C&T SOLUTION INC.

USER'S MANUAL

LLM-1U-RPL

1U EDGE AI RACKMOUNT SERVER

Table of Contents

Prefaces

Revision

Revision	Description	Date
1.0	Manual Released	2025/7/15

Disclaimer

All specifications and information in this User's Manual are believed to be accurate and up to date. C&T Solution Inc. does not guarantee that the contents herein are complete, true, accurate or non-misleading. The information in this document is subject to change without notice and does not represent a commitment on the part of C&T Solution Inc.
C&T disclaims all warranties, express or implied, including, without limitation, those of merchantability, fitness for a particular purpose with respect to contents of this User's Manual. Users must take full responsibility for the application of the product.

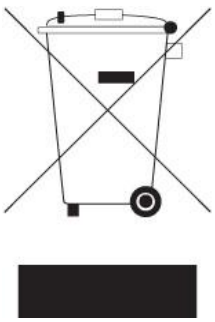
Copyright Notice

Trademarks Acknowledgment

Intel®, Celeron® and Pentium® are trademarks of Intel Corporation.
Windows® is registered trademark of Microsoft Corporation.
AMI is trademark of American Megatrend Inc.
IBM, XT, AT, PS/2 and Personal System/2 are trademarks of International Business Machines Corporation
All other products and trademarks mentioned in this manual are trademarks of their respective owners.

Environmental Protection Announcement

Do not dispose this electronic device into the trash while discarding. Please recycle to minimize pollution and ensure environment protection.



Safety Precautions

Before installing and using the equipment, please read the following precautions:

- Put this equipment on a reliable surface during installation. Dropping it or letting it fall could cause damage.
- The power outlet shall be installed near the equipment and shall be easily accessible.
- Turn off the system power and disconnect the power cord from its source before making any installation. Be sure both the system and the external devices are turned OFF. Sudden surge
- of power could ruin sensitive components. Make sure the equipment is properly grounded.
- When the power is connected, never open the equipment. The equipment should be opened only by qualified service personnel.
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Disconnect this equipment from the power before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- Avoid the dusty, humidity and temperature extremes.
- Do not place heavy objects on the equipment.
- If the equipment is not used for long time, disconnect it from the power to avoid being damaged by transient over-voltage.
- The storage temperature shall be above -20°C and below 70°C.
- The computer is provided with a battery-powered real-time clock circuit. There is a danger of explosion if incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.
- If one of the following situation arises, get the equipment checked be service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated into the equipment.
    - The equipment has been exposed to moisture.
    - The equipment does not work well or it cannot work according the user's manual.
    - The equipment has been dropped and damaged.
    - The equipment has obvious signs of breakage.

Technical Support and Assistance

1. Visit the C&T Solution Inc website at www.candtsolution.com where you can find the latest information about the product.
2. Contact your distributor, 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.

Package Contents

Before installation, please ensure all the items listed in the following table are included in the package.

Item	Description	Q'ty
1	**LLM-1U-RPL** 1U Edge AI Rackmount Server	1
2	CPU Fan Cooler	1
3	Safety Lock Toolkit	1
4	Power Cord	1

Ordering Information

Model No.	Product Description
LLM-1U-RPL	**1U Edge AI Rackmount Server with 12th/13th/14th Gen Intel® Core® Processor and Q670E PCH**

Optional Accessories

Model No.	Product Description
SFICBL022	Power Cord, 3-pin US Type, 180cm
1-TPCD00002	Power Cord, European Type, 180cm
1-TPCD00001	Power Cord, 3-pin UK Type, 180cm

Chapter 1

Product Introductions

1.1 Overview

Run Generative AI locally with the LLM-1U-RPL Series — a 1U edge AI server designed for real-time large language model (LLM) inference. Powered by advanced GPUs, it supports models up to 40 billion parameters for low-latency, secure, and on-premise AI processing without cloud dependency. Deploy in industrial sites, field locations, or enterprise data centers to bring AI closer to your data.

Key Features

- upport 12th/13th/14th Gen Intel® Core™ Processors (LGA 1700, 65W Max TDP)
- Intel® Q670E Chipset
- 2x DDR4 3200MT/s SODIMM. Max. up to 64GB
- 3x 2.5GbE (Support Wake-on-LAN and PXE)
- Triple 4K Display: 2x DP++, 1x HDMI
- 1x PCIe x16 (Gen 4) or 2x PCIe x8 (Gen 4) slot
- 1x M.2 M Key, 1x M.2 B Key, 1x M.2 E Key
- 2x 2.5" SATA SSD Drive bays
- 2x RS-232/422/485 COM Ports, 2x RS-232 (Internal)
- 6x USB 3.2 Gen 2 (Rear), Front: 2x USB 3.2 Gen 1 (Front)
- 600W Redundant Power Supply
- Support TPM 2.0
- UL 62368 Ed. 3, FCC, CE

1.2 Hardware Specification

System
Processor • Support 12th/13th/14th(Non-vPRO) Gen Intel® ADL & RPL Processor (LGA 1700, 65W/35W TDP) - Intel® Core™ i9-14900/i9-13900E/i9-12900E, 65W - Intel® Core™ i9-14900T/i9-13900TE/i9-12900TE, 35W - Intel® Core™ i7-14700/i7-13700E/i7-12700E, 65W - Intel® Core™ i7-14700T/i7-13700TE/i7-12700TE, 35W - Intel® Core™ i5-14500/i5-13500E/i5-12500E, 65 W - Intel® Core™ i5-14500T/i5-13500TE/i5-12500TE, 35W - Intel® Core™ i3-13100E/i3-12100E, 60W - Intel® Core™ i3-14100T/i3-13100TE/i3-12100TE, 35W - Intel® Core™ 300T, 35W - Intel® Pentium® G7400E, 46W / G7400TE, 35W - Intel® Celeron® G6900E, 46W / G6900TE, 35W

System Chipset	Intel® Q670E PCH
LAN Chipset	Intel® I226LM PCIe 2.5GbE LAN Intel® I226V PCIe 2.5GbE LAN Intel® I226V PCIe 2.5GbE LAN
Audio Codec	Realtek ALC897
System Memory	2x DDR4 3200MT/s SODIMM. Max. up to 64 GB (Default: 8GB & Non- ECC supported)
BIOS	AMI UEFI BIOS
Watchdog	Software Programmable Supports 1~255 sec. System Reset
TPM	TPM 2.0

Display	
DisplayPort	2x Dual Mode DisplayPort 1.4a Max Resolution 4096 x 2304 @60Hz
HDMI	1x HDMI 1.4b Max Resolution 4096 x 2304 @24Hz
Multiple Display	3x Independent Displays

Storage	
SSD/HDD	2x 2.5" Hot-swap SATA SSD Drive Bays (7mm/15mm)

I/O	
Audio	Line-out/Mic-in
COM	2x DB9 COM1: RS232/422/485 COM2: RS232
LAN	3x RJ45 (2.5GbE)
USB	6x USB 3.2 Gen2 (Read) 2x USB 3.2 Gen 1 Type-A (Front)
Others	1x Power button 1x HD LED 1x Power LED 1x Safety Lock

Expansion	
M.2 B-Key	1x M.2 B key Type: 3042 • Support PCIe x1 +USB 3.2 Gen 2x1 + USB 2.0 • Support NVMe Storage/AI Module/4G/5G
M.2 E-Key	1x M.2 E-Key Type: 2230 (Support PCIe x1 + USB 2.0; Support CNVi) Devices Supported: Intel® AX210 Wi-Fi 6E & BT-5.1 (vPro Supported)
M.2 M-Key	1x M.2 M-Key Type (2242/2280): • Support PCIe x4 Gen3 NVMe SSD • PCIe x4 Gen3 signal from PCH • Support B+M Key
PCIe	1x PCIe x16 Gen 4 or 2x PCIe x8 Gen 4
Card Dimension	267 (L) x 112 (H) mm, dual slot

Operating System	
Windows	Windows 10/11
Linux	Linux kernel

System Cooling	
Fan	1x CPU Fan Cooler 3x Hot-Swap Smart Fan
Air Filter	1x Dust Fan Filter

Power	
Power Adapter	AT, ATX (Default ATX)
Power Ignition Sensing	Adjustable Power Ignition Management
Power Supply	2x 600W (1+1) Redundancy Power Supply AC: 115 to 230 V DC: -36 to -72 V
Power Connector	IEC 60320 C14

Environment	
Operating Temp.	0°C to 35°C with 0.6 m/s airflow
Storage Temp.	-20°C to 70°C
Relative Humidity	5% to 95% (non-condensing)
Certification	UL 62368 Ed. 3, CE, FCC Class A
Vibration	With SSD: 1 Grms (5 - 500 Hz, 0.5 hr/axis)
Shock	With SSD: NA-G half-sin 11ms

Physical	
Form Factor	1U
Construction	Heavy Duty Metal
Dimension	483 (W) x 480 (D) x 44 (H) mm
Weights	4 KG
Mounting	Rackmount

*All specifications and photos are subject to change without notice.

1.3 System I/O

LLM-1U-RPL

Front Panel

USB 3.2 Gen 2 port (10 Gbps)
Used to connect USB 3.2 device

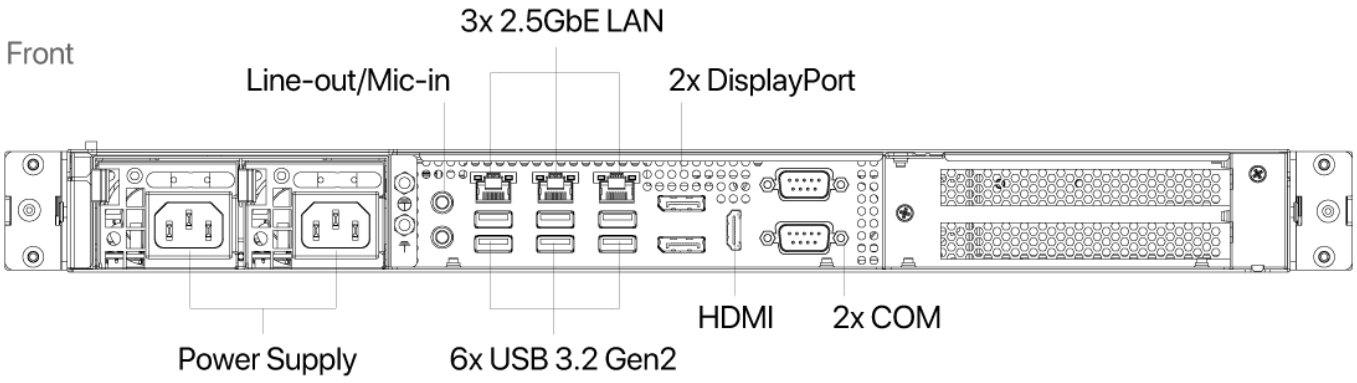
DisplayPort
Used to connect a DisplayPort monitor

HDMI port
Used to connect a HDMI monitor or connect optional split cable for dual display mode

2.5GbE LAN port
Used to connect the system to a local area network

Line-out/Mic-in
Used to connect a speaker / Used to connect a microphone

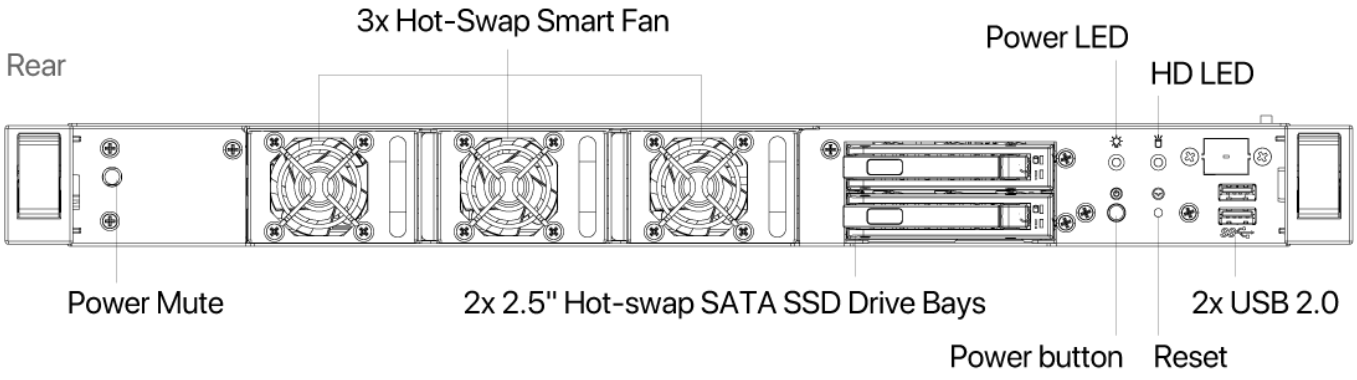
Power Supply
2x 600W (1+1) Redundancy Power Supply
AC: 115 to 230 V
DC: -36 to -72 V



Removable HDD
Removable 2.5" SATA HDD Drive Bays
(support H=7mm/15mm, hot-swappable)

