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

MS-CF02

Industrial Computer Board

User Guide

Contents

Revision

V1.0, 2023/05

Regulatory Notices

FCC-B Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and 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 in order 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

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

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/

Chemical Substances Information

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

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

Environmental Policy

- The product has been designed to enable proper reuse of parts and recycling and should not be thrown away at its end of life.
- Users should contact the local authorized point of collection for recycling and disposing of their end-of-life products.
- Visit the MSI website and locate a nearby distributor for further recycling information.
- Users may also reach us at gpcontdev@msi.com for information regarding proper Disposal, Take-back, Recycling, and Disassembly of MSI products.

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

Copyright and Trademarks Notice

HDMI™
HIGH-DEFINITION MULTIMEDIA INTERFACE

Technical Support

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

Safety Information

- 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 can not 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 into the computer.
  - The motherboard has been exposed to moisture.
  - The motherboard does not work well or you can not get it work according to user guide.
  - The motherboard has been dropped and damaged.
  - The motherboard has obvious sign of breakage.
- Do not leave this motherboard in an environment above 60°C (140°F), it may damage the motherboard.

Specifications

SKU1/ SKU2

Model	**MS-CF02-SKU1**	**MS-CF02-SKU2**
Form factor	Mini-ITX	
Dimensions	170 x 170mm (6.7 x 6.7 inches)	
Processor	• **13th** Gen Intel® **Raptor** Lake-S i9/i7/i5/i3 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 Pentium®/ Celeron® IOTG Series Processor, Max 65W - 1.6 GHz~5.1 GHz (depends on CPU) - Socket LGA 1700	
Chipset	**Intel® R680E**	**Intel® Q670E**
Memory	• 2 x DDR4 SO-DIMM slots (260-pin, vertical) - Up to 3200 MT/s - Up to 64GB	
	- Dual-Channel DDR4, **ECC/ Non-ECC**	- Dual-Channel DDR4, **Non-ECC**
Network	• 3 x Intel® I225-LM PCIe 2.5GbE RJ45 LAN - Co-Lay Intel® I225-V PCIe 2.5GbE RJ45 LAN	
Expansion Slots	• 1 x PCIe 4.0 x16 slot • 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	

Continued on next column

Model	MS-CF02-SKU1	MS-CF02-SKU2
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 4096×2304 @60Hz • 1 x HDMI™ 1.4b up to 4096x2304 @24Hz • 1 x LVDS up to 1920x1200 @60Hz (Co-lay eDP) - Switch between LVDS & eDP throuth BIOS settings. - 18/24-bit dual channel • 1 x eDP up to 4096×2304 @60 Hz (Co-lay LVDS) - Switch between eDP & LVDS throuth BIOS settings. • 4 independent display modes supported - DP1 - DP2 - HDMI™ - LVDS or eDP	
Power	• 1 x 24-pin ATX power connector • 1 x 4-pin 12V ATX power connector	
Cooling	• 1 x 4-pin PWM CPU fan connector • 1 x 4-pin PWM system fan connector	
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 Gen 2 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	

Continued on next column

Model	MS-CF02-SKU1	MS-CF02-SKU2
Onboard Connector	• 1 x ATX power connector (12-pin) • 1 x 12V ATX power connector (4-pin) • 1 x Front audio header (Headphone & Mic-in) • 1 x Audio amplifier header • 1 x LVDS Inverter box header • 1 x LVDS + eDP Wafer Connector • 1 x CPU fan box header • 1 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 • 1 x USB 3.2 Gen 1 box header • 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 LVDS power jumper • 1 x Chassis Intrusion jumper	
OS Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC (64-bit) • Linux Kernel 5.15 (ADL-S)/ Linux Kernel 5.19 (RPL-S) (by request)	
Certification	CE, FCC Class B, BSMI, RCM, VCCI, UKCA	
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	

SKU3

Model	MS-CF02-SKU3
Form factor	Mini-ITX
Dimensions	170 x 170mm (6.7 x 6.7 inches)
Processor	• **13th** Gen Intel® **Raptor** Lake-S i9/i7/i5/i3 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 Pentium®/ Celeron® IOTG Series Processor, Max 65W - 1.6 GHz~5.1 GHz (depends on CPU) - Socket LGA 1700
Chipset	**Intel® H610E**
Memory	• 2 x DDR4 SO-DIMM slots (260-pin, vertical) - Dual-Channel DDR4, Non-ECC - Up to 3200 MT/s - Up to 64GB
Network	• 3 x Intel® I225-V PCIe 2.5GbE RJ45 LAN - Co-Lay Intel® I225-LM PCIe 2.5GbE RJ45 LAN
Expansion Slots	• 1 x PCIe 4.0 x16 slot • 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)
Storage	• 3 x SATA 3.0 6Gb/s ports - 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

Continued on next column

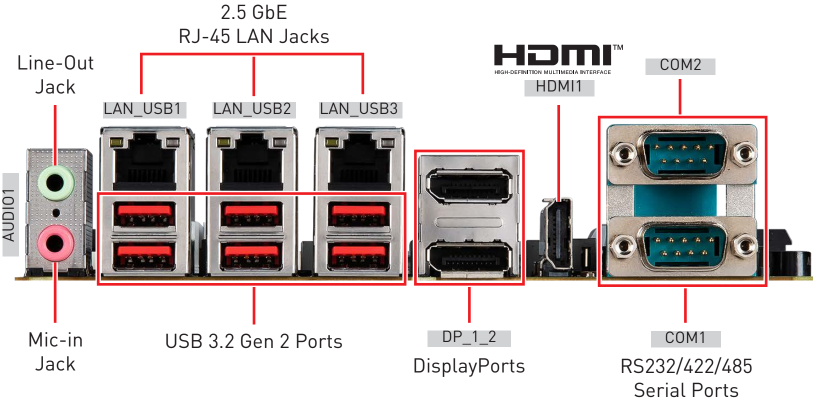
Model	MS-CF02-SKU3
Graphics	• 2 x DP 1.4a up to 4096×2304 @60Hz • 1 x HDMI™ 1.4b up to 4096x2304 @24Hz • 1 x LVDS up to 1920x1200 @60Hz (Co-lay eDP) - Auto switch between LVDS & eDP - 18/24-bit dual channel • 1 x eDP up to 4096×2304 @60 Hz (Co-lay LVDS) - Auto switch between eDP & LVDS • 3 independent display modes supported - DP1/ DP2 - HDMI™ - LVDS or eDP
Power	• 1 x 24-pin ATX power connector • 1 x 4-pin 12V ATX power connector
Cooling	• 1 x 4-pin PWM CPU fan connector • 1 x 4-pin PWM system fan connector
Rear I/O	• 1 x Line-out jack • 1 x Mic-in jack • 2 x 2.5 GbE RJ-45 LAN ports • 2 x USB 3.2 Gen 2 Type-A ports (10 Gbps) • 2 x USB 3.2 Gen 1 Type-A ports (5 Gbps) • 2 x USB 2.0 Type-A ports (480 Mbps) • 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

Continued on next column

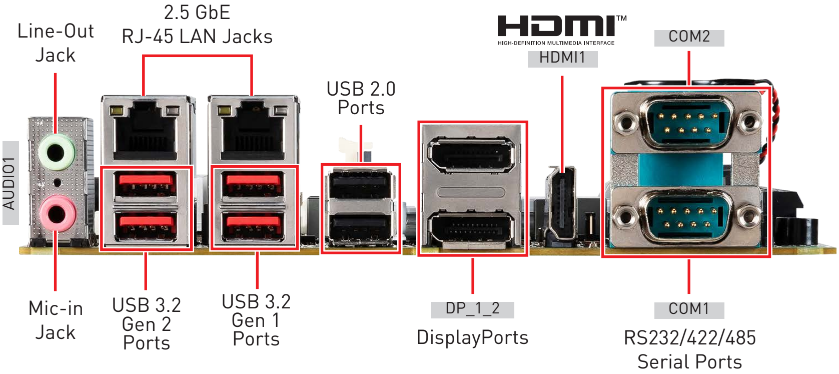
Model	MS-CF02-SKU3
Onboard Connector	• 1 x ATX power connector (12-pin) • 1 x 12V ATX power connector (4-pin) • 1 x Front audio header (Headphone & Mic-in) • 1 x Audio amplifier header • 1 x LVDS Inverter box header • 1 x LVDS + eDP Wafer Connector • 1 x CPU fan box header • 1 x System fan box header • 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 • 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 LVDS power jumper • 1 x Chassis Intrusion jumper
OS Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise LTSC (64-bit) • Linux Kernel 5.15 (ADL-S)/ Linux Kernel 5.19 (RPL-S) (by request)
Certification	CE, FCC Class B, BSMI, RCM, VCCI, UKCA
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

Rear I/O Panel

SKU1/ SKU2



SKU3



Line-Out Jack

This connector is provided for headphones or speakers.

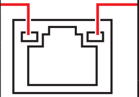
Mic-In Jack

This connector is provided for microphones.

2.5 GbE RJ-45 LAN Jack

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

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



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

USB 3.2 Gen 2 Port

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

USB 3.2 Gen 1 Port

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

USB 2.0 Port

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

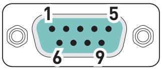
DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

HDMI™ Connector

The High-Definition Multimedia Interface (HDMI™) is an all-digital audio/ video interface capable of transmitting uncompressed streams. HDMI™ supports all TV format, including standard, enhanced, or high-definition video, plus multi-channel digital audio on a single cable.

RS232/422/485 Serial Port

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



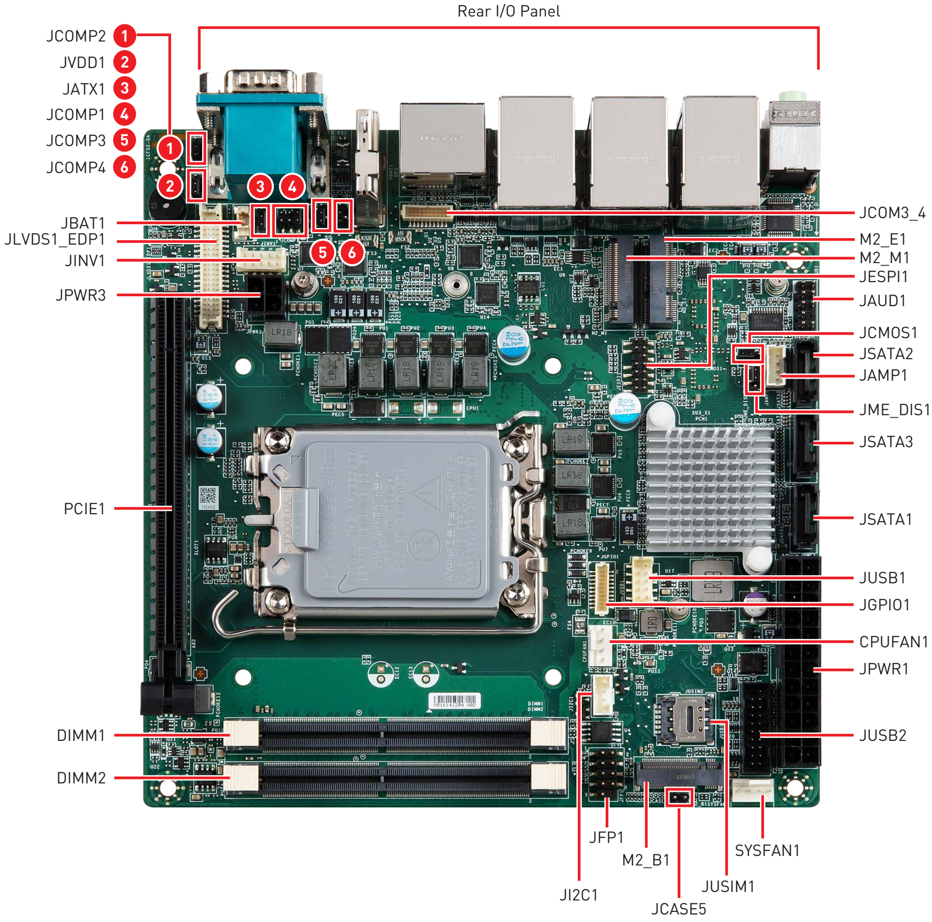
RS232		
PIN	**SIGNAL**	**DESCRIPTION**
1	NDCD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM	VCC_COM

