



MS-C910

Industrial Data Machine

User Guide

Contents

- Regulatory Notices.....4
- Safety Information7
- Specifications9
- SKU Features Comparison12
- System Overview13
 - System I/O & Controls..... 14
 - System Internal View 18
- ME Overview.....19
 - System Dimensions 19
 - PCIe and PCI Card Dimensions..... 27
- Motherboard Jumpers28
- Getting Started29
 - Safety Precautions..... 29
- System Covers.....30
 - Removing System Top Cover..... 30
 - Removing System Side Cover..... 31
- CPU & Heatsink32
 - CPU Socket..... 32
 - Locating CPU Socket..... 32
 - Installing CPU 33
 - Installing the Heatsink..... 34
 - Removing the Heatsink 35
- Memory Module36
 - DDR5 DIMM Thermal Pad Thickness Recommendations..... 36
 - Installing Memory Module..... 36
- M.2 Slots37
 - Installing M.2 SSD (2280, M-Key) 37
 - Installing M.2 Wi-Fi Card (2230, E-Key, for SKU1 Only)..... 38

Revision
V1.1, 2025/03

Mini-PCIe Slot (for SKU2 Only)	39
Installing Mini-PCIe Card	39
2.5" SSD/HDD Brackets (for SKU1~3)	40
Installing 2.5" HDD/ SSD (7mm)	40
PCIe Expansion Card.....	44
Installing PCIe Expansion Card.....	44
Power Connector	46
Connecting DC Receptacle Connector	46
DIO Connector	47
Connecting DIO Switch Connector	47
Wall Mount.....	48
Installing Wall Mount Bracket.....	48
BIOS Setup.....	49
Entering Setup	49
The Menu Bar	51
Main.....	52
Advanced	54
Boot	63
Security	64
Chipset	75
Power	76
Save & Exit.....	78
GPIO WDT Programming.....	79
Abstract	79
General Purpose IO	80
Watchdog Timer.....	81

Regulatory Notices

CE Conformity

This product has been tested and found to comply with the harmonized standards for Information Technology Equipment published under Directives of Official Journal of the European Union.



FCC-A Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.



Notice 1

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Notice 2

Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

WEEE Statement

Under the European Union (“EU”) Directive on Waste Electrical and Electronic Equipment, Directive 2012/19/EU, products of “electrical and electronic equipment” cannot be discarded as municipal waste anymore and manufacturers of covered electronic equipment will be obligated to take back such products at the end of their useful life.



Chemical Substances Information

In compliance with chemical substances regulations, such as the EU REACH Regulation (Regulation EC No. 1907/2006 of the European Parliament and the Council), MSI provides the information of chemical substances in products at:

<https://csr.msi.com/global/index>

Battery Information

Please take special precautions if this product comes with a battery.

- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.
- Avoid disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, which can result in an explosion.
- Avoid leaving a battery in an extremely high temperature or extremely low air pressure environment that can result in an explosion or the leakage of flammable liquid or gas.
- Do not ingest battery. If the coin/button cell battery is swallowed, it can cause severe internal burns and can lead to death. Keep new and used batteries away from children.

European Union:



Batteries, battery packs, and accumulators should not be disposed of as unsorted household waste. Please use the public collection system to return, recycle, or treat them in compliance with the local regulations.

BSMI:



廢電池請回收

For better environmental protection, waste batteries should be collected separately for recycling or special disposal.

California, USA:



The button cell battery may contain perchlorate material and requires special handling when recycled or disposed of in California.

For further information please visit:

<http://www.dtsc.ca.gov/hazardouswaste/perchlorate/>

Environmental Policy

- The product has been designed to enable proper reuse of parts and recycling and should not be thrown away at its end of life.
- Users should contact the local authorized point of collection for recycling and disposing of their end-of-life products.
- Visit the MSI website and locate a nearby distributor for further recycling information.
- Users may also reach us at gpcontdev@msi.com for information regarding proper disposal, take-back, recycling, and disassembly of MSI products.
- Please visit <<https://us.msi.com/page/recycling>> for information regarding the recycling of your product in the US.



Copyright and Trademarks Notice

msi **MSI** **微星** **微星科技**

MICRO-STAR INTERNATIONAL



Copyright © Micro-Star Int'l Co., Ltd. All rights reserved. The MSI logo used is a registered trademark of Micro-Star Int'l Co., Ltd. All other marks and names mentioned may be trademarks of their respective owners. No warranty as to accuracy or completeness is expressed or implied. MSI reserves the right to make changes to this document without prior notice.

HDMI™
HIGH-DEFINITION MULTIMEDIA INTERFACE

The terms HDMI™, HDMI™ High-Definition Multimedia Interface, HDMI™ Trade dress and the HDMI™ Logos are trademarks or registered trademarks of HDMI™ Licensing Administrator, Inc.

Technical Support

If a problem arises with your product and no solution can be obtained from the user's manual, please contact your place of purchase or local distributor. Alternatively, please visit <https://www.msi.com/support/> for further guidance.

Safety Information



Please read and follow these safety instructions carefully before installing, operating or performing maintenance on the equipment.

General Safety Instructions

- Always read the safety instructions carefully.
- Keep this User's Manual for future reference.
- Keep this equipment in a dry, humidity-free environment.
- Ensure that all components are securely connected to prevent issues during operation.
- Do not cover the air openings to prevent overheating.
- Avoid spilling liquids into the equipment to prevent damage or electrical shock.
- Do not leave the equipment in an unconditioned environment. Storage temperatures above 60°C (140°F) may cause damage.

Electrostatic Discharge (ESD) Precautions

The components included in this package are sensitive to electrostatic discharge. Follow these guidelines to prevent ESD-related damage:

- Hold the motherboard by the edges to avoid touching sensitive components.
- Wear an ESD wrist strap. If not available, discharge static electricity by touching a metal object before handling.
- When not installed, store the motherboard in an electrostatic shielding container or place it on an anti-static pad.

Power Safety

- Always turn off the power supply and unplug the power cord from the outlet before installing or removing any component.
- Ensure the electrical outlet provides the same voltage as indicated on the PSU before connecting.
- Arrange the power cord to avoid tripping hazards or damage. Do not place objects over the power cord.

Installation Instructions

- Lay the equipment on a stable, flat surface before setting it up.
- Before turning on the system, ensure there are no loose screws or metal components on the motherboard or within the system case.
- Do not boot the computer before completing all installations. Premature booting can cause permanent damage to components and pose safety risks.

When to Contact Service Personnel

Immediately consult service personnel if any of the following situations arise:

- The power cord or plug is damaged.
- Liquid has entered the equipment.
- The equipment has been exposed to moisture.
- The equipment does not function as described in the User Guide.
- The equipment has been dropped or physically damaged.
- The equipment shows visible signs of breakage.

Specifications

Model	SKU1	SKU2	SKU3	SKU4
Processor	<ul style="list-style-type: none">• 14th Gen Intel® IOTG Raptor Lake-S Refresh Processor Core™ i9/i7/i5/i3<ul style="list-style-type: none">- i9-14900T (35W)- i7-14700T (35W)- i5-14600T (35W)- i3-14100T (35W)- 300T (35W)• 13th Gen Intel® IOTG Raptor Lake-S Processor Core™ i9/i7/i5/i3<ul style="list-style-type: none">- i9-13900TE (35W)- i7-13700T (35W) / i7-13700TE (35W)- i5-13500T (35W) / i5-13500TE (35W)- i3-13100T (35W) / i3-13100TE (35W)• 12th Gen Intel® IOTG Alder Lake-S Processor Core™ i9/i7/i5/i3, Pentium®, Celeron®<ul style="list-style-type: none">- i9-12900TE (35W)- i7-12700TE (35W)- i5-12500TE (35W)- i3-12100TE (35W)- Pentium® G7400TE / Celeron® G6900TE (35W)			
Chipset	Intel® R680E			
iAMT Support	<ul style="list-style-type: none">• Supports Intel® AMT 16.x (Only for Intel® Core™ i9/i7/i5 Processor Series at LAN1)			
Memory	<ul style="list-style-type: none">• 2 x DDR5 SO-DIMM slots (262-pin)- Dual-channel DDR5, ECC/ Non-ECC (ECC support depends on CPU)- Up to 5600 MT/s (depends on CPU)- Up to 64GB			
Network	<ul style="list-style-type: none">• 1 x Intel® I226-LM PCIe 2.5GbE RJ45 LAN (supports iAMT 16.X)• 3 x Intel® I226-V PCIe 2.5GbE RJ45 LAN			
Storage	<ul style="list-style-type: none">• 2 x SATA 3.0 6Gb/s ports- Supports RAID 0/1, AHCI mode- Supports 2 x 2.5" SSD/HDD, 7mm			
Expansion Slots	<ul style="list-style-type: none">• 1 x M.2 M Key slot (2280, internal)- Supports PCIe 4.0 x4 & SATA 3.0 (signal from PCH)- Supports B+M Key PCIe x4/ SATA 3.0 module			
	<ul style="list-style-type: none">• 1 x PCIe 4.0 x16 slot• 3 x PCI slots• 1 x M.2 E Key slot (2230)- Supports PCIe 4.0 x1, USB 2.0 signal	<ul style="list-style-type: none">• 1 x PCIe 4.0 x16 slot• 1 x PCI slot• 1 x Mini-PCIe slot (full-size)	<ul style="list-style-type: none">• 1 x PCIe 4.0 x16 slot	<ul style="list-style-type: none">• 2 x PCIe 4.0 x8 slot

Continued on next column

Model	SKU1	SKU2	SKU3	SKU4
Audio	<ul style="list-style-type: none">• Realtek® ALC897 High Definition Audio Codec• 2 x Audio jacks (Line-out, Mic-in)			
Graphics	<ul style="list-style-type: none">• 2 x DP 1.4a up to 4096×2304 @60Hz• 2 x HDMI™ 2.0b up to 4096x2160 @60Hz• 4 independent display modes supported<ul style="list-style-type: none">- DP1 + DP2 + HDMI™1 + HDMI™2			
Internal USB Connectors	3 x USB 2.0 Type-A ports (480 Mbps)			
Front I/O	<ul style="list-style-type: none">• 4 x 2.5 Gbps RJ-45 LAN ports• 8 x USB 10Gbps Type-A ports• 2 x DisplayPort (1.4a)• 2 x HDMI™ connector (2.0b)• 4 x COM ports<ul style="list-style-type: none">- COM1~2: RS232/ 422/ 485, 0V/ 5V/ 12V- COM3~4: RS232, 0V• 1 x GPIO (DIO) port<ul style="list-style-type: none">- 8-bit (4 x GPI, 4 x GPO), 5~35V, isolation 1.3KV• 1 x Line-out jack• 1 x Mic-in jack• 1 x HDD Activity LED<ul style="list-style-type: none">- Indicates activity for 1 x M.2 M key SSD and 2 x SATA 3.0 2.5" SSD/HDD.• 1 x Power button/ LED			
Rear I/O	<ul style="list-style-type: none">• 2 x USB 5Gbps Type-A ports			
	<ul style="list-style-type: none">• 2 x Openings reserved for antennas			
Jumpers	<ul style="list-style-type: none">• 2 x COM voltage select jumpers (JCOM1~2)• 1 x Clear CMOS jumper• 1 x ME jumper• 1 x AT/ ATX mode select jumper			
Power Solution	<ul style="list-style-type: none">• 1 x 8~48V DC power jack (max 10A)• 1 x 8~48V Phoenix DC power connector (max 16A)			
Dimensions	178 (W) x 242 (D) x 217 (H) mm	142 (W) x 240 (D) x 217 (H) mm	123 (W) x 240 (D) x 217 (H) mm	127 (W) x 240 (D) x 217 (H) mm
Weight	5.0 kg	4.4 kg	4.3 kg	4.4 kg
Mounting	Wall mount			

Continued on next column

Model	SKU1	SKU2	SKU3	SKU4
Kensington Lock	Yes			
OS Support*	<ul style="list-style-type: none"> • Windows 10 IoT Enterprise 21H2 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC 24H2 (64-Bit) • Linux Kernel 5.xx, Ubuntu 22.04.3 LTS Pre-scan <p>*All drivers are based on Intel and chip vendor support.</p>			
Regulatory Compliance	FCC Class A / CE / RCM / BSMI / VCCI / UKCA / IC / IEC 62368: CE (LVD) / RoHS Compliant			
Environment	<ul style="list-style-type: none"> • Operation Temperature: -10 ~ 50°C (Air Flow: 0.7m/s) - With Industrial DC power up to 35W CPU • Operation Humidity: 5 ~ 90%, non-condensing • Storage Temperature: -20 ~ 80°C • Storage Humidity: 5~ 90%, non-condensing • Vibration : IEC 60068-2-64: 2Grms, random, 5 ~ 500Hz, 1hr/axis (w/ HDD/SSD) • Shock : IEC 60068-2-27: 50G, half sine, 11ms (w/ HDD/SSD) 			

SKU Features Comparison

SKU#		SKU1 (4-Slot)	SKU2 (2-Slot)	SKU3 (1-Slot)	SKU4 (2-Slot)
Features					
Motherboard		MS-C9101			
Riser Board		MS-C910A	MS-C910B	MS-C910C	MS-C910D
Expansions	PCIe x16	1			
	PCIe x8				2
	PCI	3	1		
	Mini-PCIe		1		
Storage	SATA	2 x 2.5" HDD/SSD			
M.2	M Key	1			
	E Key	1			
Antenna		2			

System Overview

4-Slot



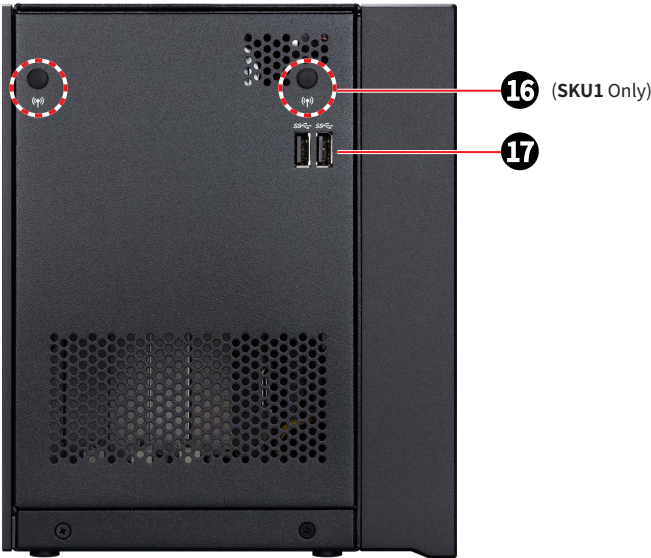
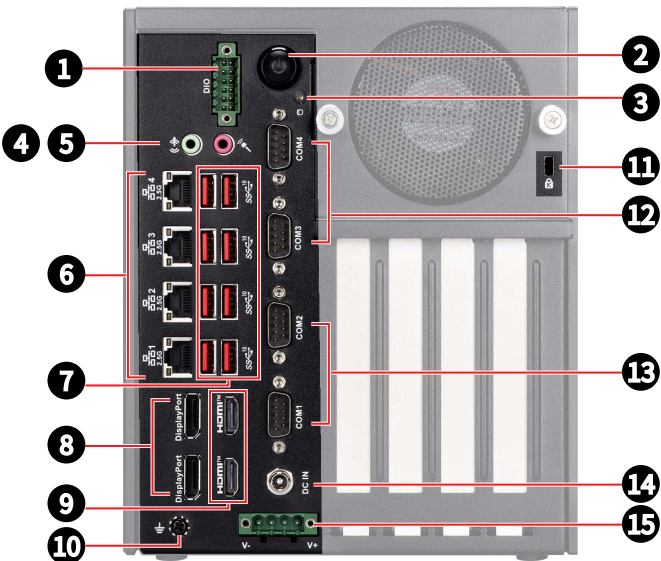
2-Slot

