

USER'S MANUAL

CT-XRL02

Mini-ITX Industrial Motherboard
with LGA 1700 Socket supporting
12th/13th/14th Gen Intel® Intel
Alder Lake-S / Raptor Lake-S
i9/i7/i5/i3 Core® /Pentium®
/Celeron® IOTG Series Processors,
Q670E Chipset



Table of Contents

Prefaces	03
Regulatory Notices	03
Safety Information	05
Technical Support and Assistance	06
Conventions Used in this Manual	06
 Chapter 1 Product Introductions	 07
1.1 Product Description	08
Block Diagram.....	09
1.2 Specifications	10
 Chapter 2 Mechanical Specifications	 12
2.1 Switch and Connector Locations	13
2.2 Connector / Switch Definition	17
2.3 I/O Interface Descriptions	18
2.3.1 CPU Socket	18
2.3.2 Memory	20
2.3.3 Storage	21
2.3.4 M2_M1: M.2 Slot	22
2.3.5 Expansion Slots	23
2.3.6 Connectors	25
2.3.7 Other Connectors	26
2.3.8 Jumpers	34
 Chapter 3 System BIOS	 36
3.1 BIOS Introduction	37
3.2 The Menu Bar	39
3.3 Main	40
3.4 Advanced	41
3.5 Boot	49
3.6 Security	50
3.7 Secure Boot	65
3.8 Chipset	68
3.9 Power	69
3.10 Save & Exit	70
 Appendix GPIO WDT BKL Programming	 71
General Purpose IO	73
Watchdog Timer	75
SMBusAccess	76
CT-XRL02 Block Diagram.....	77

Prefaces

Revision

Revision	Description	Date
1.0	Initial release	2024/11/13

Regulatory Notices

● FCC - Class 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 in a residential installation. This equipment generates, uses and radiates radio frequency energy, and, if not installed and used in accordance with the instructions, 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 following measures:

- 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.

NOTE

- The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- Shield interface cables and AC power cord, if any, must be used to comply with the emission limits.



● FCC Conditions

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.
 - This device must accept any interference received, including interference that may cause undesired operation.
- CE Conformity



● 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.



● 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.



● Green Product Features

- Reduced energy consumption during use and stand-by
- Limited use of substances harmful to the environment and health
- Easily dismantled and recycled
- Reduced use of natural resources by encouraging recycling
- Extended product lifetime through easy upgrades
- Reduced solid waste production through take-back policy

Safety Information

- The components included in this package are prone to damage from electrostatic discharge (ESD). Please adhere to the following instructions to ensure successful computer assembly.
- Ensure that all components are securely connected. Loose connections may cause the computer to not recognize a component or fail to start.
- Hold the motherboard by the edges to avoid touching sensitive components.
- It is recommended to wear an electrostatic discharge (ESD) wrist strap when handling the motherboard to prevent electrostatic damage. If an ESD wrist strap is not available, discharge yourself of static electricity by touching another metal object before handling the motherboard.
- Store the motherboard in an electrostatic shielding container or on an anti-static pad whenever the motherboard is not installed.
- Before turning on the computer, ensure that there are no loose screws or metal components on the motherboard or anywhere within the computer case.
- Do not boot the computer before installation is completed. This could cause permanent damage to the components as well as injury to the user.
- If you need help during any installation step, please consult a certified computer technician.
- Always turn off the power supply and unplug the power cord from the power outlet before installing or removing any computer component.
- Keep this user guide for future reference.
- Keep this motherboard away from humidity.
- Make sure that your electrical outlet provides the same voltage as is indicated on the PSU, before connecting the PSU to the electrical outlet.
- Place the power cord such a way that people cannot step on it. Do not place anything over the power cord.
- All cautions and warnings on the motherboard should be noted.
- If any of the following situations arises, get the motherboard checked by service personnel:
 - Liquid has penetrated the computer.
 - The motherboard has been exposed to moisture.
 - The motherboard does not work well, or you cannot get it to work according to user guide.
 - The motherboard has been dropped and damaged.
 - The motherboard has obvious signs of breakage.
- Do not leave this motherboard in an environment above 60°C (140°F), it may damage the motherboard.

Technical Support and Assistance

1. Visit the C&T Solution Inc website at <https://www.candtsolution.com> where you can find the latest information about the product.
2. Contact your distributors, our technical support team or sales representative for technical support if you need additional assistance. Please have following information ready before you call:
 - Model name and serial number
 - Description of your peripheral attachments
 - Description of your software (operating system, version, application software, etc.)
 - A complete description of the problem
 - The exact wording of any error messages

Conventions Used in this Manual



WARNING

This indication alerts operators to an operation that, if not strictly observed, may result in severe injury.



CAUTION

This indication alerts operators to an operation that, if not strictly observed, may result in safety hazards to personnel or damage to equipment.



NOTE

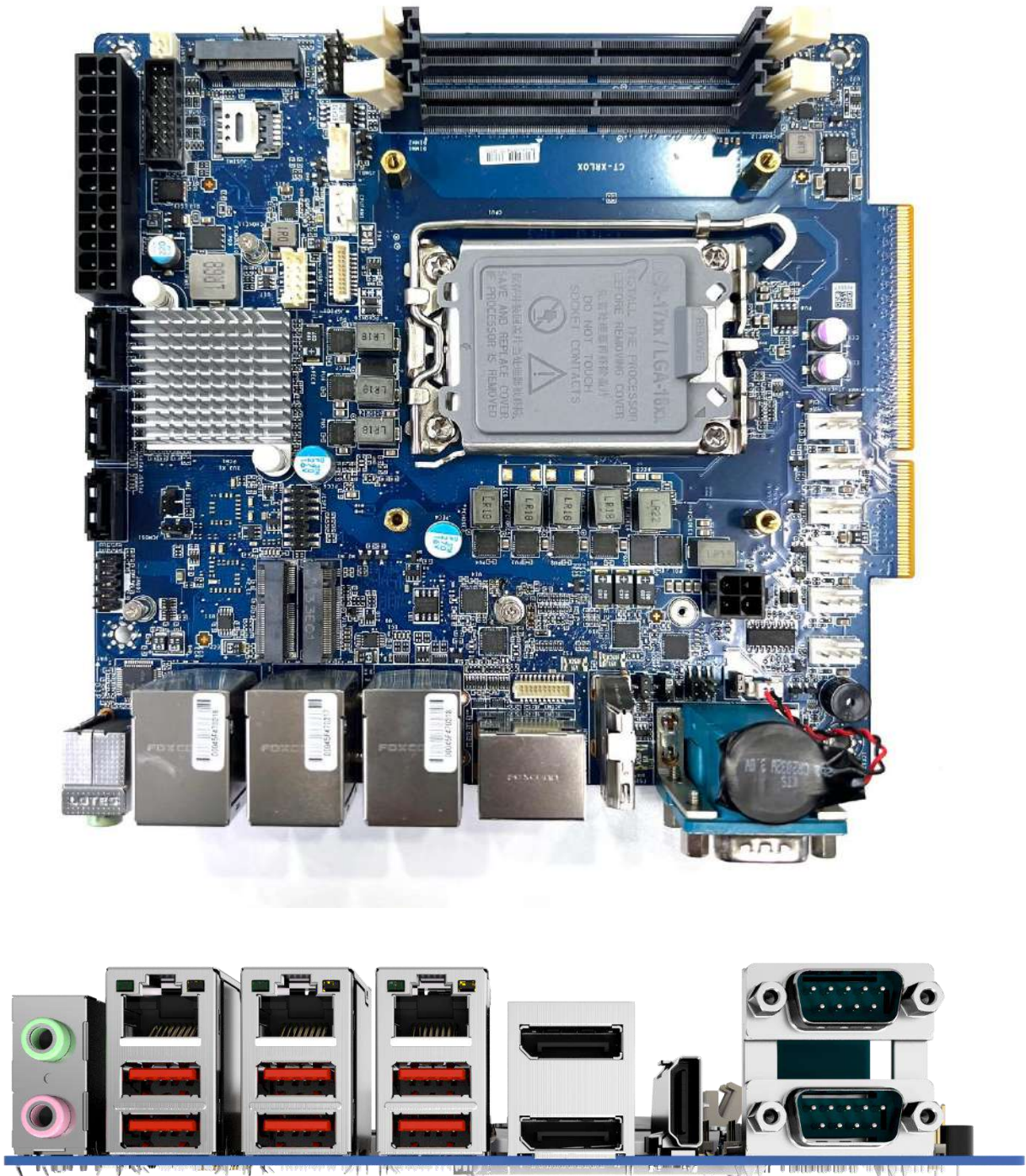
This indication provides additional information to complete a task easily.

Chapter 1

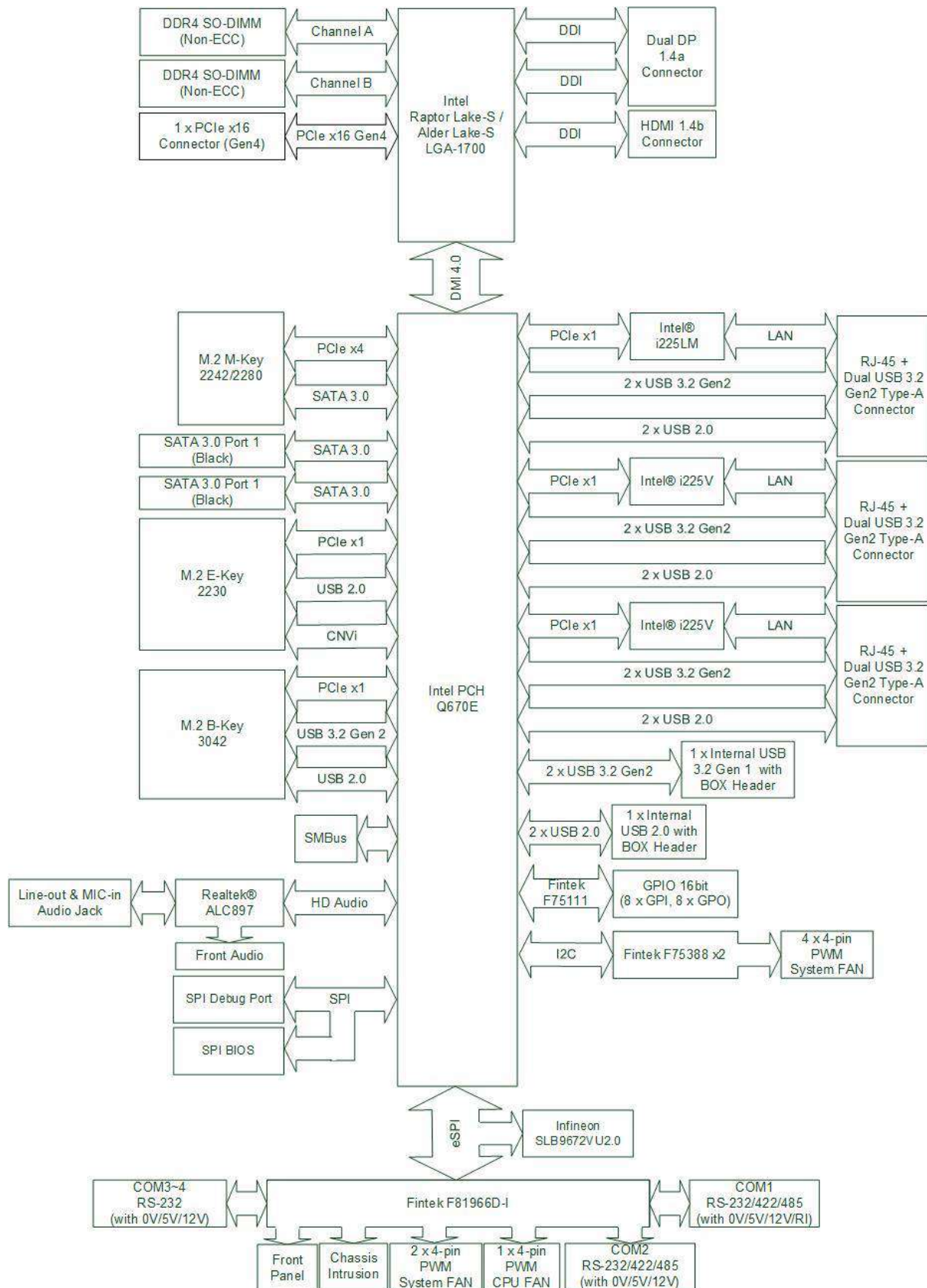
Product Introductions

1.1 Product Description

The CT-XRL02 Mini-ITX Industrial Motherboard with LGA 1700 Socket supporting 12th/13th/14th Gen Intel® Alder Lake-S/Raptor Lake-S i9/i7/i5/i3 Core®/Pentium®/ Celeron® IOTG Series Processors, Q670E Chipset



CT-XRL02 Block Diagram



1.2 Specifications

Form factor	Mini-ITX
Processor	13th/14th Gen Intel® Raptor Lake-S i9/i7/i5/i3 Core®/Pentium®/ Celeron® IOTG Series Processor, Max 65W 1.6 GHz~5.1 GHz (depends on CPU) - Socket LGA 1700 12th Gen Intel® Alder Lake-S i9/i7/i5/i3 Core®/Pentium®/ Celeron® IOTG Series Processor, Max 65W 1.6 GHz~5.1 GHz (depends on CPU) - Socket LGA 1700
Chipset	Intel® Q670E
System Memory	2 x DDR4 SO-DIMM slots (260-pin, vertical) - Up to 3200 MT/s - Up to 64GB - Dual-Channel DDR4, Non-ECC
Network	- GbE1: Intel I226LM PCIe 2.5GbE LAN PXE Support - GbE2: Intel I226V PCIe 2.5GbE LAN PXE Support - GbE3: Intel I226V PCIe 2.5GbE LAN PXE Support
Expansion Slots	1 x PCIe 4.0 x16 slot in 200-pin Gold fingers 1 x M.2 B Key slot (3042) - Supports PCIe x1, USB 3.2 Gen 1 & USB 2.0 signal - Support Nano SIM holder 1 x M.2 E Key slot (2230) - Supports PCIe x1 & USB 2.0 signal - Supports CNVi - Support Intel® AX210 Wi-Fi 6E & BT-5.1 (vPro Supported) 1 x Nano SIM Holder - Supported by M.2 B key (SIM) slot
Storage	3 x SATA 3.0 6Gb/s ports - Support RAID 0/1/5 - Support AHCI mode 1 x M.2 M Key slot (2242/ 2280) - Supports PCIe 3.0 x4 NVMe signal - Supports B+M Key module
Audio	- Realtek® ALC897 High-Definition Audio Codec - Co-lay Realtek® ALC888S-VD2
Graphics	2 x DP 1.4a up to 4096x2304 @60Hz 1 x HDMI™ 1.4b up to 4096x2304 @24Hz 3 independent display modes supported - DP1 - DP2 - HDMI