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

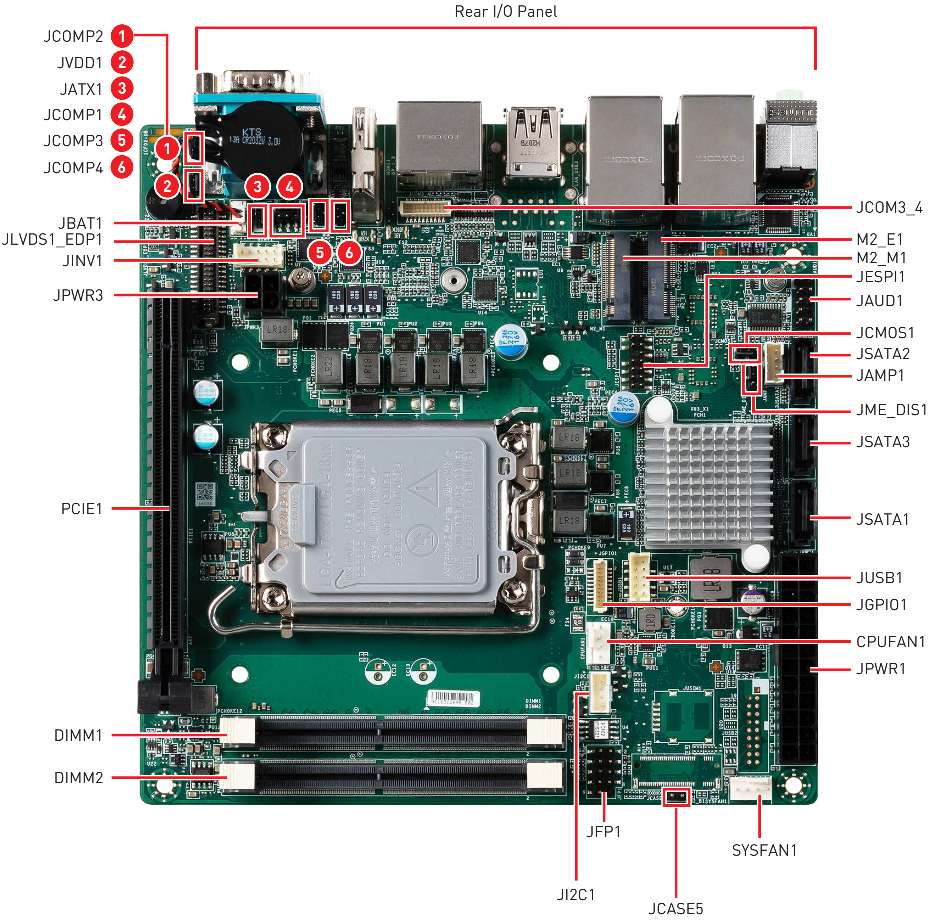
RS485		
PIN	**SIGNAL**	**DESCRIPTION**
1	TXD-	Transmit Data, Negative
2	NC	No Connection
3	TXD+	Transmit Data, Positive
4	NC	No Connection
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

Motherboard Overview

SKU1/ SKU2

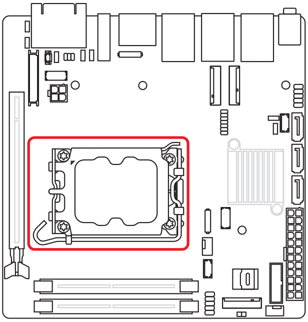


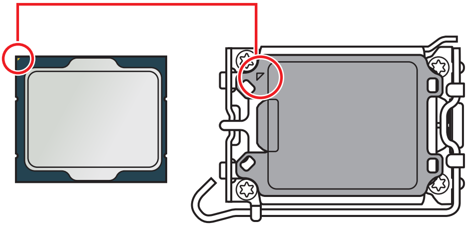
SKU3


Rear I/O Panel
JCOMP2 1
JVDD1 2
JATX1 3
JCOMP1 4
JCOMP3 5
JCOMP4 6
JBAT1
JLVDS1_EDP1
JINV1
JPWR3
PCIE1
DIMM1
DIMM2
JCOM3_4
M2_E1
M2_M1
JESPI1
JAUD1
JCMOS1
JSATA2
JAMP1
JME_DIS1
JSATA3
JSATA1
JUSB1
JGPIO1
CPUFAN1
JPWR1
JFP1
SYSFAN1
JI2C1
JCASE5

Component Contents

CPU Socket





Introduction to the LGA1700 CPU

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

Important

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

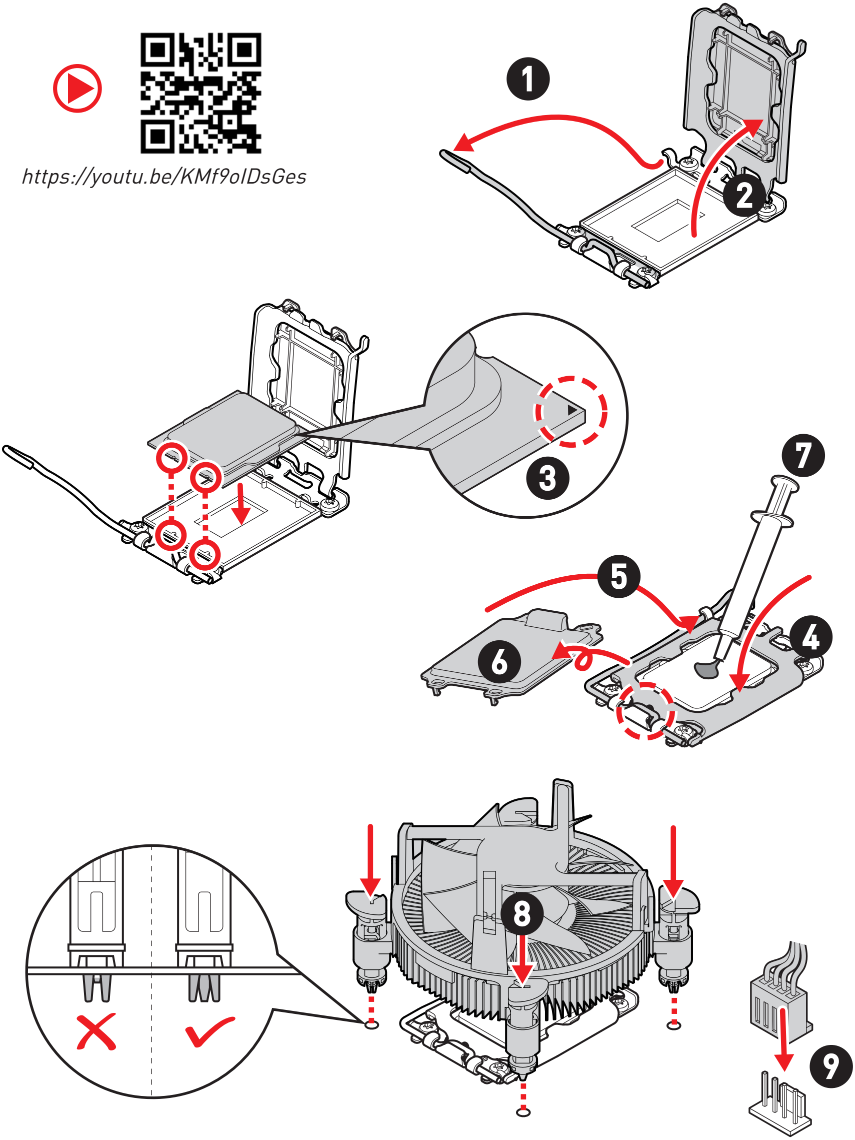
CPU & Heatsink Installation

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

Important

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

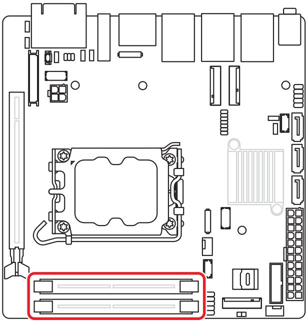
https://youtu.be/KMf9oIDsGes

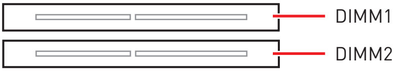


Memory

DIMM1~2: DDR4 SO DIMM Slots

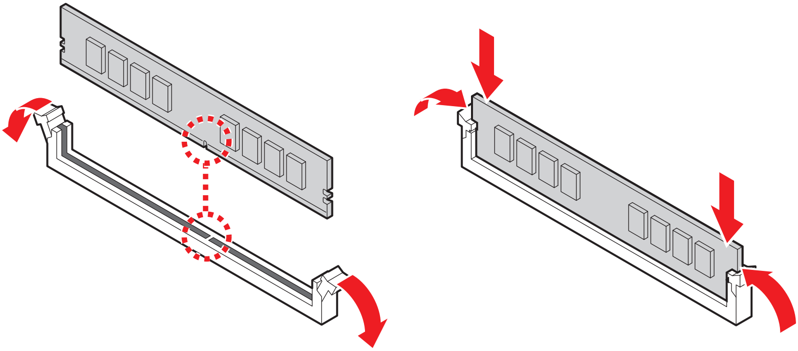
The SO-DIMM slots is intended for memory modules.





Installing DDR4 Memory

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.



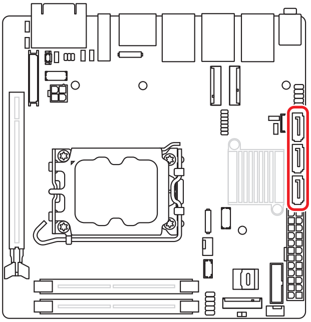
Important

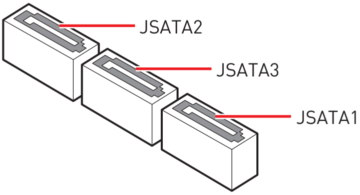
- *Always insert memory modules in the **DIMM2** slot first.*
- *You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.*
- *To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.*

Storage

JSATA1: SATA 3.0 6Gb/s Ports

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



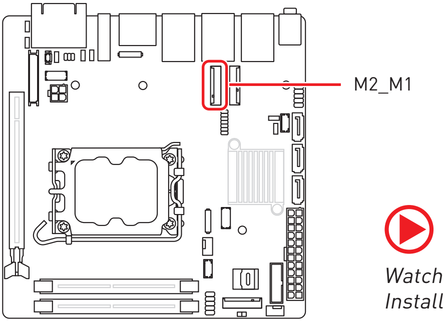


Important

- *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 sides 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

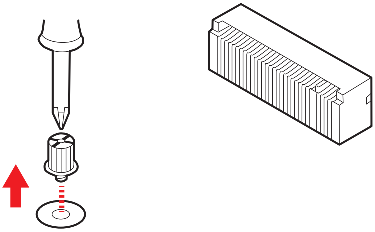
- Supports PCIe 3.0 x4 signal.
- Supports B+M key module.

Video Demonstration

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

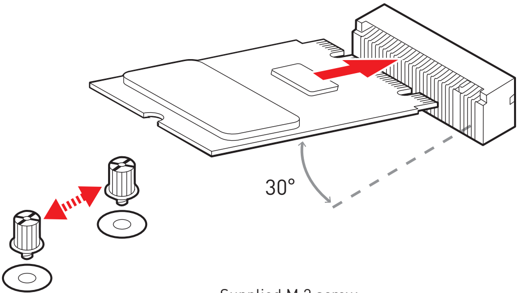
Installing M.2 SSD

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

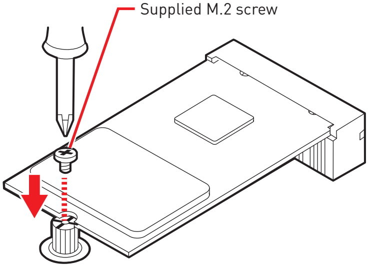


2. Set the M.2 riser screw at the appropriate location based on the length of your M.2 SSD.

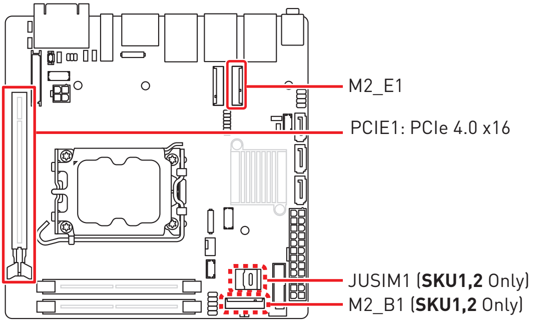
3. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



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



Expansion Slots

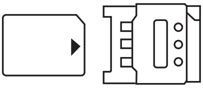


PCIE1: PCIe Expansion Slots

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.

