ASRock Industrial

IMB-1006

User Manual

Version 1.2
Updated July 11, 2023

Version 1.0
Published May, 2023

Copyright Notice:

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.

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.

HIGH-DEFINITION MULTIMEDIA INTERFACE

WARNING

THIS PRODUCT CONTAINS A BUTTON 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"

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)

UK
CA

ASRockInd INC. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related UKCA Directives. Full text of UKCA declaration of conformity is available at: http://www.asrockind.com

CE

ASRockInd INC. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related Directives. Full text of EU declaration of conformity is available at: http://www.asrockind.com

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.

Please refer to https://www.asrockind.com/general/about.asp?cat=Responsibility for information disclosure based on regulation requirements ASRockInd is complied with.

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.

Contents

Chapter 1 Introduction **1**

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

Chapter 2 Installation **9**

2.1 Screw Holes 9

2.2 Pre-installation Precautions 9

2.3 Installation of Memory Modules 10

2.4 Expansion Slots 11

2.5 Jumpers Setup 12

2.6 Onboard Headers and Connectors 15

Chapter 3 UEFI SETUP UTILITY **22**

3.1 Introduction 22

3.1.1 Entering BIOS Setup 22

3.1.2 UEFI Menu Bar 23

3.1.3 Navigation Keys 24

3.2 Main Screen (Advanced Mode) 25

3.3 Advanced Screen 26

3.3.1 CPU Configuration 27

3.3.2 Chipset Configuration 30

3.3.3 Storage Configuration 32
3.3.4 Super IO Configuration 34
3.3.5 ACPI Configuration 35
3.3.6 USB Configuration 36
3.3.7 Trusted Computing 37
3.4 Hardware Health Event Monitoring Screen 39
3.5 Security Screen 40
3.6 Boot Screen 42
3.7 Exit Screen 43

Chapter 1 Introduction

Thank you for purchasing ASRockInd ***IMB-1006*** 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. You may find the latest CPU support lists on ASRockInd website as well.

ASRockInd website https://www.asrockind.com/

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/support/index.asp

1.1 Package Contents

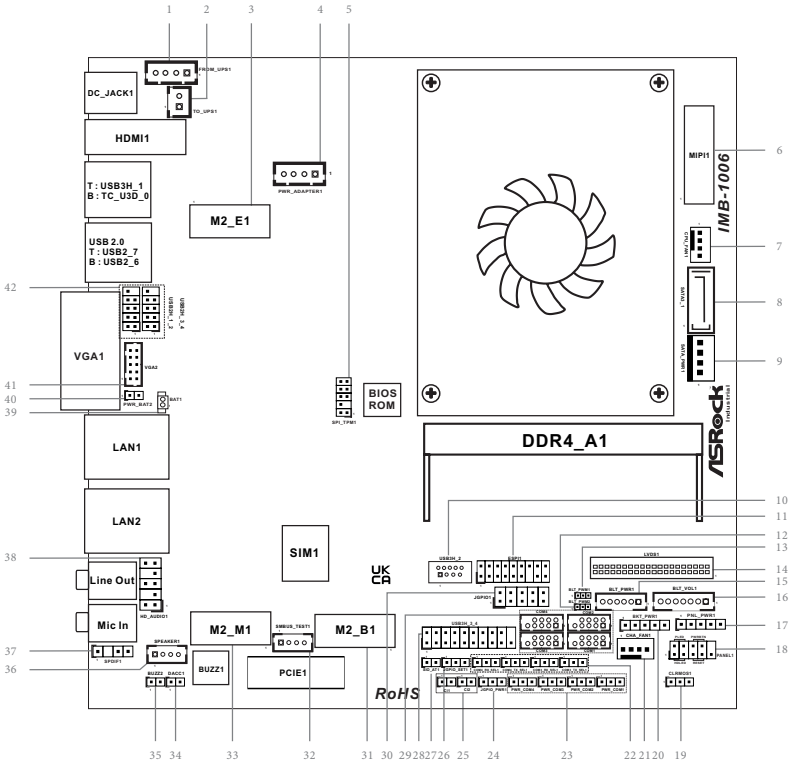
ASRockInd ***IMB-1006*** Motherboard (Mini-ITX (6.7-in x 6.7-in x 1.5-in, 17.0 cm x 17.0 cm x 3.8 cm))

1.2 Specifications

Form Factor	Dimensions	Mini-ITX (6.7-in x 6.7-in x 1.5-in, 17.0 cm x 17.0 cm x 3.8 cm)
Processor System	CPU	Intel® Alder Lake-N SoC Processors IMB-1006J (N97, QC, Max Speed Up to 3.6GHz, 12W) *For other CPU SKUs request, please contact regional Sales for availability
	Chipset	SoC
	BIOS	AMI SPI 256 Mbit
Memory	Technology	Single Channel DDR4 3200 MHz
	Capacity	16GB
	Socket	1 x 260-pin SO-DIMM
Graphics	Controller	Intel® UHD Graphics
	HDMI	HDMI 2.0b Max resolution up to 4096 x 2160@60Hz
	DisplayPort	DisplayPort 1.4a Max resolution up to 4096 x 2160@60Hz
	VGA	Max resolution up to 1920 x 1200@60Hz
	LVDS	Dual channel 24 bit up to 1920 x 1200@60Hz (connector shared with eDP)
	eDP	Max resolution up to 1920 x 1080@60Hz (connector shared with LVDS)
	Multi Display	Triple display (included 1 output from Type-C)
Expansion Slot	PCIe	1 x PCIex1 (Gen3)
	M.2	1 x M.2 (Key E, 2230) with PCIex1 ,USB 2.0 and CNVi for Wireless 1 x M.2 (Key B, 3042/3052) with PCIex1, USB 3.2 Gen1, USB 2.0 and SIM for 4G/5G
	SIM Socket	1 x SIM socket connected to M.2 key B
Audio	Interface	Interface Realtek ALC662/ALC897 HD, High Definition Audio. Mic-in, Line-out
Ethernet	Controller/ Speed	LAN1: Realtek RTL8125BG with 10/100/1000/2500 Mbps LAN2: Realtek RTL8125BG with 10/100/1000/2500 Mbps
	Controller	2 x RJ-45
Rear I/O	HDMI	1 x HDMI2.0b
	DisplayPort	1 x DP1.4a
	VGA	1
	Ethernet	2 x 2.5 Gigabit LAN
	USB	1 x USB 3.2 Gen2 (Type-C, 5V/3A, supports DP1.4a display output) 1 x USB 3.2 Gen1 2 x USB 2.0
	Audio	2 (Mic-In, Line-Out)
	DC Jack	1