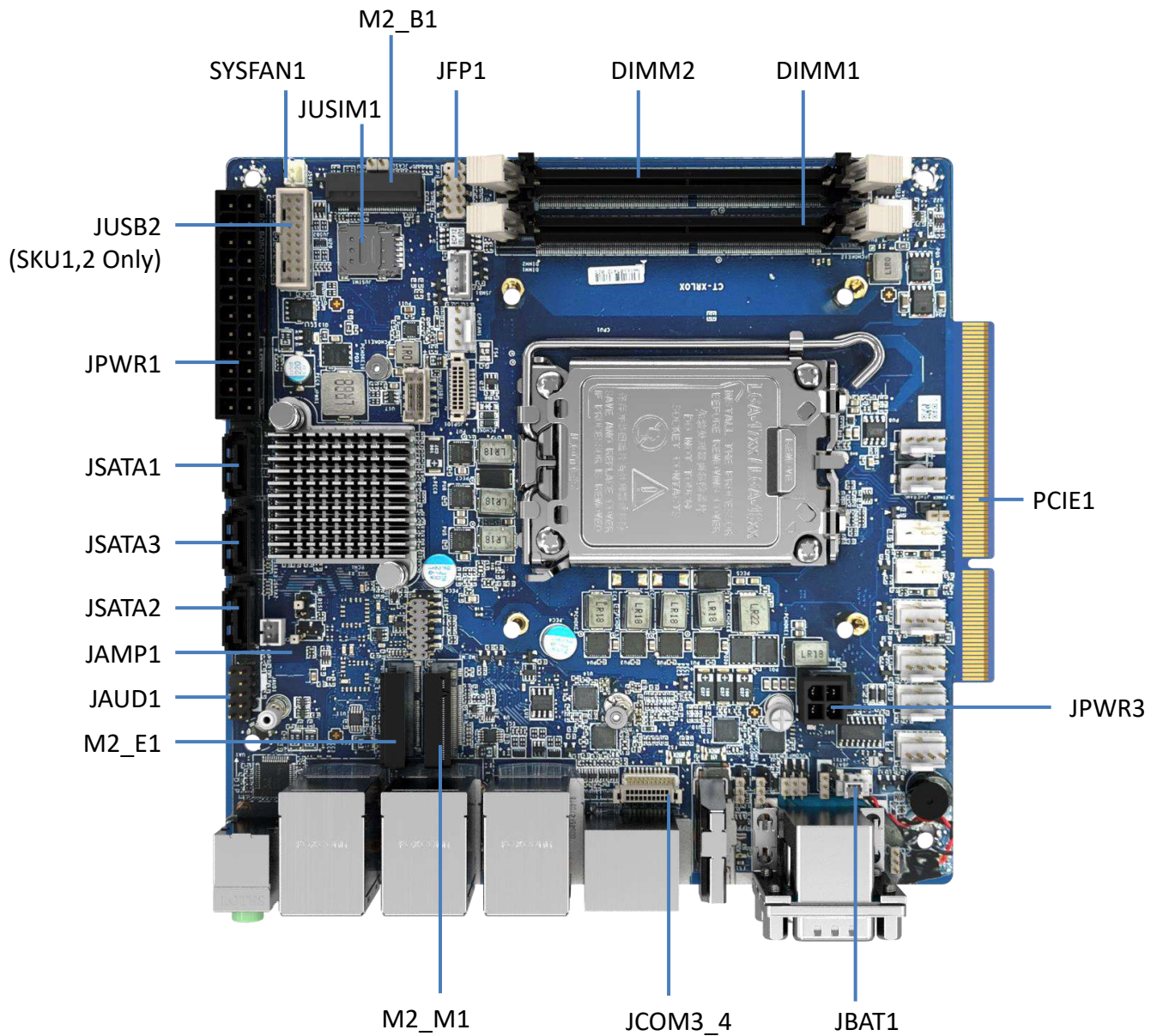
Power	• 1 x 24-pin ATX power connector • 1 x 4-pin 12V CPU power connector
Cooling	• 1 x 4-pin PWM CPU fan connector • 6 x 4-pin PWM system fan connectors
Rear I/O	• 1 x Line-out jack • 1 x Mic-in jack • 3 x 2.5 GbE RJ-45 LAN ports • 6 x USB 3.2 Gen2 Type-A ports (10 Gbps) • 2 x DisplayPort (1.4a) • 1 x HDMI connector (1.4b) • 2 x DB-9 RS-232/422/485 Serial ports - COM1: RI/0V/5V/12V, Auto-flow Control - COM2: 0V/5V/12V, Auto-flow Control
Onboard Connector	• 1 x ATX power connector (12-pin) • 1 x 12V CPU power connector (4-pin) • 1 x Front audio header (Headphone & Mic-in) • 1 x CPU fan box header • 6 x System fan box header • 1 x Front panel connector • 1 x COM port box header • 1 x GPIO (DIO) connector • 1 x I2C box header • 1 x USB 2.0 box header (support two USB 2.0 Ports) • 1 x USB 3.2 Gen1 box header (support two USB 3.2 Gen1 Ports) • 1 x CMOS battery header • 4 x COM voltage select jumpers • 1 x Clear CMOS jumper • 1 x ME jumper • 1 x AT/ ATX mode select jumper • 1 x Chassis Intrusion jumper
OS Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC (64-bit) • Linux Ubuntu 20.04/22.04 LTSC (Pre-scan)
Certification	• CE, FCC Class A
Environment	• Operating Temperature: 0 ~ 60°C (Thermal Test w/ Airflow: 0.7m/s) • Storage Temperature: -20 ~ 80°C • Operating Humidity: 10 ~ 90%, non-condensing • Storage Humidity: 10 ~ 90%, non-condensing
Dimensions	• 170 x 170mm (6.7 x 6.7 inches)

Chapter 2

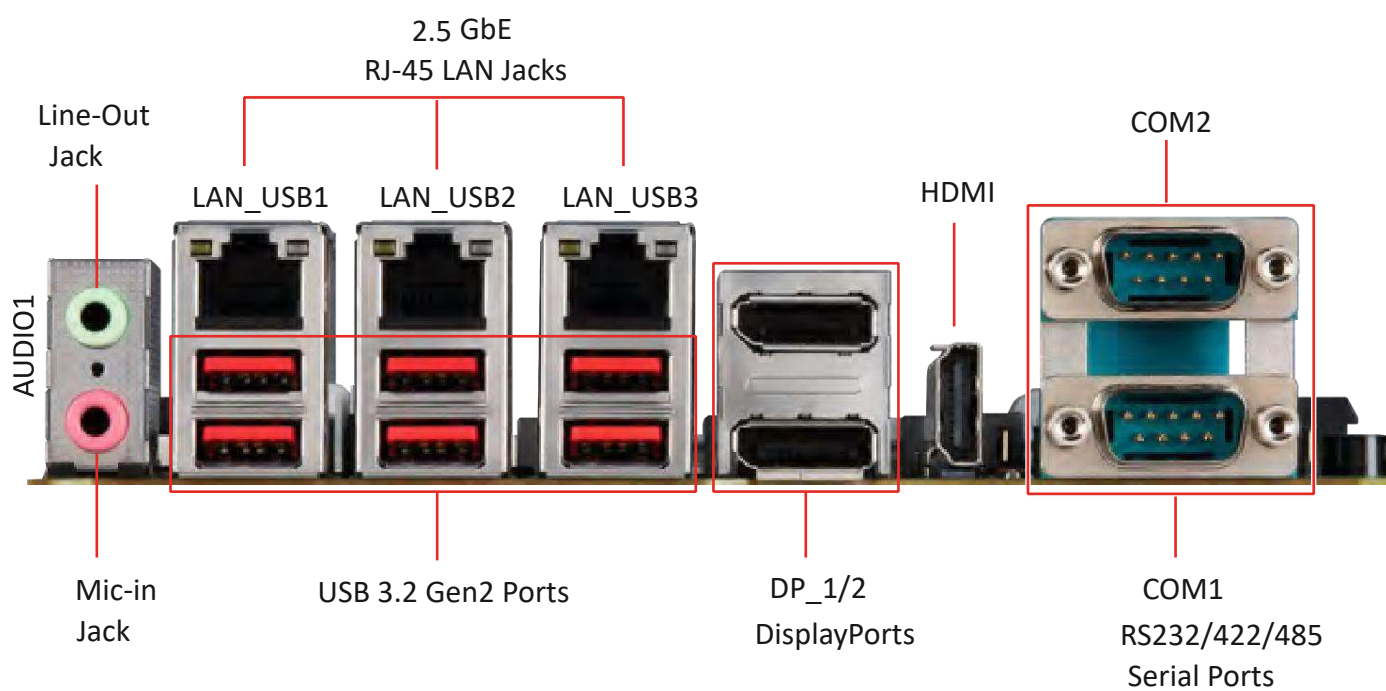
Mechanical Specifications

2.1 Switch and Connector Locations

Top View



Rear I/O Panel



- **Line-Out Jack**

This connector is provided for external headphones or speakers.

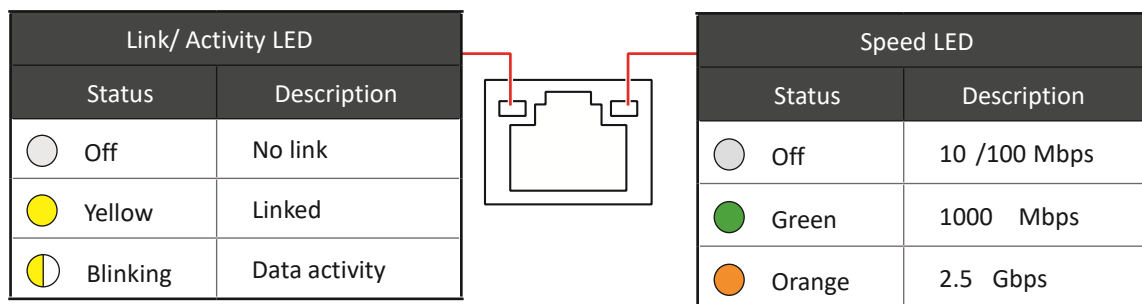
- **Mic-In Jack**

This connector is provided for external microphones.

- **2.5 GbE RJ-45 LAN Jacks**

Three standard single RJ45 LAN jacks are provided for connections to the Local Area Network (LAN).

You can connect network cables to them.



- **USB 3.2 Gen2 Port**

USB 3.2 Gen2, the SuperSpeed USB 10Gbps, delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

- **USB 3.2 Gen1 Port**

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 5Gbps.

- **USB 2.0 Port**

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

- **Important**

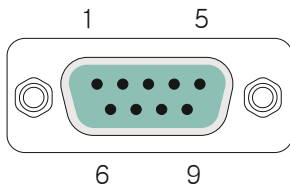
High-speed devices are recommended for USB 3.2 ports whereas low-speed devices, such as mouse or keyboard, are suggested to be plugged into the USB 2.0 ports.

- **DisplayPort**

DisplayPort is a digital display interface standard. These connectors are used to connect monitors with DisplayPort inputs.

- **RS232/422/485 Serial Port**

The serial port is a 16550A high speed communication port that sends/receives 16 bytes FIFOs. It supports barcode scanners, barcode printers, bill printers, credit card machine, etc.



RS232		
PIN	SIGNAL	DESCRIPTION
1	ND CD	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	Receive Data, Negative
5	RXD GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection
RS485		
PIN	SIGNAL	DESCRIPTION
1	TXD-	Transmit Data, Negative
2	NC	No Connection
3	TXD+	Transmit Data, Positive
4	NC	No Connection
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

2.2 Connector / Switch Definition

Component

2.2 CPU Socket

2.3 CPU & Heatsink Installation

2.4 Memory

- DIMM1~2: DDR4 SO DIMM Slots

2.5 Storage

- JSATA1: SATA 3.0 6Gb/s Ports
- M2_M1: M.2 Slot (M Key, 2242, 2280)

2.6 Expansion Slots

- PCIE1: PCIe Expansion Slots
- JUSIM1: Nano SIM Holder
- M2_E1: M.2 Slot (E Key, 2230)
- M2_B1: M.2 Slot (B Key, 3042)

2.7 Connectors

Power Connectors

- JPWR1: ATX 24-Pin Power Connector
- JPWR3: ATX 4-Pin 12V Power Connector

Audio Connectors

- JAUD1: Front Audio Header

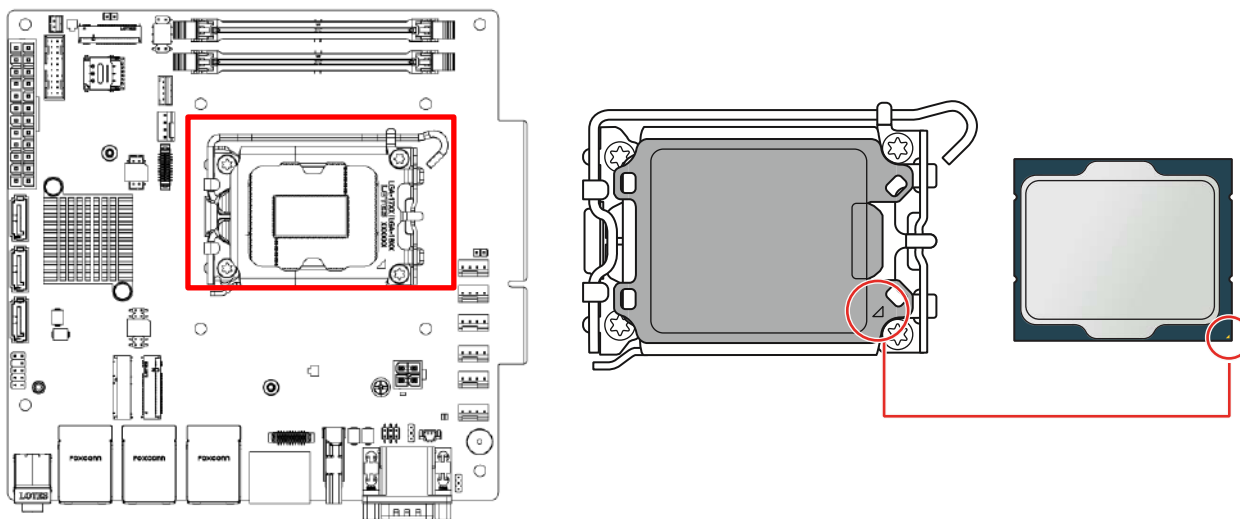
Other Connectors

- CPUFAN1, SYSFAN1: CPU/ System Fan Box Headers
- JFP1: Front Panel Connector
- JCOM3_4: COM Port Box Header
- JGPIO1: GPIO (DIO) Box Header
- JI2C1: I2C Box Header
- JUSB1: USB 2.0 Box Header
- JUSB2: USB 3.2 Gen 1 Box Header
- JBAT1: CMOS Battery Header

2.8 Jumpers

2.3 I/O Interface Descriptions

2.3.1 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**

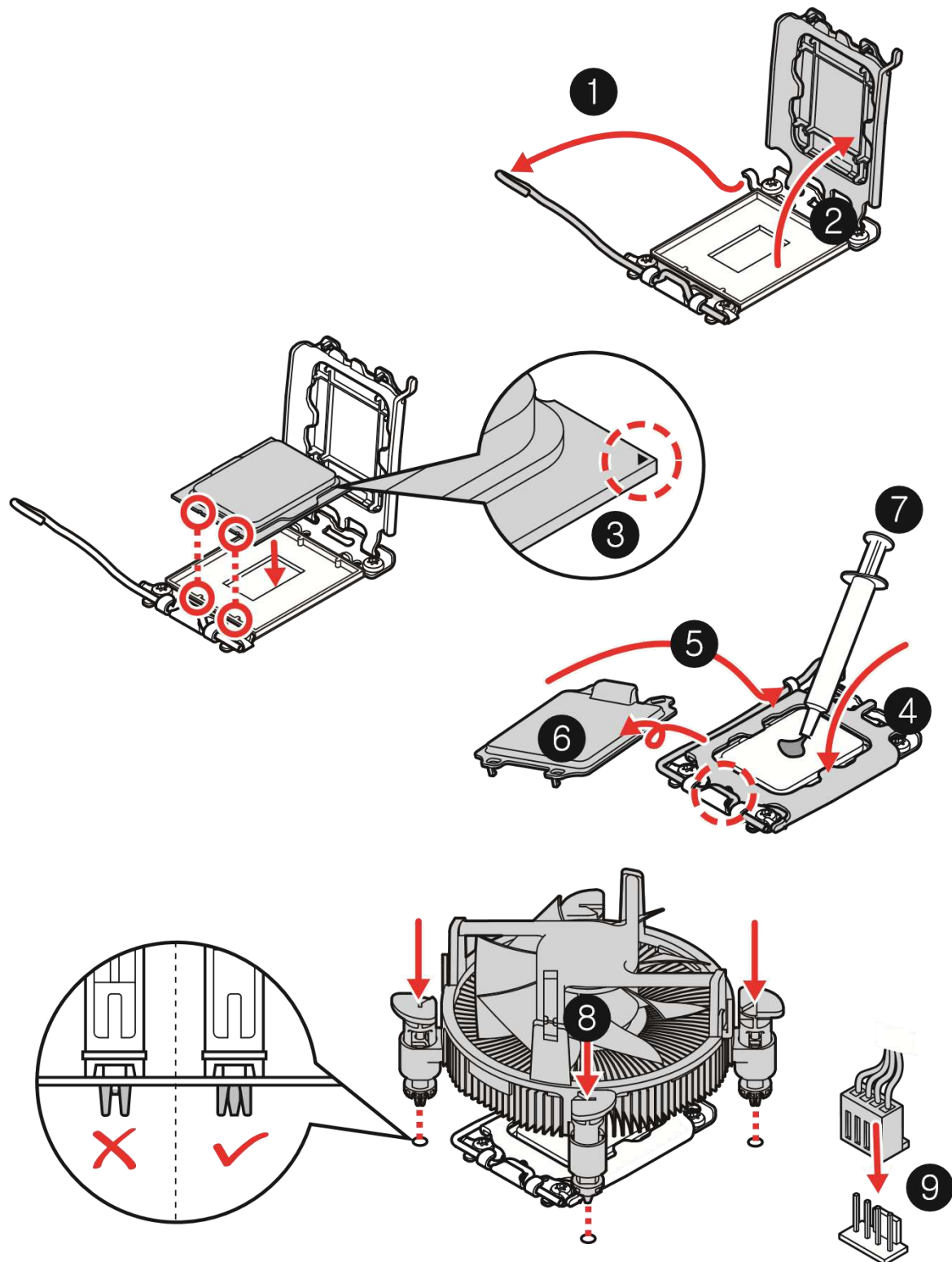
- Always unplug the power cord from the power outlet before installing or removing the CPU.
- When installing a CPU, always remember to install a CPU heatsink. A CPU heatsink is necessary to prevent overheating and maintain system stability.
- Confirm that the CPU heatsink has formed a tight seal with 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**

