EFCO
EverFine Group

U7-100 Series
Compact Fanless Box Computer

User Manual

Version 3.1

Preface

Revision History

Revision	Date	Author	Description
1.0	2018/07/12		Edition release
2.0	2020/06/01	J Yen	Update
3.0	2021/06/07	J Yen	Model name change
3.1	2022/06/030	J Yen	Modify company logo

Copyright

Information provided in this manual is intended to be accurate and reliable. However, EFCO assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, EFCO assumes no liabilities resulting from errors or omissions in this document or the use of the information contained herein.

EFCO reserves the right to make changes in the product design without notice.

Acknowledgments

All brand names and/or trademarks are the properties and registered brands of their respective owners.

For more information about this and other EFCO products, please visit our website at www.efcotec.com.

Declaration of Conformity

FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, according 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.

CE

The product(s) described in this manual complies with all applicable European Union (CE) directives if it has a CE marking. For computer systems to remain CE compliant, only CE-compliant parts may be used. Maintaining CE compliance also requires proper cable and cabling techniques.

Warnings, Cautions, and Notes

Warning!

Warnings indicate conditions, which if not observed, can cause personal injury!

Caution!

Cautions are included to help you avoid damaging hardware or losing data.

Note

Notes provide optional additional information.

Safety Instructions

Please read the following safety instructions carefully.
It is advised that you keep this manual for future reference.

1. All cautions and warnings on the device should be noted.
2. Make sure the power source matches the power rating of the device.
3. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
4. Always completely disconnect the power before working on the system's hardware.
5. No connections should be made when the system is powered on as a sudden rush of energy may damage sensitive electronic components.
6. If the device is not used for an extended period, disconnect the device from the power supply to avoid being damaged by transient over-voltage.
7. Always disconnect this device from any electrical outlet before cleaning.
8. While cleaning, use a damp cloth instead of liquid or spray detergents.
9. Make sure the device is installed near a power outlet and is easily accessible.
10. Keep this device away from any humidity.
11. Place the device on a solid surface during installation to prevent falls.
12. Do not cover the openings on the device to ensure optimal heat dissipation.
13. System enclosure may get hot during operation, use caution when handling.
14. Do not touch the heat sink or heat spreader when the system is running.
15. Never pour any liquid into the openings. This could cause fire or electric shock.
16. As most electronic components are sensitive to a static electrical charge, be sure to ground yourself to prevent static charge(s) when installing the internal components. Use a grounding wrist strap and contain all electronic components in static shielded containers.
17. If any of the following situations arises, please contact our service personnel:
    I. Damaged power cord or plug.
    II. Liquid intrusion to the device.
    III. Exposure to moisture.
    IV. The device is not working as expected or in a manner as described in this manual.
    V. The device is dropped or damaged.
    VI. Any visible signs of damage displayed on the device.
18. Do Not store this device in an uncontrolled environment where the ambient temperatures are BELOW -40°C (-40°F) or ABOVE 85°C (185°F) to prevent damage.

Table of Contents

Chapter 1

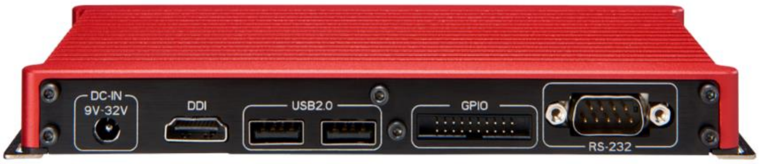
General Introduction

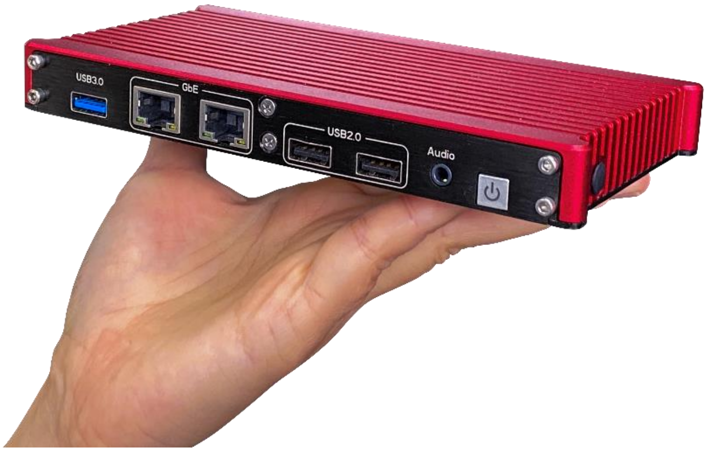
This chapter includes:

- Overview
- Product Features Specifications
- Supported CPU List
- Packing List
- Ordering Information

1.1 Overview

The U7-100 is a compact fanless box computer that has an ultra-slim size with an aluminum alloy structure. The U7-100 series support 3rd Generation Intel® Atom™ Processor, Celeron® Processor (formerly Bay Trail platform), and is designed for dedicated IoT applications such as Thin Client, Machine Vision, along with applications for factory automation, digital signage, kiosk engines, point of sale devices, and gateway programs with limited space.





1.2 Common Specifications

Model Name	U7-150	U7-130	U7-131
Mechanical			
Dimensions	173 mm x 88 mm x 21.7 mm (6.81” x 3.46” x0.85”)		
Weight	0.75kg		
Mounting	2x wall mount brackets		
Construction	Aluminum alloy structure		
Battery	N/A		
System			
Intel® Platform	Apollo Lake	Bay Trail	
CPU	Intel® Pentium® N4200 1.1/2.5 GHz, Quad Core L2 cache 2MB, 6W TDP	● Intel® Celeron® N2807 1.58 GHz, Dual Core L2 cache 1MB, 4.5W TDP ● Intel® Atom™ E3815 1.46 GHz, Single Core L2 cache 512KB, 5W TDP	
Chipset	N/A	Integrated into the SoC	
Graphics	Intel® HD Graphics Generation 9	Intel® HD Graphics Generation 7	
Memory	DDR3L with 1867 MT/s, 8GB (Max.)	DDR3L with 1333 MT/s, 8GB (Max.)	
BIOS	AMI Aptio® UEFI 2.x firmware		
Watchdog Timer	Multistage		
Operating System	Windows 10 Windows 10 IoT Enterprise 64-bit	Windows 7 Windows 7 embedded compact Windows 8 Windows Embedded 8 Standard Linux	
Power			
DC Input	9 – 32 V		
Power Mode	AT/ATX (Jumper setting)		
Storage			
mSATA	1x mSATA socket		
External			
Video Port Combination(s)	1x DDI		
GbE	2x RJ45 GbE		
USB	1x USB 3.0/2.0 port, 4x USB 2.0 ports		
COM	1x RS-232 port		
DIO	16-bit programmable GPIO		
Audio	1x Mic-in/Line-out		
USIM Socket	2x USIM sockets		
Expansion Slot			
Mini PCIe	2x Full-length Mini PCIe slot (PCIe + USB + USIM)		
Other			
Antenna	3x Antenna openings		
LED	1x Power LED (with Power Button)		
Environment			
Operating Temperature	-20ºC - +60ºC (-4ºF - +140ºF)		
Storage Temperature	-40 ºC - +85ºC (-40ºF - +185ºF)		
Relative Humidity-Operating	10% - 90% Humidity, non-condensing		
Relative Humidity-Storage	5% - 95% Humidity, non-condensing		
Certificates			
EMC	CE/FCC Class A		

1.3 Supported CPU List

The U7-100 series supports the 3rd Generation Intel® Atom™ and Celeron® processors (formerly Bay Trail platform).

Intel® Celeron® N2807 1.58 GHz Dual Core L2 cache 1MB 4.5W TDP

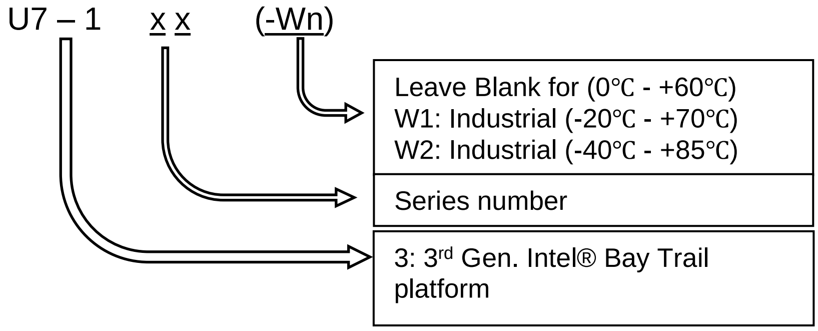
1.4 Packing List

When you receive the package of the U7-100, please check immediately if the package contains all the items listed in the following table. If any item is missing or damaged, please contact your local dealer or EFCO for further assistance.

Quantity	Item
1	U7-100 compact fanless box computer
1	AC/DC Power Adapter (24V/40W)
1	AC/DC Power Cord YP-12/YC-12, plug type B
2	Wall mount brackets

1.5 Ordering Information

Model Name Description


U7 – 1 x x (-Wn)
Leave Blank for (0℃ - +60℃)
W1: Industrial (-20℃ - +70℃)
W2: Industrial (-40℃ - +85℃)
Series number
3: 3rd Gen. Intel® Bay Trail platform

Model Name	Description (CPU, Memory)
U7-150	Base Model System
U7-130	Intel® Celeron® N2807, 4GB memory
U7-131	Intel® Atom™ E3815, 1GB memory

Chapter 2

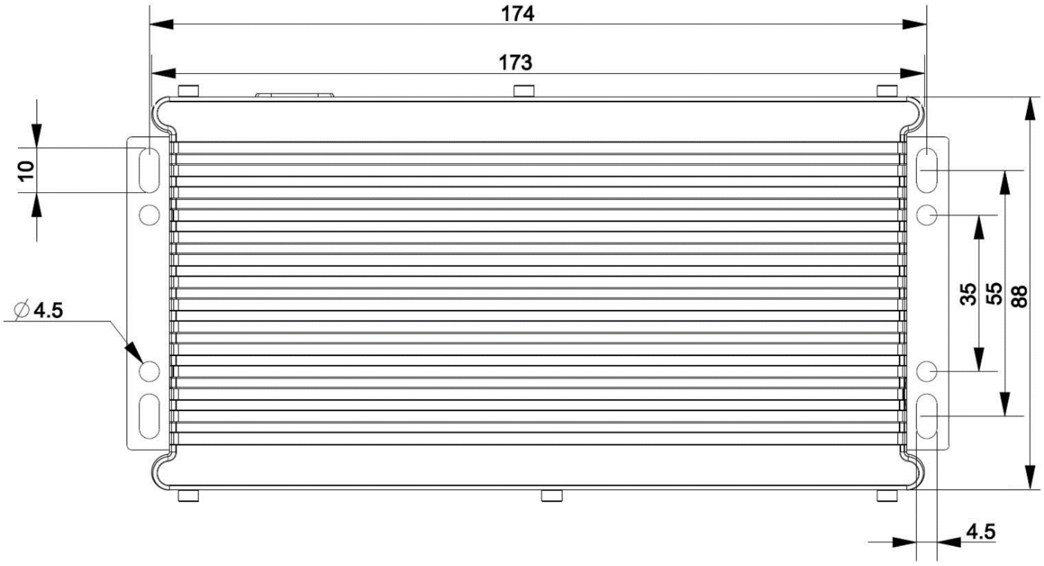
Mechanical Dimensions

This chapter includes:

- ➢ Top View
- ➢ Front View
- ➢ Rear View
- ➢ Left-Side View
- ➢ Right-Side View
- ➢ Bottom View

