MS-CF03

Industrial Computer Board

User Guide

Contents

Revision

V1.1, 2024/09

Regulatory Notices

FCC-B Radio Frequency Interference Statement

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

CE Conformity

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

WEEE Statement

Under the European Union ("EU") Directive on Waste Electrical and Electronic Equipment, Directive 2012/19/EU, products of "electrical and electronic equipment" cannot be discarded as municipal waste anymore and manufacturers of covered electronic equipment will be obligated to take back such products at the end of their useful life.

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 and locate a nearby distributor for further recycling information.
- Users may also reach us at gpcontdev@msi.com for information regarding proper Disposal, Take-back, Recycling, and Disassembly of MSI products.

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

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

Specifications

Model	MS-CF03
Processor	• 12th Gen Intel® IoTG Alder Lake-N Processor N97, QC, 12W • 12th Gen Intel® IoTG Alder Lake-N Processor N200, QC, 6W • 12th Gen Intel® IoTG Alder Lake-N Core i3-N305, OC, 9W up to 15W • 12th Gen Intel® IoTG Alder Lake-N Atom x7425E, QC, 12W
Chipset	Within processor
Memory	• 1 x DDR5 SO-DIMM slot (262-pin) - Single Channel DDR5, Non-ECC - Up to 4800 MT/s - Up to 16GB
Network	2 x Intel® I225-V 2.5GbE LAN
Expansion Slots	• 1 x M.2 E Key slot (2230) - Supports PCIe x1 & USB 2.0 signal - Supports Intel® AX210 Wi-Fi 6E & BT-5.2 • 1 x M.2 B Key slot (2242/ 2280/ 3042)* - Supports PCIe x1 signal - Supports B+M Key PCIe x1 module
Storage	• 1 x SATA 3.0 6Gb/s port - Support AHCI mode • 1 x M.2 B Key slot (2242/ 2280/ 3042)* - Supports SATA 3.0 signal - Supports B+M Key SATA 3.0 SSD
Audio	Realtek® ALC897 High Definition Audio Codec
Graphics	• 1 x DP 1.4a up to 4096×2304 @60Hz • 1 x HDMI™ 1.4b up to 3840x2160 @30Hz • 1 x LVDS up to 1920x1200 @60Hz - 18/24-bit dual channel • 1 x eDP 1.4b up to 1920×1080 @60 Hz • 3 independent display supported in OS - DP - HDMI™ - LVDS - eDP

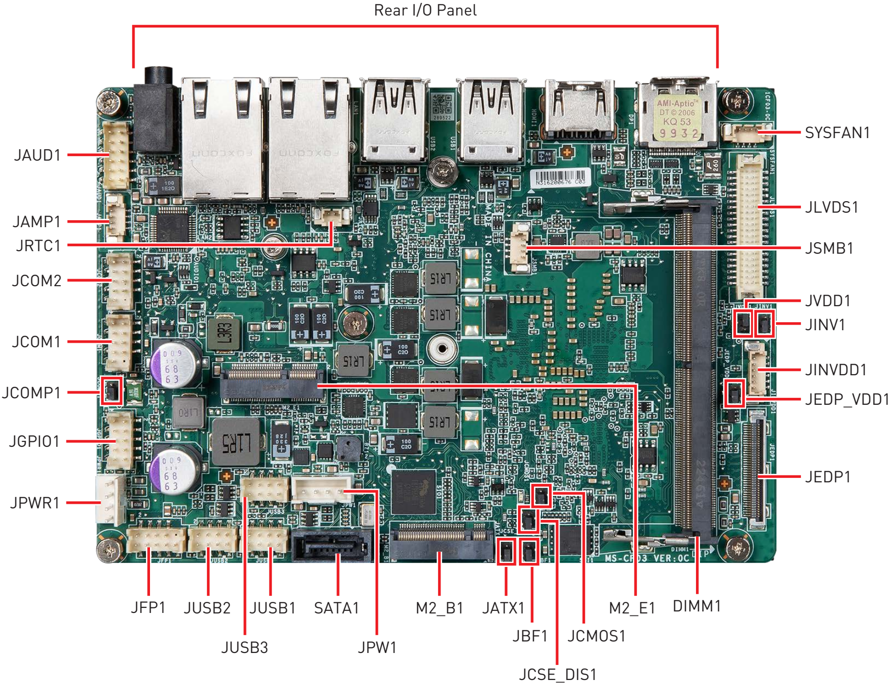
*There is only **"one" M.2 B Key Slot** on board, which is marked as **M2_B1**.

Model	MS-CF03
Power	1 x 9V~36V DC-in power connector*
Rear I/O	• 1 x Line-out jack • 2 x 2.5 GbE RJ-45 LAN ports • 2 x Dual Stacked USB 3.2 Type-A ports - 2 x USB 10Gbps Type-A ports (Bottom layer) - 2 x USB 5Gbps Type-A ports (Top layer) • 1 x DisplayPort (1.4a) • 1 x HDMI™ connector (1.4b)
Onboard Connector	• 1 x DC-in power connector (4-pin) • 1 x SATA power connector (4-pin, 5V/ 12V) • 1 x Front audio header (Headphone, Mic-in, Line-in) • 1 x Audio amplifier header • 1 x LVDS Inverter box header • 1 x LVDS wafer connector • 1 x eDP connector • 1 x PWM system fan box header • 1 x Front panel connector (Power switch, Reset switch, Power LED, HDD LED for M.2 B key) • 2 x COM port box headers • 1 x GPIO (DIO) connector • 1 x SMBus box header • 3 x USB 2.0 box headers (480 Mbps) • 1 x CMOS battery header
Onboard Jumper	• 1 x COM1 power select jumper (0V/ 5V/ 12V) • 1 x Clear CMOS jumper • 1 x CSE jumper • 1 x AT/ ATX mode select jumper • 1 x LVDS power select jumper (3V/ 5V) • 1 x eDP power select jumper (3V/ 5V) • 1 x LVDS Inverter power select jumper (5V/ 12V)
Form factor	• 3.5” SBC (Single Board Computer) - 146mm(L) x 102mm(W) x 1.6mm(T)

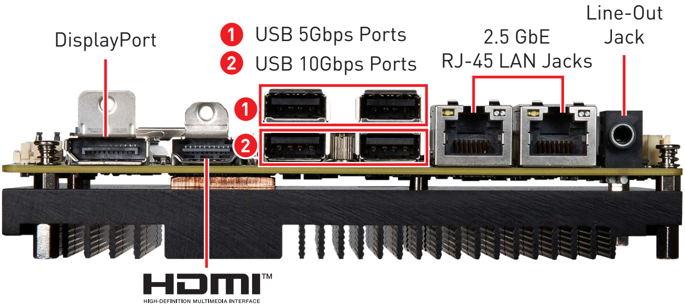
*The **power adapter** you use should provide at least **90W**.

Model	MS-CF03
OS Support	• Windows 10 IoT Enterprise LTSC (64-bit, 21H2) • Windows 11 IoT Enterprise (64-bit, 22H2, pre-scan) • Linux Kernel 5.xx Ubuntu 22.04.1 LTS (64-bit) (by request)
Certification	CE, FCC Class B, BSMI, VCCI, RCM, UKCA, IC
Environment	• Operating Temperature: -10 ~ 60°C • Storage Temperature: -20 ~ 80°C • Operating Humidity: 10 ~ 90%, non-condensing • Storage 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.

HDMI™ Connector

HDMI™ is an all-digital interface for uncompressed audio/video streams, supporting standard, enhanced, or high-definition video, and multi-channel digital audio on a single cable.

USB 10Gbps Ports

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**.

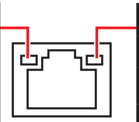
USB 5 Gbps Ports

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

2.5 GbE RJ-45 LAN Jack

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

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



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

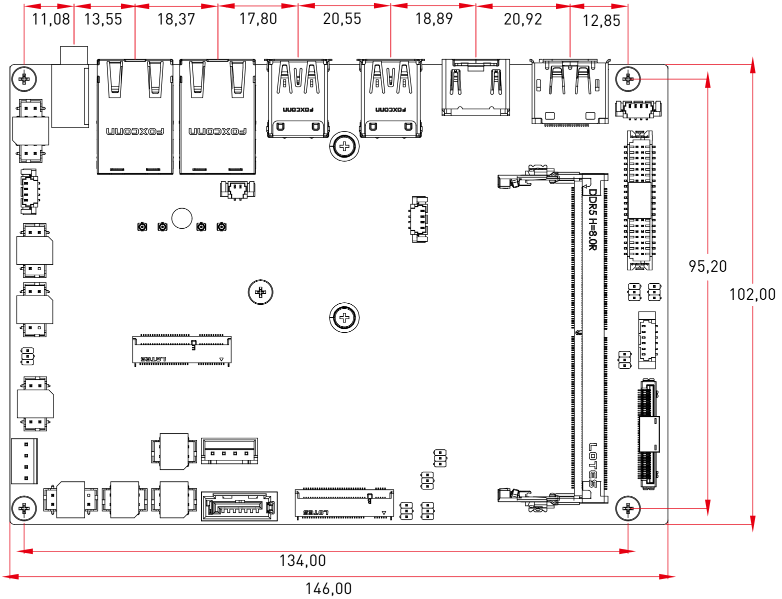
Line-Out Jack

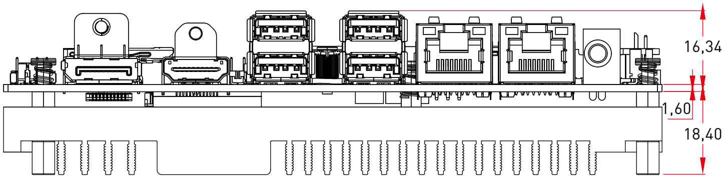
This connector is provided for headphones or speakers.

