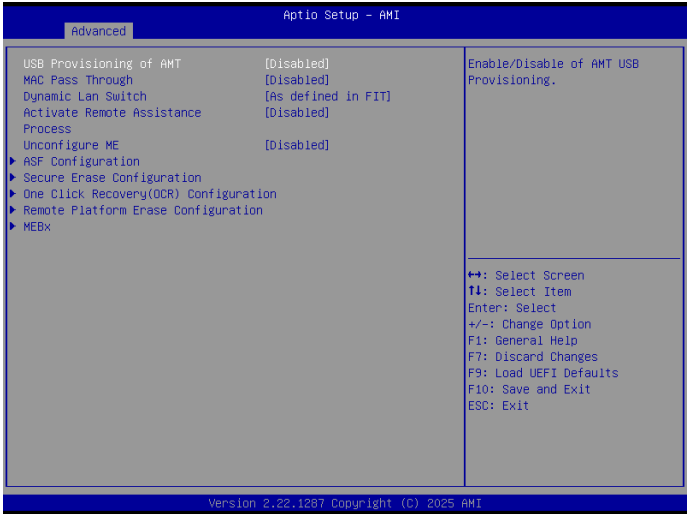
##### Type Select

Use this to select COM1 port type: [RS232], [RS422] or [RS485].

#### WDT Timeout Reset

Use this to set the Watch Dog Timer.

### 3.3.5 AMT Configuration



#### USB Provisioning of AMT

Use this to enable or disable AMT USB Provisioning. The default is [Disabled].

#### MAC Pass Through

The option enables or disables MAC Pass Through function.

#### Dynamic Lan Switch

This allows switching AMT support from Integrated LAN to Discrete LAN.

#### Activate Remote Assistance Process

Trigger CIRA boot. The default is [Disabled].

#### Un-Configure ME

Un-Configure ME without password. The default is [Disabled].

#### ASF Configuration

The option allows you to configure Alert Standard Format parameters.

#### Secure Erase Configuration

Secure Erase configuration menu.



## One Click Recovery(OCR) Configuration

Configuration setting for One Click Recovery. This allows access for AMT to boot a recovery OS application.

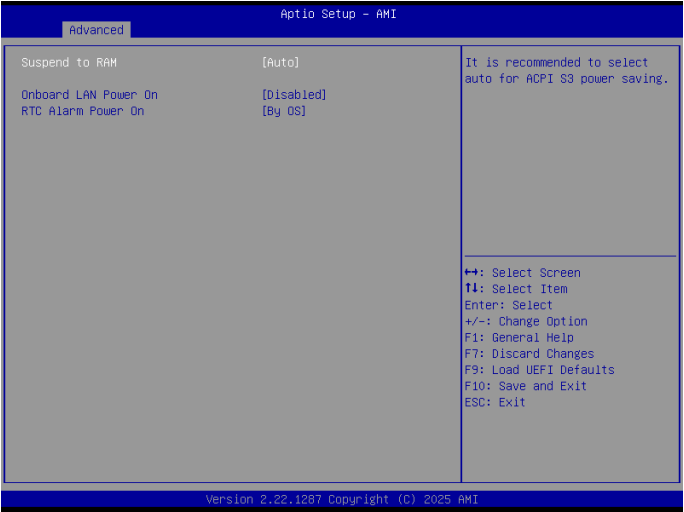
## Remote Platform Erase Configuration

Remote Platform Erase configuration menu.

## MEBx

This Formset contains forms for configuring MEBx.

### 3.3.6 ACPI Configuration



#### Suspend to RAM

Suspend to RAM allows you to select [Disabled] for ACPI suspend type S1. It is recommended to select [Auto] for ACPI S3 power saving.

