MS-CF20

Industrial Computer Board

User Guide

Contents

Regulatory Notices....4

Safety Information....7

Specifications....9

Motherboard Overview....12

- SKU1....12
- SKU2....13

Rear I/O Panel....14

- SKU1....14
- SKU2....14
- DisplayPort....15
- HDMI™ Connector....15
- RS232/422/485 Serial Port....15
- VGA Port....15
- 2.5 GbE RJ-45 LAN Jacks....16
- USB 10Gbps Ports....16
- Line-Out Jack....16
- Mic-In Jack....16
- CPU Socket....19
- CPU & Heatsink Installation....21

Memory Slots....22

Storage Connectors....24

Expansion Slots....25

- PCIe Slots....25
- PCI Slot....25
- M.2 Slots....26

Power Connectors....28

Cooling Connectors....29

Revision

V1.2, 2025/08

Audio Connectors 30
USB Connectors 31
Other Connectors and Components 33
Jumpers 39
BIOS Setup 41
Entering Setup 41
The Menu Bar 43
Main 44
Advanced 45
Boot 52
Security 53
Chipset 65
Power 66
Save & Exit 67
GPIO WDT SMBus Programming 68
Abstract 68
General Purpose IO 69
Watchdog Timer 71
SMBus Access 72

Regulatory Notices

CE Conformity

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

FCC-B Radio Frequency Interference Statement

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

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

Notice 1

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

Notice 2

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

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

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

WEEE Statement

European Union: This symbol on the product indicates that this product cannot be discarded as municipal waste. Instead, it is your responsibility to dispose of your waste electrical and electronic equipment by handing it over to a designated collection point for recycling. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.



Chemical Substances Information

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

Battery Information

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

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

European Union:



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

BSMI:



廢電池請回收
For better environmental protection, waste batteries should be collected separately for recycling or special disposal.

California, USA:



The button cell battery may contain perchlorate material and requires special handling when recycled or disposed of in California.
For further information please visit:
http://www.dtsc.ca.gov/hazardouswaste/perchlorate/

Environmental Policy

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

Copyright and Trademarks Notice

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

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

Technical Support

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

Safety Information

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

General Safety Instructions

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

Electrostatic Discharge (ESD) Precautions

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

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

Power Safety

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

Installation Instructions

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

When to Contact Service Personnel

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

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

Specifications

Model	MS-CF20-SKU1	MS-CF20-SKU2
Dimensions	305 (L) mm x 244 (W) mm x 1.6(H)mm, ATX-Size	
Processor	• Intel® Arrow Lake-S Core™ Ultra 9/7/5, up to 125W TDP	
Socket	LGA1851	
Chipset	Intel® W880	
Memory	• 4 x DDR5 UDIMM slots (288-pin, vertical) - Dual-Channel, ECC/Non-ECC (ECC support depends on CPU) - Up to 5600 MT/s - Max 192GB	
Network	• 4 x Intel® I226-LM PCIe 2.5GbE LAN - LAN1: Supports iAMT 19.X	• 2 x Intel® I226-LM PCIe 2.5GbE LAN - LAN1: Supports iAMT 19.X
Storage	• 4 x SATA 3.0 6Gb/s connectors - Support RAID 0/1/5/10 - Support AHCI mode	
Audio	• Realtek® ALC897 Audio Codec	
Graphics	• 1 x DisplayPort 1.4a, up to 4096×2304 @ 60Hz • 1 x HDMI™ 2.0b, up to 4096x2160 @ 60Hz • 1 x VGA, up to 1920x1200 @ 60Hz • 3 independent display modes supported - DP - HDMI™ - VGA	
Expansion Slots	• 2 x PCIe 5.0 x16 slots (PCIE1, 4)*signal from CPU • 1 x PCIe 4.0 x4 slot (PCIE2) signal from CPU • 3 x PCIe 4.0 x4 slots (PCIE3, 5**, 7) • 1 x PCI 3.0 x1 slot (PCI1) • 1 x M.2 M Key slot (M2_M1, 2280) - Supports PCIe 5.0 x4 NVMe • 1 x M.2 M Key slot (M2_M2, 2280) - Supports PCIe 4.0 x4/x2/x1 NVMe (shared with PCIE5) • 1 x M.2 E Key slot (2230) - Supports PCIe x1 signal - Supports Intel® Wi-Fi 6E AX210 , Intel® Wi-Fi 7 BE200. CNVi devices are not supported.	
	*PCIE1 and PCIE4 are designated for discrete graphics and storage devices. When the PCIE1 slot is in use, it operates at 5.0 x16 speed, while the PCIE4 slot becomes unavailable. If both PCIE1 and PCIE4 slots are occupied, they both run at 5.0 x8 speed. ** It is necessary to remove the M.2 screw when installing a PCIe x8 or x16 card in PCIE5.	

Continued on next column

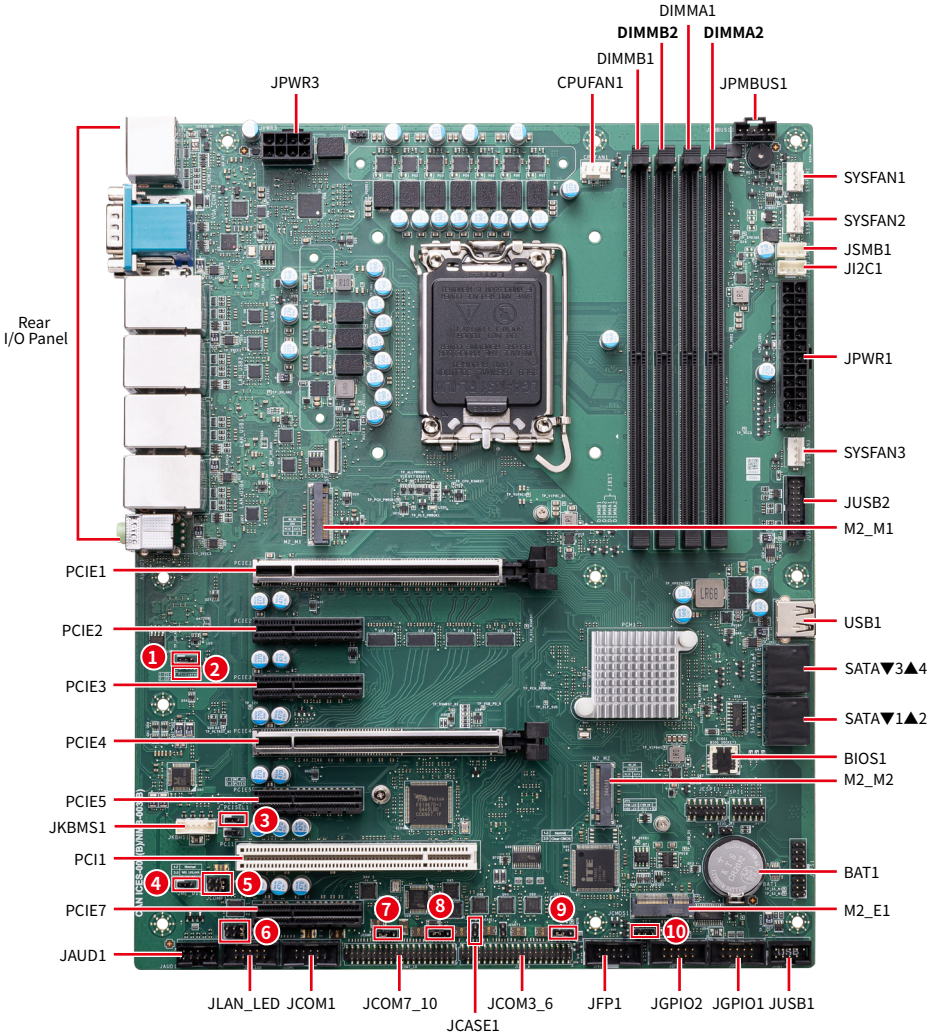
Model	MS-CF20-SKU1	MS-CF20-SKU2
Rear I/O	• 1 x DisplayPort (1.4a) • 1 x HDMI™ connector (2.0b) • 1 x VGA port • 1 x DB-9 RS-232/422/485 serial port - COM1: Ring/ 0V/ 5V/ 12V (default set to Ring), auto-flow control supported • 1 x Line-out jack • 1 x Mic-in jack • 8 x USB 10Gbps Type-A ports	
	• 4 x 2.5 GbE RJ-45 LAN ports	• 2 x 2.5 GbE RJ-45 LAN ports
Onboard Connector	• 1 x 4-pin PWM CPU fan connector • 3 x 4-pin PWM system fan connectors • 1 x Front Audio header (line-out & mic-in) • 1 x USB 5Gbps header (JUSB2) • 1 x USB 2.0 header (JUSB1) • 1 x USB 2.0 Type-A port (USB1) • 1 x Front Panel header • 1 x GPI header • 1 x GPO header • 1 x PMBus header • 1 x I2C header • 1 x SMBus header • 1 x Serial port header • 1 x LAN LED header • 1 x PS/2® keyboard & mouse connector • 1 x Chassis Intrusion header • 4 x COM voltage select jumpers • 1 x AT/ ATX mode select jumper • 2 x ME jumpers • 1 x Clear CMOS jumper • 1 x PCIE x16 & x8 Select Jumper	
	• 2 x Serial port headers (JCOM3_6, JCOM7_10)	• 1 x Serial port header (JCOM3_6)
Power	• 1 x 24-pin ATX power connector • 1 x 8-pin 12V ATX power connector	

Continued on next column

Model	MS-CF20-SKU1	MS-CF20-SKU2
OS Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit) • Windows 11 IoT Enterprise 24H2 LTSC (64-Bit) • Linux available upon request	
Certification	CE, FCC Class B, BSMI, RCM, VCCI, UKCA, CN	
Environment	• Operating Temperature: 0 ~ 60°C • Storage Temperature: -20 ~ 80°C • Relative Humidity: 10 ~ 90%, non-condensing	

