SI-642

4K Signage Player with Intel® HD Graphics 620

User's Manual

Version 1.0
(February 2021)

iBASE

Copyright

Disclaimer

IBASE reserves the right to make changes and improvements to the products described in this document without prior notice. Every effort has been made to ensure the information in the document is correct; however, IBASE does not guarantee this document is error-free. IBASE assumes no liability for incidental or consequential damages arising from misapplication or inability to use the product or the information contained herein, nor for any infringements of rights of third parties, which may result from its use.

Trademarks

All the trademarks, registrations and brands mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

Compliance

CE

In a domestic environment, this product may cause radio interference in which case users may be required to take adequate measures.

FC

This product has been tested and found to comply with the limits for a Class B 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 manufacturer's instructions, may cause harmful interference to radio communications.

WEEE

This product must not be disposed of as normal household waste, in accordance with the EU directive of for waste electrical and electronic equipment (WEEE - 2012/19/EU). Instead, it should be disposed of by returning it to a municipal recycling collection point. Check local regulations for disposal of electronic products.

Green IBASE

This product is compliant with the current RoHS restrictions and prohibits use of the following substances in concentrations exceeding 0.1% by weight (1000 ppm) except for cadmium, limited to 0.01% by weight (100 ppm).

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent chromium (Cr6+)
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ether (PBDE)

iBASE

Important Safety Information

Carefully read the precautions before using the device.

Environmental conditions:

- Lay the device horizontally on a stable and solid surface in case the device may fall, causing serious damage.
- Leave plenty of space around the device and do not block the openings for ventilation. NEVER DROP OR INSERT ANY OBJECTS OF ANY KIND INTO THE VENTIILATION OPENINGS.
- Use this product in environments with ambient temperatures between 0˚C and 45˚C.
- DO NOT LEAVE THIS DEVICE IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY IS BELOW -20° C OR ABOVE 80° C. This could damage the device. The device must be used in a controlled environment.

Care for your IBASE products:

- Before cleaning the device, turn it off and unplug all cables such as power in case a small amount of electrical current may still flow.
- Use neutral cleaning agents or diluted alcohol to clean the device chassis with a cloth. Then wipe the chassis with a dry cloth.
- Vacuum the dust with a computer vacuum cleaner to prevent the air vent or slots from being clogged.

WARNING

Attention during use:

- Do not place heavy objects on the top of the device.
- Operate this device from the type of power indicated on the marking label. If you are not sure of the type of power available, consult your distributor or local power company.
- Do not walk on the power cord or allow anything to rest on it.
- If you use an extension cord, make sure that the total ampere rating of the product plugged into the extension cord does not exceed its limits.

Avoid Disassembly

Do not disassemble, repair or make any modification to the device. Doing so could generate hazards and cause damage to the device, even bodily injury or property damage, and will void any warranty.

CAUTION

There is danger of explosion if internal lithium-ion battery is replaced by an incorrect type. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Warranty Policy

- **IBASE standard products:**

  24-month (2-year) warranty from the date of shipment. If the date of shipment cannot be ascertained, the product serial numbers can be used to determine the approximate shipping date.

- **3rd-party parts:**

  12-month (1-year) warranty from delivery for the 3rd-party parts that are not manufactured by IBASE, such as CPU, CPU cooler, memory, storage devices, power adapter, panel and touchscreen.

* PRODUCTS, HOWEVER, THAT FAIL DUE TO MISUSE, ACCIDENT, IMPROPER INSTALLATION OR UNAUTHORIZED REPAIR SHALL BE TREATED AS OUT OF WARRANTY AND CUSTOMERS SHALL BE BILLED FOR REPAIR AND SHIPPING CHARGES.

Technical Support & Services

1. Visit the IBASE website at www.ibase.com.tw to find the latest information about the product.
2. If you need any further assistance from your distributor or sales representative, prepare the following information of your product and elaborate upon the problem.

   - Product model name
   - Product serial number
   - Detailed description of the problem
   - The error messages in text or in screenshots if there is any
   - The arrangement of the peripherals
   - Software in use (such as OS and application software, including the version numbers)

3. If repair service is required, you can download the RMA form at http://www.ibase.com.tw/english/Supports/RMAService/. Fill out the form and contact your distributor or sales representative.

iBASE

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Packing List
- Accessories
- Specifications
- Product View
- Dimensions

1.1 Introduction

The SI-642-N is a 4K digital signage player that leverages the 8th Gen Intel® Core™ U-series processors. The platform can be installed in restaurant as a menu board player or used in commercial establishments to increase brand awareness and customer engagement or deployed in transportation networks to provide real-time information and advertising relevant to the traveler.

The fanless SI-642-N offers high performance and high reliability for 24/7 operation in an industrial-grade design. It is integrated with the IBASE iSMART and Observer technologies for remote monitoring, power on/off scheduling, power recovery and low temperature boot functions. With the Intel HD Graphics 620, the system can simultaneously support two independent displays (1x HDMI 2.0 & 1x Active DisplayPort 1.2) with 4K (4096 x 2160) @60Hz resolution as well as two independent audio outputs.

The SI-642-N houses the MBD642 motherboard populated with dual Gigabit LAN, 4x USB 3.1, dual channel DDR4 with up to 32GB support and expansion slots including M.2 3042 B-key for 4G/LTE, M.2 2280 M-key for storage and M.2 2240 E-key to install optional WiFi or capture cards. It also has the Intel vPro and TPM 2.0 features to deliver increased productivity, remote manageability and data security.

1.2 Features

- iSMART energy-saving & Observer remote monitoring technologies
- 8th Gen Intel® Core™ U-series processor
- 1x HDMI 2.0 + 1x Active DisplayPort 1.2 with independent audio output
- 2x DDR4 2400 SO-DIMM, dual channel, Max. 32GB
- 1x M.2 B-Key (3042) for 4G LTE
- 1x M.2 M-key (2280) for storage
- 1x M.2 E-key (2230) for WiFi or capture card option
- TPM 2.0, vPro and watchdog timer
- Slim & compact fanless design

1.3 Packing List

Your product package should include the items listed below. If any of the items below is missing, contact the distributor or the dealer from whom you purchased the product.

- SI-642 Digital Signage Player
- Power Adaptor
- Power Cord

1.4 Specifications

Product	SI-642
System	
Mainboard	MBD642
Operating System	Windows 10
CPU	Intel® 8th Gen. Intel Core™ mobile processor
Chipset	H110 PCH
Memory	2 x DDR4 SO-DIMM 2400 MHz, Max 32GB
Graphics	Intel® UHD Graphics 620
LAN Controller	1x Intel® I219LM Gigabit LAN 1x Intel® I211AT Gigabit LAN
Expansion Slots	1x B-Key (3042) for 4G LTE 1x M-key (2280) for storage 1x E-key (2230) for capture card option
Power Requirement	+12V DC
Watchdog	**Watchdog Timer 256 segments, 0, 1, 2…255 sec/min**
Chassis	**Aluminum, black & white**
Mounting	**Slim design with wall mount bracket**
Dimensions (W x H x D)	**175 x 116x 30 mm (6.88” x 4.56” x 1.18”)**

Net Weight	**1 kg**
Certificate	**CE, FCC class B, UL, CCC**
I/O Ports	
Power Jack	**1 x DC-In power jack**
Power Button	**1 X Power Button (P/N: C261050104DTSA100P)**
Display Interface	• **1 x HDMI 1.4** • **1x Active DisplayPort 1.2**
LAN	**2 x RJ45 GbE LAN**
Serial	**1 x COM RS-232 port (RJ50 connector)**
USB	**4 x USB 3.1**
Audio Jack	**1 x Line-Out**
Environment	
Temperature	• **Operating:** 0 ~ 45 °C (32 ~ 113 °F) • **Storage:** -20 ~ 80 °C (-4 ~ 176 °F)
Relative Humidity	5 ~ 90% at 45 °C (non-condensing)
Vibration Protection	SSD: random operation 5 grms, 5~500 Hz

All specifications are subject to change without prior notice.

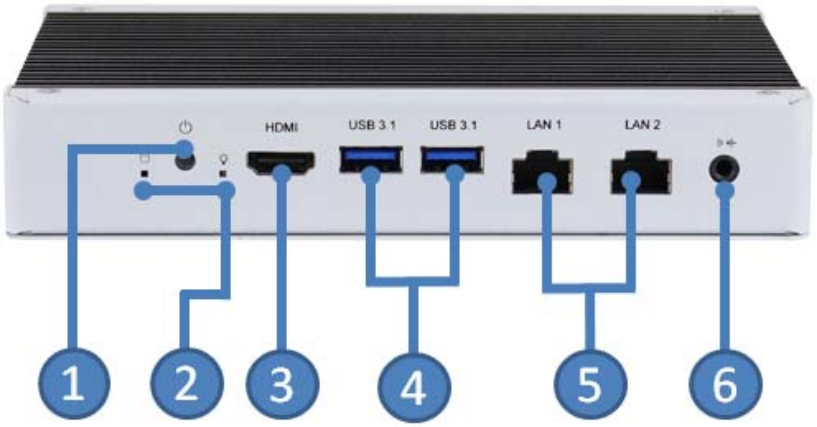
Note: The product performance relies on the system functioning as a whole. The level of CPU/APU/GPU processor, the interaction among the processor and the memory and storage bandwidth, or the functionality of the digital signage application software may affect the product performance.

1.5 Product View

Front View

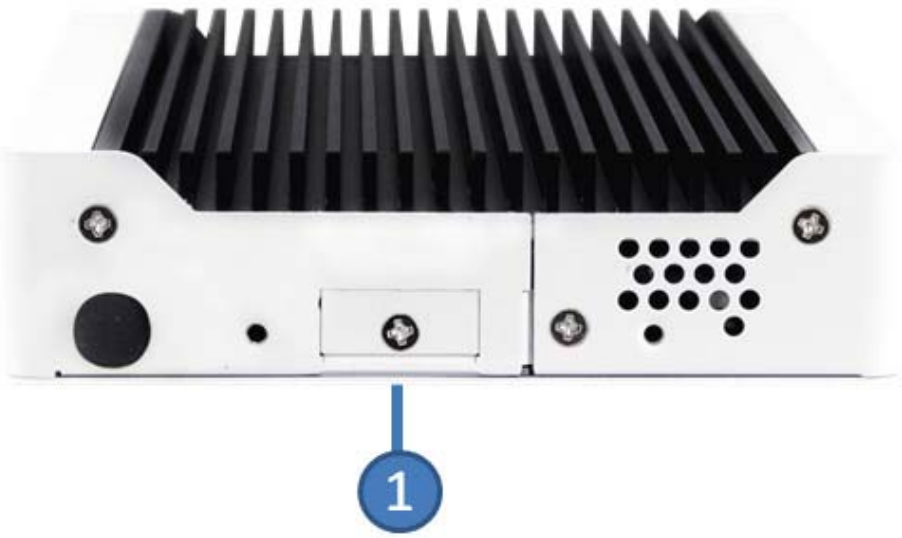
No.	Function	No.	Function
1	COM Port (COM1)	3	DP Port (CN2)
2	USB 3.1 Ports (CN3, CN4)	4	12V DC-in Connector (CN1)

Rear View



No.	Function	No.	Function
1	Power Button (SW1)	4	USB 3.1 Ports (CN7, CN8)
2	HDD Activity and Power LED	5	LAN 1 (CN9), LAN2 (CN10)
3	HDMI Port (CN6)	6	Audio Line-Out (CN11)

