msi®

MS-CF19

Industrial Computer Board

User Guide

Contents

Regulatory Notices....4

Safety Information....7

Specifications....9

Motherboard Overview....11

Rear I/O Panel....12

- DisplayPort....12
- USB 10Gbps Port....12
- 2.5 GbE RJ-45 LAN Jack....12
- 1.0 GbE RJ-45 LAN Jack....12
- DC-In Power Connector....12

ME Overview....13

- Board Dimensions....13

Memory....15

- DIMM1~2: DDR5 SO DIMM Slots....15

Storage....16

- SATA1: SATA 3.0 6Gb/s Port....16
- M2_M1: M.2 Slot (M Key, 2280)....17

Power Connector....18

- SATAPWR1: SATA Power Connector....18

Graphics Connectors....19

- JINV1: LVDS Inverter Header....19
- JLVDS1_EDP1~2: LVDS + eDP Wafer Connectors....19

Expansion Slots....21

- M2_E1: M.2 Slot (E Key, 2230)....21
- M2_B1: M.2 Slot (B Key, 2242, 3042)....21

Revision

V1.0, 2025/12

Other Connectors....22
SYSFAN1: 4-pin PWM System Fan Connector.... 22
JAUD2: Audio/ Amplifier/ SMBus Connector 23
JUSB1~2: USB 2.0 Headers.... 24
JFP1: Front Panel Connector.... 25
JGPIO1: GPIO (DIO) Header 25
JCOM1: COM Port Box Header (RS232/ 422/ 485).... 26
JRTC1: CMOS Battery.... 27
Jumpers....28
BIOS Setup....29
Entering Setup 29
Control Keys.... 30
Getting Help 30
Main Menu.... 30
Sub-Menu 30
General Help <F1>.... 30
The Menu Bar 31
Main....32
Advanced 33
Boot....40
Security 41
Chipset 53
Power 54
Save & Exit....56
GPIO WDT Programming....57
Abstract 57
General Purpose IO.... 58
Watchdog Timer.... 60

Regulatory Notices

CE Conformity

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

FCC-B Radio Frequency Interference Statement

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

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

Notice 1

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

Notice 2

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

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

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

WEEE Statement

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.

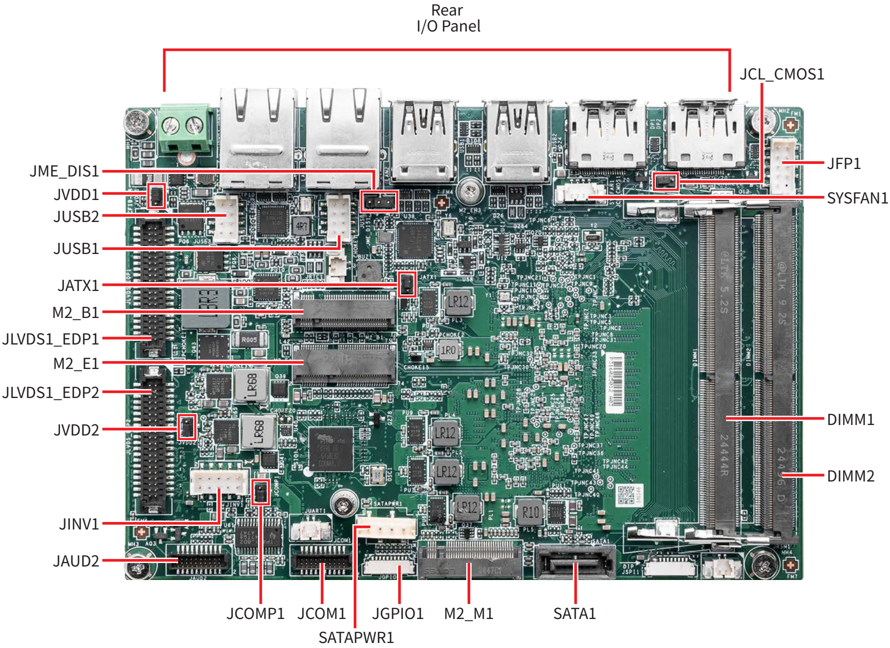
Specifications

Model	MS-CF19
Dimensions	146(L)mm x 102(W)mm x 40(H)mm, 3.5 inch (include heatsink)
Processor	● 15th Gen Intel® Arrow Lake-U Series ● 14th Gen Meteor Lake-U Series
Chipset	Within processor
iAMT Support	● AMT 17.x (Only for Intel® i7/ i5 CPU series)
Memory	● 2 x DDR5 SO-DIMM slot (262-pins) ● Dual-Channel for DDR5, Non-ECC ● Up to 6400 MT/s (Arrow Lake-U) ● Up to 5600 MT/s (Meteor Lake-U) ● Up to 96GB
Network	● 1 x Intel® I219LM 1.0 GbE LAN ● 1 x Intel® I226-V 2.5 GbE LAN
Storage	● 1 x SATA 3.0 6Gb/s port ● 1 x M.2 M Key slot (2280) ● Supports PCIe 4.0 x4 signal ● Supports NVMe devices
Expansion Slots	● 1 x M.2 E Key slot (2230) ● Supports PCIe x1 & USB 2.0 signals ● Supports CNVi modules ● Support Intel® Wi-Fi 6E AX210, AX211 (CNVi), and Intel® Wi-Fi 7 BE200 ● 1 x M.2 B Key slot (2242/ 3042) ● Supports PCIe x1/ SATA 3.0 & USB 2.0 signals
Audio	● Realtek® ALC897 High Definition Audio Codec
Graphics	● 2 x DisplayPort 1.4a, up to 4096×2304 @ 60Hz ● 2 x LVDS up to 1920x1200 @60Hz (signals share with eDP) ● Supports 18/24-bit dual channel ● Supports auto switch between eDP & LVDS ● Connector shared with eDP ● 2 x eDP up to 4096×2304 @60 Hz (signal shares with LVDS) ● Supports auto switch between eDP & LVDS ● Connector shared with LVDS ● Supports 4 independent display modes ● eDP/LVDS1 + eDP/LVDS2 + DP1 + DP2

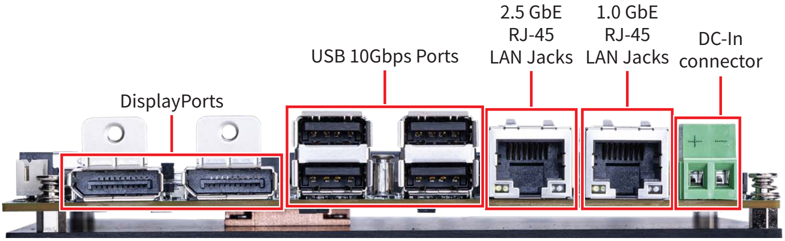
Continued on next column

Model	MS-CF19
Rear I/O	• 2 x DisplayPort (1.4a) • 4 x USB 10Gbps Type-A connectors (5V/1A) • 1 x RJ-45 2.5 Gbps LAN port • 1 x RJ-45 1.0 Gbps LAN port
USB	2 x USB 2.0 header (480 Mbps, for 4 USB ports, 5V/0.5A Each Port)
Power Connector	1 x DC-In power connector (12~24V)
Onboard Connectors	• 1 x SATA power connector • 1 x LVDS inverter header • 2 x LVDS + eDP wafer connector • 1 x 4-pin PWM system fan connector • 1 x audio/ amplifier/ SMbus connector • 1 x front panel connector • 1 x GPIO (DIO) header (8-bit, 4 x GPI, 4 x GPO) • 1 x COM (serial) port header • 1 x battery header
Jumpers	• 1 x Clear CMOS jumper • 1 x ME jumper • 1 x COM voltage select jumpers • 2 x eDP/LVDS VDD power select jumper • 1 x AT/ ATX mode select jumper
OS Support	• Windows 10 IoT Enterprise 21H2 LTSC (64-Bit) • Windows 11 IoT Enterprise 24H2 LTSC (64-Bit) • Linux (support by request)
Regulatory Compliance	CE, FCC Class B, BSMI, RCM, VCCI, UKCA, IC, IEC 62368: CE (LVD) Compliant
Environment	• Operating Temperature: -10 ~ 60°C • Thermal w/ Airflow: 0.7m/s • Storage Temperature: -20 ~ 80°C • Humidity: 10 ~ 90%, non-condensing

Motherboard Overview



Rear I/O Panel



DisplayPort

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

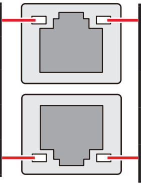
USB 10Gbps Port

This connector delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.It supports data transfer rates up to 10 Gbps.

2.5 GbE RJ-45 LAN Jack

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

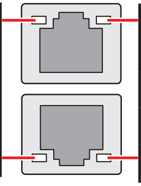
Link/ Activity LED	
Status	Description
○ Off	No link
🟡 Yellow	Linked
◐ Blinking	Data activity



○ Off	10/100 Mbps
🟢 Green	1000 Mbps
🟠 Orange	2.5 Gbps

1.0 GbE RJ-45 LAN Jack

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



○ Off	10 Mbps
🟢 Green	100 Mbps
🟠 Orange	1.0 Gbps

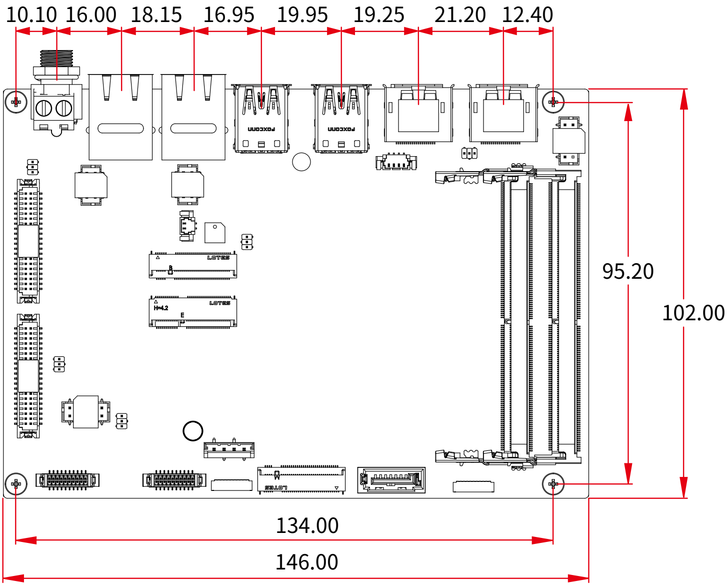
DC-In Power Connector

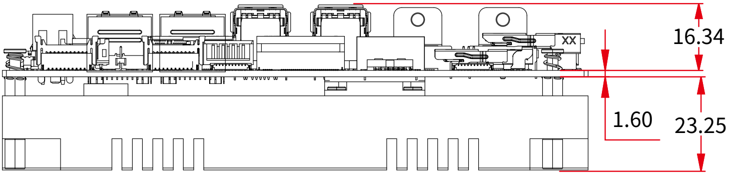
This connector supplies power to the system.