Internal Connector	USB	3 x USB 3.2 Gen1 (1 x USB 3.2 header, 1 x USB 3.2 Gen1 Type-A vertical connector) 4 x USB 2.0 (2x2.54 pitch header)
	COM	COM1, COM2 (RS-232/422/485) COM3, COM4 (RS-232/TTL-5V)
	GPIO	4 x GPI, 4 x GPO
	TPM	TPM Header
	LVDS	1 (Connector with LVDS/eDP signal, switch by BIOS)
	VGA	1
	SATA PWR Output	1
	Speaker Header	1
	MIPI Camera Header	1 (optional)
Storage	M.2	1 x M.2 (Key M, 2242/2260/2280) with PCIe Gen3x1 or SATA3 and USB 2.0 for SSD
	SATA	1 x SATA3 (6Gb/s)
Watchdog Timer	Output	From Super I/O to drag RESETCON#
	Interval	256 Segments, 0, 1, 2, ...255 Sec
Power Requirements	Input PWR	12~28V DC-In with 4-pin wafer PWR cable or DC Jack
	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 Temp	-20°C - 70°C
	Storage Temp	-40°C - 85°C
	Operating Humidity	5% - 90%
	Storage Humidity	5% - 90%

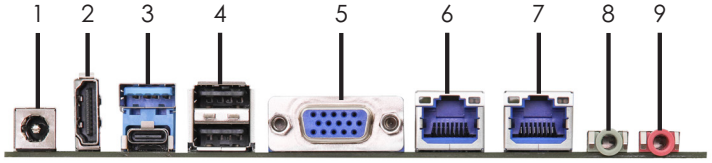
1.3 Motherboard Layout



1 : 4-pin DC-in PWR Connector (Input +12V~+28V) & UPS Module Power Output Connector (FROM_UPS1)
2 : 2-pin UPS Module Power Input Connector (TO_UPS1)
3 : M.2 Key-E Socket (M2_E1)
4 : PWR_ADAPTER1
5 : SPI_TPM Header (SPI_TPM1)
6 : MIPI Connector (MIPI1)
7 : CPU FAN Connector (+12V) (CPU_FAN1)
8 : SATA3 Connector (SATA3_1)
9 : SATA Power Output Connector (SATA_PWR1)
10 : USB 3.2 Gen1 Connector (Type A) (USB3H_2)
11 : ESPI Header (ESPI1)
12 : CON_LBKLT_CTL Voltage Level (BLT_PWM2)
13 : Brightness Control Mode (BLT_PWM1)
14 : LVDS Panel Connector (LVDS1)
15 : Backlight Power Connector (BLT_PWR1)
16 : Backlight Volume Control (BLT_VOL1)
17 : eDP and LVDS Panel Power Select (LCD_VCC) (PNL_PWR1)
18 : System Panel Header (PANEL1)
19 : Clear CMOS Header (CLRMOS1)
20 : eDP and LVDS Backlight Power Select (LCD_BLT_VCC) (BKT_PWR1)
21 : 4-pin Chassis FAN Connector (+12V) (CHA_FAN1)
22 : COM3, COM4 TX RX Selection Header
(From left to right)
COM4_RX_SEL1
COM4_TX_SEL1
COM3_RX_SEL1
COM3_TX_SEL1
23 : COM Port PWR Setting Headers (PWR_COM1~4)
24 : Digital Input / Output Power Select (JGPIO_PWR) (JGPIO_PWR1)
25 : Chassis Intrusion Headers (CI1, CI2)
26 : Digital Input / Output Default Value Setting (JGPIO_SET1)
27 : ATX/AT Mode Jumper (SIO_AT1)
28 : USB 3.2 Gen1 Connector (USB3H_3_4)
29 : Internal COM Port Headers
COM1, 2 (RS232/422/485)
COM3, 4 (RS232)
30 : Digital Input/Output Pin Header (JGPIO1)
31 : M.2 Key-B Socket (M2_B1)
32 : SMB_TEST1 (SMBUS_TEST1)
33 : M.2 Key-M Socket (M2_M1)

34 : DACC Jumper (DACC1)
35 : Buzzer Header (BUZZ2)
36 : 3W Audio AMP Output Wafer (SPEAKER1)
37 : SPDIF Header (SPDIF1)
38 : Front Panel Audio Header (HD_AUDIO1)
39 : Battery Connector (BAT1)
40 : PWR_BAT2
41 : VGA Header (VGA2)
42 : USB 2.0 Headers (USB2H_1~4)

1.4 I/O Panel



1 DC Jack (DC_JACK1)
2 HDMI Port (HDMI1)
3 Top : USB 3.2 Gen1 Port (USB3H_1)
Bottom : USB 3.2 Gen2 Type-C Port (TC_U3D_0)
4 Top : USB 2.0 Port (USB2_7)
Bottom : USB 2.0 Port (USB2_6)
5 D-Sub Port (VGA1)
6 RJ45 LAN Port (LAN1)*
7 RJ45 LAN Port (LAN2)*
8 Audio Output : Green – Line Out
9 Audio Output : Pink – Mic In

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

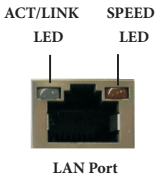
LAN Port LED Indications

Activity/Link LED

Status	Description
Off	No Link
Blinking	Data Activity
On	Link

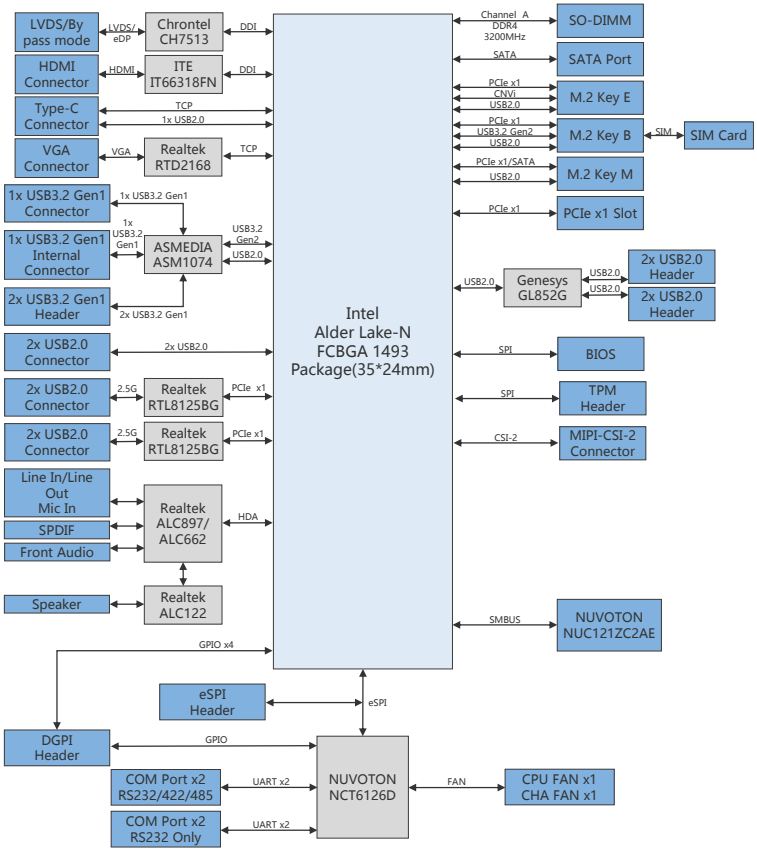
SPEED LED

Status	Description
Off	10Mbps connection
Orange	100/1000Mbps connection
Green	2.5Gbps connection



