ASRock Industrial

NUCS BOX-1360P/D4
NUCS BOX-1340P/D4

User Manual

Version 1.0
January 2023
Copyright©2024 ASRock Industrial Inc. All rights reserved.

Copyright Notice:

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

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

Disclaimer:

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

With respect to the contents of this documentation, ASRock Industrial 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 ASRock Industrial, 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 ASRock Industrial 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.

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)

Replaceable batteries

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

This product is intended to be supplied by a Listed Power Adapter or DC power source marked “L.P.S." (or "Limited Power Source"), rated 19 Vdc, 6.32 A minimum, Tma = 45 degree C minimum. All interior servicing is to be performed by qualified skilled personnel only.

Button Battery Safety Notice

⚠WARNING

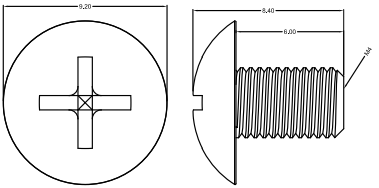
- **INGESTION HAZARD:** This product contains a button cell or coin battery.
- **DEATH** or serious injury can occur if ingested.
- A swallowed button cell or coin battery can cause **Internal Chemical Burns** in as little as **2 hours**.
- **KEEP** new and used batteries **OUT OF REACH of CHILDREN**
- **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: 3.3V
- 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.

CAUTION (or Warning)

Hot surface!
Do not touch!

The equipment should only be installed in a restricted access area.



VESA Mount: M4x6mm Screws *(for securing the VESA bracket to the monitor)*

This product should be connected by means of a power cord to a socket-outlet with earthing connection.

HIGH-DEFINITION MULTIMEDIA INTERFACE

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.

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.

Contact Information

If you need to contact ASRock Industrial or want to know more about ASRock Industrial, you're welcome to visit ASRock Industrial's website at https://www.asrockind.com; or you may contact your dealer for further information.

ASRock Industrial Incorporation

Email: Info_ipc@asrockind.com

Contents

Chapter 1 Introduction **1**

1.1 Package Contents 1

1.2 Product Specifications 2

1.3 Block Diagram 4

Chapter 2 Product Overview **5**

2.1 Front View 5

2.2 Rear View 6

2.3 Inside View 7

Chapter 3 Hardware Installation **8**

3.1 How to Remove the Bottom Case 8

3.2 How to Install the Memory Modules 9

3.3 How to Install the WiFi Module 10

3.4 How to Install the M.2 SSD (Type 2242) 11

3.5 How to Install the M.2 SSD (Type 2280) 13

3.6 How to Install the VESA Bracket 14

Chapter 4 Motherboard **16**

4.1 Motherboard Layout 16

4.2 Onboard Headers and Connectors 17

4.3 Expansion Slots (M.2 Slots) 19

Chapter 5 UEFI SETUP UTILITY **20**

5.1 Introduction 20

5.1.1 Entering BIOS Setup 20

5.1.2 UEFI Menu Bar 21

5.1.3 Navigation Keys 22

5.2 Main Screen (Advanced Mode) 23
5.3 Advanced Screen 24
5.3.1 CPU Configuration 25
5.3.2 Chipset Configuration 28
5.3.3 Super IO Configuration 30
5.3.4 AMT Configuration 31
5.3.5 ACPI Configuration 33
5.3.6 USB Configuration 34
5.3.7 Trusted Computing 35
5.4 Hardware Health Event Monitoring Screen 38
5.5 Security Screen 39
5.6 Boot Screen 40
5.7 Exit Screen 42
Chapter 6 Software Support 43
6.1 Install Operating System 43

Chapter 1 Introduction

Because the hardware specifications might be updated, the content of this documentation will be subject to change without notice.

1.1 Package Contents

- 1 x NUCS BOX-1300/D4
- 1 x 19V/90W Power Adapter
- 1 x VESA mount bracket
- 1 x Quick Installation Guide

If any items are missing or appear damaged, contact your authorized dealer.

1.2 Product Specifications

NUCS BOX-1360P/D4 NUCS BOX-1340P/D4		Barebone
CPU		Intel® 13th Gen (Raptor Lake-P) Core™ Processors NUCS BOX-1360P/D4(i7-1360P, 4P+8E) NUCS BOX-1340P/D4(i5-1340P, 4P+8E)
Chipset		MCP
BIOS		AMI SPI 256 Mbit
Memory		Supports Dual Channel DDR4 3200 MHz
Storage	**M.2 slot**	1 x M.2 (KEY M, 2242/2280) with PCIe Gen4 x4 for SSD
LAN		Intel® I226LM with 10/100/1000/2500 Mbps, supports vPro
WiFi		1 x Wi-Fi 6E 802.11ax + BT 5.3
Audio		Realtek ALC233/ALC256, High Definition Audio
Front I/O		2 x USB 3.2 Gen2 (Type-A) 1 x USB4/Thunderbolt™ 4 (5V/3A, supports DP1.4a display output)) 1 x USB 3.2 Gen2 (Type-C, 5V/1.5A, supports DP1.4a display output) 1 (headphone & microphone jack)
Rear I/O		1 x HDMI 2.0b, 1 x DP1.4a, 1 x 2.5 Gigabit LAN, 2 x USB 3.2 Gen2 (Type-A), DC-IN
Power Unit		19V/90W Power Adapter