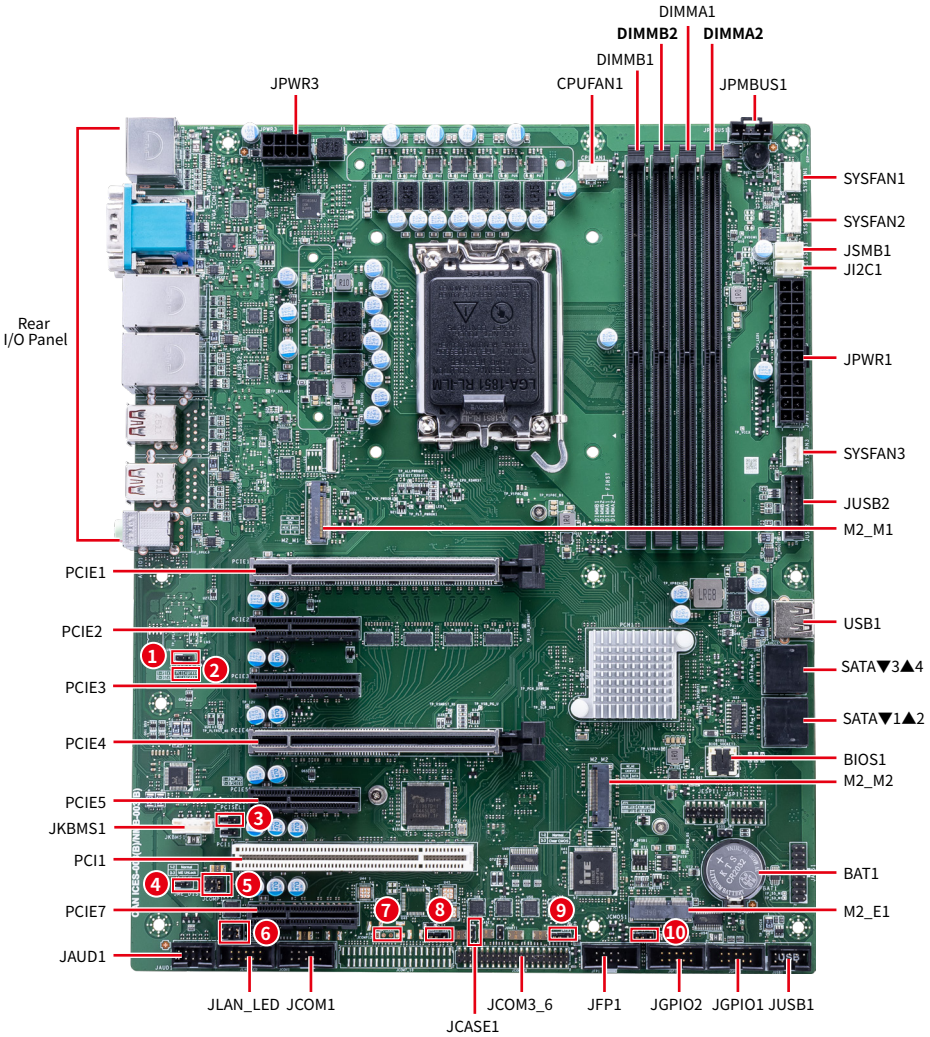
Motherboard Overview

SKU1



1. J_CFG16
2. JME_DIS2
3. J_PCISEL1
4. JME_DIS1
5. JCOMP1
6. JCOMP2
7. JCOMP12
8. JCOMP11
9. JATX1
10. JCMOS1

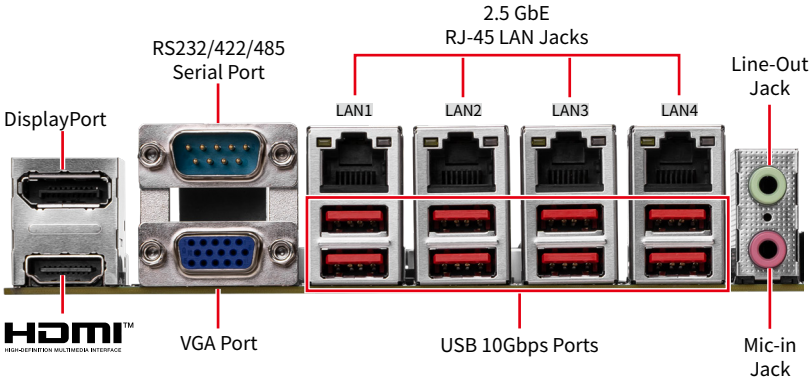
SKU2



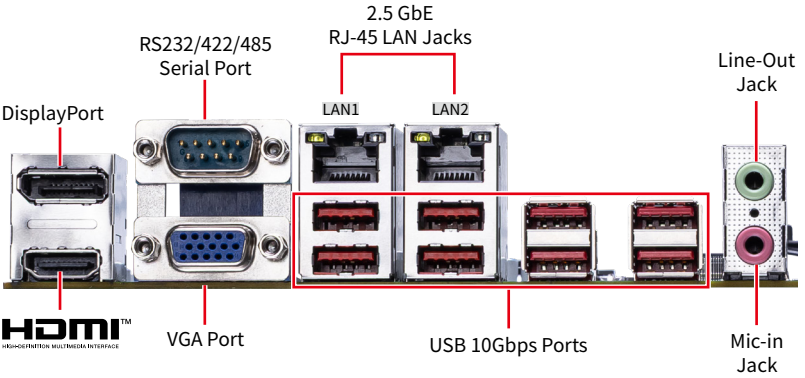
1. J_CFG16
2. JME_DIS2
3. J_PCISEL1
4. JME_DIS1
5. JCOMP1
6. JCOMP2
7. JCOMP12
8. JCOMP11
9. JATX1
10. JCMOS1

Rear I/O Panel

SKU1



SKU2



DisplayPort

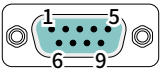
DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

HDMI™ Connector

HDMI™ is a digital interface for uncompressed audio/video streams, accommodating all TV formats and multi-channel 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	DCD	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI/POWER	RI/0V/5V/12V selected by Jumper

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

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

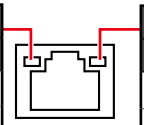
VGA Port

The VGA port supports monitors and other VGA interface devices.

2.5 GbE RJ-45 LAN Jacks

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 10Gbps Ports

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

Line-Out Jack

This connector is provided for headphones or speakers.

Mic-In Jack

This connector is provided for microphones.

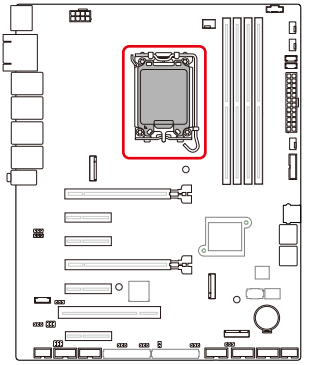
Component Contents

Component	Page
CPU Socket	**19**
Installing the CPU to the LGA1851 socket	19
CPU & Heatsink Installation	**21**
Memory Slots	**22**
DIMMA1, A2, B1, B2: DDR5 DIMM Slots	22
Memory module installation recommendation	22
Storage Connectors	**24**
SATA_1_2, SATA_3_4: SATA 3.0 6Gb/s Ports	24
Expansion Slots	**25**
PCIe Slots	**25**
PCIE1~5, 7: PCIe Expansion Slots	25
PCI Slot	**25**
PCI1: PCI Expansion Slot	25
M.2 Slots	**26**
M2_M1: M.2 Slot (M Key, PCIe 5.0 x4, 2280)	26
M2_M2: M.2 Slot (M Key, PCIe 4.0 x4/x2/x1, 2280)	26
M2_E1: M.2 Slot (E Key, 2230)	27
Power Connectors	**28**
JPWR1: 24-Pin ATX Power Connector	28
JPWR3: 8-Pin ATX 12V Power Connector	28
Cooling Connectors	**29**
CPUFAN1, SYSFAN1~3: CPU/ System Fan Connectors	29
Audio Connectors	**30**
JAUD1: Front Audio Header (Line-out/ MIC-in)	30
USB Connectors	**31**
JUSB2: USB 5Gbps Header	31
USB1: USB 2.0 Type-A Port	32
JUSB1: USB 2.0 Header	32

Other Connectors and Components	**33**
JFP1: Front Panel Header	33
JGPIO2: GPO Header	33
JGPIO1: GPI Header	33
JPMBUS1: PMBus Header	34
JSMB1: SMBus Header	34
JI2C1: I2C Header	34
JCOM1: Serial Port Header	35
JCOM3_6, JCOM7_10: COM Port Box Headers	35
JKBMS1: PS/2® Keyboard & Mouse Connector	37
JLAN_LED: LAN LED Header	37
JCASE1: Chassis Intrusion Header	37
BAT1: CMOS Battery	38
Replacing CMOS battery	38
Jumpers	**39**

CPU Socket

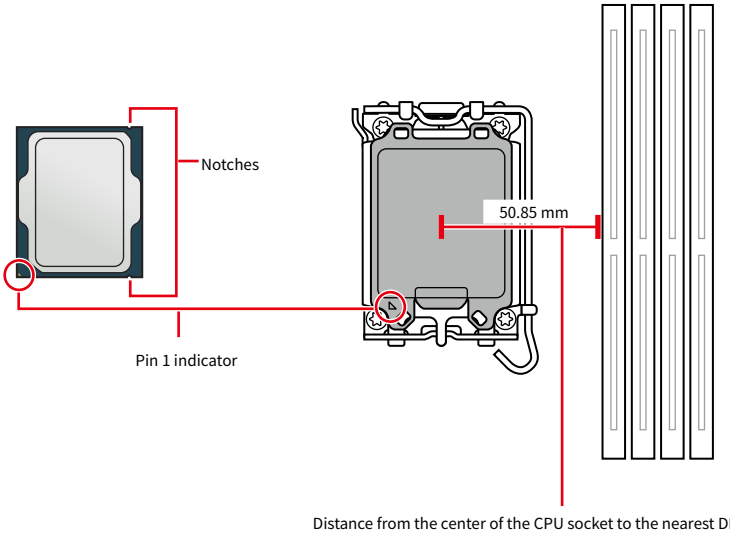
The LGA1851 socket is the CPU socket that is designed for Intel® desktop processors. It is a land grid array (LGA) socket with 1851 pins. The socket is not compatible with previous generations of Intel® processors.



Installing the CPU to the LGA1851 socket

The surface of the LGA1851 CPU has **two notches** to assist in correctly lining up the CPU for motherboard placement. The golden triangle is the Pin 1 indicator.

To install the CPU, align the two notches on the LGA1851 socket with the two corresponding notches on the CPU.