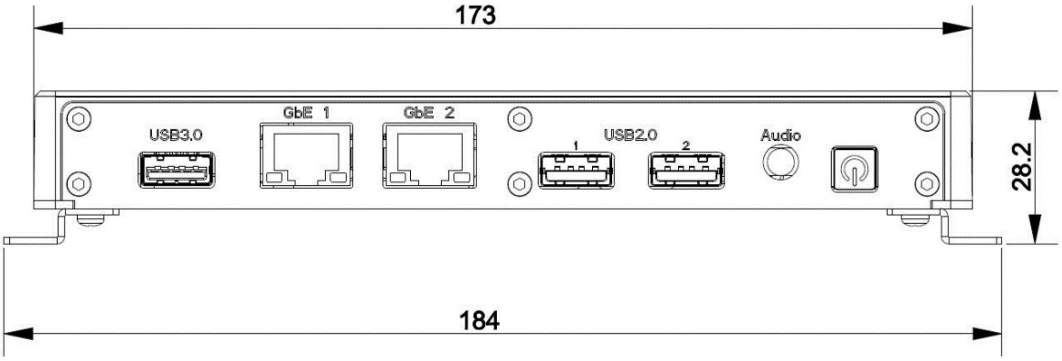
2.1 Top View

Unit: mm



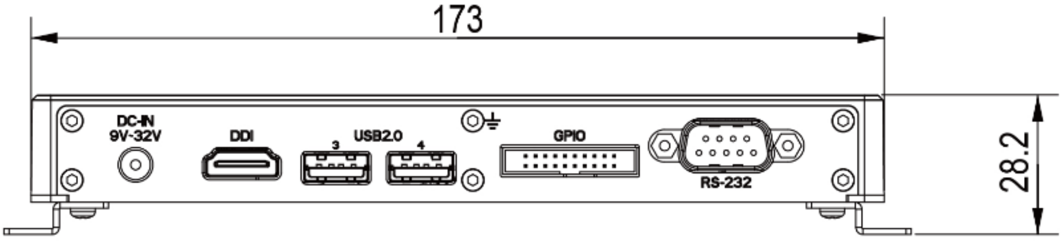
2.2 Front View

Unit: mm



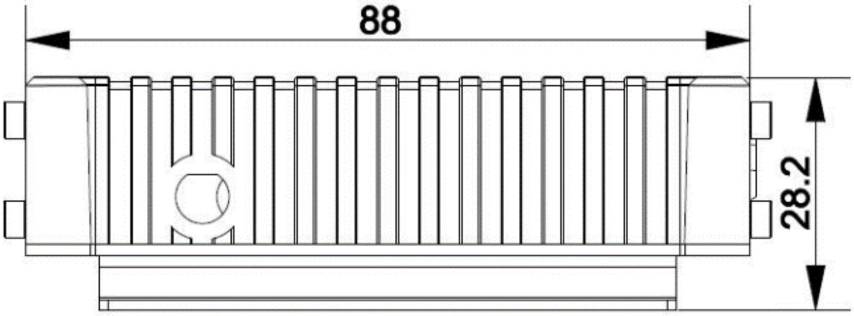
2.3 Rear View

Unit: mm



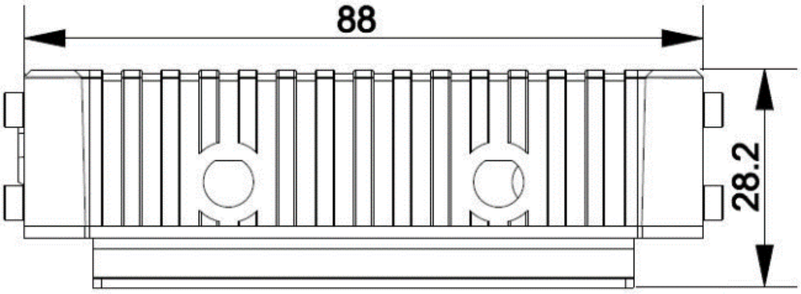
2.4 Right-Side View

Unit: mm



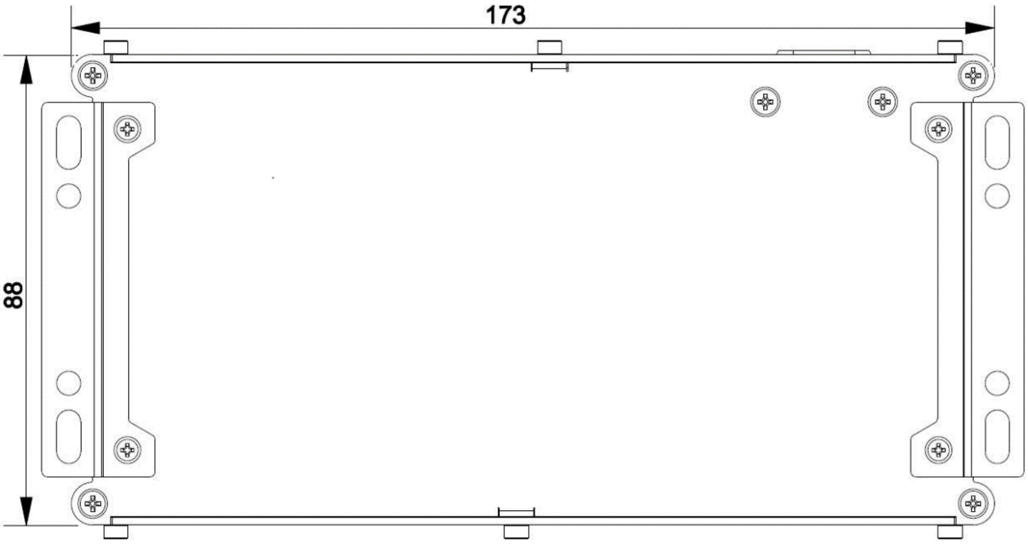
2.5 Left-Side View

Unit: mm



2.6 Bottom View

Unit: mm



Chapter 3

Hardware Function Description

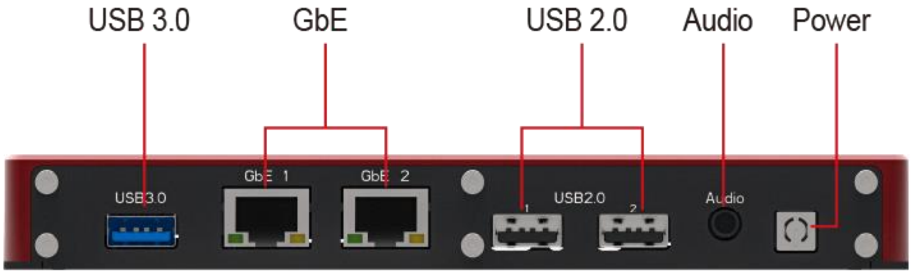
This chapter includes:

- I/O Layout
- Front Panel I/O Function
- Rear Panel I/O Function
- Right-Side I/O Function
- SSD Drive Bay
- IOM
- Card Expansion

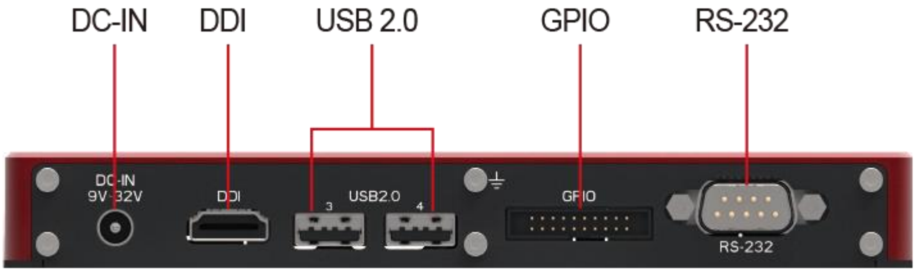
3.1 I/O Layout

The U7-100 provides sufficient I/O ports on the front panel, rear panel, right-side, and left-side panel.

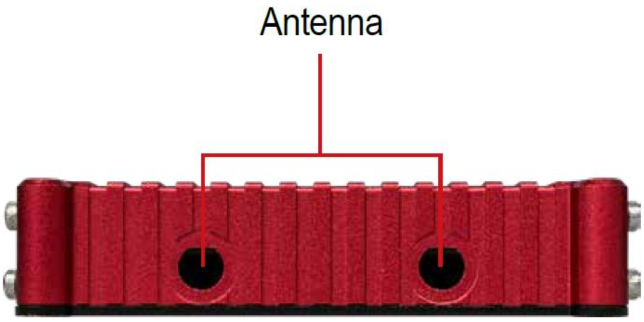
Front I/O



Rear I/O



Right side/Left side I/O

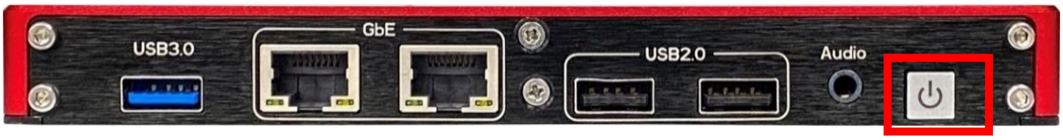


3.2 Front Panel I/O Function

Most standard computer I/O functions are placed on the front panel. In this section, we'll illustrate each I/O feature on the front panel.

3.2.1 Power Button with Power LED

The power button is a non-latched switch with LED for ATX mode on/off operation. To turn on the U7-100, press the power button, and the Green LED will light up. To turn off the U7-100, a command in the OS can be issued to shut down the system, or just simply press the power button. To force a hard reset, press and hold the power button for 5 seconds to manually shut down the system.

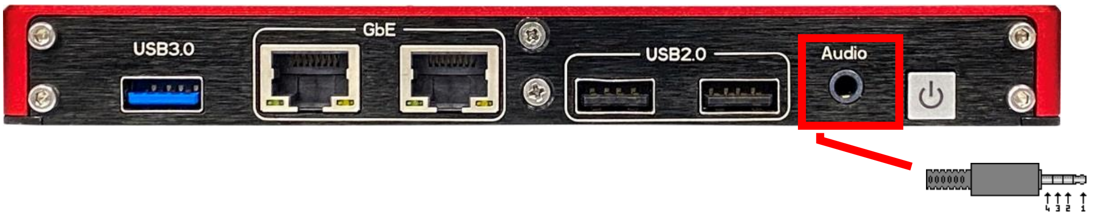


Note ☞

A five-second interval is required by the system between two on/off operations (i.e., once the system is turned off, you need to wait for five seconds to initiate another power-on operation).

3.2.2 Line-out and Mic-in Audio Jacks

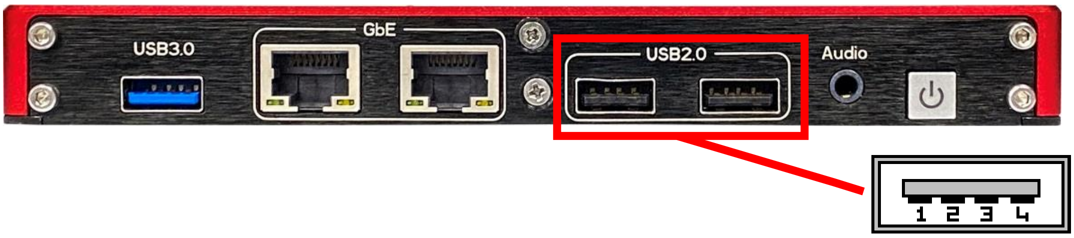
The U7-100 provides High Definition Audio functionality via the internal HDA logic of the Intel® Bay Trail SoC in combination with a Realtek ALC262 codec. There is a 3.5mm audio jack on the front panel. To utilize the audio function in Windows, you need to install the corresponding drivers for both Intel® Bay Trail SoC chipset and Realtek ALC262 codec.



PIN	Pin Name	Description
1	Mic-In	Microphone input signal
2	Audio R	Right Audio output signal
3	Audio L	Left Audio output signal
4	GND	Audio Ground

3.2.3 USB 2.0 Port

The U7-100 provides four USB 2.0 Type A connectors. Two ports on the front side and two ports on the rear side.

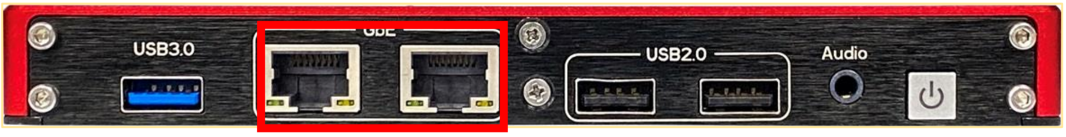


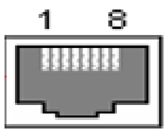
PIN	Name	Description
1	VCC	+5 VDC
2	D-	Data -
3	D+	Data +
4	GND	Ground

3.2.4 Gigabit Ethernet Port

The U7-100 offers two Gigabit Ethernet (GbE) ports that use Intel® i210 Gigabit Ethernet controllers. The GbE ports are located on the front panel and will support Wake-on-LAN function. When you plug in the Ethernet cable, you will see the Ethernet status and speed from the LED indicators on the RJ45 connector as follows:

1000 Base-T uses all pairs for bidirectional traffic in the RJ45 connector. Recommended cables to be used are the Category 5e (enhanced).





PIN	Name	Description
1	BI_DA+	Bi-directional pair A +
2	BI_DA-	Bi-directional pair A -
3	BI_DB+	Bi-directional pair B +
4	BI_DC+	Bi-directional pair C +
5	BI_DC-	Bi-directional pair C -
6	BI_DB-	Bi-directional pair B -
7	BI_DD+	Bi-directional pair D +
8	BI_DD-	Bi-directional pair D -

Active/Link LED

LED Color	Status	Description
Yellow	OFF	The Ethernet port is disconnected.
	ON	Ethernet port is connected with no data transmission
	Blinking	Ethernet port is connected, and data is transmitting/receiving

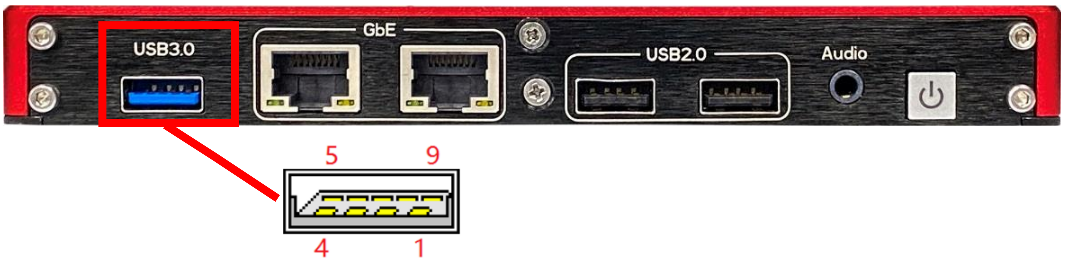
Speed LED

LED Color	Status	Description
Green Or Orange	OFF	10Mbps
	Green	100Mbps
	Orange	1000Mbps

To utilize the GbE port in Windows, you will need to install the corresponding driver for the Intel® i210 GbE controller.

3.2.5 USB 3.0 Connector

The U7-100 offers one USB 3.0 (SuperSpeed USB) port Type A connector on the front panel. The BIOS default is xHCI (Extensible Host Controller Interface) mode and is compatible with USB 3.0, USB 2.0, USB 1.1 and USB 1.0 devices. Legacy USB support is also provided so that you can use a USB keyboard/mouse in a DOS environment. To use the USB 3.0 port in a Windows environment, you will need to install the USB 3.0 driver.



PIN	Name	Description
1	VBus	+5V Power
2	USB D-	USB 2.0 data
3	USB D+	
4	GND	Ground for power return
5	StdA SSRX-	SuperSpeed receiver
6	StdA SSRX+	SuperSpeed receiver
7	GND DRAIN	Ground for signal return
8	StdA SSTX-	SuperSpeed transmitter
9	StdA SSTX+	SuperSpeed transmitter

Note

Intel USB 3.0 driver does not support Windows XP. In Windows XP, all USB 3.0 ports will work in USB 2.0 mode.

3.1

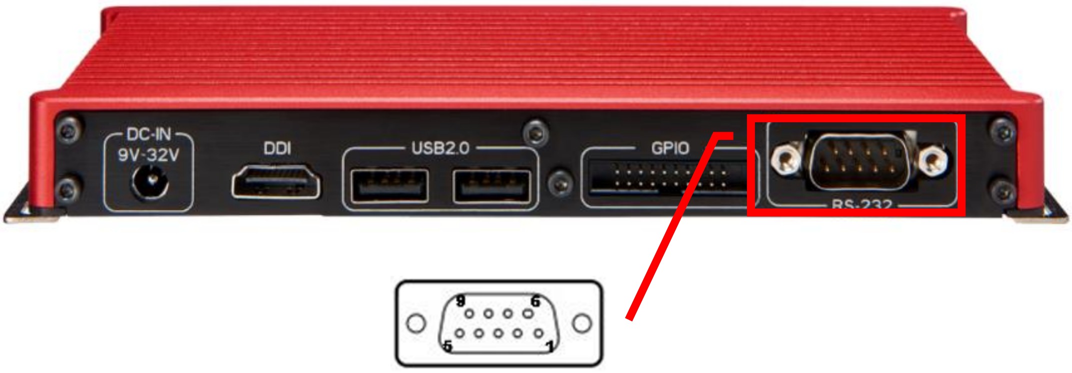
3.3 Rear Panel I/O Function

For more general application requirements, the U7-100 offers more I/O functions on the back panel.

3.3.1 COM Port

The U7-100 provides one UART port on the rear panel for communicating with external devices. COM1 is located on the back panel via 9-pin D-Sub male connectors.

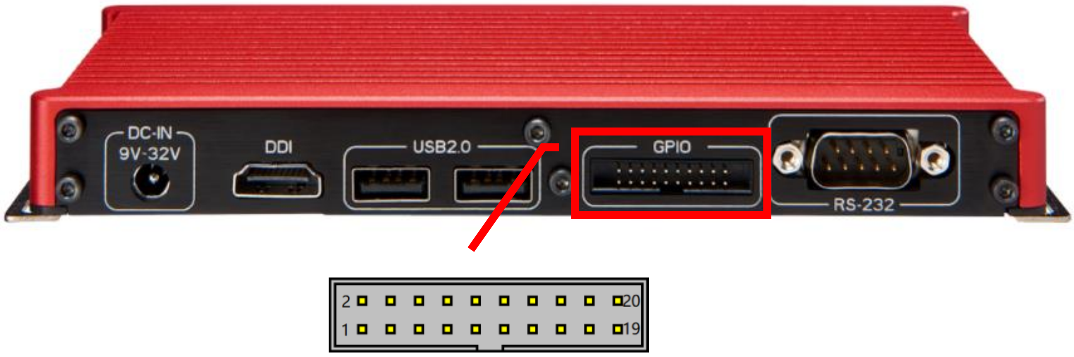
The UART ports support legacy speeds up to 115.2K bps as well as higher baud rates of 230K, 460K, or 921K bps to support higher-speed modems. All driver outputs and receiver inputs are protected against ESD strikes up to ±15Kvolts (IEC 61000-4-2 Air Gap).



D-sub-9	Signal Name	Description
1	N/A	N/A
2	UART1 RXD	Receive Data
3	UART1 TXD	Transmit Data
4	N/A	N/A
5	UART1 GND	System Ground
6	N/A	N/A
7	UART1 RTS#	Request to Send
8	UART1 CTS#	Clear to Send
9	N/A	N/A

3.3.2 DIO (Digital IO)

The U7-100 offers 16-bit programmable digital input/output (DIO) for operating directly with TTL or 5-V CMOS devices. Each bit is programmable with software.