ME Overview

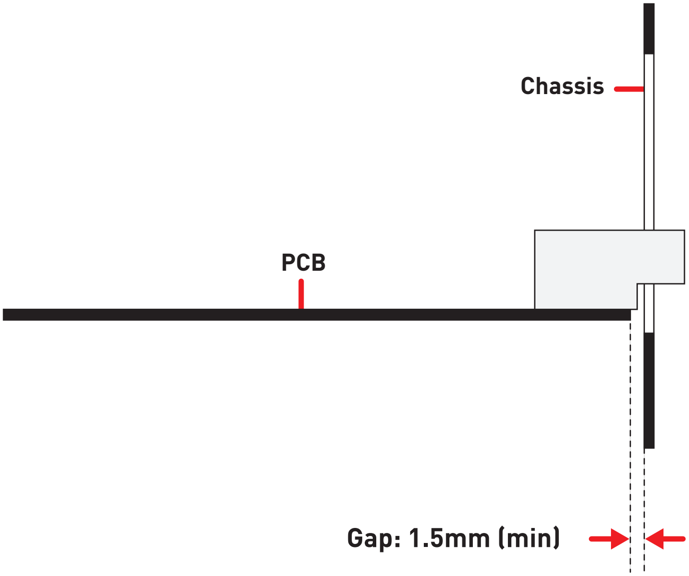
Board Dimension

Unit of measurement: mm





Suggested Chassis I/O Gap Dimension

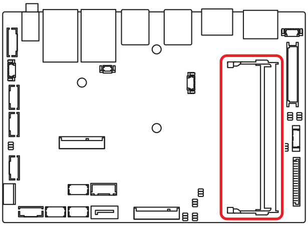


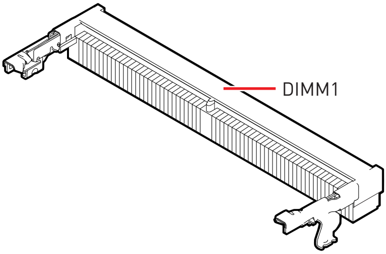
Component Contents

Memory

DIMM1: DDR5 SO DIMM Slot

The SO-DIMM slots is intended for memory modules.





Installing DDR5 Memory

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

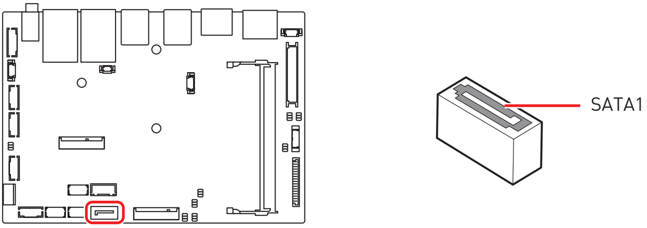
Important

- *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

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

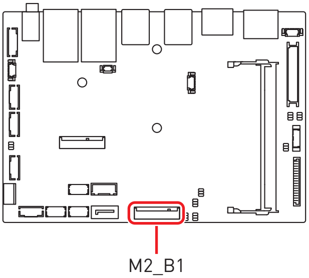


Important

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

M2_B1: M.2 Slot (B Key, 2242, 3042, 2280)

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



Feature

- Supports SATA 3.0 signal.
- Supports B+M Key SATA 3.0 SSD.

Video Demonstration

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

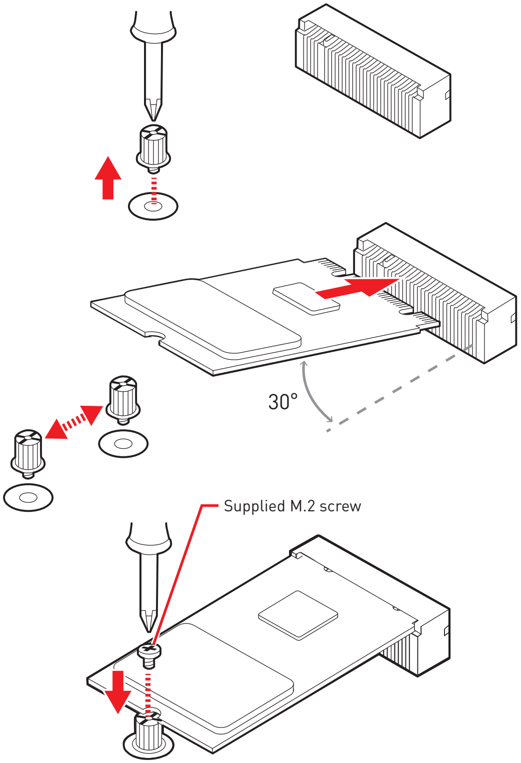
Installing M.2 SSD

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

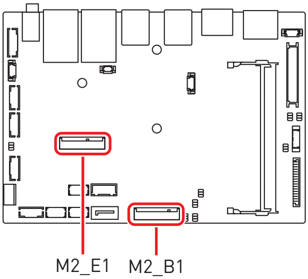
2. Set the M.2 riser screw at the appropriate location based on the length of your M.2 SSD.

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

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

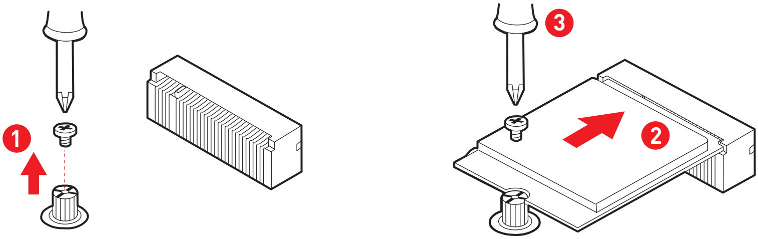


Expansion Slots



M2_B1: M.2 Slot (B Key, 2242, 3042, 2280)

Please install the module card into the M.2 slot as shown below.

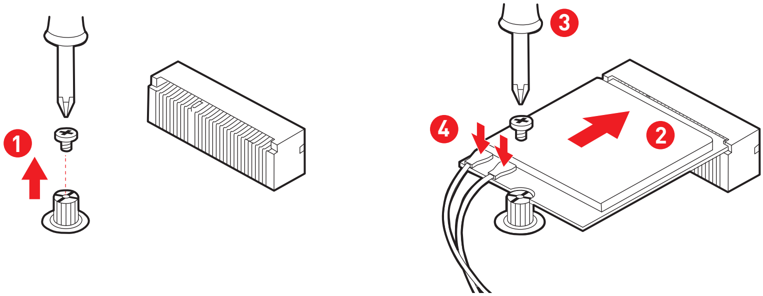


Feature

- Supports PCIe x1 signal.
- Supports B+M key PCIe x1 module.

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

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



Feature

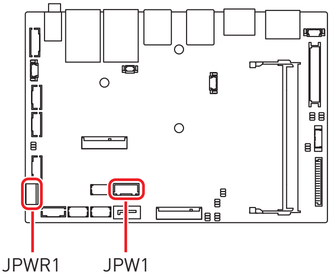
- Supports PCIe x1 & USB 2.0 signal.
- Supports Intel® Wi-Fi 6E AX210 + BT 5.2 wireless card.

Important

When adding or removing expansion cards, make sure that you unplug the power supply first. Meanwhile, read the documentation for the expansion card to configure any necessary hardware or software settings for the expansion card, such as jumpers, switches or BIOS configuration.

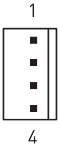
Connectors

Power Connectors



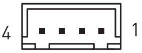
JPWR1: 4-Pin DC-In Main Power Connector

This connector allows you to connect an power supply.

JPWR1 	1	DC-IN	2	DC-IN
	3	GND	4	GND

JPW1: 4-Pin SATA Power Connector

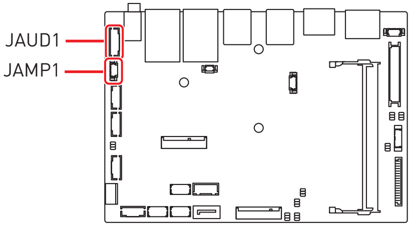
This connector is used to provide power to SATA devices.

JPW1 	1	5V	2	GND
	3	GND	4	12V

Important

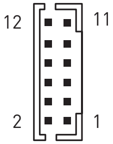
Make sure that all the power cables are securely connected to a proper power supply to ensure stable operation of the system.

Audio Connectors



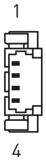
JAUD1: Front Audio Header

This connector allows you to connect front panel audio.

