MS-9B05 WindBOX

Industrial Data Machine

msi

Copyright and Trademarks Notice

Revision History

Revision	Date
V1.3	2020/12

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 Instructions

- Always read the safety instructions carefully.
- Keep this User's Manual for future reference.
- Keep this equipment away from humidity.
- Lay this equipment on a reliable flat surface before setting it up.
- The openings on the enclosure are for air convection hence protects the equipment from overheating. DO NOT COVER THE OPENINGS.
- Make sure the voltage of the power source and adjust properly 110/220V before connecting the equipment to the power inlet.
- Place the power cord such a way that people can not step on it. Do not place anything over the power cord.
- Always Unplug the Power Cord before inserting any add-on card or module.
- All cautions and warnings on the equipment should be noted.
- Never pour any liquid into the opening that could damage or cause electrical shock.
- If any of the following situations arises, get the equipment checked by service personnel:
  - ▸ The power cord or plug is damaged.
  - ▸ Liquid has penetrated into the equipment.
  - ▸ The equipment has been exposed to moisture.
  - ▸ The equipment does not work well or you can not get it work according to User's Manual.
  - ▸ The equipment has dropped and damaged.
  - ▸ The equipment has obvious sign of breakage.
- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT UNCONDITIONED, STORAGE TEMPERATURE ABOVE 60ºC, IT MAY DAMAGE THE EQUIPMENT.

警告使用者:
此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

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://www.msi.com/html/popup/csr/evmtprtt_pcm.html

Battery Information

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.

Taiwan:

For better environmental protection, waste batteries should be collected separately for recycling or special disposal.

廢電池請回收

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:

https://www.dtsc.ca.gov/hazardouswaste/perchlorate/

Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.

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-A Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. 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. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

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

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.

CONTENTS

1 Overview

Thank you for choosing the MS-9B05, an excellent industrial data machine from MSI.

The MS-9B05's wide heatsink fanless solution eliminates the noise and the risk of fan failure. Furthermore, it supports VESA wall-mount interface for various scenarios like digital signage, kiosk, industrial control and POS with affordable expenditure, which not only meets the demand of Industrial applications but also fulfills the needs of companies, governments and institutes for general applications.

System Overview

➤ **System I/O & Controls**

1 **WiFi Antenna Connector (Optional)**
This connector allows you to connect an external antenna for wireless LAN.

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

3 **Extend Switch Connector**
This connector is provided for remote power button control.

4 **USB 3.2 Gen 1 Port (For SKU1)**
USB 3.2 Gen 1, the SuperSpeed USB, delivers up to 5Gbps high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

USB 3.2 Gen 2 Port (For SKU2)
USB 3.2 Gen 2, the SuperSpeed USB 10Gbps, delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

5 **RS232/422/485 Serial Port**

The serial port is a 16550A high speed communications port that sends/receives 16 bytes FIFOs. It supports barcode scanners, barcode printers, bill printers, credit card machine, etc.
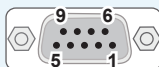
RS232

PIN	SIGNAL	DESCRIPTION
1	DCD	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	POWER	5V or 12V selected by GPIO (BIOS)

RS422

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

RS485

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

⑥ Mic-In Jack
Used as a connector for a microphone.

Line-In Jack (by AP driver)
Used for connecting external audio output devices.

⑦ S/PDIF-Out Jack
S/PDIF (Sony/Philips Digital Interface Format) is a type of digital audio interconnect used in consumer audio equipment, home theaters and other digital high-fidelity systems.

Line-Out Jack
This connector is provided for headphones or speakers.

⑧ DC Power Jack
Power supplied through this jack supplies power to the system.

⑨ Power Button
Press the button to turn the system on or off.

⑩ Hard Disk Drive LED
This indicator shows the activity status of the HDD. It flashes when the system is accessing data on the HDD and remains off when no disk activity is detected.

⑪ DVI-D Port (For SKU1)
The DVI-D (Digital Visual Interface-Digital) connector allows you to connect a monitor. It provides a high-speed digital interconnection between the computer and its display device.

⑫ DisplayPort (For SKU1)
DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

⑬ HDMI 1.4 Port HƏMI™
HIGH-DEFINITION MULTIMEDIA INTERFACE

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

⑭ USB 2.0 Port
The USB (Universal Serial Bus) port is for attaching USB devices such as keyboard, mouse, or other USB-compatible devices. It supports up to 480Mbit/s (Hi-Speed) data transfer rate.

15 **HDMI 2.0 Port** HƎMI HIGH-DEFINITION MULTIMEDIA INTERFACE **(For SKU2)**
The High-Definition Multimedia Interface (HDMI) is an all-digital audio/video interface capable of transmitting uncompressed streams. HDMI supports all TV format, including standard, enhanced, or high-definition video, plus multi-channel digital audio on a single cable.

16 **LTE Antenna Connector (Optional)**
This connector allows you to connect an external antenna for LTE.

System Specifications

Processor

- SKU1: 8th Gen Intel® Mobile Whiskey Lake-U Celeron® Processor, DC, 15W
- SKU2: 8th Gen Intel® Mobile Whiskey Lake-U Core™ i5 Processor, QC, 15W

Memory

- 2 x 260-pin SO-DIMM slots
- Support the maximum of 32GB
- SKU1: Dual-channel for DDR4 2133 MHz
- SKU2: Dual-channel for DDR4 2400 MHz

Network

- 1 x Intel® I219LM GbE LAN PHY
- 1 x Intel® I210-AT GbE LAN

Storage

- 1 x SATA 6 Gb/s, 2.5" HDD/SSD
- 1 x mSATA slot (shared with Mini PCIe)

Expansion Slot

- 1 x Half/Full-size Mini PCIe slot (w/ mSATA)
- 1 x Half/Full-size Mini PCIe slot (w/ Nano-SIM holder)
- SKU1
  - » 1 x M.2 E Key 2230 slot (2 x PCIe x1, USB 2.0)
  - » 1 x M.2 M Key 2242 slot (PCIe x4)
- SKU2
  - » 1 x M.2 E Key 2230 slot (2 x PCIe x1, USB 2.0)
  - » 1 x M.2 M Key 2242 slot (PCIe x4, SATA)