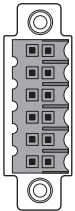














1-Slot



System I/O & Controls



	<div>DIO Port</div> <div>This Digital I/O connector is suitable for various industrial applications, including programmable logic devices and custom-embedded applications that extensively use GPIO. It can read data from environmental sensors (IR, video, temperature, 3-axis orientation, and acceleration) and output signals to DC motors (via PWM), audio devices, LCD displays, or LEDs for status indication. The isolated Digital I/O pins provide electrical protection to the system, safeguarding it from damage caused by high current devices and high voltages.</div> <div><div><div><div>12</div><div>6</div><div>7</div><div>1</div></div><table><tr><th>PIN</th><th>SIGNAL</th><th>PIN</th><th>SIGNAL</th></tr><tr><td>1</td><td>EOGND</td><td>7</td><td>EOGND</td></tr><tr><td>2</td><td>D_GPI0</td><td>8</td><td>D_GPO0</td></tr><tr><td>3</td><td>D_GPI1</td><td>9</td><td>D_GPO1</td></tr><tr><td>4</td><td>D_GPI2</td><td>10</td><td>D_GPO2</td></tr><tr><td>5</td><td>D_GPI3</td><td>11</td><td>D_GPO3</td></tr><tr><td>6</td><td>IVDD</td><td>12</td><td>VDD</td></tr></table></div></div>	PIN	SIGNAL	PIN	SIGNAL	1	EOGND	7	EOGND	2	D_GPI0	8	D_GPO0	3	D_GPI1	9	D_GPO1	4	D_GPI2	10	D_GPO2	5	D_GPI3	11	D_GPO3	6	IVDD	12	VDD
PIN	SIGNAL	PIN	SIGNAL																										
1	EOGND	7	EOGND																										
2	D_GPI0	8	D_GPO0																										
3	D_GPI1	9	D_GPO1																										
4	D_GPI2	10	D_GPO2																										
5	D_GPI3	11	D_GPO3																										
6	IVDD	12	VDD																										
	<div><div></div><div>Power Button/ LED</div><div>Press the button to turn the system on or off.</div><div><div><div></div><table><tr><th>LED Status</th><th>Description</th></tr><tr><td> Off</td><td>ACPI S4/ S5/ Deep S5, Power Off</td></tr><tr><td> Blinking</td><td>ACPI S3</td></tr><tr><td> Green</td><td>ACPI S0</td></tr></table></div></div></div>	LED Status	Description	 Off	ACPI S4/ S5/ Deep S5, Power Off	 Blinking	ACPI S3	 Green	ACPI S0																				
LED Status	Description																												
 Off	ACPI S4/ S5/ Deep S5, Power Off																												
 Blinking	ACPI S3																												
 Green	ACPI S0																												
	<div><div></div><div>HDD Activity LED</div><div>This indicator shows the activity status of the M.2 M key SSD and SATA 3.0 2.5" HDDs/SSDs. It flashes when the system is accessing data on the drives and remains off when no drive activity is detected.</div></div>																												
	<div><div>Line-Out Jack</div><div>This connector is provided for headphones or speakers.</div></div>																												
	<div><div>Mic-In Jack</div><div>This connector is provided for microphones.</div></div>																												

Continued on next column

6

2.5 Gbps LAN Jack

The standard RJ-45 LAN jack is provided for connection to the Local Area Network (LAN). You can connect a network cable to it.

LINK/ACT LED

SPEED LED

LED

Status

Description

Link/ Activity LED

Off

No link

Yellow

Linked

Blinking

Data activity

Speed LED

Off

10/100 Mbps

Green

1 Gbps

Orange

2.5 Gbps

7

USB 10Gbps Port

This connector is provided for USB peripheral devices. (Speed up to 10 Gbps)

8

DisplayPort

Supports 4096x2304@60Hz as specified in DisplayPort 1.4a.

9

HDMI™ Connector

HDMI™

HIGH-DEFINITION MULTIMEDIA INTERFACE

Supports 4096x2160@60Hz as specified in HDMI™ 2.0b.

10

Grounding Point

The Grounding Point is provided to connect a grounding wire.

11

Kensington Lock Port

The Kensington lock port allows users to secure the PC in place with a key or mechanical PIN device by attaching a rubberized metal cable.

12

RS232 Serial Port: COM3~4

The serial port is a 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial mouse or other serial devices directly to the connector.

1

5

6

9

RS232

PIN

SIGNAL

DESCRIPTION

1

ND CD

Data Carrier Detect

2

NS IN

UART Serial Input

3

NS OUT

UART Serial Output

4

ND TR

UART Data Terminal Ready

5

GND

Signal Ground

6

NDSR

Data Set Ready

7

NRTS

UART Request To Send

8

NCTS

Clear To Send

9

NC

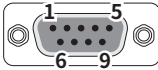
No Connection

Continued on next column

13

RS232/422/485 Serial Port: COM1~2

The serial port is a 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial mouse or other serial devices directly to the connector.



RS232		
PIN	SIGNAL	DESCRIPTION
1	NDCD	Data Carrier Detect
2	NSIN	UART Serial Input
3	NSOUT	UART Serial Output
4	NDTR	UART Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	UART Request To Send
8	NCTS	Clear To Send
9	VCC	5V/12V selected by <u>jumper JCOM1~2</u>

RS422		
PIN	SIGNAL	DESCRIPTION
1	TXD-	Transmit Data, Negative
2	RXD+	Receive Data, Positive
3	TXD+	Transmit Data, Positive
4	RXD-	Receive Data, Negative
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

RS485		
PIN	SIGNAL	DESCRIPTION
1	DATA-	Data, Negative
2	DATA+	Data, Positive
3	NC	No Connection
4	NC	No Connection
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

14

8~48V DC Power Jack

Power supplied through this jack supplies power to the system.

15

8~48V Phoenix DC Power Connector

The system is designed with a Phoenix connector that carries wide-range DC input and features reverse wiring protection.

16

Wi-Fi Antenna Connector (Openings reserved for antennas, SKU1 only)

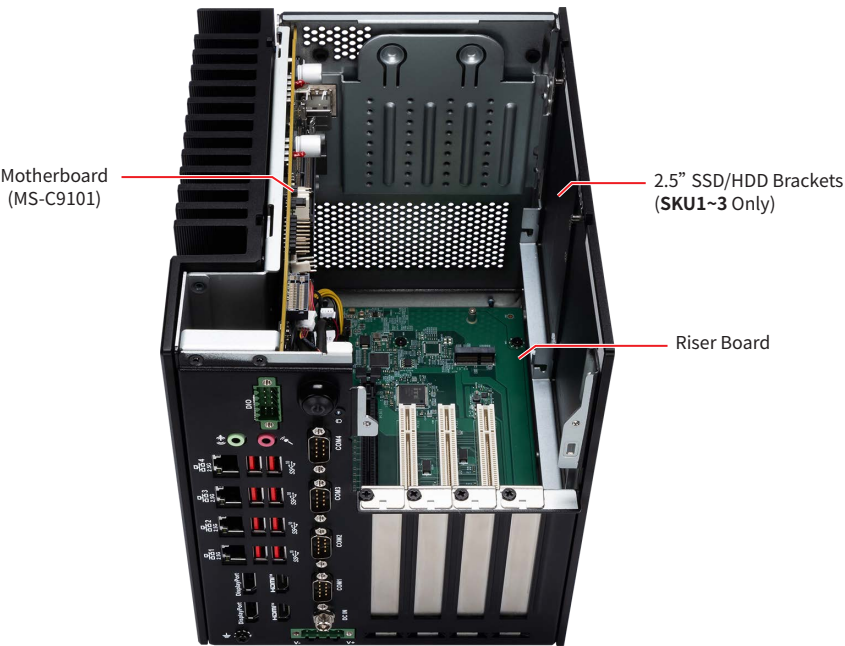
These connectors allow you to connect sn external antenna for wireless communication. User may find two on the rear side of the PC.

17

USB 5Gbps Port

This connector is provided for USB peripheral devices. (Speed up to 5 Gbps)

System Internal View

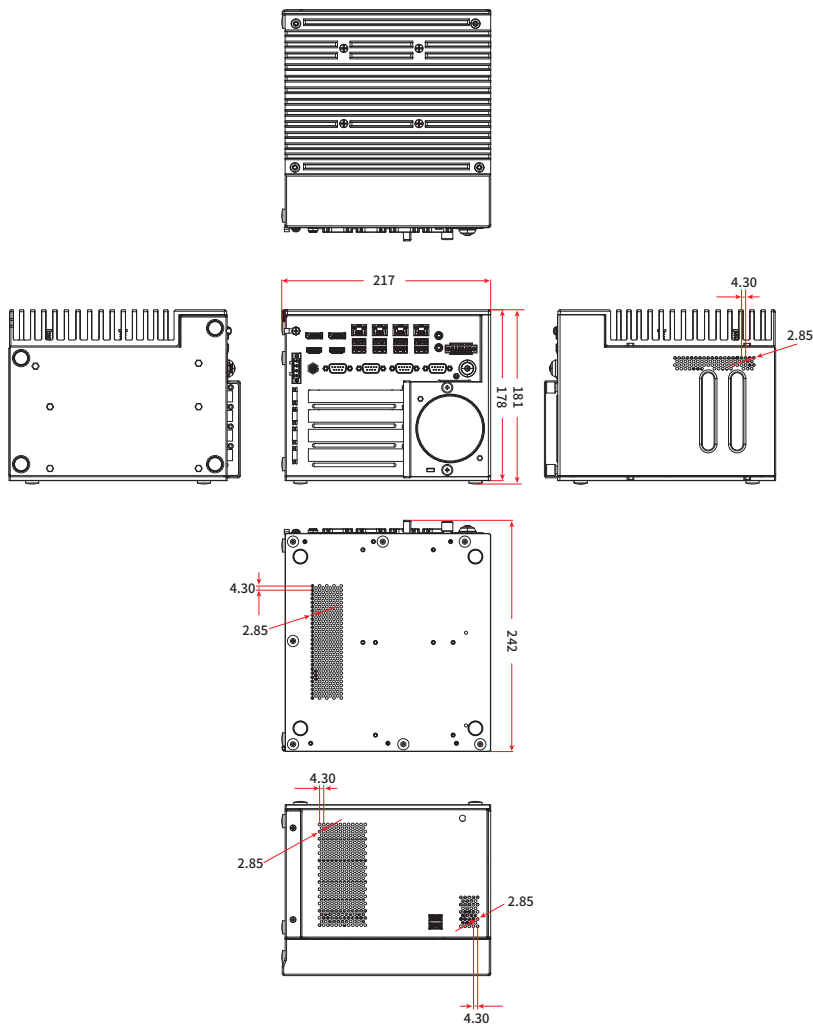


ME Overview

System Dimensions

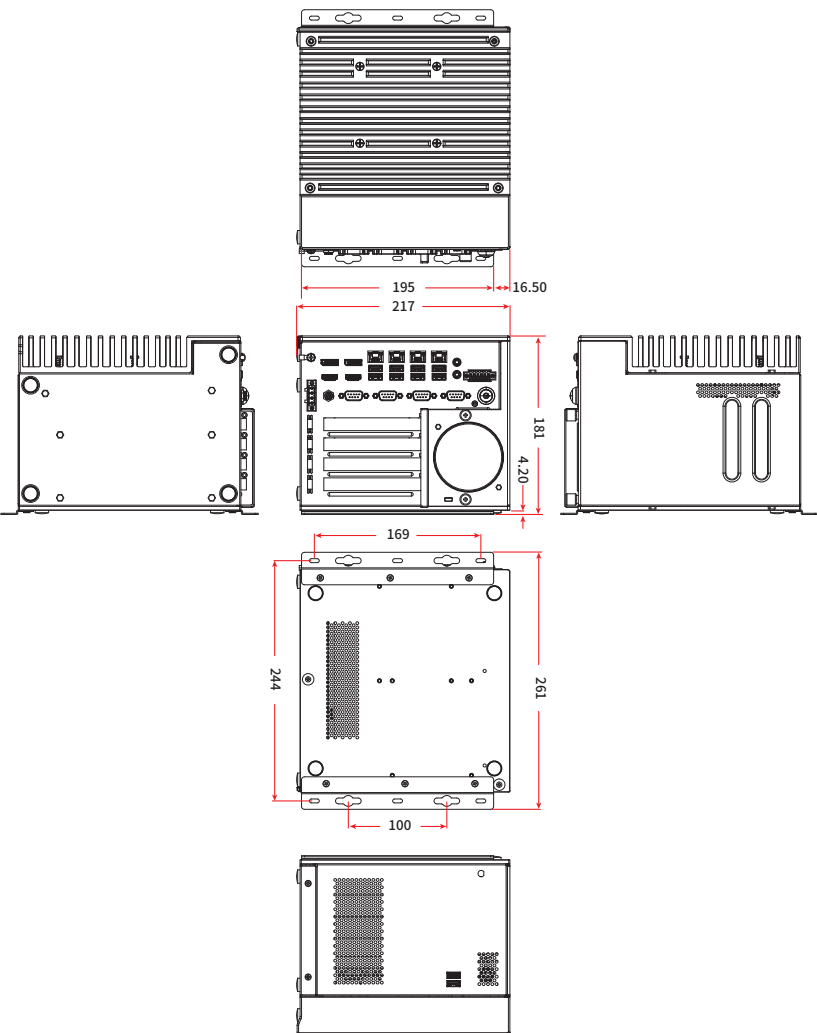
SKU1 (4-Slot)

Unit of measurement: mm



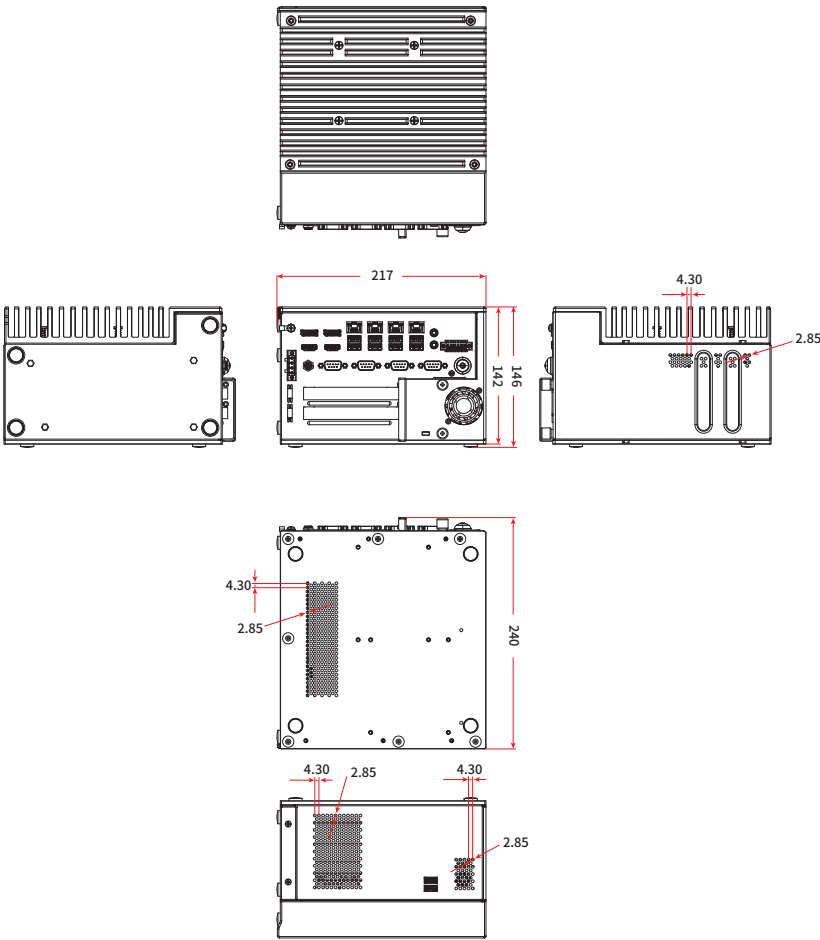
SKU1 (4-Slot, with Wall Mount Bracket)