1.5 Block Diagram

IMB-1006



Chapter 2 Installation

This is a Mini-ITX (6.7-in x 6.7-in x 1.5-in, 17.0 cm x 17.0 cm x 3.8 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

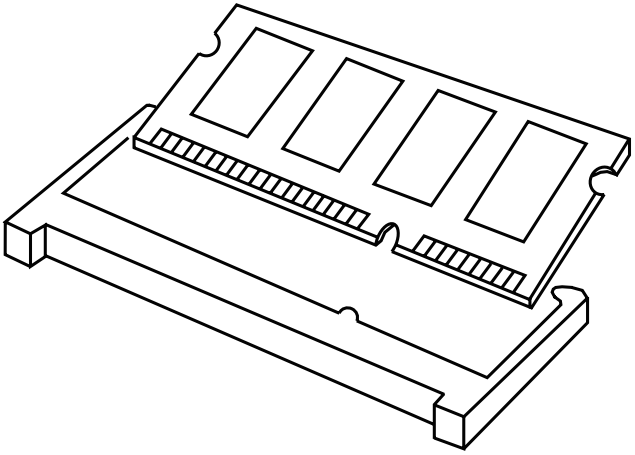
IMB-1006 provides one 260-pin DDR4 (Double Data Rate 4) SO-DIMM slots, and supports single Channel Memory Technology.

1. *Please make sure to disconnect the power supply before adding or removing SO-DIMMs or the system components.*
2. *It is not allowed to install a DDR, DDR2, or DDR3 memory module into a DDR4 slot; otherwise, this motherboard and DIMM may be damaged.*

The DIMM only fits in one correct orientation. It will cause permanent damage to the motherboard and the DIMM if you force the DIMM into the slot in the incorrect orientation.

Installing a SO-DIMM

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



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 1 PCI Express Gen3 slot, 3 M.2 sockets and 1 SIM socket on this motherboard.

PCIE slot: PCIE1 (PCIe x1 slot) is used for PCIe Gen3 x1 lane width card.

M.2 sockets: 1 x M.2 (Key E, 2230) with PCIex1, USB 2.0 and CNVi for Wireless
1 x M.2 (Key B, 3042/3052) with PCIex1, USB 3.2 Gen1, USB 2.0 and SIM for 4G/5G
1 x M.2 (KeyM, 2242/2260/2280) with PCIe Gen3x1 or SATA3 and USB 2.0 for SSD

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

M.2 Key-M Socket (M2_M1)

Pin	Signal Name	Signal Name	Pin
1	GND	+3.3V	2
3	GND	+3.3V	4
5	NA	NA	6
7	NA	NA	8
9	GND	SATA_LED	10
11	NA	+3.3V	12
13	NA	+3.3V	14
15	GND	+3.3V	16
17	NA	+3.3V	18
19	NA	NA	20
21	GND	NA	22
23	NA	NA	24
25	PETp2	NA	26
27	GND	NA	28
29	NA	NA	30
31	NA	GND	32
33	GND	USB_D+	34
35	NA	USB_D-	36
37	NA	NA	38
39	GND	NA	40
41	PERn0 / SATA-B+	NA	42
43	PERp0 / SATA-B-	NA	44
45	GND	NA	46
47	PETn0 / SATA-A-	NA	48
49	PETp0 / SATA-A+	PERST#	50
51	GND	CLKREQ#	52
53	PEFCLKn	WAKE#	54
55	PEFCLKp	NA	56
57	GND	NA	58
67	NA	NA	68
69	PEDET	+3.3V	70
71	GND	+3.3V	72
73	GND	+3.3V	74
75	GND		

M.2 Key-B Socket (M2_B1)

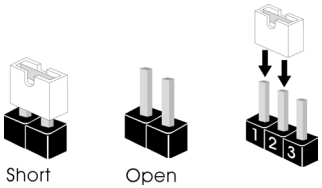
Pin	Signal Name	Signal Name	Pin
1	NA	+3.3V	2
3	GND	+3.3V	4
5	GND	FULL_Card_ Power_off	6
7	USB_D+	W_DISABLE1#	8
9	USB_D-	WWAN_LED#	10
11	GND		
		NA	20
21	GND	NA	22
23	NA	NA	24
25	NA	W_DISABLE2#	26
27	GND	NA	28
29	USB3_RX-	UIM_RESET	30
31	USB3_RX+	UIM_CLK	32
33	GND	UIM_DATA	34
35	USB3_TX-	UIM_PWR	36
37	USB3_TX+	NA	38
39	GND	NA	40
41	PERn0	NA	42
43	PERp0	NA	44
45	GND	NA	46
47	PETn0	NA	48
49	PETp0	PERST#	50
51	GND	CLKREQ#	52
53	PEFCLKn	WAKE#	54
55	PEFCLKp	NA	56
57	GND	NA	58
59	NA	NA	60
61	NA	NA	62
63	NA	NA	64
65	NA	NA	66
67	NA	NA	68
69	PEDET	+3.3V	70
71	GND	+3.3V	72
73	GND	+3.3V	74
75	NA		

M.2 Key-E Socket (M2_E1)