Rear Panel

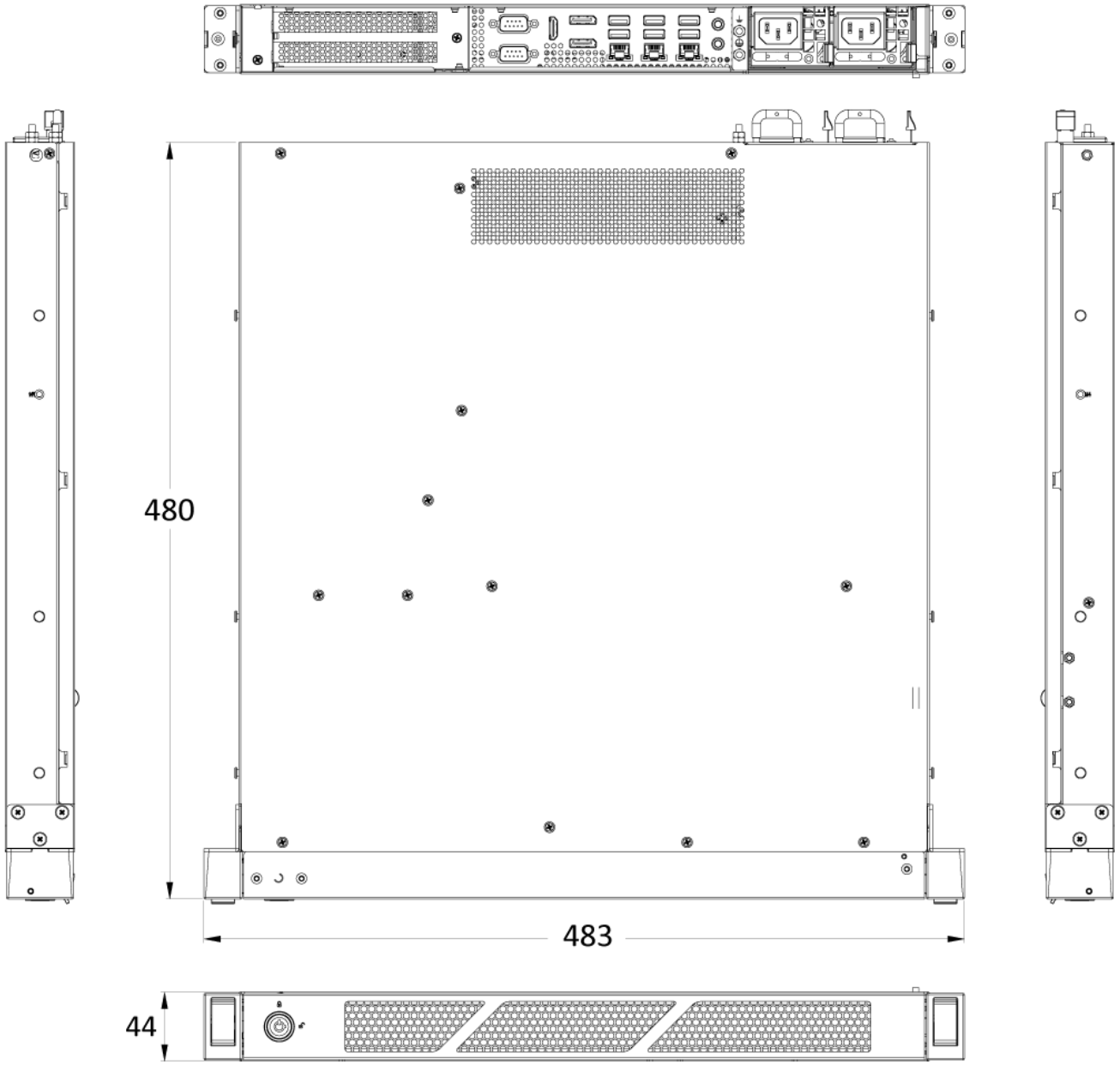
USB port
Used to connect USB device



1.4 Mechanical Dimensions

LLM-1U-RPL

Unit: mm

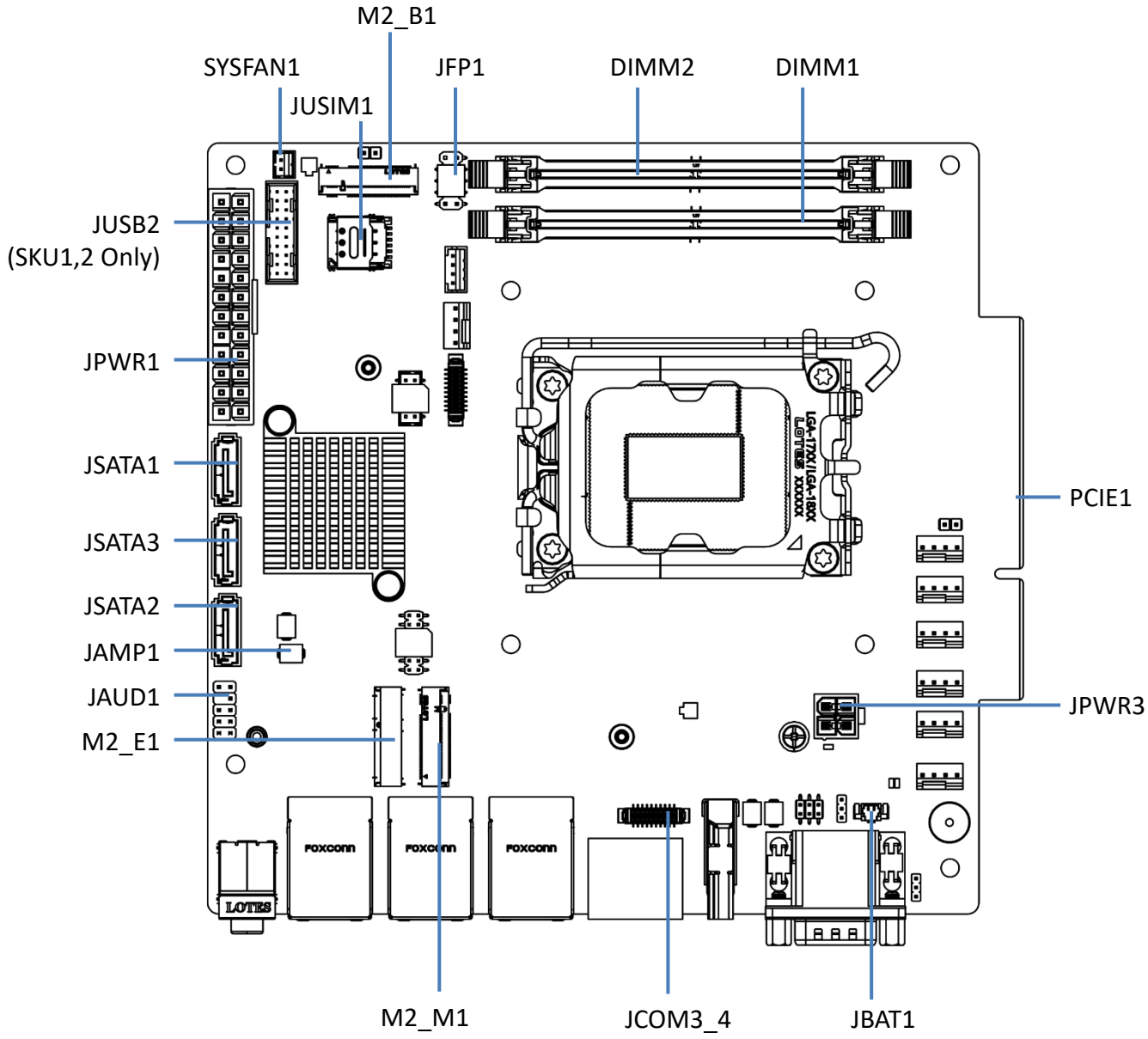


Chapter 2

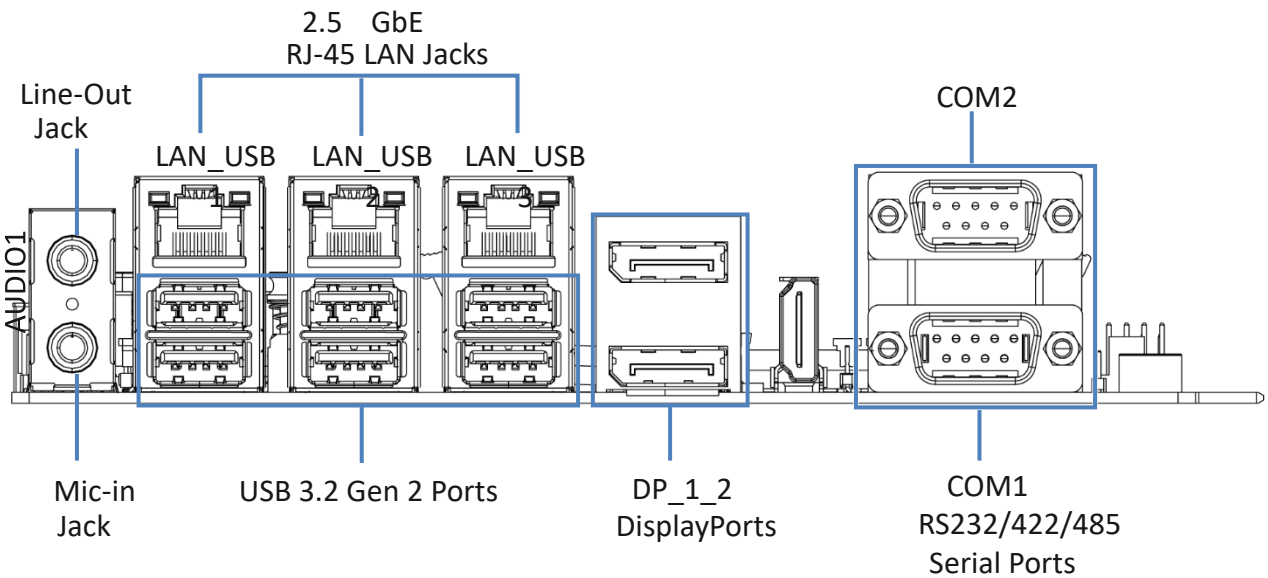
Mechanical Specifications

2.1 Switch and Connector Locations

2.1.1 SKU1/ SKU2



Rear I/O



Component Contents

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 (SKU1,2 Only)
- M2_E1: M.2 Slot (E Key, 2230)
- M2_B1: M.2 Slot (B Key, 3042) (SKU1,2 Only)

2.7 Connectors

Power Connectors

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

Audio Connectors

- JAUD1: Front Audio Header
- JAMP1: Audio Amplifier Header

Graphics Connectors

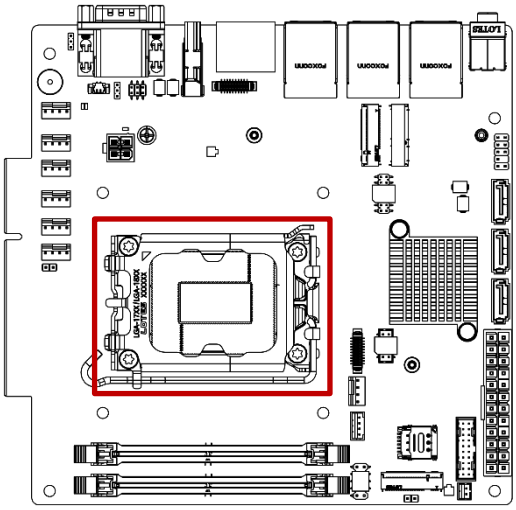
- JINV1: LVDS Inverter Box Header
- JLVDS1_EDP1: LVDS+eDP Wafer Connector

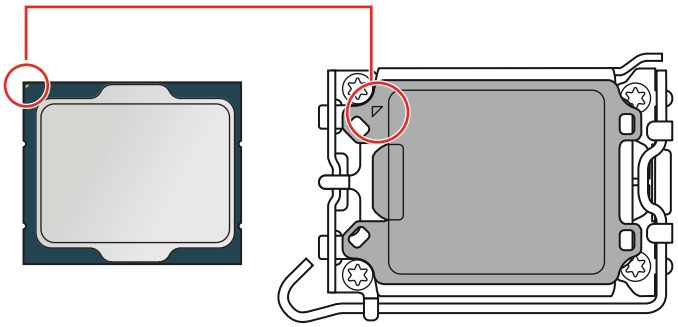
Other Connectors

- 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 (SKU1,2 Only)
- JBAT1: CMOS Battery Header

2.8 Jumpers

2.2 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.

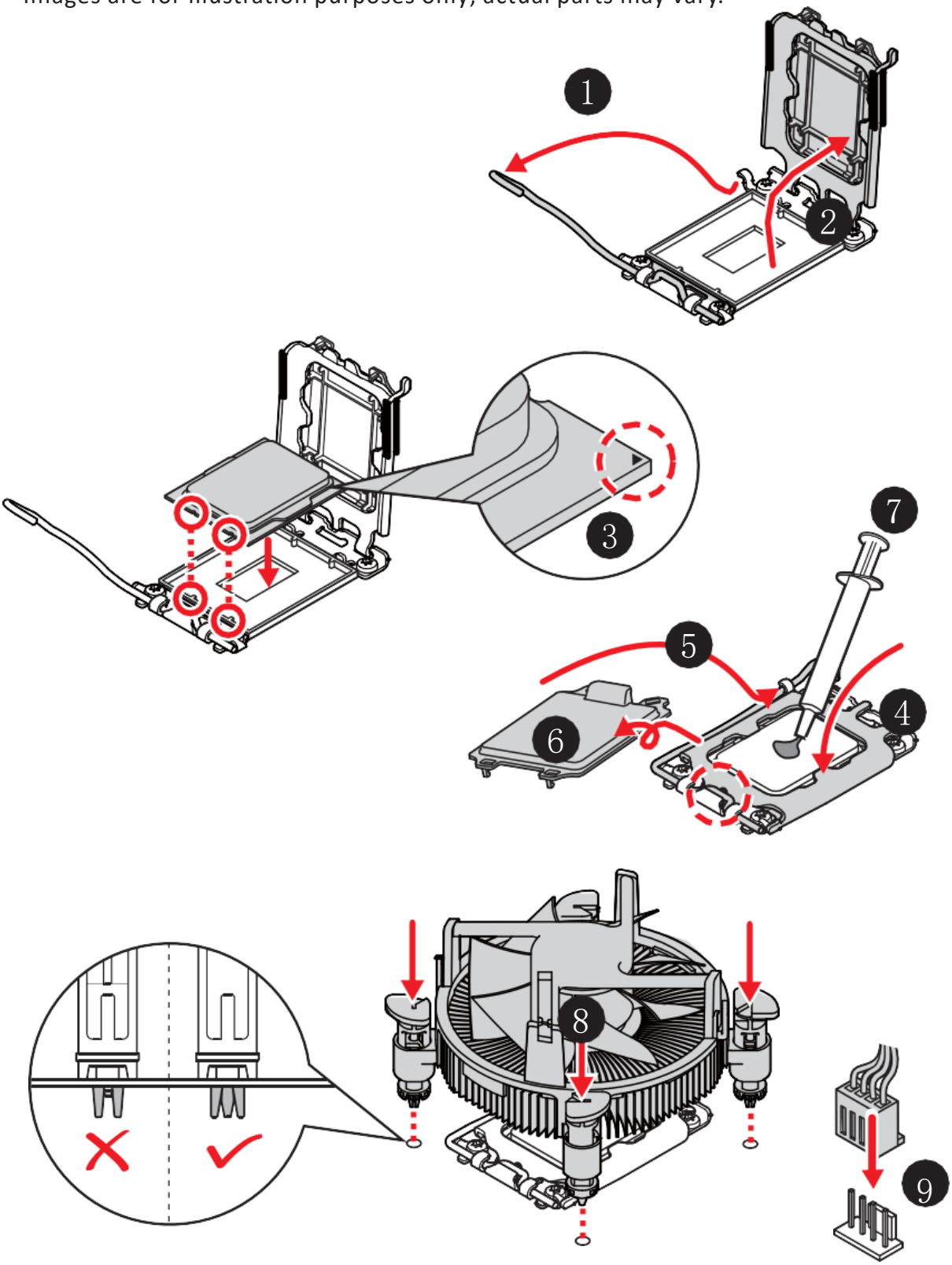
- **Important**
  - Always unplug the power cord from the power outlet before installing or removing the CPU.
  - When installing a CPU, always remember to install a CPU heatsink. A CPU heatsink is necessary to prevent overheating and maintain system stability.
  - Confirm that the CPU heatsink has formed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

2.3 CPU & Heatsink Installation

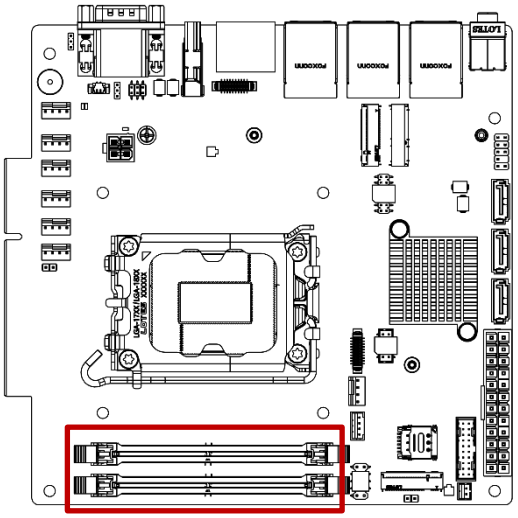
Use appropriate ground straps, gloves and ESD mats to protect yourself from electrostatic discharge (ESD) while installing the processor.

Important

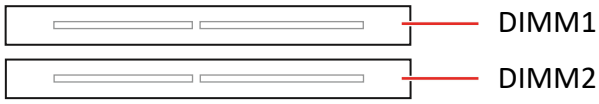
Images are for illustration purposes only; actual parts may vary.



2.4 Memory



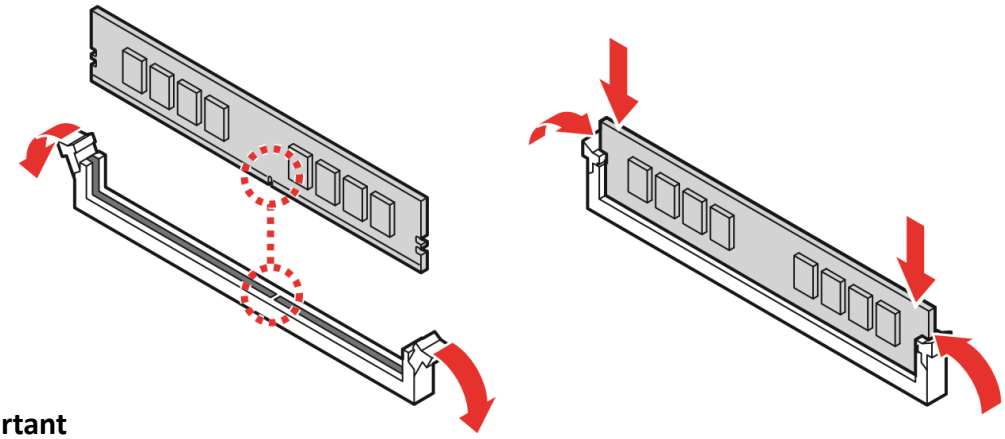
Installing DDR4 Memory



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

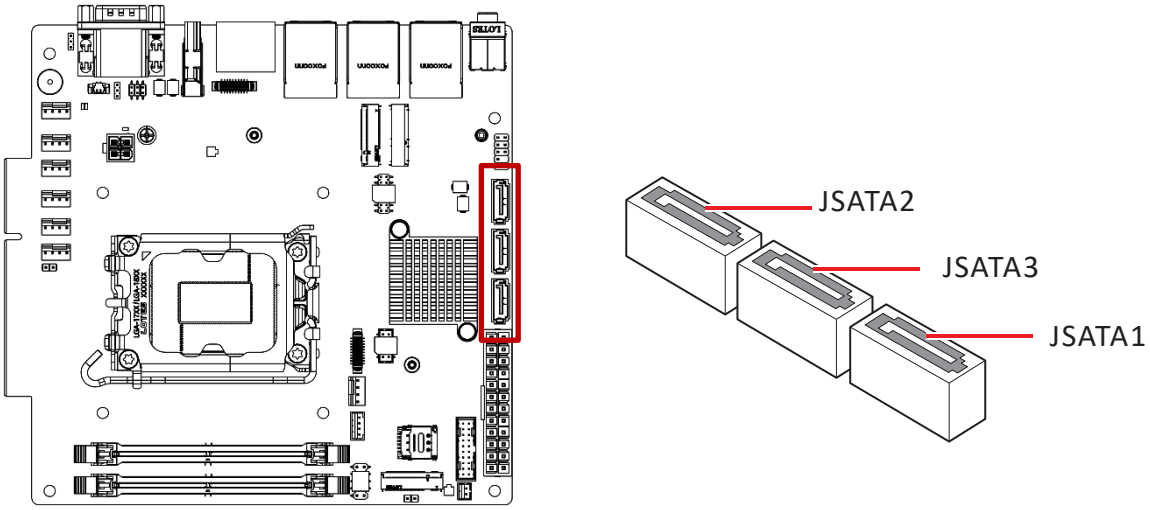
  The SO-DIMM slots are intended for memory modules.

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.a
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.

2.5 Storage



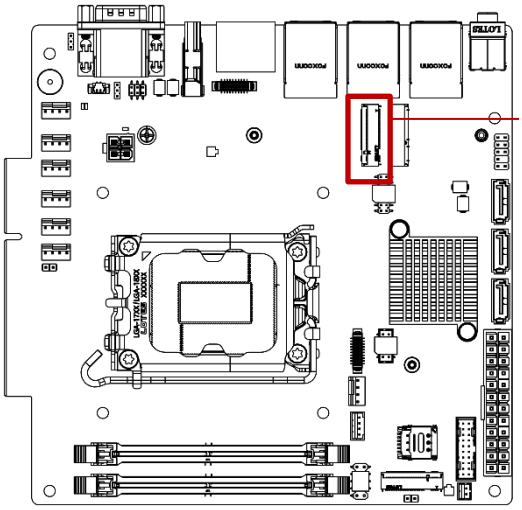
- **JSATA1: SATA 3.0 6Gb/s Ports**

  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.

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.

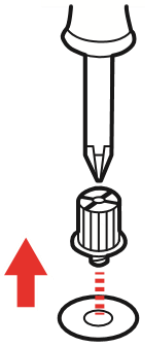


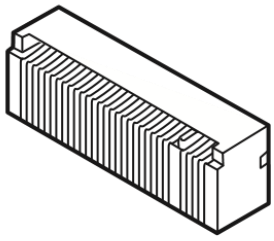
Feature

- Supports PCIe 3.0 x4 signal.
- Supports B+M key module.

Installing M.2 SSD

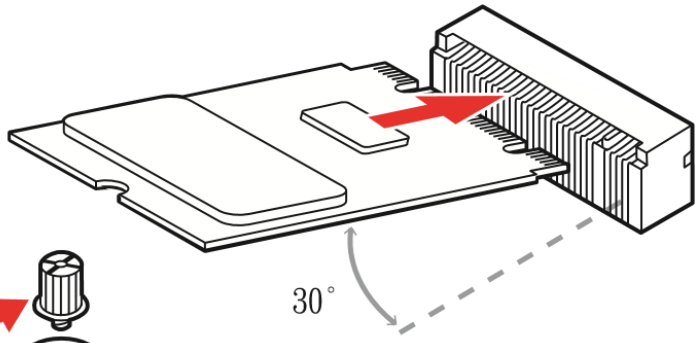
1. Loosen the M.2 riser screw from the motherboard.

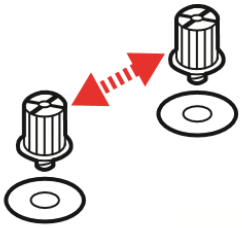




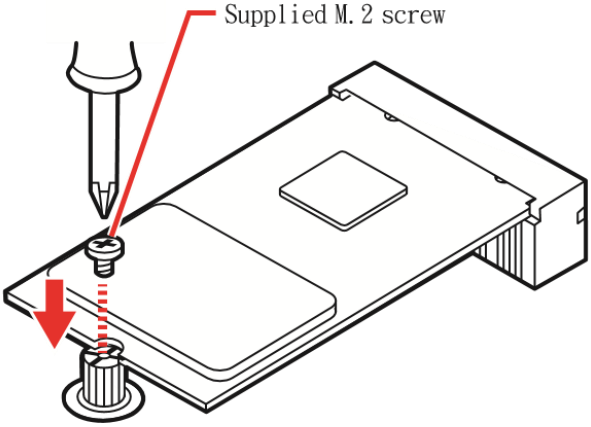
2.Set the M.2 riser screw at the appropriate location based on the length of your M.2 SSD.