Unit of measurement: mm



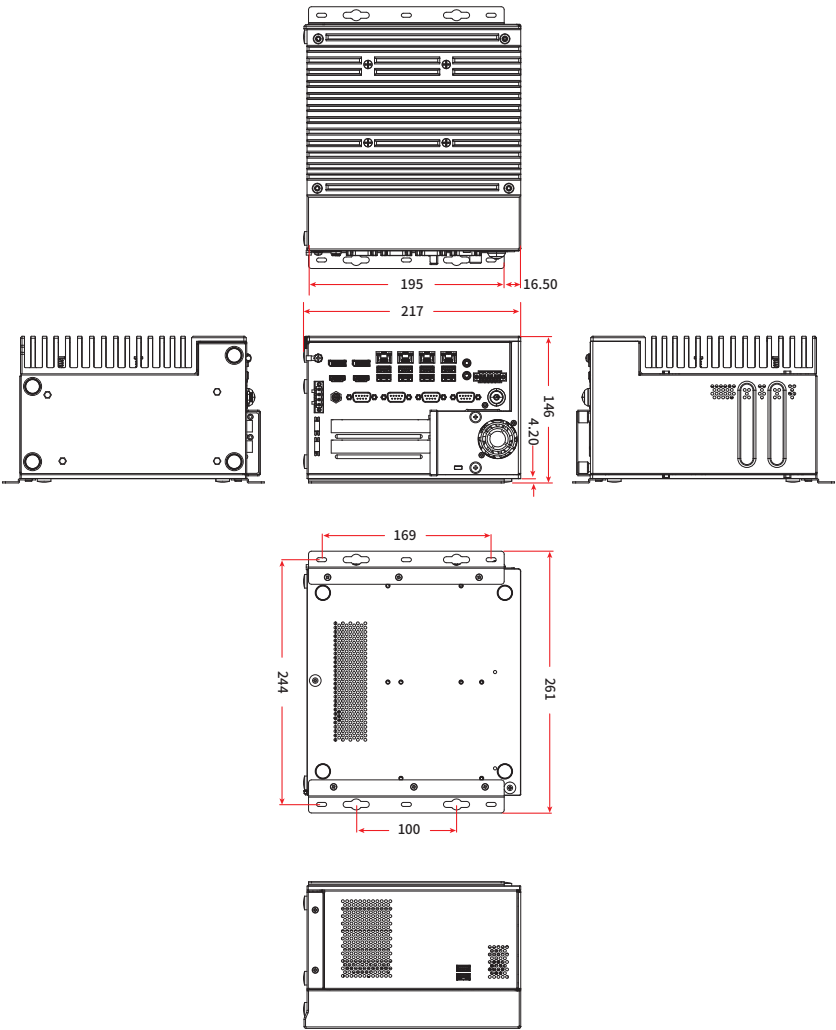
SKU2 (2-Slot)

Unit of measurement: mm



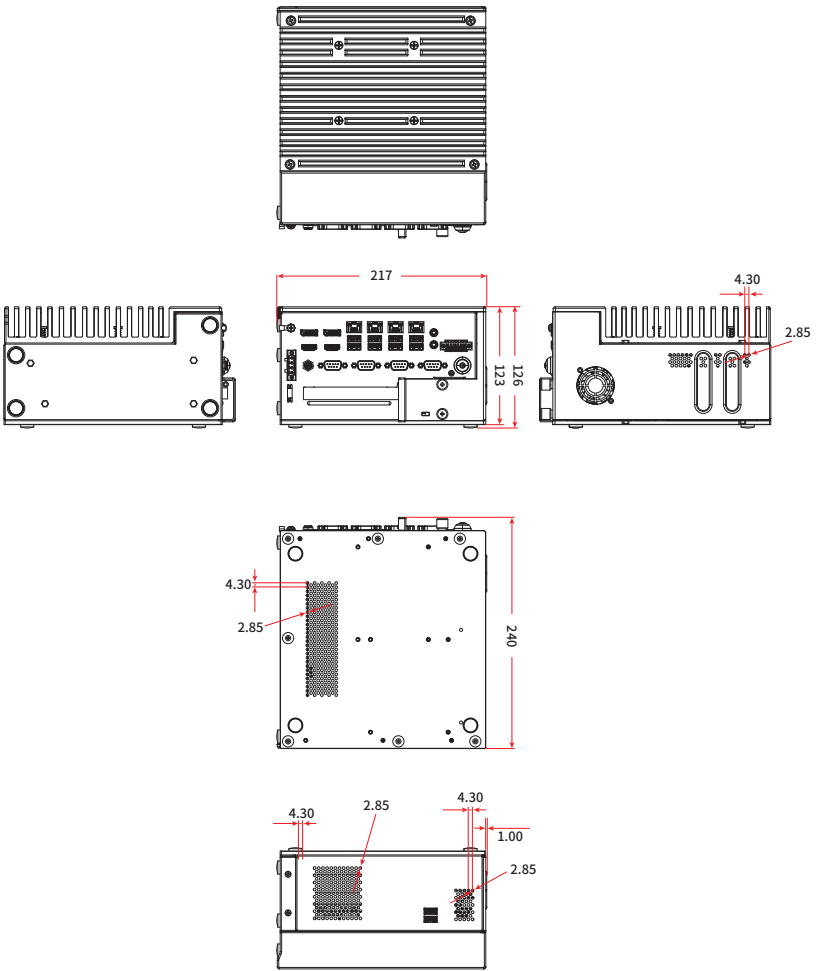
SKU2 (2-Slot, with Wall Mount Bracket)

Unit of measurement: mm



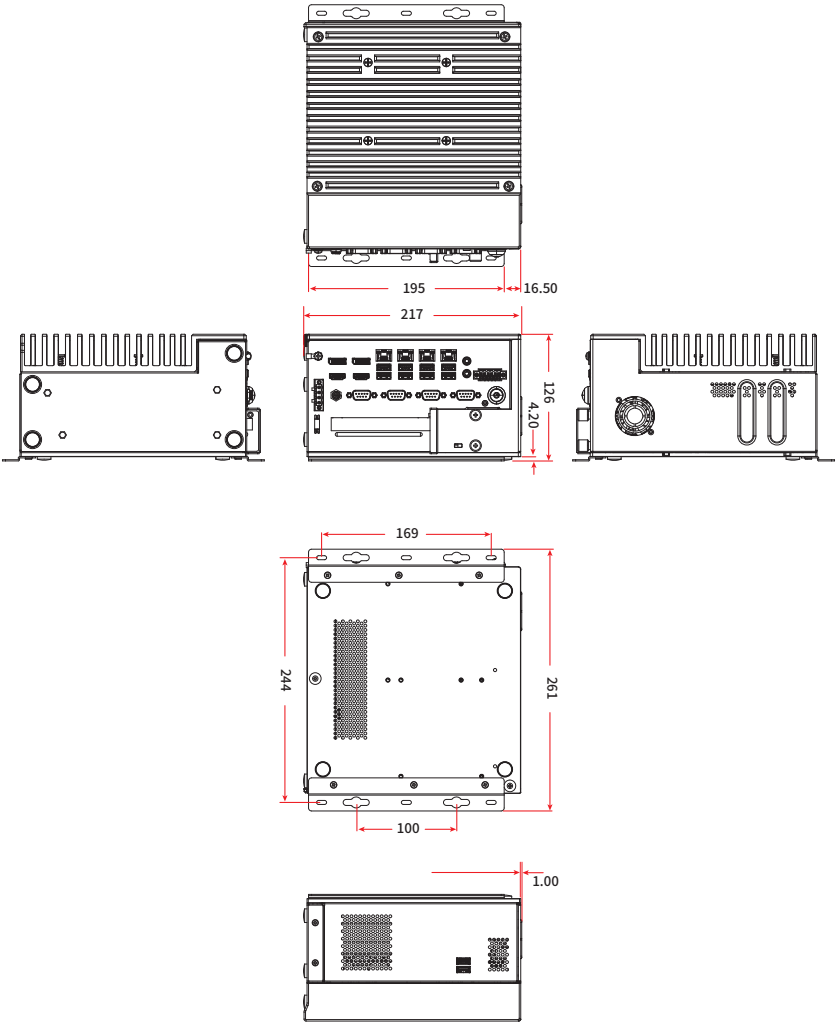
SKU3 (1-Slot)

Unit of measurement: mm



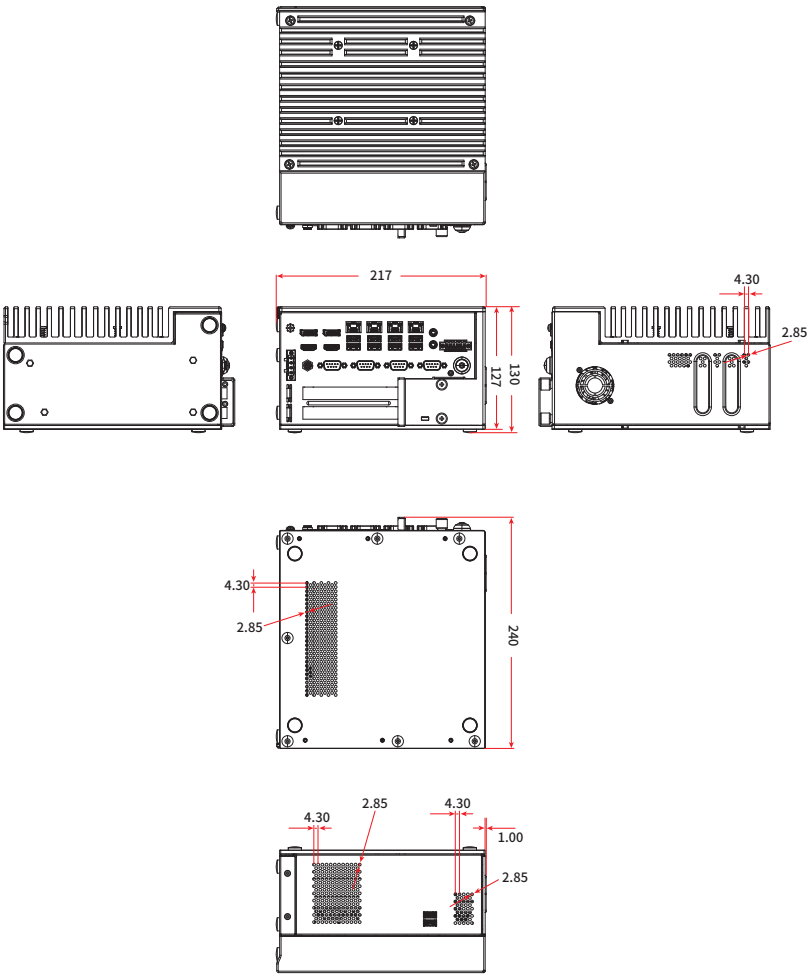
SKU3 (1-Slot, with Wall Mount Bracket)

Unit of measurement: mm



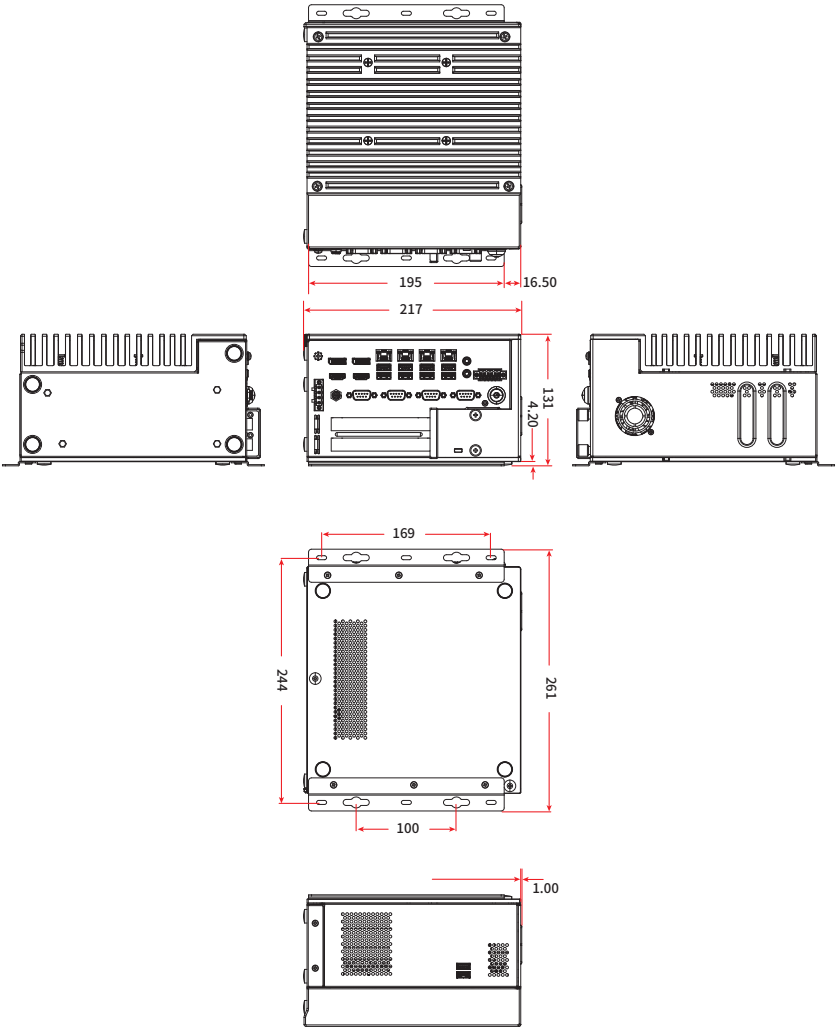
SKU4 (2-Slot)

Unit of measurement: mm



SKU4 (2-Slot, with Wall Mount Bracket)

Unit of measurement: mm



PCIe and PCI Card Dimensions

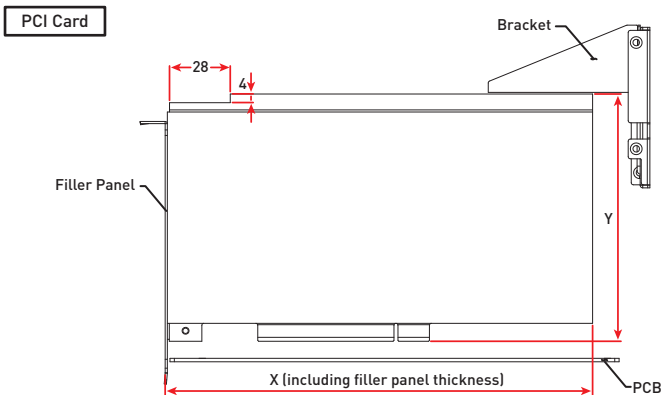
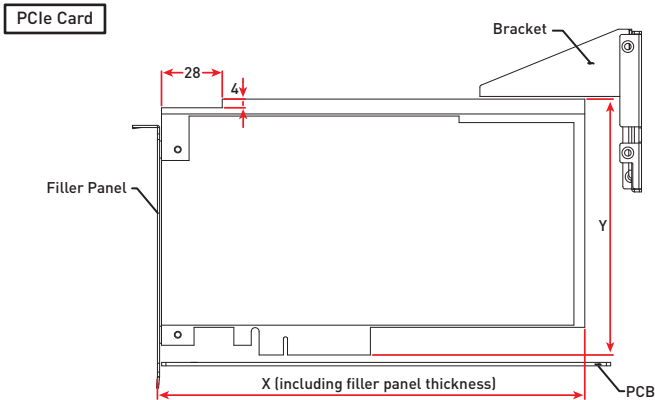
Supported PCIe and PCI Card Dimensions

Card Type		Dimensions	
		PCIe Card	PCI Card
Length (X-axis)	Max	195mm	
	Min	155mm (W/ bracket)	
Height (Y-axis)	Max	118mm (W/ bracket)	112mm (W/ bracket)
	Min	65mm (W/ bracket)	



Important

SKU1-4 support identical PCIe and PCI card dimensions.

