FWA8600

1U Rackmount Network Appliance

User's Manual

Version 1.1
(Nov. 2019)

Copyright

Disclaimer

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

Trademarks

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

Compliance

CE

This product has passed CE tests for environmental specifications and limits. This product is in accordance with the directives of the Union European (EU). If users modify and/or install other devices in this equipment, the CE conformity declaration may no longer apply.

FCC

This product has been tested and found to comply with the limits for a Class A device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with manufacturer's instructions, may cause harmful interference to radio communications.

WEEE

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

Green IBASE

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

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

Important Safety Information

Carefully read the precautions before using the device.

Environmental conditions:

- Lay the device horizontally on a stable and solid surface in case the device may fall, causing serious damage.
- Slots and openings on the chassis are for ventilation. Do not block or cover these openings. Make sure you leave plenty of space around the device for ventilation. NEVER INSERT OBJECTS OF ANY KIND INTO THE VENTILATION OPENINGS.
- Use this product in environments at ambient temperatures 0˚C ~ 40˚.
- DO NOT LEAVE THIS DEVICE IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -20˚C OR ABOVE 70˚C. This could damage the device. The device must be used in a controlled environment.

Care for your IBASE products:

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

⚠ WARNING

Attention during use:

- Do not use this product near water.
- Do not spill water or any other liquids on your device.
- Do not place heavy objects on the top of the device.
- Operate this device from the type of power indicated on the marking label. If you are not sure of the type of power available, consult your distributor or local power company.
- Do not walk on the power cord or allow anything to rest on it.
- If you use an extension cord, make sure that the total ampere rating of the product plugged into the extension cord does not exceed its limits.
- When handling processor chips or memory modules, avoid touching their pins or gold fingers. Put modules or peripherals back into antistatic bags when they are not in use or not installed in the chassis.

Avoid Disassembly

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

⚠ CAUTION

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Under no circumstances should the Lithium battery cell be shorted; otherwise the battery cell may heat up or cause potential burn hazards.

Warranty Policy

- **IBASE standard products:**

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

- **3rd-party parts:**

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

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

Technical Support & Services

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

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

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

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Packing List
- Optional Accessories
- Specifications
- Overview
- Dimensions

1.1 Introduction

The FWA8600 1U rackmount network security appliance is based on the scalable Intel Xeon Processor D-2100 series and has up to 25x GbE ports. This scalable system is designed for managing data driven workloads and enabling levels of performance in enterprise network security, Unified Threat Management and WAN optimization applications.

The FWA8600 supports up to 128GB RDIMM with four DDR4-2666 DIMM sockets and one Intel I210-AT Ethernet controller. The device comes with network interface card (NIC) slots to accommodate up to three IBN cards with 8x GbE ports each (3rd slot max. 4 ports) and one IBN-P401Q card for a maximum of 25 GbE ports. For I/O connectivity and expansion features, it offers a PCIe x8 slot, an M.2 expansion slot to interface with SATA 3.0 and PCIe x4 bus for high data throughput, as well as two USB 3.0, and an RJ45 serial console with LCM display for operation. LAN bypass is available in certain configuration.

Phot of FWA8600-NIC

The FWA8600 networking appliance is suitable for various networking and network management applications in a spectrum of organization sizes including SOHO, SMB, and enterprise markets.

1.2 Features

- Intel® Xeon® D-2100 series processor
- 4 x DDR4 RDIMM 2666 MHz; max. 128 GB (ECC or non-ECC)
- 1 x Intel® I210-AT GbE
- 4 x NIC modules with up to 24 GbE ports
- Optional IPMI module
- 1 x M.2 M2280 slot & optional PCIe (x8) expansion slot (4 lanes)
- 250W singly power supply or 300W 1+1 redundant power supply

1.3 Packing List

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

Models with a single PSU:

• FWA8600	x 1
• Full Range 250W ATX Power Supply	x 1
• Power Cord (180 cm)	x 1
• Rack Mount Bracket	x 2

Models with 1+1 redundant PSU:

• FWA8600	x 1
• 300W 1+1 Redundant Power Supply Unit	x 1
• Power Cord (180 cm)	x 2
• Rack Mount Bracket	x 2

1.4 Optional Accessories

IBASE provides the optional accessories listed below. Please contact us or your dealer for more information.

- Console Cable (160 cm, PK1-51)
- IPMI Module (IDN100)
- VGA Cable (40 cm, VGA21A)
- NIC Modules:
  IBN-R420BN (4 x RJ45 GbE, Non-Bypass)
  IBN-R420B (4 x RJ45 GbE, 2 Bypass Segment)
  IBN-R840N (8 x RJ45 GbE, Non-Bypass)
  IBN-R840 (8 x RJ45 GbE, 4 Bypass Segment)
  IBN-S400 (4 x GbE SFP, Non-Bypass)
  IBN-S800 (8 x GbE SFP, Non-Bypass)
  IBN-P400D (2 x 10GbE SFP+, Non-Bypass)
  IBN-P400Q (4 x 10GbE SFP+, Non-Bypass)
  IBN-F200 (2 x 25GbE SFP28, Non-Bypass)

1.5 Specifications

Product Name	**FWA8600-NIC**	**FWA8600-SHD**	**FWA8600-SHQ**
System			
Motherboard	MBN803		
Operating System	• Windows 10 (64-bit) • Linux Ubuntu 16.04.1		
CPU	Intel® Xeon® D-2100 BGA2518		
Chipset	Integrated		
Memory	4 x DDR4 RDIMM up to 2666 MHz; max. 128 GB (ECC or non-ECC)		
Storage	1 x 2.5" internal SATA drive bay	2 x 2.5" hot-swappable SATA drive bays	4 x 2.5" hot-swappable SATA drive bays
Network	• 2 x Intel® I210AT GbE controllers • 3 x IBN cards (3rd slot max. 4 ports) • 1 x IBN-P401Q for up to 28 GbE ports (Optional)	• 2 x Intel® I210AT GbE controllers • 2 x IBN cards • 1 x IBN-P401Q for up to 20 GbE ports (Optional)	• 2 x Intel® I210AT GbE controllers • 1 x IBN cards • 1 x IBN-P401Q for up to 12 GbE ports (Optional)

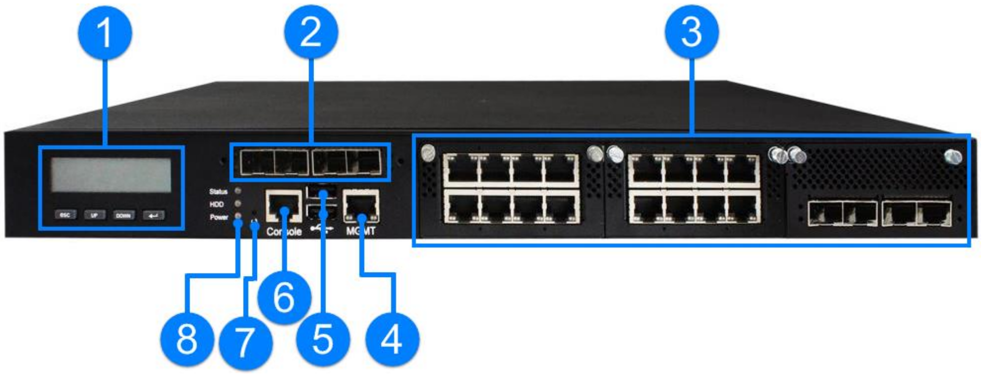
Product Name	FWA8600-NIC	FWA8600-SHD	FWA8600-SHQ
Super I/O	Nuvoton NCT5523D		
IPMI	IPMI module compliant with IPMI 2.0 (Optional)		
TPM	TPM 2.0		
Power Supply	• **Single PSU:** Full range 250W ATX power supply unit • **1+1 RPSU:** 300W 1+1 redundant power supply unit		
Power Requirement	100 ~ 240V AC		
BIOS	AMI BIOS		
Watchdog	Watchdog Timer 256 segments, 0, 1, 2…255 sec/min		
RoHS	Yes		
Chassis	Steel with textured black paint		
Dimensions (W x H x D)	438 x 44 x 451 mm (17.24” x 1.73” x 17.76”)		
Weight	10 kg (22.05 lb)		
Certificate	CE / FCC Class A		
Front I/O Ports			
LCM	1 x LCM 16x2 dots with 4 keypads		
Console	1 x Console port		
Management Port (MGMT)	1 x MGMT ports		
Ethernet Port	Up to 24 RJ45 GbE LAN ports (4 x network module slots)	Up to 20 RJ45 GbE LAN ports (3 x network module slots)	Up to 12 RJ45 GbE LAN ports (2 x network module slot)
USB	2 x USB 2.0		
HDD	N/A	2 x 2.5” hot-swappable SATA drive bays	4 x 2.5” hot-swappable SATA drive bays
Rear I/O Ports			
AC Inlet	• **Single PSU:** 1 x 100V ~ 240V AC Inlet • **1+1 RPSU:** 2 x 100V ~ 240V AC Inlet with 2 hot-swappable power supply modules		
Display	1 x VGA port (based on the optional IPMI module)		
Fan	3 x System fans		
Expansion	• 1 x PCIe (x8) slot with 4 lanes • 1 x M.2 M2280 slot with PCIe (x4) and SATA signal		

Product Name	FWA8600-NIC	FWA8600-SHD	FWA8600-SHQ
Environment			
Temperature	• **Operating:** 0 ~ 40 °C (32 ~ 104 °F) • **Storage:** -20~ 70 °C (-4 ~ 158 °F)		
Relative Humidity	5 ~ 90% at 45 °C (non-condensing)		
Vibration Protection	• **Operating:** 0.25 Grms / 3 ~ 500 Hz (Z-axis) • **Non-operating:** 1.0 Grms / 3 ~ 500 Hz (Z-axis)		
Shock Protection	• **Operating:** 20G / 11ms (X/Y/Z-axis, 3 lines in each axis) • **Non-operating:** 40G / 11ms (X/Y/Z-axis, test 3 lines in each axis)		

All specifications are subject to change without prior notice.

1.6 Overview

Front View

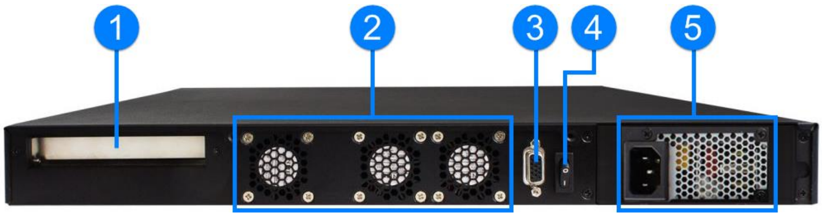


No.	Name	No.	Name
1	LCM Display with 4 buttons	5	2 USB 2.0 Ports
2	4 10GbE SFP+ Ports (Optional)	6	Console Port
3	Network Modules / 2.5" Hot-swappable Drive Bays	7	User Self-Defined GPIO Button
4	Management Port	8	LED Indicators (From top to bottom: Status, HDD, Power)

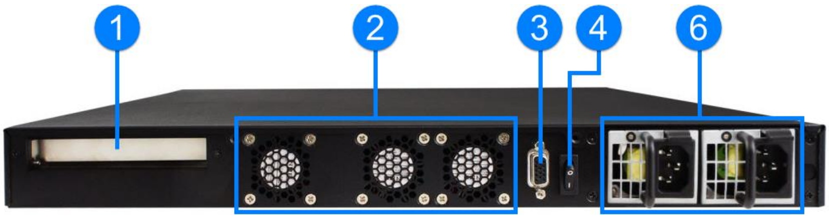
Oblique View

Rear View

- **Single Power Supply Unit**



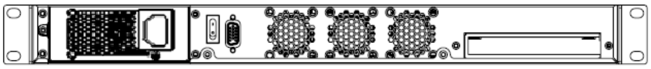
- **Redundant Power Supply Unit**



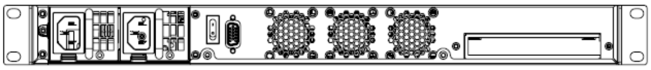
No.	Name	No.	Name
1	PCIe (x8) Expansion Card Slot (4 lanes signal only)	4	Power Switch
2	System Fan Modules	5	Single Power Supply Unit
3	VGA Port (via the optional IPMI module)	6	Reduntant Power Supply Unit

1.7 Dimensions

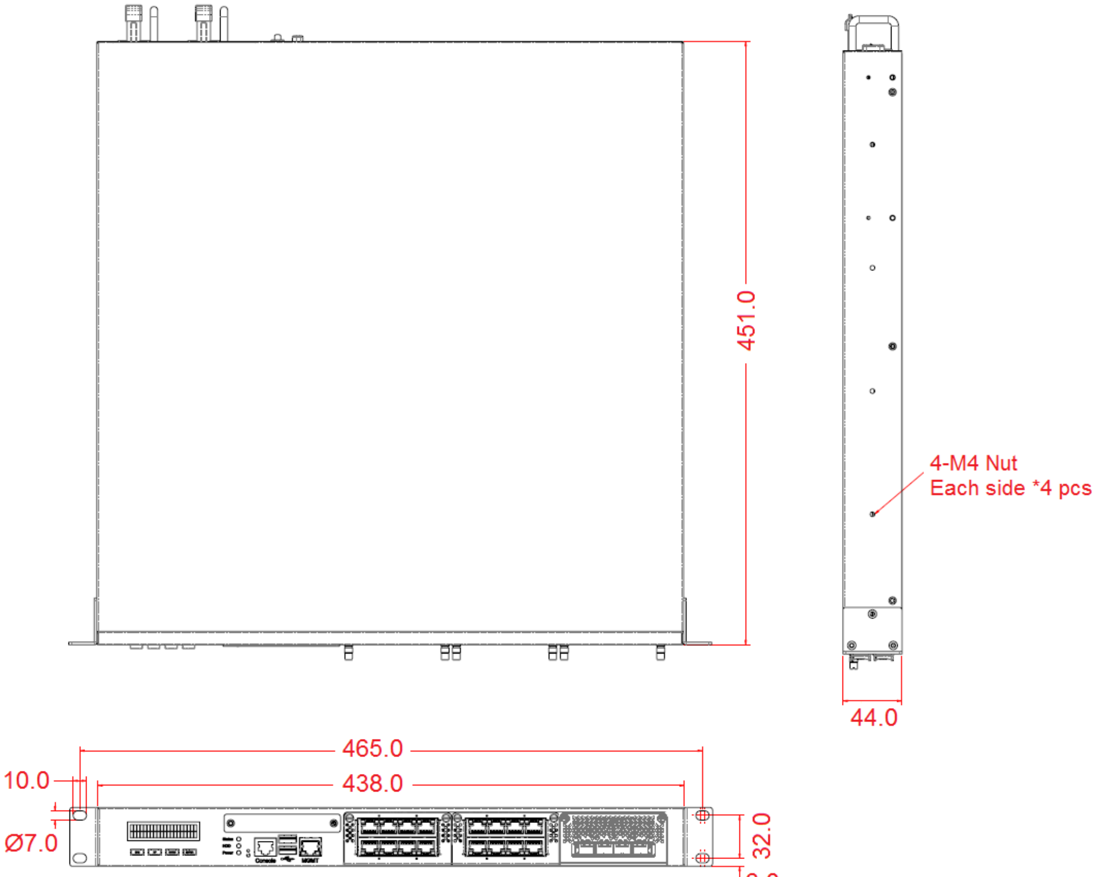
Unit: mm



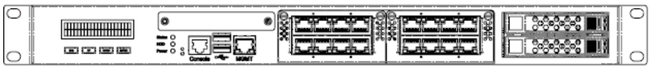
Single PSU



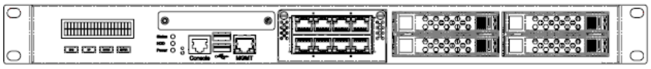
1+1 Redundant PSU



FWA8600-NIC



FWA8600-SHD



FWA8600-SHQ

Chapter 2
Hardware Configuration

The information provided in this chapter includes:

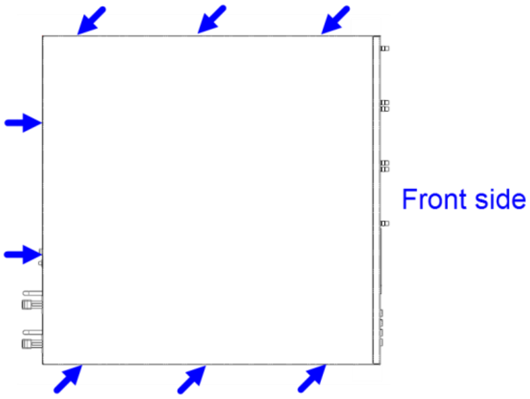
- Installation / Replacement
- Information and locations of connectors

2.1 Installation / Replacement

For the FWA8600 hot-swappable HDD (available for FWA8600-SHD and FWA8600-SHQ), or the IBN Network Interface Modules installations, you can directly install them without removing the device cover.

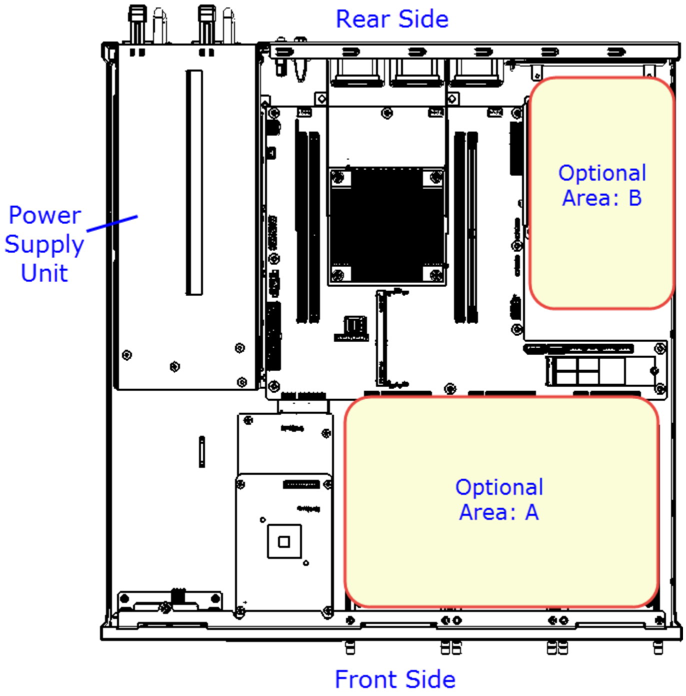
For memory, M.2, PCIe expansion card or the optional IPMI module, you need to remove 8 screws as shown below to pull out the lid.

This is illustrated by the example of FWA8600-NIC.



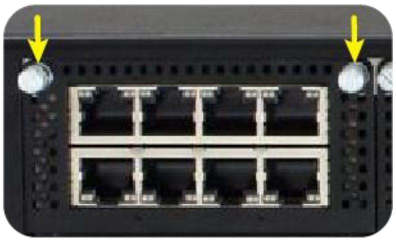
Configuration inside:

Refer to the figure below for the intenal areas to install additional 2.5” HDD/SSD, NIC modules, and expansion card. Area A accommodates NIC modules or 2.5” how-swappable HDD/SSD. Area B supports for two 2.5” HDD/SSD and an expansion card.



2.1.1 Network Module

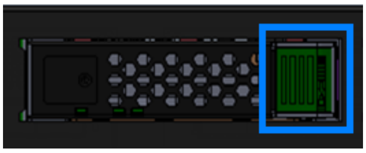
Release the two screws of the network module and pull it out carefully as shown below for replacement and installation.



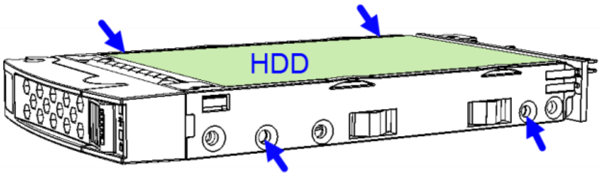
2.1.2 HDD or SSD

FWA8600-SHD & FWA8600-SHQ hot-swappable HDD/SSD:

1. Push the latch outwards to release and take out the HDD tray.

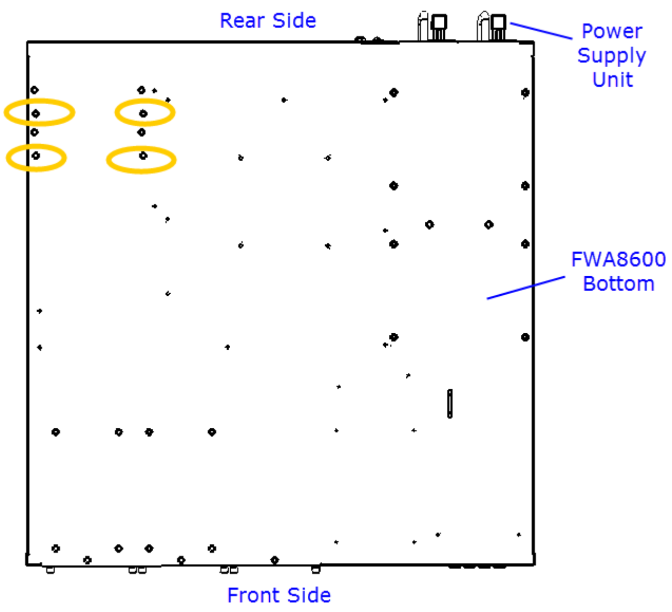


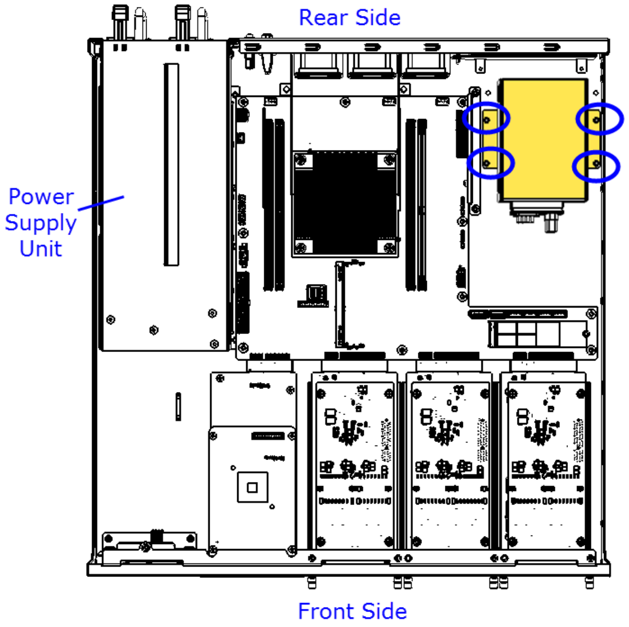
2. Remove the 4 screws on both lateral sides of the HDD tray. Install your HDD and tighten the screws.



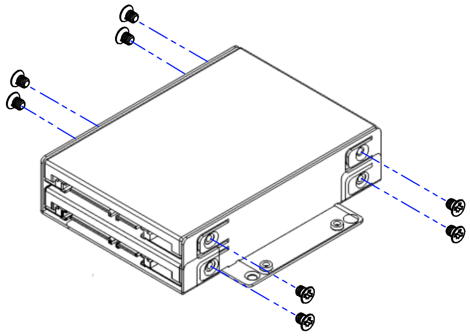
FWA8600 Internal HDD/SSD:

1. After you’ve removed the lid of the system, remove the indicated 4 screws as indicated below to release the internal 2.5” HDD/SSD and the bracket.





2. Unplug the SATA power and data cable, and remove the 4 screws from the holder bracket for each HDD/SSD for replacement.

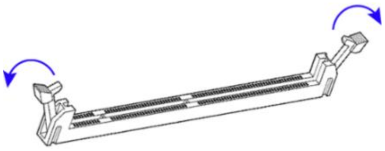


3. Take out the HDD/SSD and install a new one onto the tray. Fasten the 4 screws back for each HDD/SSD.
4. Secure the HDD/SSD and the bracket back to the system.

2.1.3 Memory Module

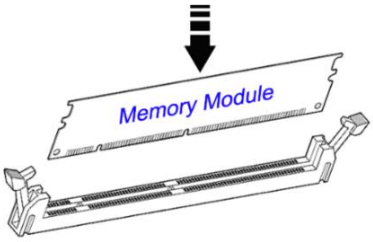
If you need to install or replace a memory module, follow the instructions below after you remove the device cover.

1. Press the ejector tab of the memory slot down and outwards with your fingertips.



2. Hold the memory module and align the key of the module with that on the memory slot.

3. Gently push the module in an upright position until the ejector tabs of the memory slot close to hold the module in place when the module touches the bottom of the slot.

