SKU1 (Intel® R680E)
SKU2 (Intel® Q670E)
SKU3 (Intel® H610E)
SKU4 (Intel® H610E)
SKU5 (Intel® Q670E)

MS-CF09

Industrial Computer Board

User Guide

Contents

Regulatory Notices....4

Safety Information....7

Specifications....9

- SKU1/ SKU2....9
- SKU3/ SKU4....12

SKU Features Comparison....14

Motherboard Overview....15

- SKU1....15
- SKU2/5....16
- SKU3....17
- SKU4....18

Rear I/O Panel....19

- DisplayPort....20
- HDMI™ Connector....20
- 2.5 GbE RJ-45 LAN Jack....20
- USB 3.2 Gen 2 Port....20
- USB 3.2 Gen 1 Port (SKU3,4 Only)....20
- USB 2.0 Port (SKU3,4 Only)....20
- Line-Out Jack....20
- Mic-In Jack....20

CPU Socket....23

- CPU & Heatsink Installation....24

Memory....25

Storage....27

Expansion Slots....28

- PCIe Slots....28
- M.2 Slots....29

Revision

V1.5, 2025/10

Connectors 30
Power Connectors 30
Cooling Connectors 31
Audio Connectors 32
Graphics Connectors 33
USB Connectors 34
Other Connectors 36
Jumpers 44
BIOS Setup 46
Entering Setup 46
The Menu Bar 48
Main 49
Advanced 50
Boot 57
Security 58
Chipset 71
Power 72
Save & Exit 73
GPIO WDT SMBus Programming 74
Abstract 74
General Purpose IO 75
Watchdog Timer 77
SMBus Access 78

Regulatory Notices

CE Conformity

Hereby, Micro-Star International CO., LTD declares that this device is in compliance with the essential safety requirements and other relevant provisions set out in the European Directive.

FCC-B Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the measures listed below:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

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:

1. **This device may not cause harmful interference, and**
2. **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

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.

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

SKU1/ SKU2/ SKU5

Model	MS-CF09-SKU1	MS-CF09-SKU2 MS-CF09-SKU5
Dimensions	244(L)mm x 244(W)mm x 1.6(H)mm, Micro-ATX size	
Processor	• Intel® Bartlett Lake-S i7/i5/i3/300 IOTG Series Processor, **Max 125W** • **14th** Gen Intel® Raptor Lake-S Refresh i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W** • **13th** Gen Intel® Raptor Lake-S i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W** • **12th** Gen Intel® Alder Lake-S i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W**	
Chipset	**Intel® R680E**	**Intel® Q670E**
iAMT Support	• Supports Intel® AMT 16.x (Only for Intel® Core™ i9/i7/i5 Processor Series at LAN1)	
Memory	• 4 x DDR5 UDIMM slots (288-pin, vertical) - Up to 4400 MT/s - Up to **128GB**	
	- Dual-Channel DDR5, **ECC*/ Non-ECC**	- Dual-Channel DDR5, **Non-ECC**
Network	• **4 x Intel® I226-LM** PCIe 2.5GbE RJ45 LAN	• **2 x Intel® I226-LM (SKU2)** PCIe 2.5GbE RJ45 LAN • **1 x Intel® I226-LM (SKU5)** • **3 x Intel® I226-V (SKU5)** PCIe 2.5GbE RJ45 LAN
Storage	• 4 x SATA 3.0 6Gb/s ports - Supports RAID 0/1/5/10 - Supports AHCI mode	

Continued on next column

*Please refer to your CPU specifications for ECC compatibility.

Model	MS-CF09-SKU1	MS-CF09-SKU2 MS-CF09-SKU5
Expansion Slots	• 1 x PCIe 5.0 x16 slot, up to 75W (PCIE1) • 2 x PCIe 4.0 x4 slot, up to 25W (PCIE2~3) • 1 x PCIe 3.0 x4 slot, up to 25W (PCIE4) • 1 x M.2 M Key slot (2280/ 22110) - Supports PCIe 4.0 x4 signal (signal from CPU) - Supports B+M Key PCIe x4 module • 1 x M.2 M Key slot (2242/ 2280) - Supports PCIe 4.0 x4/x2/x1 signal - Supports SATA 3.0 signal - Supports B+M Key PCIe x4 module • **1 x M.2 M Key slot (2242/ 2280)** - Supports PCIe 3.0 x4/x2/x1 signal - Supports B+M Key PCIe x4 module	• 1 x PCIe 5.0 x16 slot, up to 75W (PCIE1) • 2 x PCIe 4.0 x4 slot, up to 25W (PCIE2~3) • 1 x PCIe 3.0 x4 slot, up to 25W (PCIE4) • 1 x M.2 M Key slot (2280/ 22110) - Supports PCIe 4.0 x4 signal (signal from CPU) - Supports B+M Key PCIe x4 module • 1 x M.2 M Key slot (2242/ 2280) - Supports PCIe 4.0 x4/x2/x1 signal - Supports SATA 3.0 signal - Supports B+M Key PCIe x4 module
Audio	Realtek® ALC897 High Definition Audio Codec	
Graphics	• 2 x DP 1.4a up to 4096×2304 @60Hz • 2 x HDMI™ 2.0b up to 4096x2160 @60Hz • 1 x eDP 1.4b up to 4096×2160 @60Hz • **4 independent display modes** supported - DP1 + DP2 + HDMI™1 + HDMI™2 - DP1 + DP2 + HDMI™1/2 + eDP - DP1/2 + HDMI™1 + HDMI™2 + eDP	
Rear I/O	• 2 x DisplayPort (1.4a) • 2 x HDMI™ connector (2.0b) • 8 x USB 3.2 Gen 2 Type-A ports (10 Gbps) • 1 x Line-out jack • 1 x Mic-in jack	
	• **4 x 2.5 GbE RJ-45 LAN ports**	• **2 x 2.5 GbE RJ-45 LAN ports (SKU2)** • **4 x 2.5 GbE RJ-45 LAN ports (SKU5)**
Internal USB Connectors	• **1 x USB 3.2 Gen 1 connector** • 1 x USB 2.0 connector • **2 x USB 2.0 Type-A connectors**	
Power Connectors	• 1 x 24-pin ATX power connector • 1 x 8-pin ATX 12V power connector	

Continued on next column

Model	MS-CF09-SKU1	MS-CF09-SKU2 MS-CF09-SKU5
Fan Connectors	• 1 x 4-pin PWM CPU fan connector • 3 x 4-pin PWM system fan connector	
System Connectors	• 1 x Front panel connector • 1 x Front LAN LED connector • 1 x Front audio connector (Line-out & Mic-in) • 1 x S/PDIF connector • 1 x eDP connector • 1 x PS/2® Keyboard & Mouse connector • 1 x Parallel port connector • **6 x COM port connectors** • 2 x GPIO (DIO) connectors (5V, 16-bit 8 x GPI/GPO) • 1 x PMBus connector (3.3V) • 1 x SMBus connector (5V) • 1 x I2C connector • 1 x Chassis intrusion header • 1 x CMOS battery header	
Jumpers	• 6 x COM voltage select jumpers • 1 x Clear CMOS jumper • 1 x ME jumper (for iAMT BIOS flash) • 1 x AT/ ATX mode select jumper • 1 x eDP Power Select Jumper	
OS Driver Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC 24H2 (64-bit) • Linux Kernel 5.xx, Ubuntu 22.04 LTS Pre-scan	
Certification	CE, FCC Class B, BSMI, RCM, VCCI, UKCA	
Environment	• Operating Temperature: 0 ~ 60°C • Storage Temperature: -20 ~ 80°C • Relative Humidity: 10 ~ 90%, non-condensing	

SKU3/ SKU4

Model	MS-CF09-SKU3	MS-CF09-SKU4
Dimensions	244(L)mm x 244(W)mm x 1.6(H)mm, Micro-ATX size	
Processor	• Intel® Bartlett Lake-S i7/i5/i3/300 IOTG Series Processor, **Max 125W** • **14th** Gen Intel® Raptor Lake-S Refresh i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W** • **13th** Gen Intel® Raptor Lake-S i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W** • **12th** Gen Intel® Alder Lake-S i9/i7/i5/i3 Pentium®/ Celeron® IOTG Series Processor, **Max 125W**	
Chipset	**Intel® H610E**	
Memory	• 2 x DDR5 UDIMM slots (288-pin, vertical) - Up to 4400 MT/s - Up to **64GB** - Dual-Channel DDR5, **Non-ECC**	
Network	• **4 x Intel® I226-V** PCIe 2.5GbE RJ45 LAN	• **2 x Intel® I226-V** PCIe 2.5GbE RJ45 LAN
Storage	• 4 x SATA 3.0 6Gb/s ports	
Expansion Slots	• 1 x PCIe 5.0 x16 slot, up to 75W (PCIE1) • 1 x PCIe 3.0 x4 slot, up to 25W (PCIE4)	
Audio	• Realtek® ALC897 High Definition Audio Codec	
Graphics	• 2 x DP 1.4a up to 4096×2304 @60Hz • 2 x HDMI™ 2.0b up to 4096x2160 @60Hz • 1 x eDP 1.4b up to 4096×2160 @60Hz • **3 independent display modes** supported - DP1 + DP2 + HDMI™1/2 - DP1/2 + HDMI™1 + HDMI™2 - DP1 + DP2 + eDP - DP1 + HDMI™1/2 + eDP - HDMI™1 + HDMI™2 + eDP	
Rear I/O	• 2 x DisplayPort (1.4a) • 2 x HDMI™ connector (2.0b) • 2 x USB 3.2 Gen 2 Type-A ports (10 Gbps) • 2 x USB 3.2 Gen 1 Type-A ports (5 Gbps) • 4 x USB 2.0 Type-A ports (480 Mbps) • 1 x Line-out jack • 1 x Mic-in jack	
	• **4 x 2.5 GbE RJ-45 LAN ports**	• **2 x 2.5 GbE RJ-45 LAN ports**

Continued on next column

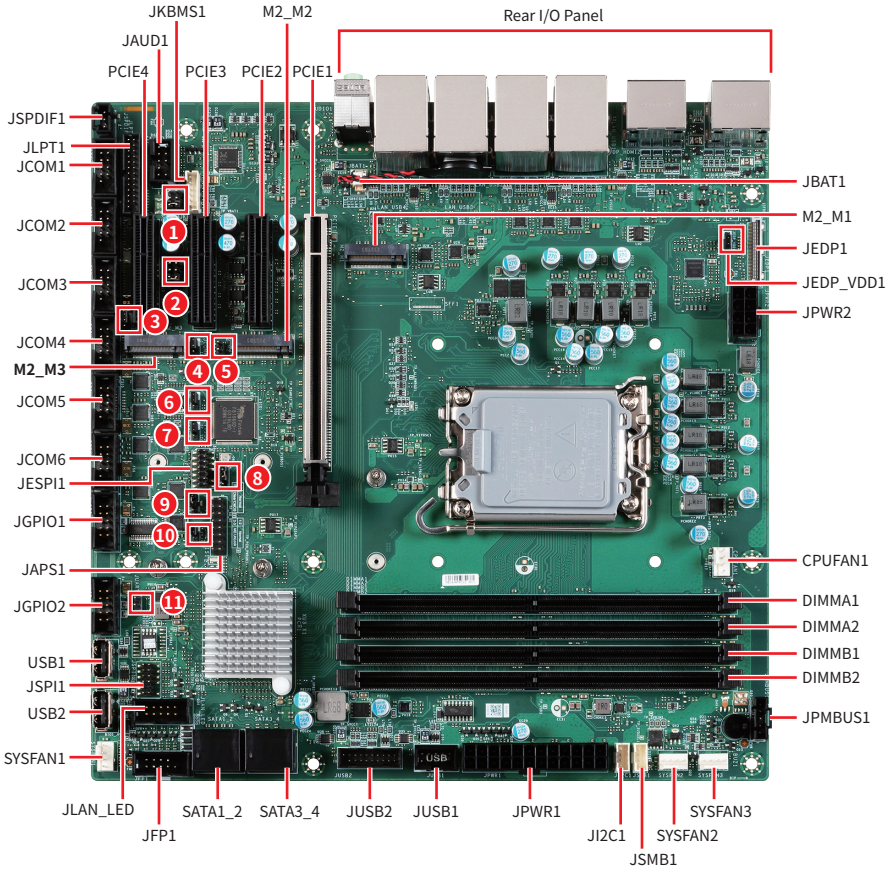
Model	MS-CF09-SKU3	MS-CF09-SKU4
Internal USB Connectors	• 1 x USB 2.0 connector	
Power Connectors	• 1 x 24-pin ATX power connector • 1 x 8-pin 12V ATX power connector	
Fan Connectors	• 1 x 4-pin PWM CPU fan connector • 3 x 4-pin PWM system fan connector	
System Connectors	• 1 x Front panel connector • 1 x Front LAN LED connector • 1 x Front audio connector (Line-out & Mic-in) • 1 x S/PDIF connector • 1 x eDP connector • 1 x PS/2® Keyboard & Mouse connector • 1 x Parallel port connector • **4 x COM port connectors** • 2 x GPIO (DIO) connectors (5V, 16-bit 8 x GPI/GPO) • 1 x PMBus connector (3.3V) • 1 x SMBus connector (5V) • 1 x I2C connector • 1 x Chassis intrusion header • 1 x CMOS battery header	
Jumpers	• 4 x COM voltage select jumpers • 1 x Clear CMOS jumper • 1 x ME jumper • 1 x AT/ ATX mode select jumper • 1 x eDP Power Select Jumper	
OS Driver Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC 24H2 (64-bit) • Linux Kernel 5.xx, Ubuntu 22.04 LTS Pre-scan	
Certification	CE, FCC Class B, BSMI, RCM, VCCI, UKCA	
Environment	• Operating Temperature: 0 ~ 60°C • Storage Temperature: -20 ~ 80°C • Relative Humidity: 10 ~ 90%, non-condensing	