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

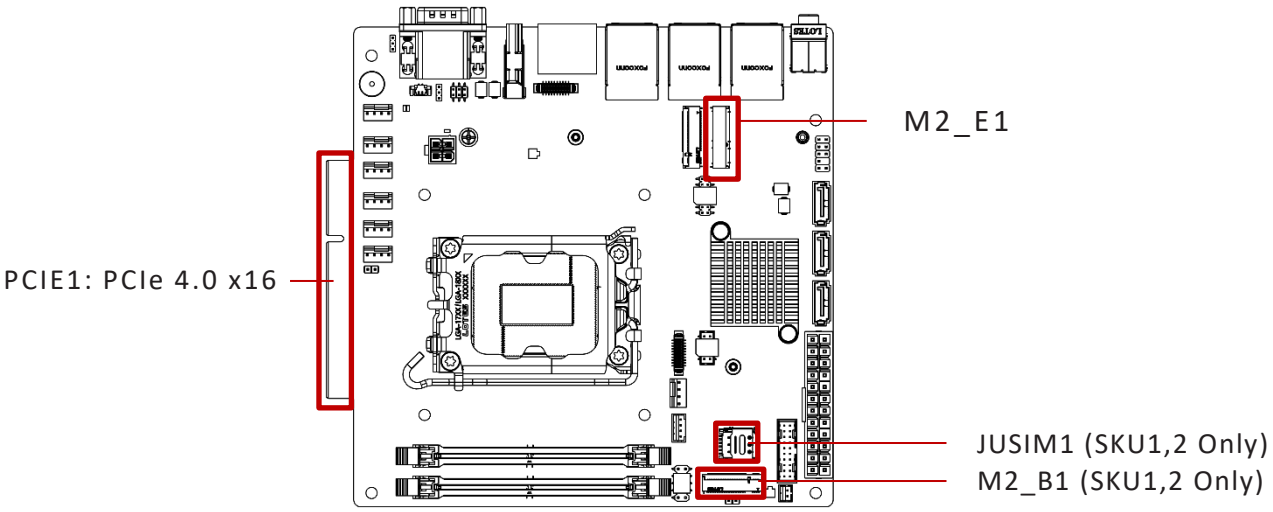




4.Secure the M.2 SSD in place with the supplied M.2 screw



2.6 Expansion Slots

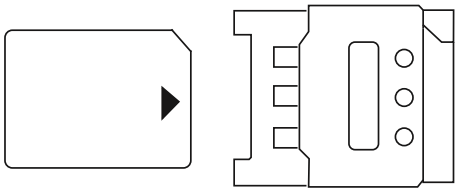


- **PCIE1: PCIe Expansion Slots**

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

- **JUSIM1: Nano SIM Holder (SKU1,2 Only)**

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

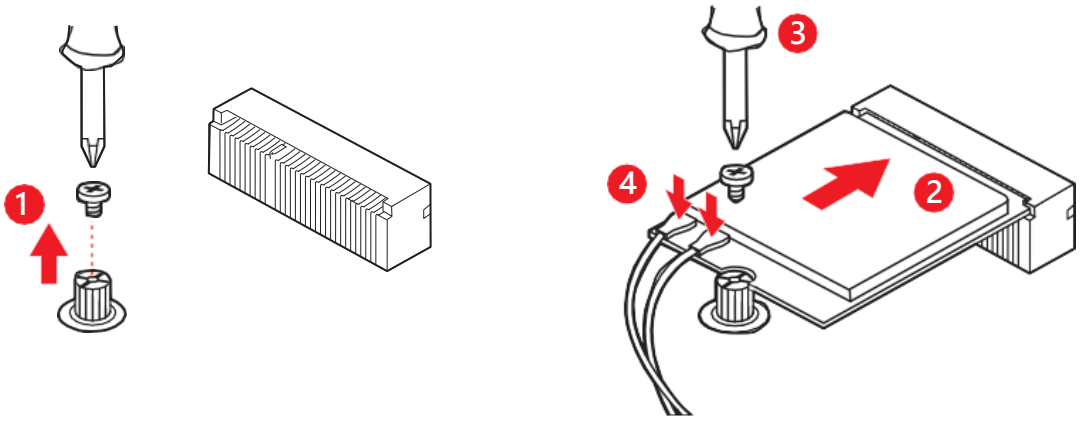


- **Important**

  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/ Bluetooch card into the M.2 slot as shown below.

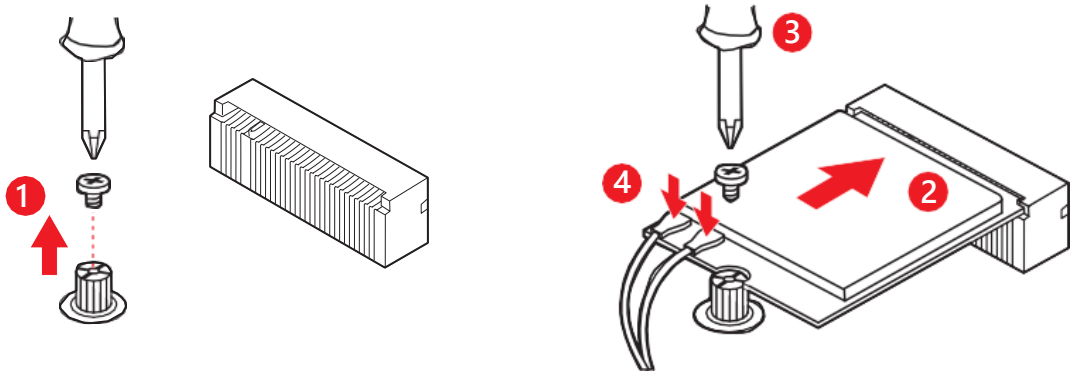


Feature

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

M2_B1: M.2 Slot (B Key, 3042) (SKU1,2 Only)

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

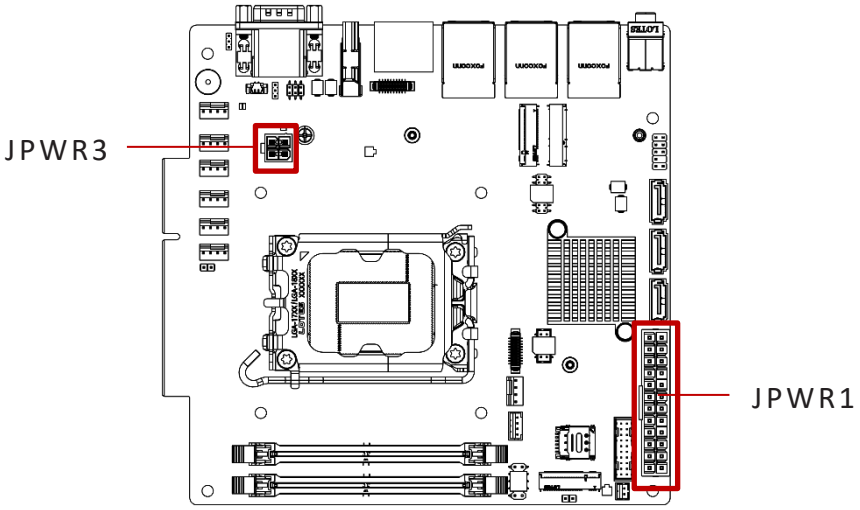


Feature

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

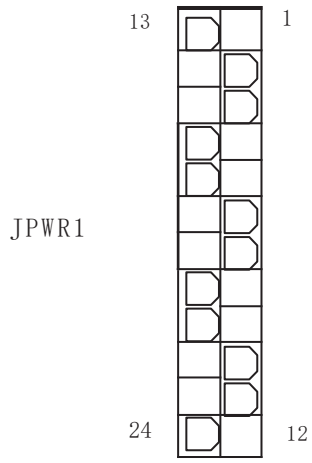
2.7 Connectors

Power Connectors



JPWR1: ATX 24-Pin Power Connector

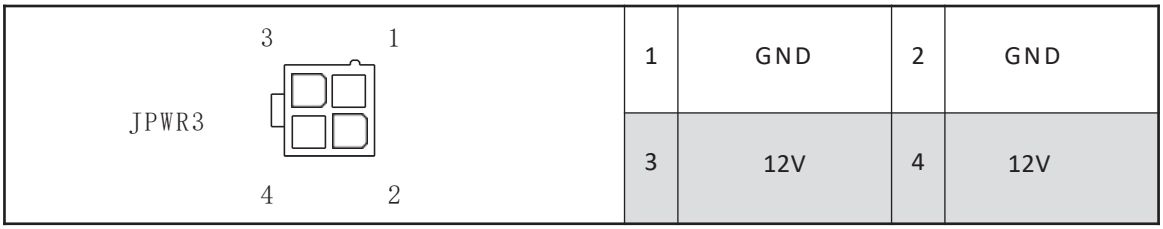
This connector allows you to connect an ATX power supply.



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 allows you to connect an ATX 4-Pin power supply.

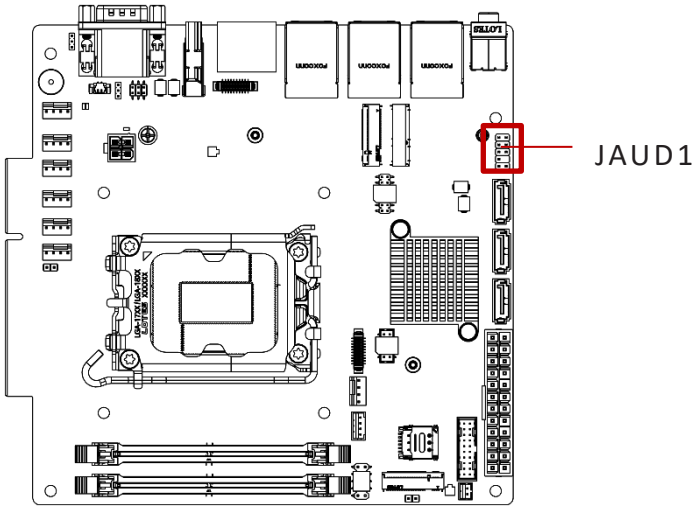


1	GND	2	GND
3	12V	4	12V

Important

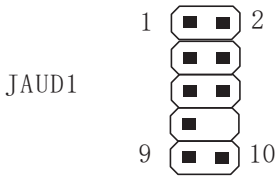
Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Audio Connectors



JAUD1: Front Audio Header

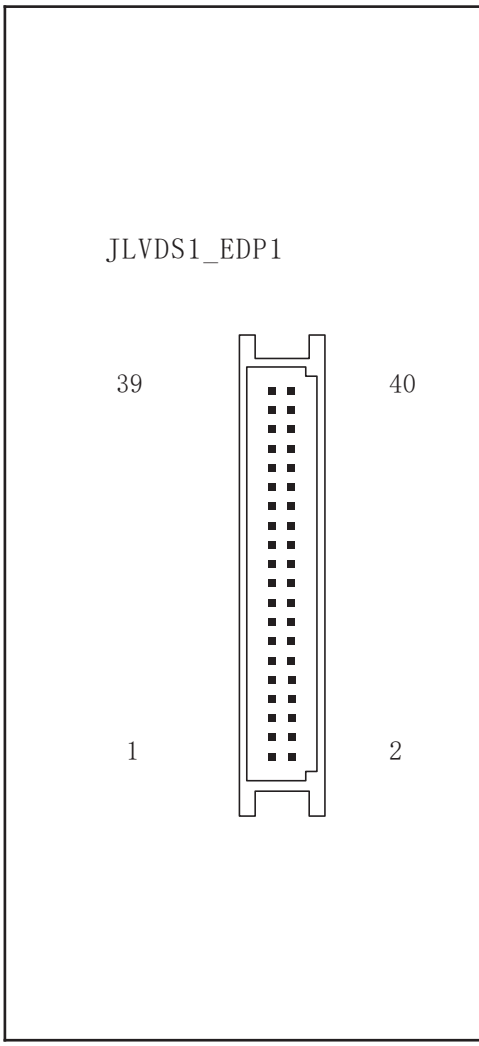
This connector allows you to connect front panel audio.



	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

- **JLVDS1_EDP1: LVDS+eDP Wafer Connector**

  This connector is designed for use with LVDS/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 JVDD1 LVDS power jumper to the appropriate power voltage.



1	EDP_LINE3_DP	2	EDP_LINE2_DP
3	EDP_LINE3_DN	4	EDP_LINE2_DN
5	DDC0_CLK_7513_R	6	DDC0_DATA_7513_R
7	LCD_VDD	8	LCD_VDD
9	LCD_VDD	10	VCC3
11	BKLT_EN	12	LVDS_DETECT#
13	LVDSA_DATA1+	14	EHPDET/LVDSA_ DATA0-
15	LVDSA_DATA1-	16	LVDSA_DATA0-
17	GND	18	GND
19	LVDSA_DATA3+	20	LVDSA_DATA2+
21	LVDSA_DATA3-	22	LVDSA_DATA2-
23	GND	24	GND
25	LVDSB_DATA1+	26	LVDSB_DATA0+
27	LVDSB_DATA1-	28	LVDSB_DATA0-
29	GND	30	GND
31	LVDSB_DATA3+	32	LVDSB_DATA2+
33	LVDSB_DATA3-	34	LVDSB_DATA2-
35	NC	36	GND
37	LVDSB_CLK+	38	LVDSA_CLK+
39	LVDSB_CLK-	40	LVDSA_CLK-

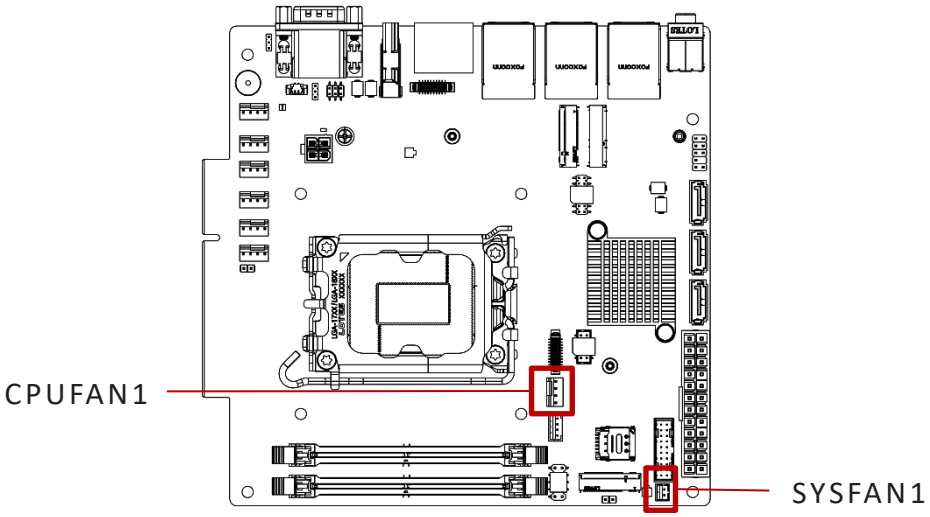
- **Important**

  Pin 12 is a detective pin. When using a customized LVDS cable, pin 12 should be a signal ground with a low impedance. Otherwise, LVDS will not function.

Other Connectors

CPUFAN1, SYSFAN1: 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.



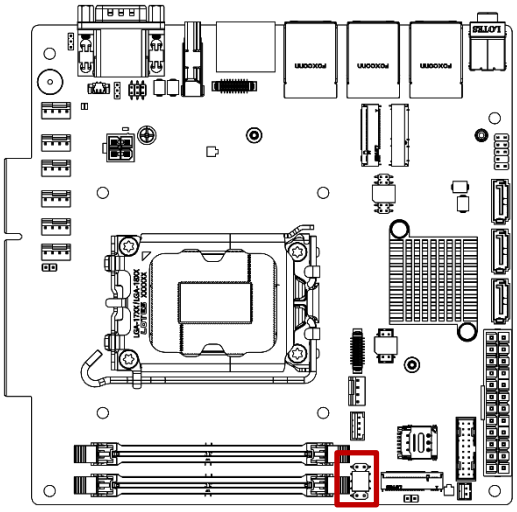
CPUFAN1 4 1 SYSFAN1				
	1	GND	2	FANPOWER
	3	FANSENSE	4	FAN_PWM

- **Important**

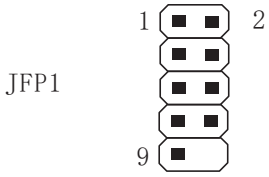
  Please refer to the recommended CPU fans at processor's official website or consult the vendors for proper CPU cooling fan.

- **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.



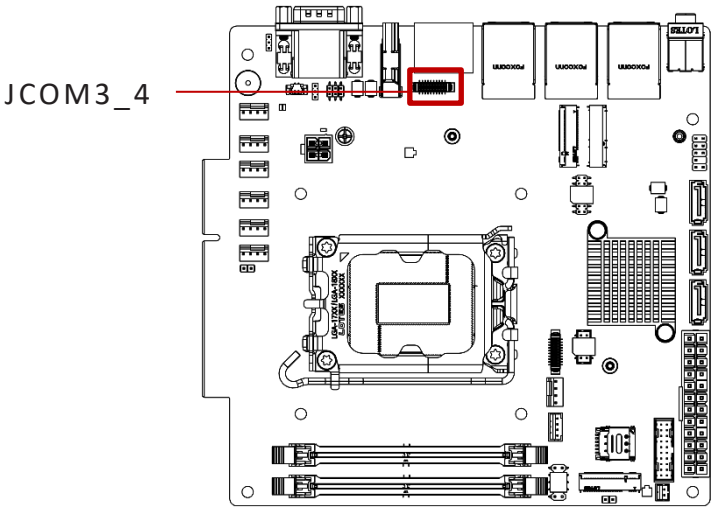
JFP1

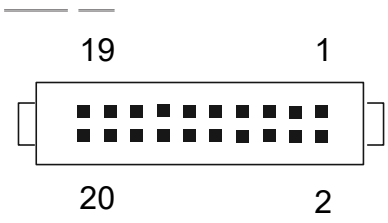


	1	HDDLED+	2	POWERLED
	3	HDDLED-	4	POWERLED
	5	RESETSWITCH-	6	POWERSWITCH+
	7	RESETSWITCH+	8	POWERSWITCH-
	9	NC	10	Nopin

- **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.





1	NDCD3#	2	NDCD4#
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).

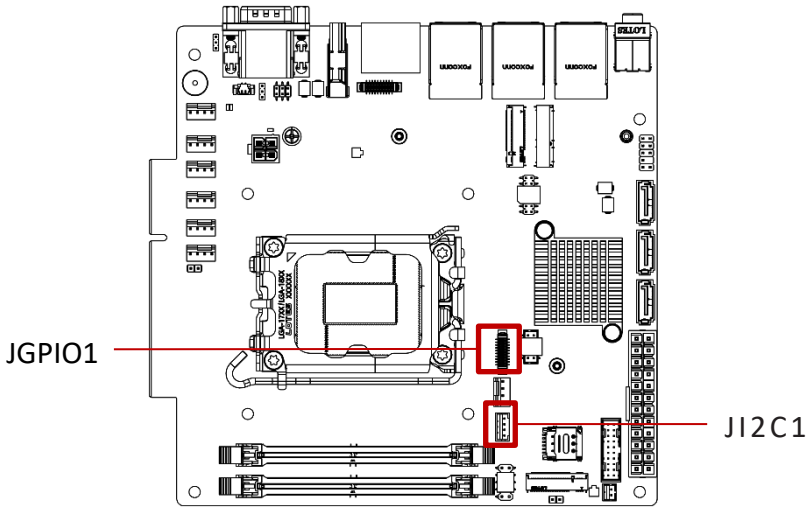
SKU3

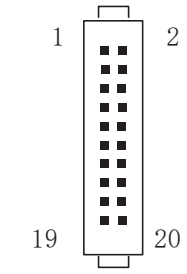
- COM1 Connector (Rear I/O)
  Supports RS-232/ 422/ 485, With Ring/ 0V/ 5V/ 12V (Default set to Ring).
- COM2 Connector (Rear I/O)
  Supports RS-232/ 422/ 485, With 0V/ 5V/ 12V (Default set to 5V).
- JCOM3_4 Connector
  Supports RS-232, With 0V/ 5V/ 12V (Default set to 5V)

RS232		
PIN	SIGNAL	DESCRIPTION
1	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+	Receive Data, Positive
3	422 RXD+	Transmit Data, Positive
4	422 RXDGND	Receive Data, Negative
5	NC	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9		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.