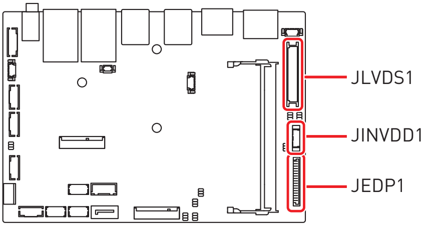
JAUD1 	1	LINE_IN_RA	2	MIC1_RA
	3	LINE_IN_LA	4	MIC1_LA
	5	LOUT_RA	6	MIC1_JD
	7	LOUT_LA	8	LINE_IN_JD
	9	FRONT_JD	10	GND
	11	GND	12	GND

JAMP1: Audio Amplifier Header

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

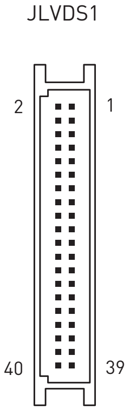
JAMP1 	1	AMP_L-	2	AMP_L+
	3	AMP_R-	4	AMP_R+

Graphics Connectors



JLVDS1: LVDS Wafer Connector

This connector is designed for use with LVDS interface flat panels. When connecting your flat panel to this connector, be sure to check the panel datasheet to ensure that you set the **LVDS power select jumper (JVDD1)** to the appropriate power voltage.

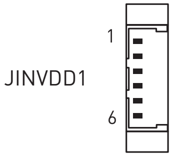
	1	12V	2	12V
	3	LCD_VDD	4	12V
	5	LCD_VDD	6	LCD_VDD
	7	DDC_CLK	8	DDC_DATA
	9	L_BKLT_CTRL#	10	LCDEN
	11	INV_ON	12	LVDS_DETECT#_C
	13	LVDSA_DATA1	14	LVDSA_DATA0
	15	LVDSA_DATA#1	16	LVDSA_DATA#0
	17	GND	18	GND
	19	LVDSA_DATA3	20	LVDSA_DATA2
	21	LVDSA_DATA#3	22	LVDSA_DATA#2
	23	GND	24	GND
	25	LVDSB_DATA1	26	LVDSB_DATA0
	27	LVDSB_DATA#1	28	LVDSB_DATA#0
	29	GND	30	GND
	31	LVDSB_DATA3	32	LVDSB_DATA2
	33	LVDSB_DATA#3	34	LVDSB_DATA#2
	35	GND	36	GND
	37	LVDSB_CLK	38	LVDSA_CLK
	39	LVDSB_CLK#	40	LVDSA_CLK#

⚠ ***Important***

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

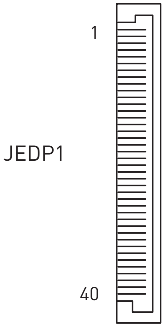
JINVDD1: LVDS Inverter Box Header

The connector is provided for LCD backlight options, be sure to check the panel datasheet to ensure that you set the **LVDS Inverter Power Select Jumper (JINV1)** to the appropriate power voltage (5V/12V).

	1	5V/12V	2	5V/12V
	3	BKLT_EN	4	BKLT_CTRL
	5	GND	6	GND

JEDP1: eDP Connector

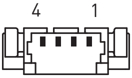
This connector is designed for use with eDP interface flat panels. When connecting your flat panel to this connector, be sure to check the panel datasheet to ensure that you set the **eDP power select jumper (JEDP_VDD1)** to the appropriate power voltage.

	1	LCD_VDD1	2	LCD_VDD1
	3	LCD_VDD1	4	LCD_VDD1
	5	LCD_VDD1	6	VCC3
	7	SMB_CLK	8	SMB_DATA
	9	GND	10	HPD
	11	N/C	12	N/C
	13	GND	14	DPC_LINE3_DN
	15	DPC_LINE3_DP	16	GND
	17	DPC_LINE2_DN	18	DPC_LINE2_DP
	19	GND	20	DPC_LINE1_DN
	21	DPC_LINE1_DP	22	GND
	23	DPC_LINE0_DN	24	DPC_LINE0_DP
	25	GND	26	DSP_DDPC_AUXP
	27	DSP_DDPC_AUXN	28	GND
	29	VCC3	30	GND
	31	+12V	32	GND
	33	GND	34	VCC5
	35	GND	36	BKLTCTL
	37	BKLT_EN	38	+12V
	39	VCC3	40	GND

Other Connectors

SYSFAN1: PWM System Fan Box Header

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.

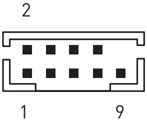
SYSFAN1 	1	GND	2	FAN POWER
	3	FAN SENSE	4	FAN_PWM

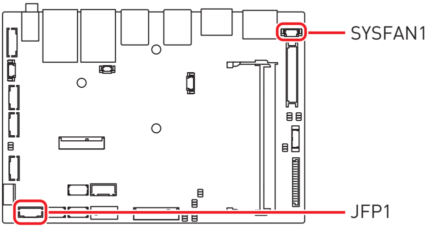
Important

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

JFP1: Front Panel Connector

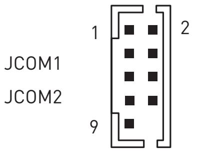
This front-panel connector is provided for electrical connection to the front panel switches & LEDs and is compliant with Intel Front Panel I/O Connectivity Design Guide.

JFP1 	1	HDD LED+	2	POWER LED
	3	HDD LED-	4	SUS LED
	5	GND	6	POWER SWITCH+
	7	RESET SWITCH+	8	POWER SWITCH-
	9	NC	10	No pin

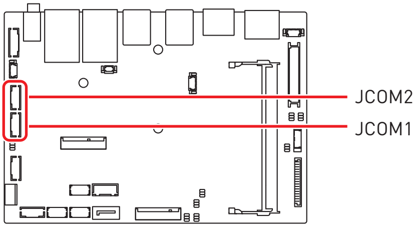


JCOM1, JCOM2: COM Port Box Headers

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



1	DCD#	2	SIN
3	SOUT	4	DTR
5	GND	6	DSR#
7	RTS	8	CTS#
9	VCC_COM (**JCOM1**) NC (**JCOM2**)	10	No pin



- **JCOM1**
  - Supports RS-232/ 422/ 485
  - With 0V/ 5V/ 12V
- **JCOM2**
  - Supports RS-232

RS232

PIN	SIGNAL	DESCRIPTION
1	NDCD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM/ NC	VCC_COM/ No Connection
10	No Pin	No Pin

RS422

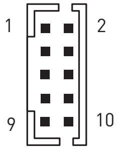
PIN	SIGNAL	DESCRIPTION
1	422 TXD-	Transmit Data, Negative
2	422 TXD+	Receive Data, Positive
3	422 RXD+	Transmit Data, Positive
4	422 RXD-	Receive Data, Negative
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection
10	NC	No Connection

RS485

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

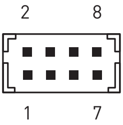
JGPIO1: GPIO (DIO) Box Header

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

JGPIO1 	1	GND	2	VCC5
	3	GPO0	4	GPI0
	5	GPO1	6	GPI1
	7	GPO2	8	GPI2
	9	GPO3	10	GPI3

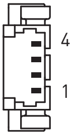
JUSB1~3: USB 2.0 Box Headers

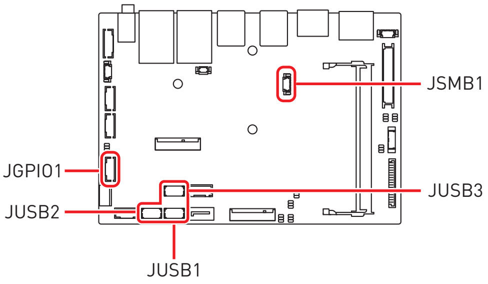
These connectors are ideal for connecting USB devices such as keyboard, mouse, or other USB-compatible devices.

JUSB1 JUSB2 JUSB3 	1	5V	2	GND
	3	USB_0-	4	USB_1+
	5	USB_0+	6	USB_1-
	7	GND	8	5V

JSMB1: SMBus Box Header

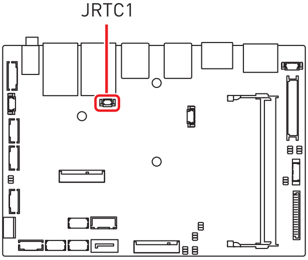
This connector, known as I2C, is for users to connect System Management Bus (SMBus) interface.

JSMB1 	1	5VSB	2	SMBCLK
	3	SMBDATA	4	GND



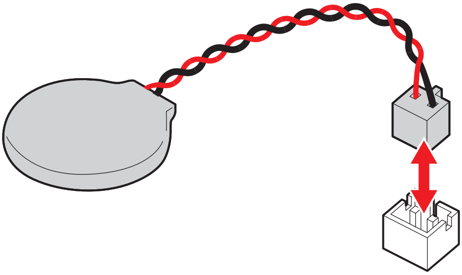
JRTC1: CMOS Battery Header

If the CMOS battery is out of charge, the time in the BIOS will be reset and the data of system configuration will be lost. In this case, you need to replace the CMOS battery.



Replacing CMOS battery

1. Unplug the battery wire from the JRTC1 connector and remove the battery.
2. Connect the new CR2032 battery with wire to the JRTC1 connector.