Configuration options: [Auto] [Disabled]

#### Onboard LAN Power On

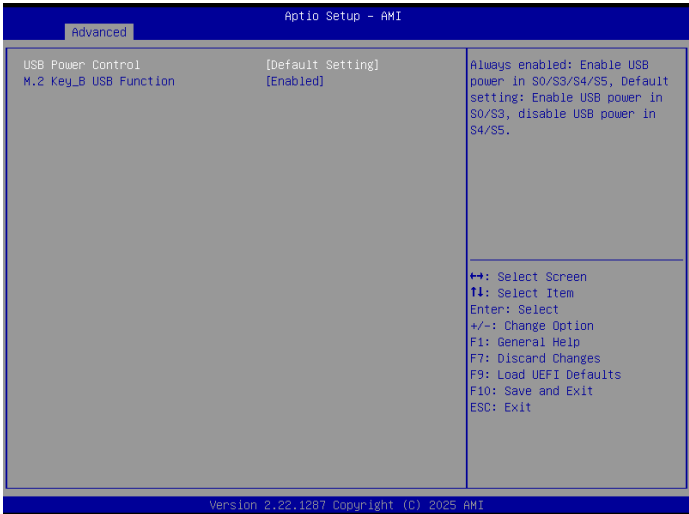
Use this item to enable or disable onboard LAN to turn on the system from the power-soft-off mode.

#### RTC Alarm Power On

RTC Alarm Power On allows the system to be waked up by the real time clock alarm. Set it to By OS to let it be handled by your operating system.

Configuration options: [Enabled] [Disabled] [By OS]

### 3.3.7 USB Configuration



#### USB Power Control

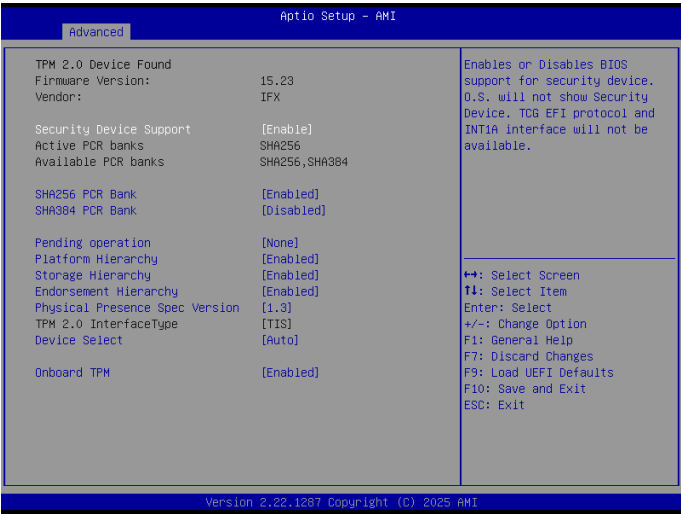
Use this option to control USB power.

#### M.2 Key\_B USB Function

Use this item to enable or disable M.2 Key\_B USB Configuration.

Configuration options: [Enabled] [Disabled]

### 3.3.8 Trusted Computing



NOTE: Options vary depending on the version of your connected TPM module.

#### Security Device Support

Security Device Support allows you to enable or disable BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

Configuration options: [Enabled] [Disabled]

#### Active PCR banks

This item displays active PCR Banks.

#### Available PCR Banks

This item displays available PCR Banks.

#### SHA256 PCR Bank

SHA256 PCR Bank allows you to enable or disable SHA256 PCR Bank.

Configuration options: [Enabled] [Disabled]

## Pending Operation

Pending Operation allows you to schedule an Operation for the Security Device.

NOTE: Your computer will reboot during restart in order to change State of the Device.

Configuration options: [None] [TPM Clear]

## Platform Hierarchy

This item allows you to enable or disable Platform Hierarchy.

Configuration options: [Enabled] [Disabled]

## Storage Hierarchy

This item allows you to enable or disable Storage Hierarchy.

Configuration options: [Enabled] [Disabled]

## Endorsement Hierarchy

This item allows you to enable or disable Endorsement Hierarchy.

Configuration options: [Enabled] [Disabled]

## Physical Presence Spec Version

Select this item to tell OS to support PPI spec version 1.2 or 1.3. Please note that some HCK tests might not support version 1.3.