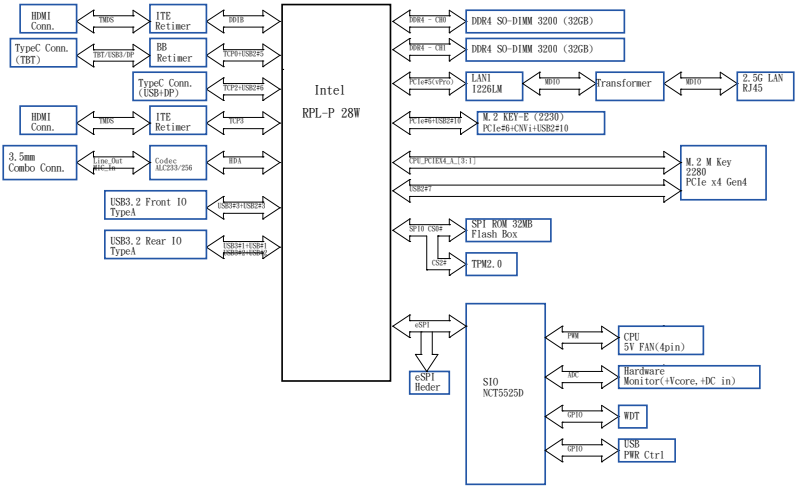
English

Dimensions (L x W x H)	117.5 x 110.0 x 38mm (4.63" x 4.33" x 1.50")
VESA	Bracket included , supports 75 x 75 and 100 x 100 mm
Net Weight	1.0 Kg
Operating Temperature	0°C~40°C

1.3 Block Diagram

NUCS BOX-1360P/D4

NUCS BOX-1340P/D4

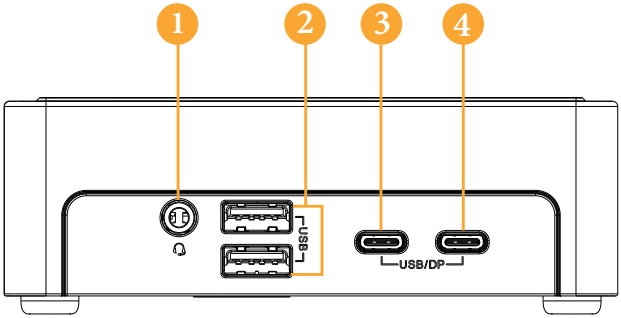


English

Chapter 2 Product Overview

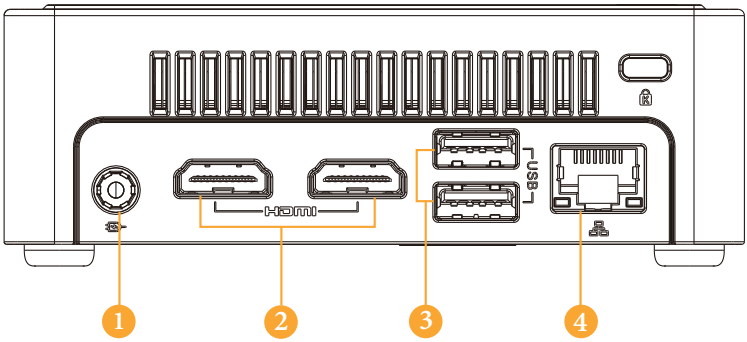
This chapter provides diagrams showing the location of important components of the NUCS BOX-1360/D4 / NUCS BOX-1340P/D4.

2.1 Front View



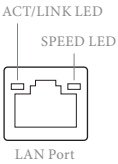
No.	Description
1	Audio (Mic-in, Line-out)
2	USB 3.2 Gen2 (Type-A)
3	USB4 / Thunderbolt™ 4 (5V/3A, supports DP1.4a display output)
4	USB 3.2 Gen2 (Type-C, 5V/1.5A, supports DP1.4a display output)

2.2 Rear View



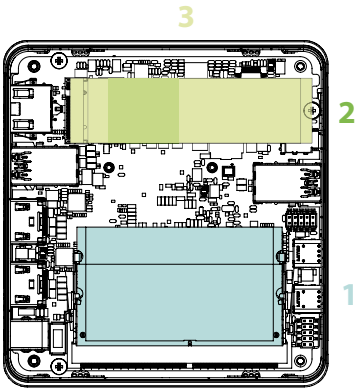
No.	Description
1	DC-IN
2	2 x HDMI
3	2 x USB3.2 Gen2 Ports (Type-A)
4	RJ-45 (2.5G)*

** There is one LED on the LAN port. Please refer to the table below for the LAN port LED indications.*



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

2.3 Inside View



No.	Description
1	SO-DIMM Slots
2	Wifi Module Slot
3	M.2 Slot (2242/2280)

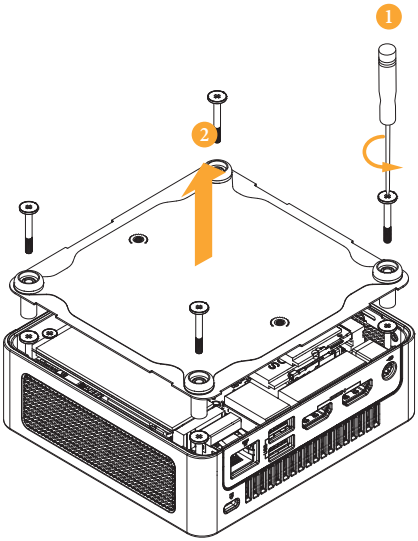
SO-DIMM memory, Wifi module and M.2 are not included with this system.

Chapter 3 Hardware Installation

This chapter helps you install or remove important components.

3.1 How to Remove the Bottom Case

1. Remove the four screws on the bottom case.
2. Then lift up and remove the bottom panel.

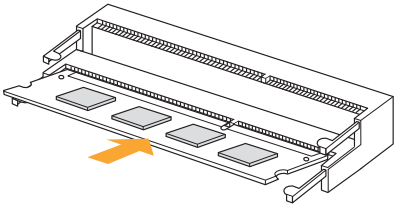


3.2 How to Install the Memory Modules

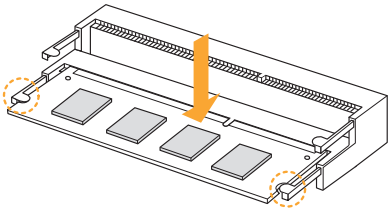
1. The NUCS BOX-1360P/D4 / NUCS BOX-1340P/D4 requires DDR4 SO-DIMM.
2. For dual channel configuration, you always need to install identical (the same brand, speed, size and chip-type) Memory Module SO-DIMM pairs.

