ASRock Industrial

NUC-358H
NUC-325

User Manual

Version 1.0
Updated April 8, 2026

Version 1.0
Published April, 2026

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.

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.

HIGH-DEFINITION MULTIMEDIA INTERFACE

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"

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)

CE

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

Chapter 1 Introduction

Thank you for purchasing ASRockInd ***NUC-358H / NUC-325*** 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/NUC-358H

https://www.asrockind.com/NUC-325

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

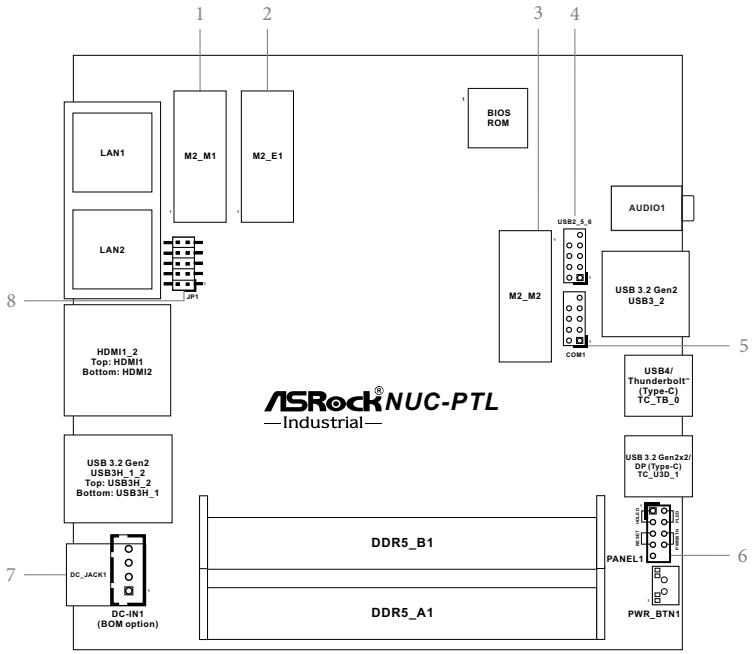
ASRockInd ***NUC-358H / NUC-325*** Motherboard (NUC (4.09-in x 4.02-in x 1.5-in, 10.4 cm x 10.2 cm x 3.8 cm))

1.2 Specifications

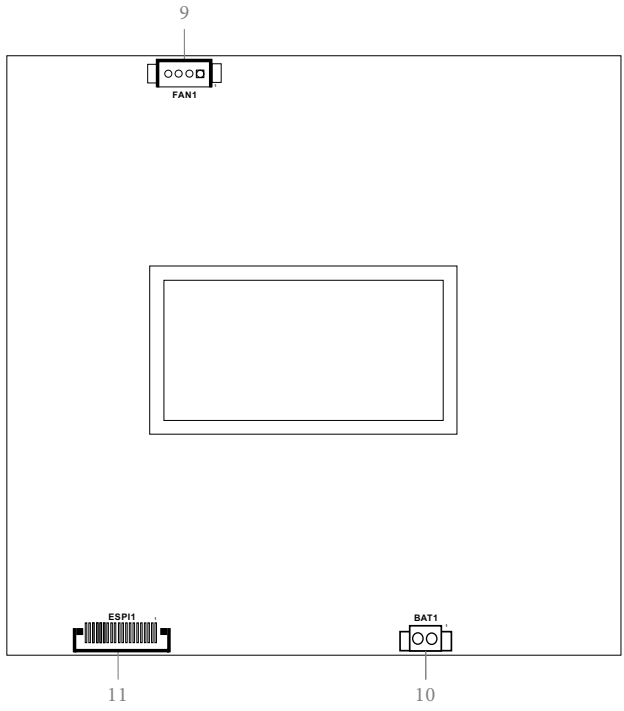
Form Factor	Dimensions	NUC (4.09-in x 4.02-in x 1.5-in, 10.4 cm x 10.2 cm x 3.8 cm
Processor System	CPU	Intel® Core™ Ultra Series 3 Processors (Panther Lake-H) NUC-358H (Ultra X7 358H, 4P+8E+4LPE) NUC-325 (Ultra 5 325, 4P+4LPE)
	Chipset	MCP
	BIOS	AMI SPI 256 Mbit
Memory	Technology	Dual Channel DDR5 7200 MHz (Ultra X7 358H) Dual Channel DDR5 6400 MHz (Ultra 5 325)
	Capacity	128GB (64 GB per DIMM)
	Socket	2 x 262-pin SO-DIMM
Graphics	Controller	Intel® Graphics
	HDMI	HDMI 2.1 Max resolution up to 7680x4320@60Hz
	DisplayPort	DisplayPort 2.1/ 1.4a, DP++ Max resolution up to 4096x2160@60Hz
	MultiDisplay	Max 4 display (Included 2 outputs from Type-C)
Expansion Slot	M.2	1 x M.2 (Key E, 2230) with PCIe x1, USB 2.0 and CNVio2/CNVIo3 for Wireless
Audio	Interface	Realtek ALC256, High Definition Audio
Ethernet	Controller/ Speed	LAN1: Intel® I226LM with 10/100/1000/2500 Mbps, supports vPro LAN2: Intel® I226V with 10/100/1000/2500 Mbps
	Controller	2 x RJ-45
Front I/O	USB	1 x USB 3.2 Gen2 (Type-A) 1 x USB4/Thunderbolt™ 4 (5V/3A, Supports DP 2.1 display output) 1 x USB 3.2 Gen2x2 (Type-C, 5V/3A, Supports DP1.4a display output) *For Thunderbolt support, please refer to support list.
	Audio	1 (headphone & microphone jack)
Rear I/O	HDMI	2 x HDMI 2.1
	Ethernet	2 x 2.5 Gigabit LAN
	USB	2 x USB 3.2 Gen2 (Type-A)
	DC Jack	1