ME Overview

Board Dimensions

Unit of measurement: mm





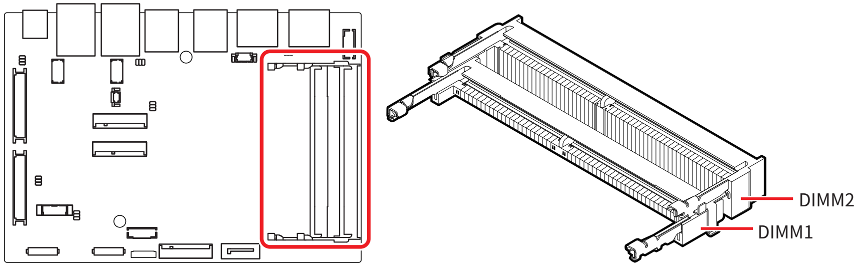
Component Contents

Component	Page
Memory	**15**
DIMM1~2: DDR5 SO DIMM Slots	15
Storage	**16**
SATA1: SATA 3.0 6Gb/s Port	16
M2_M1: M.2 Slot (M Key, 2280)	17
Power Connector	**18**
SATAPWR1: SATA Power Connector	18
Graphics Connectors	**19**
JINV1: LVDS Inverter Header	19
JLVDS1_EDP1~2: LVDS + eDP Wafer Connectors	19
Expansion Slots	**21**
M2_E1: M.2 Slot (E Key, 2230)	21
M2_B1: M.2 Slot (B Key, 2242, 3042)	21
Other Connectors	**22**
SYSFAN1: 4-pin PWM System Fan Connector	22
JAUD2: Audio/ Amplifier/ SMBus Connector	23
JUSB1~2: USB 2.0 Headers	24
JFP1: Front Panel Connector	25
JGPIO1: GPIO (DIO) Header	25
JCOM1: COM Port Box Header (RS232/ 422/ 485)	26
JBAT1: CMOS Battery	27
Jumpers	**28**

Memory

DIMM1~2: DDR5 SO DIMM Slots

The DIMM slot is intended for memory modules.



Installing DDR5 SO DIMM Memory Module

1. Locate the SO-DIMM slot. Align the notch on the DIMM with the key on the slot and insert the DIMM into the slot.
2. Push the DIMM gently downwards until the slot levers click and lock the DIMM in place.

- *To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.*

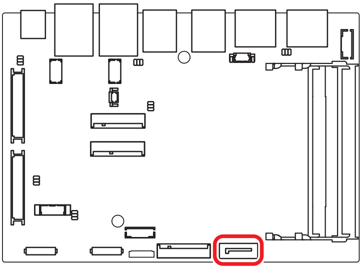
Important

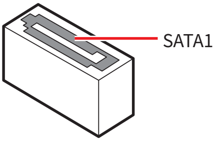
- *Always insert memory modules in the **DIMM2** slot first.*
- *You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.*
- *To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.*

Storage

SATA1: SATA 3.0 6Gb/s Port

The connector is a SATA 6Gb/s interface port, and can connect to one SATA device.



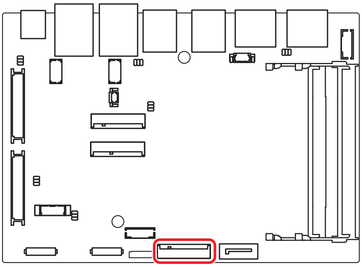


Important

- *The SATA connector 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, 2280)

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



Features

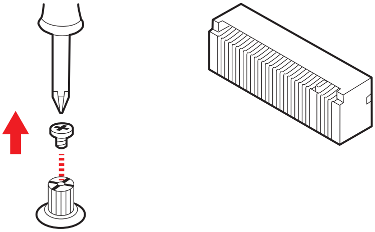
- Supports PCIe 4.0 x4 signal
- Supports NVMe devices

Video Demonstration

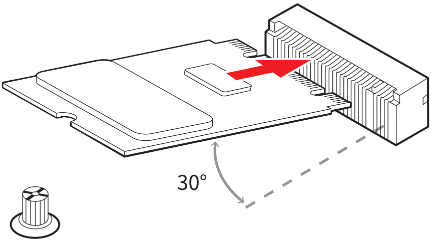
Watch the video to learn how to Install M.2 SSD.

Installing M.2 SSD

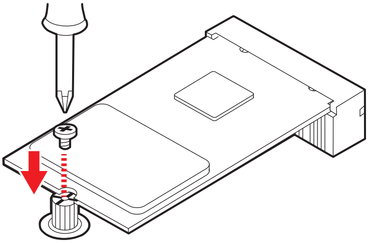
1. Loosen the M.2 screw from the motherboard.



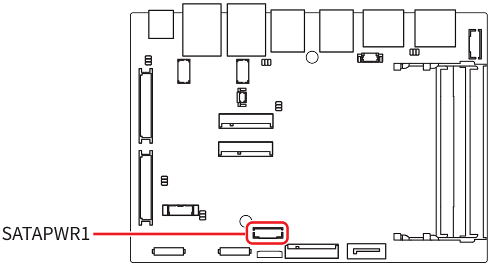
2. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



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

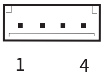


Power Connector



SATAPWR1: SATA Power Connector

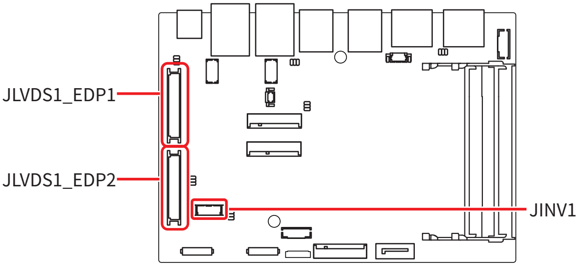
This connector is used to provide power to SATA devices.

SATAPWR1 	1	VCC5	2	GND
	3	GND	4	+12V

Important

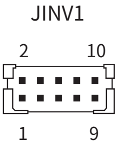
Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Graphics Connectors



JINV1: LVDS Inverter Header

The connector is provided for LCD backlight options.

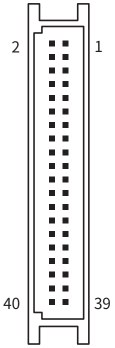
	1	GND	2	GND
	3	VCC5	4	VCC5
	5	+12V	6	+12V
	7	INV_ON1_1	8	INV_ON1_2
	9	L_BKLT_CTRL#1_1	10	L_BKLT_CTRL#1_2

JLVDS1_EDP1~2: LVDS + eDP Wafer Connectors

These connectors are provided for LVDS/eDP interface flat panels. After connecting an LVDS/eDP interface flat panel to the connector, be sure to check the panel datasheet and set the JVDD1 LVDS jumper to proper power voltage.

Important

Please refer to the following pages for the pin-out of the LVDS + eDP Wafter Connector and the pin-out for LVDS/eDP interface flat panels.

eDP Panel (P1)	CF17 Motherboard (P2)				eDP Panel (P1)
	JLVDS1_EDP1				
Lane3_P	EDP_1_LINE3_DP	1	2	EDP_1_LINE2_DP	Lane2_P
Lane3_N	EDP_1_LINE3_DN	3	4	EDP_1_LINE2_DN	Lane2_N
	DDC0_CLK_7513_R_1	5	6	DDC0_DATA_7513_R_1	
LCD_VCC	LCD_VDD_1	7	8	LCD_VDD_1	LCD_VCC
LCD_VCC	LCD_VDD_1	9	10	VCC3	
	LCDEN_1	11	12	LVDS_DETECT#_C_1	LCD_GND
Lane1_P	LVDSA_DATA1_1	13	14	LVDSA_DATA0_1	HPD
Lane1_N	LVDSA_DATA#1_1	15	16	LVDSA_DATA#0_1	
H_GND	GND	17	18	GND	H_GND
	LVDSA_DATA3_1	19	20	LVDSA_DATA2_1	Lane0_P
	LVDSA_DATA#3_1	21	22	LVDSA_DATA#2_1	Lane0_N
H_GND	GND	23	24	GND	H_GND
	LVDSB_DATA1_1	25	26	LVDSB_DATA0_1	
	LVDSB_DATA#1_1	27	28	LVDSB_DATA#0_1	
H_GND	GND	29	30	GND	GND
	LVDSB_DATA3_1	31	32	LVDSB_DATA2_1	
	LVDSB_DATA#3_1	33	34	LVDSB_DATA#2_1	
	CH7513_GPIO5_1	35	36	GND	GND
	LVDSB_CLK_1	37	38	LVDSA_CLK_1	AUX_CH_P
	LVDSB_CLK#_1	39	40	LVDSA_CLK#_1	AUX_CH_N

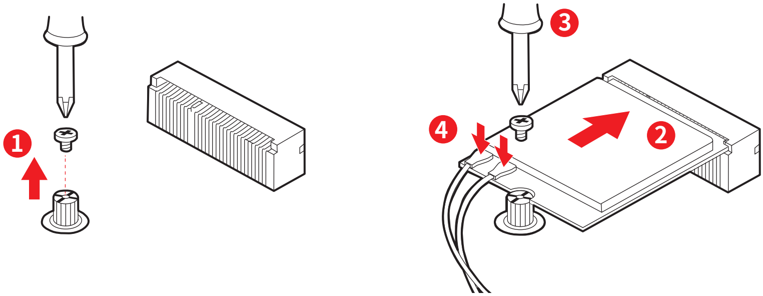
Important

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.