WARNING

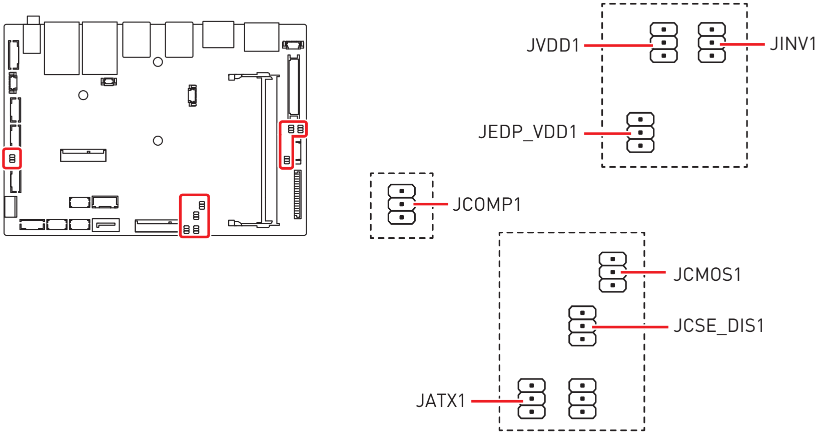
KEEP OUT OF REACH OF CHILDREN

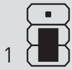
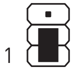
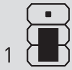
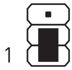
- *Swallowing can lead to chemical burns, perforation of soft tissue, and even death.*
- *Severe burns can occur within 2 hours of ingestion.*
- *If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.*

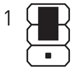
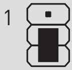
Jumpers

Important

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



Jumper Name	Default Setting	Description
JCOMP1		**COM Power Select Jumper** 1-2: 5V Power (Default) 2-3: 12V Power
JCMOS1		**Clear CMOS Jumper** 1-2: Normal (Default) 2-3: Clear CMOS
JCSE_DIS1		**CSE Jumper** 1-2: Normal (Default) 2-3: ME disable
JATX1		**AT/ ATX Mode Select Jumper** 1-2: ATX (Default) 2-3: AT
JVDD1		**LVDS Power Select Jumper** 1-2: 3V (Default) 2-3: 5V

Jumper Name	Default Setting	Description
JINV1		**LVDS Inverter Power Select Jumper**
		1-2: 5V (Default) 2-3: 12V
JEDP_VDD1		**eDP Power Select Jumper**
		1-2: 5V 2-3: 3V (Default)

BIOS Setup

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

Users may need to run the Setup program when:

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

Important

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

Entering Setup

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

Press <DEL> or <F2> to enter SETUP

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

Important

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

Control Keys

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

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

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

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

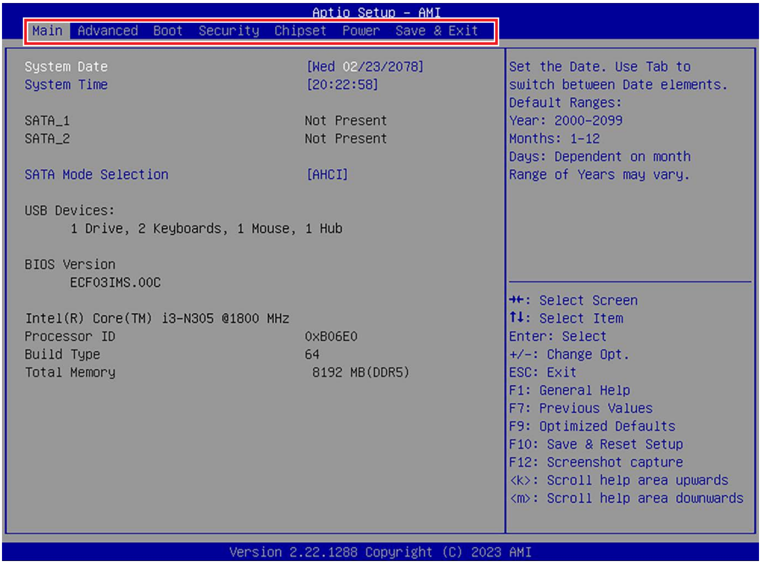
Sub-Menu

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

General Help <F1>

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

The Menu Bar



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

  System Date                          [Wed 02/23/2078]    Set the Date. Use Tab to
  System Time                          [20:22:58]          switch between Date elements.
                                                           Default Ranges:
  SATA_1                               Not Present         Year: 2000-2099
  SATA_2                               Not Present         Months: 1-12
                                                           Days: Dependent on month
  SATA Mode Selection                  [AHCI]              Range of Years may vary.

  USB Devices:
        1 Drive, 2 Keyboards, 1 Mouse, 1 Hub

  BIOS Version
        ECF03IMS.00C
                                                           →←: Select Screen
  Intel(R) Core(TM) i3-N305 @1800 MHz                      ↑↓: Select Item
  Processor ID                         0xB06E0             Enter: Select
  Build Type                           64                  +/-: Change Opt.
  Total Memory                          8192 MB(DDR5)      ESC: Exit
                                                           F1: General Help
                                                           F7: Previous Values
                                                           F9: Optimized Defaults
                                                           F10: Save & Reset Setup
                                                           F12: Screenshot capture
                                                           <k>: Scroll help area upwards
                                                           <m>: Scroll help area downwards

                      Version 2.22.1288 Copyright (C) 2023 AMI
```

▶ Main

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

▶ Advanced

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

▶ Boot

Use this menu to specify the priority of boot devices.

▶ Security

Use this menu to set supervisor and user passwords.

▶ Chipset

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

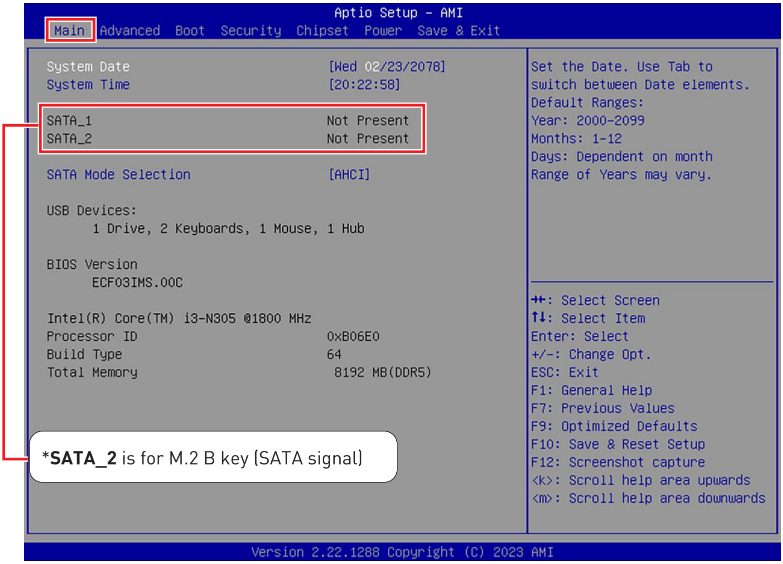
▶ Power

Use this menu to specify your settings for power management.

▶ Save & Exit

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

Main



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

 System Date                        [Wed 02/23/2078]    Set the Date. Use Tab to
 System Time                        [20:22:58]          switch between Date elements.
                                                        Default Ranges:
 SATA_1                             Not Present         Year: 2000-2099
 SATA_2                             Not Present         Months: 1-12
                                                        Days: Dependent on month
 SATA Mode Selection                [AHCI]              Range of Years may vary.

 USB Devices:
       1 Drive, 2 Keyboards, 1 Mouse, 1 Hub

 BIOS Version
       ECF03IMS.00C
                                                        →←: Select Screen
 Intel(R) Core(TM) i3-N305 @1800 MHz                    ↑↓: Select Item
 Processor ID                       0xB06E0             Enter: Select
 Build Type                         64                  +/-: Change Opt.
 Total Memory                        8192 MB(DDR5)      ESC: Exit
                                                        F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset Setup
                                                        F12: Screenshot capture
                                                        <k>: Scroll help area upwards
                                                        <m>: Scroll help area downwards

                    Version 2.22.1288 Copyright (C) 2023 AMI
```

***SATA_2** is for M.2 B key (SATA signal)

▶ System Date

This setting allows you to set the system date. Use <Tab> key to switch between date elements.

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

▶ System Time

This setting allows you to set the system time. Use <Tab> key to switch between time elements.

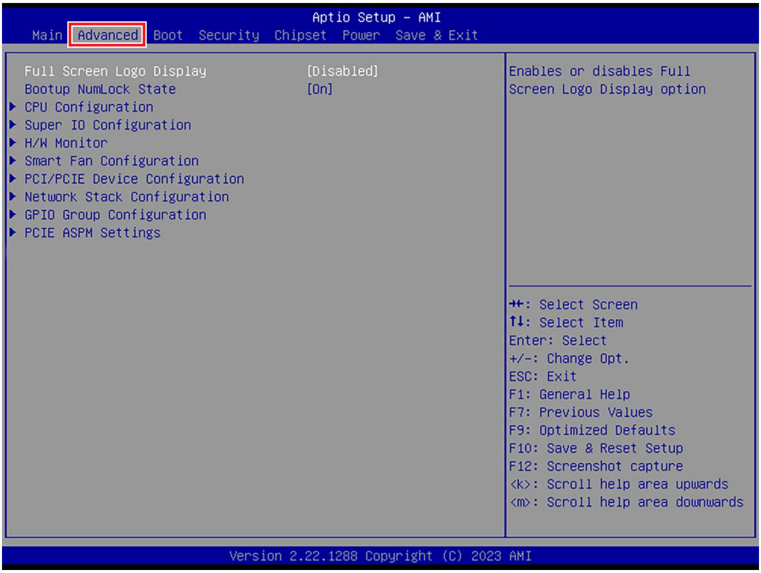
Format: <Hour> <Minute> <Second>.