Side View

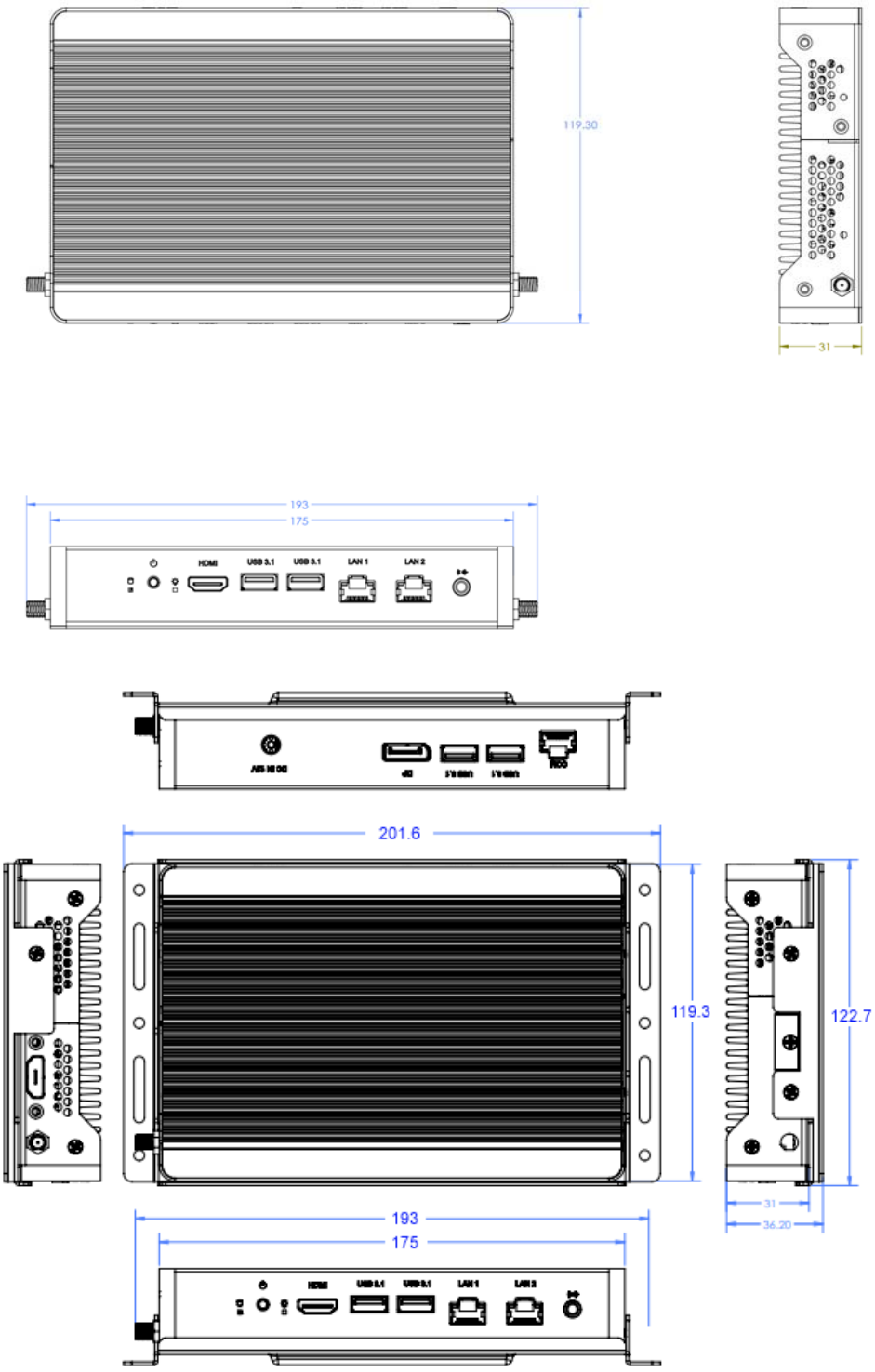


No.	Function
1	SIM Card Slot

Oblique View

1.6 Dimensions

Unit: mm



Chapter 2
Hardware Installation & Motherboard Information

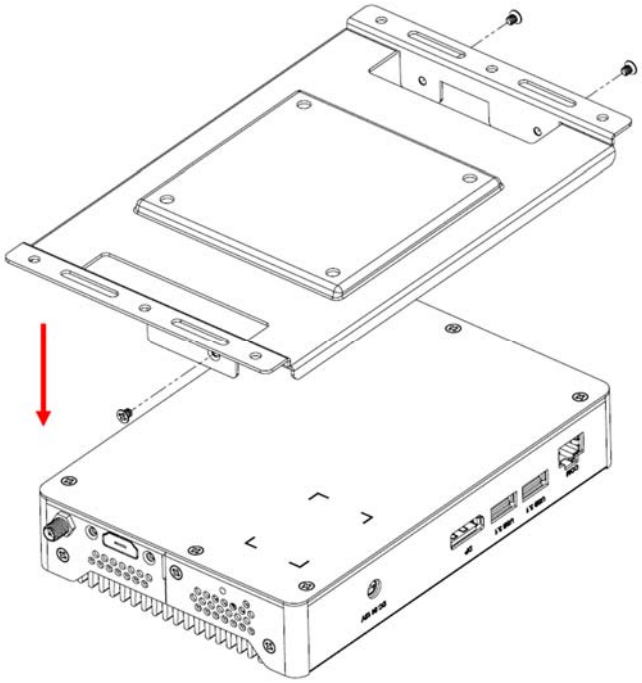
The information provided in this chapter includes:

- Installation of memory, M.2 and mini PCIe card
- Information and locations of connectors

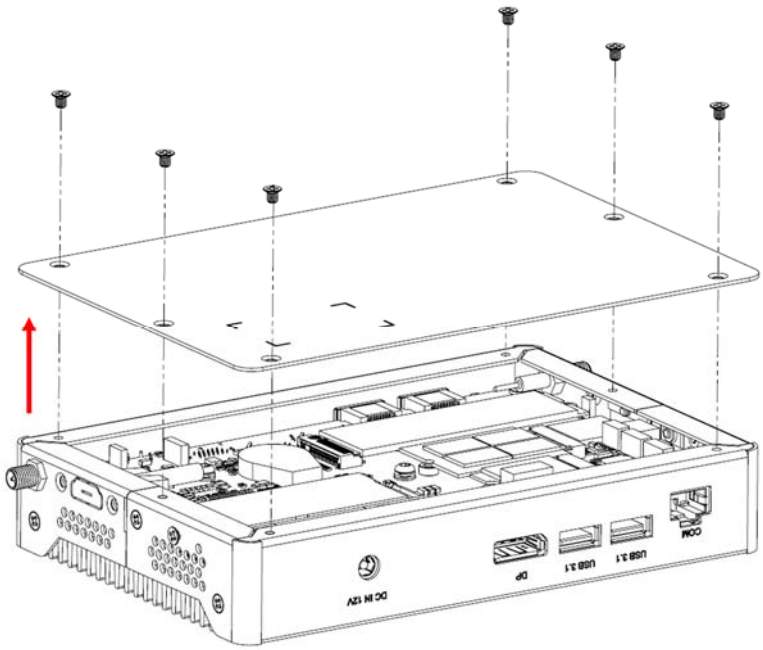
2.1 Installation / Replacement

The following pictures show how to disassemble the SI-642.

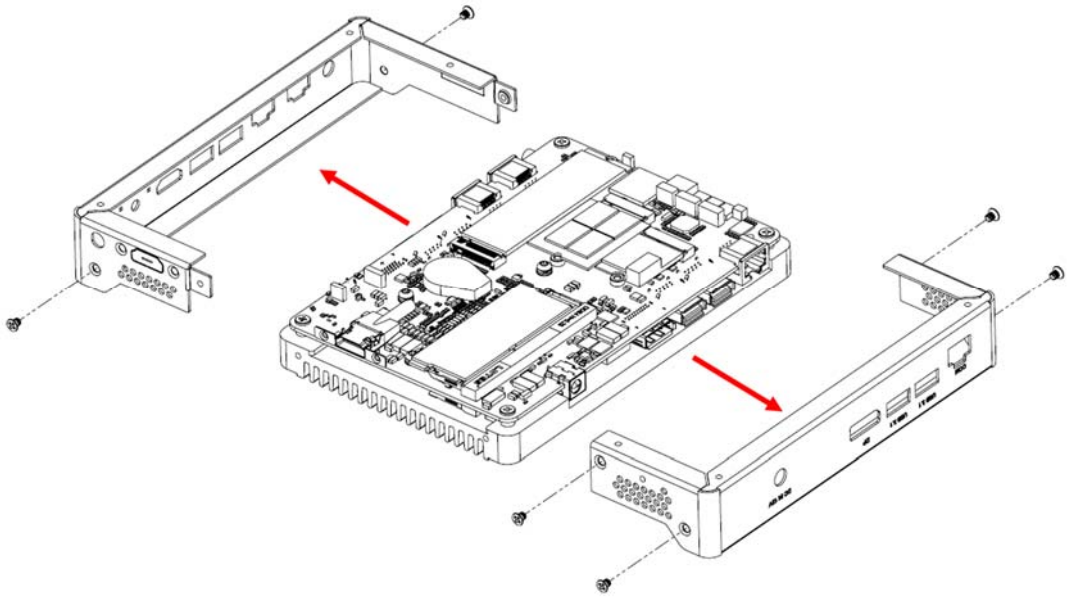
1. Remove the bracket holder (wall mount) by releasing the three (3) screws shown below.



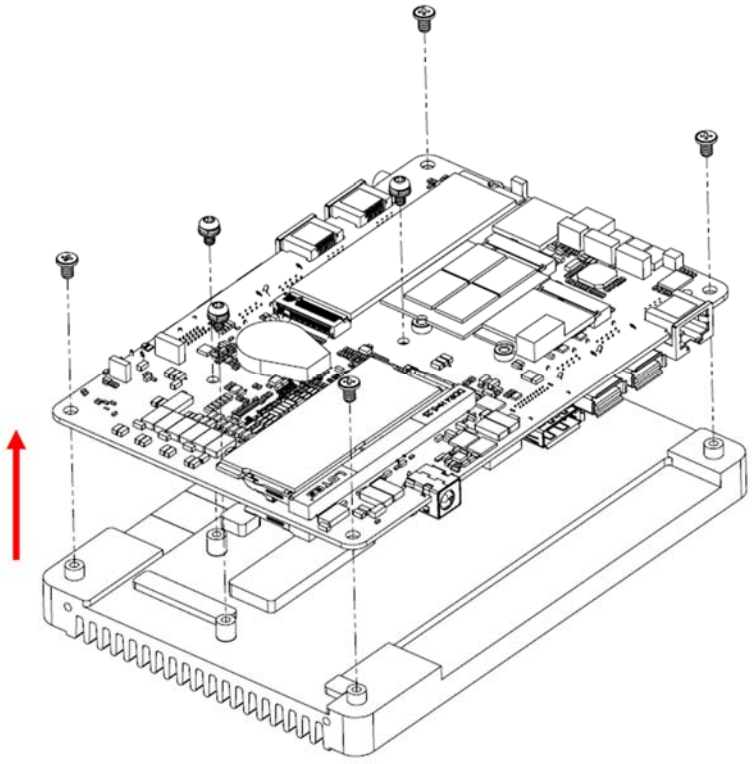
2. Remove the cover plate by releasing the six (6) screws shown below.



3. Remove the I/O connector cover plates by releasing the six (6) screws shown below.

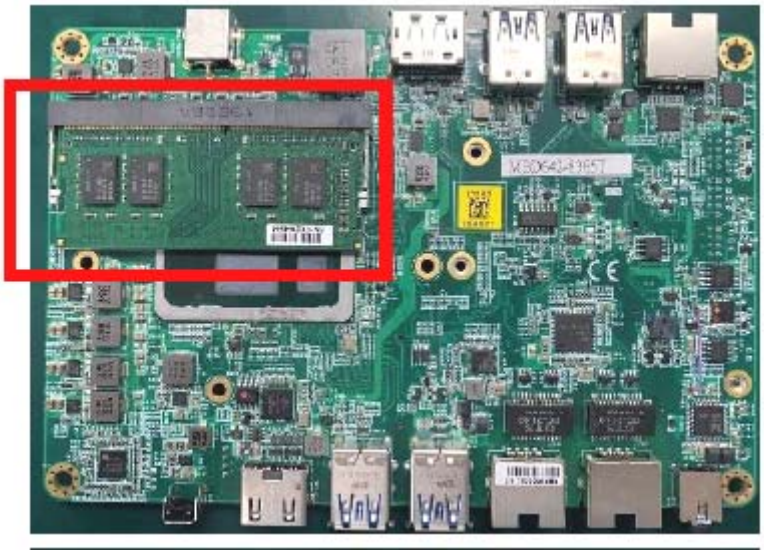


4. Separate the system board from the base heat sink by releasing the six (6) screws shown below.

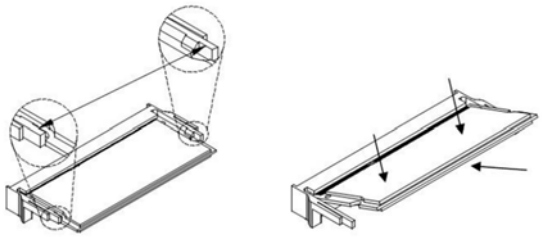


2.1.1 Memory

To install the modules, locate the memory slot on the motherboard and perform the following steps:



The MBD642 series supports two DDR4 memory sockets. To install the modules, locate the memory slot on the board and perform the following steps:



1. Align the key of the memory module with that on the memory slot and insert the module slantwise.
2. Gently push the module in an upright position until the clips of the slot close to hold the module in place when the module touches the bottom of the slot.

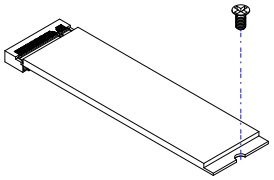
To remove the module, press the ejector tabs outwards with your fintertips to eject the module.

2.1.2 Mini-PCIe & M.2 Cards

1. Locate the M.2 slot inside the device.

2. Align the key of the M.2 card to the interface, and insert the card slantwise.
3. Fix the M.2 card with an M3 screw.

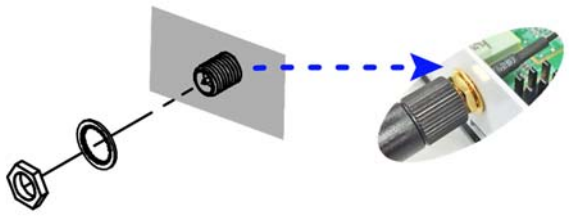
M.2:



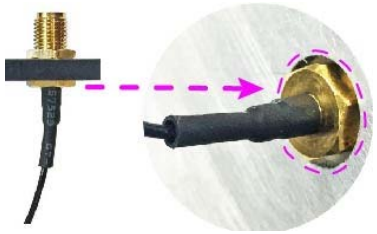
2.1.3 WiFi / 3G / 4G Antenna Installation

Thread the WiFi / 3G / 4G antenna extension cable through an antenna hole of the front I/O cover and fasten the antenna as shown below. Then apply adhesive to the edge of the hex nut behind the front I/O cover to prevent the extension cable from falling if the cable becomes loose.

1. Thread and fasten the hex nut and the washer. Then install the antenna.



2. Apply adhesive around here.



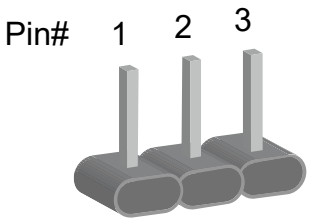
Info: The diameter of the nut is around 6.35 mm (0.25”-36UNC).

2.2 Setting the Jumpers

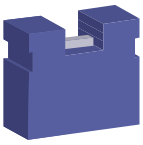
Set up and configure your SI-642 by using jumpers for various settings and features according to your needs and applications. Contact your supplier if you have doubts about the best configuration for your use.

2.3.1 How to Set Jumpers

Jumpers are short-length conductors consisting of several metal pins with a non-conductive base mounted on the circuit board. Jumper caps are used to have the functions and features enabled or disabled. If a jumper has 3 pins, you can connect either PIN1 to PIN2 or PIN2 to PIN3 by shorting.

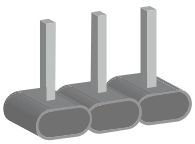
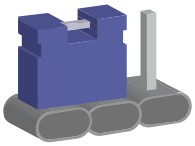
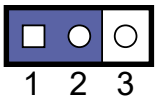
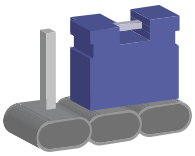
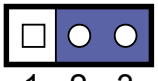


A 3-pin jumper



A jumper cap

Refer to the illustration below to set jumpers.