Expansion Slots

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

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

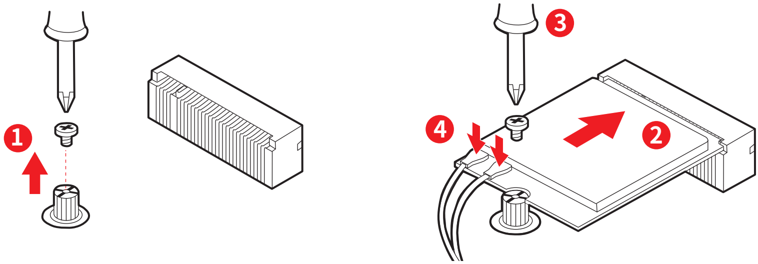


Features

- Supports PCIe x1 & USB 2.0 signals
- Supports CNVi modules

M2_B1: M.2 Slot (B Key, 2242, 3042)

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



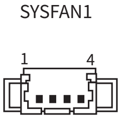
Features

- Supports PCIe x1/ SATA 3.0 & USB 2.0 signals

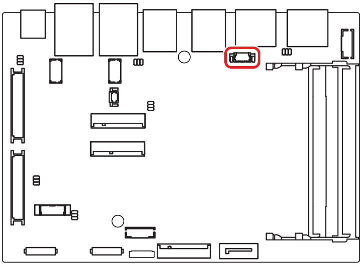
Other Connectors

SYSFAN1: 4-pin PWM System Fan Connector

The fan power connector supports 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. If the motherboard has a System Hardware Monitor chipset onboard, you must use a specially designed fan with speed sensor to take advantage of the fan control.



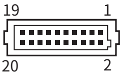
1	GND	2	+12V
3	SYS1_FANTAC	4	SIO_SYS1_FAN



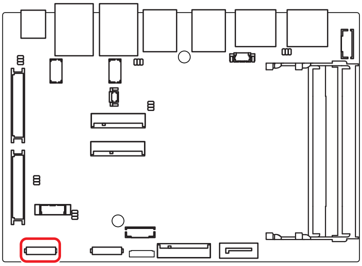
JAUD2: Audio/ Amplifier/ SMBus Connector

This connector allows you to connect audio. It also supports amplifier function to enhance audio performance and SMBus, known as I2C, for connecting System Management Bus (SMBus) interface.

JAUD1

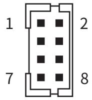


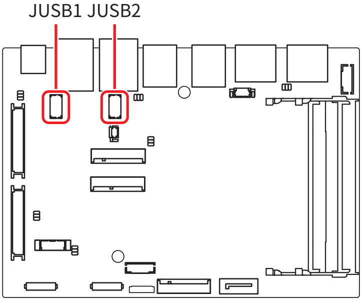
1	LINE_IN_RA	2	MIC1_RA
3	LINE_IN_LA	4	MIC1_LA
5	LINE_OUT_R_F_J	6	MIC1_JD
7	LINE_OUT_L_F_J	8	LINE1_JD
9	FRONT_JD	10	AGND
11	AGND	12	AGND
13	5VSB	14	AMP_L-
15	SMBCLK_MAIN	16	AMP_L+
17	SMBDATA_MAIN	18	AMP_R-
19	GND	20	AMP_R+



JUSB1~2: USB 2.0 Headers

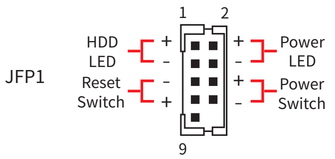
These headers is ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices. It supports data transfer rate up to 480 Mbps.

JUSB1~2		1	5V	2	GND
		3	USB1-	4	USB2+
		5	USB1+	6	USB2-
		7	GND	8	5V



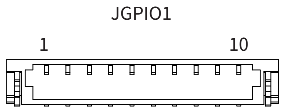
JFP1: Front Panel Connector

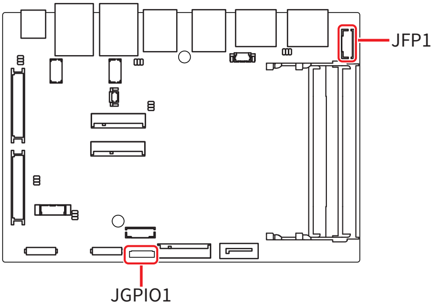
This front-panel header is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.

	1	HDD+	2	Power_LED
	3	HDDLED-	4	SUS_LED
	5	GND	6	PSIN#_R
	7	FP_RST#	8	GND
	9	NC		

JGPIO1: GPIO (DIO) Header

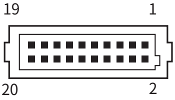
This connector is provided for the General-Purpose Input/Output (GPIO) peripheral module.

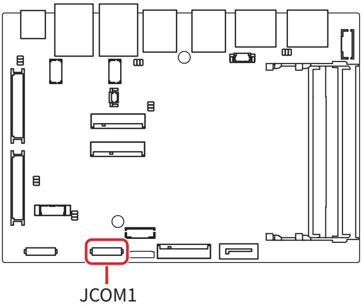
	1	GND	2	VCC5F
	3	N_GPI0	4	N_GPO0
	5	N_GPI1	6	N_GPO1
	7	N_GPI2	8	N_GPO2
	9	N_GPI3	10	N_GPO3



JCOM1: COM Port Box Header (RS232/ 422/ 485)

These headers are 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial device to it.

	RS232			RS422			RS485		
JCOM1  	1	2	DCD	1	2	TXD-	1	2	D-
	3	4	RXD	3	4	TXD+	3	4	D+
	5	6	TXD	5	6	RXD+	5	6	NC
	7	8	DTR	7	8	RXD-	7	8	NC
	9	10	GND	9	10	GND	9	10	GND
	11	12	DSR	11	12	NC	11	12	NC
	13	14	RTS	13	14	NC	13	14	NC
	15	16	CTS	15	16	NC	15	16	NC
	17	18	POWER	17	18	NC	17	18	NC
	19	20	NC	19	20	NC	19	20	NC



Important

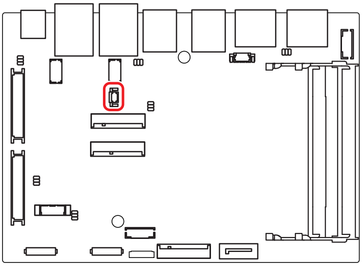
After connect COM port headers to printer, garbage can’ t be printed when power on/ off.

Features

- Support True RS-232
- Support Auto flow control
- RS- 422/ 485 support TR 1000+ Meter
- RS- 232/ 422/ 485, selection by BIOS control

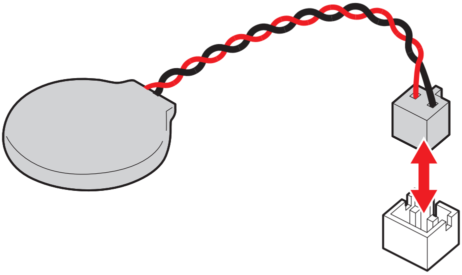
JRTC1: CMOS Battery

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. 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

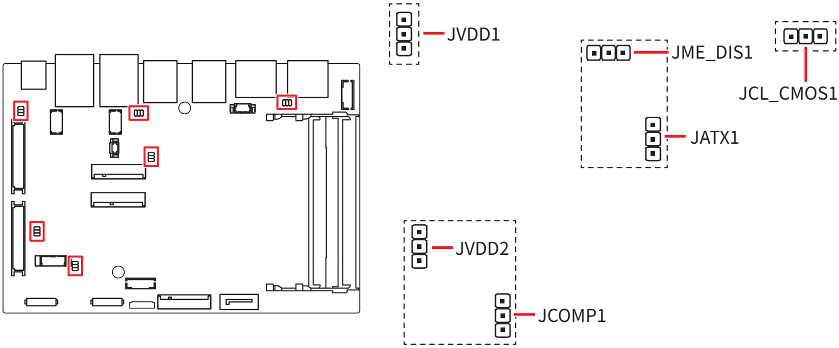
KEEP OUT OF REACH OF CHILDREN

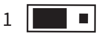
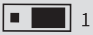
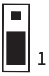
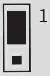
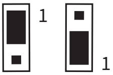
- *Swallowing can lead to chemical burns, perforation of soft tissue, can death.*
- *Severe burns can occur within 2 hours of ingestion.*
- *If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.*

Jumpers

Important

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



Jumper Name	Default Setting	Description
JCL_CMOS1		**Clear CMOS Jumper** 1-2: Normal (Default) 2-3: Clear CMOS
JME_DIS1		**ME Jumper** 1-2: Normal (Default) 2-3: ME disabled
JCOMP1		**COM Voltage Select Jumper** 1-2: 5V Power (Default) 2-3: 12V Power
JATX1		**AT/ ATX Mode Select Jumper** 1-2: ATX (Default) 2-3: AT
JVDD1 JVDD2		**eDP/LVDS VDD Power Select Jumper** 1-2: 3.3 V Power (Default) 2-3: 5V

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
F8	Search setup items
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.