▶ SATA Mode Selection

This setting specifies SATA controller mode.

[AHCI]	AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.

Advanced



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

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

                  Version 2.22.1288 Copyright (C) 2023 AMI
```

▶ Full Screen Logo Display

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

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

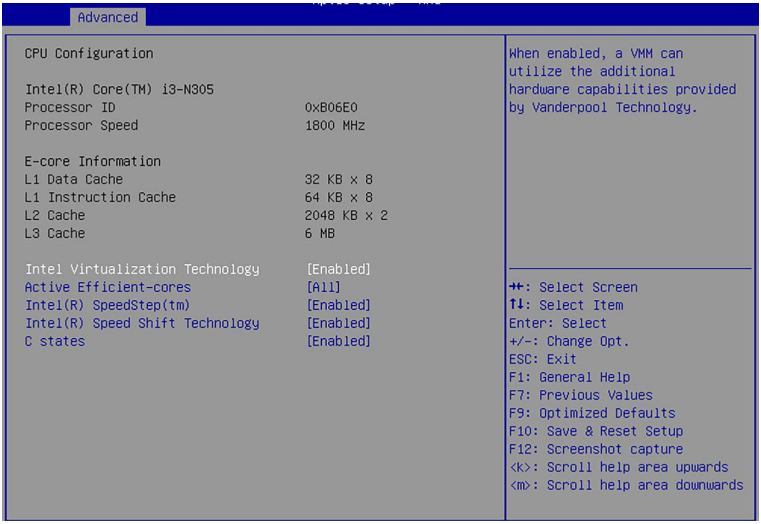
Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

▶ Bootup NumLock State

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

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

▶ CPU Configuration



```
Advanced

CPU Configuration                                        When enabled, a VMM can
                                                         utilize the additional
Intel(R) Core(TM) i3-N305                                hardware capabilities provided
Processor ID                      0xB06E0                by Vanderpool Technology.
Processor Speed                   1800 MHz

E-core Information
L1 Data Cache                     32 KB x 8
L1 Instruction Cache              64 KB x 8
L2 Cache                          2048 KB x 2
L3 Cache                          6 MB

Intel Virtualization Technology   [Enabled]
Active Efficient-cores            [All]                  →←: Select Screen
Intel(R) SpeedStep(tm)            [Enabled]              ↑↓: Select Item
Intel(R) Speed Shift Technology   [Enabled]              Enter: Select
C states                          [Enabled]              +/-: Change Opt.
                                                         ESC: Exit
                                                         F1: General Help
                                                         F7: Previous Values
                                                         F9: Optimized Defaults
                                                         F10: Save & Reset Setup
                                                         F12: Screenshot capture
                                                         <k>: Scroll help area upwards
                                                         <m>: Scroll help area downwards
```

▶ Intel Virtualization Technology

Enables or disables Intel Virtualization technology.

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

[Disabled] Disables this function.

▶ Active Efficient-cores

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

▶ Intel(R) SpeedStep(TM)

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

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

[Disabled] Disables this function.

▸ Intel(R) Speed Shift Technology

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

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

[Disabled] Disable this function.

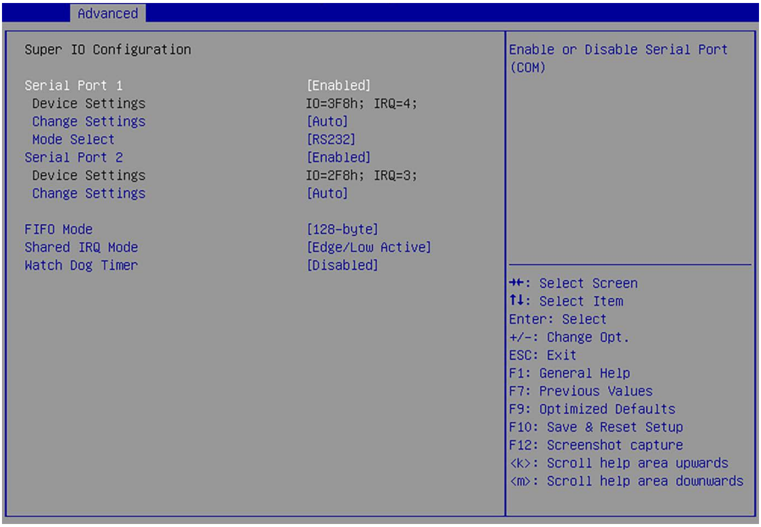
▸ C States

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

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

[Disabled] Disable this function.

▶ Super IO Configuration



```
Advanced

Super IO Configuration                                         Enable or Disable Serial Port
                                                               (COM)
Serial Port 1                         [Enabled]
 Device Settings                      IO=3F8h; IRQ=4;
 Change Settings                      [Auto]
 Mode Select                          [RS232]
Serial Port 2                         [Enabled]
 Device Settings                      IO=2F8h; IRQ=3;
 Change Settings                      [Auto]

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

▶ Serial Port 1/ 2

This setting enables or disables the specified serial port.

» Change Settings

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

» Mode Select

Select an operation mode for Serial Port 1/ 2.

▶ FIFO Mode

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

▶ Shared IRQ Mode

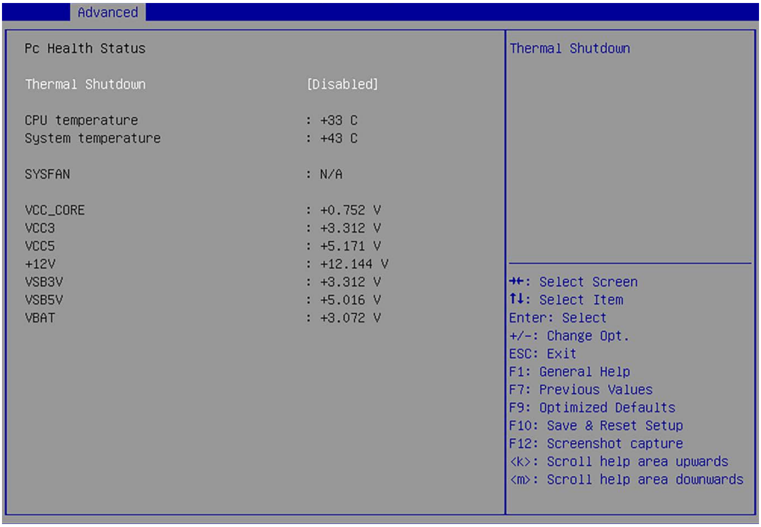
This setting provides the system with the ability to share interrupts among its serial ports.

▶ Watch Dog Timer

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

H/W Monitor (PC Health Status)

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



```
        Advanced
 Pc Health Status                                        Thermal Shutdown

 Thermal Shutdown                    [Disabled]

 CPU temperature                     : +33 C
 System temperature                  : +43 C

 SYSFAN                              : N/A

 VCC_CORE                            : +0.752 V
 VCC3                                : +3.312 V
 VCC5                                : +5.171 V
 +12V                                : +12.144 V
 VSB3V                               : +3.312 V          →←: Select Screen
 VSB5V                               : +5.016 V          ↑↓: Select Item
 VBAT                                : +3.072 V          Enter: Select
                                                         +/-: Change Opt.
                                                         ESC: Exit
                                                         F1: General Help
                                                         F7: Previous Values
                                                         F9: Optimized Defaults
                                                         F10: Save & Reset Setup
                                                         F12: Screenshot capture
                                                         <k>: Scroll help area upwards
                                                         <m>: Scroll help area downwards
```

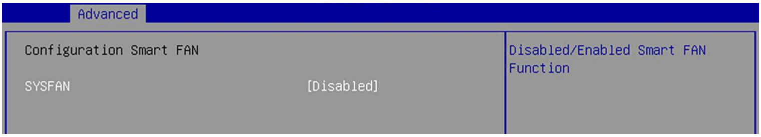
▸ Thermal Shutdown

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

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

[Disabled] Disable this function.

Smart Fan Configuration



```
        Advanced
 Configuration Smart FAN                                 Disabled/Enabled Smart FAN
                                                         Function
 SYSFAN                              [Disabled]
```

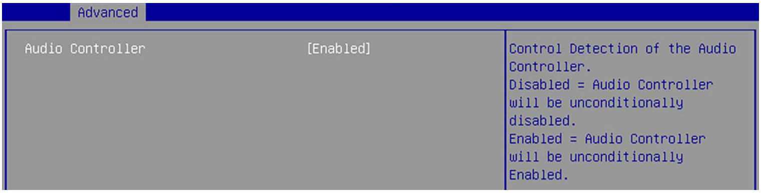
▸ SYSFAN

This setting enables or disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the system fan speed automatically depending on the current system temperature, avoiding the overheating to damage your system. The following items will display when **SYSFAN** is enabled.