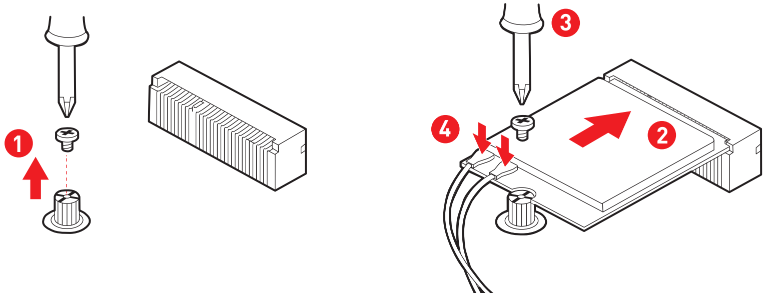


Important

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.

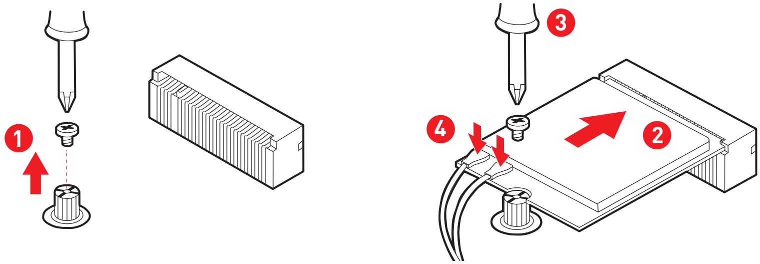


Feature

- 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.

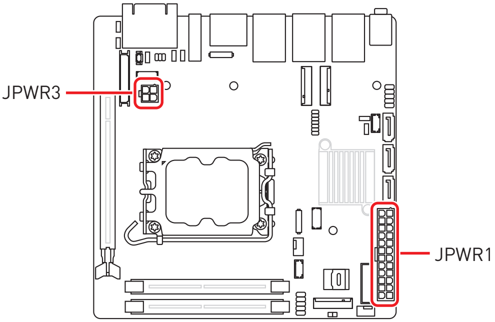


Feature

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

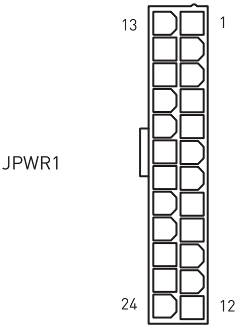
Connectors

Power Connectors



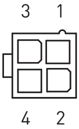
JPWR1: ATX 24-Pin Power Connector

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	PWR OK
	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

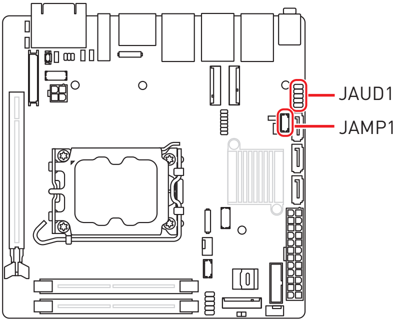
This connector is used to provide power to SATA devices.

JPWR3 	1	GND	2	GND
	3	12V	4	12V

Important

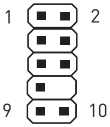
Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Audio Connectors



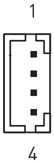
JAUD1: Front Audio Header

This connector allows you to connect front panel audio.

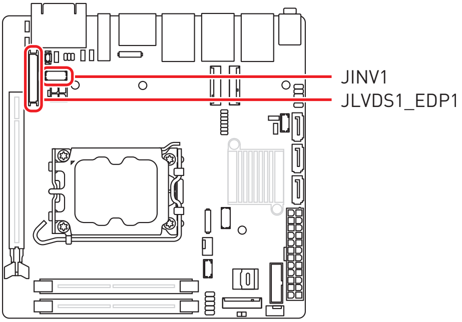
JAUD1 	1	MIC_L	2	GND
	3	MIC_R	4	PRESENCE#
	5	F_OUTR	6	MIC2_JD
	7	HPON	8	No pin
	9	F_OUTL	10	LIN2_JD

JAMP1: Audio Amplifier Header

The connector is used to connect audio amplifiers to enhance audio performance.

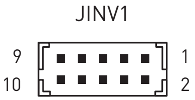
JAMP1 	1	AMP_OUT_R-	2	AMP_OUT_R+
	3	AMP_OUT_L-	4	AMP_OUT_L+

Graphics Connectors



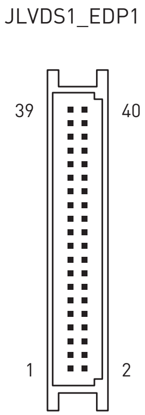
JINV1: LVDS Inverter Box Header

The connector is provided for LCD backlight options.

	1	GND	2	GND
	3	VCC5	4	VCC5
	5	+12V	6	+12V
	7	INV_ON#1	8	NC
	9	L_BKLT_CTRL#1	10	NC

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-

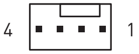
Important

Pin 12 is a detect 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

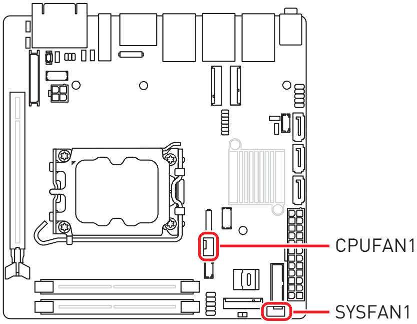
CPUFAN1, SYSFAN1: CPU/ System Fan Box Headers

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 SYSFAN1		1	GND	2	FAN POWER
		3	FAN SENSE	4	FAN_PWM

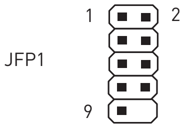
Important

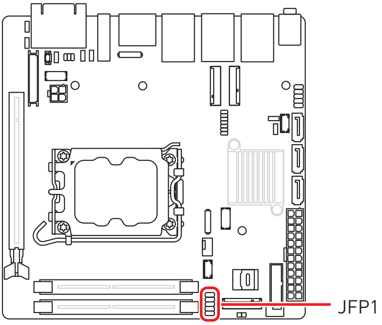
Please refer to the recommended CPU fans at processor's official website or consult the vendors for proper CPU cooling fan.



JFP1: Front Panel Connector

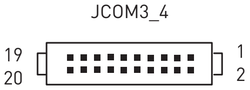
This front-panel connector is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.

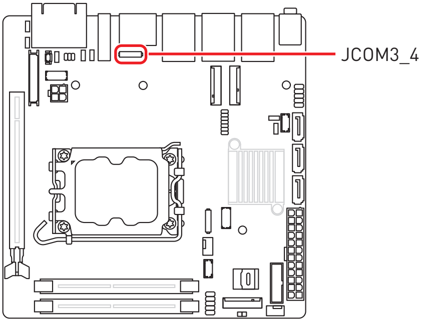
	1	HDD LED+	2	POWER LED
	3	HDD LED-	4	POWER LED
	5	RESET SWITCH-	6	POWER SWITCH+
	7	RESET SWITCH+	8	POWER SWITCH-
	9	NC	10	No pin



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.

	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).

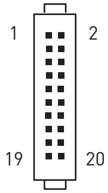
RS232		
PIN	**SIGNAL**	**DESCRIPTION**
1	NDCD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM	VCC_COM

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

RS485		
PIN	**SIGNAL**	**DESCRIPTION**
1	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

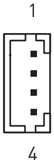
JGPIO1: GPIO (DIO) Box Header

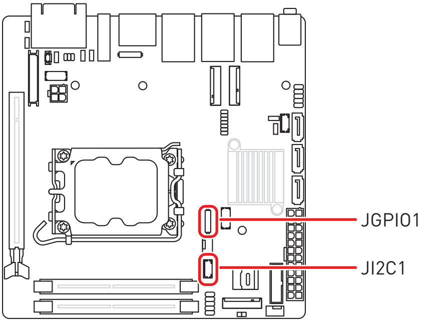
This connector is provided for the General-Purpose Input/Output (GPIO) peripheral module.

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

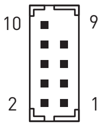
This connector is used to connect to the System Management Bus (SMBus).

JI2C1 	1	3VSB	2	I2C_CLK
	3	I2C_DATA-	4	GND



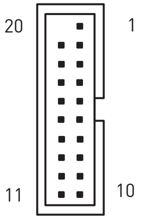
JUSB1: USB 2.0 Box Header

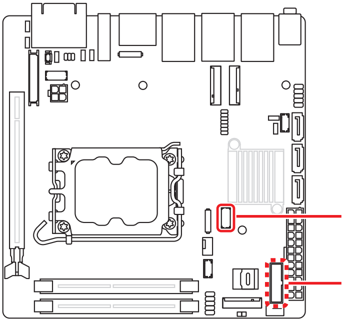
These connectors are ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices.

<table>
<tr><td rowspan="5">JUSB1 
</td><td>1</td><td>5V</td><td>2</td><td>5V</td></tr>
<tr><td>3</td><td>USB_D-</td><td>4</td><td>USB_D-</td></tr>
<tr><td>5</td><td>USB_D+</td><td>6</td><td>USB_D+</td></tr>
<tr><td>7</td><td>GND</td><td>8</td><td>GND</td></tr>
<tr><td>9</td><td>No pin</td><td>10</td><td>NC</td></tr>
</table>

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).

<table>
<tr><td rowspan="10">JUSB1 
</td><td>1</td><td>5V</td><td>2</td><td>USB_3.2 RX-</td></tr>
<tr><td>3</td><td>USB_3.2 RX+</td><td>4</td><td>GND</td></tr>
<tr><td>5</td><td>USB_3.2 TX-</td><td>6</td><td>USB_3.2 TX+</td></tr>
<tr><td>7</td><td>GND</td><td>8</td><td>USB_D-</td></tr>
<tr><td>9</td><td>USB_D+</td><td>10</td><td>NC</td></tr>
<tr><td>11</td><td>USB_D+</td><td>12</td><td>USB_D-</td></tr>
<tr><td>13</td><td>GND</td><td>14</td><td>USB_3.2 TX+</td></tr>
<tr><td>15</td><td>USB_3.2 TX-</td><td>16</td><td>GND</td></tr>
<tr><td>17</td><td>USB_3.2 RX+</td><td>18</td><td>USB_3.2 RX-</td></tr>
<tr><td>19</td><td>5V</td><td>20</td><td>No Pin</td></tr>
</table>

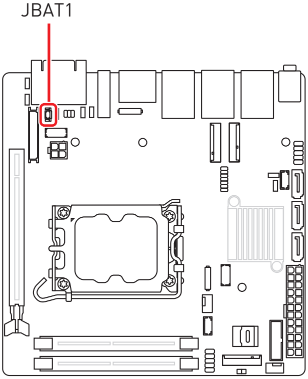


JUSB1

JUSB2 (**SKU1,2** Only)

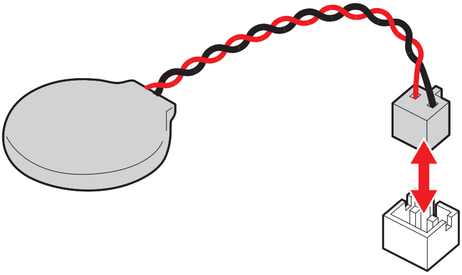
JBAT1: CMOS Battery Header

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

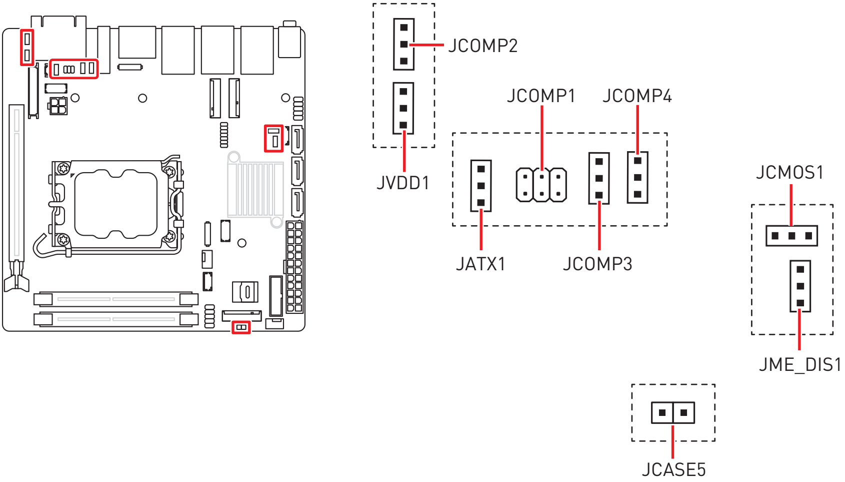
KEEP OUT OF REACH OF CHILDREN

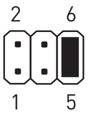
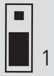
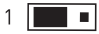
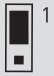
- *Swallowing can lead to chemical burns, perforation of soft tissue, can death.*
- *Severe burns can occur within 2 hours of ingestion.*
- *If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.*

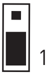
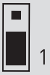
Jumpers

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.