Pin	Signal Name	Signal Name	Pin
1	GND	+3.3V	2
3	USB_D+	+3.3V	4
5	USB_D-	NA	6
7	GND	NA	8
9	CNV_WGR_D1-	CNV_RF_ RESET	10
11	CNV_WGR_ D1+	NA	12
13	GND	MODEM_ CLKREQ	14
15	CNV_WGR_D0-	NA	16
17	CNV_WGR_ D0+	GND	18
19	GND	NA	20
21	CNV_WGR_ CLK-	CNV_BRI_RSP	22
23	CNV_WGR_ CLK+		
33	GND	CNV_BGI_DT	32
35	PETp	CNV_RGI_RSP	34
37	PETn	CNV_BRI_DT	36
39	GND	NA	38
41	PERp	NA	40
43	PERn	NA	42
45	GND	NA	44
47	PEFCLKp	NA	46
49	PEFCLKn	NA	48
51	GND	SUSCLK	50
53	CLKREQ#	PERST0#	52
55	NA	W_DISABLE1#	54
57	GND	W_DISABLE2#	56
59	CNV_WT_D1-	SMB_DATA	58
61	CNV_WT_D1+	SMB_CLK	60
63	GND	NA	62
65	CNV_WT_D0-	NA	64
67	CNV_WT_D0+	NA	66
69	GND	NA	68
71	CNV_WT_CLK-	NA	70
73	CNV_WT_ CLK+	+3.3V	72
75	GND	+3.3V	74

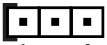
2.5 Jumpers Setup

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**

CON_LBKLT_CTL Voltage Level
(3-pin BLT_PWM2)
(see p. 4, No. 12)



Setting	Description
1-2	+3V (Default)
2-3	+5V

Brightness Control Mode
(3-pin BLT_PWM1)
(see p. 4, No. 13)

Setting	Description
1-2	From eDP PWM to CON_LBKLT_CTL
2-3	From LVDS PWM to CON_LBKLT_CTL (Default)

Note: 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.

---

eDP and LVDS Panel Power Select (LCD_VCC)
(5-pin PNL_PWR1)
(see p. 4, No. 17)

Setting	Description
1-2	LCD_VCC: +3V (Default)
2-3	LCD_VCC: +5V
4-5	LCD_VCC: +12V

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

Clear CMOS Header
(3-pin CLRMOS1)
(see p. 4, No. 19)

Setting	Description
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 pin 2 and pin 3 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 date, time, user default profile will be cleared only if the CMOS battery is removed.

---

eDP and LVDS Backlight Power Select (LCD_BLT_VCC)
(5-pin BKT_PWR1)
(see p. 4, No. 20)

Setting	Description
1-2	LCD_BLT_VCC: +5V (Default)
2-3	LCD_BLT_VCC: +12V
4-5	LCD_BLT_VCC: DC Input

Use this to set up the backlight power of the LVDS connector and the panel backlight power of BLT_PWM1.

COM3, COM4 TX RX Selection Headers
(from left to right: 3-pin
COM4_RX_SEL1
COM4_TX_SEL1
COM3_RX_SEL1
COM3_TX_SEL1)
(see p. 4, No. 22)

Setting	Description
1-2	TTL: 0V~5V
2-3	-5V~+5V (RS-232) (Default)

COM Port PWR Setting Headers
(3-pin PWR_COM1~4 (For COM Port1~4))
(see p. 4, No. 23)

Setting	Description
1-2	+5V (Default)
2-3	+12V

The maximum current for per port is 1A, and the power supply is either 5V or 12V. Use the jumper to set the power for COM port pin 9.

Digital Input / Output Power Select (JGPIO_PWR)
(3-pin JGPIO_PWR1)
(see p. 4, No. 24)

Setting	Description
1-2	+12V
2-3	+5V (Default)

Chassis Intrusion Headers

(2-pin CI1, CI2)

(see p. 4, No. 25)

CI1

Setting	Description
Close	Active Case Open
Open	Normal (Default)

CI2

Setting	Description
Close	Normal (Default)
Open	Active Case Open

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.

Digital Input / Output Default Value Setting

(3-pin JGPIO_SET1)

(see p. 4, No. 26)

Setting	Description
1-2	Pull-High (Default)
2-3	Pull-Low

The header is used for GPIO default value setting for either pull high or pull low. Pulling the header to a high/low value means the voltage is anchored to VCC/GND, in a stable, non-floating state.

ATX/AT Mode Jumper

(2-pin SIO_AT1)

(see p. 4, No. 27)

Setting	Description
Open	ATX Mode (Default)
Short	AT Mode

The header provides auto boot function when AC power on. If you need the function, short SIO_AT1 pin 1 and pin 2.

DACC Jumper

(2-pin DACC1)

(see p. 4, No. 34)

Setting	Description
Open	Normal
Short	Auto Clear CMOS (Power off) (Default)

*Auto clear CMOS when system boot improperly.

PWR_BAT2

(2-pin PWR_BAT2)

(see p. 4, No. 40)

Setting	Description
Open	Normal (Default)
Short	Charge Battery

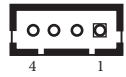
* Only supported by chargeable battery.

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 to the motherboard!

4-pin DC-in PWR Connector & UPS Module Power Output Connector (Input +12V~+28V)

(4-pin FROM_UPS1)
(see p. 4, No. 1)



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

Please connect a DC +12V~+28V power supply to this connector.

2-pin UPS Module Power Input Connector

(2-pin TO_UPS1)
(see p. 4, No. 2)

Pin	Signal Name
1	GND
2	DC Input

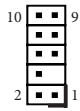
PWR_ADAPTER1

(4-pin PWR_ADAPTER1)
(see p. 4, No. 4)

Pin	Signal Name
1	GND
2	5VA_CONTROL
3	5VA
4	GND

SPI_TPM Header

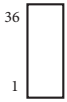
(9-pin SPI_TPM1)
(see p. 4, No. 5)



Pin	Signal Name	Signal Name	Pin
1	TPM PWR	RST#	2
3		CS#	4
5	IRA	MOSI	6
7	MISO	GND	8
9	CLK	GND	10

MIPI1

(36-pin MIPI1)
(see p. 4, No. 6)



Pin	Signal Name
1	GND
2	CSI_B_DN2
3	CSI_B_DP2
4	GND
5	CSI_B_DN1
6	CSI_B_DP1
7	GND
8	CSI_B_CLK_N
9	CSI_B_CLK_P
10	GND
11	CSI_B_DN0
12	CSI_B_DP0
13	CSI_B_DN3
14	CSI_B_DP3
15	GND
16	GND
17	+2.8V
18	GND
19	+2.8V
20	+1.8V
21	+1.2V
22	GND
23	IMBCLKOUT0
24	GND
25	I2C1_SCL
26	I2C1_SDA
27	N/C
28	BUF_PLT_RST_1.8_R_N
29	N/C
30	GND
31	N/C
32	+1.2V
33	GND
34	GPP_S1
35	GPP_S2
36	GPP_S3

CPU Fan Connector (+12V)

(4-pin CPU_FAN1)

(see p. 4, No. 7)

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

The board offers three 4-pin CPU fan (Smart Fan) connectors which are compatible with 3-pin CPU fan. If you connect a 3-pin CPU fan to the CPU fan connector on this motherboard, please connect it to pin 1-3. The maximum current is 1A.