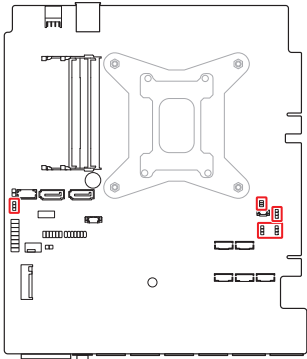


Motherboard Jumpers

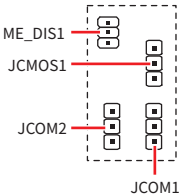







Important

Avoid adjusting jumpers when the system is on; it will damage the motherboard.



JATX1



Jumper Name	Default Setting	Description
JCOM1	 1	COM1 Power Select Jumper
		1-2: 5V Power (Default) 2-3: 12V Power
JCOM2	 1	COM2 Power Select Jumper
		1-2: 5V Power (Default) 2-3: 12V Power
JCMOS1	 1	Clear CMOS Jumper
		1-2: Normal (Default) 2-3: Clear CMOS
JME_DIS1	 1	ME Jumper
		1-2: Normal (Default) 2-3: ME disable
JATX1	 1	AT/ ATX Mode Select Jumper
		1-2: ATX (Default) 2-3: AT

Getting Started



Important

- All information is subject to change without prior notice.
- Before you remove or install any components, make sure the system is not turned on or connected to the power.
- The illustrations are provided for **demonstrative purposes only**. The appearance and internal view of your system may differ based on the model you have purchased.

Necessary Tools



Screwdriver



Pliers



Tweezers



Anti-Static Gloves

Safety Precautions

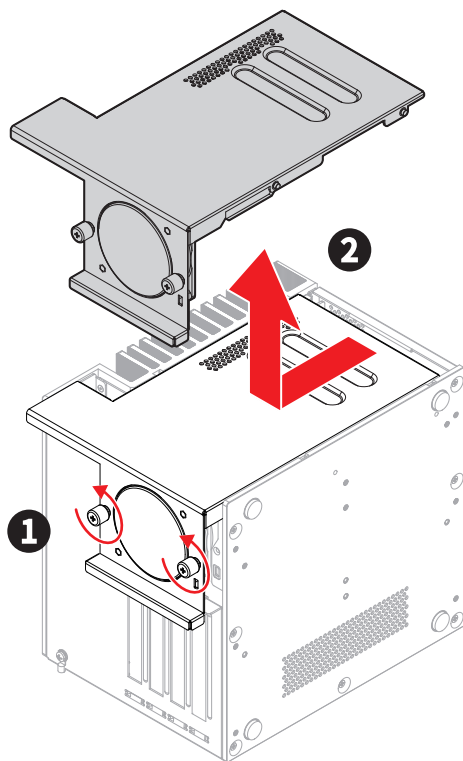
The following precautions should be observed while handling the system:

- Place the system on a flat and stable surface.
- Do not place the system in environments subject to mist, smoke, vibration, excessive dust, salty or greasy air, or other corrosive gases and fumes.
- Do not drop or jolt the system.
- Do not use another power adapter other than the one enclosed with the system.
- Disconnect the power cord before performing any installation procedures on the system.
- Do not perform any maintenance with wet hands.
- Prevent foreign substances, such as water, other liquids or chemicals, from entering the system while performing installation procedures on the system.
- Use a grounded wrist strap before handling system components such as CPU, Memory, HDD, expansion cards, etc.
- Place system components on a grounded antistatic pad or on the bed that came with the components whenever the components are separated from the system.

System Covers

Removing System Top Cover

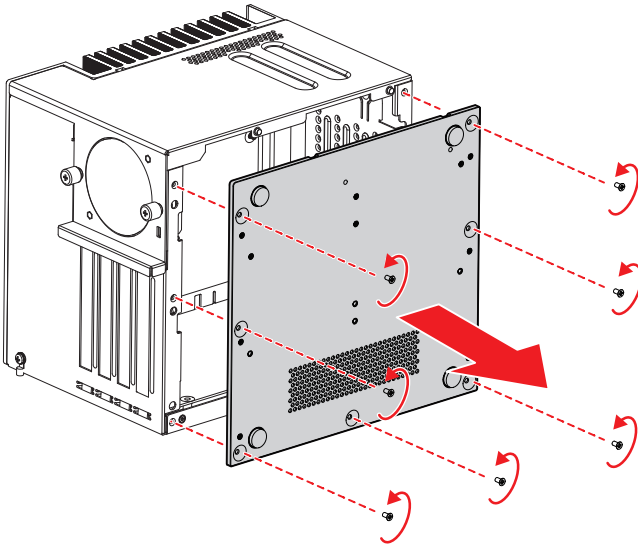
1. Loosen the thumbscrews to release the top cover.
 2. Carefully push forward and lift the top cover to remove it from the system.
- Follow the above procedures in reverse order to install the cover.



Removing System Side Cover

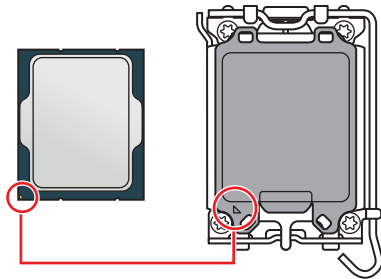
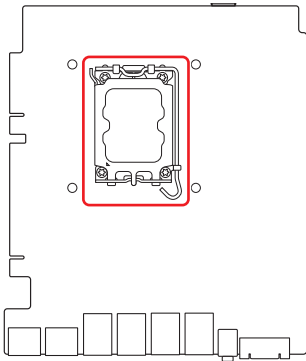
Loosen and completely remove the screws to release the side cover.

- *Follow the above procedures in reverse order to install the side cover.*



CPU & Heatsink

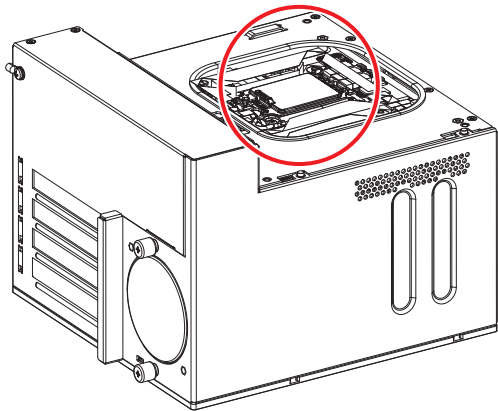
CPU Socket



Introduction to the LGA1700 CPU

The surface of the LGA1700 CPU has four notches and a golden triangle to assist in correctly lining up the CPU for motherboard placement. The golden triangle is the Pin 1 indicator.

Locating CPU Socket

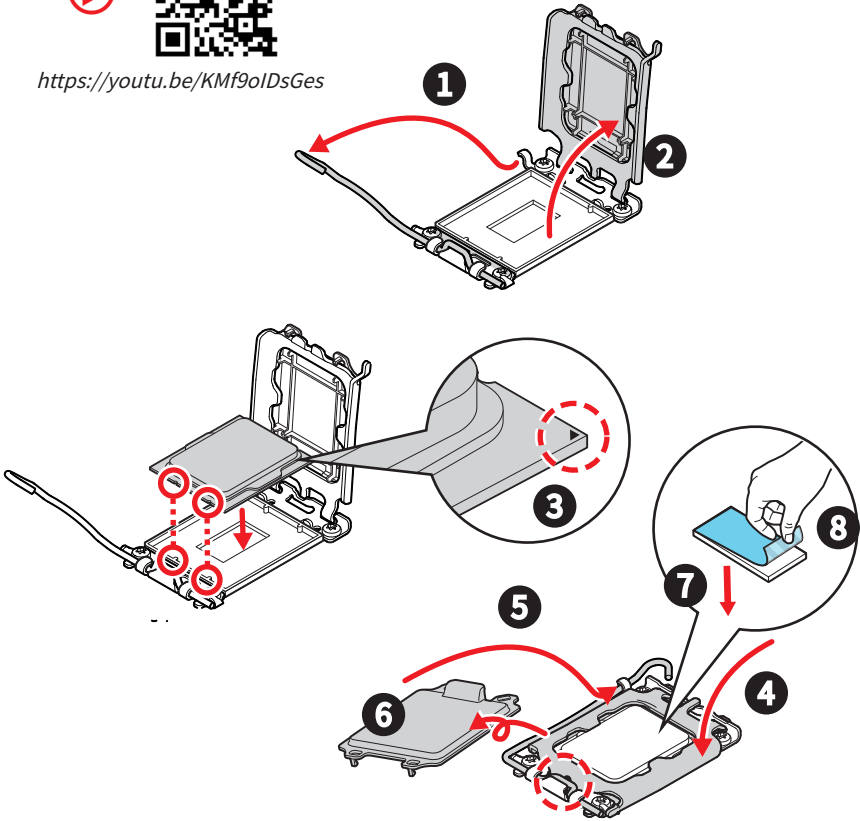


Installing CPU

Use appropriate ground straps, gloves and ESD mats to protect yourself from electrostatic discharge (ESD) while installing the processor.



<https://youtu.be/KMf9oIDsGes>

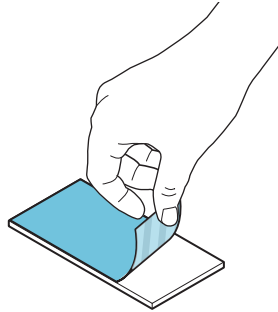
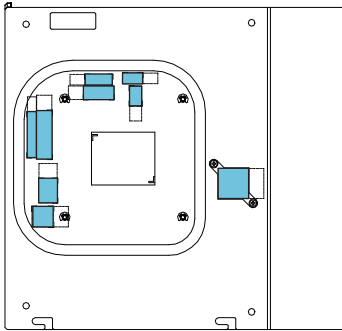


Important

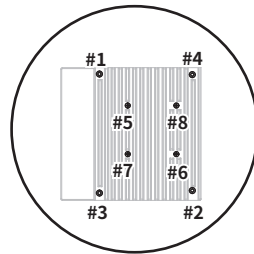
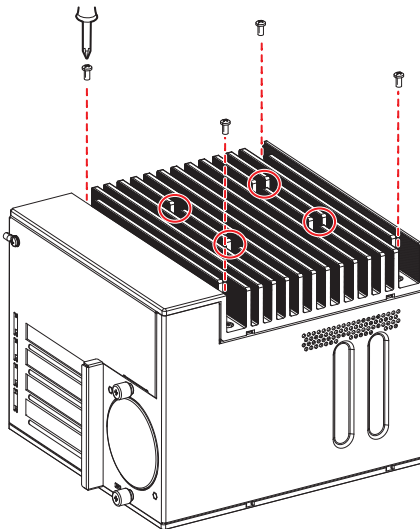
- Always unplug the power cord from the power outlet before installing or removing the CPU.
- Whenever the CPU is not installed, always protect the CPU socket pins by covering the socket with the plastic cap.

Installing the Heatsink

1. Carefully remove the protective films from the thermal pads located on the bottom of the heatsink.



2. Gently lower the heatsink down and place it upon the system.
3. Tighten **M4x8 screws** and the **spring-loaded screws** in **diagonal sequence**. This ensures even pressure distribution and prevents warping.



#1~4: M4x8 Screw

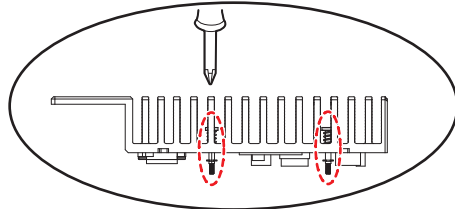
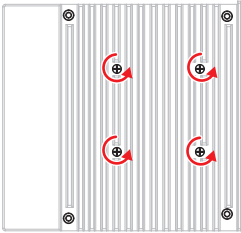
#5~8: Spring-loaded Screw

Important

Confirm that the heatsink has formed a tight seal with the CPU before booting your system.

Removing the Heatsink

1. Lay the system down on a flat, stable surface.
2. Identify and loosen the **spring-loaded screws** in the center of the heatsink.



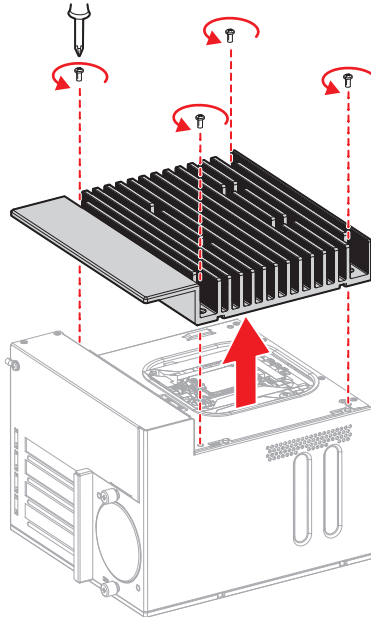
Side View



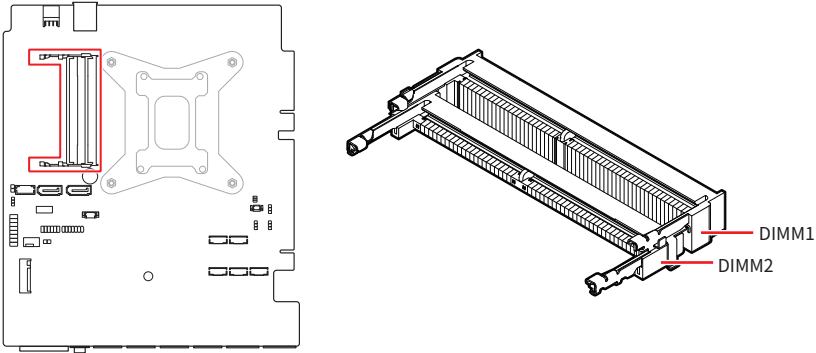
Important

These screws are designed to be loosened but not removed.

3. Find the **M4x8 screws** at the four corners of the heatsink. Loosen and completely remove these screws.
4. Lift the heatsink to remove it from the system.



Memory Module



DDR5 DIMM Thermal Pad Thickness Recommendations

DIMM Type	Single-sided DIMM (chip on one side)	Double-sided DIMM (chips on both sides)
Location (Thermal Pad)		
Closest to Motherboard	2.0mm	1.0mm
In the Middle of Two DIMMs	2.25mm	1.25mm

Installing Memory Module

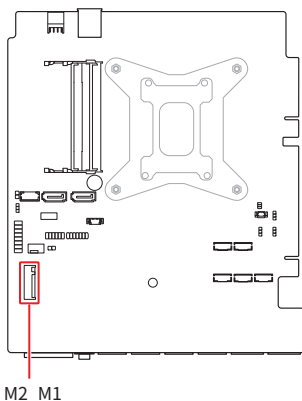
1. Locate the SO-DIMM slot. Align the notch on the DIMM with the key on the slot and insert the DIMM into the slot.
2. Push the DIMM gently downwards until the slot levers click and lock the DIMM in place.
 - To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.

Important

- Always insert memory modules in the **DIMM2** slot first.
- You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.
- To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.

M.2 Slots

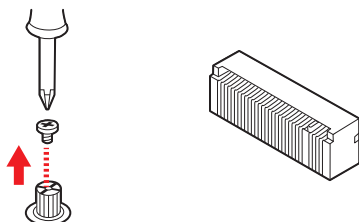
Installing M.2 SSD (2280, M-Key)



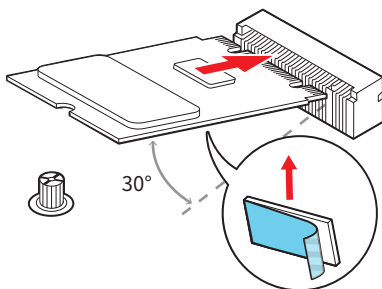
Feature

- Supports PCIe 4.0 x4 & SATA 3.0 signal (signal from PCH)
- Supports B+M Key PCIe x4/ SATA 3.0 module

1. Loosen the M.2 screw from the motherboard.



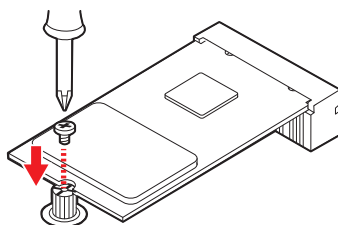
2. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



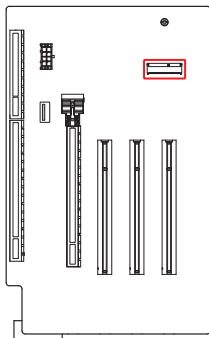
3. Apply a thermal pad to the backside of the M.2 SSD and remove the protective film from it.