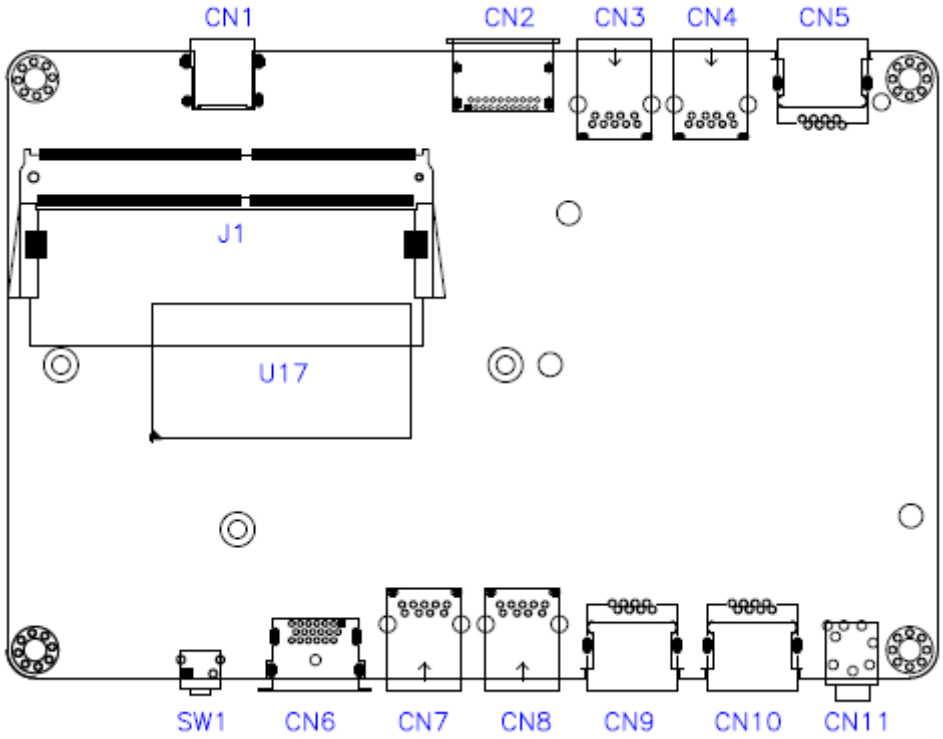
Pin closed	Oblique view	Illustration
Open		
1-2		
2-3		

When two pins of a jumper are encased in a jumper cap, this jumper is **closed**, i.e. turned **On**.

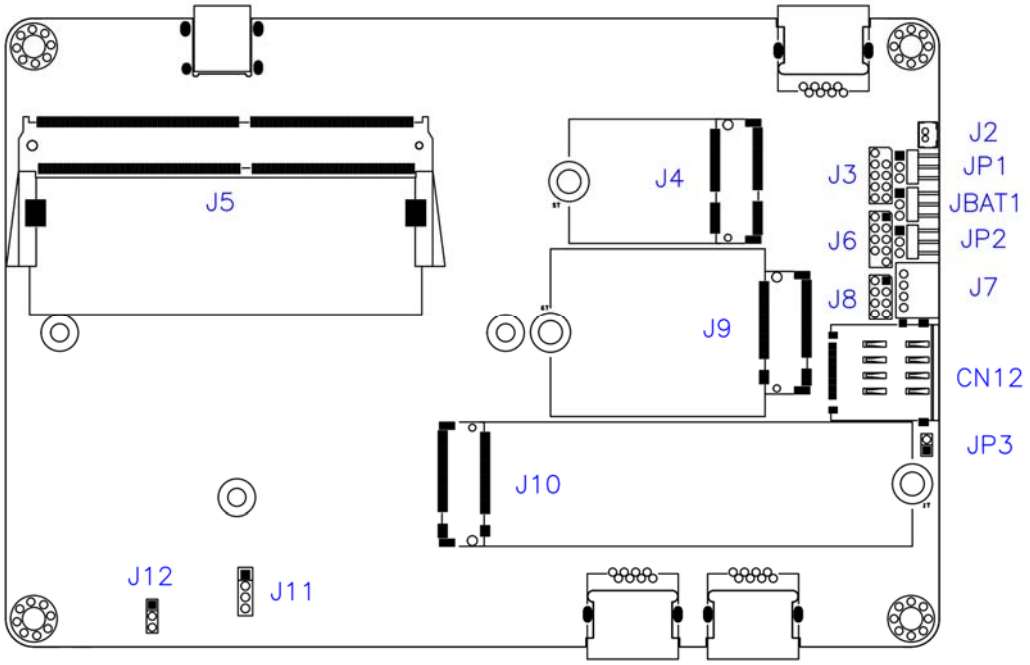
When a jumper cap is removed from two jumper pins, this jumper is **open**, i.e. turned **Off**.

2.3 Jumper & Connector Locations on Motherboard

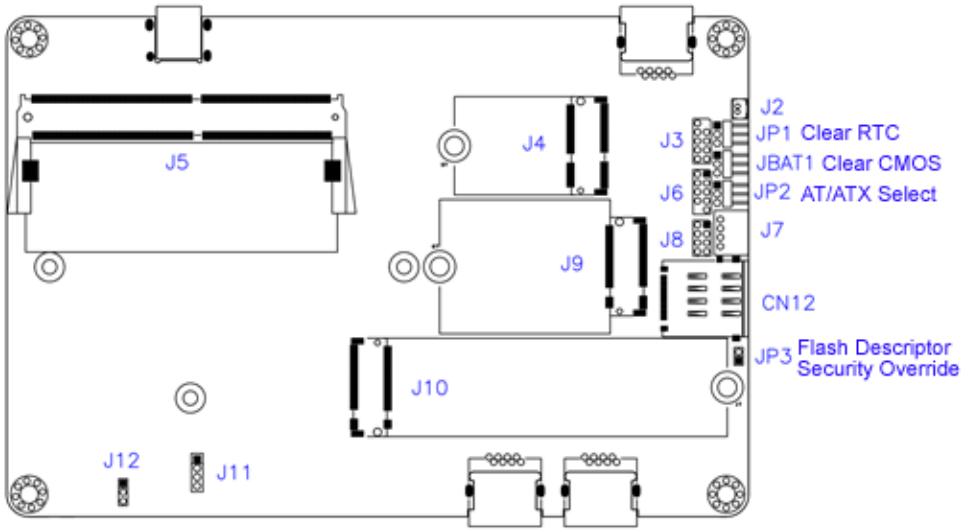
Motherboard: MBD642



MBD642 – top and I/O



MBD642 – back and I/O



2.4.1 JBAT1: Clear CMOS

JBAT1	Function	Pin closed
1	Normal (Default)	1-2
1	Clear CMOS	2-3

2.4.2 JP1: Clear RTC

JP1	Function	Pin closed
1	Normal (Default)	1-2
1	Clear RTC	2-3

2.4.3 JP2: AT/ATX Mode Selection

JP2	Function	Pin closed
1	ATX	1-2
1	AT	2-3

2.4.4 JP3: Flash Descriptor Security Override (Factory use only)

JP3	Pin	Function
1	Open	Disabled (Default)
1	Pin 1-2 Closed	Enabled

2.4.5 Pin Assignment for COM1 (RJ45) Port

Signal Name	Pin #	Pin#	Function
RTS, Request to Send	1	2	Data Terminal Ready
TXD, Transmit Data	3	4	GND, Ground
GND, Ground	5	6	RXD, Receive Data
DSR, Data Set Ready	7	8	CTS, Clear to Send

Chapter 3
Driver Installation

The information provided in this chapter includes:

- Intel® Chipset Software Installation Utility
- VGA Driver
- HD Audio Driver
- LAN Driver
- Intel® Management Engine Drivers Installation
- Intel® Serial IO Drivers Installation

3.1 Introduction

This section describes the installation procedures for software drivers. The software drivers are available on IBASE website www.ibase.com.tw. Register as a member of our website to download all the necessary drivers and extract for installation.

Note: After installing your Windows operating system, you must install the Intel® Chipset Software Installation Utility first before proceeding with the drivers installation.

3.2 Intel® Chipset Software Installation Utility

The Intel® Chipset drivers should be installed first before the software drivers to install INF files for Plug & Play function for the chipset components. Follow the instructions below to complete the installation.

1. Insert the disk enclosed in the package with the board. Click Intel on the left pane and then Intel(R) Whiskeylake-U Chipset Drivers on the right pane.

2. Click **Intel(R) Chipset Software Installation Utility**.

3. When the *Welcome* screen to the Intel® Chipset Device Software appears, click **Next** to continue.

4. Accept the software license agreement and proceed with the installation process.

5. On the *Readme File Information* screen, click **Install**.

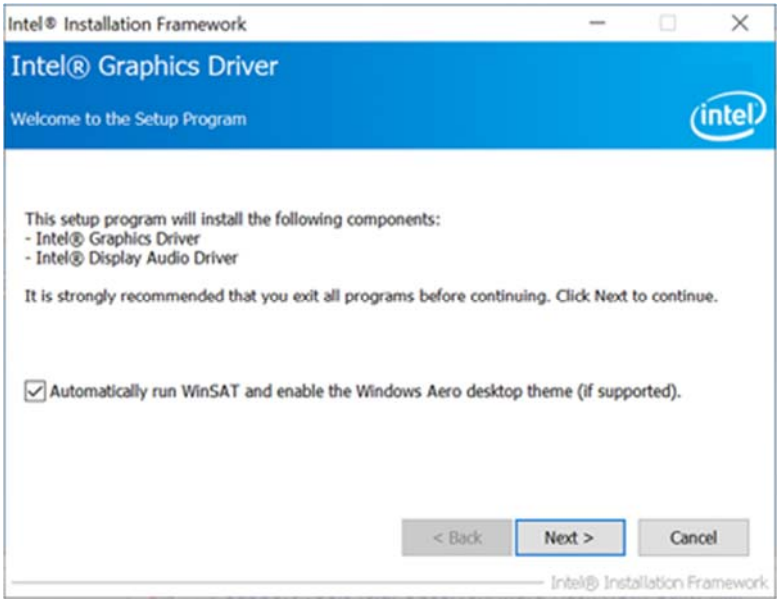
6. After the installation, click **Finish** to complete the setup process.

3.3 VGA Driver Installation

1. Insert the disk enclosed in the package with the board. Click **Intel** on the left pane and then **Intel(R) Whiskeylake-U Chipset Drivers** on the right pane.

2. Click **Intel(R) HD Graphics Driver**.

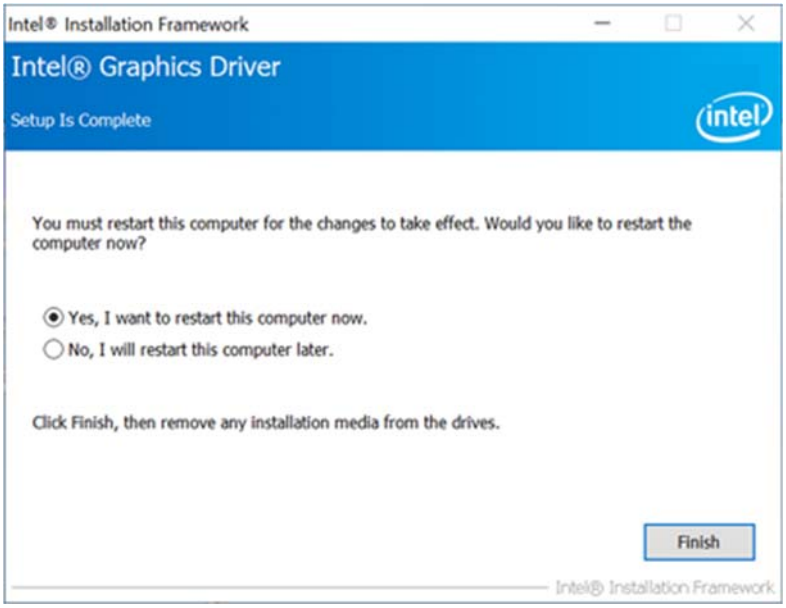
3. When the *Welcome* screen appears, click **Next** to continue.



4. Click **Yes** to accept the license agreement and click **Next**.

5. On the *Readme File Information* screen, click **Next** until the installation starts.

6. When Setup is complete, restart the computer.



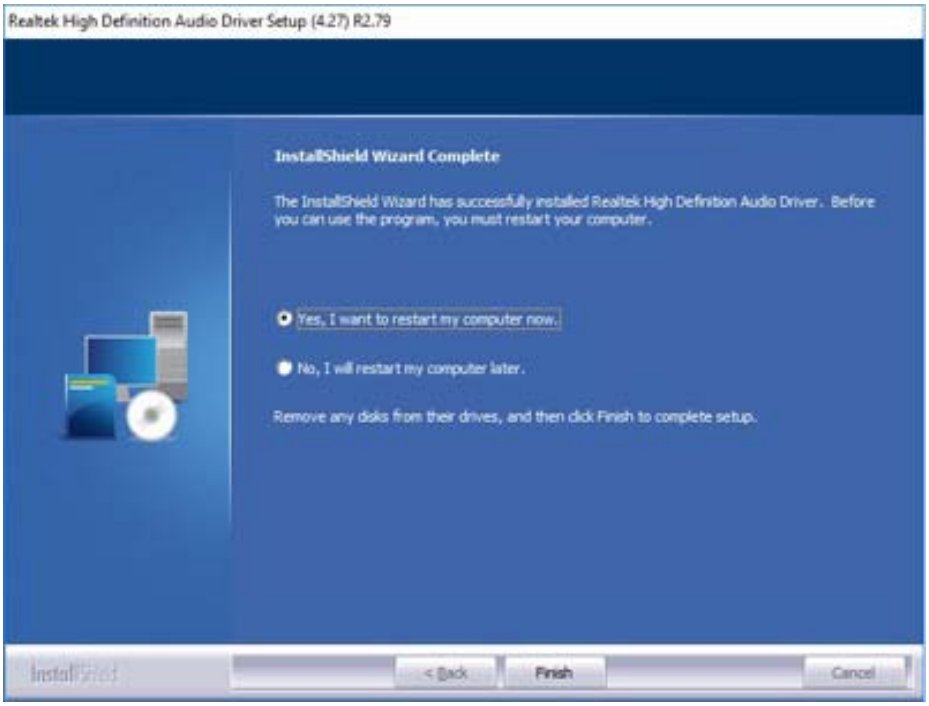
3.4 HD Audio Driver Installation

1. Insert the disk enclosed in the package with the board. Click **Intel** on the left pane and then **Intel(R) Whiskeylake-U Chipset Drivers** on the right pane.

2. Click **Realtek High Definition Audio Driver**.

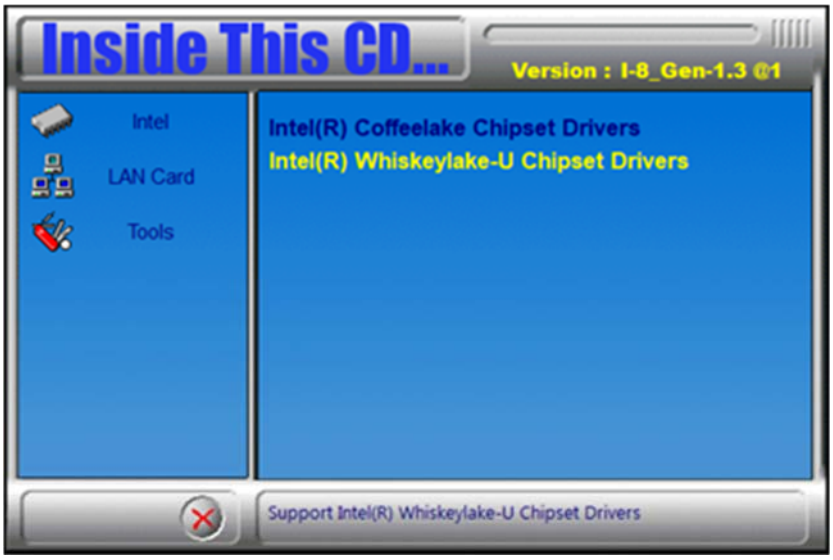
3. On the *Welcome* screen of the InstallShield Wizard, click **Next**.