» **Min. Speed (%)**

The beginning speed of the System fan.

▶ PCI/PCIE Device Configuration



```
Audio Controller                    [Enabled]
```

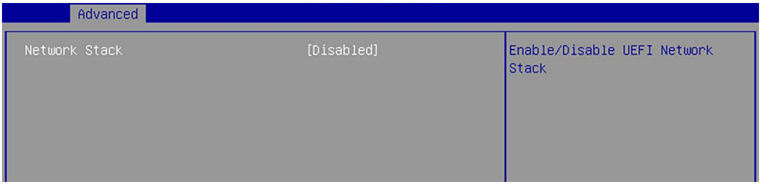
Control Detection of the Audio Controller.
Disabled = Audio Controller will be unconditionally disabled.
Enabled = Audio Controller will be unconditionally Enabled.

▶ 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.



```
Network Stack                       [Disabled]
```

Enable/Disable UEFI Network Stack

▶ Network Stack

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

» **IPV4 PXE Support**

Enables or disables IPv4 PXE boot support.

» **IPV4 HTTP Support**

Enables or disables Ipv4 HTTP Support.

» **IPV6 PXE Support**

Enables or disables Ipv6 PXE Support.

» **IPV6 HTTP Support**

Enables or disables Ipv6 HTTP Support.

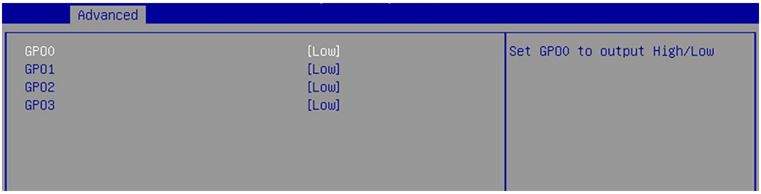
» **PXE boot wait time**

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

» **Media detect count**

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

▶ GPIO Group Configuration



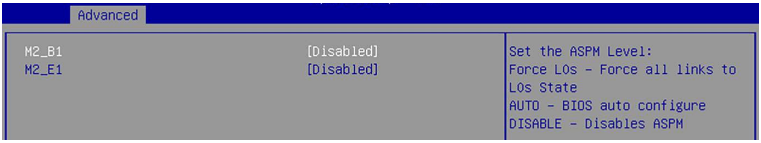
```
GPO0                                   [Low]        Set GPO0 to output High/Low
GPO1                                   [Low]
GPO2                                   [Low]
GPO3                                   [Low]
```

▸ GPO0 ~ GPO3

These settings control the operation mode of the specified GPIO.

▶ PCIE ASPM settings

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



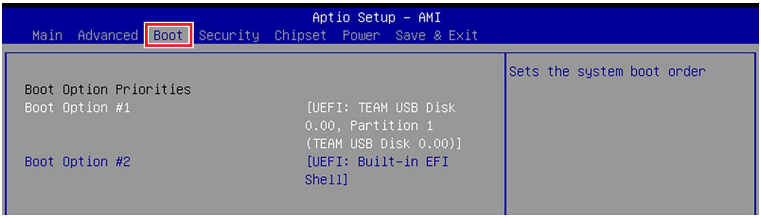
```
M2_B1                                  [Disabled]   Set the ASPM Level:
M2_E1                                  [Disabled]   Force L0s - Force all links to
                                                    L0s State
                                                    AUTO - BIOS auto configure
                                                    DISABLE - Disables ASPM
```

▸ M2_B1/ M2_E1

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

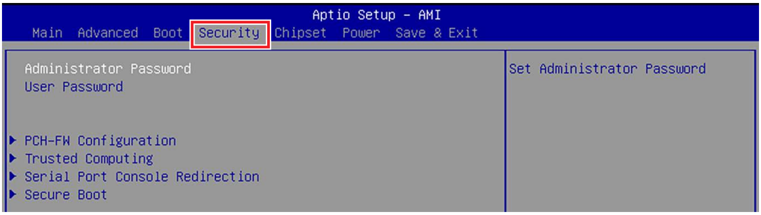


```
                              Aptio Setup - AMI
  Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

  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]
```

▶ 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


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

▶ Administrator Password

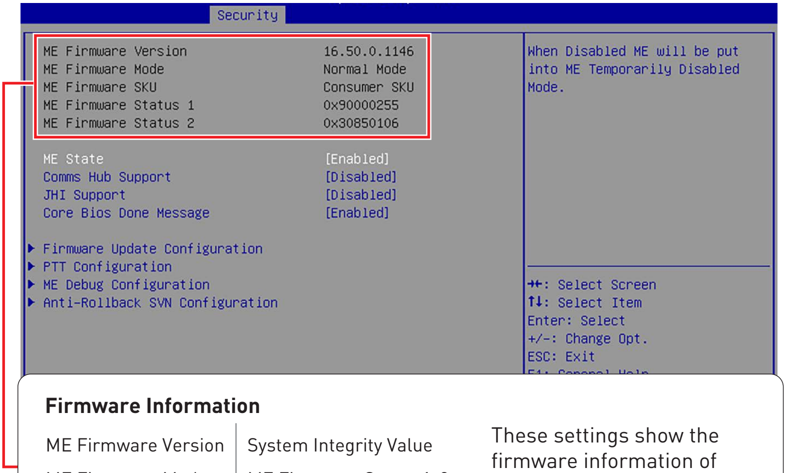
Administrator Password controls access to the BIOS Setup utility.

▶ User Password

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

▶ PCH-FW Configuration

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



```
                         Security

 ME Firmware Version                  16.50.0.1146       When Disabled ME will be put
 ME Firmware Mode                     Normal Mode        into ME Temporarily Disabled
 ME Firmware SKU                      Consumer SKU       Mode.
 ME Firmware Status 1                 0x90000255
 ME Firmware Status 2                 0x30850106

 ME State                             [Enabled]
 Comms Hub Support                    [Disabled]
 JHI Support                          [Disabled]
 Core Bios Done Message               [Enabled]

▶ Firmware Update Configuration
▶ PTT Configuration                                      →←: Select Screen
▶ ME Debug Configuration                                 ↑↓: Select Item
▶ Anti-Rollback SVN Configuration                        Enter: Select
                                                         +/-: Change Opt.
                                                         ESC: Exit
                                                         F1: General Help
```

Firmware Information

ME Firmware Version	System Integrity Value
ME Firmware Mode	ME Firmware Status 1-2
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.

▶ Comms Hub Support

Enables or disables the communications hub support.

▶ JHI Support

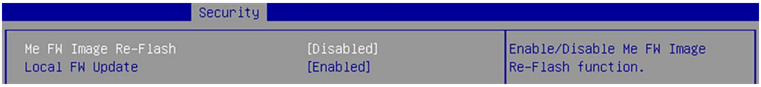
Enables or disables JHI Support. JHI stands for Intel® Dynamic Application Loader Host Interface Service (Intel® DAL HIS) and is the engineering name for this feature. Enabling JHI Support in the BIOS settings allows the system to utilize this interface for communication between trusted applications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

▶ Core BIOS Done Message

Enables or disables Core BIOS Done Message sent to ME.

▶ Firmware Update Configuration

This menu will display when **ME State** is enabled.



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

» ME FW Image Re-Flash

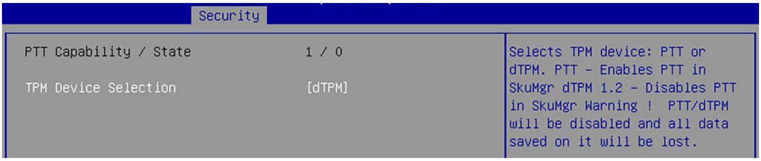
Enables or disables the ME Firmware Image Re-flashing**.**

» Local FW Update

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

▶ PTT Configuration

Intel® Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows. This menu will display when **ME State** is enabled.



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

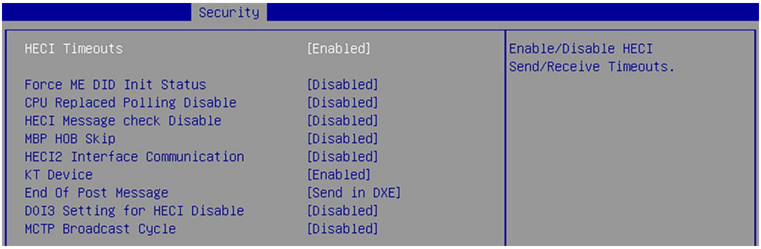
» TPM Device Selection

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

[PTT]	Enables PTT in SkuMgr.
[dTPM]	Disables PTT in SkuMgr. **Warning! PTT/ dTPM will be disabled and all data saved on it will be lost.**

▶ ME Debug Configuration

This menu allows you to configure debug-related options for the Intel® Management Engine (ME). This menu will display when **ME State** is enabled.



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

- **HECI2 Interface Communication**

  This setting Adds/ Removes HECI2 device from PCI space.

- **KT Device**

  Enables or disables Key Transfer (KT) Device.

- **End of Post Message**

  Enables or disables End of Post Message sent to ME.