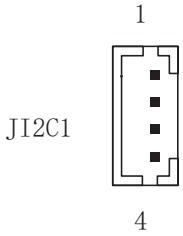




	1	GND	2	GND
	3	N_GPO0	4	N_GPI0
	5	N_GPO1	6	N_GPI1
	7	N_GPO2	8	N_GPI2
	9	N_GPO3	10	N_GPI3
	11	N_GPO4	12	N_GPI4
	13	N_GPO5	14	N_GPI5
	15	N_GPO6	16	N_GPI6
	17	N_GPO7	18	N_GPI7
	19	VCC5	20	VCC5

- **JI2C1: I2C Box Header**

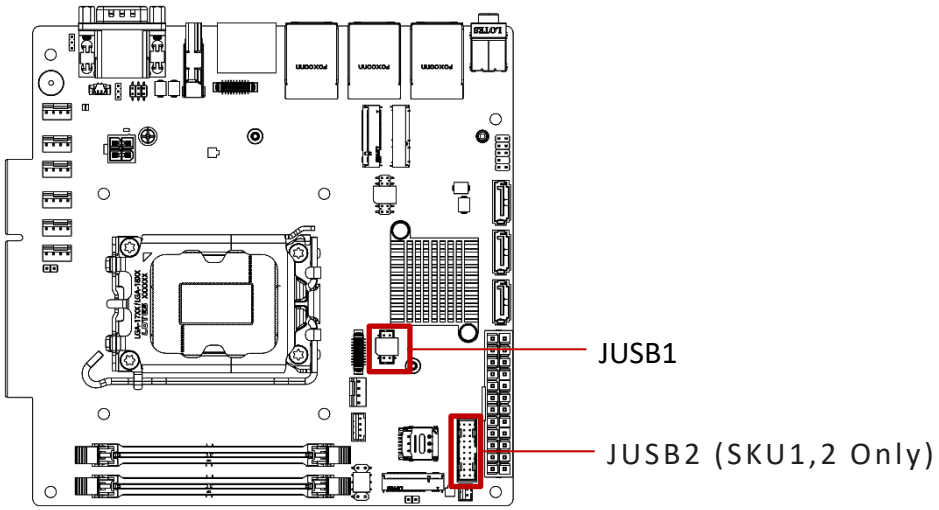
  This connector is used to connect to the System Management Bus (SMBus).

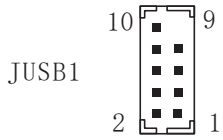


	1	3VSB	2	I2C_CLK
	3	I2C_DATA-	4	GND

- **JUSB1: USB 2.0 Box Header**

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

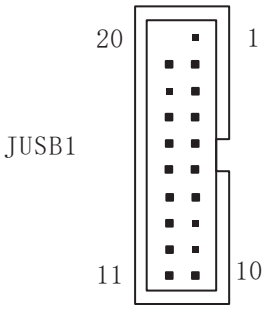




	1	5V	2	5V
	3	USB_D-	4	USB_D-
	5	USB_D+	6	USB_D+
	7	GND	8	GND
	9	Nopin	10	NC

- **JUSB2: USB 3.2 Gen 1 Box Header (SKU1,2 Only)**

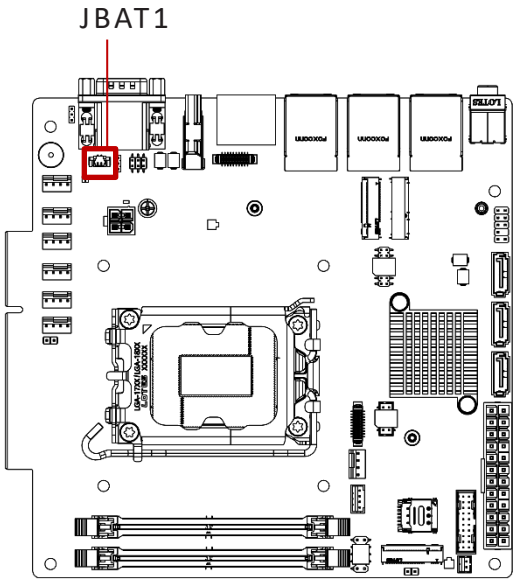
  This port is backward-compatible with USB 2.0 devices and supports data transfer rate up to 5 Gbit/s (SuperSpeed).



	1	5V	2	USB_3.2RX-
	3	USB_3.2RX+	4	GND
	5	USB_3.2TX-	6	USB_3.2TX+
	7	GND	8	USB_D-
	9	USB_D+	10	NC
	11	USB_D+	12	USB_D-
	13	GND	14	USB_3.2TX+
	15	USB_3.2TX-	16	GND
	17	USB_3.2RX+	18	USB_3.2RX-
	19	5V	20	NoPin

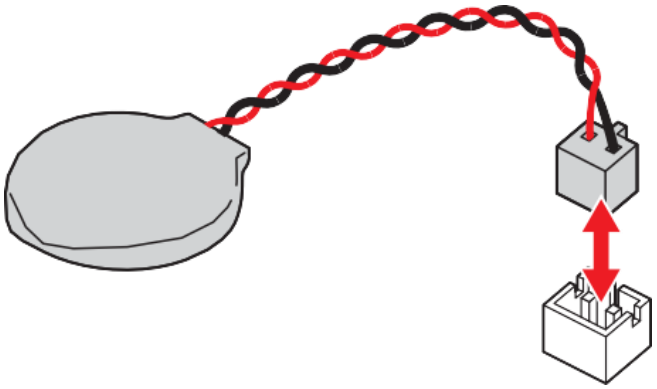
- **JBAT1: CMOS Battery Header**

  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.

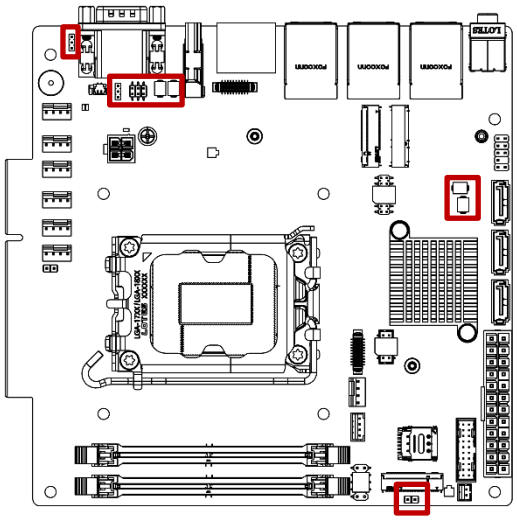


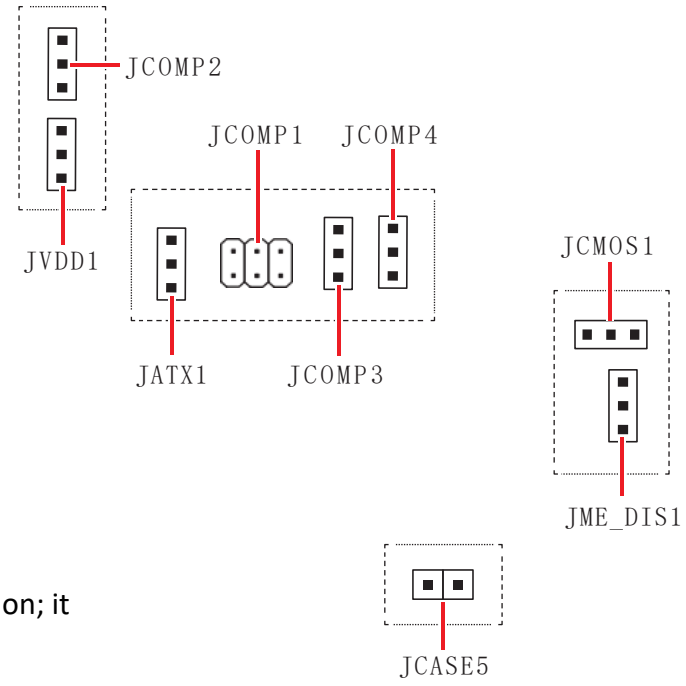
WARNING

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.

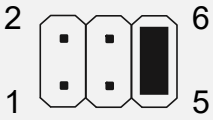
2.8 Jumpers

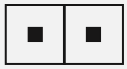




- **Important**

  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 JCOMP3 JCOMP4		COM Voltage Select Jumper 1-2: 5V Power (Default) 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		AT/ ATX Mode Select Jumper 1-2: ATX (Default) 2-3: AT
JVDD1		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.

Chapter 3

System Setup

3.1 Rail Kit Installation Guide

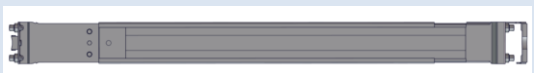
The purpose of this document is to provide the steps to install rail kit (PN: 3RAMISAQ001) to the enclosure and the enclosure to the rack.

WARNING

To ensure safety and prevent system damage, before disassembly, please switch off the system and disconnect the unit from its power source.

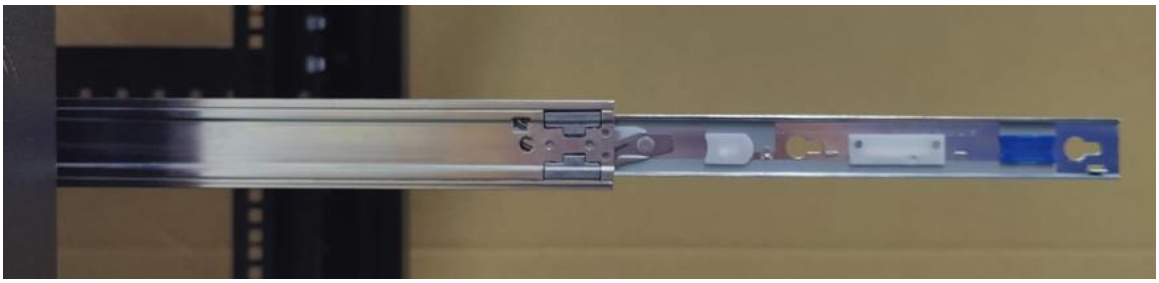
LLM-1U-RPL Edge AI Rackmount Server

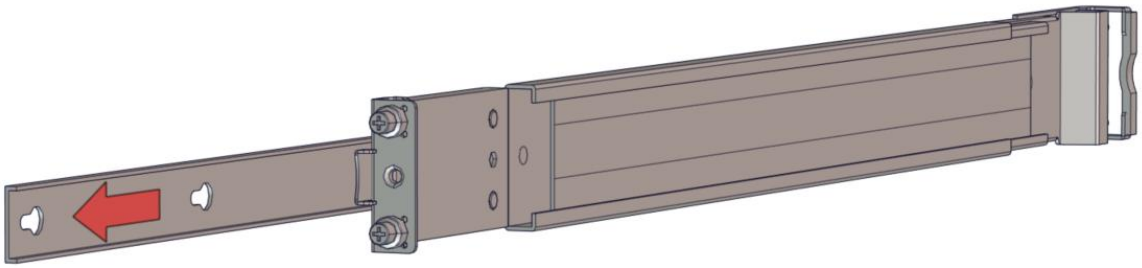
The rail kit comes with the following:

No.	Description	Qty	
1	Rail kit assembly (left and right)	1 set	
2	Inner rail screws	2	

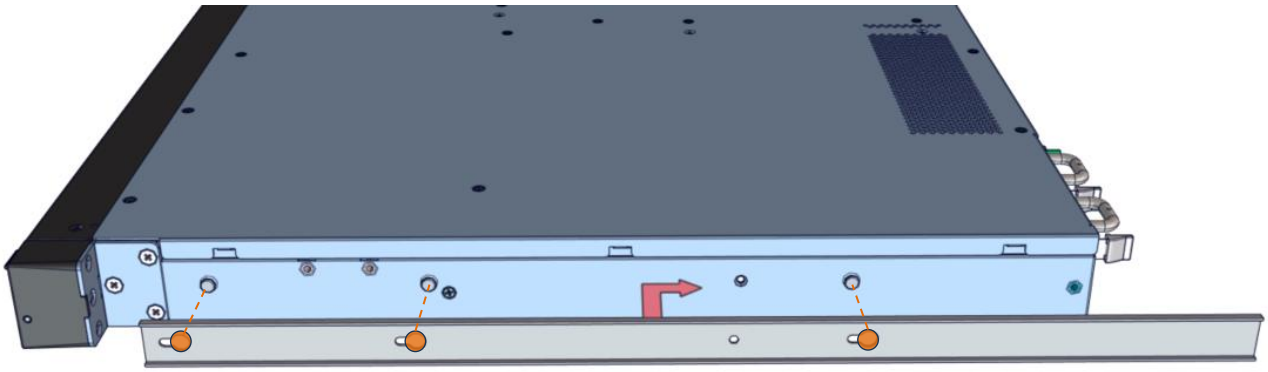
1. Remove the rail kit from the box

2. Separate the inner rails from the main assembly. Slide the white latch forward when the inner rail is halfway out for a complete removal.



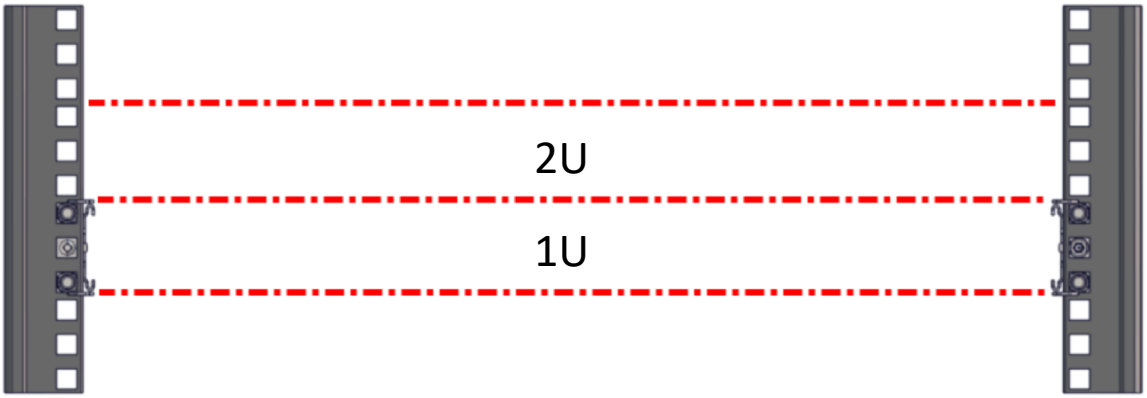


3. Install the inner rail to the sides of the enclosure. Align the holes of the inner rail to the pins of the enclosure, then slide it towards the back.

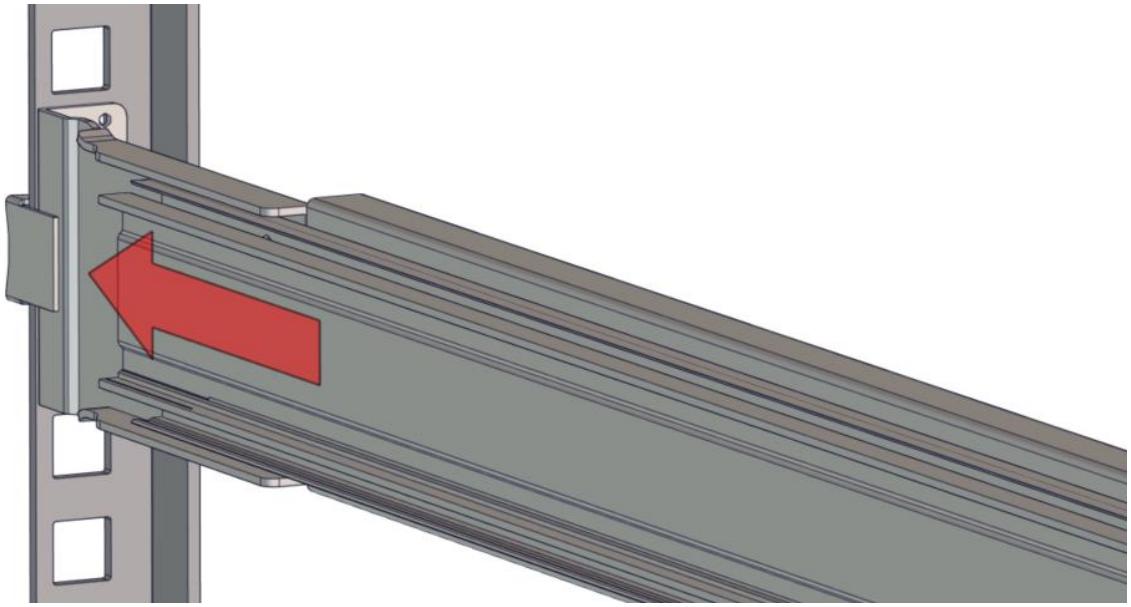


4. Secure the inner rails with the provided screws.

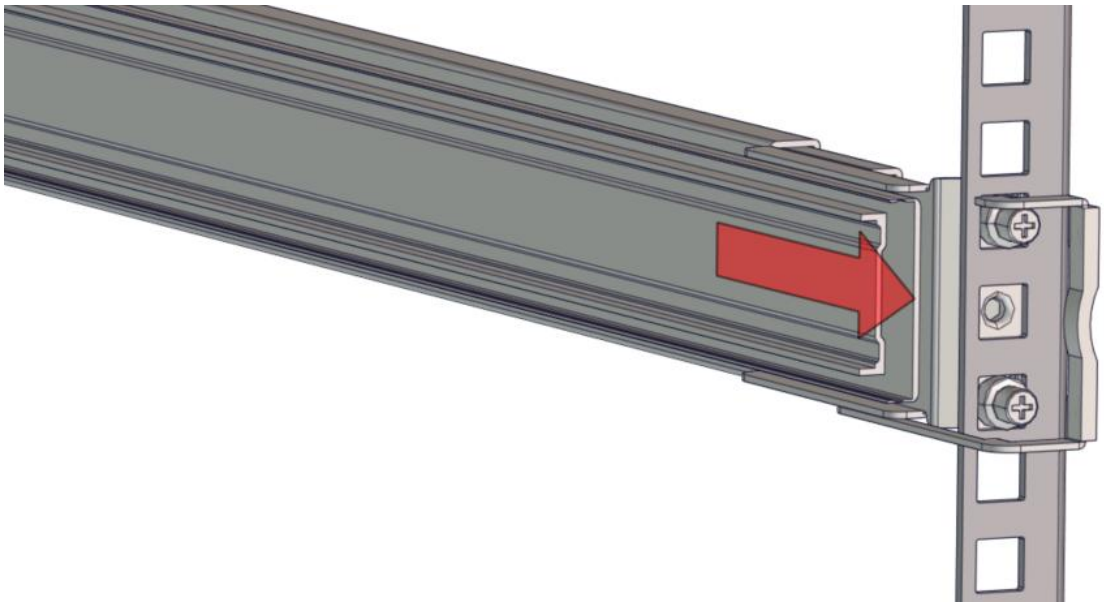
5. Note the location of where the rail will be on the rack



6. Mount the cabinet section rails into the cabinet rack using the tool-less installation features. Locate the desired "U" space and align the guide pins through the rack flange. The clamp hooks will ramp around the flange and hook on automatically. Move to the back of the rack to complete the installation.



7. Apply the same procedure to align the pins on the same "U" space location as in the front. Adjust the rails to the appropriate rack depth and align the guide pins through the rack flange. The clamp hooks will ramp around the flange and hook on automatically. Secure the rail to the rear posts with screws, if needed.