Important

- *Please note that LGA1851 and LGA1700 sockets have different physical configurations and pin layouts. Before installation, ensure your CPU is compatible with the LGA1851 socket. Incorrect installation may damage the CPU, socket, and motherboard. DO NOT install a CPU designed for LGA1155, LGA1156, LGA1151, LGA1200, and LGA1700 sockets on the LGA1851 socket.*
- *Please ensure that the motherboard and power supply are turned off and always disconnect the power cord from the power outlet before installing or removing the CPU.*
- *Please retain the CPU protective cap after installing the processor. MSI will deal with Return Merchandise Authorization (RMA) requests if only the motherboard comes with the protective cap on the CPU socket.*
- *Whenever the CPU is not installed, always protect the CPU socket pins by covering the socket with the protective cap.*
- *The CPU should only fit in one orientation, so do not force it. Gently place the CPU into the socket without applying excessive pressure.*
- *Please handle the CPU by the edges only; avoid touching the pins or the surface of the CPU. Any damage to the pins can result in a malfunctioning CPU.*
- *When installing a CPU, always remember to install a CPU heatsink. A CPU heatsink is necessary to prevent overheating and maintain system stability.*
- *Please install the CPU cooler according to the manufacturer' s instructions. Make sure it is securely a tight seal with the CPU and attached to the motherboard to ensure proper heat dissipation.*
- *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.*

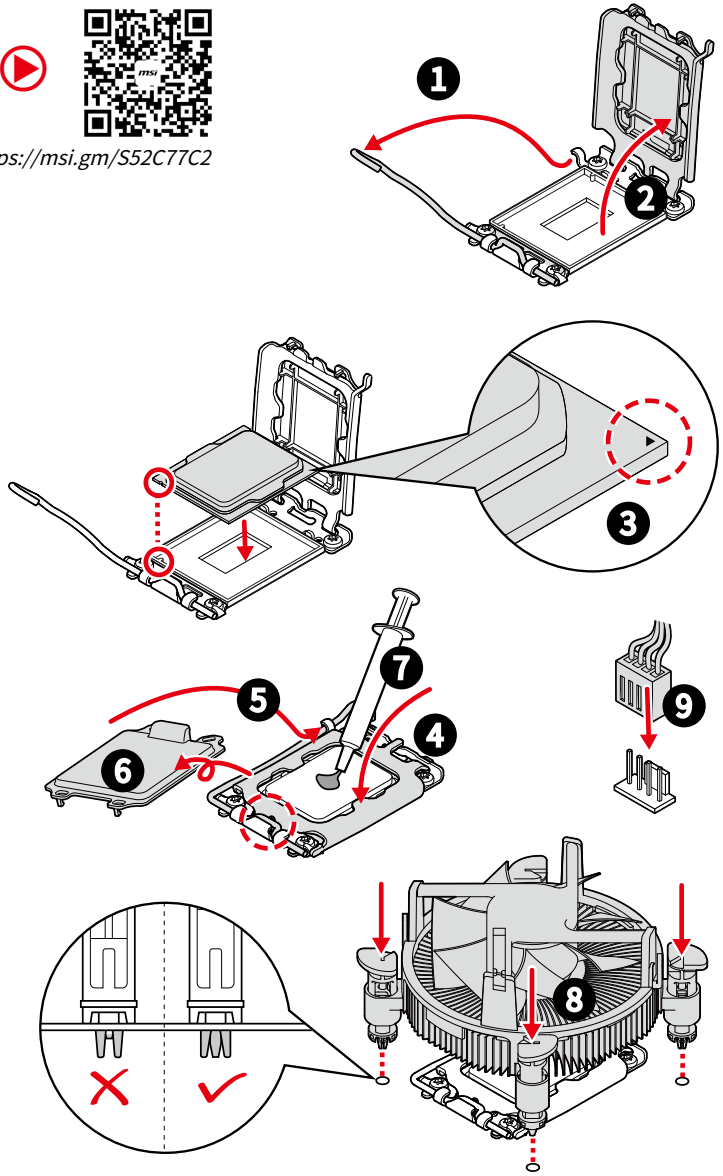
CPU & Heatsink Installation

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.

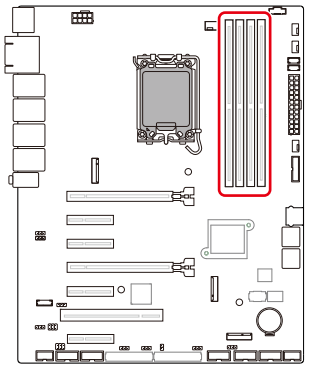
https://msi.gm/S52C77C2

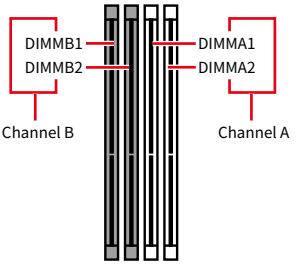


Memory Slots

DIMMA1, A2, B1, B2: DDR5 DIMM Slots

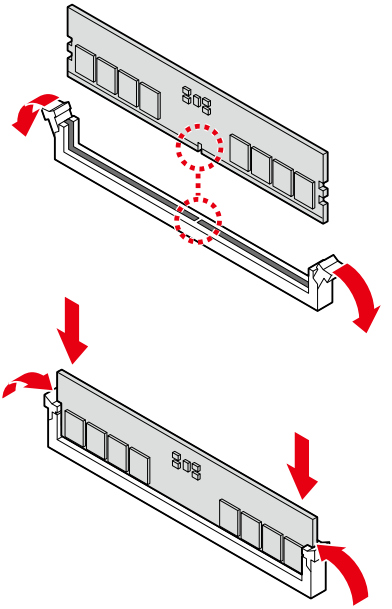
The DIMM slots are intended for memory modules.



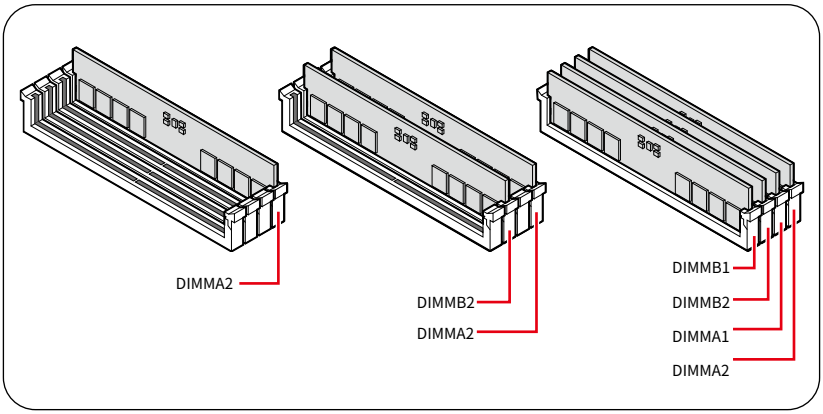


Installing Memory Modules

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



Memory module installation recommendation



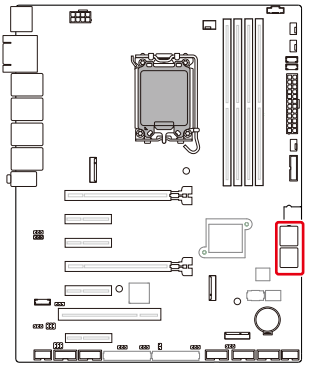
Important

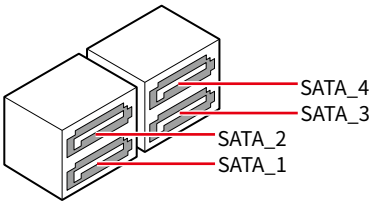
- *You can barely see the golden finger if the memory module is properly inserted in the DIMM slot.*
- *Only support **UDIMM**.*
- *There should be at least 1 DDR5 DIMM populated.*
- *Paired memory installation for Max performance.*
- *If only **1 DIMM** is populated in a channel, then populate it in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

Storage Connectors

SATA_1_2, SATA_3_4: SATA 3.0 6Gb/s Ports

These ports are SATA 6Gb/s interface port, it can connect to one SATA device.

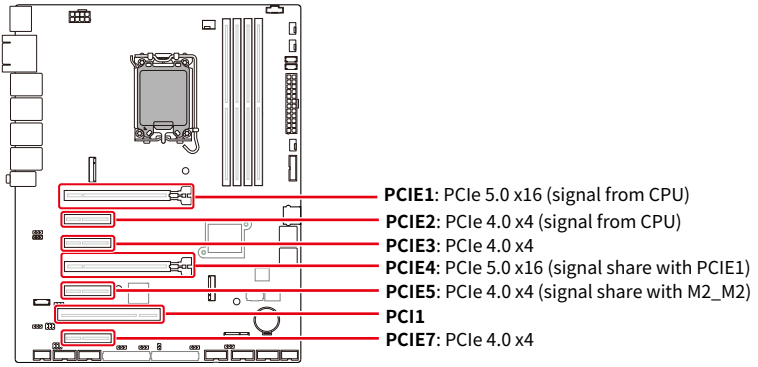




Important

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

Expansion Slots



PCIe Slots

PCIE1~5, 7: PCIe Expansion Slots

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

PCI Slot

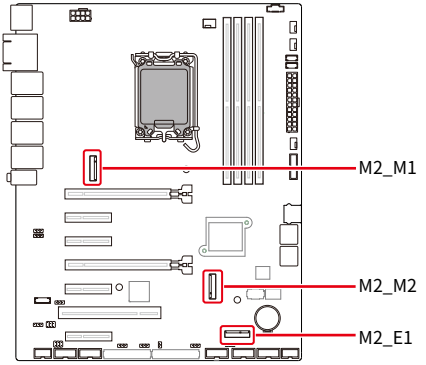
PCI1: PCI Expansion Slot

The PCI (Peripheral Component Interconnect) slot supports PCI interface expansion cards.

Important

- *PCIE1 and PCIE4 are designated for discrete graphics and storage devices.*
- *When the PCIE1 slot is occupied, it will operate at 5.0 x16 speed, while the PCIE4 slot will not be available. Both PCIE1,4 slots will run at 5.0 x8 speed when occupied.*
- *It is necessary to remove the M.2 screw when installing a PCIe x8 or x16 card in PCIE5.*
- *When adding or removing expansion cards, make sure that you unplug the power supply first. Meanwhile, read the documentation for the expansion card to configure any necessary hardware or software settings for the expansion card, such as jumpers, switches or BIOS configuration.*

M.2 Slots

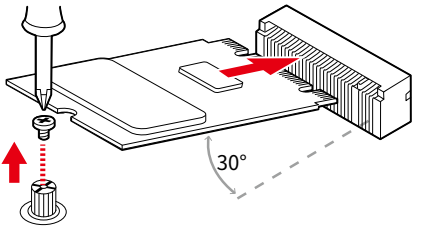


M2_M1: M.2 Slot (M Key, PCIe 5.0 x4, 2280)

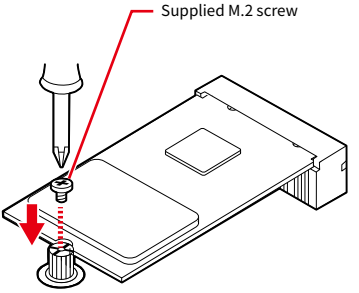
M2_M2: M.2 Slot (M Key, PCIe 4.0 x4/x2/x1, 2280)

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

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

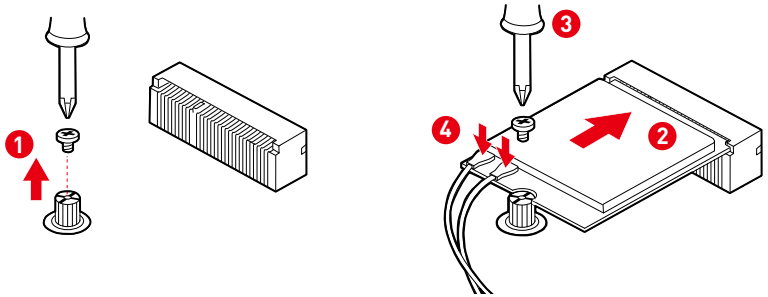


2. Secure the M.2 SSD in place with the supplied M.2 screw.



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

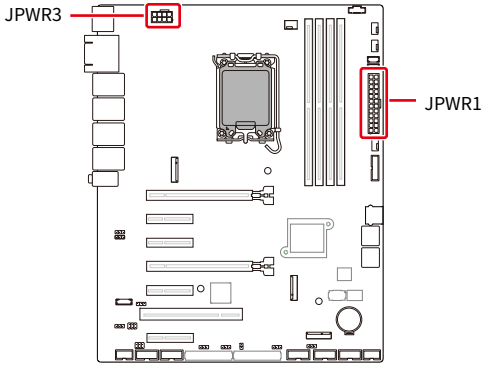
Please install the Wi-Fi/ Bluetooth card into the M.2 slot as shown below.