BIOS Setup

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

Users may need to run the Setup program when:

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

Important

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

Entering Setup

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

Press <DEL> or <F2> to enter SETUP

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

Important

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

Control Keys

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

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

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

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

Sub-Menu

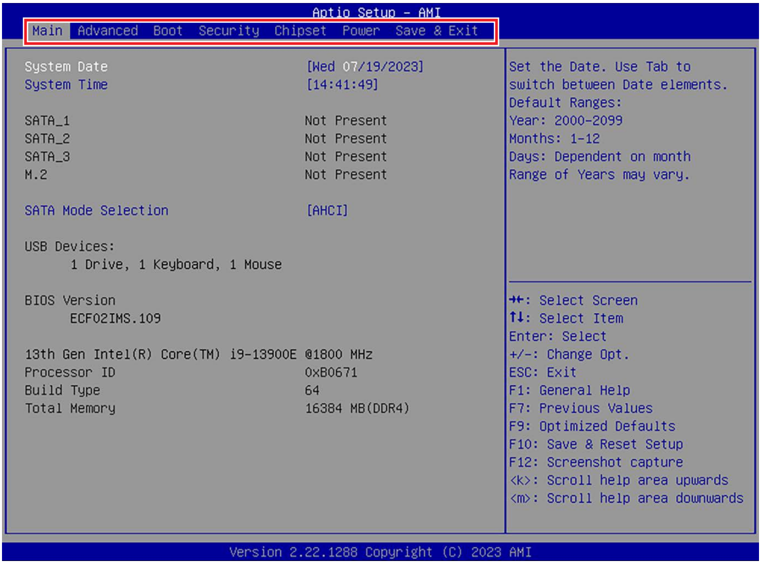
If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use **arrow keys (↑↓)** to highlight the field and press **<Enter>** to call up the sub-menu. Then you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

General Help <F1>

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

BIOS Item Contents

The Menu Bar



```
                              Aptio Setup - AMI
  Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

 System Date                     [Wed 07/19/2023]   Set the Date. Use Tab to
 System Time                     [14:41:49]         switch between Date elements.
                                                    Default Ranges:
 SATA_1                          Not Present        Year: 2000-2099
 SATA_2                          Not Present        Months: 1-12
 SATA_3                          Not Present        Days: Dependent on month
 M.2                             Not Present        Range of Years may vary.

 SATA Mode Selection             [AHCI]

 USB Devices:
       1 Drive, 1 Keyboard, 1 Mouse

 BIOS Version                                       →←: Select Screen
       ECF02IMS.109                                 ↑↓: Select Item
                                                    Enter: Select
 13th Gen Intel(R) Core(TM) i9-13900E @1800 MHz     +/-: Change Opt.
 Processor ID                    0xB0671            ESC: Exit
 Build Type                      64                 F1: General Help
 Total Memory                    16384 MB(DDR4)     F7: Previous Values
                                                    F9: Optimized Defaults
                                                    F10: Save & Reset Setup
                                                    F12: Screenshot capture
                                                    <k>: Scroll help area upwards
                                                    <m>: Scroll help area downwards

                  Version 2.22.1288 Copyright (C) 2023 AMI
```

▶ Main

Use this menu for basic system configurations, such as time, date, etc.

▶ Advanced

Use this menu to set up the items of special enhanced features.

▶ Boot

Use this menu to specify the priority of boot devices.

▶ Security

Use this menu to set supervisor and user passwords.

▶ Chipset

This menu controls the advanced features of the on-board chipsets.

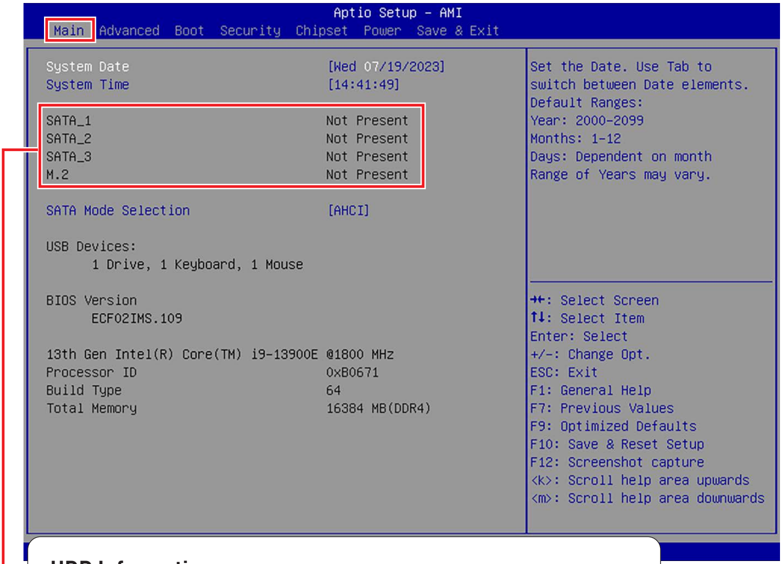
▶ Power

Use this menu to specify your settings for power management.

▶ Save & Exit

This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

Main



```
                              Aptio Setup - AMI
 Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

 System Date                        [Wed 07/19/2023]    Set the Date. Use Tab to
 System Time                        [14:41:49]          switch between Date elements.
                                                        Default Ranges:
 SATA_1                             Not Present         Year: 2000-2099
 SATA_2                             Not Present         Months: 1-12
 SATA_3                             Not Present         Days: Dependent on month
 M.2                                Not Present         Range of Years may vary.

 SATA Mode Selection                [AHCI]

 USB Devices:
       1 Drive, 1 Keyboard, 1 Mouse

 BIOS Version                                           →←: Select Screen
       ECF02IMS.109                                     ↑↓: Select Item
                                                        Enter: Select
 13th Gen Intel(R) Core(TM) i9-13900E @1800 MHz         +/-: Change Opt.
 Processor ID                       0xB0671             ESC: Exit
 Build Type                         64                  F1: General Help
 Total Memory                       16384 MB(DDR4)      F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards
```

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

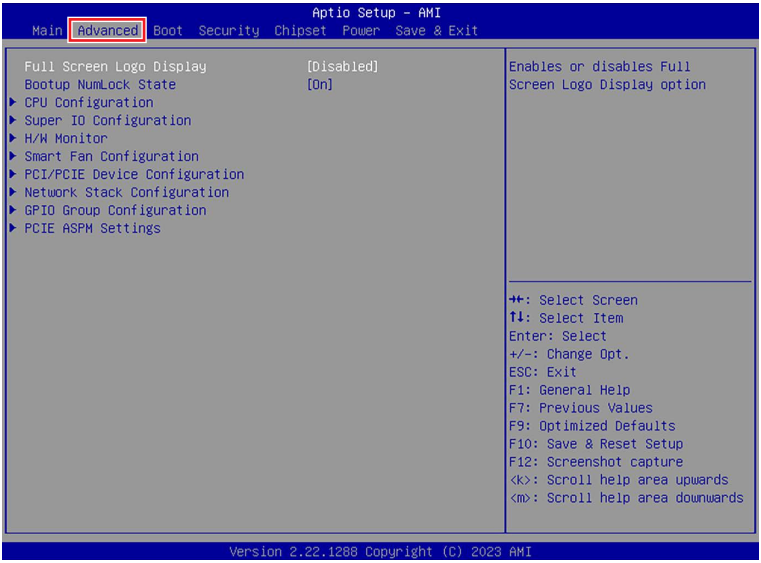
This setting specifies SATA controller mode.

[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.*

Advanced



```
                              Aptio Setup - AMI
  Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

  Full Screen Logo Display             [Disabled]      Enables or disables Full
  Bootup NumLock State                 [On]            Screen Logo Display option
▶ CPU Configuration
▶ Super IO Configuration
▶ H/W Monitor
▶ Smart Fan Configuration
▶ PCI/PCIE Device Configuration
▶ Network Stack Configuration
▶ GPIO Group Configuration
▶ PCIE ASPM Settings
                                                       →←: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       ESC: Exit
                                                       F1: General Help
                                                       F7: Previous Values
                                                       F9: Optimized Defaults
                                                       F10: Save & Reset Setup
                                                       F12: Screenshot capture
                                                       <k>: Scroll help area upwards
                                                       <m>: Scroll help area downwards

                   Version 2.22.1288 Copyright (C) 2023 AMI
```

▶ Full Screen Logo Display

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

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

[Disabled] BIOS will display the normal POST messages, instead of the full-screen logo.

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

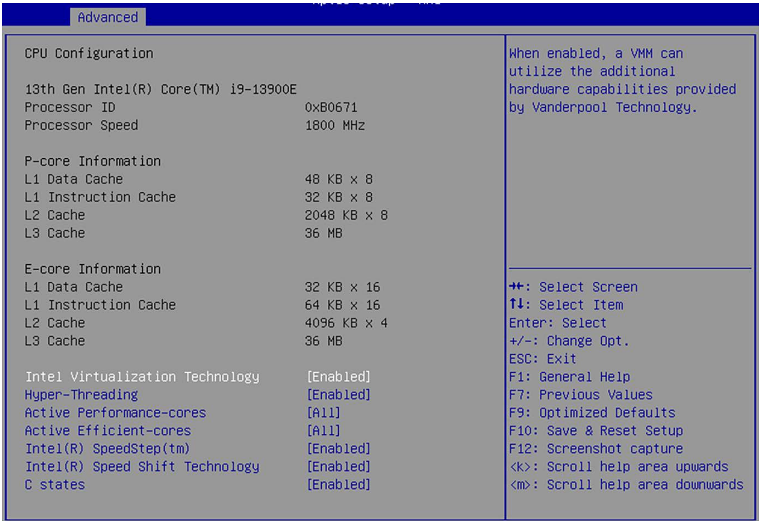
▶ Bootup NumLock State

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

[On] Turn on the Num Lock key when the system is powered on.

[Off] Allow users to use the arrow keys on the numeric keypad.

▶ CPU Configuration



```
        Advanced

 CPU Configuration                                   When enabled, a VMM can
                                                     utilize the additional
 13th Gen Intel(R) Core(TM) i9-13900E                hardware capabilities provided
 Processor ID                   0xB0671              by Vanderpool Technology.
 Processor Speed                1800 MHz

 P-core Information
 L1 Data Cache                  48 KB x 8
 L1 Instruction Cache           32 KB x 8
 L2 Cache                       2048 KB x 8
 L3 Cache                       36 MB

 E-core Information
 L1 Data Cache                  32 KB x 16           →←: Select Screen
 L1 Instruction Cache           64 KB x 16           ↑↓: Select Item
 L2 Cache                       4096 KB x 4          Enter: Select
 L3 Cache                       36 MB                +/-: Change Opt.
                                                     ESC: Exit
 Intel Virtualization Technology [Enabled]           F1: General Help
 Hyper-Threading                [Enabled]            F7: Previous Values
 Active Performance-cores       [All]                F9: Optimized Defaults
 Active Efficient-cores         [All]                F10: Save & Reset Setup
 Intel(R) SpeedStep(tm)         [Enabled]            F12: Screenshot capture
 Intel(R) Speed Shift Technology [Enabled]           <k>: Scroll help area upwards
 C states                       [Enabled]            <m>: Scroll help area downwards
```

▸ Intel Virtualization Technology

Enables or disables Intel Virtualization technology.