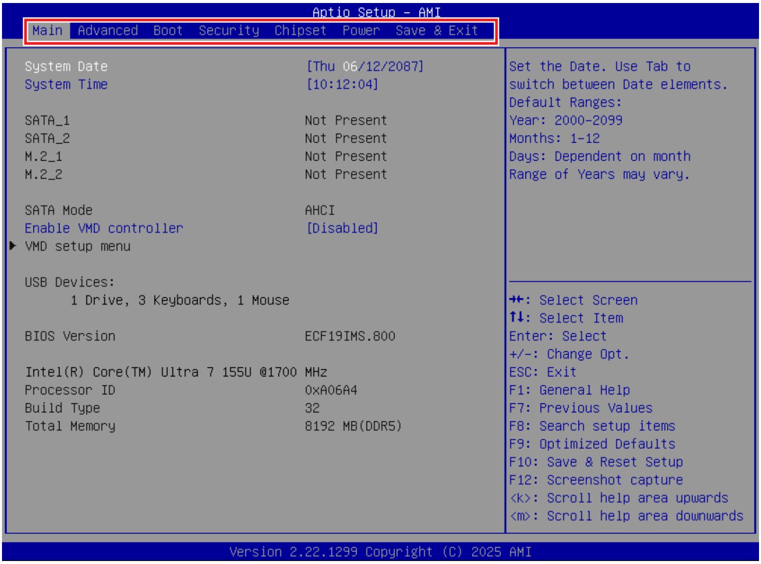
Sub-Menu

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



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

  System Date                     [Thu 06/12/2087]   Set the Date. Use Tab to
  System Time                     [10:12:04]         switch between Date elements.
                                                     Default Ranges:
  SATA_1                          Not Present        Year: 2000-2099
  SATA_2                          Not Present        Months: 1-12
  M.2_1                           Not Present        Days: Dependent on month
  M.2_2                           Not Present        Range of Years may vary.

  SATA Mode                       AHCI
  Enable VMD controller           [Disabled]
▶ VMD setup menu

  USB Devices:                                       ----------------------------------
        1 Drive, 3 Keyboards, 1 Mouse                →←: Select Screen
                                                     ↑↓: Select Item
  BIOS Version                    ECF19IMS.800       Enter: Select
                                                     +/-: Change Opt.
  Intel(R) Core(TM) Ultra 7 155U @1700 MHz           ESC: Exit
  Processor ID                    0xA06A4            F1: General Help
  Build Type                      32                 F7: Previous Values
  Total Memory                    8192 MB(DDR5)      F8: Search setup items
                                                     F9: Optimized Defaults
                                                     F10: Save & Reset Setup
                                                     F12: Screenshot capture
                                                     <k>: Scroll help area upwards
                                                     <m>: Scroll help area downwards

               Version 2.22.1299 Copyright (C) 2025 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 onboard chipsets.

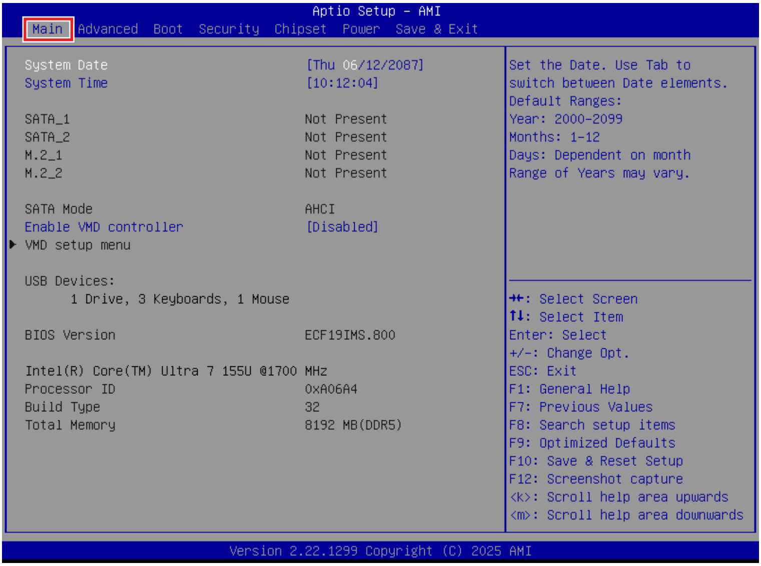
▶ Power

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                          [Thu 06/12/2087]    Set the Date. Use Tab to
  System Time                          [10:12:04]          switch between Date elements.
                                                           Default Ranges:
  SATA_1                               Not Present         Year: 2000-2099
  SATA_2                               Not Present         Months: 1-12
  M.2_1                                Not Present         Days: Dependent on month
  M.2_2                                Not Present         Range of Years may vary.

  SATA Mode                            AHCI
  Enable VMD controller                [Disabled]
► VMD setup menu

  USB Devices:
        1 Drive, 3 Keyboards, 1 Mouse                      →←: Select Screen
                                                           ↑↓: Select Item
  BIOS Version                         ECF19IMS.800        Enter: Select
                                                           +/-: Change Opt.
  Intel(R) Core(TM) Ultra 7 155U @1700 MHz                 ESC: Exit
  Processor ID                         0xA06A4             F1: General Help
  Build Type                           32                  F7: Previous Values
  Total Memory                         8192 MB(DDR5)       F8: Search setup items
                                                           F9: Optimized Defaults
                                                           F10: Save & Reset Setup
                                                           F12: Screenshot capture
                                                           <k>: Scroll help area upwards
                                                           <m>: Scroll help area downwards

                  Version 2.22.1299 Copyright (C) 2025 AMI
```

▶ System Date

This setting allows you to set the system date.

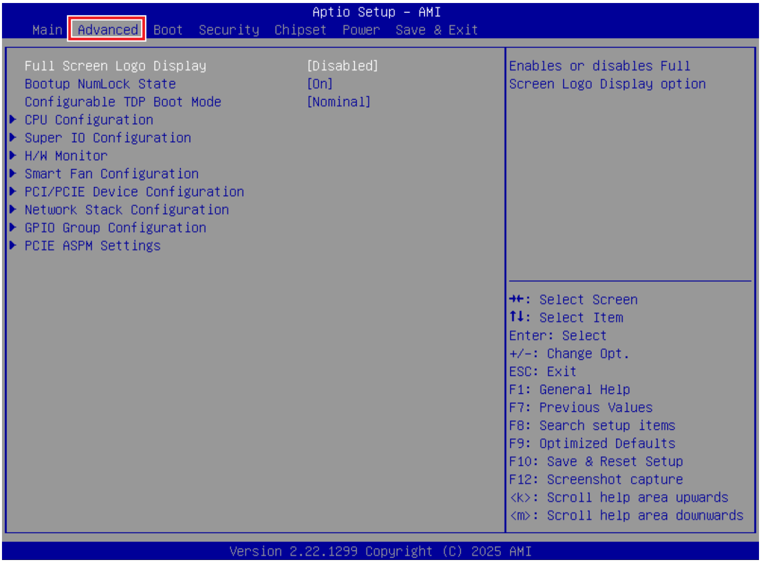
Format: <Day> <Month> <Date> <Year>.

▶ System Time

This setting allows you to set the system time.

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

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
  Configurable TDP Boot Mode          [Nominal]
▶ 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
                                                    F8: Search setup items
                                                    F9: Optimized Defaults
                                                    F10: Save & Reset Setup
                                                    F12: Screenshot capture
                                                    <k>: Scroll help area upwards
                                                    <m>: Scroll help area downwards

              Version 2.22.1299 Copyright (C) 2025 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.Nominal, Down or Up.

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

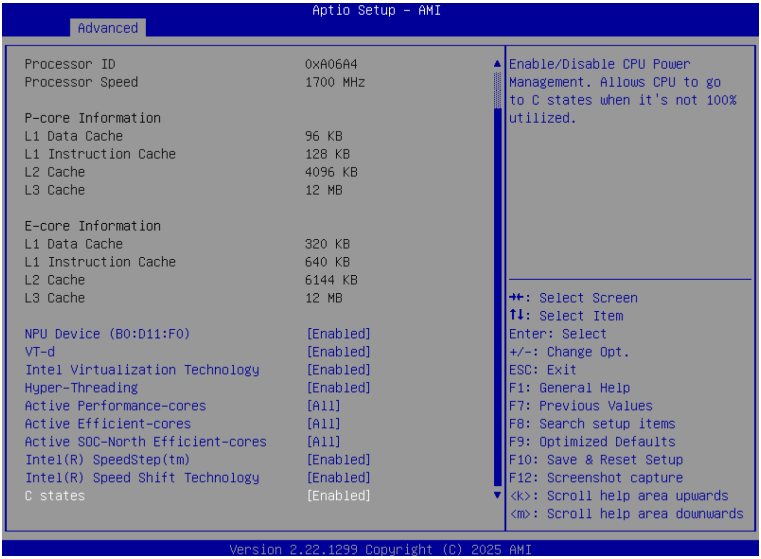
[Off] Allow users to use the arrow keys on the numeric keypad.

▶ Confugurable TDP Boot Mode

This feature allows you sets the TDP (Thermal Design Power) Boot mode to either Nominal, Level1 or Level2.

TDP Power Spec			
Processor Family	Nominal	Level1	Level2
Intel® U/P/N-Series	15W (Default)	12W	28W

CPU Configuration



```
                              Aptio Setup - AMI
         Advanced

  Processor ID                          0xA06A4          ▲ Enable/Disable CPU Power
  Processor Speed                       1700 MHz           Management. Allows CPU to go
                                                           to C states when it's not 100%
  P-core Information                                       utilized.
  L1 Data Cache                         96 KB
  L1 Instruction Cache                  128 KB
  L2 Cache                              4096 KB
  L3 Cache                              12 MB

  E-core Information
  L1 Data Cache                         320 KB
  L1 Instruction Cache                  640 KB
  L2 Cache                              6144 KB
  L3 Cache                              12 MB              →←: Select Screen
                                                           ↑↓: Select Item
  NPU Device (B0:D11:F0)                [Enabled]          Enter: Select
  VT-d                                  [Enabled]          +/-: Change Opt.
  Intel Virtualization Technology       [Enabled]          ESC: Exit
  Hyper-Threading                       [Enabled]          F1: General Help
  Active Performance-cores              [All]              F7: Previous Values
  Active Efficient-cores                [All]              F8: Search setup items
  Active SOC-North Efficient-cores      [All]              F9: Optimized Defaults
  Intel(R) SpeedStep(tm)                [Enabled]          F10: Save & Reset Setup
  Intel(R) Speed Shift Technology       [Enabled]          F12: Screenshot capture
  C states                              [Enabled]        ▼ <k>: Scroll help area upwards
                                                           <m>: Scroll help area downwards