Feature

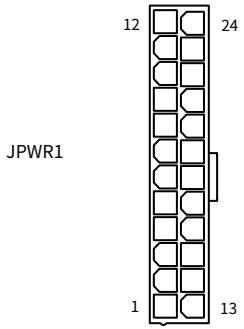
- Supports PCIe x1 signal.
- Supports Intel® Wi-Fi 6E AX210, Intel® Wi-Fi 7 BE200. CNVi devices are not supported.

Power Connectors



JPWR1: 24-Pin ATX Power Connector

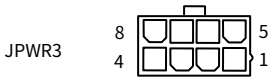
This connector allows you to connect an ATX power supply.



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

JPWR3: 8-Pin ATX 12V Power Connector

This connector allows you to connect an ATX power supply.

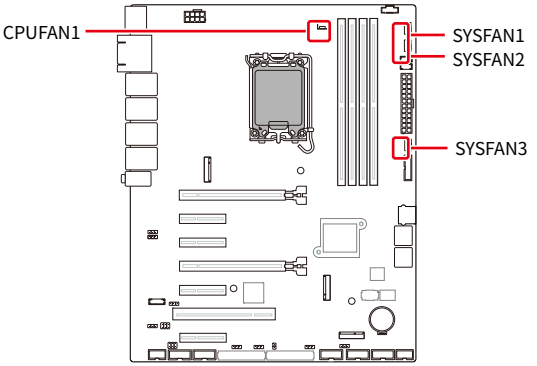


1	GND	5	P12V
2	GND	6	P12V
3	GND	7	P12V
4	GND	8	P12V

Important

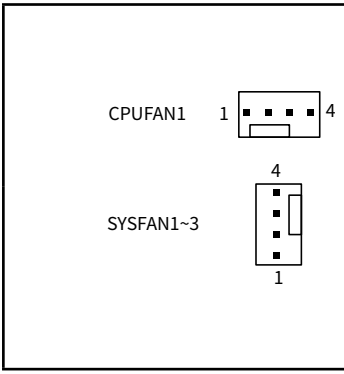
Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Cooling Connectors



CPUFAN1, SYSFAN1~3: CPU/ System Fan Connectors

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

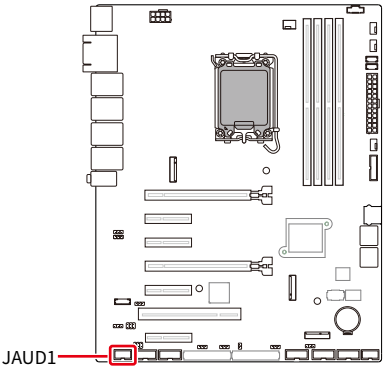


1	GND	2	FAN POWER
3	FAN SENSE	4	FAN_PWM

Important

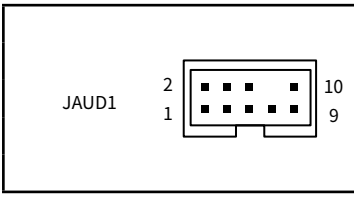
Please refer to the recommended CPU fans at processor' s official website or consult the vendors for proper CPU cooling fan.

Audio Connectors



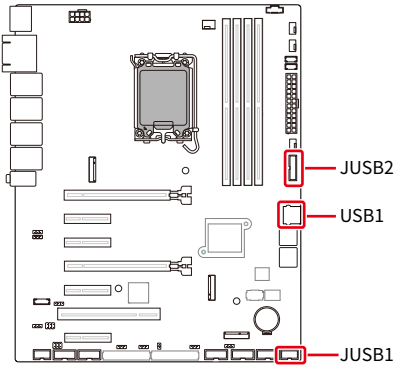
JAUD1: Front Audio Header (Line-out/ MIC-in)

This header allows you to connect front panel audio.



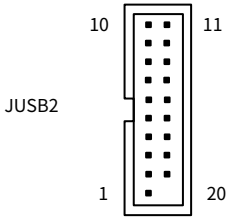
1	MIC_L	2	GND
3	MIC_R	4	NC
5	LINE_OUT_R	6	MIC_JD
7	HP_ON	8	No pin
9	LINE_OUT_L	10	LINE_OUT_JD

USB Connectors



JUSB2: USB 5Gbps Header

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



1	V_{BUS}	11	D+
2	SSRX-	12	D-
3	SSRX+	13	GND
4	GND	14	SSTX+
5	SSTX-	15	SSTX-
6	SSTX+	16	GND
7	GND	17	SSRX+
8	D-	18	SSRX-
9	D+	19	V_{BUS}
10	NC	20	No Pin

USB1: USB 2.0 Type-A Port

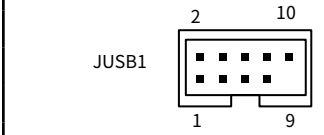
The USB (Universal Serial Bus) port is for attaching USB devices such as keyboard, mouse, or other USB-compatible devices. It supports data transfer rate up to **480 Mbps**.



1	V_{BUS}
2	D-
3	D+
4	GND

JUSB1: USB 2.0 Header

This header is ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices. It supports data transfer rate up to **480 Mbps**.

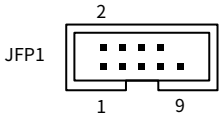


1	V_{BUS}	2	V_{BUS}
3	D-	4	D-
5	D+	6	D+
7	GND	8	GND
9	No Pin	10	NC

Other Connectors and Components

JFP1: Front Panel Header

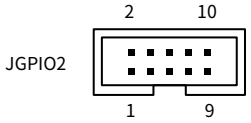
This front-panel header is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.



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

JGPIO2: GPO Header

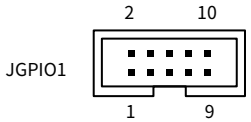
This header is provided for the General-Purpose Output (GPO) peripheral module.



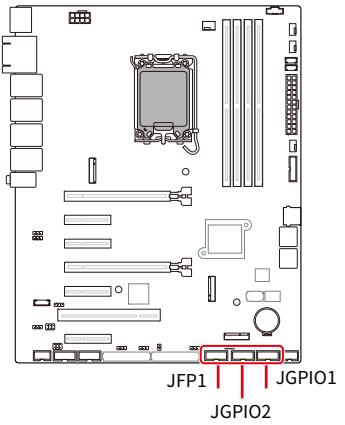
1	GND	2	N_GPIO_VCC (VCC5)
3	N_GPO0	4	N_GPO4
5	N_GPO1	6	N_GPO5
7	N_GPO2	8	N_GPO6
9	N_GPO3	10	N_GPO7

JGPIO1: GPI Header

This header is provided for the General-Purpose Input (GPI) peripheral module.

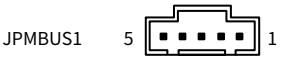


1	GND	2	N_GPIO_VCC (VCC5)
3	N_GPI0	4	N_GPI4
5	N_GPI1	6	N_GPI5
7	N_GPI2	8	N_GPI6
9	N_GPI3	10	N_GPI7



JPMBUS1: PMBus Header

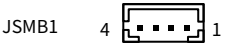
Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



1	SMBCLK
2	SMBDATA
3	SMBALERT#
4	GND
5	3.3V

JSMB1: SMBus Header

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



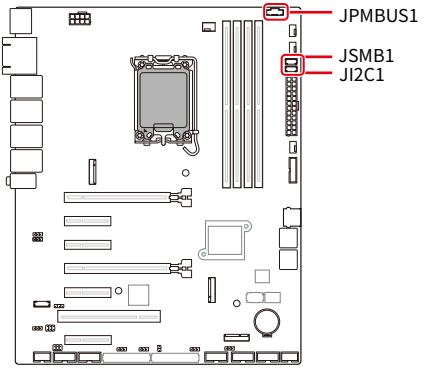
1	5V
2	SMBCLK
3	SMBDATA
4	GND

JI2C1: I2C Header

This header is provided for users to connect I^2C (Inter-Integrated Circuit) interface.

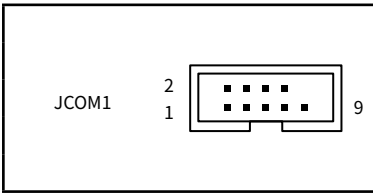


1	NC
2	I2C_CLK
3	I2C_DATA
4	GND



JCOM1: Serial Port Header

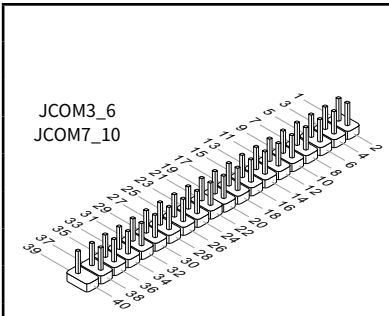
This header is 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial device to it.