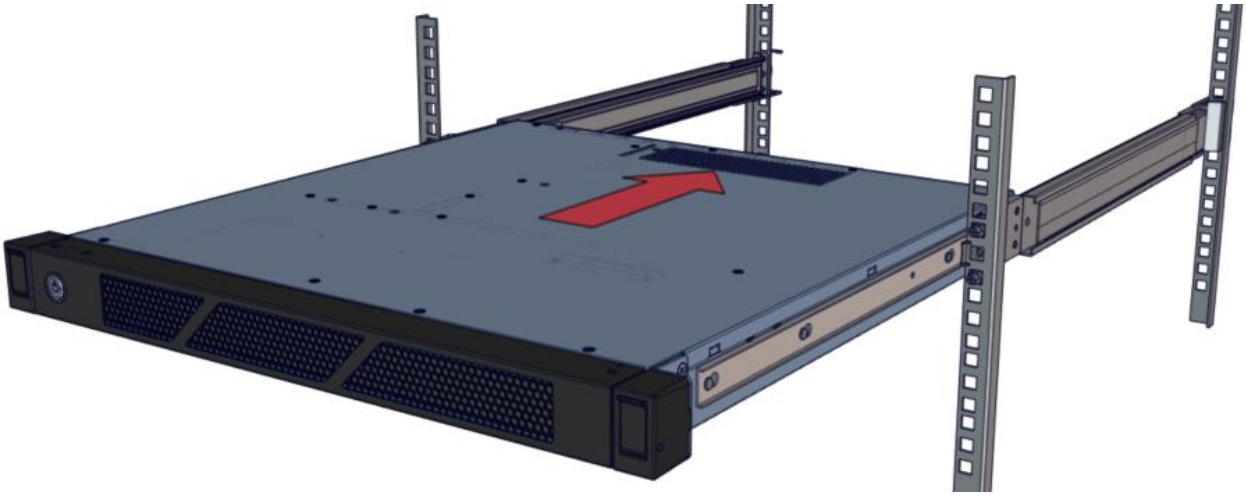


8. Lift the enclosure and align it towards the front of the installed outer rail

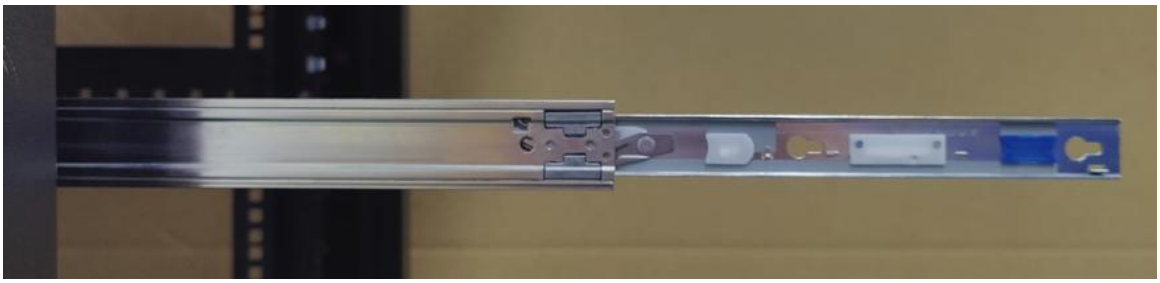
At least two people are recommended for mounting process.

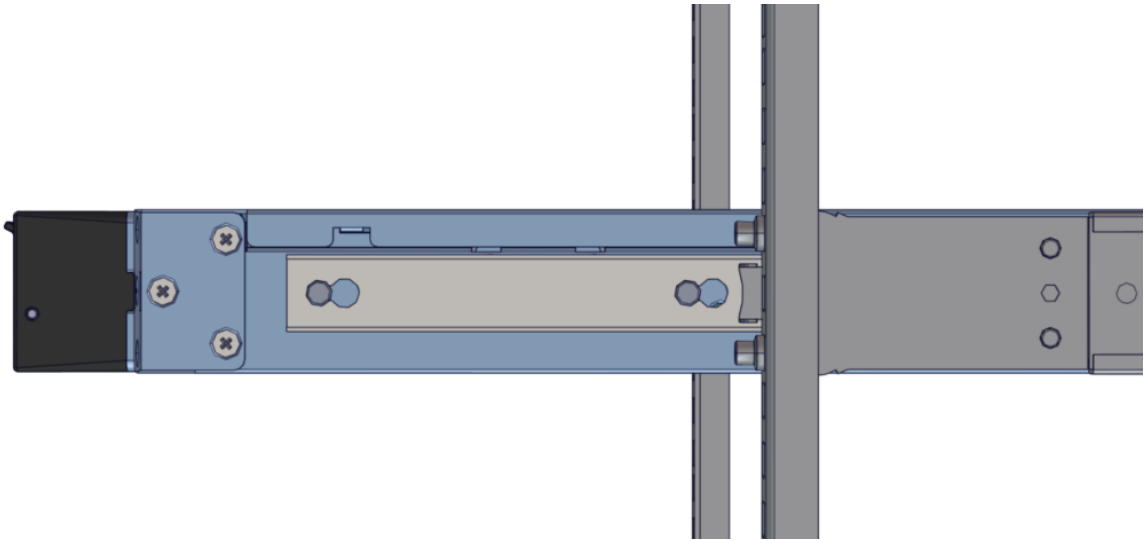
It is recommended to mount the unit with no hard drives installed.

9. Slide the enclosure toward the back of the rack.

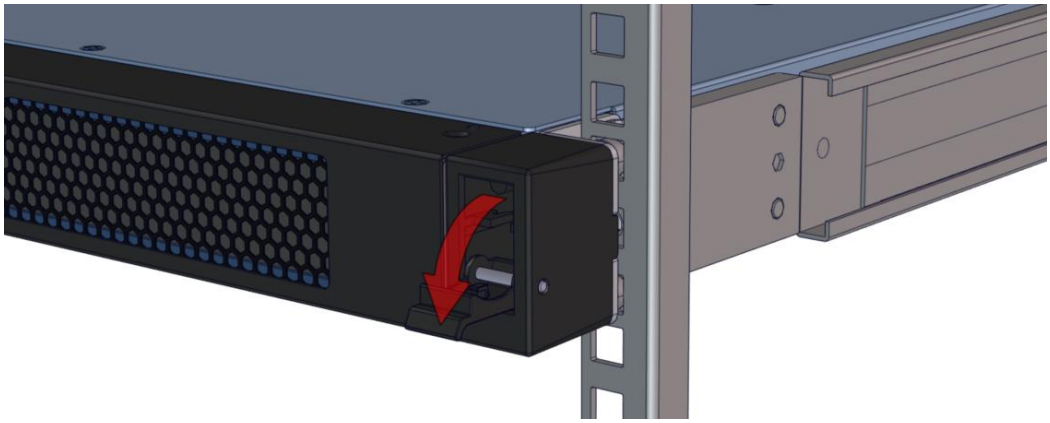


10. Slide the blue inner rail latch for complete insertion.

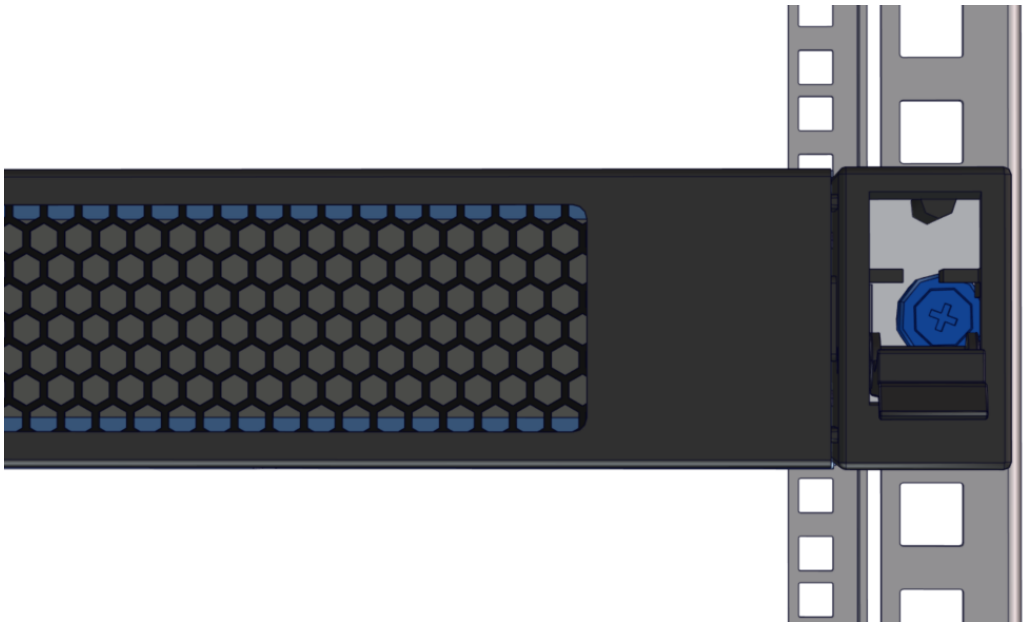




11. Open the covers of the enclosure's ears



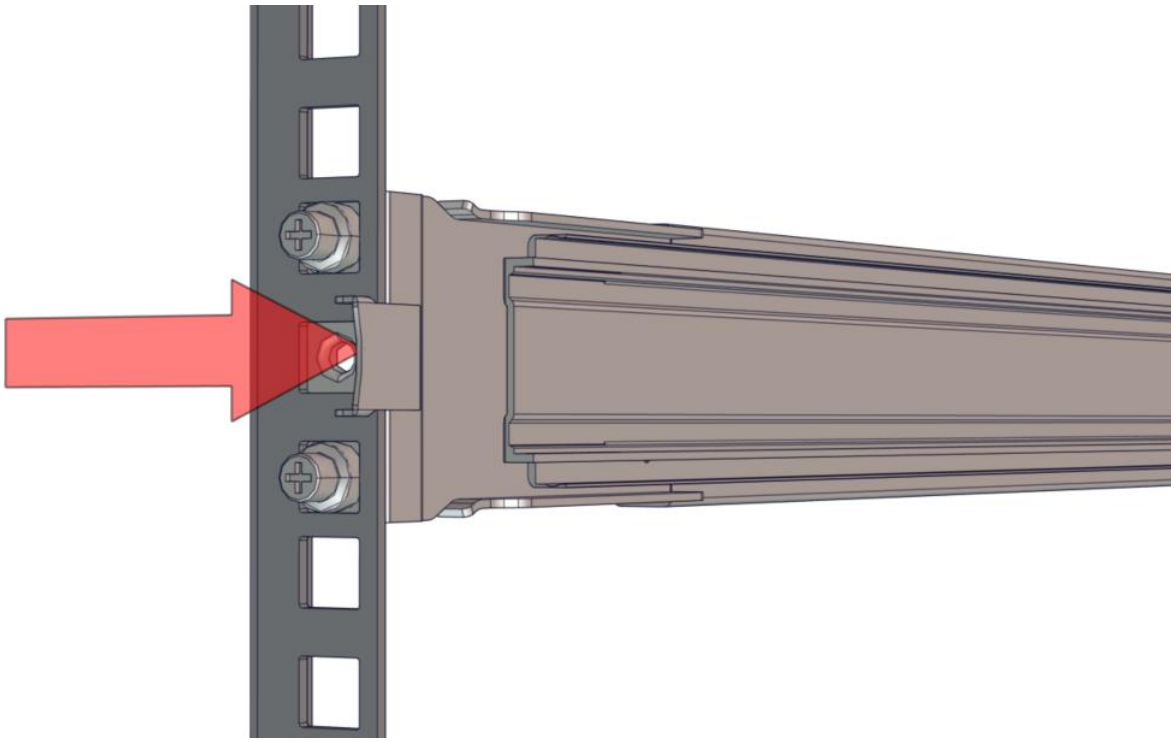
12. Tighten the thumbscrews into the rail kit



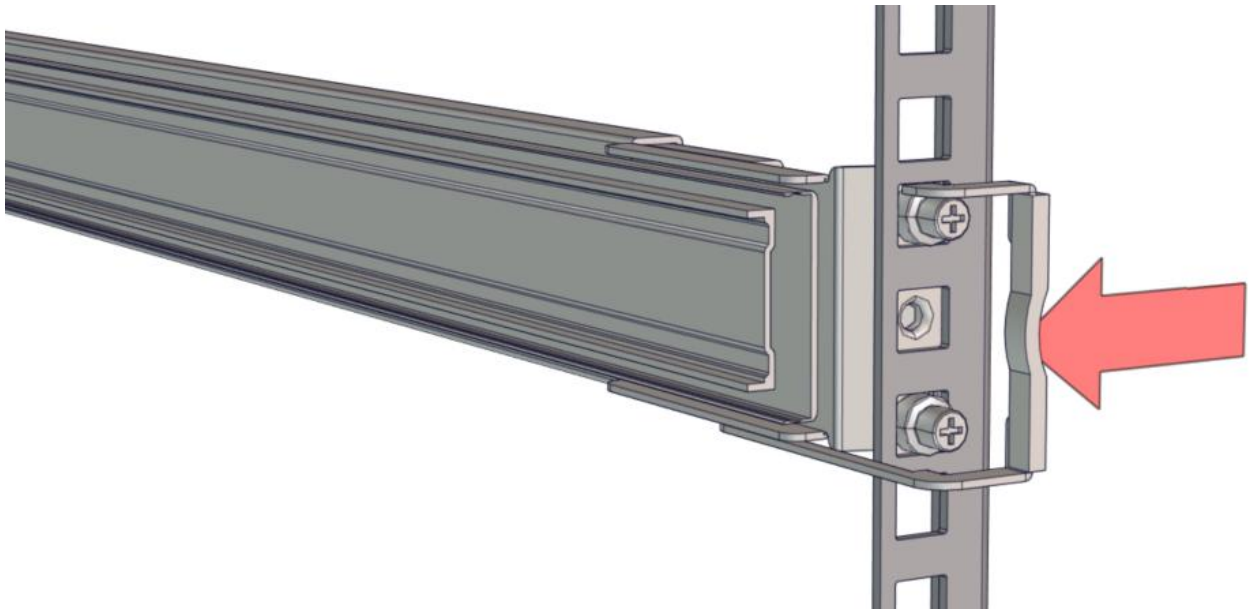
How to remove rail kit assembly from the rack

Press the spring-loaded assembly on the end of the rail kit to release the clamp hook from the rack flange.

Front:



Rear:



Chapter 4

BIOS Setup

4.1 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.

4.1.1 Control Keys

← →	SelectScreen
↑ ↓	SelectItem
Enter	Select
+ -	ChangeValue
Esc	Exit
F1	GeneralHelp
F7	PreviousValues
F9	OptimizedDefaults
F10	Save&Reset*
F12	Screenshotcapture
<K>	Scrollhelpareaupwards
<M>	Scrollhelpareadownwards

* 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.

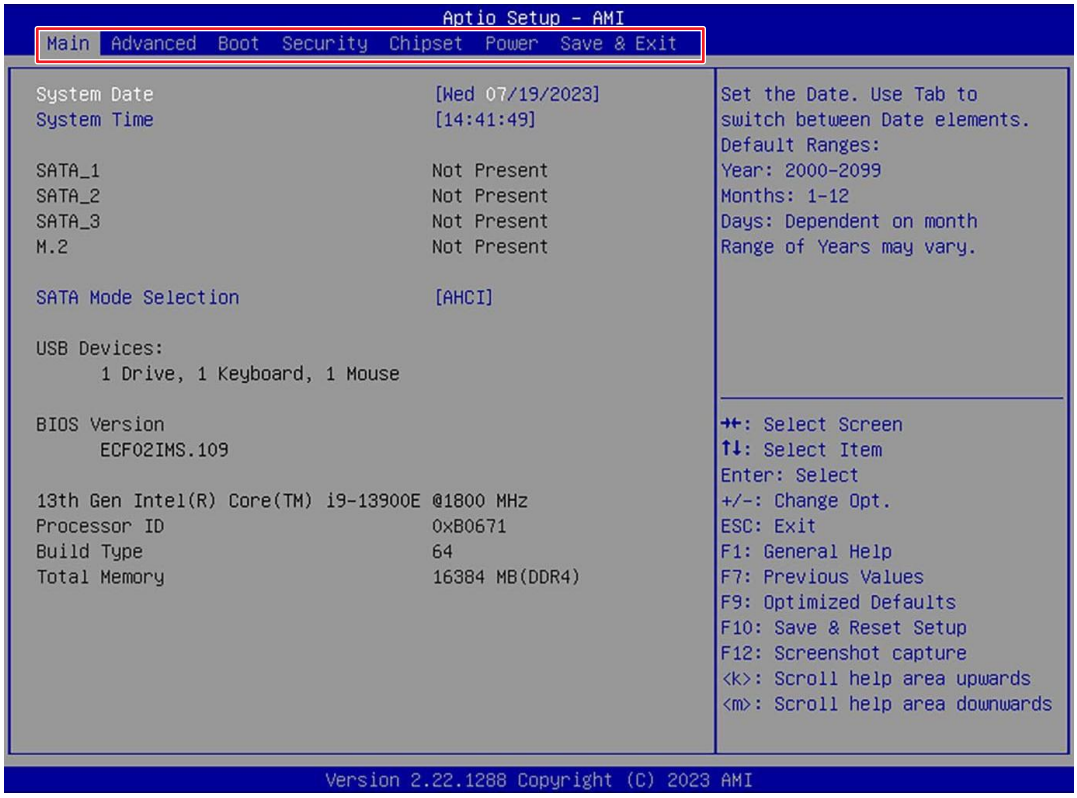
Sub-Menu

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.

4.1.2 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.

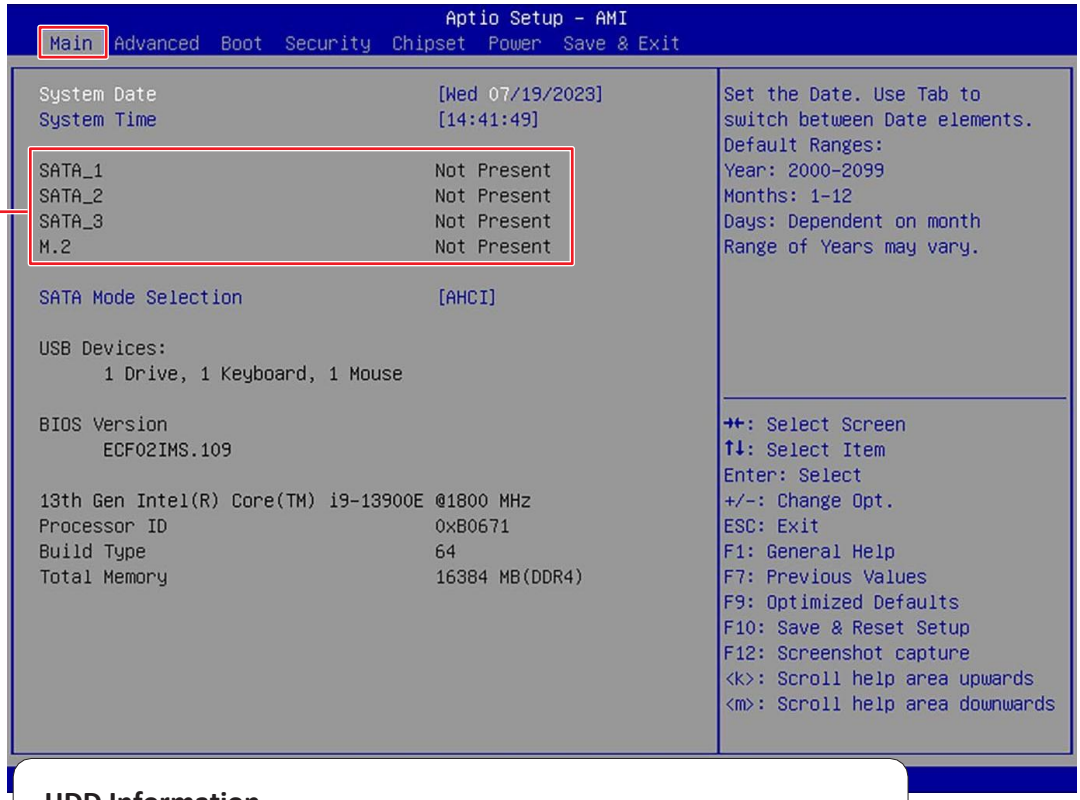
▶ **Power**

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.