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

▸ Hyper-Threading (HT Function)

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

▸ Active Performance-cores

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

▸ Active Efficient-cores

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

▶ Intel(R) SpeedStep(TM)

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

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

[Disabled] Disables this function

▶ Intel(R) Speed Shift Technology

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

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

[Disabled] Disable this function.

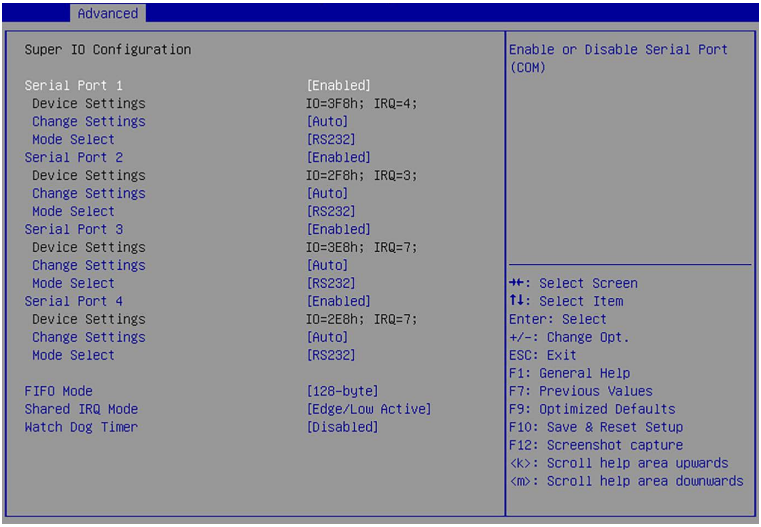
▶ C States

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

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

[Disabled] Disable this function.

Super IO Configuration



```
Advanced

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

▸ Serial Port 1/ 2/ 3/ 4

This setting enables or disables the specified serial port.

» 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

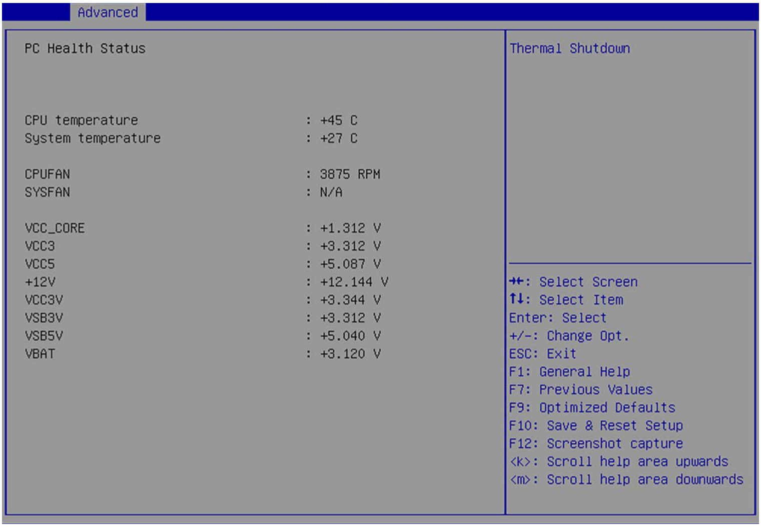
This setting provides the system with the ability to share interrupts among its serial ports.

▸ 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.



```
Advanced

PC Health Status                                        Thermal Shutdown


CPU temperature                   : +45 C
System temperature                : +27 C

CPUFAN                            : 3875 RPM
SYSFAN                            : N/A

VCC_CORE                          : +1.312 V
VCC3                              : +3.312 V
VCC5                              : +5.087 V
+12V                              : +12.144 V           →←: Select Screen
VCC3V                             : +3.344 V            ↑↓: Select Item
VSB3V                             : +3.312 V            Enter: Select
VSB5V                             : +5.040 V            +/-: Change Opt.
VBAT                              : +3.120 V            ESC: Exit
                                                        F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards
```

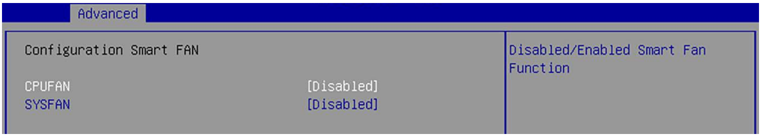
▶ Thermal Shutdown

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

[Enabled] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.

[Disabled] Disable this function.

Smart Fan Configuration



```
Advanced

Configuration Smart FAN                                 Disabled/Enabled Smart Fan
                                                        Function
CPUFAN                            [Disabled]
SYSFAN                            [Disabled]
```

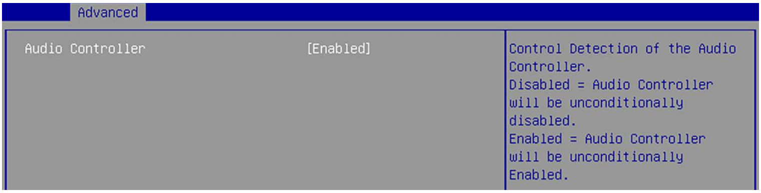
▶ CPUFAN/ SYSFAN

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



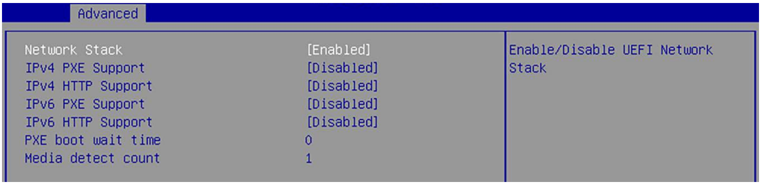
```
Advanced

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

Audio Controller

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

Network Stack Configuration

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



```
Advanced

Network Stack                         [Enabled]         Enable/Disable UEFI Network
IPv4 PXE Support                      [Disabled]        Stack
IPv4 HTTP Support                     [Disabled]
IPv6 PXE Support                      [Disabled]
IPv6 HTTP Support                     [Disabled]
PXE boot wait time                    0
Media detect count                    1
```

Network Stack

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

» **IPV4 PXE Support**

Enables or disables IPv4 PXE boot support.

» **IPV4 HTTP Support**

Enables or disables Ipv4 HTTP Support.

» **IPV6 PXE Support**

Enables or disables Ipv6 PXE Support.

» **IPV6 HTTP Support**

Enables or disables Ipv6 HTTP Support.

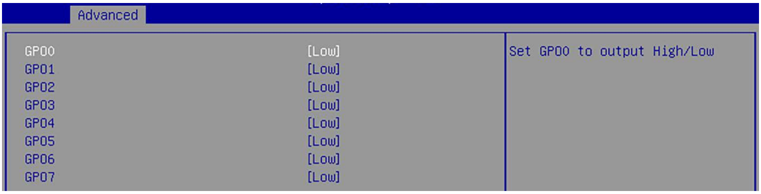
» **PXE boot wait time**

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

» **Media detect count**

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

▶ GPIO Group Configuration



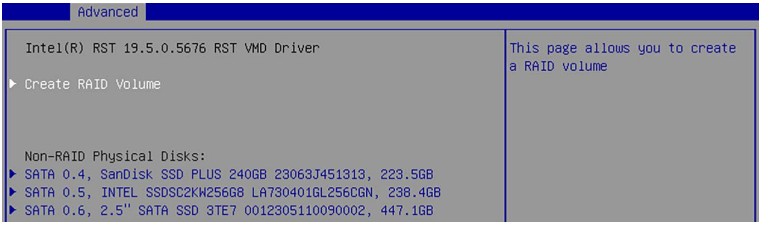
```
Advanced

GPO0                                  [Low]      Set GPO0 to output High/Low
GPO1                                  [Low]
GPO2                                  [Low]
GPO3                                  [Low]
GPO4                                  [Low]
GPO5                                  [Low]
GPO6                                  [Low]
GPO7                                  [Low]
```

▸ 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.



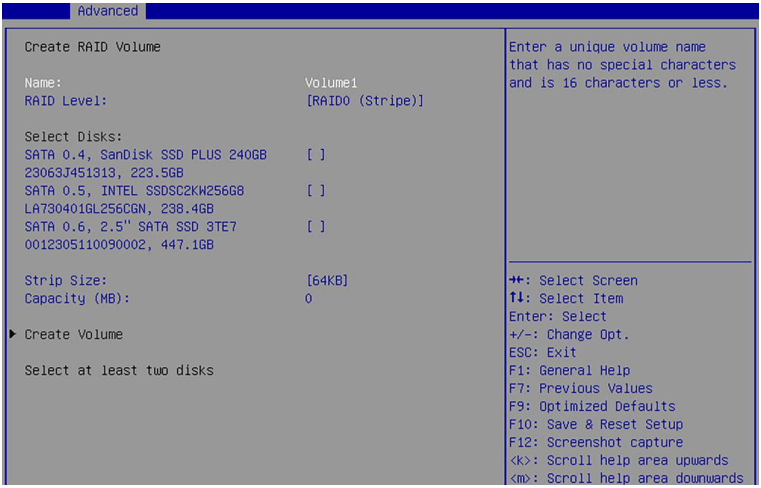
```
Advanced

 Intel(R) RST 19.5.0.5676 RST VMD Driver                        This page allows you to create
                                                                a RAID volume
▶ Create RAID Volume


 Non-RAID Physical Disks:
▶ SATA 0.4, SanDisk SSD PLUS 240GB 23063J451313, 223.5GB
▶ SATA 0.5, INTEL SSDSC2KW256G8 LA730401GL256CGN, 238.4GB
▶ SATA 0.6, 2.5" SATA SSD 3TE7 0012305110090002, 447.1GB
```

Important

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

▸ Create RAID Volume

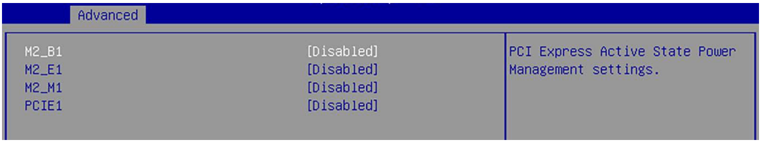
This menu allows for the management of RAID volumes.



```
Advanced

 Create RAID Volume                                     Enter a unique volume name
                                                        that has no special characters
 Name:                          Volume1                 and is 16 characters or less.
 RAID Level:                    [RAID0 (Stripe)]

 Select Disks:
 SATA 0.4, SanDisk SSD PLUS 240GB   [ ]
 23063J451313, 223.5GB
 SATA 0.5, INTEL SSDSC2KW256G8      [ ]
 LA730401GL256CGN, 238.4GB
 SATA 0.6, 2.5" SATA SSD 3TE7       [ ]
 0012305110090002, 447.1GB
                                                        ──────────────────────────────
 Strip Size:                    [64KB]                  →←: Select Screen
 Capacity (MB):                 0                       ↑↓: Select Item
                                                        Enter: Select
▶ Create Volume                                         +/-: Change Opt.
                                                        ESC: Exit
 Select at least two disks                              F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards
```

▶ PCIE ASPM settings

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



```
M2_B1                                      [Disabled]
M2_E1                                      [Disabled]
M2_M1                                      [Disabled]
PCIE1                                      [Disabled]
```

PCI Express Active State Power Management settings.

▶ M2_B1/ M2_E1/ M2_M1/ PCIE1

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

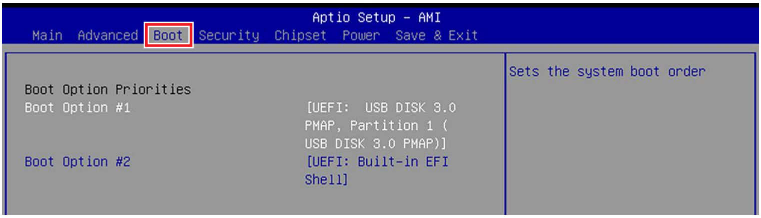
[L0s] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.

[L1] Higher latency, lower power “standby” state **(optional)**.

[L0sL1] Activate both L0s and L1 support.

[Disabled] Disable this function.