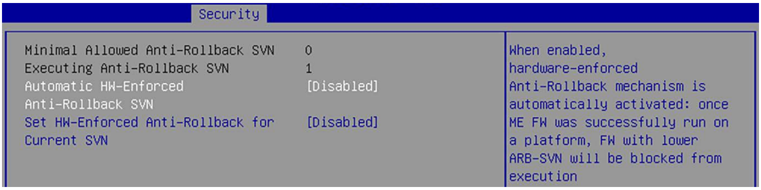
- **DOI3 Setting for HECI Disable**

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

- **MCTP Broadcast Cycle**

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

▶ Anti-Rollback SVN Configuration



```
                              Security

 Minimal Allowed Anti-Rollback SVN    0              When enabled,
 Executing Anti-Rollback SVN          1              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
```

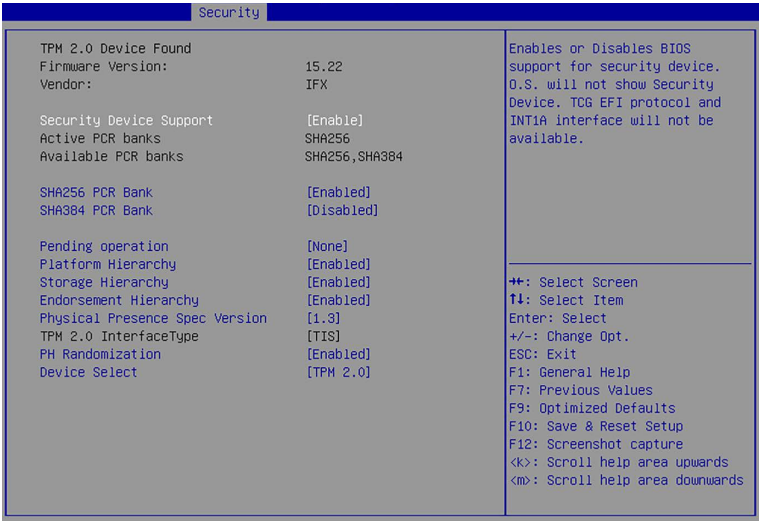
- **Automatic HW-Enforced Anti-Rollback SVN**

  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.

▶ Trusted Computing



```
                                Security

  TPM 2.0 Device Found                                      Enables or Disables BIOS
  Firmware Version:                  15.22                  support for security device.
  Vendor:                            IFX                    O.S. will not show Security
                                                            Device. TCG EFI protocol and
  Security Device Support            [Enable]               INT1A interface will not be
  Active PCR banks                   SHA256                 available.
  Available PCR banks                SHA256,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.
  PH Randomization                   [Enabled]              ESC: Exit
  Device Select                      [TPM 2.0]              F1: General Help
                                                            F7: Previous Values
                                                            F9: Optimized Defaults
                                                            F10: Save & Reset Setup
                                                            F12: Screenshot capture
                                                            <k>: Scroll help area upwards
                                                            <m>: Scroll help area downwards
```

▸ Security Device Support

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

▸ SHA256/ 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 selection.

▸ Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

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

▸ Physical Presence Spec Version

This settings show the Physical Presence Spec Version.

▸ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

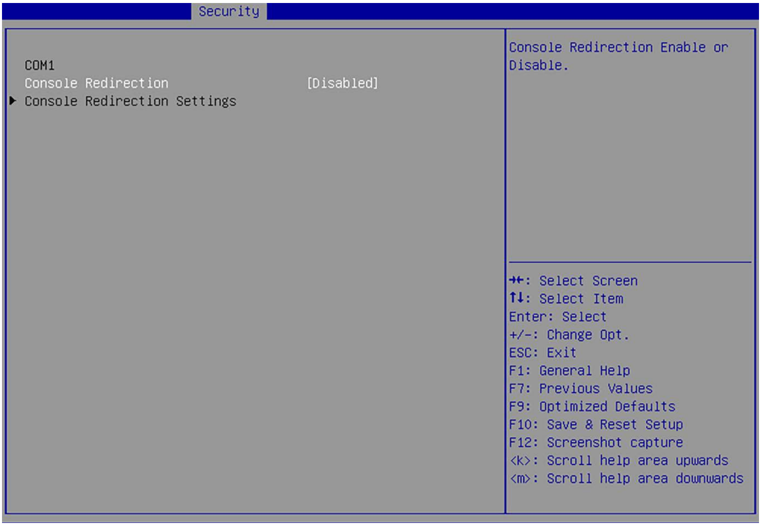
▸ PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

▸ Device Select

Select your TPM device through this setting.

▶ Serial Port Console Redirection

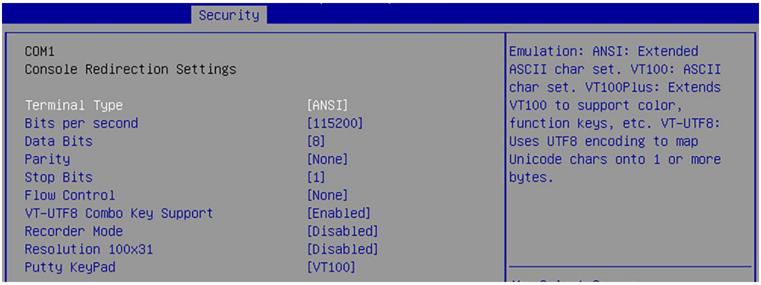


```
                              Security

  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
                                                    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)



```
COM1
Console Redirection Settings

Terminal Type                    [ANSI]
Bits per second                  [115200]
Data Bits                        [8]
Parity                           [None]
Stop Bits                        [1]
Flow Control                     [None]
VT-UTF8 Combo Key Support        [Enabled]
Recorder Mode                    [Disabled]
Resolution 100x31                [Disabled]
Putty KeyPad                     [VT100]
```

```
Emulation: ANSI: Extended
ASCII char set. VT100: ASCII
char set. VT100Plus: Extends
VT100 to support color,
function keys, etc. VT-UTF8:
Uses UTF8 encoding to map
Unicode chars onto 1 or more
bytes.
```

» Terminal Type

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

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

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

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

» Flow Control

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

» VT-UTF8 Combo Key Support

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

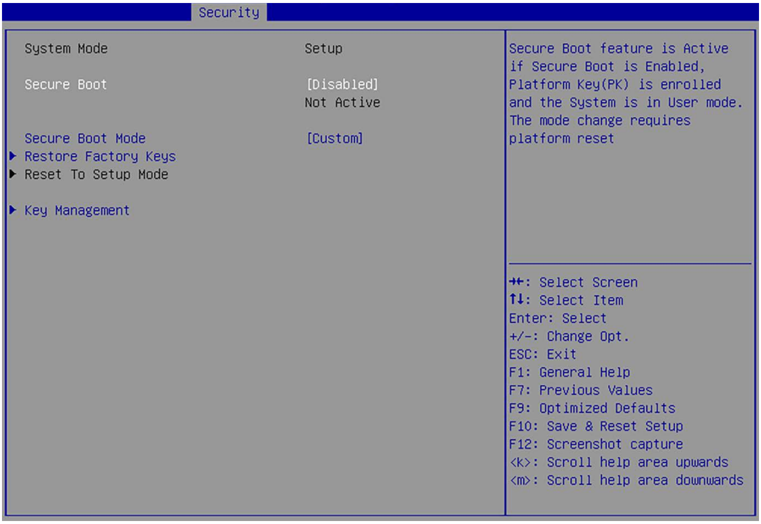
» Recorder Mode, Resolution 100x31

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

» Putty KeyPad

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

▶Secure Boot



```
                                  Security

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

▶ Key Management

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

▶ Secure Boot

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

▶ Secure Boot Mode

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

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

▶ Restore Factory Keys

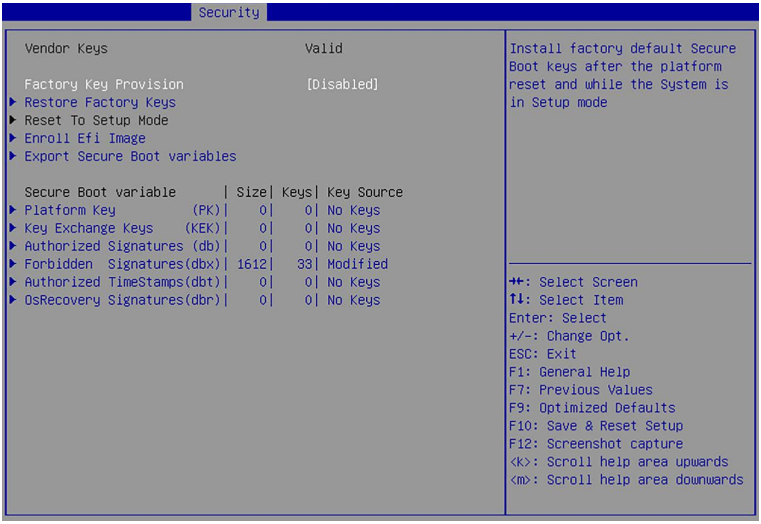
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▶ Reset to setup Mode

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

▸ **Key Management**

Press **Enter** key to enter the sub-menu. Manage the secure boot keys. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.



```
                              Security
 Vendor Keys                                   Valid              | Install factory default Secure
                                                                  | Boot keys after the platform
 Factory Key Provision                         [Disabled]         | reset and while the System is
▸ Restore Factory Keys                                            | in Setup mode
▸ Reset To Setup Mode                                             |
▸ Enroll Efi Image                                                |
▸ Export Secure Boot variables                                    |
                                                                  |
 Secure Boot variable       | Size| Keys| Key Source              |
▸ Platform Key          (PK)|    0|    0| No Keys                 |
▸ Key Exchange Keys    (KEK)|    0|    0| No Keys                 |
▸ Authorized Signatures (db)|    0|    0| No Keys                 |
▸ Forbidden  Signatures(dbx)| 1612|   33| Modified                |
▸ 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
                                                                  | F9: Optimized Defaults
                                                                  | F10: Save & Reset Setup
                                                                  | F12: Screenshot capture
                                                                  | <k>: Scroll help area upwards
                                                                  | <m>: Scroll help area downwards
```

» **Platform Key (PK):**

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

» **Set New Key**

Sets a new PK to your system.