The SO-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 at incorrect orientation.

1. Carefully insert the SO-DIMM memory modules into the slot at a 30-degree angle.

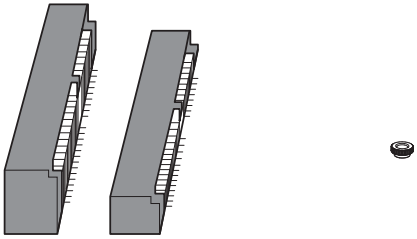


2. Push down until the modules snap into place.

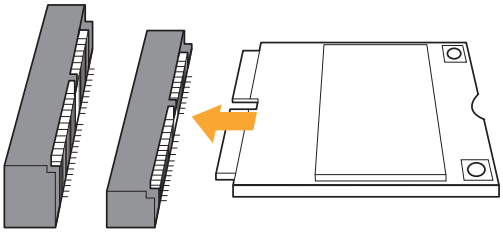


3.3 How to Install the WiFi Module

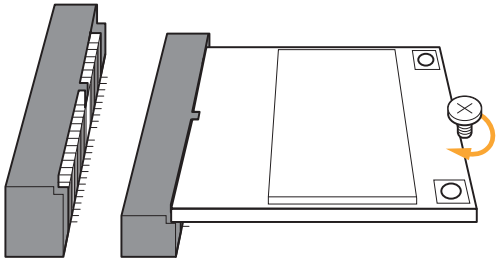
1. Locate the WiFi Module slot on the motherboard.



2. Carefully insert the WiFi Module into the slot.

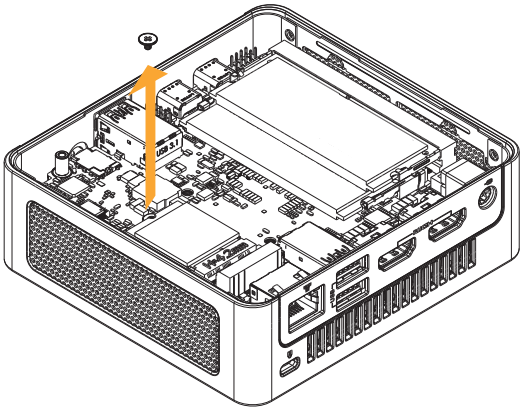


3. Tighten the screw to secure the WiFi Module to the motherboard.

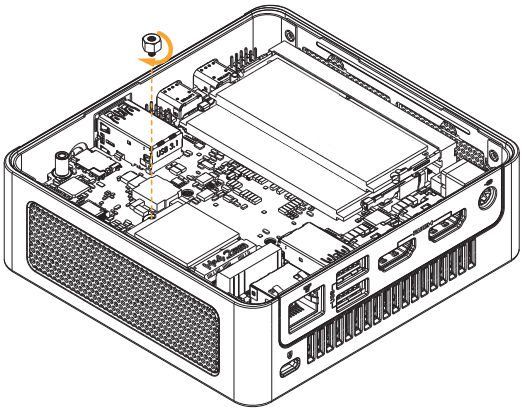


3.4 How to Install the M.2 SSD (Type 2242)

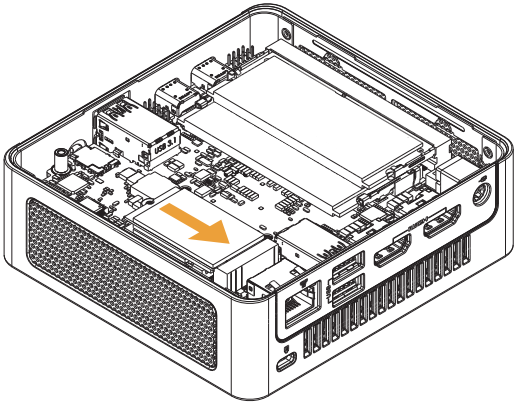
1. Release and remove the screw.



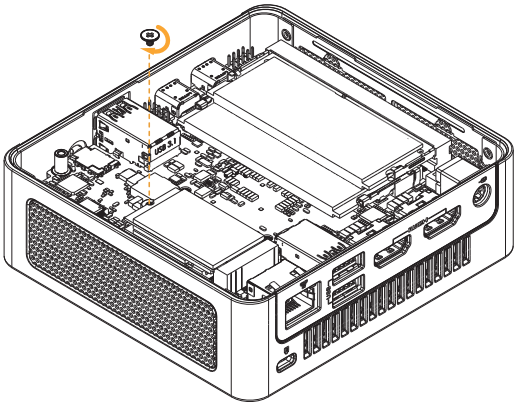
2. Locate the M.2 slot on the motherboard. Install the standoff.