4.2 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

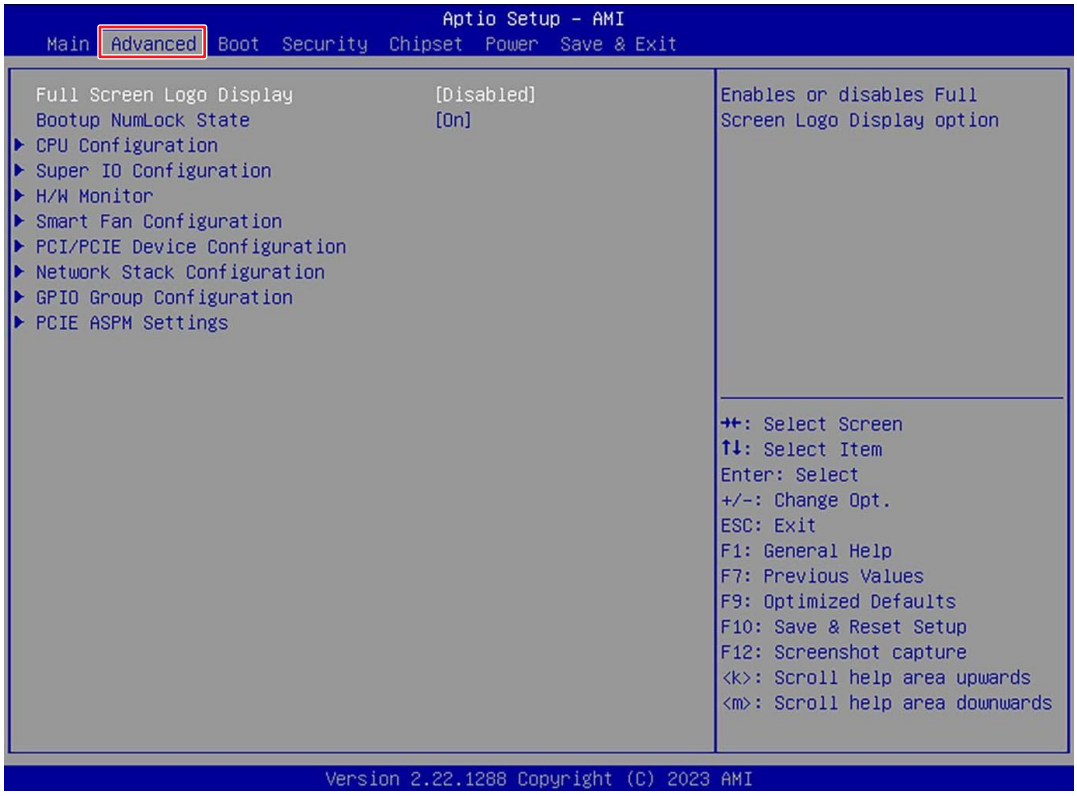
This setting specifies SATA controller mode.

[AHCI]	AHCI (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.

⚠Important

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

4.3 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.

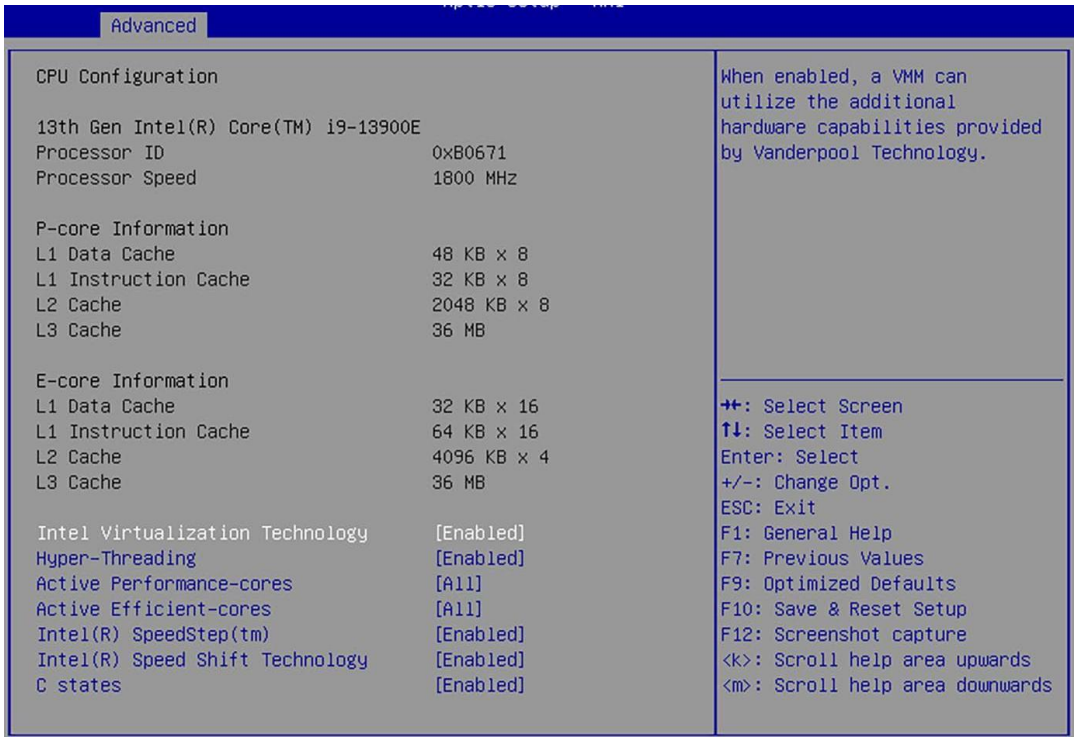
Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

▶ 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.

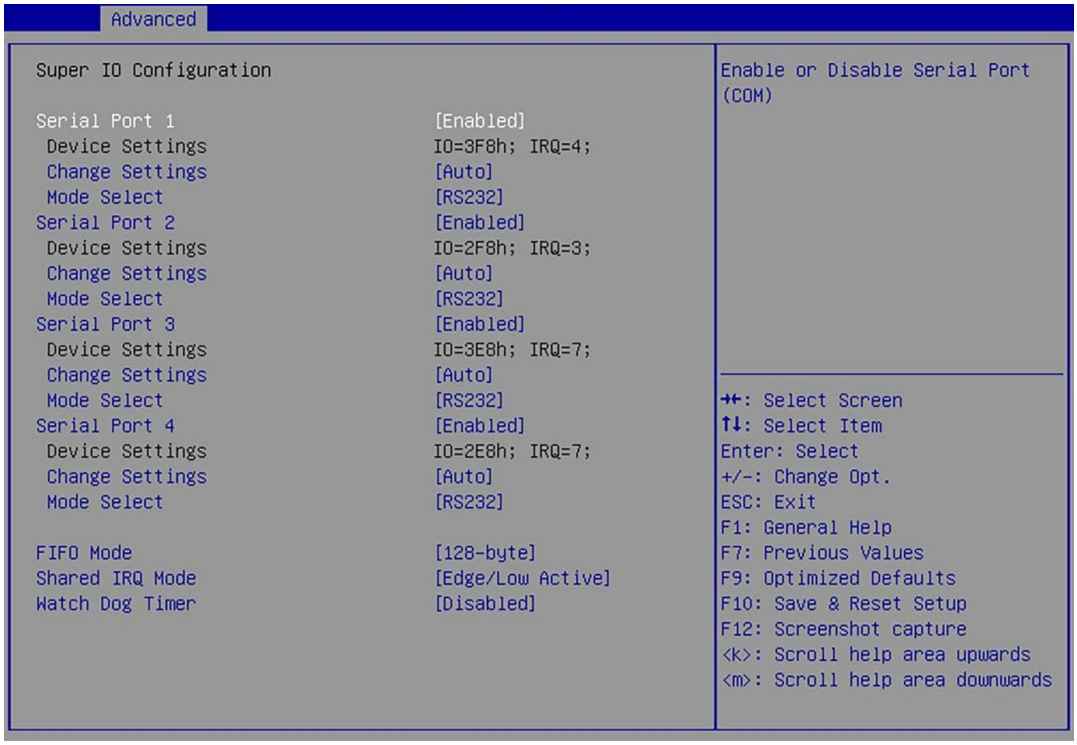
▶ **C States**

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

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

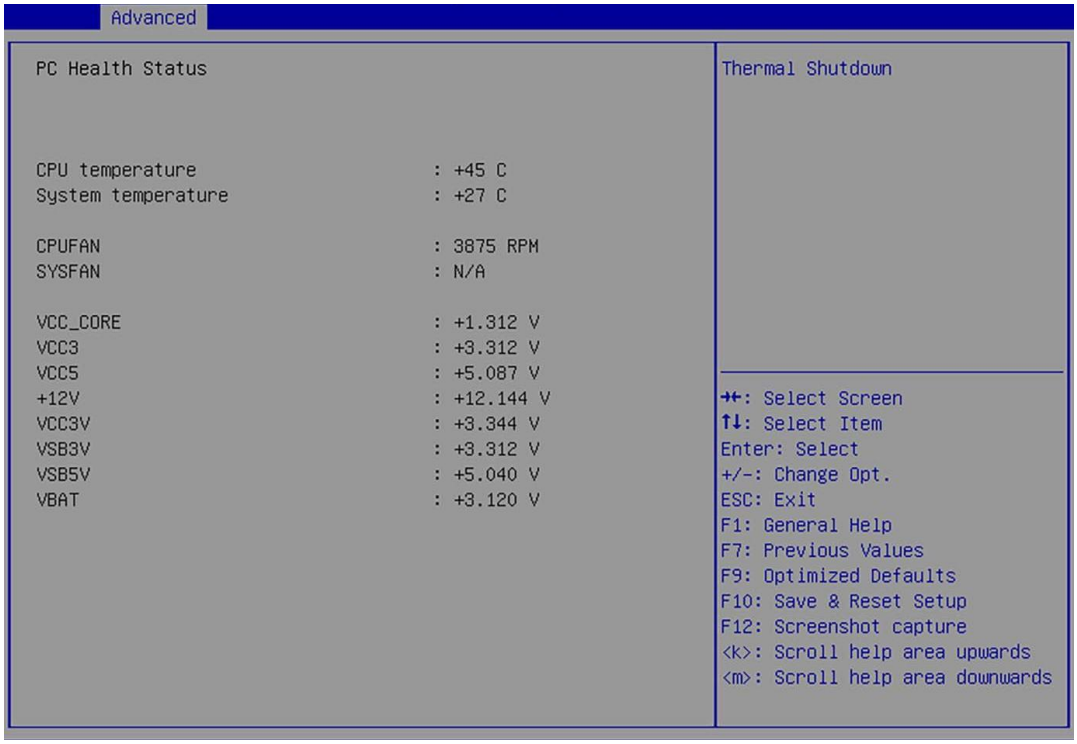
This setting provides the system with the ability to share interrupts among its serial ports.

▶ 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 current 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

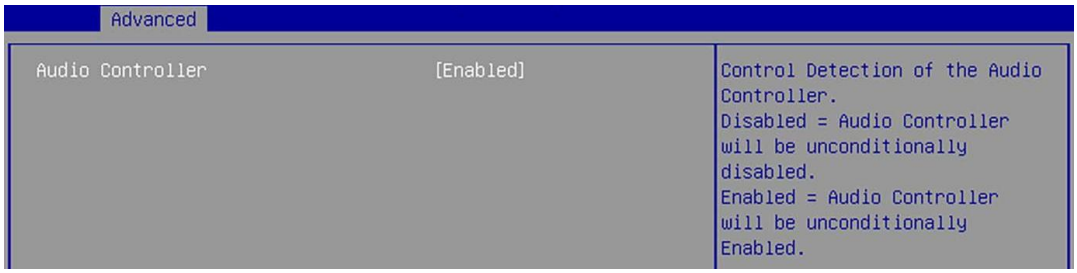
▶ CPUFAN/ SYSFAN

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.

» **Min. Speed (%)**

The beginning speed of the System fan.

▶ PCI/PCIE Device Configuration

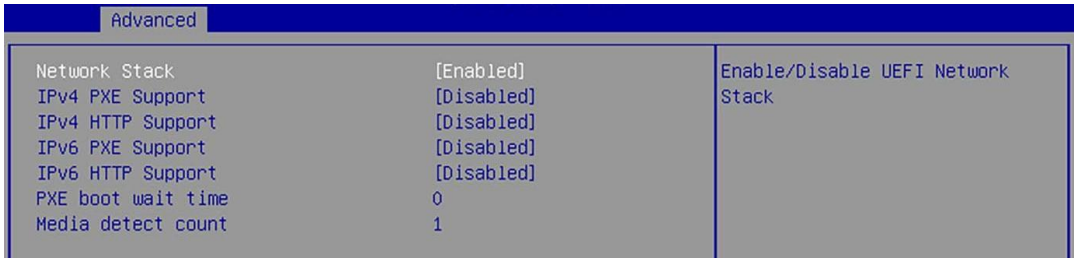


▶ Audio Controller

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.

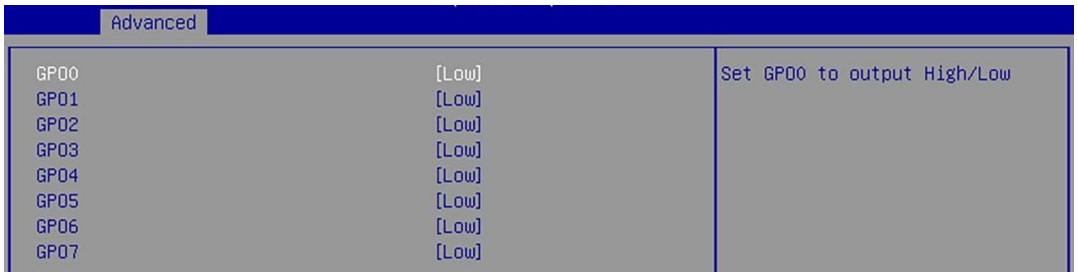
» **PXE boot wait time**

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

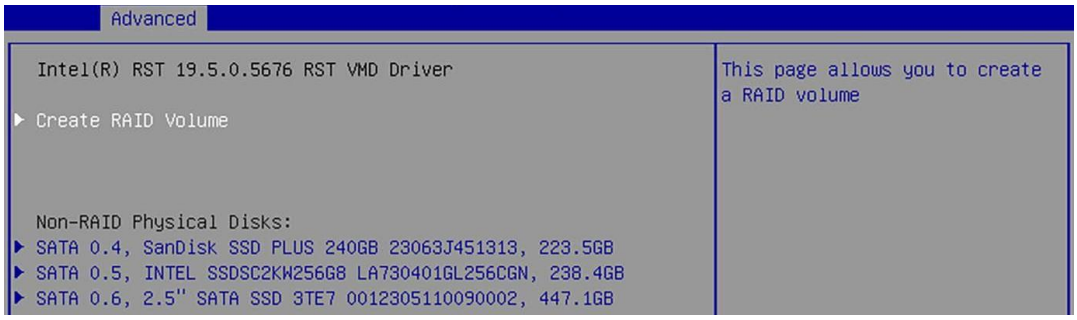


▶ GPO0 ~ GPO7

These settings control the operation mode of the specified GPIO.

▶ 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.

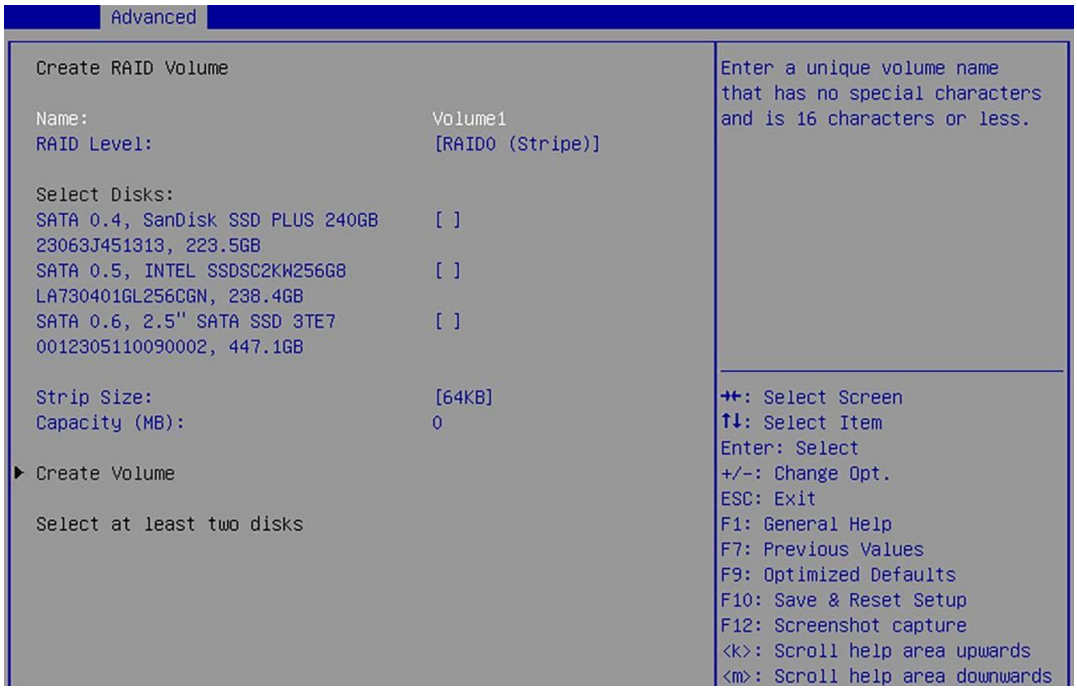


Important

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

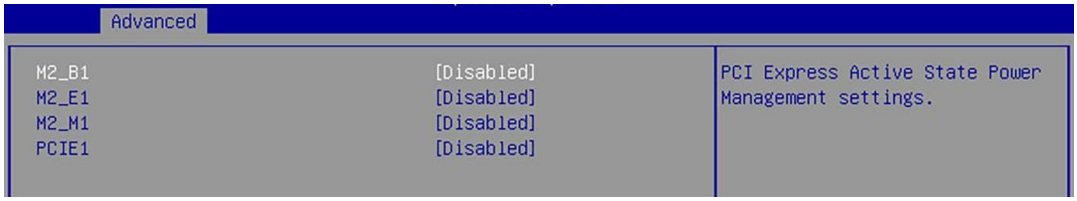
▶ Create RAID Volume

This menu allows for the management of RAID volumes.



▶ PCIE ASPM settings

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

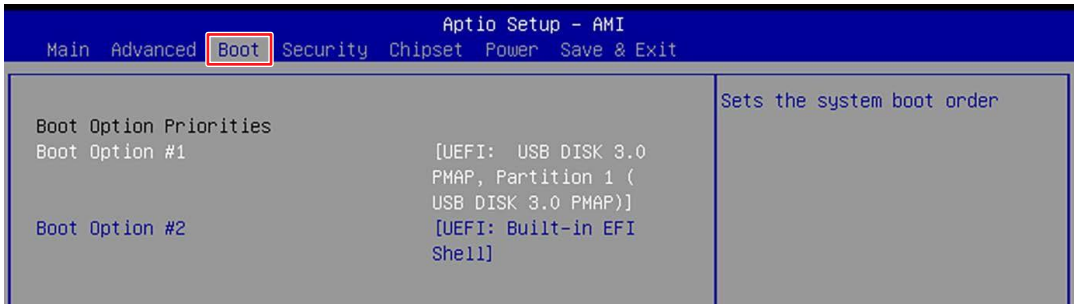


▶ M2_B1/ M2_E1/ M2_M1/ PCIE1

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.