Boot



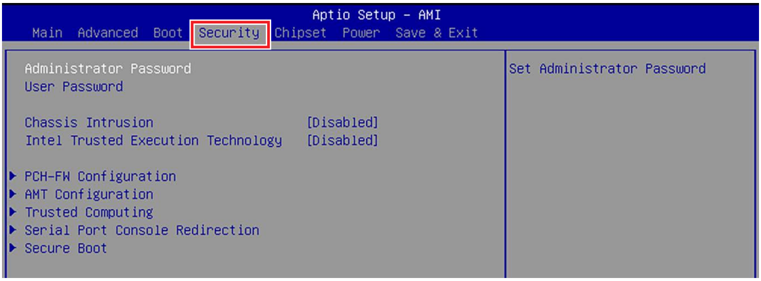
```
Boot Option Priorities
Boot Option #1                [UEFI:  USB DISK 3.0
                              PMAP, Partition 1 (
                              USB DISK 3.0 PMAP)]
Boot Option #2                [UEFI: Built-in EFI
                              Shell]
```

Sets the system boot order

▶ Boot Option #1-2

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

Security



```
Administrator Password
User Password

Chassis Intrusion                         [Disabled]
Intel Trusted Execution Technology        [Disabled]

▶ PCH-FW Configuration
▶ AMT Configuration
▶ Trusted Computing
▶ Serial Port Console Redirection
▶ Secure Boot
```

Set Administrator Password

▶ 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

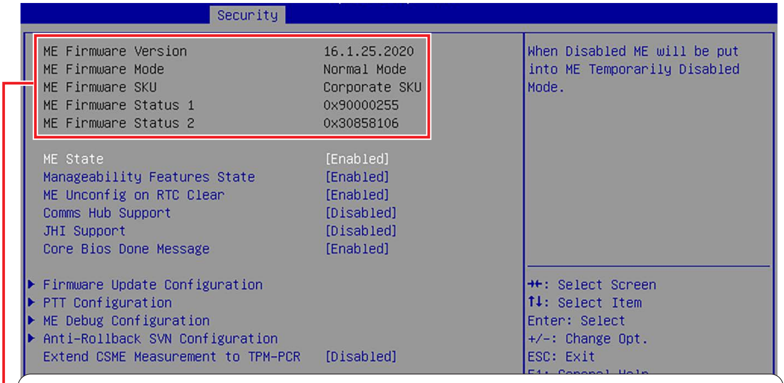
Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware-based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

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.



```
                    Security
ME Firmware Version                16.1.25.2020      When Disabled ME will be put
ME Firmware Mode                   Normal Mode       into ME Temporarily Disabled
ME Firmware SKU                    Corporate SKU     Mode.
ME Firmware Status 1               0x90000255
ME Firmware Status 2               0x30858106

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

▶ Firmware Update Configuration                      →←: Select Screen
▶ PTT Configuration                                  ↑↓: Select Item
▶ ME Debug Configuration                             Enter: Select
▶ Anti-Rollback SVN Configuration                    +/-: Change Opt.
  Extend CSME Measurement to TPM-PCR [Disabled]      ESC: Exit
                                                     F1: General Help
```

Firmware Information

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

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

▸ ME State

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

» **Manageability Feature State**

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

» **ME Unconfig on RTC Clear**

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

» **Comms Hub Support**

Enables or disables the communications hub support.

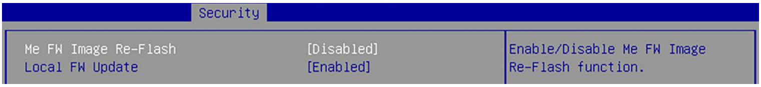
» **JHI Support**

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

» **Core BIOS Done Message**

Enables or disables Core BIOS Done Message sent to ME.

▶ Firmware Update Configuration



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

» ME FW Image Re-Flash

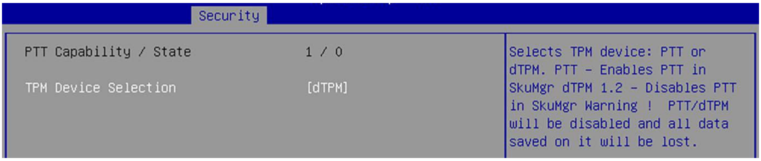
Enables or disables the ME Firmware Image Re-flashing**.**

» 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.



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

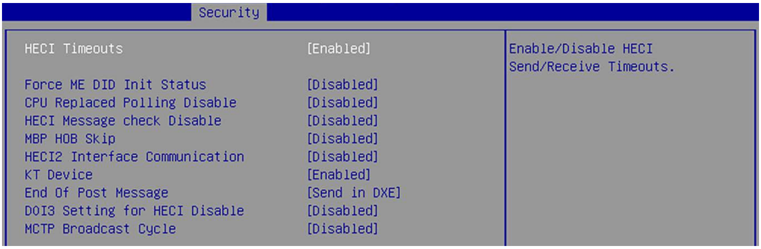
» TPM Device Selection

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).



```
Security
HECI Timeouts                     [Enabled]      Enable/Disable HECI
                                                 Send/Receive Timeouts.
Force ME DID Init Status          [Disabled]
CPU Replaced Polling Disable      [Disabled]
HECI Message check Disable        [Disabled]
MBP HOB Skip                      [Disabled]
HECI2 Interface Communication     [Disabled]
KT Device                         [Enabled]
End Of Post Message               [Send in DXE]
D0I3 Setting for HECI Disable     [Disabled]
MCTP Broadcast Cycle              [Disabled]
```

» HECI Timeouts

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

» Force ME DID Init Status

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

» CPU Replaced Polling Disable

Setting this option disables the CPU replacement polling loop.

HECI Message Check Disable

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

MBP HOB Skip

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

HECI2 Interface Communication

This setting Adds/ Removes HECI2 device from PCI space.

KT Device

Enables or disables Key Transfer (KT) Device.

End of Post Message

Enables or disables End of Post Message sent to ME.

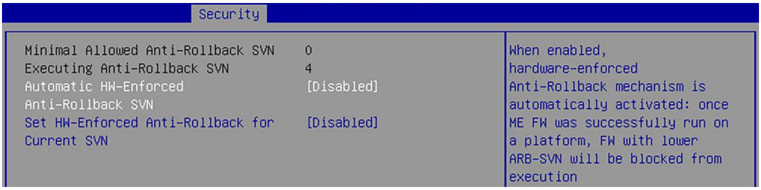
DOI3 Setting for HECI Disable

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

MCTP Broadcast Cycle

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

Anti-Rollback SVN Configuration



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

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

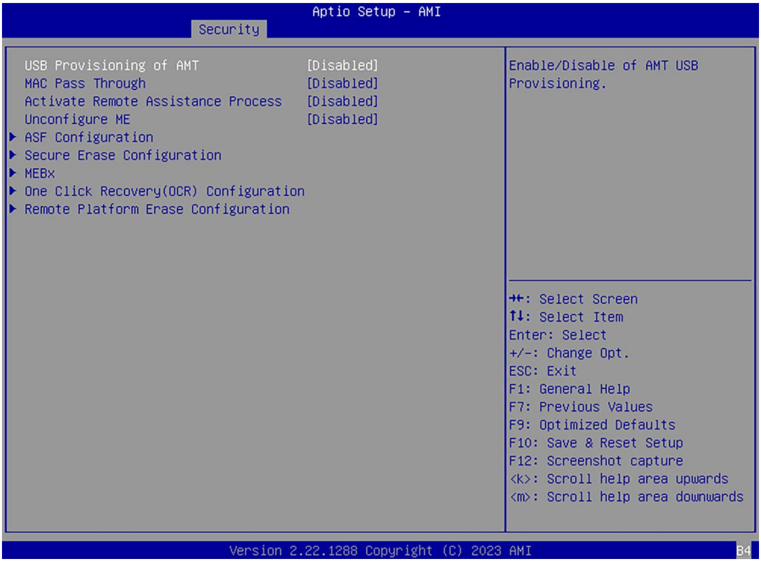
Enables or disables the Extend CSME Measurement to TPM-PCR. This item enables capturing and recording the Intel® Converged Security and Management Engine (Intel® CSME) firmware in the Trusted Platform Module Platform Configuration Registers (TPM-PCR). This enhances system security by protecting against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



```
                              Aptio Setup - AMI
                       Security

  USB Provisioning of AMT               [Disabled]    Enable/Disable of AMT USB
  MAC Pass Through                      [Disabled]    Provisioning.
  Activate Remote Assistance Process    [Disabled]
  Unconfigure ME                        [Disabled]
▶ ASF Configuration
▶ Secure Erase Configuration
▶ MEBx
▶ One Click Recovery(OCR) Configuration
▶ Remote Platform Erase Configuration

                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      ESC: Exit
                                                      F1: General Help
                                                      F7: Previous Values
                                                      F9: Optimized Defaults
                                                      F10: Save & Reset Setup
                                                      F12: Screenshot capture
                                                      <k>: Scroll help area upwards
                                                      <m>: Scroll help area downwards

                  Version 2.22.1288 Copyright (C) 2023 AMI                    B4
```

▸ USB Provisioning of AMT

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

▸ Mac PASS Through

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

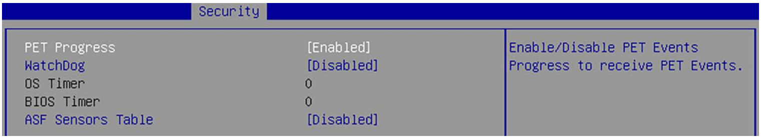
▸ Activate Remote Assistance Process

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

▸ Unconfigure ME

Enables or disables the Unconfigure ME.

▶ ASF Configuration



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

» PET Progress

Enables or disable the this item to receive PET Events.

» WatchDog

Enables or disable the watchdog timer.

» OS Timer

This item displays OS Timer.

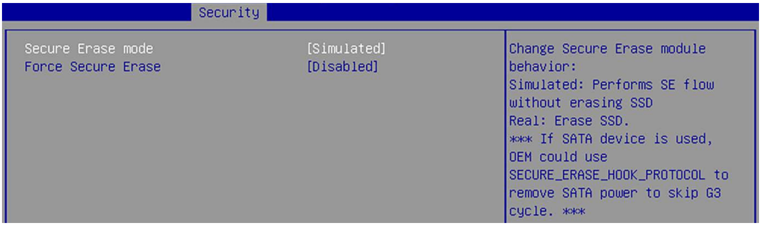
» BIOS Timer

This item displays BIOS Timer.

» ASF Sensor Table

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

▶ Secure Erase Configuration



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

» Secure Erase Mode

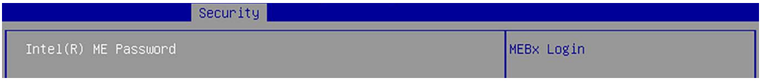
This setting change Secure Erase module behavior.

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

» Force Secure Erase

Enables or disables to force Secure Erase on next boot.

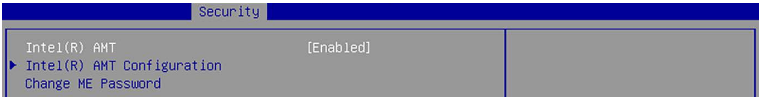
▶ MEBx (Management Engine BIOS Extension)



```
                         Security
 Intel(R) ME Password                          MEBx Login
```

» 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.



```
                         Security
 Intel(R) AMT                        [Enabled]
▶Intel(R) AMT Configuration
 Change ME Password
```

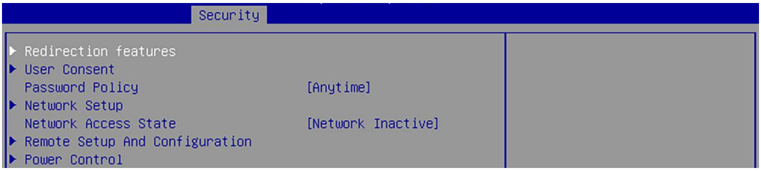
» Intel(R) AMT

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

Important

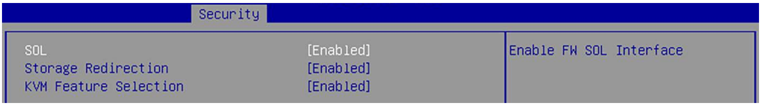
*The **MEBx menu** can be accessed only by pressing the **<DEL> or <F2> key** during the process of booting up the system.*

» Intel(R) AMT Configuration



```
                         Security
▶Redirection features
▶User Consent
 Password Policy                     [Anytime]
▶Network Setup
 Network Access State                [Network Inactive]
▶Remote Setup And Configuration
▶Power Control
```

» Redirection features



```
                         Security
 SOL                                 [Enabled]       Enable FW SOL Interface
 Storage Redirection                 [Enabled]
 KVM Feature Selection               [Enabled]
```

- **SOL**

  Enables or disables SOL (Serial Over LAN).