- Use a **7.5mm** thick thermal pad for chip-free SSD and a **6.25mm** thick thermal pad for SSD with chips.

4. Secure the M.2 SSD in place with the supplied M.2 screw.



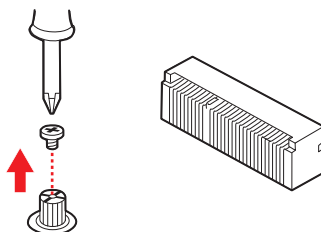
Installing M.2 Wi-Fi Card (2230, E-Key, for SKU1 Only)



Feature

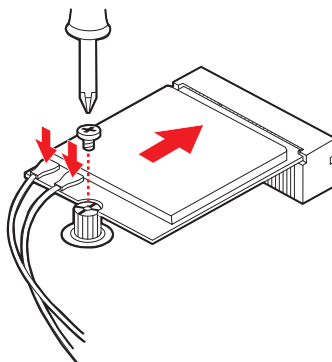
- Supports PCIe 4.0 x1, USB 2.0 signal

1. Loosen the M.2 screw from the motherboard.



2. Insert your M.2 Wi-Fi card into the M.2 slot at a 30-degree angle.

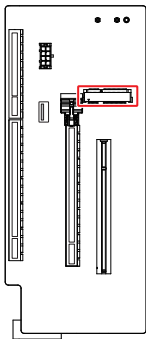
3. Secure the M.2 Wi-Fi card in place with the supplied M.2 screw.



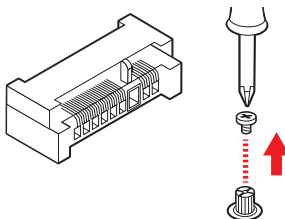
4. Locate the antenna cables and gently connect them to the Wi-Fi card.

Mini-PCle Slot (for SKU2 Only)

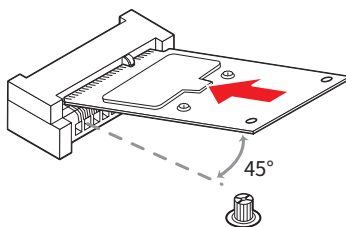
Installing Mini-PCle Card



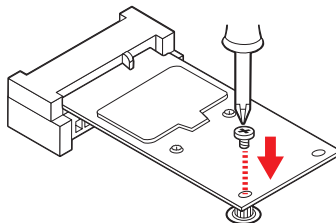
1. Loosen the riser screw from the motherboard.



2. Insert the card into the slot at a 45-degree angle.



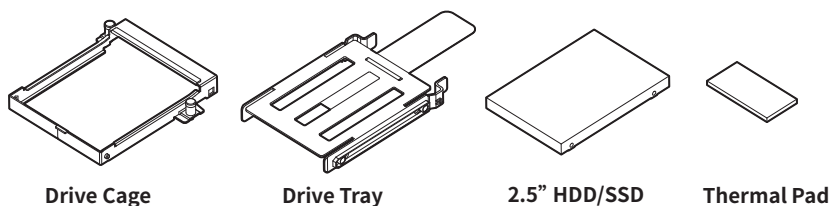
3. Push the card gently downwards and fasten it with the screw.



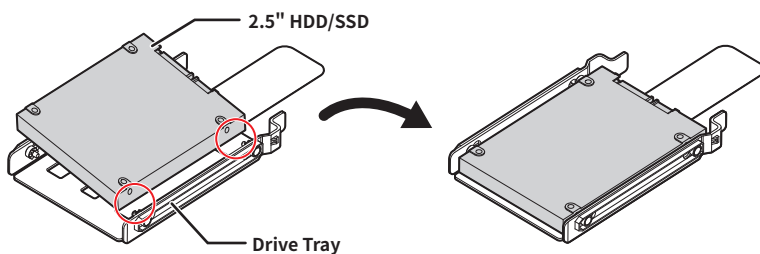
2.5" SSD/HDD Brackets (for SKU1~3)

Installing 2.5" HDD/ SSD (7mm)

1. Identify the components necessary for HDD/SSD installation.



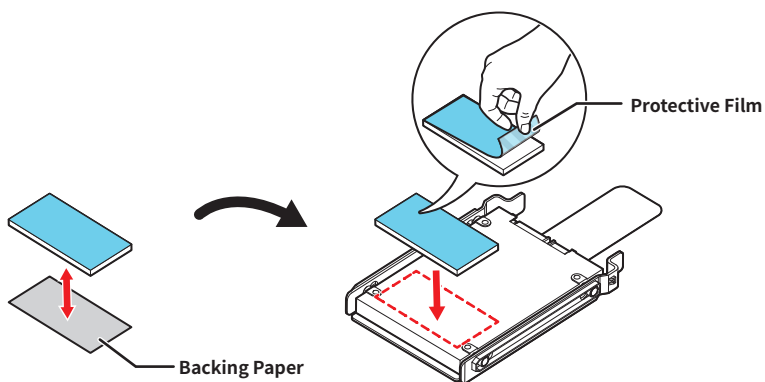
2. Fit the HDD/SSD into the drive tray. Be sure to put the HDD/SSD in the correct orientation.



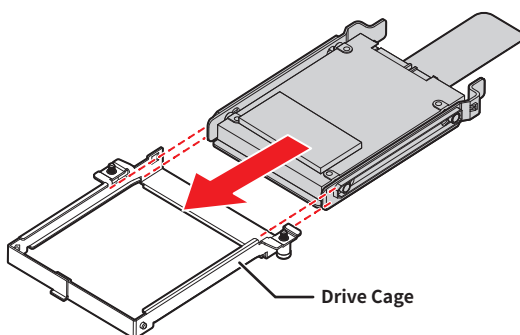
Important

- Before assembly, please make sure the HDD/SSD is compatible with the tray.
 - Please make sure the HDD is properly and completely fixed to the tray.
-

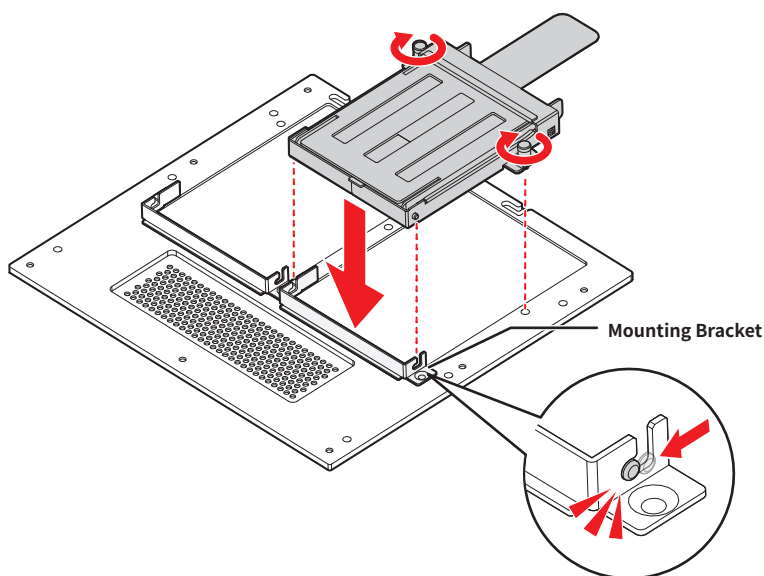
-
3. Remove the thermal pad from the **backing paper**.
 4. Carefully attach it to the HDD/SSD.
 - Check the following illustration for the exact location of the thermal pad.
 5. After the thermal pad is in place, peel off the **protective film**.



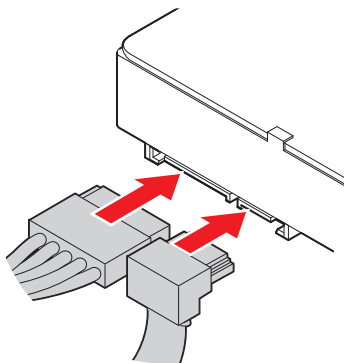
-
6. Slide the drive assembly into the **drive cage**.



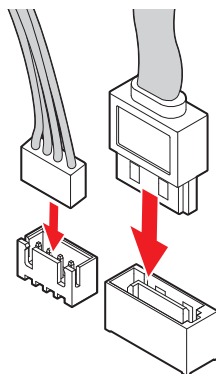
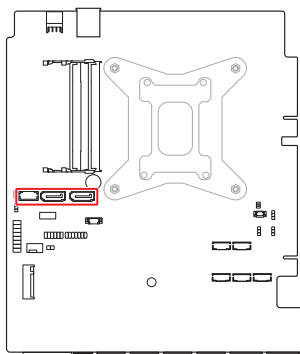
-
7. Remove the system side cover.
(Please refer to the "**Removing System Side Cover**" section.)
 8. Flip over the system side cover and locate the **mounting bracket**.
 9. Align the **standoffs** on the side of the drive cage with the hole on the mounting bracket, then pull the inner rail forwards till it locks into place.
 10. Tighten the screw to secure the **drive set**.
 - Repeat the same procedures to install the other drive set.
 11. Install the side cover back to the system.



-
12. Align the SATA data & power connector and connect to the HDD/SSD.



-
13. Connect the **SATA signal & power connector** to the motherboard to complete the installation.

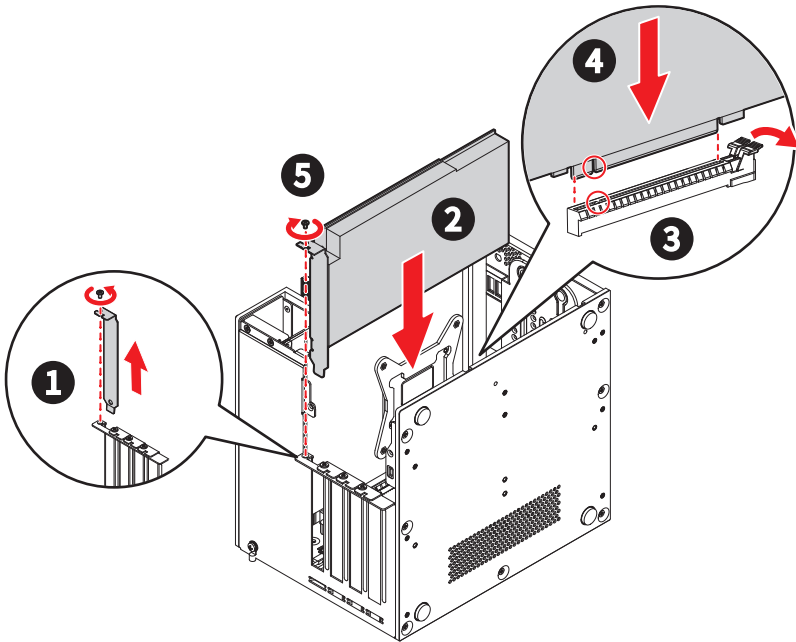


-
- Follow the above procedures in reverse order to replace the HDD/SSD if needed.

PCIe Expansion Card

Installing PCIe Expansion Card

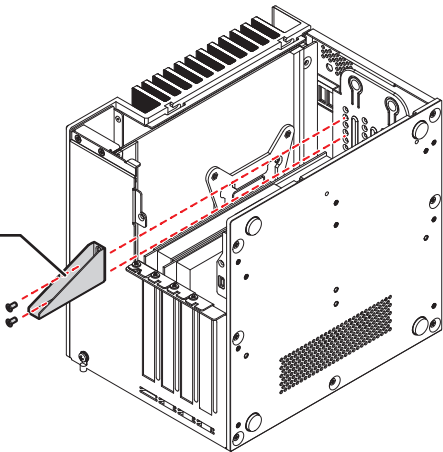
1. Remove the filler panel from the chassis.
 2. Check the card's keyed components for correct alignment with the slot and lower the card into the slot.
 3. Flip the latch outward and insert the card vertically into the slot, ensuring that the off-center notch at the bottom aligns with the slot.
 4. Push the card firmly into the slot until it clicks and the side clips automatically close.
 5. Use the **M3x5 screw** to fix the card in place.
- Repeat the same procedures to install the other PCIe expansion card.



6. Place the bracket above the card and screw it to the back panel as indicated.

Protective Bracket

A protective bracket is provided to cut down on system vibrations that may damage the card.

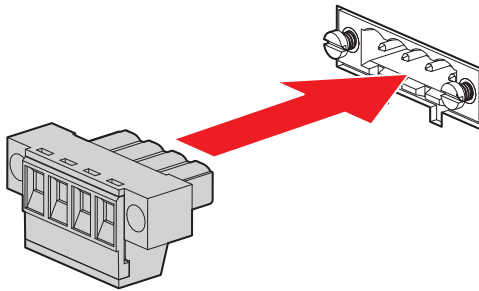


Power Connector

With a redundant power supply solution, users may feed the power through the DC power jack and/or through the 8V~48V Phoenix DC connector.

Connecting DC Receptacle Connector

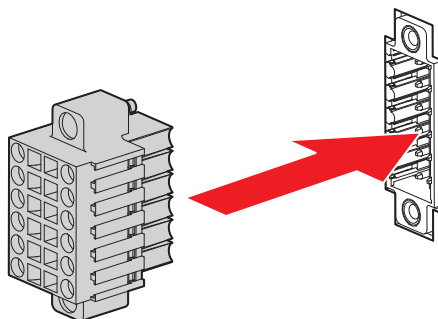
1. Locate the DC power connector on the front panel.
2. Connect a DC receptacle connector to it.



DIO Connector

Connecting DIO Switch Connector

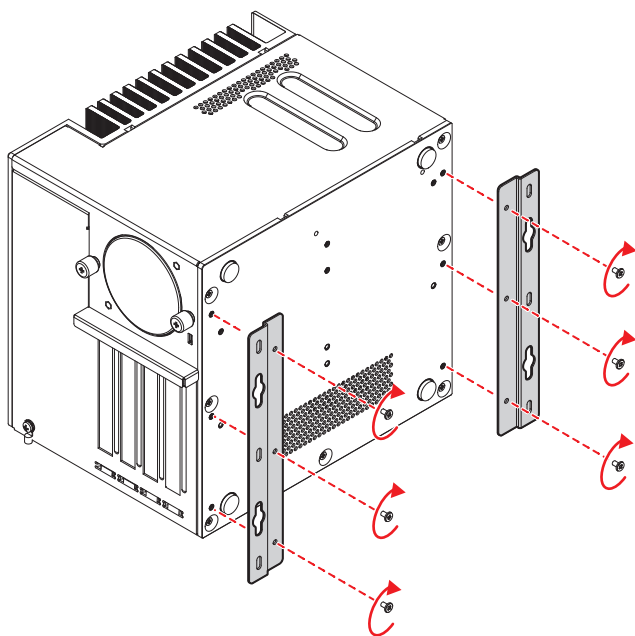
1. Locate the DIO connector on the front panel.
2. Insert the DIO switch connector at a 45-degree angle.



Wall Mount

Installing Wall Mount Bracket

1. Flip over the system and locate the bracket screw holes.
2. Place the brackets along the sides with screw holes aligned.
3. Fasten the screws to fix the brackets.



Screws for Wall Mount Brackets

Screw Type: M3x5 screw

BIOS Setup

This chapter provides information on the BIOS Setup program and allows users to configure the system for optimal use.

Users may need to run the Setup program when:

- An error message appears on the screen at system startup and requests users to run SETUP.
- Users want to change the default settings for customized features.



