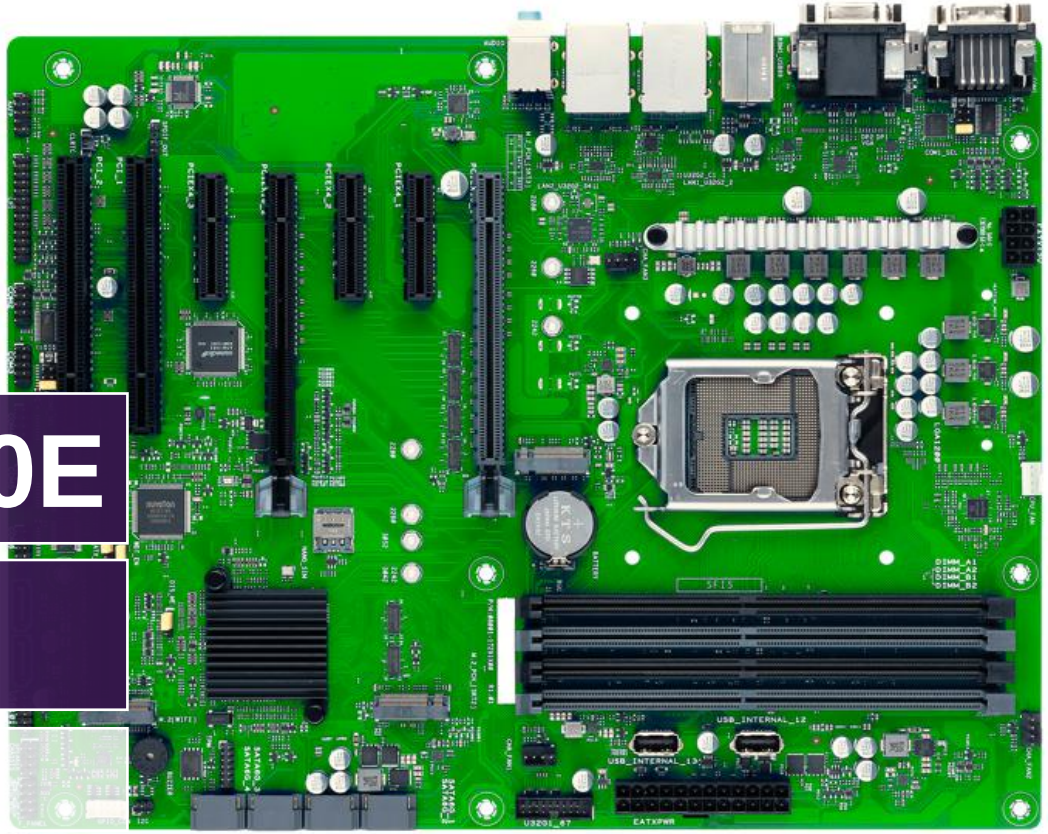
RUBY-D812-Q470E

Industrial ATX Board



Version 1.2

Revision History

R1.0	Preliminary
R1.1	Update REAR IO Com port pin define information
R1.2	Add information about Support 11th CPU limitation

Contents

Preface

This user's guide provides information about the components, features, connectors and BIOS Setup menus available on the RUBY-D812. This document should be referred to when designing ATX IMB application. The other reference documents that should be used include the following:

- ✧Intel Comet Lake Design Guide
- ✧Intel Comet Lake Specification

Please contact Portwell Sales Representative for above documents.

Disclaimer

The information contained within this user's guide, including but not limited to any product specification, is subject to change without notice.
Portwell provides no warranty with regard to this user's guide or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. Portwell assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the user's guide. In no event shall Portwell be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this user's guide or any other information contained herein or the use thereof.

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this User's guide or the Portwell website, are the property of their respective trademark holders. These trademark holders are not affiliated with Portwell, our products, or our website.

Warranty

Portwell makes no representation, warranty or guaranty, express or implied regarding the products except its standard form of limited warranty (“Limited Warranty”). Portwell may in its sole discretion modify its Limited Warranty at any time and from time to time.

Beginning on the date of shipment to its direct customer and continuing for the published warranty period, Portwell represents that the products are new and warrants that each product failing to function properly under normal use, due to a defect in materials or workmanship or due to non conformance to the agreed upon specifications, will be repaired or exchanged, at Portwell’s option and expense.

Certification

Portwell is certified to DIN EN ISO 9001:2000 standard.

Technical Support

Portwell technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented.

We request that you first visit our website at http://www.portwell.com.tw/support/ for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at tsd@mail.portwell.com.twfor further assistance. Thank you!

1 Introduction

RUBY-D812-Q470E based on the Intel® Core™ Processor which offers 14nm Hi-K process technology with energy efficient architecture. RUBY-D812 support dual channels DDR4 Long - DIMM up to 128GB.

Desktop solution is still popular in the market of DVR and Factory Automation which can fulfill most of these applications; therefore, with high performance and high-end specifications, RUBY-D812 is our first generation Comet -S chip architecture on ATX IMB line.

2 Specifications

Main Processor	◆ Intel® Comet -S Core™ i Processors
System Chipset	◆ Intel®Q470E Express chipset
System BIOS	◆ AMI UEFI BIOS
Main Memory	◆ Up to 128GB in 4 slots DDR4 Long-DIMM sockets. Supports dual channel DDR4 2400/2666/2933 MHz SDRAM
Graphics	◆ Controller: Intel® Gfx Gen 9, UHD 630 graphics ◆ VGA: Supports VGA up to resolution 1920 x 1200 ◆ Dual DP: Supports DP up to resolution 4096 x 2160 ◆ HDMI: Supports HDMI up to resolution 4096 x 2160
Expansion Interface	◆ One SIM slot ◆ One M.2 (Key E_2230) for Wireless(PCIe x1 / USD2.0) ◆ One M.2 (Key M_2242/2260/2280) for SSD(PCIe x4 / SATA) ◆ One M.2 (Key B_3042/3052, 2260/2280) for Wireless(PCIe x1 / USB3.2 Gen1 / USD2.0) ◆ Two PCIe x16 slot(1 x16 mode / 2 x8 mode) ◆ Three PCIe x4 slot ◆ Two PCI slot
SATA Interface	◆ Six SATA ports(SATA 6Gb/s) *If install M.2 PCIe x4/ SATA SSD on M.2 M key slot, 2/ 1 SATA port will be disabled
Input/Output	◆ COM Ports: 2x RS-232/422/485 (one on REAR I/O, one on board header)，4x RS-232 on board header ◆ USB Port: 4x USB 3.2 Gen2(3 x type A, 1 x Type C), 1 x Header support additional 2 x USB3.2 Gen1 connectors & 1 x Header support additional 2 x USB2.0 connectors & 2 x Vertical connector ◆ Audio Interface: Line-in / Line-Out / Mic-In

Ethernet	◆ Supports one 10/100/1000 Mbps Ethernet port (s) via PCI Express x1 bus ◆ Supports one 10/100/1000/2500 Mbps Ethernet port (s) via PCI Express x1 bus
High Drive GPIO	◆ One pin-header for GPIO(8bit GPIO)
Mechanical and environmental specifications	◆ Operating temperature: 0 ~ 60° C ◆ Storage temperature:-20 ~ 80° C ◆ Humidity: 15 ~ 95% non-condensing ◆ Power supply voltage: ATX ◆ Board size: 304.8mm x 243.8 mm

2.1 Supported Operating Systems

The RUBY-D812 supports the following operating systems.

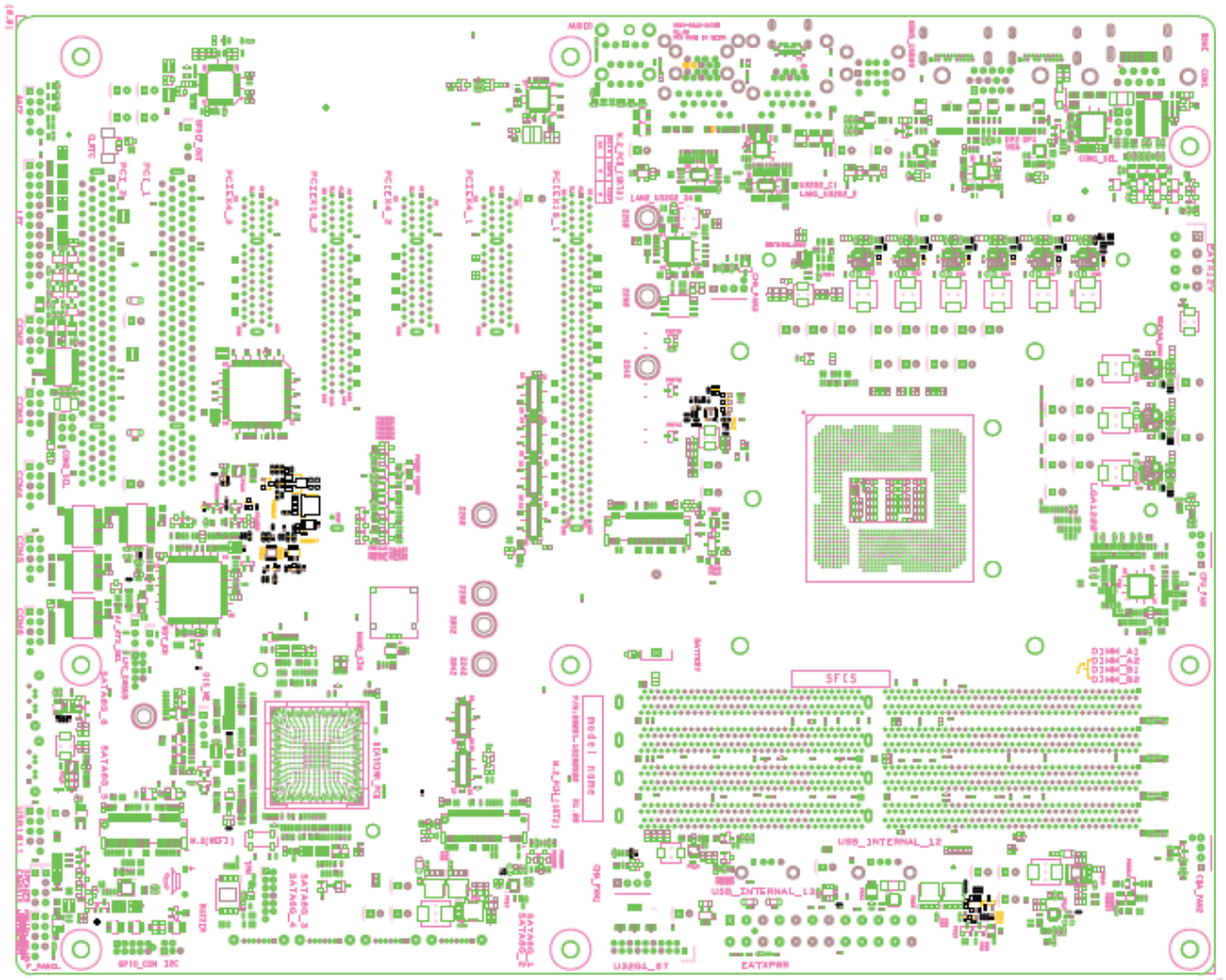
✧ Windows* 10 IOT Enterprise RS51(64-bit)

✧ Ubuntu, SuSe, Redhat Enterprise 1,2 (Kernel 4.14)

✧ Yocto Project* BSP tool-based embedded Linux distribution1 (64-bit)

✧ Wind River VxWorks 7.0

2.2 Mechanical Dimensions



2.3 Power Consumption

Test Configuration	
CPU Type	Intel® Core™ i9-10900TE CPU @ 1.8GHz
SBC BIOS	Portwell, Inc. RUBY-D812 TEST BIOS (0.04.00)
Memory	WARIS UB-DIMM DDR4 2133 16GB
VGA Card	Onboard Intel® UHD Graphics 630
VGA Driver	Intel® UHD Graphics 630 ver:26.20.100.7926_Q0
LAN Card	Onboard Intel® Ethernet Connection I219-LM
LAN Driver	Intel® Ethernet Connection I219-LM Version: 12.18.9.23
LAN Card #2	Onboard Intel® I225V Gigabit Network Connection
LAN Driver #2	Intel® I225V Gigabit Network Connection Version: 26.4
Audio Card	Onboard Realtek ALC897 High Definition Audio
Audio Driver	Realtek ALC897 High Definition Audio Version: 6.0.9222.1
Chipset Driver	Intel® Comet lake-S Chipset Device Software Version:3.1.7.142
USB 3.0 Driver	Intel® USB 3.0 eXtensible Host Controller Adaptation Driver
SATA HDD	Intel SSD 256G
Power Supply	FSP460-60PFB 460W / GADIWA 5V/12V DC POWER

Power consumption			
ATX:			
Item	Power ON	Full Loading 10Min	Full Loading 30Min
CPU +12V	0.98A	2.05A	1.98A
System +12V	0.83A	1.48A	1.26A
System +3.3V	0.55A	0.65A	0.69A
System +5V	1.11A	1.37A	1.34A
System+ Device +12V	0.97A	1.81A	1.56A
System+ Device +5V	1.87A		
USB2.0 Loading Test	4.98 V/ 570 mA		

2.4 Environmental Specifications

Storage Temperature : -20~80°C

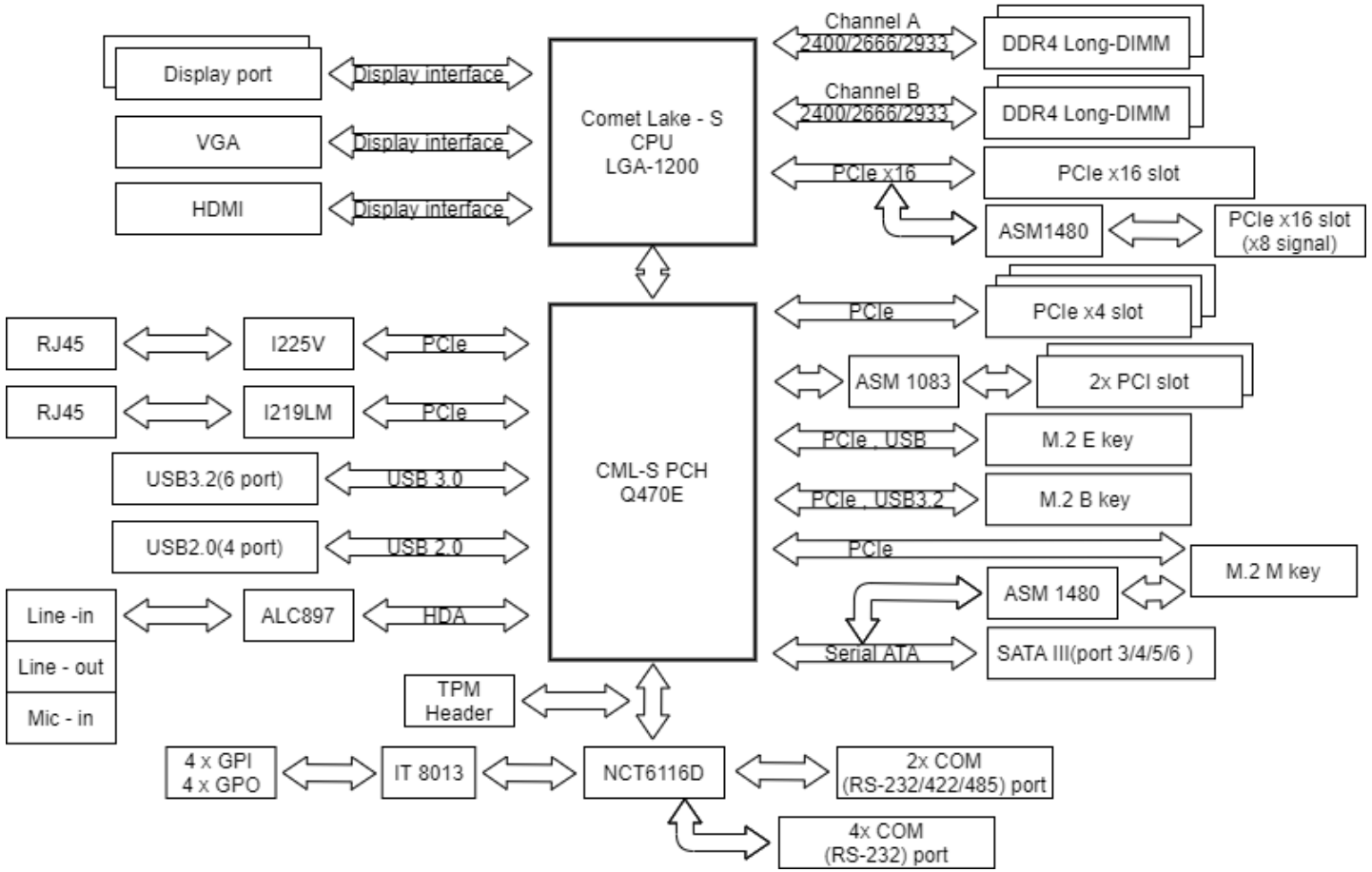
Operation Temperature : 0~60°C

Storage Humidity : 15~95%

Operation Humidity: 10~90%

3 Block Diagram

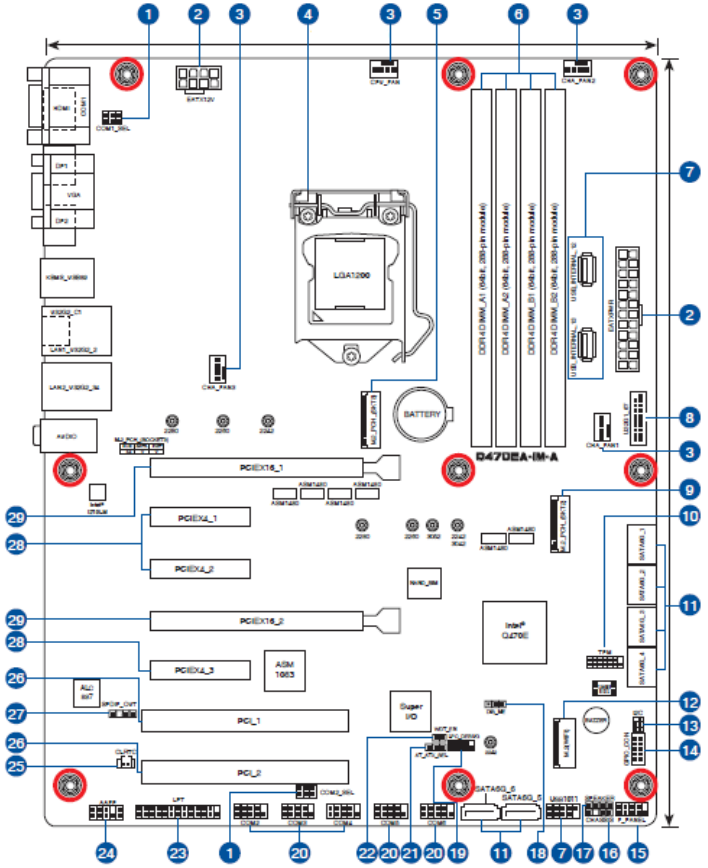
※The RUBY-D812 support 10th generation intel CPU only



4 Hardware Configuration

4.1 Jumpers and Connectors

This chapter indicates jumpers', headers' and connectors' locations. Users may find useful information related to hardware settings in this chapter.



4.2 Jumpers Settings

For users to customize RUBY-D812's features. In the following sections, Short means covering a jumper cap over jumper pins; Open or N/C (Not Connected) means removing a jumper cap from jumper pins. Users can refer to Figure 1 for the Jumper allocations.

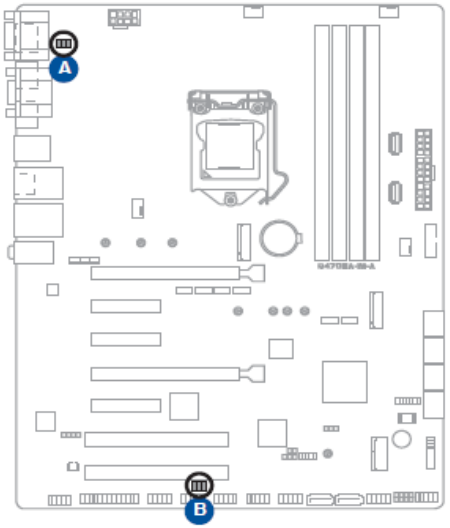
Jumper Table

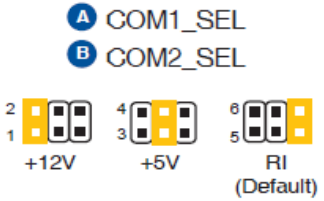
The jumper settings are schematically depicted in this manual as follows:

Jumper Function List	
1	COM RING/+5V/+12V selection jumper (6-pin COM1_SEL)
2	EATX Power connectors (24-pin EATXPWR, 8-pin EATX12V)
3	CPU and Chassis Fan headers (4-pin CPU_FAN, 4-pin CHA_FAN1/2/3)
4	Intel® LGA1200 CPU socket
5	M.2 socket 3 (M.2_PCH_(SKT3))
6	DDR4 DIMM slots
7	USB 2.0 connectors / header (USB_INTERNAL_12, USB_INTERNAL_13, USB1011)
8	USB 3.2 Gen 1 header (20-1 pin U32G1_67)
9	M.2 socket 2 (M.2_PCH_(SKT2))
10	TPM header (14-1 pin TPM)
11	SATA 6.0Gb/s ports (7-pin SATA6G_1-6)

12	M.2 Wi-Fi
13	I2C header (6-pin I2C)
14	General Purpose Input/Output header (10-pin GPIO_CON)
15	System Panel header (10-1 pin F_PANEL)
16	Chassis Intrusion header (4-1 pin CHASSIS)
17	Speaker header (4-pin SPEAKER)
18	Disable ME jumper (3-pin DIS_ME)
19	LPC Debug header (10-1 pin LPC_DEBUG)
20	COM Port headers (10-1 pin COM2, COM3, COM4, COM5, COM6)
21	AT/ATX Mode selection jumper (3-pin AT_ATX_SEL)
22	WDT Enable jumper (2-pin WDT_EN)
23	LPT header (26-1 pin LPT)
24	Front Panel Audio header (10-1 pin AAFP)
25	Clear CMOS header (2-pin CLRTC)
26	PCI slots
27	Digital Audio header (4-1 pin SPDIF_OUT)
28	PCI Express 3.0/2.0 x4 slots
29	PCI Express 3.0/2.0 x16 slots

1: COM RING/+5V/+12V selection jumper (6-pin COM1_SEL)

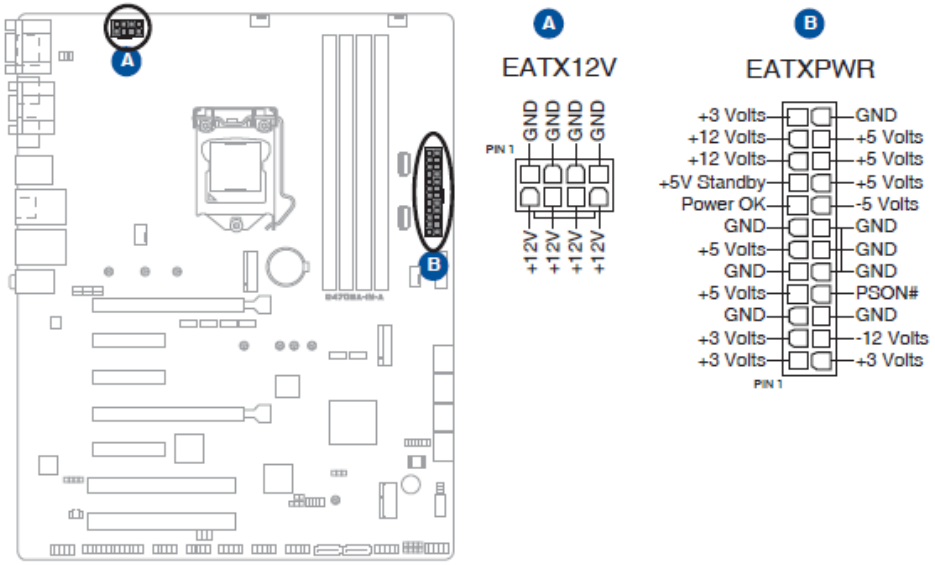




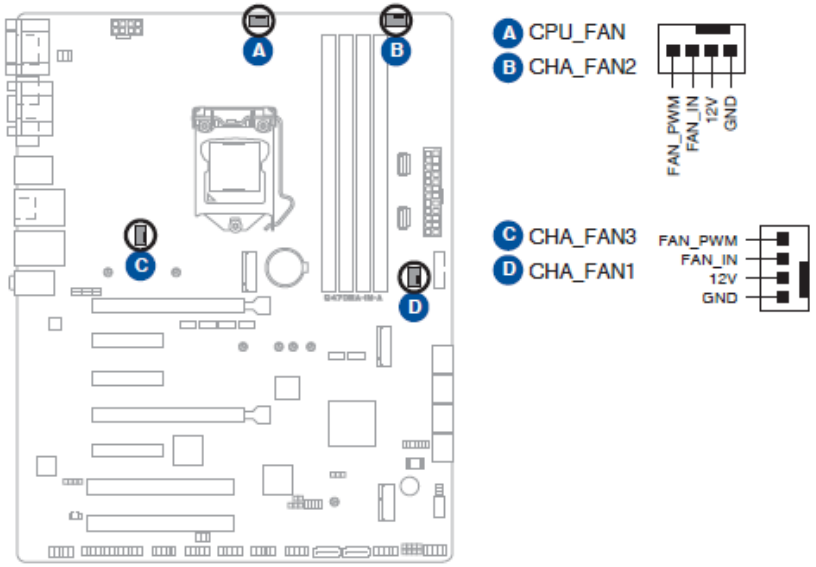
	RS232	RS485	RS422
Pin1	DCD	B	T(B)
Pin2	RXD	A	T(A)
Pin3	TXD	NC	R(A)
Pin4	DTR	NC	R(B)
Pin5	GND	GND	GND
Pin6	DSR	NC	NC
Pin7	RTS	NC	NC
Pin8	CTS	NC	NC
Pin9	RI/5V/12V	NC/5V/12V	NC/5V/12V