SKU Features Comparison

SKU#		SKU1	SKU2	SKU5	SKU3	SKU4
Chipset		Intel® R680E	Intel® Q670E		Intel® H610E	
LAN1		Intel® I226-LM			Intel® I226-V	
LAN2		Intel® I226-LM		Intel® I226-V	Intel® I226-V	
LAN3		Intel® I226-LM		Intel® I226-V	Intel® I226-V	
LAN4		Intel® I226-LM		Intel® I226-V	Intel® I226-V	
USB	Rear	8 x USB 3.2 Gen 2			2 x USB 3.2 Gen 2 2 x USB 3.2 Gen 1 4 x USB 2.0	
	Internal	2 x USB 3.2 Gen 1 4 x USB 2.0			2 x USB 2.0	
COM	RS-232/422/485	6	2		1	
	RS-232		4		3	
PCIe x4 Slot (PCIE2~3)		Yes				
M.2 M Key	From CPU	Yes				
	From PCH	Yes				
	From PCH	Yes				
Display Mode		4 independent display			3 independent display	

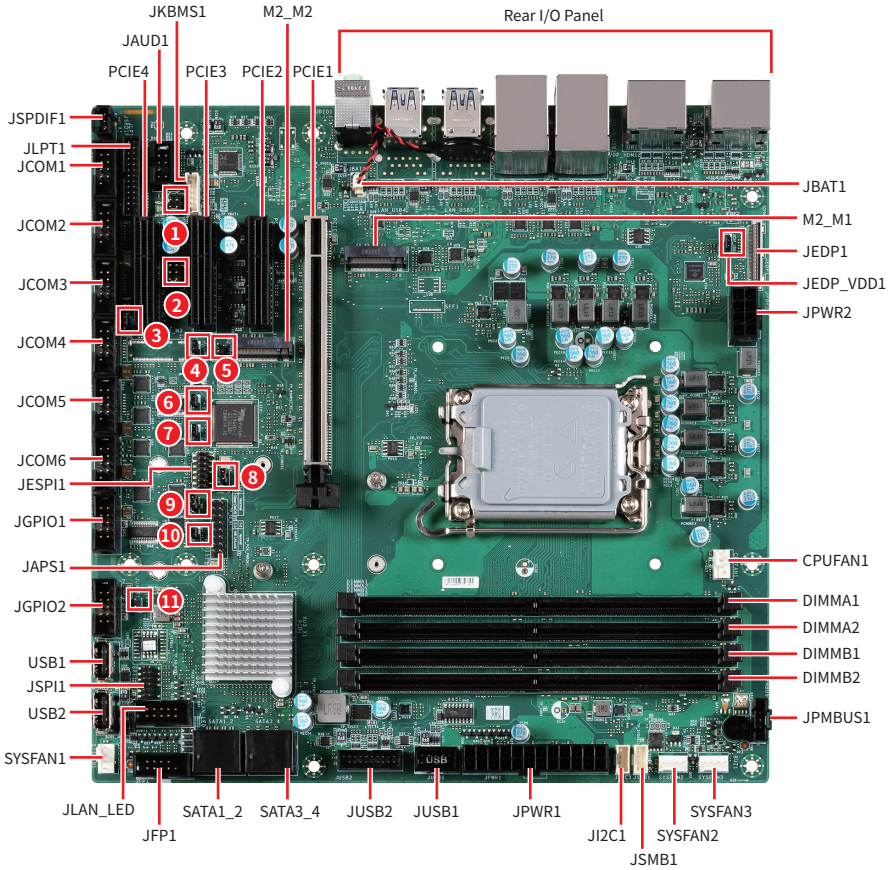
Motherboard Overview

SKU1



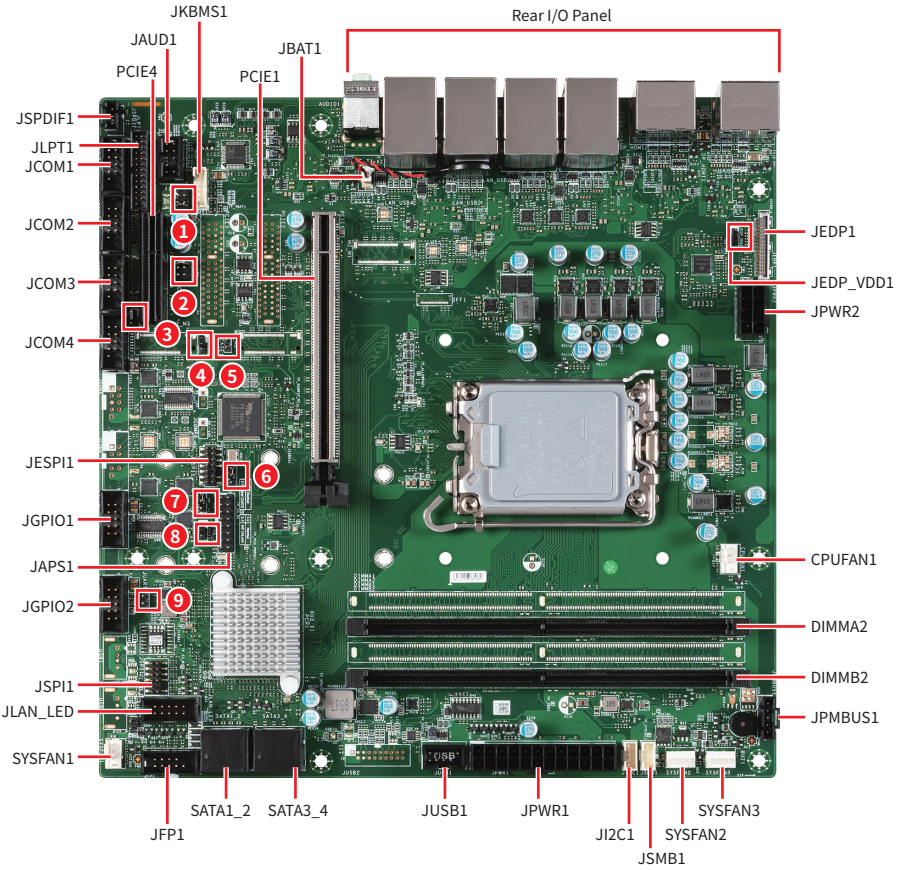
1 JCOMP1
2 JCOMP2
3 JCOMP3
4 JCOMP4
5 JCASE1
6 JCOMP5
7 JCOMP6
8 JATX1
9 JCMOS1
10 JME_DIS1
11 JUART1

SKU2/5



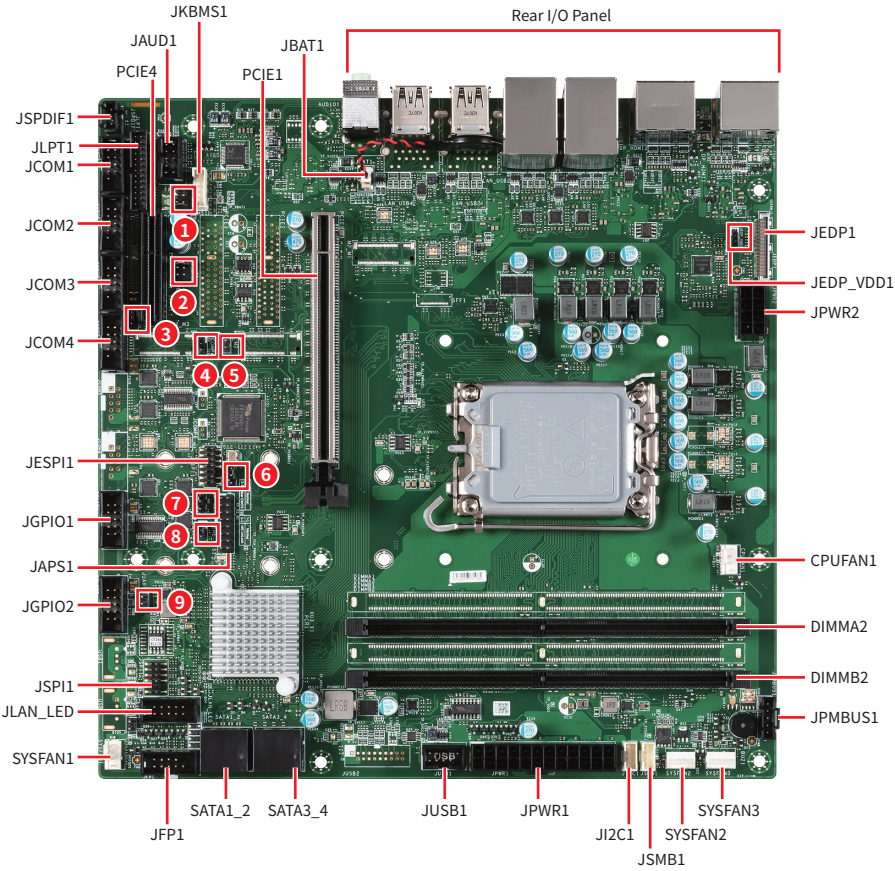
1 JCOMP1
2 JCOMP2
3 JCOMP3
4 JCOMP4
5 JCASE1
6 JCOMP5
7 JCOMP6
8 JATX1
9 JCMOS1
10 JME_DIS1
11 JUART1

SKU3



1. JCOMP1
2. JCOMP2
3. JCOMP3
4. JCOMP4
5. JCASE1
6. JATX1
7. JCMOS1
8. JME_DIS1
9. JUART1

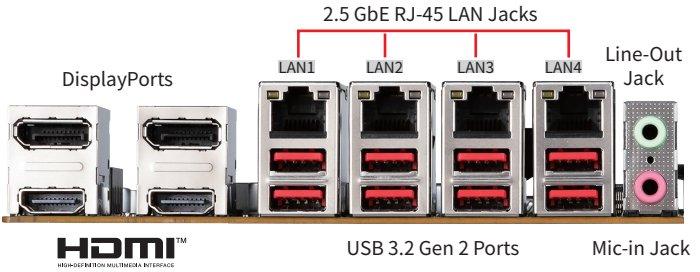
SKU4



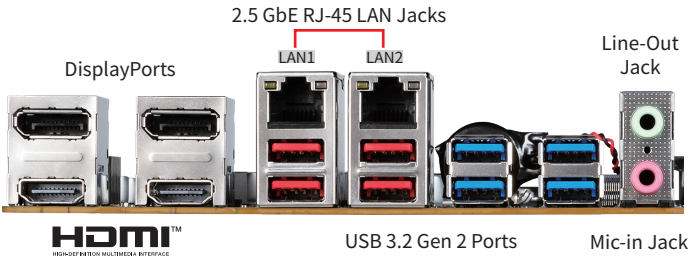
1. JCOMP1
2. JCOMP2
3. JCOMP3
4. JCOMP4
5. JCASE1
6. JATX1
7. JCMOS1
8. JME_DIS1
9. JUART1

Rear I/O Panel

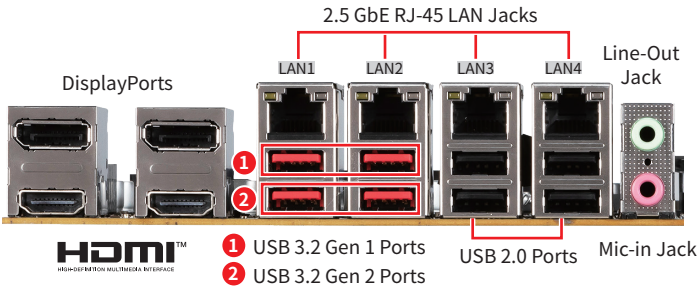
SKU1
SKU5



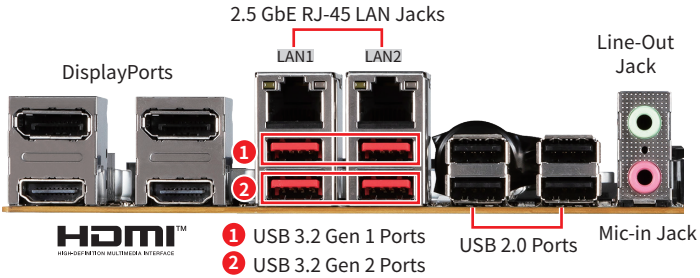
SKU2



SKU3



SKU4



DisplayPort

DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

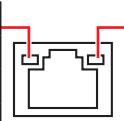
HDMI™ Connector

HDMI™ is an all-digital interface for uncompressed audio/video streams, supporting standard, enhanced, or high-definition video, and multi-channel digital audio on a single cable.