Important

- *MS-9B05 only supports installing ONE WiFi / BT module. Please install your WiFi / BT module to Mini PCIe slot1, Mini PCIe slot2 or M.2 E Key slot.*
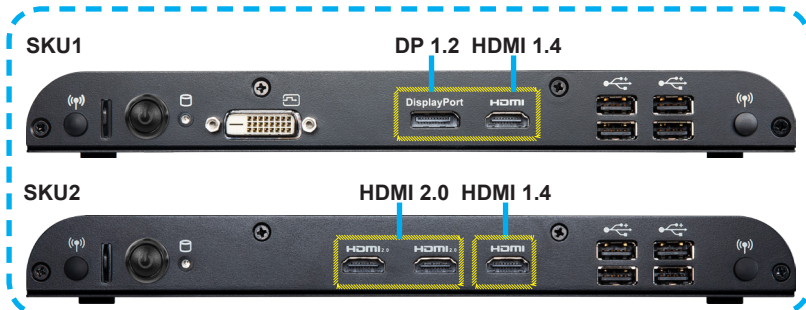
Audio

- Realtek® ALC887-VD2-CG HDA Codec
- Compliant with Azalia 1.0 specs

Graphics

- Intel® UHD Graphics 620
- Shared system memory up to 1.7 GB SDRAM
- 3 independent displays
- SKU1
  - » HDMI 1.4 up to 4096 x 2160 @24Hz
  - » DisplayPort 1.2 up to to 4096 x 2304 @60Hz
  - » DVI-D up to 1920 x 1200 @60Hz
- SKU2
  - » HDMI 2.0 up to 4096 x 2160 @60Hz
  - » HDMI 1.4 up to 4096 x 2160 @24Hz

Important

- *MS-9B05 supports **Collage Display Mode** with two independent displays.*

Check https://www.intel.com/content/www/us/en/support/articles/000006547/graphics-drivers.html for details.

- ***SKU2's HDMI 2.0 port does not support audio and hot plug.** To ensure proper operation of the HDMI 2.0 display, follow the instructions:*

  1. *Connect the HDMI cable from the display to the HDMI 2.0 port on the system left panel. Connect the display power cord.*

  2. *Disconnect the system power cord to ensure a complete system shutdown.*

  3. *Reconnect the system power cord and power on the system.*

  4. *Power on the display. The display should be able to work properly.*

Left Panel Input/Output

- 2 x WiFi Antenna Connectors (Optional)
- 1 x Power Button
- 1 x Hard Disk Drive LED
- 1 x DVI-D Port (For SKU1)
- 1 x DisplayPort (For SKU1)
- 1 x HDMI 1.4 Port
- 2 x HDMI 2.0 Ports (For SKU2)
- 4 x USB 2.0 Ports

Right Panel Input/Output

- 2 x WiFi Antenna Connectors (Optional)
- 2 x GbE RJ45 Ports
- 1 x Extend Switch Connector
- 2 x USB 3.2 Gen 1 Ports (For SKU1)
- 2 x USB 3.2 Gen 2 Ports (For SKU2)
- 2 x RS232/422/485 Serial Ports
- 1 x Mic-In Jack/ Line-In Jack (Line-In by AP driver)
- 1 x S/PDIF-Out Jack/ Line-Out Jack
- 1 x DC Power Jack

Power Supply

- DC-in 9~36V with Lockable DC Jack

Dimension & Weight

- 260 x 185 x 27mm
- 1.77 kg

OS Support

- Windows 10 IoT Enterprise LTSC/SAC 1809 (64-bit, RS5)
- Linux Ubuntu/ Linux Fedora (by request)

Regulatory Compliance

- EMC: FCC, CE, RCM, VCCI, BSMI
- Safety: BSMI, CE

Environment

- Operating Temperature:
  - » -10 ~ 50°C (SSD)
  - » -10 ~ 40°C (HDD)
- Storage Temperature: -20 ~ 80°C
- Humidity: 10 ~ 90% RH, non-condensing

Motherboard Jumpers
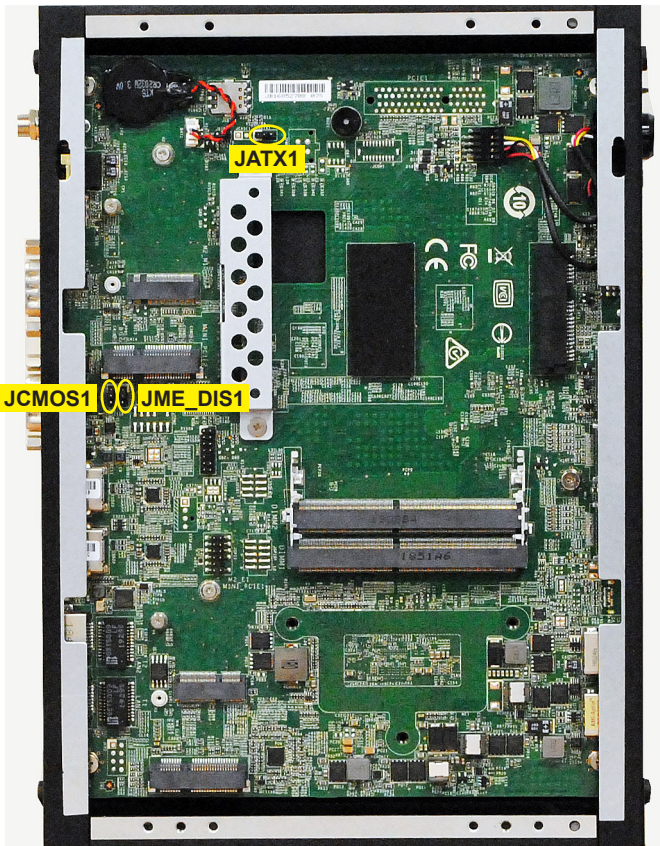
Jumper Name	Default Setting	Description	
JCMOS1	1	1-2: Normal	2-3: Clear CMOS
JATX1	1	1-2: ATX	2-3: AT
JME_DIS1	1	1-2: Normal	2-3: ME Disable

2 Getting Started

This chapter provides you with the information on hardware setup procedures. While doing the installation, be careful in holding the components and follow the installation procedures. For some components, if you install in the wrong orientation, the components will not work properly.

Use a grounded wrist strap before handling computer components. Static electricity may damage the components.

Important

Always unplug the power cord before installing any components.