Important

- Please note that BIOS update assumes technician-level experience.
- As the system BIOS is under continuous update for better system performance, the illustrations in this chapter should be held for reference only.

Entering Setup

Power on the computer and the system will start POST (Power On Self Test) process. When the message below appears on the screen, press or <F2> key to enter Setup, <F11> key to Boot Menu, <F12> key to PXE Boot .

Press or <F2> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system by turning it **OFF** and **On** or pressing the **RESET** button. You may also restart the system by simultaneously pressing <Ctrl>, <Alt>, and <Delete> keys.



Important

The items under each BIOS category described in this chapter are under continuous update for better system performance. Therefore, the description may be slightly different from the latest BIOS and should be held for reference only.

Control Keys

← →	Select Screen
↑ ↓	Select Item
Enter	Select
+ -	Change Value
Esc	Exit
F1	General Help
F7	Previous Values
F9	Optimized Defaults
F10	Save & Reset*
F12	Screenshot capture
<K>	Scroll help area upwards
<M>	Scroll help area downwards

* When you press <F10>, a confirmation window appears and it provides the modification information. Select between **Yes** or **No** to confirm your choice.

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

The main menu lists the setup functions you can make changes to. You can use the **arrow keys** (↑ ↓) to select the item. The on-line description of the highlighted setup function is displayed at the bottom of the screen.

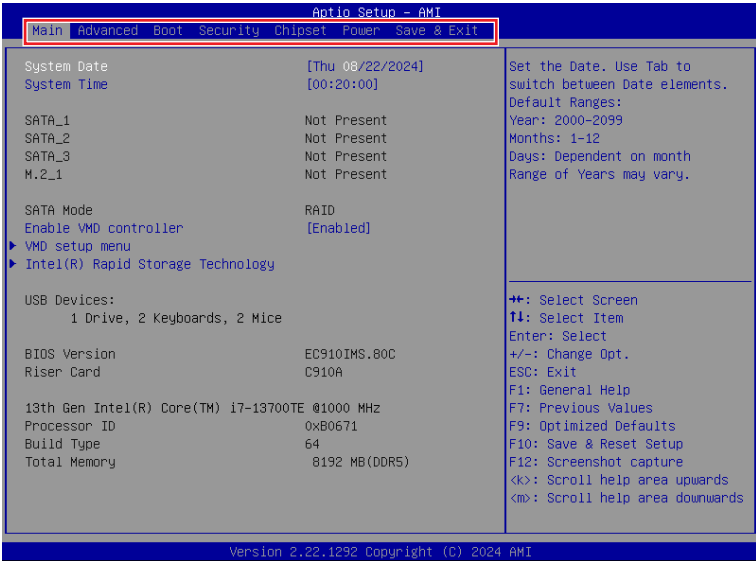
Sub-Menu

If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use **arrow keys** (↑ ↓) to highlight the field and press <Enter> to call up the sub-menu. Then you can use the **control keys** to enter values and move from field to field within a sub-menu. If you want to return to the main menu, just press the <Esc>.

General Help <F1>

The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing <F1>. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press <Esc> to exit the Help screen.

The Menu Bar



- **Main**
Use this menu for basic system configurations, such as time, date, etc.
- **Advanced**
Use this menu to set up the items of special enhanced features.
- **Boot**
Use this menu to specify the priority of boot devices.
- **Security**
Use this menu to set supervisor and user passwords.
- **Chipset**
This menu controls the advanced features of the on-board chipsets.
- **Power**
Use this menu to specify your settings for power management.
- **Save & Exit**
This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

Main

Apilo Setup - AMI

Main Advanced Boot Security Chipset Power Save & Exit

System Date [Thu 08/22/2024]

System Time [00:20:00]

SATA_1 Not Present

SATA_2 Not Present

SATA_3 Not Present

M.2_1 Not Present

SATA Mode RAID

Enable VMD controller [Enabled]

VMD setup menu

Intel(R) Rapid Storage Technology

USB Devices:

1 Drive, 2 Keyboards, 2 Mice

BIOS Version EC910IMS.80C

Riser Card C910A

13th Gen Intel(R) Core(TM) i7-13700TE @1000 MHz

Processor ID 0xB0671

Build Type 64

Total Memory 8192 MB (DDR5)

Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 2000-2099 Months: 1-12 Days: Dependent on month Range of Years may vary.

+-: Select Screen

F1: Select Item

Enter: Select

+/-: Change Opt.

ESC: Exit

F1: General Help

F7: Previous Values

F9: Optimized Defaults

F10: Save & Reset Setup

F12: Screenshot capture

<k>: Scroll help area upwards

<m>: Scroll help area downwards

HDD/SSD Information

- RAID (VMD) Disabled: Display HDD/SSD information as plugging in status.
- RAID (VMD) Enabled: Display "Not Present" only.

*SATA_3 is for M.2 M key (SATA signal)

► **System Date**

This setting allows you to set the system date. Use <Tab> key to switch between date elements.

Format: <Day> <Month> <Date> <Year>.

► **System Time**

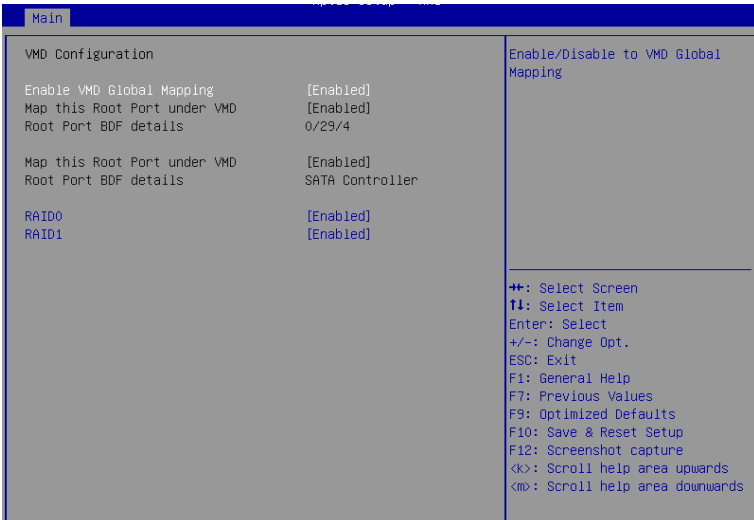
This setting allows you to set the system time. Use <Tab> key to switch between time elements.

Format: <Hour> <Minute> <Second>.

► **Enable VMD controller**

Enables or disables VMD (RAID) controller.

► **VMD Setup Menu (VMD Configuration)**



► **Enabled VMD Global Mapping**

Enables or disables Intel VMD mapping. Intel VMD enables direct control and management of NVMe SSDs from the PCIe bus without additional hardware adapters.

► **Map This Root Port under VMD**

Enables or disables the mapping of the specified PCIe root port under Intel VMD control.

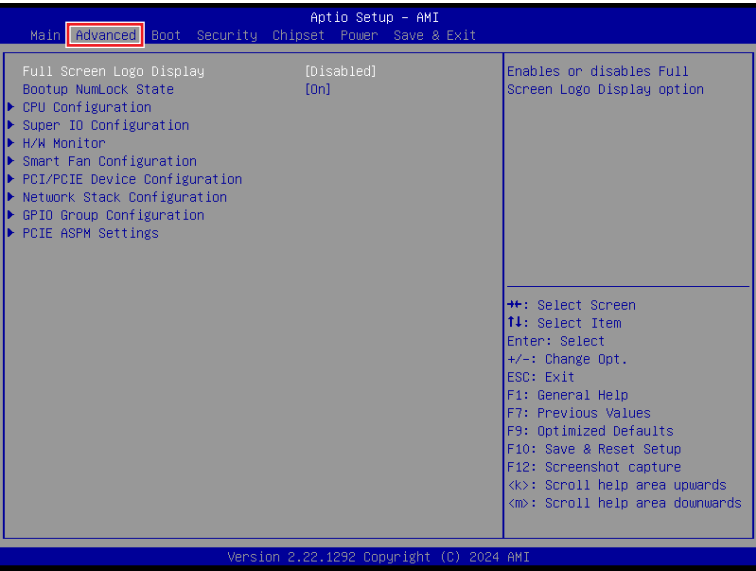
► **RAID0**

Enables or disables RAID 0.

► **RAID1**

Enables or disables RAID 1.

Advanced



► Full Screen Logo Display

This BIOS feature determines if the BIOS should hide the normal POST messages with the motherboard or system manufacturer’ s full-screen logo.

- [Enabled] BIOS will display the full-screen logo during the boot-up sequence, hiding normal POST messages.
- [Disabled] BIOS will display the normal POST messages, instead of the full-screen logo.

Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

► Bootup NumLock State

This setting is to set the state of the Num Lock key on the keyboard when the system is powered on.

- [On] Turn on the Num Lock key when the system is powered on.
- [Off] Allow users to use the arrow keys on the numeric keypad.

► CPU Configuration

Advanced		VT-d capability	
CPU Configuration			
Intel(R) Core(TM) i9-14900T			
Processor ID	0xB0671		
Processor Speed	1100 MHz		
P-core Information			
L1 Data Cache	48 KB × 8		
L1 Instruction Cache	32 KB × 8		
L2 Cache	2048 KB × 8		
L3 Cache	36 MB		
E-core Information			
L1 Data Cache	32 KB × 16		
L1 Instruction Cache	64 KB × 16		
L2 Cache	4096 KB × 4		
L3 Cache	36 MB		
VT-d	[Enabled]		
Intel Virtualization Technology	[Enabled]		
Hyper-Threading	[Enabled]		
Active Performance-cores	[All]		
Active Efficient-cores	[All]		
Intel(R) SpeedStep(tm)	[Enabled]		
Intel(R) Speed Shift Technology	[Enabled]		
		▲ VT-d capability ⇐: Select Screen T1: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <↑>: Scroll help area upwards <↓>: Scroll help area downwards	

► VT-d

Enables or disables Intel VT-D (Intel Virtualization for Directed I/O) technology.

► Intel Virtualization Technology

Enables or disables Intel Virtualization technology.

[Enabled] Enables Intel Virtualization technology and allows a platform to run multiple operating systems in independent partitions. The system can function as multiple systems virtually.

[Disabled] Disables this function.

► Hyper-Threading (HT Function)

Enables or disables Intel Hyper-Threading technology.

The processor uses Hyper-Threading technology to improve utilization of the CPU resources and potentially increasing overall performance by allowing it to handle multiple threads simultaneously. If you disable the function, it will restricts the CPU to operate as a single-threaded processor, with only one logical core per physical core. Please disable this item if your operating system does not support HT Function or unreliability and instability may occur.

► Active Performance-cores

Select the number of active Performance-cores (P-cores).

► Active Efficient-cores

Select the number of active Efficient-cores (E-cores).

► **Intel (R) SpeedStep (TM)**

Enhanced Intel SpeedStep® Technology enables the OS to control and activate performance states (P-States) of the processor.

[Enabled] When enabled, Intel SpeedStep® technology is activated.
This technology allows the processor to manage its power consumption via performance state (P-State) transitions.

[Disabled] Disables this function

► **Intel (R) Speed Shift Technology**

Intel® Speed Shift Technology is an energy-efficient method that allows frequency control by hardware rather than the OS.

[Enabled] When enabled, Intel® Speed Shift Technology is activated.
The technology enables the management of processor power consumption via hardware performance state (P-State) transitions.

[Disabled] Disable this function.

► **C States**

This setting controls the C-States (CPU Power states).

[Enabled] Detects the idle state of system and reduce CPU power consumption accordingly.

[Disabled] Disable this function.

► Super IO Configuration

Advanced	
Super IO Configuration	
Serial Port 1	[Enabled]
Device Settings	IO=3F8h; IRQ=4;
Change Settings	[Auto]
Mode Select	[RS232]
Serial Port 2	[Enabled]
Device Settings	IO=2F8h; IRQ=3;
Change Settings	[Auto]
Mode Select	[RS232]
Serial Port 3	[Enabled]
Device Settings	IO=3E8h; IRQ=7;
Change Settings	[Auto]
Serial Port 4	[Enabled]
Device Settings	IO=2E8h; IRQ=7;
Change Settings	[Auto]
FIFO Mode	[128-byte]
Watch Dog Timer	[Disabled]
Enable or Disable Serial Port (COM) ++: Select Screen T1: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards	

► Serial Port 1/ 2/ 3/ 4

This setting enables or disables the specified serial port.

» Device Settings

This setting shows the address & IRQ of the specified serial port or parallel port.

» Change Settings

This setting is used to change the address & IRQ settings of the specified serial port or parallel port.

» Mode Select

Select an operation mode for Serial Port 1/ 2/ 3/ 4.

► FIFO Mode

This setting controls the FIFO (First In First Out) data transfer mode.

► Watch Dog Timer

You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

► **H/W Monitor (PC Health Status)**

These items display the current status of all monitored hardware devices/ components such as voltages, temperatures and all fans' speeds.

Advanced	
PC Health Status	Thermal Shutdown
Thermal Shutdown	[Disabled]
CPU temperature	: +36 °C
System temperature	: +33 °C
SYSFAN	: 942 RPM
VCC_CORE	: +0.768 V
VCC3	: +3.312 V
VCC5	: +5.003 V
+12V	: +12.056 V
VCC3V	: +3.312 V
VS83V	: +3.296 V
VS85V	: +4.896 V
VBAT	: +3.088 V
++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards	

► **Thermal Shutdown**

This setting determines the behavior of the system when the CPU temperature reaches a predefined threshold.

- [Enabled] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.
- [Disabled] Disable this function.

► **Smart Fan Configuration**

Advanced		
Configuration Smart FAN		Disabled/Enabled Smart FAN Function
SYSFAN	[55 °C]	
Min. Speed (%)	[0.0%]	

► **SYSFAN**

This setting enables or disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the CPU/system fan speed automatically depending on the current CPU/system temperature, avoiding the overheating to damage your system. The following item will display when **SYSFAN1** is enabled.

» **Min. Speed (%)**

The beginning speed of the System fan.

► **PCI/PCIE Device Configuration**

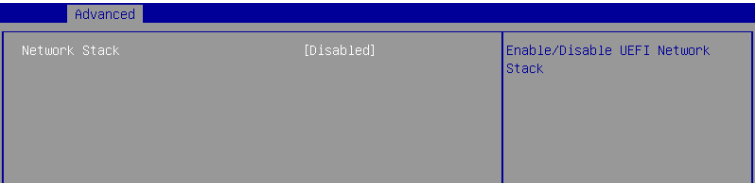
Advanced		
Audio Controller	[Enabled]	Control Detection of the Audio Controller. Disabled = Audio Controller will be unconditionally disabled. Enabled = Audio Controller will be unconditionally Enabled.

► **Audio Controller**

This setting enables or disables the detection of the onboard audio controller.

► **Network Stack Configuration**

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS.



► **Network Stack**

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS. The following items will display when **Network Stak** is enabled.

» **IPv4 PXE Support**

Enables or disables IPv4 PXE boot support.

» **IPv4 HTTP Support**

Enables or disables Ipv4 HTTP Support.

» **IPv6 PXE Support**

Enables or disables Ipv6 PXE Support.

» **IPv6 HTTP Support**

Enables or disables Ipv6 HTTP Support.

» **PXE boot wait time**

Use this option to specify the wait time to press the ESC key to abort the PXE boot. Press “+” or “-” on your keyboard to change the value. The default setting is 0.

» **Media detect count**

Use this option to specify the number of times media will be checked. Press “+” or “-” on your keyboard to change the value. The default setting is 1.