SATA3 Connector

(SATA3_1)

(see p. 4, No. 8)

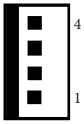
Pin	Signal Name
1	GND
2	SATA-A+
3	SATA-A-
4	GND
5	SATA-B-
6	SATA-B+
7	GND

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. 9)



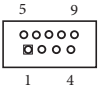
Pin	Signal Name
1	+5V
2	GND
3	GND
4	+12V

Please connect a SATA power cable to this connector.

USB 3.2 Gen1 Connector

(4-pin USB3H_2)

(see p. 4, No. 10)



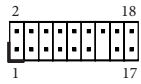
Pin	Signal Name
1	USB_PWR
2	USB_D-
3	USB_D+
4	GND
5	SSRX-
6	SSRX+
7	GND
8	SSTX-
9	SSTX+

There is one USB 3.2 Gen1 Type-A vertical connector on this motherboard. The maximum power current support is 0.5A.

ESPI Header

(17-pin ESPI1)

(see p. 4, No. 11)



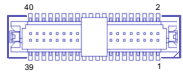
Pin	Signal Name	Signal Name	Pin
1	ESPI_CLK	GND	2
3	ESPI_CS#	SMB_CLK_MAIN	4
5	ESPI_RST#	SMB_DATA_MAIN	6
7	ESPI_IO3	ESPI_IO2	8
9	+3V	ESPI_IO1	10
11	ESPI_IO0	GND	12
13		S_PWRDWN#	14
15	+3VSB	DUMMY	16
17	GND	GND	18

The header is reserved for Port 80 code display and for debugging purposes.

LVDS Panel Connector

(40-pin LVDS1)

(see p. 4, No. 14)



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 pin definition (switch by BIOS):

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

Backlight Power Connector

(6-pin BLT_PWR1)

(see p. 4, No. 15)

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

Backlight Volume Control

(7-pin BLT_VOL1)

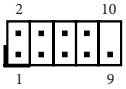
(see p. 4, No. 16)

Pin	Signal Name
1	GPIO_VOL_UP
2	GPIO_VOL_DW
3	PWRDN
4	BRIGHTNESS_UP
5	BRIGHTNESS_DW
6	GND
7	GND

System Panel Header

(9-pin PANEL1)

(see p. 4, No. 18)



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.

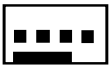
PWRBTN (Power Switch):
Connect to the power switch on the chassis front panel. You may configure the way to turn off your system using the power switch.
RESET (Reset Switch):
Connect to the reset switch on the chassis front panel. Press the reset switch to restart the computer if the computer freezes 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 assignments are matched correctly.

Chassis FAN Connectors (+12V)

(4-pin CHA_FAN1)

(see p. 4, No. 21)



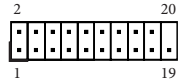
Pin	Signal Name
1	GND
2	+12V
3	CHA_FAN_SPEED
4	FAN_SPEED_CONTROL

The board offers three 4-pin chassis fan (Smart Fan) connectors which are compatible with 3-pin chassis fan. If you connect a 3-pin chassis fan to the chassis fan connector on this motherboard, please connect it to pin 1-3. The maximum current is 1A.

USB 3.2 Gen1 Header

(19-pin USB3H_3_4)

(see p. 4, No. 28)



Pin	Signal Name	Signal Name	Pin
1	DUMMY	IntA_P_D+	2
3	IntA_P_D+	IntA_P_D-	4
5	IntA_P_D-	GND	6
7	GND	IntA_P_SSTX+	8
9	IntA_P_SSTX+	IntA_P_SSTX-	10
11	IntA_P_SSTX-	GND	12
13	GND	IntA_P_SSRX+	14
15	IntA_P_SSRX+	IntA_P_SSRX-	16
17	IntA_P_SSRX-	Vbus	18
19	Vbus		

There is one USB 3.2 Gen1 connector on this motherboard. This header can support two USB 3.2 Gen1 ports with maximum power current 0.9A per port.

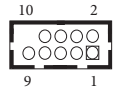
Internal COM Port Headers

COM1, 2 (RS232/422/485)

COM3, 4 (RS232)

(9-pin COM1~4)

(see p. 4, No. 29)



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

There are four 2.54mm-pitch COM port headers (COM1~COM4), with COM1, 2 ports supporting RS232/422/485, and with COM3, 4 ports supporting RS232. The maximum current for per port is 1A, and the power supply of pin 9 is either 5V or 12V. Use COM Port PWR Setting Jumper to set the power for COM port pin 9.

* This motherboard supports RS232/422/485 on COM1, 2 ports. Please refer to the table below for the pin definition. In addition, COM1, 2 ports (RS232/422/485) can be adjusted in BIOS setup utility > Advanced Screen > Super IO Configuration. You may refer to our user manual for details.

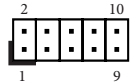
COM1, 2 Ports Pin Definition

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

Digital Input/Output Pin Header

(10-pin JGPIO1)

(see p. 4, No. 30)



Pin	Signal Name	Signal Name	Pin
1	SIO_GP34	SOC_E15	2
3	SIO_GP35	SOC_E01	4
5	SIO_GP36	SOC_E02	6
7	SIO_GP37	SOC_E13	8
9	JGPIO_PWR	GND	10

SMB_TEST1

(4-pin SMBUS_TEST1)

(see p. 4, No. 32)

Pin	Signal Name
1	GP_E01
2	SMB_CLK
3	SMB_DATA
4	GND

Buzzer Header

(2-pin BUZZ2)

(see p. 4, No. 35)

Pin	Signal Name
1	Buzz+
2	Buzz-

This header provides additional external Buzzer to boot up debugging.

3W Audio AMP Output Wafer

(4-pin SPEAKER1)

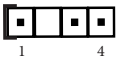
(see p. 4, No. 36)

Pin	Signal Name
1	OUTLN
2	OUTLP
3	OUTRP
4	OUTRN

SPDIF Header

(3-pin SPDIF1)

(see p. 4, No. 37)



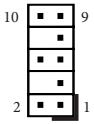
Pin	Signal Name
1	+5V
2	
3	SPDIF OUT
4	GND

SPDIF header, providing SPDIF audio output to HDMI VGA card, allows the system to connect HDMI Digital TV/projector/LCD devices. Please connect the SPDIF connector of HDMI VGA card to this header.

Front Panel Audio Header

(8-pin HD_AUDIO1)

(see p. 4, No. 38)



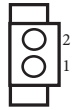
Pin	Signal Name	Signal Name	Pin
1	MIC2_L	OUT_RET	2
3	MIC2_R		4
5	OUT2_R	PRESENCE#	6
7	J_SENSE		8
9	OUT2_L	GND	10

This is line out/microphone interface for front panel audio cable that allows jack detection, convenient connection and control of audio devices.