System Internal View
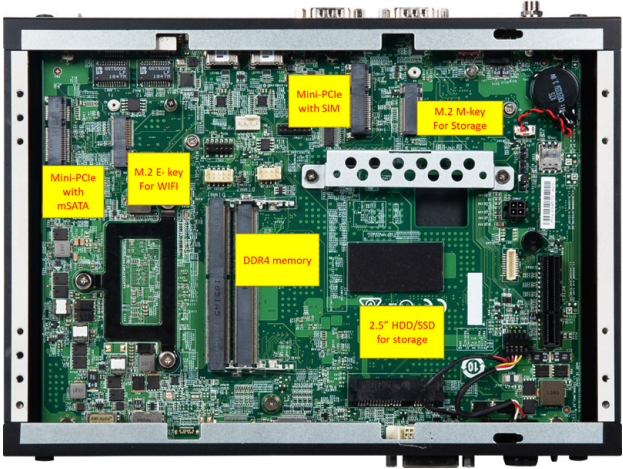
Memory

1. Locate the SO-DIMM slot.
2. Align the notch on the DIMM with the key on the slot and insert the DIMM into the slot at a 45-degree angle.
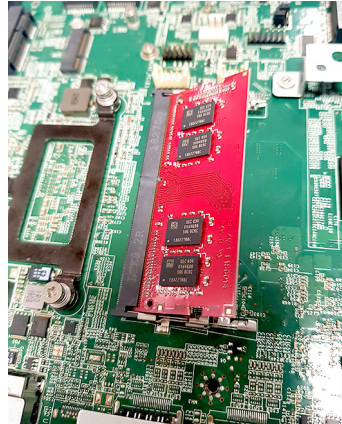
3. Push the DIMM gently downwards until the slot levers click and lock the DIMM in place.
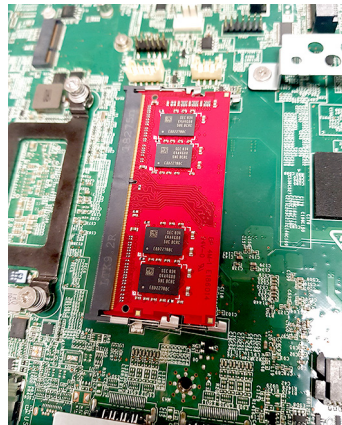
Important

• *You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.*
• *To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.*

M.2 Slot

1. Locate the M.2 slot. Remove the M.2 card screw preinstalled on the motherboard.
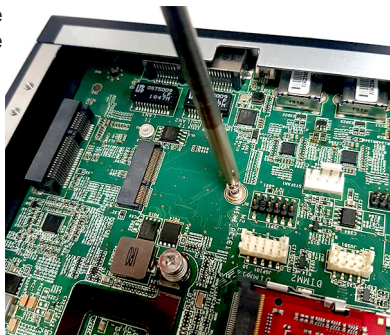
2. Insert the card into the slot at a 45-degree angle.
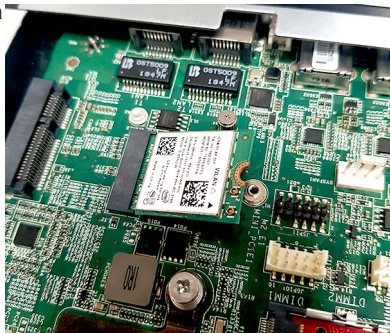
3. Push the card gently downwards and fasten it with a screw.
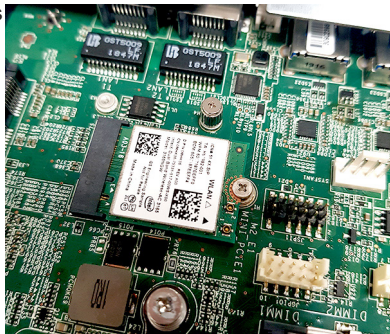
Mini-PCIe Slot

1. Locate the Mini-PCIe slot. Remove the Mini-PCIe card screw preinstalled on the motherboard.
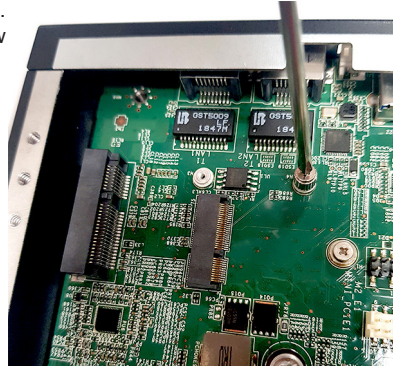
2. Insert the card into the slot at a 45-degree angle.
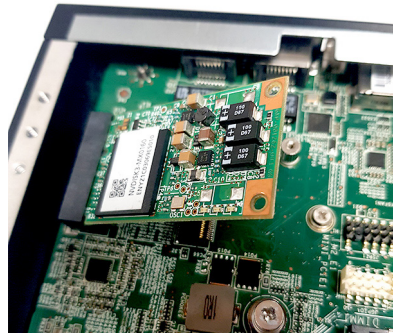
3. Push the card gently downwards and fasten it with a screw.
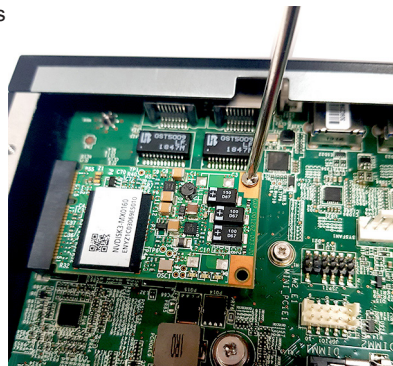
2.5" HDD/SSD

1. Unscrew the HDD bracket and remove it from the system; then, paste the thermal pad.
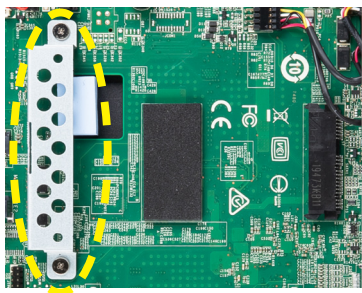
2. Fix the HDD and bracket with screws.