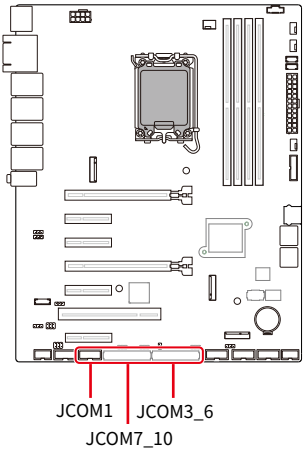
1	DCD	2	RXD
3	TXD	4	DTR
5	GND	6	DSR
7	RTS	8	CTS
9	RI/POWER	10	No Pin

JCOM3_6, JCOM7_10: COM Port Box Headers

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



1	11	21	31	DCD	Data Carrier Detect
2	12	22	32	RXD	Receive Data
3	13	23	33	TXD	Transmit Data
4	14	24	34	DTR	Data Terminal Ready
5	15	25	35	GND	Ground
6	16	26	36	DSR	Data Set Ready
7	17	27	37	RTS	Request To Send
8	18	28	38	CTS	Clear To Send
9	19	29	39	POWER	5V or 12V selected by Jumper
10	20	30	40	No pin	Key



Important

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

Feature

- Supports True RS-232, TTL RS-232
- JCOM1: Auto flow control, RS- 422/485 with transmission range over 1000 meters

SKU1

- JCOM1

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

- JCOM3_6, JCOM7_10

Supports RS-232, with 0V/ 5V/ 12V (default set to 5V).

SKU2

- JCOM1

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

- JCOM3_6

Supports RS-232, with 0V/ 5V/ 12V (default set to 5V).

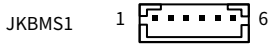
RS232		
PIN	**SIGNAL**	**DESCRIPTION**
1	DCD	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI/POWER	RI/0V/5V/12V selected by Jumper

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

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

JKBMS1: PS/2® Keyboard & Mouse Connector

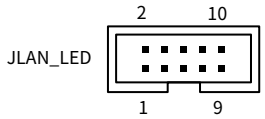
This connector is provided to connect a keyboard and a mouse.



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

JLAN_LED: LAN LED Header

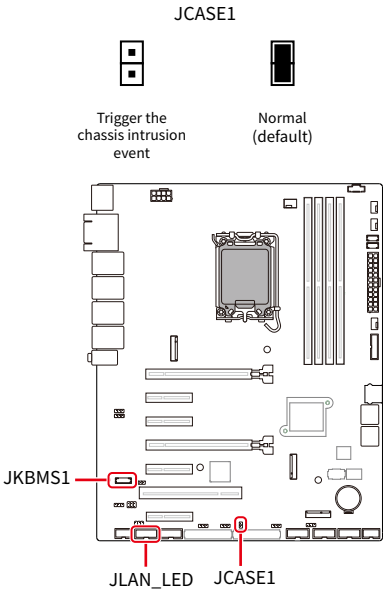
This header is provided for rear panel LAN LEDs.



1	LAN1_ACT_LINK	2	LAN1_LED_LINK#
3	LAN2_ACT_LINK	4	LAN2_LED_LINK#
5	LAN3_ACT_LINK	6	LAN3_LED_LINK#
7	LAN4_ACT_LINK	8	LAN4_LED_LINK#
9	NC	10	NC

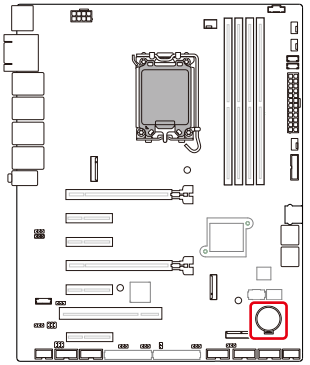
JCASE1: Chassis Intrusion Header

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



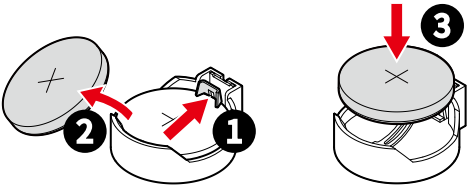
BAT1: CMOS Battery

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. Push the retainer clip to free the battery.
2. Remove the battery from the socket.
3. Install the new CR2032 coin-cell battery with the **+** sign facing up. Ensure that the retainer holds the battery securely.



WARNING

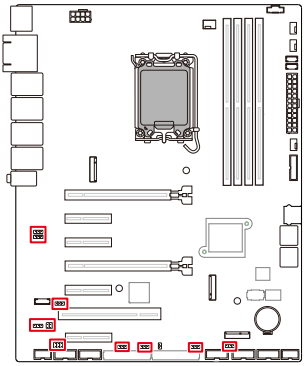
KEEP OUT OF REACH OF CHILDREN

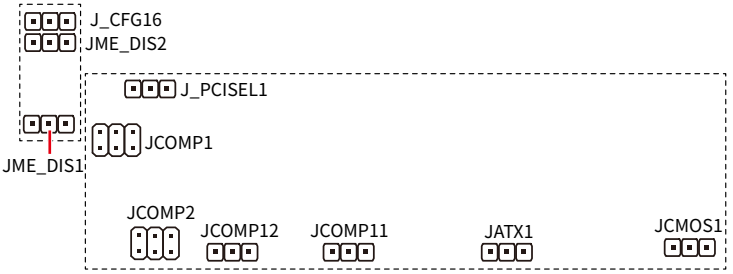
- *Swallowing can lead to chemical burns, perforation of soft tissue, can death.*
- *Severe burns can occur within 2 hours of ingestion.*
- *If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.*

Jumpers

Important

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





Jumper Name	Default Setting	Description
J_CFG16	1 	**PCIE x16 & x8 Select Jumper (PCIE 1 slot)** 1-2: 1 x 16 PCIExpress _ Auto switch (Default) 2-3: 1 x 8 PCIExpress _ Manual switch ***When the PCIE1 slot is occupied, it will operate at 5.0 x16 speed, while the PCIE4 slot will not be available. Both PCIE1,4 slots will run at 5.0 x8 speed when occupied. However, if the jumper is set to pins 2–3, the PCIe 1 slot can only run at 5.0 x8 speed.**
JME_DIS1~2	1 	**ME Jumper** 1-2: Normal (Default) 2-3: ME Unlock ***JME_DIS1 and JME_DIS2 must be set to the same position.**

Jumper Name	Default Setting	Description
J_PCISEL1	1 	**PCI IO Power Select Jumper** 1-2: 5V (Default) 2-3: 3.3V
JCOMP1~2	2 6  1 5	**COM Voltage Select Jumper** 1-2: 5V 3-4: 12V 5-6: RI (Default)
JCOMP11~12	1 	**COM Voltage Select Jumper** 1-2: 5V (Default) 2-3: 12V
JATX1	1 	**AT/ ATX Mode Select Jumper** 1-2: ATX (Default) 2-3: AT
JCMOS1	1 	**Clear CMOS Jumper** 1-2: Normal (Default) 2-3: Clear CMOS

BIOS Setup

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

Users may need to run the Setup program when:

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

Important

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

Entering Setup

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

Press <DEL> or <F2> to enter SETUP

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

Important

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

Control Keys

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

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

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

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

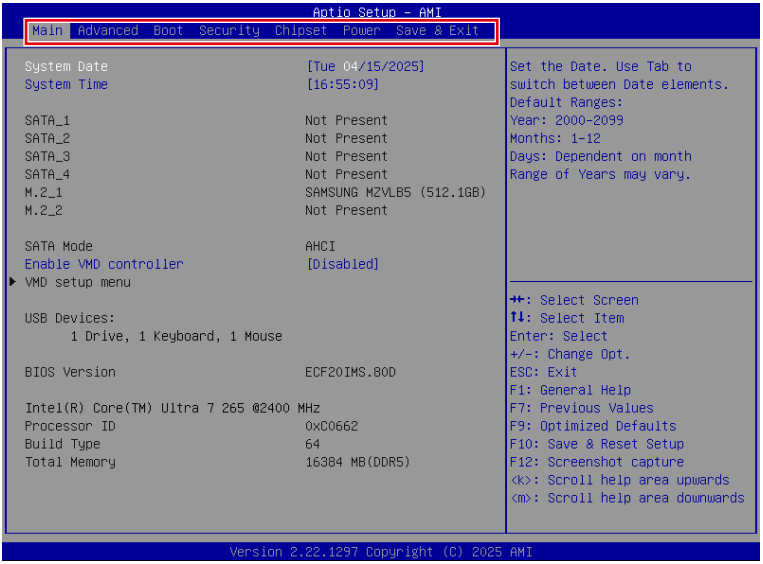
Sub-Menu

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

General Help <F1>

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

The Menu Bar



- **Main**

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

- **Advanced**

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

- **Boot**

  Use this menu to specify the priority of boot devices.

- **Security**

  Use this menu to set supervisor and user passwords.

- **Chipset**

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

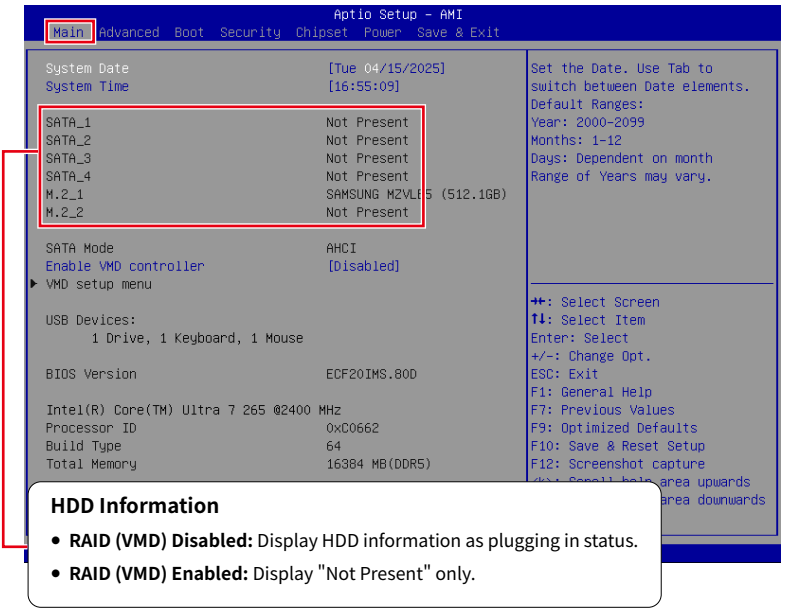
- **Power**

  Use this menu to specify your settings for power management.

- **Save & Exit**

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

Main



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

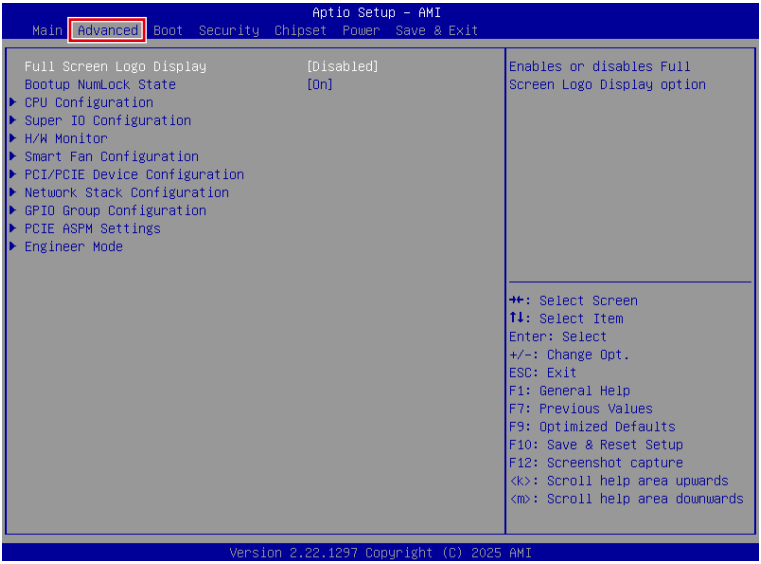
This setting allows you to set the system time.