2.5 GbE RJ-45 LAN Jack

The standard single RJ45 LAN jack is provided for connection to the Local Area Network (LAN). You can connect a network cable to it.

Link/ Activity LED	
Status	**Description**
Off	No link
Yellow	Linked
Blinking	Data activity



Speed LED	
Status	**Description**
Off	10/100 Mbps
Green	1000 Mbps
Orange	2.5 Gbps

USB 3.2 Gen 2 Port

USB 3.2 Gen 2, the **SuperSpeed USB 10Gbps**, delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

USB 3.2 Gen 1 Port (SKU3,4 Only)

The USB (Universal Serial Bus) port is for attaching USB devices such as keyboards, mouse, or other USB-compatible devices. USB 3.2 Gen 1 supports data transfer rates up to **5 Gbps**.

USB 2.0 Port (SKU3,4 Only)

This connector is provided for USB peripheral devices. (Speed up to **480 Mbps**)

Important

High-speed devices are recommended for USB 3.2 ports whereas low-speed devices, such as mouse or keyboard, are suggested to be plugged into the USB 2.0 ports.

Line-Out Jack

This connector is provided for headphones or speakers.

Mic-In Jack

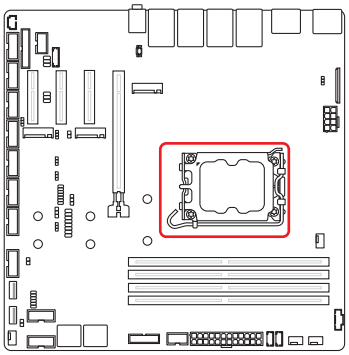
This connector is provided for microphones.

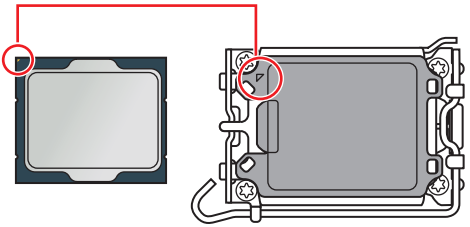
Component Contents

Component	Page
CPU Socket	**23**
Memory	**25**
DIMM1~2: DDR5 DIMM Slots	25
Storage	**27**
SATA1_2, 3_4: SATA 3.0 6Gb/s Ports	27
Expansion Slots	**28**
PCIe Slots	**28**
PCIE1~4: PCIe Expansion Slots	28
M.2 Slots	**29**
M2_M1: M.2 Slot (M Key, 2280/ 22110)	29
M2_M2~3: M.2 Slot (M Key, 2242/ 2280)	29
Connectors	**30**
Power Connectors	**30**
PWR1: 24-Pin ATX Power Connector	30
JPWR2: 8-Pin ATX 12V Power Connector	30
Cooling Connectors	**31**
CPUFAN1, SYSFAN1~3: CPU/ System Fan Connectors	31
Audio Connectors	**32**
JAUD1: Front Audio Connector (Line-out/ MIC-in)	32
JSPDIF1: S/PDIF Connector	32
Graphics Connectors	**33**
JEDP1: eDP Connector	33
USB Connectors	**34**
USB1~2: USB 2.0 Type-A Connector	34
JUSB1: USB 2.0 Connector	34
JUSB2: USB 3.2 Gen 1 Connector	35

Component	Page
Other Connectors	**36**
JFP1: Front Panel Connector	36
JLAN_LED1: Front LAN LED Connector	36
JGPIO1: GPO Connector	37
JGPIO2: GPI Connector	37
JPMBUS1: PMBus Connector	38
JSMB1: SMBus Connector	38
JI2C1: I2C Connector	38
COM1~6: Serial Port Connectors	39
JLPT1: Parallel Port Connector	41
JCASE1: Chassis Intrusion Header	42
JKBMS1: PS/2® Keyboard & Mouse Connector	42
JBAT1: CMOS Battery Header	43
Replacing CMOS battery	43
Jumpers	**44**

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.

Important

- *Always unplug the power cord from the power outlet before installing or removing the CPU.*
- *When **installing a CPU**, always remember to install a CPU heatsink. A CPU heatsink is necessary to prevent overheating and maintain system stability.*
- *Confirm that the CPU heatsink has formed a tight seal with the CPU before booting your system.*
- ***Overheating** can seriously damage the CPU and motherboard. Always make sure the cooling fans work properly to protect the CPU from overheating. Be sure to apply an even layer of thermal paste (or thermal tape) between the CPU and the heatsink to enhance heat dissipation.*
- *Whenever the CPU is not installed, always protect the CPU socket pins by covering the socket with the plastic cap.*
- *If you purchased a separate CPU and heatsink/ cooler, Please refer to the documentation in the heatsink/ cooler package for more details about installation.*

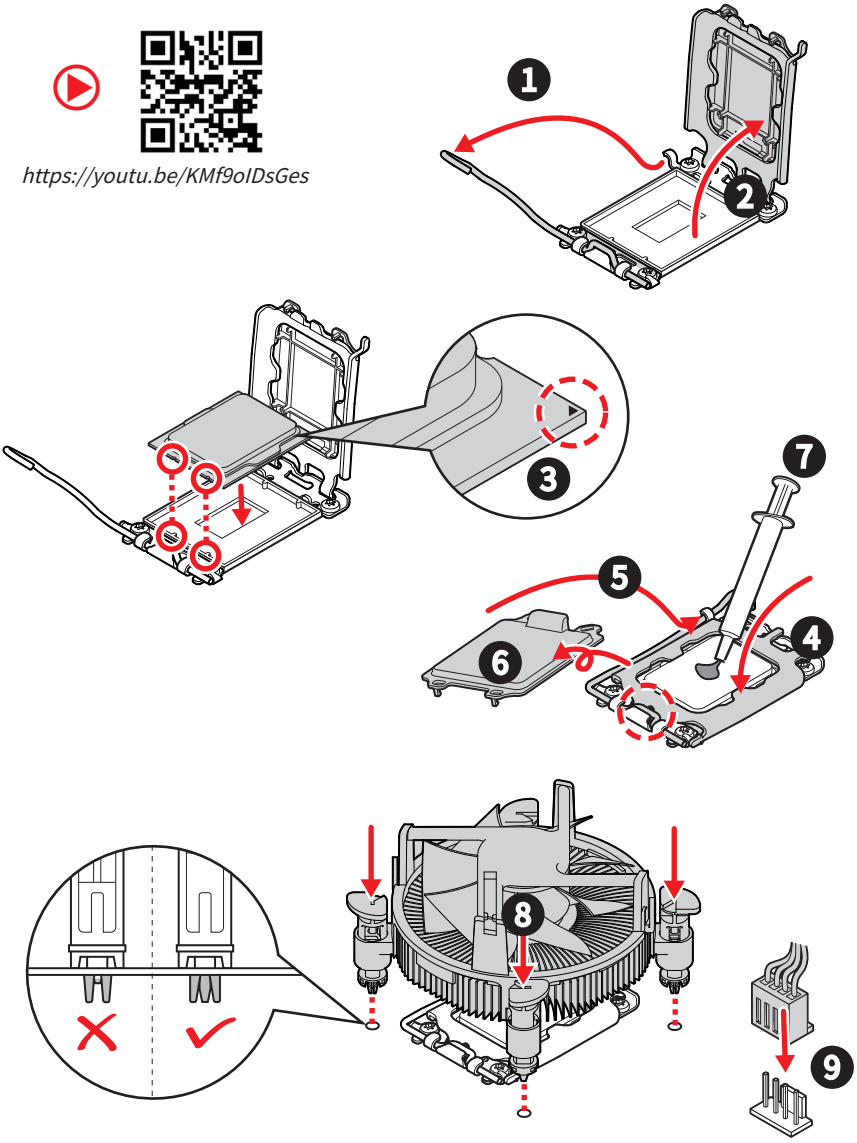
CPU & Heatsink Installation

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

Important

Images are for illustration purposes only; actual parts may vary.

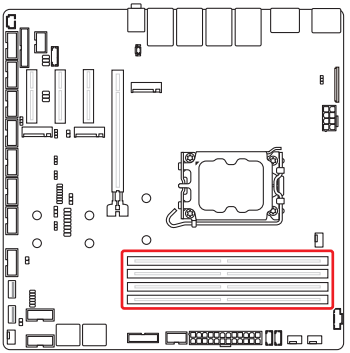
https://youtu.be/KMf9oIDsGes

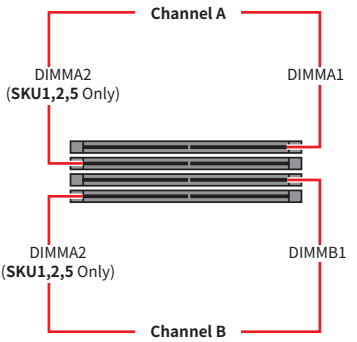


Memory

DIMM1~2: DDR5 DIMM Slots

The SO-DIMM slots is intended for memory modules.





Recommended Memory Population

Quantity of DIMMs		1	2			3		4
Channel A	DIMMA1				V		V	V
	DIMMA2	V	V		V	V	V	V
Channel B	DIMMB1			V		V		V
	DIMMB2		V	V		V	V	V

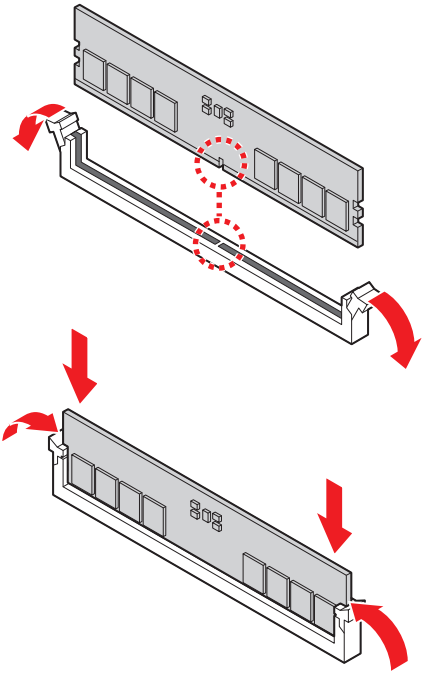
**"V" indicates a populated DIMM slot. **

Important

- *Only support **UDIMM**.*
- *There should be at least 1 DDR5 DIMM populated.*
- *Paired memory installation for Max performance.*
- *If only **1 DIMM** is populated in a channel, then populate it in the **DIMMA2** slot.*
- *Populate the same DIMM type in each channel, specifically: 1. Use the same DIMM size; 2. Use the same number of ranks per DIMM.*
- *We don't suggest other memory installation.*

Installing Memory Modules

1. Open the side clips to unlock the DIMM slot.
2. Insert the DIMM vertically into the slot, ensuring that the off-center notch at the bottom aligns with the slot.
3. Push the DIMM firmly into the slot until it clicks and the side clips automatically close.
4. Verify that the side clips have securely locked the DIMM in place.



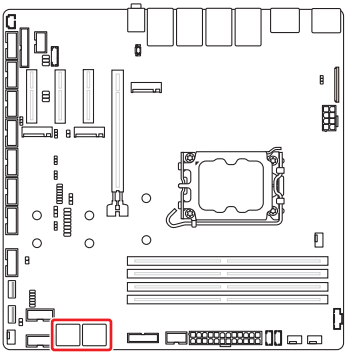
Important

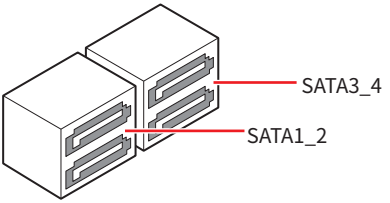
You can barely see the golden finger if the memory module is properly inserted in the DIMM slot.

Storage

SATA1_2, 3_4: SATA 3.0 6Gb/s Ports

These connector are SATA 6Gb/s interface port, it can connect to SATA devices.