3. Align the SATA data & power connectors and connect the HD to the system.
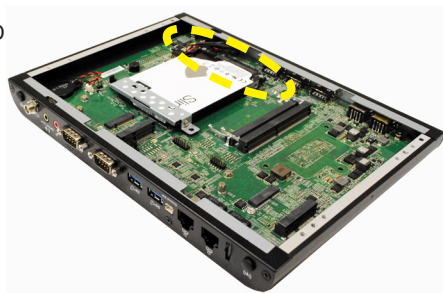
4. Fasten the HDD module to the system with 2 screws.

Wall Mount (Optional)

1. Flip over the system and locate the screw holes for wall mount brackets.

2. Assemble the wall mount brackets by inserting the rubber pads into the bracket holes and then inserting the screws.
3. Place the wall mount brackets along the sides of the system with screw holes aligned.
4. Fasten the screws to fix the wall mount brackets to the system.
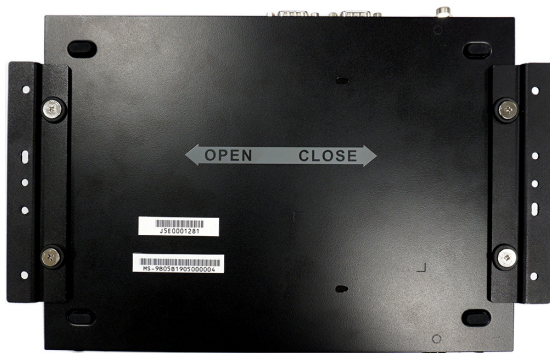
DIN Rail Mount 1 (Optional)

1. Install the wall mount brackets.
2. Put the DIN rails on the wall mount brackets with screw holes aligned.
3. Insert screws through the wall mount brackets into the DIN rails and tighten until each DIN rail is secure.
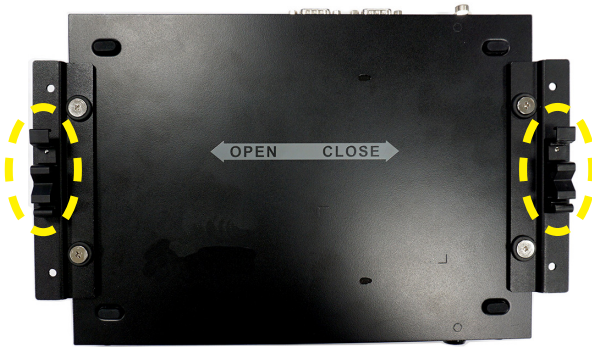
DIN Rail Mount 2 (Optional)

1. Check the VESA mount plate for the DIN rail screw holes.

2. Put the DIN rails on the VESA mount plate with screw holes aligned.

3. Insert screws through the VESA mount plate into the DIN rails and tighten until each DIN rail is secure.

4. Mount the VESA mount plate onto the system and tighten the thumbscrew of the VESA mount plate.

VESA Mount

1. Locate the VESA mount screw holes on the intended device.
2. Fasten the VESA mount plate to the device with the supplied screws.
3. Mount the system onto the VESA mount plate.
4. Tighten the thumbscrew at the bottom of the VESA mount plate to secure the system.

3 **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.

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 Option
F1	General Help
F7	Previous Values
F9	Optimized Defaults
F10	Save & Reset
Esc	Exit

Getting Help

After entering the Setup menu, the first menu you will see is the Main Menu.

Main Menu

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

Sub-Menu

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

General Help <F1>

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

The Menu Bar
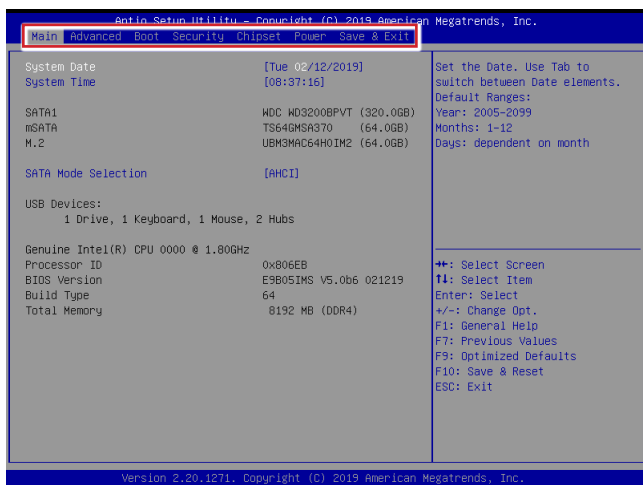
▸**Main**

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

▸**Advanced**

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

▸**Boot**

Use this menu to specify the priority of boot devices.

▸**Security**

Use this menu to set supervisor and user passwords.

▸**Chipset**

This menu controls the advanced features of the 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 Utility - Copyright (C) 2019 American Megatrends, Inc.
  Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

  System Date                    [Tue 02/12/2019]      Set the Date. Use Tab to
  System Time                    [08:37:16]            switch between Date elements.
                                                       Default Ranges:
  SATA1                          WDC WD3200BPVT (320.0GB)  Year: 2005-2099
  mSATA                          TS64GMSA370   (64.0GB)    Months: 1-12
  M.2                            UBM3MAC64H0IM2 (64.0GB)   Days: dependent on month

  SATA Mode Selection            [AHCI]

  USB Devices:
       1 Drive, 1 Keyboard, 1 Mouse, 2 Hubs

  Genuine Intel(R) CPU 0000 @ 1.80GHz
  Processor ID                   0x806EB             ++: Select Screen
  BIOS Version                   E9B05IMS V5.0b6 021219  ↑↓: Select Item
  Build Type                     64                  Enter: Select
  Total Memory                   8192 MB (DDR4)      +/-: Change Opt.
                                                     F1: General Help
                                                     F7: Previous Values
                                                     F9: Optimized Defaults
                                                     F10: Save & Reset
                                                     ESC: Exit