Battery Connector

(BAT1)

(see p. 4, No. 39)

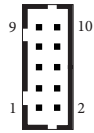


Pin	Signal Name
1	+BAT
2	GND

VGA Header

(10-pin VGA2)

(see p. 4, No. 41)

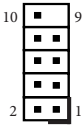


Pin	Signal Name	Signal Name	Pin
1	RED	GND	2
3	GREEN	GND	4
5	BLUE	GND	6
7	HSYNC	VSYNC	8
9	DDC_CLK	DDC_DATA	10

USB 2.0 Headers

(9-pin USB2H_1~4)

(see p. 4, No. 42)



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

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, mulfunction 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:

Main	For setting system time/date information
Advanced	For advanced system configurations
H/W Monitor	Displays current hardware status
Security	For security settings
Boot	For configuring boot settings and boot priority
Exit	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

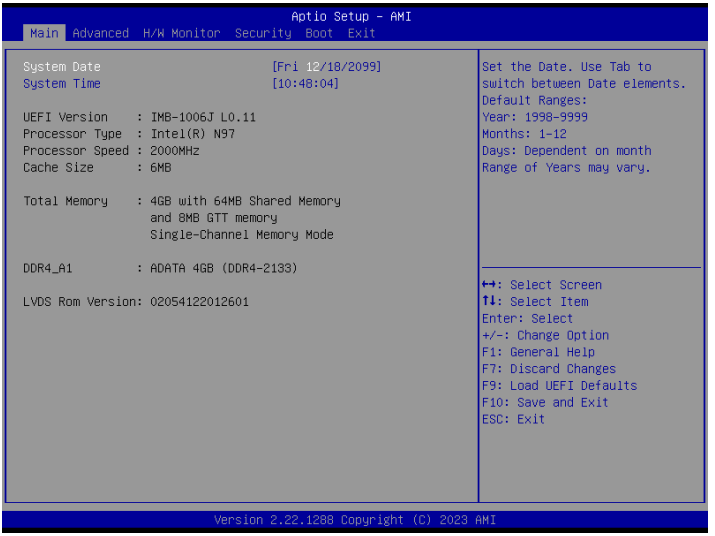
Use <←> key or <→> key to choose among the selections on the menu bar, and use < ↑ > key or < ↓ > key to move the cursor up or down to select items, then press <Enter> to get into the sub screen. You can also use the mouse to click your required item.

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 (Advanced Mode)

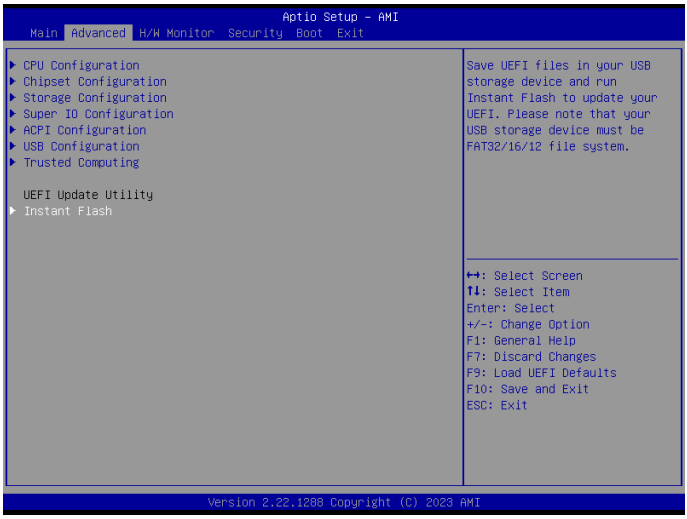
When you enter the UEFI SETUP UTILITY, the Main screen will appear and display the system overview.



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, ACPI Configuration, USB Configuration, and Trusted Computing.

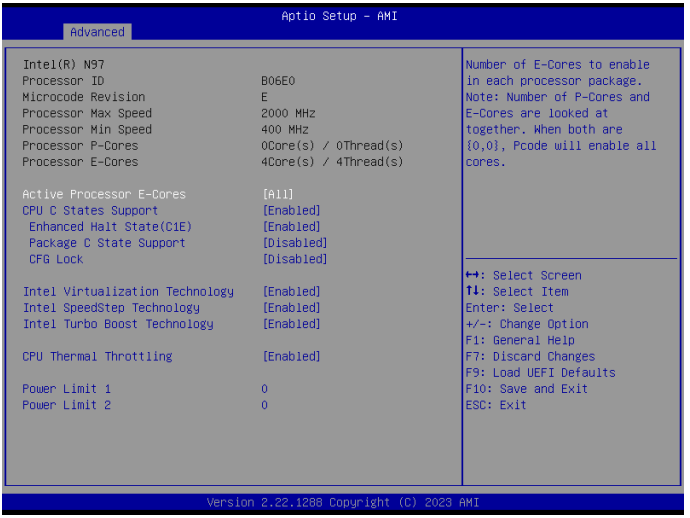


Setting wrong values in this section may cause the system to malfunction.

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



Active Processor E-Cores

This 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}, Pcode will enable all cores.

CPU C States Support

This 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]

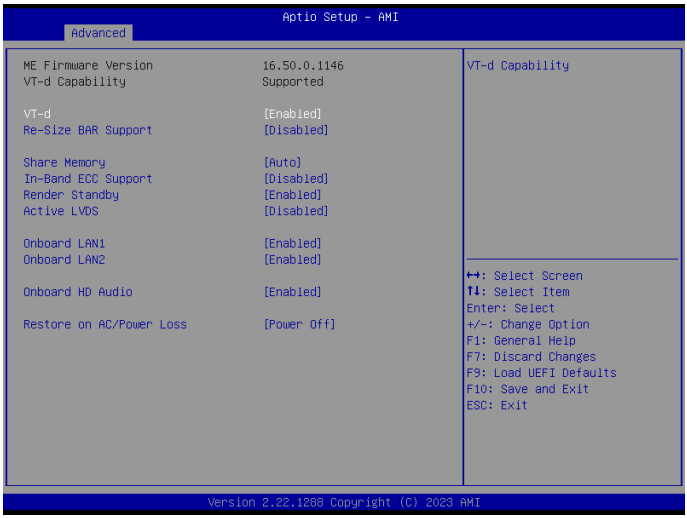
Power Limit 1

"Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit. If value is 0, BIOS will program Processor Base Power (TDP) value."

Power Limit 2

"Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*Processor Base Power (TDP). For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit."