4. When the driver is completely installed, restart the computer for changes to take effect.



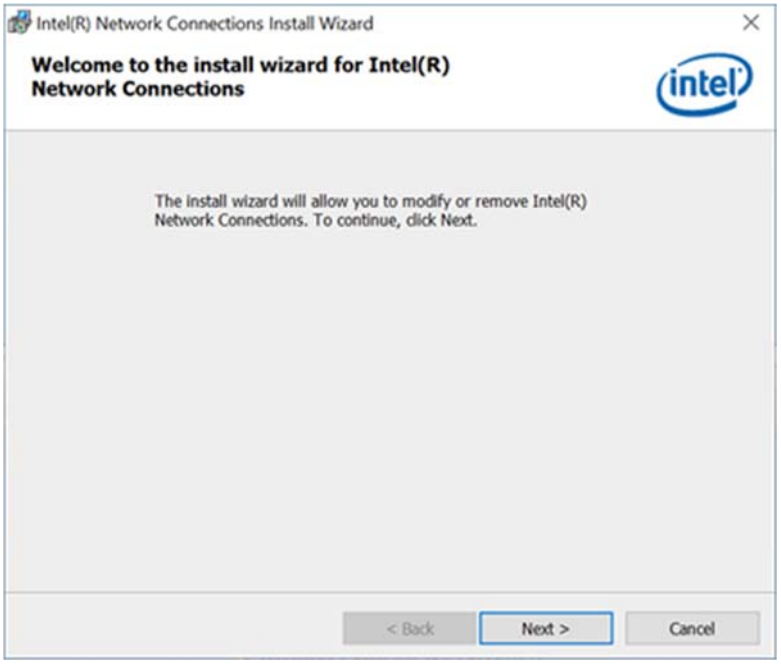
3.5 LAN Driver Installation

1. Insert the disk enclosed in the package with the board. Click **Intel** on the left pane and then **Intel(R) Whiskeylake-U Chipset Drivers** on the right pane.



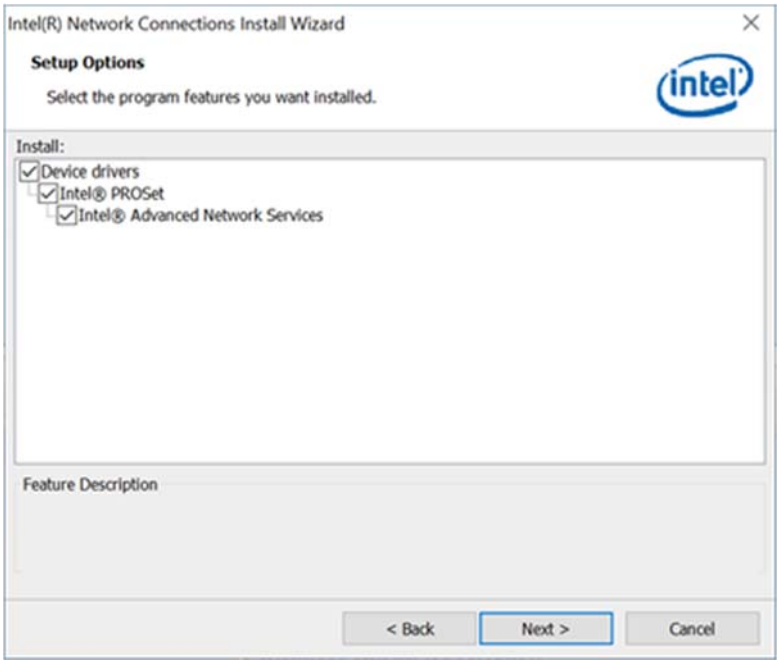
2. Click **Intel(R) PRO LAN Network Drivers**..

3. When the *Welcome* screen appears, click **Next**.



4. Accept the license agreement and click **Next**.

5. On the *Setup Options* screen, select the desired features you want installed. Then click **Next** to continue.



6. When the Install wizard has completed the installation, click **Finish**.

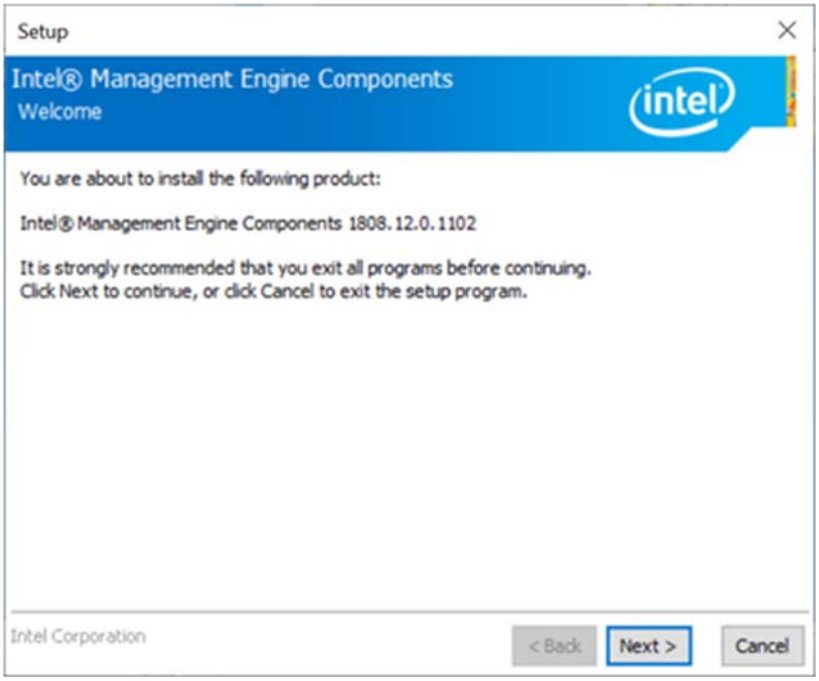
3.6 Intel® Management Engine Components Drivers Installation

1. Insert the disk enclosed in the package with the board. Click **Intel** on the left pane and then **Intel(R) Whiskeylake-U Chipset Drivers** on the right pane.

2. Click **Intel(R) ME 12.x Drivers**.

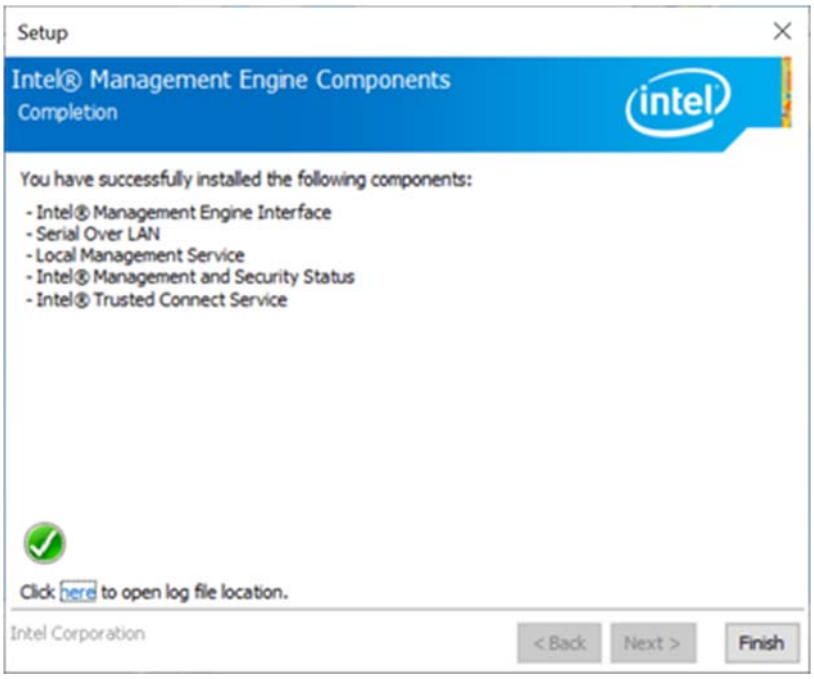
.

3. When the *Welcome* screen appears, click **Next**.



4. Accept the license agreement and click **Next**.

5. After Intel Management Engine Components have been successfully installed, click **Finish**.

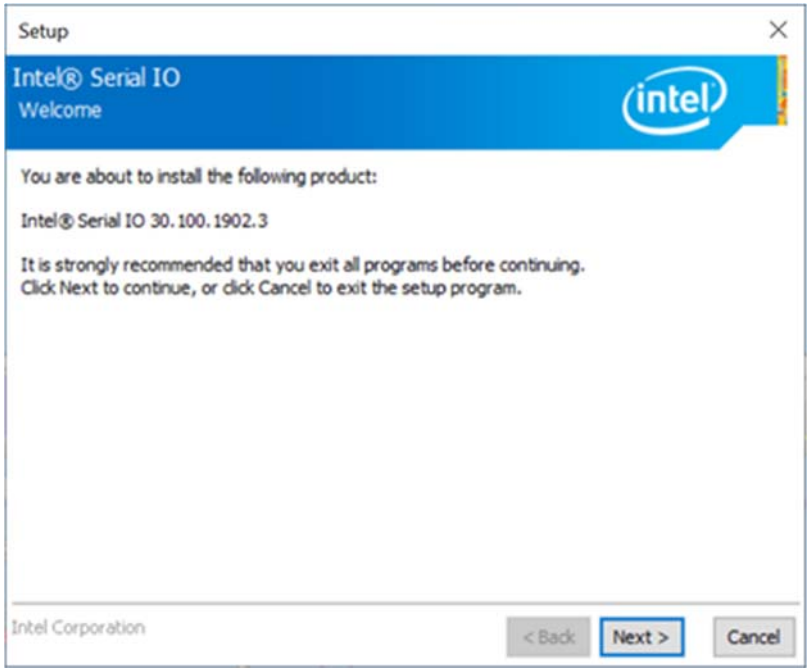


3.7 Intel® Serial IO Drivers Installation

1. Insert the disk enclosed in the package with the board. Click **Intel** on the left pane and then **Intel(R) Whiskeylake-U Chipset Drivers** on the right pane.

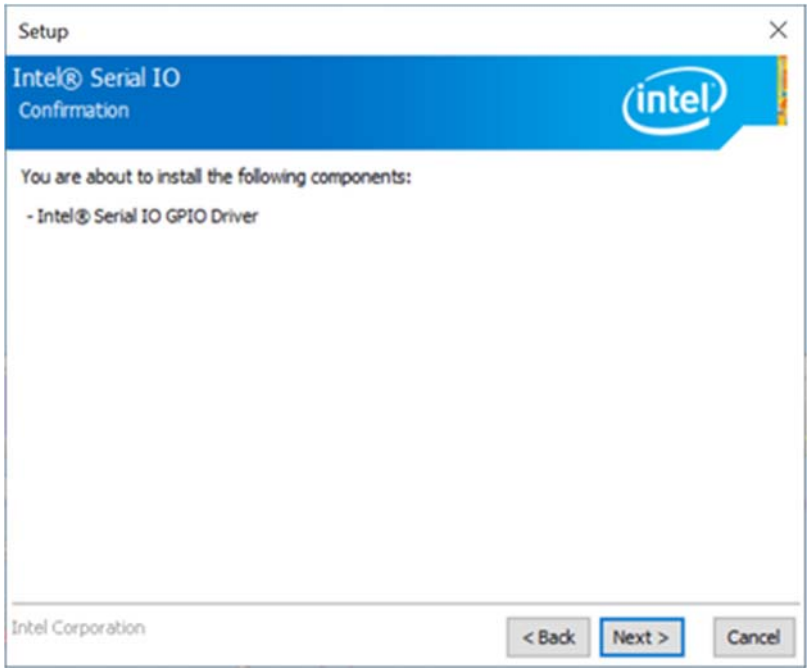
2. Click **Intel(R) Serial IO Drivers**.

3. When the *Welcome* screen appears, click **Next**.



4. Accept the license agreement and click **Next** until the installation starts.

5. When prompted to install the driver, click **Next**.



6. After completing the installation, restart the computer for changes to take effect.

Chapter 4
BIOS Setup

This chapter describes the different settings available in the AMI BIOS that comes with the board. The topics covered in this chapter are as follows:

- Main Settings
- Advanced Settings
- Chipset Settings
- Security Settings
- Boot Settings
- Save & Exit

4.1 Introduction

The BIOS (Basic Input/Output System) installed in the ROM of your computer system supports Intel® processors. The BIOS provides critical low-level support for standard devices such as disk drives, serial ports and parallel ports. It also provides password protection as well as special support for detailed fine-tuning of the chipset controlling the entire system.

4.2 BIOS Setup

The BIOS provides a Setup utility program for specifying the system configurations and settings. The BIOS ROM of the system stores the Setup utility. When you turn on the computer, the BIOS is immediately activated. Press the <Del> key immediately allows you to enter the Setup utility. If you are a little bit late pressing the <Del> key, POST (Power On Self Test) will continue with its test routines, thus preventing you from invoking the Setup.

If you still need to enter Setup, restart the system by pressing the ”Reset” button or simultaneously pressing the <Ctrl>, <Alt> and <Delete> keys. You can also restart by turning the system Off and back On again.