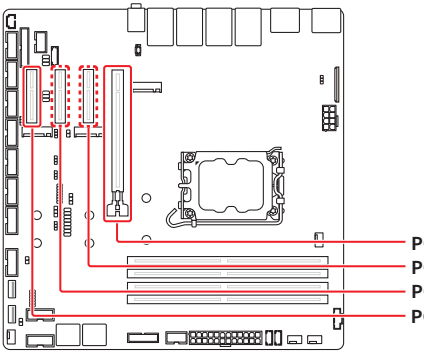


Important

- *These SATA connectors support hot plug.*
- *Please do not fold the SATA cable at a 90-degree angle. Data loss may result during transmission otherwise.*
- *SATA cables have identical plugs on either sides of the cable. However, it is recommended that the flat connector be connected to the motherboard for space saving purposes.*

Expansion Slots

PCIe Slots



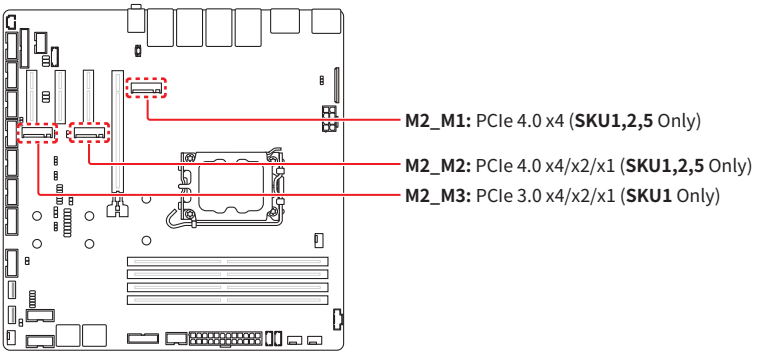
PCIE1~4: PCIe Expansion Slots

The PCI Express (Peripheral Component Interconnect Express) slots support PCIe interface expansion cards.

Important

When adding or removing expansion cards, make sure that you unplug the power supply first. Meanwhile, read the documentation for the expansion card to configure any necessary hardware or software settings for the expansion card, such as jumpers, switches or BIOS configuration.

M.2 Slots

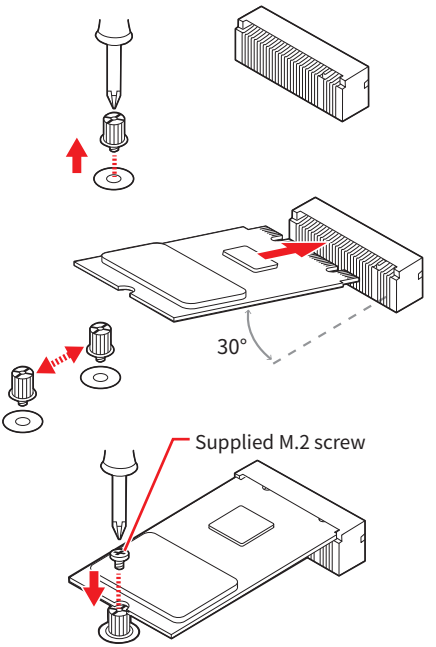


M2_M1: M.2 Slot (M Key, 2280/ 22110)

M2_M2~3: M.2 Slot (M Key, 2242/ 2280)

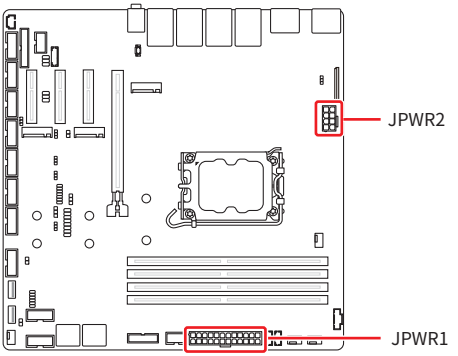
Please install the M.2 solid-state drive (SSD) into the M.2 slot as shown below.

1. Loosen the M.2 riser screw from the motherboard.
2. Move and fasten the M.2 riser screw to the appropriate location according your M.2 SSD size.
3. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.
4. Secure the M.2 SSD in place with the supplied M.2 screw.



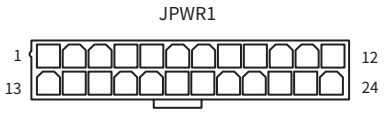
Connectors

Power Connectors



PWR1: 24-Pin ATX Power Connector

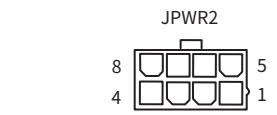
This connector allows you to connect an ATX power supply.



1	+3.3V	13	+3.3V
2	+3.3V	14	-12V
3	GND	15	GND
4	+5V	16	PS-ON#
5	GND	17	GND
6	+5V	18	GND
7	GND	19	GND
8	PWR OK	20	Res
9	5VSB	21	+5V
10	+12V	22	+5V
11	+12V	23	+5V
12	+3.3V	24	GND

JPWR2: 8-Pin ATX 12V Power Connector

This connector allows you to connect an ATX power supply.

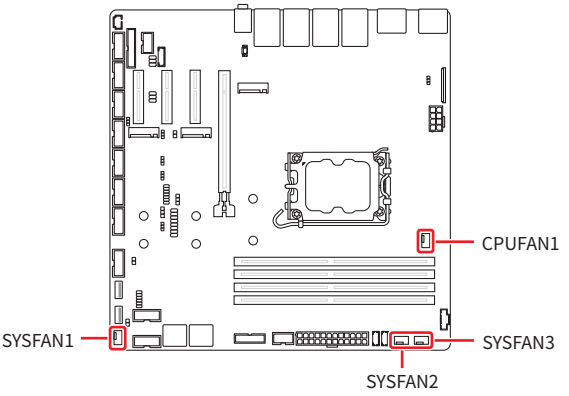


1	GND	5	P12V
2	GND	6	P12V
3	GND	7	P12V
4	GND	8	P12V

Important

Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Cooling Connectors



CPUFAN1, SYSFAN1~3: CPU/ System Fan Connectors

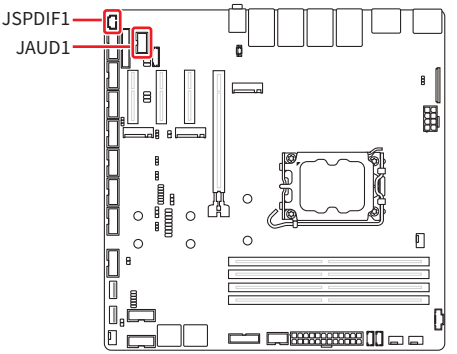
The fan power connector supports CPU/ system cooling fans with +12V. When connecting the wire to the connectors, always note that the red wire is the positive and should be connected to the +12V; the black wire is Ground and should be connected to GND.

CPUFAN1 SYSFAN1~3	1 4	1	GND	2	FAN POWER
		3	FAN SENSE	4	FAN_PWM

Important

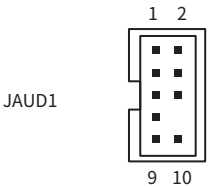
Please refer to the recommended CPU fans at processor' s official website or consult the vendors for proper CPU cooling fan.

Audio Connectors



JAUD1: Front Audio Connector (Line-out/ MIC-in)

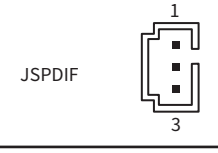
This connector allows you to connect front panel audio.



1	MIC_L	2	GND
3	MIC_R	4	N/C
5	LINE_OUT_R	6	MIC_JD
7	HP_ON	8	No pin
9	LINE_OUT_L	10	LINE_OUT_JD

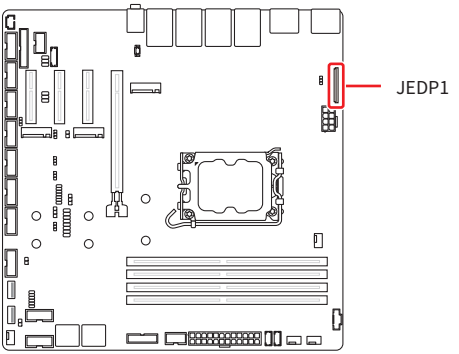
JSPDIF1: S/PDIF Connector

This pinheader is used to connect S/PDIF (Sony & Philips Digital Interconnect Format) interface for digital audio transmission.



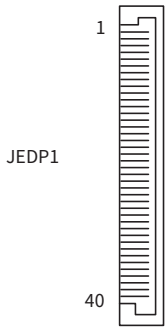
1	5V
2	SPDIFO
3	GND

Graphics Connectors



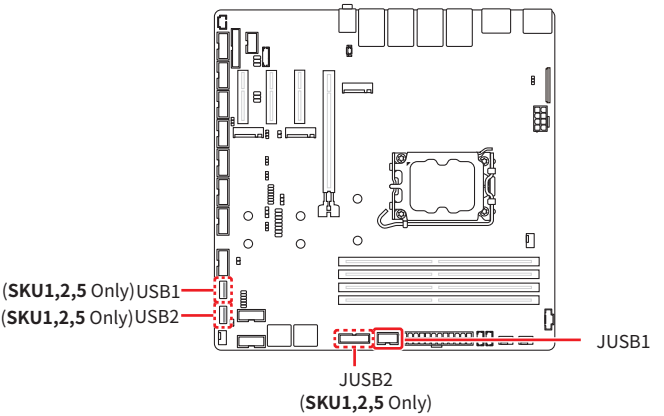
JEDP1: eDP Connector

This connector is designed for use with eDP interface flat panels. When connecting your flat panel to this connector, be sure to check the panel datasheet to ensure that you set the **eDP power select jumper (JEDP_VDD1)** to the appropriate power voltage.



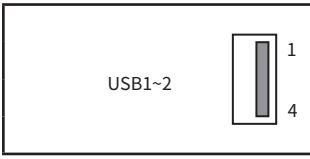
1	LCD_VDD	21	eDP DATA1+
2	LCD_VDD	22	GND
3	LCD_VDD	23	eDP DATA0-
4	LCD_VDD	24	eDP DATA0+
5	LCD_VDD	25	GND
6	INTR#	26	eDP AUX+
7	SMBCLK	27	eDP AUX-
8	SMBDATA	28	GND
9	GND	29	AUX POWER
10	eDP_HPD	30	GND
11	N/C	31	12V
12	N/C	32	GND
13	GND	33	GND
14	eDP DATA3-	34	5V
15	eDP DATA3+	35	GND
16	GND	36	eDP BKLT CTL
17	eDP DATA2-	37	eDP_BKLT_EN
18	eDP DATA2+	38	12V
19	GND	39	3.3V
20	eDP DATA1-	40	GND

USB Connectors



USB1~2: USB 2.0 Type-A Connector

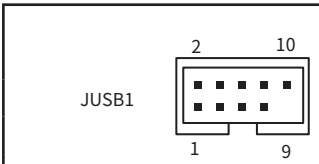
The USB (Universal Serial Bus) port is for attaching USB devices such as keyboard, mouse, or other USB-compatible devices. It supports speed up to **480 Mbps** data transfer rate.



1	POWER
2	USB_D-
3	USB_D+
4	GND

JUSB1: USB 2.0 Connector

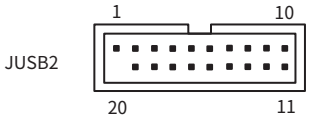
This header is ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices.



1	5V	2	5V
3	USB_D-	4	USB_D-
5	USB_D+	6	USB_D+
7	GND	8	GND
9	No Pin	10	N/C

JUSB2: USB 3.2 Gen 1 Connector

This port is backward-compatible with USB 2.0 devices and supports data transfer rate up to 5 Gbps (SuperSpeed).

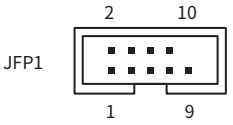


1	5V	11	USB_D+
2	USB 3.2 RX-	12	USB_D-
3	USB 3.2 RX+	13	GND
4	GND	14	USB3.2 TX+
5	USB 3.2 TX-	15	USB 3.2 TX-
6	USB 3.2 TX+	16	GND
7	GND	17	USB 3.2 RX+
8	USB_D-	18	USB 3.2 RX-
9	USB_D+	19	5V
10	NC	20	No Pin

Other Connectors

JFP1: Front Panel Connector

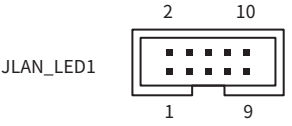
This front-panel connector is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.



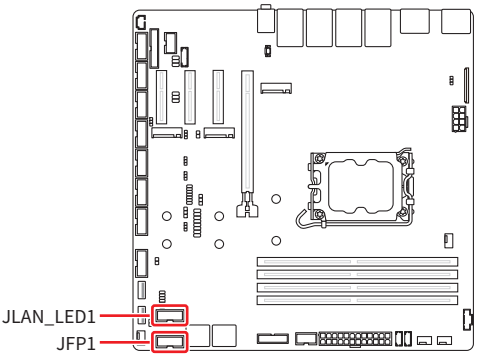
1	HDD LED+	2	POWER LED
3	HDD LED-	4	POWER LED
5	RESET SWITCH-	6	POWER SWITCH+
7	RESET SWITCH+	8	POWER SWITCH-
9	N/C	10	No pin

JLAN_LED1: Front LAN LED Connector

This connector is provided for front panel LAN LEDs.