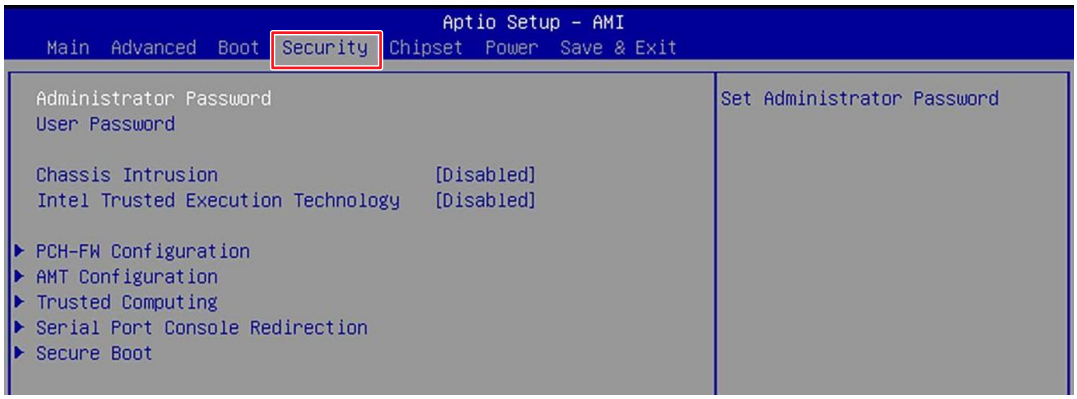
4.4 Boot



▶ Boot Option #1-2

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

4.5 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

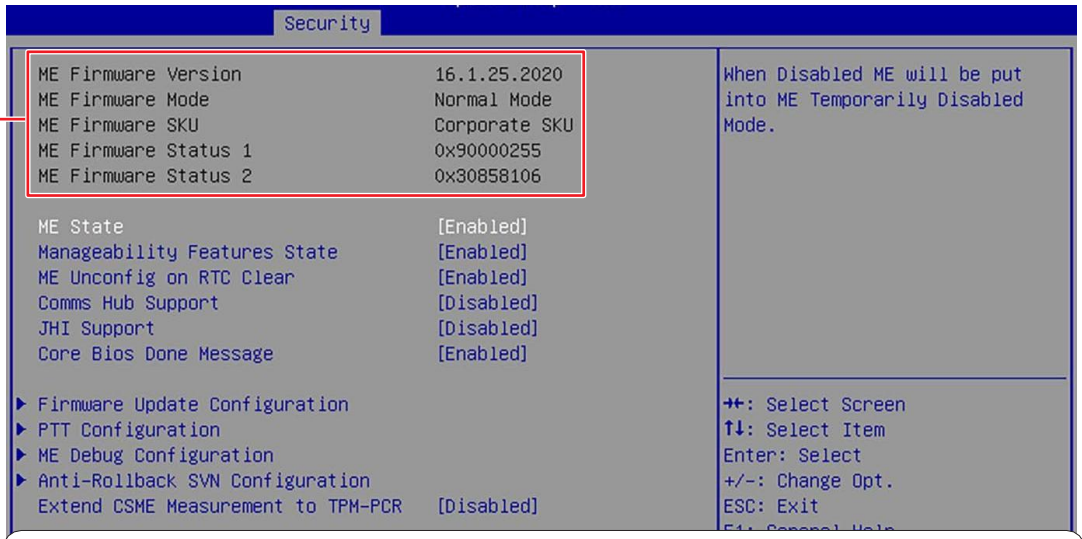
Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware- based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

Important

- The following items **must be enabled** before **"Intel Trusted Execution Technology"** can be enabled:
  - All Intel processor cores
  - Hyper-threading
  - Intel Virtualization Technology (VT-x)
  - 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.



Firmware Information

ME Firmware Version	ME Firmware SKU	These settings show the firmware information of the Intel ME (Management Engine).
ME Firmware Mode	ME Firmware Status 1-2	

▶ 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**

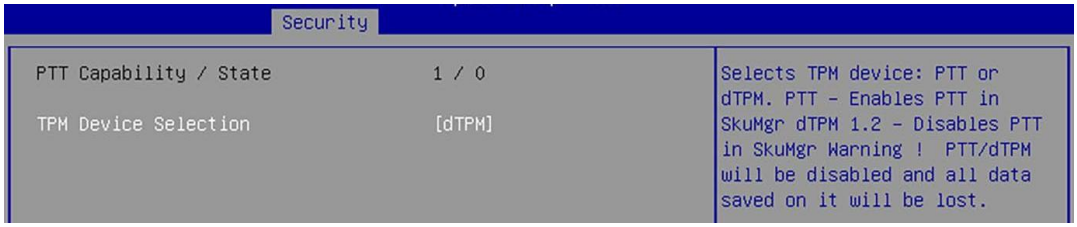
Enables or disables the ME Firmware Image Re-flashing**.**

» **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.



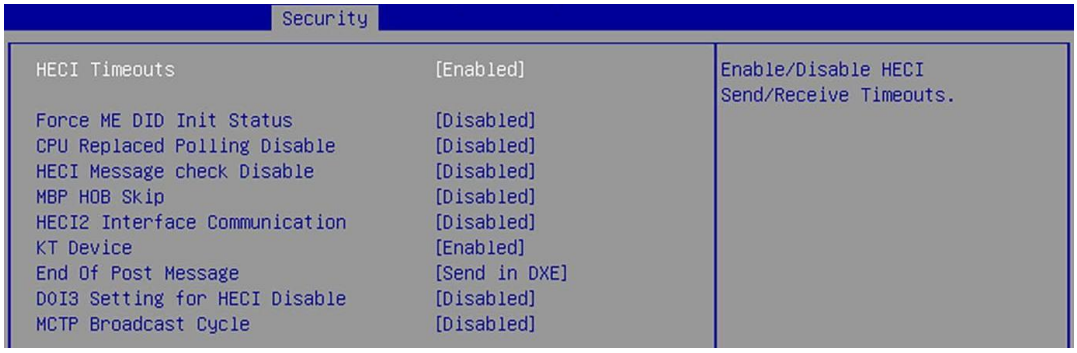
» **TPM Device Selection**

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.

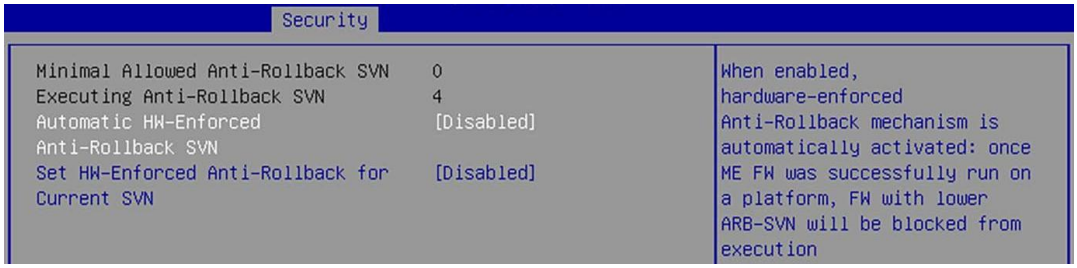
» **DOI3 Setting for HECI Disable**

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.

▶ **Extend CSME Measurement to TPM-PCR**

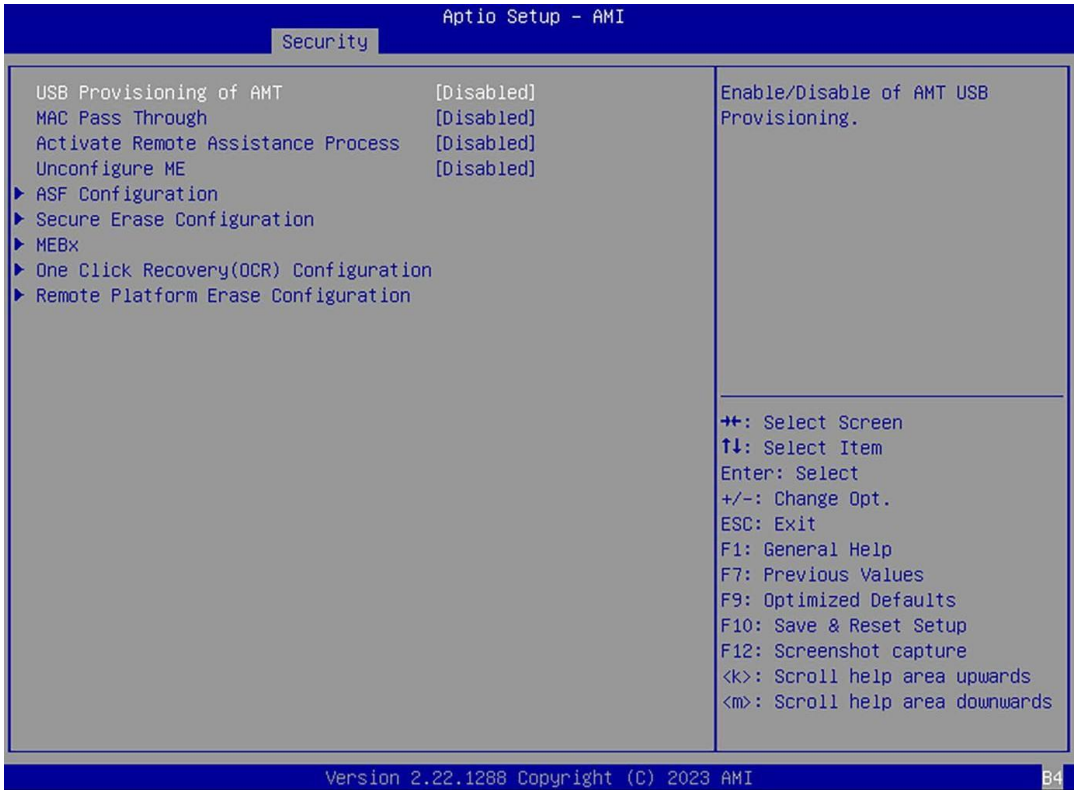
Enables or disables the Extend CSME Measurement to TPM-PCR. This item enables capturing and recording the Intel® Converged Security and Management Engine (Intel® CSME) firmware in the Trusted Platform Module Platform Configuration Registers (TPM-PCR). This enhances system security by protecting against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

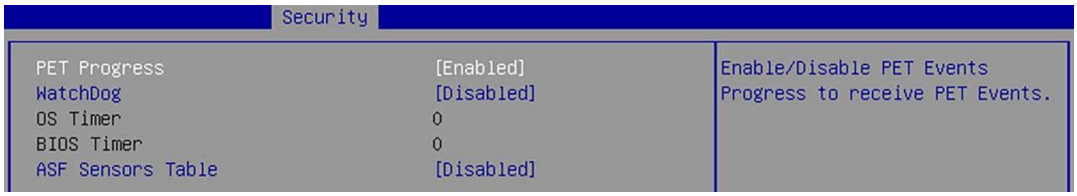
▶ Activate Remote Assistance Process

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.

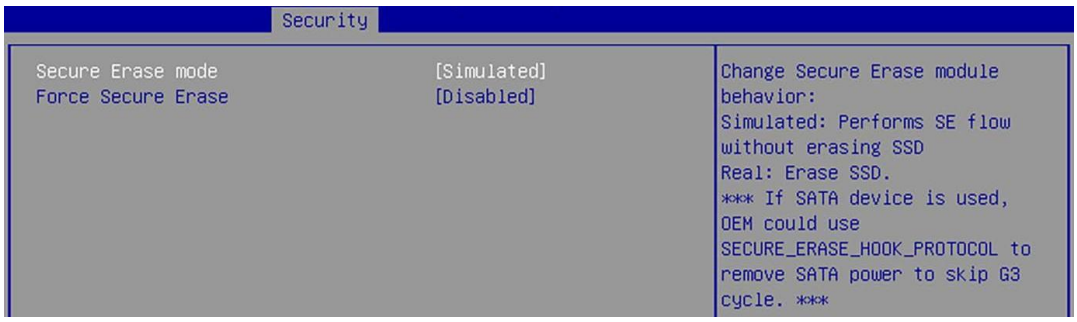
» **BIOS Timer**

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 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)

» **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.

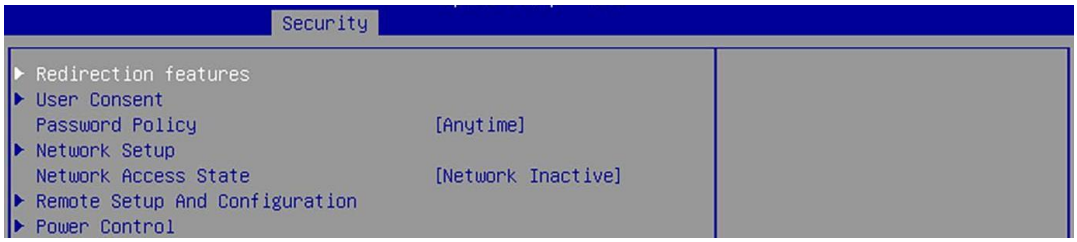
» **Intel(R) AMT**

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

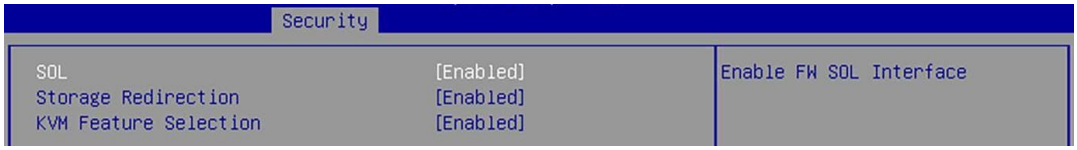
Important

The **MEBx menu** can be accessed only by pressing the **<DEL> 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**

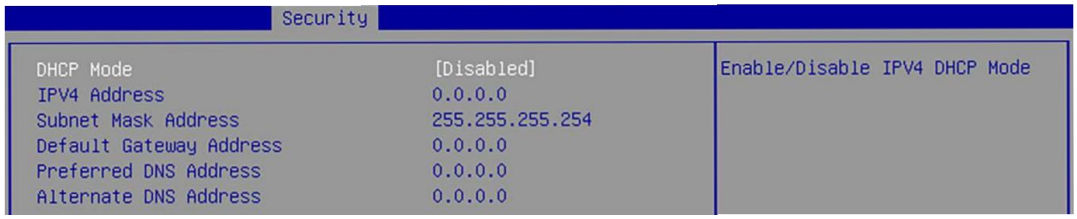
  Determines if the Intel® ME Fully Qualified Domain Name (FQDN, which is "HostName. DomainName") is **shared** with the host OS or **dedicated** exclusively to the Intel ME.

- **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**

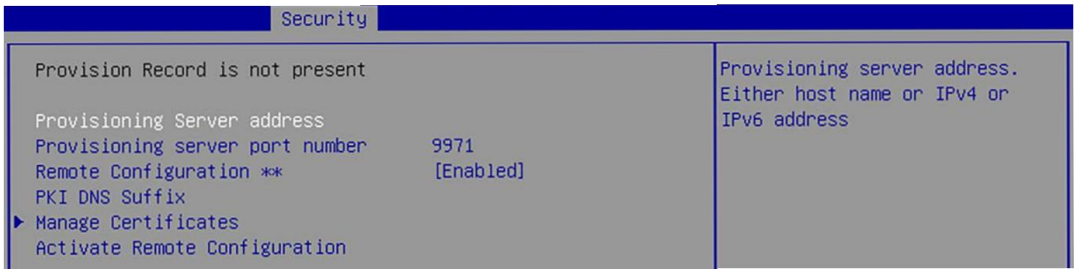
[Network Active]

[Network Inactive]

[Full Unprovision]

The IPv6 Interface ID is automatically generated using a random number as described in RFC 3041.

» **Remote Setup And Configuration**

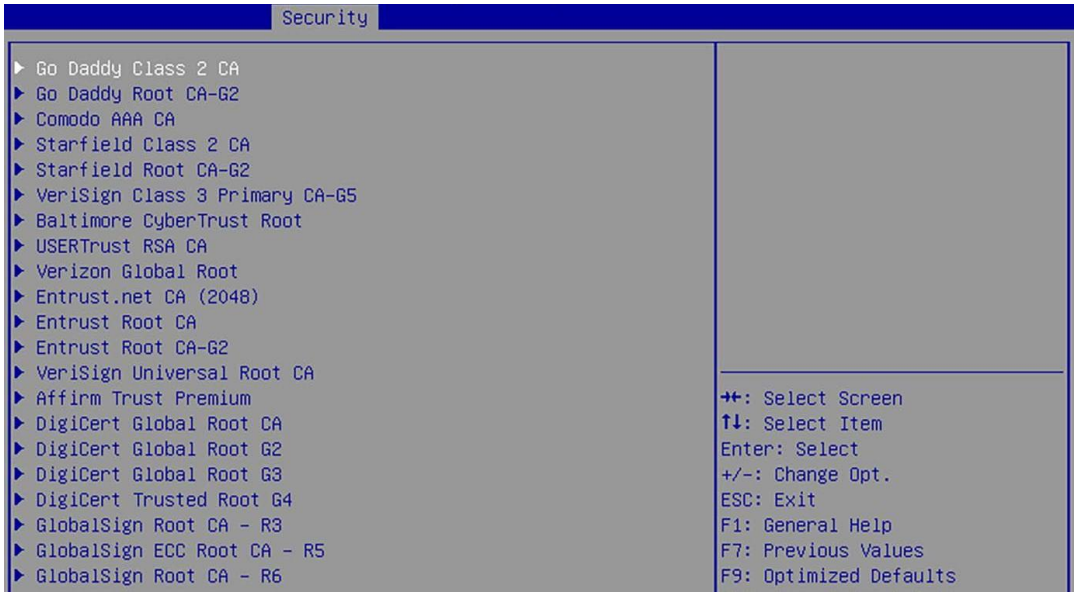


- **Remote Configuration****

  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:

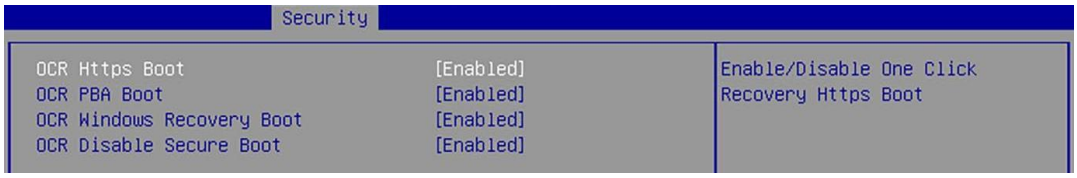


The details of the selected certificate hash includes "Hash Name, Active State, Default State, Hash Type and Hash Data".

» 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**

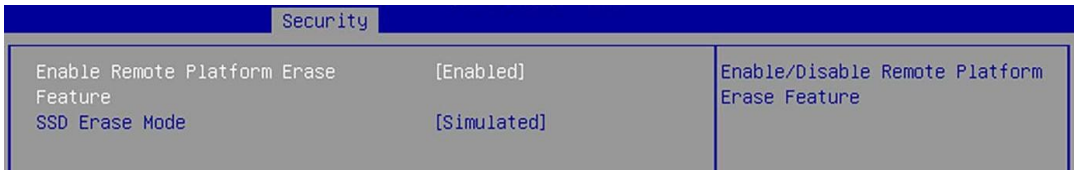
Enables or disables the Windows Recovery Boot for the OCR boot process. When enabled, the OCR boot process will prioritize Windows recovery options, allowing users to restore the system to a previous Windows state or initiate other Windows-specific recovery procedures.