► **GPIO Group Configuration**

Advanced	
GPIO Group Configuration	
GP00	[Low]
GP01	[Low]
GP02	[Low]
GP03	[Low]
Set GP00 to output High/Low	
GPIO Status	
GP00	: 0
GP01	: 0
GP02	: 0
GP03	: 0
GPI Status	
GPI0	: 0
GPI1	: 0
GPI2	: 0
GPI3	: 0
++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards	

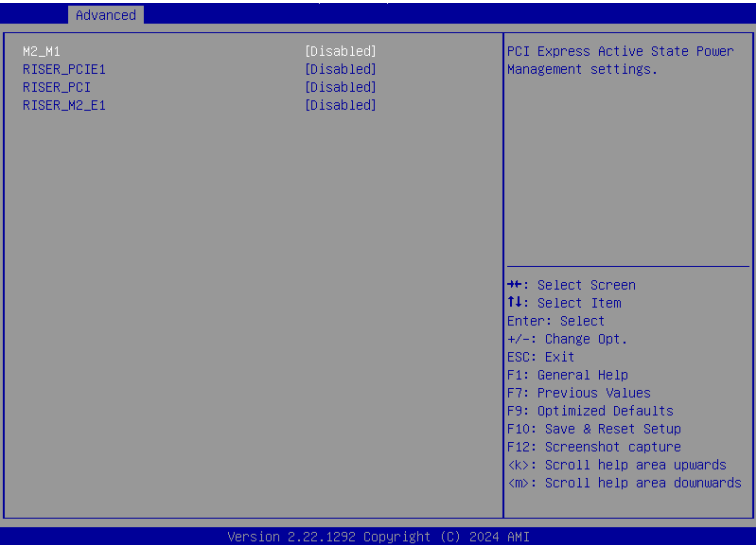
Version 2.22.1232 Copyright (C) 2024 AMI

► **GP00 ~ GP03**

These settings control the operation mode of the specified GPIO.

► **PCIE ASPM settings**

This menu provide settings for PCIe ASPM (Active State Power Management) level for different installed devices.



► **M2_M1/ RISER_PCIE1/ RISER_PCI/ RISER_M2_E1**

Sets PCI Express ASPM (Active State Power Management) state for power saving.

Lanes form PCH (RISER_PCI/ RISER_M2_E1):

- [Disabled] Disable this function.
- [L1] Higher latency, lower power “standby” state.
- [Auto] Set the best state supported by the system.

Lanes form SA (M2_M1/ RISER_PCIE1):

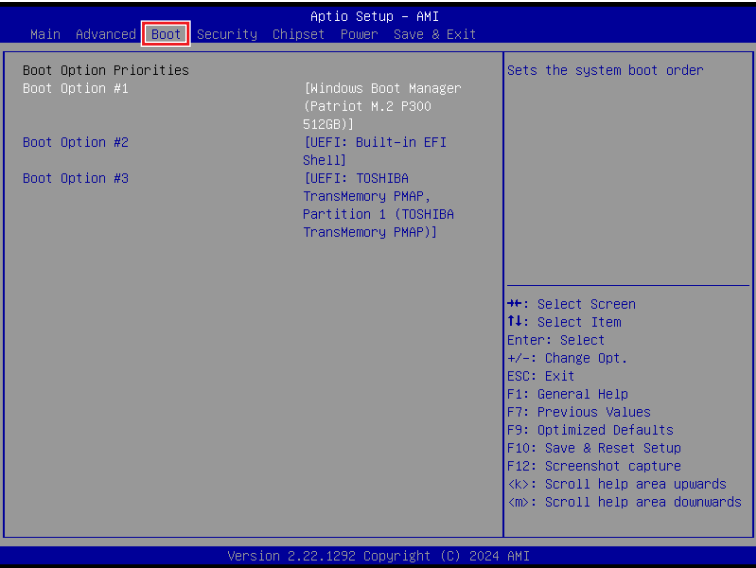
- [L0sL1] Activate both L0s and L1 support.
- [L0s] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.



Important

Expansion slots availability varies by SKU. Please refer to the **Specifications** and **Expansion Slots** sections for information.

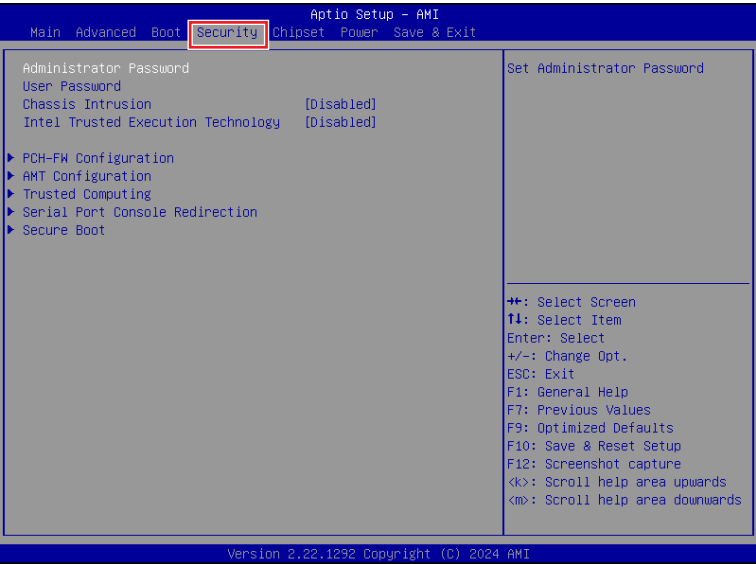
Boot



► **Boot Option #1-3**

This setting allows users to set the sequence of boot devices where BIOS attempts to load the disk operating system.

Security



► **Administrator Password**

Administrator Password controls access to the BIOS Setup utility.

► **User Password**

User Password controls access to the system at boot and to the BIOS Setup utility.

► **Chassis Intrusion**

Enables or disables recording messages while the chassis is opened. This function is ready for the chassis equips a chassis intrusion jumper (switch).

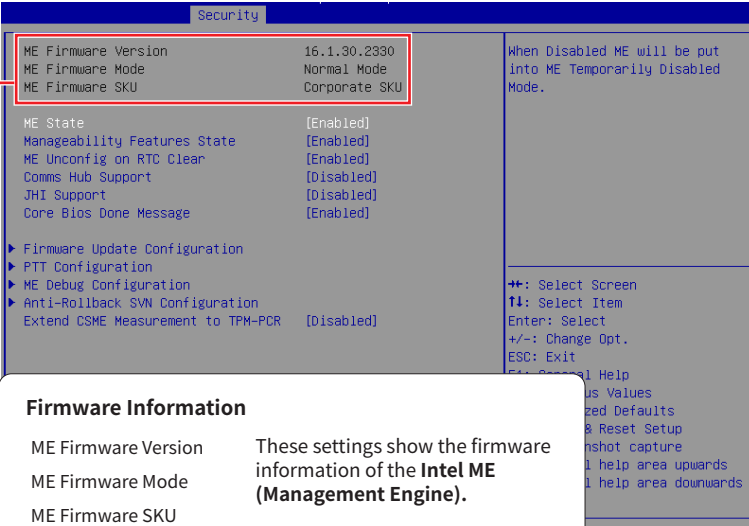
- [Enabled] Once the chassis is **opened**, the system will record and issue a warning message. A beep sound will be emitted before this function is reset.
- [Disabled] Once the chassis is **closed**, the system will record and issue a warning message.
- [Reset] Clear the warning message. After clearing the message, please return to Enabled or Disabled.

► **Intel Trusted Execution Technology**

Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware-based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

► PCH-FW Configuration

This menu allows you to configure settings related to the PCH firmware.



The screenshot shows the BIOS Security menu. A red box highlights the 'Firmware Information' section, which includes the following settings:

Setting	Value
ME Firmware Version	16.1.30.2930
ME Firmware Mode	Normal Mode
ME Firmware SKU	Corporate SKU

Below this section, other settings are listed:

- ME State [Enabled]
- Manageability Features State [Enabled]
- ME Unconfig on RTC Clear [Enabled]
- Comms Hub Support [Disabled]
- JHI Support [Disabled]
- Core BIOS Done Message [Enabled]

At the bottom, there are expandable sections:

- Firmware Update Configuration
- PTT Configuration
- ME Debug Configuration
- Anti-Rollback SVN Configuration
- Extend CSME Measurement to TPM-PCR [Disabled]

On the right side of the screen, there is a list of navigation keys:

- ++: Select Screen
- f1: Select Item
- Enter: Select
- +/-: Change Opt.
- ESC: Exit
- Star: General Help
- us Values
- ized Defaults
- & Reset Setup
- shot capture
- help area upwards
- help area downwards

Firmware Information

ME Firmware Version These settings show the firmware information of the **Intel ME (Management Engine)**.

ME Firmware Mode

ME Firmware SKU

► ME State

This menu controls the Intel® Management Engine State (ME state) parameters, which provides various management and security capabilities. The following items will display when **ME State** is enabled.

» Manageability Feature State

Enables or disables Manageability Feature State. Enabling this item for remote management capabilities.

» ME Unconfig on RTC Clear

Enables or disables ME Unconfig on RTC Clear. Enabling this item resets the ME configuration to its default state, removing any customizations or settings applied.

» Comms Hub Support

Enables or disables the communications hub support.

» JHI Support

Enables or disables JHI Support. JHI stands for Intel® Dynamic Application Loader Host Interface Service (Intel® DAL HIS) and is the engineering name for this feature. Enabling JHI Support in the BIOS settings allows the system to utilize this interface for communication between trusted applications and host-based applications.

» Core BIOS Done Message

Enables or disables Core BIOS Done Message sent to ME.

► Extend CSME Measurement to TPM-PCR

This setting enables or disables Intel® Converged Security and Management Engine (CSME) measurement extend to TPM-PCR.

► **Firmware Update Configuration**

This menu will display when **ME State** is enabled.

Security		
Me FW Image Re-Flash	[Disabled]	Enable/Disable Me FW Image Re-Flash function.
Local FW Update	[Enabled]	

» **ME FW Image Re-Flash**

Enables or disables the ME Firmware Image Re-flashing.

» **Local FW Update**

Enables or disables the capability to perform a firmware update.

► **PTT Configuration**

Intel® Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows. This menu will display when **ME State** is enabled.

Security		
PTT Capability / State	1 / 0	Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.
TPM Device Selection	[dTPM]	

» **TPM Device Selection**

Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[PTT] Enables PTT in SkuMgr.

[dTPM] Disables PTT in SkuMgr. **Warning! PTT/ dTPM will be disabled and all data saved on it will be lost.**

► **ME Debug Configuration**

This menu allows you to configure debug-related options for the Intel® Management Engine (ME). This menu will display when **ME State** is enabled.

Security		
HECI Timeouts	[Enabled]	Enable/Disable HECI Send/Receive Timeouts.
Force ME DID Init Status	[Disabled]	
CPU Replaced Polling Disable	[Disabled]	
HECI Message check Disable	[Disabled]	
MBP HOB Skip	[Disabled]	
HECI2 Interface Communication	[Disabled]	
KT Device	[Enabled]	
End Of Post Message	[Send in DXE]	
DOI3 Setting for HECI Disable	[Disabled]	
MCTP Broadcast Cycle	[Disabled]	

» **HECI Timeouts**

This setting enables/ disables the HECI (Host Embedded Controller Interface) send/ receive timeouts.

» **Force ME DID Init Status**

Forces the ME Device ID (DID) initialization status value.

» **CPU Replaced Polling Disable**

Setting this option disables the CPU replacement polling loop.

» **HECI Message Check Disable**

This setting disables message check for BIOS boot path when sending messages.

» **MBP HOB Skip**

Setting this option will skip ME's Memory-Based Protection (MBP) HOB region.

» **HECI2 Interface Communication**

This setting Adds/ Removes HECI2 device from PCI space.

» **KT Device**

Enables or disables Key Transfer (KT) Device.

» **End of Post Message**

Enables or disables End of Post Message sent to ME.

» **DOI3 Setting for HECI Disable**

Setting this option disables setting DOI3 bit for all HECI devices.

» **MCTP Broadcast Cycle**

Enables or disables Management Component Transport Protocol (MCTP) Broadcast Cycle.

► **Anti-Rollback SVN Configuration**

Security		
Minimal Allowed Anti-Rollback SVN	0	When enabled, hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution
Executing Anti-Rollback SVN	4	
Automatic HW-Enforced Anti-Rollback SVN	[Disabled]	
Set HW-Enforced Anti-Rollback for Current SVN	[Disabled]	

» **Automatic HW-Enforced Anti-Rollback SVN**

Setting this item enables will automatically activate the hardware-enforced anti-rollback protection based on the Secure Version Number (SVN). Once enabled, the hardware will enforce that only firmware updates with an SVN equal to or higher than the current SVN can be installed.

» **Set HW-Enforced Anti-Rollback for Current SVN**

Enable HW ERB mechanism for current ARB SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent. This item will display when **Automatic HW-Enforced Anti-Rollback SVN** is enabled.

► **AMT Configuration**

Intel® Active Management Technology (Intel® AMT) is hardware-based technology for remotely managing and securing PCs out-of-band (OOB).



► **USB Provisioning of AMT**

Enables or disables the ability to provision AMT using a USB device.

► **Mac PASS Through**

Enables or disables the ability of AMT to pass through network traffic without altering the original MAC (Media Access Control) addresses of the network interface. Enabling Mac PASS Through ensures that the network traffic appears to originate from the original MAC address of the system.

► **Activate Remote Assistance Process**

Enables or disables remote assistance sessions to be initiated on systems with AMT support.

► **Unconfigure ME**

Enables or disables the Unconfigure ME.

► ASF Configuration

Security		
PET Progress	[Enabled]	Enable/Disable PET Events Progress to receive PET Events.
WatchDog	[Disabled]	
OS Timer	0	
BIOS Timer	0	
ASF Sensors Table	[Disabled]	

» PET Progress

Enables or disable the this item to receive PET Events.

» WatchDog

Enables or disable the watchdog timer.

» OS Timer

This item displays OS Timer.

» BIOS Timer

This item displays BIOS Timer.

» ASF Sensor Table

Enables or disable the Alert Standard Format (ASF) Sensor Table.

► Secure Erase Configuration

Security		
Secure Erase mode	[Simulated]	Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD. *** If SATA device is used, OEM could use SECURE_ERASE_HOOK_PROTOCOL to remove SATA power to skip G3 cycle. ***
Force Secure Erase	[Disabled]	

» Secure Erase Mode

This setting change Secure Erase module behavior.

[Simulated] Performs SE flow without erasing SSD.

[Real] Erase SSD.

» Force Secure Erase

Enables or disables to force Secure Erase on next boot.

► MEBx (Management Engine BIOS Extension)

Security	
Intel(R) ME Password	MEBx Login

► **One Click Recovery (OCR) Configuration**

Security		
OCR Https Boot	[Enabled]	Enable/Disable One Click Recovery Https Boot
OCR PBA Boot	[Enabled]	
OCR Windows Recovery Boot	[Enabled]	
OCR Disable Secure Boot	[Enabled]	

» **OCR Https Boot**

Enables or disables the use of HTTPS (Hypertext Transfer Protocol Secure) for the OCR boot process. When enabled, the OCR process will utilize HTTPS for enhanced security during the process of booting up the system.

» **OCR PBA Boot**

Enables or disables the PBA (Pre-Boot Authentication) for the OCR boot process. When enabled, users may be required to authenticate themselves before the OCR boot process begins, adding an extra layer of security.

» **OCR Windows Recovery Boot**

Enables or disables the Windows Recovery Boot for the OCR boot process. When enabled, the OCR boot process will prioritize Windows recovery options, allowing users to restore the system to a previous Windows state or initiate other Windows-specific recovery procedures.

» **OCR Disable Secure Boot**

Enabling this item will disable Secure Boot during the OCR process.

► **Remote Platform Erase Configuration**

Intel® Remote Platform Erase (Intel® RPE) Configuration provides settings for the remote erasure of the platform information or specific storage devices connected to the system.

Security		
Enable Remote Platform Erase Feature	[Enabled]	Enable/Disable Remote Platform Erase Feature
SSD Erase Mode	[Simulated]	

» **Enable Remote Platform Erase Feature**

Enables or disables the ability to initiate the remote erasure process for the system or selected storage devices.

» **SSD Erase Mode**

This setting determines the erase mode to be used specifically for solid-state drives (SSDs) during the erasure process.