Internal Connector	USB	2 x USB 2.0 (1 x 2.00 pitch header)
	COM	1 x COM (RS-232/RS-422/RS-485)
Storage	M.2	1 x M.2 (KEY M, 2242) with PCIe Gen4 x4 for SSD 1 x M.2 (KEY M, 2242/2280) with PCIe Gen5 x4 for SSD
	RAID	Intel® VMD RAID 0/1 **supported by identical interface (PCIe) PCIe interface: 2*M.2 Key M
Security	TPM	Intel® PTT
Watchdog Timer	Output	From Super I/O to drag RESETCON#
	Interval	256 Segments, 0, 1, 2, ...255sec
Power Requirements	Input PWR	12V~24V DC-In 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 Temperature	-20 °C ~ 70 °C
	Storage Temperature	-40 ° C ~ 85 °C
	Operating Humidity	5% ~ 90% (non-condensing)
	Storage Humidity	5% ~ 90% (non-condensing)

1.3 Motherboard Layout



1 : M.2 Key-M Socket (M2_M1)
2 : M.2 Key-E Socket (M2_E1)
3 : M.2 Key-M Socket (M2_M2)
4 : USB 2.0 Header (USB2_5_6)
5 : COM Port Header (RS232/422/485) (COM1)
6 : System Panel Header (PANEL1)
7 : 4-pin DC-in Wafer (DC_IN1) (BOM option)
8 : JP1 Header (JP1)



Back Side :

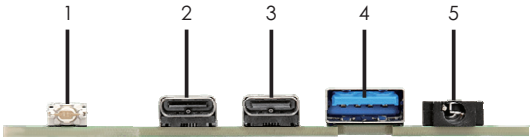
9 : Fan Connector (FAN1)

10 : Battery Connector (BAT1)

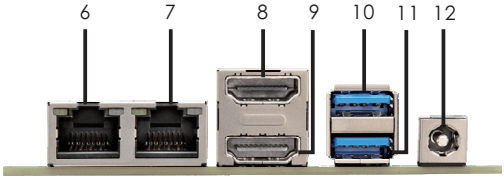
11 : ESPI Connector (ESPI1)

1.4 I/O Panel

Front I/O :



Rear I/O :



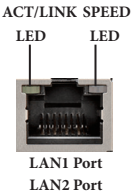
1 Power Button (PWR_BTN1)
2 USB 3.2 Gen2x2/DP Type-C Port (TC_U3D_1)
3 USB4/Thunderbolt™ Type-C Port (TC_TB_0)
4 USB 3.2 Gen2 Port (USB3_2)
5 Combo Audio Jack (AUDIO1) (Headphone + MIC)
6 RJ-45 LAN Port (LAN1)* (supports vPro)
7 RJ-45 LAN Port (LAN2)*
8 HDMI Port (HDMI1)
9 HDMI Port (HDMI2)
10 USB 3.2 Gen2 Ports (USB3H_2)
11 USB 3.2 Gen2 Ports (USB3H_1)
12 DC-In Jack (DC_JACK1)

* There are two LEDs on the LAN1 and LAN2 ports. Please refer to the table below for LAN1 and LAN2 ports LED indications.