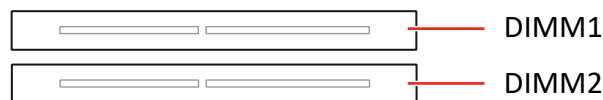
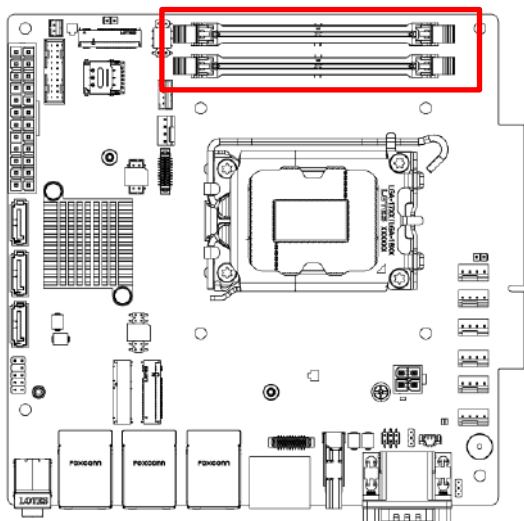
Use appropriate ground straps, gloves and ESD mats to protect yourself from electrostatic discharge (ESD) while installing the processor.

- **⚠ Important**

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



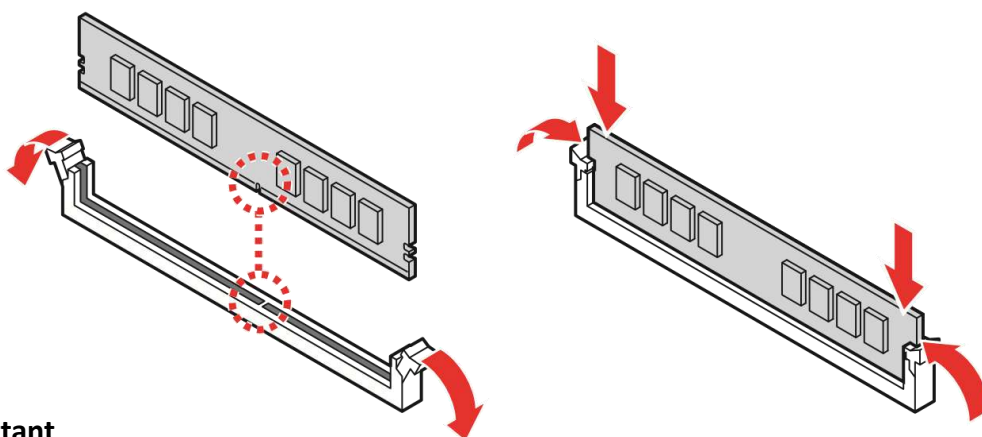
2.3.2 Memory



- **DIMM1~2: DDR4 SO DIMM Slots**

The SO-DIMM slots are intended for memory modules.

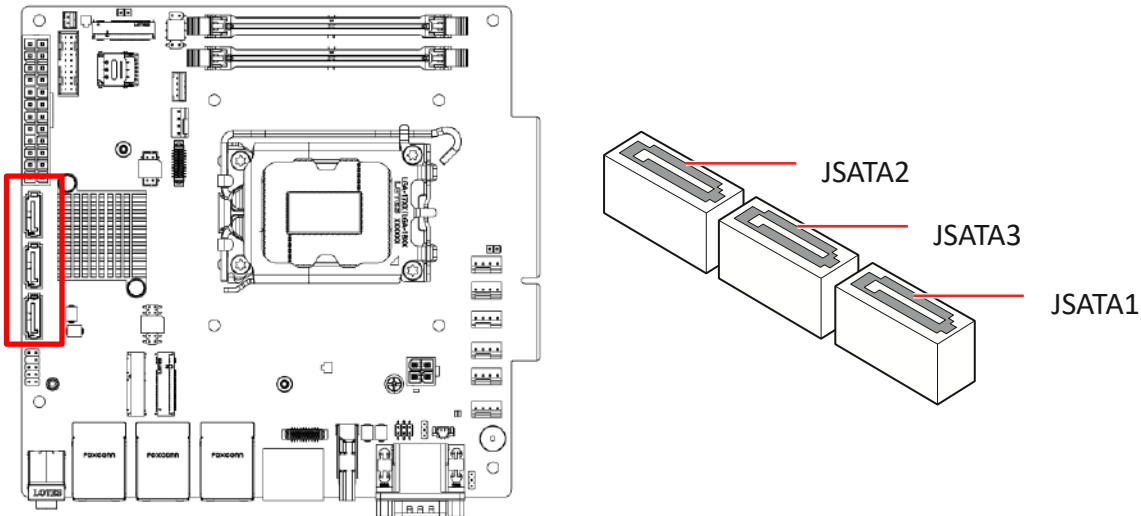
1. Open the side clips to unlock the DIMM slot.
2. Insert the DIMM vertically into the slot, ensuring that the off-center notch at the bottom aligns with the slot.
3. Push the DIMM firmly into the slot until it clicks and the side clips automatically close
4. Verify that the side clips have securely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



- **⚠ Important**

- 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.

2.3.3 Storage



- **JSATA1: SATA 3.0 6Gb/s Ports**

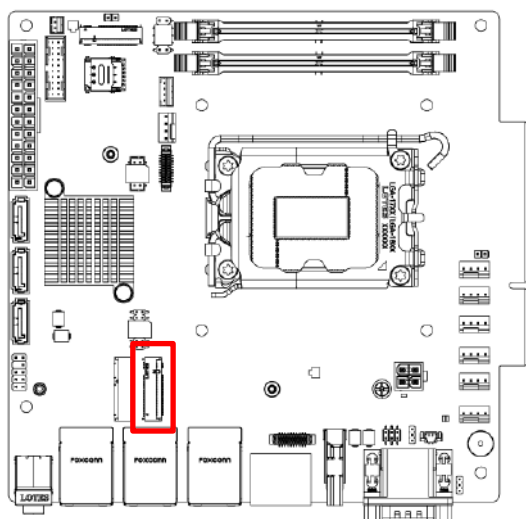
This connector is SATA 6Gb/s interface port, it can connect to one SATA device.

- **Important**

- This SATA port supports 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 side of the cable. However, it is recommended that the flat connector be connected to the motherboard for space saving purposes.

2.3.4 M2_M1: M.2 Slot (M Key, 2242, 2280)

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



M2_M1

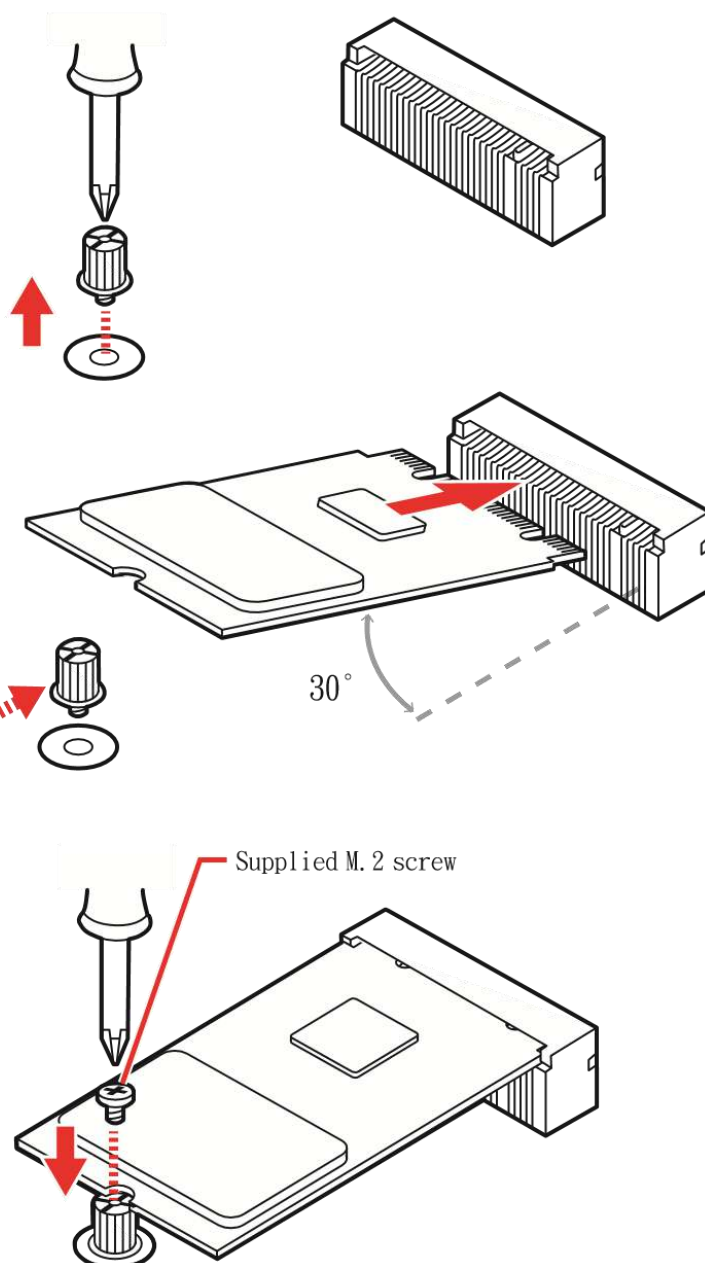
- **Video Demonstration**

Watch the video to learn how to Install M.2 SSD.

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

2. Set the M.2 riser screw at the appropriate location based on the length of your M.2 SSD.

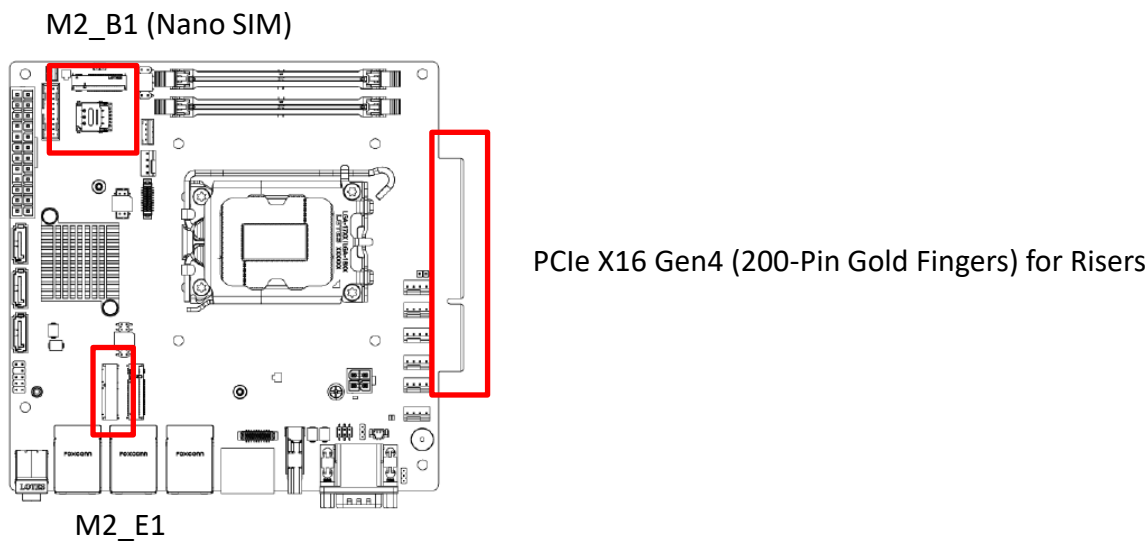
3. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



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

2.3.5 Expansion Slots

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

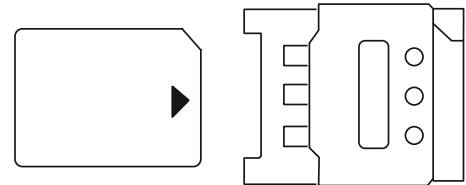


- **PCIE1: PCIe Expansion Slots**

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

- **JUSIM1: Nano SIM Holder**

This holder is provided for 3G, 4G LTE, 5G Nano SIM cards.

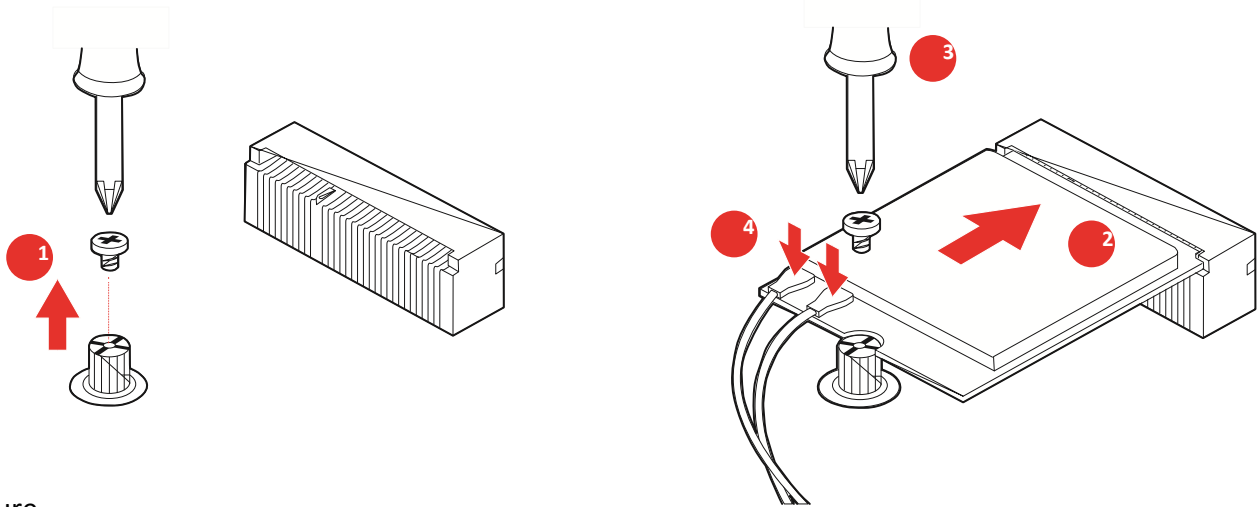


- **⚠ Important**

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.