[Simulated] **Simulates** the erasure process **without permanently** deleting SSD data to estimate the time and resources required.

[Real] **Actual** erasure process that **permanently** deletes the SSD data to ensure that the data is no longer accessible.

► Trusted Computing

Security		
TPM 2.0 Device Found		Enables or Disables BIOS support for security device. O.S. will not show Security Device, TCG EFI protocol and INT1A interface will not be available.
Firmware Version:	15.23	
Vendor:	IFX	
Security Device Support	[Enable]	
Active PCR banks	SHA256	
Available PCR banks	SHA256,SHA384	
SHA256 PCR Bank	[Enabled]	
SHA384 PCR Bank	[Disabled]	
Pending operation	[None]	++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards
Platform Hierarchy	[Enabled]	
Storage Hierarchy	[Enabled]	
Endorsement Hierarchy	[Enabled]	
Physical Presence Spec Version	[1,3]	
TPM 2.0 InterfaceType	[TIS]	
PH Randomization	[Enabled]	
Device Select	[TPM 2.0]	

► Security Device Support

This item enables or disables BIOS support for security device. When set to [Disable], the OS will not show security device.

► SHA256/ SHA384 PCR Bank

These settings enables or disables the SHA256 PCR Bank and SHA384 PCR Bank.

► Pending Operation

When **Security Device Support** is set to [Enable], **Pending Operation** will appear. It is advised that users should routinely back up their TPM secured data.

[TPM Clear] Clear all data secured by TPM.

[None] Discard the selection.

► Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

These settings enables or disables the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

► Physical Presence Spec Version

This settings show the Physical Presence Spec Version.

► TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

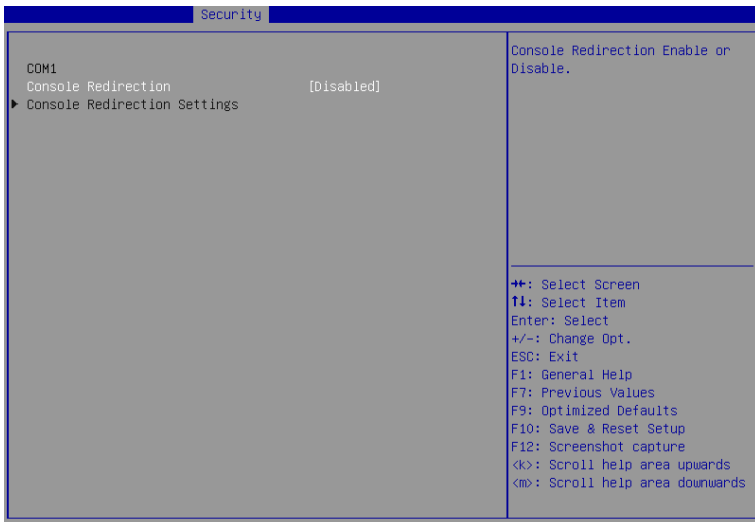
► PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

► Device Select

Select your TPM device through this setting.

► Serial Port Console Redirection



► Console Redirection

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables or disables the operation of console redirection. When set to [Enabled], BIOS redirects and sends all contents that should be displayed on the screen to the serial COM port for display on the terminal screen. Besides, all data received from the serial port is interpreted as keystrokes from a local keyboard.

► **Console Redirection Settings (COM1)**

Security		
COM1		
Console Redirection Settings		
Terminal Type	[ANSI]	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	[115200]	
Data Bits	[8]	
Parity	[None]	
Stop Bits	[1]	
Flow Control	[None]	
VT-UTF8 Combo Key Support	[Enabled]	
Recorder Mode	[Disabled]	
Resolution 100x31	[Disabled]	
Putty KeyPad	[VT100]	

» **Terminal Type**

To operate the system's console redirection, you need a terminal supporting ANSI terminal protocol and a RS-232 null modem cable connected between the host system and terminal(s). You can select emulation for the terminal from this setting.

[ANSI] Extended ASCII character set.

[VT100] ASCII character set.

[VT100Plus] Extends VT100 to support color, function keys, etc.

[VT-UTF8] Uses UTF8 encoding to map Unicode characters onto one or more bytes.

» **Bits per second, Data Bits, Parity, Stop Bits**

These setting specifies the transfer rate (bits per second, data bits, parity, stop bits) of Console Redirection.

» **Flow Control**

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» **VT-UTF8 Combo Key Support**

This setting enables or disables the VT-UTF8 combination key support for ANSI/VT100 terminals.

» **Recorder Mode, Resolution 100x31**

These settings enables or disables the recorder mode and the resolution 100x31.

» **Putty KeyPad**

PuTTY is a terminal emulator for Windows. This setting controls the numeric keypad for use in PuTTY.

► Secure Boot



► Secure Boot

Secure Boot function can be enabled only when the **Platform Key (PK)** is enrolled and running accordingly.

► Secure Boot Mode

Selects the secure boot mode. This item appears when **Secure Boot** is enabled.

[Standard] The system will automatically load the secure keys from BIOS.

[Custom] Allows user to configure the secure boot settings and manually load the secure keys.

► Restore Factory Keys

Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when "**Secure Boot Mode**" sets to [Custom].

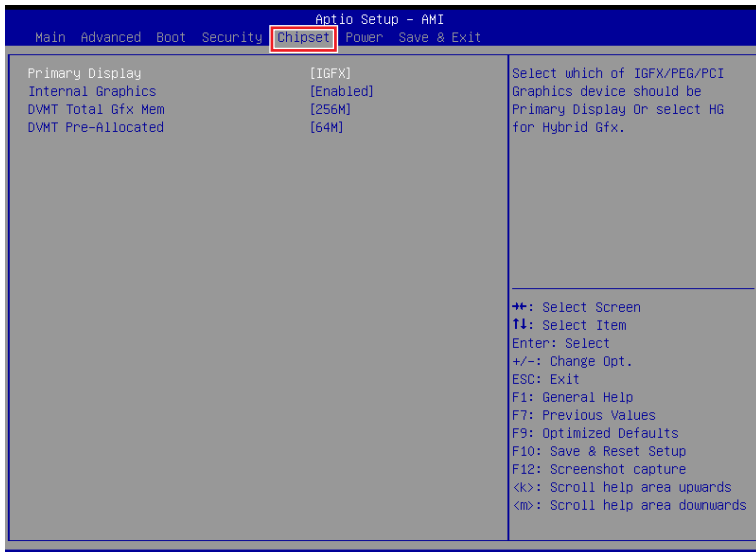
► Reset to setup Mode

Allows you to delete all the Secure Boot keys (PK, KEK, db, dbt, dbx). The settings will be applied after reboot or at the next reboot. This item appears when "**Secure Boot Mode**" sets to [Custom].

► Key Management

Press **Enter** key to enter the sub-menu. Manage the secure boot keys. This item appears when "**Secure Boot Mode**" sets to [Custom].

Chipset



► Primary Display

Use the field to select the primary display of the system.

► Internal Graphics

This setting enables or disables the internal graphics function.
Available settings are:

- | | |
|------------|--|
| [Auto] | The internal graphics will be automatically enabled or disabled. |
| [Enabled] | Enables the internal graphics. |
| [Disabled] | Disables the internal graphics. |

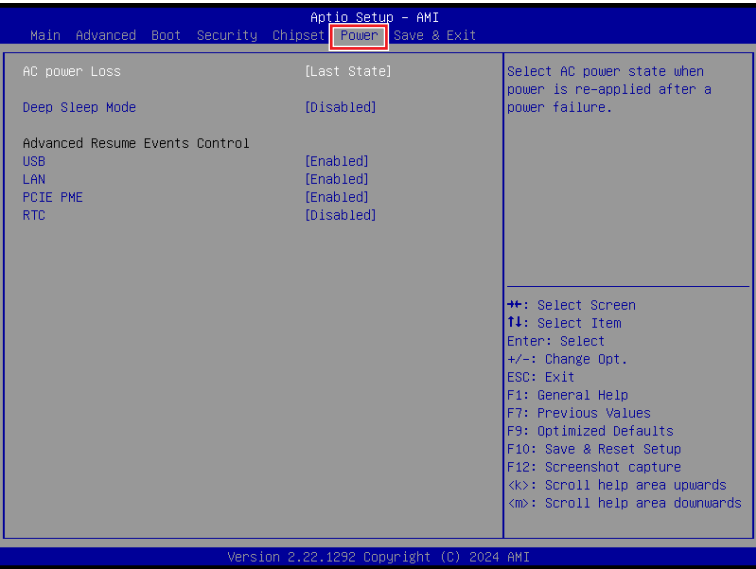
► DVMT Total Gfx Mem

This setting specifies the total graphics memory size for Dynamic Video Memory Technology (DVMT).

► DVMT Pre-Allocated

This setting defines the DVMT pre-allocated memory. Pre-allocated memory is the small amount of system memory made available at boot time by the system BIOS for video. Pre-allocated memory is also known as locked memory. This is because it is “locked” for video use only and as such, is invisible and unable to be used by the operating system.

Power



► Restore AC Power Loss

This setting specifies whether your system will reboot after a power failure or interrupt occurs. Available settings are:

- [Power Off] Leaves the computer in the power off state.
- [Power On] Leaves the computer in the power on state.
- [Last State] Restores the system to the previous status before power failure or interrupt occurred.

► Deep Sleep Mode

The setting enables or disables the Deep S5 power saving mode. S5 is almost the same as G3 Mechanical Off, except that the PSU still supplies power, at a minimum, to the power button to allow return to S0. A full reboot is required. No previous content is retained. Other components may remain powered so the computer can “wake” on input from the keyboard, clock, modem, LAN, or USB device.

► USB

The item allows the activity of the USB device to wake up the system from S4/ S5 sleep state.

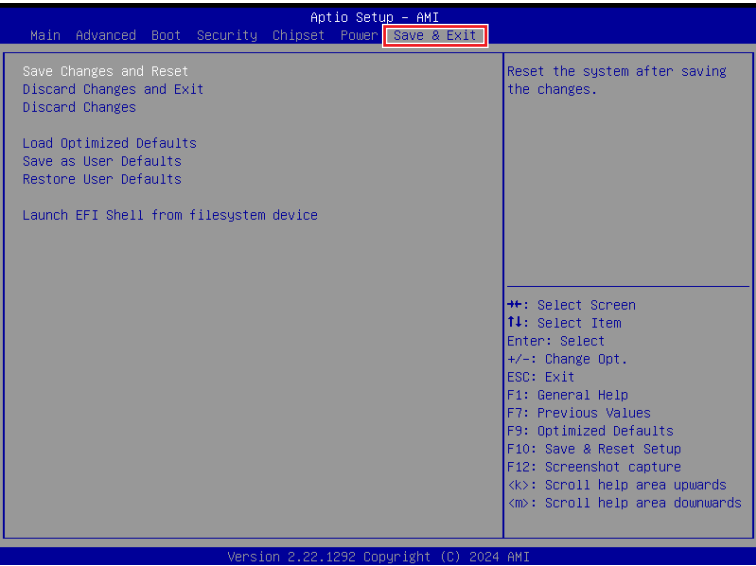
► **LAN/ PCIE PME**

Enables or disables the system to be awakened from the power saving modes when activity or input signal of Intel LAN device and onboard PCIE PME is detected.

► **RTC**

When [Enabled], you can set the date and time at which the RTC (real-time clock) alarm awakens the system from suspend mode.

Save & Exit



- **Save Changes and Reset**
Save changes to CMOS and reset the system.
- **Discard Changes and Exit**
Abandon all changes and exit the Setup Utility.
- **Discard Changes**
Abandon all changes.
- **Load Optimized Defaults**
Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.
- **Save as User Defaults**
Save changes as the user's default profile.
- **Restore User Defaults**
Restore the user's default profile.
- **Launch EFI Shell from filesystem device**
This setting helps to launch the EFI Shell application from one of the available file system devices.

GPIO WDT Programming

This chapter provides GPIO (General Purpose Input/ Output), WDT (Watch Dog Timer), programming guide.

Abstract

In this section, code examples based on C programming language provided for customer interest. **Inportb**, **Outportb**, **Inportl** and **Outportl** are basic functions used for access IO ports and defined as following.

Inportb: Read a single 8-bit I/O port.

Outportb: Write a single byte to an 8-bit port.

Inportl: Reads a single 32-bit I/O port.

Outportl: Write a single long to a 32-bit port.

General Purpose IO

1. General Purposed IO – GPIO/DIO

The GPIO port configuration addresses are listed in the following table:

Name	IO Port	IO address	Name	IO Port	IO address
N_GPIO0	0xA05	Bit 0	N_GPO0	0xA05	Bit 3
N_GPIO1	0xA05	Bit 7	N_GPO1	0xA05	Bit 4
N_GPIO2	0xA05	Bit 2	N_GPO2	0xA05	Bit 5
N_GPIO3	0xA05	Bit 1	N_GPO3	0xA05	Bit 6

1.1 Set output value of GPO

1. Read the value from GPO port.
2. Set the value of GPO address.
3. Write the value back to GPO port.

Example: Set **N_GPO0** output “high”

```
val = Inportb (0xA05);           // Read value from N_GPO0 port.
val = val | (1<<3);              // Set N_GPO0 address (bit 3) to 1 (output “high”).
Outputb (0xA05, val);           // Write back to N_GPO0 port.
```

Example: Set **N_GPO1** output “low”

```
val = Inportb (0xA05);           // Read value from N_GPO1 port.
val = val & ~(1<<4);             // Set N_GPO1 address (bit 4) to 0 (output “low”).
Outputb (0xA05, val);           // Write back to N_GPO1 port.
```

1.2 Read input value from GPI

1. Read the value from GPI port.
2. Get the value of GPI address.

Example: Get **N_GPI2** input value.

```
val = Inportb (0xA05);           // Read value from N_GPI2 port.
val = val & (1<<2);              // Read N_GPI2 address (bit 2).
if (val)    printf (“Input of N_GPI2 is High”);
else       printf (“Input of N_GPI2 is Low”);
```


Watchdog Timer

2. Watchdog Timer – WDT

The base address (WDT_BASE) of WDT configuration registers is [0xA10](#).

2.1 Set WDT Time Unit

```
val = Inportb (WDT_BASE + 0x05);    // Read current WDT setting
val = val | 0x08;                    // minute mode. val = val & 0xF7 if second mode
Outportb (WDT_BASE + 0x05, val);    // Write back WDT setting
```

2.2 Set WDT Time

```
Outportb (WDT_BASE + 0x06, Time);    // Write WDT time, value 1 to 255.
```

2.3 Enable WDT

```
val = Inportb (WDT_BASE + 0x0A);    // Read current WDT_PME setting
val = val | 0x01;                    // Enable WDT OUT: WDOUT_EN (bit 0) set to 1.
Outportb (WDT_BASE + 0x0A, val);    // Write back WDT setting.
val = Inportb (WDT_BASE + 0x05);    // Read current WDT setting
val = val | 0x20;                    // Enable WDT by set WD_EN (bit 5) to 1.
Outportb (WDT_BASE + 0x05, val);    // Write back WDT setting.
```

2.4 Disable WDT

```
val = Inportb (WDT_BASE + 0x05);    // Read current WDT setting
val = val & 0xDF;                    // Disable WDT by set WD_EN (bit 5) to 0.
Outportb (WDT_BASE + 0x05, val);    // Write back WDT setting.
```

2.5 Check WDT Reset Flag

If the system has been reset by WDT function, this flag will set to 1.

```
val = Inportb (WDT_BASE + 0x05);    // Read current WDT setting.
val = val & 0x40;                    // Check WDTMOUT_STS (bit 6).
if (val)    printf ("timeout event occurred");
else        printf ("timeout event not occurred");
```

2.6 Clear WDT Reset Flag

```
val = Inportb (WDT_BASE + 0x05);    // Read current WDT setting
val = val | 0x40;                    // Set 1 to WDTMOUT_STS (bit 6);
Outportb (WDT_BASE + 0x05, val);    // Write back WDT setting
```