The following message will appear on the screen:

```
Press <DEL> to Enter Setup
```

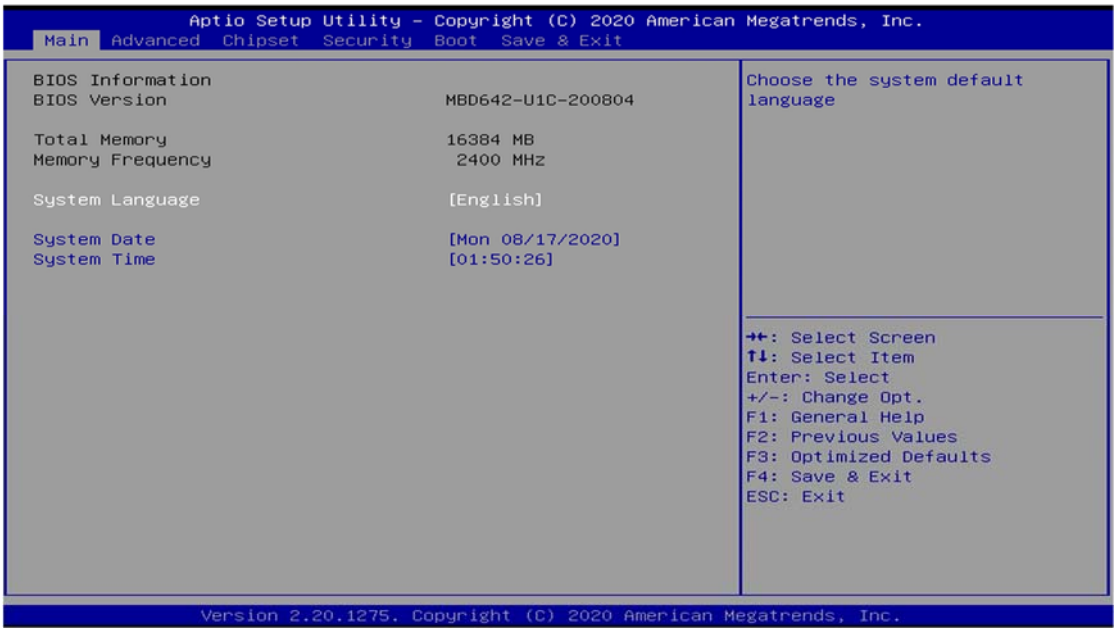
In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

When you enter the BIOS Setup utility, the *Main Menu* screen will appear on the screen. The Main Menu allows you to select from various setup functions and exit choices.

Warning: It is strongly recommended that you avoid making any changes to the chipset defaults.

These defaults have been carefully chosen by both AMI and your system manufacturer to provide the absolute maximum performance and reliability. Changing the defaults could make the system unstable and crash in some cases.

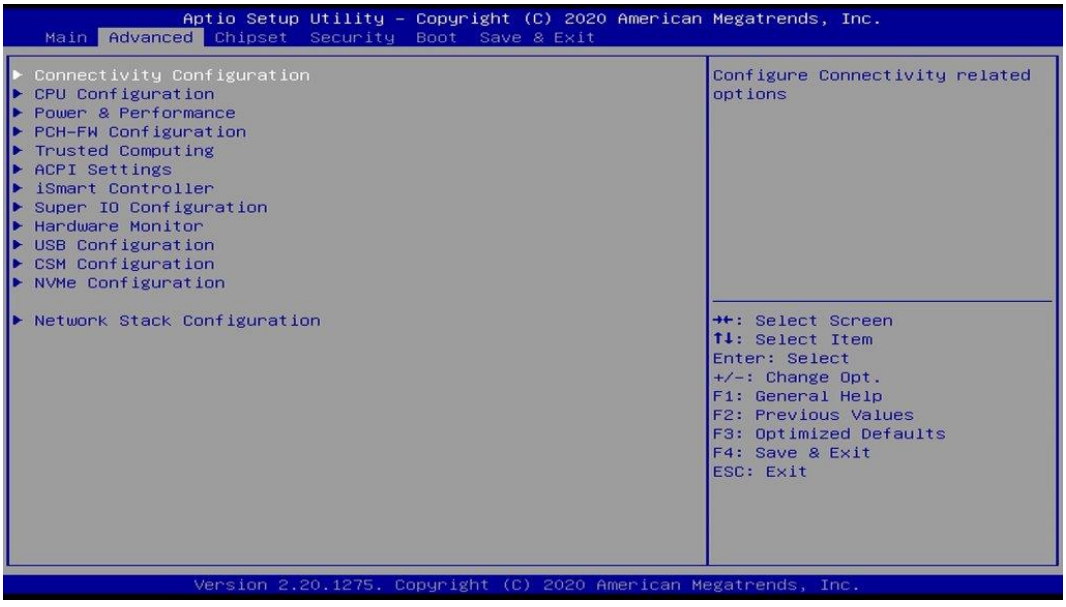
4.3 Main Settings



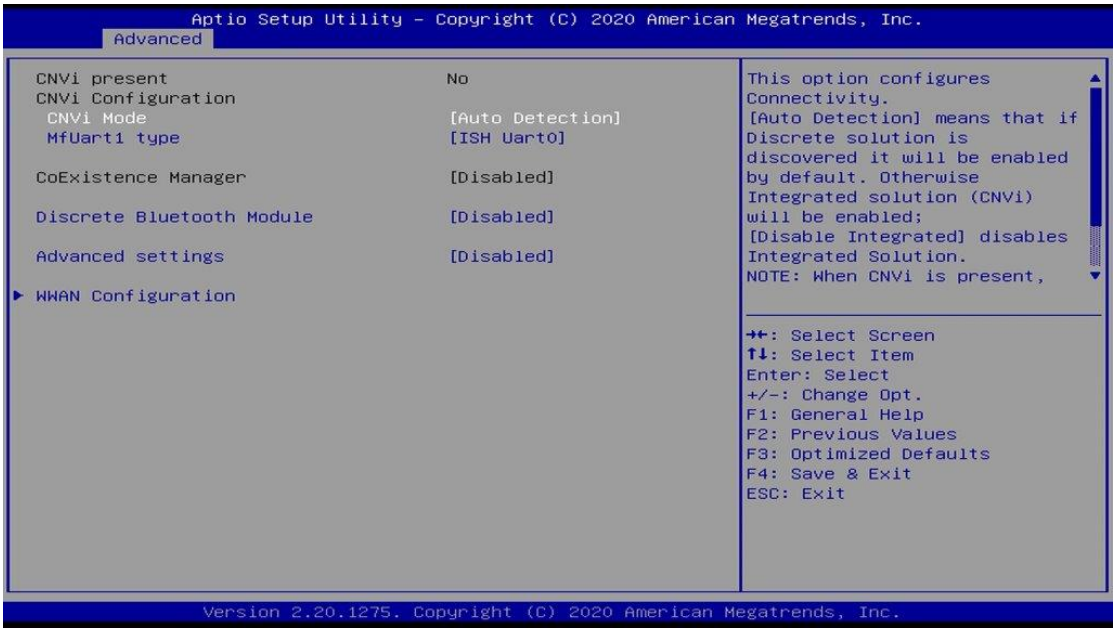
BIOS Setting	Description
System Date	Sets the date. Use the <Tab> key to switch between the data elements.
System Time	Set the time. Use the <Tab> key to switch between the data elements.

4.4 Advanced Settings

This section allows you to configure, improve your system and allows you to set up some system features according to your preference.

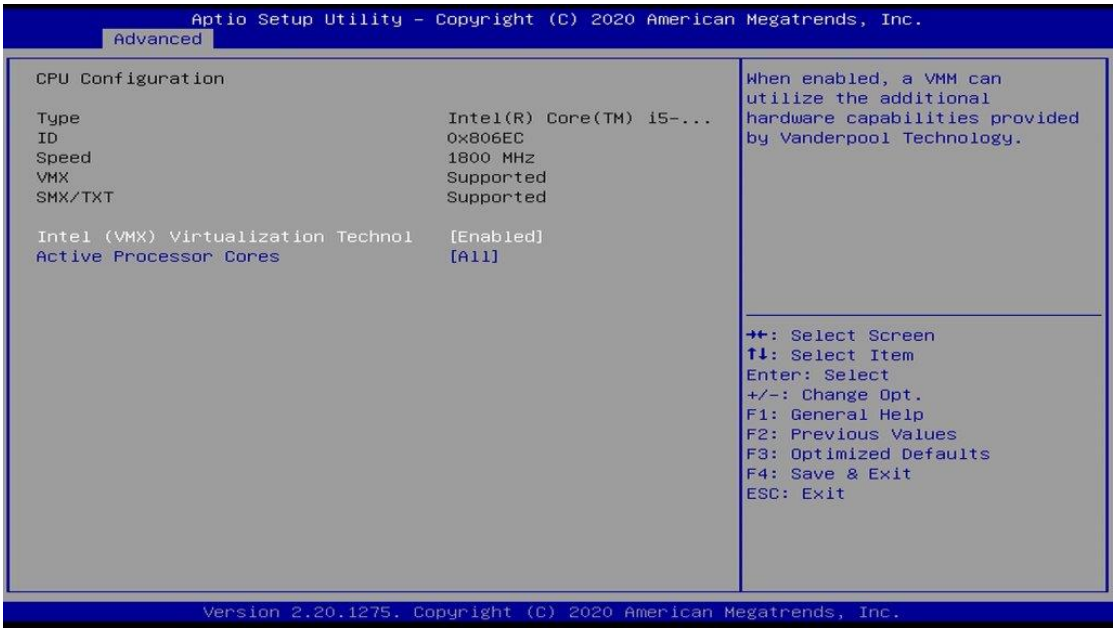


4.4.1 Connectivity Configuration



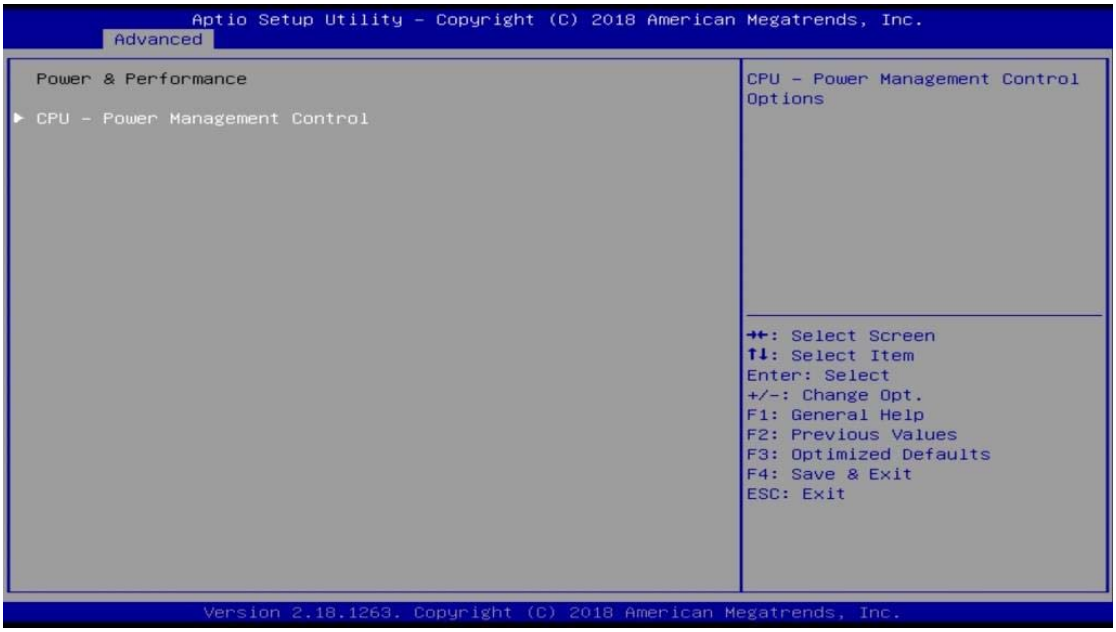
BIOS Setting	Description
CNVi Mode	This option configures connectivity. **Auto Detection** means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNV1) will be enabled. **Disable Integrated** disables Integrated Solution.
MfUart1 type	This is a test option whch allows configuration of UART type for WiFi side band communication.
CoExistence Manager	CoEx Manager mitigates radio coexistence issues between Intel WWAN (modem) and Intel WLAN (WiFi/BT). This should be enabled only if both WWAN and WLAN solution are based on Intel components.
Discrete Bluetooth Module	Serial I/O UART0 needs to be enabled to select BT module.
Advanced settings	Configures ACPI objects for wireless devices.
WWAN Configuration	Configures WWAN related options.

4.4.2 CPU Configuration



BIOS Setting	Description
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Procesor Cores	Number of cores to enable in each processor package.
Intel Trusted Execution Technology	Enables / Disables utilization of additional hardware capabilities provided by Intel(R) Trusted Execution Technology. Changes require a full power cycle to take effect.

4.4.3 Power & Performance



BIOS Setting	Description
CPU – Power Management Control	CPU power management control options.
Turbo Mode	Enables/Disables processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).

4.4.4 PCH-FW Configuration

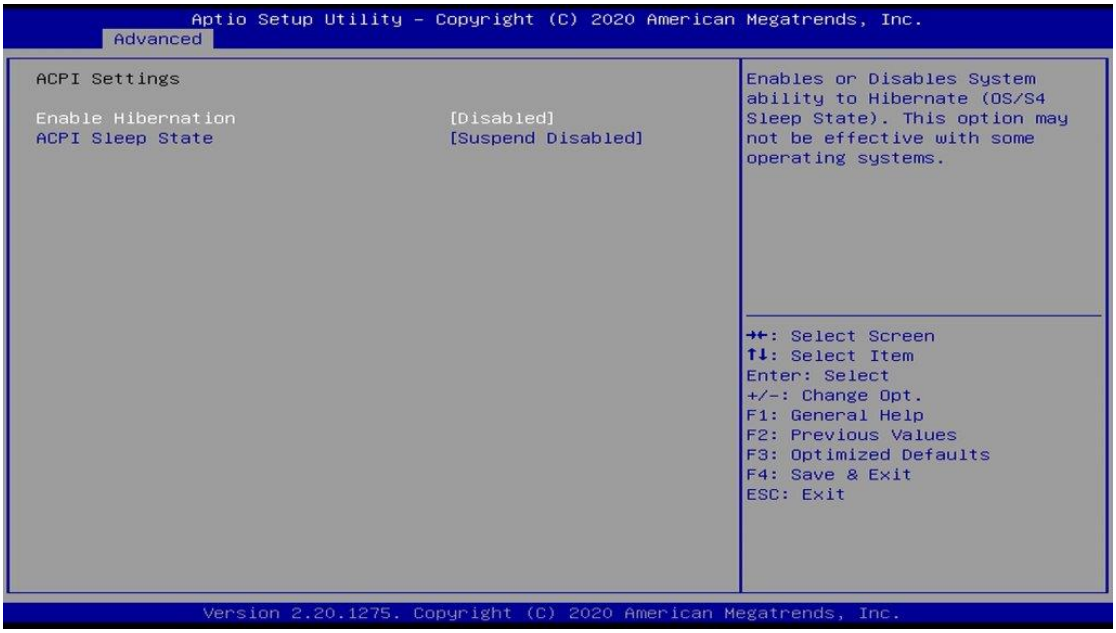
BIOS Setting	Description
ME State	When disable, ME will be put into ME Temporarily Disabled Mode.
AMT BIOS Features	When disabled, AMT BIOS Features are no longer supported and user is no longer able to access MEBx Setup. Note: This option does not disable Manageability Features in FW.