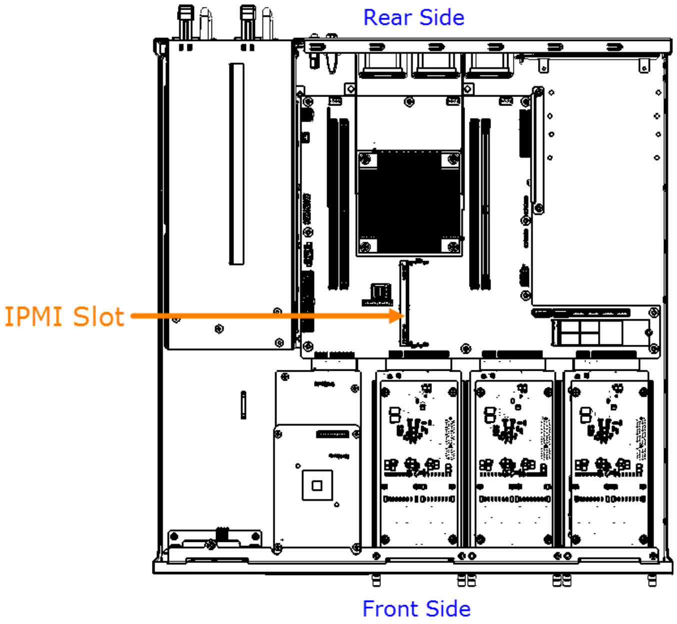


To remove the module, press the ejector tabs outwards with your fingertips to eject the module.

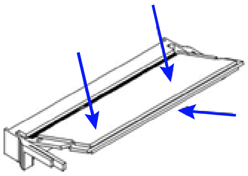
2.1.4 IPMI Module

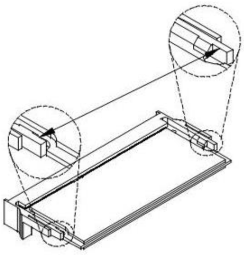
If you need to install an IPMI module, remove the system lid firstly and then follow the instructions below.

Note: IPMI modules are optional items.



1. Locate the IPMI slot and align the key of the module with that on the slot.
2. Insert the module slantwise and gently push the module straight down until the clips of the slot close to hold the module in place when the module touches the bottom of the slot.

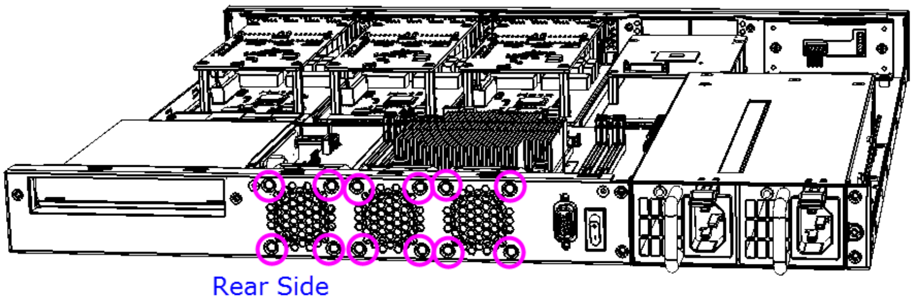




To remove the module, press the clips outwards with your thumb and index finger of both hands.

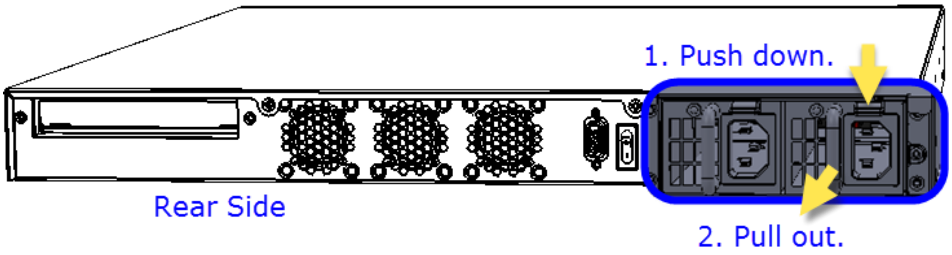
2.1.5 Fan

If you need to install or replace a fan module,remove the device cover first. Release the 4 screws of the fan module on the rear side of the device, take out the fan to replace with a new one, and tighten the screws.

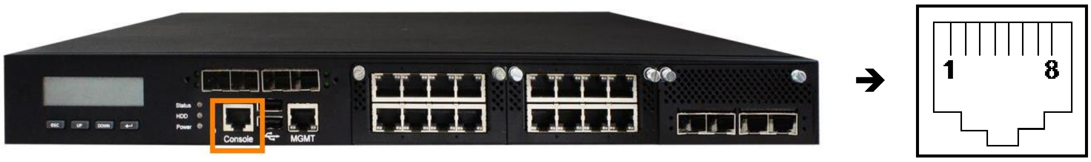


2.1.6 Redundant Power Supply Unit

If you need to install or replace a redundant power supply unit, push the latch downwards first. Grasp the handle, pull the PSU out carefully and replace it with a new one.



2.2 Pinout for Console Port

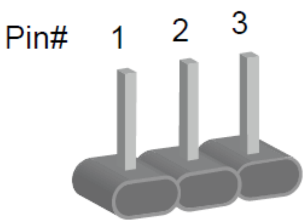


Pin	Signal Name	Pin	Signal Name
1	RTS	5	Ground
2	DTR	6	RXD
3	TXD	7	DSR
4	Ground	8	CTS

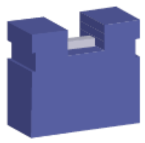
2.3 Setting the Jumper

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

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

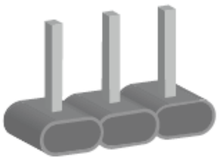
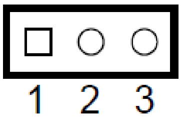
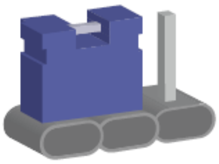
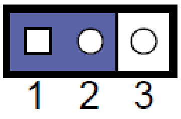
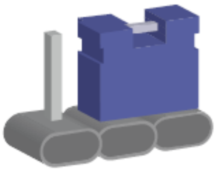
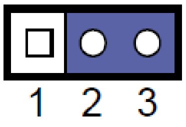


A 3-pin jumper



A jumper cap

Refer to the illustration below to set jumpers.

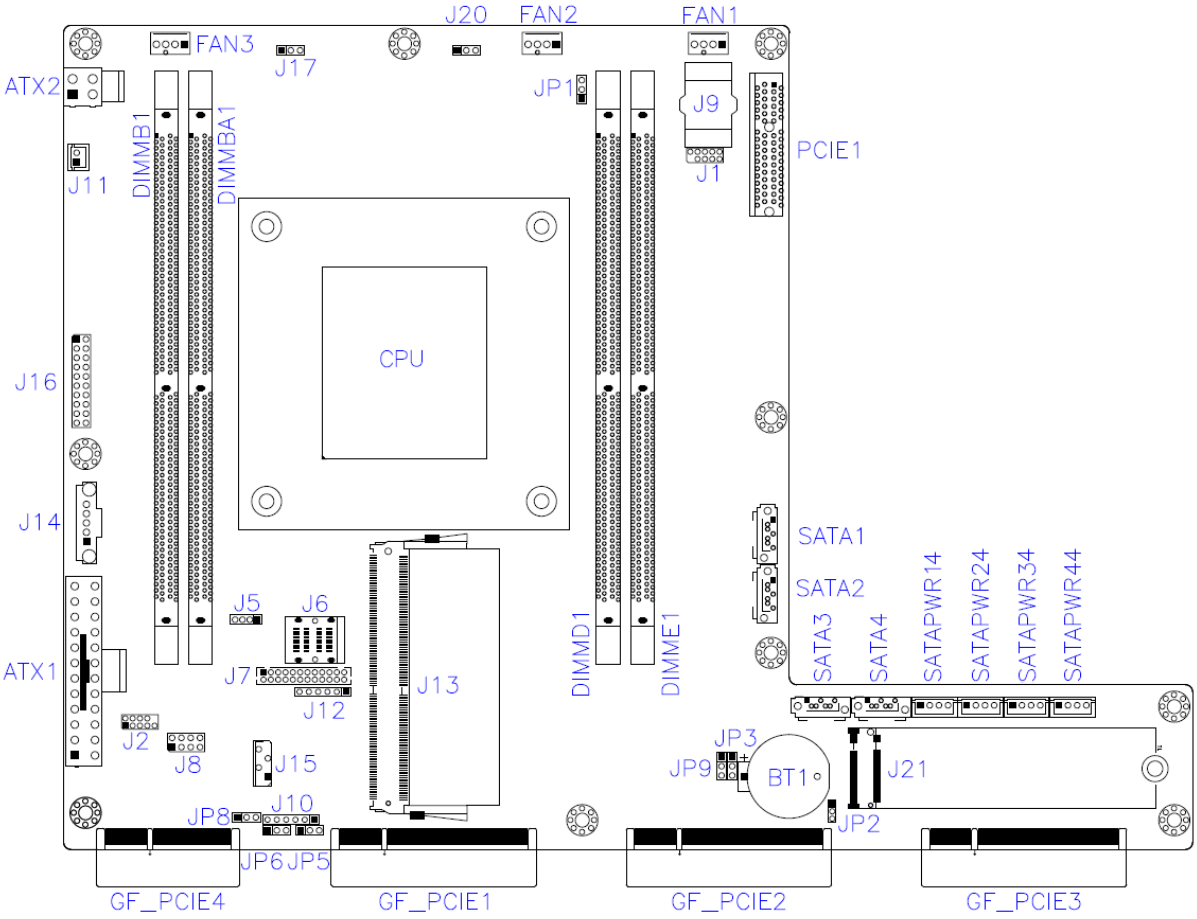
Pin closed	Oblique view	Schematic illustration
Open		
1-2		
2-3		

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

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

2.4 Jumper & Connector Locations on Motherboard

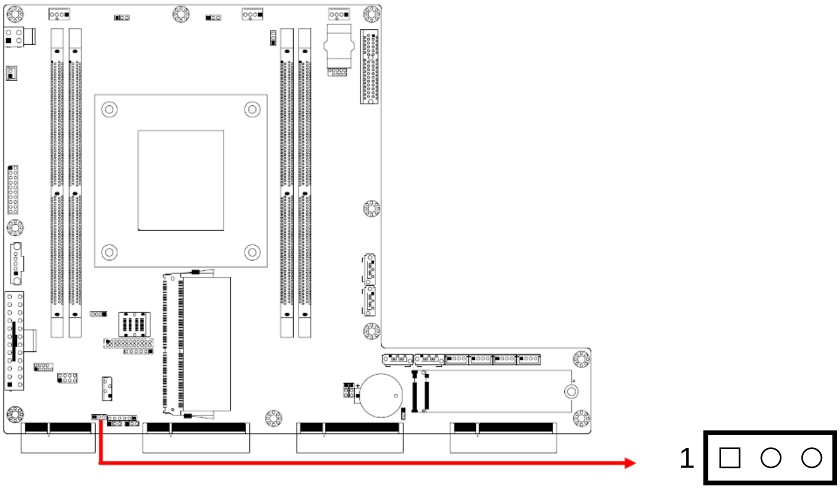
Motherboard: MBN803

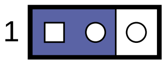
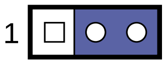


2.5 Jumper Quick Reference

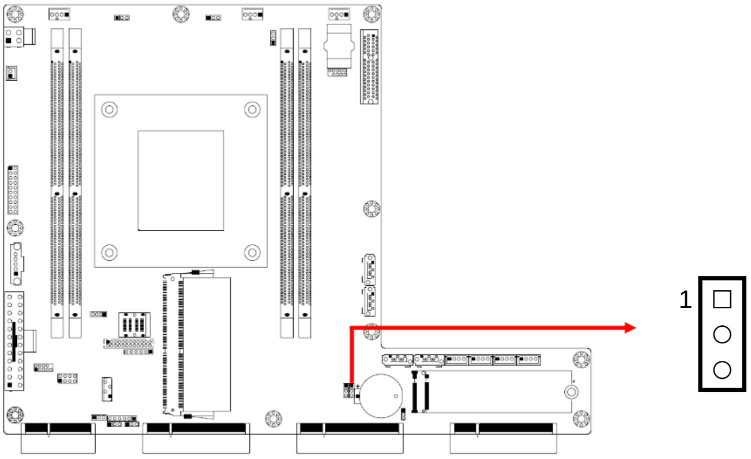
Function	Connector Name	Page
AT & ATX Mode	JP8	19
Clearing CMOS Data	JP3	20
Clearing ME Register	JP9	21
Factory Use Only	JP1, JP5, JP6	--

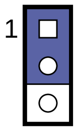
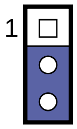
2.5.1 AT & ATX Mode (JP8)



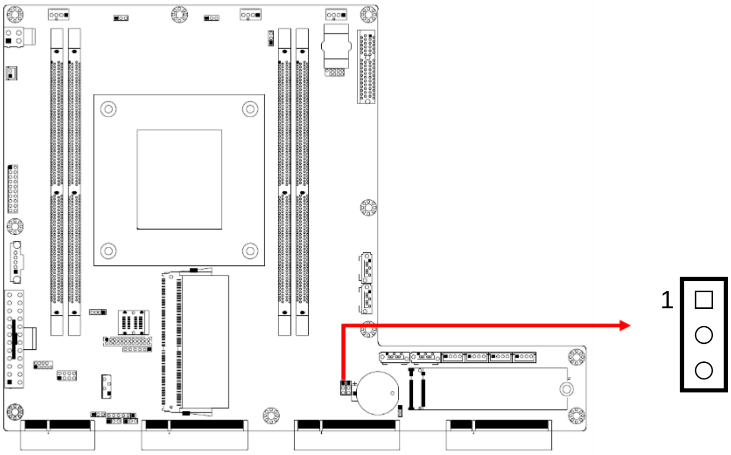
Function	Pin closed	Illustration
AT Mode (Default)	1-2	
ATX Mode	2-3	

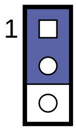
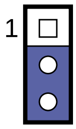
2.5.2 Clearing CMOS Data (JP3)



Function	Pin closed	Illustration
Normal (Default)	1-2	
Clearing CMOS	2-3	

2.5.3 Clearing ME Register (JP9)



Function	Pin closed	Illustration
Normal (Default)	1-2	
Clearing ME Register	2-3	

2.6 Connectors Quick Reference

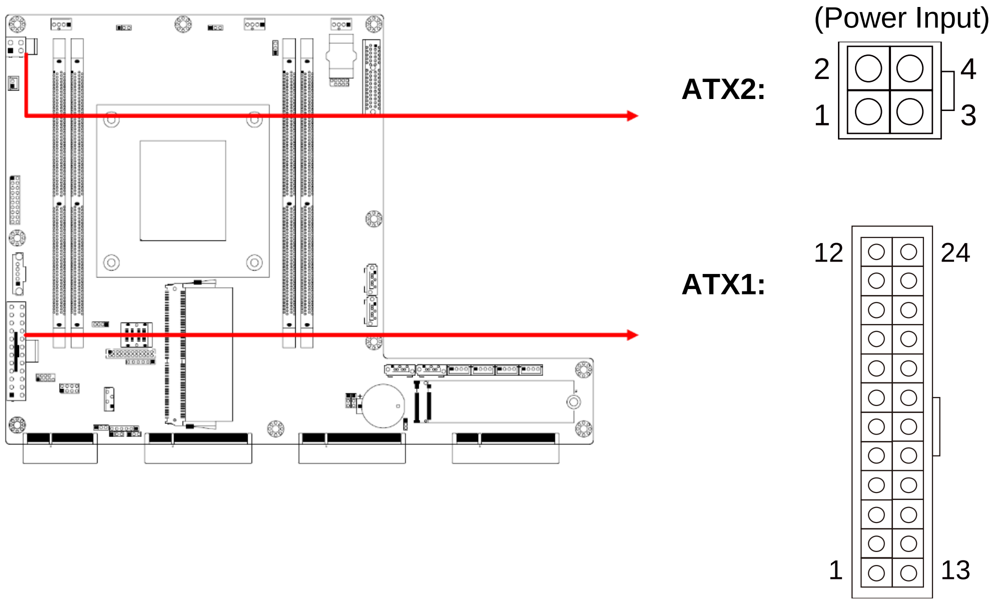
Function	Connector Name	Page
ATX Power Connector	ATX1, ATX2	23
External Power Switch Connector	J11	24
Front Panel Setting Connector	J16	24
PM Bus Port [1]	J14	25
Digital I/O Connector	J8	25
IPMB Port (Reserved)	J15	26
Fan Connector	FAN1, FAN2, FAN3	26
SATA Power Connector	SATAPWR1, SATAPWR2, SATAPWR3, SATAPWR4	27
SATA RAID Key	J5	27
SATA III Port	SATA1, SATA2, SATA3, SATA4	--
10 GbE Port (Mini-SAS HD type)	J6	--
10 GbE LED Port	J7	--
Socket for BIOS Chip	J9	--
IPMI Connector [2]	J13	--
DDR4 Memory Slot	DIMMA1, DIMMB1, DIMMD1, DIMME1	--
M.2 M2280 Slot	J21	--
PCIe (x4) Slot	**Standard:** PCIE1 **For IDN803**: GF_PCIE4 [3]	
PCIe (x8) Slot	**For IBN Card only:** GF_PCIE1, GF_PCIE2, GF_PCIE3	--
Factory Use Only	J1, J2, J5, J8, J10, J12, J17, J20	--

[1]: Applicable to redundant power supply unit only.

[2]: Applicable to IBASE IDN100 card only.

[3]: Applicable to IBASE IDN803 only.

2.6.1 ATX Power Connector (ATX1, ATX2)



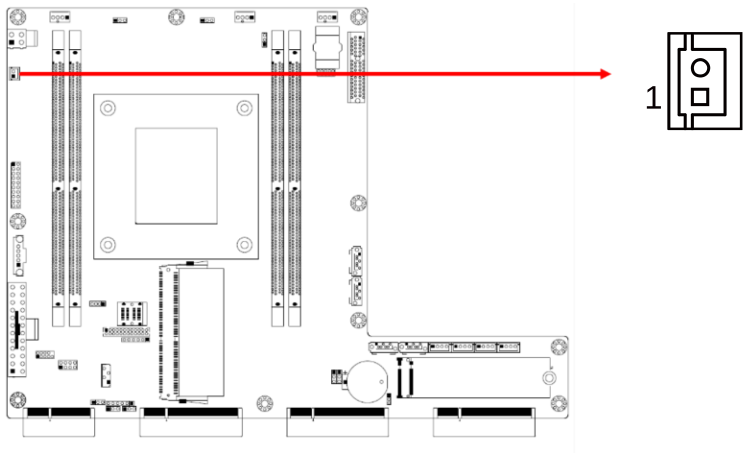
ATX2: Power Input

Pin	Assignment	Pin	Assignment
1	Ground	3	VCC12
2	Ground	4	VCC12

ATX1:

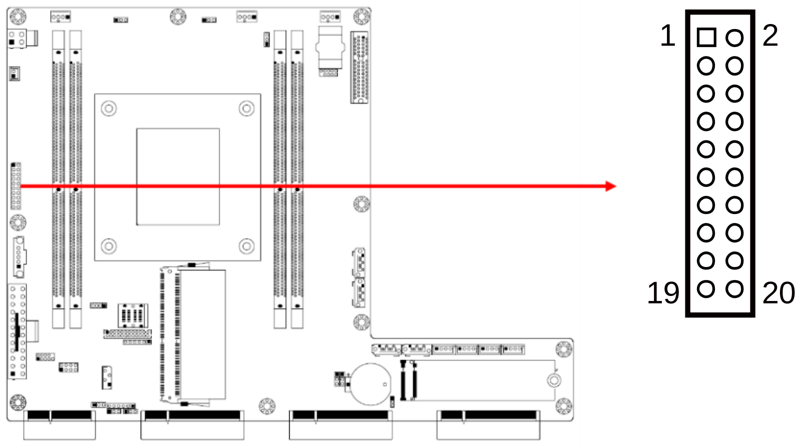
Pin	Assignment	Pin	Assignment
1	VCC3_3	13	VCC3_3
2	VCC3_3	14	-12V
3	Ground	15	Ground
4	VCC5	16	ATX_PSON#_Q
5	Ground	17	Ground
6	VCC5	18	Ground
7	Ground	19	Ground
8	Power good	20	-5V
9	5VSB_PS	21	VCC5
10	VCC12	22	VCC5
11	VCC12	23	VCC5
12	VCC3_3	24	Ground

2.6.2 External Power Switch Connector (J11)



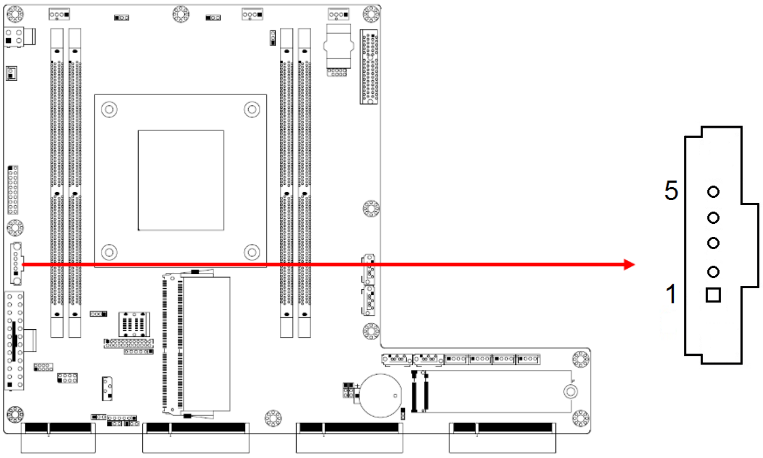
Pin	Signal Name	Pin	Signal Name
1	ATX_PSON#_EN_R	2	Ground

2.6.3 Front Panel Setting Connector (J16)



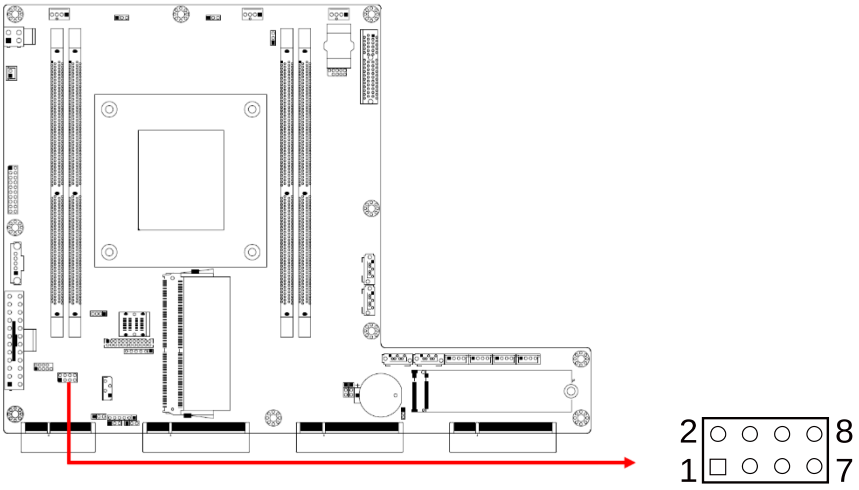
Pin	Signal Name	Pin	Signal Name
1	VCC5	2	SPEAKER
3	NC	4	NC
5	Ground	6	NC
7	NC	8	NC
9	5VDUAL	10	5VDUAL
11	5VDUAL	12	5VDUAL
13	Ground	14	ATXPWR_BTN#
15	NC	16	NC
17	Ground	18	FRST_OUT
19	VCC3_3	20	-HDD_LED