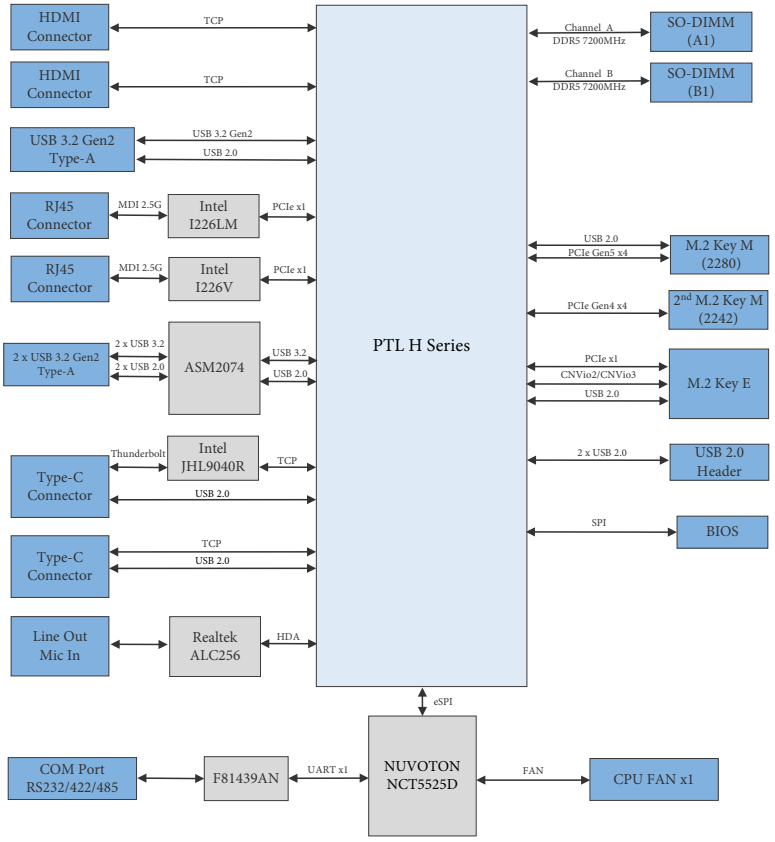
LAN1, LAN2 Ports LED Indications

Activity/Link LED	
Status	Description
Off	No Link
Blinking	Data Activity
On	Link

SPEED LED	
Status	Description
Off	10/100Mbps connection
Orange	1Gbps connection
Green	2.5Gbps connection



1.5 Block Diagram



Chapter 2 Installation

This is a NUC (4.09-in x 4.02-in x 1.5-in, 10.4 cm x 10.2 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.

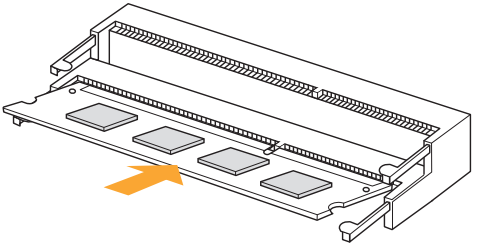
1. Unplug the power cord from the wall socket before touching any component.
2. To avoid damaging the motherboard components due to static electricity, NEVER place your motherboard directly on the carpet or the like. Also remember to use a grounded wrist strap or touch a safety grounded object before 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.

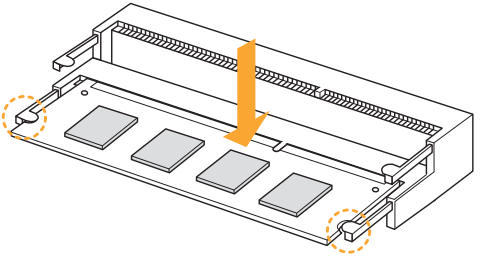
2.3 Installation of Memory Modules

NUC-358H / NUC-325 provides two 262-pin DDR5 (Double Data Rate 5) 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.



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.



1. *For dual channel configuration, you always need to install identical (the same brand, speed, size and chip-type) DDR5 DIMM pairs.*
2. *It is unable to activate Dual Channel Memory Technology with only one memory module installed.*

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.*

2.4 Expansion Slots

There are three M.2 sockets on this motherboard.

M.2 sockets:

1 x M.2 (Key E, 2230) with PCIe x1, USB 2.0 and CNVio2/CNVio3 for Wireless
1 x M.2 (KEY M, 2242) with PCIe Gen4 x4 for SSD
1 x M.2 (KEY M, 2242/2280) with PCIe Gen5 x4 for SSD

M.2 Key-E Socket (M2_E1)

Pin	Signal	Signal	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+		
		CNV_BGI_DT	32
33	GND	CNV_RGI_RSP	34
35	PETp	CNV_BRI_DT	36
37	PETn	NA	38
39	GND	NA	40
41	PERp	NA	42
43	PERn	NA	44
45	GND	NA	46
47	PEFCLKp	NA	48
49	PEFCLKn	NA	50
51	GND	PERST0#	52
53	CLKREQ#	W_DISABLE1#	54
55	NA	W_DISABLE2#	56
57	GND	NA	58
59	CNV_WT_D1-	NA	60
61	CNV_WT_D1+	NA	62
63	GND	NA	64
65	CNV_WT_D0-	NA	66
67	CNV_WT_D0+	NA	68
69	GND	NA	70
71	CNV_WT_CLK-	+3.3V	72
73	CNV_WT_CLK+	+3.3V	74
75	GND		

M.2 Key-M Socket (M2_M1)