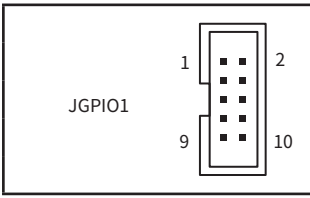


1	I225_ACT_LINK_1	2	I225_LED2_LINK#_1
3	I225_ACT_LINK_2	4	I225_LED2_LINK#_2
5	I225_ACT_LINK_3	6	I225_LED2_LINK#_3
7	I225_ACT_LINK_4	8	I225_LED2_LINK#_4
9	N/C	10	N/C



JGPIO1: GPO Connector

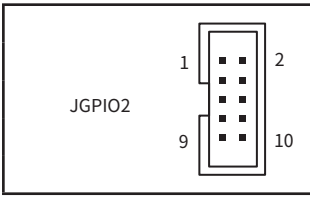
These connectors are provided for the General-Purpose Output (GPO) peripheral module.



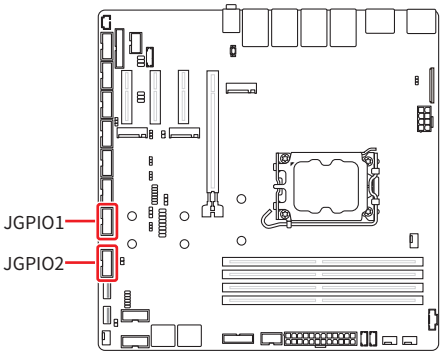
1	GND	2	N_GPIO_VCC (VCC5)
3	N_GPO0	4	N_GPO4
5	N_GPO1	6	N_GPO5
7	N_GPO2	8	N_GPO6
9	N_GPO3	10	N_GPO7

JGPIO2: GPI Connector

These connectors are provided for the General-Purpose Input (GPI) peripheral module.



1	GND	2	N_GPIO_VCC (VCC5)
3	N_GPI0	4	N_GPI4
5	N_GPI1	6	N_GPI5
7	N_GPI2	8	N_GPI6
9	N_GPI3	10	N_GPI7



JPMBUS1: PMBus Connector

Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.

JPMBUS1	1	SMBCLK
	2	SMBDATA
	3	SMBALERT#
	4	GND
	5	3V

JSMB1: SMBus Connector

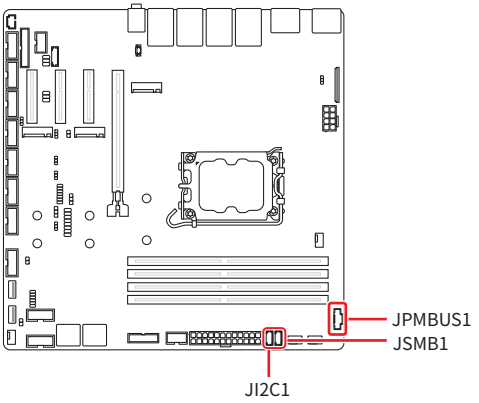
This connector is provided for users to connect to System Management Bus (SMBus) interface.

JSMB1	1	5V
	2	SMBCLK
	3	SMBDATA
	4	GND

JI2C1: I2C Connector

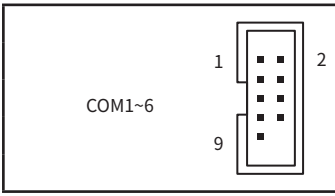
This connector is provided for users to connect I²C (Inter-Integrated Circuit) interface.

JI2C1	1	N/C
	2	I2C_CLK
	3	I2C_DATA
	4	GND

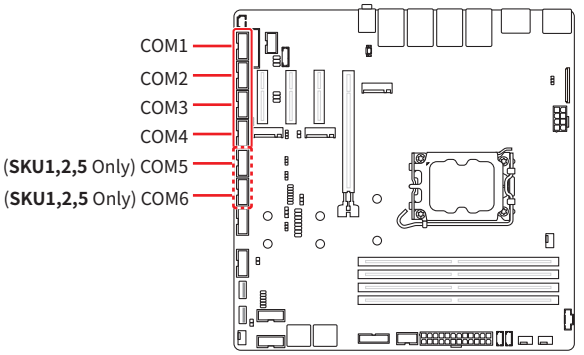


COM1~6: Serial Port Connectors

This connector is a 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial device to it.



1	DCD	2	SIN
3	SOUT	4	DTR
5	GND	6	DSR#
7	RTSD	8	CTS#
9	VCC_COM	10	No Pin



Important

After connect Serial port connectors to printer, garbage can' t be printed when power on/off.

Features

- COM1~6 support auto flow control.*
- RS- 422/485 support TR 1000+ Meter.*

***SKU2,5 (Intel® Q670E)** only supports auto flow control and TR 1000+ Meter through COM1 and COM2. **SKU3 and SKU4 (Intel® H610E)** support auto flow control and TR 1000+ Meter through COM1.

SKU1 (Intel® R680E)

- **COM1/2**

Support RS-232/ 422/ 485, with Ring/0V/5V/12V (Default set to Ring).

- **COM3~6**

Support RS-232/ 422/ 485, with 0V/5V/12V (Default set to 5V).

SKU2/5 (Intel® Q670E)

- **COM1/2**

Support RS-232/ 422/ 485, with Ring/0V/5V/12V (Default set to Ring).

- **COM3~6**

Support RS-232, with 0V/5V/12V (Default set to 5V).

SKU3/4 (Intel® H610E)

- **COM1**

Supports RS-232/ 422/ 485, with Ring/0V/5V/12V (Default set to Ring).

- **COM2~4**

Support RS-232, with 0V/5V/12V (Default set to 5V).

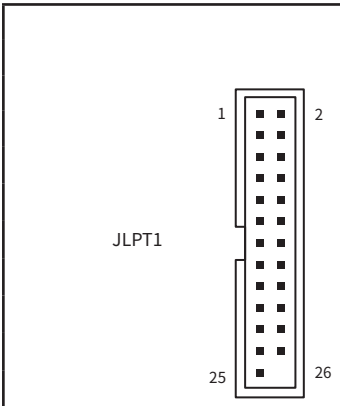
RS232		
PIN	**SIGNAL**	**DESCRIPTION**
1	NDCD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM	VCC_COM

RS422		
PIN	**SIGNAL**	**DESCRIPTION**
1	422 TXD-	Transmit Data, Negative
2	422 TXD+	Transmit Data, Positive
3	422 RXD+	Receive Data, Positive
4	422 RXD-	Receive Data, Negative
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

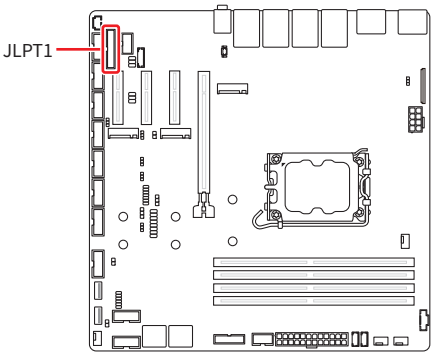
RS485		
PIN	**SIGNAL**	**DESCRIPTION**
1	D-	Data, Negative
2	D+	Data, Positive
3	NC	No Connection
4	NC	No Connection
5	GND	Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

JLPT1: Parallel Port Connector

The mainboard provides a 26-pin header for connection to an optional parallel port bracket. The parallel port is a standard printer port that supports Enhanced Parallel Port (EPP) and Extended Capabilities Parallel Port (ECP) mode.

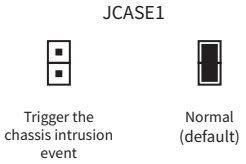


1	RSTB#	2	AFD#
3	PRND0	4	ERR#
5	PRND1	6	PINIT#
7	PRND2	8	LPT_SLIN#
9	PRND3	10	GND
11	PRND4	12	GND
13	PRND5	14	GND
15	PRND6	16	GND
17	PRND7	18	GND
19	ACK#	20	GND
21	BUSY	22	GND
23	PE	24	GND
25	SLCT	26	No Pin



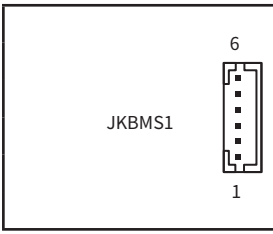
JCASE1: Chassis Intrusion Header

This connector connects to the chassis intrusion switch cable. If the chassis is opened, the chassis intrusion mechanism will be activated. The system will record this status and show a warning message on the screen. To clear the warning, you must enter the BIOS utility and clear the record.

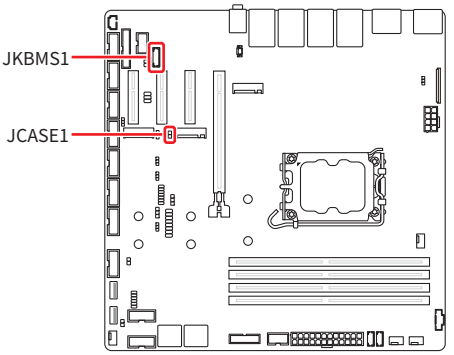


JKBMS1: PS/2® Keyboard & Mouse Connector

This connector is provided to connect a keyboard and a mouse.

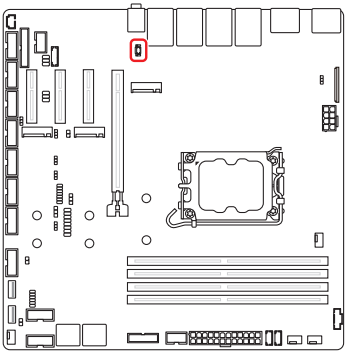


1	KBDAT
2	GND
3	MSDAT
4	KBCLK
5	5V
6	MSCLK



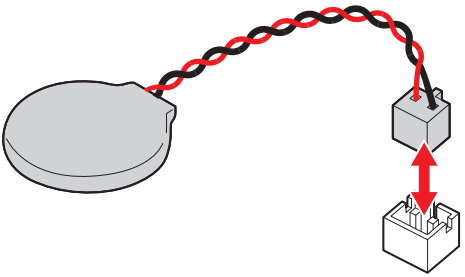
JBAT1: CMOS Battery Header

If the CMOS battery is out of charge, the time in the BIOS will be reset and the data of system configuration will be lost. In this case, you need to replace the CMOS battery.



Replacing CMOS battery

1. Unplug the battery wire from the BAT1 connector and remove the battery.
2. Connect the new CR2032 battery with wire to the BAT1 connector.



WARNING

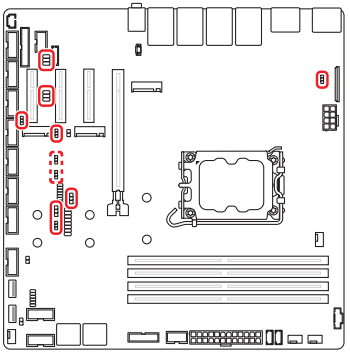
KEEP OUT OF REACH OF CHILDREN

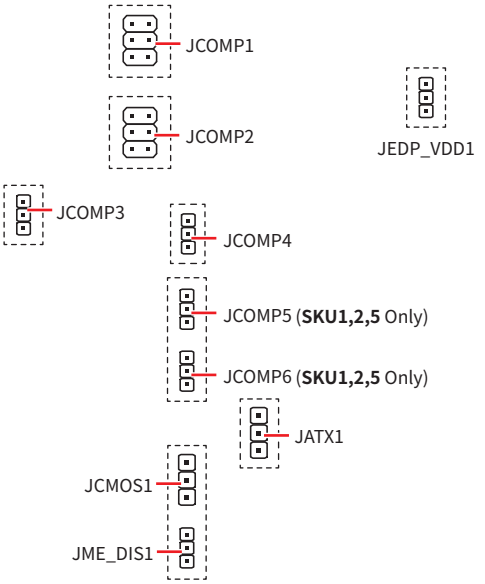
- *Swallowing can cause chemical burns, perforation of soft tissue, and even death.*
- *Severe burns can occur within 2 hours of ingestion.*
- *If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.*

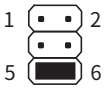
Jumpers

Important

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





Jumper	Default Setting	Description
JCOMP1~2		**COM Voltage Select Jumper** 1-2: 5V 3-4: 12V 5-6: NRI (Default)
JCOMP3~6		**COM Voltage Select Jumper** 1-2: 5V (Default) 2-3: 12V
JATX1		**AT/ ATX Mode Select Jumper** 1-2: ATX (Default) 2-3: AT

Jumper	Default Setting	Description
JCMOS1		**Clear CMOS Jumper** 1-2: Normal (Default) 2-3: Clear CMOS
JME_DIS1		**ME Jumper** 1-2: ME enabled (Default) 2-3: ME disabled
JEDP_VDD1		**eDP Power Select Jumper** 1-2: 5V 2-3: 3.3V (Default)

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 <DEL> or <F2> key to enter Setup, **<F11>** key to Boot Menu, **<F12>** key to PXE Boot .