                  Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.
```

‣ **System Date**

This setting allows you to set the system date. The date format is <Day>, <Month> <Date> <Year>.

‣ **System Time**

This setting allows you to set the system time. The time format is <Hour> <Minute> <Second>.

‣ **SATA Mode Selection**

This setting specifies the SATA controller mode.

Advanced
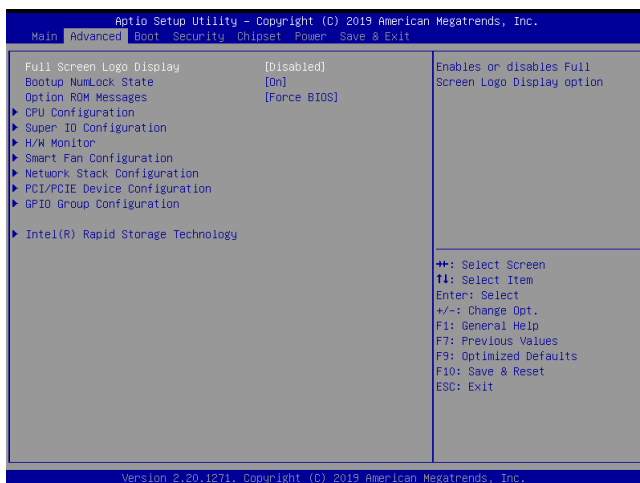
▸ **Full Screen Logo Display**

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

When it is enabled, the BIOS will display the full-screen logo during the boot-up sequence, hiding normal POST messages.

When it is disabled, the 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 of delay to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, it is recommended that you disable this BIOS feature for a faster boot-up time.

▸ **Bootup NumLock State**

This setting is to set the Num Lock status when the system is powered on. Setting to [On] will turn on the Num Lock key when the system is powered on. Setting to [Off] will allow users to use the arrow keys on the numeric keypad.

▸ **Option ROM Messages**

This item is used to determine the display mode when an optional ROM is initialized during POST. When set to [Force BIOS], the display mode used by AMI BIOS is used. Select [Keep Current] if you want to use the display mode of optional ROM.

▶ **CPU Configuration**

```
        Advanced
  CPU Configuration

  Genuine Intel(R) CPU 0000 @ 1.80GHz
  Processor ID                    0x806EB
  Processor Speed                 2000 MHz
  L2 Cache                        256 KB x 4
  L3 Cache                        8 MB

  Intel Virtualization Technology [Enabled]
  Active Processor Cores          [All]
  Hyper-Threading                 [Enabled]
  Intel(R) SpeedStep(tm)          [Enabled]
  C states                        [Enabled]
```
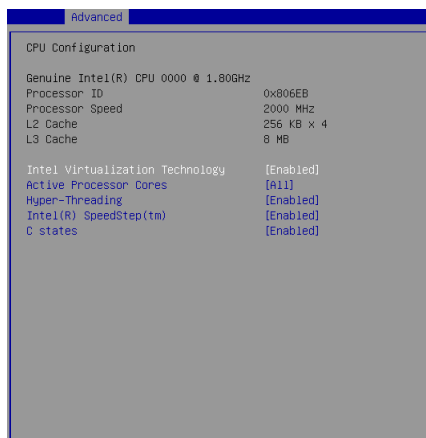
▶ **Intel Virtualization Technology**

Virtualization enhanced by Intel Virtualization Technology will allow a platform to run multiple operating systems and applications in independent partitions. With virtualization, one computer system can function as multiple "Virtual" systems.

▶ **Active Processor Cores**

This setting specifies the number of active processor cores.

▶ **Hyper-Threading**

The processor uses Hyper-Threading technology to increase transaction rates and reduces end-user response times. The technology treats the two cores inside the processor as two logical processors that can execute instructions simultaneously. In this way, the system performance is highly improved. If you disable the function, the processor will use only one core to execute the instructions. Please disable this item if your operating system doesn□ support HT Function, or unreliability and instability may occur.

▶ **Intel(R) SpeedStep(tm)**

EIST (Enhanced Intel SpeedStep Technology) allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. When disabled, the processor will return the actual maximum CPUID input value of the processor when queried.

▶ **C States**

This setting controls the C-State (CPU Power state). C-State performance indicates the ability to run the processor in lower power states when the PC is idle. This setting enables/disables the C-State Configuration for power saving purposes.

▶ **Super IO Configuration**
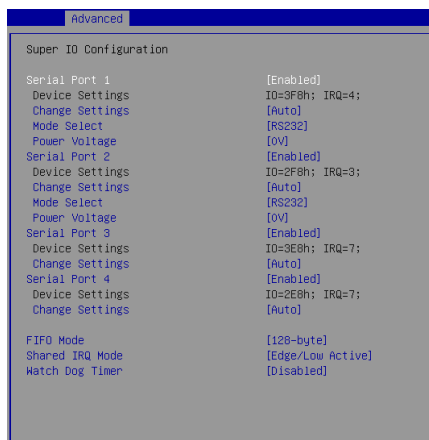
▶ **Serial Port 1/ 2/ 3/ 4**

This setting enables/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 the specified serial port.

▶ **FIFO Mode**

This setting controls the FIFO 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 watch-dog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watch dog polls it.

▸ **H/W Monitor**

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              [Disabled]

CPU temperature               : +36 C
System temperature            : +24 C

SYSFAN1                       : N/A

VCC_CORE                      : +0.736 V
VCC3                          : +3.279 V
VCC5                          : +5.003 V
+12V                          : +12.144 V
VSB3V                         : +3.280 V
VSB5V                         : +4.992 V
VBAT                          : +3.040 V
```

▸ **Thermal Shutdown**

This setting enables/disables the thermal shutdown function for system thermal protection.

▸ **Smart Fan Configuration**

```
  Advanced

Configuration Smart FAN

SYSFAN1                       [Disabled]
 Type                         [4 Pin]
```

▸ **SYSFAN1**

This setting enables/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.

▶ **Type**

This setting specifies the fan type.

▶ **Network Stack Configuration**

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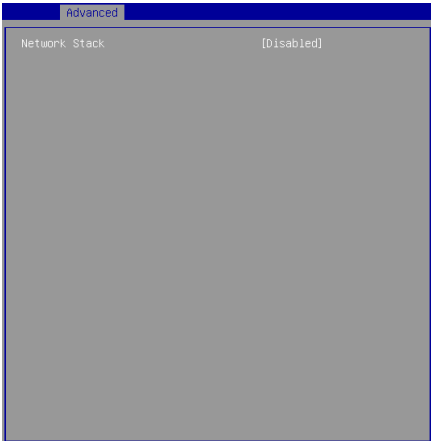
▶ **Network Stack**

When this setting is set to [Enabled], the system will boot via the network instead of a disk drive.