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]

Re-Size BAR Support

If system has Resizable BAR capable PCIe Devices, this option enables or disables Resizable BAR Support.

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

In-Band ECC Support

This allows you to enable or disable In-Band ECC.

Configuration options: [Enabled] [Disabled]

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]).

Onboard LAN1

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

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: [Enabled] [Disabled]

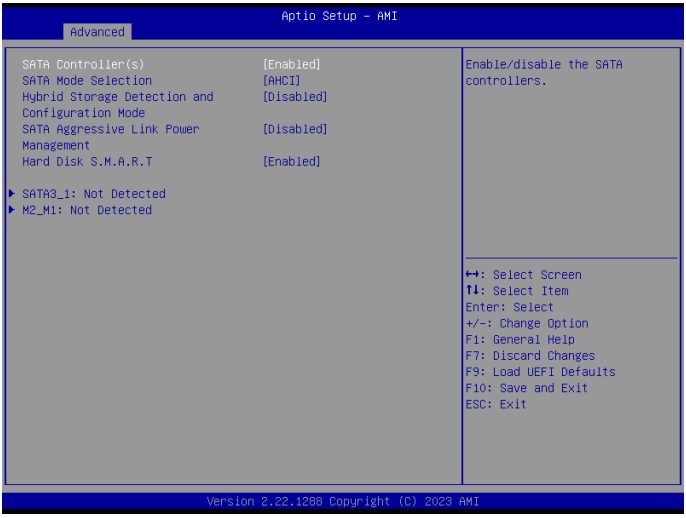
Restore on AC/Power Loss

The option 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



SATA Controller(s)

The option 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

The option 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.

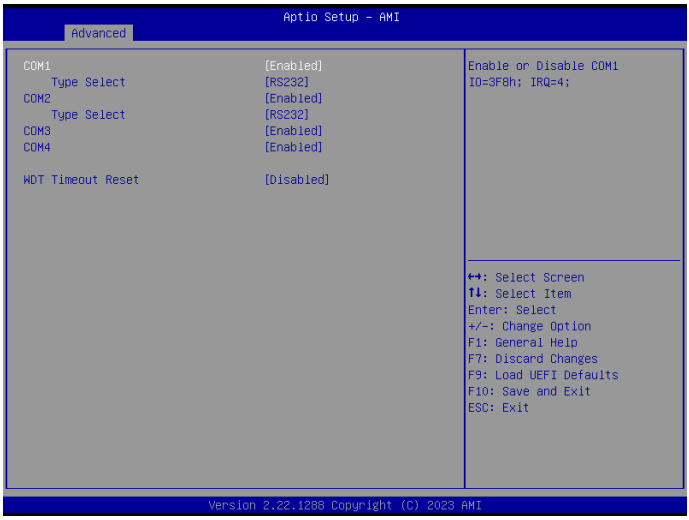
Configuration options: [Enabled] [Disabled]

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].

COM2 Configuration

Use this to set parameters of COM2.

Type Select

Use this to select COM2 port type: [RS232], [RS422] or [RS485].

COM3 Configuration

Use this to set parameters of COM3.

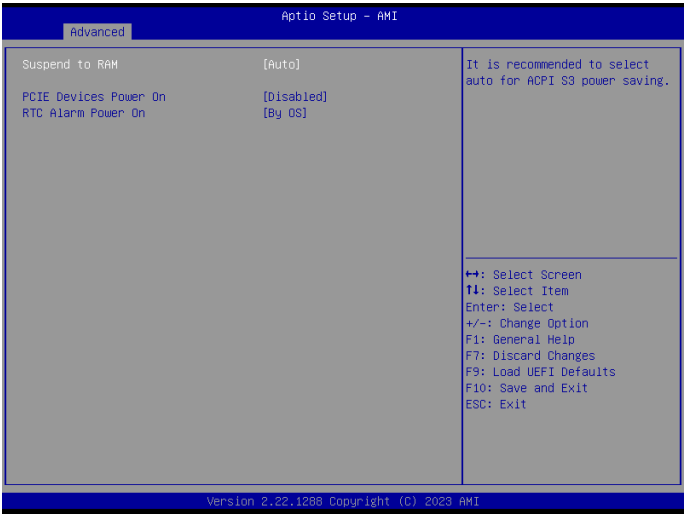
COM4 Configuration

Use this to set parameters of COM4.

WDT Timeout Reset

Use this to set the Watch Dog Timer.

3.3.5 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]

PCIE Devices Power On

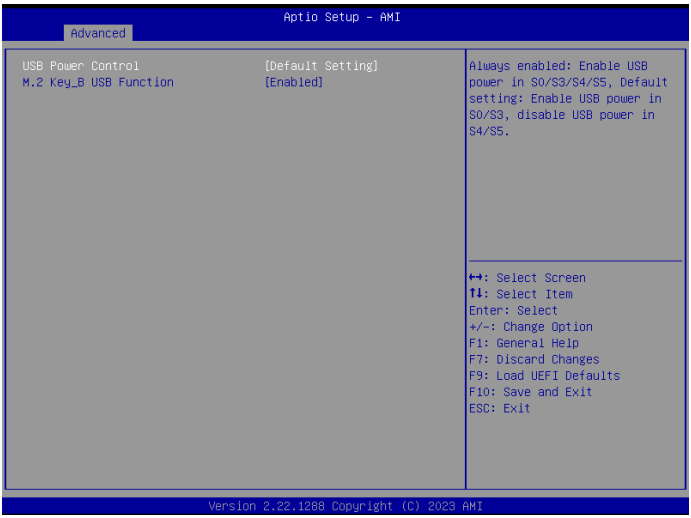
Use this item to enable or disable PCIE devices to turn on the system from the power-soft-off mode.

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]

3.3.6 USB Configuration



USB Power Control

Use this option to control USB power.

M.2 Key_B USB Function

Enable or disable M.2 Key-B USB function.

3.3.7 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]

SHA384 PCR Bank

SHA384 PCR Bank allows you to enable or disable SHA384 PCR Bank.

Configuration options: [Enabled] [Disabled]

SM3_256 PCR Bank

SM3_256 PCR Bank allows you to enable or disable SM3_256 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.