GPIO 1 Table

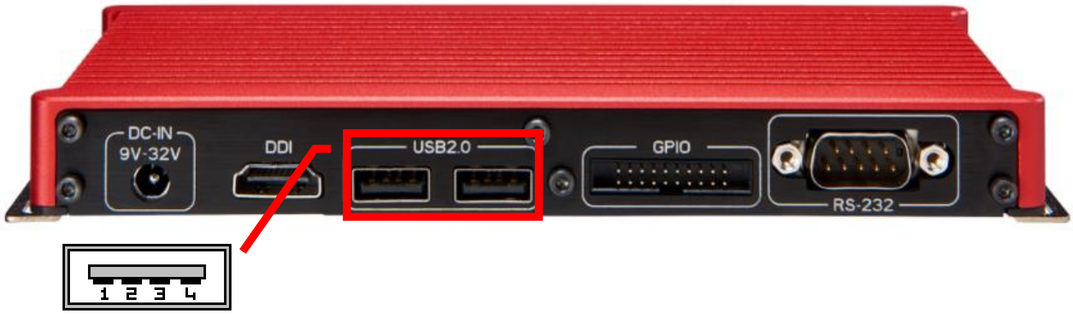
PIN	Name	Mapping I2C GPIO Function
19	GPIO 0	I2C IO 00
17	GPIO 1	I2C IO 01
15	GPIO 2	I2C IO 02
13	GPIO 3	I2C IO 03
11	GPIO 4	I2C IO 04
9	GPIO 5	I2C IO 05
7	GPIO 6	I2C IO 06
5	GPIO 7	I2C IO 07
3	GND	Common Ground
1	VCC3V3	Common Voltage

GPIO 2 Table

PIN	Name	Mapping I2C GPIO Function
20	GPIO 8	I2C IO 10
18	GPIO 9	I2C IO 11
16	GPIO 10	I2C IO 12
14	GPIO 11	I2C IO 13
12	GPIO 12	I2C IO 14
10	GPIO 13	I2C IO 15
8	GPIO 14	I2C IO 16
6	GPIO 15	I2C IO 17
4	GND	Common Ground
2	VCC3V3	Common Voltage

3.3.3 USB 2.0 Port

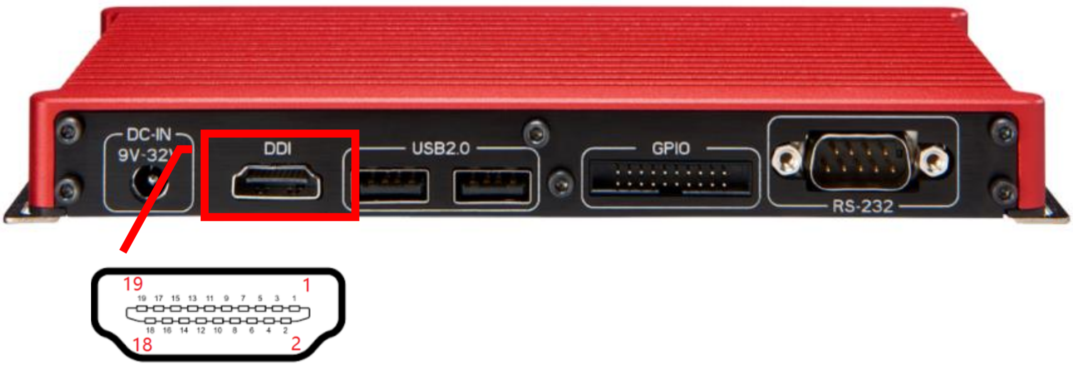
The U7-100 provides two additional ports for USB 2.0 Type A connectors on the rear panel.



PIN	Name	Description
1	VCC	+5 VDC
2	D-	Data -
3	D+	Data +
4	GND	Ground

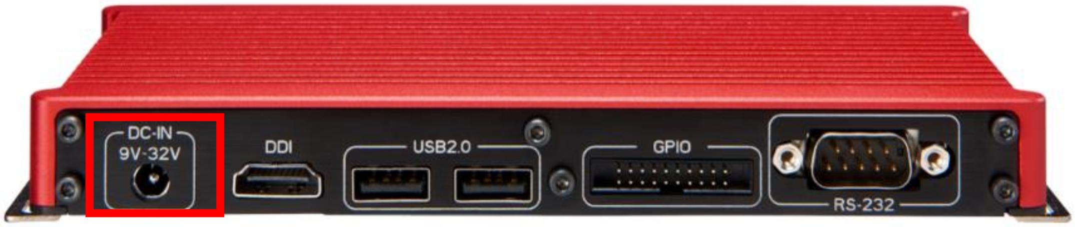
3.3.4 DDI Connector

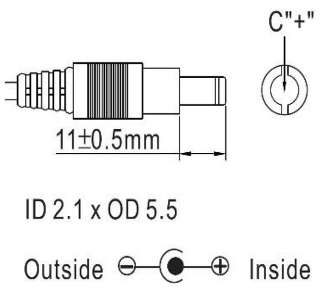
The U7-100 provides a high-resolution DDI display output on the front panel and will support display resolution up to 1920x1200. To achieve the best DDI output resolution in Windows, you need to install the corresponding graphics driver.



PIN	Signal	Description	PIN	Signal	Description
1	TMDS Data2+		11	TMDS Clock Shield	
2	TMDS Data2 Shield		12	TMDS Clock-	
3	TMDS Data2-		13	CEC	control
4	TMDS Data1+		14	Reserved/HEC Data−	N.C. on device
5	TMDS Data1 Shield		15	SCL	DDC clock
6	TMDS Data1-		16	SDA	DDC data
7	TMDS Data0+		17	DDC/HEC/CEC Ground	
8	TMDS Data0 Shield		18	+5 V Power	power EDID/DDC
9	TMDS Data0-		19	Hot Plug Detect/HEC Data+	
10	TMDS Clock+				

3.3.5 DC Jack for DC Input





The U7-100 series allows a wide range of DC power input from 9V to 32V. It offers a 2-pin DC power jack. The 2-pin power connector is used to connect the power plug of an AC/DC adapter. It's convenient for indoor usage where AC power is available. Since there is no specific rule of pin definition for this type of connector, confirm the polarity of the power connector before plugging it into U7-100 if you're not using the power adapter provided by EFCO.

Caution!

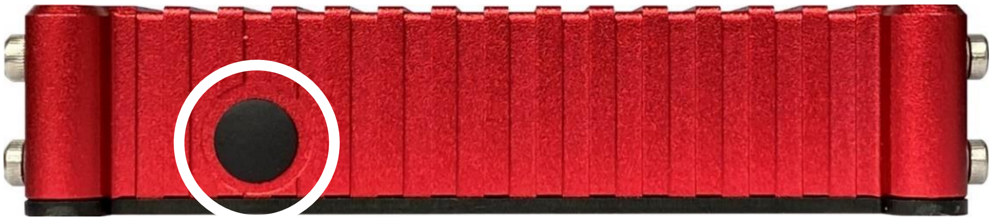
1. Make sure the polarity of the power plug and voltage is correct before plugging it into the system
2. Supplying a voltage over 32V will damage the system.

3.2 Left-side and Right-side Panel I/O Function

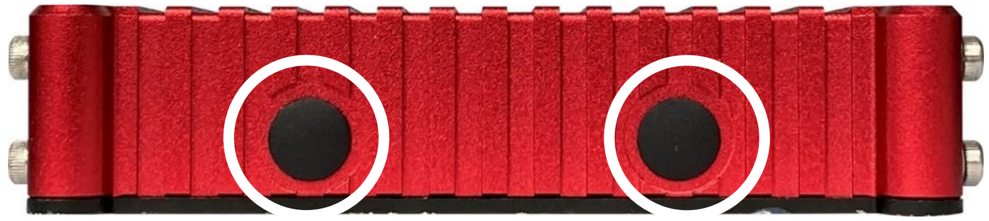
The U7-100 offers more I/O functions on its left-side and right-side panel.

3.4.1 Antenna Hole

The U7-100 series provides three antenna holes for wireless applications.



Left-side Panel



Right-side Panel

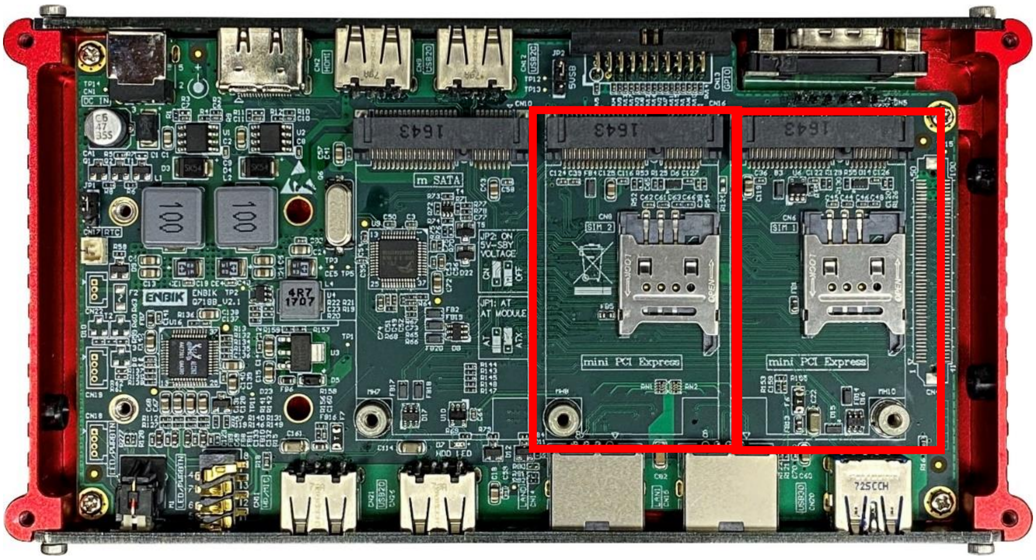
3.3 Internal I/O Functions

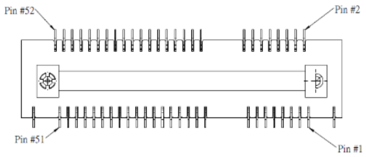
U7-100 provides other useful features via the on-board connectors, such as one mSATA socket and two Mini PCIe sockets.

The U7-100 provides two onboard full-length Mini PCIe slots with USIM sockets. By installing a Mini PCIe module, your system can support expanded features such as Wi-Fi, 3G, 4G, GPS, and Bluetooth.

3.5.1 Mini PCI Express Connector (with USIM Socket)

Two full-length Mini PCIe connectors are designed with USIM card support. With a USIM card installed, the unit is capable of connecting your system to the internet through a local telecom operator’s GPRS/3G/4G network. For Wi-Fi /3G/4G communication, the U7-100 provides multiple SMA antenna apertures on the side panels for multi-antenna configuration.





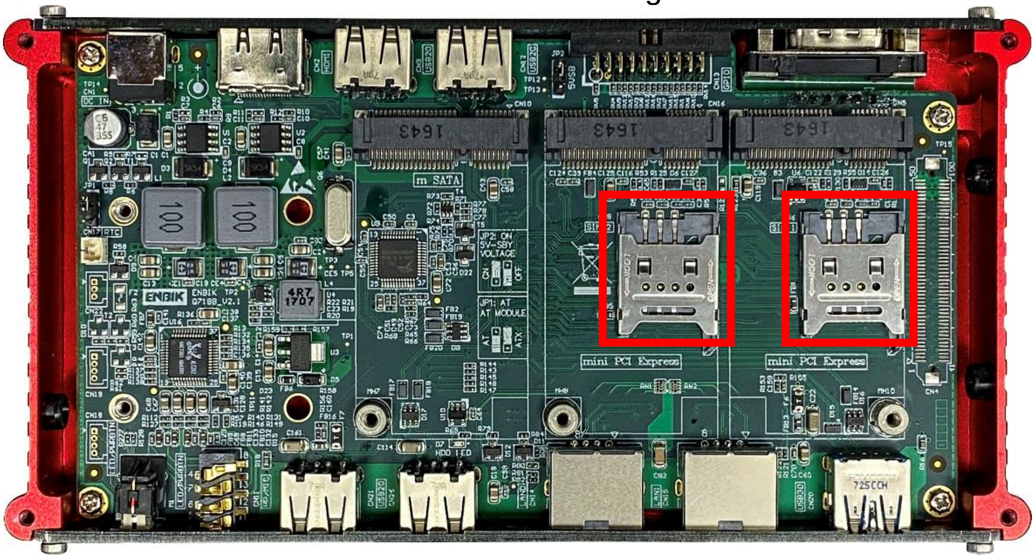
Top Side	
1	PCIe Wake#
3	Reserved
5	Reserved
7	PCIe CLKREQ#
9	GND
11	PCIe REFCLK-
13	PCIe REFCLK+
15	GND

Bottom Side	
2	3.3V
4	GND
6	1.5V
8	UIM PWR
10	UIM DATA
12	UIM CLK
14	UIM RESET
16	UIM VPP

Mechanical Key			
17	Reserved (UIM C8)	18	GND
19	Reserved (UIM C4)	20	Reserved
21	GND	22	PCIe RST#
23	PCIe PERn0	24	+3.3V SB
25	PCIe PERp0	26	GND
27	GND	28	+1.5V
29	GND	30	SMB CLK
31	PCIe PETn0	32	SMB DATA
33	PCIe PETp0	34	GND
35	GND	36	USB D-
37	GND	38	USB D+
39	+3.3V	40	GND
41	+3.3V	42	LED WWAN#
43	GND	44	LED WLAN#
45	Reserved	46	LED WPAN#
47	Reserved	48	+1.5V
49	Reserved	50	GND
51	Reserved	52	+3.3V

3.5.2 USIM Socket

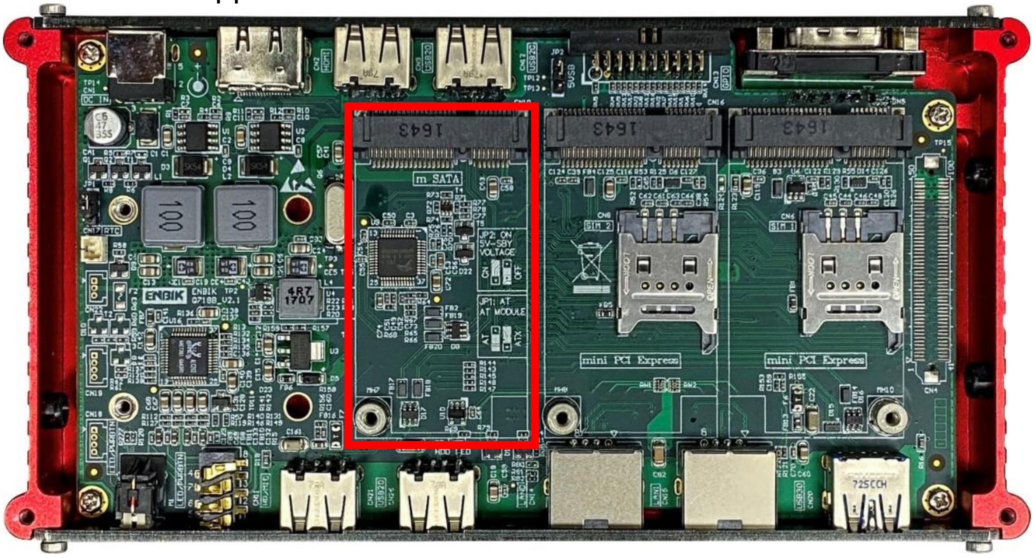
The U7-100 series provides 2 USIM sockets for wireless applications when a 3G/4G wireless module is installed into a full-length Mini PCIe socket.