4.4.5 ACPI Settings

BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. OS will not show security device. TCG EFI protocol and INTIA interface will not be available.
SHA-1 PCR Bank	Options: Enable or Disable
Pending operation	Schedule an operation for the security device. Note: Your computer will reboot during restart in order to change state of security device.
Platform Hierarchy Storage Hierarchy Enorsement Hierarchy	Options: Enable or Disable
TPM2.0 UEFI Spec Version	Select the TCG2 Spec Version Support. TCG_1_2: the compatible mode for Win8/Win10 TCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	Select to tell OS to support PPI Spect Version 1.2 or 1.3. Some HCK tests might not support 1.3.
Device Select	TPM 1.2 will restrict support to TPM 1.2 devices. TPM 2.0 will restrict support to TPM 2.0 devices. Auto will support both with the default set to TPM

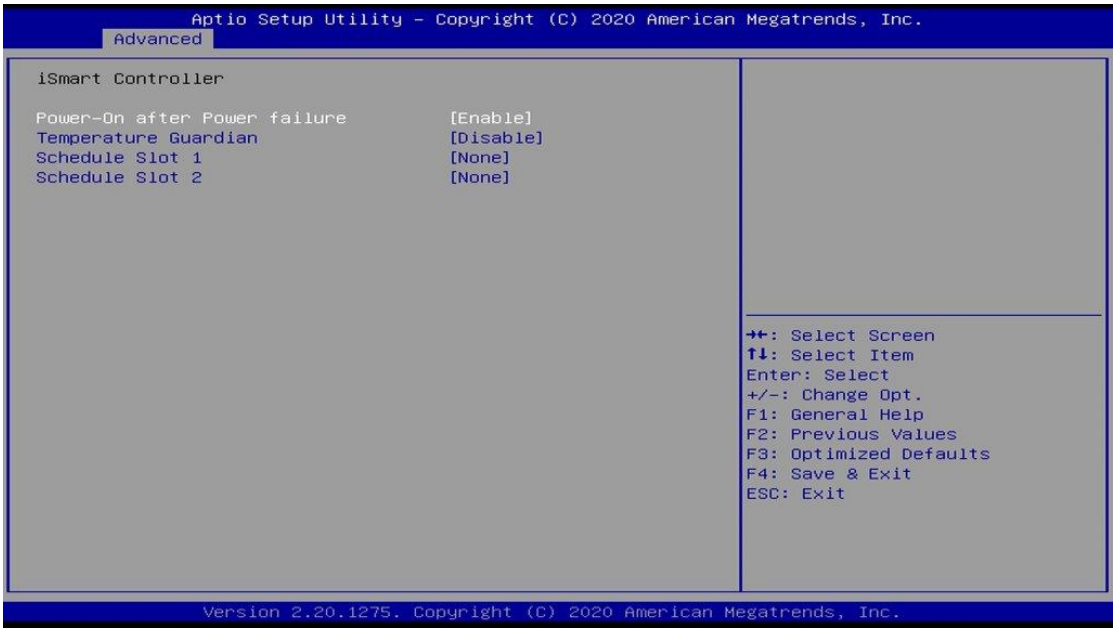
	2.0 devices. If not found, TPM 1.2 devices will be enumerated.

4.4.6 ACPI Settings



BIOS Setting	Description
Enable Hibernation	Enables / Disables system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
ACPI Sleep State	Selects the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

4.4.7 iSmart Controller

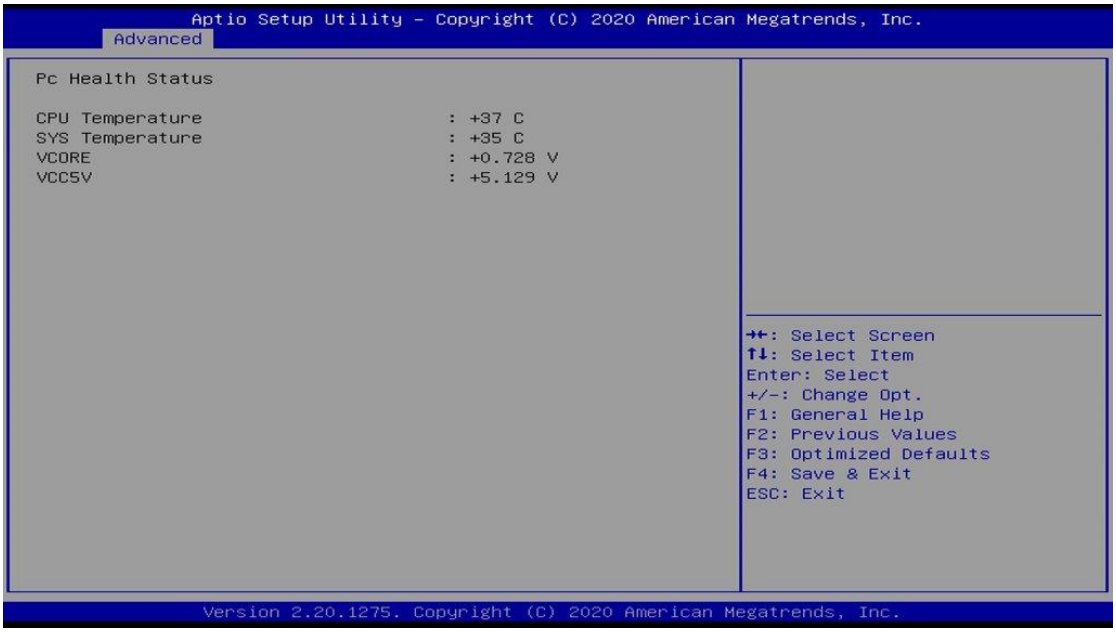


BIOS Setting	Description
Power-On after Power failure	Enables / Disables the system to be turned on automatically after a power failure.
Schedule Slot 1 / 2	Sets up the hour / minute for system powe-on. **Important:** If you would like to set up a schedule between adjacent days, configure two schedule slots. For example, if setting up a schedule from Wednesday 5 p.m. to Thursday 2 a.m., configure two schedule slots. But if setting up a schedule from 3 p.m to 5 p.m. on Wednesday, configure only a schedule slot.

4.4.8 Super IO Configuration

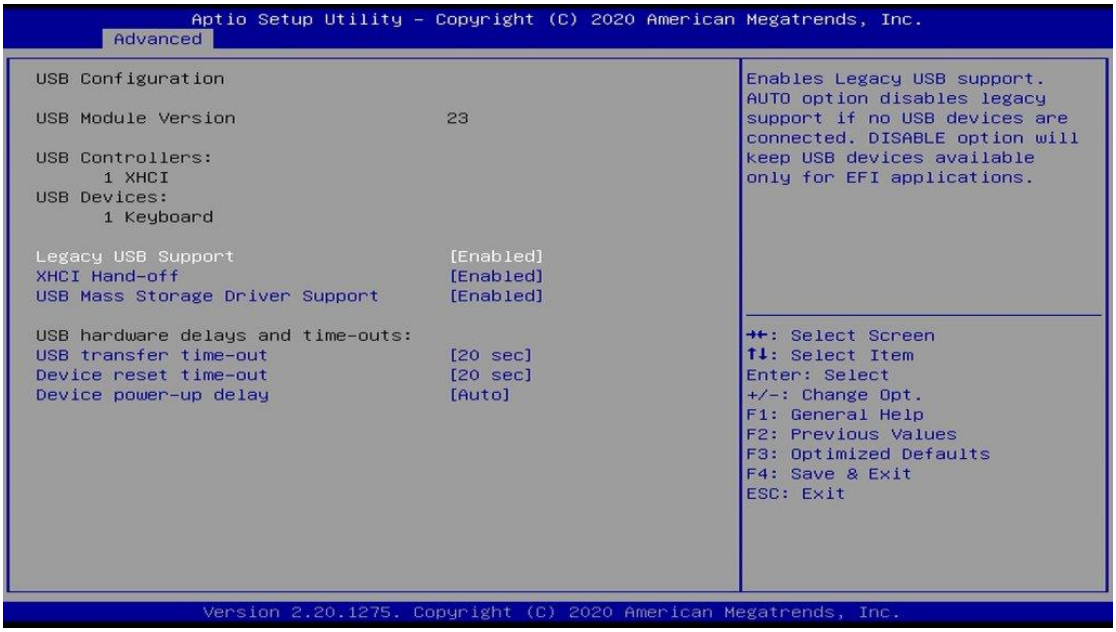
BIOS Setting	Description
Serial Port 1 Configuration	Sets parameters of Serial Port 1 (COMA).
Serial Port	Enable / Disable the serial port.
Change Settings	Select an optimal setting for the Super IO device.

4.4.9 Hardware Monitor



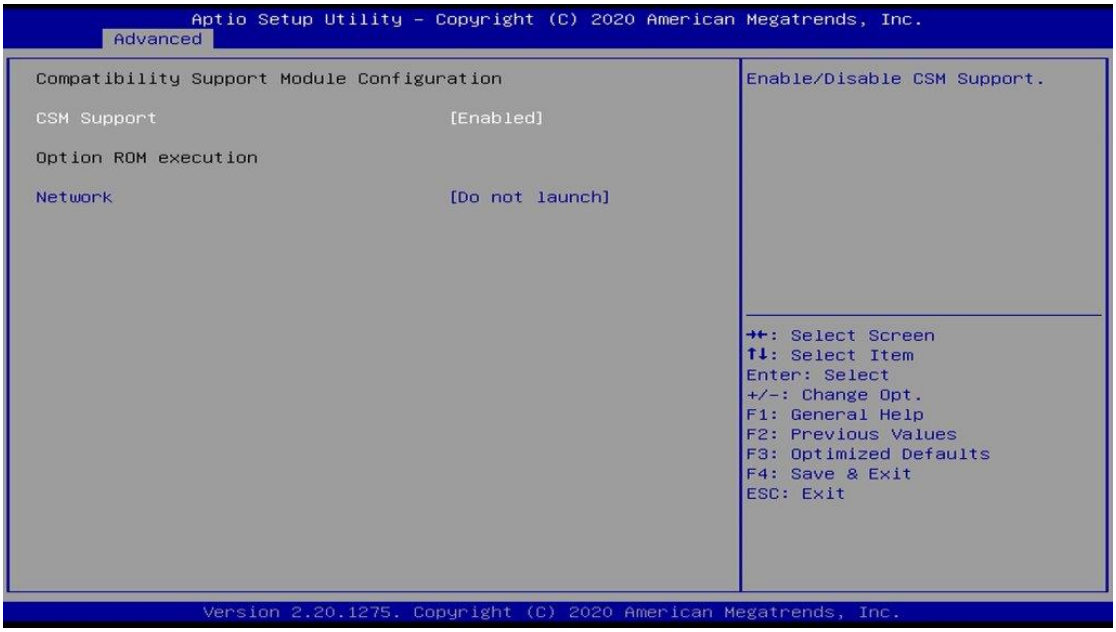
BIOS Setting	Description
Temperatures / Voltages	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only values as monitored by the system and show the PC health status.

4.4.10 USB Configuration



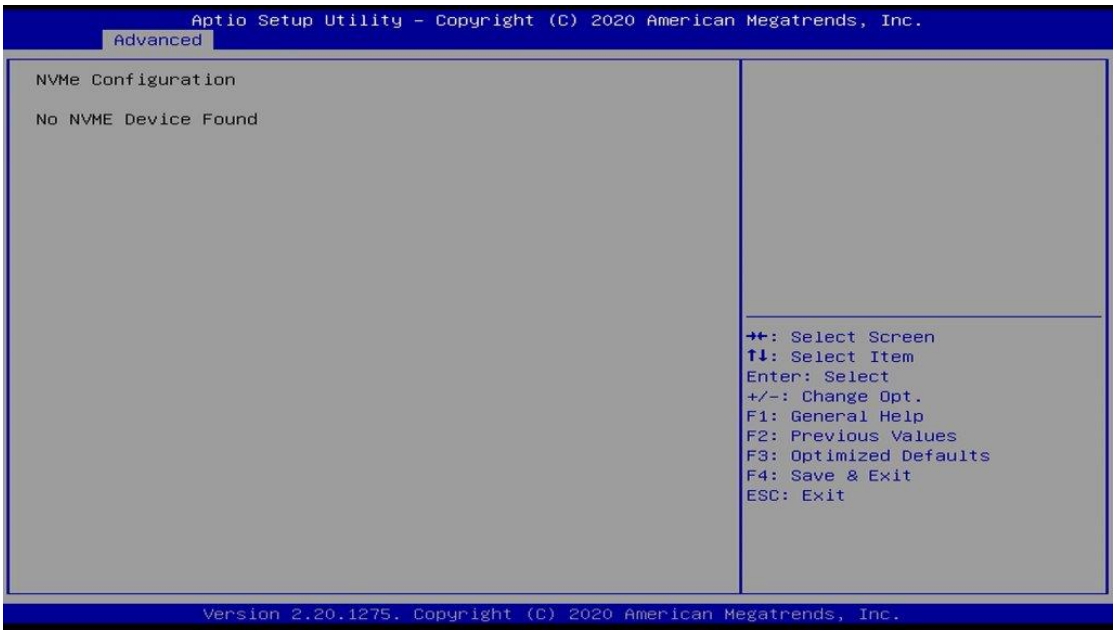
BIOS Setting	Description
Legacy USB Support	• **Enable:** Enables Ledacy USB Support. • **Auto:** Disables legacy support if no USB devices are connected. • **Disable:** Keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables the support for USB mass storage driver.
USB Transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	Seconds of delaying execution of start unit command to USB mass storage device.
Device power-up delay	The maximum time the device will take before it properly reports itself to the Host Controller. “Auto” uses default value for a Root port it is 100ms. But for a Hub port, the delay is taken from Hub descriptor.