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

► Enable VMD controler

Enables or disables VMD (RAID) controler.

Advanced



► Full Screen Logo Display

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

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

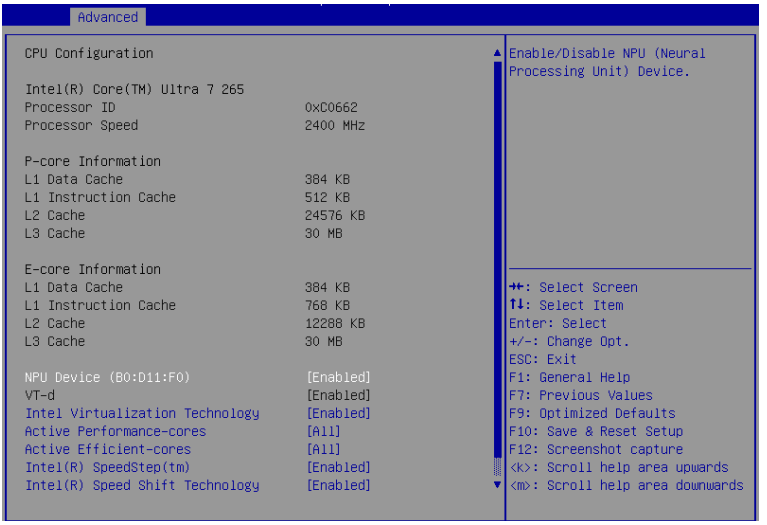
Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

► Bootup NumLock State

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

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

► CPU Configuration



▸ NPU Device

Enables or disables the Neural Processing Unit (NPU) for AI workload acceleration.

▸ VT-d

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

▸ Intel Virtualization Technology

Enables or disables Intel Virtualization technology.

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

[Disabled] Disables this function.

▸ 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.

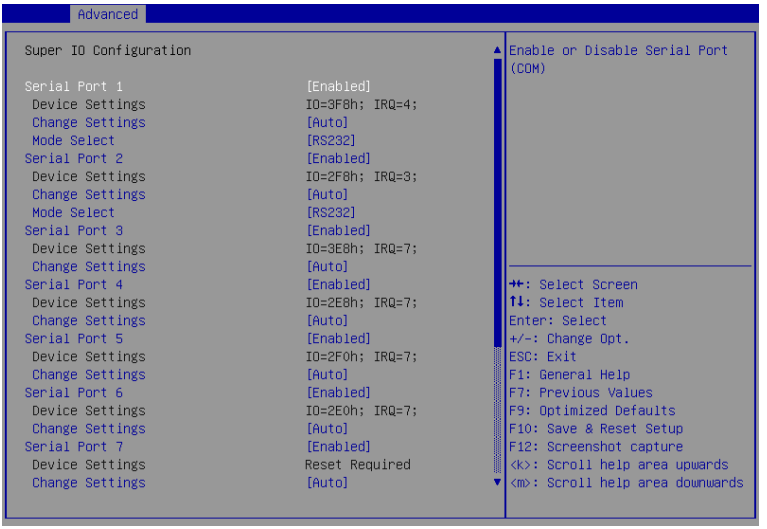
▸ **Intel(R) Speed Shift Technology**

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.

► Super IO Configuration



▸ Serial Port 1/ 2/ 3/ 4/ 5/ 6/ 7/ 8/ 9/ 10, Parallel Port

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/ 5/ 6, Parallel Port.

▸ FIFO Mode

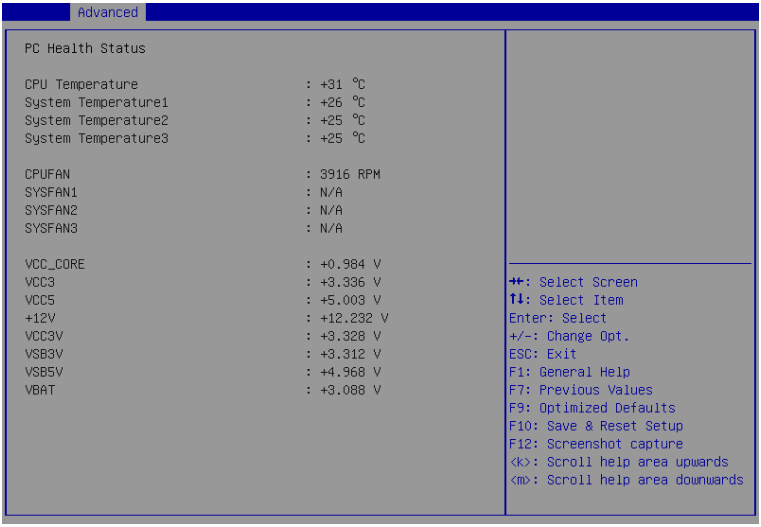
This setting controls the FIFO (First In First Out) data transfer mode.

▸ Watch Dog Timer

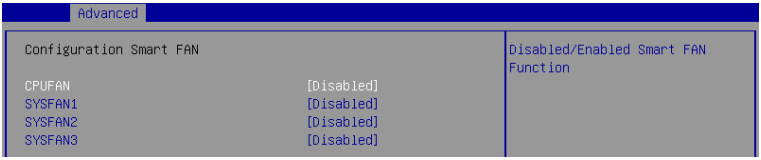
You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

► H/W Monitor (PC Health Status)

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



► Smart Fan Configuration



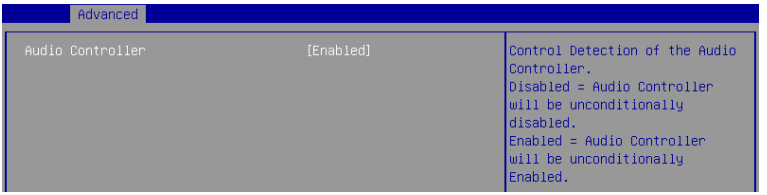
▸ CPUFAN/ SYSFAN1~3

This setting enables or disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the CPU/system fan speed automatically depending on the current CPU/system temperature, avoiding the overheating to damage your system. The following item will display when CPUFAN/ SYSFAN1~3 is enabled.

» **Min. Speed (%)**

The beginning speed of the System fan.

► PCI/PCIE Device Configuration

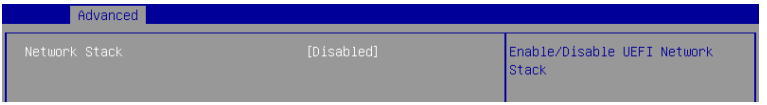


▸ Audio Controller

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

► Network Stack Configuration

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



▸ Network Stack

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

» **IPv4 PXE Support**

Enables or disables IPv4 PXE boot support.

» **IPv4 HTTP Support**

Enables or disables IPv4 HTTP Support.

» **IPv6 PXE Support**

Enables or disables IPv6 PXE Support.

» **IPv6 HTTP Support**

Enables or disables IPv6 HTTP Support.

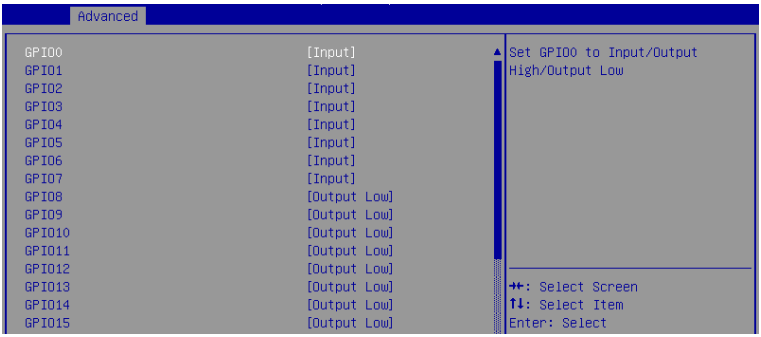
» **PXE boot wait time**

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

» **Media detect count**

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

► GPIO Group Configuration

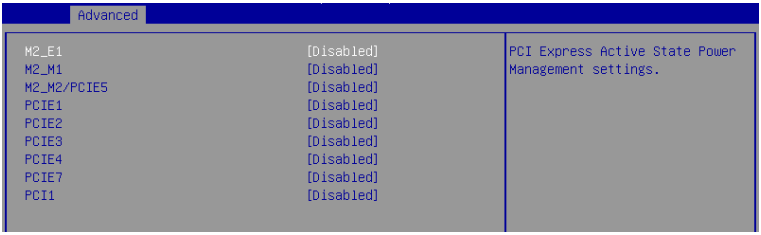


▸ GPIO0 ~ GPO15

These settings control the operation mode of the specified GPIO.

► PCIE ASPM settings

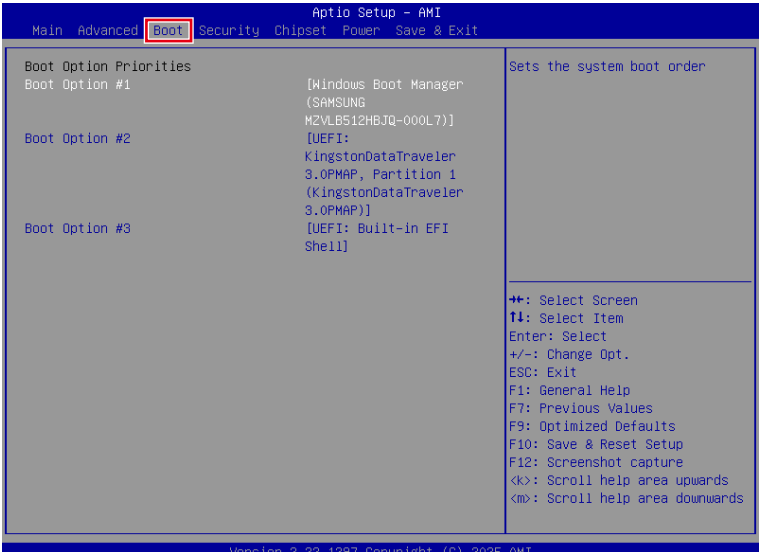
This menu provide settings for PCIe ASPM (Active State Power Management) level for different installed devices.