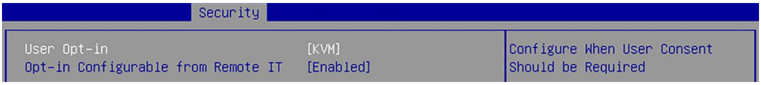
- **Storage Redirection**

  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



```
                              Security
 User Opt-in                          [KVM]        Configure When User Consent
 Opt-in Configurable from Remote IT   [Enabled]    Should be Required
```

- **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.

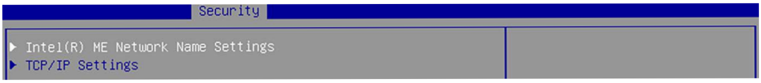
[During Setup And Configuration] Allows changing the Intel® MEBx password via the network interface during setup and configuration but not afterward. **Once the setup and configuration process is complete, the Intel MEBx password cannot be changed via the network interface.**

[Anytime] Allows changing the Intel® MEBx password through the network interface at any time.

Important

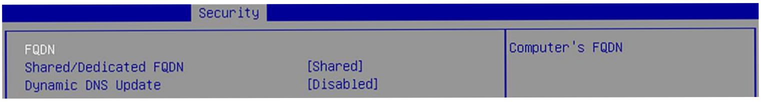
- *The Password Policy involves 2 passwords: the* ***Intel® MEBx password (local)****, entered when physically at the system, and the* ***network password (remote)****, used for accessing an Intel ME enabled system through the network. By default,* ***they are the same until the network password is changed 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



```
                         Security
▶ Intel(R) ME Network Name Settings
▶ TCP/IP Settings
```

- **Intel ® ME Network Name Settings**



```
                         Security
  FQDN                                               Computer's FQDN
  Shared/Dedicated FQDN            [Shared]
  Dynamic DNS Update               [Disabled]
```

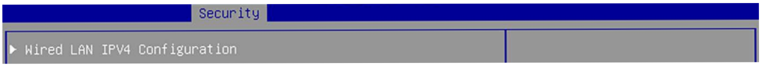
- **Shared/Dedicated FQDN**

  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**

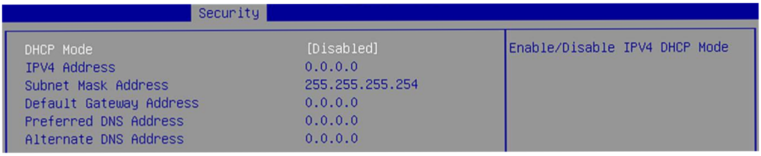
  Enables or disables automatic registration of the firmware's IP addresses and FQDN in the Domain Name System (DNS) using the Dynamic DNS Update protocol. **To enable Dynamic DNS Update, the Host Name and Domain Name must be set.**

- **TCP/IP Settings**



```
                         Security
▶ Wired LAN IPV4 Configuration
```

- **Wired Lan IPV4 Configuration**



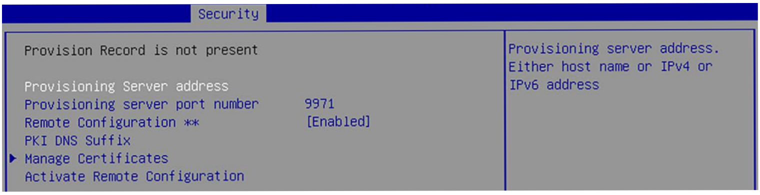
```
                         Security
  DHCP Mode                        [Disabled]        Enable/Disable IPV4 DHCP Mode
  IPV4 Address                     0.0.0.0
  Subnet Mask Address              255.255.255.254
  Default Gateway Address          0.0.0.0
  Preferred DNS Address            0.0.0.0
  Alternate DNS Address            0.0.0.0
```

- **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



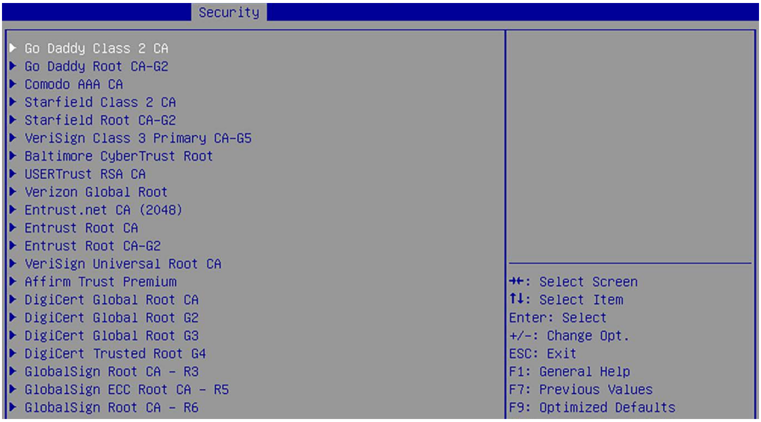
```
                         Security
  Provision Record is not present                    Provisioning server address.
                                                     Either host name or IPv4 or
  Provisioning Server address                        IPv6 address
  Provisioning server port number  9971
  Remote Configuration **          [Enabled]
  PKI DNS Suffix
▶ Manage Certificates
  Activate Remote 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:

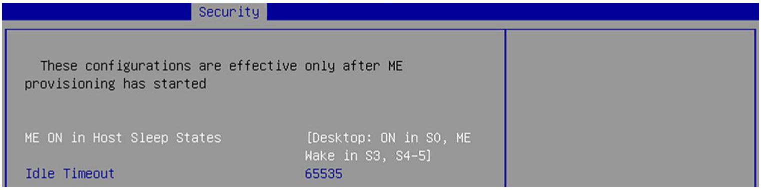


```
                         Security
▶ Go Daddy Class 2 CA
▶ Go Daddy Root CA-G2
▶ Comodo AAA CA
▶ Starfield Class 2 CA
▶ Starfield Root CA-G2
▶ VeriSign Class 3 Primary CA-G5
▶ Baltimore CyberTrust Root
▶ USERTrust RSA CA
▶ Verizon Global Root
▶ Entrust.net CA (2048)
▶ Entrust Root CA
▶ Entrust Root CA-G2
▶ VeriSign Universal Root CA
▶ Affirm Trust Premium                                  →←: Select Screen
▶ DigiCert Global Root CA                               ↑↓: Select Item
▶ DigiCert Global Root G2                               Enter: Select
▶ DigiCert Global Root G3                               +/-: Change Opt.
▶ DigiCert Trusted Root G4                              ESC: Exit
▶ GlobalSign Root CA - R3                               F1: General Help
▶ GlobalSign ECC Root CA - R5                           F7: Previous Values
▶ GlobalSign Root CA - R6                               F9: Optimized Defaults
```

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

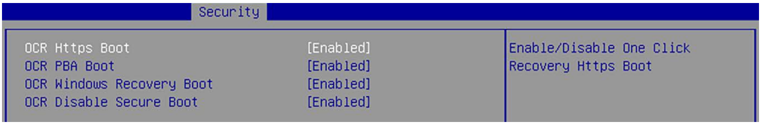
» Power control

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



```
                         Security

  These configurations are effective only after ME
provisioning has started


ME ON in Host Sleep States           [Desktop: ON in S0, ME
                                     Wake in S3, S4-5]
Idle Timeout                         65535
```

▶ One Click Recovery (OCR) Configuration



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

» OCR Https Boot

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

» OCR PBA Boot

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

» OCR Windows Recovery Boot

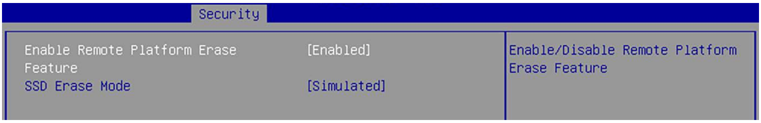
Enables or disables the Windows Recovery Boot for the OCR boot process. When enabled, the OCR boot process will prioritize Windows recovery options, allowing users to restore the system to a previous Windows state or initiate other Windows-specific recovery procedures.

» OCR Disable Secure Boot

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

▶ Remote Platform Erase Configuration

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



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

» Enable Remote Platform Erase Feature

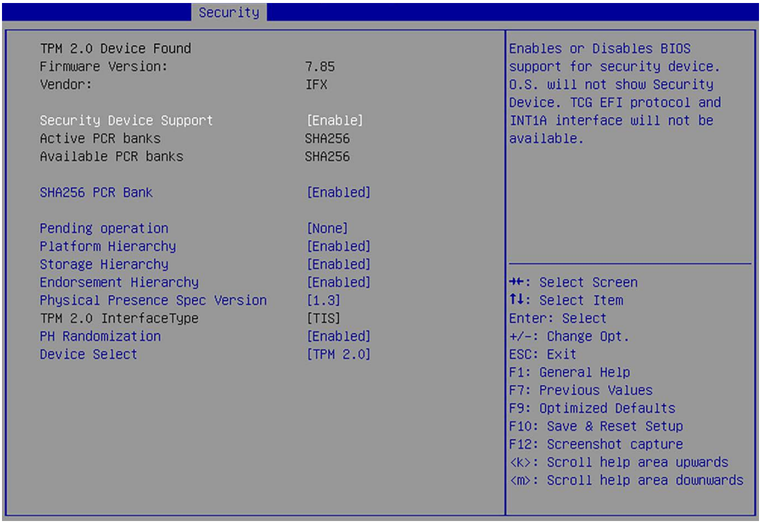
Enables or disables the ability to initiate the remote erasure process for the system or selected storage devices.

» SSD Erase Mode

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

[Simulated]	**Simulates** the erasure process **without permanently** deleting SSD data to estimate the time and resources required.
[Real]	**Actual** erasure process that **permanently** deletes the SSD data to ensure that the data is no longer accessible.

▶ Trusted Computing



```
                              Security

TPM 2.0 Device Found                               Enables or Disables BIOS
Firmware Version:               7.85               support for security device.
Vendor:                         IFX                O.S. will not show Security
                                                   Device. TCG EFI protocol and
Security Device Support         [Enable]           INT1A interface will not be
Active PCR banks                SHA256             available.
Available PCR banks             SHA256

SHA256 PCR Bank                 [Enabled]

Pending operation               [None]
Platform Hierarchy              [Enabled]
Storage Hierarchy               [Enabled]
Endorsement Hierarchy           [Enabled]          →←: Select Screen
Physical Presence Spec Version  [1.3]              ↑↓: Select Item
TPM 2.0 InterfaceType           [TIS]              Enter: Select
PH Randomization                [Enabled]          +/-: Change Opt.
Device Select                   [TPM 2.0]          ESC: Exit
                                                   F1: General Help
                                                   F7: Previous Values
                                                   F9: Optimized Defaults
                                                   F10: Save & Reset Setup
                                                   F12: Screenshot capture
                                                   <k>: Scroll help area upwards
                                                   <m>: Scroll help area downwards
```

▸ 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.

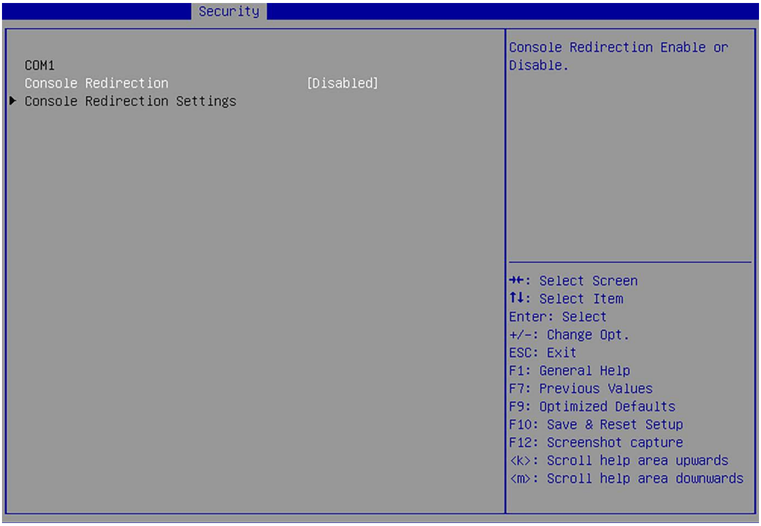
▸ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

▸ Device Select

Select your TPM device through this setting.

Serial Port Console Redirection



```
COM1
Console Redirection                    [Disabled]
▶ Console Redirection Settings
```

```
Console Redirection Enable or
Disable.
```

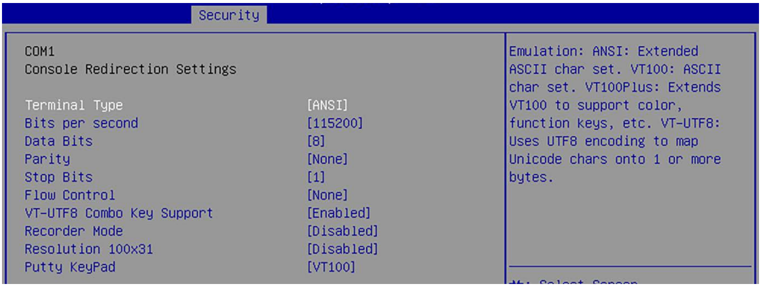
```
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
ESC: Exit
F1: General Help
F7: Previous Values
F9: Optimized Defaults
F10: Save & Reset Setup
F12: Screenshot capture
<k>: Scroll help area upwards
<m>: Scroll help area downwards
```

▶ 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**.