PIN No.	Description
1-2(Short)	+12V
2-3(Short)	+5V
5-6(Short)	★RI (Default)

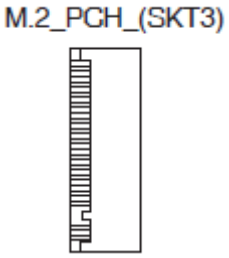
2: EATX Power connectors (24-pin EATXPWR, 8-pin EATX12V)



3: CPU and Chassis Fan headers (4-pin CPU_FAN, 4-pin CHA_FAN1/2/3)

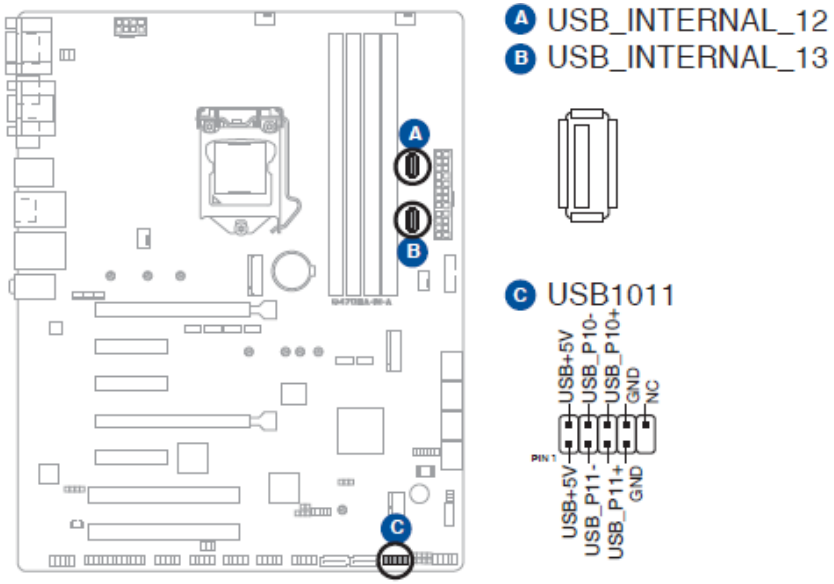


5: M.2 socket 3 (M.2_PCH_(SKT3))



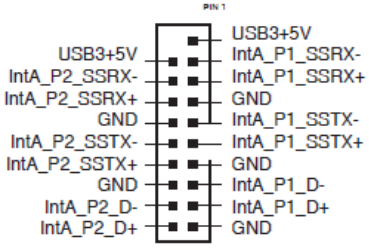
- The M.2 SSD module is purchased separately.
- This socket supports M Key and 2242/2260/2280 storage devices

7: USB 2.0 connectors / header (USB_INTERNAL_12, USB_INTERNAL_13, USB1011)



NOTE: These Universal Serial Bus (USB) ports / header are for USB 2.0 devices

8: USB 3.2 Gen 1 header (20-1 pin U32G1_67)

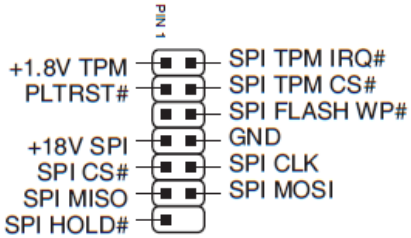


9: M.2 socket 2 (M.2_PCH_(SKT2))

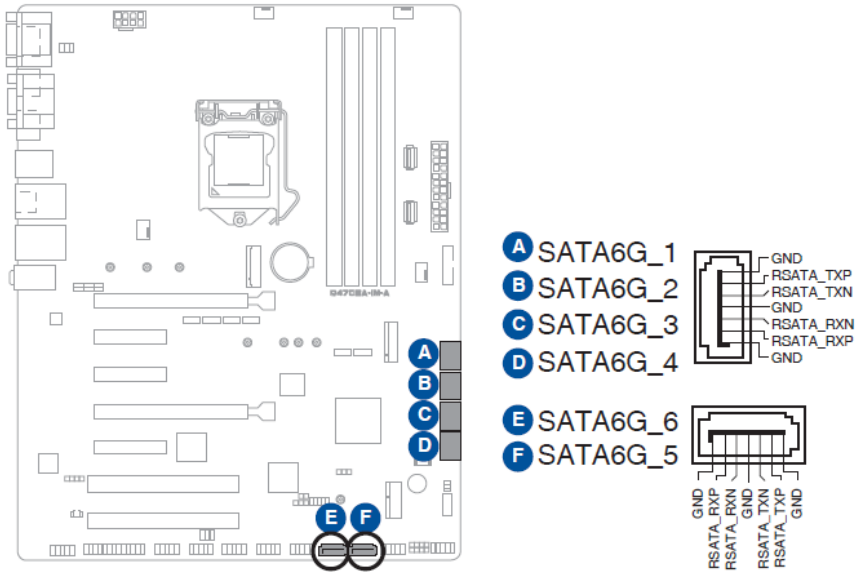
M.2_PCH_(SKT2)

- The M.2 4G/5G module is purchased separately.
- This socket supports B Key and 3042/3052 (PCIe x1/USB3.2 GEN1/USB 2.0) devices.

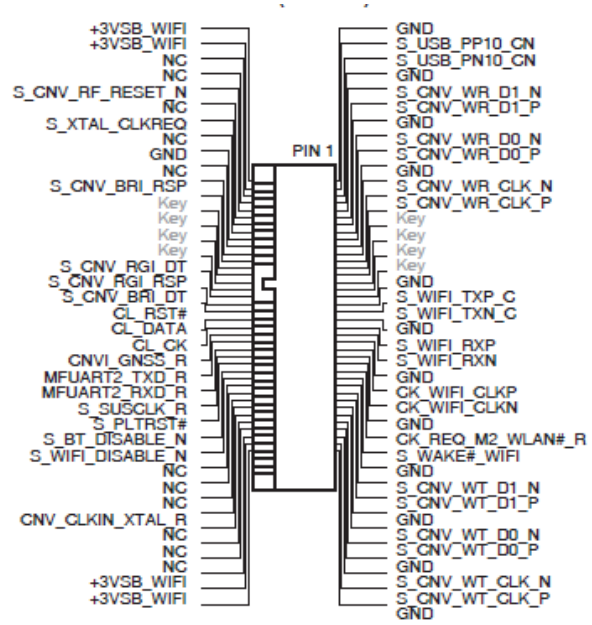
10: TPM header (14-1 pin TPM)



11: SATA 6.0Gb/s ports (7-pin SATA6G_1-6)

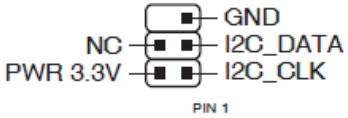


12: M.2 Wi-Fi

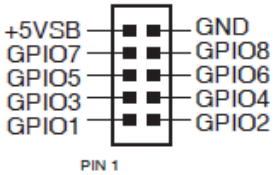


- The M.2 Wi-Fi module is purchased separately.

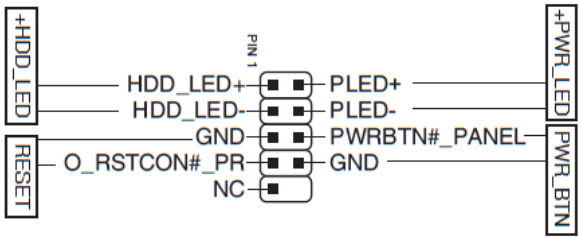
13: I2C header (6-pin I2C)



14: General Purpose Input/Output header (10-pin GPIO_CON)



15: System Panel header (10-1 pin F_PANEL)



- System power LED (2-pin +PWR_LED)

  This 2-pin header is for the system power LED. Connect the chassis power LED cable to this header. The system power LED lights up when you turn on the system power, and blinks when the system is in sleep mode.

- Hard disk drive activity LED (2-pin +HDD_LED)

  This 2-pin header is for the HDD Activity LED. Connect the HDD Activity LED cable to this header. The IDE LED lights up or flashes when data is read from or written to the HDD.

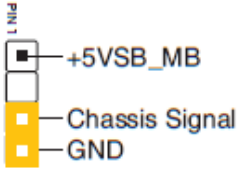
- ATX power button/soft-off button (2-pin PWR_BTN)

  This 2-pin header is for the system power button.

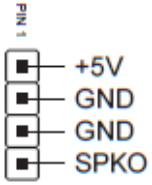
- Reset button (2-pin RESET)

This 2-pin header is for the chassis-mounted reset button for system reboot without turning off the system power.

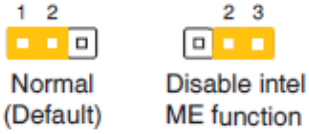
16: Chassis Intrusion header (4-1 pin CHASSIS)



17: Speaker header (4-pin SPEAKER)

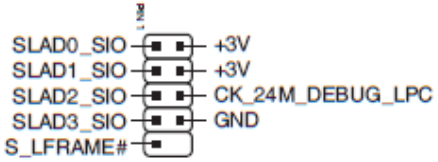


18: Disable ME jumper (3-pin DIS_ME)

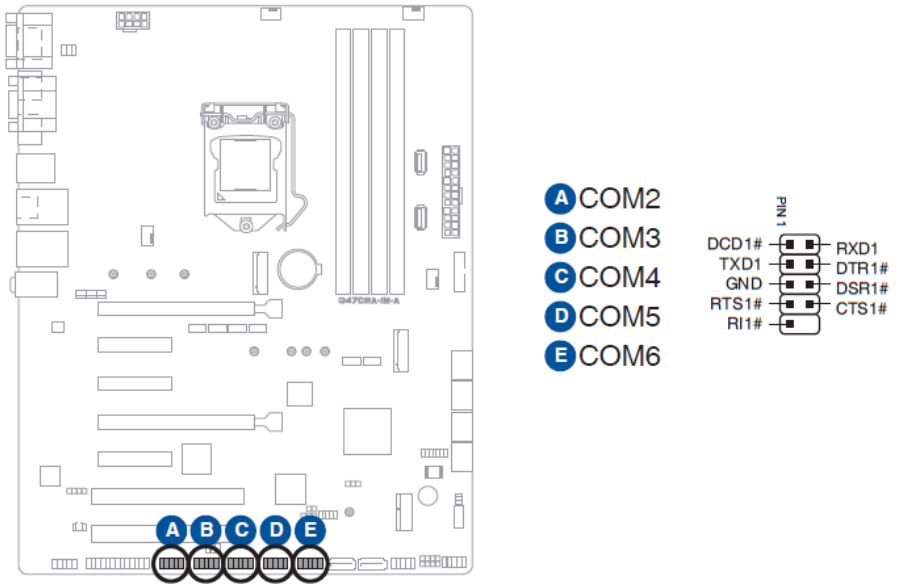


PIN No.	Description
1-2(Short)	★Normal(Default)
2-3(Short)	Disable intel ME function

19: LPC Debug header (10-1 pin LPC_DEBUG)

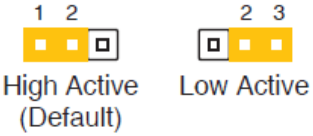


20: COM Port headers (10-1 pin COM2, COM3, COM4, COM5, COM6)



A COM2
B COM3
C COM4
D COM5
E COM6

21: AT/ATX Mode selection jumper (3-pin AT_ATX_SEL)

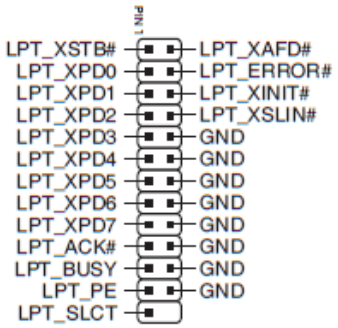


PIN No.	Description
1-2(Short)	★High Active
2-3(Short)	Low Active

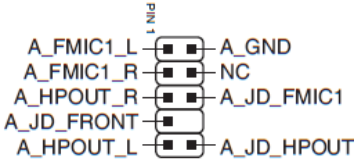
22: WDT Enable jumper (2-pin WDT_EN)

NOTE: By default, this jumper is set to HW WDT enabled with a jumper cap attached.

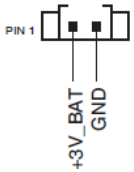
23: LPT header (26-1 pin LPT)



24: Front Panel Audio header (10-1 pin AAFP)



25: Clear CMOS header (2-pin CLRTC)

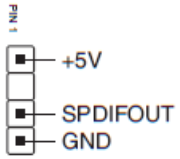


To erase the RTC RAM:

1. Turn OFF the computer and unplug the power cord.
2. Use a metal object such as a screwdriver to short the two pins.
3. Plug the power cord and turn ON the computer.
4. Hold down the <Del> key during the boot process and enter BIOS Setup to re-enter data.

NOTE: If the steps above do not help, remove the onboard battery and move the jumper again to clear the CMOS RTC RAM data. After clearing the CMOS, reinstall the battery.

27: Digital Audio header (4-1 pin SPDIF_OUT)



5 Signal Descriptions

5.1 Watch Dog Signal

WDT setting

SIO_INDEX_PORT is 0x2E

SIO_DATA_PORT is 0x2F

1. Set WDT Time Unit

```
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO

Outportb(SIO_INDEX_PORT, 0x07);
Outportb(SIO_DATA_PORT,    0x08);
Outportb(SIO_INDEX_PORT, 0xF0); //select WDT setting
val = Inportb(SIO_DATA_PORT) // Read current WDT setting

val = val | 0x08; // minute mode, val = val & 0xF7 if second mode
Outportb(SIO_INDEX_PORT, 0xF0); //select WDT setting
Outportb(SIO_DATA_PORT,    val); // Write back WDT setting

Outportb(SIO_INDEX_PORT, 0xAA); // Lock SIO
```

2. Set WDT Time

```
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO

Outportb(SIO_INDEX_PORT, 0x07);
Outportb(SIO_DATA_PORT,    0x08);
Outportb(SIO_INDEX_PORT, 0xF1); //select time value
Outportb(SIO_DATA_PORT,    Time); // Write WDT time, value 1 to 255

Outportb(SIO_INDEX_PORT, 0xAA); // Lock SIO
```

3. Enable WDT

```
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO

Outportb(SIO_INDEX_PORT, 0x07); // select device
Outportb(SIO_DATA_PORT,    0x08); // device 8
Outportb(SIO_INDEX_PORT, 0x30); //select WDT status port
val = Inportb(SIO_DATA_PORT) // Read current WDT status

val = val | 0x01; // Enable WDT Timer
```

```
Outportb(SIO_INDEX_PORT, 0x30); //select WDT status port
Outportb(SIO_DATA_PORT,    val); // Write back WDT status

Outportb(SIO_INDEX_PORT, 0xAA); // Lock SIO
```

4. Disable WDT

```
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO
Outportb(SIO_INDEX_PORT, 0x87); // Unlock SIO

Outportb(SIO_INDEX_PORT, 0x07);
Outportb(SIO_DATA_PORT,    0x08);
Outportb(SIO_INDEX_PORT, 0xF1); //select time value
Outportb(SIO_DATA_PORT,    0x00); // Clear WDT time, it means WDT Time-Out disable
Outportb(SIO_INDEX_PORT, 0x30); //select WDT status port

val = Inportb(SIO_DATA_PORT) // Read current WDT status
val = val & 0xFE; // Disable WDT Timer
Outportb(SIO_INDEX_PORT, 0x30); //select WDT status port
Outportb(SIO_DATA_PORT,    val); // Write back WDT status

Outportb(SIO_INDEX_PORT, 0xAA); // Lock SIO
```

5.2 GPIO Signal

GPIO Setting

1. Get SMBUS_BASE address

```
val = 0x8000FC20;
Outportd(0xCF8, val);
val = Inportd(0xCFC);
SMBUS_BASE = val & 0x0000FFE0;
```

2. Set GPIOn to GPI or GPO

```
Status = Inportb(SMBUS_BASE + 0x00);
Outportb(SMBUS_BASE + 0x00, Status); // SMBus Clear Status

Outportb(SMBUS_BASE + 0x02, 0x08); // Set SMBus CMD to Byte Data
Outportb(SMBUS_BASE + 0x04, 0x41); // Set SMBus Slave Address to 0x40 and excute Read flow
Outportb(SMBUS_BASE + 0x03, 0x00); // Set SMBus Reg
val = Inportb(SMBUS_BASE + 0x02);
val = val | 0x40;
Outportb(SMBUS_BASE + 0x02, val); // Excute SMBus Command

Status = Inportb(SMBUS_BASE + 0x00); // Get SMBus Status
while (!(Status & 0x8E)) { // Wait for SMBus finished command
```

```
    MicroSecondDelay(10);
    Status = Inportb(SMBUS_BASE + 0x00);
}

val = Inportb(SMBUS_BASE + 0x05); // Get SMBus Data
val = val | (0x01 << GPIOn); // GPI, val = val | ~(0x01 << GPIOn) if GPO, GPIOn is value 0 to 7

Status = Inportb(SMBUS_BASE + 0x00);
Outportb(SMBUS_BASE + 0x00, Status); // SMBus Clear Status

Outportb(SMBUS_BASE + 0x02, 0x08); // Set SMBus CMD to Byte Data
Outportb(SMBUS_BASE + 0x04, 0x40); // Set SMBus Slave Address to 0x40 and excute Write flow
Outportb(SMBUS_BASE + 0x03, 0x00); // Set SMBus Reg
Outportb(SMBUS_BASE + 0x05, val); // Set SMBus Data
val = Inportb(SMBUS_BASE + 0x02);
val = val | 0x40;
Outportb(SMBUS_BASE + 0x02, val); // Excute SMBus Command

Status = Inportb(SMBUS_BASE + 0x00); // Get SMBus Status
while (!(Status & 0x8E)) { // Wait for SMBus finished command
    MicroSecondDelay(10);
    Status = Inportb(SMBUS_BASE + 0x00);
}
```

3. Get GPIOn GPI value

```
Status = Inportb(SMBUS_BASE + 0x00);
Outportb(SMBUS_BASE + 0x00, Status); // SMBus Clear Status

Outportb(SMBUS_BASE + 0x02, 0x08); // Set SMBus CMD to Byte Data
Outportb(SMBUS_BASE + 0x04, 0x41); // Set SMBus Slave Address to 0x40 and excute Read flow
Outportb(SMBUS_BASE + 0x03, 0x09); // Set SMBus Reg
val = Inportb(SMBUS_BASE + 0x02);
val = val | 0x40;
Outportb(SMBUS_BASE + 0x02, val); // Excute SMBus Command

Status = Inportb(SMBUS_BASE + 0x00); // Get SMBus Status
while (!(Status & 0x8E)) { // Wait for SMBus finished command
    MicroSecondDelay(10);
    Status = Inportb(SMBUS_BASE + 0x00);
}

val = Inportb(SMBUS_BASE + 0x05); // Get SMBus Data
if (val & (0x01 << GPIOn)) // Determine if GPIOn is High or Low, GPIOn is value 0 to 7
    return HIGH; //GPI High
else
```

```
    return LOW; //GPI Low
```

4. Set GPIOn GPO value

```
Status = Inportb(SMBUS_BASE + 0x00);
Outportb(SMBUS_BASE + 0x00, Status); // SMBus Clear Status

Outportb(SMBUS_BASE + 0x02, 0x08); // Set SMBus CMD to Byte Data
Outportb(SMBUS_BASE + 0x04, 0x41); // Set SMBus Slave Address to 0x40 and excute Read flow
Outportb(SMBUS_BASE + 0x03, 0x0A); // Set SMBus Reg
val = Inportb(SMBUS_BASE + 0x02);
val = val | 0x40;
Outportb(SMBUS_BASE + 0x02, val); // Excute SMBus Command

Status = Inportb(SMBUS_BASE + 0x00); // Get SMBus Status
while (!(Status & 0x8E)) { // Wait for SMBus finished command
    MicroSecondDelay(10);
    Status = Inportb(SMBUS_BASE + 0x00);
}

val = Inportb(SMBUS_BASE + 0x05); // Get SMBus Data
val = val | (0x01 << GPIOn); // GPO High, val = val | ~(0x01 << GPIOn) if GPO Low, GPIOn is value 0 to 7
```

```
Status = Inportb(SMBUS_BASE + 0x00);
Outportb(SMBUS_BASE + 0x00, Status); // SMBus Clear Status

Outportb(SMBUS_BASE + 0x02, 0x08); // Set SMBus CMD to Byte Data
Outportb(SMBUS_BASE + 0x04, 0x40); // Set SMBus Slave Address to 0x40 and excute Write flow
Outportb(SMBUS_BASE + 0x03, 0x0A); // Set SMBus Reg
Outportb(SMBUS_BASE + 0x05, val); // Set SMBus Data
val = Inportb(SMBUS_BASE + 0x02);
val = val | 0x40;
Outportb(SMBUS_BASE + 0x02, val); // Excute SMBus Command

Status = Inportb(SMBUS_BASE + 0x00); // Get SMBus Status
while (!(Status & 0x8E)) { // Wait for SMBus finished command
    MicroSecondDelay(10);
    Status = Inportb(SMBUS_BASE + 0x00);
}
```

6 System Resources

6.1 Intel® Comet Lake -S PCH

Intel® Q470E Chipset

※The RUBY-D812 support 10th generation intel CPU only

6.2 Main Memory

RUBY-D812 provides 4x Long-DIMM sockets. The maximum memory can be up to 128GB. Memory clock and related settings can be detected by BIOS via SPD interface.

Watch out the contact and lock integrity of memory module with socket, it will impact on the system reliability. Follow normal procedures to install memory module into memory socket. Before locking, make sure that all modules have been fully inserted into the card slots.

6.3 Installing the Single Board Computer

To install your RUBY-D812 into standard chassis or proprietary environment, please perform the following:
Step 1 : Check all jumpers setting on proper position
Step 2 : Install and configure CPU,CPU cooling and memory module on right position

Step 3 : Place RUBY-D812 into the dedicated position in the system
Step 4 : Attach cables to existing peripheral devices and secure it

WARNING

Please ensure that mother board is properly inserted and fixed by mechanism.

Note:

Please refer to section 6.3.1 to 6.3.4 to install INF/Graphic/LAN

6.3.1 Chipset Component Driver

RUBY-D812 is based on Intel® Q470E chipset and desktop processors including Core™ i7 / i5 / i3 sku . It's a new chipset that some old operating systems might not be able to recognize. To overcome this compatibility issue, for Windows Operating Systems such as Windows 10, please install its INF before any of other Drivers are installed.

6.3.2 Intel® UHD Graphics 630

RUBY-D812 has integrated Intel® UHD Graphics 630 which supports DirectX 12、OpenGL 4.5. It is the most advanced design to gain an outstanding graphic performance. RUBY-D812 supports VGA, DP,HDMI display output. This combination makes RUBY-D812 an excellent performance hardware.

Drivers Support

Please find the Graphic driver in the RUBY-D812 of Portwell download center. The driver supports Windows 10.

6.3.3 Intel LAN I225V / I219LM Gigabit Ethernet Controller

- Intel I225V Gigabit Ethernet controller and 1x RJ45 connectors on rear I/O
- Intel I219LM Gigabit Ethernet controller and 1x RJ45 connectors on rear I/O

Drivers Support

Please find Intel I225V / I219LM LAN driver in the RUBY-D812 of Portwell download center. The driver supports Windows 10.

7 BIOS Setup Items

7.1 Introduction

The following section describes the BIOS setup program. The BIOS setup program can be used to view and change the BIOS settings for the module. Only experienced users should change the default BIOS settings.

7.2 BIOS Setup

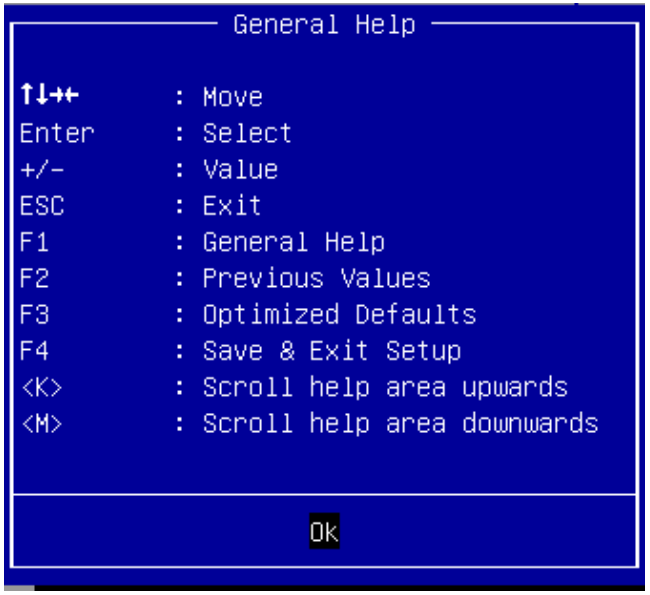
Power on the computer and the system will start POST (Power on Self Test) process. When the message below appears on the screen, press <Delete> or <ESC> key will enter BIOS setup screen.