Pin	Signal	Signal	Pin
1	GND	+3.3V	2
3	GND	+3.3V	4
5	PERn3	NA	6
7	PERp3	NA	8
9	GND	HDLED	10
11	PETn3	+3.3V	12
13	PETp3	+3.3V	14
15	GND	+3.3V	16
17	PERn2	+3.3V	18
19	PERp2	NA	20
21	GND	NA	22
23	PETn2	NA	24
25	PETp2	NA	26
27	GND	NA	28
29	PERn1	NA	30
31	PERp1	GND	32
33	GND	USB_D+	34
35	PETn1	USB_D-	36
37	PETp1	GND	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	NA	54
55	PEFCLKp	NA	56
57	GND	NA	58
67	NA	NA	68
69	NA	+3.3V	70
71	GND	+3.3V	72
73	GND	+3.3V	74
75	GND		

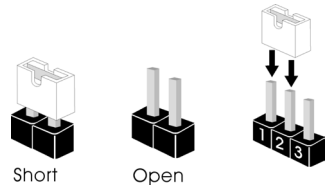
M.2 Key-M Socket (M2_M2)

Pin	Signal	Signal	Pin
1	GND	+3.3V	2
3	GND	+3.3V	4
5	PERn3	NA	6
7	PERp3	NA	8
9	GND	HDLED	10
11	PETn3	+3.3V	12
13	PETp3	+3.3V	14
15	GND	+3.3V	16
17	PERn2	+3.3V	18
19	PERp2	NA	20
21	GND	NA	22
23	PETn2	NA	24
25	PETp2	NA	26
27	GND	NA	28
29	PERn1	NA	30
31	PERp1	NA	32
33	GND	NA	34
35	PETn1	NA	36
37	PETp1	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	NA	54
55	PEFCLKp	NA	56
57	GND	NA	58
67	NA	NA	68
69	NA	+3.3V	70
71	GND	+3.3V	72
73	GND	+3.3V	74
75	GND		

* Pin34 and Pin36 are defined as USB 2.0 signal to support Key-M to Key-B extension card.

2.5 Jumpers Setup

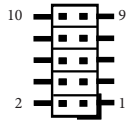
The illustration shows how jumpers are setup. When the jumper cap is placed on pins, the jumper is "Short." If no jumper cap is placed on pins, the jumper is "Open." The illustration shows a 3-pin jumper whose pin1 and pin2 are "Short" when jumper cap is placed on these 2 pins.



JP1 Header

(10-pin JP1)

(see p. 4, No. 8)



Pin	Signal Name
JP1_12	Short : ATX Mode (Default)
JP1_12	Open : AT Mode
JP1_34	CMOS Normal (Default)
JP1_46	Short : Clear CMOS
JP1_57	Short : DACC* (Default)
JP1_910	Short: Active Case Open

* Auto clear CMOS when system boot improperly.

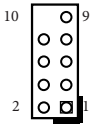
2.6 Onboard Headers and Connectors

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!

USB 2.0 Header

(9-pin USB2_5_6)

(see p. 4, No. 4)

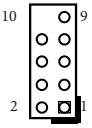


Pin	Signal Name	Signal Name	Pin
1	USB_PWR	USB_PWR	2
3	-A	-B	4
5	+A	+B	6
7	GND	GND	8
9	DUMMY		10

COM Port Header (RS232/422/485)

(9-pin COM1)

(see p. 4, No. 5)



Pin	Signal Name	Signal Name	Pin
1	DDCD#1	RRXD1	2
3	TTXD1	DDTR#1	4
5	GND	DDSR#1	6
7	RRTS#1	CCTS#1	8
9	DUMMY		10

This motherboard supports RS232/422/485 on COM1 port. Please refer to the table below for the pin definition. In addition, COM1 port (RS232/422/485) can be adjusted in BIOS setup utility > Advanced Screen > Super IO Configuration. You may refer to page 31 for details.

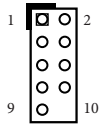
COM1 Port Pin Definition

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	NA	NA	NA

System Panel Header

(9-pin PANEL1)

(see p. 4, No. 6)



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

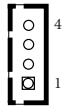
PWRBTN (Power Switch):
Connect to the power switch on the chassis front panel. You may configure the way to turn off your system using the power switch.
RESET (Reset Switch):
Connect to the reset switch on the chassis front panel. Press the reset switch to restart the computer if the computer freezes 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 system is in S3 sleep state. The LED is off when the system is in 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.

4-pin DC-In Wafer (BOM option)

(4-pin DC-IN1)

(see p. 4, No. 7)



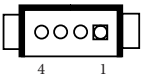
Pin	Signal Name
1	GND
2	DC Input
3	DC Input
4	GND

Back Side :

Fan Connector

(4-pin FAN1)

(see p. 5, No. 9)



Pin	Signal Name
1	GND
2	+5V
3	FAN_SPEED
4	FAN_SPEED_CONTROL

Battery Connector

(2-pin BAT1)

(see p. 5, No. 10)

Pin	Signal Name
1	+BAT
2	GND

ESPI Connector

(20-pin ESPI1)

(see p. 5, No. 11)