▶ **PCI/PCIE Device Configuration**
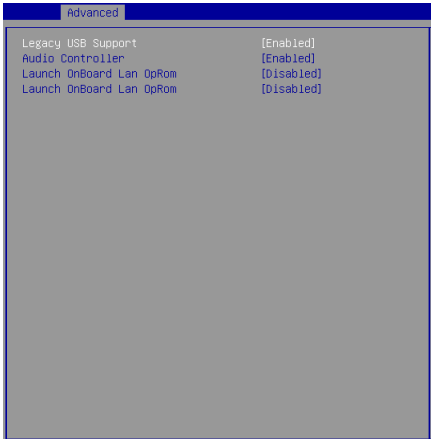
▶ **Legacy USB Support**

Set to [Enabled] if you need to use any USB 1.1/2.0 device in the operating system that does not support or have any USB 1.1/2.0 driver installed, such as DOS and SCO Unix.

▸ **Audio Controller**

This setting enables/disables the onboard audio controller.

▸ **Launch OnBoard LAN OpROM**

These settings enable/disable the initialization of the onboard/onchip LAN Boot ROM during bootup. Selecting [Disabled] will speed up the boot process.

▸ **GPIO Group Configuration**
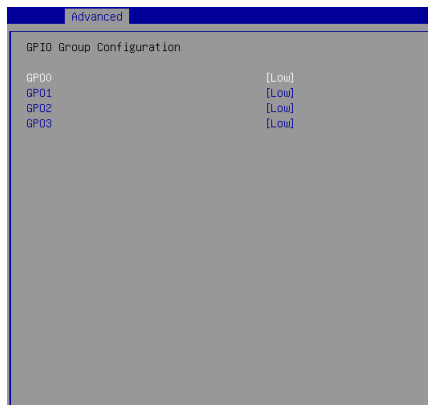
▸ **GPO0 ~ GPO3**

These settings control the operation mode of the specified GPIO.

▸ **Intel(R) Rapid Storage Technology**

Intel® Rapid Storage Technology offers greater levels of performance, responsiveness, and expandability of systems where one or multiple serial ATA (SATA) or PCIe drives are installed. When using one or multiple disks, users can take advantage of enhanced performance and lower power consumption. Also, when using multiple disks, users can have added protection against data loss in the event of a hard drive failure.
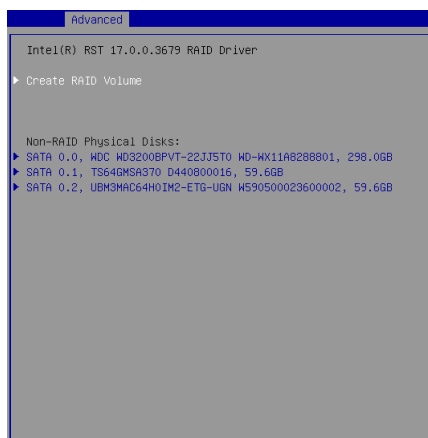
Boot
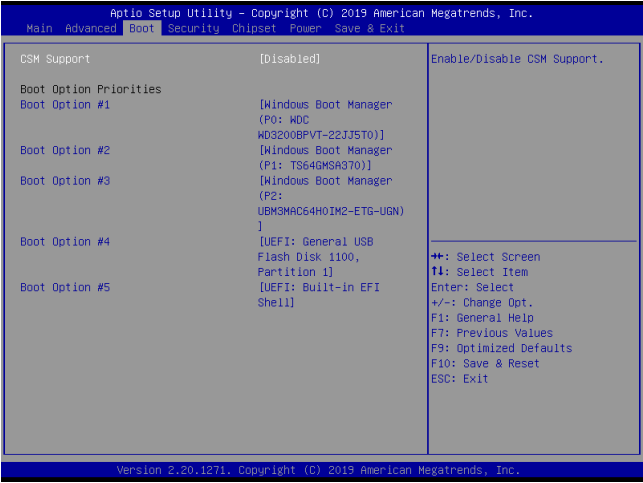
▸ **CSM Support**

This setting enables/disables the support for Compatibility Support Module, a part of the Intel Platform Innovation Framework for EFI providing the capability to support legacy BIOS interfaces.

▸ **Boot Option Priorities**

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

Security
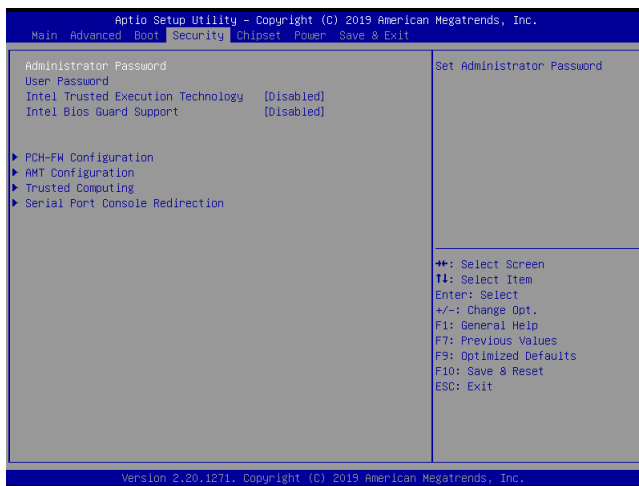
▸ **Administrator Password**

Administrator Password controls access to the BIOS Setup utility.

▸ **User Password**

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

▸ **Intel Trusted Execution Technology**

Intel Trusted Execution Technology provides highly scalable platform security in physical and virtual infrastructures.

▸ **Intel BIOS Guard Support**

Intel BIOS Guard Support ensures that updates to system BIOS flash are secure.

▶ **PCH-FW Configuration**
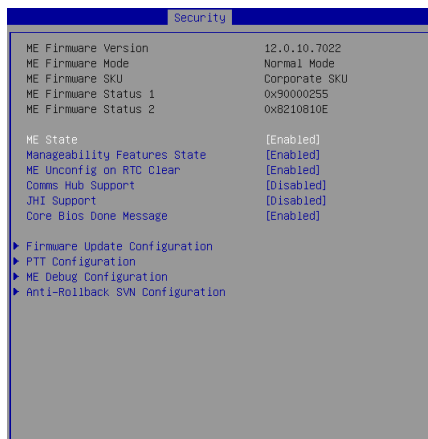
▶ **ME Firmware Version, ME Firmware Mode, ME Firmware SKU, ME Firmware Status 1, ME Firmware Status 2**

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

▶ **ME State**

This setting enables/disables the ME status.

▶ **Manageability Features State**

This setting enables/disables the Manageability Features State.