Press<Delete> or <ESC> to enter SETUP

If the message disappears before responding and still wish to enter Setup, please restart the system by turning it OFF and On or pressing the RESET button. It can be also restarted by pressing <Ctrl>, <Alt>, and <Delete> keys on keyboard simultaneously.

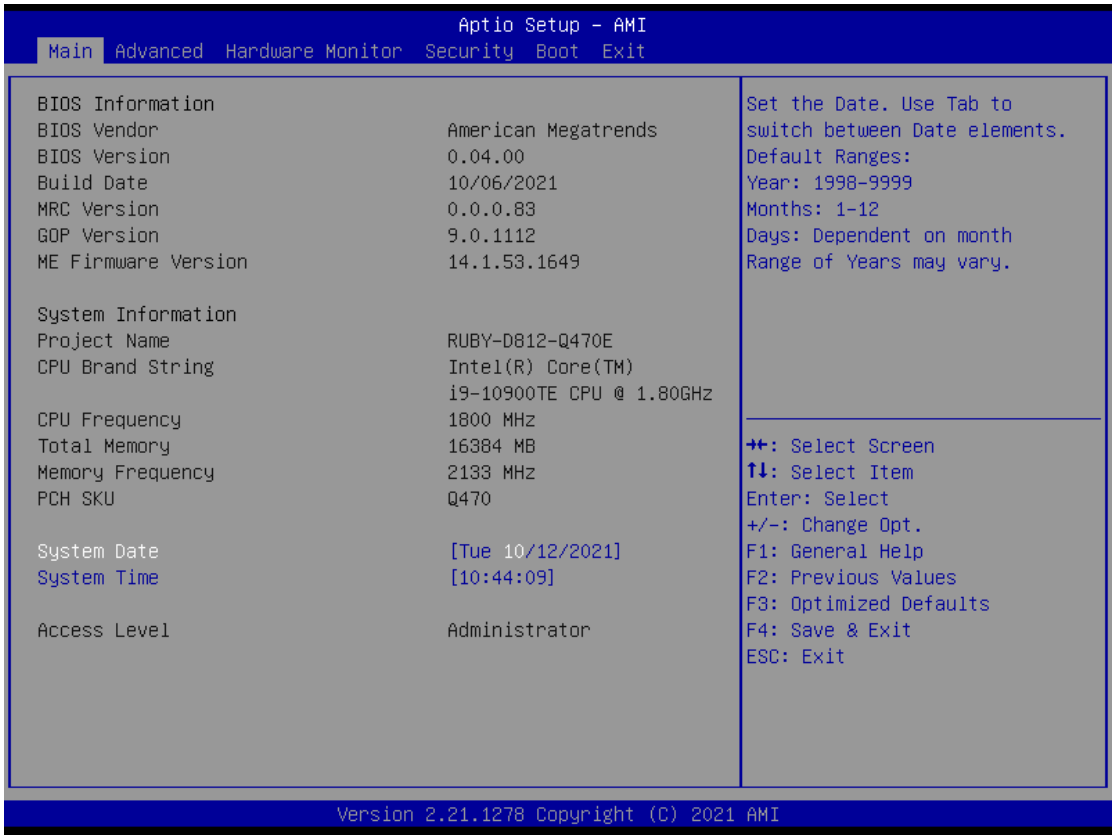
Press <F1> to Run General Help or Resume

The BIOS setup program provides a General Help screen. The menu can be easily called up from any menu by pressing <F1>. The Help screen lists all the possible keys to use and the selections for the highlighted item. Press <Esc> to exit the Help Screen.


General Help
↑↓→← : Move
Enter : Select
+/- : Value
ESC : Exit
F1 : General Help
F2 : Previous Values
F3 : Optimized Defaults
F4 : Save & Exit Setup
<K> : Scroll help area upwards
<M> : Scroll help area downwards
Ok

7.2.1 Main

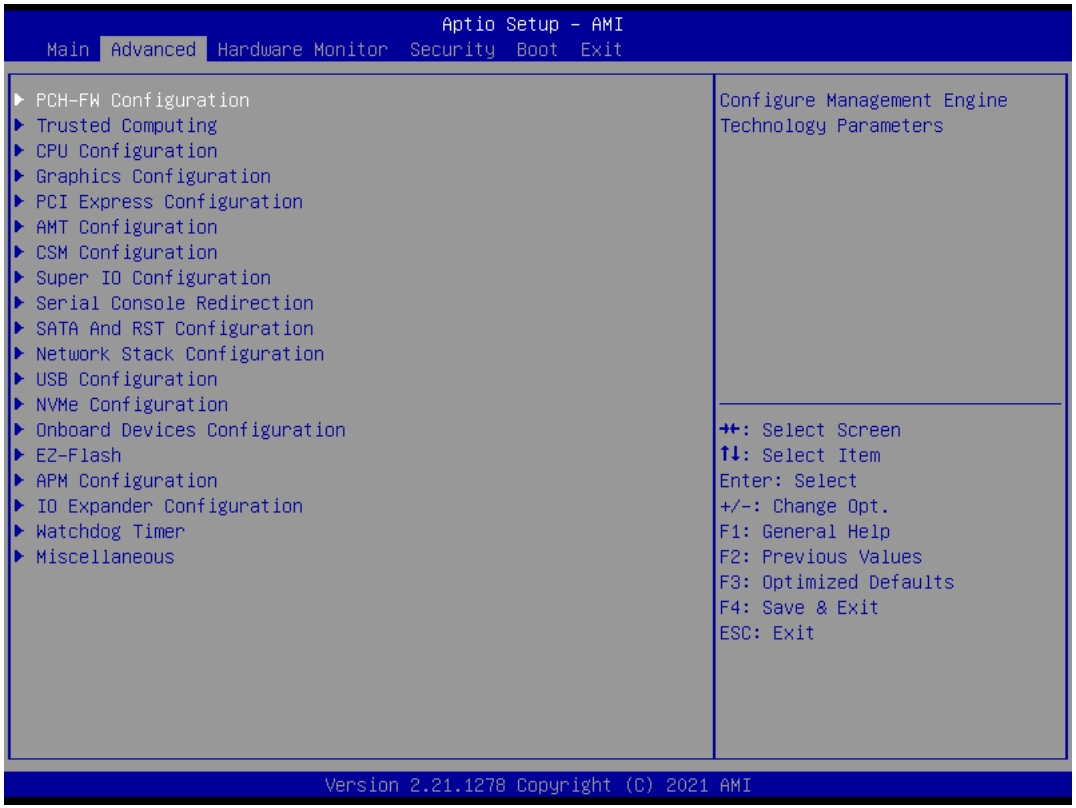
Use this menu for basic system configurations, such as time, date etc.



Feature	Description	Options
System Date	The date format is <Day>, <Month> <Date> <Year>. Use [+] or [—] to configure system Date.	
System Time	The time format is <Hour> <Minute> <Second>. Use [+] or [—] to configure system Time.	

7.2.2 Advanced

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



PCH-FW Configuration

Configure Management Engine Technology Parameters

Feature	Description	Options
TPM Device Selection	Selects TPM device: PTT or dTPM. PTT-Enable PTT in SkuMgr dTPM1.2 –Disables PTT in SkuMgr Warning! PTT/Dtpm will be disabled and all data saved on it will be lost.	★PTT, dTPM

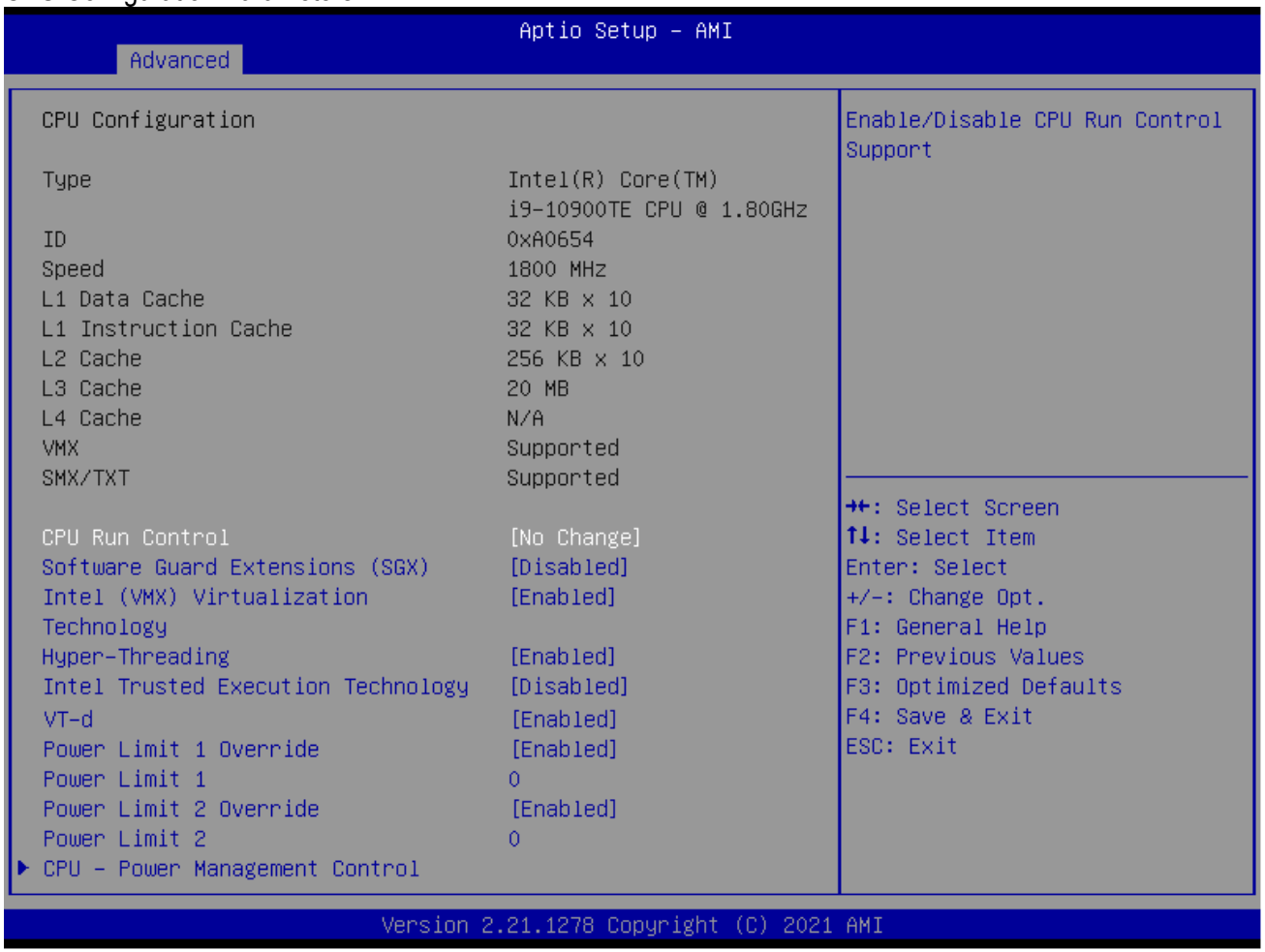
Trusted Computing

Trusted Computing Settings

Feature	Description	Options
Security Device Support	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.	★Enable, Disable

CPU Configuration

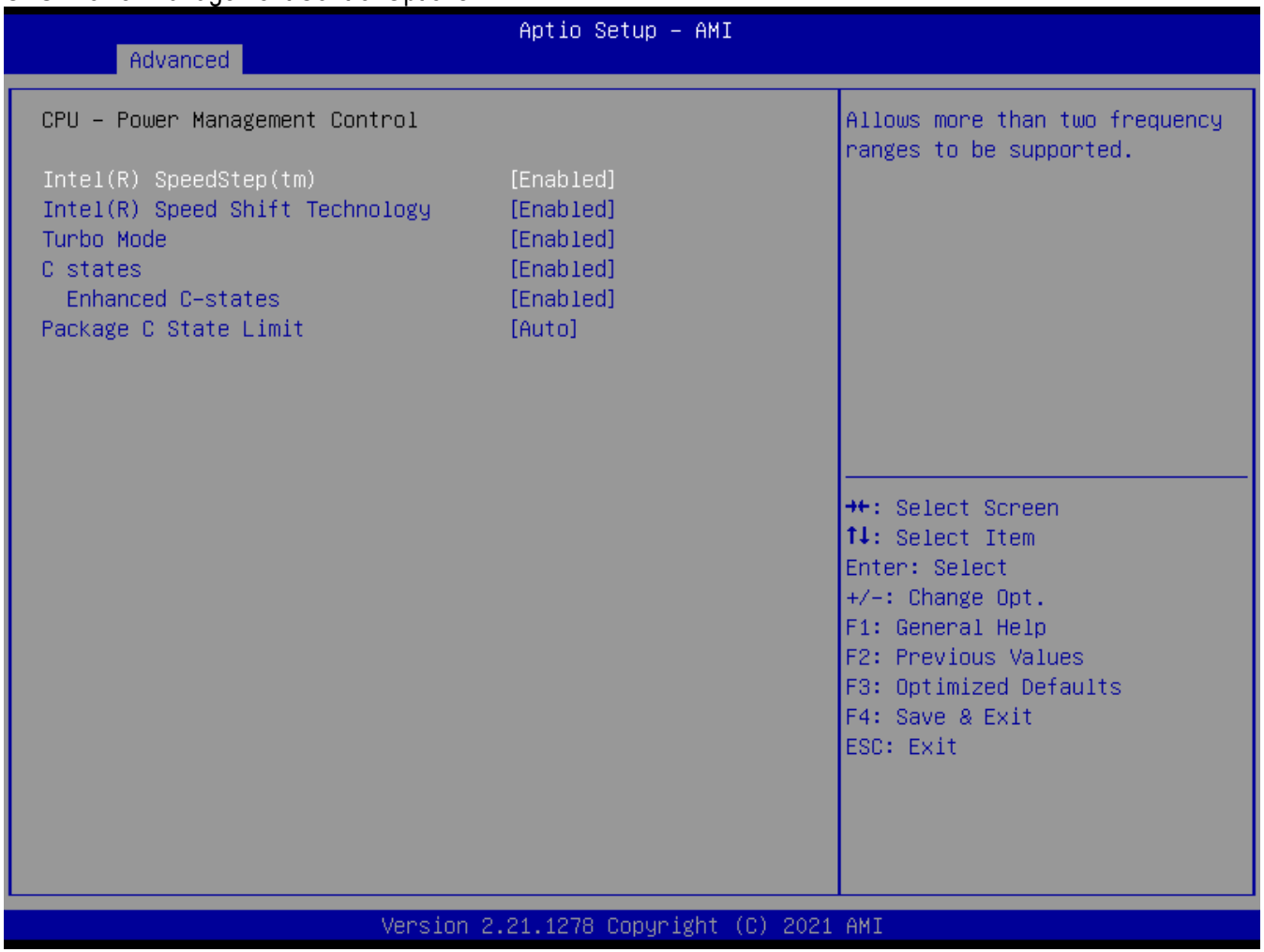
CPU Configuration Parameters



Feature	Description	Options
CPU Run Control	Enable/Disable CPU Run Control Support	★No Change, Enable, Disabled
Software Guard Extensions(SGX)	Enable/Disable Software Guard Extensions(SGX)	★Disabled, Enabled, Software Controlled
Intel (VMX)Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.	★Enabled ,Disabled
Hyper-Threading	Enable or Disable Hyper-Threading Technology.	★Enabled ,Disabled
Intel Trusted Execution Technology	Enables utilization of additional hardware capabilities provided by Intel(R) Trusted Execution Technology. Changes require a full power cycle to take effect.	★Disabled, Enabled
VT-d	VT-d capability	★Enabled ,Disabled
Power Limit 1 Override	Enable/Disable Power Limit 1 override. If this option is disables, BIOS will program the default values for power Limit 1 and Power Limit 1 Time Window.	★Disabled, Enabled
Power Limit 1 Override [Enable]		
Power Limit 1	Power Limit 1 in Milli Wattts. BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits(specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP Limit.	★0
Power Limit 2 Override	Enable/Disable Power Limit 1 override. If this option is disables, BIOS will program the default values for power Limit 2 .	★Enabled ,Disabled
Power Limit 2	Power Limit 2 value in Milli Wattts. BIOS will round to the nearest 1/8W when programming. If value is 0, BIOS will program this value as 1.25*TDP. For 12.50w, enter 12500. Processor applies control policies such that the package power does not exceed this limit.	★0

CPU- Power Management Control

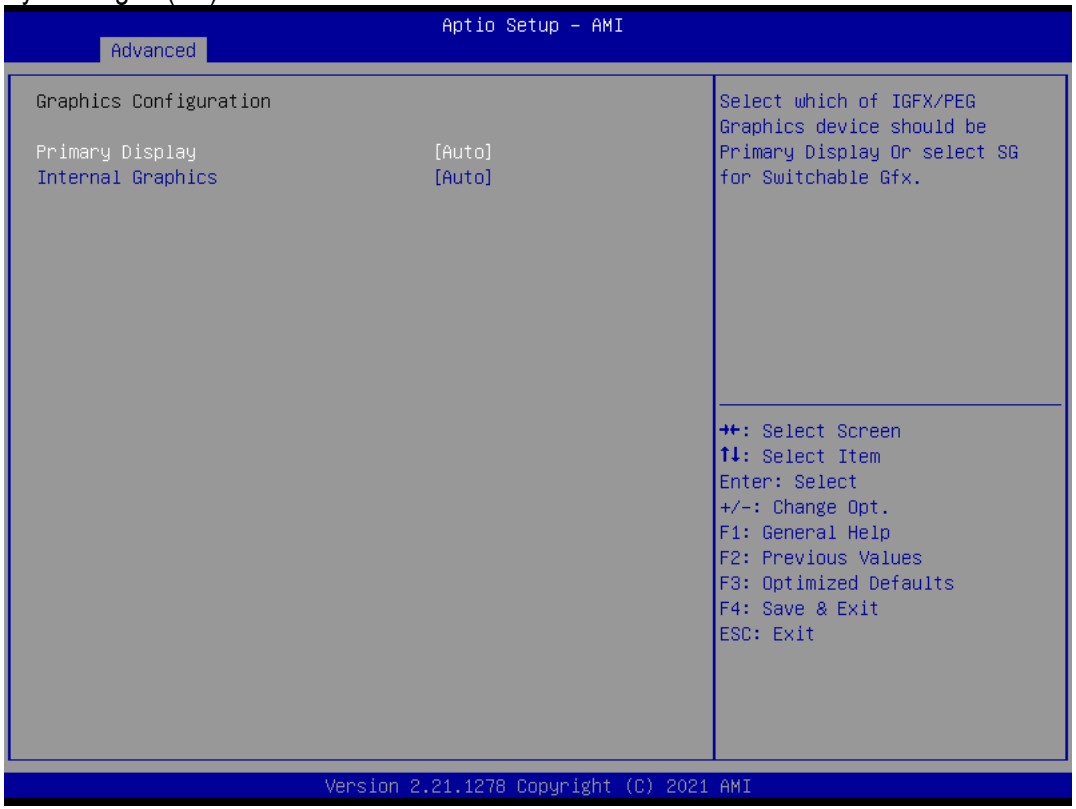
CPU- Power Management Control Options



Feature	Description	Options
Intel(R) SpeedStep(tm)	Allows more than two frequency ranges to be supported.	★Enabled ,Disabled
Intel(R) Speed Shift Technology	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.	★Enabled ,Disabled
Turbo Mode	Enable/Disable processor Turbo Mode(requires Intel Speed Step or Intel Speed Shift to be available and enabled)	★Enabled ,Disabled
C states	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.	★Enabled ,Disabled
Enhanced C-states	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.	★Enabled ,Disabled
Package C State Limit	Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit.	★Auto, C0/C1,C2,C3,C6, C7,C7S,C8,C9,C10,Cpu Default

Graphics Configuration

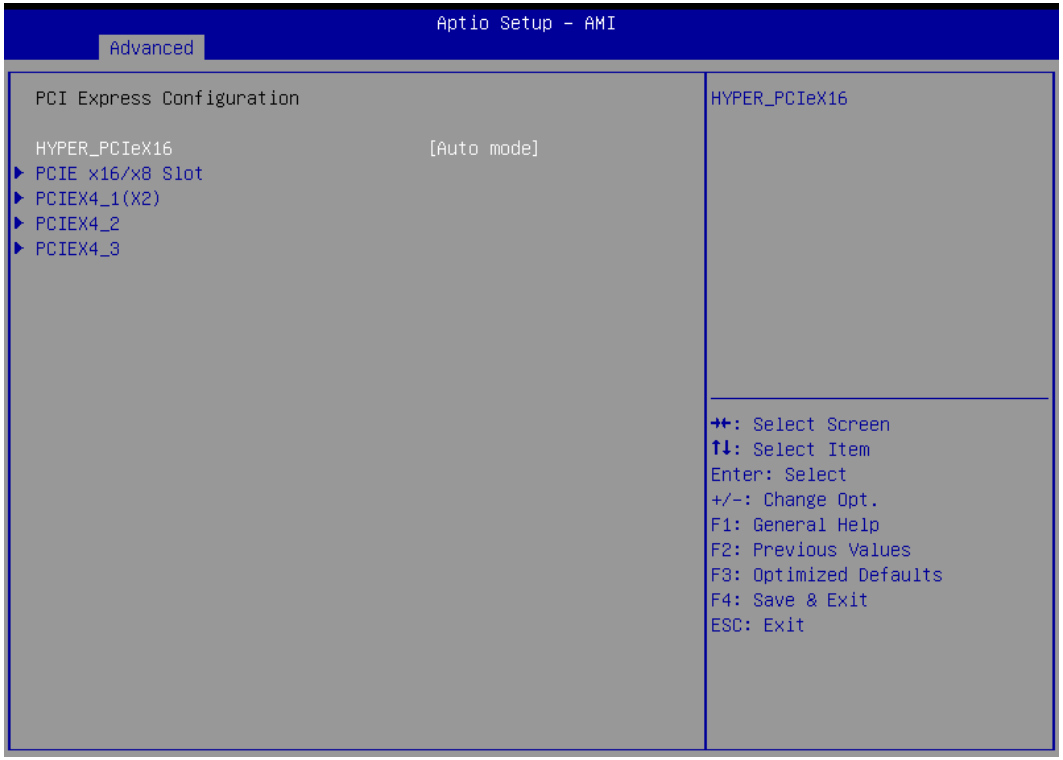
System Agent(SA)Parameters



Feature	Description	Options
Primary Display	Select which of IGFX/PEG Graphics device should be Primary Display Or select SG for Switchable Gfx.	★Auto, IGFX,PCI,PEG
Internal Graphics	Keep IGFX enabled based on the setup options.	★Auto ,Disabled ,Enabled

PCI Express Configuration

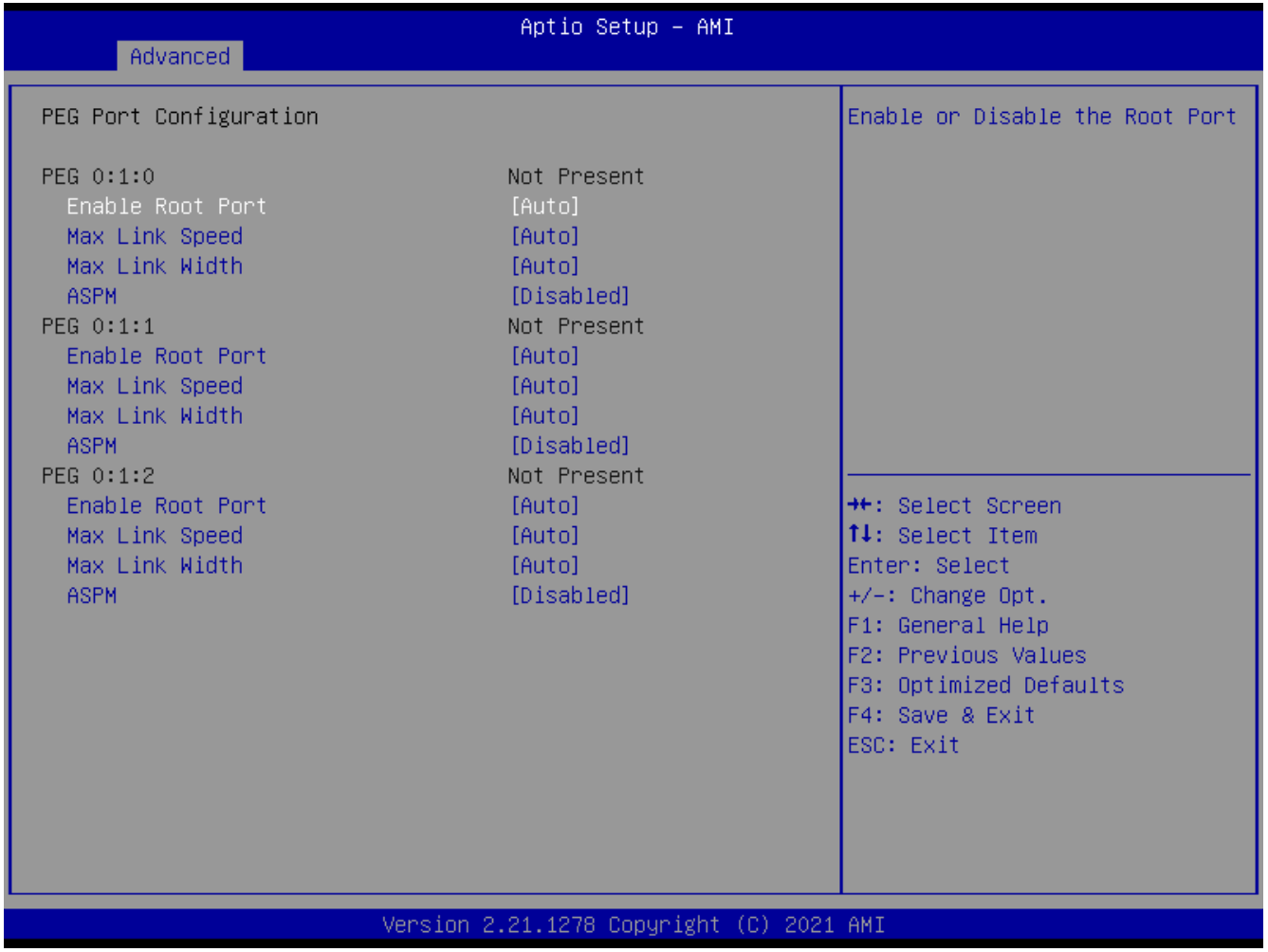
PCI Express Configuration



Feature	Description	Options
HYPER_PCIeX16	HYPER_PCIeX16	★Auto mode , PCIe x8/x4/x4 mode
PCIE x16/x8 Slot	PCIE x16/x8 Slot Options	
PCIEX4_1(X2)	PCI Express Root Port Settings	
PCIEX4_2/ PCIEX4_3	PCI Express Root Port Settings	