                  Version 2.22.1299 Copyright (C) 2025 AMI
```

NPU Device

Enables or disables NPU (neural processing unit) device.

VT-d

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

Enables or disables Intel® Virtualization technology.

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).

- **Active SOC-North Efficient-cores**

  Select the number of active Low Power Efficient-cores (LP 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.

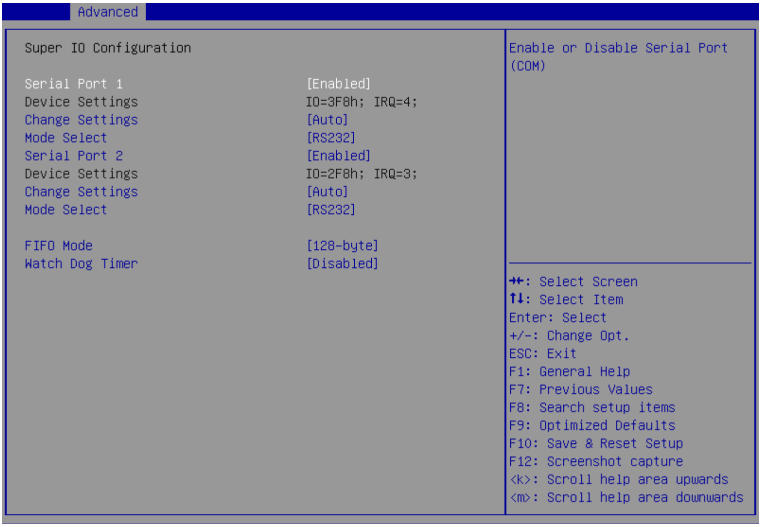
- **C States**

  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]

FIFO Mode                      [128-byte]
Watch Dog Timer                [Disabled]
                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/-: Change Opt.
                                                        ESC: Exit
                                                        F1: General Help
                                                        F7: Previous Values
                                                        F8: Search setup items
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards
```

▸ Serial Port 1/ 2

This setting enables or disables the specified serial port.

» Device Settings

This setting shows the address & IRQ of 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.

▸ FIFO Mode

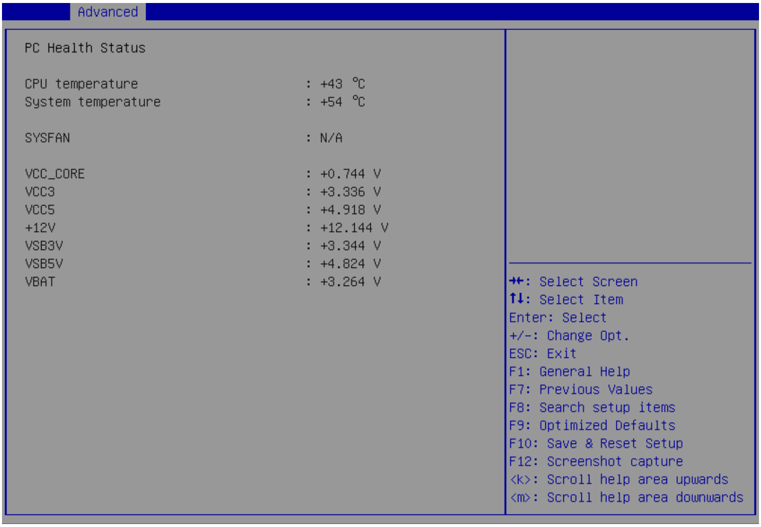
This setting controls the FIFO (First In First Out) data transfer mode.

▸ 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)

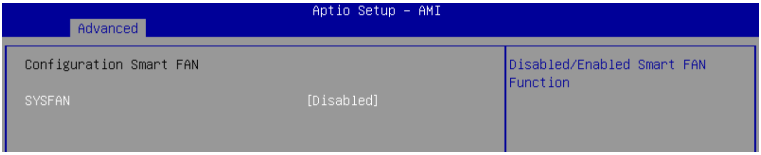
These items display the current status of all monitored hardware devices/ components such as voltages, temperatures and all fans’ speeds.



```
Advanced

PC Health Status

CPU temperature                      : +43 °C
System temperature                   : +54 °C

SYSFAN                               : N/A

VCC_CORE                             : +0.744 V
VCC3                                 : +3.336 V
VCC5                                 : +4.918 V
+12V                                 : +12.144 V
VSB3V                                : +3.344 V
VSB5V                                : +4.824 V
VBAT                                 : +3.264 V
```

```
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
ESC: Exit
F1: General Help
F7: Previous Values
F8: Search setup items
F9: Optimized Defaults
F10: Save & Reset Setup
F12: Screenshot capture
<k>: Scroll help area upwards
<m>: Scroll help area downwards
```

▶ Smart Fan Configuration



```
                         Aptio Setup - AMI
Advanced

Configuration Smart FAN

SYSFAN                               [Disabled]
```

```
Disabled/Enabled Smart FAN
Function
```

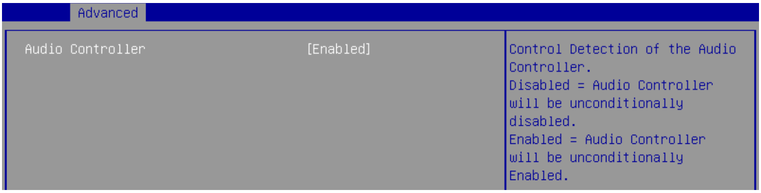
▸ SYSFAN

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 SYSFAN is enabled.

» Min. Speed (%)

The beginning speed of the System fan.

▶ PCI/PCIE Device Configuration



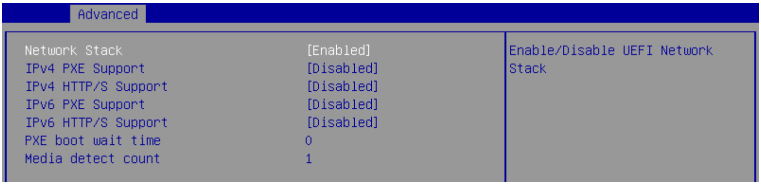
```
Advanced

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/S Support                     [Disabled]
IPv6 PXE Support                        [Disabled]
IPv6 HTTP/S 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 Stack is enabled.

» IPV4 PXE Support

Enables or disables IPv4 PXE boot support.

» IPV4 HTTP/S Support

Enables or disables Ipv4 HTTP/S Support.

» IPV6 PXE Support

Enables or disables Ipv6 PXE Support.

» IPV6 HTTP/S Support

Enables or disables Ipv6 HTTP/S Support.

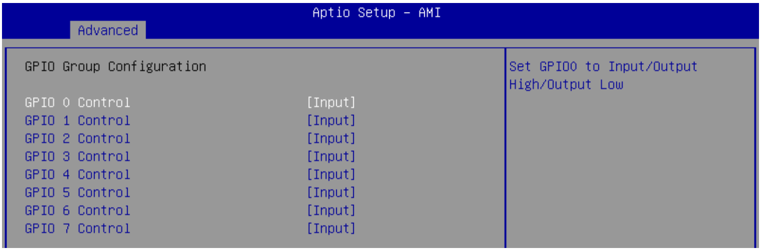
» PXE boot wait time

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



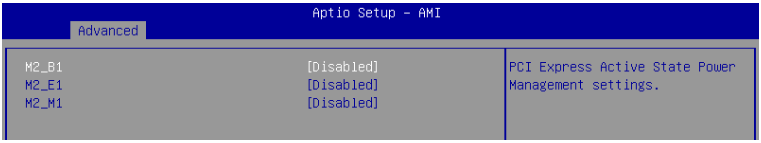
```
                               Aptio Setup - AMI
      Advanced
 GPIO Group Configuration                               Set GPIO0 to Input/Output
                                                        High/Output Low
 GPIO 0 Control                  [Input]
 GPIO 1 Control                  [Input]
 GPIO 2 Control                  [Input]
 GPIO 3 Control                  [Input]
 GPIO 4 Control                  [Input]
 GPIO 5 Control                  [Input]
 GPIO 6 Control                  [Input]
 GPIO 7 Control                  [Input]
```

▸ GPIO 0 ~ GPIO 7

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.



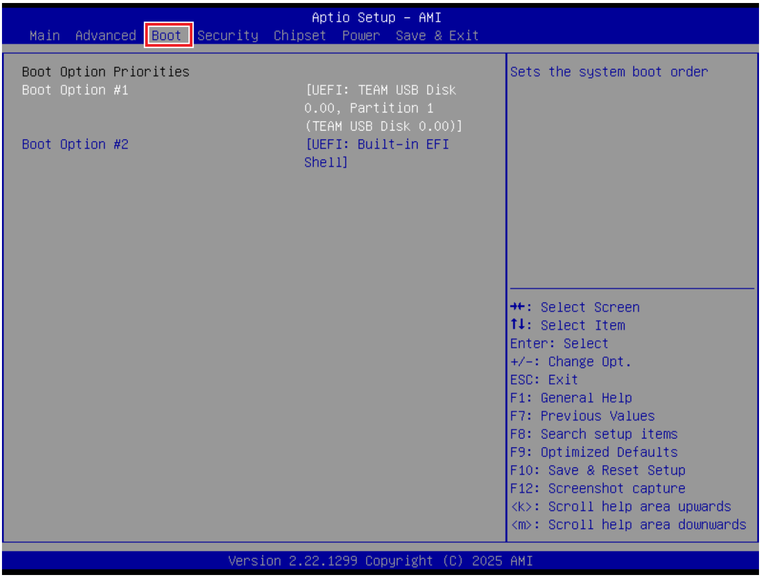
```
                               Aptio Setup - AMI
      Advanced
 M2_B1                           [Disabled]             PCI Express Active State Power
 M2_E1                           [Disabled]             Management settings.
 M2_M1                           [Disabled]
```

▸ M2_B1, M2_E1, M2_M1

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

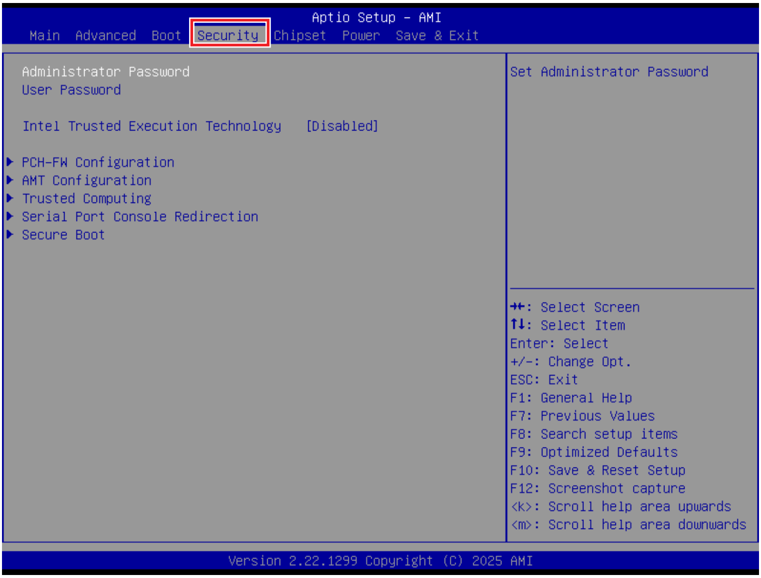