3. Carefully insert the M.2 SSD (Type 2242) into the slot.

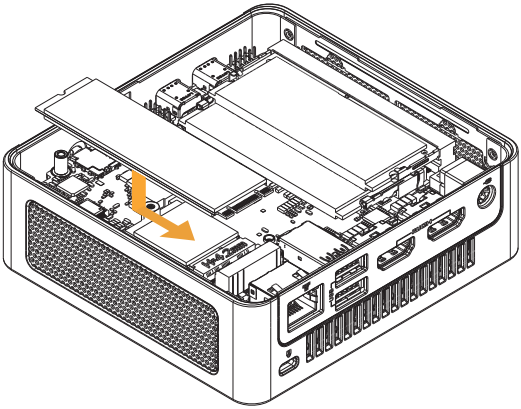


4. Tighten the screw to secure the M.2 SSD (Type 2242) to the motherboard.

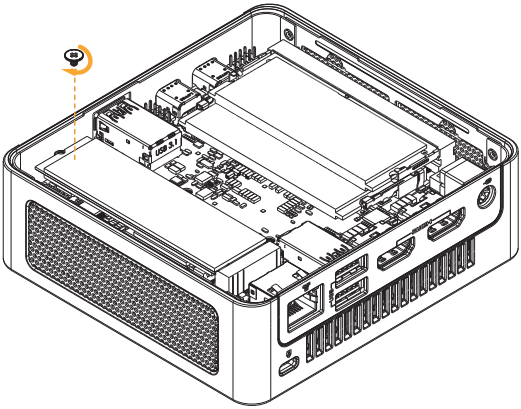


3.5 How to Install the M.2 SSD (Type 2280)

1. Carefully insert the M.2 SSD (Type 2280) into the slot.

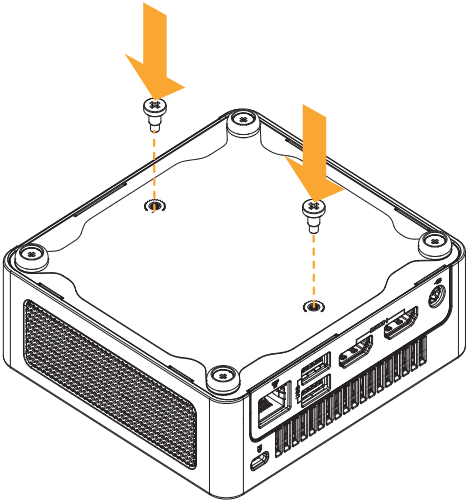


2. Tighten the screw to secure the M.2 SSD (Type 2280) to the motherboard.

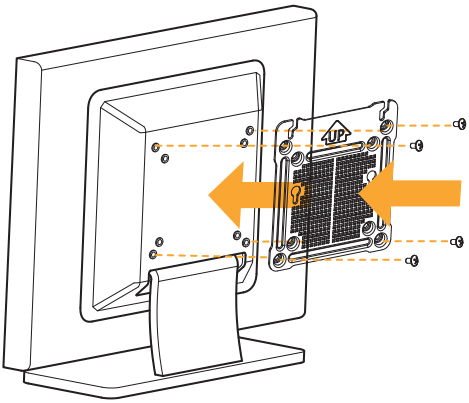


3.6 How to Install the VESA Bracket

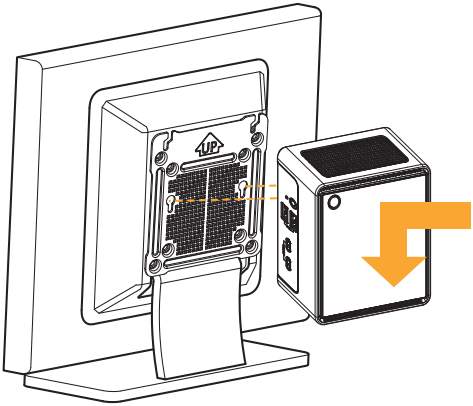
1. Attach the two screws to the base of the NUCS BOX-1360P/D4 / NUCS BOX-1340P/D4.



2. Attach the VESA Bracket to the rear of a compatible display using the four screws.
*Choose mounting holes depending on the mounting hole pattern of your LCD screen (75 mm × 75 mm or 100 mm × 100 mm).

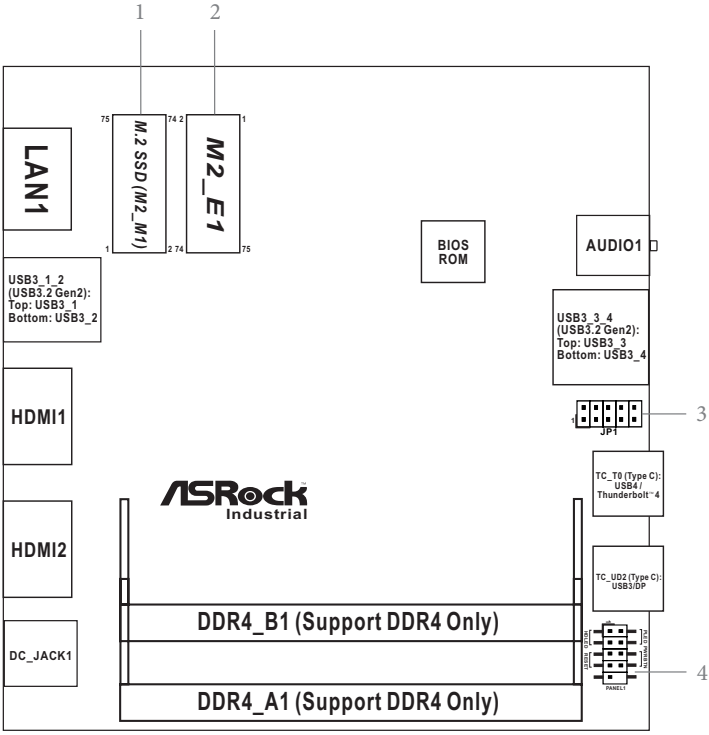


3. Mount the NUCS BOX-1360P/D4 / NUCS BOX-1340P/D4 by sliding it into place.



Chapter 4 Motherboard

4.1 Motherboard Layout



1 : M.2 Key-M Socket (M2_M1)
2 : M.2 Key-E Socket (M2_E1)
3 : JP1
JP1_21: SIO AT Mode
JP1_35: DACC
JP1_46: CMOS2
JP1_68: CMOS
4 : System Panel Header (PANEL1)

<u>Back Side:</u>
Power Button (PWR_BTN1)
Fan Connector (FAN1)
Battery Connector (BAT1)
ESPI Connector (ESPI1)

English

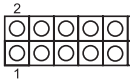
4.2 Onboard Headers and Connectors

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

JP1 Header

(10-pin JP1)

(see p. 16, No. 3)



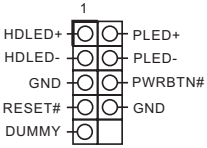
JP1_21: SIO AT Mode
JP1_35: DACC*
JP1_46: CMOS2
JP1_68: CMOS

Auto clear CMOS when system boot improperly.