2.6.4 PM Bust Port (J14)



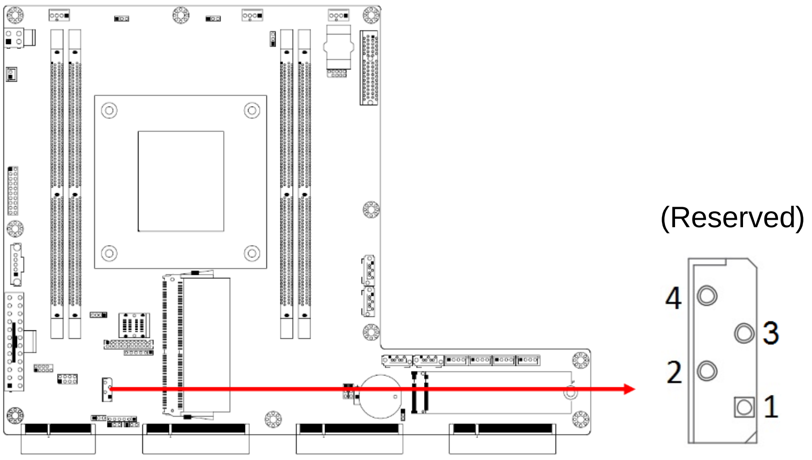
Pin	Signal Name	Pin	Signal Name
1	SMB_PWR_5VDUAL_CLK	4	Ground
2	SMB_PWR_5VDUAL_DAT	5	VCC3_3
3	PL_SMB Alert		

2.6.5 Digital I/O Connector (J8)



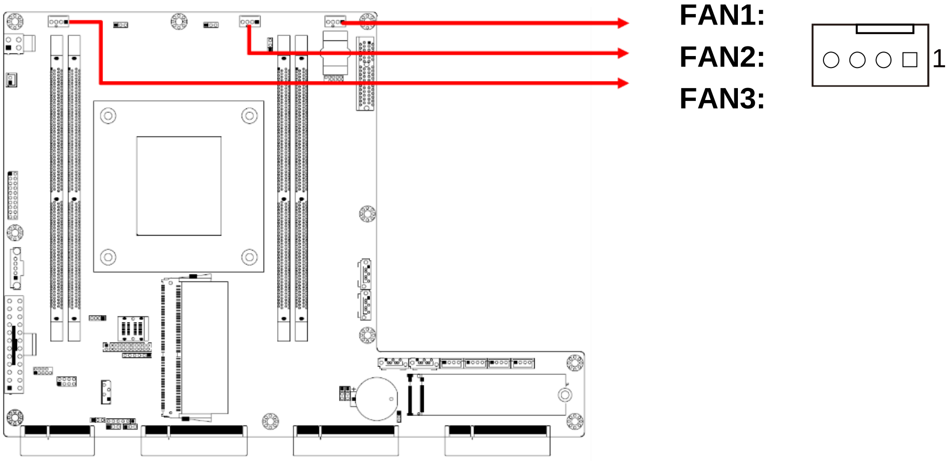
Pin	Signal Name	Pin	Signal Name
1	Ground	2	VCC5
3	INT0_SIOGP22	4	INT0_SIOGP25
5	INT0_SIOGP23	6	INT0_SIOGP26
7	INT0_SIOGP24	8	INT0_SIOGP27

2.6.6 IPMB Port (J15)



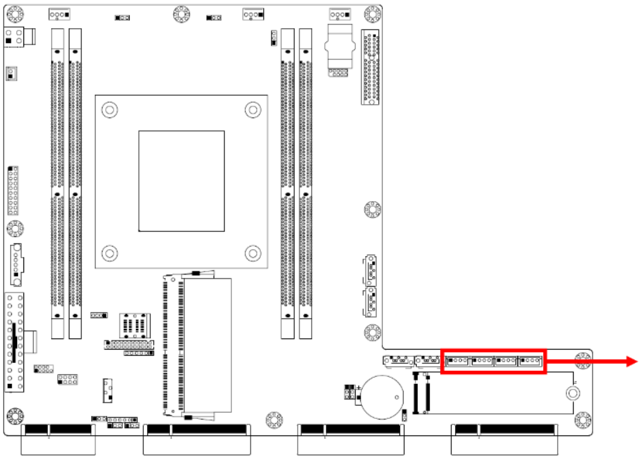
Pin	Signal Name	Pin	Signal Name
1	SMB_IPMB_STBY_LVC5_DATA	3	SMB_IPMB_STBY_LVC5_CLK
2	Ground	4	P5V_STBY

2.6.7 Fan Connector (FAN1, FAN2, FAN3)

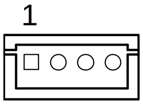


Pin	Signal Name	Pin	Signal Name
1	SYSFAN_G	3	SYSFAN_RPM
2	SYSFAN_12V	4	SYSFAN_PWM

2.6.8 SATA Power Connector (SATAPWR14, SATAPWR24, SATAPWR34, SATAPWR44)

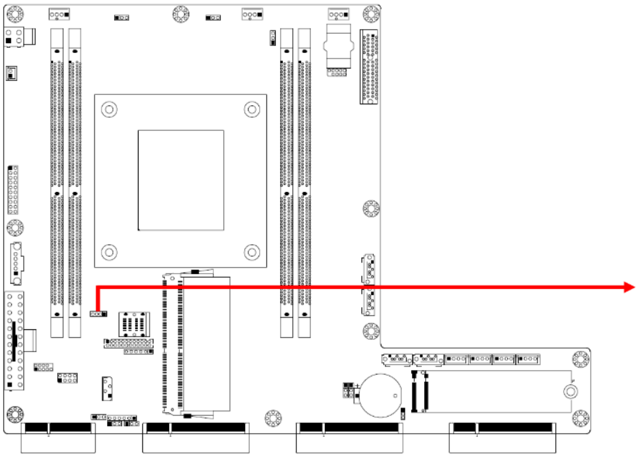


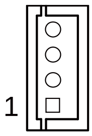
(From left to right)
SATAPWR14
SATAPWR24
SATAPWR34
SATAPWR44



Pin	Signal Name	Pin	Signal Name
1	VCC5	3	Ground
2	Ground	4	VCC12

2.6.9 SATA RAID Key (J5)





Pin	Signal Name	Pin	Signal Name
1	Ground	3	Ground
2	P3V3_AUX	4	SATA_RAID_KEY

Chapter 3
BIOS Setup

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

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

3.1 Introduction

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

3.2 BIOS Setup

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

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

The following message will appear on the screen:

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

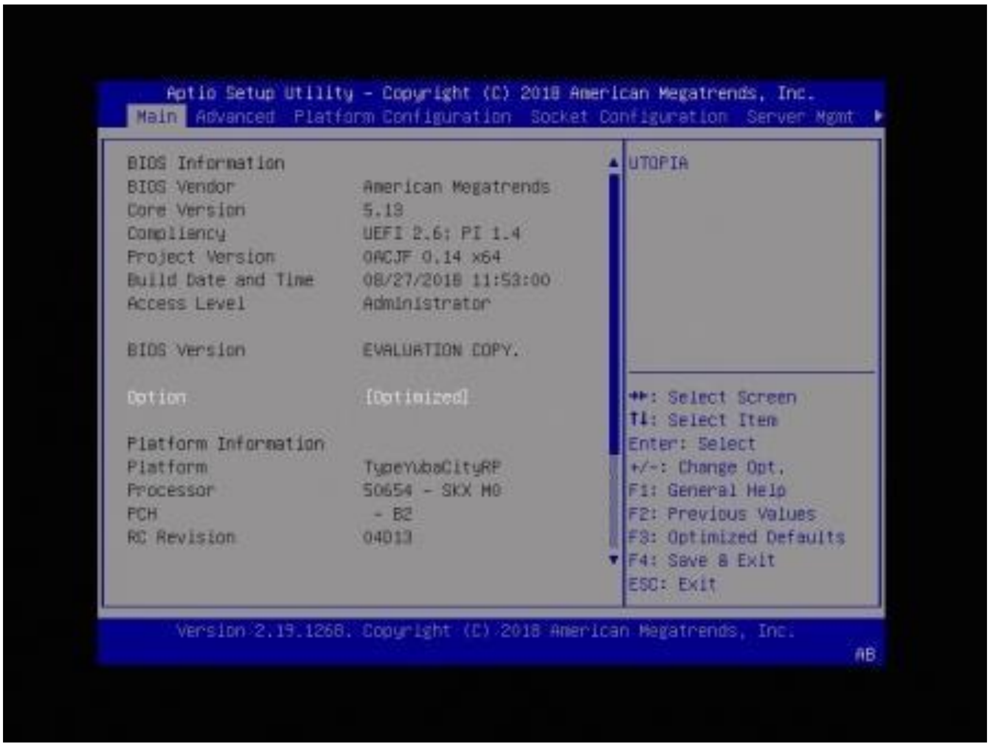
In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

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

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

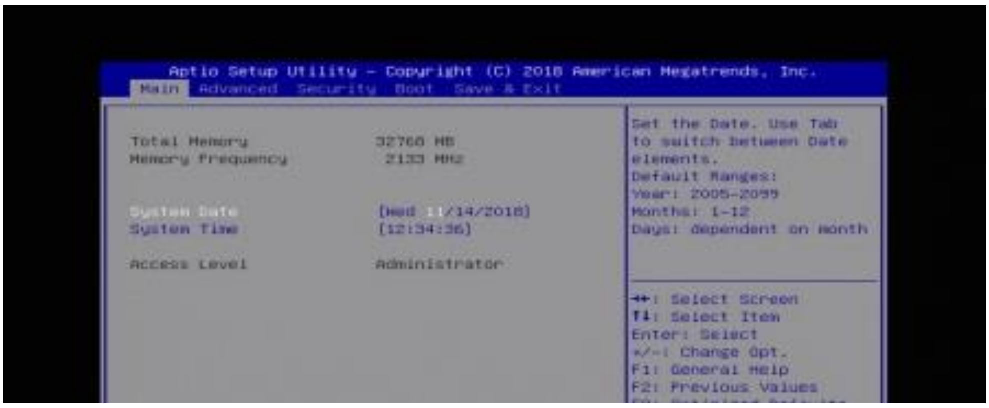
These defaults have been carefully chosen by both AMI and your system manufacturer to provide the absolute maximum performance and reliability. Changing the defaults could make the system unstable and crash in some cases.

3.3 Main Settings



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
 Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt ►

 BIOS Information                                    ▲ UTOPIA
 BIOS Vendor              American Megatrends
 Core Version             5.13
 Compliancy               UEFI 2.6; PI 1.4
 Project Version          0ACJF 0.14 x64
 Build Date and Time      08/27/2018 11:53:00
 Access Level             Administrator

 BIOS Version             EVALUATION COPY.

 Option                   [Optimized]                  ↔: Select Screen
                                                       ↑↓: Select Item
 Platform Information                                  Enter: Select
 Platform                 TypeYubaCityRP               +/-: Change Opt.
 Processor                50654 - SKX M0               F1: General Help
 PCH                       - B2                        F2: Previous Values
 RC Revision              04013                        F3: Optimized Defaults
                                                     ▼ F4: Save & Exit
                                                       ESC: Exit

        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                     AB
```

BIOS Setting	Description
Option	UTOPIA. Allows you to choose Optimized or Show All Items.

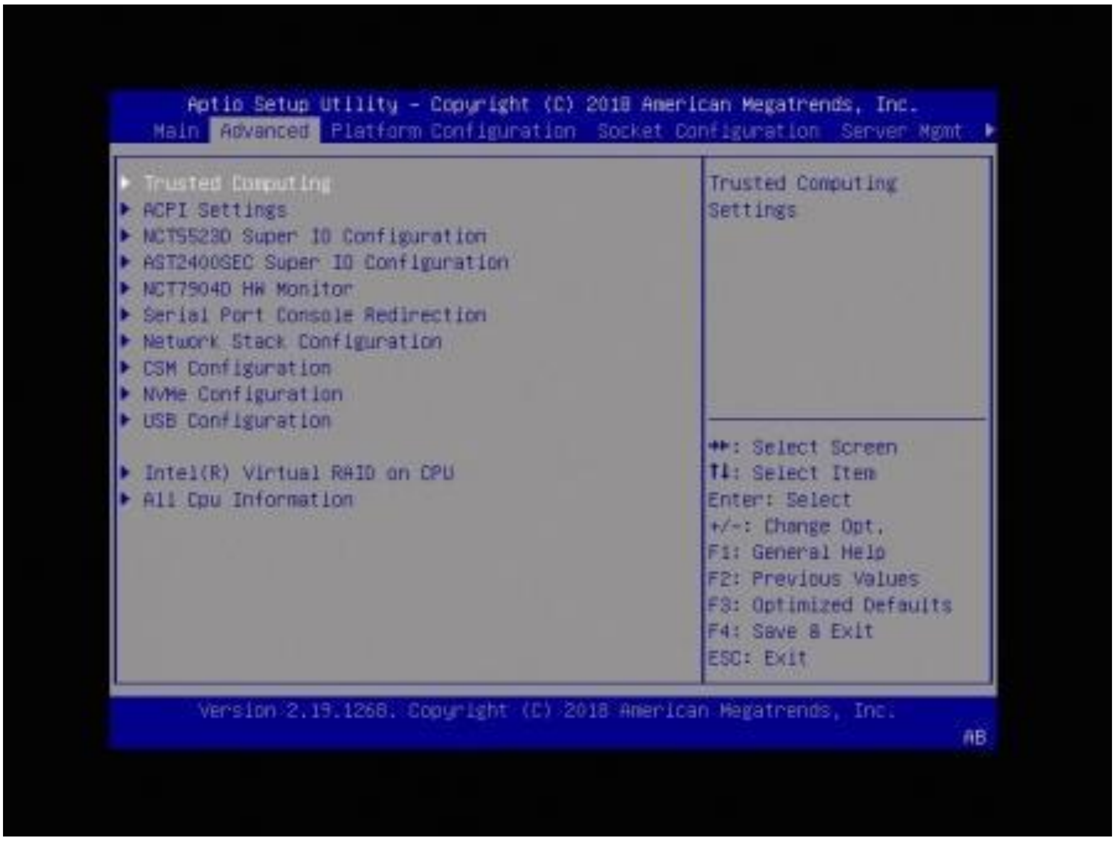


```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
 Main  Advanced  Security  Boot  Save & Exit

                                              Set the Date. Use Tab
 Total Memory             32768 MB            to switch between Date
 Memory Frequency          2133 MHz           elements.
                                              Default Ranges:
                                              Year: 2005-2099
 System Date              [Wed 11/14/2018]    Months: 1-12
 System Time              [12:34:36]          Days: dependent on month

 Access Level             Administrator

                                              ↔: Select Screen
                                              ↑↓: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              F1: General Help
                                              F2: Previous Values
```

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

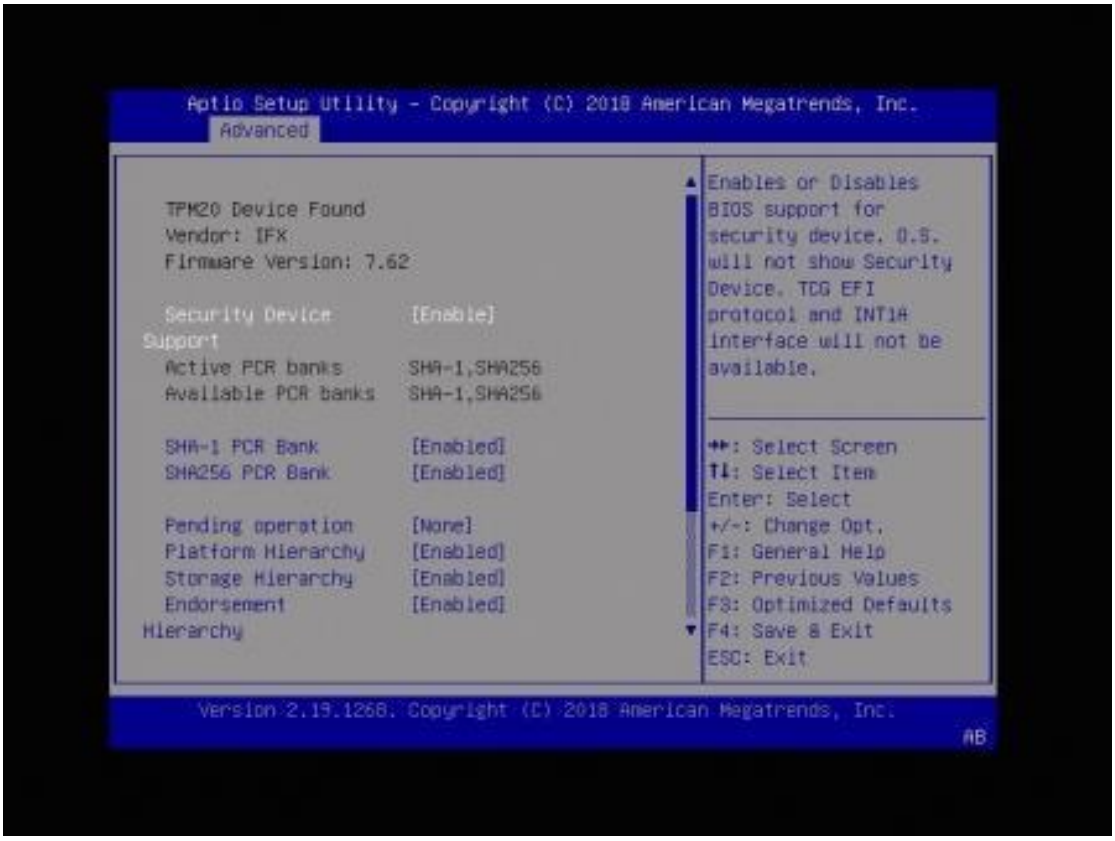
3.4 Advanced Settings

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



```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  ▶

 ▶ Trusted Computing                                  Trusted Computing
 ▶ ACPI Settings                                      Settings
 ▶ NCT5523D Super IO Configuration
 ▶ AST2400SEC Super IO Configuration
 ▶ NCT7904D HW Monitor
 ▶ Serial Port Console Redirection
 ▶ Network Stack Configuration
 ▶ CSM Configuration
 ▶ NVMe Configuration
 ▶ USB Configuration
                                                      ↔: Select Screen
 ▶ Intel(R) Virtual RAID on CPU                       ↑↓: Select Item
 ▶ All Cpu Information                                Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

         Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                          AB
```

3.4.1 Trusted Computing

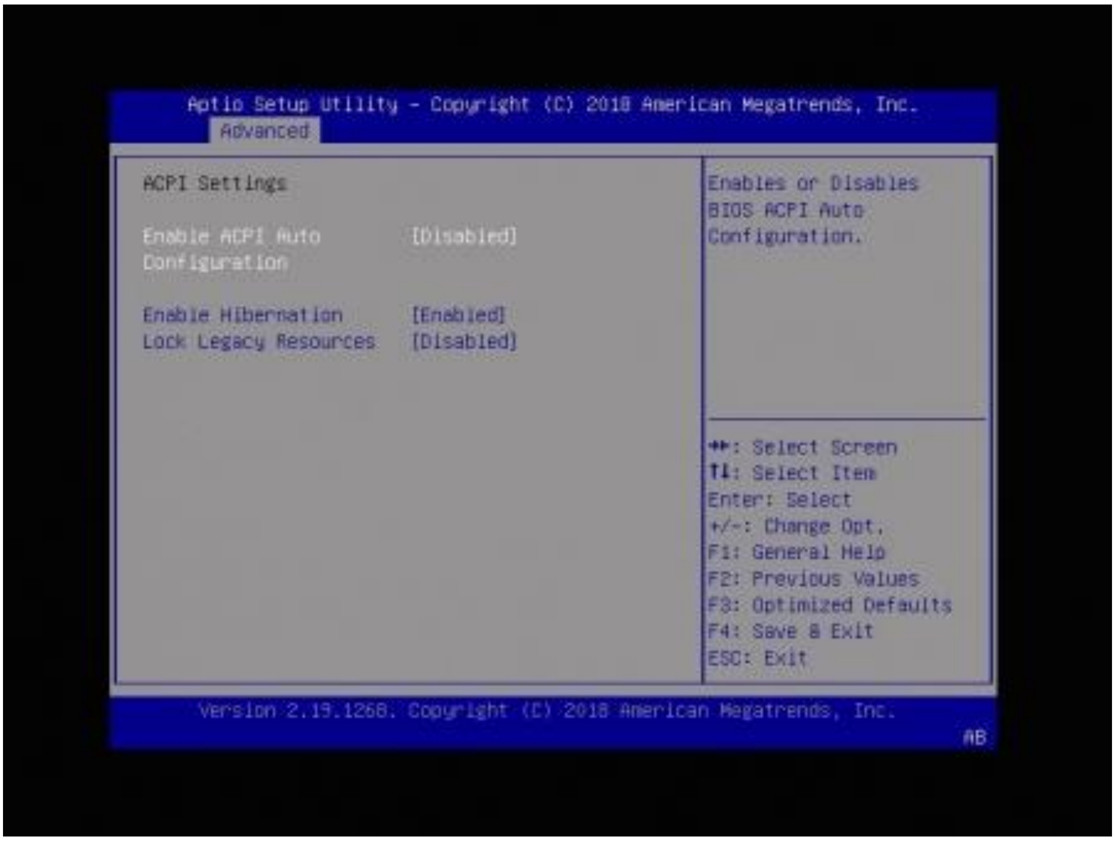


```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
              Advanced

    TPM20 Device Found                          Enables or Disables
    Vendor: IFX                                 BIOS support for
    Firmware Version: 7.62                      security device. O.S.
                                                will not show Security
    Security Device        [Enable]             Device. TCG EFI
  Support                                       protocol and INT1A
    Active PCR banks       SHA-1,SHA256         interface will not be
    Available PCR banks    SHA-1,SHA256         available.

    SHA-1 PCR Bank         [Enabled]            →←: Select Screen
    SHA256 PCR Bank        [Enabled]            ↑↓: Select Item
                                                Enter: Select
    Pending operation      [None]               +/-: Change Opt.
    Platform Hierarchy     [Enabled]            F1: General Help
    Storage Hierarchy      [Enabled]            F2: Previous Values
    Endorsement            [Enabled]            F3: Optimized Defaults
  Hierarchy                                     F4: Save & Exit
                                                ESC: Exit

        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. The operating system will not show the security device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank	Enables / Disables SHA-1 PCR Bank.
SHA256 PCR Bank	Enables / Disables SHA256 PCR Bank
Pending Operation	Schedule an operation for the security device. Note: Your computer will reboot during restart in order to change state of security device. Options: None, TPM Clear
Platform Hierarchy	Enables / Disables Platform Hierarchy.
Storage Hierarchy	Enables / Disables Storage Hierarchy.
Endorsement Hierarchy	Enables / Disables Endorsement Hierarchy.
TPM 2.0 UEFI Spec Version	Select the TCG2, the new TCG2 protocol.

BIOS Setting	Description
Physical Pressence Spec Version	The operating system will support the PPI spec version 1.2 or 1.3 on the basis of the version you choose. Note: Some HCK tests might not support 1.3.
Device Select	TPM “1.2” or “2.0” will restrict support to TPM “1.2” or “2.0” devices. “Auto” will support both with the default sest to TPM2.0 devices if not found.

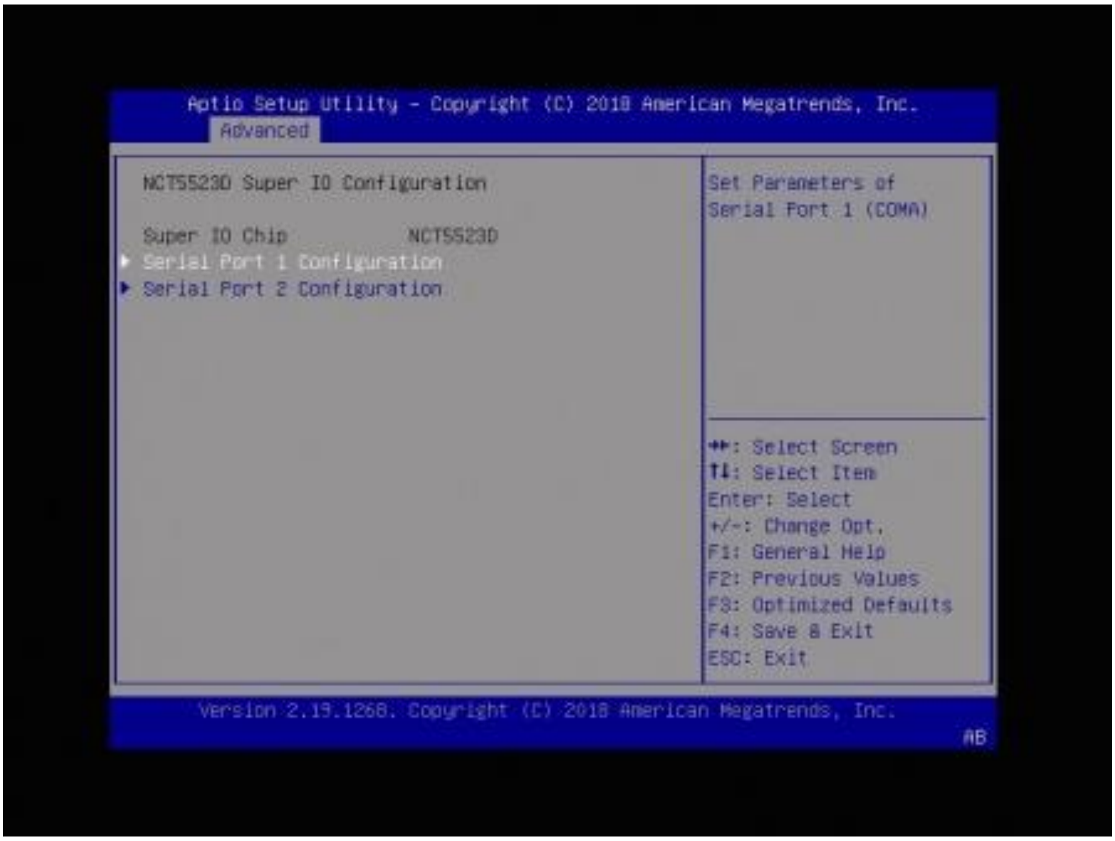
3.4.2 ACPI Settings



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

ACPI Settings                                   Enables or Disables
                                                BIOS ACPI Auto
Enable ACPI Auto           [Disabled]           Configuration.
Configuration

Enable Hibernation         [Enabled]
Lock Legacy Resources      [Disabled]

                                                ↔: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/-: Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Enable ACPI Auto Configuration	Enables / Disables BIOS ACPIU auto configuration.
Enable Hibernation	Enables / Disables the system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OS.
Lock Legacy Resources	Enables / Disables Lock of Legacy Resources.