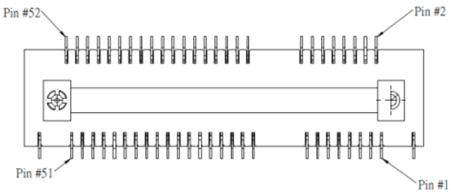


PIN	Name	Description
C1	VCC	+5 VDC power supply input (optional use by the card)
C2	RESET	Reset signal, used to reset the card's communications. Either used by itself (reset signal supplied from the interface device) or in combination with an internal reset control circuit (optional use by the card). If internal reset is implemented, the voltage supply on VCC is mandatory
C3	CLOCK	Provides the card with a clock signal, from which data communications timing is derived
C4	RESERVED	AUX1, optionally used for USB interfaces and other uses.
C5	GND	Ground (reference voltage)
C6	VPP	Programing voltage input (optional). This contact may be used to supply the voltage required to program or to erase the internal non-volatile memory. ISO/IEC 7816-3:1997 designated this as a programming voltage: an input for a higher voltage to program persistent memory (e.g., EEPROM). ISO/IEC 7816-3:2006 designates it SPU, for either standard or proprietary use, as input and/or output.
C7	I/O	Input or Output for serial data (half-duplex) to the integrated circuit inside the card.
C8	RESERVED	AUX2, optionally used for USB interfaces and other uses.

3.5.3 mSATA Socket

The U7-100 supports one mSATA SSD socket.

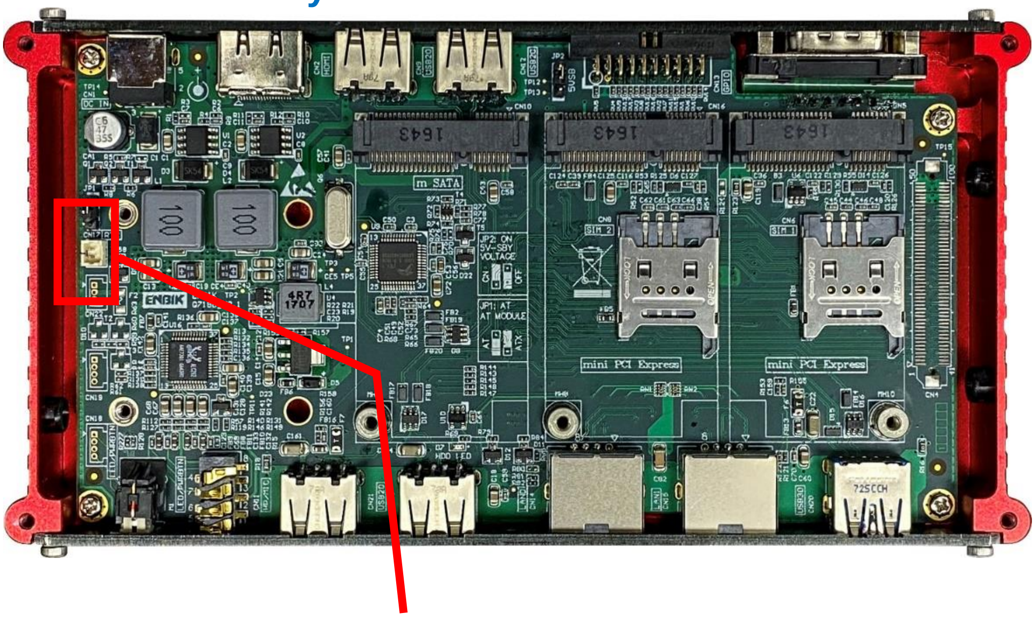


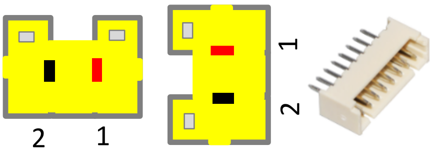


Top Side			Bottom Side	
1	NC		2	3.3V
3	NC		4	GND
5	NC		6	NC
7	NC		8	NC
9	GND		10	NC
11	NC		12	NC
13	NC		14	NC
15	GND		16	NC

Mechanical Key				
17	NC		18	GND
19	NC		20	NC
21	GND		22	NC
23	SATA_Rp0		24	+3.3V
25	SATA_Rn0		26	GND
27	GND		28	NC
29	GND		30	NC
31	SATA_Tn0		32	NC
33	SATA_Tp0		34	GND
35	GND		36	NC
37	GND		38	NC
39	+3.3V		40	GND
41	+3.3V		42	NC
43	NC		44	NC
45	NC		46	NC
47	NC		48	NC
49	NC		50	NC
51	NC		52	+3.3V

3.5.4 CMOS Battery Connector





2-pin wafer, pitch 1.25mm
Brand: TXGA
Model name: FWF12506-S02S24W5M

PIN	Name	Function
1	RTC Bat	RTC Battery V+
2	GND	RTC Battery Ground

Chapter 4

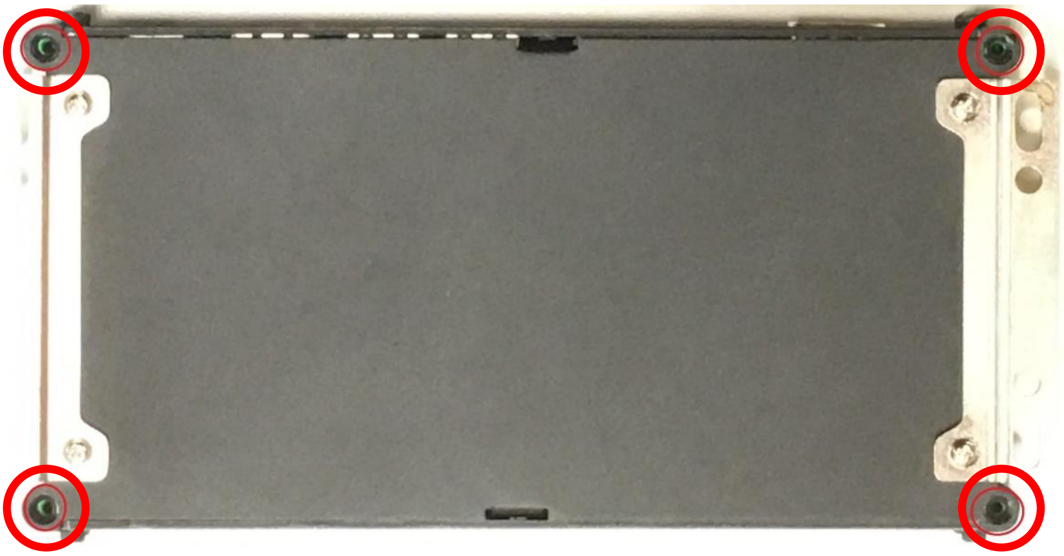
Hardware Installation

This chapter includes:

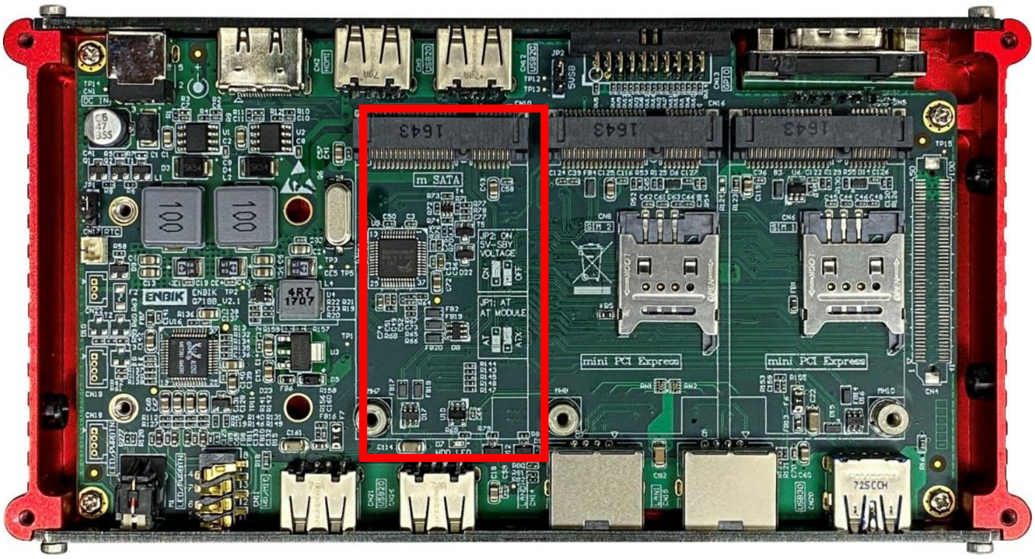
- LGA1151 CPU Installation and Replacement
- SO-DIMM Memory Installation
- Mini PCIe / mSATA Module Installation
- 2.5” SATA SSD/HDD Installation
- IOM Installation
- Mounting Bracket Installation