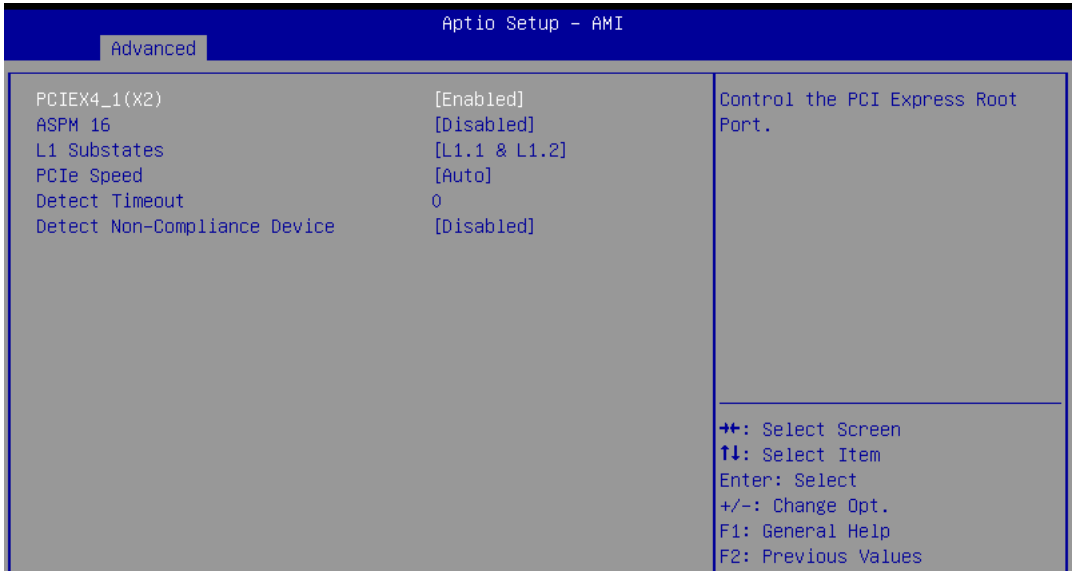
PCIE x16/x8 Slot

PEG Port Configuration



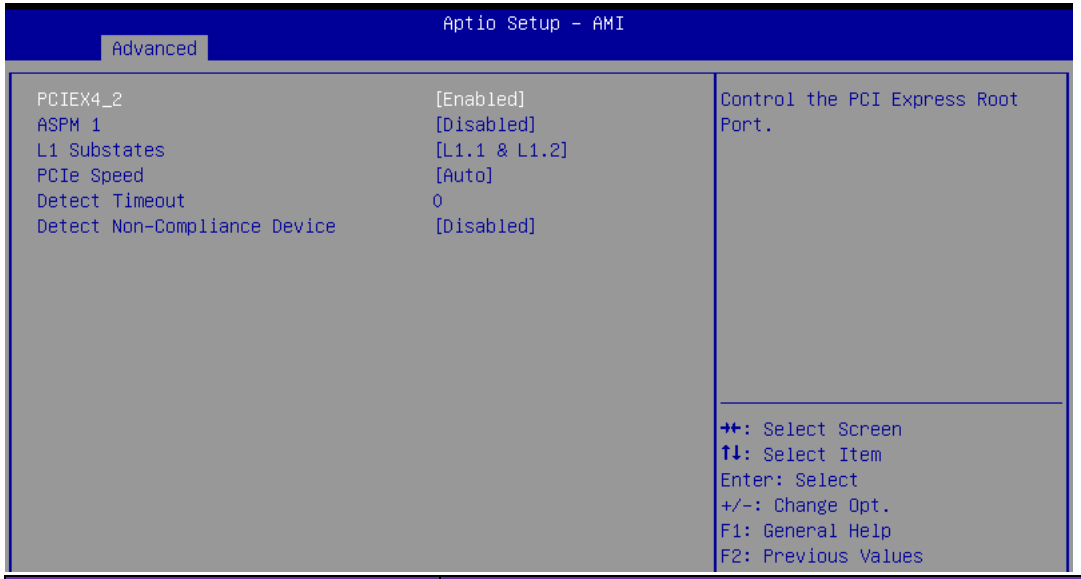
Feature	Description	Options
PEG 0:1:0		
Enable Root Port	Enable or Disable the Root Port	★Auto, Disabled, Enabled
Max Link Speed	Configure PEG 0:1:0 Max Speed	★Auto,Gen1,Gen2,Gen3
Max Link Width	Force PEG link to retrain to x1/2/4/8	★Auto, Force x1, Force x2,Force x4 Force x8
ASPM	Control ASPM support for the PEG 0. This has no effect if PEG is not currently active device.	★Disabled, Auto, ASPM L0s, ASPM L1, ASPM L0sL1
PEG 0:1:1		
Enable Root Port	Enable or Disable the Root Port	★Auto, Disabled, Enabled
Max Link Speed	Configure PEG 0:1:1 Max Speed	★Auto,Gen1,Gen2,Gen3
Max Link Width	Force PEG link to retrain to x1/2/4/8	★Auto, Force x1, Force x2,Force x4
ASPM	Control ASPM support for the PEG 1. This has no effect if PEG is not currently active device.	★Disabled, Auto, ASPM L0s, ASPM L1, ASPM L0sL1
PEG 0:1:2		
Enable Root Port	Enable or Disable the Root Port	★Auto, Disabled, Enabled
Max Link Speed	Configure PEG 0:1:2 Max Speed	★Auto,Gen1,Gen2,Gen3
Max Link Width	Force PEG link to retrain to x1/2/4/8	★Auto, Force x1, Force x2
ASPM	Control ASPM support for the PEG 2. This has no effect if PEG is not currently active device.	★Disabled, Auto, ASPM L0s, ASPM L1, ASPM L0sL1

PCIEX4_1(X2)



Feature	Description	Options
PCIEX4_1(X2)	Control the PCI Express Root Port.	★Enable ,Disable
ASPM 16	Set the ASPM Level: Force L0s- Force all links to L0s State AUTO- BIOS auto configure DISABLE- Disables ASPM	★Disable, L0s, L1, L0sL1,Auto
L1 Substates	PCI Express L1 Substates settings	★L1.1&L1.2, Disable, L1.1
PCIe Speed	Configure PCIe Speed	★Auto,Gen1,Gen2,Gen3
Detect Timeout	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.	★0
Detect Non-Compliance Device	Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.	★Disabled, Enabled

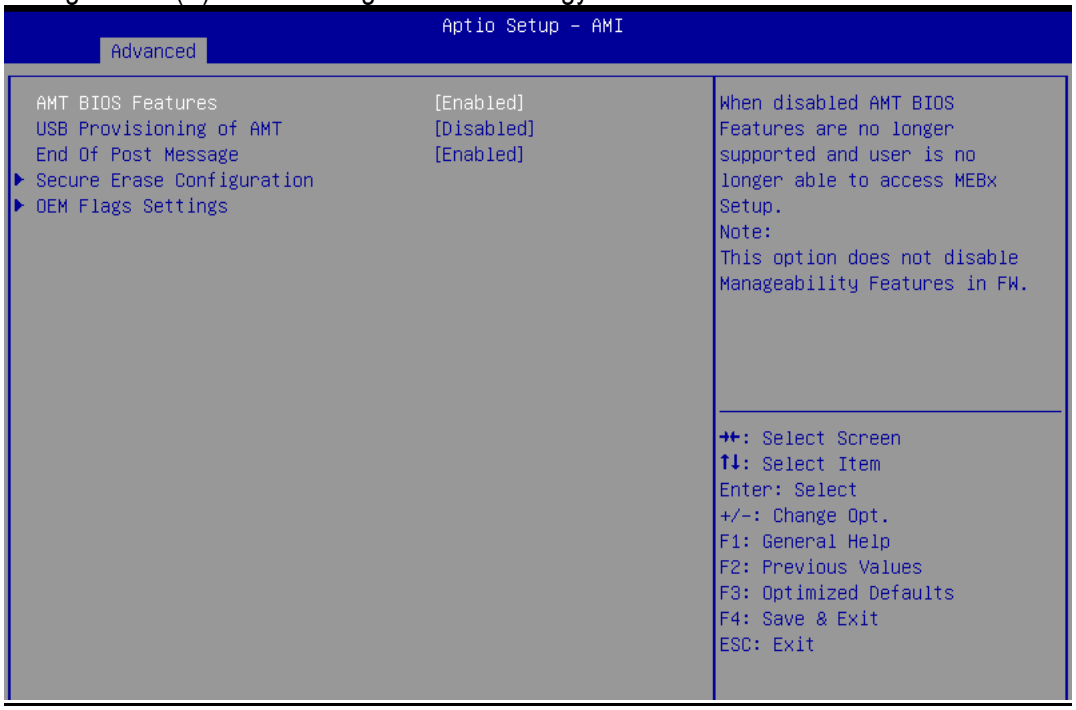
PCIEX4_2/ PCIEX4_3



Feature	Description	Options
PCIEX4_1(X2)	Control the PCI Express Root Port.	★Enable ,Disable
ASPM 16	Set the ASPM Level: Force L0s- Force all links to L0s State AUTO- BIOS auto configure DISABLE- Disables ASPM	★Disable, L0s, L1, L0sL1,Auto
L1 Substates	PCI Express L1 Substates settings	★L1.1&L1.2, Disable, L1.1
PCIe Speed	Configure PCIe Speed	★Auto,Gen1,Gen2,Gen3
Detect Timeout	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.	★0
Detect Non-Compliance Device	Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.	★Disabled, Enabled

AMT Configuration

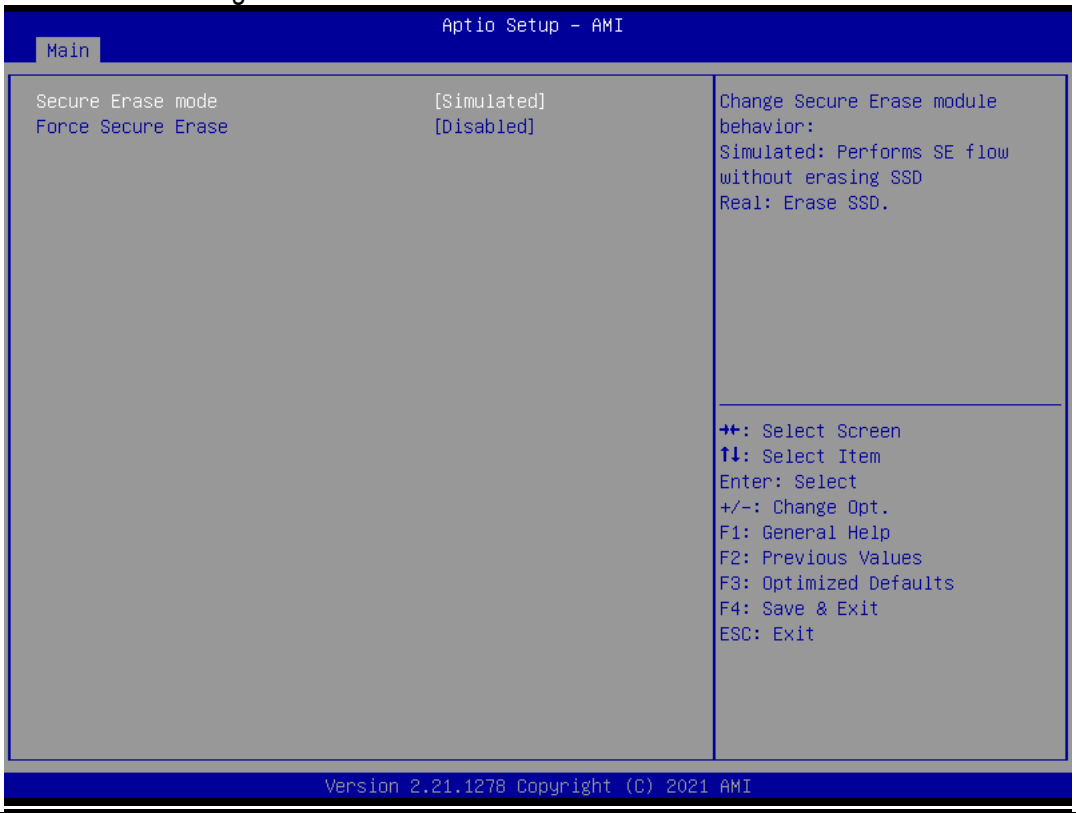
Configure Intel(R) Active Management Technology Parameters



Feature	Description	Options
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.	★Enabled ,Disabled
USB Provisioning of AMT	Enable/Disable of AMT USB Provisioning.	★Disabled, Enable
End Of Post Message	Enable/Disable End of Post message sent to ME	★Enabled ,Disabled

Secure Erase Configuration

Secure Erase Configuration menu



Feature	Description	Options
Secure Erase mode	Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD.	★Simulation, Real
Force Secure Erase	Force Secure Erase on next boot	★Disabled, Enable

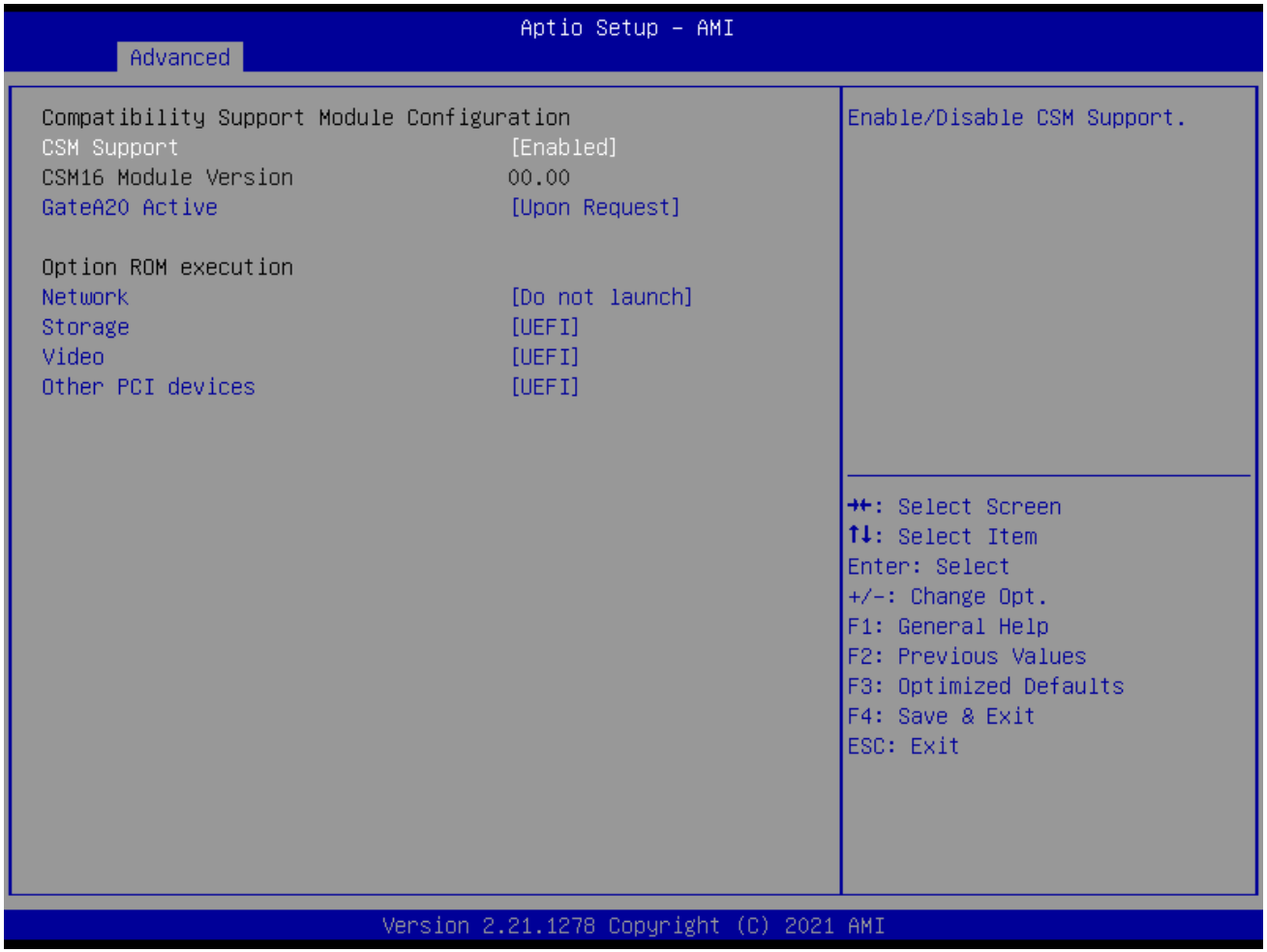
OEM Flags Settings

Configure OEM Flags

Feature	Description	Options
MEBx Selection Screen	OEMFLag Bit 2: Enable MEBx selection screen with 2 options: Press 1 to enter ME Configuration Screens Press 2 to initiate a remote connection Note: Network Access must be activated from MEBx Setup for this screen to be displayed.	★Disabled, Enable
Unconfigure ME	OEMFlag Bit 15: Unconfigure ME with resetting MEBx password to default.	★Disabled, Enable

CSM Configuration

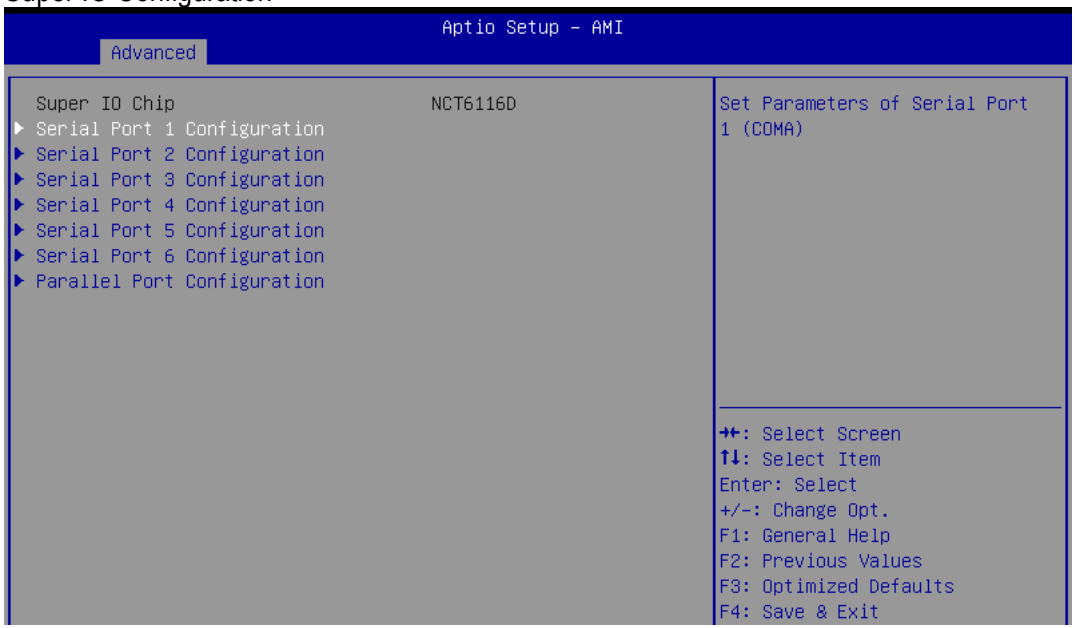
CSM Configuration: Enable/Disable, Option ROM execution settings, etc.



Feature	Description	Options
CSM Support	Enable/Disable CSM Support	★Disable, Enabled
CSM Support [Enable]		
GeteA20 Active	UPON REQUEST – GA20 can be disabled using BIOS services. ALWAYS- do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.	★Upon Request, Always
Network	Controls the execution of UEFI and Legacy Network OpROM.	★Do not launch, UEFI, Legacy
Storage	Controls the execution of UEFI and Legacy Storage OpROM	★UEFI, Do not launch, Legacy
Video	Controls the execution of UEFI and Legacy Video OpROM	★UEFI, Do not launch, Legacy
Other PCI device	Determines OpROM execution policy for devices other than Network, Storage, or Video	★UEFI, Do not launch, Legacy

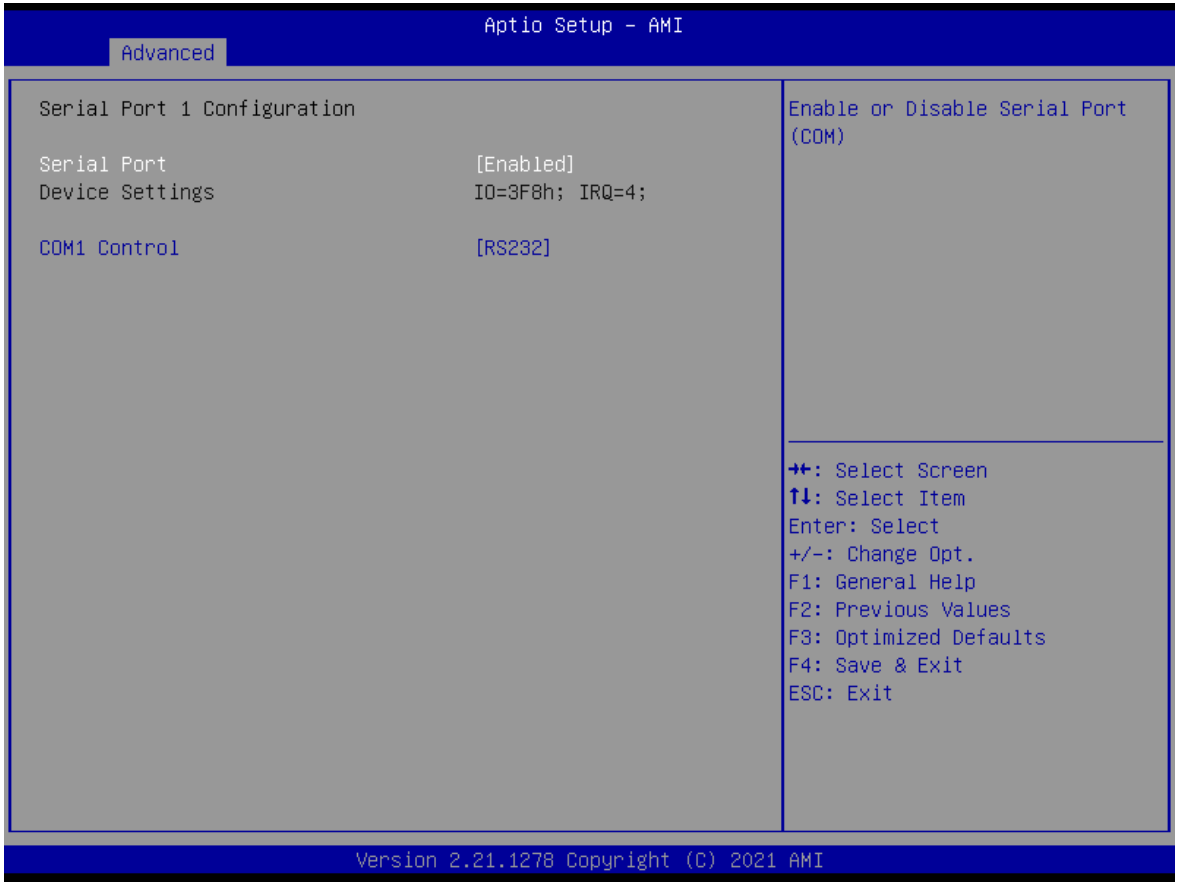
Super IO Configuration

Super IO Configuration



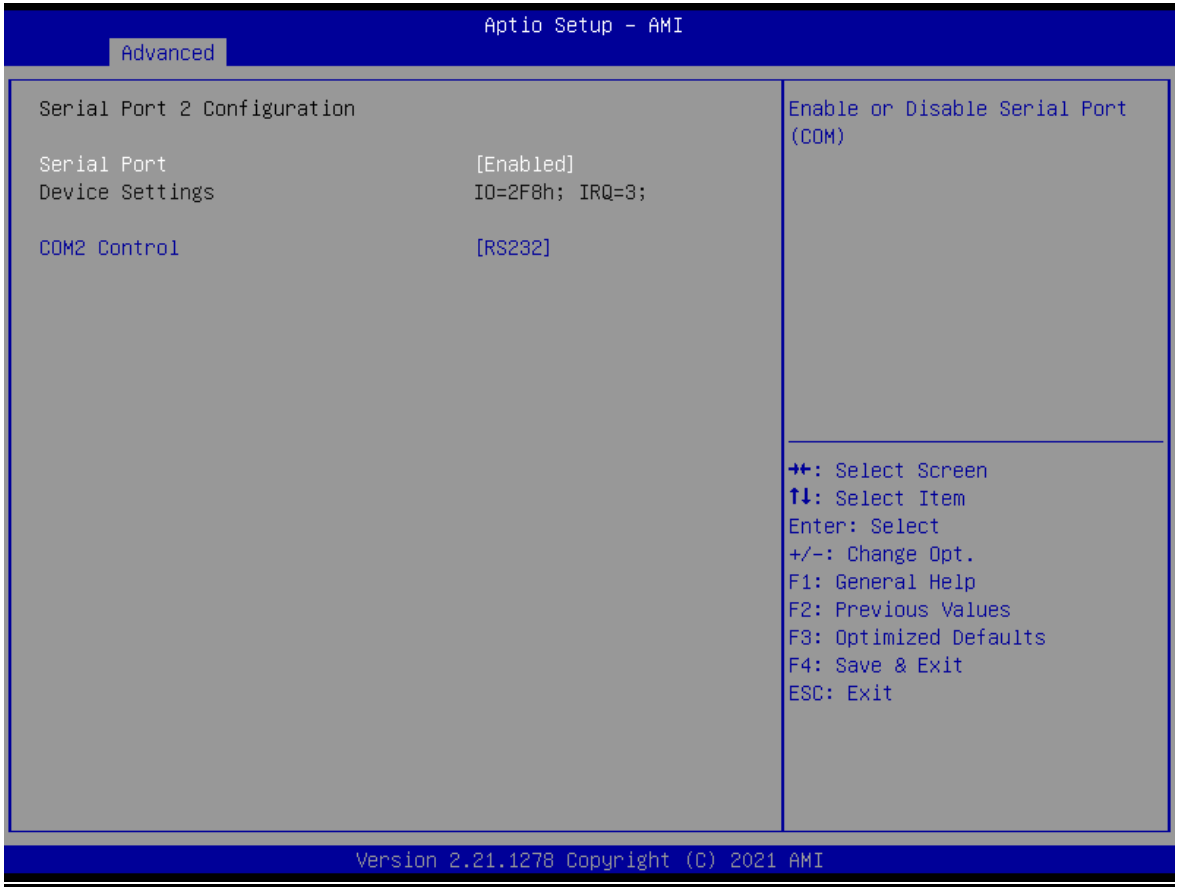
Feature	Description	Options
Serial Port 1 Configuration	Set Parameters of Serial Port1(COMA)	
Serial Port 2 Configuration	Set Parameters of Serial Port2(COMB)	
Serial Port 3 Configuration	Set Parameters of Serial Port3(COMC)	
Serial Port 4 Configuration	Set Parameters of Serial Port4(COMD)	
Serial Port 5 Configuration	Set Parameters of Serial Port5(COME)	
Serial Port 6 Configuration	Set Parameters of Serial Port6(COMF)	
Parallel Port Configuration	Set Parameters of Parallel Port(LPT/LPTE)	