System Panel Header

(9-pin PANEL1)

(see p. 16, No. 4)



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.

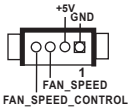
Backside:

Power Button

(PWR_BTN1)

Fan Connector

(FAN1)



Battery Connector

(BAT1)

ESPI Connector

(ESPI1)

4.3 Expansion Slots (M.2 Slots)

There are 2 M.2 sockets on this motherboard.

M.2 sockets:

1 x M.2 (Key M, 2242/2260/2280) with PCIex4 for SSD
*M.2 Key M 2280(Supported by bracket)
1 x M.2 (Key E, 2230) with PCIe x1, USB 2.0 and CNVi for Wireless

M.2 Key-M Socket
(M2_M1)

PIN	SIGNAL	SIGNAL	PIN
75	GND		
73	GND	+3.3V	74
71	GND	+3.3V	72
69	PEDET	+3.3V	70
67	NA	NA	68
57	GND	NA	58
55	PEFCLKp	NA	56
53	PEFCLKn	WAKE#	54
51	GND	CLKREQ#	52
49	PETP0	PERST#	50
47	PETn0	NA	48
45	GND	NA	46
43	PERp0	NA	44
41	PERn0	NA	42
39	GND	NA	40
37	PETp1	GND	38
35	PETn1	USB2_DN	36
33	GND	USB2_DP	34
31	PERp1	GND	32
29	PERn1	NA	30
27	GND	NA	28
25	PETp2	NA	26
23	PETn2	NA	24
21	GND	NA	22
19	PERp2	NA	20
17	PERn2	+3.3V	18
15	GND	+3.3V	16
13	PETp3	+3.3V	14
11	PETn3	+3.3V	12
9	GND	LED#	10
7	PERp3	NA	8
5	PERn3	NA	6
3	GND	+3.3V	4
1	GND	+3.3V	2

M.2 Key-E Socket
(M2_E1)

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

Chapter 5 UEFI SETUP UTILITY

5.1 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.

5.1.1 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.

5.1.2 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.

5.1.3 Navigation Keys

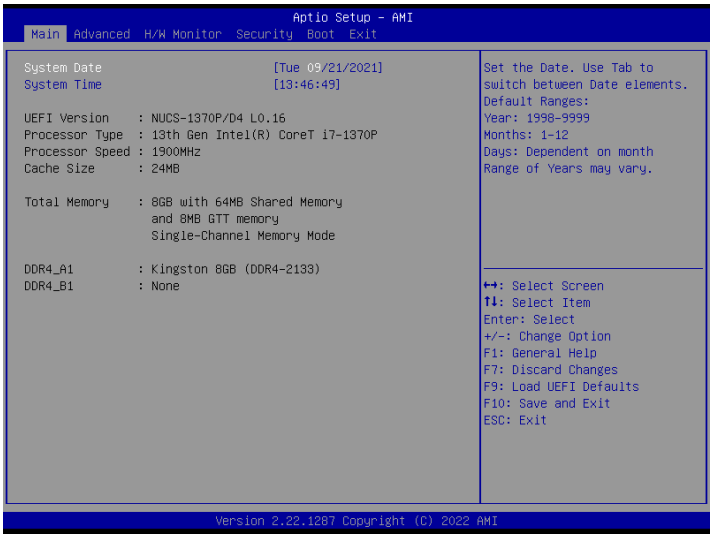
Use <←> key or <→> key to choose among the selections on the menu bar, and use < ↑ > key or < ↓ > key to move the cursor up or down to select items, then press <Enter> to get into the sub screen. You can also use the mouse to click your required item.

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

5.2 Main Screen (Advanced Mode)

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

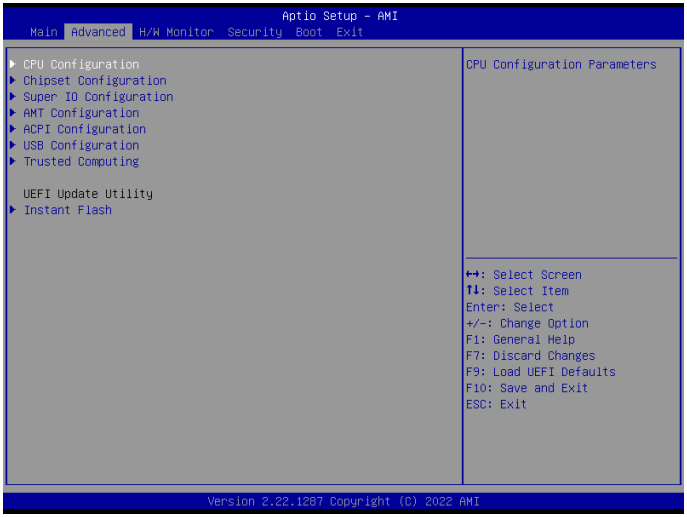


Because the UEFI software is constantly being updated, the following UEFI setup screens and descriptions are for reference purpose only, and they may not exactly match what you see on your screen. Options may also vary depending on the features of your motherboard.

English

5.3 Advanced Screen

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



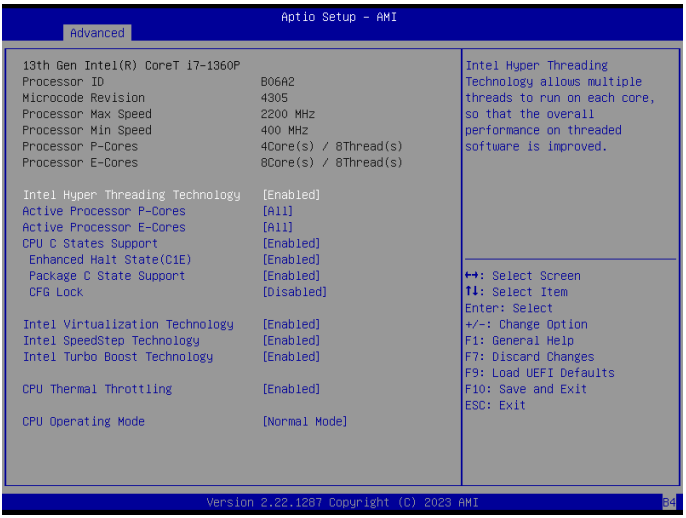
Setting wrong values in this section may cause the system to malfunction.