4.1 mSATA SSD Installation

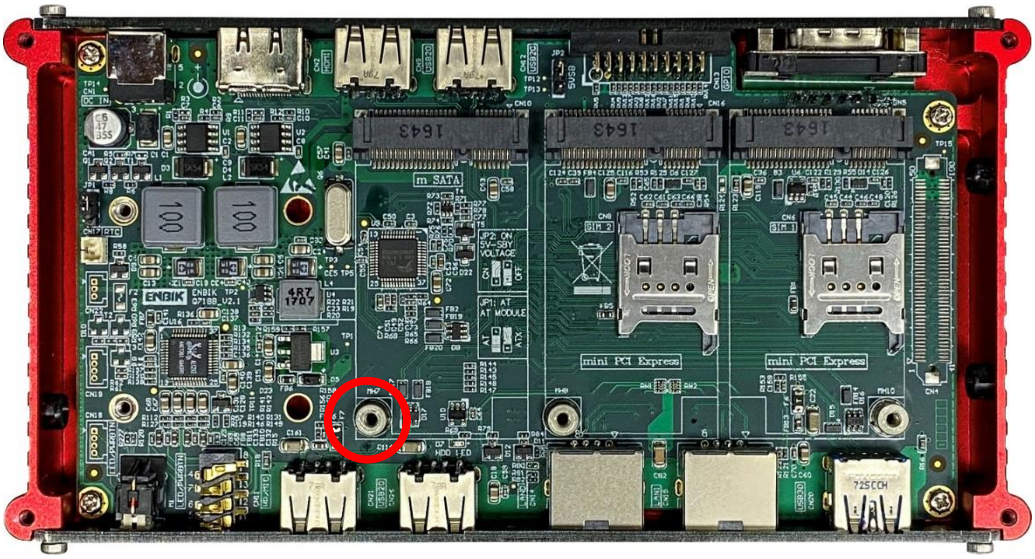
1. Remove the bottom screws and cover



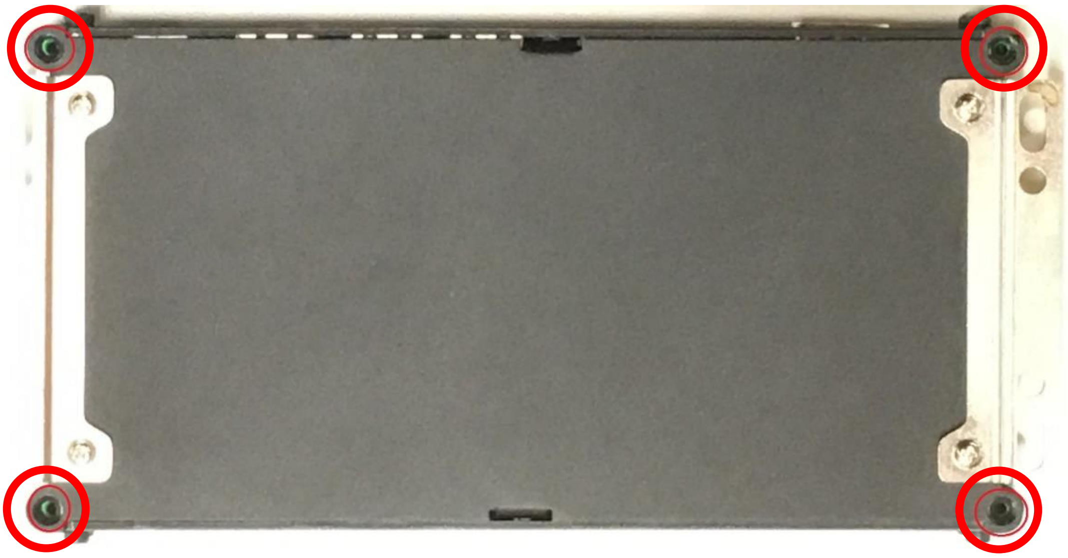
2. Find the mSATA socket



3. Place the mSATA SSD module into the socket and fix the module with M2.5 screws.

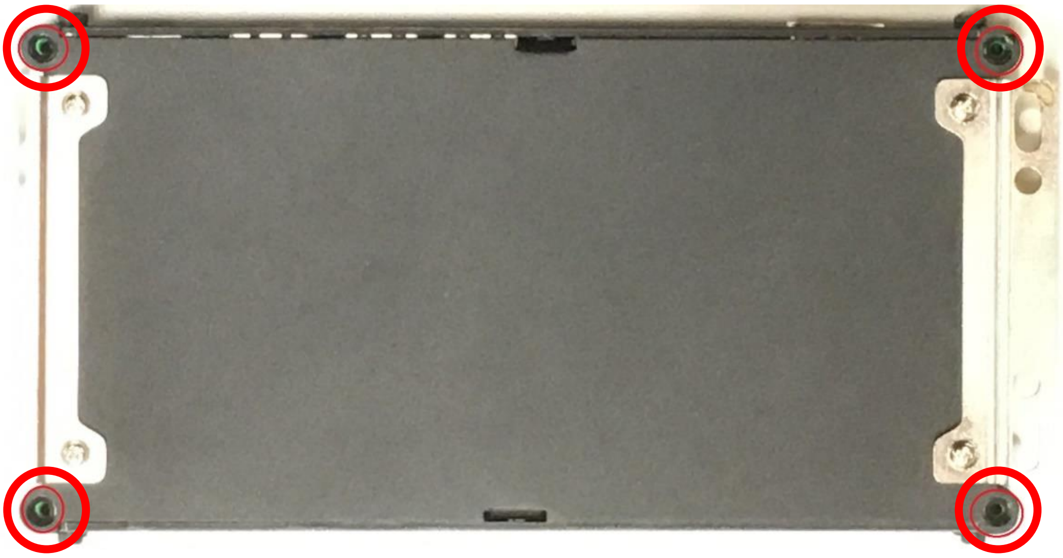


4. Reinstall the bottom cover and screws.

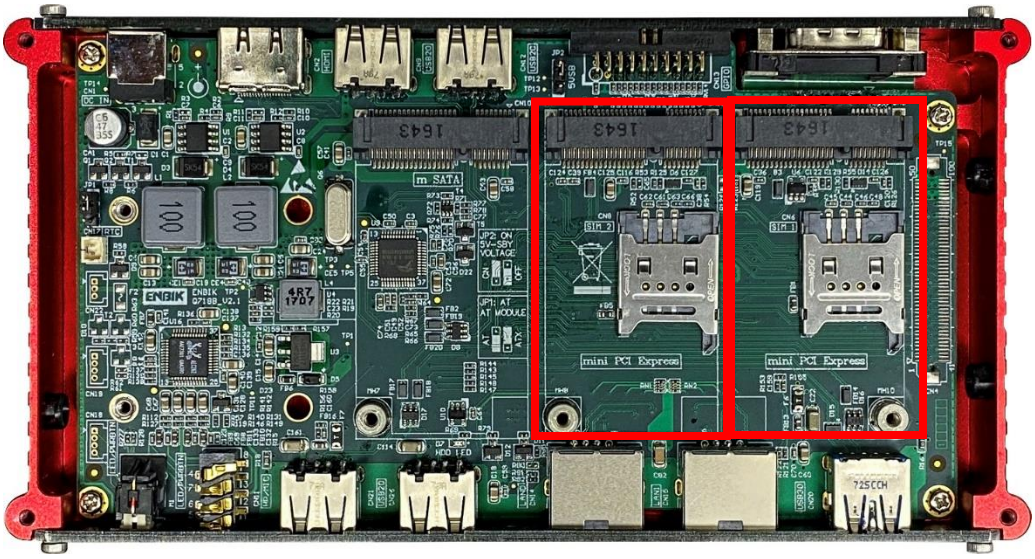


4.2 Mini PCIe Module Installation

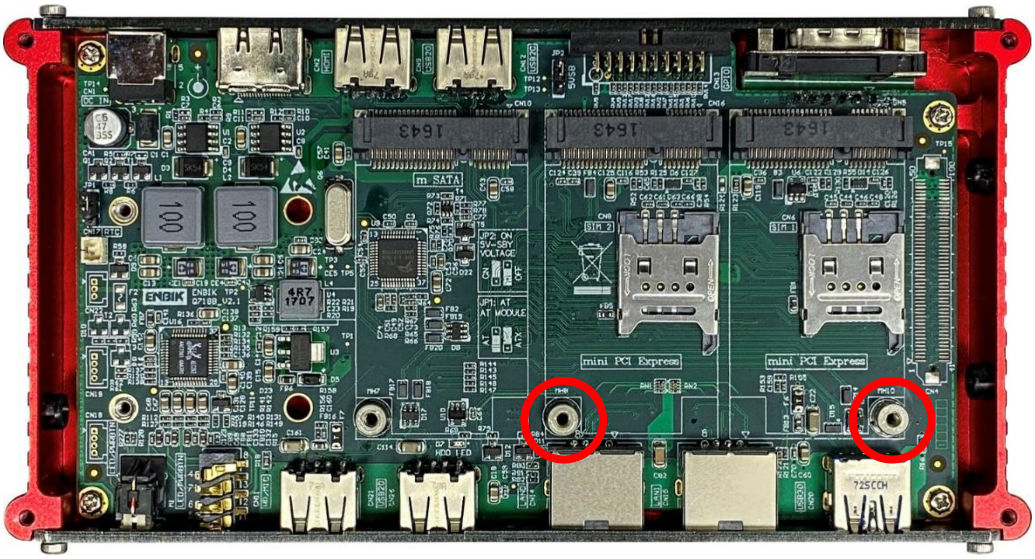
1. Remove the bottom screws and cover



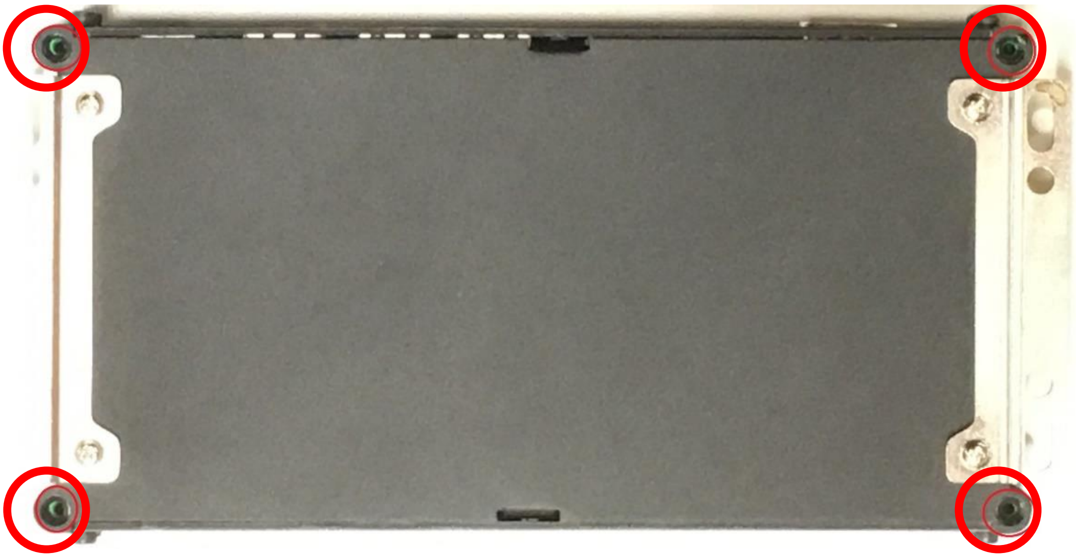
2. Find the full-length Mini PCIe socket



3. Place the Mini PCIe module into the socket and fix the module with M2.5 screws.



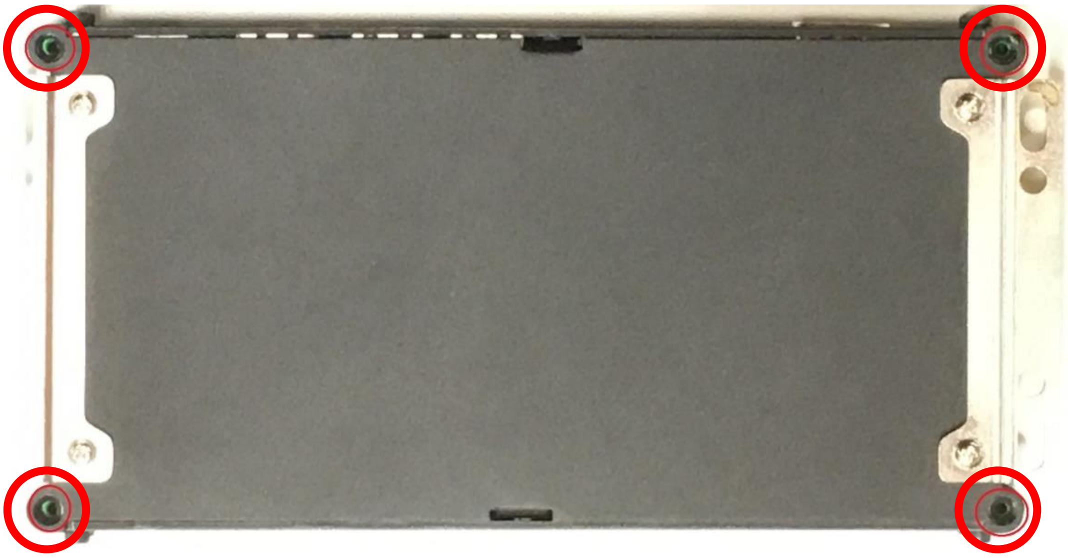
4. Reinstall the bottom cover and screws



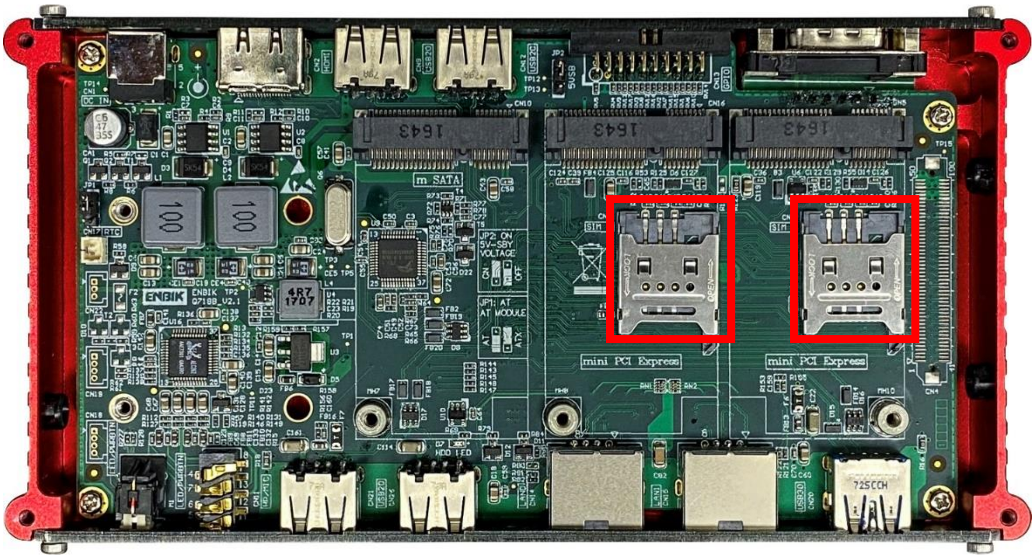
.

4.3 USIM Card Installation

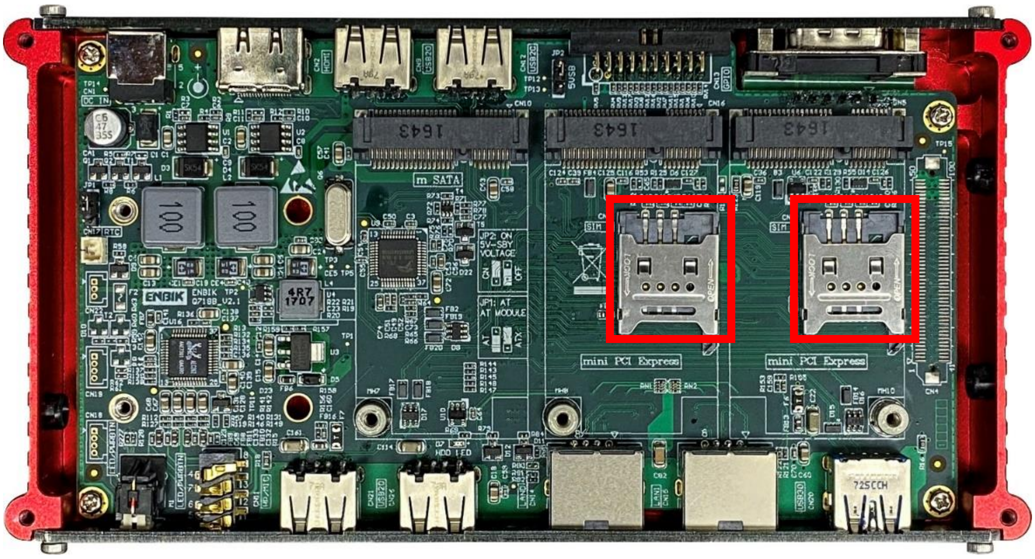
1. Remove the bottom screws and cover



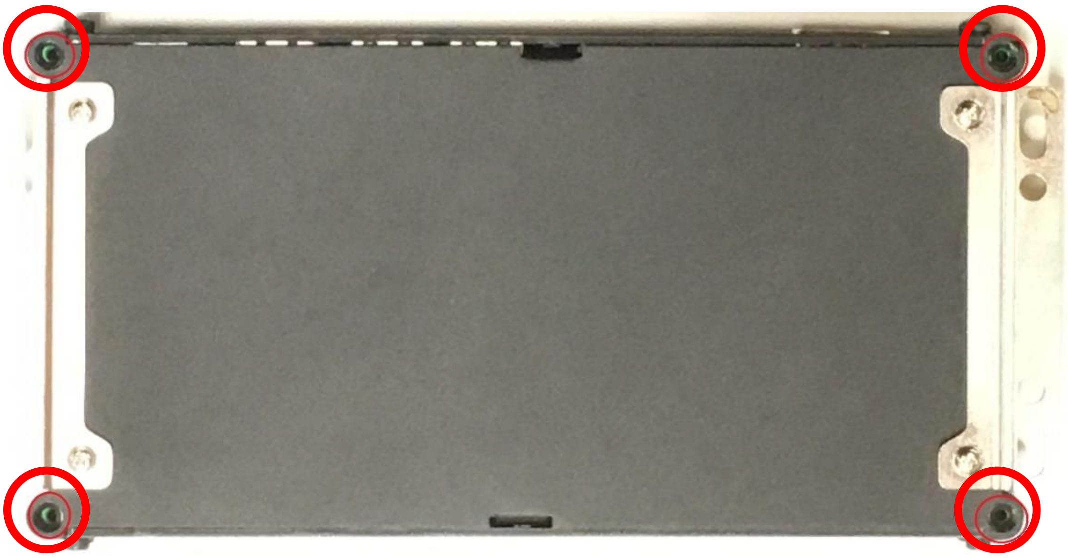
2. Find the USIM card socket and pull the locker open



3. Place the USIM card into the socket and pull the locker close.



4. Reinstall the bottom cover and screws.



Chapter 5

Function Settings

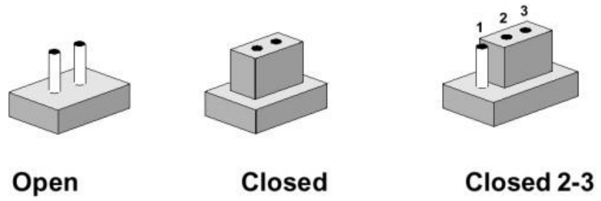
This chapter includes:

- Jumper
- AT/ATX Power Mode Select

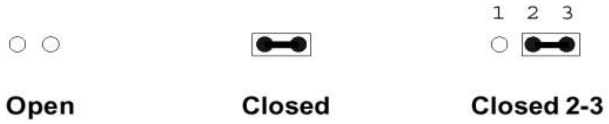
5.1 Jumper

You can configure your board to match the needs of your application by setting jumpers. A jumper is the simplest kind of electric switch.

It consists of two metal pins and a small metal clip (often protected by a plastic cover) that slides over the pins to connect them. To “close” a jumper, you connect the pins with the clip. To “open” a jumper, you remove the clip. Sometimes a jumper will have three pins, labeled 1, 2, and 3. In this case, you would connect two pins.



The jumper settings are schematically depicted in this manual as follows:

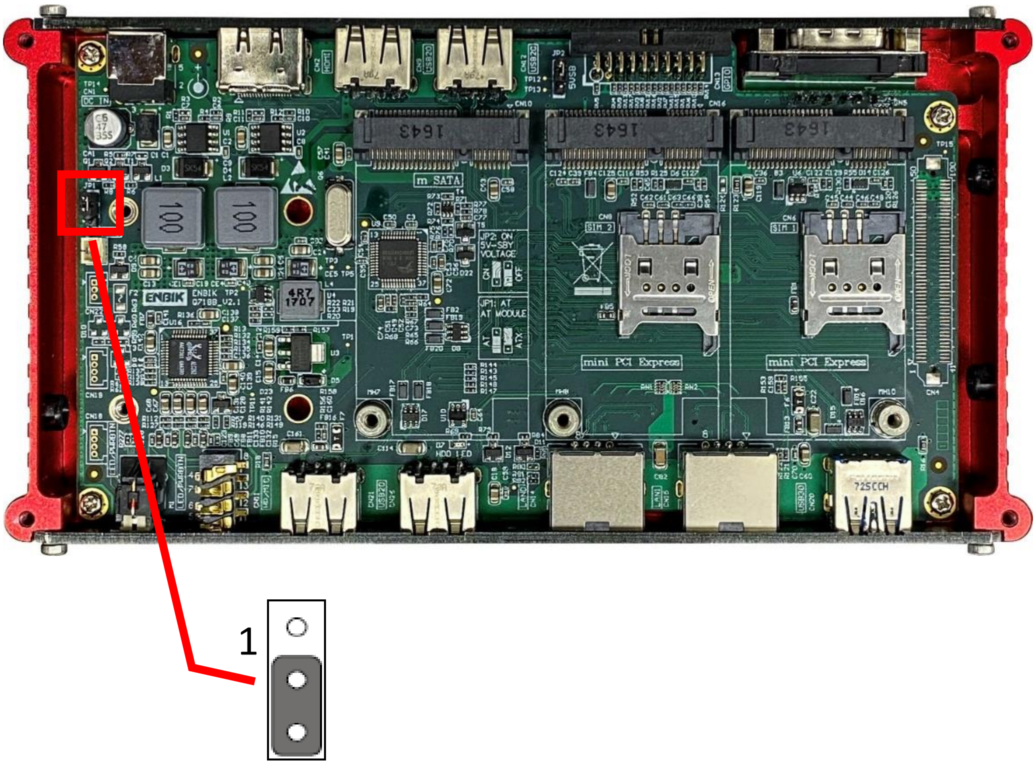


A pair of needle-nose pliers may be helpful when working with jumpers.