4.4.11 CSM Configuration

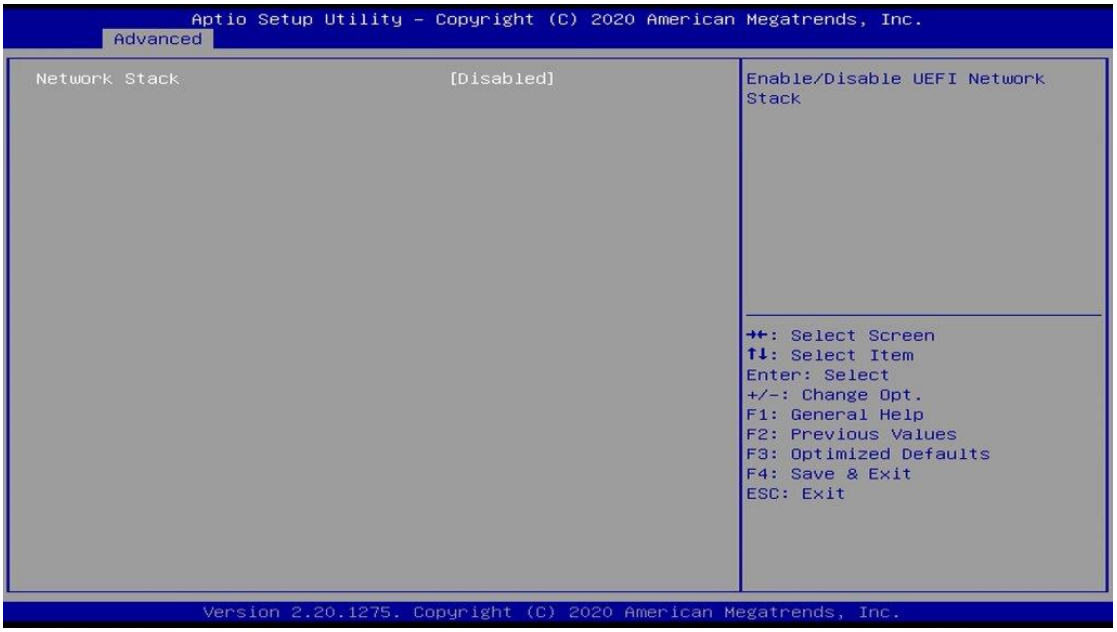


BIOS Setting	Description
CSM Support	Enables/Disables CSM Support.
Network	Controls the execution of UEFI and Legacy PXE OpROM.

4.4.12 NVMe Configuration

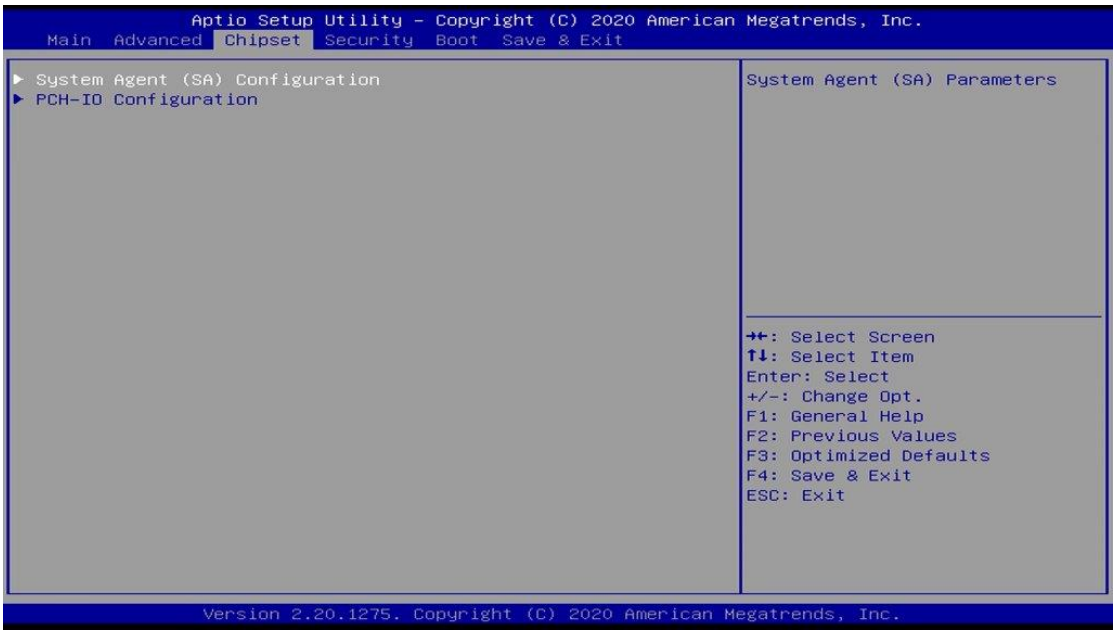


4.4.13 Network Stack Configuration



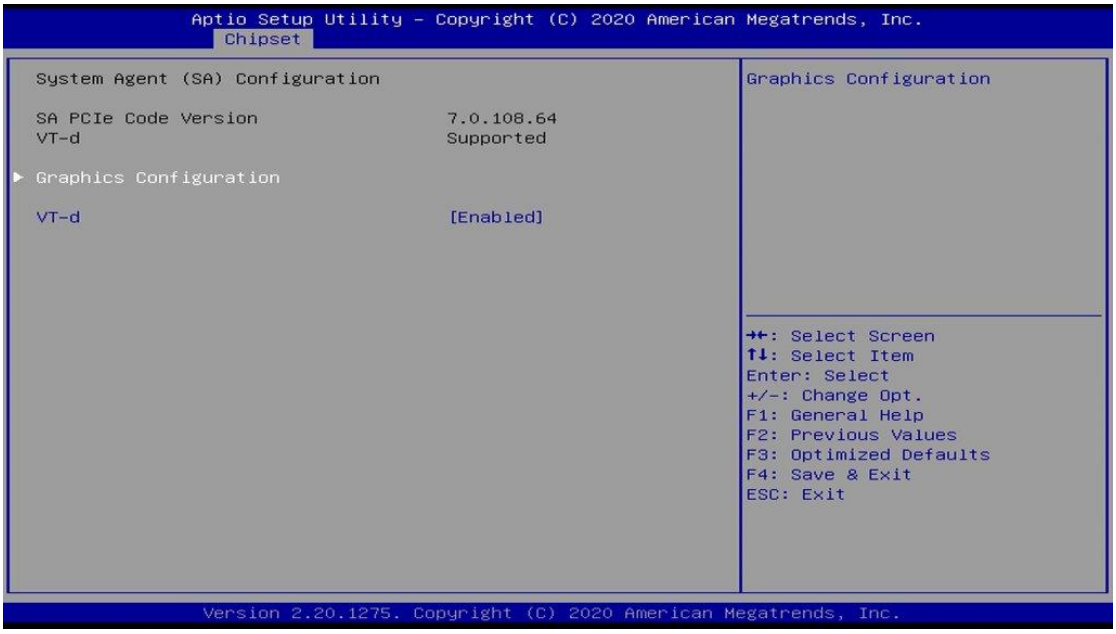
BIOS Setting	Description
Network Stack	Enables / Disables UEFI Network Stack.

4.5 Chipset Settings



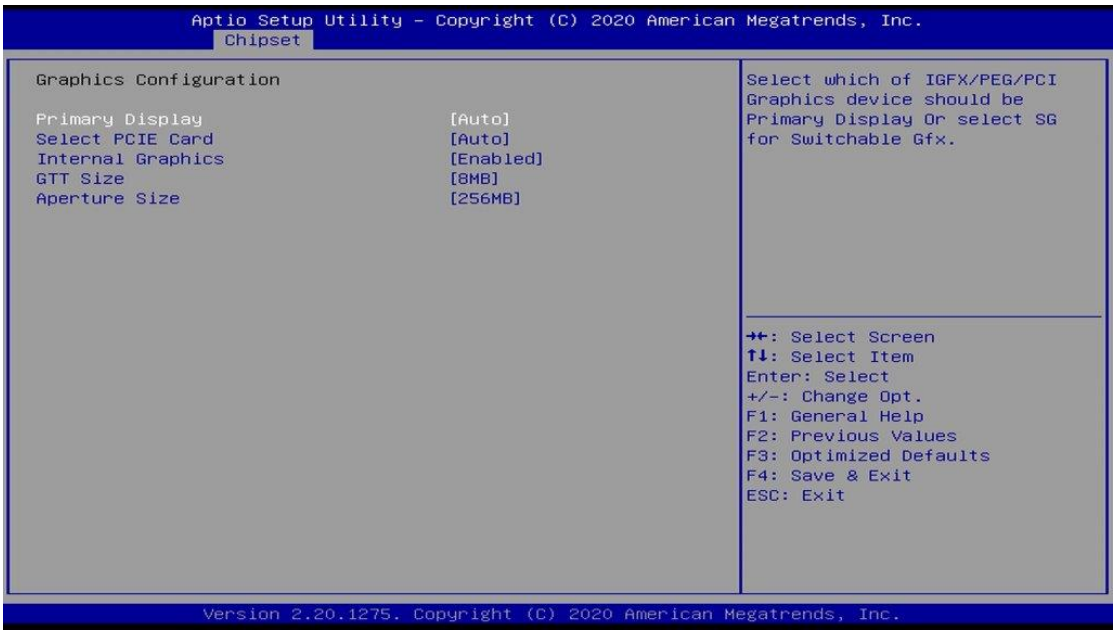
BIOS Setting	Description
System Agent (SA) Configuration	System Agent (SA) parameters
PCH-IO Configuration	PCH parameters

4.5.1 System Agent (SA) Configuration



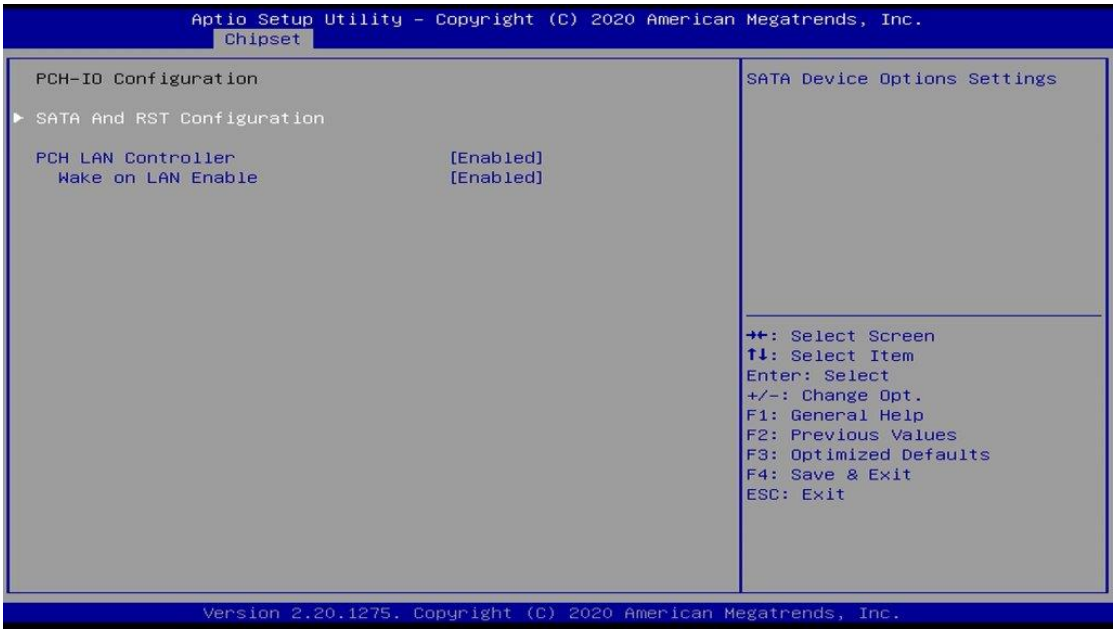
BIOS Setting	Description
Graphics Configuration	Configures the graphics settings.
VT-d	Checks if VT-d function on MCH is supported.

4.5.1.1. Graphics Configuration



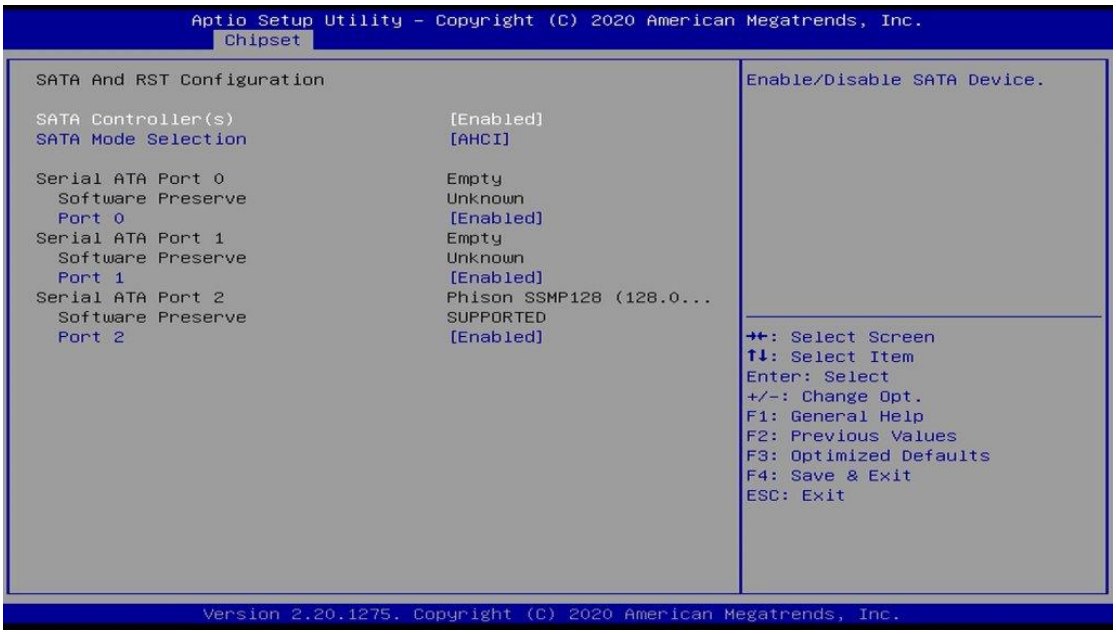
BIOS Setting	Description
Primary Display	Select which of IGFX/PEG/PCI Graphics device should be primary display or select SG for switchable Gfx. Options: Auto, IGFX, PEG, PCI, SG
Select PCIE Card	Selects the card used on the platform. **Auto** skips GPIO based Power Enable to dGPU. **E1k Creek 4:** DGPU Power Enable = Active Low. **PEG Eva1:** DGPU Power Enable = Active High.
Internal Graphics	Keep IGFX enabled based on the setup options. Options: Auto, Disabled, Enabled
GTT Size	Sets the GTT size as 2 MB, 4 MB, or 8 MB.
Aperture Size	Sets the aperture size as 128 MB, 256 MB, 512 MB, 1024 MB or 2048 MB. **Note:** Above 4 GB MMIO BIOS assignment is automatically enabled when selecting 2048 MB aperture. To use this feature, disable CSM support.