- **M2_E1: M.2 Slot (E Key, 2230)**

Please install the Wi-Fi/ Bluetooth card into the M.2 slot as shown below.

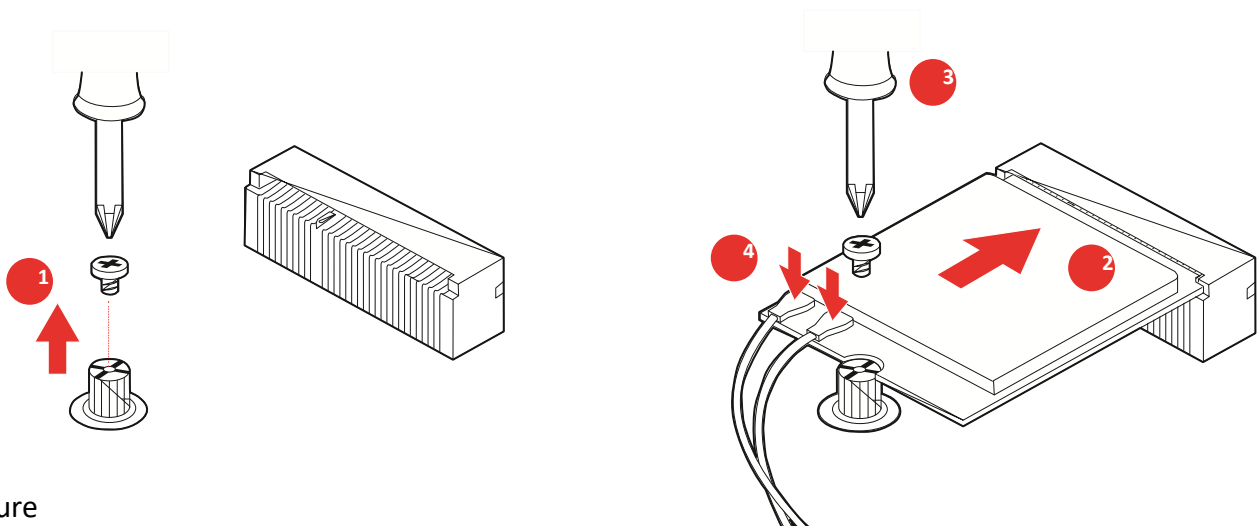


Feature

- Supports PCIe x 1 & USB 2.0 signal.
- Supports CNVi.

- **M2_B1: M.2 Slot (B Key, 3042)**

Please install supported cellular modules into the M.2 slot as shown below

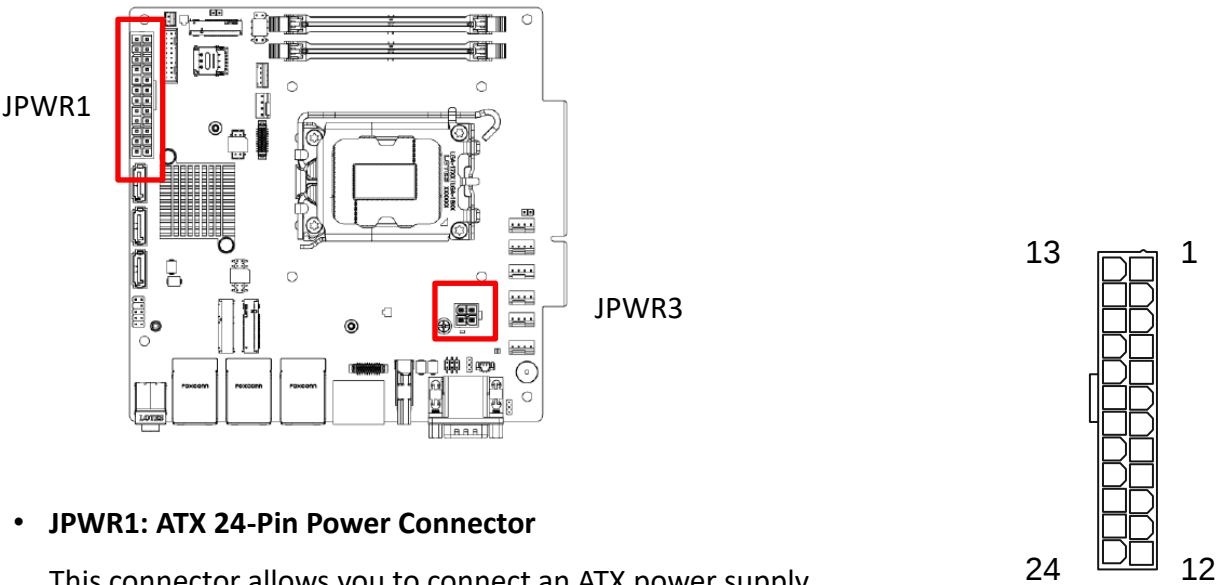


Feature

- Supports PCIe x 1, USB 3.2 Gen 2 x 1, USB 2.0 signal.
- Supports 3G, 4G LTE, 5G modules.

2.3.6 Connectors

Power Connectors



- JPWR1: ATX 24-Pin Power Connector**

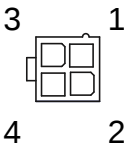
This connector allows you to connect an ATX power supply.

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

- JPWR3: ATX 4-Pin 12V Power Connector**

This connector is used to provide power to SATA devices.

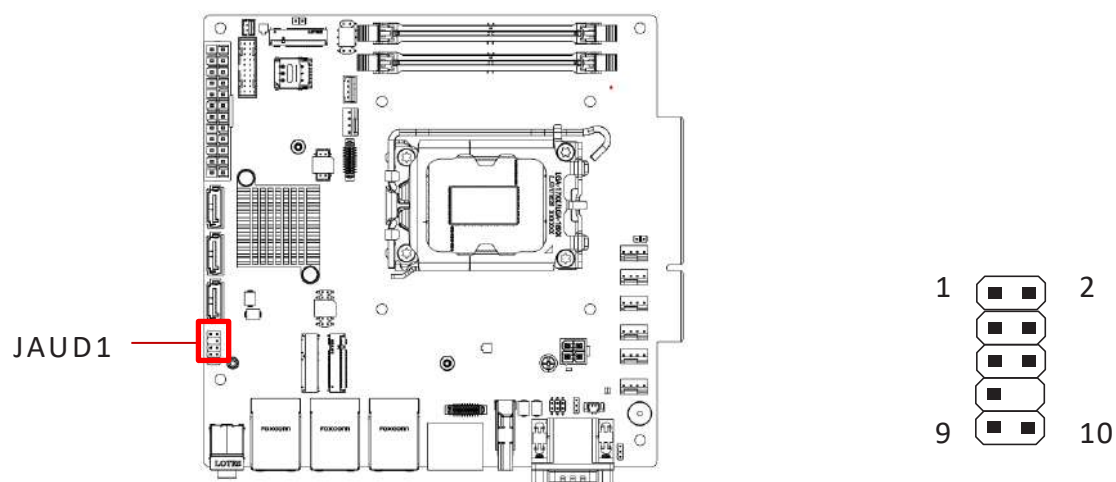
1	GND	2	GND
3	12V	4	12V



- ⚠ Important**

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

Audio Connectors

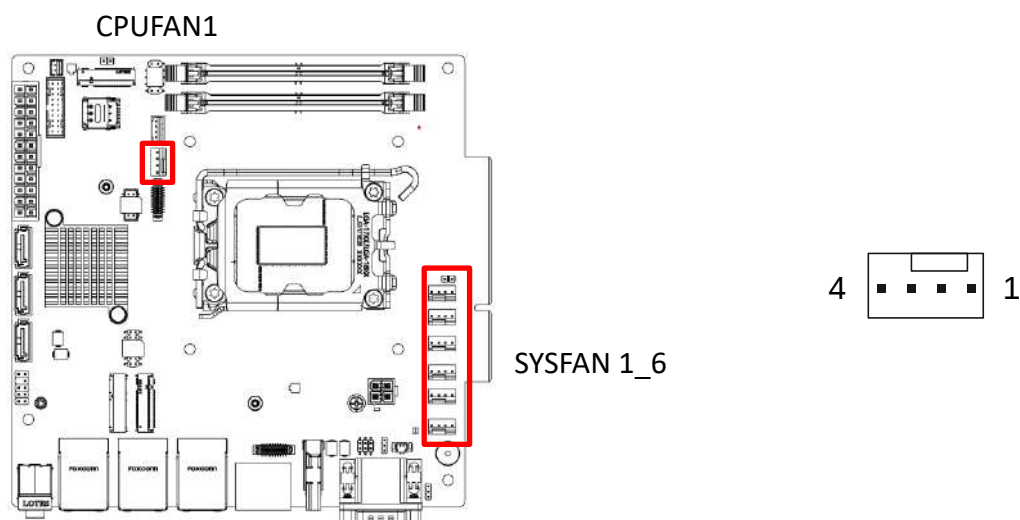


JAUD1: Front Audio Header

This connector allows you to connect front panel audio.

1	MIC_L	2	GND
3	MIC_R	4	PRESENCE#
5	F_OUTR	6	MIC2_JD
7	HPON	8	Nopin
9	F_OUTL	10	LIN2_JD

2.3.7 Other Connectors



- **CPUFAN1, SYSFAN1_6: CPU/ System Fan Box Headers**

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.

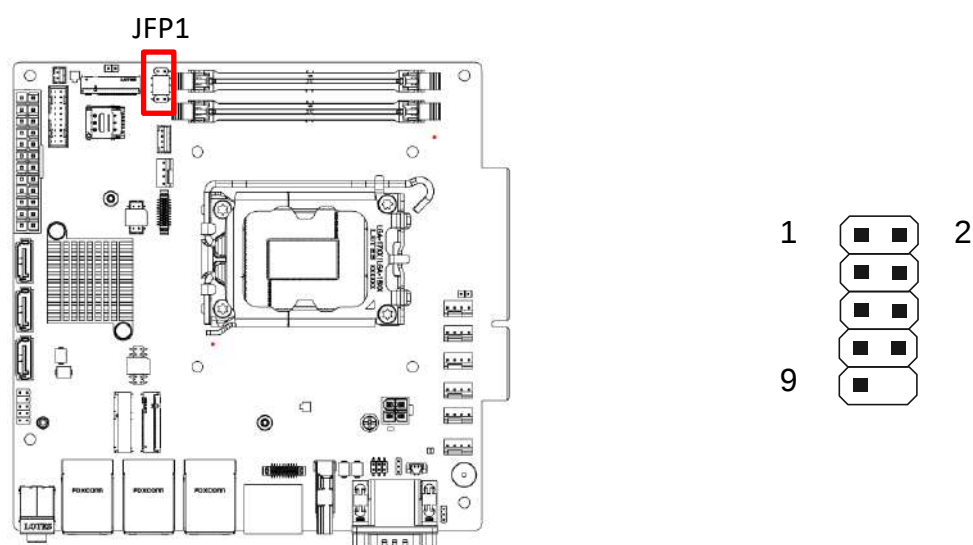
1	GND	2	FAN POWER
3	FAN SENSE	4	FAN_PWM

- **⚠ Important**

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

- **JFP1: Front Panel Connector**

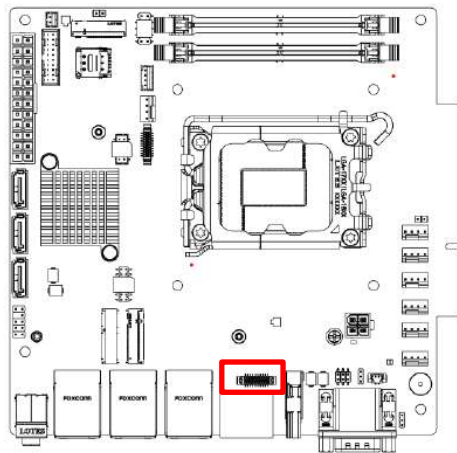
This front-panel connector is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.



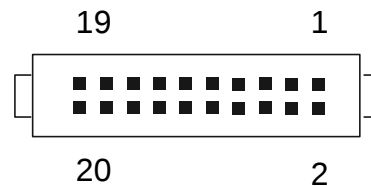
1	HDD LED+	2	POWER LED
3	HDD LED-	4	POWER LED
5	RESET SWITCH-	6	POWER SWITCH+
7	RESET SWITCH+	8	POWER SWITCH-
9	NC	10	No pin

- **JCOM3_4: COM Port Box Header**

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



JCOM3_4



1	ND3D3#	2	ND3D4#
3	NSIN3	4	NSIN4
5	NSOUT3	6	NSOUT4
7	NDTR3	8	NDTR4
9	GND	10	GND
11	NDSR3#	12	NDSR4#
13	NRTS3	14	NRTS4
15	NCTS3#	16	NCTS4#
17	VCC_COM3	18	VCC_COM4
19	NC	20	NC

- **Important**

After connect COM port box headers to printer, garbage can't be printed when power on/off.

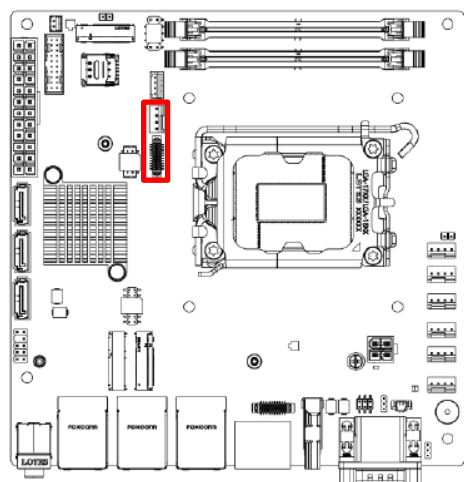
Feature

- Support True RS-232
- Support TTL RS-232
- Support Auto flow control
- RS- 422/ 485 support TR 1000+ Meter
- RS- 232/ 422/ 485, selection by BIOS control
SKU1/ SKU2
- COM1 Connector (Rear I/O)
Supports RS-232/ 422/ 485, With Ring/ 0V/ 5V/ 12V (Default set to Ring).
- COM2 (Rear I/O), JCOM3_4 Connector
Supports RS-232/ 422/ 485, With 0V/ 5V/ 12V (Default set to 5V).
- SKU3
COM1 Connector (Rear I/O)
- Supports RS-232/ 422/ 485, With Ring/ 0V/ 5V/ 12V (Default set to Ring).
COM2 Connector (Rear I/O)
- Supports RS-232/ 422/ 485, With 0V/ 5V/ 12V (Default set to 5V).
JCOM3_4 Connector
- Supports RS-232, With 0V/ 5V/ 12V (Default set to 5V)

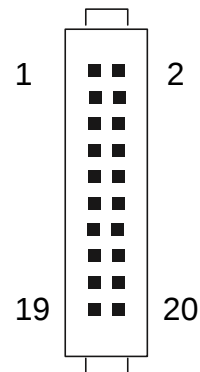
RS232		
PIN	SIGNAL	DESCRIPTION
1	ND CD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM	VCC_COM
RS422		
PIN	SIGNAL	DESCRIPTION
1	422 TXD-	Transmit Data, Negative
2	422 TXD+	Receive Data, Positive
3	422 RXD+	Transmit Data, Positive
4	422 RXD-	Receive Data, Negative
5	RXD GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection
RS485		
PIN	SIGNAL	DESCRIPTION
1	TXD-	Transmit Data, Negative
2	NC	No Connection
3	TXD+	Transmit Data, Positive
4	NC	No Connection
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

- **JGPIO1: GPIO (DIO) Box Header**

This connector is provided for the General-Purpose Input/Output (GPIO) peripheral module.