Instant Flash

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

Configuration options: [Easy Mode] [Advanced Mode]

5.3.1 CPU Configuration



Intel Hyper Threading Technology

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

Configuration options: [Enabled] [Disabled]

Active Processor P-Cores

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

Active Processor E-Cores

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

CPU C States Support

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

Configuration options: [Enabled] [Disabled]

Enhanced Halt State (C1E)

Allows you to enable Enhanced Halt State (C1E) for lower power consumption.

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

Package C State Support

Allows you to enable CPU, PCIe, Memory, Graphics C State Support for power saving.

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

CFG Lock

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® 7 / 8 / 8.1 / 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.

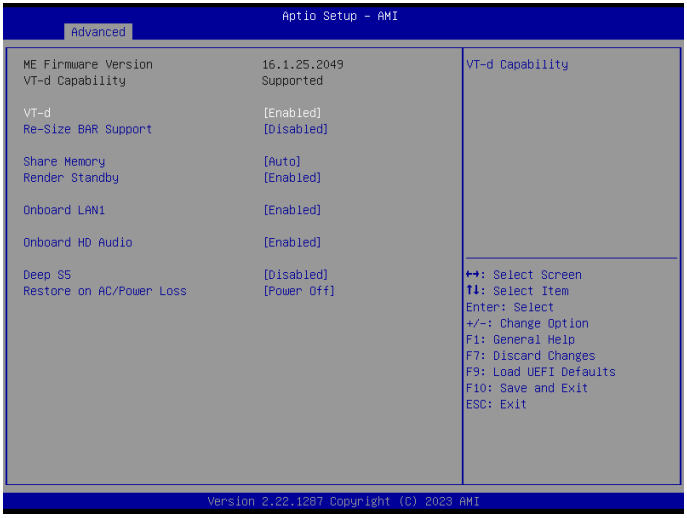
Configuration options: [Enabled] [Disabled]

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]

5.3.2 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] [1024M] Options vary depending on the memory you use on your motherboard.

Render Standby

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

Onboard LAN1

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

Onboard HD Audio

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

Configuration options: [Enabled] [Disabled]

Deep S5

Mobile platforms support Deep S4/S5 in DC only and desktop platforms support Deep S4/S5 in AC only. The default value is [Disabled].

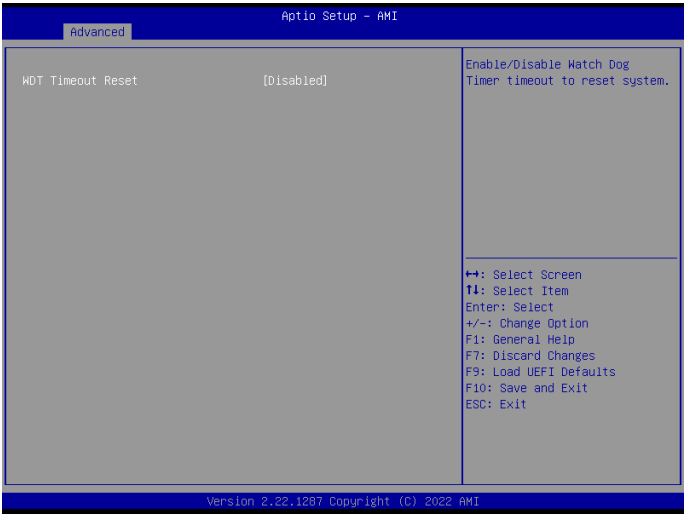
Restore on AC/Power Loss

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

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

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

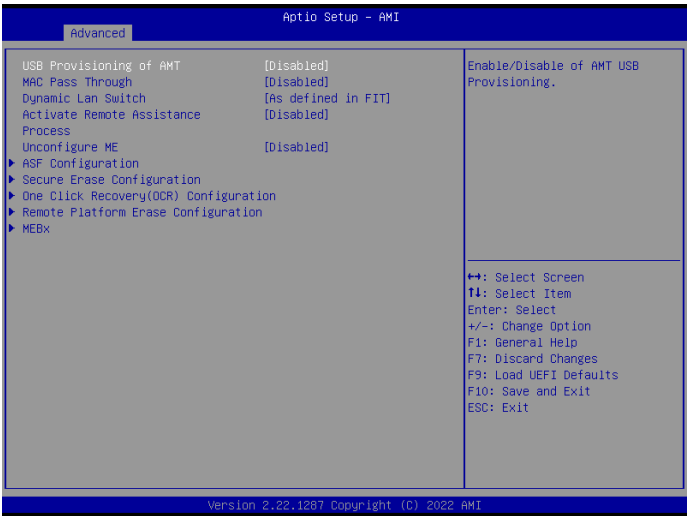
5.3.3 Super IO Configuration



WDT Timeout Reset

Use this to set the Watch Dog Timer.

5.3.4 AMT Configuration



USB Provisioning of AMT

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

MAC Pass Through

Use this to enable or disable MAC Pass Through. The default is [Disabled].

Dynamic Lan Switch

The option allows switching AMT support from Integrated LAN to Discrete LAN.

Activate Remote Assistance Process

Trigger CIRA boot. The default is [Disabled].

UnConfigure ME

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

PET Progress

User can enable or disable PET Events progress to receive PET events or not. The default is [Enabled].