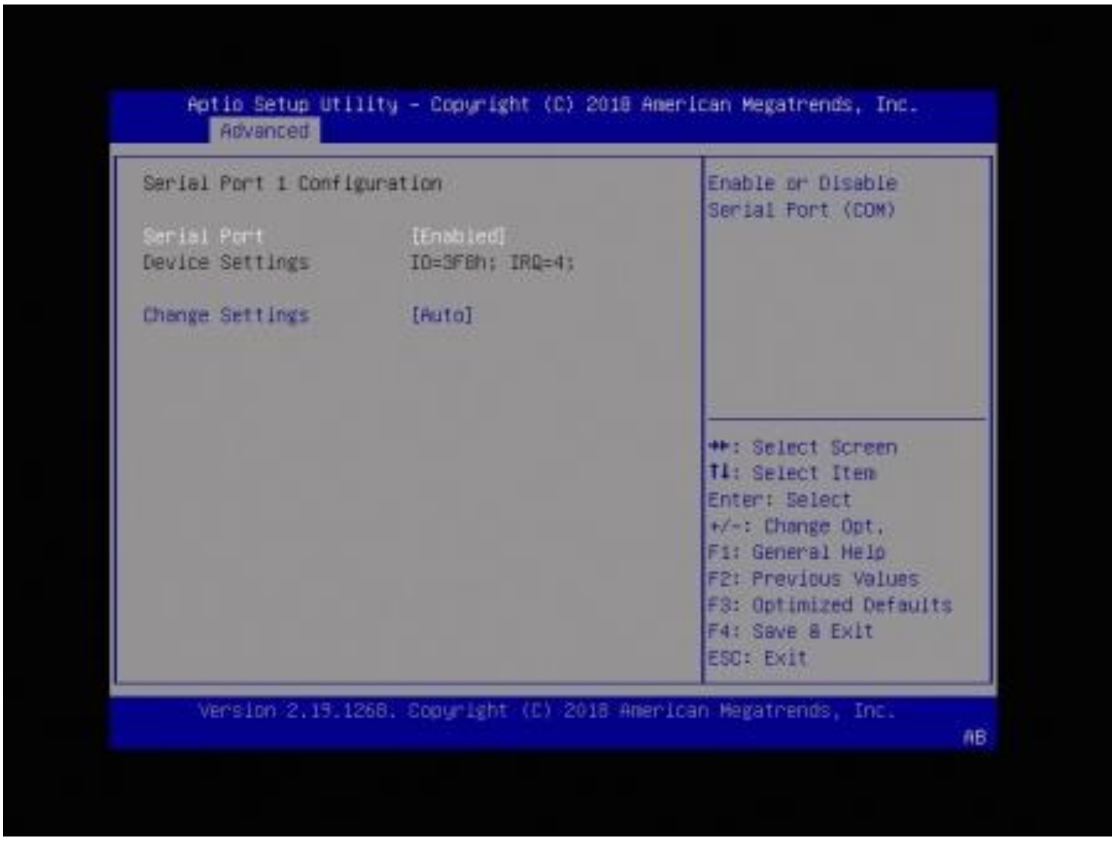
3.4.3 NCT5523D Super I/O Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

NCT5523D Super IO Configuration              Set Parameters of
                                             Serial Port 1 (COMA)
Super IO Chip            NCT5523D
▶ Serial Port 1 Configuration
▶ Serial Port 2 Configuration
                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                              AB
```

BIOS Setting	Description
Serial Ports Configuration	Sets Parameters of Serial Ports. You can enable / disable the serial port and select an optimal settings for the Super IO device.

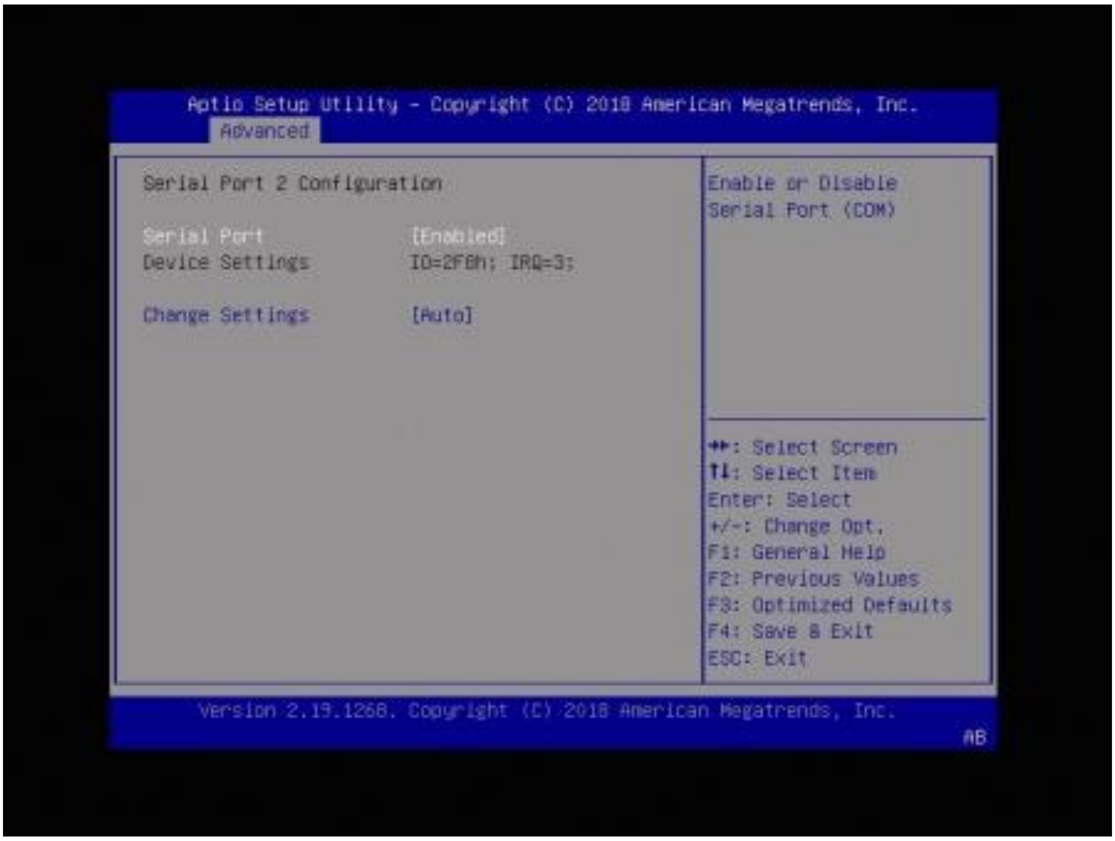
3.4.3.1. Serial Port 1 Configuration



```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
           Advanced

  Serial Port 1 Configuration                  Enable or Disable
                                               Serial Port (COM)
  Serial Port              [Enabled]
  Device Settings          IO=3F8h; IRQ=4;

  Change Settings          [Auto]

                                               →←: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit

        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                     AB
```

BIOS Setting	Description
Serial Port	Sets parameters of Serial Ports (COM).
Change Settings	Selects an optimal settings for the Super I/O device. Options: • Auto • IO=3F8h ; IRQ=4 • IO=3F8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=2F8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=3E8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=2E8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12

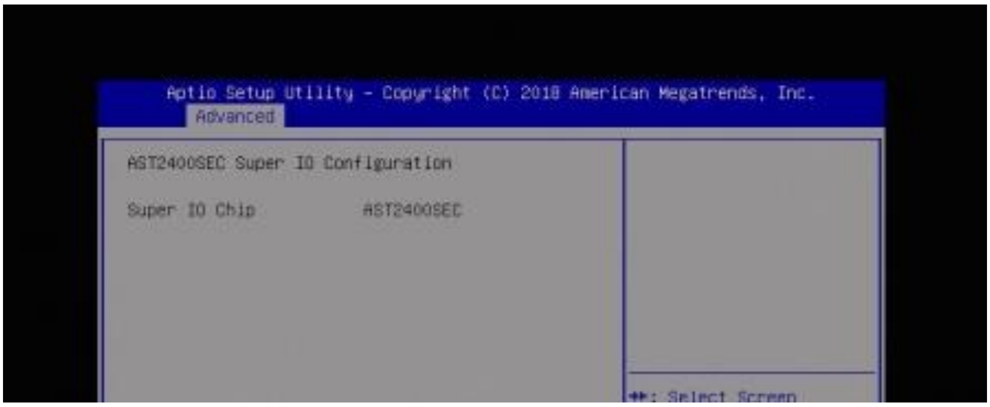
3.4.3.2. Serial Port 2 Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

Serial Port 2 Configuration                        Enable or Disable
                                                   Serial Port (COM)
Serial Port               [Enabled]
Device Settings           IO=2F8h; IRQ=3;

Change Settings           [Auto]

                                                   ↔: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                  AB
```

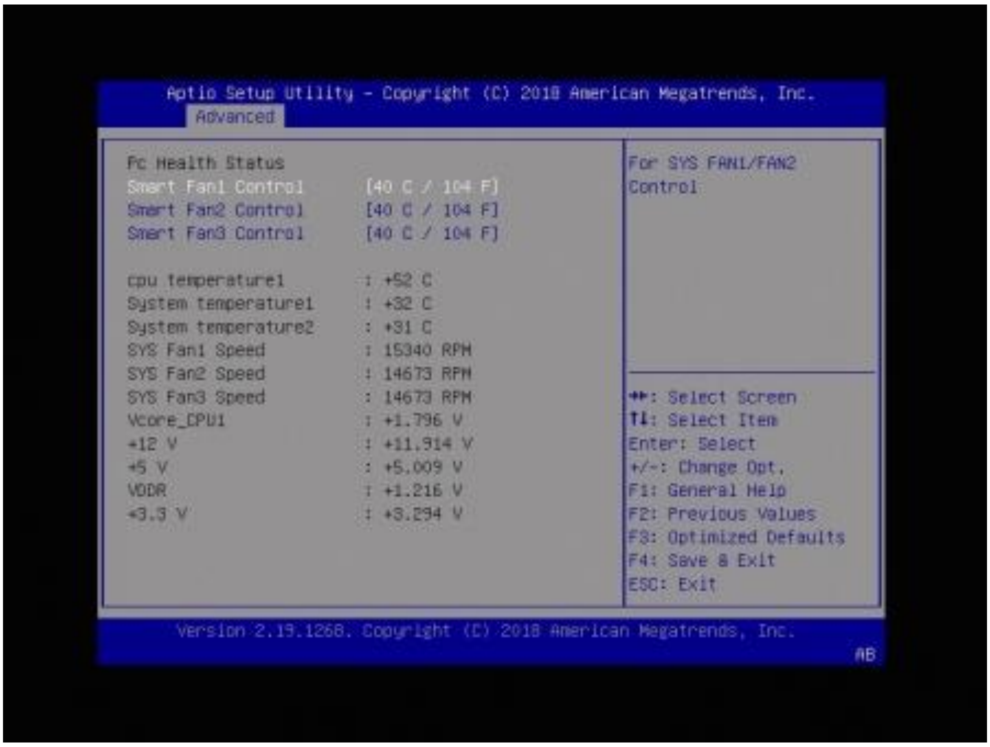
BIOS Setting	Description
Serial Port	Sets parameters of Serial Ports (COM).
Change Settings	Selects an optimal settings for the Super I/O device. Options: • Auto • IO=2F8h ; IRQ=3 • IO=3F8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=2F8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=3E8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12 • IO=2E8h ; IRQ=3, 4, 5, 6, 7, 9. 10, 11, 12

3.4.4 AST2400SEC Super I/O Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
     Advanced

AST2400SEC Super IO Configuration

Super IO Chip            AST2400SEC

                                                ++: Select Screen
```

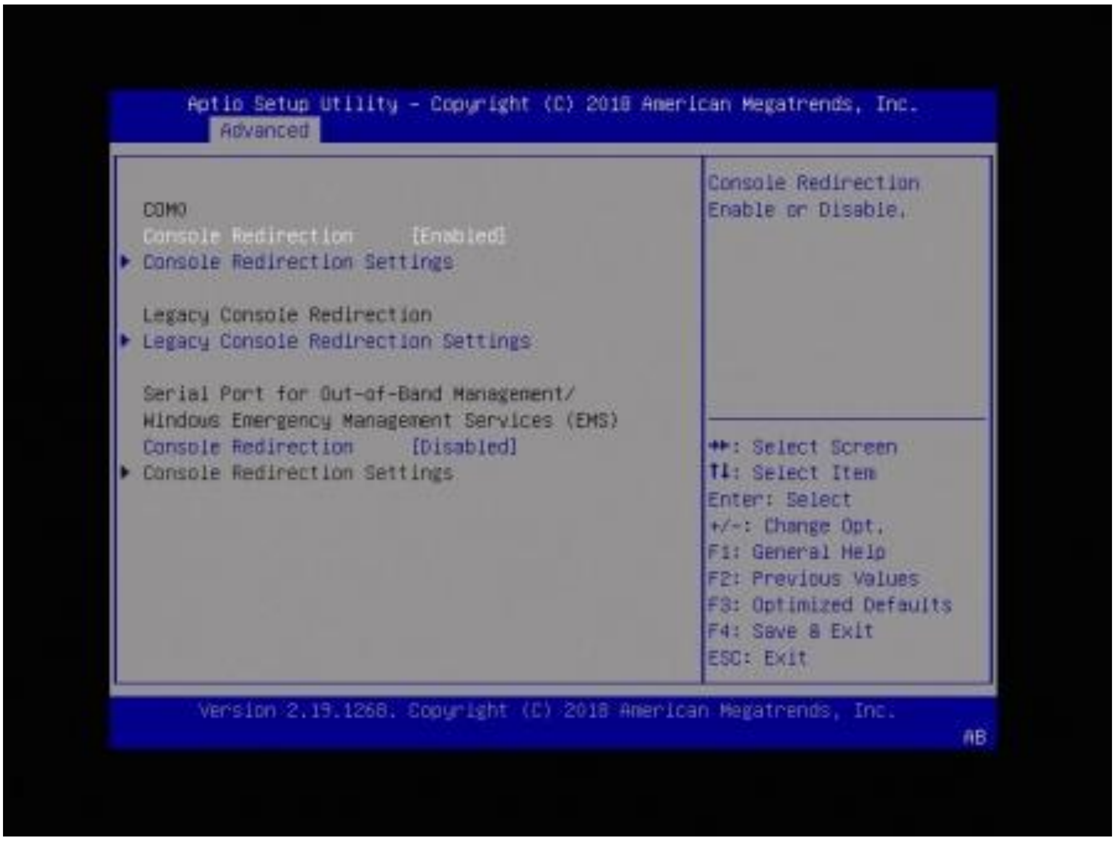
3.4.5 NCT7904D HW Monitor



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
     Advanced

Pc Health Status                                For SYS FAN1/FAN2
Smart Fan1 Control        [40 C / 104 F]        Control
Smart Fan2 Control        [40 C / 104 F]
Smart Fan3 Control        [40 C / 104 F]

cpu temperature1          : +52 C
System temperature1       : +32 C
System temperature2       : +31 C
SYS Fan1 Speed            : 15340 RPM
SYS Fan2 Speed            : 14673 RPM
SYS Fan3 Speed            : 14673 RPM           ++: Select Screen
Vcore_CPU1                : +1.796 V            ↑↓: Select Item
+12 V                     : +11.914 V           Enter: Select
+5 V                      : +5.009 V            +/-: Change Opt.
VDDR                      : +1.216 V            F1: General Help
+3.3 V                    : +3.294 V            F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                AB
```

BIOS Setting	Description
Smart Fans Control	This field enables or disables the smart fan control Options: Disabled, 40°C, 45°C, 50°C, 55°C
Temperatures / Voltages / Fan Speed	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only as monitored by the system and showing the PC health status

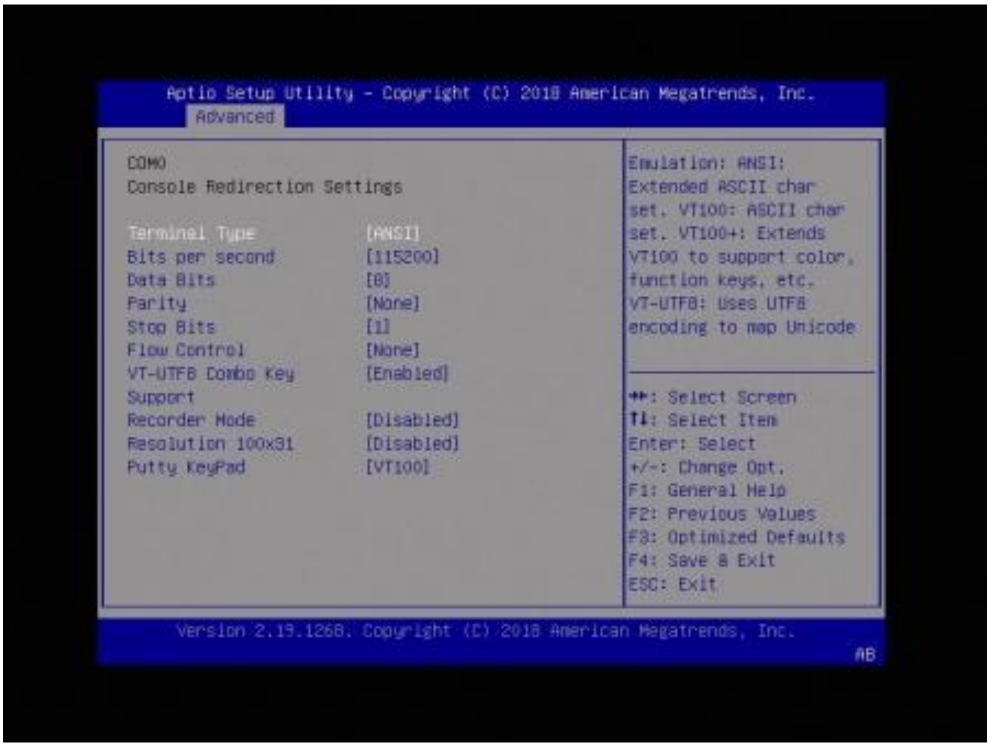
3.4.6 Serial Port Console Redirection



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
        Advanced

  COM0                                        Console Redirection
  Console Redirection        [Enabled]        Enable or Disable.
▶ Console Redirection Settings

  Legacy Console Redirection
▶ Legacy Console Redirection Settings

  Serial Port for Out-of-Band Management/
  Windows Emergency Management Services (EMS)
  Console Redirection        [Disabled]       →←: Select Screen
▶ Console Redirection Settings                ↑↓: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              F1: General Help
                                              F2: Previous Values
                                              F3: Optimized Defaults
                                              F4: Save & Exit
                                              ESC: Exit

     Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                  AB
```

BIOS Setting	Description
Console Redirection	Enables / Disables Console Redirection.
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. Sets parameters of Console Redirection.
Legacy Console Redirection Settings	Allows you to configure the legacy console redirection settings.
Console Redirection	Enables / Disables console redirection.

3.4.6.1. Console Redirection Settings

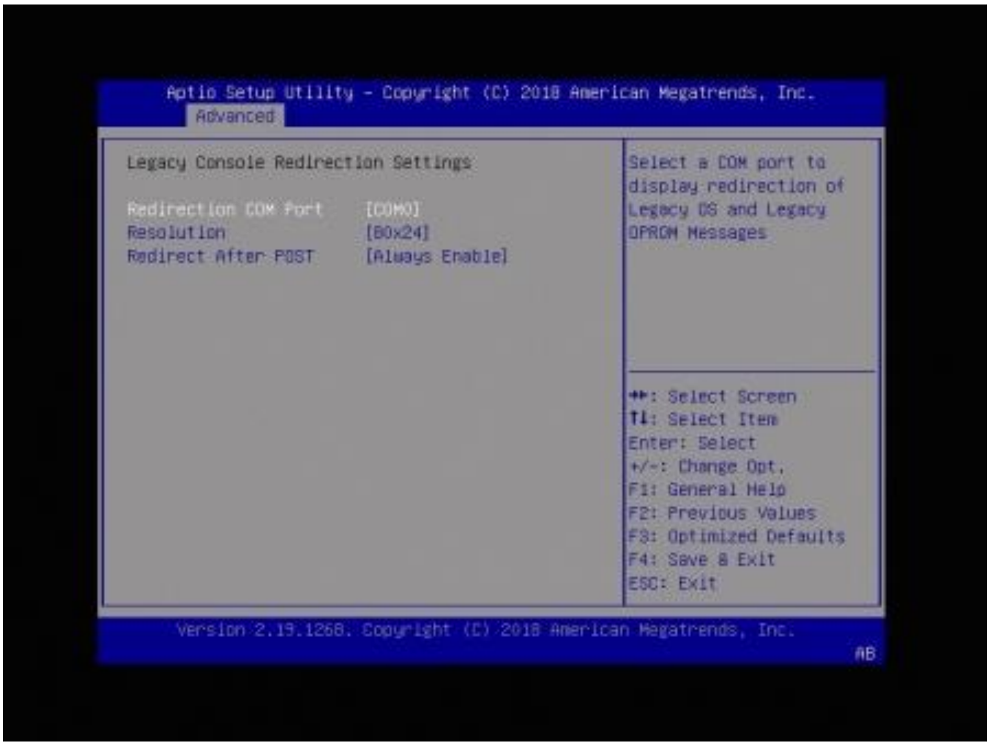