Configuration options: [1.2] [1.3]

## TPM 2.0 InterfaceType

This item allows you to view the Communication Interface to TPM 2.0 Device: CRB or ITS.

## Device Select

This item allows you to select the TPM device to be supported.

[TPM 1.2] restricts support to TPM 1.2 devices.

[TPM 2.0] restricts support to TPM 2.0 devices.

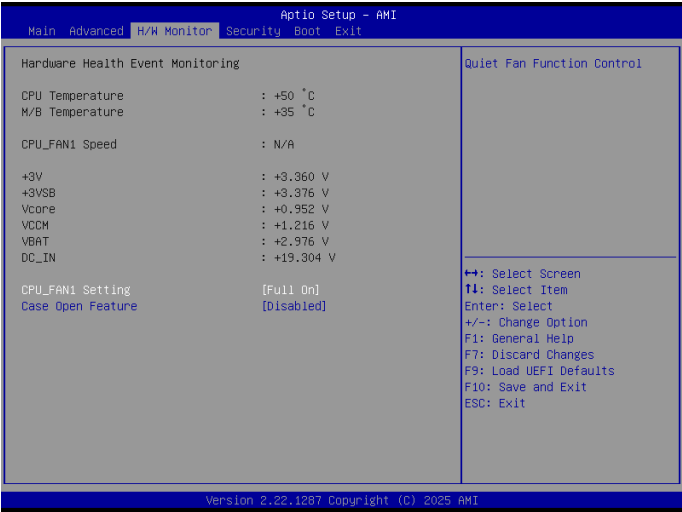
[Auto] supports both TPM 1.2 and TPM 2.0 devices with the default set to TPM 2.0 devices. If TPM 2.0 devices are not found, TPM 1.2 devices will be enumerated.

## Onboard TPM

Enable/disable Intel PTT in ME. Disable this option to use discrete TPM Module.

### 3.4 Hardware Health Event Monitoring Screen

This section allows you to monitor the status of the hardware on your system, including the parameters of the CPU temperature, motherboard temperature, CPU fan speed, and the critical voltage.



NOTE: Options vary depending on the features of your motherboard.

#### CPU\_Fan 1 Setting

This item allows you to select a fan mode for CPU Fan 1. The default value is [Full On].

Configuration options: [Full On] [Automatic Mode]

#### Case Open Feature

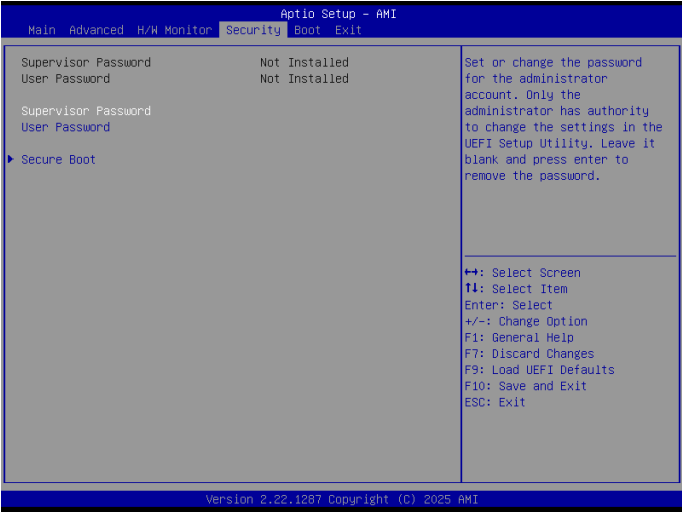
This item allows you to enable or disable case open detection feature. The default is value [Disabled].

#### Clear Status

This option appears only when the case open has been detected. Use this option to keep or clear the record of previous chassis intrusion status.

### 3.5 Security Screen

In this section you may set or change the supervisor/user password for the system. You may also clear the user password.