WatchDog

Use this to enable or disable AMT WatchDog Timer. The default is [Disabled].

ASF Sensors Table

Use this to enable or disable ASF Sensor Table. The default is [Disabled].

Secure Erase mode

Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD. Real: Erase SSD.

Force Secure Erase

Use this to enable or disable Force Secure Erase on next boot. The default is [Disabled].

OCR Http Boot

Use this to enable or disable One Click Recovery Https Boot. The default is [Enabled].

OCR PBA Boot

Use this to enable or disable One Click Recovery PBA Boot. The default is [Enabled].

OCR Windows Recovery Boot

Use this to enable or disable One Click Recovery Windows Recovery Boot. The default is [Enabled].

OCR Disable Secure Boot

Use this to allows CSME to request Secure Boot to be disabled for One Click Recovery. The default is [Enabled].

Enable Remote Platform Erase Feature

Use this to enable or disable Remote Platform Erase Feature. The default is [Enabled].

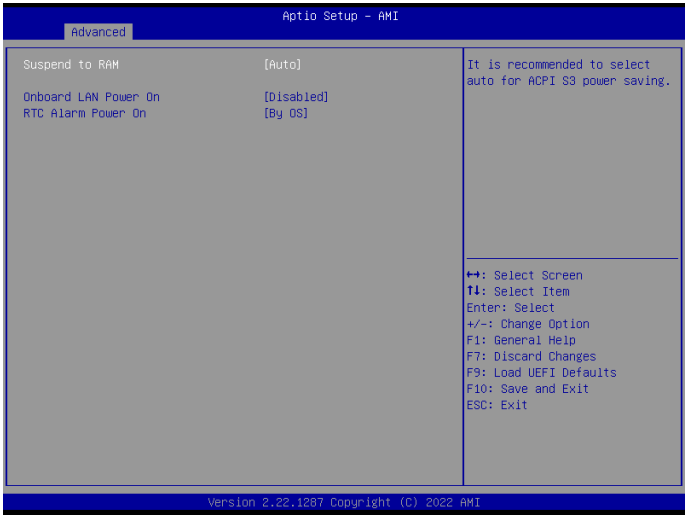
SSD Erase mode

Change RPE SSD Erase Action behavior: Simulated: Performs RPE SSD Erase flow without erasing SSD Real: Erase SSD.

Intel(R) ME Password

MEBx Login

5.3.5 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]

Onboard LAN Power On

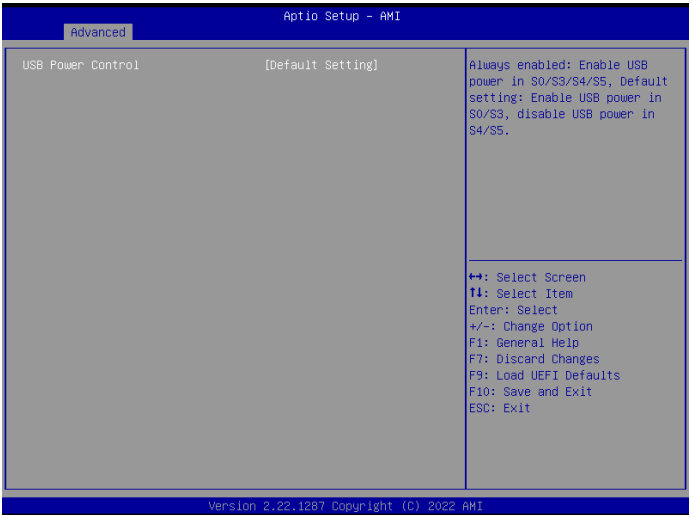
Use this item to enable or disable onboard LAN to turn on the system from the power-soft-off mode.

RTC Alarm Power On

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

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

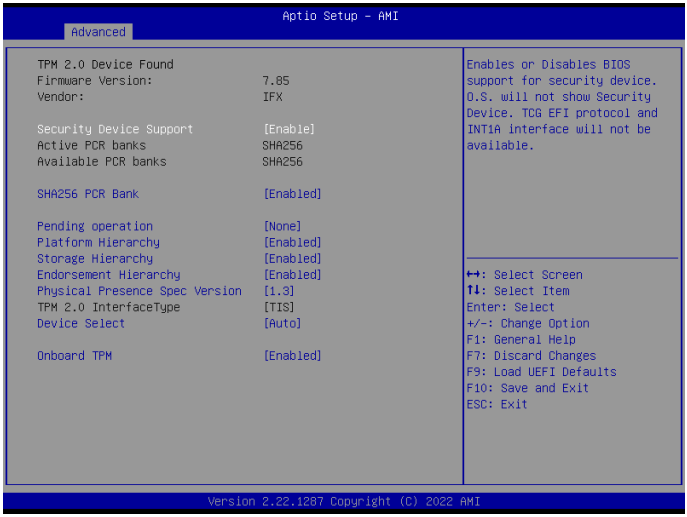
5.3.6 USB Configuration



USB Power Control

Use this option to control USB power.

5.3.7 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]

Pending Operation

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

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

Configuration options: [None] [TPM Clear]

Platform Hierarchy

This item allows you to enable or disable Platform Hierarchy.

Configuration options: [Enabled] [Disabled]

Storage Hierarchy

This item allows you to enable or disable Storage Hierarchy.

Configuration options: [Enabled] [Disabled]

Endorsement Hierarchy

This item allows you to enable or disable Endorsement Hierarchy.

Configuration options: [Enabled] [Disabled]

Physical Presence Spec Version

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

Configuration options: [1.2] [1.3]

TPM 2.0 InterfaceType

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

Device Select

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

[TPM 1.2] restricts support to TPM 1.2 devices.

[TPM 2.0] restricts support to TPM 2.0 devices.