Serial Port 1 Configuration



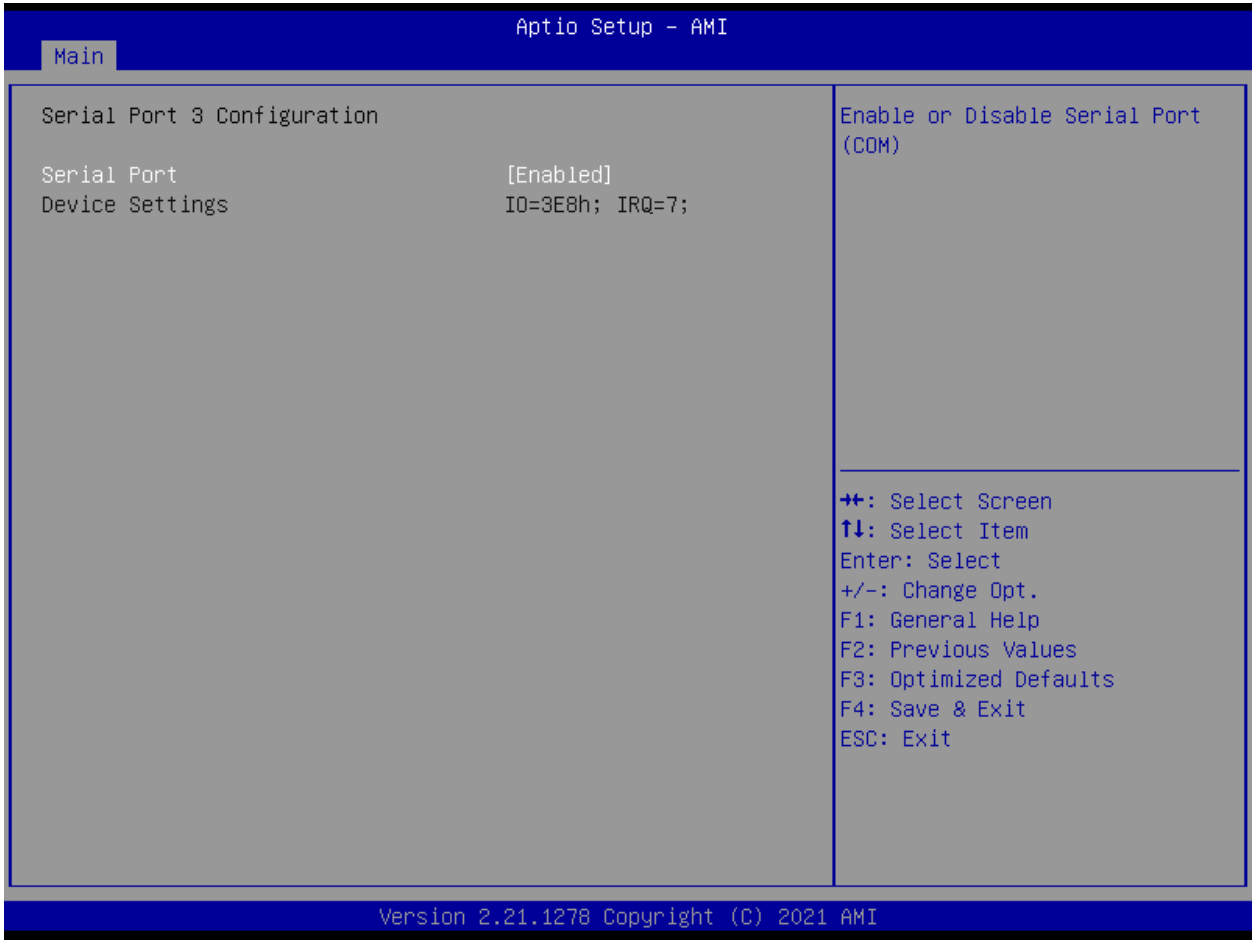
Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled
COM1 Control	Select COM1 mode. RS232, RS422 or RS485	★RS232,RS422,RS485

Serial Port 2 Configuration



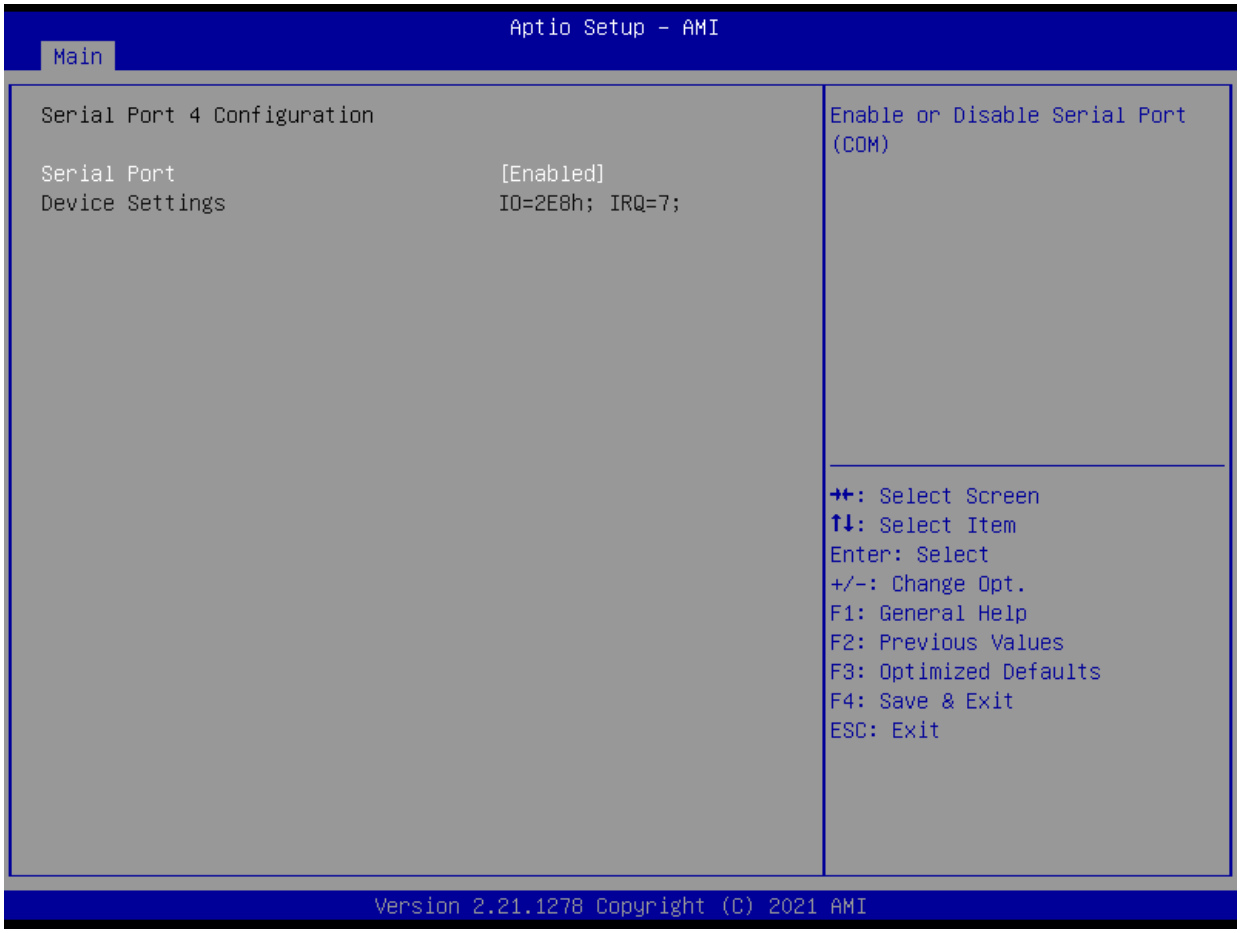
Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled
COM2 Control	Select COM2 mode. RS232, RS422 or RS485	★RS232,RS422,RS485

Serial Port 3 Configuration



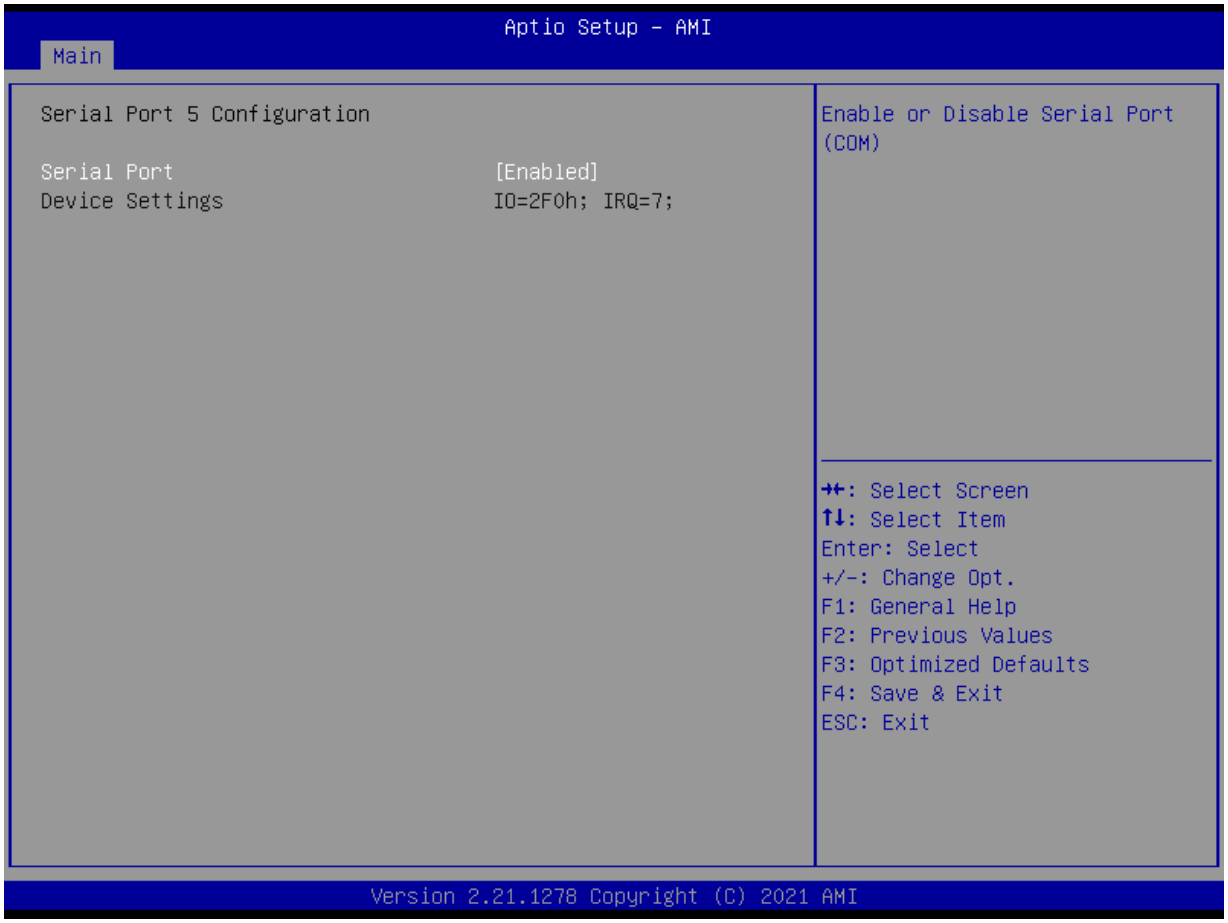
Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled

Serial Port 4 Configuration



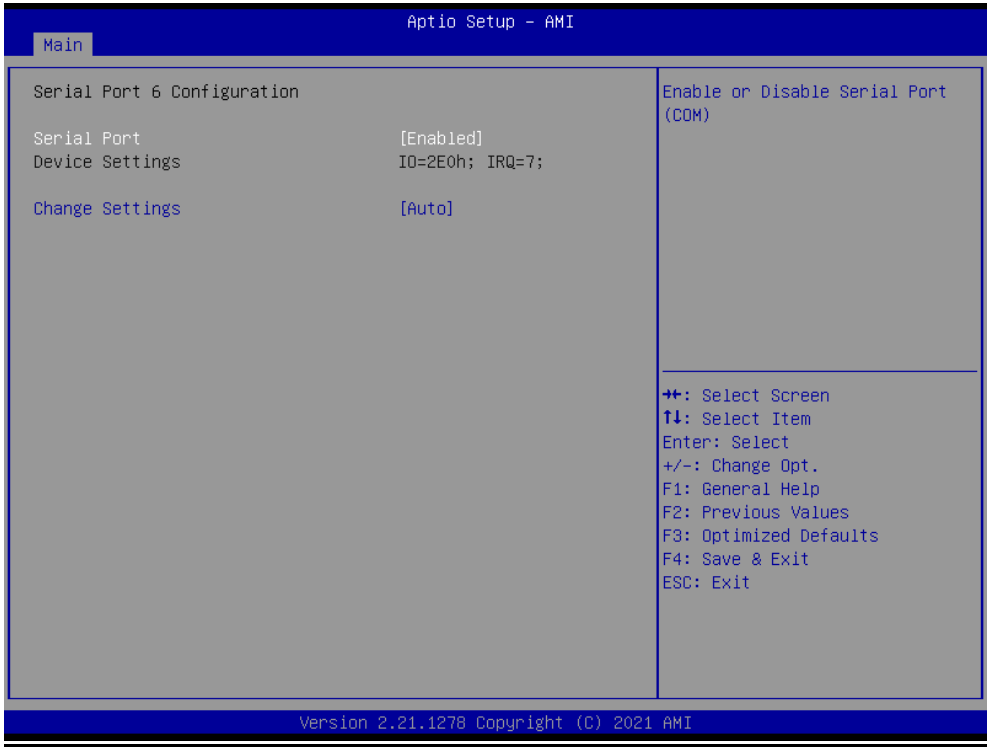
Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled

Serial Port 5 Configuration



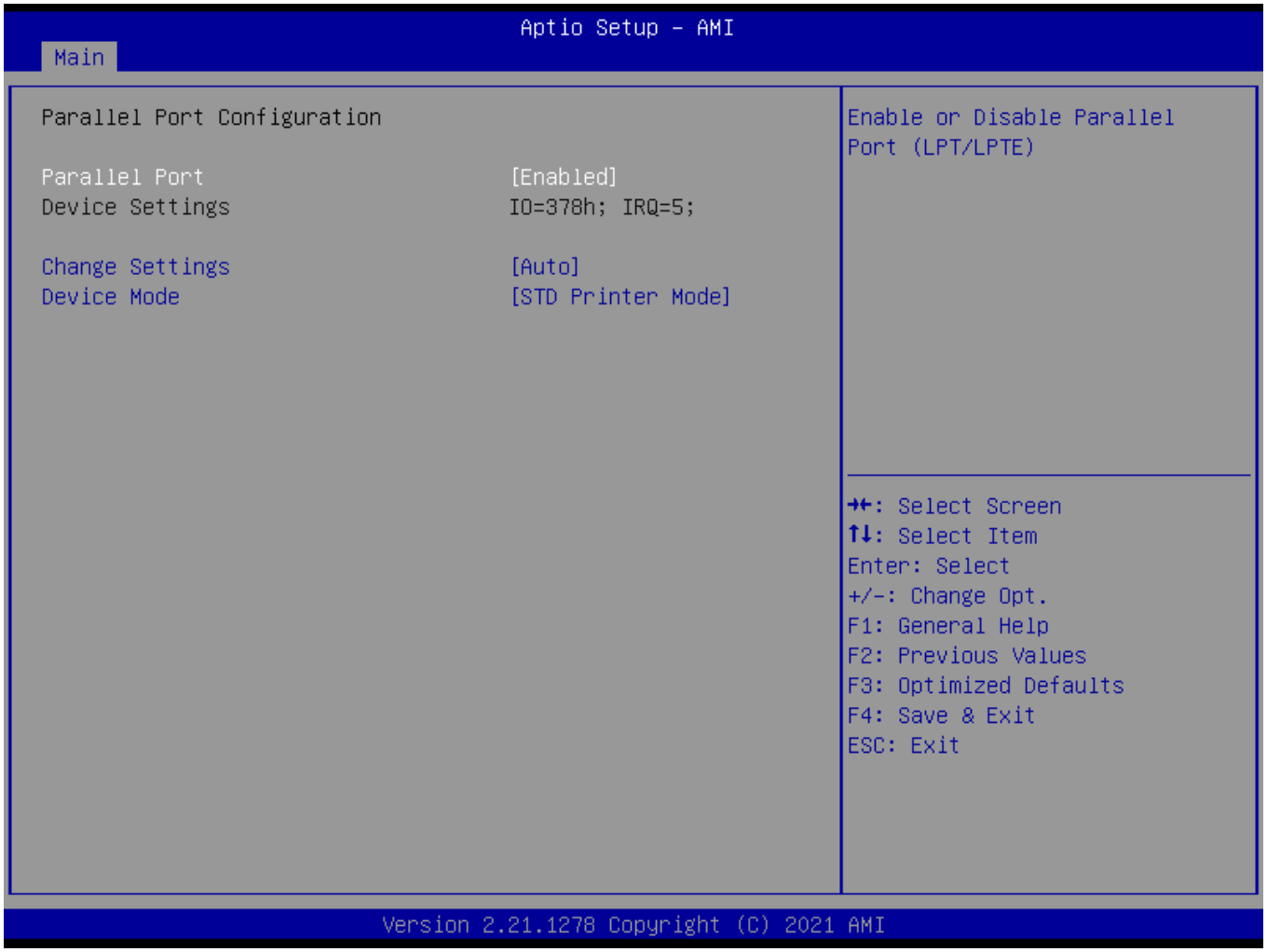
Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled

Serial Port 6 Configuration



Feature	Description	Options
Serial Port	Enable or Disable Serial Port (COM)	★Enabled ,Disabled
Change Settings	Select an optimal settings for Super IO Device.	★Auto, IO=2F0h;IRQ=7 IO=3E8h;IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h;IRQ=3,4,5,6,7,9,10,11,12; IO=2F0h;IRQ=3,4,5,6,7,9,10,11,12; IO=2E0h;IRQ=3,4,5,6,7,9,10,11,12;

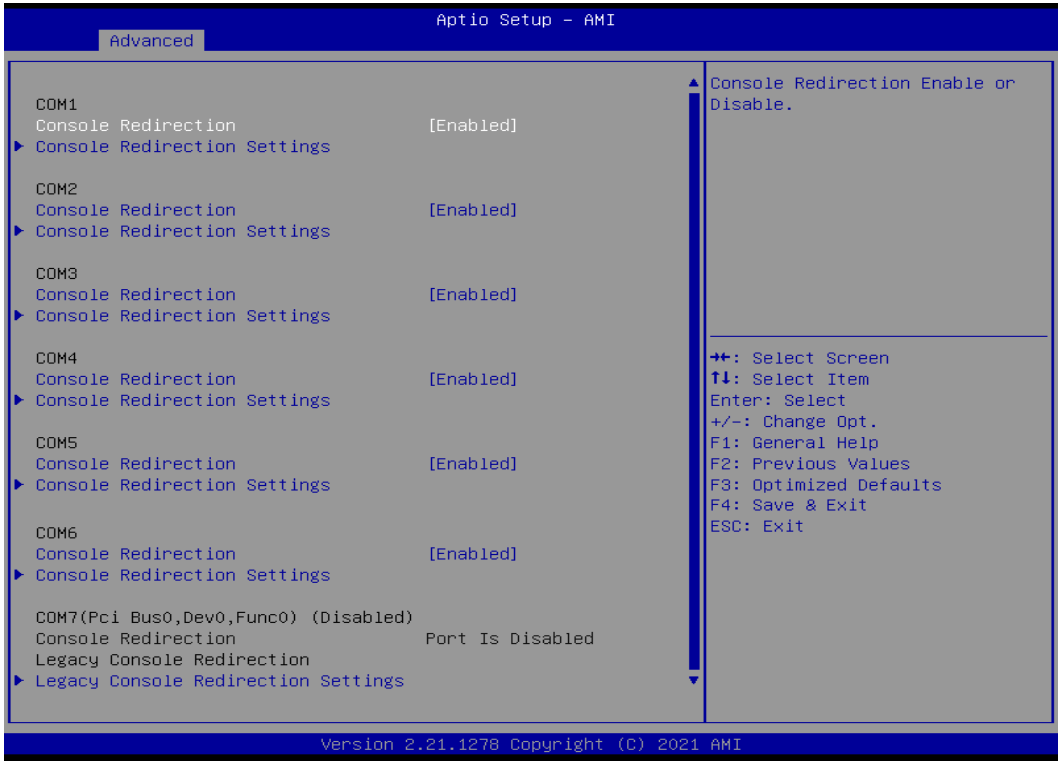
Parallel Port Configuration



Feature	Description	Options
Parallel Port	Enable or Disable Parallel Port (LPT/LPTE)	★Enabled ,Disabled
Change Settings	Select an optimal settings for Super IO Device.	★Auto, IO=378h;IRQ=5 IO=378h;IRQ=5,6,7,9,10,11,12; IO=278h;IRQ=5,6,7,9,10,11,12; IO=3BCh;IRQ=5,6,7,9,10,11,12;
Device Mode	Change the Printer Port mode.	★STD Printer Mode, SPP Mode, EPP-1.9 and SPP Mode, EPP-1.7 and SPP Mode, ECP Mode, ECP and EPP 1.9 Mode, ECP and EPP 1.7 Mode