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

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

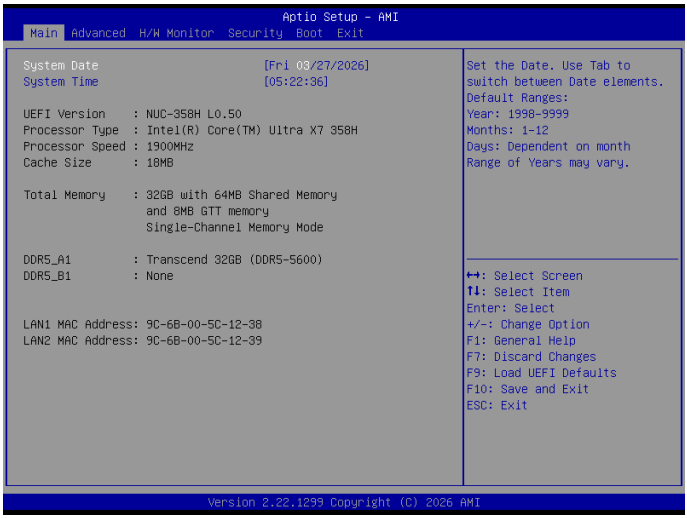
Use < ← > key or < → > key to choose among the selections on the menu bar, and use < ↑ > key or < ↓ > key to move the cursor up or down to select items, then press <Enter> to get into the sub screen. You can also use the mouse to click your required item.

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)

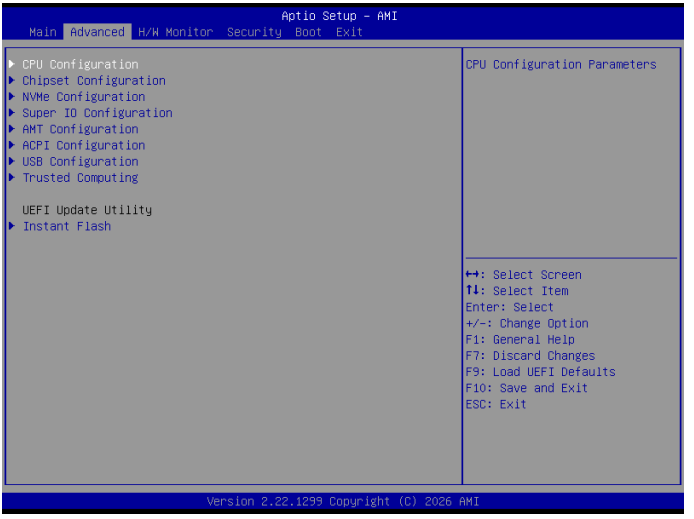
When you enter the UEFI SETUP UTILITY, the Main screen will appear and display the system overview.



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, NVMe Configuration, Super IO Configuration, AMT Configuration, ACPI Configuration, USB Configuration, and Trusted Computing.

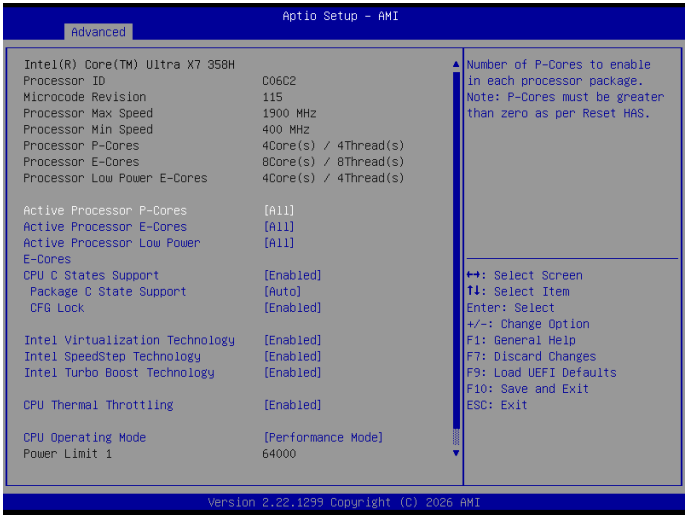


Setting wrong values in this section may cause the system to malfunction.

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 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 P-Cores

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

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.

Active Processor Low Power E-Cores

Sets the number of Low Power E-Cores to enable in each processor package. This setting is evaluated together with the P-Core and E-Core settings. If all three are set to 0, all cores will be enabled automatically.

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]

Package C State Support

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

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

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].

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]

CPU Operating Mode

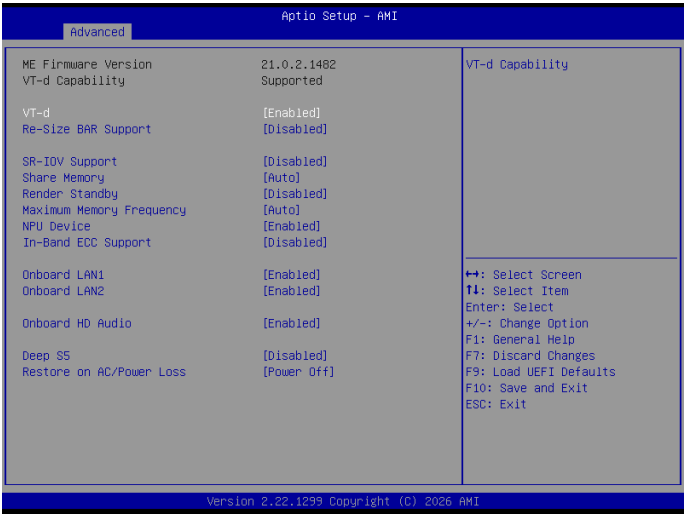
If working at [Normal Mode], M/B works with the default Smart Fan Setting and can provide better cooler experience. If [Performance Mode] is selected, CPU can provide optimal performance, but the CPU fan speed will work at higher speed.