Press <DEL> 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.

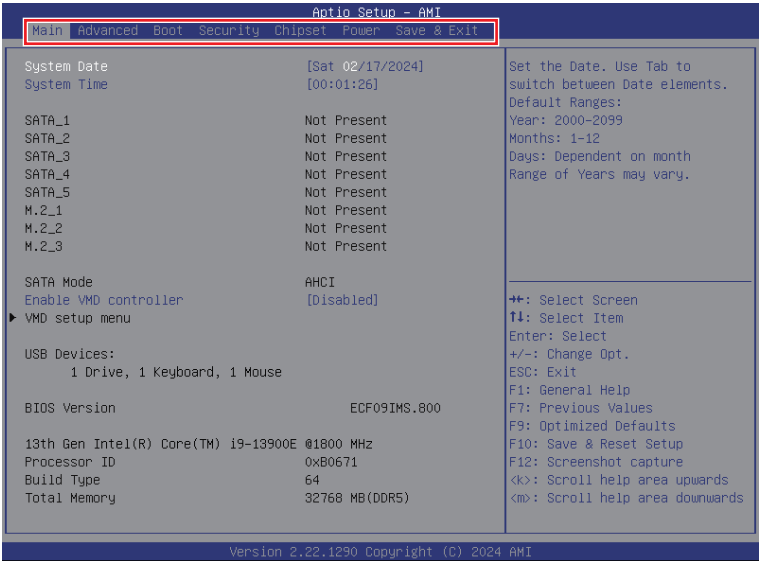
Sub-Menu

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>

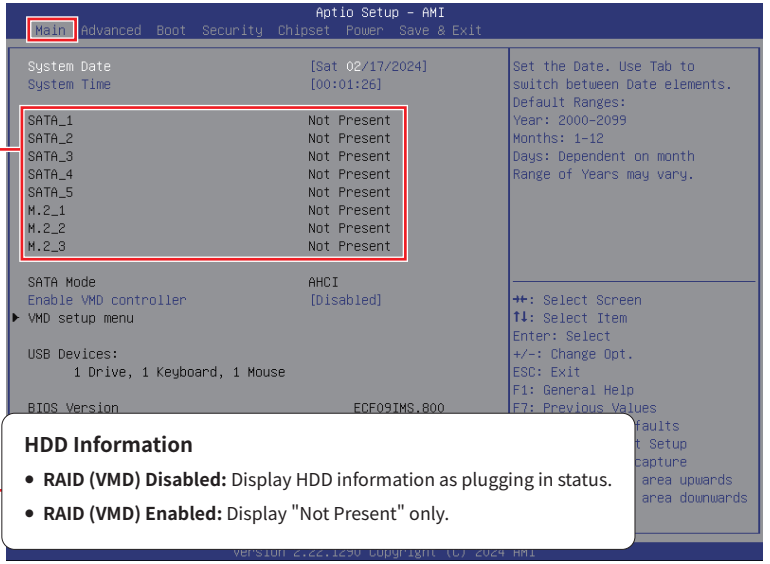
The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing **<F1>**. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press **<Esc>** to exit the Help screen.

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



► System Date

This setting allows you to set the system date.

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

► System Time

This setting allows you to set the system time.

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

► SATA Mode Selection

This setting specifies SATA controller mode.

[AHCI]	AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.
[RAID]	RAID (Redundant Array of Independent Disks) is a virtual disk storage technology that combines multiple physical disks into one unit for data redundancy, performance improvement, or both.

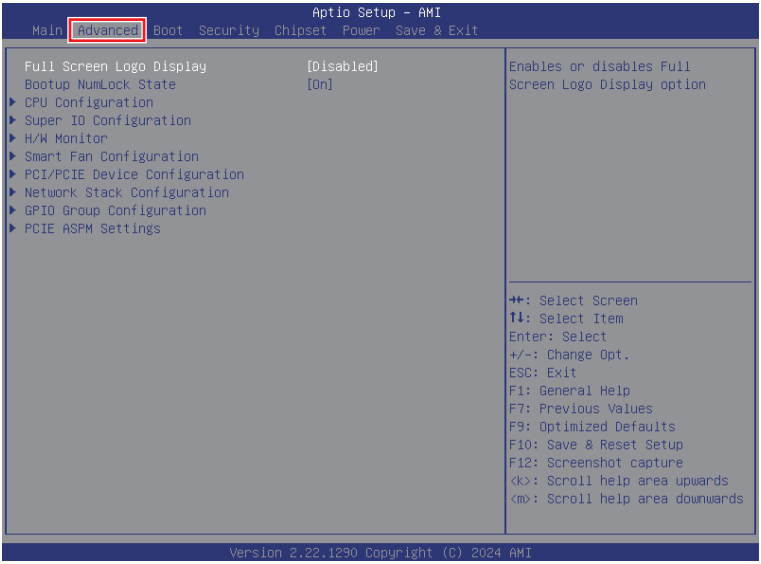
► Enable VMD controller

Enables or disables VMD (RAID) controller.

Important

SKU2,5 (Intel® Q670E) *does not support M.2_3 (M2_M3, M.2 M Key); while* ***SKU3/4 (Intel® H610E)*** *does not support SATA_5 (M2_M2, M.2 M Key with SATA signal), M.2_1~3 (M2_M1~3, M.2 M Key) and VMD controller.*

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.

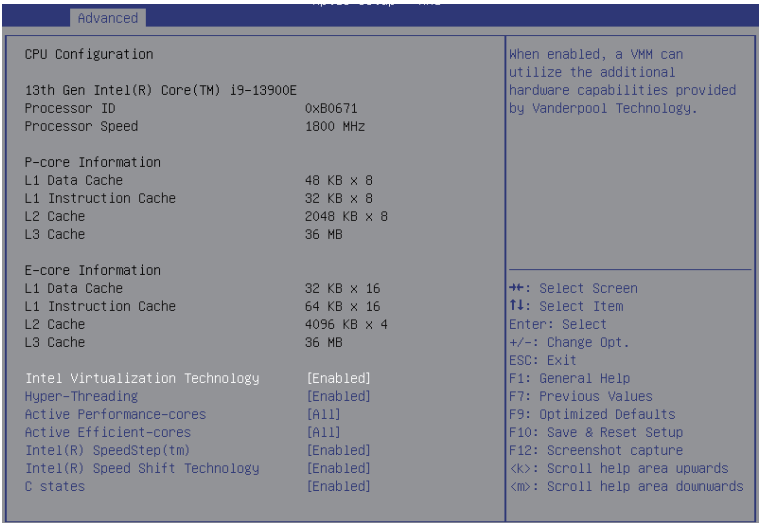
Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

► 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



▸ 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.

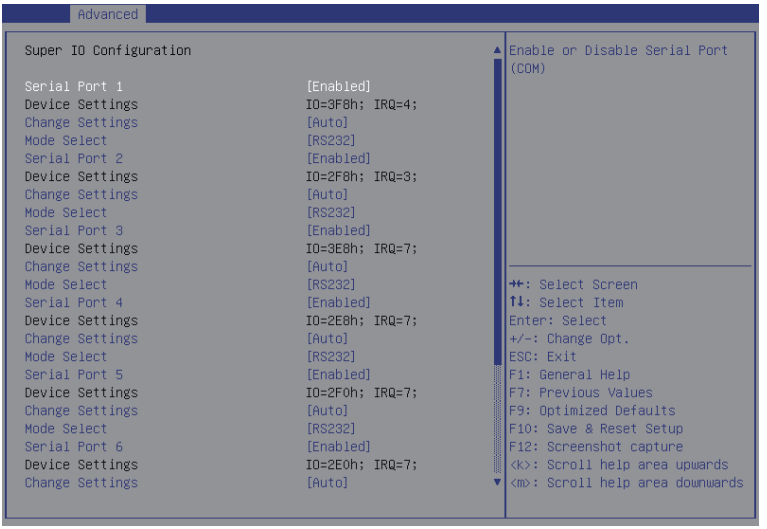
▸ **C States**

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



- **Serial Port 1/ 2/ 3/ 4/ 5/ 6, Parallel Port**

  This setting enables or disables the specified serial port or parallel 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/ 5/ 6, Parallel Port.

- **FIFO Mode**

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

- **Shared IRQ Mode**

  This setting provides the system with the ability to share interrupts among its serial ports.

- **Watch Dog Timer**

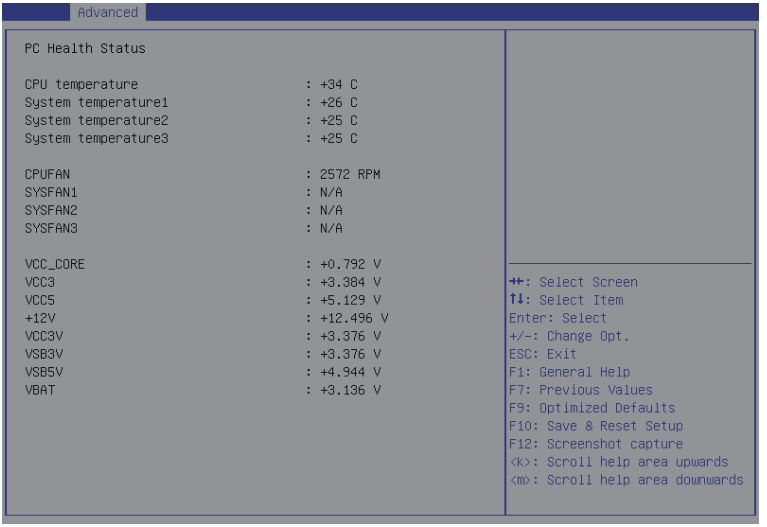
  You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

Important

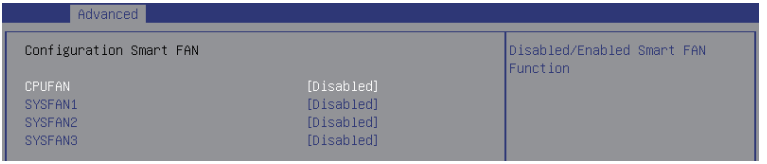
*Serial port availability varies by SKU. Please refer to the **Specifications** and **COM1~6: Serial Port Connectors** sections for information on supported serial ports.*

► 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.



► Smart Fan Configuration



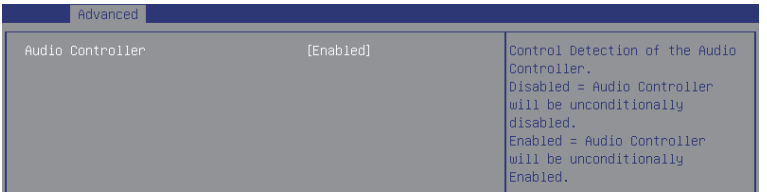
▸ CPUFAN/ SYSFAN1~3

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 CPUFAN/ SYSFAN1~3 is enabled.

» **Min. Speed (%)**

The beginning speed of the System fan.

► PCI/PCIE Device Configuration

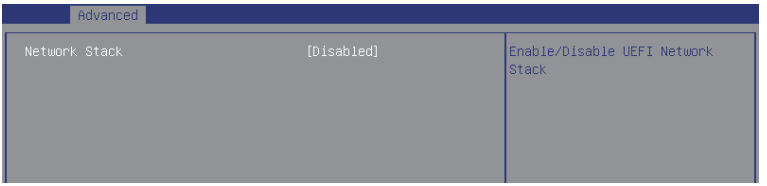


▸ Audio Controller

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.