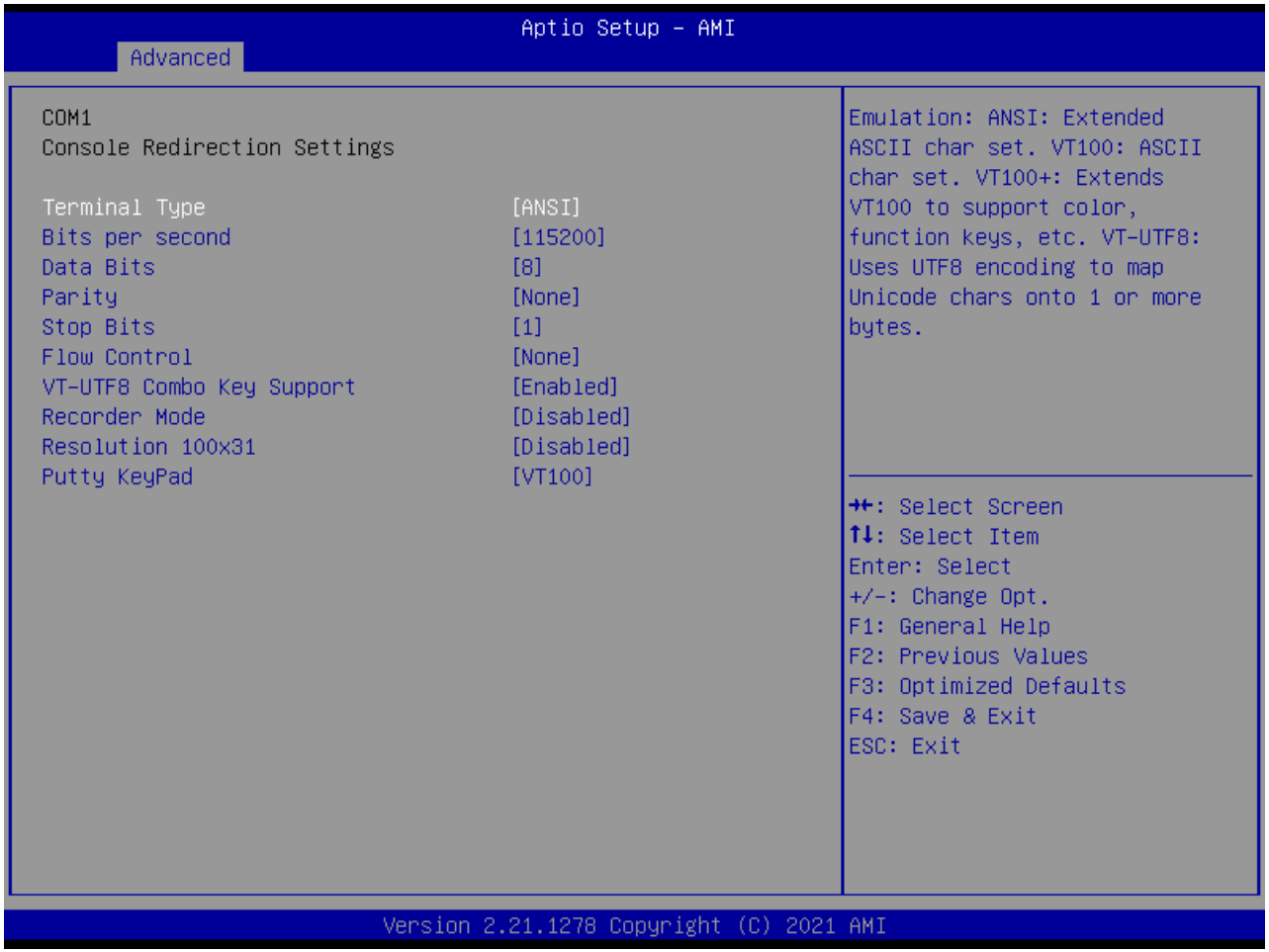
Serial Console Redirection

Serial Console Redirection



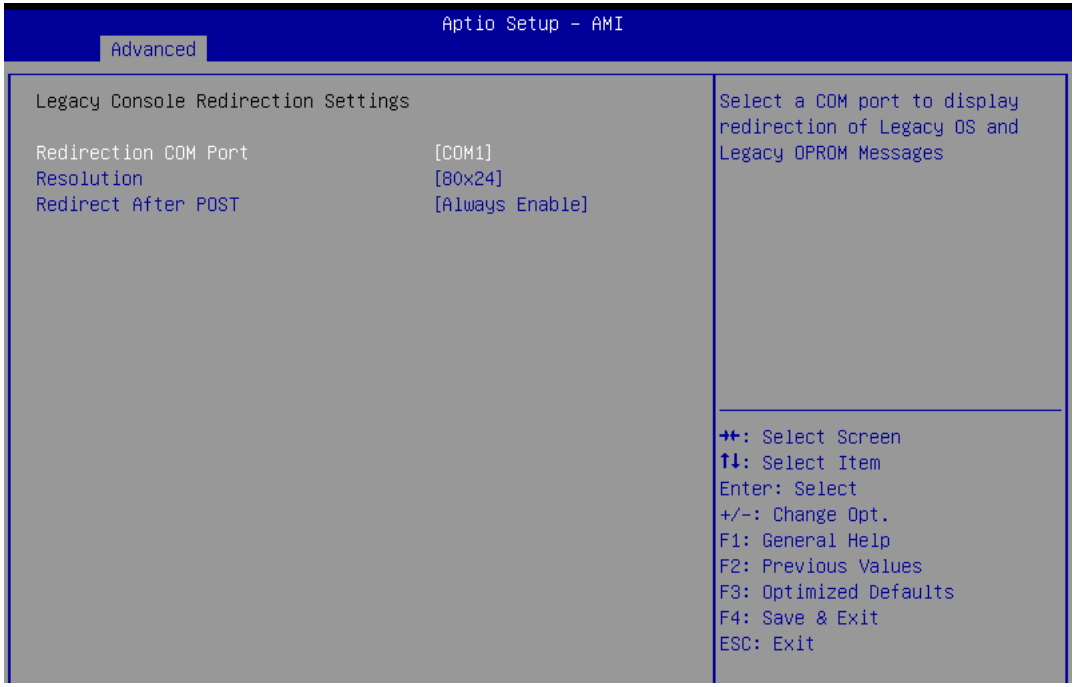
Feature	Description	Options
Console Redirection	Console Redirection Enable or Disable	★Disabled, Enabled
Console Redirection [Enabled]		
Console Redirection Settings	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	
Legacy Console Redirection Settings	Legacy Console Redirection Settings	

Console Redirection Settings



Feature	Description	Options
Terminal Type	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.	★ANSI, VT100, VT100+, VT-UTF8
Bits per second	Select Serial port transmission speed. The speed must be matched on other side. Long or noisy lines may require lower speeds.	★115200, 9600, 19200, 38400, 57600
Data bits	Data bits	★8, 7
Parity	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.	★None, Even, Odd, Mark, Space
Stop Bits	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.	★1,2
Flow Control	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.	★None, Hardware RTS/CTS
VT-UTFB Combo Key Support	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals	★Enabled, Disabled
Recorder Mode	With this mode enabled only text will be sent. This is to capture Terminal data.	★Disabled, Enabled
Resolution 100x31	Enables or disables extended terminal resolution	★Disabled, Enabled
Putty KeyPad	Select FunctionKey and KeyPad on Putty	★VT100, LINUX,XTERMR6, SCO, ESCN, VT400

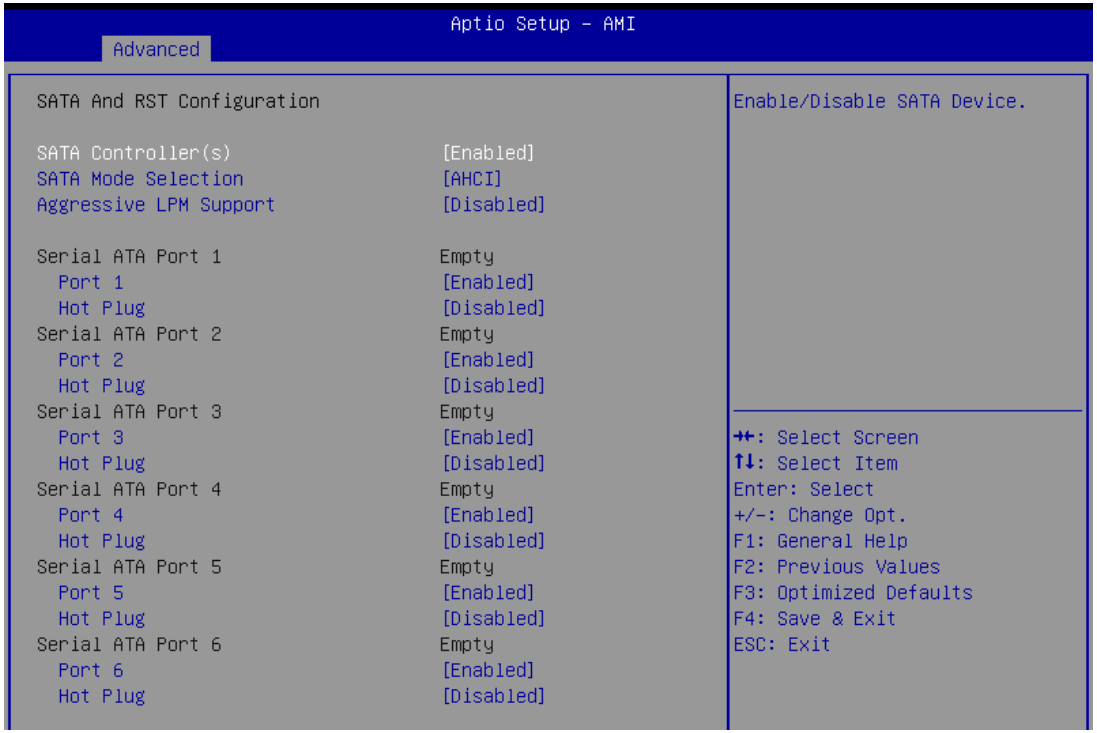
Legacy Console Redirection Settings



Feature	Description	Options
Redirection COM Port	Select s COM port to display redirection of Legacy OS and Legacy OPROM Messages.	★COM1,COM2,COM3,COM4,COM5,COM6 COM7(Pci Bus0,Dev0,Func0)(Disabled)
Resolution	On Legacy OS, the number of Rows and Columns supported redirection.	★80X24,80X25
Redirect After POST	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.	★Always Enable, BootLoader

SATA And RST Configuration

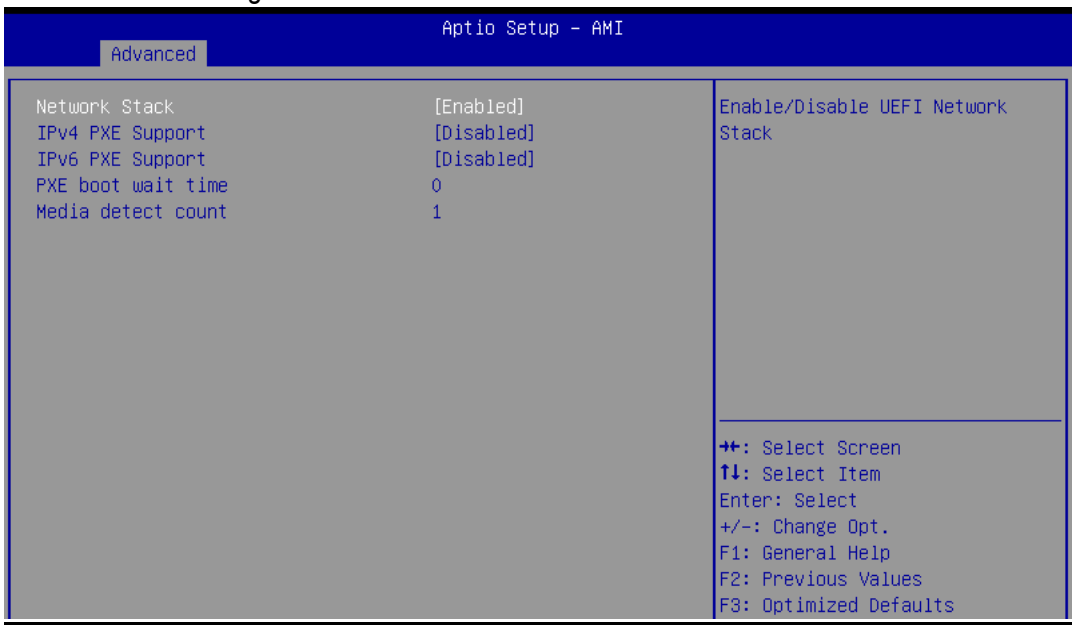
SATA Device Options Settings



Feature	Description	Options
SATA Controller(s)	Enable/disable the SATA controllers.	★Enabled , Disabled
SATA Mode Selection	Determines how SATA controller(s) operate.	★AHCI, Intel RST With Intel Optane System Acceleration
Aggressive LPM Support	Enable PCH to aggressively enter link power state.	★Disabled, Enabled
Port1~Port6	Enable or Disable SATA Port	★Enabled, Disabled
Hot Plug	Designates this port as Hot Pluggable.	★Disabled, Enabled

Network Stack Configuration

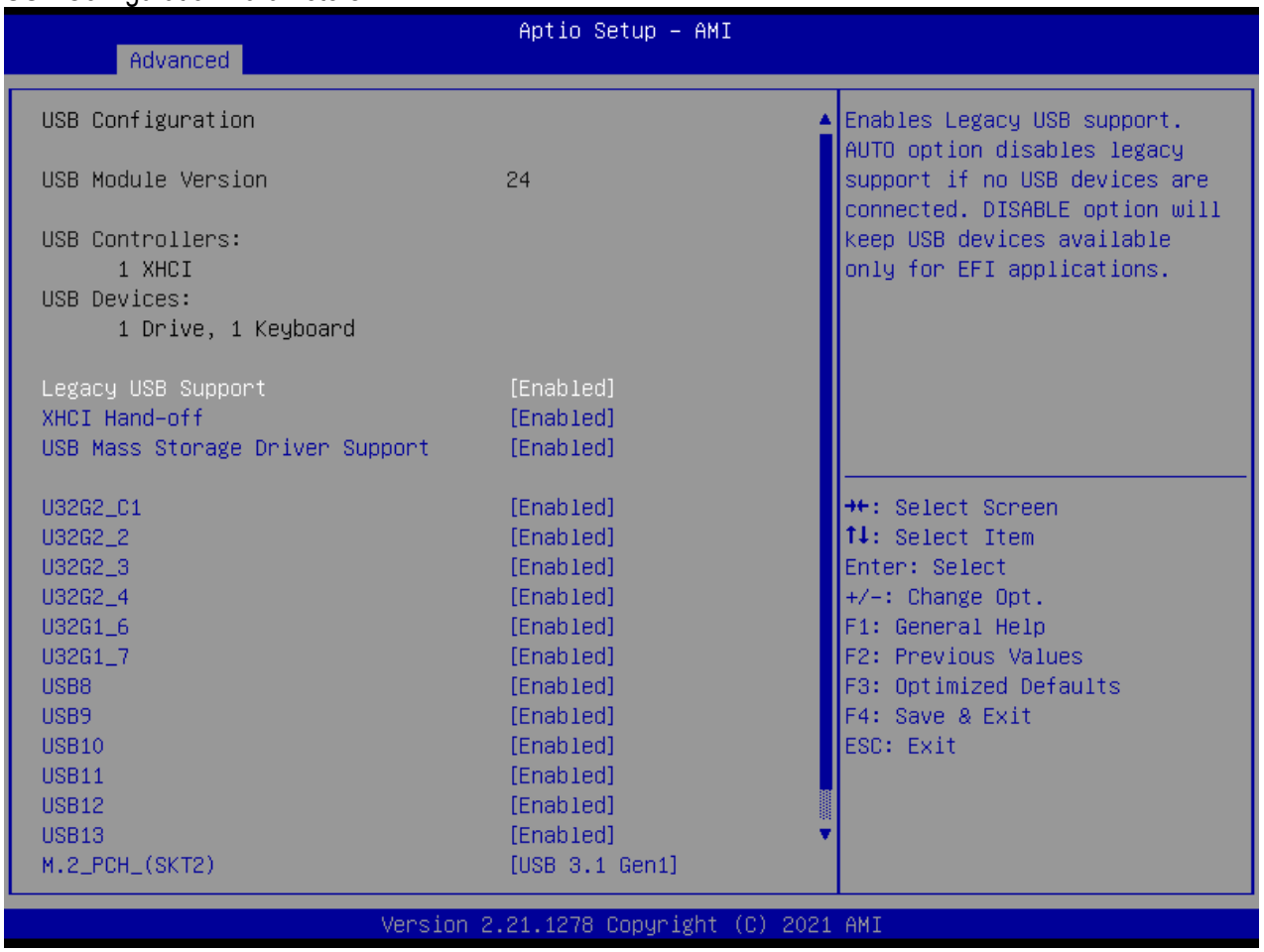
Network Stack Settings



Feature	Description	Options
Network Stack	Enable/ Disable UEFI Network Stack	★Disabled, Enabled
Network Stack [Enabled]		
Ipv4 PXE Support	Enable/Disable IPv4 PXE boot support. If disable, IPv4 PXE boot support will not be available.	★Disabled, Enabled
Ipv6 PXE Support	Enable/Disable IPv6 PXE boot support. If disable, IPv6 PXE boot support will not be available.	★Disabled, Enabled
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.	★0
Media detect count	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.	★1

USB Configuration

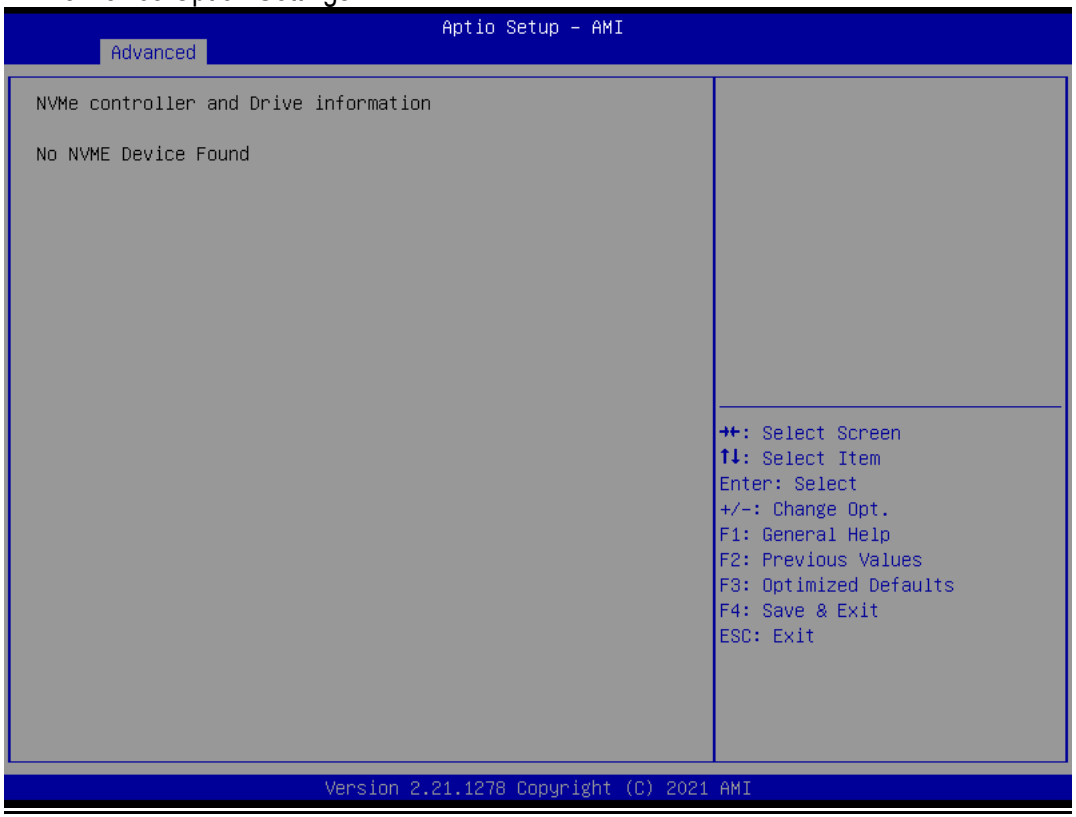
USB Configuration Parameters



Feature	Description	Options
Legacy USB Support	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.	★Enabled, Disabled, Auto
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver	★Enabled, Disabled
USB Mass Storage Driver Support	Enable/Disable USB Mass Storage Driver Support	★Enabled, Disabled
U32G2_C1	Enable/Disable this USB Physical Connector (Physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	★Enabled, Disabled
U32G2_2~ U32G2_4	Enable/Disable this USB Physical Connector (Physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	★Enabled, Disabled
U32G1_6~ U32G1_7	Enable/Disable this USB Physical Connector (Physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	★Enabled, Disabled
USB8~13	Enable/Disable this USB Physical Connector (Physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	★Enabled, Disabled
M.2_PCH_(SKT2)	To configure USB3 Port5 Speed Select. (USB3.1)/(USB3.0)	★USB 3.1 Gen1, USB 3.1 Gen2

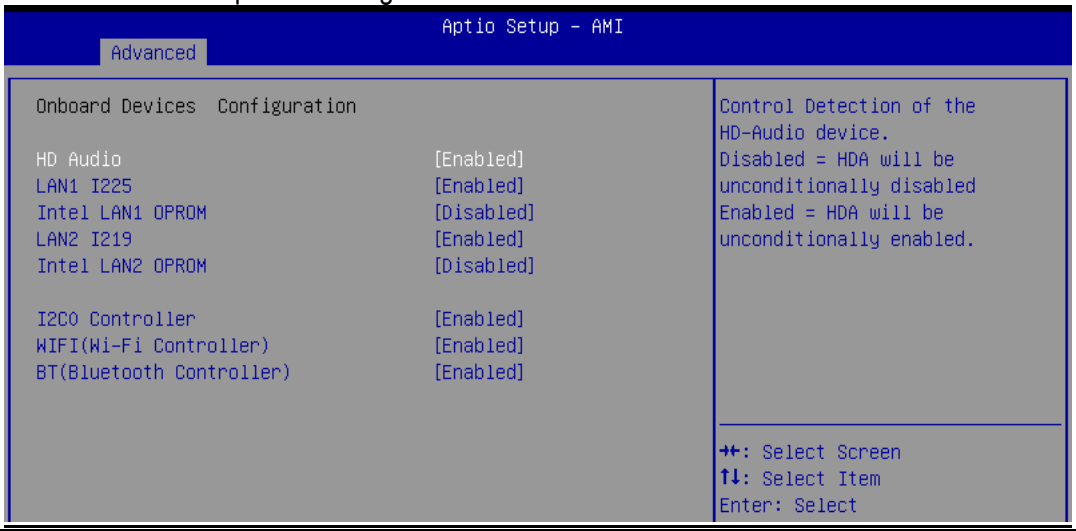
NVMe Configuration

NVMe Device Option Settings



Onboard Devices Configuration

Onboard Devices Options Settings



Feature	Description	Options
HD Audio	Control Detection of the HD-Audio device. Disabled= HDA will be unconditionally disabled. Enabled= HDA will be unconditionally enabled.	★Enabled, Disabled
LAN1 I225	Enable/Disable LAN1 I225.	★Enabled, Disabled
Intel LAN1 OPROM	Launch Intel PXE OPROM.	★Disabled, Enabled
LAN2 I219	Enable/Disable LAN2 I219	★Enabled, Disabled
Intel LAN2 OPROM	Launch Intel PXE OPROM.	★Enabled, Disabled
I2C0 Controller	Enable/Disable Serial Io Controller. If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device.	★Enabled, Disabled
WIFI (Wi-Fi Controller)	Enable/Disable WIFI (Wi-Fi Controller).	★Enabled, Disabled
BT (Bluetooth Controller)	Enable/Disable BT (Bluetooth Controller).	★Enabled, Disabled

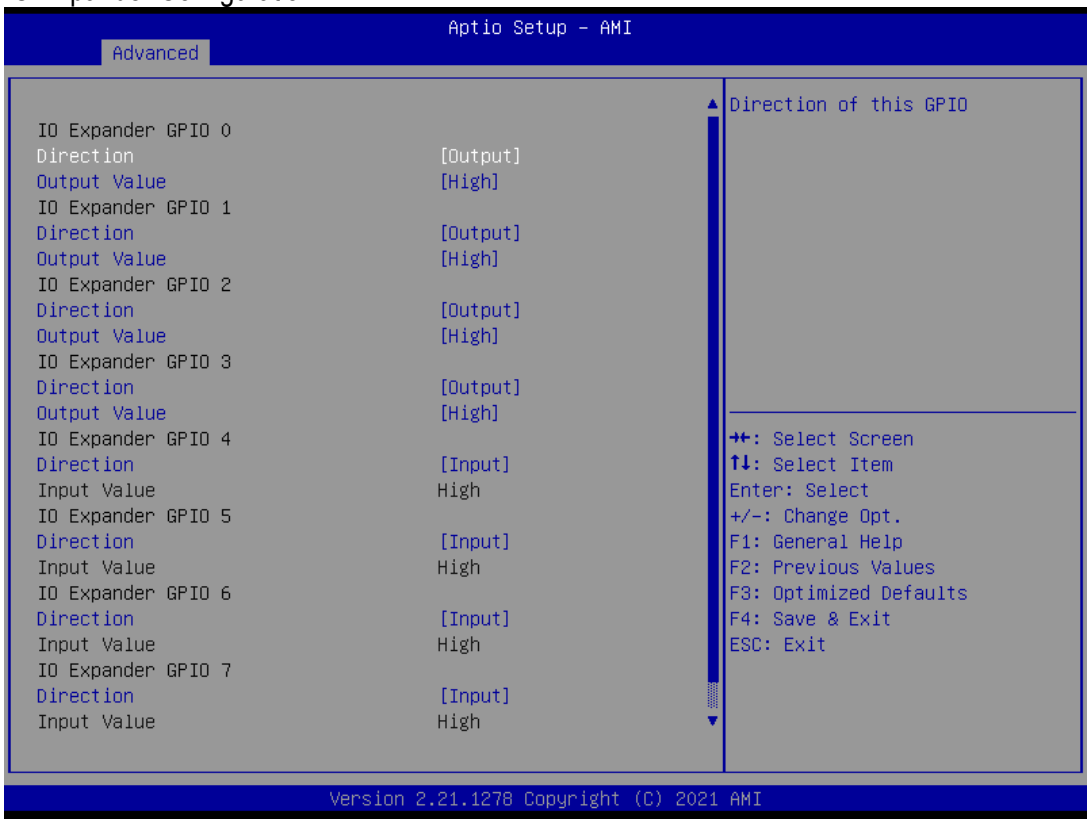
APM Configuration

Advance Power Management

Feature	Description	Options
ErP Ready	Allow BIOS to switch off some power at S4/S5 to get the system ready for ErP requirement. When set to Enabled, all other PME options will be switched off.	★Disabled, Enabled
Restore AC Power Loss	Select AC power state when power is re-applied after a power failure.	★S5 State, S0 State
Power On By PCIE	Enable or disable the Wake-on-LAN function of the onboard LAN controller or other installed PCIE LAN devices.	★Disabled, Enabled
Power On By PCI	Power On By PCI.	★Disabled, Enabled
Power On By PS2	Enable/disable resume from S5 via PS2.	★Disabled, Enabled
Power On By Ring	Power On By Ring.	★Disabled, Enabled
Power On By RTC	Select whether to enable Wake Up on Alarm, to turn on your system on a special day of the week or daily. NOTE: Values in these fields may be overwritten by the operating system.	★Disabled, Single event, Daily event, Weekly event, Monthly event
Alarm day of Week	Select the day of the week when the system is to wake up.	★Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Day of the Month	RTC Alarm Date (Days)	★15
Wake up hour	Select 0-23 For example enter 3 for 3am and 15 for 3 pm.	★0
Wake up minute	Select 0-59 for Minute.	★0
Wake up second	Select 0-59 for Second.	★0