The following tables list the function of each of the board’s jumpers and DIP switches.

Label	Function	Note
JP1	AT/ATX Power Mode Select	2 x 1 header, pitch 2.00

5.2 AT/ATX Power Mode Select



Closed PIN	Function	Note
1-2	AT mode	N/A
2-3	ATX mode	Default

Chapter 6

BIOS Settings

This chapter includes:

- Entering BIOS Setup Program
- Setup Menu and Navigation
- Advanced Setup Options

6.1 Entering the BIOS Setup Program

The BIOS setup program can be accessed by pressing the <DEL> or <ESC> key during POST.

6.1.1 Boot Selection Popup

The BIOS offers the ability to access a Boot Selection Popup menu by pressing the <F11> key during POST. If this option is used, a selection will be displayed after POST allowing the operator to select either the boot device that should be used or an option to enter the BIOS setup program.

6.1.2 Setup Menu and Navigation

The BIOS setup screen is composed of the menu bar and sub-screens. The menu bar is shown below:

Main	Advanced	Chipset	Security	Boot	Save & Exit

The left frame displays all the options that can be configured in the selected menu.
Only the blue options can be configured (greyed-out options are not available). The selected option will be highlighted in white.
The right frame displays the key legend. Above the key legend is an area reserved for text messages. These text messages explain the options and the possible impacts when changing the selected option in the left frame.
The setup program uses a key-based navigation system. Most of the keys can be used at any time while in setup. The table below explains the supported keys:

Key	**Description**
← → Left/Right	Select a setup menu (e.g., Main, Boot, Exit)
↑ ↓ Up/Down	Select a setup item or submenu
+ - Plus/Minus	Change the field value of a particular setup item
Tab	Select setup fields (e.g., in date and time)
F1	Display General Help screen
F2	Load previous settings
F9	Load optimal default settings
F10	Save changes and exit setup
ESC	Discard changes and exit setup
ENTER	Display options of a particular setup item or enter submenu

6.2 Main Setup Screen

When you first enter the BIOS setup, you will see the main setup screen. This screen displays the BIOS, processor, memory, and board information and is used for configuring the systems date and time.

Feature	Options	Description
Main BIOS Version	N/A	Displays the main BIOS version
OEM BIOS Version	N/A	Displays the additional OEM BIOS version
Build Date	N/A	Displays the date the BIOS was built
Product Revision	N/A	Displays the hardware revision of the board
Serial Number	N/A	Displays the serial number of the board
BC Firmware Revision	N/A	Displays the firmware revision of the board controller
MAC Address	N/A	Displays the MAC address of the onboard Ethernet controller
Boot Counter	N/A	Displays the number of boot-ups. (max. 16777215)
Running Time	N/A	
Microcode Patch	N/A	Displays the microcode patch loaded for the onboard CPU
Total Memory	N/A	The total amount of low voltage DDR3 present on the system
Intel(R) GOP Driver	N/A	
Sec RC Version	N/A	
TXE FW Version	N/A	
System Date	Day of the week, month/day/year	Specifies the current system date
System Time	Hour: Minute: Second	Specifies the current system time

6.3 Advanced Setup

Select the Advanced tab from the Setup menu to enter the advanced BIOS setup screen.

Advanced Setup Options	
Watchdog	Thermal Configuration
Hardware Health Monitoring	SATA
Graphics	LPSS & SCC Configuration
Intel(R) I210 Gigabit Network	PCI & PCI Express
Intel(R) I211 Gigabit Network	UEFI Network Stack
Driver Health	CSM & Option ROM Control
Trusted Computing	Info Report Configuration
RTC Wake Settings	USB
Module Serial Ports	Diagnostic Settings
Reserve Legacy Interrupt	Platform Trust Technology
ACPI	Security Configuration
Serial Port Console Redirection	Intel RMT Configuration
CPU	PC Speaker
PPM Configuration	

6.3.1 Watchdog Submenu

Feature	Options	Description
POST Watchdog	Disabled	Configure POST Watchdog
	30 seconds	
Intervals (minutes)	1, 2, 5, 10, 30	
Stop for User Interaction	Yes / No	Decide if POST watchdog should be stopped during Setup of boot menu or while waiting for a password
Runtime Watchdog	Disabled	
	One-time Trigger	
	Single event	
	Repeat event	
Delay	Disabled	Select the delay time before the runtime watchdog becomes active. This ensures the system has enough time to load
Intervals (seconds)	10,30	
Intervals (minutes)	1, 2, 5, 10, 30	
Event 1	ACPI Event	Select the type of event that will be generated when timeout 1 is reached.
	Reset	
	Power Button	
Event 2	**Disabled**	Select the type of event that will be generated when timeout 2 is reached.
	ACPI Event	
	Reset	
	Power Button	
Event 3	**Disabled**	Select the type of event that will be generated when timeout 3 is reached.
	ACPI Event	
	Reset	
	Power Button	
Time out 1		
Intervals (seconds)	1, 2, 5, 10, 30	Select the timeout value for the first stage watchdog event
Intervals (minutes)	1, 2, 5, 10, 30	
Time out 1		
Intervals (seconds)	1, 2, 5, 10, 30	Select the timeout value for the second stage watchdog event
Intervals (minutes)	1, 2, 5, 10, 30	
Time out 1		
Intervals (seconds)	1, 2, 5, 10, 30	Select the timeout value for the third stage watchdog event
Intervals (minutes)	1, 2, 5, 10, 30	
Watchdog ACPI	**Shutdown**	Select the operating system event that is initiated by the watchdog ACPI
Event	Restart	**Note:** These options preform a critical but orderly O/S shutdown or restart.

6.3.2 Hardware Health Monitoring Submenu

6.4. Feature	6.5. Options	6.6. Description
6.7. CPU Temperature	**6.8. N/A**	6.9. Displays the actual CPU Temperature in Celsius
6.10. Board Temperature	6.11. N/A	6.12. Displays the actual Board Temperature in Celsius
6.13. 5V Standard	6.14. N/A	6.15. Displays the actual 5V Voltage
6.16. 5V Standby	6.17. N/A	6.18. Displays the actual 5V Voltage
6.19. Input Current (5V Standard)	6.20. N/A	6.21. Displays the Actual Input Current of 5V power plane
6.22. CPU Fan Speed	6.23. N/A	6.24. Displays the actual CPU Fan Speed in RPM

6.25. Fan PWM Frequency Mode	6.26. Select the fan PWM base frequency mode	
	6.27. Low Frequency	6.28. 11.0 to 88.2Hz
	6.29. High Frequency	6.30. 1k to 63kHz
6.31. Fan PWM Frequency (kHz)	6.32. 1 - 63	6.33. Select the fan PMW base frequency (1kHz–63kHZ)
6.34.	6.35.	6.36.

6.37. **Feature**	6.38. **Options**	6.39. **Description**
6.40. Fan Speed Setting	6.41. 0%	6.42. Boot up fan speed in percent of the maximum supported speed
	6.43. 10%	
	6.44. 25%	
	6.45. 40%	
	6.46. 50%	
	6.47. 60%	
	6.48. 75%	
	6.49. 90%	
	6.50. 100%	

6.3.3 Graphics Submenu

Feature	**Options**	**Description**
Active LFP / EDP	**N/A**	

6.3.4 Intel® Ethernet Connection I210 Submenu

Feature	**Options**	**Description**
NIC Configuration	Submenu	Configure Boot Protocol, Wake on LAN, Link Speed, and VLAN.
Blink LEDs	**0** - 15	Identify the physical network port by blinking the associated LED.
UEFI Driver	N/A	Displays the UEFI Driver version.
Adapter PBA	N/A	Displays the Adapter PBA.
Chip Type	N/A	Displays the type of Chip in which the Ethernet controller is integrated.
PCI Device ID	N/A	Displays the PCI Device ID of the Ethernet controller.
Bus: Device: Function	N/A	Displays the PCI Bus: Device: Function number of the Ethernet controller.
Link Status	N/A	Displays the Link Status.
MAC Address	N/A	Displays the MAC Address.
Virtual MAC Address	N/A	Programmatically assignable MAC address for port

6.3.4.1 NIC Configuration Submenu

Feature	**Options**	**Description**
Link Speed	**Auto Negotiated**	Specifies the port speed used for the selected boot protocol.
	10 Mbps Half	
	10 Mbps Full	
	100 Mbps Half	

	100 Mbps Full	
Wake on LAN	Disabled	Enables the server to be powered on using an in-band magic packet.
	Enabled	

6.3.5 Intel® Ethernet Connection I211 Submenu

Feature	Options	Description
NIC Configuration	submenu	Configure Boot Protocol, Wake on LAN, Link Speed and VLAN
Blink LEDs	0 - 15	Identify the physical network port by blinking the associated LED
UEFI Driver	N/A	Displays the UEFI Driver version.
Adapter PBA	N/A	Displays the Adapter PBA
Chip Type	N/A	Displays the type of the Chip in which the Ethernet controller is integrated
PCI Device ID	N/A	Displays the PCI Device ID of the Ethernet controller
Bus: Device: Function	N/A	Displays the PCI Bus: Device: Function number of the Ethernet controller
Link Status	N/A	Displays the Link Status
MAC Address	N/A	Displays the MAC Address
Virtual MAC Address	N/A	Programmatically assignable MAC address for port

6.3.5.1 NIC Configuration Submenu

Feature	Options	Description
Link Speed	**Auto Negotiated**	Specifies the port speed used for the selected boot protocol.
	10 Mbps Half	
	10 Mbps Full	
	100 Mbps Half	
	100 Mbps Full	
Wake on LAN	Disabled	Enables the server to be powered on using an in-band magic packet
	Enabled	

6.3.6 Driver Health Submenu

Feature	Options	Description
Intel® PRO/1000	No option	Provides health status for drivers/controllers

Intel PRO/1000 Submenu

Feature	Options	Description
Controller Information	No option	Provides health Status for drivers/controllers

6.3.7 Trusted Computing Submenu

Feature	Options	Description
Security Device Support	Disabled	Enable or disable BIOS support for a security device. O.S. will not show the security device. TCG EFI protocol and INT1A interface will not be available.
	Enabled	

6.3.8 RTC Wake Settings Submenu

Feature	Options	Description
RTC Wake Mode	**Disabled**	Set system wake mode on alarm event. When enabled, the system will wake from the specified Sx states on the hr.: min: sec specified.
	Wake from S5 only	
	Wake from S4 and S5	
	Wake from S3, S4, and S5	
Wake up hour		Select 0-23. For example, enter 3 for 3 am and 15 for 3 pm.
Wake up minute		0-59
Wake up second		0-59

6.3.9 Module Serial Ports Submenu

Feature	Options	Description
Serial Port 0	**Disabled**	Enable or disable module serial port 0. PCI mode for Windows 7 or ACPI mode for Windows 8.x and newer and Linux
	Enabled in PCI mode	
	Enabled in ACPI mode	

6.3.10 Reserve Legacy Interrupt Submenu

Feature	Options	Description
Reserve Legacy Interrupt 1/2/3	**None**	The interrupt reserved here will not be assigned to any PCI or PCI Express device and thus may be available for some legacy bus device.
	IRQ3	
	IRQ4	
	IRQ5	
	IRQ6	
	IRQ10	
	IRQ11	
	IRQ14	
	IRQ15	

6.3.11 ACPI Submenu

Feature	Options	Description
Enable ACPI Auto Configuration	**Disabled**	Enables or Disables BIOS ACPI Auto Configuration.
	Enabled	

Hibernation Support	Disabled	Enable or disable the system's ability to hibernate (operating system S4 sleep state). This option may not be valid with some operating systems.
	Enabled	
ACPI Sleep State	Suspend Disabled	Select the state used for ACPI system sleep/suspend.
	S3 (Suspend to RAM)	
Lock Legacy Resources	**Disabled**	Enable or disable locking of legacy resources.
	Enabled	
Lid Button Support	Disabled	Activate ACPI sleep lid button support.
	Enabled	
Sleep Button Support	Disabled	Activate ACPI sleep button support.
	Enabled	

6.3.12 Serial Port Console Redirection Submenu

Feature	Options	Description
COM0	N/A	Enable or disable serial port 0 console redirection.
Console Redirection		
COM1	N/A	Enable or disable serial port 1 console redirection.
Console Redirection		
COM2 (Pci, Bus0, Dev30, Func3)	**Disabled**	Enable or disable serial port 0 console redirection.
Console Redirection	Enabled	
Console Redirection Settings	submenu	Opens console redirection configuration submenu.
Legacy Console Redirection Settings	submenu	Opens console redirection configuration submenu.
Serial Port for Out-of-Band		
Management / EMS	**Disabled**	Enable or disable Serial Port for Out-of-Band Management
Console Redirection	Enabled	/Windows Emergency Management Services.

6.3.13 Console Redirection Settings COM2 Submenu

Feature	Options	Description
Terminal Type	VT100	Select the terminal type.
	VT100+	
	VT-UTF8	
	ANSI	
Baud rate	9600	Select the baud rate.
	19200	
	38400	
	57600	

	115200	
Data Bits	7	Set the number of data bits.
	8	
Parity	**None**	Select parity.
	Even	
	Odd	
	Mark	
	Space	
Stop Bits	**1**	Set the number of stop bits.
	2	
Flow Control	**None**	Select flow control.
	Hardware RTS/CTS	
VT-UTF8 Combo Key Support	Disabled	Enable VT-UTF8 combination key support for ANSI/VT100 terminals.
	Enabled	
Recorder Mode	**Disabled**	With recorder mode enabled, only text output will be sent over the terminal. This is helpful in capturing and recording terminal data.
	Enabled	
Resolution 100x31	**Disabled**	Enable or disable extended terminal resolution.
	Enabled	
Legacy OS Redirection Resolution	**80x24**	The number of rows and columns supported for legacy OS redirection.
	80x25	
Putty Keypad	**VT100**	Select Function Key and Keypad on Putty.
	LINUX	
	XTERMR6	
	SCO	
	ESCN	
	VT400	
Redirection After BIOS POST	**Enabled**	
	Disabled	

6.3.14 Legacy Console Redirection Settings Submenu

Feature	Options	Description
Legacy Serial Redirection Port	**COM0 (Disabled)**	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
	COM1 (Disabled)	
	COM2 (PCI Bus0, Dev30, Func3)	

6.3.15 CPU Submenu

Feature	Options	Description
Socket 0 CPU Information	submenu	Socket specific CPU Information
CPU Speed	N/A	Displays the CPU clock frequency.
64-bit	N/A	Displays whether 64-bit is supported.
UEFI Driver	N/A	Displays the UEFI Driver version.
Limit CPUID Maximum	**Disabled** Enabled	When enabled, the Processor will limit the maximum CPUID input value to 03h when queried, even if the Processor supports a higher CPUID input value. When disabled, the Processor will return the actual maximum CPUID input value of the Processor when queried.
Bi-directional PROCHOT	Disabled **Enabled**	When a processor thermal sensor trips (either CORE), the PROCHOT# will be driven. If bidirectional is enabled, external agents can drive PROCHOT# to throttle the processor.
Intel Virtualization Technology	Disabled **Enabled**	When enabled, a VMM can utilize the integrated hardware virtualization support.
Power Technology	Disable **Energy Efficient** Custom	Enable power management features.