▸ M2_E1, M2_M1, / M2_M2/PCIE5, PCIE1~4, 7, PCI1

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

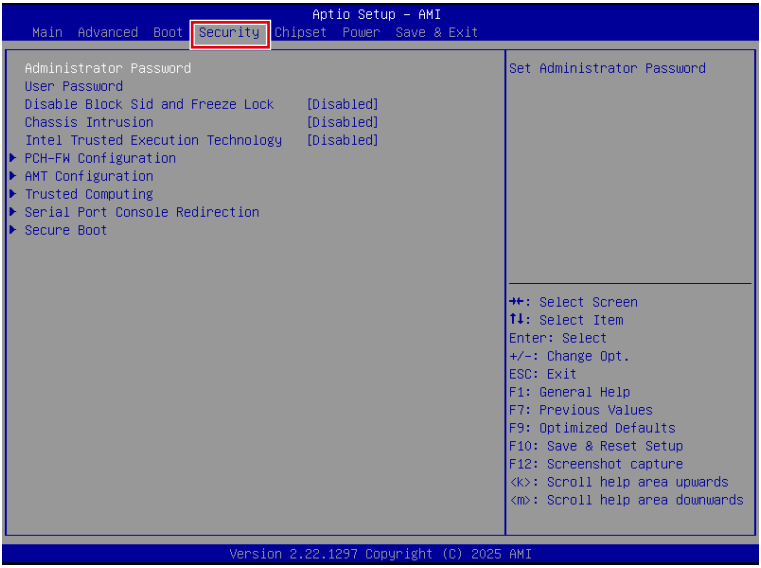
Boot



► **Boot Option #1-3**

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

Security



► Administrator Password

Administrator Password controls access to the BIOS Setup utility.

► User Password

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

► Disable Block Sid and Freeze Lock

Enables access to the System ID (SID) and disables BIOS flash region protection after boot. This setting allows system maintenance, diagnostics, and firmware updates but may lower system security.

► 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**

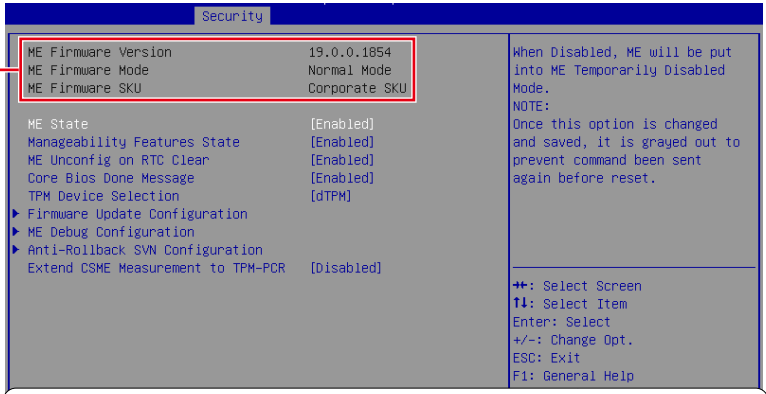
Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware-based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

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

► PCH-FW Configuration

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



ME Firmware Version ME Firmware Mode ME Firmware SKU	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.

▸ Core BIOS Done Message

Enables or disables Core BIOS Done Message sent to ME.

▸ 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.**

▸ **Firmware Update Configuration**



» **ME FW Image Re-Flash**

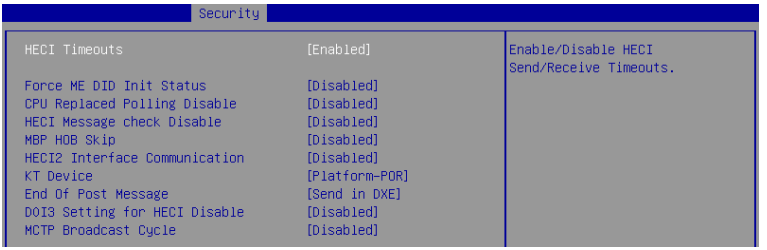
Enables or disables the ME Firmware Image Re-flashing.

» **FW Update**

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

▸ **ME Debug Configuration**

This menu allows you to configure debug-related options for the Intel® Management Engine (ME).



» **HECI Timeouts**

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

» **Force ME DID Init Status**

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

» **CPU Replaced Polling Disable**

Setting this option disables the CPU replacement polling loop.

» **HECI Message Check Disable**

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

» **MBP HOB Skip**

Setting this option will skip ME' s Memory-Based Protection (MBP) H0B region.

» **HECI2 Interface Communication**

This setting Adds/ Removes HECI2 device from PCI space.

» **KT Device**

Enables or disables Key Transfer (KT) Device.

» **End of Post Message**

Enables or disables End of Post Message sent to ME.

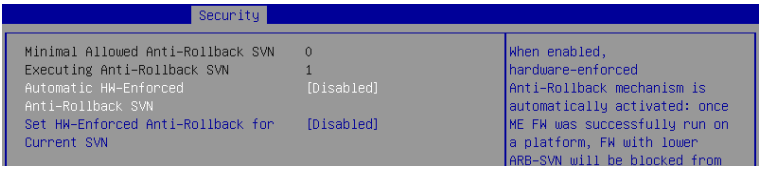
» **DOI3 Setting for HECI Disable**

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

» **MCTP Broadcast Cycle**

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

▸ **Anti-Rollback SVN Configuration**



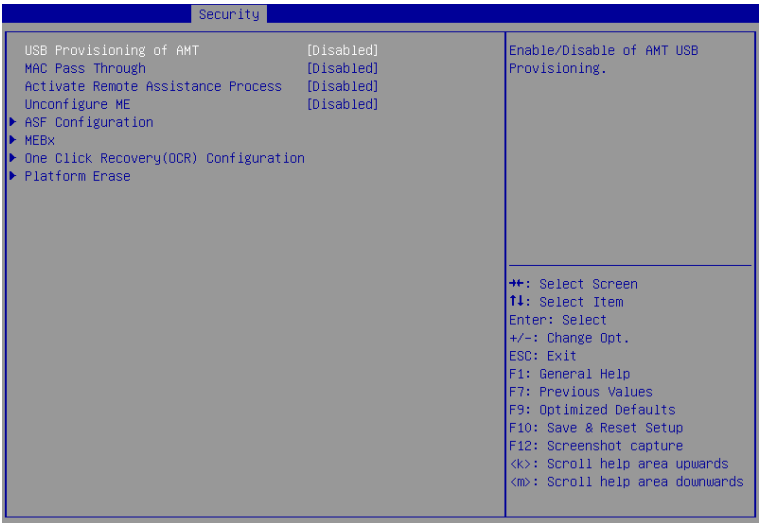
» **Automatic HW-Enforced Anti-Rollback SVN**

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

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

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

► AMT Configuration



▸ USB Provisioning of AMT

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

▸ Mac PASS Through

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

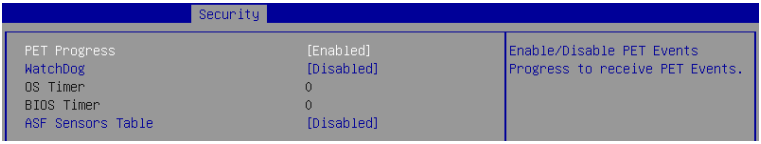
▸ Activate Remote Assistance Process

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

▸ Unconfigure ME

Enables or disables the Unconfigure ME.

▸ ASF Configuration



» **PET Progress**

Enables or disable the this item to receive PET Events.

» **WatchDog**

Enables or disable the watchdog timer.

» **OS Timer**

This item displays OS Timer.

» **BIOS Timer**

This item displays BIOS Timer.

» **ASF Sensor Table**

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

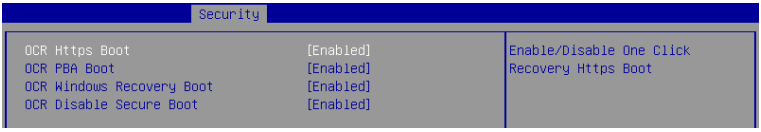
▸ MEBx



» **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.

▸ One Click Recovery (OCR) Configuration



» **OCR Https Boot**

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

» **OCR PBA Boot**

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

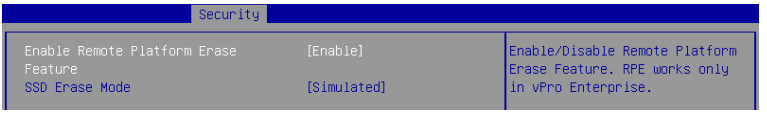
» **OCR Windows Recovery Boot**

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

» **OCR Disable Secure Boot**

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

▸ Platform Erase



» **Enable Remote Platform Erase Feature**

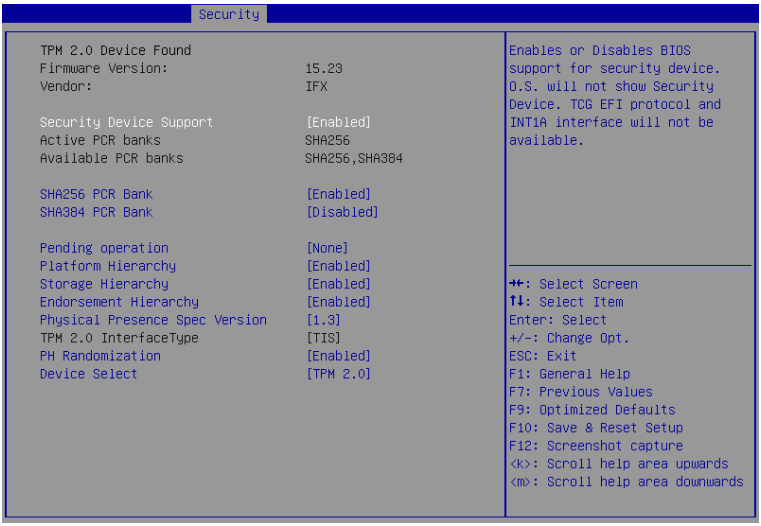
Enables or disables the ability to initiate the remote erasure process for the system or selected storage devices.

» **SSD Erase Mode**

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

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

► Trusted Computing



▸ Security Device Support

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

▸ SHA256, 384 PCR Bank

These settings enables or disables the SHA-1 PCR Bank and SHA256, 384 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 InterfaceType

This setting shows the TPM 2.0 Interface Type.