Configuration options: [Normal Mode] [Performance Mode]

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.

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.

Configuration options: [Enabled] [Disabled]

SR-IOV Support

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

Virtualization Support.

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]
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.

Configuration options: [Enabled] [Disabled]

Maximum Memory frequency

Maximum Memory Frequency Selections in MHz.

NPU Device

This allows you to enable or disable NPU (Neural Processing Unit) Device.

Configuration options: [Enabled] [Disabled]

In-Band ECC Support

Enable/Disable In-Band ECC. Will be enabled if memory has symmetric configuration.

Onboard LAN1

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

Configuration options: [Enabled] [Disabled]

Onboard LAN2

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

Configuration options: [Enabled] [Disabled]

Onboard HD Audio

This allows you to enable or disable the onboard HD audio.

Configuration options: [Enabled] [Disabled]

Deep S5

Mobile platforms support Deep S5 in DC only and desktop platforms support Deep S5 in AC only. The default value is [Disabled].

Configuration options: [Auto] [Disabled]

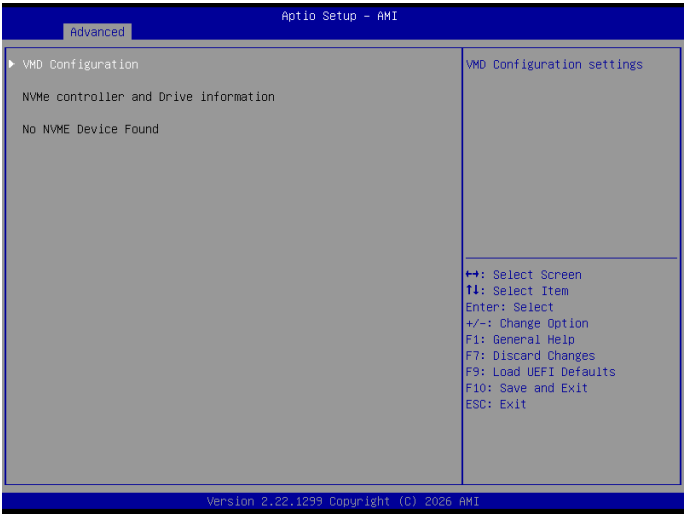
Restore on AC/Power Loss

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.

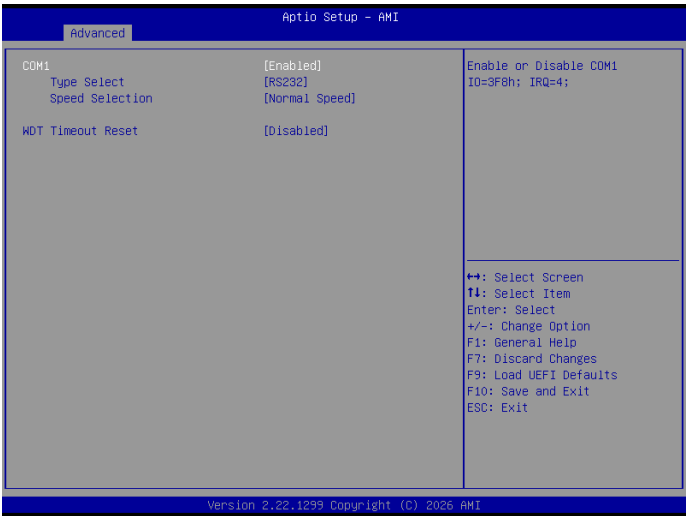
3.3.3 NVMe Configuration



VMD Configuration

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

3.3.4 Super IO Configuration



COM1

Use this to set parameters of COM1.

Type Select

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

Speed Selection

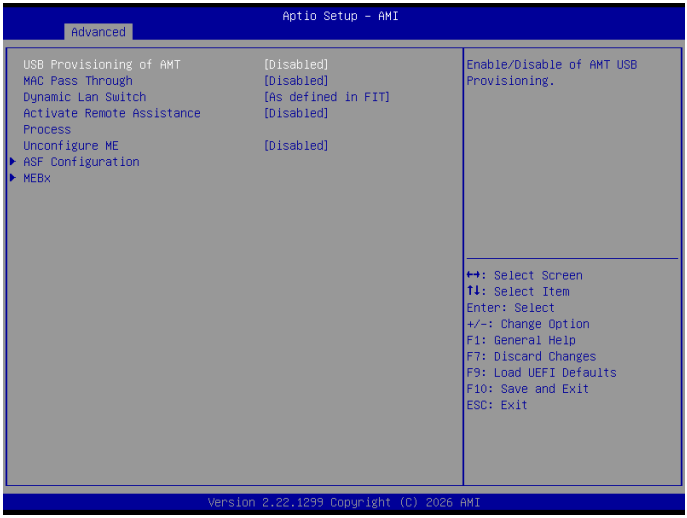
Select High Speed and install the required driver to support a baud rate of 921600.