```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
  Advanced

COM0                                       Emulation: ANSI:
Console Redirection Settings               Extended ASCII char
                                           set. VT100: ASCII char
Terminal Type            [ANSI]            set. VT100+: Extends
Bits per second          [115200]          VT100 to support color,
Data Bits                [8]               function keys, etc.
Parity                   [None]            VT-UTF8: Uses UTF8
Stop Bits                [1]               encoding to map Unicode
Flow Control             [None]
VT-UTF8 Combo Key        [Enabled]
Support                                    ↔: Select Screen
Recorder Mode            [Disabled]        ↑↓: Select Item
Resolution 100x31        [Disabled]        Enter: Select
Putty KeyPad             [VT100]           +/-: Change Opt.
                                           F1: General Help
                                           F2: Previous Values
                                           F3: Optimized Defaults
                                           F4: Save & Exit
                                           ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                              AB
```

BIOS Setting	Description
Terminal Type	Emulation: **ANSI:** Extended ASCII charset. **VT100:** ASCII charset. **VT100+:** Extends VT100 to support color, function keys, etc. **VT-UTF8:** Uses UTF8 encoding to map Unicode.
Bits per second	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. Options: 9600, 19200, 38400, 57600, 115200
Data Bits	Options: 7, 8
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. Options: 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. Options: 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. Options: None, Hardware RTS/CTS

BIOS Setting	Description
VT-VTF8 Combo Key Support	Enables / Disables VT-UTFB combination key support for ANSI/VT100 terminals.
Recorder Mode	With this mode enabled, only text will be sent. This is to capture terminal data.
Resolution 100x31	Enables / Disables extended terminal resolution.
Putty Key pad	Select FunctionKey and keyPad on Putty. Options: VT100, LINUX, XTERMR6, SC0, ESCN, VT400

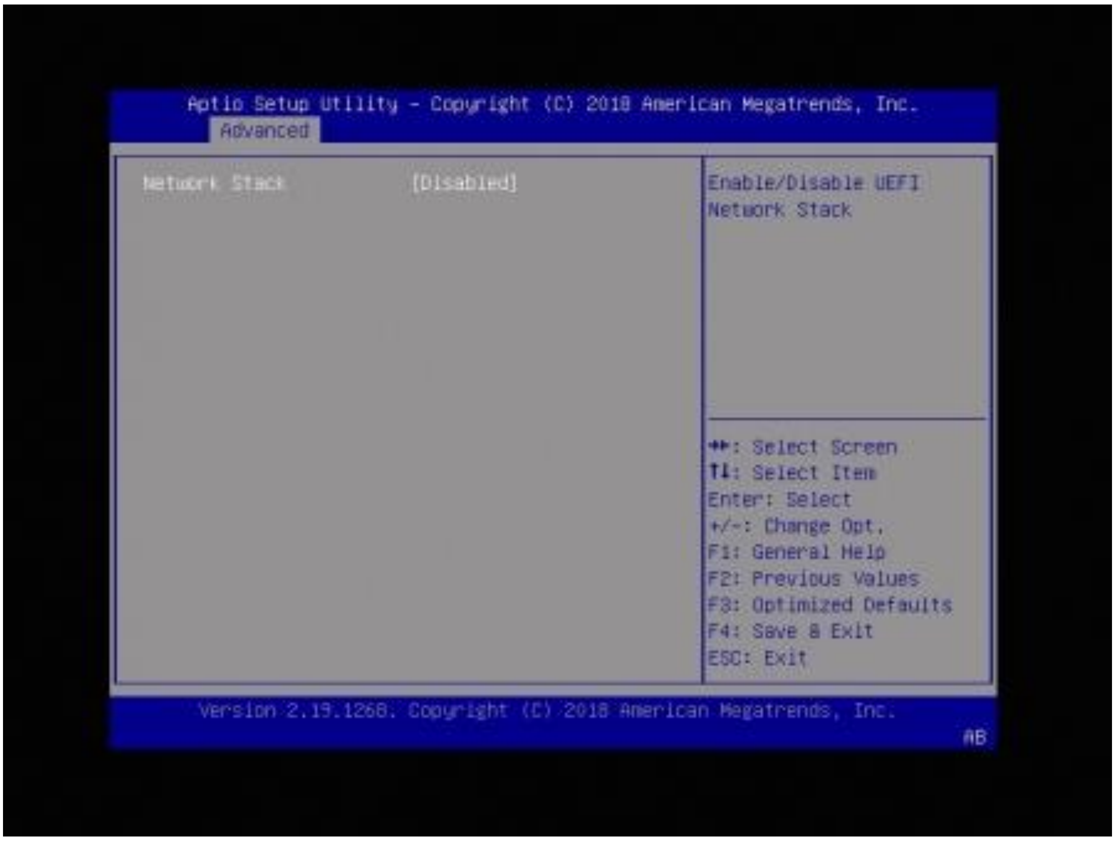
3.4.6.2. Legacy Console Redirection Settings



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
    Advanced

  Legacy Console Redirection Settings                  Select a COM port to
                                                       display redirection of
  Redirection COM Port       [COM0]                    Legacy OS and Legacy
  Resolution                 [80x24]                   OPROM Messages
  Redirect After POST        [Always Enable]

                                                       ←→: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit

         Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                       AB
```

BIOS Setting	Description
Redirection COM Port	Selects a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
Resolution	On Legacy OS, the number of rows and columns supported redirection. Options: 80x24, 80x25
Redirect After POST	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. Options: Always Enable, Bootloader

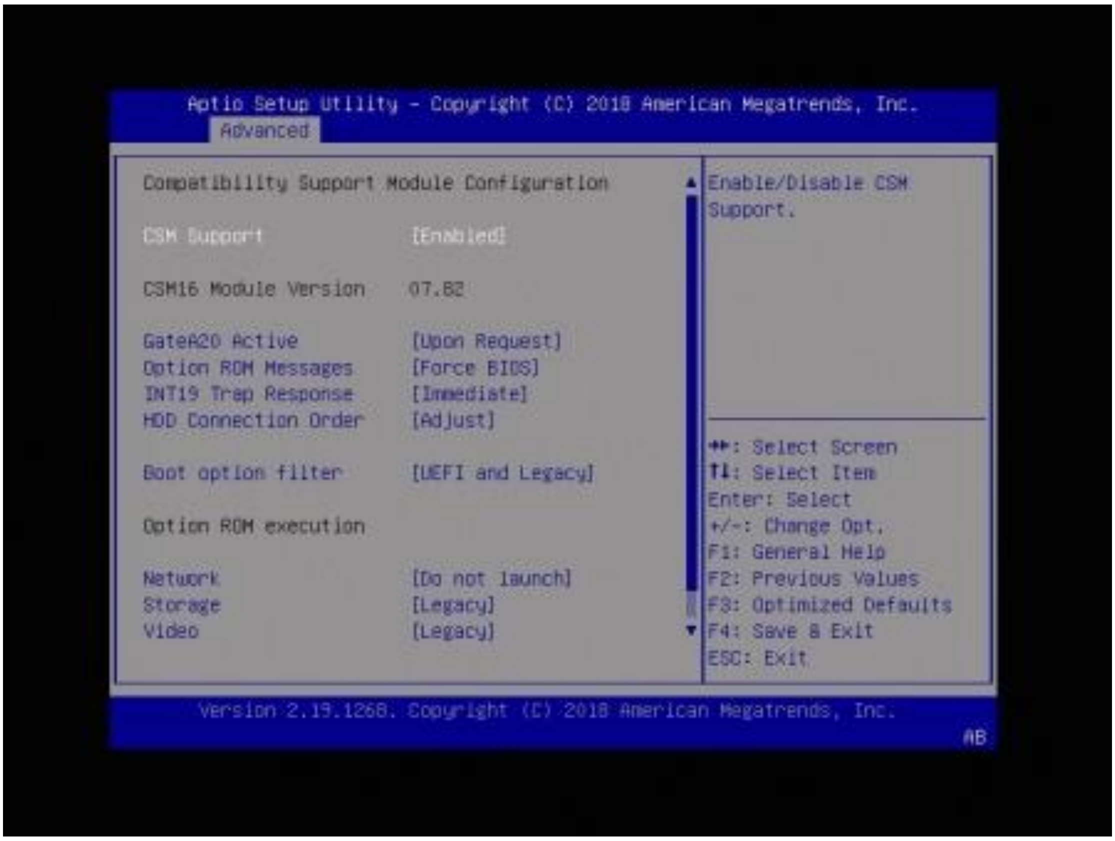
3.4.7 Network Stack Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

Network Stack            [Disabled]          Enable/Disable UEFI
                                             Network Stack

                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                              AB
```

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

3.4.8 CSM Configuration

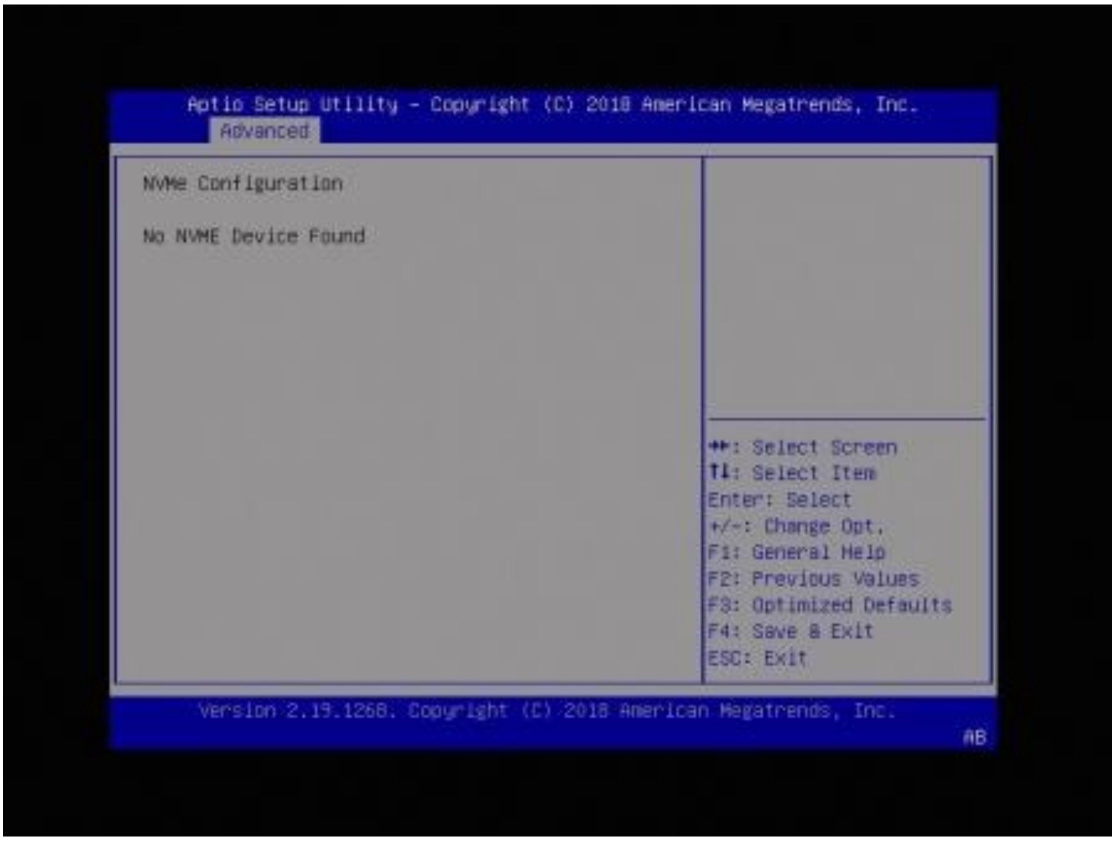


```
          Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
            Advanced

  Compatibility Support Module Configuration        Enable/Disable CSM
                                                    Support.
  CSM Support              [Enabled]

  CSM16 Module Version     07.82

  GateA20 Active           [Upon Request]
  Option ROM Messages      [Force BIOS]
  INT19 Trap Response      [Immediate]
  HDD Connection Order     [Adjust]
                                                    ←→: Select Screen
  Boot option filter       [UEFI and Legacy]        ↑↓: Select Item
                                                    Enter: Select
  Option ROM execution                              +/-: Change Opt.
                                                    F1: General Help
  Network                  [Do not launch]          F2: Previous Values
  Storage                  [Legacy]                 F3: Optimized Defaults
  Video                    [Legacy]                 F4: Save & Exit
                                                    ESC: Exit

          Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                         AB
```

BIOS Setting	Description
CSM Support	Enables / Disables CSM support.
GateA20 Active	**Upon Request** disables GA20 when using BIOS services. **Always** cannot disable GA20, but is useful when any RT code is executed above 1 MB.
Option ROM Messages	Sets display mode for Option ROM. Options: Force BIOS, Keep Current
INT19 Trap Response	BIOS reaction on INT19 trapping by Option ROM. • Immediate executes the trap right away. • Postponed executes the trap during legacy boot.
HDD Connection Order	Some OS require HDD handles to be adjusted, i.e. OS is installed on drive 80h. Options: Adjust, Keep
Boot option filter	Controls the priority of Legacy and UEFI ROMs. Options: UEFI and Legacy, Legacy only, UEFI only
Network	Controls the execution of UEFI and Legacy Network OpROM. Options: Do not launch, UEFI, Legacy

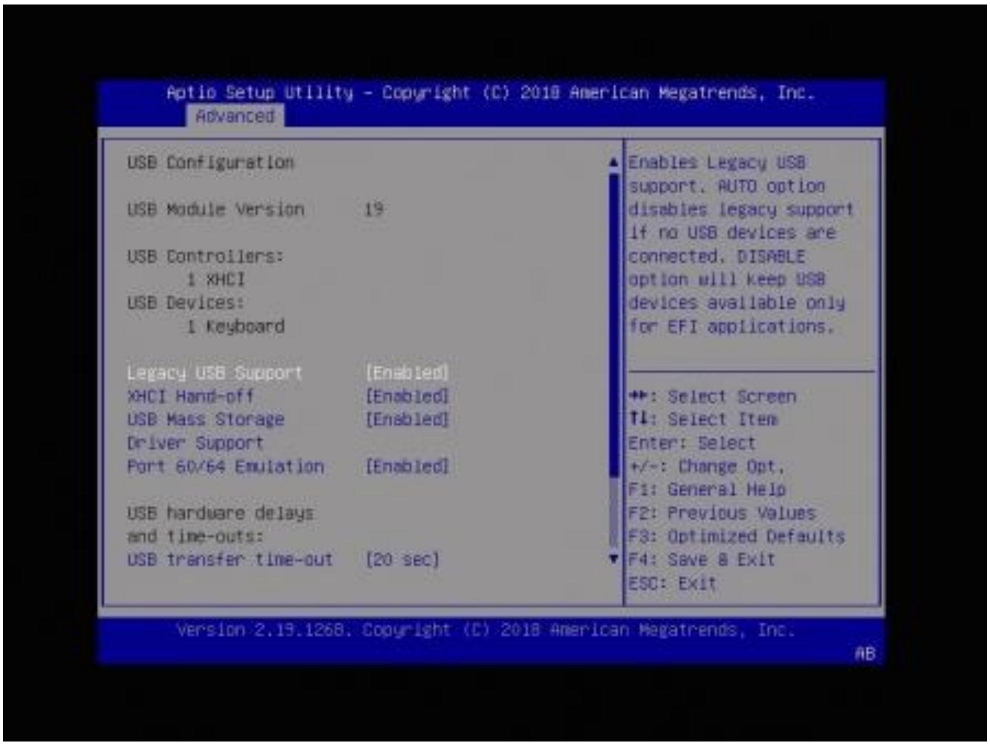
BIOS Setting	Description
Storage	Controls the execution of UEFI and Legacy Storage OpROM. Options: Do not lanuch, UEFI, Legacy
Video	Controls the execution of UEFI and Legacy Video OpROM. Options: Do not lanuch, UEFI, Legacy
Other PCI devices	Determines OpROM execution policy for devices other than network, storage or video. Options: Do not lanuch, UEFI, Legacy

3.4.9 NVMe Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

NVMe Configuration

No NVME Device Found

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
AB
```

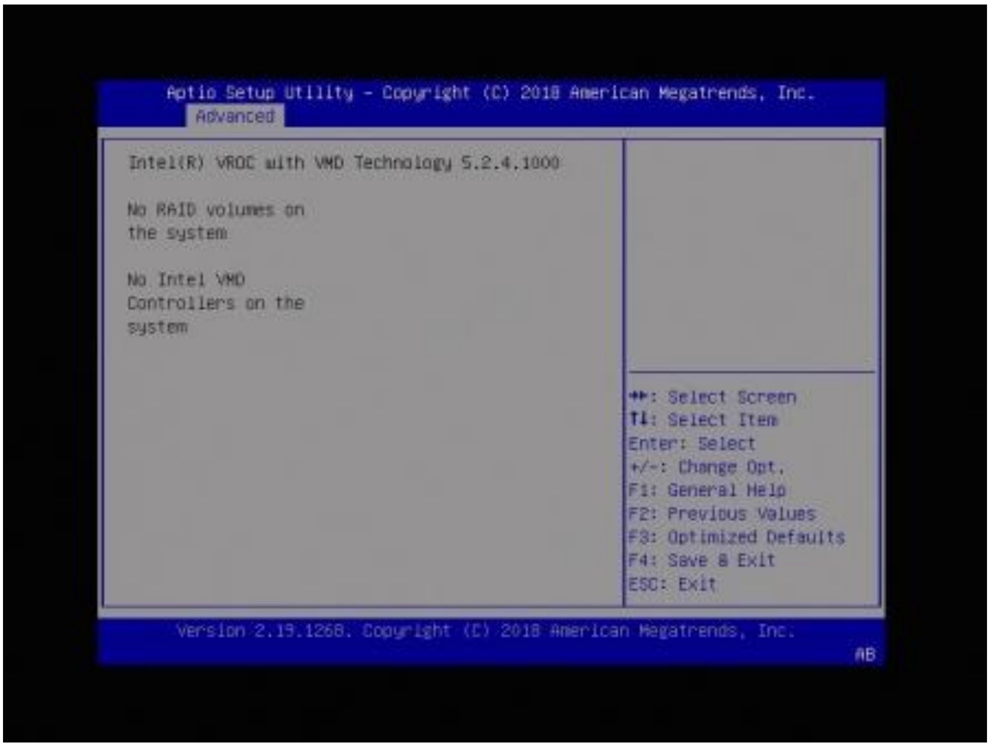
3.4.10 USB Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
          Advanced
 USB Configuration                            ▲ Enables Legacy USB
                                                support. AUTO option
 USB Module Version        19                   disables legacy support
                                                if no USB devices are
 USB Controllers:                               connected. DISABLE
       1 XHCI                                   option will keep USB
 USB Devices:                                   devices available only
       1 Keyboard                               for EFI applications.

 Legacy USB Support        [Enabled]
 XHCI Hand-off             [Enabled]            ◄►: Select Screen
 USB Mass Storage          [Enabled]            ↑↓: Select Item
 Driver Support                                 Enter: Select
 Port 60/64 Emulation      [Enabled]            +/-: Change Opt.
                                                F1: General Help
 USB hardware delays                            F2: Previous Values
 and time-outs:                                 F3: Optimized Defaults
 USB transfer time-out     [20 sec]           ▼ F4: Save & Exit
                                                ESC: Exit
         Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
Legacy USB Support	Enables / Disables Legacy USB support. • **Auto** disables legacy support if there is no USB device connected. • **Disable** keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables USB mass storage driver support.
USB Transfer time-out	Sets the time-out value 1, 5, 10 or 20 sec(s) for Control, Bulk, and Interrupt transfers.
Device reset time-out	Sets the seconds (10, 20, 30, 40 secs) of delaying execution of start unit command to USB mass storage device.
Device power-up delay	The maximum time the device will take before it properly reports itself to the Host Controller. Auto uses default value for a Root port it is 100ms. But for a Hub port, the delay is taken from Hub descriptor. Options: Auto, Manual

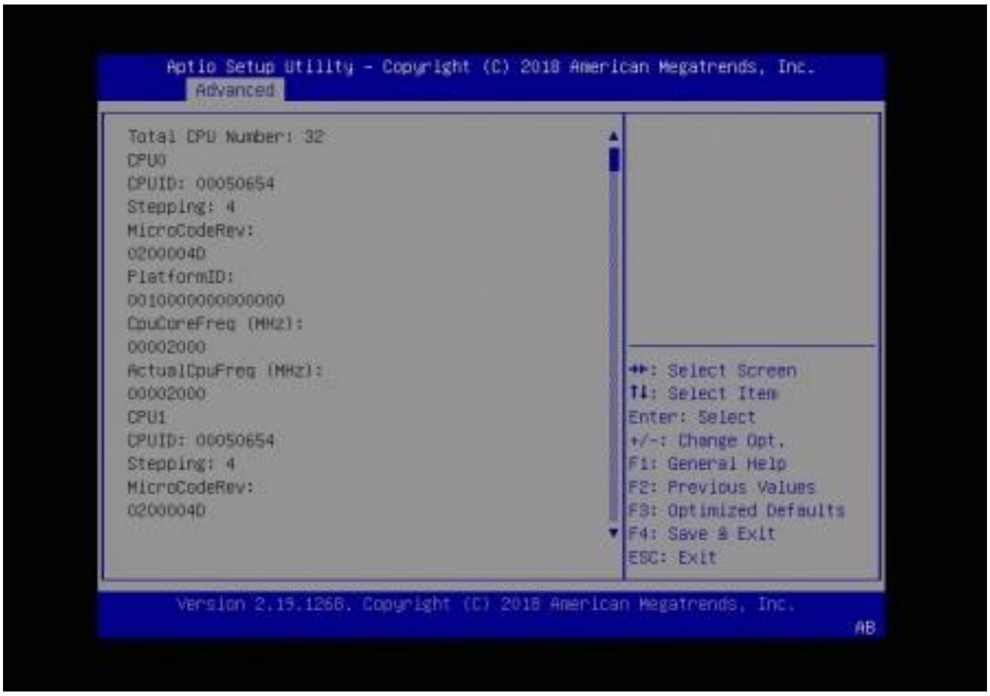
3.4.11 Intel(R) Virtual RAID on CPU



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

Intel(R) VROC with VMD Technology 5.2.4.1000

No RAID volumes on
the system

No Intel VMD
Controllers on the
system

                                         →←: Select Screen
                                         ↑↓: Select Item
                                         Enter: Select
                                         +/-: Change Opt.
                                         F1: General Help
                                         F2: Previous Values
                                         F3: Optimized Defaults
                                         F4: Save & Exit
                                         ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                            AB
```

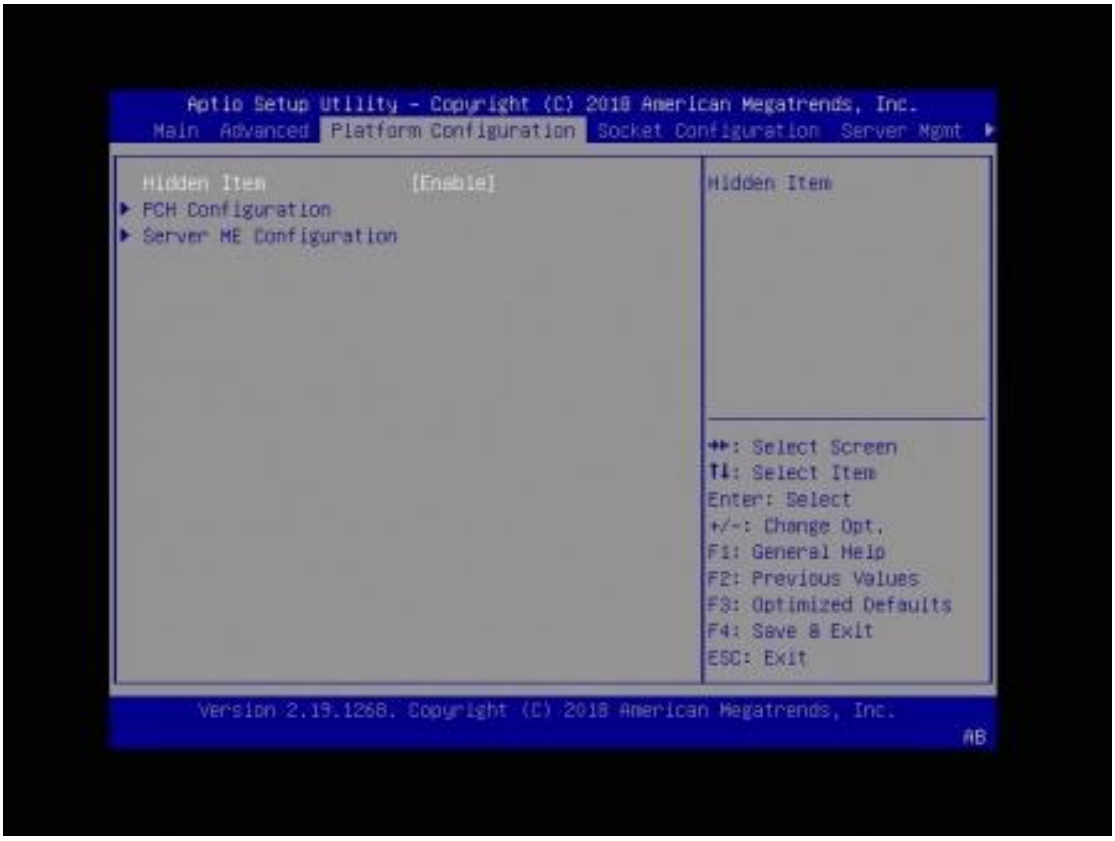
3.4.12 All CPU Information

Displays all your CPU information.



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Advanced

Total CPU Number: 32
CPU0
CPUID: 00050654
Stepping: 4
MicroCodeRev:
0200004D
PlatformID:
0010000000000000
CpuCoreFreq (MHz):
00002000
ActualCpuFreq (MHz):
00002000
CPU1
CPUID: 00050654
Stepping: 4
MicroCodeRev:
0200004D
                                         →←: Select Screen
                                         ↑↓: Select Item
                                         Enter: Select
                                         +/-: Change Opt.
                                         F1: General Help
                                         F2: Previous Values
                                         F3: Optimized Defaults
                                         F4: Save & Exit
                                         ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                            AB
```