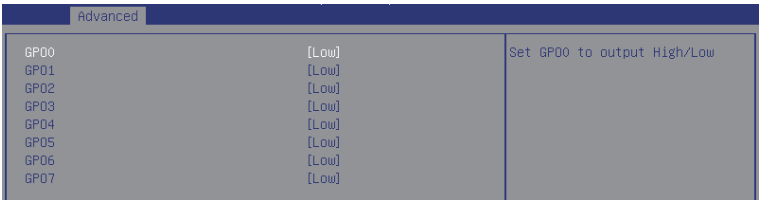
» **PXE boot wait time**

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

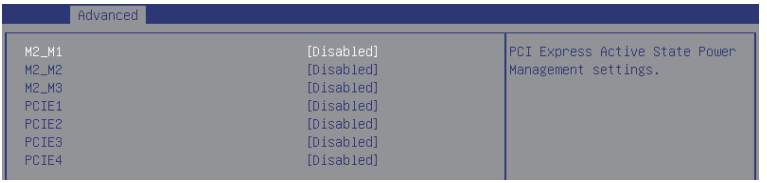


▸ **GPO0 ~ GPO7**

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_M1~3, PCIE1~4**

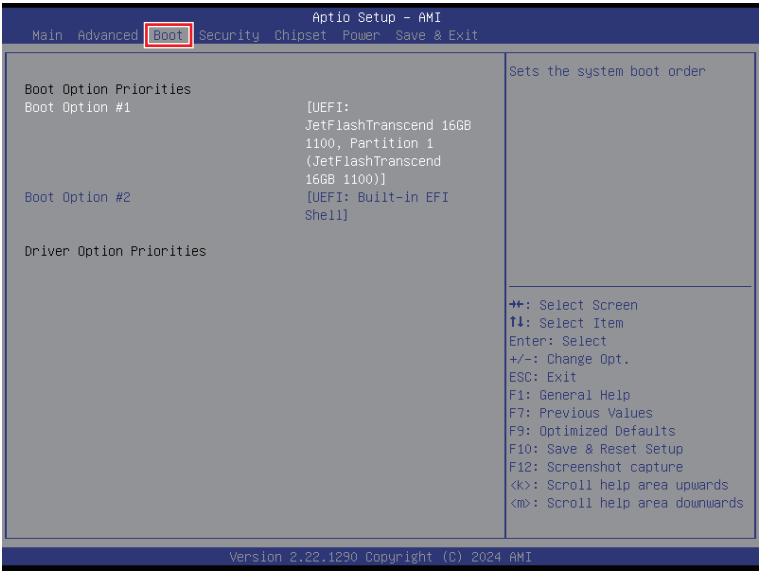
Sets PCI Express ASPM (Active State Power Management) state for power saving.

[L0s]	Initiate an automatic shutdown of the system to protect from potential damage due to overheating.
[L1]	Higher latency, lower power “standby” state **(optional)**.
[L0sL1]	Activate both L0s and L1 support.
[Disabled]	Disable this function.

Important

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

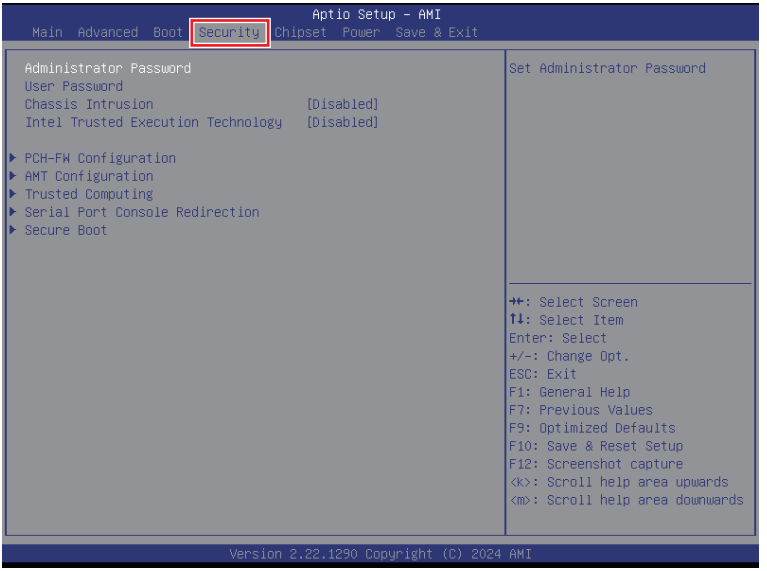
Boot



► **Boot Option #1-2**

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**

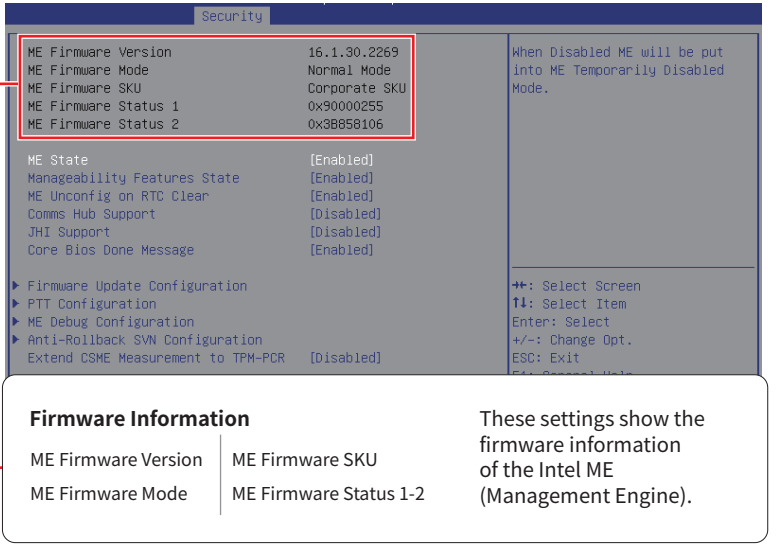
Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware-based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

Important

- ***SKU3/4 (Intel® H610E)*** *does not support* ***"Intel Trusted Execution Technology" and "AMT Configuration"****.*

► PCH-FW Configuration

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



Firmware Information

ME Firmware Version	ME Firmware SKU
ME Firmware Mode	ME Firmware Status 1-2

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

▸ 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.

▸ Firmware Update Configuration

» **ME FW Image Re-Flash**

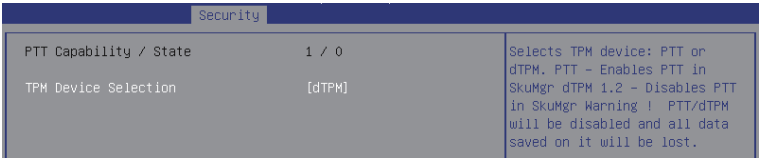
Enables or disables the ME Firmware Image Re-flashing**.**

» **Local FW Update**

Enables or disables the capability to perform a firmware update of the ME locally.

▸ PTT Configuration

Intel® Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.



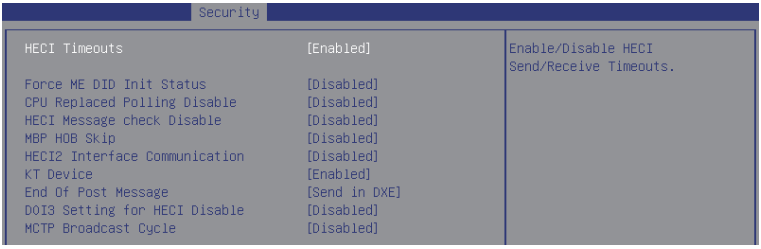
» **TPM Device Selection**

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).



» **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) H0B 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**

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

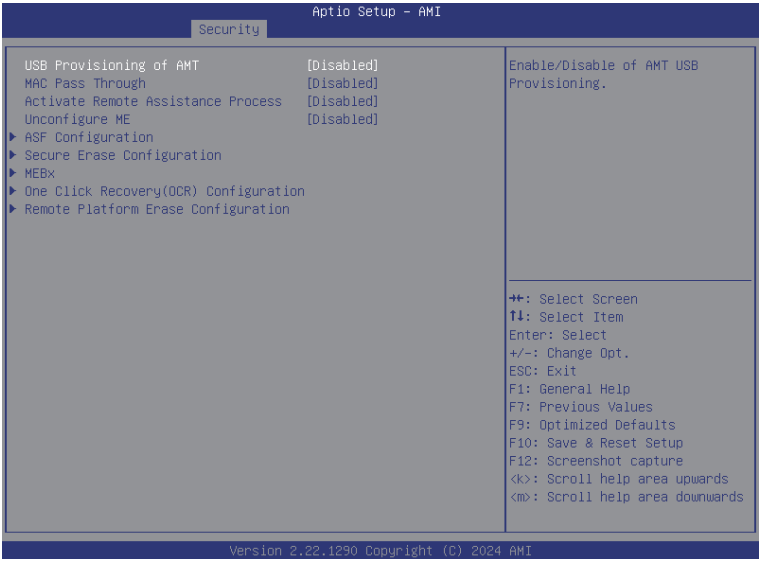
Setting this item enables will automatically activate the hardware-enforced anti-rollback protection based on the Secure Version Number (SVN). Once enabled, the hardware will enforce that only firmware updates with an SVN equal to or higher than the current SVN can be installed.

» **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.

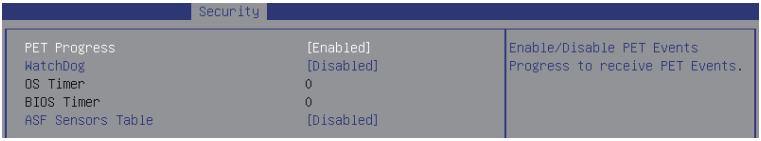
▸ Unconfigure ME

Enables or disables the Unconfigure ME.

Important

SKU3/4 (Intel® H610E) *does not support* ***"AMT Configuration"****.*

▸ ASF Configuration



» **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.

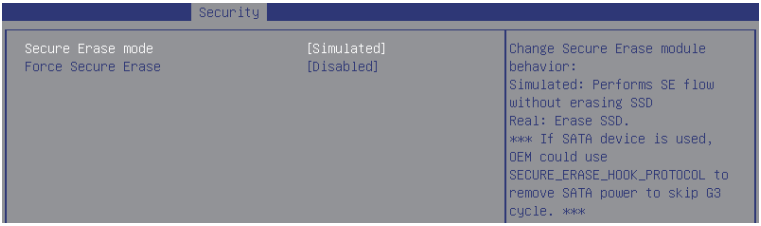
» **BIOS Timer**

This item displays BIOS Timer.

» **ASF Sensor Table**

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

▸ Secure Erase Configuration



» **Secure Erase Mode**

This setting change Secure Erase module behavior.

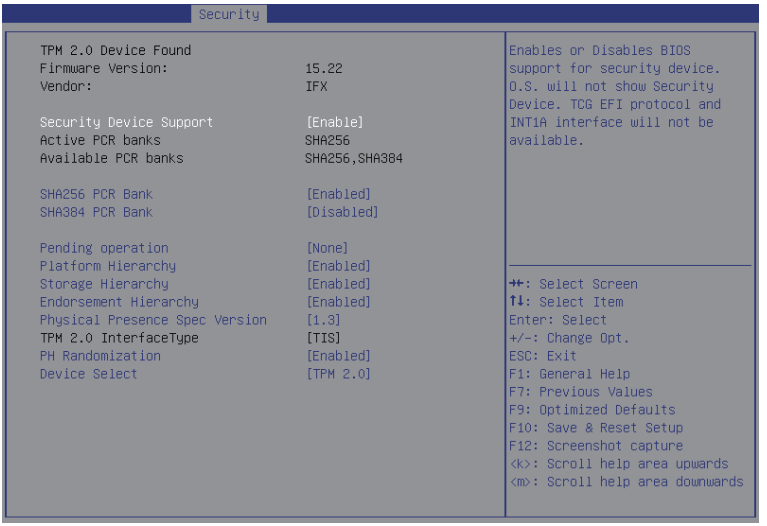
[Simulated]	Performs SE flow without erasing SSD.
[Real]	Erase SSD.

» **Force Secure Erase**

Enables or disables to force Secure Erase on next boot.

▸ MEBx (Management Engine BIOS Extension)

► Trusted Computing



▸ 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 PCR Bank, 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 se lection.

▸ 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.

▸ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

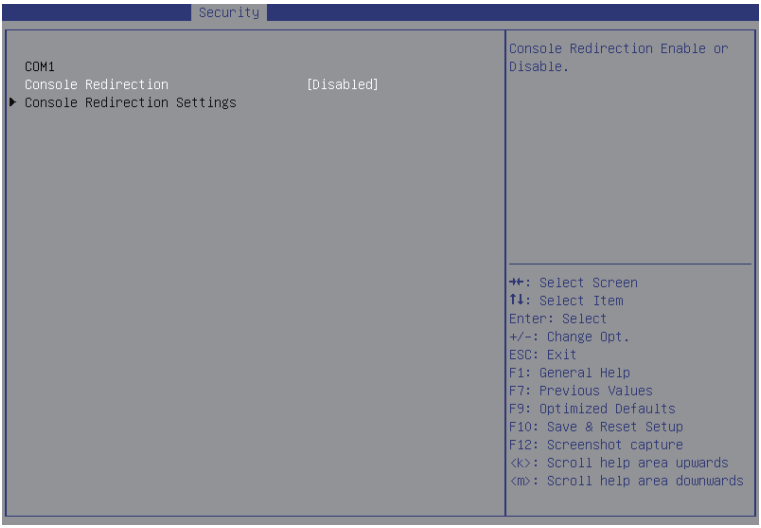
▸ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

▸ 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

This option appears when Console Redirection is **enabled**.

» **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.