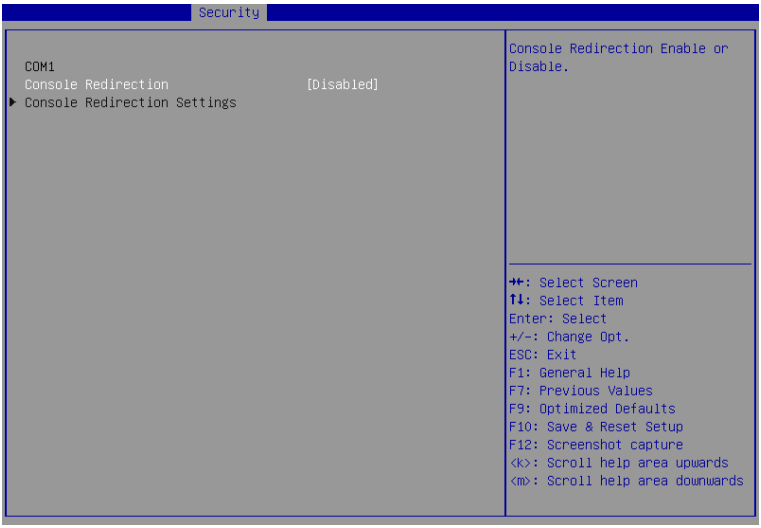
▸ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

▸ Device Select

Select your TPM device through this setting.

► Serial Port Console Redirection



▸ Console Redirection

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

▸ Console Redirection Settings (COM1)

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

» **Terminal Type**

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

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

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

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

» **Flow Control**

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

» **VT-UTF8 Combo Key Support**

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

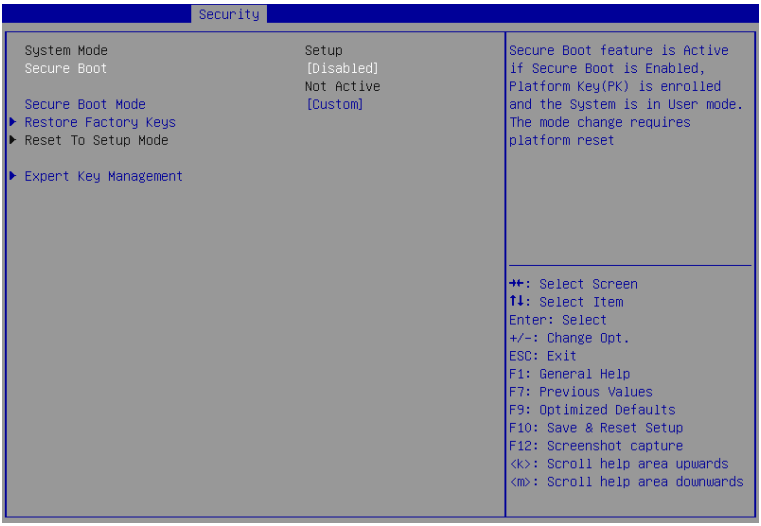
» **Recorder Mode, Resolution 100x31**

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

» **Putty KeyPad**

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

► Secure Boot



▸ Secure Boot

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

▸ Secure Boot Mode

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

[Standard]	The system will automatically load the secure keys from BIOS.
[Custom]	Allows user to configure the secure boot settings and manually load the secure keys.

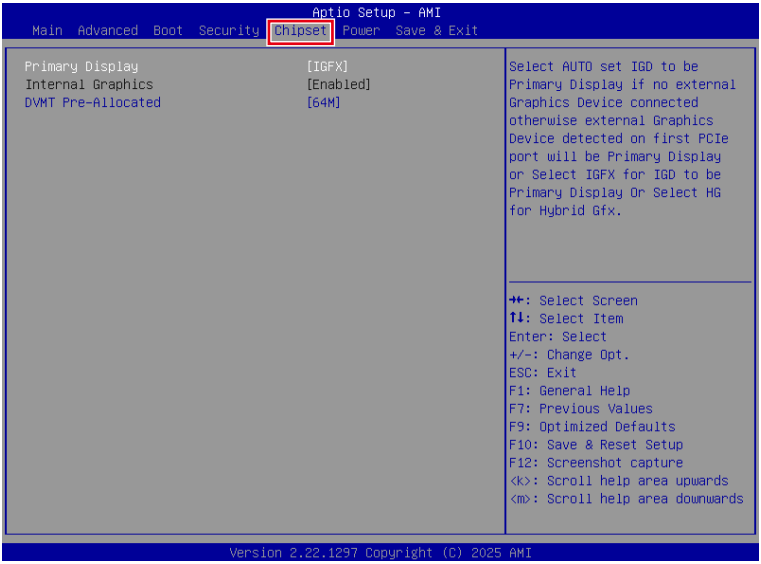
▸ Restore Factory Keys

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

▸ Reset to Setup Mode

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

Chipset



► Primary Display

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

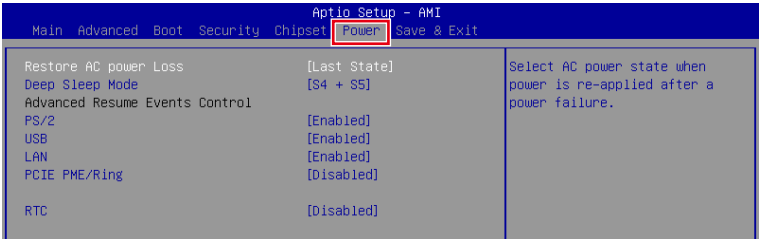
► Internal Graphics

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

► DVMT Pre-Allovated

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

Power



► Restore AC Power Loss

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

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

► Deep Sleep Mode

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

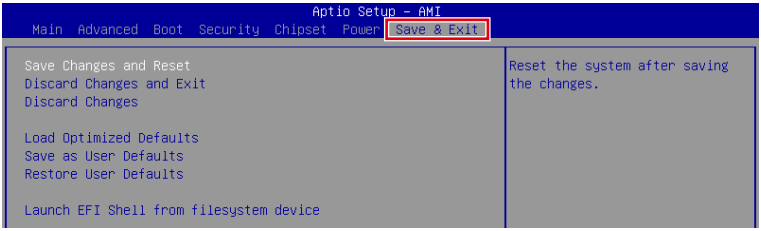
► PS/2, USB, LAN, PCIE PME/Ring

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

► RTC

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

Save & Exit



- **Save Changes and Reset**

  Save changes to CMOS and reset the system.

- **Discard Changes and Exit**

  Abandon all changes and exit the Setup Utility.

- **Discard Changes**

  Abandon all changes.

- **Load Optimized Defaults**

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

- **Save as User Defaults**

  Save changes as the user' s default profile.

- **Restore User Defaults**

  Restore the user' s default profile.

- **Launch EFI Shell from filesystem device**

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

GPIO WDT SMBus Programming

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) and SMBus Access.

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	Direction Port	Output Setting Port	Input Value Port	Bit Address
GPIO0	0x10	0x11	0x12	0
GPIO1	0x10	0x11	0x12	1
GPIO2	0x10	0x11	0x12	2
GPIO3	0x40	0x41	0x42	3
GPIO4	0x10	0x11	0x12	4
GPIO5	0x10	0x11	0x12	5
GPIO6	0x10	0x11	0x12	6
GPIO7	0x10	0x11	0x12	7
GPIO8	0x20	0x21	0x22	0
GPIO9	0x20	0x21	0x22	1
GPIO10	0x20	0x21	0x22	2
GPIO11	0x20	0x21	0x22	3
GPIO12	0x20	0x21	0x22	4
GPIO13	0x20	0x21	0x22	5
GPIO14	0x20	0x21	0x22	6
GPIO15	0x20	0x21	0x22	7

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

1.1 Set GPIO Mode (Input or Output):

1. Read the value from Direction port.
2. Set the GPIO address value.
   Use 1 for output mode or 0 for input mode.
3. Write the value back to Direction port.

Example: Set **GPIO3** to Input mode

```
val =SMBus_ReadByte (0x6E, 0x40);   // Read value from GPIO3 direction port through SMBus.
val = val | (0<<3);                 // Set GPIO3 address (bit 3) to 0 (input mode).
SMBus_WriteByte (0x6E, 0x40, val);  // Write back to GPIO9 direction port through SMBus.
```

Example: Set **GPIO9** to Output mode

```
val =SMBus_ReadByte (0x6E, 0x20);  // Read value from GPIO9 direction port through SMBus.
val = val | (1<<1);                // Set GPIO9 address (bit 1) to 1 (output mode).
SMBus_WriteByte (0x6E, 0x20, val); // Write back to GPIO9 direction port through SMBus.
```

1.2 Set output value of GPIO:

1. Read the value from Output Setting port.
2. Set the value of GPIO address.
3. Write the value back to Output Setting port.

Example: Set **GPIO10** output "high"

```
val =SMBus_ReadByte (0x6E, 0x21);  // Read value from GPIO10 Output Setting port through SMBus.
val = val | (1<<2);                // Set GPIO10 address (bit 2) to 1 (output "high").
SMBus_WriteByte (0x6E, 0x21, val); // Write back to GPIO10 Output Setting port through SMBus.
```

Example: Set **GPIO11** output "low"

```
val = SMBus_ReadByte (0x6E, 0x21); // Read value from GPIO11 Output Setting port through SMBus.
val = val & (~(1<<3));             // Set GPIO11 address (bit 3) to 0 (output "low").
SMBus_WriteByte (0x6E, 0x21, val); // Write back to GPO11 Output Setting port through SMBus.
```

1.3 Read input value from GPIO:

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

Example: Get **GPIO2** input value.

```
val = SMBus_ReadByte (0x6E, 0x12); // Read value from GPIO2 port through SMBus.
val = val & (1<<2);                // Read GPIO2 address (bit 2).
if (val)    printf ("Input of  GPIO2  is High");
else        printf ("Input of  GPIO2  is Low");
```

Example: Get **GPIO3** input value.

```
val = SMBus_ReadByte (0x6E, 0x42); // Read value from GPIO3 port through SMBus.
val = val & (1<<3);                // Read GPIO3 address (bit 3).
if (val)    printf ("Input of  GPIO3  is High");
else        printf ("Input of  GPIO3  is Low");
```

Watchdog Timer

2. Watchdog Timer – WDT

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

2.1 Set WDT Time Unit

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

2.2 Set WDT Time

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

2.3 Enable WDT

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

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

2.4 Disable WDT

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

2.5 Check WDT Reset Flag

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

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

2.6 Clear WDT Reset Flag

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

SMBus Access

3. SMBus Access

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

```
#define IO_SC               0xCF8
#define IO_DA               0xCFC
#define PCIBASEADDRESS      0x80000000
#define PCI_BUS_NUM         0x80
#define PCI_DEV_NUM         31
#define PCI_FUN_NUM             4
```

3.1 Get SMBus Base Address

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

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

3.2 SMBus_ReadByte (char DEVID, char offset)

Read the value of OFFSET from SMBus device DEVID.

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

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

Write DATA to OFFSET on SMBus device DEVID.

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