```
                              Aptio Setup - AMI
  Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

 Boot Option Priorities                                    Sets the system boot order
 Boot Option #1                 [UEFI: TEAM USB Disk
                                0.00, Partition 1
                                (TEAM USB Disk 0.00)]
 Boot Option #2                 [UEFI: Built-in EFI
                                Shell]
                                                           →←: Select Screen
                                                           ↑↓: Select Item
                                                           Enter: Select
                                                           +/-: Change Opt.
                                                           ESC: Exit
                                                           F1: General Help
                                                           F7: Previous Values
                                                           F8: Search setup items
                                                           F9: Optimized Defaults
                                                           F10: Save & Reset Setup
                                                           F12: Screenshot capture
                                                           <k>: Scroll help area upwards
                                                           <m>: Scroll help area downwards

                  Version 2.22.1299 Copyright (C) 2025 AMI
```

▶ 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



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

  Administrator Password                          Set Administrator Password
  User Password

  Intel Trusted Execution Technology    [Disabled]

▶ PCH-FW Configuration
▶ AMT Configuration
▶ Trusted Computing
▶ Serial Port Console Redirection
▶ Secure Boot
                                                  →←: Select Screen
                                                  ↑↓: Select Item
                                                  Enter: Select
                                                  +/-: Change Opt.
                                                  ESC: Exit
                                                  F1: General Help
                                                  F7: Previous Values
                                                  F8: Search setup items
                                                  F9: Optimized Defaults
                                                  F10: Save & Reset Setup
                                                  F12: Screenshot capture
                                                  <k>: Scroll help area upwards
                                                  <m>: Scroll help area downwards

              Version 2.22.1299 Copyright (C) 2025 AMI
```

▶ Administrator Password

Administrator Password controls access to the BIOS Setup utility.

▶ User Password

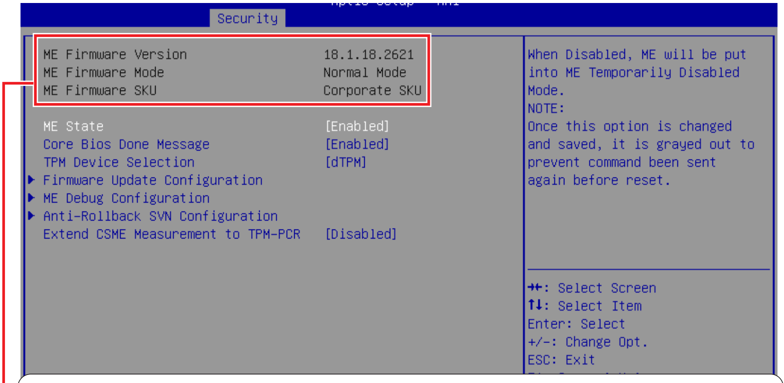
User Password controls access to the system at boot and to the BIOS Setup utility.

▶ 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.

▶ PCH-FW Configuration

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



```
                           Security
 ME Firmware Version                  18.1.18.2621    When Disabled, ME will be put
 ME Firmware Mode                     Normal Mode     into ME Temporarily Disabled
 ME Firmware SKU                      Corporate SKU   Mode.
                                                      NOTE:
 ME State                             [Enabled]       Once this option is changed
 Core Bios Done Message               [Enabled]       and saved, it is grayed out to
 TPM Device Selection                 [dTPM]          prevent command been sent
▶ Firmware Update Configuration                       again before reset.
▶ ME Debug Configuration
▶ Anti-Rollback SVN Configuration
 Extend CSME Measurement to TPM-PCR   [Disabled]
                                                      ──────────────────────────────
                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      ESC: Exit
```

Firmware Information

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.

▸ Core Bios Done Message

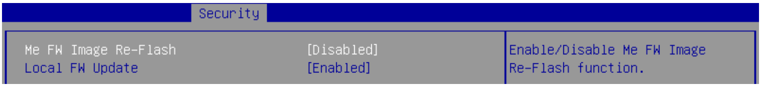
Enables or disables Core BIOS Done Message sent to ME.

▸ 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



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

» ME FW Image Re-Flash

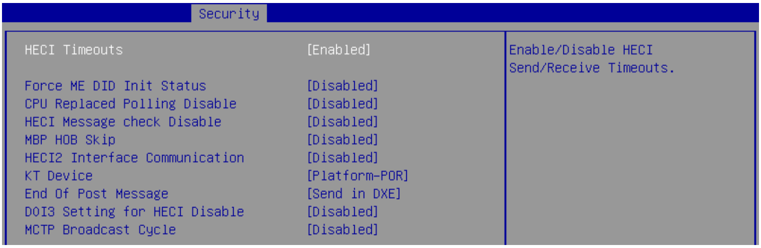
Enables or disables the ME Firmware Image Re-flashing.

» Local FW Update

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

▸ 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                          [Platform-POR]
 End Of Post Message                [Send in DXE]
 DOI3 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) 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.

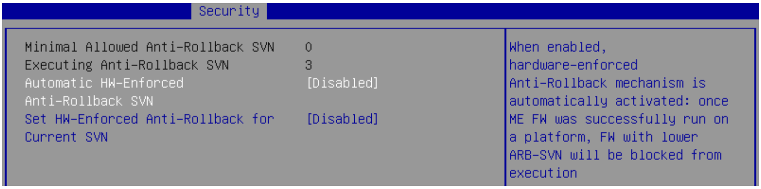
» DOI3 Setting for HECI Disable

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



```
Minimal Allowed Anti-Rollback SVN     0              When enabled,
Executing Anti-Rollback SVN           3              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**

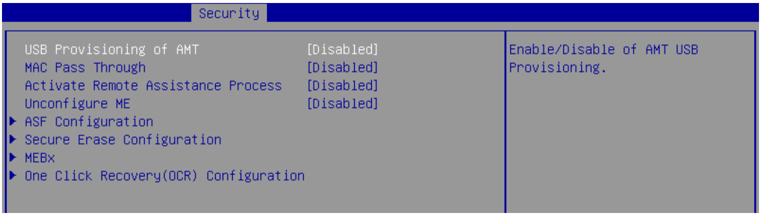
Enable HW ERB mechanism for current ARB SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent. This item will display when **Automatic HW-Enforced Anti-Rollback SVN** is enabled.

▸ Extend CSME Measurement to TPM-PCR

This setting enables or disables Intel® Converged Security and Management Engine (CSME) measurement extend to TPM-PCR.

▶AMT Configuration

Intel® Active Management Technology (Intel® AMT) is hardware-based technology for remotely managing and securing PCs out-of-band (OOB).



```
                              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
```

▸ 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.

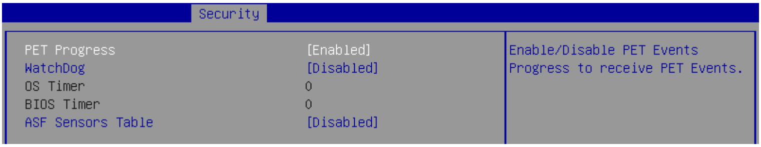
▸ Activate Remote Assistance Process

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.

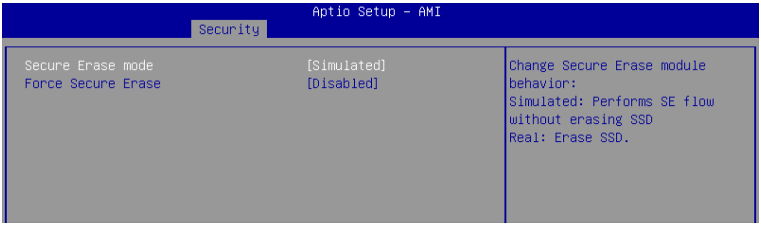
» BIOS Timer

This item displays BIOS Timer.

» ASF Sensor Table

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

Secure Erase Configuration



```
                         Aptio Setup - AMI
              Security

 Secure Erase mode               [Simulated]       Change Secure Erase module
 Force Secure Erase              [Disabled]        behavior:
                                                   Simulated: Performs SE flow
                                                   without erasing SSD
                                                   Real: Erase SSD.
```

» Secure Erase Mode

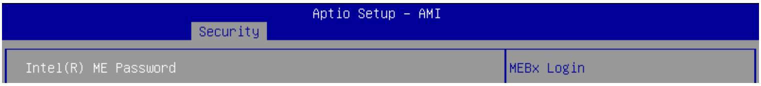
This setting change Secure Erase module behavior.

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

» Force Secure Erase

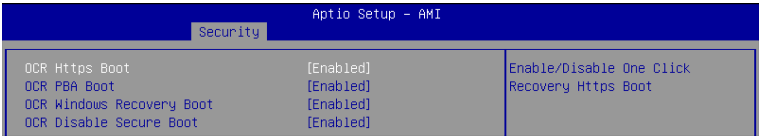
Enables or disables to force Secure Erase on next boot.

MEBx (Management Engine BIOS Extension)



```
                         Aptio Setup - AMI
              Security

 Intel(R) ME Password                              MEBx Login
```

One Click Recovery (OCR) Configuration



```
                         Aptio Setup - AMI
              Security

 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.