Socket 0 CPU Information Submenu

Feature	Options	Description
CPU Name	N/A	Displays socket specific CPU name.
CPU Signature	N/A	Displays CPU signature number.
Microcode Patch	N/A	Displays the CPU microcode patch number.
Max CPU Speed	N/A	Displays the maximum CPU clock frequency.
Min CPU Speed	N/A	Displays the minimum CPU clock frequency.
Processor Cores	N/A	Displays the number of CPU cores
Intel HT Technology	N/A	Displays the Intel HT Technology support information.
Intel VT-x Technology	N/A	Displays the Intel VT-x Technology support information.
L1 Data Cache	N/A	Displays the Socket L1 data cache information.
L1 Code Cache	N/A	Displays the Socket L1 code cache information.
L2 Cache	N/A	Displays the Socket L2 data cache information.
L3 Cache	N/A	Displays the Socket L3 data cache information.

6.3.16 PPM Configuration Submenu

Feature	Options	Description
EIST	**Disabled** Enabled	Enable/Disable Intel SpeedStep
CPU C state Report	Disabled	Enable/Disable CPU C state report to OS

	Enabled	
Max CPU C-state	C7	This option controls Max C state that the processor will support.
	C6	
	C1	
SOix	**Disabled**	Enable/Disable CPU SOix state
	Enabled	

6.3.17 Thermal Configuration Submenu

Feature	Options	Description
DTS	**Disabled**	Enabled/Disabled Digital Thermal Sensor.
	Enabled	
Critical Trip Point	**95**	This value controls the temperature of the ACPI critical Trip Point - the point in which the OS will shut the system off. Note: 100C is the Plan of Record (PDR) for all Intel Mobile processors.
OS Hibernate Temperature	**85**	The temperature that should cause the OS to trigger the system to hibernate
Passive Trip Point	85	This value controls the temperature of the ACPI critical Trip Point - the point in which the OS will begin throttling the processor.
Full Speed Fan Trip Point	**80**	The temperature at which the fan device will be activated at full speed
Half-Speed Fan Trip Point	**60**	The temperature at which the fan device will be activated at half speed
Fan Hysteresis	**7**	The number of degrees below the fan activation threshold that must be reached before turning off the fan

6.3.18 SATA Submenu

Feature	Options	Description
SATA Controller	**Enabled**	Enable/Disable SATA Device
	Disabled	
SATA Mode Selection	AHCI	Determines how the SATA controller operates.
SATA Interface Speed	Gen1	Select SATA Interface Speed, CHV A1 always with Gen1 Speed.
	Gen2	
	Gen3	
SATA Test Mode	Enabled	Test Mode enable/disable.
	Disabled	

Aggressive LPM Support	**Enabled**	Enable PCH to enter link power state aggressively.
	Disabled	
Software Feature Mask Configuration	submenu	RAID OPROM/RST driver will refer to the SWFM configuration to enable/disable the storage features.
SATA Port 0		
Port 0	**Enabled**	Enable / Disable SATA Port.
	Disabled	
Spin Up Device	Enabled	If enabled for any ports, Staggered Spin Up will be performed, and only the drivers which have this option enabled will spin up at boot. Otherwise, all drivers spin up at boot.
	Disabled	
Device Sleep Support	**Enabled**	Enable/Disable Device Sleep Support on that port.
	Disabled	
Port 1	**Enabled**	Enable / Disable SATA Port.
	Disabled	
Spin Up Device	Enabled	If enabled for any ports, Staggered Spin Up will be performed, and only the drivers which have this option enabled will spin up at boot. Otherwise, all drivers spin up at boot.
	Disabled	
Device Sleep Support	**Enabled**	Enable/Disable Device Sleep Support on that port.
	Disabled	

Software Feature Mask Configuration Submenu

Feature	Options	Description
SSD/HDD Unlock	**Enabled**	If enabled, indicates that the SSD/HDD password unlock in the O/S is enabled.
	Disabled	
LED Locate	**Enabled**	If enabled, indicates that the LED/SGPIO hardware is attached, and ping to locate feature is enabled in the OS.
	Disabled	

6.3.19 LPSS & SCC Configuration Submenu

Feature	Options	Description
SCC eMMC Support (D16:F0)	**ACPI mode**	SCC eMMC Support Enable\Disable
	PCI mode	
	Disabled	
eMMC Secure Erase	Enabled	Disable/Enable eMMC Secure Erase. When enabled, all the data on the eMMC will be erased.
	Disabled	
SCC SD Card Support(D18:F0)	ACPI mode	SCC SD Card Support Enable\Disable
	PCI mode	
	Disabled	
LPSS with GPIO Device Support	Disabled	Enable/Disable GPIO ACPI Devices Support, disable it will disable all LPSS devices.
	Enabled	

LPSS DMA #2 (D24:F0)	**ACPI mode**	Enable/Disable LPSS DMA #2 Support
	PCI mode	
	Disabled	
LPSS I2C #3 (D24:F3)	**ACPI mode**	Enable/Disable LPSS I2C #3 Support
	PCI mode	
	Disabled	
Runtime D3 Support	**Enabled**	Enable/Disable Runtime D3 Support
	Disabled	
LPSS I2C #4 (D24:F4)	ACPI mode	Enable/Disable LPSS I2C #4 Support
	PCI mode	
	Disabled	
Runtime D3 Support	**Enabled**	Enable/Disable Runtime D3 Support
	Disabled	
LPSS DMA #1 (D30:F0)	**ACPI mode**	Enable/Disable LPSS DMA #1 Support
	PCI mode	
	Disabled	
LPSS HSUART #1 (D30:F3)	ACPI mode	Enable/Disable LPSS HSUART #1 Support
	PCI mode	
	Disabled	

6.3.20 PCI & PCI Express Submenu

Feature	Options	Description
PCI Latency Timer	**32 PCI Bus Clocks**	Value to be programmed into the PCI latency timer register.
	64 PCI Bus Clocks	
	96 PCI Bus Clocks	
	128 Bus Clocks	
	160 PCI Bus Clocks	
	192 PCI Bus Clocks	
	224 PCI Bus Clocks	
	248 PCI Bus Clocks	
PCI-X Latency Timer	32 PCI Bus Clocks	Value to be programmed into the PCI latency timer register.
	64 PCI Bus Clocks	
	96 PCI Bus Clocks	
	128 Bus Clocks	
	160 PCI Bus Clocks	
	192 PCI Bus Clocks	
	224 PCI Bus Clocks	
	248 PCI Bus Clocks	
VGA Palette Snoop	**Disabled**	

	Enabled	Enable or disable VGA palette registers snooping.
PERR# Generation	**Disabled**	Enable or disable a PCI device to generate PERR#.
	Enabled	
SERR# Generation	**Disabled**	Enable or disable a PCI device to generate SERR#.
	Enabled	
Above 4G Decoding	**Disabled**	Enables or disables 64bit capable Devices to be Decoded in above 4G Address Space (Only if System Supports 64bit PCI Decoding).
	Enabled	
Do not Reset VC-TC Mapping	**Disabled**	If the system has Virtual Channels, Software can reset Traffic Class mapping through Virtual Channels, to its default state. Setting this option to Enabled will not modify VC Resources.
	Enabled	

6.3.21 UEFI Network Stack Submenu

Feature	**Options**	**Description**
UEFI Network Stack	**Disabled**	Enable or disable the UEFI network stack.
	Enabled	
IPv4 PXE Support	Disabled	Enable IPv4 PXE boot support. If disabled IPv4 PXE boot option will not be created.
	Enabled	
IPv6 PXE Support	Disabled	Enable IPv6 PXE boot support. If disabled IPv6 PXE boot option will not be created.
	Enabled	
PXE boot wait time	0	Wait time to press ESC key to abort the PXE boot
Media detect count	1	Number of times the presence of media will is to be checked

6.3.22 CSM & Option ROM Control Submenu

Feature	**Options**	**Description**
CSM Support	Disabled	Enable/Disable CSM Support.
	Enabled	
CSM16 Module Version	No option	BIOS CSM module version
Gate A20 Active	**Upon Request**	Upon Request: Gate A20 can be disabled using BIOS services.
	Always	Always: Do not allow disabling Gate A20. This option is useful when any runtime code is executed above 1MB.
Option ROM Messages	**Force BIOS**	Set display mode for option ROMs.
	Keep Current	
	Immediate	

INT19 Trap Response	Postponed	BIOS reaction on INT19 trapping by Option ROM: IMMEDIATE - execute the trap right away. POSTPONED - execute the trap during legacy boot.
Boot Option Filter	**UEFI and Legacy**	Controls which devices/boot loaders the system should boot to.
	Legacy only	
	UEFI only	
PXE Option ROM Launch Policy	Do not launch	Controls the execution of UEFI and Legacy PXE option ROMs.
	UEFI ROM Only	
	Legacy ROM Only	
Storage Option ROM Launch Policy	Do not launch	Controls the execution of UEFI and legacy mass storage device option ROMs.
	UEFI ROM Only	
	Legacy ROM Only	
Video Option ROM Launch Policy	Do not launch	Controls the execution of UEFI and legacy video option ROMs.
	UEFI ROM Only	
	Legacy ROM Only	
Other Option ROM Launch Policy	Do not launch	Controls the execution of option ROMs for PCI / PCI Express devices other than network, mass storage, or video.
	UEFI ROM Only	
	Legacy ROM Only	

6.3.23 Info Report Configuration Submenu

Feature	Options	Description
Post Report	**Disabled**	Post Report Support Enabled/Disabled
	Enabled	
Delay Time	5	Post Report Wait Time: 0~10 Seconds
Info Error Message	**Disabled**	Info Error Message Support Enabled/Disabled
	Enabled	
Summary Screen	**Disabled**	Summary Screen Support Enabled/Disabled
	Enabled	
Delay Time	5	Summary Screen Wait Time: 0~10 Seconds

6.3.24 USB Submenu

Feature	Options	Description
USB Module Version	No option	BIOS USB module version
USB Controllers	No option	Number of USB controllers found on the system
USB Devices	No option	Number of USB devices found on the system
Legacy USB Support	**Enabled**	Enable legacy USB support. Auto option disables legacy support if no USB devices are
	Disabled	

	Auto	connected. Disable option will keep USB devices available only for EFI applications and BIOS setup.
xHCI Hand-off	Enabled	This is a workaround for O/S' without xHCI hand-off support.
	Disabled	The xHCI ownership change should be claimed by xHCI O/S driver.
USB Mass Storage Driver Support	Disabled	Enable or disable USB mass storage driver support.
	Enabled	
Port 60/64 Emulation	Disabled	Enables I/O port 60h/64h emulation support. This should be enabled for complete USB keyboard legacy support for non-USB aware O/S'.
	Enabled	
USB Transfer Timeout	1 sec	The timeout value for control, bulk, and interrupt transfers.
	5 sec	
	10 sec	
	20 sec	
Device Reset Timeout	10 sec	USB mass storage device Start Unit command timeout.
	20 sec	
	30 sec	
	40 sec	
Device Power-up Delay Selection	Auto	Define maximum time a USB device might need before it accurately reports itself to the host controller. Auto selects a default value, which is 100ms for a root port or derived from the hub descriptor for a hub port.
	Manual	

6.3.25 Diagnostic Settings Submenu

Feature	Options	Description
Relay Interface	**Disabled**	Select the relay interface to which the POST code will be redirected.
	I2C	
	SMBus	
	BC Diagnostic Console	
Primary Port Address Low byte	128	Set the Address for the primary debug port. The standard address value is 0x80. However, any multiple of 8 is valid for a primary debug port address, i.e., the low three bits muse be zero.
Primary Port Address High byte	0	Above
Relay Device Address (Dec)	226	Specify the I2C/SMBus device Address of, e.g., a 7-Segment LCD. The factory setting for the SparkFun device is 0xE2. However, any even device address (bit 0 = 0) can be specified.
BC Diagnostic Console	**Disabled**	

Interface	BC AUX Port	Select the interface to be used for the BC Diagnostic Console output or disable the BC Diagnostic Console output.
Primary Bit	**No Parity**	Choose the parity bits for the BC Diagnostic Console Interface.
	Even Parity	
	Odd Parity	
Stop Bits	**1 Stop Bit**	Choose the stop bits for the BC Diagnostic Console Interface.
	2 Stop Bits	
Data Bits	5 Data Bits	Choose the data bits for the BC Diagnostic Console Interface.
	6 Data Bits	
	7 Data Bits	
	8 Data Bits	
Baud rate	1200 Baud	Choose the baud rate for the BC Diagnostic Console Interface.
	2400 Baud	
	4800 Baud	
	9600 Baud	
	19200 Baud	
	38400 Baud	

6.3.26 Platform Trust Technology Submenu

Feature	Options	Description
fTPM	Enabled	Enable/Disable fTPM
	Disabled	

6.3.27 Security Configuration Submenu

Feature	Options	Description
TXE HWRFPO	Enabled	
	Disabled	
TXE Firmware Update	**Enabled**	
	Disabled	
TXE EOP Message	**Enabled**	Send EOP Message Before entering OS
	Disabled	

6.3.28 Intel RMT Configuration Submenu

Feature	Options	Description
Intel RMT Support	**Disabled**	Intel RMT (Ready Mode Technology) SSDT table will be loaded if enabled.
	Enabled	
HW Notification	**Disabled**	Hardware notification enabling status.
	Enabled	

6.3.29 PC Speaker Submenu

Feature	Options	Description
Debug Beeps	**Enabled**	Enable or disable general debug / status beep generation.
	Disabled	
Input Device Debug Beeps	**Disabled**	Enable or disable input device debug beeps.
	Enabled	
Output Device Debug Beeps	**Disabled**	Enable or disable output device debug beeps.
	Enabled	
USB Driver Beeps	**Disabled**	Enable or disable USB driver beeps.
	Enabled	

6.4 Chipset Setup

Select the Chipset tab from the setup menu to enter the Chipset setup screen.