#### Supervisor Password

Set or change the password for the administrator account. Only the administrator has authority to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

#### User Password

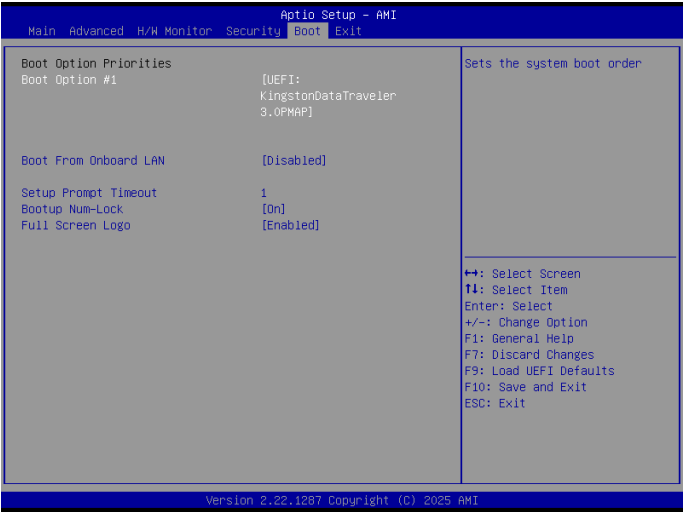
Set or change the password for the user account. Users are unable to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

#### Secure Boot

Press [Enter] to configure the Secure Boot Settings. The feature protects the system from unauthorized access and malwares during POST.

## 3.6 Boot Screen

This section displays the available devices on your system for you to configure the boot settings and the boot priority.



### Boot Option #1

The item allows you to set the system boot order.

### Boot From Onboard LAN

The item allows the system to be waked up by the onboard LAN.

Configuration options: [Enabled] [Disabled]

### Setup Prompt Timeout

The item allows you to configure the number of seconds to wait for the UEFI setup utility.

Configuration options: [1] - [65535]

### Bootup Num-Lock

The item allows you to select whether Num Lock should be turned on or off when the system boots up.

Configuration options: [On] [Off]

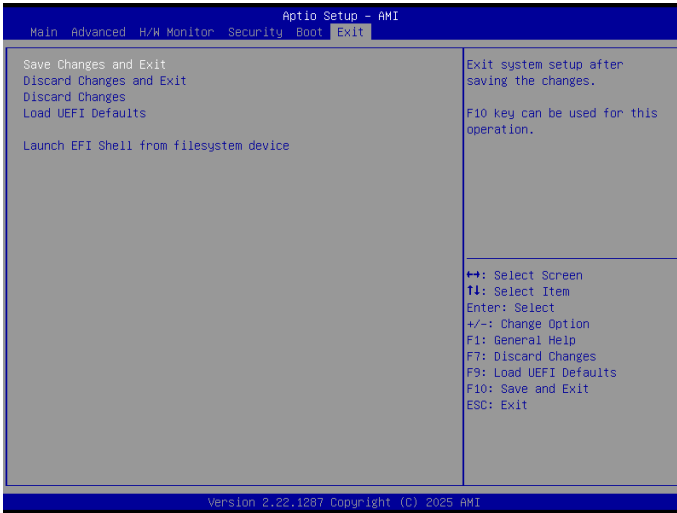
### Full Screen Logo

[Enabled] Select this item to display the boot logo.

[Disabled] Select this item to show normal POST messages.



### 3.7 Exit Screen



#### Save Changes and Exit

When you select this option, the following message “Save configuration changes and exit setup?” will pop out. Press <F10> key or select [Yes] to save the changes and exit the UEFI SETUP UTILITY.

#### Discard Changes and Exit

When you select this option, the following message “Discard changes and exit setup?” will pop out. Press <ESC> key or select [Yes] to exit the UEFI SETUP UTILITY without saving any changes.

#### Discard Changes

When you select this option, the following message “Discard changes?” will pop out. Press <F7> key or select [Yes] to discard all changes.

#### Load UEFI Defaults

The item allows you to load UEFI default values for all options. The F9 key can be used for this operation.

#### Launch EFI Shell from filesystem device

The item allows you to copy shellx64.efi to the root directory to launch EFI Shell.