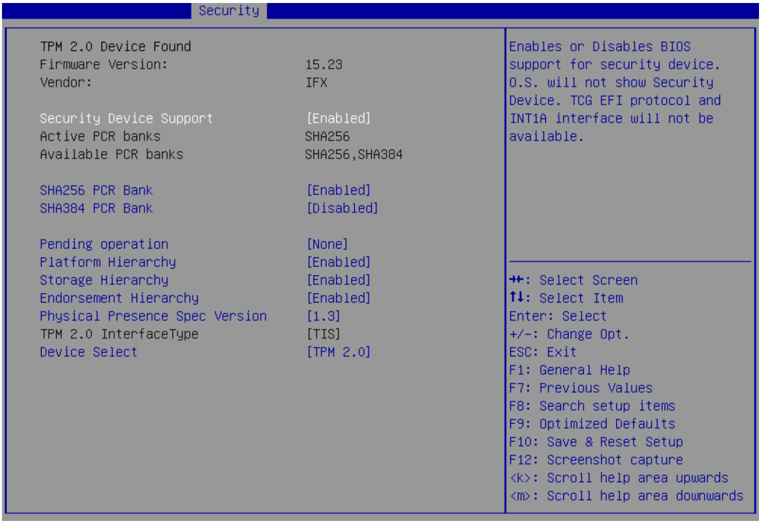
» OCR Windows Recovery Boot

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.

▶Trusted Computing



```
                          Security
 TPM 2.0 Device Found                                 Enables or Disables BIOS
 Firmware Version:                15.23               support for security device.
 Vendor:                          IFX                 O.S. will not show Security
                                                      Device. TCG EFI protocol and
 Security Device Support          [Enabled]           INT1A interface will not be
 Active PCR banks                 SHA256              available.
 Available PCR banks              SHA256,SHA384

 SHA256 PCR Bank                  [Enabled]
 SHA384 PCR Bank                  [Disabled]

 Pending operation                [None]
 Platform Hierarchy               [Enabled]
 Storage Hierarchy                [Enabled]           →←: Select Screen
 Endorsement Hierarchy            [Enabled]           ↑↓: Select Item
 Physical Presence Spec Version   [1.3]               Enter: Select
 TPM 2.0 InterfaceType            [TIS]               +/-: Change Opt.
 Device Select                    [TPM 2.0]           ESC: Exit
                                                      F1: General Help
                                                      F7: Previous Values
                                                      F8: Search setup items
                                                      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, SHA384 PCR Bank

These settings enables or disables the SHA256 PCR Bank and SHA384 PCR Bank.

▸ Pending Operation

When Security Device Support is set to [Enable], Pending Operation will appear. It is advised that users should routinely back up their TPM secured data.

[TPM Clear]	Clear all data secured by TPM.
[None]	Discard the se lection.

▸ Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

These settings enables or disables the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

▸ Physical Presence Spec Version

This settings show the Physical Presence Spec Version.

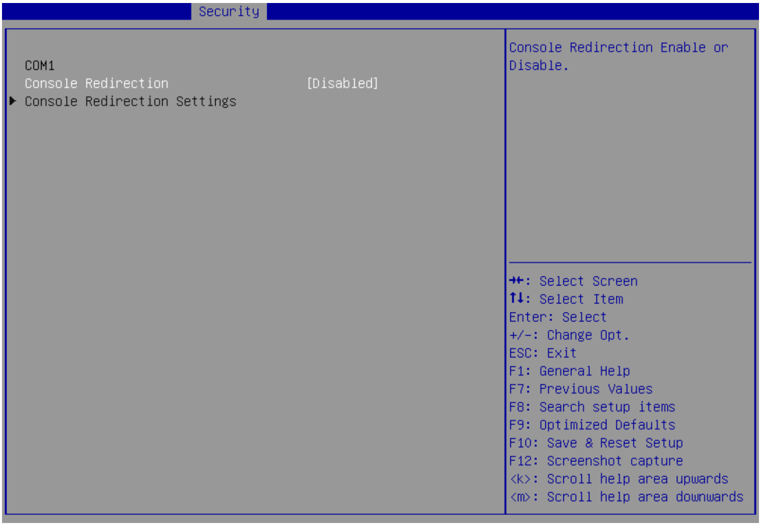
▸ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

▸ Device Select

Select your TPM device through this setting.

▶ Serial Port Console Redirection



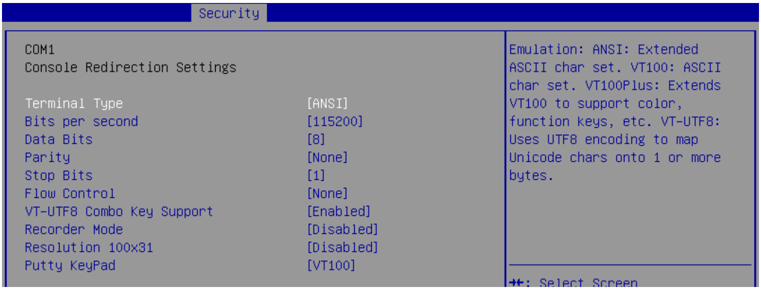
```
                              Security

  COM1                                                   Console Redirection Enable or
  Console Redirection                [Disabled]          Disable.
▶ Console Redirection Settings

                                                         →←: Select Screen
                                                         ↑↓: Select Item
                                                         Enter: Select
                                                         +/-: Change Opt.
                                                         ESC: Exit
                                                         F1: General Help
                                                         F7: Previous Values
                                                         F8: Search setup items
                                                         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]               ──────────────────────────
                                                        →←: Select Screen
```

» 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.

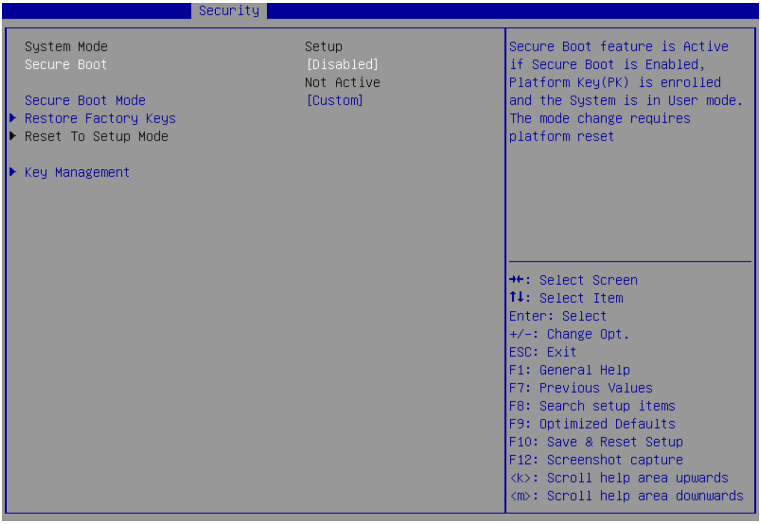
» Recorder Mode, Resolution 100x31

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

▶ Key Management
                                                            →←: Select Screen
                                                            ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Opt.
                                                            ESC: Exit
                                                            F1: General Help
                                                            F7: Previous Values
                                                            F8: Search setup items
                                                            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

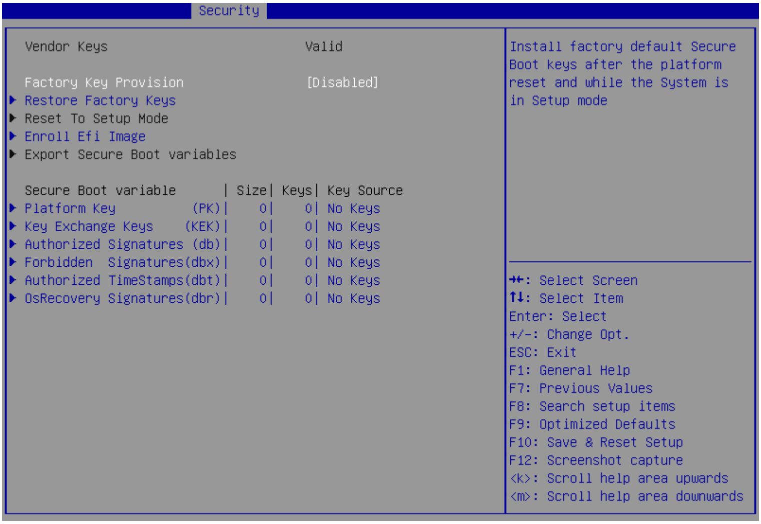
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▸ 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            |
▶ Authorized TimeStamps(dbt)|    0|    0| No Keys            | →←: Select Screen
▶ OsRecovery Signatures(dbr)|    0|    0| No Keys            | ↑↓: Select Item
                                                             | Enter: Select
                                                             | +/-: Change Opt.
                                                             | ESC: Exit
                                                             | F1: General Help
                                                             | F7: Previous Values
                                                             | F8: Search setup items
                                                             | 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) :**

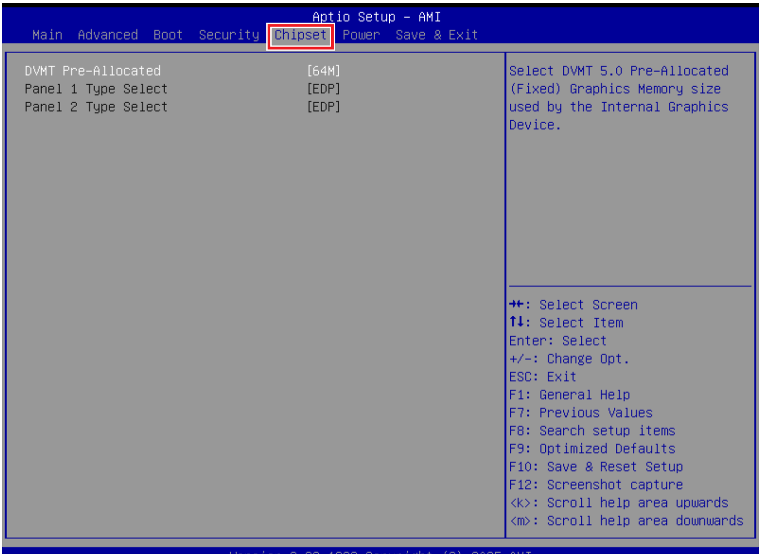
Authorized Signatures (db) lists the signatures that can be loaded.

» **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 Signatures (dbr):**
  Lists the available signatures for OS recovery.

Chipset



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

  DVMT Pre-Allocated                    [64M]      Select DVMT 5.0 Pre-Allocated
  Panel 1 Type Select                   [EDP]      (Fixed) Graphics Memory size
  Panel 2 Type Select                   [EDP]      used by the Internal Graphics
                                                   Device.

                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   ESC: Exit
                                                   F1: General Help
                                                   F7: Previous Values
                                                   F8: Search setup items
                                                   F9: Optimized Defaults
                                                   F10: Save & Reset Setup
                                                   F12: Screenshot capture
                                                   <k>: Scroll help area upwards
                                                   <m>: Scroll help area downwards
```