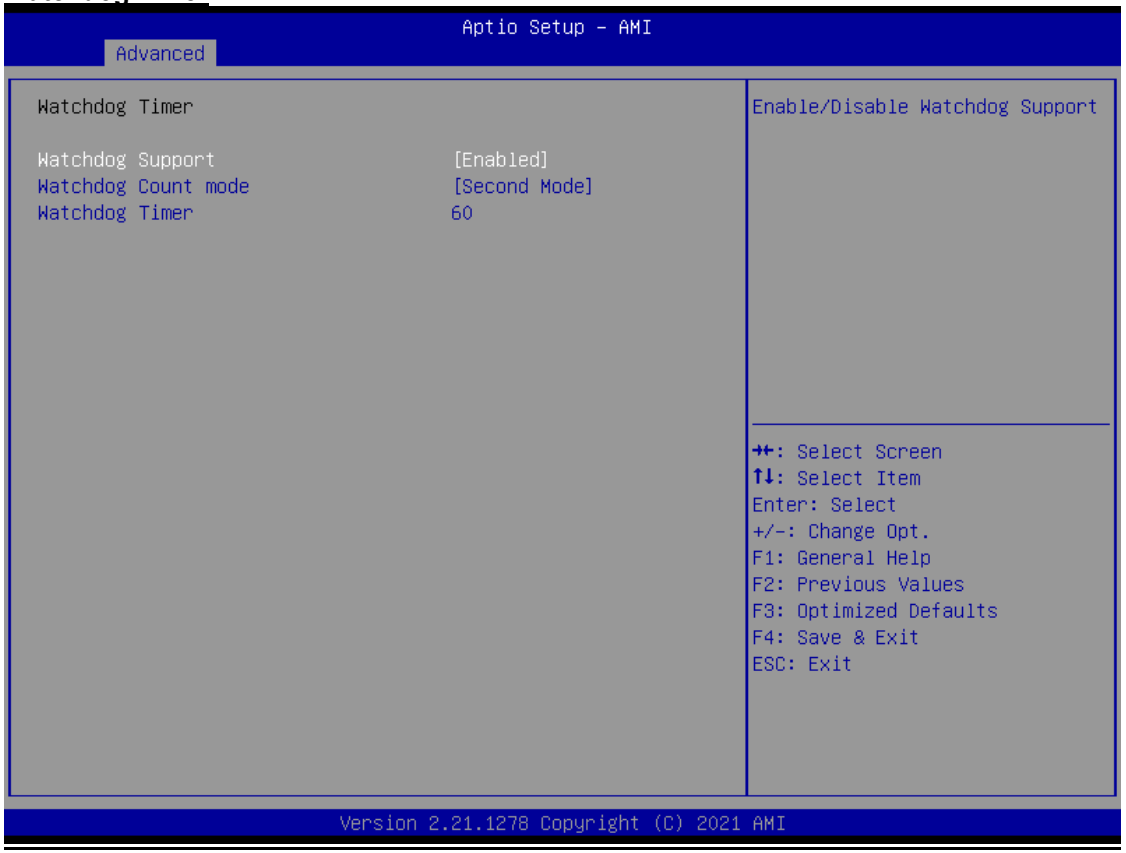
IO Expander Configuration

IO Expander Configuration



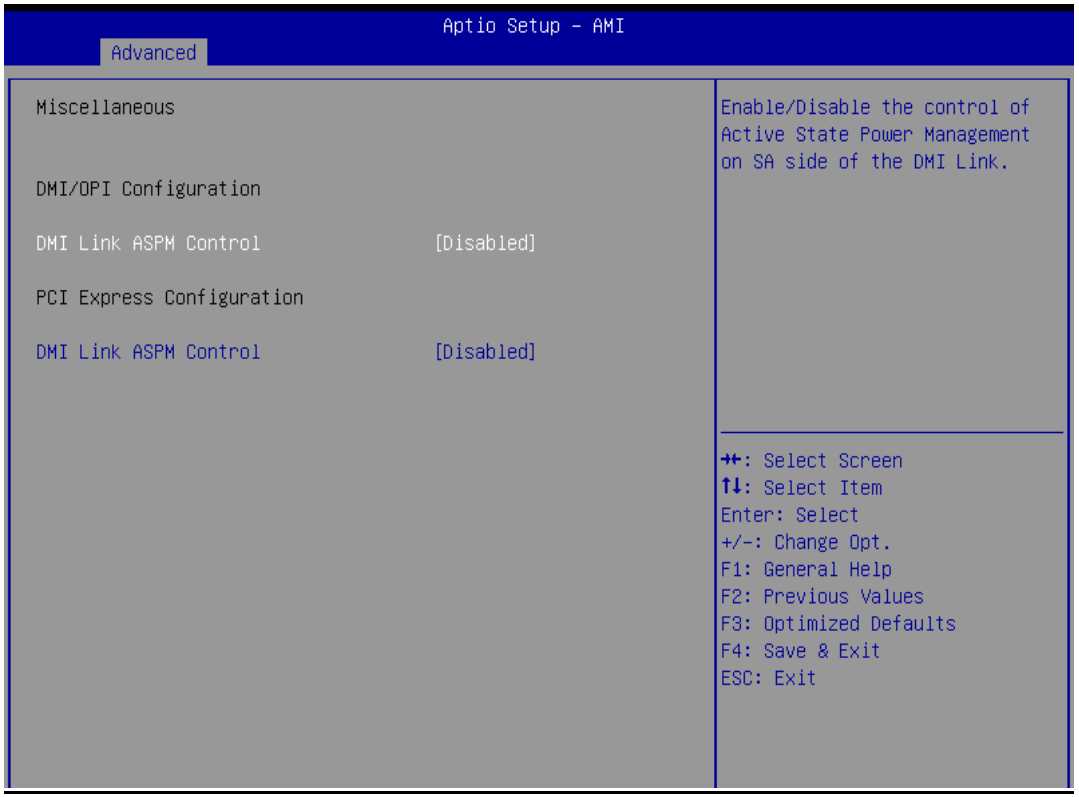
Feature	Description	Options
IO Expander GPIO 0~7		
Direction	Direction of this GPIO.	★Output, Input
Output Value	Output Value of this GPIO.	★High, Low

Watchdog Timer



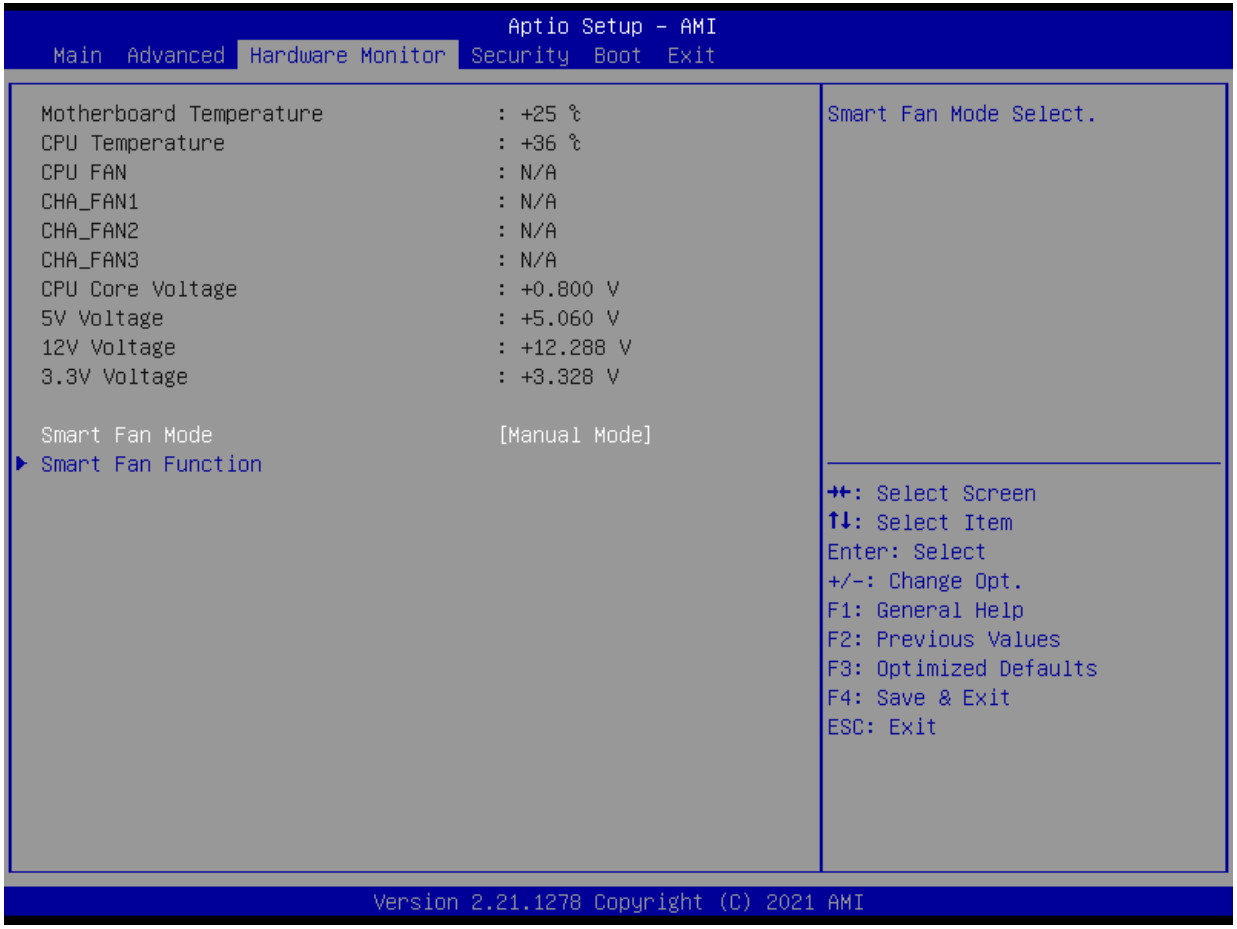
Feature	Description	Options
Watchdog Support	Enable/Disable Watchdog Support.	★Enable, Disabled
Watchdog Count mode	Select Watchdog Timer I count mode.	★Second Mode, Minute Mode
Watchdog Timer	Watchdog Timer I Time-out value.	★60

Miscellaneous



Feature	Description	Options
DMI/OPI Configuration		
DMI Link ASPM Control	Enable/Disable the control of Active State Power Management on SA side of the DMI Link.	★Disabled, L0s, L1, L0sL1
PCI Express Configuration		
DMI Link ASPM Control	The control of Active State Power Management of the DMI Link.	★Disabled, L0s, L1, L0sL1, Auto

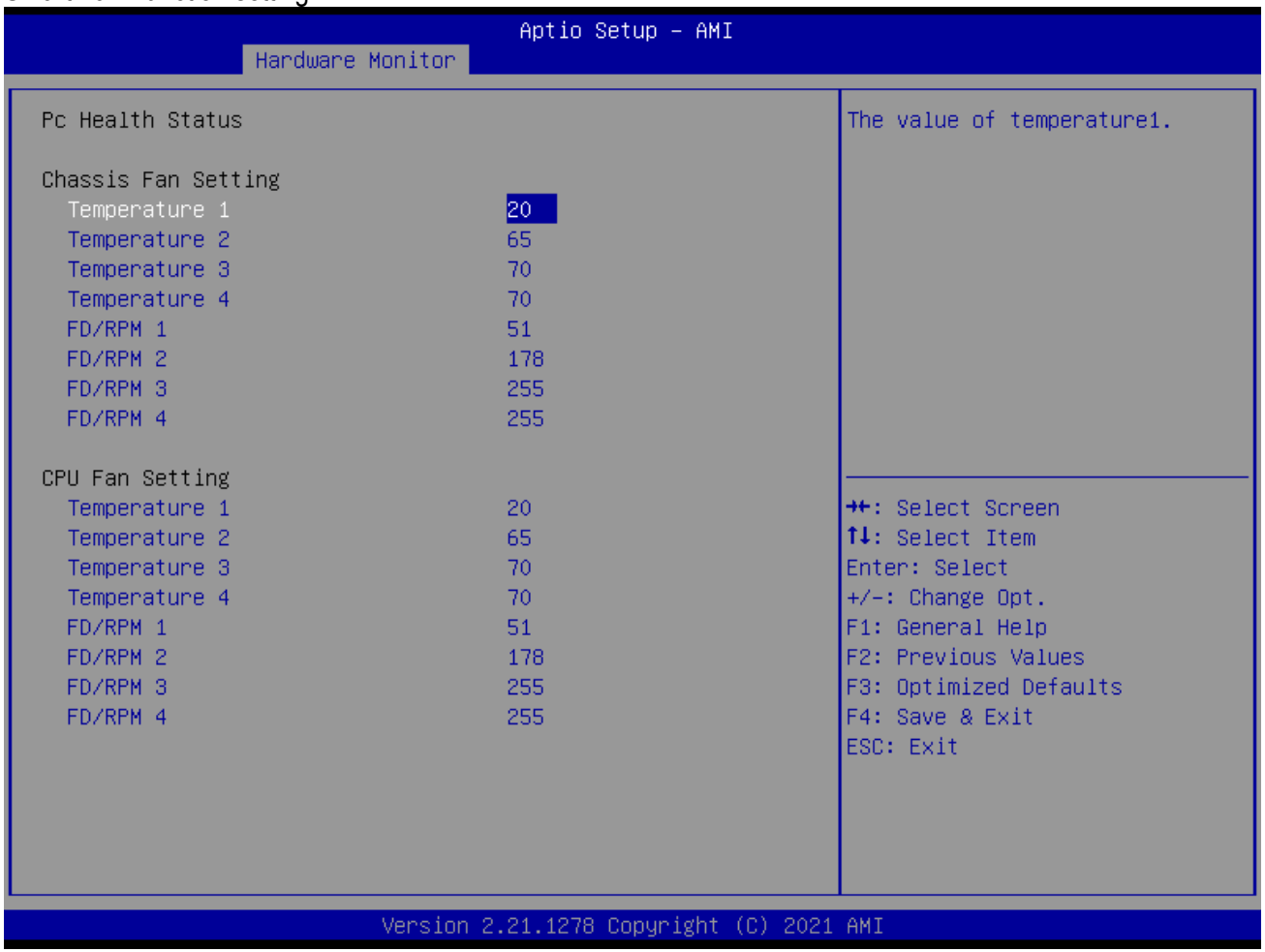
7.2.3 H/W Monitor



Feature	Description	Options
Smart Fan Mode	Smart Fan Mode Select	★Normal, Disabled, Manual Mode

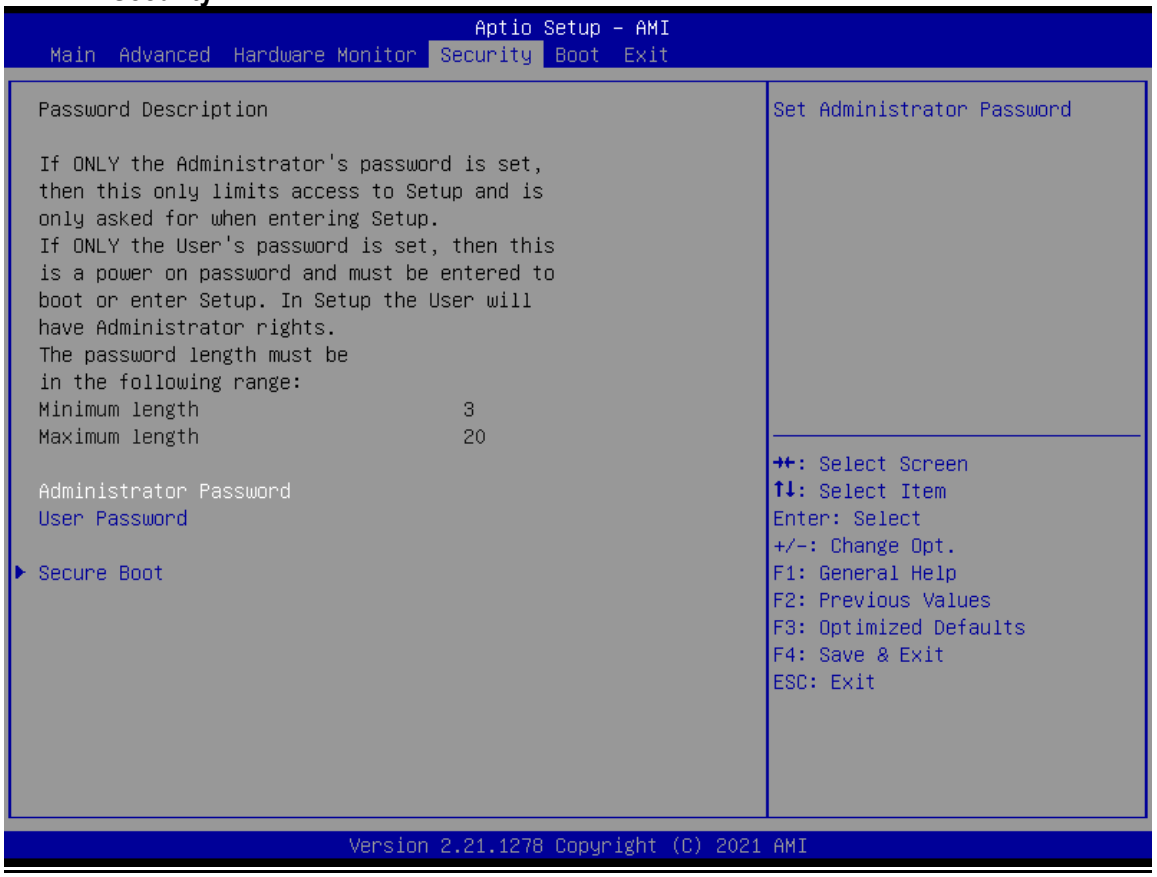
Smart Fan Function

Smart Fan Function setting



Feature	Description	Options
Chassis Fan Setting		
Temperature 1	The value of temperature 1.	★20
Temperature 2	The value of temperature 2.	★65
Temperature 3	The value of temperature 3.	★70
Temperature 4	The value of temperature 4.	★70
FD/RPM 1	The value of Fan Duty/RPM 1 when temperature is T1.	★51
FD/RPM 2	The value of Fan Duty/RPM 2 when temperature is T2.	★178
FD/RPM 3	The value of Fan Duty/RPM 3 when temperature is T3.	★255
FD/RPM 4	The value of Fan Duty/RPM 4 when temperature is T4.	★255
CPU Fan Setting		
Temperature 1	The value of temperature 1.	★20
Temperature 2	The value of temperature 2.	★65
Temperature 3	The value of temperature 3.	★70
Temperature 4	The value of temperature 4.	★70
FD/RPM 1	The value of Fan Duty/RPM 1 when temperature is T1.	★51
FD/RPM 2	The value of Fan Duty/RPM 2 when temperature is T2.	★178
FD/RPM 3	The value of Fan Duty/RPM 3 when temperature is T3.	★255
FD/RPM 4	The value of Fan Duty/RPM 4 when temperature is T4.	★255

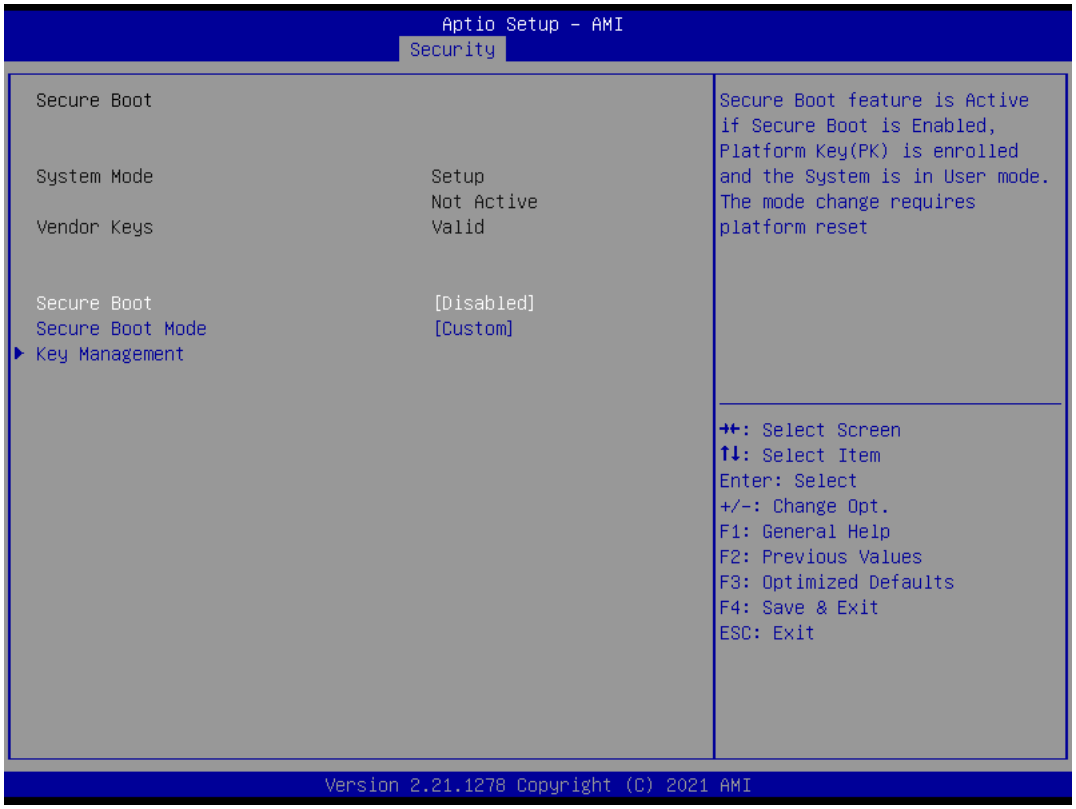
7.2.4 Security



Feature	Description	Options
Administrator Password	Set Administrator password.	
User Password	Set User Password	