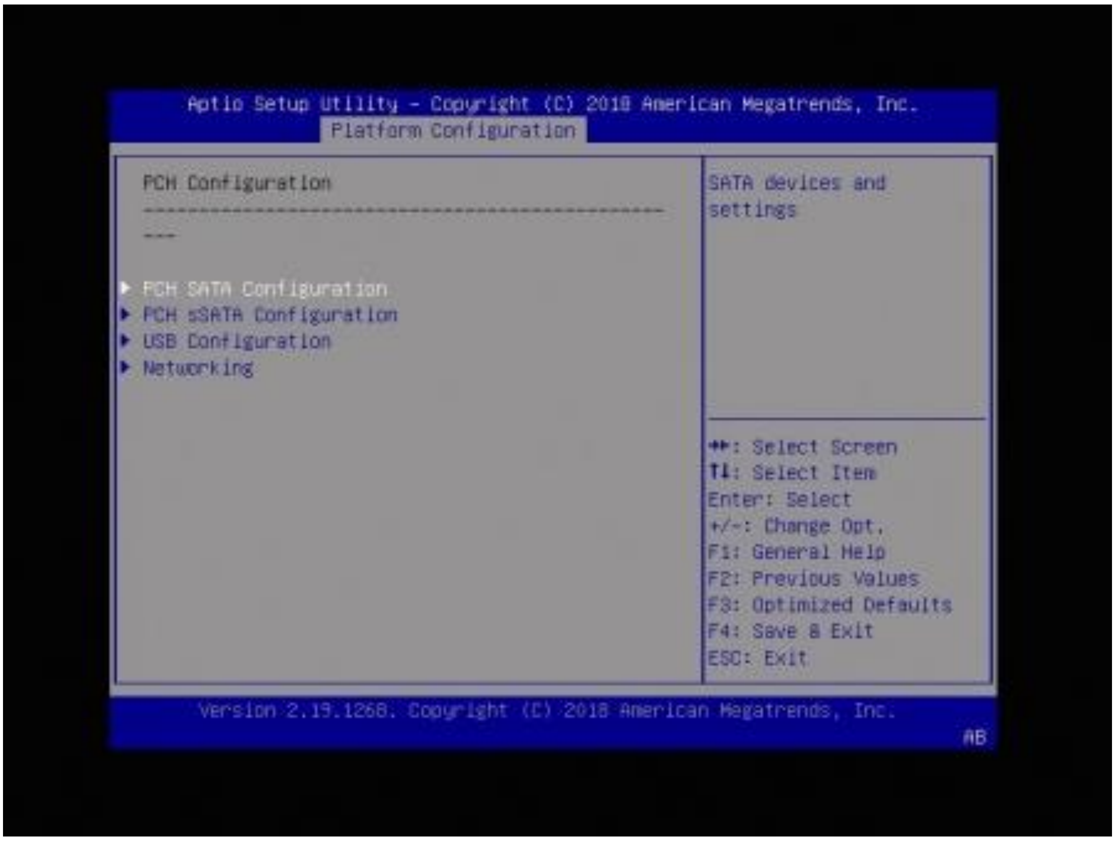
3.5 Platform Configuration



```
     Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
   Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt ▶

   Hidden Item             [Enable]          Hidden Item
 ▶ PCH Configuration
 ▶ Server ME Configuration

                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

       Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
Hidden Item	Enables / Disables the hidden items.
PCM Configuration	Displays and provides option to change the PCM settings.
Server ME Configfuration	Displays the ME configuration data.

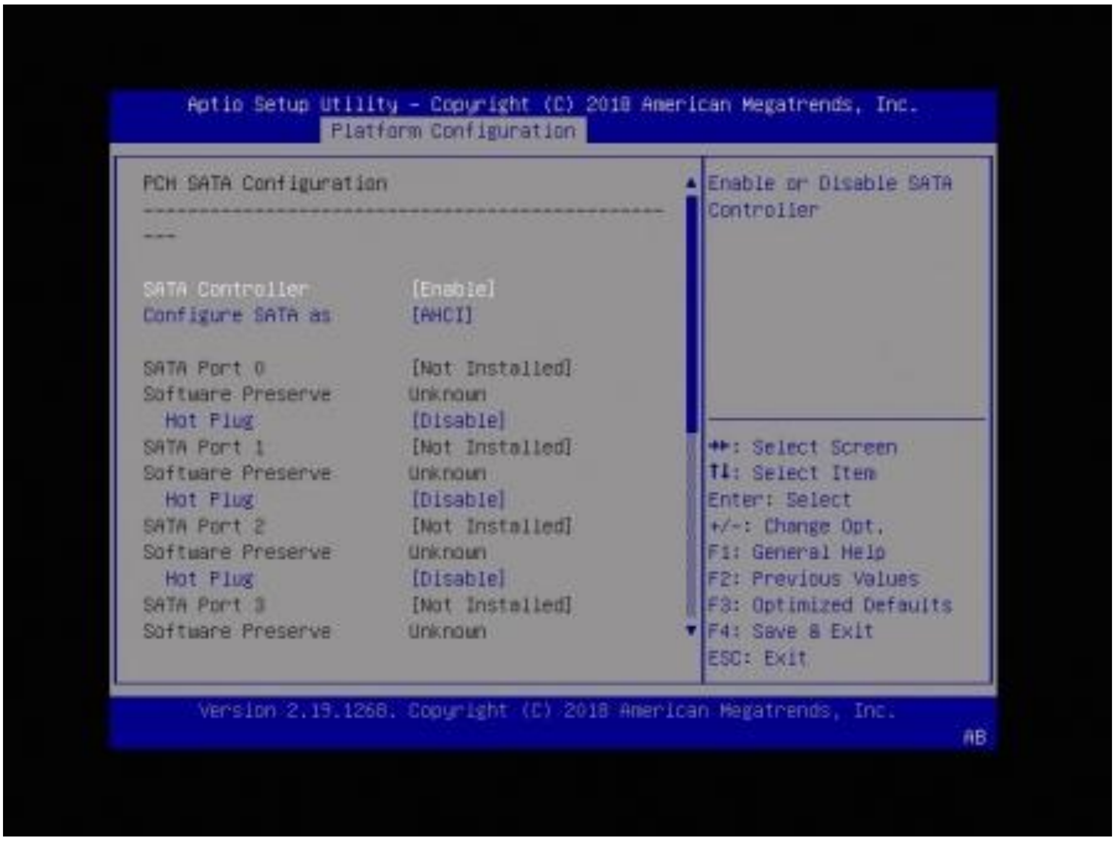
3.5.1 PCH Configuration



```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                         Platform Configuration
  PCH Configuration                                   | SATA devices and
  --------------------------------------------------- | settings
  ---                                                 |
                                                      |
▶ PCH SATA Configuration                              |
▶ PCH sSATA Configuration                             |
▶ USB Configuration                                   |
▶ Networking                                          |
                                                      | ↔: Select Screen
                                                      | ↑↓: Select Item
                                                      | Enter: Select
                                                      | +/-: Change Opt.
                                                      | F1: General Help
                                                      | F2: Previous Values
                                                      | F3: Optimized Defaults
                                                      | F4: Save & Exit
                                                      | ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
PCH SATA Configuration	Configures the SATA devices and settings.
PCH sSATA Configuration	Configures the sSATA devices and settings.
USB Configuration	USB devices and settings/
Networking	Network devices and settings.

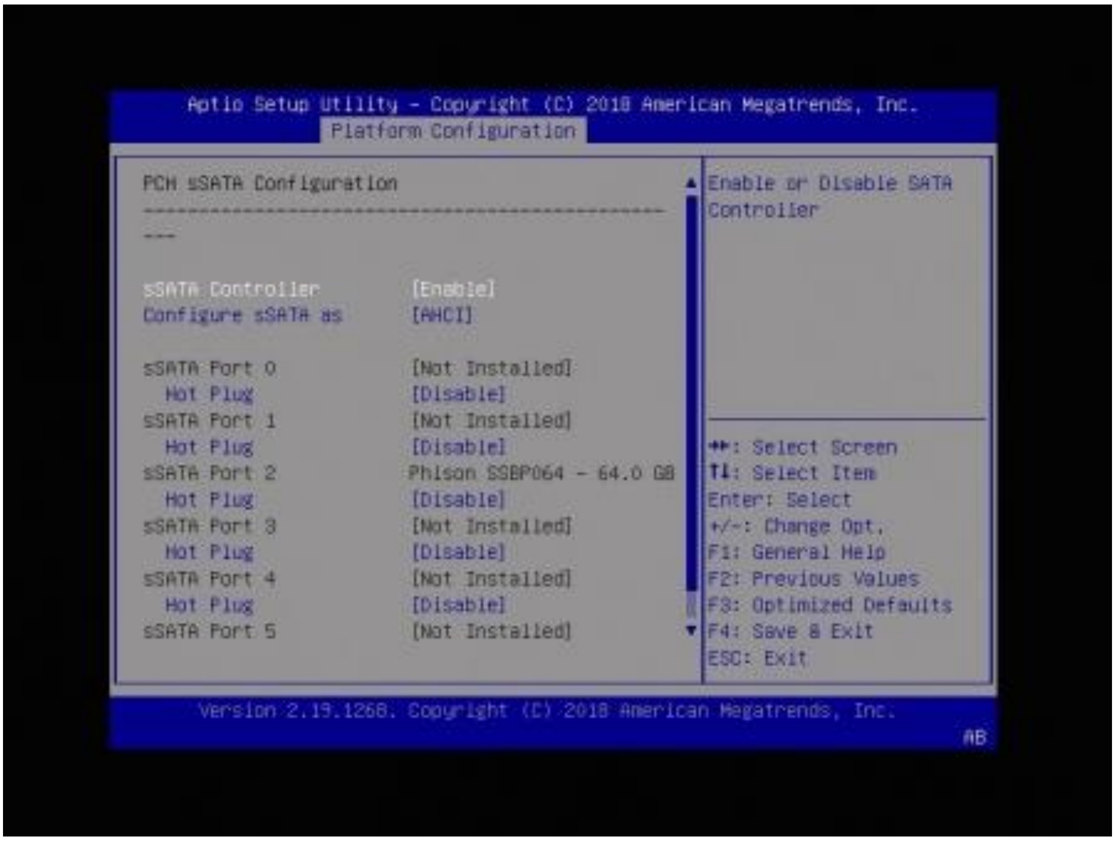
3.5.1.1. PCH SATA Configuration



```
      Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
                          Platform Configuration
 PCH SATA Configuration                              Enable or Disable SATA
 ------------------------------------------------    Controller
 ---

 SATA Controller          [Enable]
 Configure SATA as        [AHCI]

 SATA Port 0              [Not Installed]
 Software Preserve        Unknown
   Hot Plug               [Disable]
 SATA Port 1              [Not Installed]            →←: Select Screen
 Software Preserve        Unknown                    ↑↓: Select Item
   Hot Plug               [Disable]                  Enter: Select
 SATA Port 2              [Not Installed]            +/-: Change Opt.
 Software Preserve        Unknown                    F1: General Help
   Hot Plug               [Disable]                  F2: Previous Values
 SATA Port 3              [Not Installed]            F3: Optimized Defaults
 Software Preserve        Unknown                    F4: Save & Exit
                                                     ESC: Exit

      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
SATA Controller	Enables / Disables SATA controller.
Configure SATA as	Identify the SATA port is connected to SSD or HDD. Options: AHCI, RAID
SATA Ports	Enables / Disables SATA ports.
SATA Ports Hot Plug	Enables / Disables SATA ports hot plug.

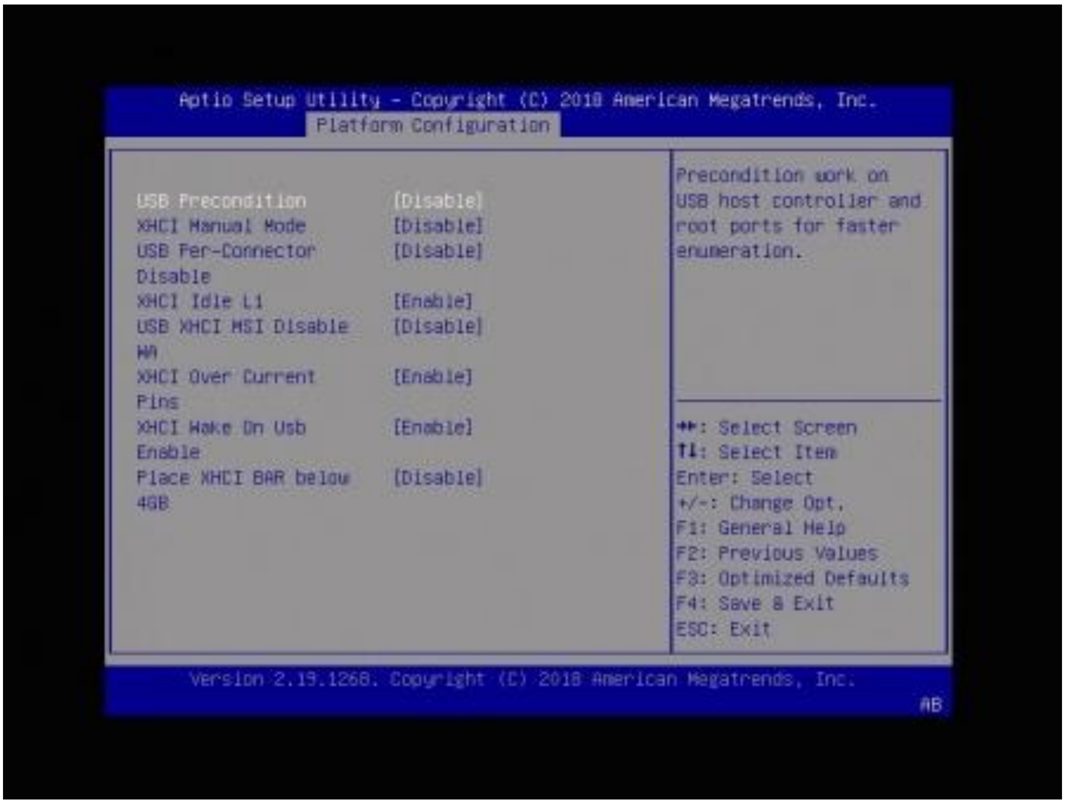
3.5.1.2. PCH sSATA Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                       Platform Configuration
  PCH sSATA Configuration                          ▲ Enable or Disable SATA
  ------------------------------------------------   Controller
  ---

  sSATA Controller          [Enable]
  Configure sSATA as        [AHCI]

  sSATA Port 0              [Not Installed]
    Hot Plug                [Disable]
  sSATA Port 1              [Not Installed]
    Hot Plug                [Disable]            ++: Select Screen
  sSATA Port 2              Phison SSBP064 - 64.0 GB  ↑↓: Select Item
    Hot Plug                [Disable]            Enter: Select
  sSATA Port 3              [Not Installed]      +/-: Change Opt.
    Hot Plug                [Disable]            F1: General Help
  sSATA Port 4              [Not Installed]      F2: Previous Values
    Hot Plug                [Disable]            F3: Optimized Defaults
  sSATA Port 5              [Not Installed]    ▼ F4: Save & Exit
                                                 ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
sSATA Controller	Enables / Disables sSATA controller.
Configure sSATA as	Identify the sSATA ports are connected to SSD or HDD. Options: AHCI, RAID
sSATA Ports	Enables / Disables SATA ports.
sSATA Ports Hot Plug	Enables / Disables SATA ports hot plug.

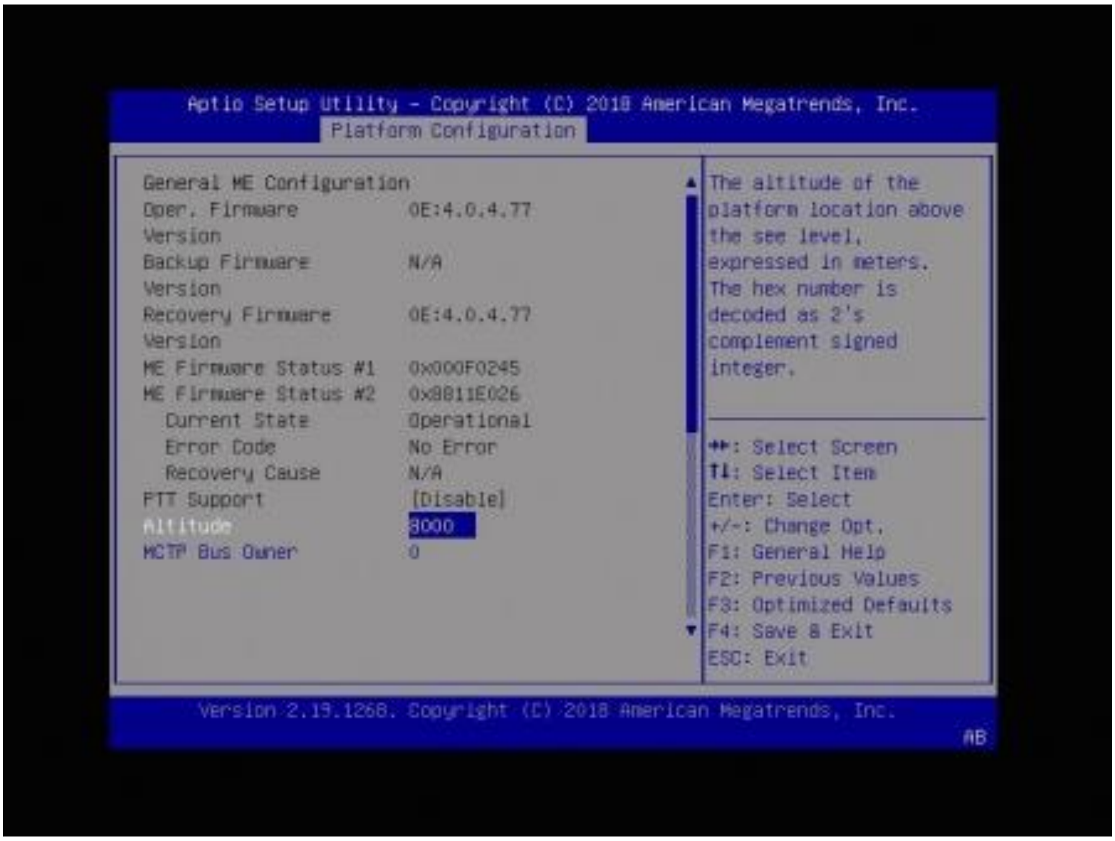
3.5.1.3. USB Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                          Platform Configuration

  USB Precondition         [Disable]        Precondition work on
  XHCI Manual Mode         [Disable]        USB host controller and
  USB Per-Connector        [Disable]        root ports for faster
  Disable                                   enumeration.
  XHCI Idle L1             [Enable]
  USB XHCI MSI Disable     [Disable]
  WA
  XHCI Over Current        [Enable]
  Pins
  XHCI Wake On Usb         [Enable]         →←: Select Screen
  Enable                                    ↑↓: Select Item
  Place XHCI BAR below     [Disable]        Enter: Select
  4GB                                       +/-: Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F3: Optimized Defaults
                                            F4: Save & Exit
                                            ESC: Exit

        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
USB Precondition	Precondition work on USB host controller and root ports for faster enumeration.
XHCI Manual Mode	Enables / Disables this mode to use by validation, not for end-user.
USB Per-Connector Disable	Selectively enables / disables each of the USB physical connector (physical port).
XHCI Idle L1	Disabling XHCI Idle L1 to workaround USB3 hot plug will fail after 1 hot plug removal. Please put the system to G3 for the new settings to take effect.
USB XHCI MSI Disable WA	Enabling this item is to hide MSI capability on XHCI.
XHCI Over Current Pins	Enables / Disables support for XHCI over current pin mapping.
XHCI Wake On USB Enable	Enables / Disables the support for the connection or disconnection of XHCI Wake On USB.
Place XHCI BAR below 4 GB	Enables / Disables to work around WS2K12 KDUSB 64-bit BAR issue.

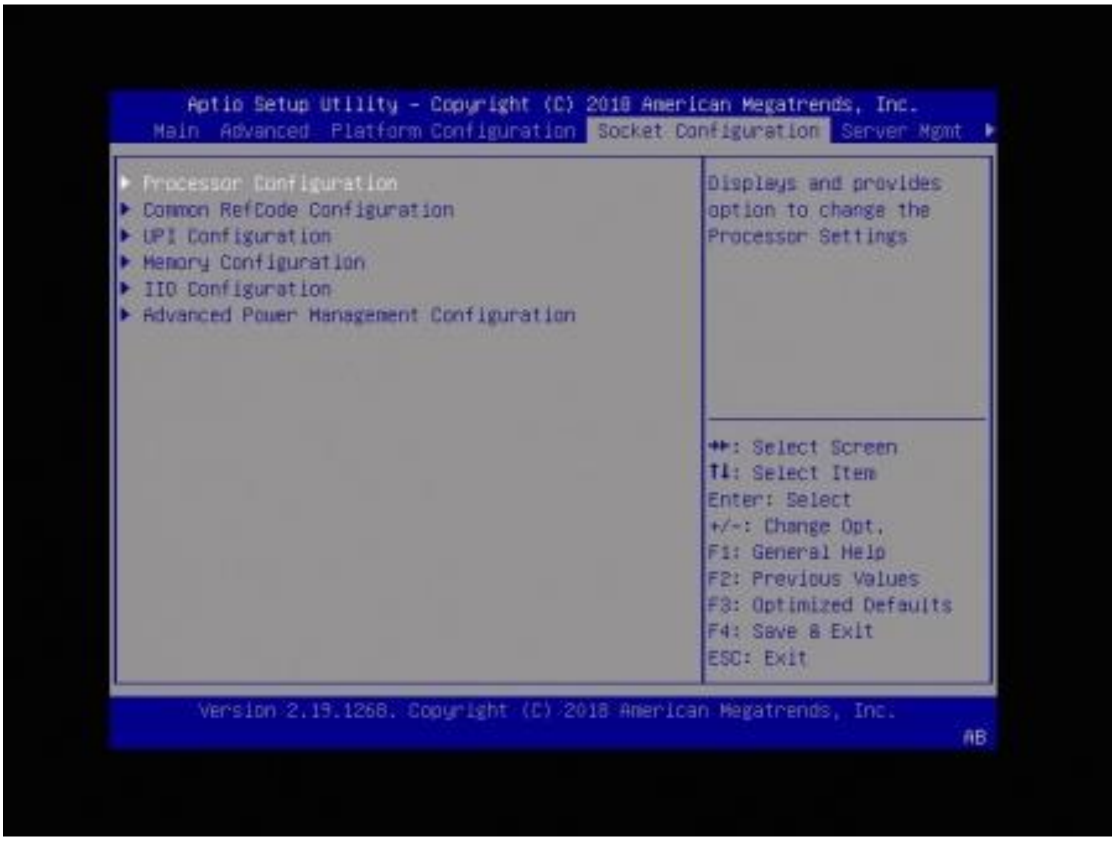
3.5.2 Server ME Configuration



```
       Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                      Platform Configuration
 General ME Configuration                    │The altitude of the
 Oper. Firmware          0E:4.0.4.77         │platform location above
 Version                                     │the see level,
 Backup Firmware         N/A                 │expressed in meters.
 Version                                     │The hex number is
 Recovery Firmware       0E:4.0.4.77         │decoded as 2's
 Version                                     │complement signed
 ME Firmware Status #1   0x000F0245          │integer.
 ME Firmware Status #2   0x8811E026          │
   Current State         Operational         │
   Error Code            No Error            │→←: Select Screen
   Recovery Cause        N/A                 │↑↓: Select Item
 PTT Support             [Disable]           │Enter: Select
 Altitude                8000                │+/-: Change Opt.
 MCTP Bus Owner          0                   │F1: General Help
                                             │F2: Previous Values
                                             │F3: Optimized Defaults
                                             │F4: Save & Exit
                                             │ESC: Exit
       Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Altitude	The altitude of the platform location above the see level, expressed in meters. The hex number is decoded as 2’s complement signed integer.
MCTP Bus Owner	MCTP bus owner location on PCIe: [15:8] bus, [7:3] devices, [2:0] function. If all zeros sending bus owner is disabled.