6.4.1 Processor (Integrated Components) Submenu

Feature	Options	Description
Memory Information		
Total memory	No option	The total amount of memory detected by the system
Memory Slot 0	No option	Memory detected by the system on Slot 0
Memory Slot 2	No option	Memory detected by the system on Slot 2
Max TOLUD	**2 GB**	The maximum value of the TOLUD Dynamic assignment would adjust TOLUD automatically based on the largest MMIO length of installed graphic controller.
	3 GB	

6.4.1.1 Intel IGD Configuration Submenu

Feature	Options	Description
Internal Graphics Device	**Enabled**	Keep Internal Graphics Device (IGD) enabled based on the setup options.
	Disabled	
IGD Turbo	**Auto**	Select the IGD Turbo feature, if Auto selected, IGD Turbo will only be enabled when SOC stepping is B0 or above.
	Enabled	
	Disabled	
GFX Boost	Enabled	Enable/Disable GFX Boost
	Disabled	
PAVC	Disabled	Enable/Disable Protected Audio Video Control
	Enabled	
PR3 (For Win 10 only)	Disabled	Enable/Disable PR3 (For Win 10 only)
	Enabled	
DVMT Pre-Allocated	**32M**	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
	64M	
	96M	
	128M	
	160M	
	192M	
	224M	
	256M	
	288M	
	320M	
	352M	
	384M	
	416M	

Feature	Options	Description
DVMT Pre-Allocated **Continued**	448M 480M 512M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128MB **256MB** Max	Select DVMT 5.0 Total Graphics Memory size used by the Internal Graphics Device.
Aperture Size	128MB **256MB** 512MB	Select the Aperture Size
GTT Size	2MB **4MB** 8MB	Select the GTT Size
IGD Thermal	Enabled **Disabled**	Enable/Disable IGD Thermal
Spread Spectrum clock	**Enabled** Disabled	Enable/Disable Spread Spectrum clock
WOPCMSZ	**1MB** 2MB 4MB 8MB	Select a size for WOPCMSZ
ISP Enable/Disable	**Enabled** Disabled	Enable/Disable ISP PCI Device Selection
ISP PCI Device Selection	Disabled ISP PCI Device as B0D2F0 **ISP PCI Device as B0D3F0** ISP PCI Device as B0D3F0 with Virtual ISP B0D2F0	Default ISP is PCI B0D2F0 for Windows Boot. Linux Boot to Select B0D3F0.
PUNIT Power Configuration	Disabled **Enabled**	Enable or disable Punit Power configuration.
Svid Configuration	**Platform Defaults** Svid Config 0 Svid Config 1 Svid Config 3 Svid Config 4 BSW I2C PMIC Config	Choose the right SVID Config

6.4.1.2 Graphics Power Management Control Submenu

Feature	Options	Description
RC6 (Render Standby)	**Enabled**	Check to enable render standby support.
	Disabled	
Power Meter Lock	**Enabled**	Enable/Disable Power Meter Lock.
	Disabled	

6.4.1.3 Memory Configuration Options Submenu

Feature	Options	Description
Rank Margin Tool EV Mode	**Disabled**	Enable/Disable Rank Margin Tool print out message support. Please make sure MRS Debug Message Level at least minimum
	Enabled	
DDR DVFS	Disabled	Enable or disable DDR Dynamic Voltage and Frequency Scaling in MRC
	Enabled	
Memory Frequency Override	**Disabled**	Allows override of memory frequency parameters that are automatically obtained from DDR3 DIMM SPD. May cause memory instability if the selected frequency is not supported by the memory device. This option does not affect systems configured without 'UseDimmSpd' option
	Enabled	
Frequency A Selection	Auto	Frequency A Selection
	800	
	1067	
	1600	
	800(SKU333)	
	1000(SKU333)	
	1333(SKU333)	
	900(SKU360)	
	1800(SKU360)	
	933(SKU373)	
	1866(SKU373)	
Frequency B Selection	Auto	Option to Select Frequency B (Min DDR DVFS Frequency)
	1067	
	800(SKU333)	
	1000(SKU333)	
	900(SKU360)	
	933(SKU373)	
Auto Detect LPDDR3 DRAM	Disabled	Enable or disable automatic detection of LPDDR3 DRAM parameters
	Enabled	

LPDDR3 Chip Select	**1 Rank**	LPDDR3 Chip Select (Number of Rank) Configuration.
	2 Ranks	Auto Detect must be disabled to use this option.
Feature	**Options**	**Description**
Channel selection	Auto	Select the number of channels - Auto = dual-channel
	Single	
	Dual	
Channel selection Bit 3:0	0 - F, default is **2**	NOTE: Only bits [3:1] are used for final channel select value. BMISC Channel Select Bits 3:0: Specifies the address bits to use to stripe memory across multiple PMI channels.
Channel selection 4	0 - F, default is **1**	BMISC Channel Select 4 for channel hashing.
Bank Address Hashing	Disabled	Enable or disable Bank Address Hashing
	Enabled	
Rank Select Interleaving	Disabled	Enable or disable Rank Select Interleaving
	Enabled	
Dynamic Self Refresh	Disabled	Enable or disable PUNIT driven DUNIT DDR dynamic self refresh
	Enabled	
DRAM PM5	Disabled	Enable or disable DRAM PM5 PUNIT configuration
	Enabled	
DDR3 2N Mode	**Disabled**	Set the DDR3 mode to 2N. 1N mode is used by default.
	Enabled	
RX Power Training	**Enabled**	Enable/Disable RX Power Training
	Disabled	
TX Power Training	**Enabled**	Enable/Disable TX Power Training
	Disabled	
MRC Fast Boot	**Enabled**	Enable/Disable MRC fast boot. Forces MRC training to occur when disabled.
	Disabled	
Scrambler	**Enabled**	Enable/Disable Scrambler
	Disabled	
DRP Lock	Disabled	DRP Lock
	Enabled	
REUT Lock	Disabled	REUT Lock
	Enabled	
RH Prevention	**Disabled**	Prevents Row Hammer attacks by increasing the average time between sending REF commands to DRAM.
	Enabled	

6.4.2 Platform Controller Hub (PCH) Submenu

Feature	Options	Description
Security Configuration	Submenu	Security Configuration settings.

Azalia Configuration	Submenu	Azalia HD Audio Options
USB Configuration	Submenu	USB Configuration settings
PCI Express Configuration	Submenu	PCI Express Configuration settings
Serial IRQ Mode	Quiet	Configure serial IR mode.
Feature	**Options**	**Description**
Serial IRQ Mode	**Continuous**	Configure serial IR mode.
CLKRUN# Logic	**Disabled**	Enable the CLKRUN# logic to stop the LPC clocks when possible. Requires Serial IRQ Mode to be set to Quiet as well.
	Enabled	
Isolate SMBus Segments	**Never**	Allows to isolate the off-module/external SMBus segment from the on-module SMBus segment. This can be a workaround for non-spec conforming external SMBus devices.
	During POST	
	Always	

6.4.2.1 Security Configuration Submenu

Feature	Options	Description
RTC Lock	Disabled	Enable or disable bytes 38h-3Fh in the upper and lower 128-byte bank of RTC RAM lockdown.
	Enabled	
BIOS Lock	**Enabled**	Enable/Disable the BIOS Lock Enable feature.
	Disabled	
Global SMI Lock	**Enabled**	Enable or Disable SMI lock.
	Disabled	

6.4.2.2 Azalia Configuration Submenu

Feature	Options	Description
LPE Audio Support	**Disabled**	Security Configuration settings. Enable/Disable LPE Audio Support.
	PCI mode	
	ACPI mode	
Audio Controller	Disabled	Control Detection of the Azalia device. Disabled = Azalia will be unconditionally disabled. Enabled = Azalia will be unconditionally Enabled.
	Enabled	
Azalia Vci Enable	Disabled	Enable/Disable Virtual Channel 1 of Audio Controller.
	Enabled	
Azalia Docking Support Enable	**Disabled**	Enable/Disable Azalia Docking Support of Audio Controller.
	Enabled	
Azalia PME Enable	Disabled	Enable/Disable Power Management capability of Audio Controller.
	Enabled	
Azalia DDI Codec	Disabled	Enable/Disable internal DDI codec for Azalia
	Enabled	
Azalia DDI Codec Port B	Disabled	Enable/Disable internal DDI port codec for Azalia
	Enabled	

Azalia DDI Codec Port C	Disabled	Enable/Disable internal DDI port codec for Azalia
	Enabled	
Azalia DDI Codec Port D	Disabled	Enable/Disable internal DDI port codec for Azalia
	Enabled	

6.4.2.3 USB Configuration Submenu

Feature	Options	Description
XHCI Mode	**Enabled**	Mode of operation of xHCI controller
	Disabled	
SSIC Support Enable	Enabled	Enable/Disable SSIC Support
	Disabled	
SSIC Init Sequence	**SSIC initialization Sequence 1**	SSIC Initialization Sequence 1 - Windows, SSIC Initialization
	SSIC initialization Sequence 2	Sequence 2 - Android.
SSIC Port 1	Enabled	Enable/Disable SSIC Port 1.
	Disabled	
SSIC Port 2	Enabled	Enable/Disable SSIC Port 2.
	Disabled	
HSIC Port 1	**Enabled**	Enable/Disable HSIC Port 1.
	Disabled	
HSIC Port 2	**Enabled**	Enable/Disable HSIC Port 2.
	Disabled	
USB2 PHY Power Getting	**Auto**	Configure USB2 PHY Power Gating
	Disabled	
	Enabled	
USB3 PHY Power Getting	**Auto**	Configure USB3 PHY Power Gating
	Disabled	
	Enabled	
USB OTG Support	PCI mode	Enable/Disable USB OTG Support
	Disabled	

6.4.2.4 PCI Express Configuration Submenu

Feature	Options	Description
PCI Express Root Port 1	Submenu	Control the PCI Express Root Port.
PCI Express Root Port 2	Submenu	Control the PCI Express Root Port.
PCI Express Root Port 3	Submenu	Control the PCI Express Root Port.
PCI Express Root Port 4	Submenu	Control the PCI Express Root Port.
PCI Express S0ix Settings	Submenu	PCI Express S0ix Settings

Native PCI Express Support	Disabled	Enable or disable native OS PCI Express support.
	Enabled	

6.4.2.5 PCI Express Root Port 1/2/3/4 Submenu

Feature	Options	Description
PCI Express Root Port 1	**Enabled**	Control the PCI Express Root Port.
	Disabled	
ASPM	**Auto**	PCI Express Active State Power Management settings.
	Disabled	
	L0s	
	L1	
	L0sL1	
URR	**Disabled**	PCI Express Unsupported Request Reporting Enable/Disable.
	Enabled	
FER	**Disabled**	Enable or disable PCI Express device Fatal Error Reporting.
	Enabled	
NFER	**Disabled**	Enable or disable PCI Express device Non-Fatal Error Reporting
	Enabled	
CER	**Disabled**	Enable or disable PCI Express device Correctable Error Reporting.
	Enabled	
SEFE	**Disabled**	Root PCI Express System Error on Fatal Error Enable/Disable.
	Enabled	
SENFE	**Disabled**	Enable or disable Root PCI Express System Error on Non-Fatal Error.
	Enabled	
SECE	**Disabled**	Root PCI Express System Error on Correctable Error
	Enabled	Enable/Disable.
PME SCI	Disabled	Enable or disable PCI Express PME (power management event) SCI.
	Enabled	
Ext Sync	**Disabled**	Enable Express Ext Sync Enable/Disable.
	Enabled	
PCIe Spee	**Auto**	Configure PCIe Speed. CHV A1 always with Gen1 Speed.
	Gen 2	
	Gen 1	
Detect Non-compliant Device	**Disabled**	Try to detect also a non-compliant PCI Express device. If enabled, it will take more time during POST.
	Enabled	
L1 Substates	Disabled	PCI Express L1 Substates settings.
	L1.1	
	L1.2	
	L1.1 & L1.2	
Non-Common Clock with	Enabled	

SSC Enabled Mode	**Disabled**	Assume the root port is operating at a non-common clock with SSC enabled.
Transmitter Half Swing	Enabled	Transmitter Half Swing Enable/Disable.
	Disabled	
Tx Eq Deemphasis Selection	3.5dB	Select the level of de-emphasis for an Upstream component.
	6dB	

6.4.2.6 PCI Express S0ix Settings Submenu

Feature	Options	Description
D0 S0ix Policy	**PCIe RC shall be in D3**	PCIe D0 S0ix Policy
	S0i1 is the deepest S0ix state	
	PCIe RC is in D0 when entering S0IX	
	Reserved	
Evaluate CLKREQ State	**Enabled**	Enable/disable evaluation of CLKREQ state
	Disabled	
CLKREQ# Enable	**CLKREQ#[0]**	CLKREQ#[x] shall be evaluated during PCIe in D0 S0ix entry and exit criteria checking
	CLKREQ#[1]	
	CLKREQ#[2]	
	CLKREQ#[3]	
S0ix LTR Threshold	1ns	PCIe S0ix LTR Threshold: Latency Scale
	32ns	
	1024ns	
	32,768ns	
	1,048,576ns	
	33,554,321ns	
PCIe LTR Threshold	**150**	PCIe S0ix LTR Threshold: Latency Value. This value is multiplied by latency Scale

6.5 Security Setup

Select the Security tab from the setup menu to enter the Security setup screen.

Feature	Options	Description
BIOS Password	Enter password	Set BIOS Password
BIOS Lock	**Enabled**	Enable/Disable the BIOS Lock Enable feature.
	Disabled	
HDD Security Configuration	Submenu	Set HDD Password
Secure Boot Menu	Submenu	Customizable Secure Boot settings

6.5.1 HDD Security Configuration Submenu

Feature	Options	Description
Set User Password	Enter password	Set HDD user password. It is recommended to power cycle system after setting HDD passwords

6.5.2 Secure Boot Menu Submenu

Feature	Options	Description
System Mode	No option	Secure Boot information
Secure Boot	No option	Secure Boot information
Vendor Keys	No option	Secure Boot information
Secure Boot	**Disabled**	Secure Boot Can be enabled if 1.System running in User mode with enrolled Platform Key (PK) 2. CSM function is disabled
	Enabled	
Secure Boot Mode	Standard	Secure Boot mode selector. 'Custom' Mode enables users to change Image Execution policy and manage Secure Boot Keys
	Custom	
Key Management	Submenu	Enables experienced users to modify Secure Boot variables

6.6 Boot Setup

Select the Boot tab from the setup menu to enter the Boot setup screen.

Feature	Options	Description
Setup Prompt Timeout	**1**	The number of seconds to wait for the setup activation key. 65535(0xFFFF) means indefinite waiting. 0 means no wait (not recommended).
Bootup Number State	**On**	Select the keyboard Num Lock state
	Off	
Power Loss Control	**Remain Off**	Determines if the system is turned on/off after a power loss failure.
	Turn On	
	Last State	
AT Shutdown Mode	System Reboot	Determines the behavior of an AT-powered system after a shutdown.
	Hot S5	
Enter Setup If No Boot Device	No	Select whether the setup menu should be started if no boot device is connected.
	Yes	
Enter Popup Boot Menu	No	Select whether the popup boot menu can be started.
	Yes	
Boot Priority Selection	UEFI Standard	Set boot priority selection method. Type Based: Determine boot priority by device type. UEFI Standard: Determine boot priority by specific device selection. Devices must be present; priority will be changed if devices are removed or added.
	Type Based	
Boot Option Sorting Method	**Legacy First**	UEFI First: Try all UEFI boot options before the first legacy boot option. Legacy First: Vice versa.
	UEFI First	
Type Based Boot Priority	**Device Boot Priority Selection**	

Feature	Options	Description
Battery Support	**Auto (Battery Manager)**	Battery system support selection. Select 'Battery-Only On I2C
	Battery-Only On I2C Bus	Bus' for battery-only systems using I2C bus and 'Battery-Only
	Battery-Only On SMBus	On SMBus' for battery-only systems using SMBus. Select Auto for systems equipped with a real battery system manager (connected via 12C or SMBus)
System Off Mode	**G3/Mech Off**	Define the system state after shutdown when a battery system is present.
	S5/Sof Off	
Quiet Boot	**Disabled**	Enables or disables Quiet Boot option
	Enabled	
Device-Based Boot Priority	**Device Boot Priority Selection**	

UEFI Fast Boot	**Disabled**	Enable or disable boot with initialization of a minimal set of devices required to launch an active boot option. It does not affect BBS/legacy boot options.
	Enabled	
UEFI Screenshot Capability	**Disabled**	If Enabled, you can press LCtrl+Lalt+F12 to take a screenshot from the current screen. It will be saved as a PNG image on the first writable FAT32 partition found.
	Enabled	
New Boot Option Policy	**Default**	Controls the placement of newly detected UEFI boot options
	Place First	
	Place Last	

6.7 Save & Exit Setup

Select the Save & Exit tab from the setup menu to enter the Save & Exit setup screen.

Feature	Options	Description
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
Save Changes		Save changes made so far to any of the setup options.
Discard Changes		Discard changes made so far to any of the setup options.
Restore Defaults		Restore/Load default values for all setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override		
Generate Menu Layout File		The menu layout file will be generated and stored on the first writable file system found.