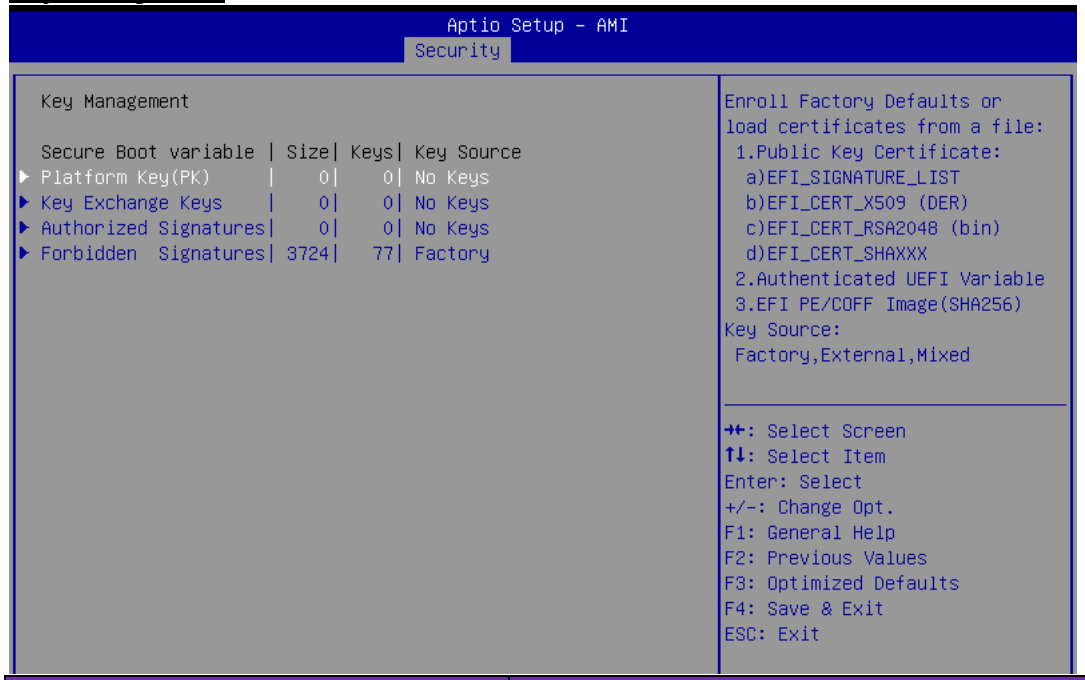
Secure Boot

Secure Boot configuration



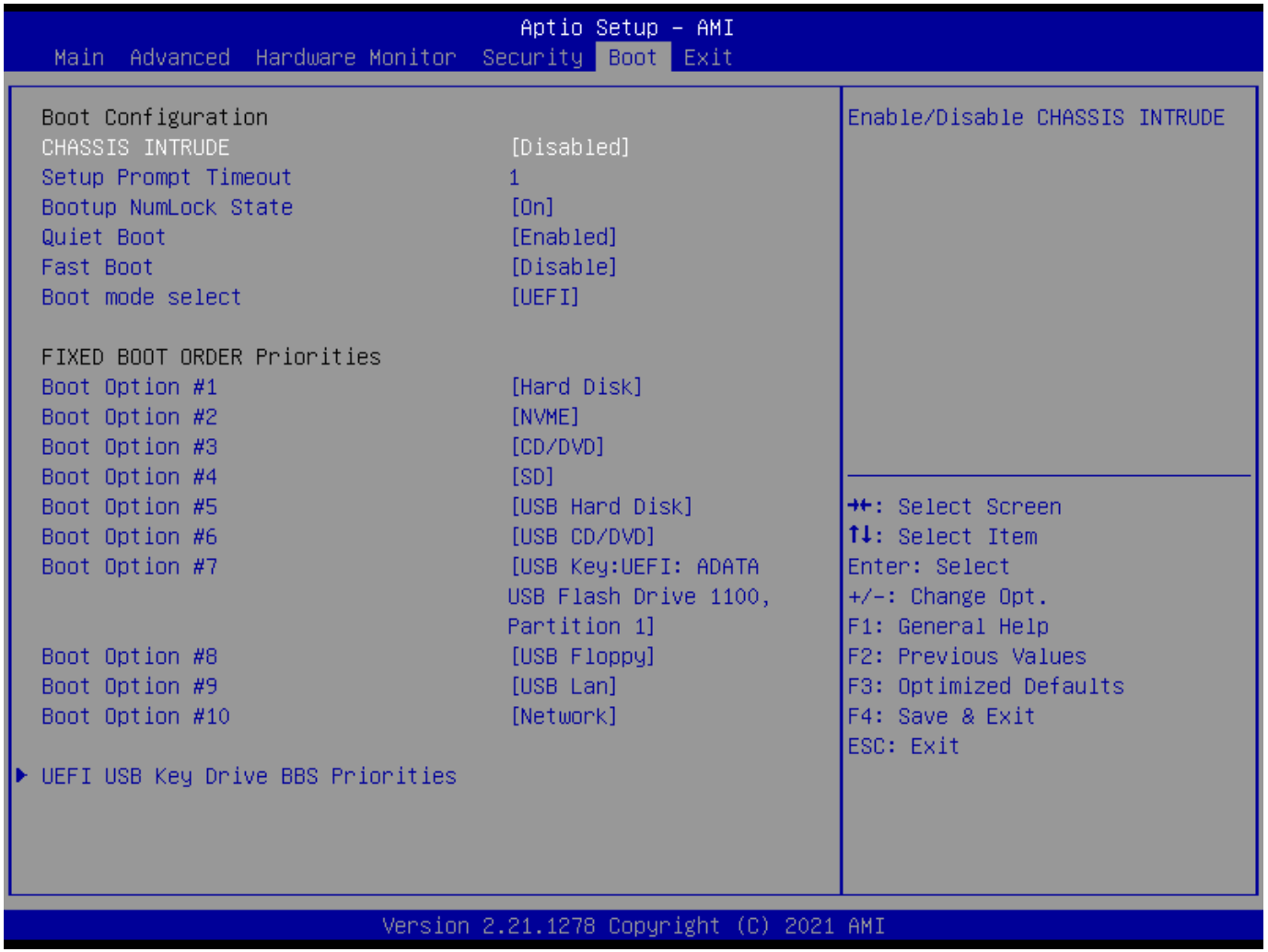
Feature	Description	Options
Secure Boot	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset.	★Disabled, Enabled
Secure Boot Mode	Secure Boot Mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication	★Custom ,Standard

Key Management



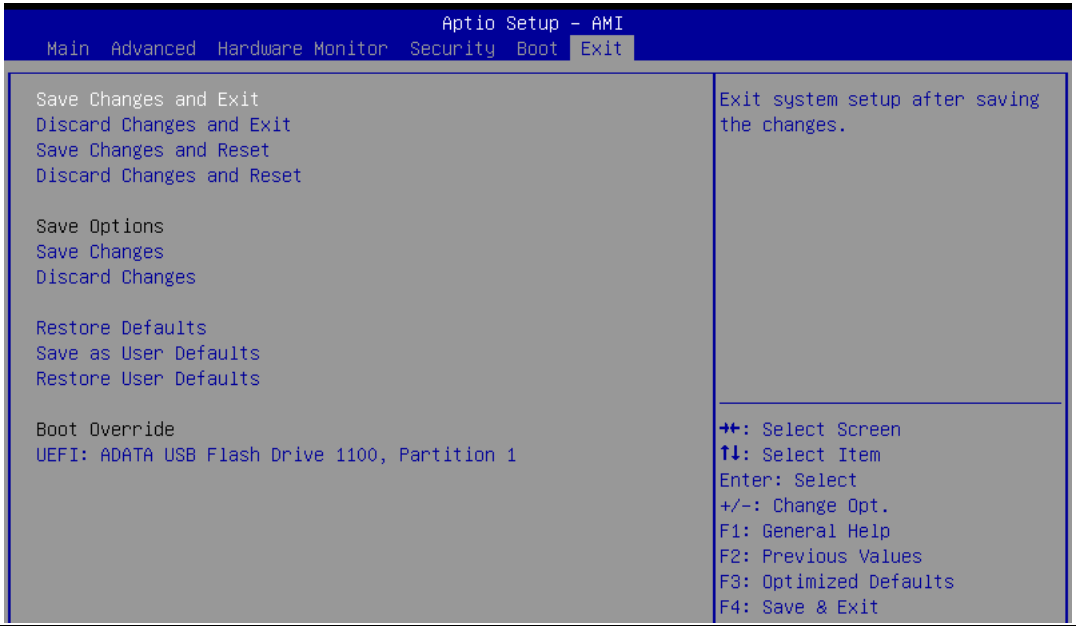
Feature	Description	Options
Platform Key(PK)	Enroll Factory Defaults or load certificates from a file: 1.Publuc Key Certificate: a)EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER) c) EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Factory, External, Mixed	
Key Exchange Keys		
Authorized Signatures		
Forbidden Signatures		

7.2.5 Boot


Aptio Setup - AMI
Main Advanced Hardware Monitor Security Boot Exit
Boot Configuration
CHASSIS INTRUDE [Disabled]
Setup Prompt Timeout 1
Bootup NumLock State [On]
Quiet Boot [Enabled]
Fast Boot [Disable]
Boot mode select [UEFI]
FIXED BOOT ORDER Priorities
Boot Option #1 [Hard Disk]
Boot Option #2 [NVME]
Boot Option #3 [CD/DVD]
Boot Option #4 [SD]
Boot Option #5 [USB Hard Disk]
Boot Option #6 [USB CD/DVD]
Boot Option #7 [USB Key:UEFI: ADATA USB Flash Drive 1100, Partition 1]
Boot Option #8 [USB Floppy]
Boot Option #9 [USB Lan]
Boot Option #10 [Network]
UEFI USB Key Drive BBS Priorities
Enable/Disable CHASSIS INTRUDE
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.21.1278 Copyright (C) 2021 AMI

Feature	Description	Options
CHASSIS INTRUDE	Enable/Disable CHASSIS INTRUDE	★Disabled, Enabled
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.	★1
Bootup NumLock State	Select the keyboard NumLock state	★On, Off
Quiet Boot	Enables or disables Quiet Boot option	★Enabled, Disabled
Fast Boot	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.	★Disabled, Enabled
Boot mode select	Select boot mode LEGACY/UEFI	★UEFI, LEGACY
Boot Option #1~#10	Sets the system boot order	★Hard Disk, NVME, CD/DVD,SD, USB Hard Disk, USB CD/DVD, USB Key, USB Floppy, USB Lan, Network, Disabled

7.2.6 Exit



Feature	Description	Options
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	Rest system setup without saving any changes.	
Save Changes	Save Changes done so far to any of the setup options.	
Discard Changes	Discard Changes done so far to any of the setup options.	
Restore Defaults	Restore/Load Default values for all the setup options.	
Save as Use Defaults	Save the changes done so far as User Defaults	
Restore User Defaults	Restore the User Defaults to all the setup options.	

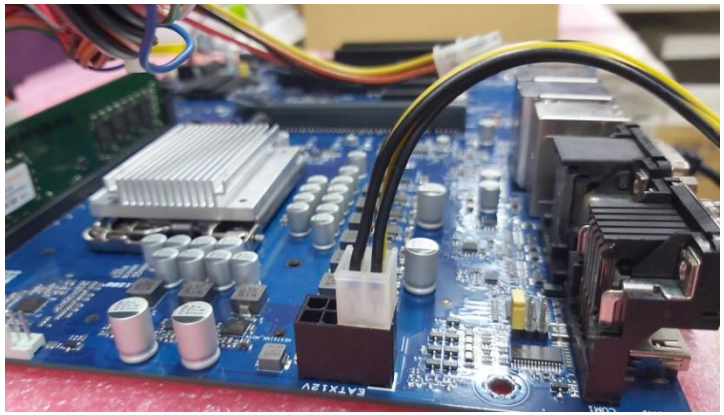
8 Troubleshooting

This section provides a few useful tips to quickly get RUBY-D812 running with success. This section will primarily focus on system integration issues, in terms of BIOS setting, and OS diagnostics.

8.1 Hardware Quick Installation

ATX Power Setting

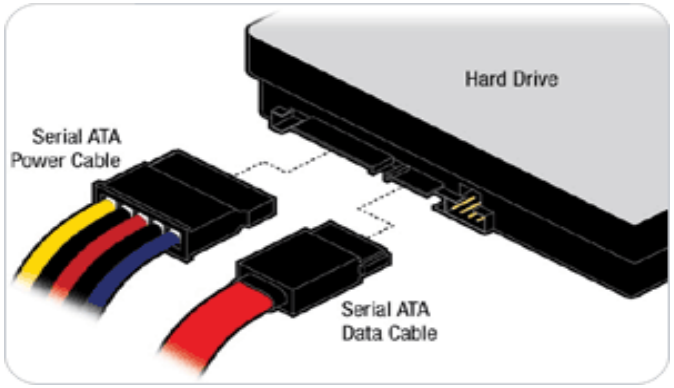
Unlike other Single board computer, RUBY-D812 supports ATX only. Therefore, there is no other setting that needs to be set up. However, there are only two connectors that must be connected—8-pin EATX12V & 24-pin EATXPW on the RUBY-D812 board.



Serial ATA

Unlike IDE bus, each Serial ATA channel can only connect to one SATA hard disk at a time;

The installation of Serial ATA is simpler and easier than IDE, because SATA hard disk doesn't require setting up Master and Slave, which can reduce mistake of hardware installation.



RUBY-D812 can support six SATA interface (SATAIII, 6.0Gb/s) on board. It has SATA ports on board.

8.2 BIOS Setting

It is assumed that users have correctly adopted modules and connected all the devices cables required before turning on ATX power. DDR4 UB-DIMM Memory, keyboard, mouse, SATA hard disk, VGA connector, power cable of the device, ATX accessories are good examples that deserve attention. With no assurance of properly and correctly accommodating these modules and devices, it is very possible to encounter system failures that result in malfunction of any device.

To make sure that you have a successful start with RUBY-D812, it is recommended, when going with the boot-up sequence, to hit "delete " or " Esc" key and enter the BIOS setup menu to tune up a stable BIOS configuration so that you can wake up your system far well.

Loading the default optimal setting

When prompted with the main setup menu, please scroll down to “Restore Defaults”, press “Enter” and select “Yes” to load default optimal BIOS setup. This will force your BIOS setting back to the initial factory configurations. It is recommended to do this so you can be sure the system is running with the BIOS setting that Portwell has highly endorsed. As a matter of fact, users can load the default BIOS setting at any time when system appears to be unstable in boot up sequence.

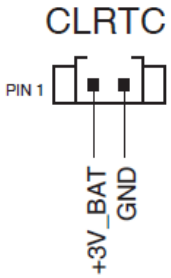
8.3 FAQ

Information & Support

Question: I forgot my password of system BIOS, what am I supposed to do?

Answer: You can switch off your power supply then find the 2-pin CLRTC on the RUBY-D812 board .Then Use a metal object such as a screwdriver to short the two pins and wait 5 seconds to clean your password then to switch on your power supply.

Clear CMOS header (2-pin CLRTC)：CMOS Setting



Question: How to update the BIOS file of RUBY-D812?

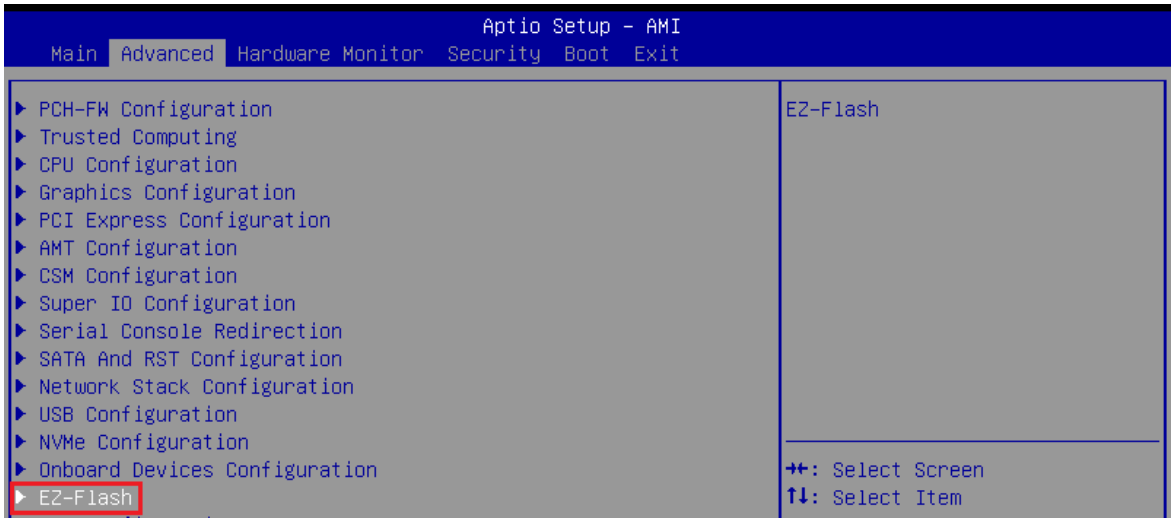
Answer: 1. Please visit web site of Portwell download center as below hyperlink

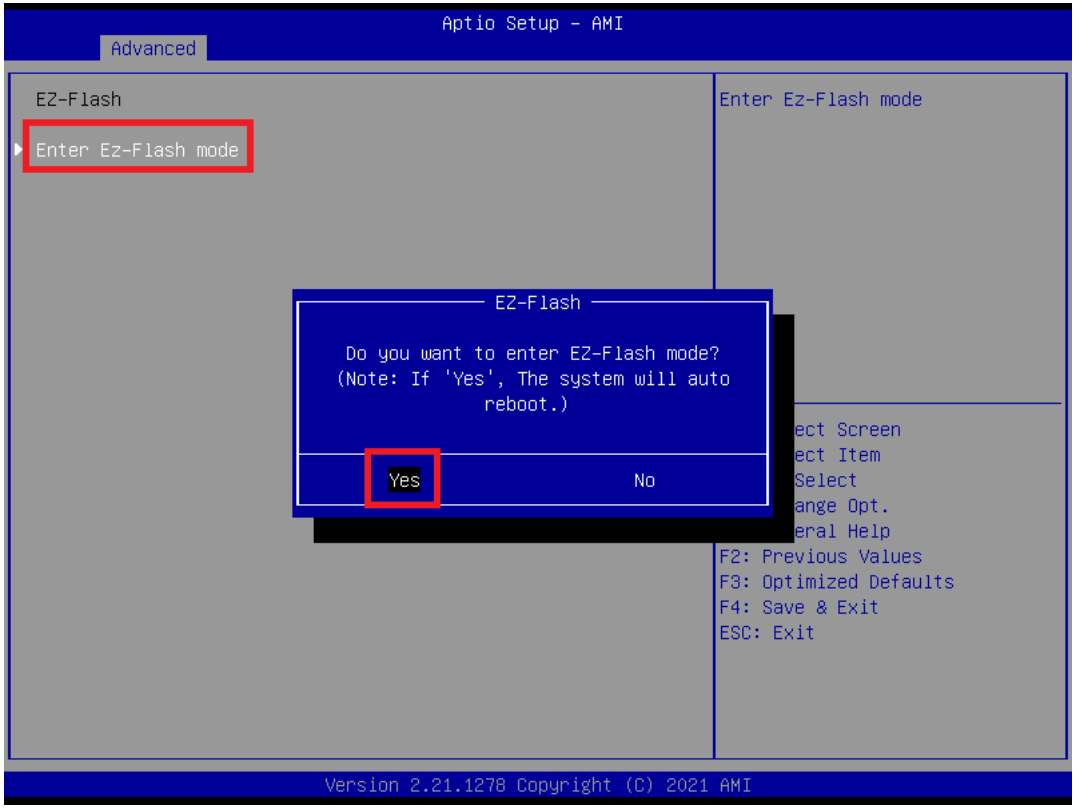
https://www.portwell.com.tw/support-center/download-center/

2. Select "Search download" and type the keyword "RUBY-D812".

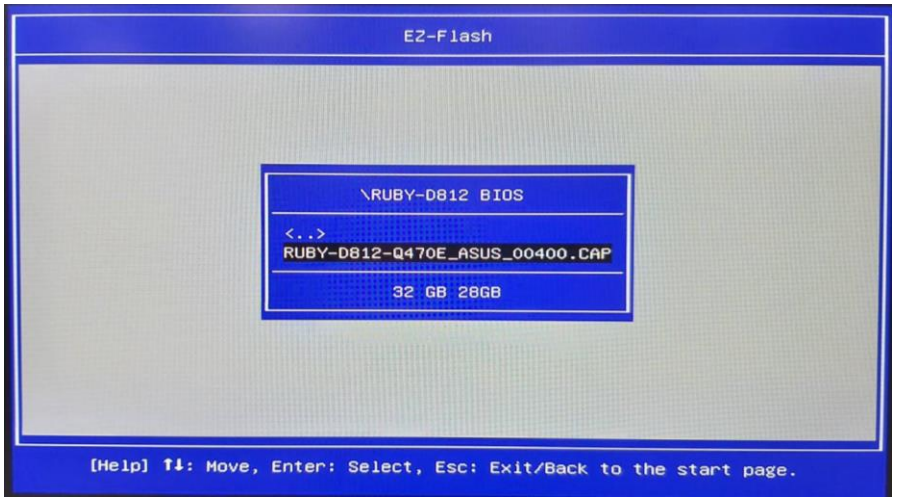
3. Find the "BIOS "page and download the ROM file and unzip file to USB flash drive (FAT 32 / 16 format).

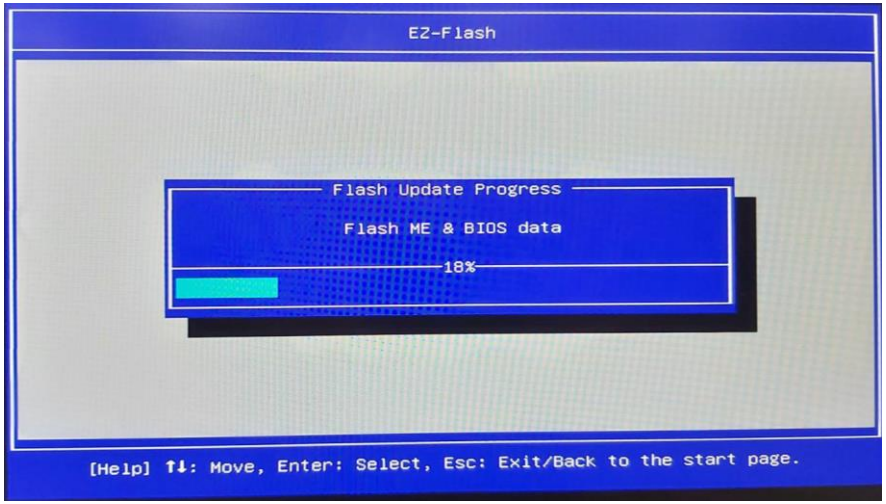
4. Boot into BIOS and switch to "Advanced" page then select" EZ-Flash".



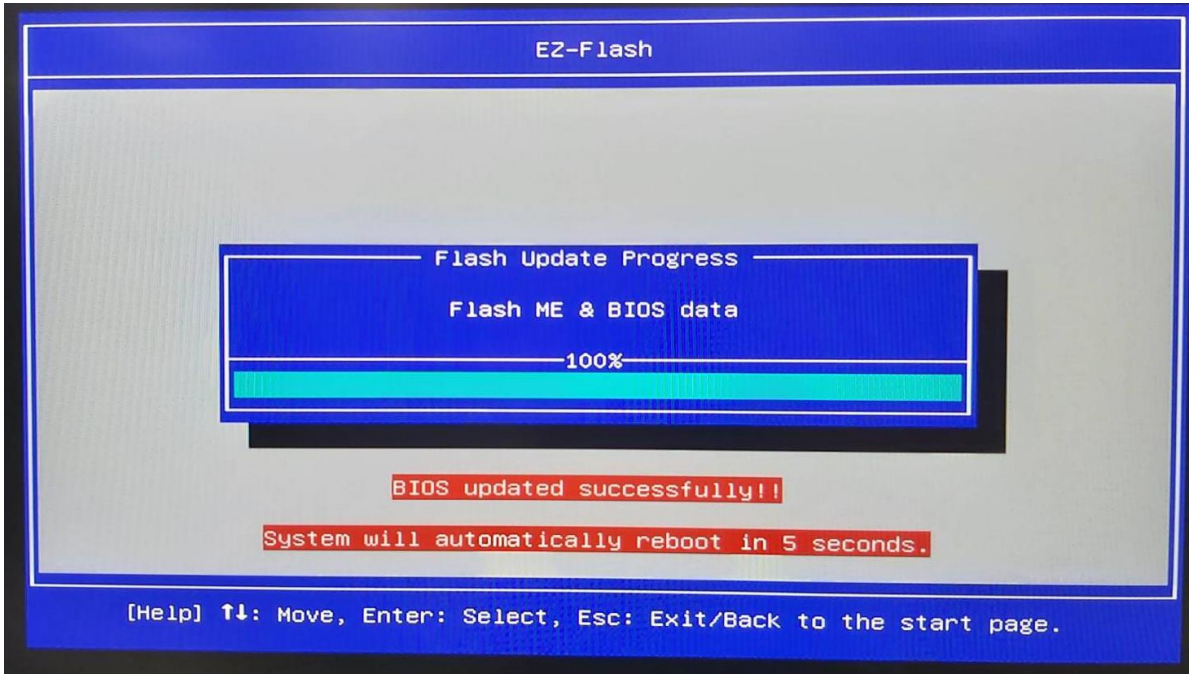

Aptio Setup – AMI
Advanced
EZ-Flash
Enter Ez-Flash mode
Enter Ez-Flash mode
EZ-Flash
Do you want to enter EZ-Flash mode?
(Note: If 'Yes', The system will auto reboot.)
Yes
No
ect Screen
ect Item
Select
ange Opt.
eral Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.21.1278 Copyright (C) 2021 AMI

5. Enter EZ-Flash mode, Select the USB Drive and Click the BIOS file then start updating BIOS.





6. When you see the “BIOS updated successfully” message, which means the BIOS update processes finished.
   Please cut the AC power of and **wait for 10 seconds** before powering on.



Question: What are the display options while using RUBY-D812 board?

Answer: - The RUBY-D812 supports VGA、HDMI、DP display output.

Note:

Please visit our Download Center to get the Catalog, User manual, BIOS, and Driver files.

https://www.portwell.com.tw/support-center/download-center/

If you have other additional technical information or request which is not covered in this manual, please fill in the technical request form as below hyperlink.

https://www.portwell.com.tw/support-center/technical-request/

We will do our best to provide a suggestion or solution for you.

Thanks

9 Portwell Software Service

1. If you have customized requirements of BIOS, you can contact person of our company or branch.
2. If you have requirements of WDT、GPIO APP, you can contact our headquarter or branch, and we can render you assistance on developing.

Portwell Worldwide:	
Portwell, Inc.	E-mail: info@portwell.com.tw
Shanghai Portwell	E-mail: info@portwell.com.cn
Portwell Japan, Inc	E-mail: info@portwell.co.jp
American Portwell Technology	E-mail: info@portwell.com
European Portwell Technology	E-mail: info@portwell.eu
Portwell UK Ltd.	E-mail: info@portwell.co.uk
Portwell Deutschland GmbH	E-mail: info@portwell.eu
Portwell India Technology	E-mail: info@portwell.in
Portwell Korea, Inc.	E-mail: info@portwell.co.kr
Portwell Latin America	E-mail: vendas@portwell.com.br

10 Industry Specifications

10.1 Industry Specifications

The list below provides links to industry specifications that apply to Portwell modules.

Low Pin Count Interface Specification, Revision 1.0 (LPC) http://www.intel.com/design/chipsets/industry/lpc.htm
Universal Serial Bus (USB) Specification, Revision 2.0 http://www.usb.org/home
PCI Specification, Revision 2.3 https://www.pcisig.com/specifications
Serial ATA Specification, Revision 3.0 http://www.serialata.org/
PCI Express Base Specification, Revision 2.0 https://www.pcisig.com/specifications