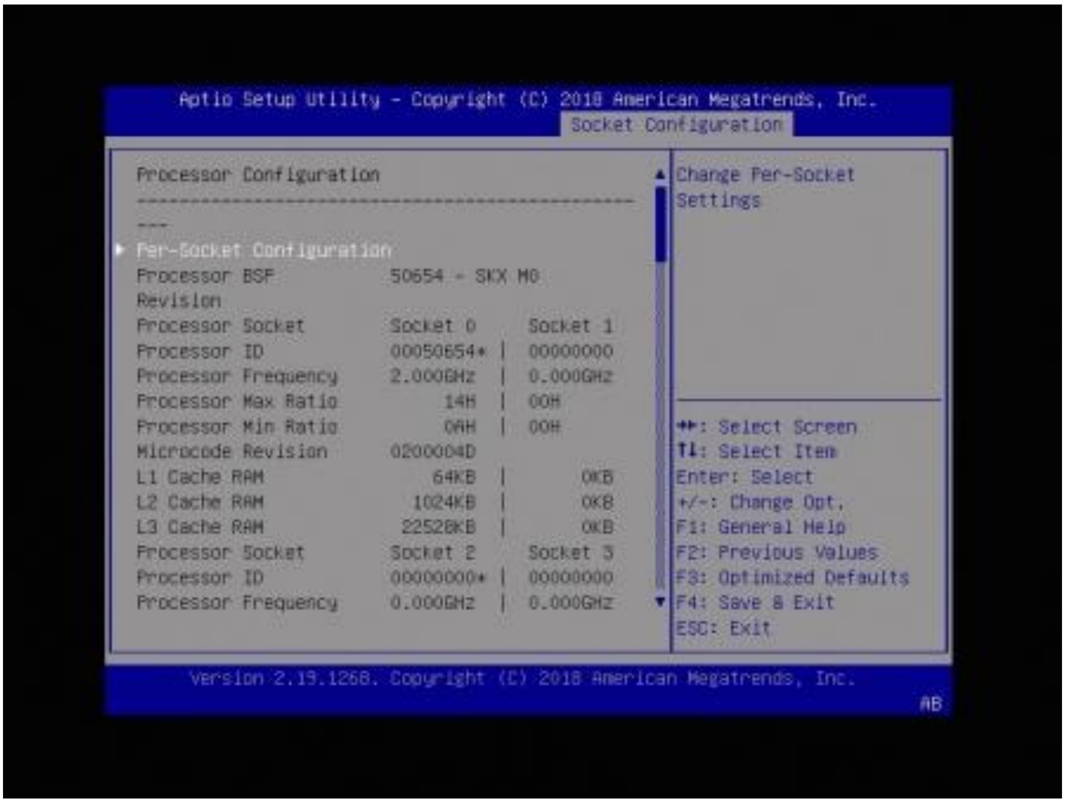
3.6 Socket Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Main  Advanced  Platform Configuration  Socket Configuration  Server Mgmt  ►

► Processor Configuration                    Displays and provides
► Common RefCode Configuration               option to change the
► UPI Configuration                          Processor Settings
► Memory Configuration
► IIO Configuration
► Advanced Power Management Configuration
                                             ↔: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                AB
```

BIOS Setting	Description
Processor Configuration	Displays and provides option to change the processor settings.
Common RefCode Configuration	Displays and provides option to change the Common RefCode settings.
UPI Configuration	Displays and provides option to change the UPI General Settings.
Memory Configuration	Displays and provides option to change the Memory settings.
IIO Configuration	Displays and provides option to change the IIO settings.
Advanced Power Management Configuration	Displays and provides option ot change the Power Management settings.

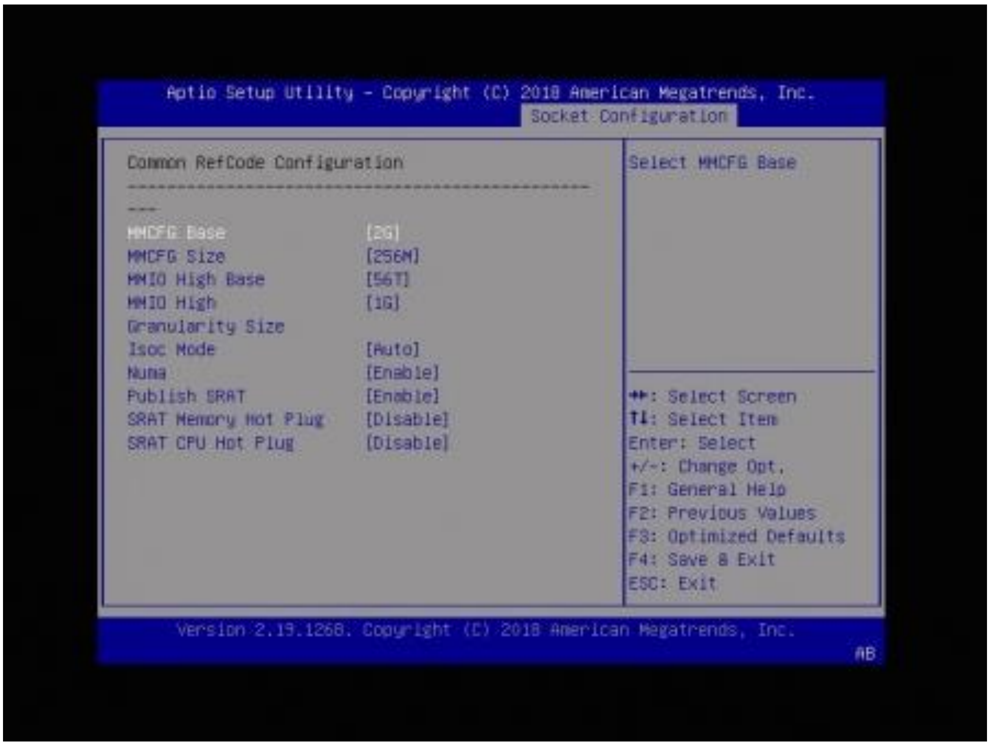
3.6.1 Processor Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                        Socket Configuration

  Processor Configuration                                ▲ Change Per-Socket
  -----------------------------------------------------   Settings
  ---
▶ Per-Socket Configuration
  Processor BSF          50654 - SKX M0
  Revision
  Processor Socket       Socket 0     Socket 1
  Processor ID           00050654* |  00000000
  Processor Frequency    2.000GHz  |  0.000GHz
  Processor Max Ratio         14H  |  00H
  Processor Min Ratio         0AH  |  00H             ↔: Select Screen
  Microcode Revision     0200004D                     ↑↓: Select Item
  L1 Cache RAM               64KB  |       0KB        Enter: Select
  L2 Cache RAM             1024KB  |       0KB        +/-: Change Opt.
  L3 Cache RAM            22528KB  |       0KB        F1: General Help
  Processor Socket       Socket 2     Socket 3        F2: Previous Values
  Processor ID           00000000* |  00000000        F3: Optimized Defaults
  Processor Frequency    0.000GHz  |  0.000GHz     ▼  F4: Save & Exit
                                                      ESC: Exit

     Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Per-Socket Configuration	Configures the per-Socket settings.
Trace HUB STH ACPI-BAR BASE	Enables / Disables Set PCH_TRACE_HUB_FW_BASE_ADDRESS in MSR_TRACE_HUB_STH_ACPIBAR_BASE (MAR 80h).
Hyper-Threading (ALL)	Enables / Disables hyper threading (Software Method to enable/disable logical processor threads.
Intel Enahced Debug	Enables / Disables the function of Intel Enahced Debug. Options: Disable, 4096K
IED Trace Memory	Option to allocate memory for PSMI trace. Options: Disable, 4M, 8M, 16M, 32M, 64M, 128M, 256M, 512M, 1G
TSEG SMRAM Size	Option to change the size of SMRAM for TSEG. Options: 4M, 8M, 16M, 32M, 64M, 128M
Allow mixed freq among CPUs	Keeps (mixed) power-on freqency of each CPU socket. Caution: This is for Intel PPV test only.

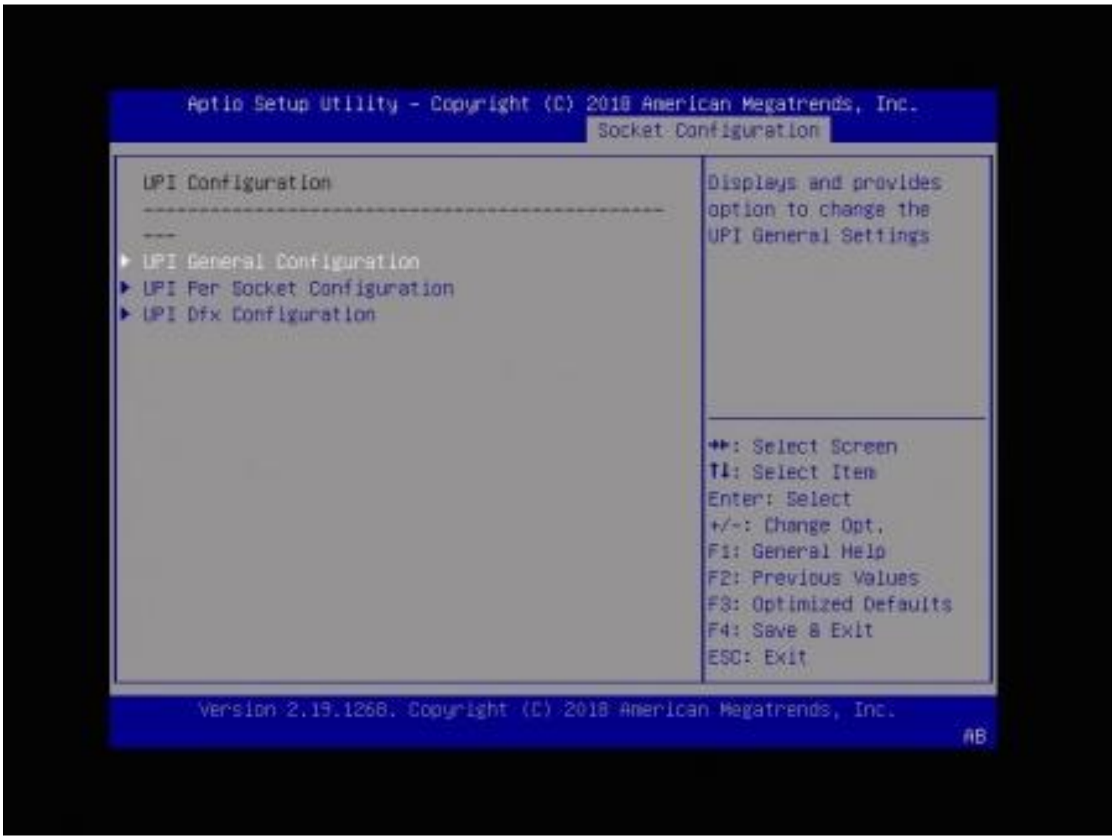
3.6.2 Common RefCode Configuration



```
       Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration

  Common RefCode Configuration                       Select MMCFG Base
  ------------------------------------------------
  ---
  MMCFG Base                [2G]
  MMCFG Size                [256M]
  MMIO High Base            [56T]
  MMIO High                 [1G]
  Granularity Size
  Isoc Mode                 [Auto]
  Numa                      [Enable]
  Publish SRAT              [Enable]                 ↔: Select Screen
  SRAT Memory Hot Plug      [Disable]                ↑↓: Select Item
  SRAT CPU Hot Plug         [Disable]                Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit

          Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
MMCFG Base	Select MMCFG Base. Options: 1G, 1.5G, 1.75G, 2G, 2.25G, 3G
MMCFG Size	Select MMCFG Size. Options: 64M, 128M, 256M, 512M, 1G, 2G
MMIO High Base	Select MMIO High Base. Options: 56T, 40T, 24T, 16T, 4T, 1T
MMIO High Granularity Size	Selects the allocation size used to assign MMIOH resources. Total MMIOH space can be up to 32xgranularity. Options: 1G, 4G, 16G, 64G, 256G, 1024G
Isoc Mode	Enables / Disables Isoc mode.
Numa	Enables / Disables Non-uniform Memory Access (NUMA).
Publish SRAT	Enables / Disables to publish the SRAT ACPI table to the OS.
SRAT Memory Hot Plug	Fix for OS that does not support memory hot plug. Example: SuSE SLES10 SP2 This function is enabled by default.
SRAT CPU Hot Plug	Set processor flag to be enabled for all processor entries in SRAT.

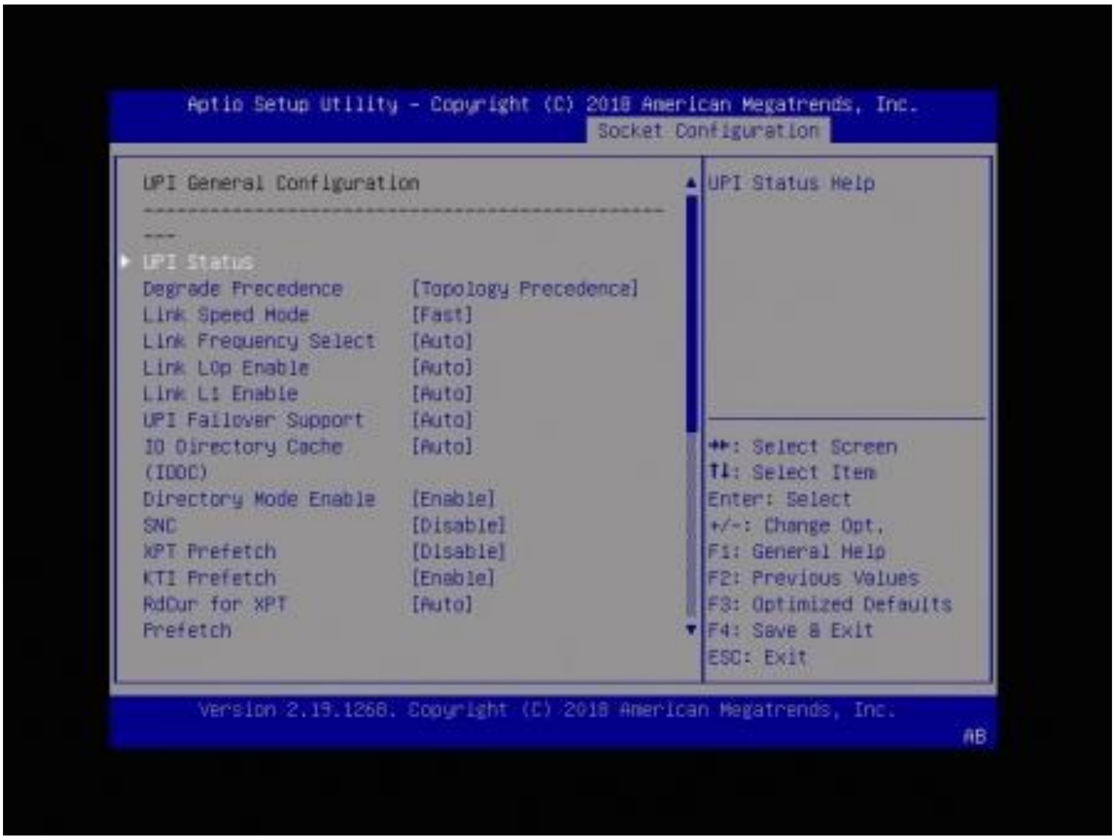
3.6.3 UPI Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                             Socket Configuration
 UPI Configuration                                    Displays and provides
 -------------------------------------------------    option to change the
 ---                                                  UPI General Settings
► UPI General Configuration
► UPI Per Socket Configuration
► UPI Dfx Configuration
                                                      ↔: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
UPI General Confguration	Displays and provides option to change the UPI general settings.
UPI Per Socket Configuration	Configures the UPI per socket.
UPI Dfx Configuration	Configures UPI Dfx functions.

3.6.3.1. UPI General Configuration

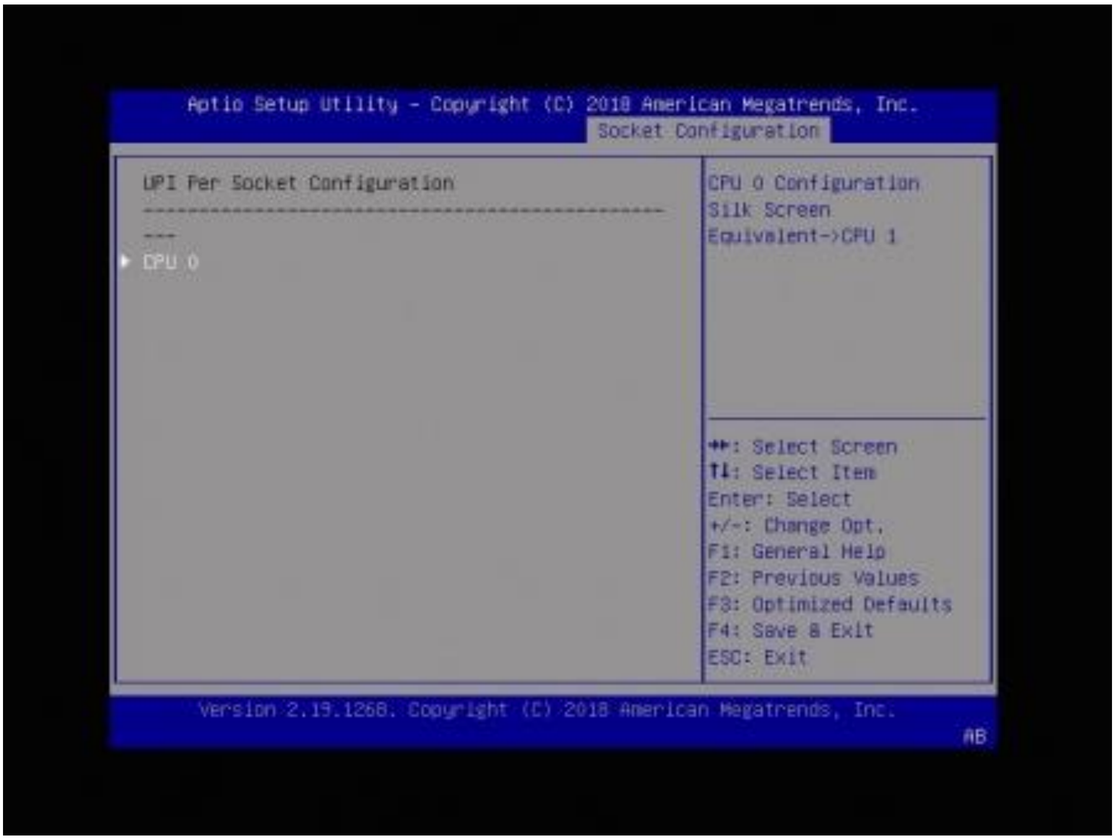


```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                  Socket Configuration
 UPI General Configuration                         ▲ UPI Status Help
 ------------------------------------------------
 ---
▶ UPI Status
 Degrade Precedence       [Topology Precedence]
 Link Speed Mode          [Fast]
 Link Frequency Select    [Auto]
 Link L0p Enable          [Auto]
 Link L1 Enable           [Auto]
 UPI Failover Support     [Auto]
 IO Directory Cache       [Auto]                     ◆◆: Select Screen
 (IODC)                                              ↑↓: Select Item
 Directory Mode Enable    [Enable]                   Enter: Select
 SNC                      [Disable]                  +/-: Change Opt.
 XPT Prefetch             [Disable]                  F1: General Help
 KTI Prefetch             [Enable]                   F2: Previous Values
 RdCur for XPT            [Auto]                     F3: Optimized Defaults
 Prefetch                                          ▼ F4: Save & Exit
                                                     ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                          AB
```

BIOS Setting	Description
UPI Status	UPI status help.
Degrade Precedence	Choose Topology Precedence to degrade features if system options are in conflict or chooses Feature Precedence to degrade topology if system options are in conflict.
Link Speed Mode	Select the UPI link speed as either the PDR speed (Fast) or default speed (Slow). Options: Slow, Fast
Link Frequency Select	Allows for selecting the UPI link frequency. Options: 9.6 GB/s, 10.4 GB/s, Auto, User Per Link Setting
Link L0p / L1 Enable	Enable the function to set as the C_10p_en. Disable the function to reset it. “Auto” decides based on S1 Compatibility.
UPI Failover Support	Enable the function to set as the c_fallover_en. Disable the function to reset it. “Auto” decides based on S1 Compatibility.

BIOS Setting	Description
IO Directory Cache (IODC)	Generates snoops instead of memory lookups for remote InvItoM (IIO). Options: Disable, Auto, Enable for Remote InvItoM Hybrid Push, InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, Enable for remote InvItoM and Remote WViLF.
Directory Mode Enable	Enables / Disables the directory mode.
SNC	“Auto” supports 1-cluster or 2-clusters depending on IMC interleave. SNC and IMC interleave both “Auto” will support 1-cluster (XPT/KTI Prefetch enable) 2-IMC way interleave.
XPT Prefetch	Enables / Disables XPT.Prefetch.
KTI Prefetch	Enables / Disables KTI Prefectch.
RdCur for XPT Prefetch	Enable the function to set the suppress_mem _rd_prefetch_rdcur. Disable the function to reset it. “Auto” decides based on the S1 compatibility.
UPI VNA Credit Override	Global options UPI VNA credit override: maximum, minimum, per link.
CRC Mode	Allosw you to set the UPU CRC mode. Options: 16 Bit CRC, 32 Bit Rolling CRC, Auto (sets to 16-bit)
UPI Load Board for Failed Links	For debugging purposes, UPI link will remain enabled for h/w continuous training in spite of previous failure.
UPI Debug Print Level	Enables / Disables UPI debug print level. Options: Fatal, Warning, Summary, Detail, All.
Local/Remote Threshold	Local / Remote threshold settings. Options: Disable, Auto, Low, Medium, High
TSC Sync Support	TSC Sync Support for all precesors. Options: Disable, Enable, Auto
Stale AtoS	Stale A to S Dir optimization. Options: Disable, Enable, Auto
LLC dead line alloc	Enabling is to opportunistically fill dead lines in LLC. Disabling is never filling dead lines in LLC.