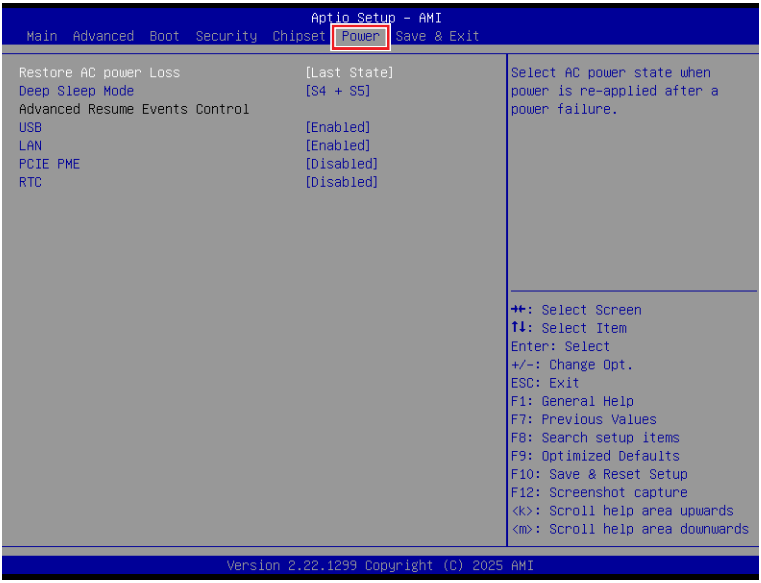
▶ DVMT Pre-Allocated

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

▶ Panel 1/ 2 Type Select

Set your video signal interface as LVDs or eDP.

Power



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

 Restore AC power Loss                 [Last State]   Select AC power state when
 Deep Sleep Mode                       [S4 + S5]      power is re-applied after a
 Advanced Resume Events Control                       power failure.
 USB                                   [Enabled]
 LAN                                   [Enabled]
 PCIE PME                              [Disabled]
 RTC                                   [Disabled]

                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      ESC: Exit
                                                      F1: General Help
                                                      F7: Previous Values
                                                      F8: Search setup items
                                                      F9: Optimized Defaults
                                                      F10: Save & Reset Setup
                                                      F12: Screenshot capture
                                                      <k>: Scroll help area upwards
                                                      <m>: Scroll help area downwards

              Version 2.22.1299 Copyright (C) 2025 AMI
```

▶ 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

This setting provides two options: [S4+S5] and [Disabled]. It enables a power-saving mode that reduces energy consumption when the system is off or in a low-power state. Some components remain powered to allow wake-up via the power button or RTC.

▶ USB

The item allows the activity of the USB device to wake up the system from S3 sleep state.

▶ LAN/ PCIE PME

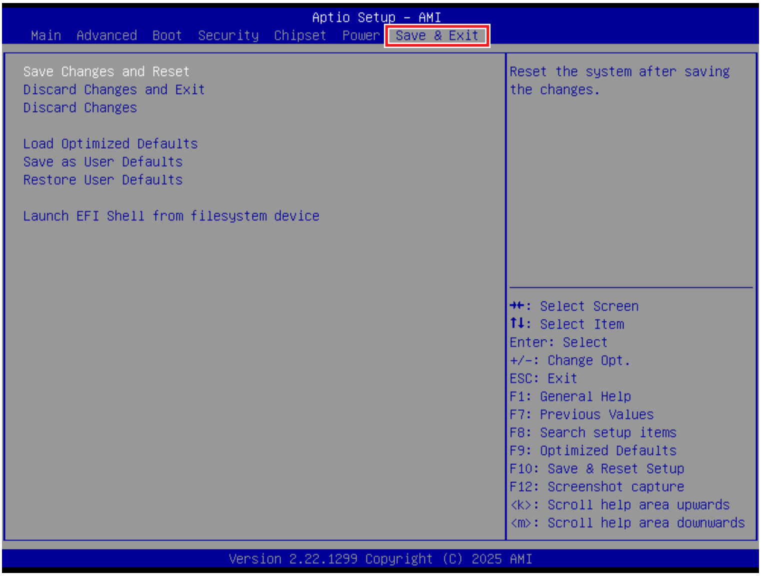
Enables or disables the system to be awakened from the power saving modes when activity or input signal of Intel® LAN device and onboard PCIE PME is detected.

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

▶ RTC

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

Save & Exit



```
                              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

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 ESC: Exit
                                                 F1: General Help
                                                 F7: Previous Values
                                                 F8: Search setup items
                                                 F9: Optimized Defaults
                                                 F10: Save & Reset Setup
                                                 F12: Screenshot capture
                                                 <k>: Scroll help area upwards
                                                 <m>: Scroll help area downwards

                  Version 2.22.1299 Copyright (C) 2025 AMI
```

▶ 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 Programming

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

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

The GPIO port configuration addresses are listed in the following table:

Name	Output Enable	Output Value	Input Value	Bit
GPIO0	0xB0	0xB1	0xB2	0
GPIO1	0xB0	0xB1	0xB2	1
GPIO2	0xB0	0xB1	0xB2	2
GPIO3	0xB0	0xB1	0xB2	3
GPIO4	0xB0	0xB1	0xB2	4
GPIO5	0xB0	0xB1	0xB2	5
GPIO6	0xB0	0xB1	0xB2	6
GPIO7	0xB0	0xB1	0xB2	7

Note: GPIO control is done via port 0xA00 (index) and 0xA01 (data) for register access. Changes to output value registers are only applied when the GPIO is in output mode.

1.1 Set GPIO Mode (Input or Output):

1. Read the current value from the Output Enable register.
2. Modify the corresponding bit:
   - ✓ Set the bit to 1 for Output mode.
   - ✓ Clear the bit to 0 for Input mode.
3. Write the updated value back to the Output Enable register.

Example: Set **GPIO3** to Input mode

```
Outportb (0xA00, 0xB0);   // Select GPIO3 Output Enable Register (0xB0)
val = Inportb (0xA01);    // Read current value from the register
val = val & (~(1 << 3));  // Clear bit 3 (GPIO3) to 0 (Input mode)
 Outportb (0xA01, val);   // Write the updated value back to the register.
```

Example: Set **GPIO7** to Output mode

```
Outportb (0xA00, 0xB0);   // Select GPIO7 Output Enable Register (0xB0)
val = Inportb (0xA01);    // Read current value from the register
val = val | (1<<7);       // Set bit 7 (GPIO7) to 1 (Output mode)
 Outportb (0xA01, val);   // Write the updated value back to the register
```

1.2 Set output value of GPIO:

1. Read the current value from the Output value register.
2. Modify the corresponding bit.
   - ✓ Write 1 for logic High.
   - ✓ Write 0 for logic Low.
3. Write the updated value back to the Output value register.

Example: Set **GPIO2** output “high”

```
Outportb (0xA00, 0xB1);   // Select GPIO2 Output value Register (0xB1)
val = Inportb (0xA01);    // Read current value from the register
val = val | (1<<2);       // Set bit 2 (GPIO2) to 1 (output “high”)
 Outportb (0xA01, val);   // Write the updated value back to the register
```

Example: Set **GPIO6** output “low”

```
Outportb (0xA00, 0xB1);   // Select GPIO6 Output value Register (0xB1)
val = Inportb (0xA01);    // Read current value from the register
val = val & (~(1<<6));    // Clear bit 6 (GPIO6) to 0 (output “low”)
 Outportb (0xA01, val);   // Write the updated value back to the register
```

1.3 Read input value from GPIO:

1. Read the register value.
2. Mask the corresponding bit to get the pin state:
   - ✓ Bit = 1 : Input is High
   - ✓ Bit = 0 : Input is Low

Example: Get **GPIO1** input value.

```
Outportb (0xA00, 0xB2);   // Select GPIO1 Input value Register (0xB2)
val = Inportb (0xA01);    // Read current value from the register
val = val & (1<<1);       // Read GPIO1 (bit 1).
if (val)       printf (“Input of   GPIO1   is High”);
else           printf (“Input of   GPIO1   is Low”);
```

Watchdog Timer

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
```