JI2C1
JGPIO1

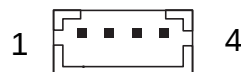


JGPIO1

1	GND	2	GND
3	N_GPO0	4	N_GPI0
5	N_GPO1	6	N_GPI1
7	N_GPO2	8	N_GPI2
9	N_GPO3	10	N_GPI3
11	N_GPO4	12	N_GPI4
13	N_GPO5	14	N_GPI5
15	N_GPO6	16	N_GPI6
17	N_GPO7	18	N_GPI7
19	VCC5	20	VCC5

- **JI2C1: I2C Box Header**

This connector is used to connect to the System Management Bus (SMBus).

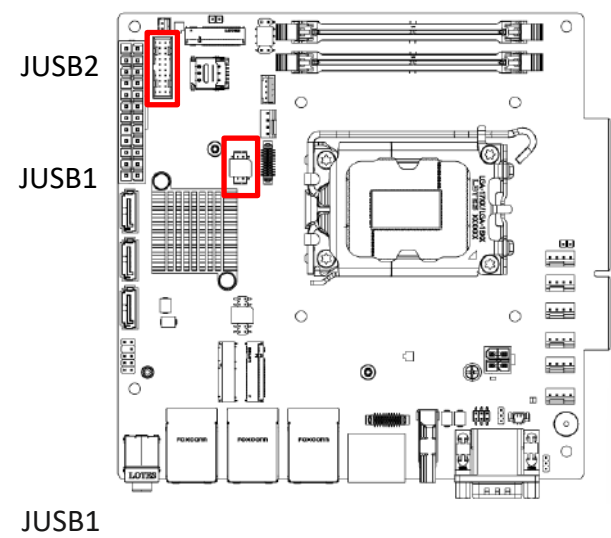


JI2C1

1	3VSB	2	I2C_CLK
3	I2C_DATA-	4	GND

• **JUSB1: USB 2.0 Box Header**

These connectors are ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices.



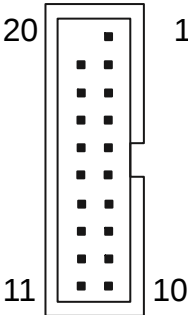
1	5V	2	5V
3	USB_D-	4	USB_D-
5	USB_D+	6	USB_D+
7	GND	8	GND
9	No pin	10	NC

• **JUSB2: USB 3.2 Gen1 Box Header**

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

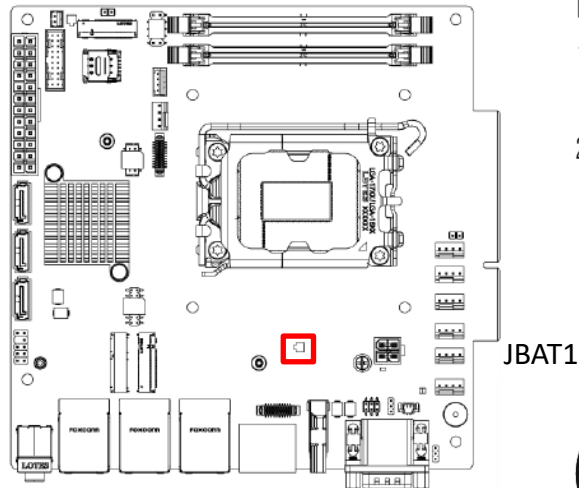
J12C1

1	5V	2	USB_3.2 RX-
3	USB_3.2 RX+	4	GND
5	USB_3.2 TX-	6	USB_3.2 TX+
7	GND	8	USB_D-
9	USB_D+	10	NC
11	USB_D+	12	USB_D-
13	GND	14	USB_3.2 TX+
15	USB_3.2 TX-	16	GND
17	USB_3.2 RX+	18	USB_3.2 RX-
19	5V	20	No Pin



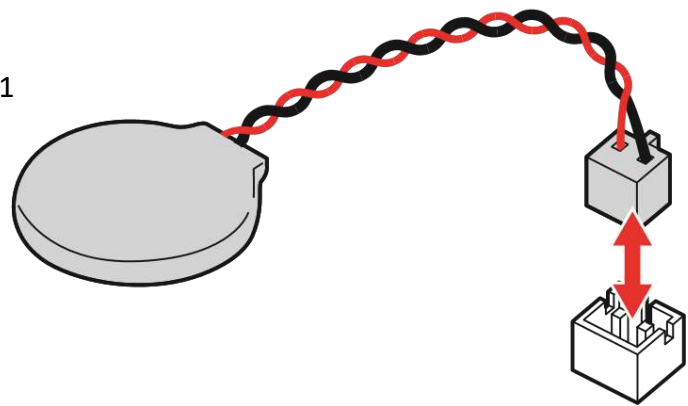
- **JBAT1: CMOS Battery Header**

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.



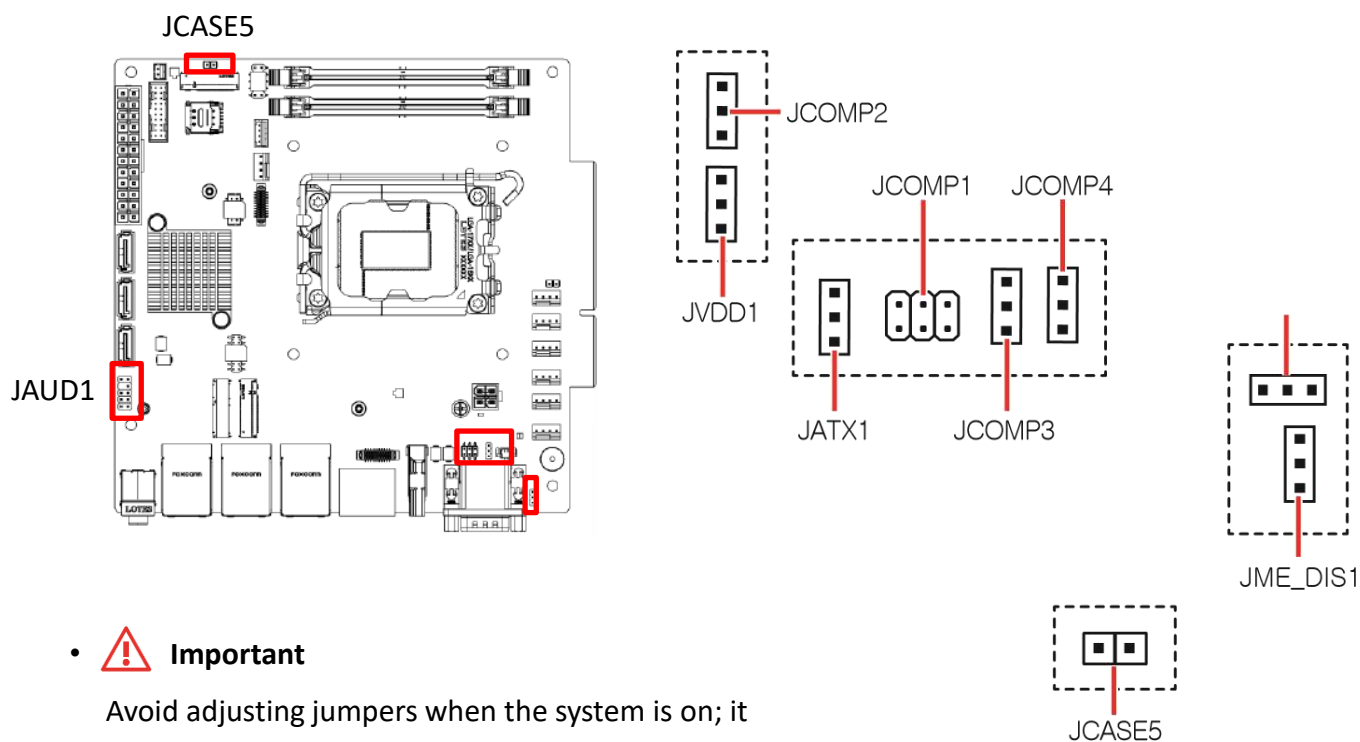
WARNING

KEEP OUT OF REACH OF CHILDREN

Swallowing can lead to chemical burns, perforation of soft tissue, can 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.

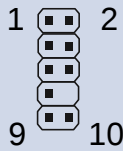
2.3.8 Jumpers



• **⚠ Important**

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

Jumper Name	Default Setting	Description
JCOMP1		COM Voltage Select Jumper
		1-2: 5V Power 3-4: 12V Power 5-6: NRI (Default)
JCOMP2		COM Voltage Select Jumper
JCOMP3		1-2: 5V Power (Default)
JCOMP4		2-3: 12V Power
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

Jumper Name	Default Setting	Description																				
JATX1	 1	AT/ ATX Mode Select Jumper																				
		1-2: ATX (Default) 2-3: AT																				
JVDD1	 1	LVDS Power Jumper																				
		1-2: 3.3V (Default) 2-3: 5V																				
JCASE5	 Normal (default)	Chassis Intrusion Jumper																				
		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.																				
JAUD1		<table><tr><td>1</td><td>MIC_L</td><td>2</td><td>GND</td></tr><tr><td>3</td><td>MIC_R</td><td>4</td><td>PRESENCE#</td></tr><tr><td>5</td><td>F_OUTR</td><td>6</td><td>MIC2_JD</td></tr><tr><td>7</td><td>HPON</td><td>8</td><td>Nopin</td></tr><tr><td>9</td><td>F_OUTL</td><td>10</td><td>LIN2_JD</td></tr></table>	1	MIC_L	2	GND	3	MIC_R	4	PRESENCE#	5	F_OUTR	6	MIC2_JD	7	HPON	8	Nopin	9	F_OUTL	10	LIN2_JD
1	MIC_L	2	GND																			
3	MIC_R	4	PRESENCE#																			
5	F_OUTR	6	MIC2_JD																			
7	HPON	8	Nopin																			
9	F_OUTL	10	LIN2_JD																			

Chapter 3

System BIOS

3.1 BIOS Introduction

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

BIOS Setup

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**

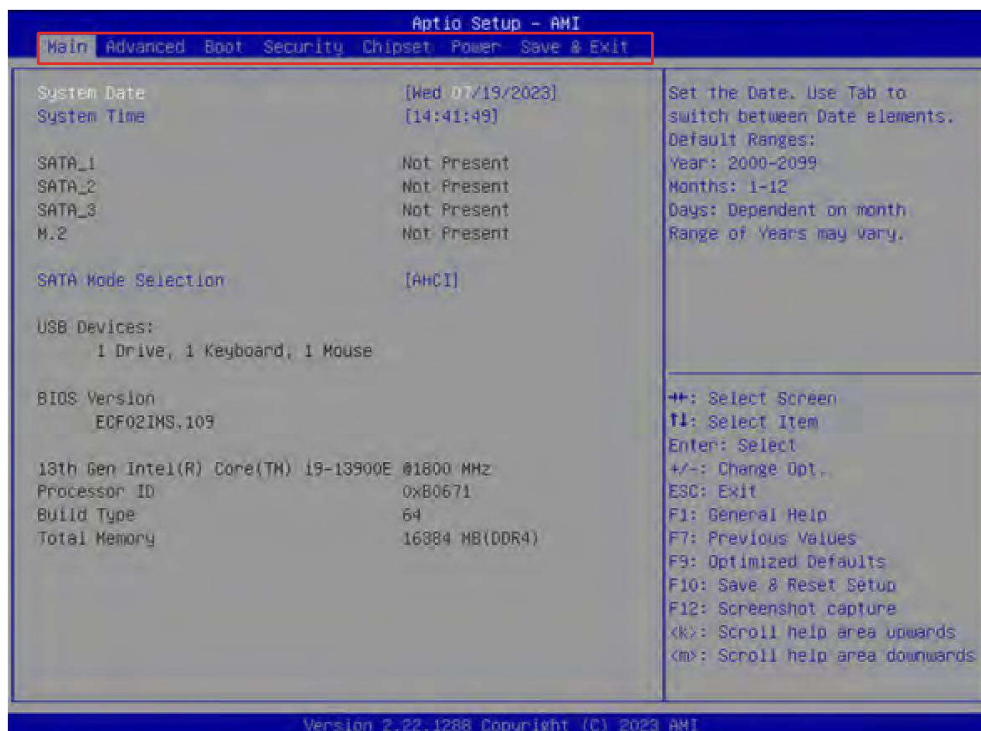
If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use arrow keys (↑↓) to highlight the field and press <Enter> to call up the sub-menu. Then you can use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

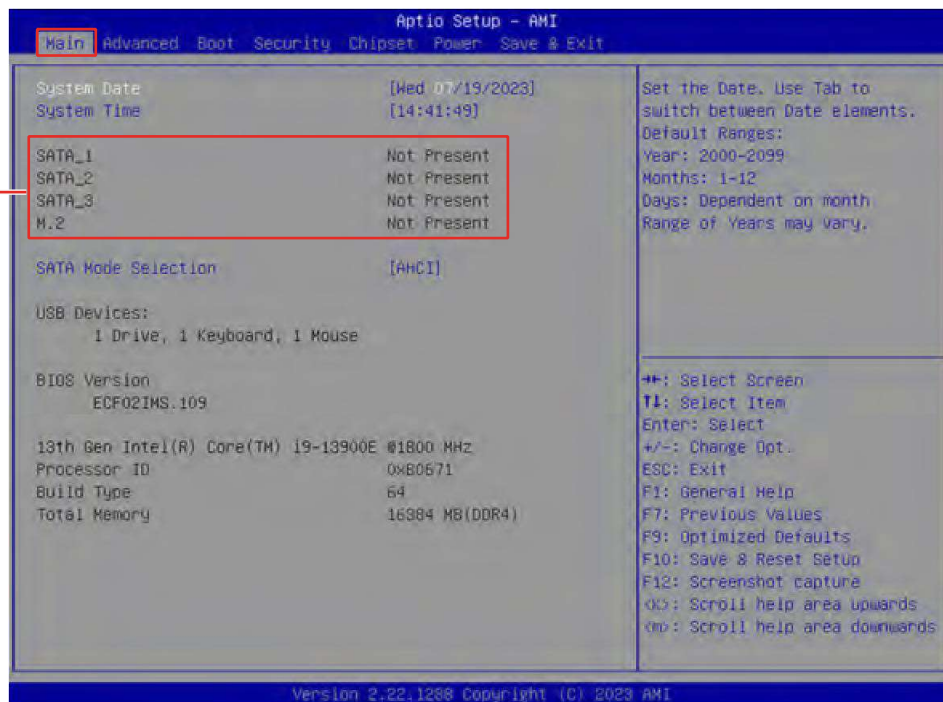
3.2 The Menu Bar

Press to enter BIOS CMOS Setup Utility. The Main setup screen is showed as following when the setup utility is entered. System Date/Time is set up in the Main Menu.



- **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.

3.3 Main



HDD Information

RAID (VMD) Disabled: Display HDD information as plugging in status.

RAID (VMD) Enabled: Display "Not Present" only.

■ 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

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.