WDT Timeout Reset

Use this to set the Watch Dog Timer.

Configuration options: [Enabled] [Disabled]

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].

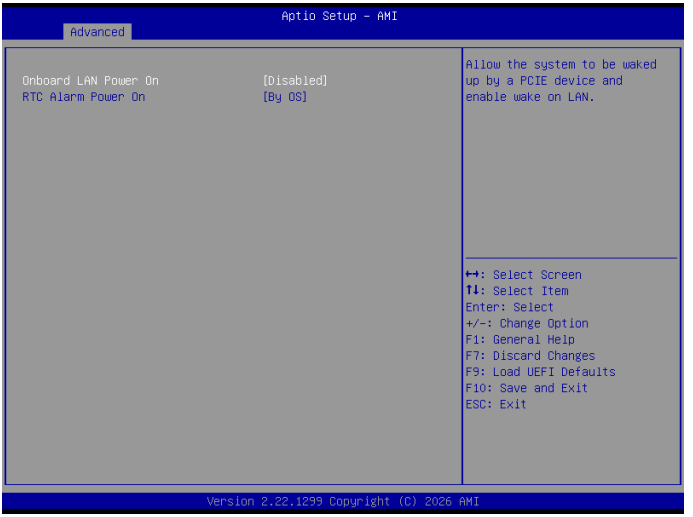
ASF Configuration

The option allows you to configure Alert Standard Format parameters.

MEBx

This Formset contains forms for configuring MEBx.

3.3.6 ACPI Configuration



Onboard LAN Power On

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

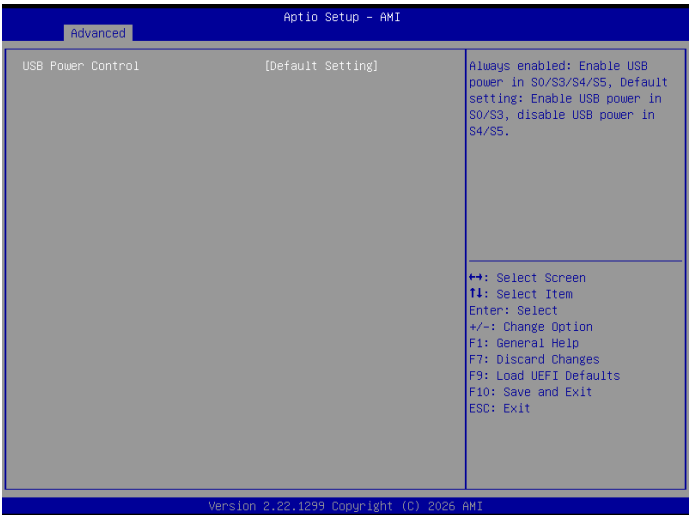
Configuration options: [Enabled] [Disabled]

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

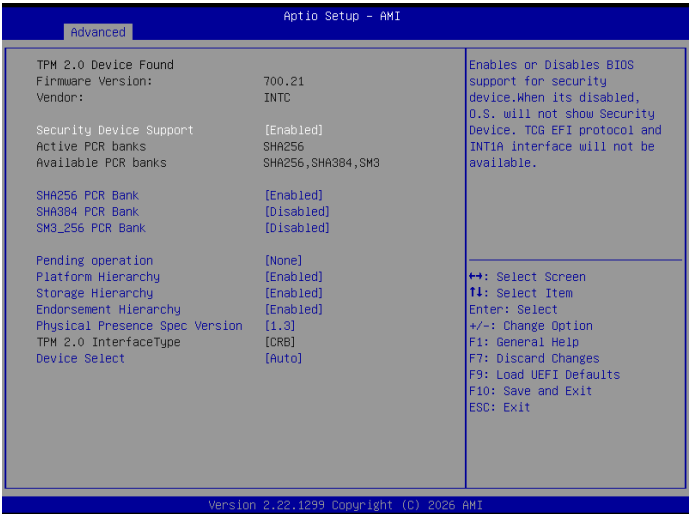


USB Power Control

Use this option to control USB power.

Configuration options: [Always Enabled] [Default Setting]

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]

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.