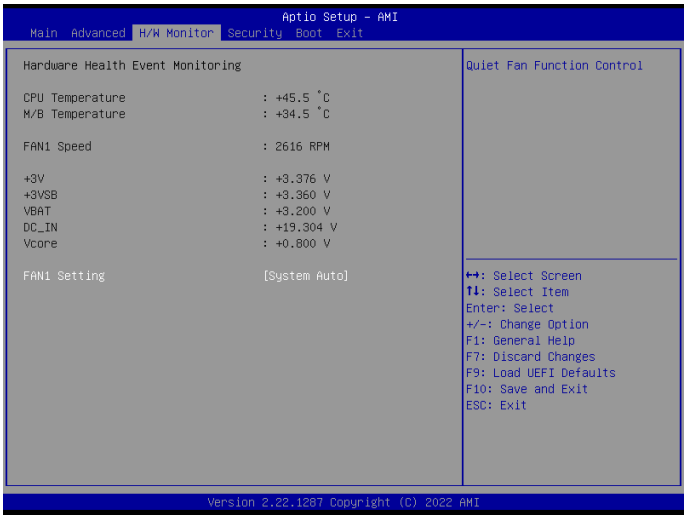
[Auto] supports both TPM 1.2 and TPM 2.0 devices with the default set to TPM 2.0 devices. If TPM 2.0 devices are not found, TPM 1.2 devices will be enumerated.

Onboard TPM

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

5.4 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, chassis fan speed, and the critical voltage.



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

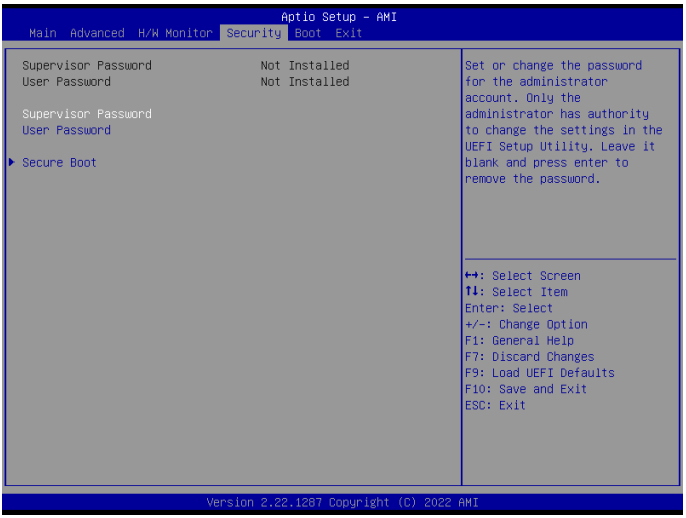
Fan1 Setting

This item allows you to select a fan mode for Fan 1. The default value is [System Auto].

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

5.5 Security Screen

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



Supervisor Password

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

User Password

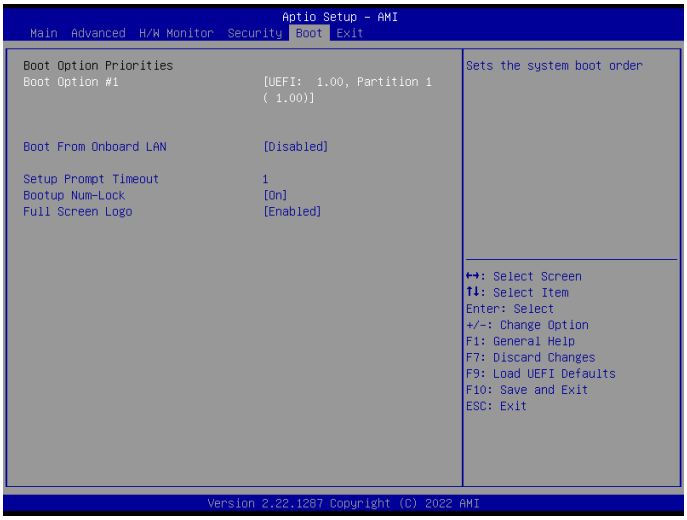
Set or change the password for the user account. Users are unable to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

Secure Boot

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

5.6 Boot Screen

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



Boot Option #1

The item allows you to set the system boot order.

Boot From Onboard LAN

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

Configuration options: [Enabled] [Disabled]

Setup Prompt Timeout

The item allows you to 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.

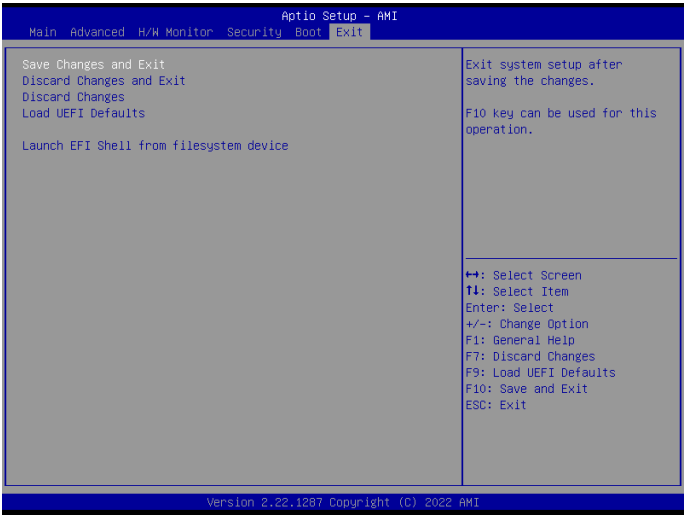
Configuration options: [On] [Off]

Full Screen Logo

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

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

5.7 Exit Screen



Save Changes and Exit

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

Discard Changes and Exit

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

Discard Changes

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

Load UEFI Defaults

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

Launch EFI Shell from filesystem device

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

Chapter 6 Software Support

6.1 Install Operating System

This motherboard supports various Microsoft® Windows® operating systems:
11 64-bit / 10 64-bit. Because motherboard settings and hardware options vary, use the setup procedures in this chapter for general reference only. Refer your OS documentation for more information.