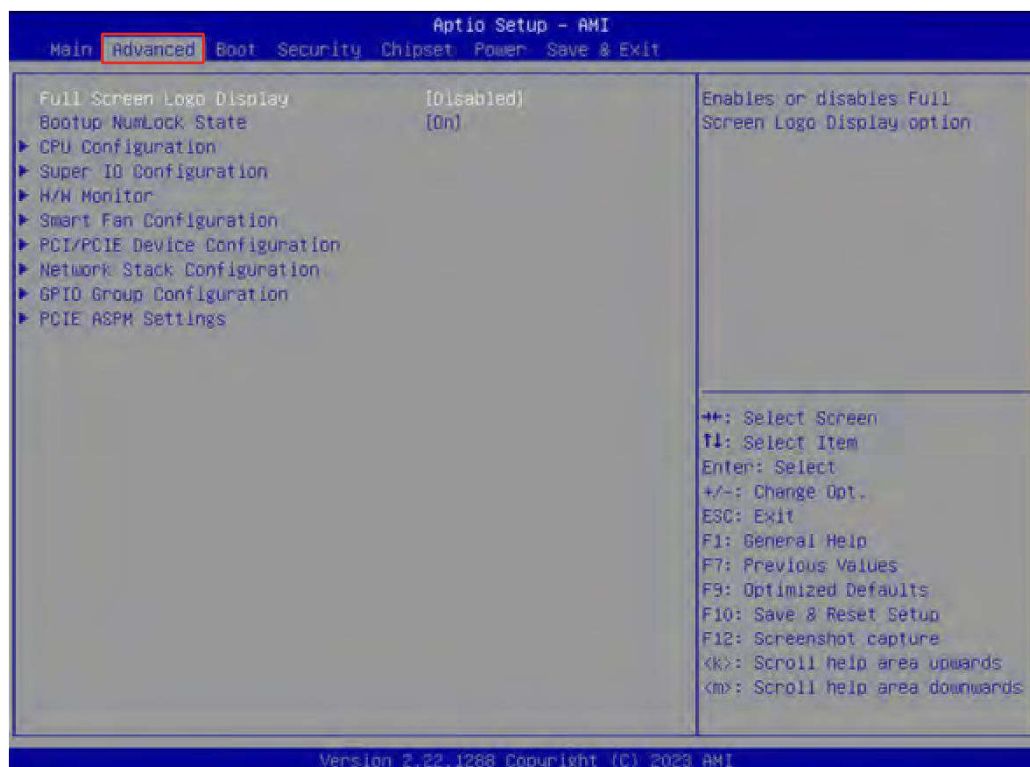
[RAID] RAID

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.

• Important

SKU3 (Intel® H610E) does not support M.2_2 (M.2 B Key) and SATA [RAID] mode.

3.4 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 enough time. Therefore, it is recommended to disable this BIOS feature for faster boot-up.

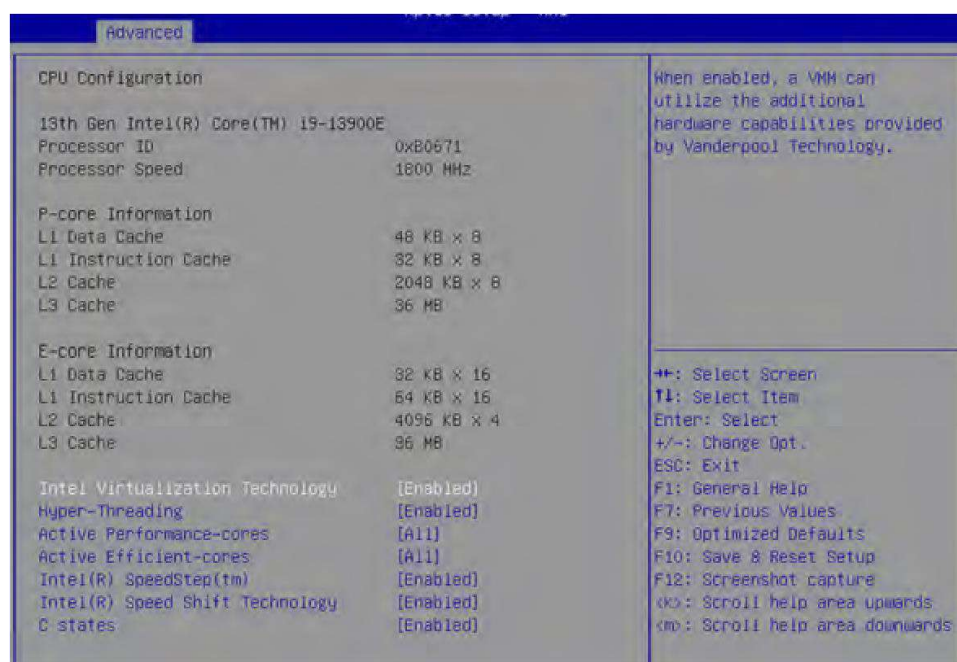
■ Bootup NumLock State

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 increase overall performance by allowing it to handle multiple threads simultaneously. If you disable the function, it will restrict 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] Disables this function

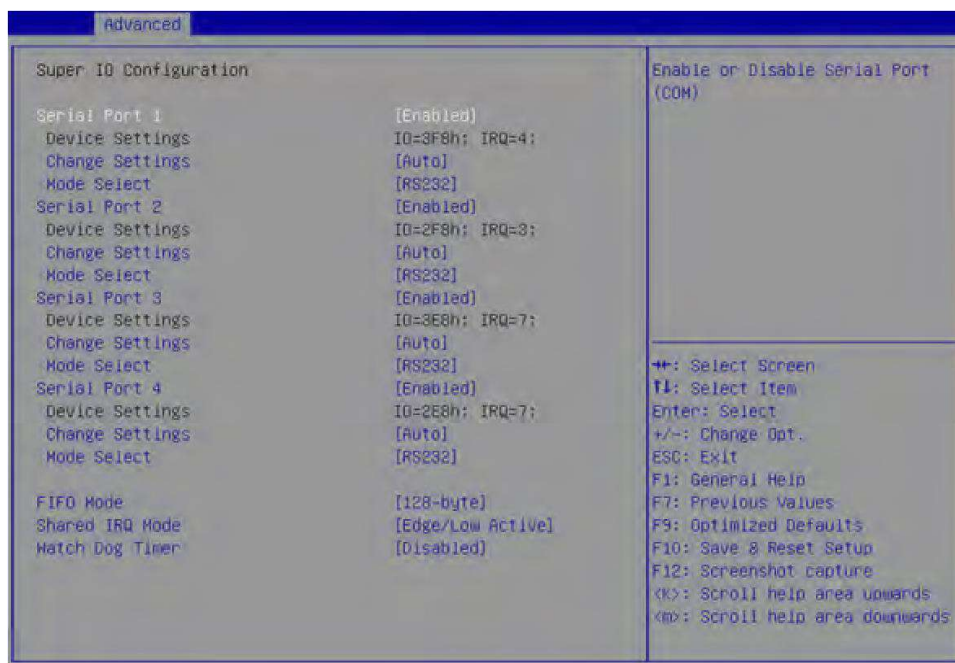
■ C States

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

This setting enables or disables the specified serial port.

» Change Settings

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

■ Shared IRQ Mode

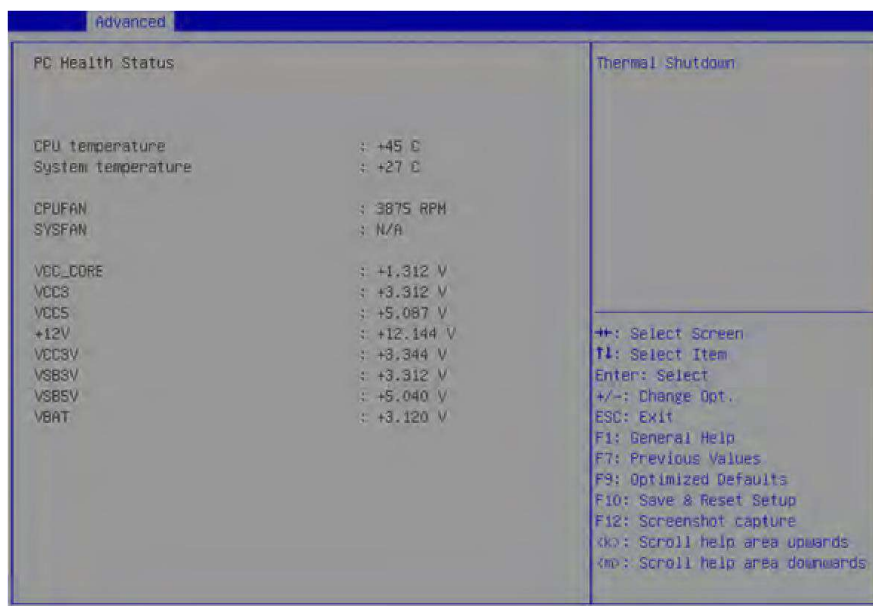
This setting provides the system with the ability to share interrupts among its serial ports.

■ 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.

H/W Monitor (PC Health Status)

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



■ 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



■ CPUFAN/ 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 CPUFAN/ SYSFAN is enabled.

PCI/PCIE Device Configuration

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

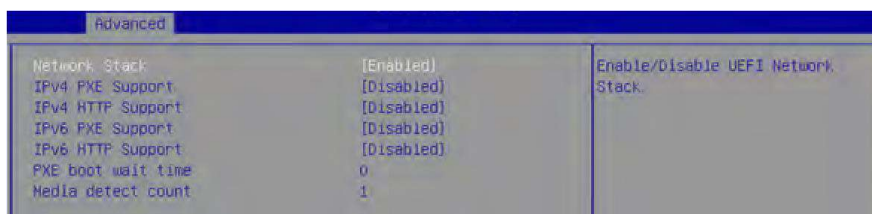


■ Audio Controller

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 Stack 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.

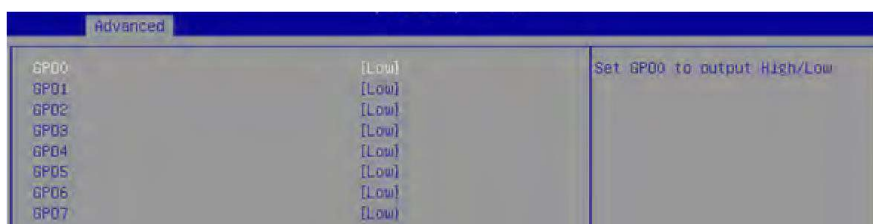
» PXE boot wait time

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

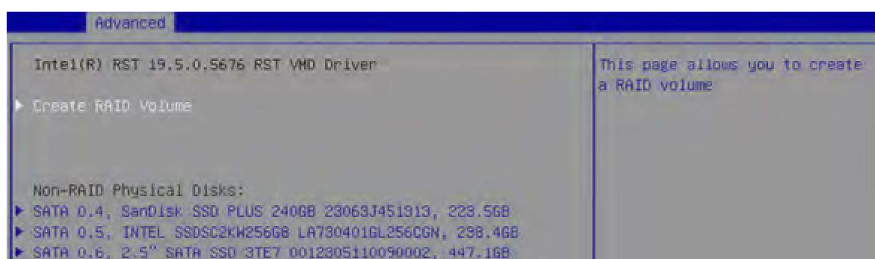


■ GPIO0 ~ GPIO7

These settings control the operation mode of the specified GPIO.

Intel(R) RST

Enables or disables Intel® RST. Intel® Rapid Storage Technology (Intel® RST) is a feature that combines the capabilities of both hardware and software to enhance storage performance, data protection, and flexibility.

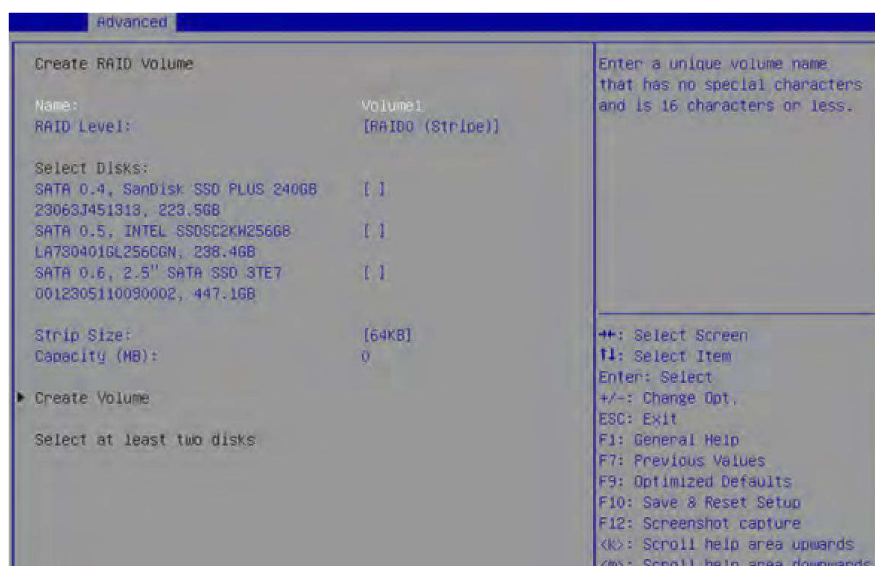


• Important

SKU3 (Intel® H610E) does not support "Intel(R) RST".

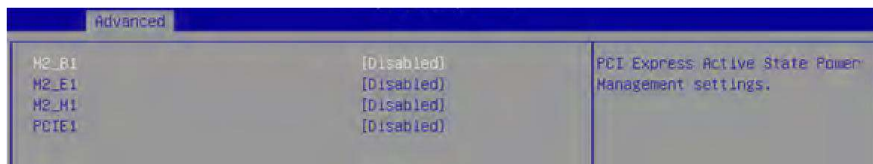
■ Create RAID Volume

This menu allows for the management of RAID volumes.



PCIe ASPM settings

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



■ M2_B1/ M2_E1/ M2_M1/ PCIE1

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. |

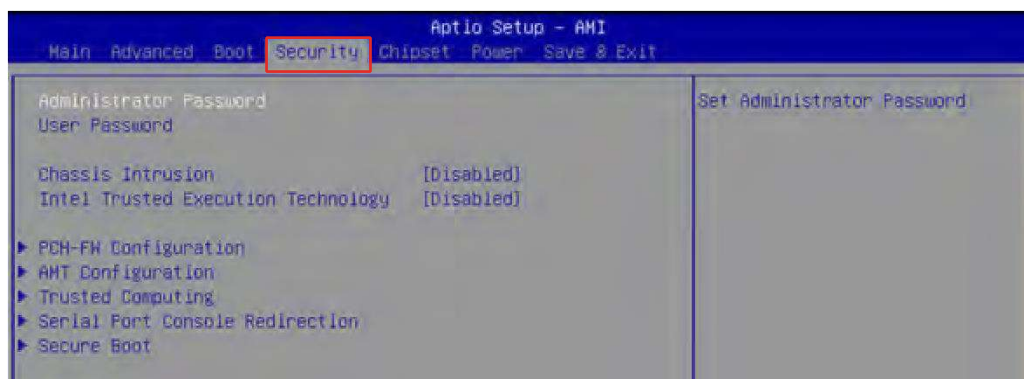
3.5 Boot



■ Boot Option #1-2

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

3.6 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

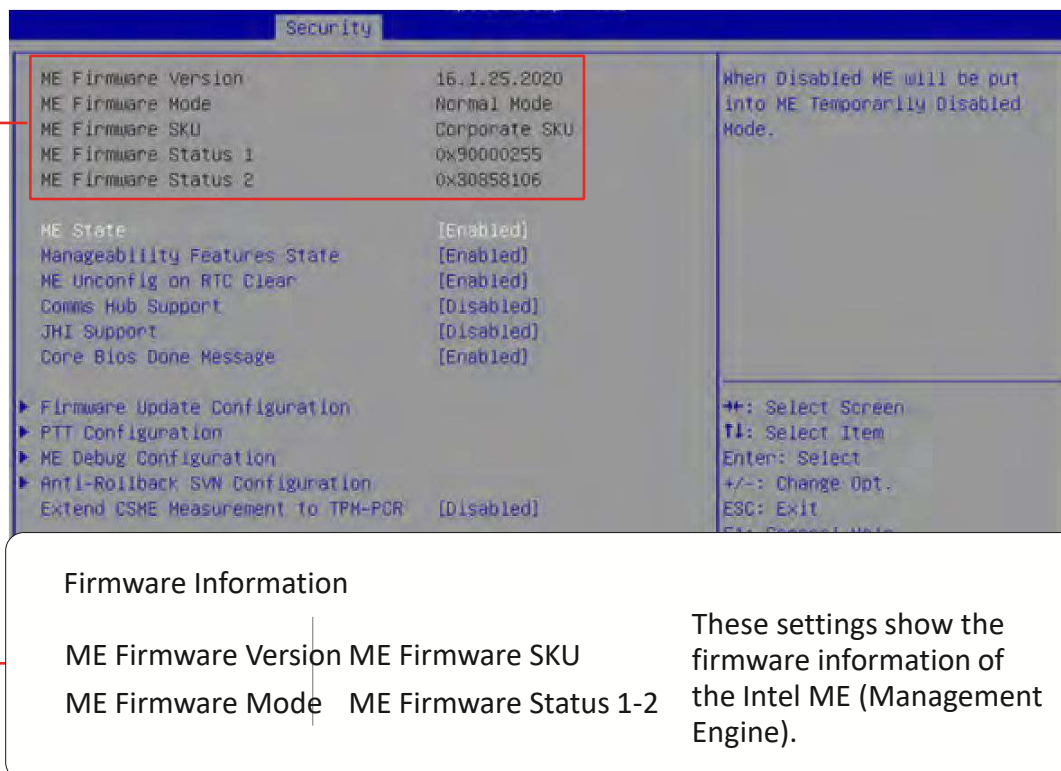
Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

• Important

- The following items must be enabled before “Intel Trusted Execution Technology” can be enabled:
 - All Intel processor cores
 - Hyper-threading
 - Intel Virtualization Technology
 - Trusted Platform Module (TPM)
 - Secure Boot
- SKU3 (Intel® H610E) does not support “Intel Trusted Execution Technology”.