» **Delete Key**

Deletes the PK from your system.

» **Key Exchange Keys (KEK):**

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

» **Set New Key**

Sets a new KEK to your system.

» **Append Key**

Loads an additional KEK from storage devices to your system.

» **Delete Key**

Deletes the KEK from your system.

» **Authorized Signatures (db) :**

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

» **Set New Key**

Sets a new db to your system.

- **Append Key**

  Loads an additional db from storage devices to your system.

- **Delete Key**

  Deletes the db from your system.

- **Forbidden Signatures (dbx):**

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

- **Set New Key**

  Sets a new dbx to your system.

- **Append Key**

  Loads an additional dbx from storage devices to your system.

- **Delete Key**

  Deletes the dbx from your system.

- **Authorized TimeStamps (dbt):**

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

- **Set New Key**

  Sets a new DBT to your system.

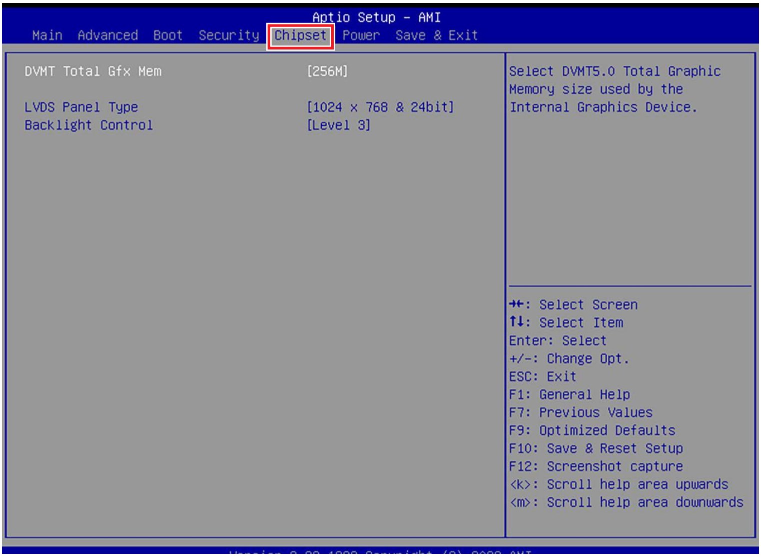
- **Append Key**

  Loads an additional DBT from storage devices to your system.

- **OsRecovery Singnatures (dbr):**

  Lists the available signatures for OS recovery.

Chipset



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

  DVMT Total Gfx Mem                  [256M]                  Select DVMT5.0 Total Graphic
                                                              Memory size used by the
  LVDS Panel Type                     [1024 x 768 & 24bit]    Internal Graphics Device.
  Backlight Control                   [Level 3]

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

               Version 2.20.1280 Copyright (C) 2020 AMI
```

▶ DVMT Total Gfx Mem

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

▶ LVDS Panel Type

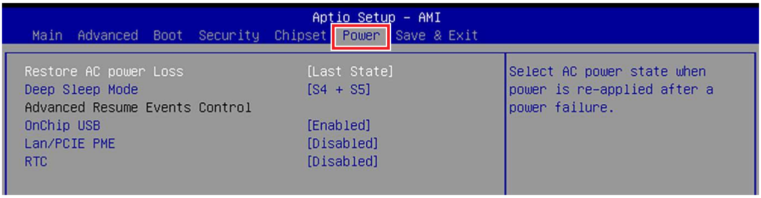
This setting specifies the LVDS Panel's resolution and distribution formats.

▶ Backlight Control

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

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

Power



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

▶ Restore AC Power Loss

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

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

▶ Deep Sleep Mode

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

▶ OnChip USB

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

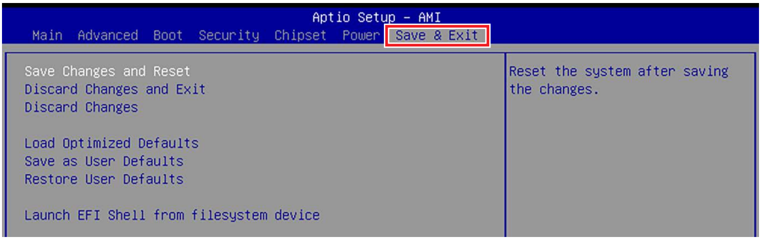
▶ LAN/ PCIE PME

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.

▶ RTC

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

Save & Exit



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

Load Optimized Defaults
Save as User Defaults
Restore User Defaults

Launch EFI Shell from filesystem device
```

▶ Save Changes and Reset

Save changes to CMOS and reset the system.

▶ Discard Changes and Exit

Abandon all changes and exit the Setup Utility.

▶ Discard Changes

Abandon all changes.

▶ Load Optimized Defaults

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

▶ Save as User Defaults

Save changes as the user’s default profile.

▶ Restore User Defaults

Restore the user’s default profile.

▶ Launch EFI Shell from filesystem device

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

GPIO WDT BKL SMBus Access Programming

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

Abstract

In this section, code examples based on C programming language provided for customer interest. **Inportb, Outportb, Inportl** and **Outportl** are basic functions used for access IO ports and defined as following.

Inportb: Read a single 8-bit I/O port.

Outportb: Write a single byte to an 8-bit port.

Inportl: Reads a single 32-bit I/O port.

Outportl: Write a single long to a 32-bit port.

General Purpose IO

1. General Purposed IO – GPIO/DIO

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

Name	IO Port	IO address	Name	IO Port	IO address
N_GPI0	0xA10	Bit 0	**N_GPO0**	0xA10	Bit 4
N_GPI1	0xA10	Bit 1	**N_GPO1**	0xA10	Bit 5
N_GPI2	0xA10	Bit 2	**N_GPO2**	0xA10	Bit 6
N_GPI3	0xA10	Bit 3	**N_GPO3**	0xA10	Bit 7

1.1 Set output value of GPO

1. Read the value from GPO port.
2. Set the value of GPO address.
3. Write the value back to GPO port.

Example: Set **N_GPO0** output “high”

```
val = Inportb (0xA10);          // Read value from N_GPO0 port.
val = val | (1<<4);             // Set N_GPO0 address (bit 4) to 1 (output “high”).
Outportb (0xA10, val);          // Write back to N_GPO0 port.
```

Example: Set **N_GPO1** output “low”

```
val = Inportb (0xA10);          // Read value from N_GPO1 port.
val = val & (~(1<<5));          // Set N_GPO1 address (bit 5) to 0 (output “low”).
Outportb (0xA10, val);          // Write back to N_GPO1 port.
```

1.2 Read input value from GPI

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

Example: Get **N_GPI2** input value.

```
val = Inportb (0xA10);          // Read value from N_GPI2 port.
val = val & (1<<2);             // Read N_GPI2 address (bit 2).
if (val)      printf (“Input of   N_GPI2   is High”);
else          printf (“Input of   N_GPI2   is Low”);
```

2. Watchdog Timer – WDT

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

2.1 Set WDT Time Unit

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

2.2 Set WDT Time

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

2.3 Enable WDT

```
val = Inportb (WDT_BASE + 0x0A);        // Read current WDT_PME setting
val = val | 0x01;                       // Enable WDT OUT: WDOUT_EN (bit 0) set to 1.
Outportb (WDT_BASE + 0x0A, val);        // Write back WDT setting.
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val | 0x20;                       // Enable WDT by set WD_EN (bit 5) to 1.
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting.
```

2.4 Disable WDT

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

2.5 Check WDT Reset Flag

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

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

2.6 Clear WDT Reset Flag

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

LVDS Backlight Control

3. LVDS Backlight Control – BKL

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

3.1 Set the Level of LVDS Backlight

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

Example 3: Set **LVDS backlight level to** “100%”

```
SMBus_WriteByte (0x42, 0x00, 0x0D)
SMBus_WriteByte (0x42, 0x35, 0xFF)
```

3.2 Read the Level of LVDS Backlight

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

Example 4: Get **LVDS backlight level**

```
SMBus_WriteByte(0x42, 0x00, 0x0D);
BKL_Value = SMBus_ReadByte(0x42, 0x35);
```

SMBus Access

4. SMBus Access

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

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

4.1 Get SMBus Base Address

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

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

4.2 SMBus_ReadByte (char DEVID, char offset)

Read the value of OFFSET from SMBus device DEVID.

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

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

Write DATA to OFFSET on SMBus device DEVID.

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