▶ **ME Unconfig on RTC Clear**

This setting enables/disables ME firmware unconfigure on RTC clear.

▶ **Comms Hub Support**

This setting enables/disables Communications Hub Support.

▶ **JHI Support**

This setting enables/disables support for Intel Dynamic Application Loader Host Interface (JHI).

▶ **Core BIOS Done Message**

This setting enables/disables Core BIOS Done Message sent to ME..

▶ **Firmware Update Configuration**

```
                        Security
 Me FW Image Re-Flash              [Disabled]
```

▶ **ME FW Image Re-Flash**

This setting enables/disables the ME FW image reflash.

▶ **PTT Configuration**

Intel Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.

```
                        Security
 PTT Capability / State            1 / 0

 TPM Device Selection              [dTPM]
```

▸ **ME Debug Configuration**

```
                    Security
HECI Timeouts                      [Enabled]

Force ME DID Init Status           [Disabled]
CPU Replaced Polling Disable       [Disabled]
ME DID Message                     [Enabled]
HECI Retry 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]
```

▸ **Anti-Rollback SVN Configuration**

```
                    Security
Minimal Allowed Anti-Rollback SVN    1
Executing Anti-Rollback SVN          4
Automatic HW-Enforced              [Disabled]
Anti-Rollback SVN
Set HW-Enforced Anti-Rollback for  [Disabled]
Current SVN
```

▸ **AMT Configuration**

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

```
                    Security
ASF support                        [Enabled]

USB Provisioning of AMT            [Disabled]
▶ CIRA Configuration
▶ ASF Configuration
▶ Secure Erase Configuration
▶ OEM Flags Settings
▶ MEBx Resolution Settings
```
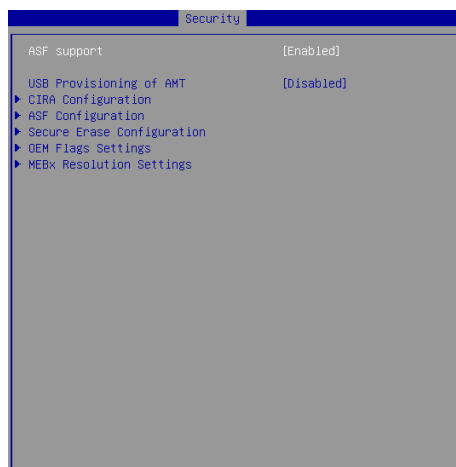
▸ **Trusted Computing**

```
                    Security
TPM20 Device Found
Firmware Version:                  5.63
Vendor:                            IFX

Security Device Support            [Enable]
Active PCR banks                   SHA-1,SHA256
Available PCR banks                SHA-1,SHA256

SHA-1 PCR Bank                     [Enabled]
SHA256 PCR Bank                    [Enabled]

Pending operation                  [None]
Platform Hierarchy                 [Enabled]
Storage Hierarchy                  [Enabled]
Endorsement Hierarchy              [Enabled]
TPM2.0 UEFI Spec Version           [TCG_2]
Physical Presence Spec Version     [1.3]
TPM 20 InterfaceType               [TIS]
```

▸ **Security Device Support**

This setting enables/disables BIOS support for security device. When set to [Disable], the OS will not show security device. TCG EFI protocol and INT1A interface will not be available.

▸ **SHA-1 PCR Bank, SHA256 PCR Bank**

These settings enable/disable the SHA-1 PCR Bank and SHA256 PCR Bank.

▶ **Pending Operation**

When *Security Device Support* is set to [Enable], *Pending Operation* will appear. Set this item to [TPM Clear] to clear all data secured by TPM or [None] to discard the selection. It is advised that users should routinely back up their TPM secured data.

▶ **Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy**

These settings enable/disable the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

▶ **TPM2.0 UEFI Spec Version, Physical Presence Spec Version**

This settings show the TPM2.0 UEFI Spec Version and Physical Presence Spec Version.

▶ **TPM2.0 Interface Type**

This setting shows the TPM2.0 Interface Type.

▶ **Serial Port Console Redirection**
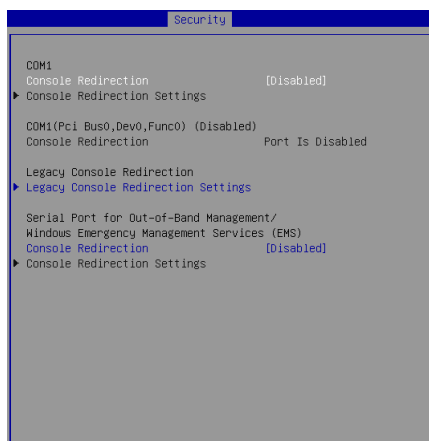
COM1

▶ **Console Redirection**

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables/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**

▶ **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). This setting specifies the type of terminal device for console redirection.

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

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

▶ **Recorder Mode, Resolution 100x31**

These settings enable/disable 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.

Legacy Console Redirection

▶ **Legacy Console Redirection Settings**

```
                        Security
Legacy Console Redirection Settings

Redirection COM Port              [COM1]
Resolution                        [80x24]
Redirect After POST               [Always Enable]
```

▶ **Redirection COM Port**

This setting specifies the COM port for redirection.

▶ **Resolution**

This setting specifies the redirection resolution of legacy OS.

▶ **Redirect After POST**

This setting determines whether or not to keep terminals' console redirection running after the POST has booted.

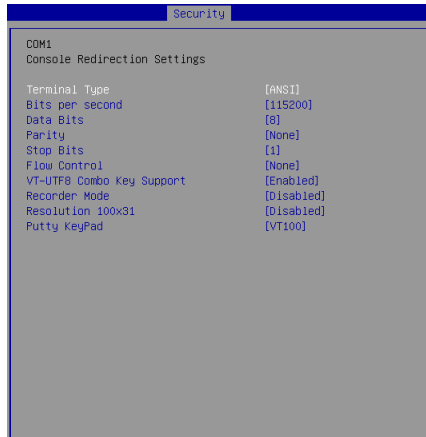**Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS)**

▶ **Console Redirection**

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables/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**
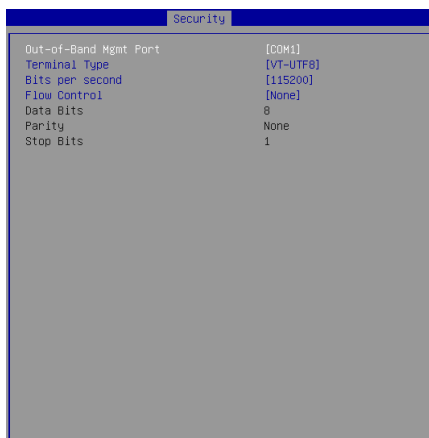
▶ **Out-of-Band Mgmt Port**

This setting specifies the Out-of-Band Management Port.