PCH-FW Configuration

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



■ ME State

This menu controls the Intel® Management Engine State (ME state) parameters, which provides various management and security capabilities. The following items will be displayed 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

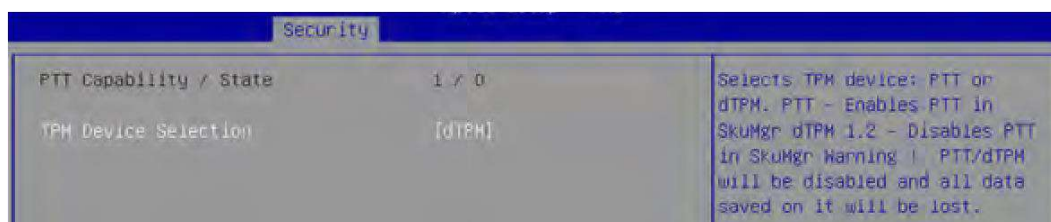
Enables or disables the ME Firmware Image Re-flashing.

» 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

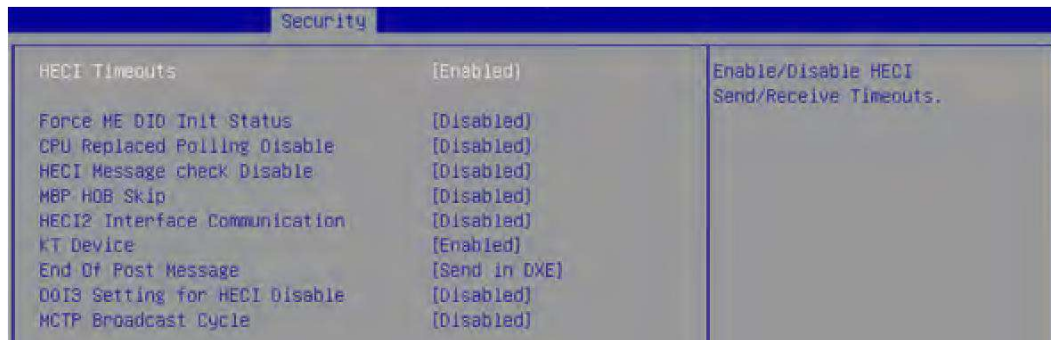
Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[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) 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.

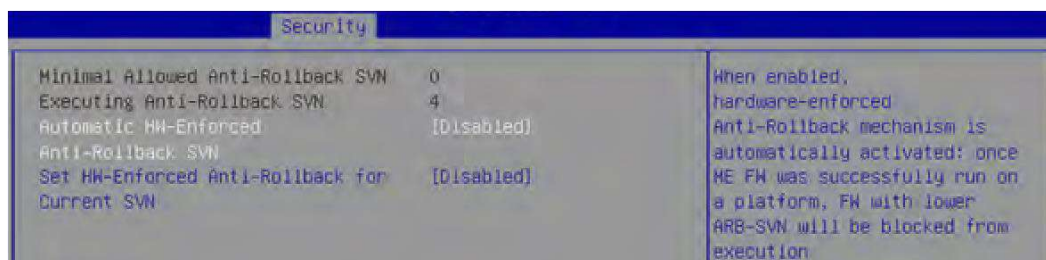
» DOI3 Setting for HECI Disable

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



» 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.

■ Extend CSME Measurement to TPM-PCR

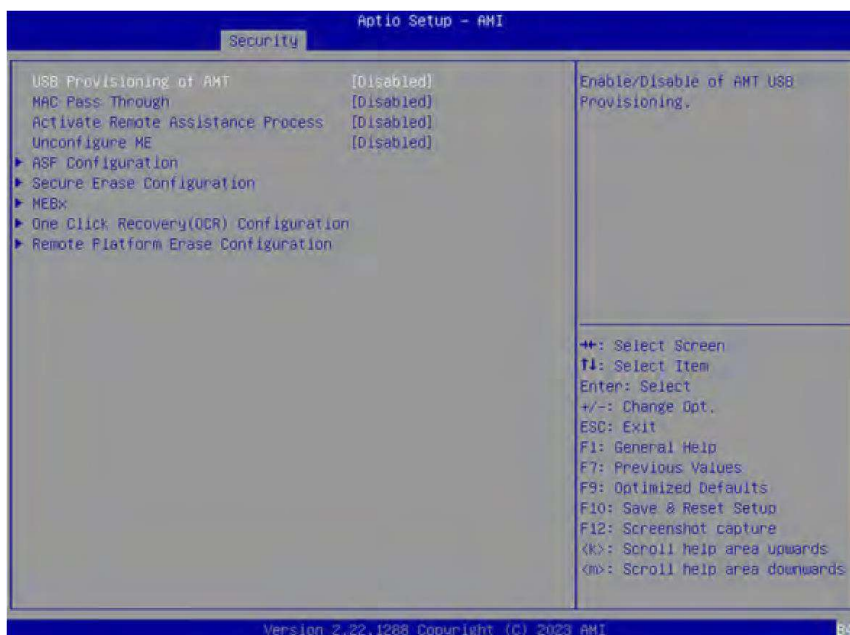
Enables or disables the Extend CSME Measurement to TPM-PCR. This item enables capturing and recording the Intel® Converged Security and Management Engine (Intel® CSME) firmware in the Trusted Platform Module Platform Configuration Registers (TPM-PCR). This enhances system security by protecting against unauthorized modifications.

• Important

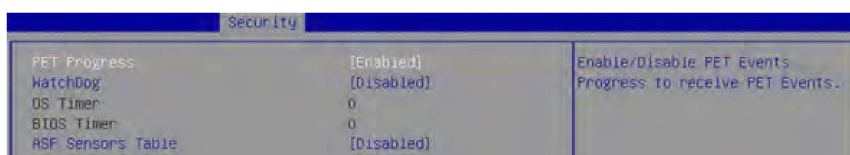
Please note that for “Extend CSME Measurement to TPM-PCR” function to work, your system should have a TPM module installed and enabled in the BIOS, which is a separate hardware component providing secure storage and cryptographic functions.

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**



» **PET Progress**
Enables or disable the this item to receive PET Events.

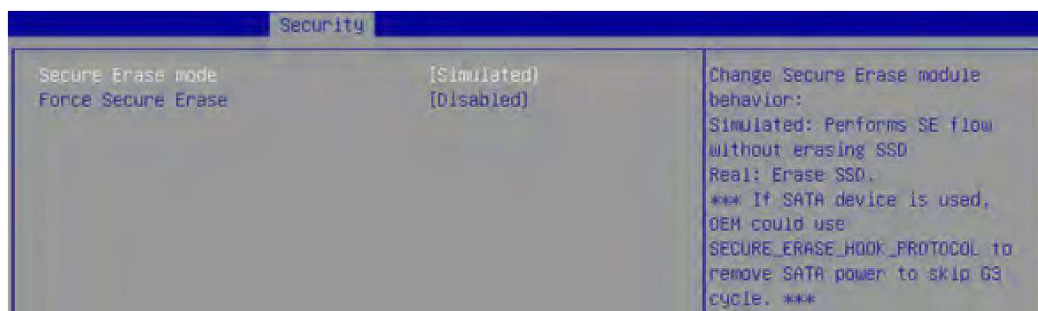
» **WatchDog**
Enables or disable the watchdog timer.

» **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 changes Secure Erase module behavior.

[Simulated] Performs SE flow without erasing SSD.

[Real] Erase SSD.

» Force Secure Erase

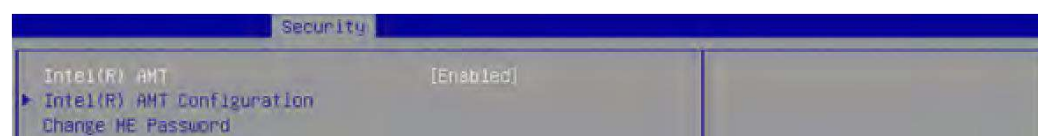
Enables or disables to force Secure Erase on next boot.

MEBx (Management Engine BIOS Extension)



» Intel(R) ME Password

Set the Intel® ME Password for securing access to the ME configuration through the MEBx menu. Upon setting up Intel® ME Password for the first time, type “admin” as the default password, then enter your own.



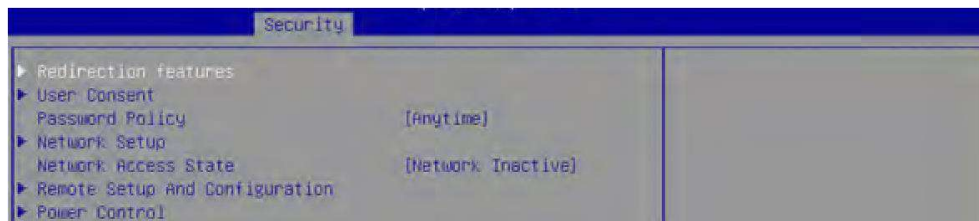
» Intel(R) AMT

Enables or disables Intel(R) AMT (Intel® Active Management Technology).

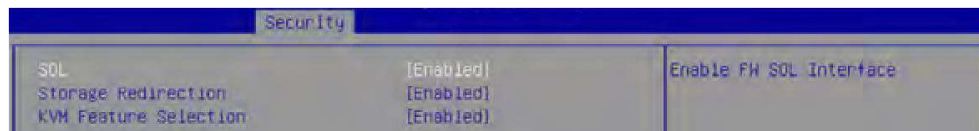
• Important

The MEBx menu can be accessed only by pressing the or <F2> key during the process of booting up the system.

» Intel(R) AMT Configuration



» Redirection features



- SOL
Enables or disables SOL (Serial Over LAN).
- Storage Redirection
Enables or disables Storage Redirection.
- KVM Feature Selection
Enables or disables the ability to remotely control a system's keyboard, video, and mouse (KVM) by a distant management console.

» User consent



- User Opt-in

[None]	Local user consent is not required for a remote console to establish KVM remote control session.
[KVM]	Local user consent is required for a remote console to establish KVM remote control session.
[ALL]	Local user consent is required for SOL, IDER and KVM.
- Opt-in Configurable from Remote IT
Enables or disables remote User's ability to set the User Opt-in.

» Password Policy

This feature determines when the user is allowed to change the Intel® MEBX password through the network.

[Default Password Only]	Allows changing the Intel® MEBx password through the network interface only if the default password has not been changed yet.
[During Setup And Configuration]	Allows changing the Intel® MEBx password via the network interface during setup and configuration but not afterward. Once the setup and configuration process is complete, the Intel MEBx password cannot be changed via the network interface.
[Anytime]	Allows changing the Intel® MEBx password through the network interface at any time.

- **Important**

- The Password Policy involves 2 passwords: the Intel® MEBx password (local), entered when physically at the system, and the network password (remote), used for accessing an Intel ME enabled system through the network. By default, they are the same until the network password is changed via the network. Once changed over the network, the network password remains separate from the local Intel® MEBx password.
- The Intel MEBx password can always be changed via the Intel® MEBX user interface, regardless of the setting.

» Network Setup



- Intel® ME Network Name Settings

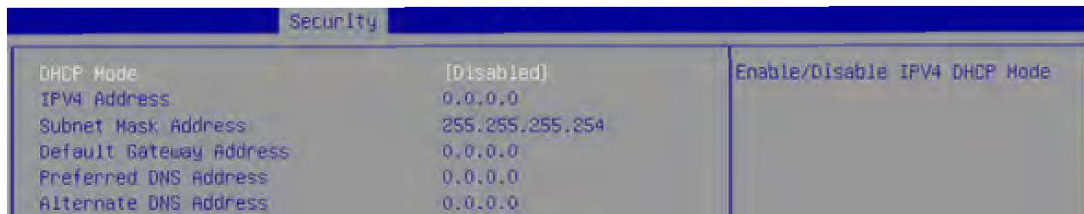


- Shared/Dedicated FQDN
Determines if the Intel® ME Fully Qualified Domain Name (FQDN, which is "HostName.DomainName") is shared with the host OS or dedicated exclusively to the Intel ME.
- Dynamic DNS Update
Enables or disables automatic registration of the firmware's IP addresses and FQDN in the Domain Name System (DNS) using the Dynamic DNS Update protocol. To enable Dynamic DNS Update, the Host Name and Domain Name must be set.

- TCP/IP Settings



- Wired Lan IPV4 Configuration

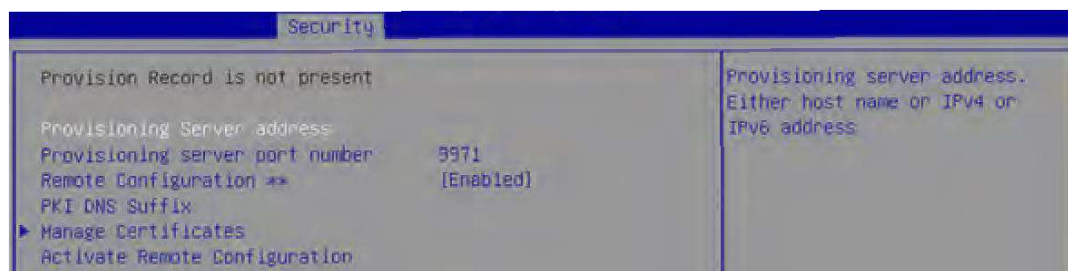


- DHCP Mode

Enables or disables the DHCP (Dynamic Host Configuration Protocol) mode. The items shown above will display when DHCP Mode is set to disabled.

- » Network Access State

- » Remote Setup And Configuration

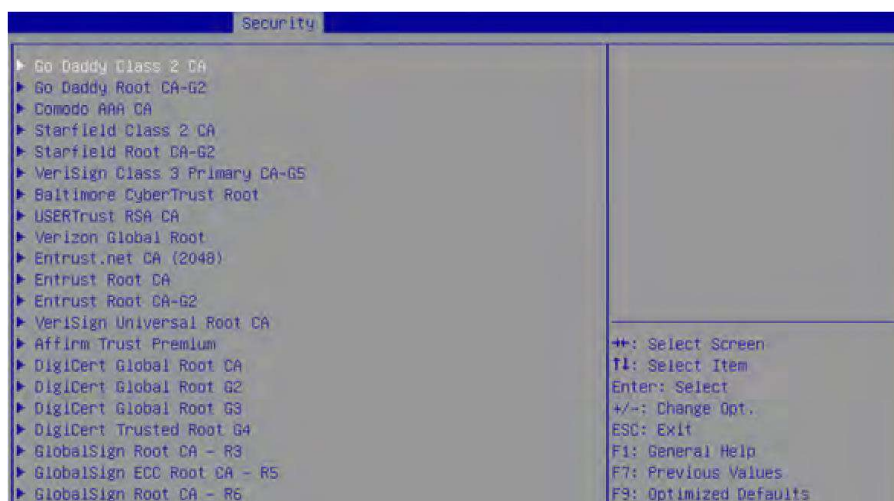


- Remote Configuration**

Enables or disables the Remote Configuration**.