4.5.2 PCH-IO Configuration



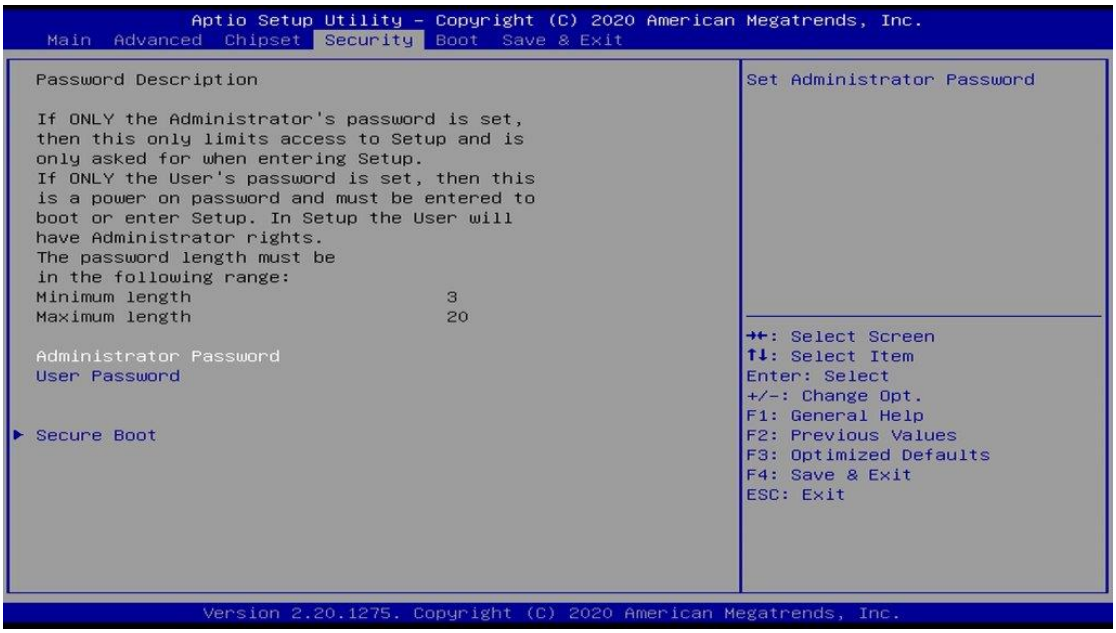
BIOS Setting	Description
SATA and RST Configuration	Configures SATA devices.
PCH LAN Controller	Enables / Disables the onboard NIC.
Wake on LAN Enable	Enables / Disables the integrated LAN to wake up the system.
PS_ON Enable	Enables / Disables PS_ON support a new C10 state from the CPU on desktop SKUs that enables a lower power target that will be required by the California Energy commission (CEC).

4.5.2.1. SATA and RST Configuration:



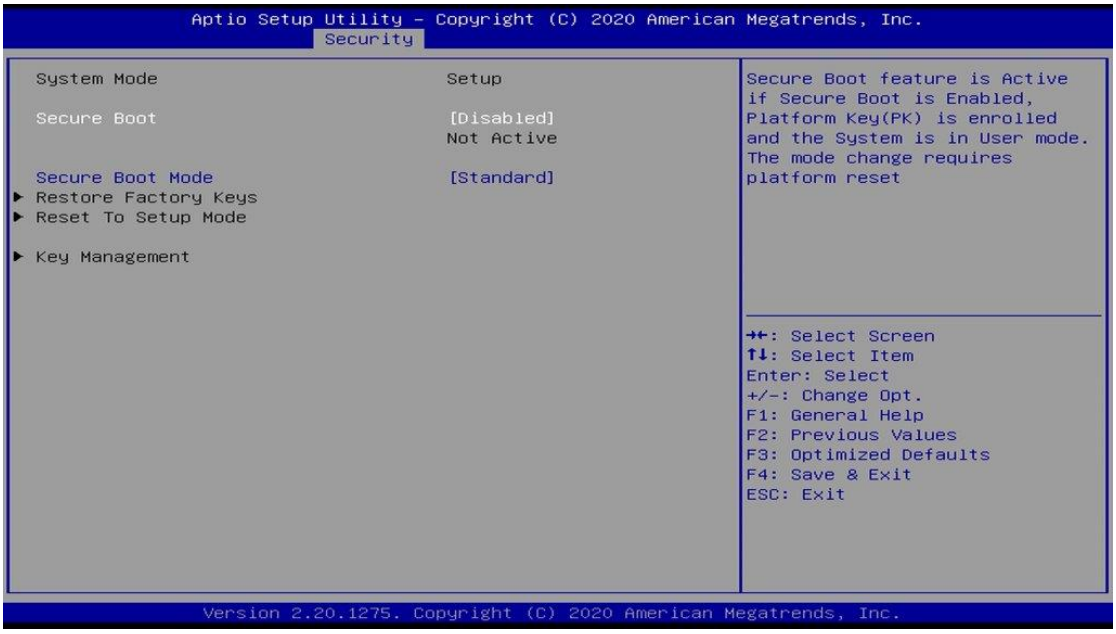
BIOS Setting	Description
SATA Controller(s)	Enables / Disables the SATA device.
SATA Mode Selection	Determines how SATA controller(s) operate. Options: AHCI / Intel RST Premium
Serial ATA Ports	Enables / Disables serial ports.
SATA Ports Hot Plug	Enables / Disables SATA Ports HotPlug.

4.6 Security Settings



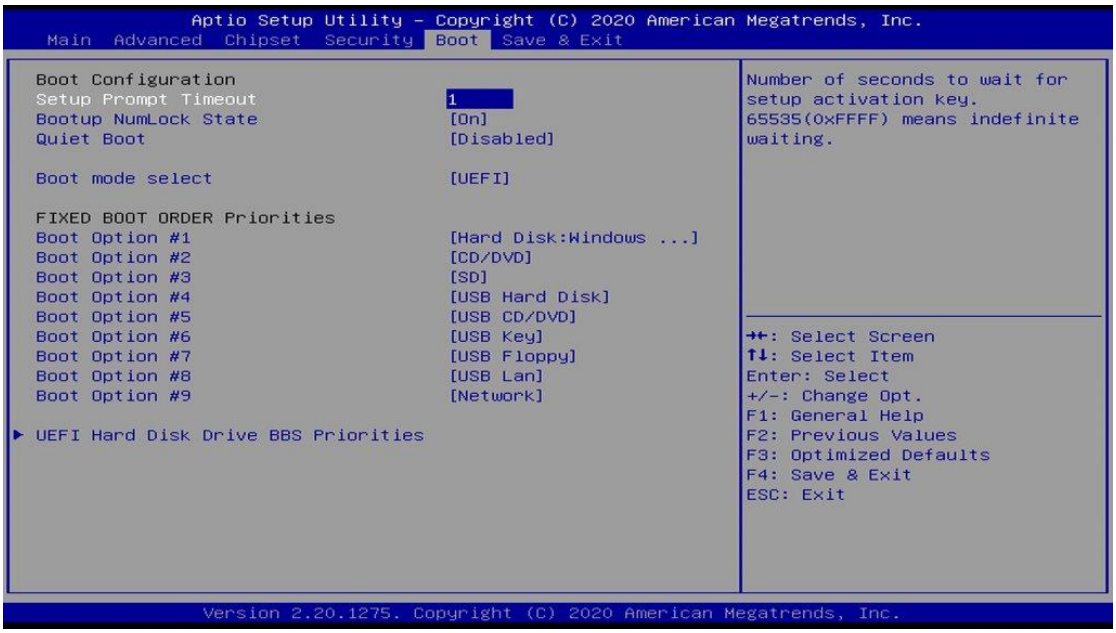
BIOS Setting	Description
Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Configures Secure Boot.

4.6.1 Secure Boot



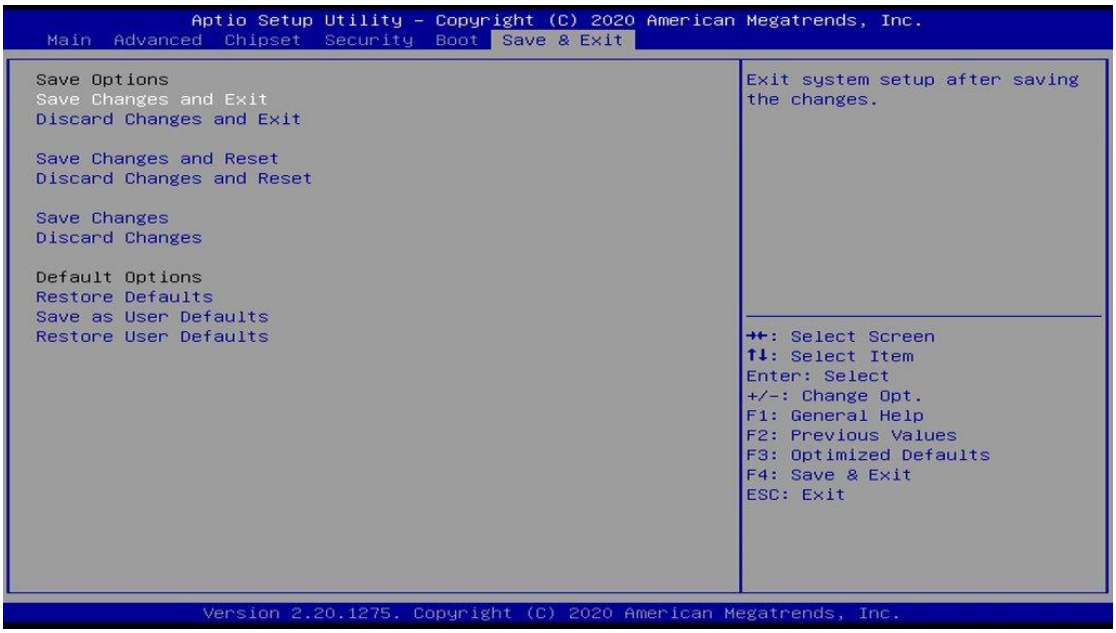
BIOS Setting	Description
Secure Boot	Secure Boot feature is Active if Secure Boot is enabled. Platform Key (PK) Is enrolled and the system is in User mode. The mode change requires platform reset.
Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys	Forces system to user mode. Install factory default Secure Boot key databases.
Key Management	Enables expert users to modify Secure Boot Policy variables without full authentication.

4.7 Boot Settings



BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
Boot mode select	Selects a Boot mode, Legacy / UEFI.
Boot Option Priorities	Sets the system boot order.

4.8 Save & Exit Settings



BIOS Setting	Description
Save Changes and Exit	Exits system setup after saving the changes.
Discard Changes and Exit	Exits system setup without saving any changes.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options.
Restore Defaults	Restores / Loads defaults values for all the setup options.
Save as User Defaults	Saves the changes done so far as User Defaults.
Restore User Defaults	Restores the user defaults to all the setup options.

Appendix

This section provides the mapping addresses of peripheral devices and the sample code of watchdog timer configuration.

- I/O Port Address Map
- Interrupt Request Lines (IRQ)

A. I/O Port Address Map

Each peripheral device in the system is assigned a set of I/O port addresses which also becomes the identity of the device. The following table lists the I/O port addresses used.

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000A20-0x00000A2F	Motherboard resources
0x0000002E-0x0000002F	Motherboard resources
0x0000004E-0x0000004F	Motherboard resources
0x00000061-0x00000061	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000065-0x00000065	Motherboard resources
0x00000067-0x00000067	Motherboard resources
0x00000070-0x00000070	Motherboard resources
0x00000070-0x00000070	System CMOS/real time clock
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Motherboard resources
0x00000680-0x0000069F	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x00001800-0x000018FE	Motherboard resources
0x0000164E-0x0000164F	Motherboard resources
0x00000800-0x0000087F	Motherboard resources
0x000000F0-0x000000F0	Numeric data processor
0x0000F050-0x0000F057	Standard SATA AHCI Controller
0x0000F040-0x0000F043	Standard SATA AHCI Controller
0x0000F020-0x0000F03F	Standard SATA AHCI Controller
0x000003F8-0x000003FF	Communications Port (COM1)
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer

Address	Device Description
0x00000000-0x00000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x0000E000-0x0000EFFF	Intel(R) Xeon(R) E3 - 1200/1500 v5/6th Gen Intel(R) Core(TM) PCIe Controller (x16) - 1901
0x0000E000-0x0000EFFF	NVIDIA GeForce GTX 1050
0x000003B0-0x000003BB	Intel(R) Xeon(R) E3 - 1200/1500 v5/6th Gen Intel(R) Core(TM) PCIe Controller (x16) - 1901
0x000003B0-0x000003BB	NVIDIA GeForce GTX 1050
0x000003C0-0x000003DF	Intel(R) Xeon(R) E3 - 1200/1500 v5/6th Gen Intel(R) Core(TM) PCIe Controller (x16) - 1901
0x000003C0-0x000003DF	NVIDIA GeForce GTX 1050
0x0000FF00-0x0000FFFE	Motherboard resources
0x0000F000-0x0000F01F	Intel(R) 100 Series/C230 Series Chipset Family SMBus - A123
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Programmable interrupt controller
0x00000028-0x00000029	Programmable interrupt controller
0x0000002C-0x0000002D	Programmable interrupt controller
0x00000030-0x00000031	Programmable interrupt controller
0x00000034-0x00000035	Programmable interrupt controller
0x00000038-0x00000039	Programmable interrupt controller
0x0000003C-0x0000003D	Programmable interrupt controller
0x000000A0-0x000000A1	Programmable interrupt controller
0x000000A4-0x000000A5	Programmable interrupt controller
0x000000A8-0x000000A9	Programmable interrupt controller
0x000000AC-0x000000AD	Programmable interrupt controller
0x000000B0-0x000000B1	Programmable interrupt controller
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller
0x000000BC-0x000000BD	Programmable interrupt controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x00001854-0x00001857	Motherboard resources

B. Interrupt Request Lines (IRQ)

Peripheral devices use interrupt request lines to notify CPU for the service required. The following table shows the IRQ used by the devices on board.

Level	Function
IRQ 14	Motherboard resources
IRQ 17	High Definition Audio Controller
IRQ 13	Numeric data processor
IRQ 4294967293	Standard SATA AHCI Controller
IRQ 4	Communications Port (COM1)
IRQ 0	System timer
IRQ 4294967294	Intel(R) Xeon(R) E3 - 1200/1500 v5/6th Gen Intel(R) Core(TM) PCIe Controller (x16) - 1901
IRQ 54 ~ IRQ 204	Microsoft ACPI-Compliant System
IRQ 256 ~ IRQ 511	Microsoft ACPI-Compliant System
IRQ 4294967289	Intel(R) Management Engine Interface
IRQ 4294967291	Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 11	Intel(R) 100 Series/C230 Series Chipset Family SMBus - A123
IRQ 11	Intel(R) 100 Series/C230 Series Chipset Family Thermal subsystem - A131
IRQ 4294967292	Intel(R) Ethernet Connection (2) I219-V
IRQ 4294967290	NVIDIA GeForce GTX 1050
IRQ 8	System CMOS/real time clock
IRQ 16	High Definition Audio Controller