▶ **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). This setting specifies the type of terminal device for console redirection.

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

This 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.

Chipset

```
                Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc.
     Main  Advanced  Boot  Security  Chipset  Power  Save & Exit

  DVMT Total Gfx Mem               [256M]                    Select DVMT5.0 Total Graphic
  Primary IGFX Boot Display        [VBIOS Default]           Memory size used by the
                                                             Internal Graphics Device.




                                                             →←: Select Screen
                                                             ↑↓: Select Item
                                                             Enter: Select
                                                             +/-: Change Opt.
                                                             F1: General Help
                                                             F7: Previous Values
                                                             F9: Optimized Defaults
                                                             F10: Save & Reset
                                                             ESC: Exit




                Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.
```

▶ **DVMT Total Gfx Mem**

This setting specifies the memory size for DVMT.

▶ **Primary IGFX Boot Display**

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

Power
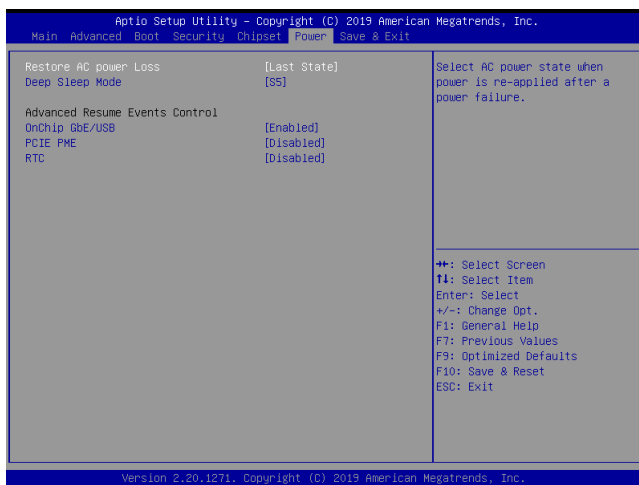
▸ **Restore AC Power Loss**

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

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

▸ **Deep Sleep Mode**

The setting enables/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.

** Advanced Resume Events Control **

▸ **OnChip GbE/USB**

This field specifies whether the system will be awakened from power saving modes when activity or input signal of onchip LAN or USB devices is detected.
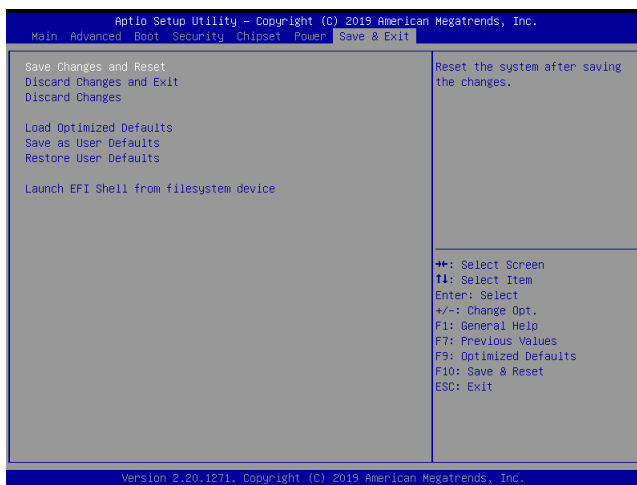
▸ **PCIE PME**

This field specifies whether the system will be awakened from power saving modes when activity or input signal of 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

```
               Aptio Setup Utility - Copyright (C) 2019 American Megatrends, Inc.
       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.
                                                        F1: General Help
                                                        F7: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset
                                                        ESC: Exit


               Version 2.20.1271. Copyright (C) 2019 American Megatrends, Inc.
```

▸ **Save Changes and Reset**

Save changes to CMOS and reset the system.

▸ **Discard Changes and Exit**

Abandon all changes and exit the Setup Utility.

▸ **Discard Changes**

Abandon all changes.

▸ **Load Optimized Defaults**

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

▸ **Save as User Defaults**

Save changes as the user's default profile.

▸ **Restore User Defaults**

Restore the user's default profile.

▸ **Launch EFI Shell from filesystem device**

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

Appendix
GPIO WDT Programming

This appendix provides WDT (Watch Dog Timer) and GPIO (General Purpose Input/ Output) programming guide.

Abstract

In this document, 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 Purposed IO

1. General Purposed IO – GPIO/DIO

The GPIO port configuration addresses listed in the following table:

Name	IO Port	IO address	Name	IO Port	IO address
N_GPI0	0xA05	Bit 3	N_GPO0	0xA05	Bit 0
N_GPI1	0xA05	Bit 4	N_GPO1	0xA05	Bit 7
N_GPI2	0xA05	Bit 5	N_GPO2	0xA05	Bit 2
N_GPI3	0xA05	Bit 6	N_GPO3	0xA05	Bit 1

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 (0xA05);          // Read value from N_GPO0 port.
val = val | (1<<0);             // Set N_GPO0 address (bit 0) to 1 (output "high").
Outportb (0xA05, val);          // Write back to N_GPO0 port.
```

Example: Set **N_GPO1** output "low"

```
val = Inportb (0xA05);          // Read value from N_GPO1 port.
val = val & (~(1<<7));          // Set N_GPO1 address (bit 7) to 0 (output "low").
Outportb (0xA05, 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 (0xA05);          // Read value from N_GPI2 port.
val = val & (1<<5);             // Read N_GPI2 address (bit 5).
if (val)     printf ("Input of    N_GPI2    is High");
else         printf ("Input of    N_GPI2    is Low");
```

Watchdog Timer

2. Watchdog Timer – WDT

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

2.1   Set WDT Time Unit

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

2.2   Set WDT Time

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

2.3   Enable WDT

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

2.4   Disable WDT

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

2.5   Check WDT Reset Flag

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

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

2.6   Clear WDT Reset Flag

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