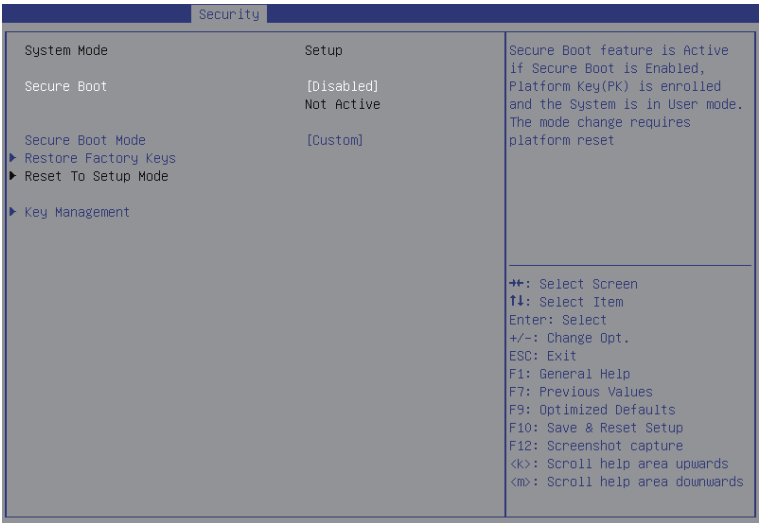
» **Recorder Mode, Resolution 100x31**

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

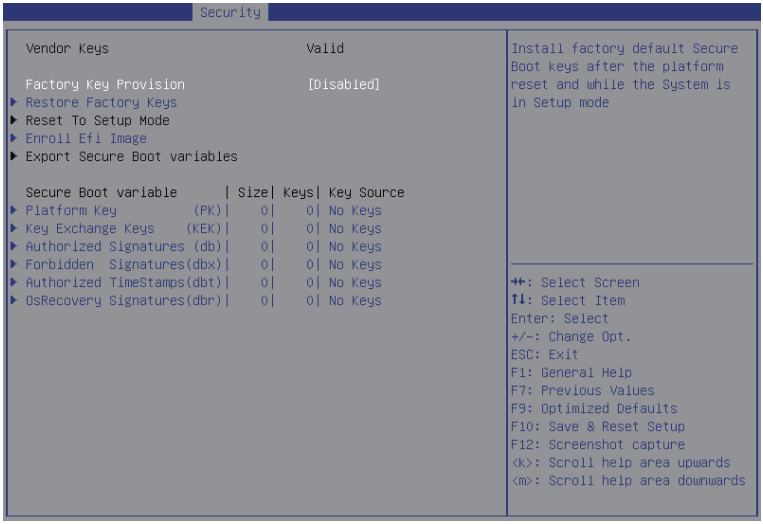
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▸ 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]**.



» **Platform Key (PK):**

The Platform Key (PK) can protect the firmware from any un-authenticated changes. The system will verify the PK before your system enters the OS. Platform Key (PK) is used for updating KEK.

» **Set New Key**

Sets a new PK to your system.

» **Delete Key**

Deletes the PK from your system.

» **Key Exchange Keys (KEK):**

Key Exchange Key (KEK) is used for updating DB or DBX.

» **Set New Key**

Sets a new KEK to your system.

» **Append Key**

Loads an additional KEK from storage devices to your system.

» **Delete Key**

Deletes the KEK from your system.

» **Authorized Signatures (db) :**

Authorized Signatures (db) lists the signatures that can be loaded.

» **Set New Key**

Sets a new db to your system.

» **Append Key**

Loads an additional db from storage devices to your system.

» **Delete Key**

Deletes the db from your system.

» **Forbidden Signatures (dbx):**

Forbidden Signatures (dbx) lists the forbidden signatures that are not trusted and cannot be loaded.

» **Set New Key**

Sets a new dbx to your system.

» **Append Key**

Loads an additional dbx from storage devices to your system.

» **Delete Key**

Deletes the dbx from your system.

» **Authorized TimeStamps (dbt):**

Authorized TimeStamps (dbt) lists the authentication signatures with authorization time stamps.

» **Set New Key**

Sets a new DBT to your system.

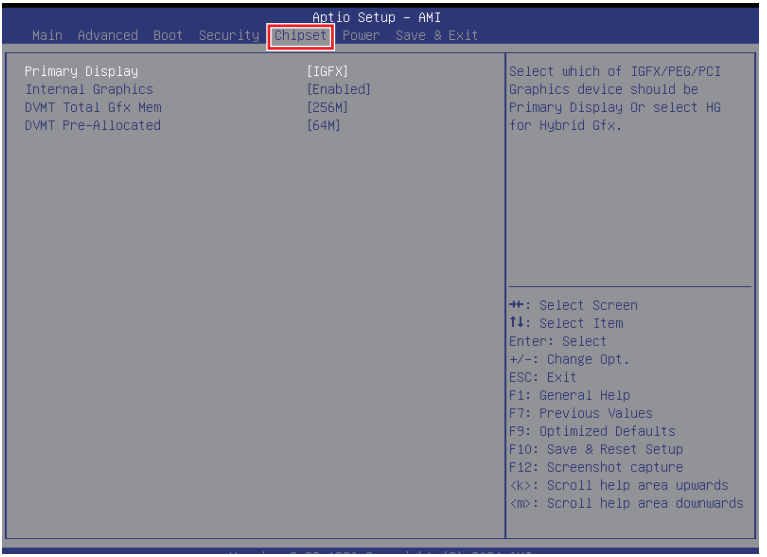
» **Append Key**

Loads an additional DBT from storage devices to your system.

» **OsRecovery Singnatures (dbr):**

Lists the available signatures for OS recovery.

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.

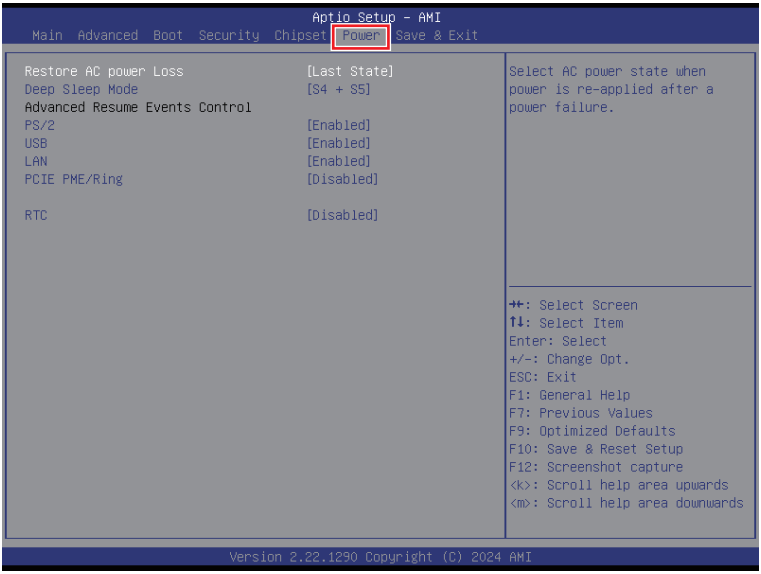
► DVMT Total Gfx Mem

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.

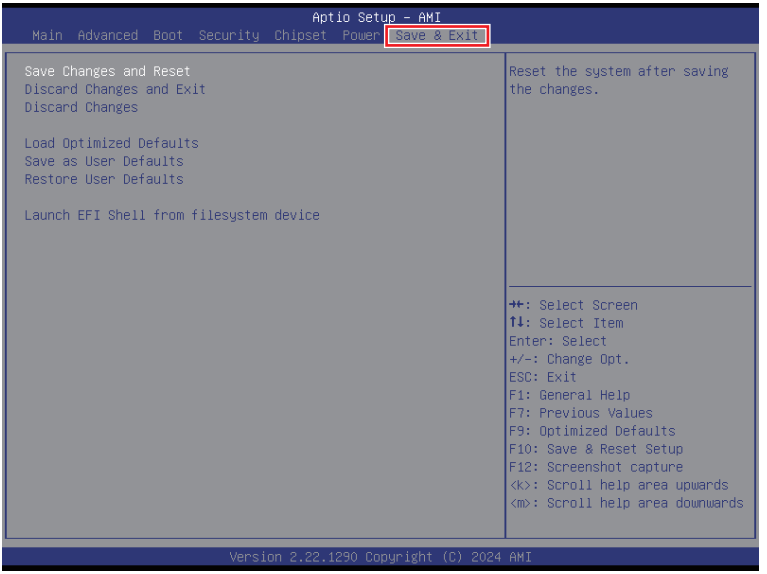
► PS/2, USB, LAN, PCIE PME

The setting allows the activity of the specified device to wake up the system from power saving modes.

► RTC

When [Enabled], your can set the date and time at which the RTC (real-time clock) alarm awakens the system from power saving modes.

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 SMBus Programming

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) and SMBus Access 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_GPI0	0x12	Bit 0	**N_GPO0**	0x21	Bit 0
N_GPI1	0x12	Bit 1	**N_GPO1**	0x21	Bit 1
N_GPI2	0x12	Bit 2	**N_GPO2**	0x21	Bit 2
N_GPI3	0x42	Bit 3	**N_GPO3**	0x21	Bit 3
N_GPI4	0x12	Bit 4	**N_GPO4**	0x21	Bit 4
N_GPI5	0x12	Bit 5	**N_GPO5**	0x21	Bit 5
N_GPI6	0x12	Bit 6	**N_GPO6**	0x21	Bit 6
N_GPI7	0x12	Bit 7	**N_GPO7**	0x21	Bit 7

Note: GPIO should be accessed through controller device **0x6E** on SMBus.
The associated access method in examples (**SMBus_ReadByte**, **SMBus_WriteByte**) are provided in part 3.

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 =SMBus_ReadByte (0x6E, 0x21);  // Read value from N_GPO0 port through SMBus.
val = val | (1<<0);                // Set N_GPO0address (bit 0) to 1 (output “high”).
SMBus_WriteByte (0x6E, 0x21, val); // Write back to N_GPO0 port through SMBus.
```

Example: Set **N_GPO1** output “low”

```
val = SMBus_ReadByte (0x6E, 0x21); // Read value from N_GPO1 port through SMBus..
val = val & (~(1<<1));             // Set N_GPO1 address (bit 1) to 0 (output “low”).
SMBus_WriteByte (0x6E, 0x21, val); // Write back to N_GPO1 port through SMBus.
```

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 = SMBus_ReadByte (0x6E, 0x12); // Read value from N_GPI2 port through SMBus.
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");
```

Example: Get **N_GPI3** input value.

```
val = SMBus_ReadByte (0x6E, 0x42); // Read value from N_GPI3 port through SMBus.
val = val & (1<<3);                // Read N_GPI3 address (bit 3).
if (val)    printf ("Input of  N_GPI3  is High");
else        printf ("Input of  N_GPI3  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
```

SMBus Access

3. SMBus Access

The base address of SMBus must know before access.
The relevant bus and device information are as following.

```
#define IO_SC               0xCF8
#define IO_DA               0xCFC
#define PCIBASEADDRESS      0x80000000
#define PCI_BUS_NUM         0
#define PCI_DEV_NUM         31
#define PCI_FUN_NUM         4
```

3.1 Get SMBus Base Address

```
int SMBUS_BASE;
int DATA_ADDR = PCIBASEADDRESS + (PCI_BUS_NUM<<16) +
                                 (PCI_DEV_NUM<<11) +
                                 (PCI_FUN_NUM<<8);

Outportl (DATA_ADDR + 0x20, IO_SC);
SMBUS_BASE = Inportl (IO_DA) & 0xfffffff0;
```

3.2 SMBus_ReadByte (char DEVID, char offset)

Read the value of OFFSET from SMBus device DEVID.

```
Outportb (LOWORD (SMBUS_BASE), 0xFE);
Outportb (LOWORD (SMBUS_BASE) + 0x04, DEVID + 1); //out Base + 04, (DEVID + 1)
Outportb (LOWORD (SMBUS_BASE) + 0x03, OFFSET);   //out Base + 03, OFFSET
Outportb (LOWORD (SMBUS_BASE) + 0x02, 0x48);     //out Base + 02, 48H
mdelay (20);                                     //delay 20ms to let data ready
while ((Inportl (SMBUS_BASE) & 0x01) != 0);      //wait SMBus ready
SMB_DATA = Inportb (LOWORD (SMBUS_BASE) + 0x05); //input Base + 05
```

3.3 SMBus_WriteByte (char DEVID, char offset, char DATA)

Write DATA to OFFSET on SMBus device DEVID.

```
Outportb (LOWORD (SMBUS_BASE), 0xFE);
Outportb (LOWORD (SMBUS_BASE) + 0x04, DEVID);    //out Base + 04, (DEVID)
Outportb (LOWORD (SMBUS_BASE) + 0x03, OFFSET);   //out Base + 03, OFFSET
Outportb (LOWORD (SMBUS_BASE) + 0x05, DATA);     //out Base + 05, DATA
Outportb (LOWORD (SMBUS_BASE) + 0x02, 0x48);     //out Base + 02, 48H
mdelay (20);                                     //wait 20ms
```