```
                              Security

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

» Terminal Type

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

[ANSI]	Extended ASCII character set.
[VT100]	ASCII character set.
[VT100Plus]	Extends VT100 to support color, function keys, etc.
[VT-UTF8]	Uses UTF8 encoding to map Unicode characters onto one or more bytes.

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

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

» Flow Control

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

» VT-UTF8 Combo Key Support

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

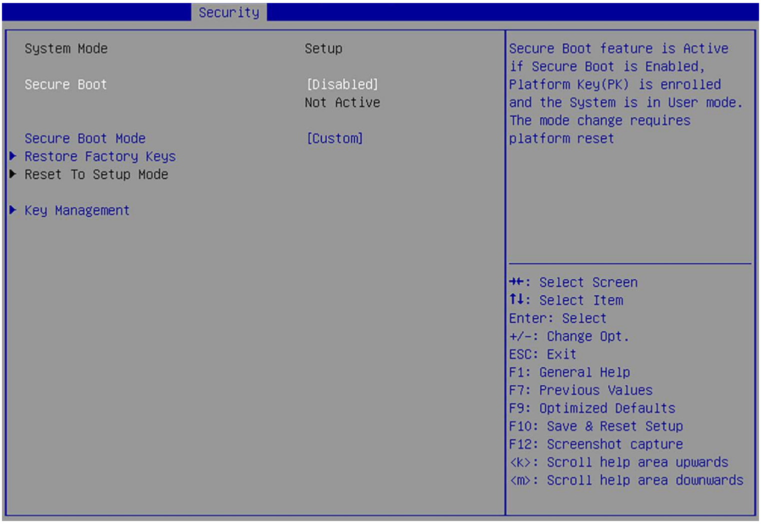
» Recorder Mode, Resolution 100x31

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

» Putty KeyPad

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

▶ Secure Boot



```
                          Security

 System Mode                         Setup              Secure Boot feature is Active
                                                        if Secure Boot is Enabled,
 Secure Boot                         [Disabled]         Platform Key(PK) is enrolled
                                     Not Active         and the System is in User mode.
                                                        The mode change requires
 Secure Boot Mode                    [Custom]           platform reset
▶ Restore Factory Keys
▶ Reset To Setup Mode

▶ Key Management

                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/-: Change Opt.
                                                        ESC: Exit
                                                        F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards
```

▶ 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

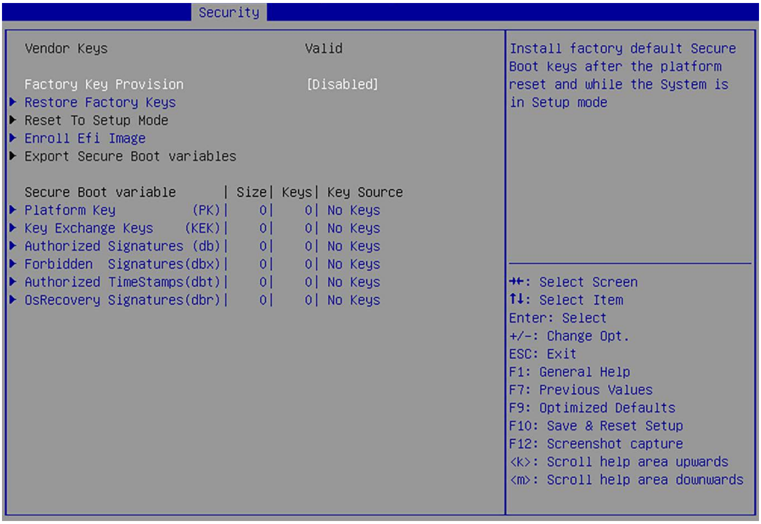
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▶ 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]**.



```
                              Security
  Vendor Keys                          Valid                Install factory default Secure
                                                            Boot keys after the platform
  Factory Key Provision                [Disabled]           reset and while the System is
▶ Restore Factory Keys                                      in Setup mode
▶ Reset To Setup Mode
▶ Enroll Efi Image
▶ Export Secure Boot variables

  Secure Boot variable      | Size| Keys| Key Source
▶ Platform Key          (PK)|    0|    0| No Keys
▶ Key Exchange Keys    (KEK)|    0|    0| No Keys
▶ Authorized Signatures (db)|    0|    0| No Keys
▶ Forbidden  Signatures(dbx)|    0|    0| No Keys            →←: Select Screen
▶ Authorized TimeStamps(dbt)|    0|    0| No Keys            ↑↓: Select Item
▶ OsRecovery Signatures(dbr)|    0|    0| No Keys            Enter: Select
                                                            +/-: Change Opt.
                                                            ESC: Exit
                                                            F1: General Help
                                                            F7: Previous Values
                                                            F9: Optimized Defaults
                                                            F10: Save & Reset Setup
                                                            F12: Screenshot capture
                                                            <k>: Scroll help area upwards
                                                            <m>: Scroll help area downwards
```

» **Platform Key (PK):**

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

» **Set New Key**

Sets a new PK to your system.

» **Delete Key**

Deletes the PK from your system.

» **Key Exchange Keys (KEK):**

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

» **Set New Key**

Sets a new KEK to your system.

» **Append Key**

Loads an additional KEK from storage devices to your system.

» **Delete Key**

Deletes the KEK from your system.

» **Authorized Signatures (db) :**

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

» **Set New Key**

Sets a new db to your system.

» **Append Key**

Loads an additional db from storage devices to your system.

» **Delete Key**

Deletes the db from your system.

» **Forbidden Signatures (dbx):**

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

» **Set New Key**

Sets a new dbx to your system.

» **Append Key**

Loads an additional dbx from storage devices to your system.

» **Delete Key**

Deletes the dbx from your system.

» **Authorized TimeStamps (dbt):**

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

» **Set New Key**

Sets a new DBT to your system.

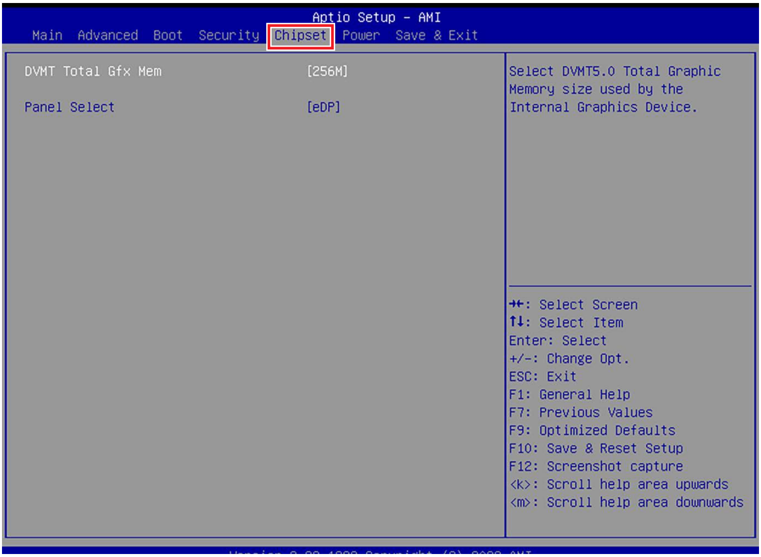
» **Append Key**

Loads an additional DBT from storage devices to your system.

» **OsRecovery Singnatures (dbr):**

Lists the available signatures for OS recovery.

Chipset



```
                              Aptio Setup - AMI
   Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

 DVMT Total Gfx Mem                 [256M]        Select DVMT5.0 Total Graphic
                                                  Memory size used by the
 Panel Select                       [eDP]         Internal Graphics Device.

                                                  →←: Select Screen
                                                  ↑↓: Select Item
                                                  Enter: Select
                                                  +/-: Change Opt.
                                                  ESC: Exit
                                                  F1: General Help
                                                  F7: Previous Values
                                                  F9: Optimized Defaults
                                                  F10: Save & Reset Setup
                                                  F12: Screenshot capture
                                                  <k>: Scroll help area upwards
                                                  <m>: Scroll help area downwards
```

▶ 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

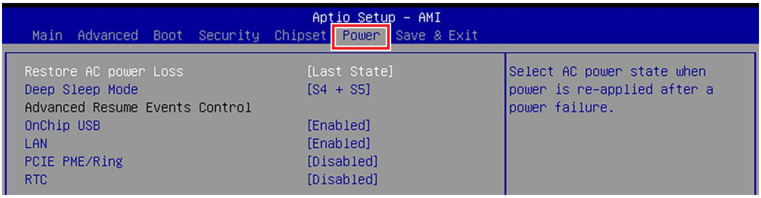
This setting specifies the LCD Panel's resolution and distribution formats. The item **will display when LVDS is enabled**.

▸ 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%

Power



```
Restore AC power Loss                 [Last State]
Deep Sleep Mode                       [S4 + S5]
Advanced Resume Events Control
OnChip USB                            [Enabled]
LAN                                   [Enabled]
PCIE PME/Ring                         [Disabled]
RTC                                   [Disabled]
```

Select AC power state when power is re-applied after a power failure.

▶ 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.

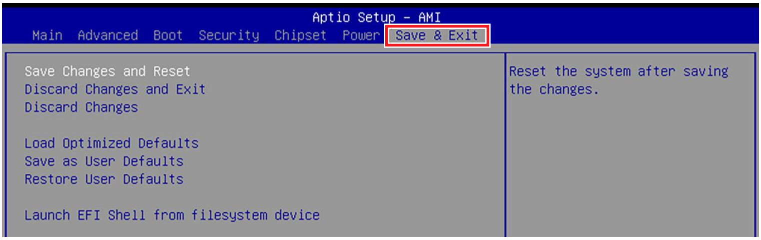
▶ PCIE PME/Ring

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.

Save & Exit



```
Aptio Setup - AMI
Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

Save Changes and Reset                          Reset the system after saving
Discard Changes and Exit                        the changes.
Discard Changes

Load Optimized Defaults
Save as User Defaults
Restore User Defaults

Launch EFI Shell from filesystem device
```

▶ Save Changes and Reset

Save changes to CMOS and reset the system.

▶ Discard Changes and Exit

Abandon all changes and exit the Setup Utility.

▶ Discard Changes

Abandon all changes.

▶ Load Optimized Defaults

Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.

▶ Save as User Defaults

Save changes as the user's default profile.

▶ Restore User Defaults

Restore the user's default profile.

▶ Launch EFI Shell from filesystem device

This setting helps to launch the EFI Shell application from one of the available file system devices.

GPIO WDT 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.

1.1 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.

2.1 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
```

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.

3.1 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)
```

3.2 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);
```

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
```