» **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**

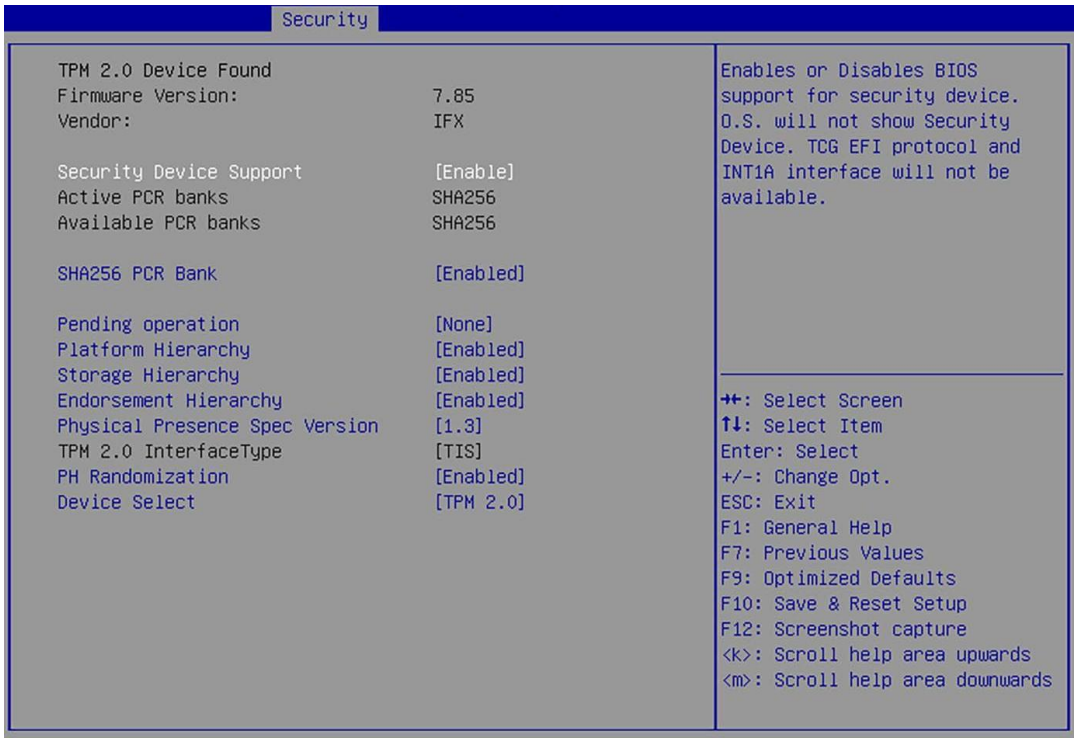
Enables or disables the ability to initiate the remote erasure process for the system or selected storage devices.

» **SSD Erase Mode**

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

[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 enables or disables 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 enables or disables the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

▶ Physical Presence Spec Version

This settings show the Physical Presence Spec Version.

▶ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

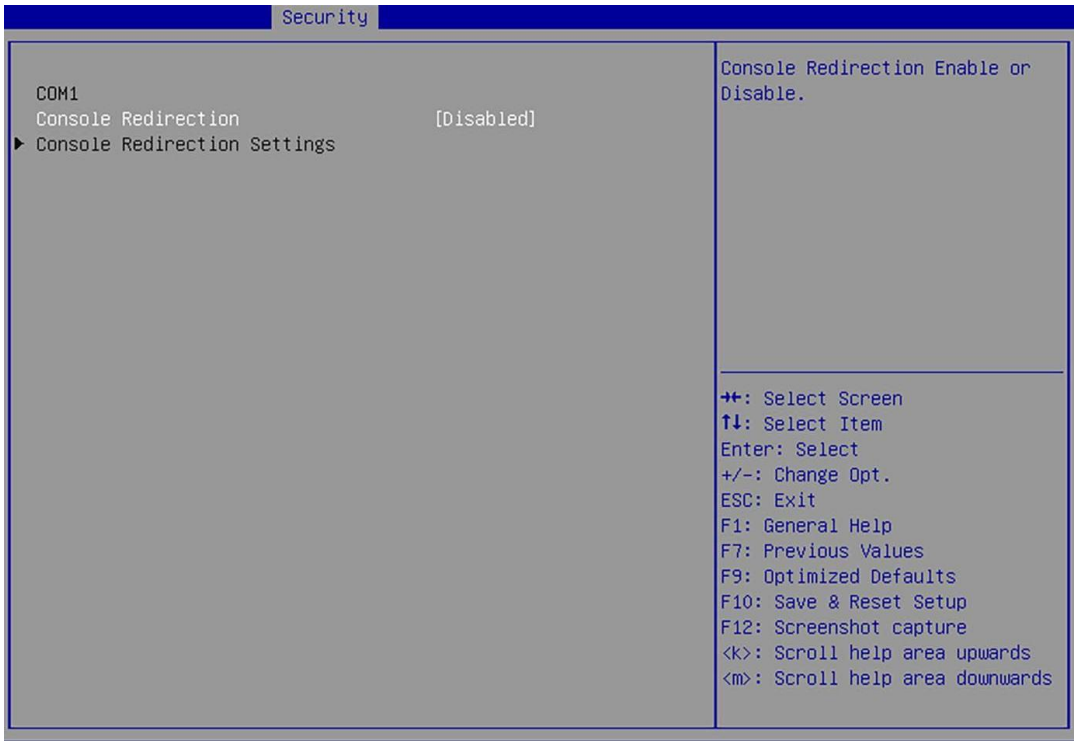
▶ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

▶ Device Select

Select your TPM device through this setting.

▶ Serial Port Console Redirection

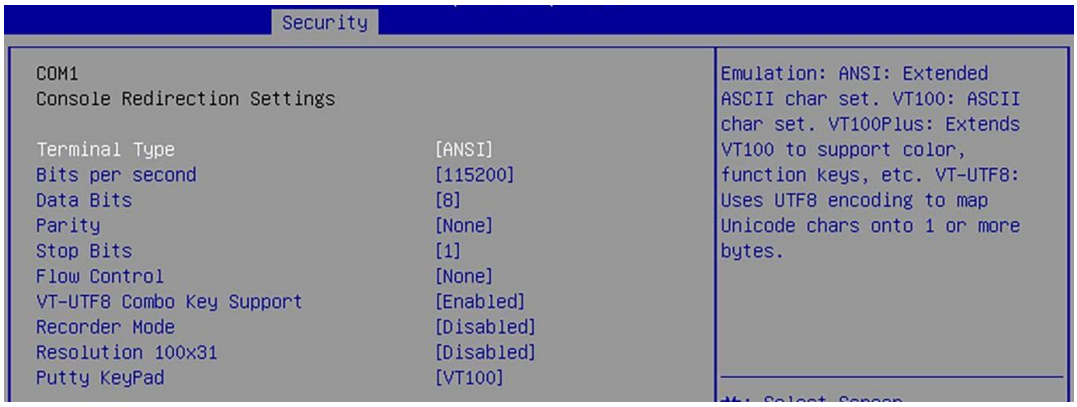


▶ Console Redirection

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

▶ Console Redirection Settings (COM1)

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.

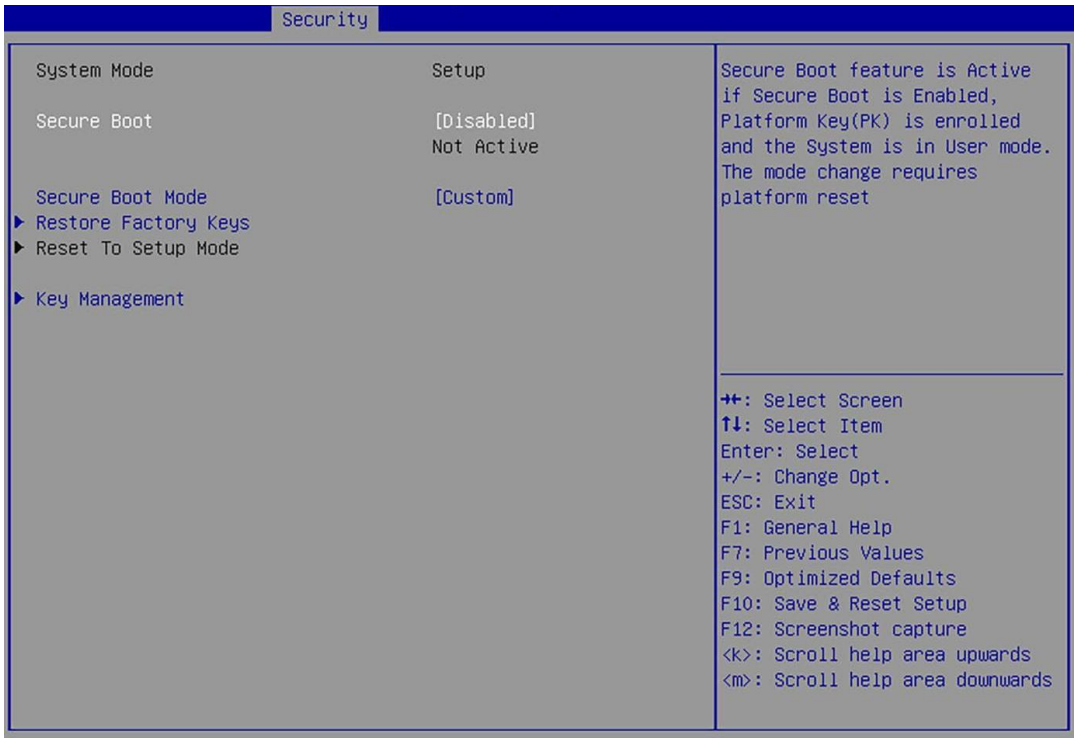
» Recorder Mode, Resolution 100x31

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

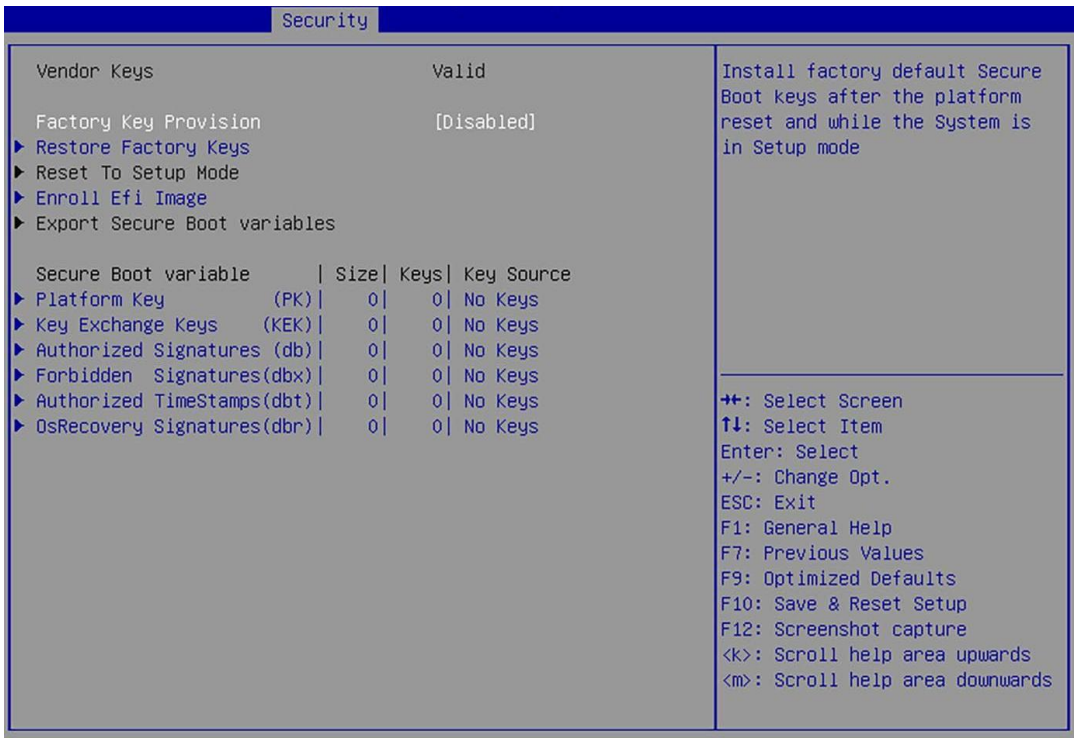
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▶ 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.

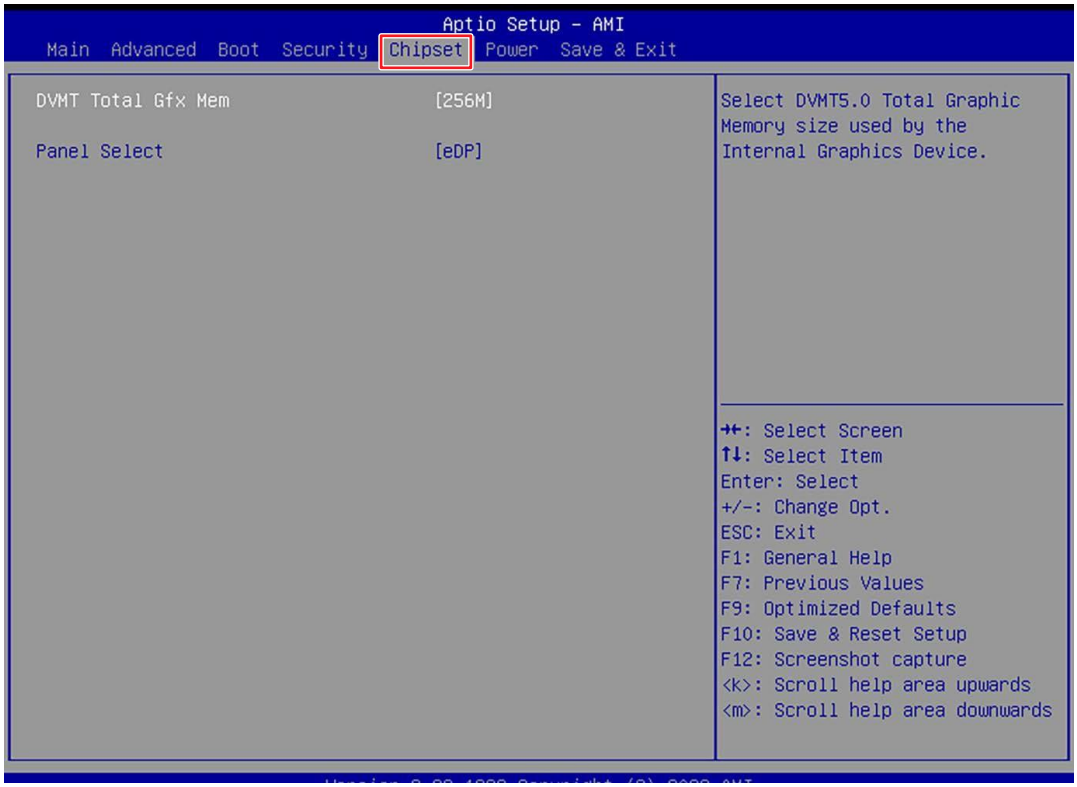
» **Append Key**

Loads an additional DBT from storage devices to your system.

» **OsRecovery Singnatures (dbr):**

Lists the available signatures for OS recovery.

4.6 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

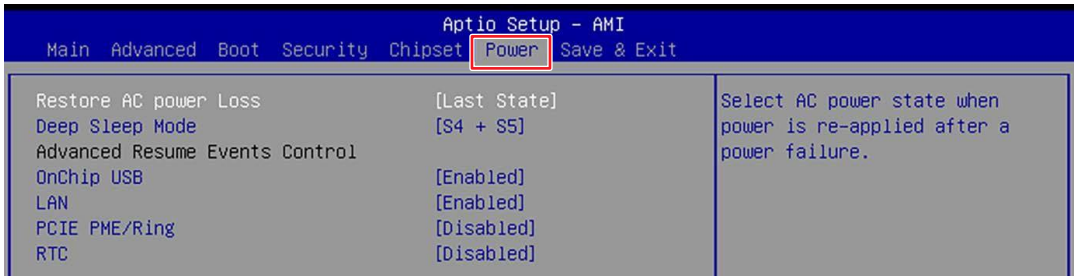
This setting specifies the LCD Panel's resolution and distribution formats. The item **will display when LVDS is enabled**.

▶ 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%

4.7 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.

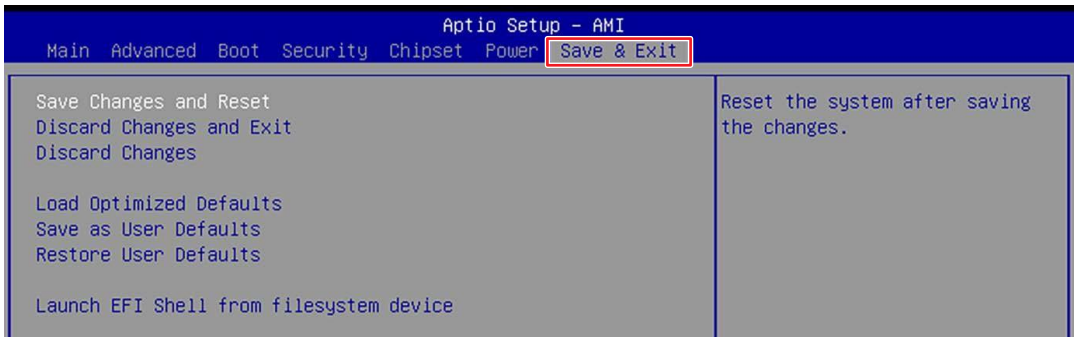
▶ PCIE PME/Ring

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

4.8 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 SMBus Access Programming

GPIO WDT BKL Programming

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) and LVDS Backlight 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	0x22	Bit 4	**N_GPO0**	0x11	Bit 4
N_GPI1	0x22	Bit 5	**N_GPO1**	0x11	Bit 5
N_GPI2	0x22	Bit 6	**N_GPO2**	0x11	Bit 6
N_GPI3	0x22	Bit 7	**N_GPO3**	0x11	Bit 7
N_GPI4	0x42	Bit 0	**N_GPO4**	0x21	Bit 0
N_GPI5	0x42	Bit 1	**N_GPO5**	0x21	Bit 1
N_GPI6	0x42	Bit 2	**N_GPO6**	0x21	Bit 2
N_GPI7	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. 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.
```

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,              // Read value from N_GPI3 port through SMBus.
0x22);  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.

1. Set WDT Time Unit

```
val = Inportb (WDT_BASE +                  // Read current WDT setting
0x05);  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 +                  // Read current WDT_PME setting
0x0A);  val = val | 0x01;                  // Enable WDT OUT: WDOUT_EN (bit 0) set to 1.
Outportb (WDT_BASE + 0x0A,                 // Write back WDT setting.
val);  val = Inportb (WDT_BASE +           // Read current WDT setting
0x05);  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 +                  // Read current WDT setting
0x05);  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 +                    // Read current WDT setting.
0x05);  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 +                    // Read current WDT setting
0x05);  val = val | 0x40;                    // Set 1 to WDTMOUT_STS (bit 6);
Outportb (WDT_BASE + 0x05, val);          // Write back WDT setting
```

LVDS Backlight Control - BKL

3. LVDS Backlight Control – BKL

The controller support **LVDS** backlight level control from 0(0%) to 255(100%), the default backlight level is 100%. It must be controlled by SMBus access. The details of SMBus access (SMBus_ReadByte, SMBus_WriteByte) are provided in this document.

1. Set the Level of LVDS Backlight

1. Write **0x0D** into address **0x00** on SMBus device **0x42**.
2. Write desired backlight level from 0(0%) to 255(100%) into address **0x35** on SMBus device **0x42**.

Example 3: Set **LVDS backlight level to** "100%"

SMBus_WriteByte (0x42, 0x00, 0x0D)

SMBus_WriteByte (0x42, 0x35, 0xFF)

2. Read the Level of LVDS Backlight

4. Write **0x0D** into address **0x00** on SMBus device 0x42.
5. Read current backlight level from address **0x35** on SMBus device **0x42**.

Example 4: Get **LVDS backlight level**

SMBus_WriteByte(0x42, 0x00, 0x0D);

BKL_Value = SMBus_ReadByte(0x42, 0x35);

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) & 0xfffffff0;
```

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