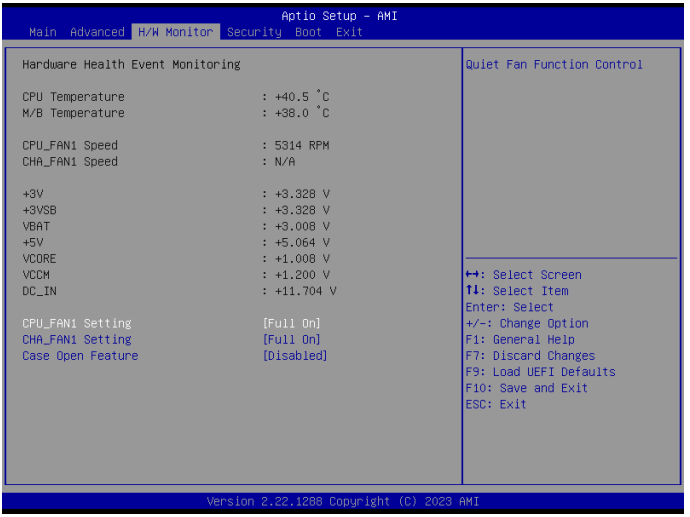
[TPM 1.2] restricts support to TPM 1.2 devices.

[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.

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, chassis 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]

CHA_Fan 1 Setting

This allows you to set chassis fan 1's speed. The default value is [Full On].

Configuration options: [Full On] [Automatic Mode]

Case Open Feature

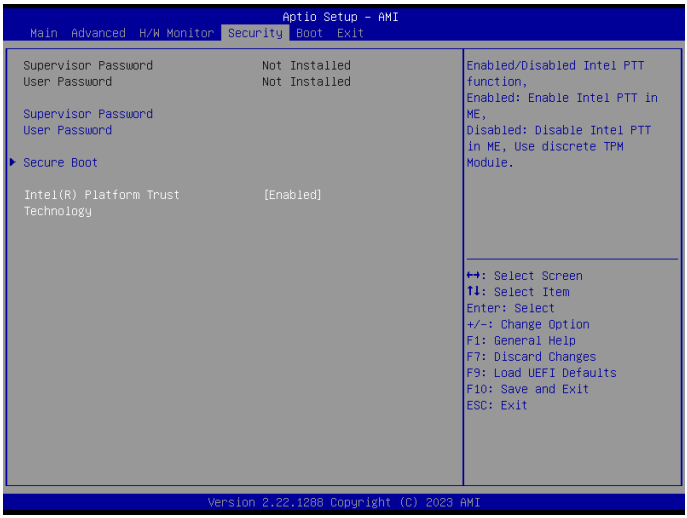
This allows you to enable or disable case open detection feature. The default is value [Disabled].

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 the authority to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

User Password

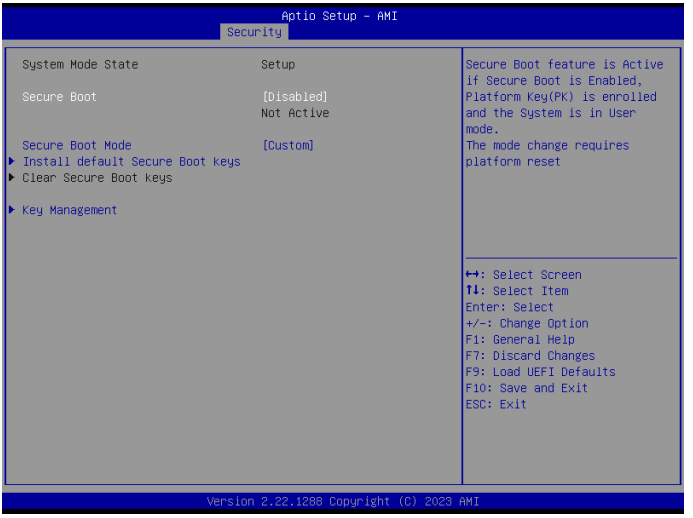
Set or change the password for the user account. Users are unable to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

Secure Boot

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

Intel(R) Platform Trust Technology

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



Secure Boot Mode

[Standard] Select this item and the system will automatically load the Secure Boot keys from the BIOS database.

[Custom] Select this item and Secure Boot Policy variables can be configured by a physically present user without full authentication.

Install Default Secure Boot Keys

Please install default secure boot keys if it's the first time you use secure boot.

Clear Secure Boot Keys

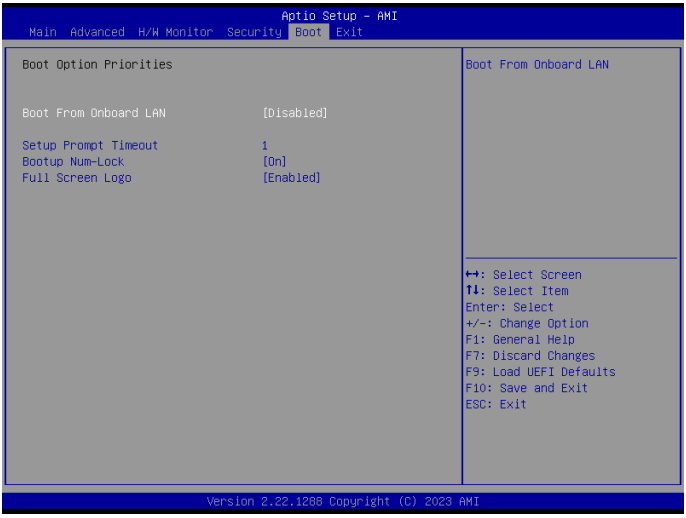
This item appears only when you load the default Secure Boot keys. Use this item to clear all default Secure Boot keys.

Key Management

This item enables expert users to modify Secure Boot Policy variables without full authentication. This appears only when you set Secure Boot Mode to [Custom].

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 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.

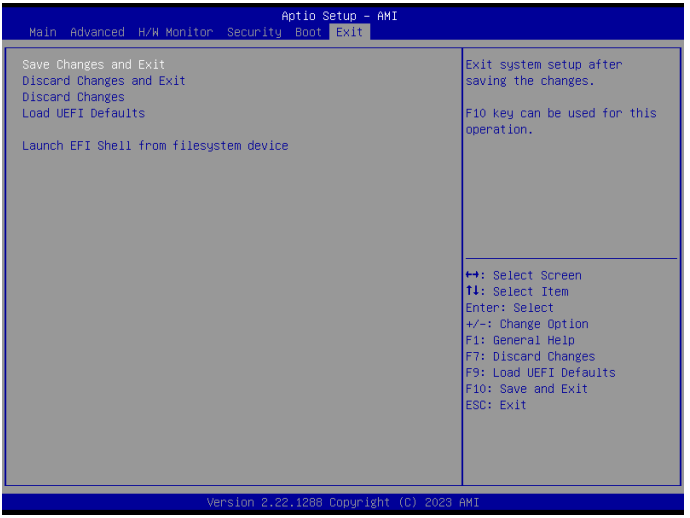
Configuration options: [On] [Off]

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. 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. 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. Select [Yes] to discard all the 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.