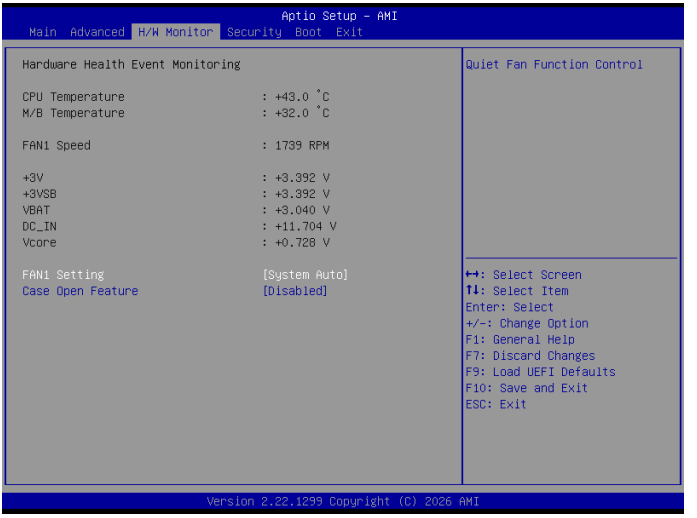
[TPM 1.2] restricts support to TPM 1.2 devices.

[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, fan speed, and the critical voltage.



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

Fan1 Setting

This allows you to set FAN1's speed. The default value is [System Auto].

Configuration options: [System Auto] [Full On] [Automatic Mode].

Case Open Feature

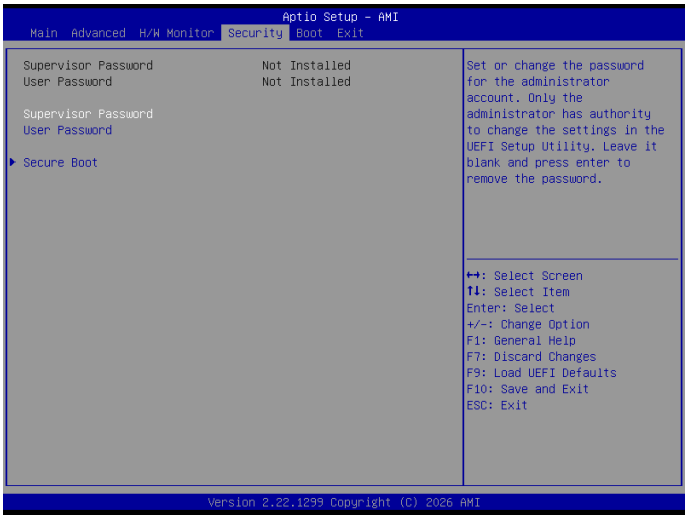
This allows you to enable or disable case open detection feature. The default is value [Disabled].

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

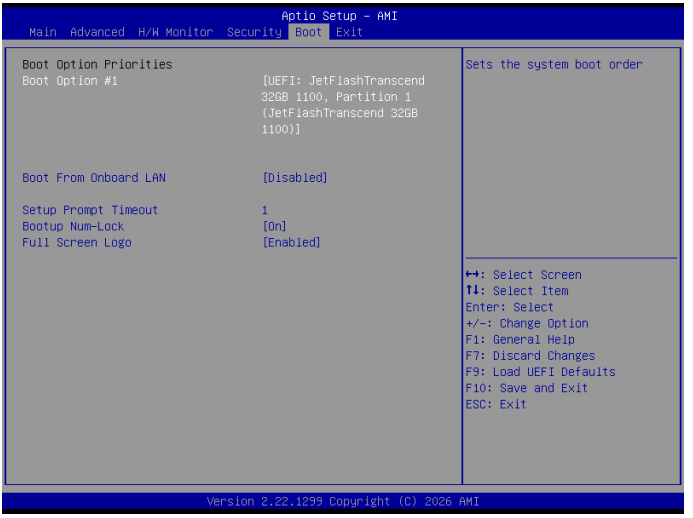
Set or change the password for the user account. Users are unable to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

Secure Boot

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

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 configures 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.

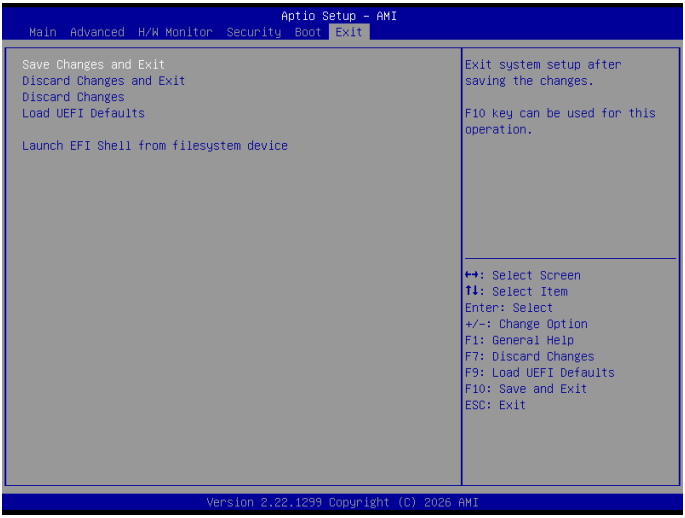
Configuration options: [On] [Off]

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.