- Manage Certificates

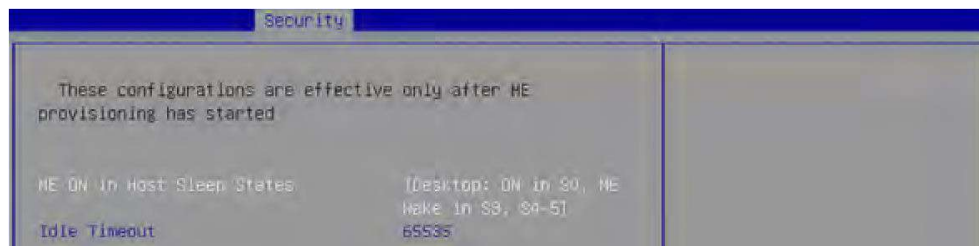
This item display when Remote Configuration** is disabled. After entering the Manage Certificates menu, the following screen will display:



The details of the selected certificate hash include "Hash Name, Active State, Default State, Hash Type and Hash Data".

» Power control

This menu configures the Intel ME platform power-related policies, and the configurations are effective only after ME provisioning has started.



• One Click Recovery (OCR) Configuration

» 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

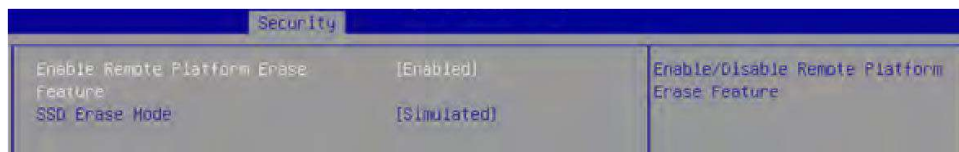
Enables or disables the Windows Recovery Boot for the OCR boot process. When enabled, the OCR boot process will prioritize Windows recovery options, allowing users to restore the system to a previous Windows state or initiate other Windows-specific recovery procedures.

» 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.



- » 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.

[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 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

These settings enable or disable the SHA-1 PCR Bank and SHA256 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 enable or disable the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

■ Physical Presence Spec Version

These settings show the Physical Presence Spec Version.

■ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

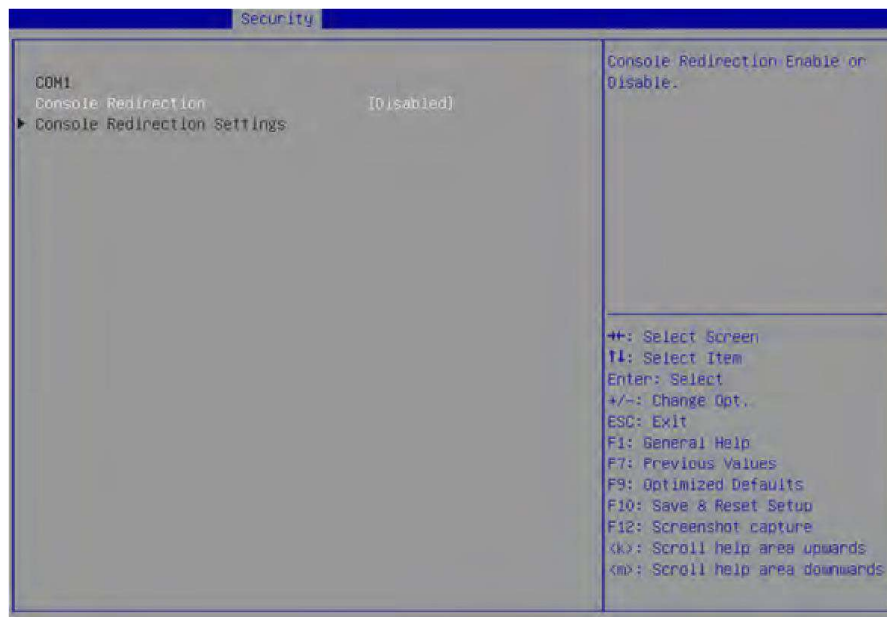
■ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

■ Device Select

Select your TPM device through this setting.

Serial Port Console Redirection

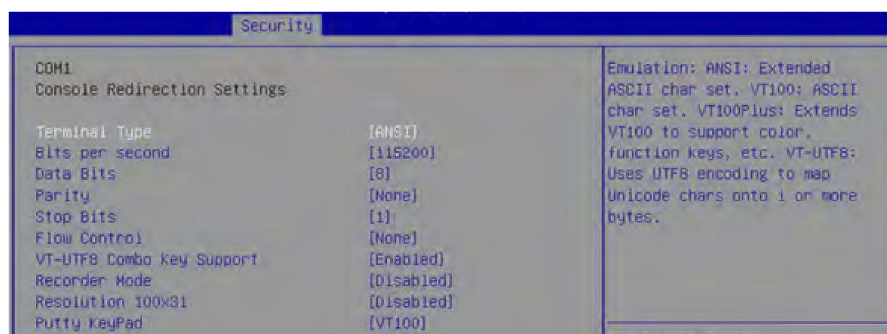


■ Console Redirection

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)

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 settings specify 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.

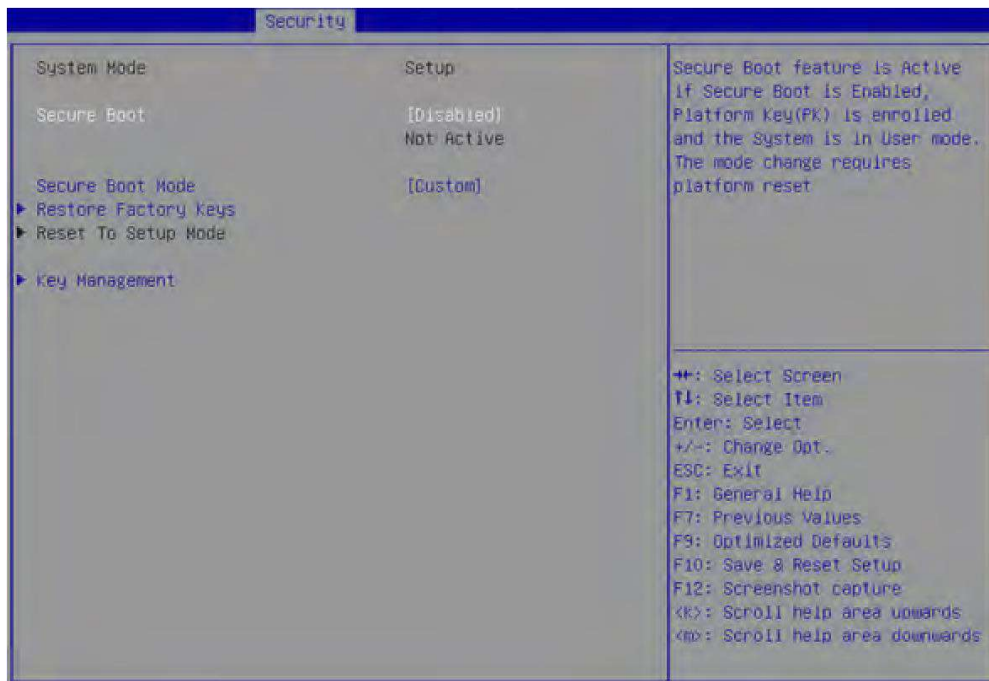
» Recorder Mode, Resolution 100x31

These settings enable or disable 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.

3.7 Secure Boot



- **Secure Boot**

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

- **Secure Boot Mode**

Select 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**

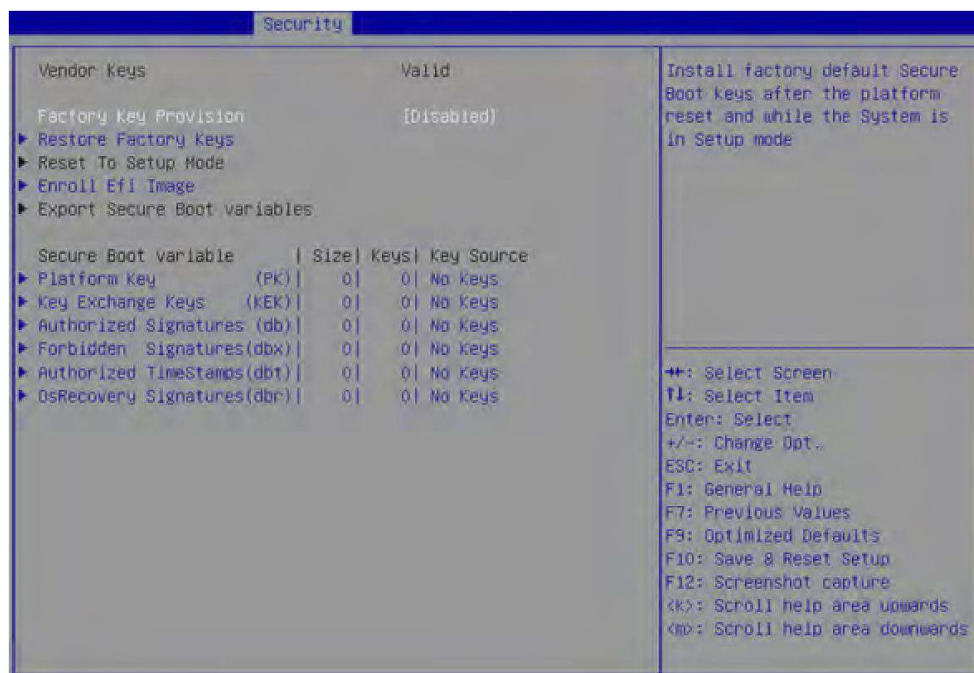
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when "Secure Boot Mode" sets to [Custom].

- **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.

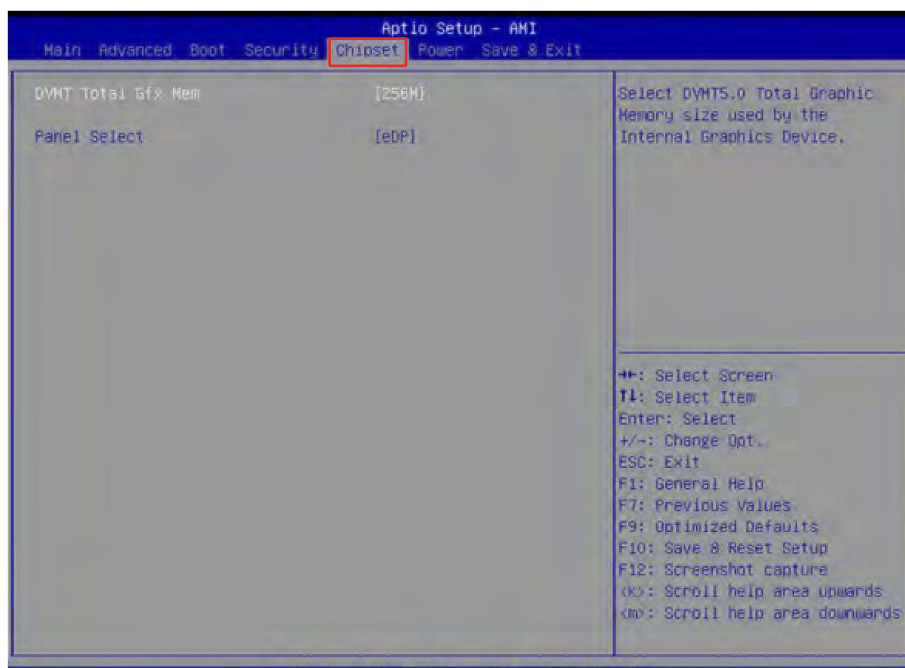
» Append Key

Loads an additional DBT from storage devices to your system.

» OsRecovery Singnatures (dbr):

Lists the available signatures for OS recovery.

3.8 Chipset



- **DVMT Total Gfx Mem**

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

- **Panel Select**

Set your video signal interface as LVDs or eDP.

- **LCD Panel Type**

This setting specifies the LCD Panel's resolution and distribution formats. The item will display when LVDS is enabled.

- **Panel 1/ 2 Backlight Control**

This setting controls the intensity of the LED's backlight output. When lighting conditions are brighter, set it high for a clearer image and low when it is darker.

LED's backlight output	
[Level 1]	20%
[Level 2]	40%
[Level 3]	60%
[Level 4]	80%
[Level 5]	100%

3.9 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.

- **OnChip USB**

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

- **LAN**

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

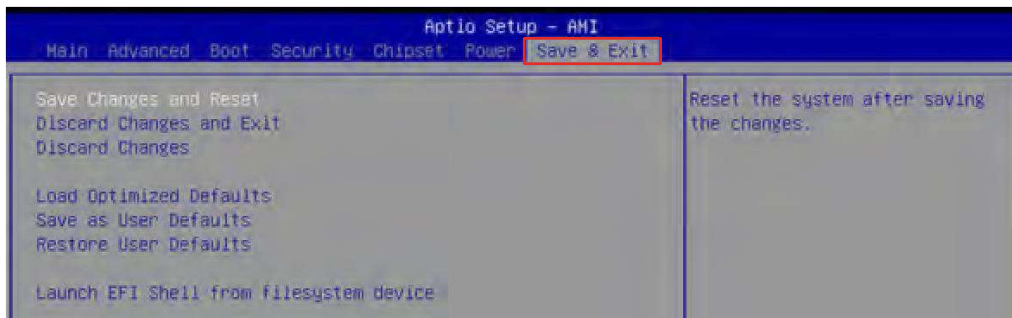
- **PCIe PME/Ring**

Enables or disables the system to be awakened from power saving modes when activity or input signal of onboard PCIe PME/Ring 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.

3.10 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.

Appendix

GPIO WDT BKL Programming Block Diagram

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) and CT-XRL02 Block Diagram

Abstract

In this section, code examples based on C programming language are 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	0x22	Bit 4	N_GPO0	0x11	Bit 4
N_GPIO1	0x22	Bit 5	N_GPO1	0x11	Bit 5
N_GPIO2	0x22	Bit 6	N_GPO2	0x11	Bit 6
N_GPIO3	0x22	Bit 7	N_GPO3	0x11	Bit 7
N_GPIO4	0x42	Bit 0	N_GPO4	0x21	Bit 0
N_GPIO5	0x42	Bit 1	N_GPO5	0x21	Bit 1
N_GPIO6	0x42	Bit 2	N_GPO6	0x21	Bit 2
N_GPIO7	0x42	Bit 3	N_GPO7	0x21	Bit 3

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 4.

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, 0x11);           // Read value from N_GPO0 port through SMBus.
val = val | (1<<4);                          // Set N_GPO0address (bit 4) to 1 (output “high”).
SMBus_WriteByte (0x6E, 0x11, val);           // Write back to N_GPO0 port through SMBus.
```

Example: Set N_GPO1 output “low”

```
val = SMBus_ReadByte (0x6E, 0x11);           // Read value from N_GPO1 port through SMBus.
val = val & (~(1<<5));                       // Set N_GPO1 address (bit 5) to 0 (output “low”).
SMBus_WriteByte (0x6E, 0x11, 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, 0x22);           // Read value from N_GPI2 port through SMBus.  
val = val & (1<<6);                          // Read N_GPI2 address (bit 6).  
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, 0x22);           // Read value from N_GPI3 port through SMBus.  
val = val & ~(1<<7));                      // Read N_GPI3 address (bit 7).  
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.

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

4. 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
```

4.1 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) & 0xffffffff0;
```

4.2 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
```

4.3 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
(SMBUS_BASE) + 0x02, 0x48); //out Base + 02, 48H
mdelay (20); //wait 20ms
```