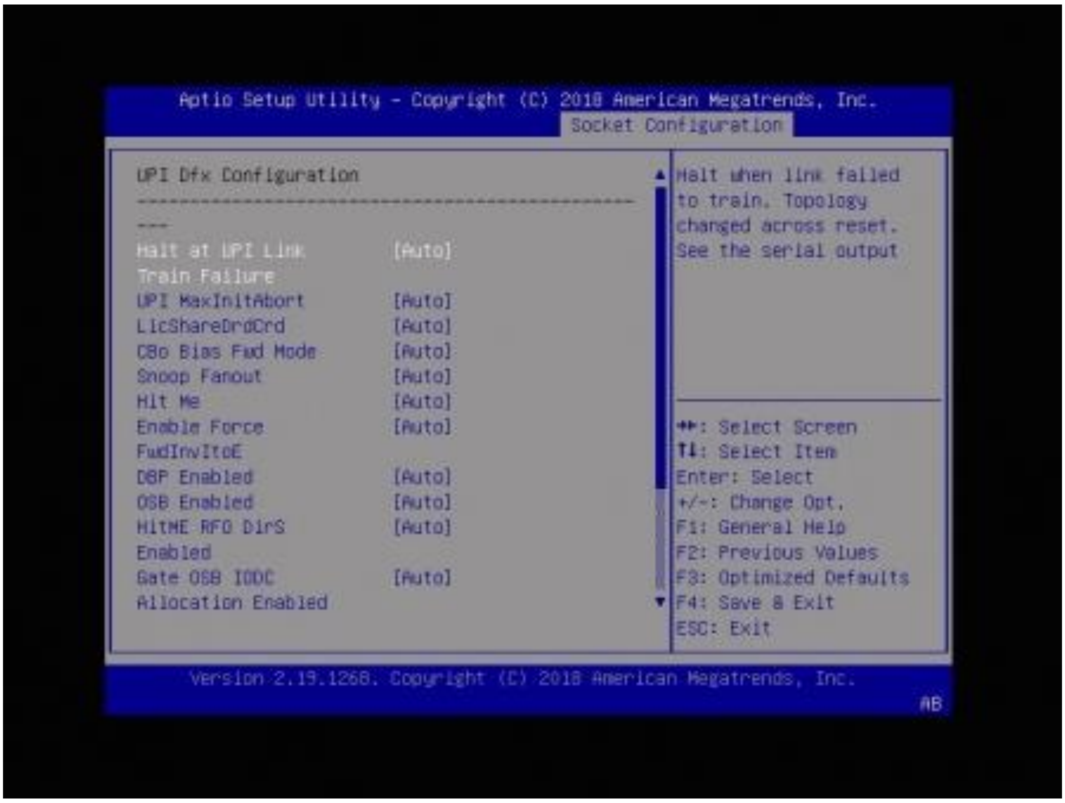
3.6.3.2. UPI Per Socket Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                        Socket Configuration

UPI Per Socket Configuration                 CPU 0 Configuration
----------------------------------------     Silk Screen
---                                          Equivalent->CPU 1
▶ CPU 0

                                             ↔: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                  AB
```

BIOS Setting	Description
CPU 0	CPU 0 configuration silk screen equivalent to CPU 1.

3.6.3.3. UPI Dfx Configuration

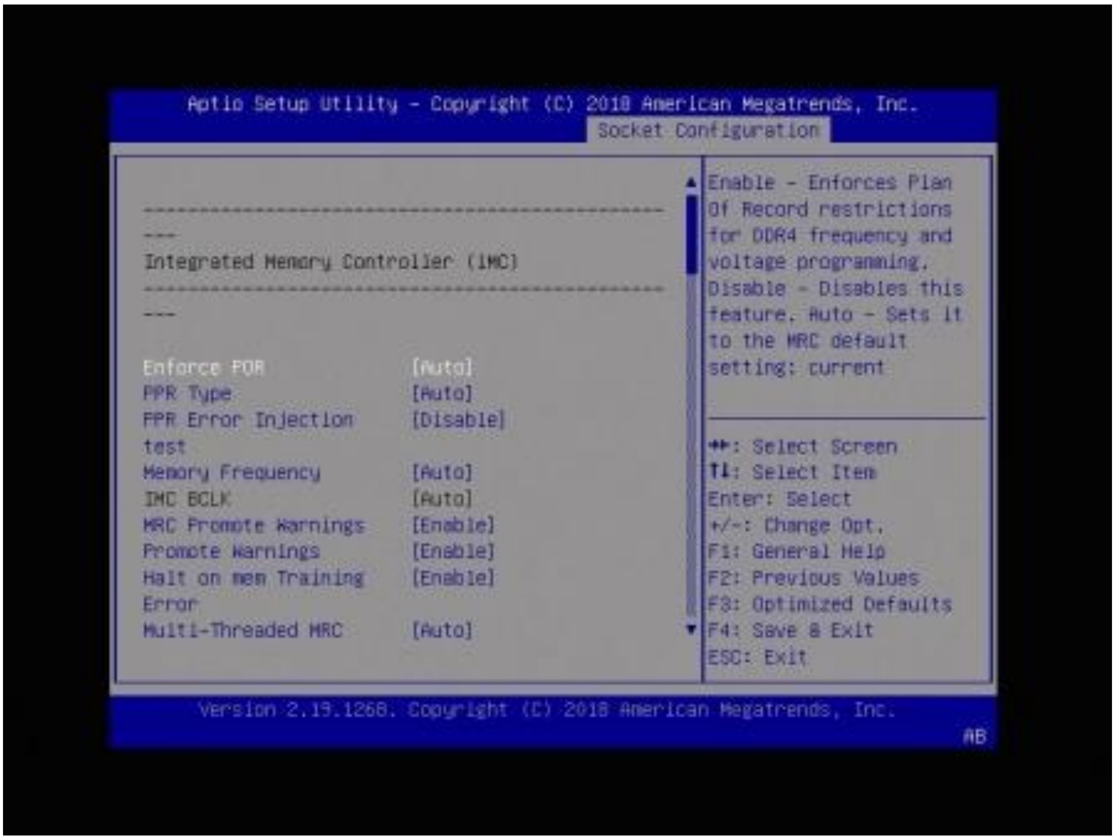


```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                        Socket Configuration
UPI Dfx Configuration                              Halt when link failed
-------------------------------------------------  to train. Topology
---                                                changed across reset.
Halt at UPI Link          [Auto]                   See the serial output
Train Failure
UPI MaxInitAbort          [Auto]
LlcShareDrdCrd            [Auto]
CBo Bias Fwd Mode         [Auto]
Snoop Fanout              [Auto]
Hit Me                    [Auto]
Enable Force              [Auto]                   ↔: Select Screen
FwdInvItoE                                         ↑↓: Select Item
DBP Enabled               [Auto]                   Enter: Select
OSB Enabled               [Auto]                   +/-: Change Opt.
HitME RFO DirS            [Auto]                   F1: General Help
Enabled                                            F2: Previous Values
Gate OSB IODC             [Auto]                   F3: Optimized Defaults
Allocation Enabled                                 F4: Save & Exit
                                                   ESC: Exit
Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                AB
```

BIOS Setting	Description
Halt at UPI Link Train Failure	Halt when link faliled to train. Topology changed across reset. See the serial output. Options: Disable, Enable, Auto
UPI MaxUnitAbort	Options: Disable, Enable, Auto
LlcShareDrdCrd	Enables / Disables migration from SF to LLC and to leave shared lines in the LLC for Drd and Crd. Options: Disable, Enable, Auto
CBo Bias Fwd Mode	0 – Mode 0 (Fwd only when Hom ! = Req, Default) 1 – Mode 1 (Fwd when Hom ! = Req & Hom ! = Local) 2 – Mode 2 (Disable Bias Fwd) Options: Mode0, Mode1, Mode3, Mode4, Auto
Snoop Fanout	Options: Disable, Enable, Auto
Hit Me	Enables / Disables CHA HitME cache. Options: Disable, Enable, Auto
Enable Force FwdInvItoE	Options: Disable, Enable, Auto

BIOS Setting	Description
DBP Enabled	Options: Disable, Enable, Auto
OSB Enabled	Options: Disable, Enable, Auto
HitME RFO DirS Enabled	Enables HitME DIR=S RFO optimization. Options: Disable, Enable, Auto
Gate OSB IODC Allocation Enabled	When OSB indicates that there aren't enough snoop credits don't allocate IODC entry. Options: Disable, Enable, Auto
Dual Link Interleave Mode	Only valid in 2 socket 2 Link Topology. Options: Enable CHA interleaving (disable SNC, XOR-based Intlv), Disable D2C, Auto
Dfx System Degrade Mode	System topology degrade mode options. Options: Degrade_to_1S, Degrade_to_Supported, No_Degrade
VN1	Options: Disable, Enable, Auto
Direct to Core (D2C)	Options: Disable, Enable, Auto
Direct to UPI (D2K)	Options: Disable, Enable, Auto

3.6.4 Memory Configuration

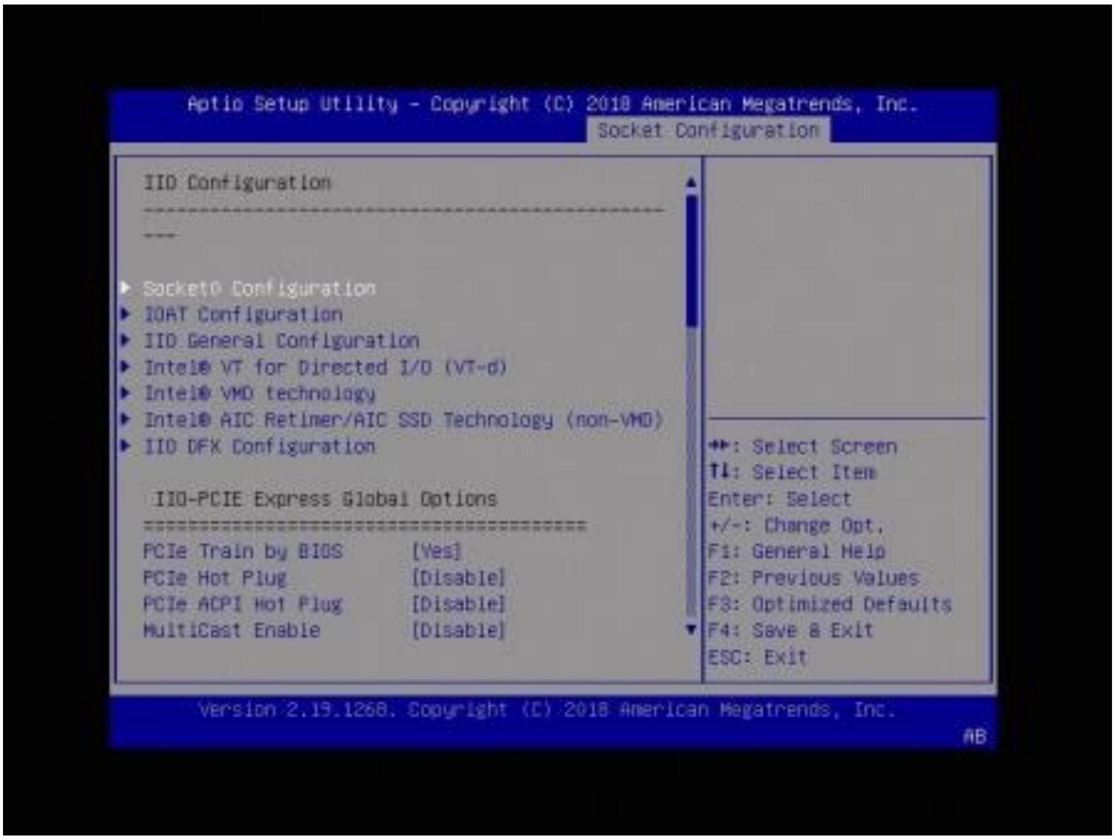


```
     Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                               Socket Configuration
 ---------------------------------------------- ▲ Enable - Enforces Plan
 ---                                              Of Record restrictions
 Integrated Memory Controller (IMC)               for DDR4 frequency and
 ----------------------------------------------   voltage programming.
 ---                                              Disable - Disables this
                                                  feature. Auto - Sets it
 Enforce POR                [Auto]                to the MRC default
 PPR Type                   [Auto]                setting: current
 PPR Error Injection        [Disable]
 test                                             ↔: Select Screen
 Memory Frequency           [Auto]                ↑↓: Select Item
 IMC BCLK                   [Auto]                Enter: Select
 MRC Promote Warnings       [Enable]              +/-: Change Opt.
 Promote Warnings           [Enable]              F1: General Help
 Halt on mem Training       [Enable]              F2: Previous Values
 Error                                            F3: Optimized Defaults
 Multi-Threaded MRC         [Auto]              ▼ F4: Save & Exit
                                                  ESC: Exit
     Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                     AB
```

BIOS Setting	Description
Enforce POR	Enforces plan of record restrictions for DDR4 frequency and voltage programming. Disable – Disables this feature. “Auto” sets it to the MRC default setting. Options: Auto, PDR, Disable
PPR Type	Selects Post Package Repair type – hard, soft, disabled. Auto – Sets it to the MRC default setting; current default is disabled. Options: Auto, Hard PPR, Soft PPR, PPR Disabled
PPR Error Injection test	Enables / Disables support for c-script err injection test.
Memory Frequency	Maximum memory frequency selections in Mhz. Options: Auto, 800, 1000, 1066, 1200, 1333, 1400, 1600, 1800, 1866, 2000, 2133, etc.

BIOS Setting	Description
MRC Promote Warnings	Determines if MRC warnings are promoted to system level.
Promote Warnings	Determines if warnings are promoted to system level.
Halt on mem Training Error	Enables / Disables halt on mem training error.
Multi-Threaded MRC	Enable – Executes the memory reference code multi-threaded. Disable – Disables this feature. Auto – Sets it to MRC default setting; tthe current default is Enable.
SPD CRC Check	Enables / Disables to turn on checking the SPD CRC.
Enhanced Log Parsing	Enables / Disables additional output in debug log for easier machine parsing.
LRDIMM Module Delay	When disabled, MRC will not use SPD bytes 90-95 for LRDIMM module delay. When “Auto” is selected, MRC will coundary check the values and use default values, if SPD is 0 or out of range.
MemTest	Enable – Enables memory test during normal bootl Disable – Disables this feature. Auto – Sets it to MRC deafult setting; the current default is Enable.
Memory Type	Selects the memory type supported by this platform. Options: RDIMMs only, UDIMMs only, UDIMMs and RDIMMs
Rank Margin Tool	Enable – Enables the legacy rank margin tool to run after DDR4 memory training. Disable – Disables this feature. Auto – Sets it to MRC default setting.
Backside RMT	Enable – Enables the legacy Backside Rank Margin tool. Disable – Disables this feature. Auto – Sets it to MRC default setting; the current default is Enable.
Backside CMD RMT	Enables / Disables the backside CMD RMT.

3.6.5 IIO Configuration



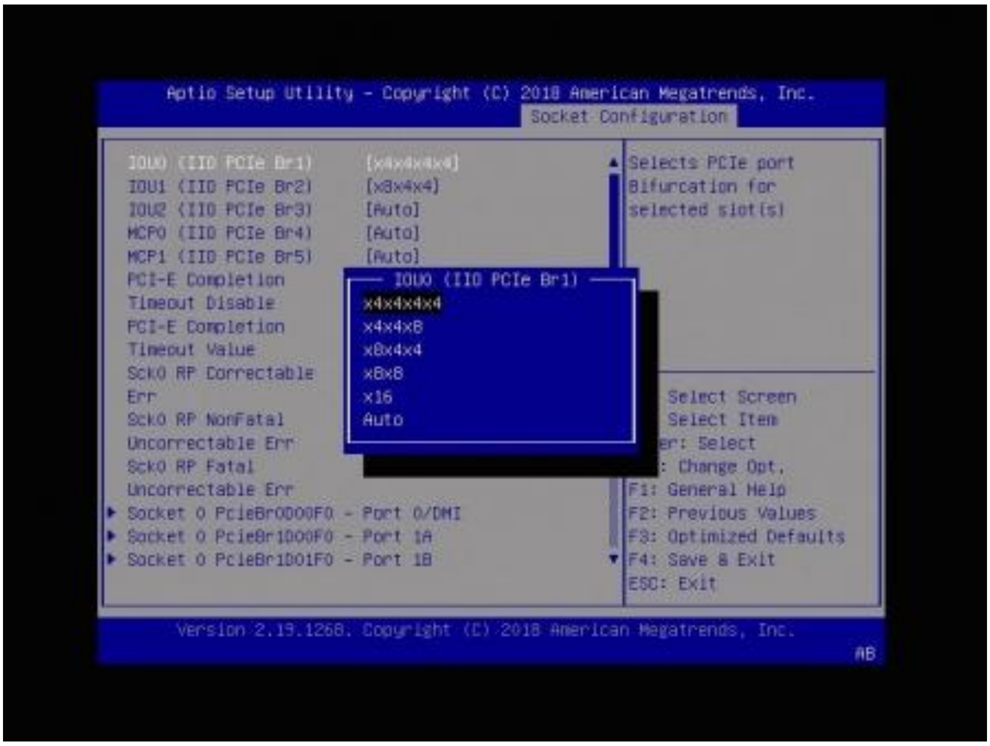
```
     Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                         Socket Configuration
 IIO Configuration                                ▲
 ------------------------------------------------
 ---

▶ Socket0 Configuration
▶ IOAT Configuration
▶ IIO General Configuration
▶ Intel® VT for Directed I/O (VT-d)
▶ Intel® VMD technology
▶ Intel® AIC Retimer/AIC SSD Technology (non-VMD)
▶ IIO DFX Configuration                            →←: Select Screen
                                                   ↑↓: Select Item
  IIO-PCIE Express Global Options                  Enter: Select
 =========================================         +/-: Change Opt.
 PCIe Train by BIOS        [Yes]                   F1: General Help
 PCIe Hot Plug             [Disable]               F2: Previous Values
 PCIe ACPI Hot Plug        [Disable]               F3: Optimized Defaults
 MultiCast Enable          [Disable]          ▼    F4: Save & Exit
                                                   ESC: Exit
      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                       AB
```

BIOS Setting	Description
Socket 0 Configuration	Configures the socket 0.
IOAT Configuration	All IOAT configuration options.
IIO General Configuration	Option to change the IIO general settings.
Intel® VT for Directed I/O (VT-d)	Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) configuratio menu.
Intel® VMD Technology	Press <Enter> to bring up the Intel® VMD for volume management device configuration menu.
Intel® AIC Retimer / AIC SSD Technology (non-VMD)	Press <Enter> to bring up the Intel® AIC Retimer/AIC SSD Configuration menu.
IIO DFX Configuration	Enables / Disables DFX configuration.
PCIe Train by BIOS	Assumes IIO is strapped for Malt-for-BIOS because straps are unreliable in A-0 Silicon. Options: No, Yes
PCIe Hot Plug	Enables / Disables PCIe Hot Plug globally. Options: Disable, Enable, Auto, Manual

BIOS Setting	Description
PCIe ACPI Hot Plug	Enables / disables PCIe ACPI Hot Plug globally, or allow per-port control. When disabled, MSI is generated on HP event. When enabled, _HPGPE message is generated. Options: Disable, Enable, Per-Port
MultiCast Enable	Enables / Disables multi-cast (for validation use).
NoSnoop Read Config	Enables / Disables NoSnoop reading
NoSnoop Write Config	Enables / Disables NoSnoop writing.
Max Read Comp Comb Size	Minimum or Maximum the size.
Problematic Port	Selects whether problematic port lock flows need to be enabled in the system. Selection allows for P-P or NP-NP lock flows or neither. Options: Disable, NP-NP problematic, P-P problematic
DMI Allocating Write Flows	Selects DMI Vc0/VCp writer selection as either allocating or non-allocating or non-allocating. Auto enables POR setting. Options: Non-Allocating, Allocating
PCIe Allocating Write Flows	Selects Vc0/VCp writers selection for all CPU PCIe ports as either allocating or non-allocating. Auto enables POR setting. Options: Non-Allocating, Allocating
Skip Halt On DMI Degradation	Enables / Disables this option to avoid the system to be halted on DMI width/link degradation.
Rx Clock WA	HSX HSD# 4166557
PME2ACK Timeout	Controls duration to wait between PME_TIRN OFF and PME_T0_ACK. Options: 1 ms, 10 ms, 50 ms, Test Mode
MCTP	Enables / Disables MCTP.
Hide PCU Func 6	Enables / Disables hide power control unit device 30 function 6.
EN1K	Enables / Disables 1K granularity for I/O space decode in each of the virtual P2P bridges corresponding to root ports, and DMI ports.
Dual CV IO Flow	Allows ucode to enable dual CV feature in the Cbo.

BIOS Setting	Description
PCIE Coherent Read Partial	Configures Coherent Reads for available settings. Options: PCIRdCur Setting, PRd Setting
PCIE Coherent Read Full	Configures coherent reads for available settings. Options: PCIRdCur Setting, PRd Setting
PCI-E Completion Timeout (Global) Disable	Enables / Disables the completion timeout (D:x F:0 0:88h B:4) where x is 0-3. Options: Yes, No, Per-Port
PCI-E Global Timeout Value	Program the completion timeout value (D:x F:0 0: 88h B:3-0) where x is 0-3. Options: 50µs to 10ms, 16ms to 55ms, 65ms to 210ms, 260ms to 900ms, 1s to 3.5s, 4s to 13s, 17s to 64s
PCI-E ASPM Support (Global)	Enables / Disables the ASPM support for all downstream devices. Options: Disable, Per-Port, L1 Only
PCIE Stop & Scream Support	Enables / Disables PCIe stop & scream support.
Snoop Response Hold Off	Sets Snoop Response Hold Off value, 256 cycles as default.
PCIe Latency Tolerance Reporting	Auto/Disable – Turns off the Latency Tolerance Report feature of the PCIe root port and endpoint. Enable – Turns on the Latency Tolerance Report feature.
PCIe Extended Tag Enable	Auto/Enable – BIOS sets 8-bit Tag Field for PCIe root port/endpoint. Disable – BIOS sets 5-bit Tag Field for PCIe root port/endpoint.
PCIe Atomic Operation Request Support	Enables / Disables Atomic operation feature in PCIe device control2 register of IIO root ports and endpoints.
PCIe Max Read Request Size	Set the max. reading request Ssze in endpoints. Options: Auto, 128B, 256B, 512B, 1024B, 2048B, 4096B
PCIe Relaxed Ordering	Enables / Disables PCIe relaxed ordering.
PCIe PHY test mode	Enables / Disables PCIe PHY test mode.

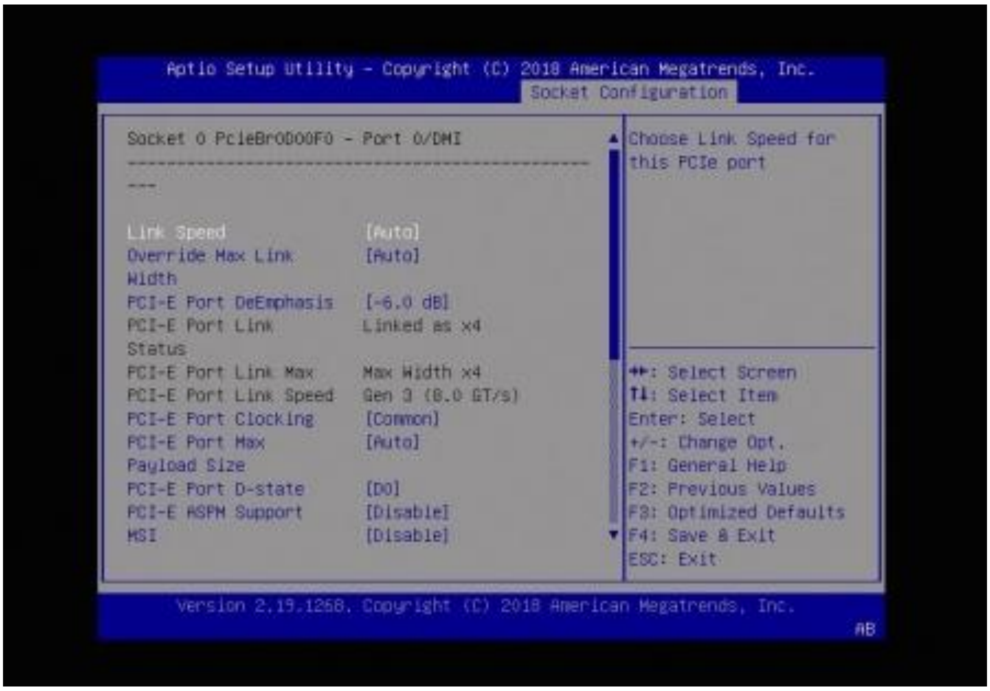
3.6.5.1. Socket 0 Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                         Socket Configuration
 IOU0 (IIO PCIe Br1)     [x4x4x4x4]       ▲ Selects PCIe port
 IOU1 (IIO PCIe Br2)     [x8x4x4]           Bifurcation for
 IOU2 (IIO PCIe Br3)     [Auto]             selected slot(s)
 MCP0 (IIO PCIe Br4)     [Auto]
 MCP1 (IIO PCIe Br5)     [Auto]
 PCI-E Completion     ── IOU0 (IIO PCIe Br1) ──
 Timeout Disable        x4x4x4x4
 PCI-E Completion       x4x4x8
 Timeout Value          x8x4x4
 Sck0 RP Correctable    x8x8
 Err                    x16                     Select Screen
 Sck0 RP NonFatal       Auto                    Select Item
 Uncorrectable Err                            er: Select
 Sck0 RP Fatal                                : Change Opt.
 Uncorrectable Err                          F1: General Help
▶ Socket 0 PcieBr0D00F0 - Port 0/DMI        F2: Previous Values
▶ Socket 0 PcieBr1D00F0 - Port 1A           F3: Optimized Defaults
▶ Socket 0 PcieBr1D01F0 - Port 1B         ▼ F4: Save & Exit
                                            ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
IOU0 / IOU1 / IOU2 (IIO PCIe Br1 / Br2 / Br3)	Selects PCIe port Bifurcation for selected slot(s). Options: x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, Auto
MCP0 / MCP1	Selects PCIe port Bifucation for selected slot(s). Options: x16, Auto
PCI-E Completion Timeout Disable	Enables / Disables the Completion Timout (D:x F:0 0:88h B:4) where x is 0-3. Options: No, Yes
PCI-E completion Timeout Value	Programs the completion timeout value (D:x F:0 0:88h B:3-0) where x is 0-3. Options: 50µs to 10ms, 16ms to 55ms, 65ms to 210ms, 260ms to 900ms, 1s to 3.5s, 4s to 13s, 17s to 64s
Sck0 RP Correctable Err	Applies to root ports only. Enables / Disables interrupt on correctable errors.
Sck0 RP NonFatal Uncorrectable Err	Applies to root ports only. Enables / Disables interrupt on a non-fatal error.
Sck0 RP Fatal Uncorrectable Err	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.
Socket 0 PCIe Ports	Provdes settings related to PCIe ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A).

Socket 0 PCIe Ports

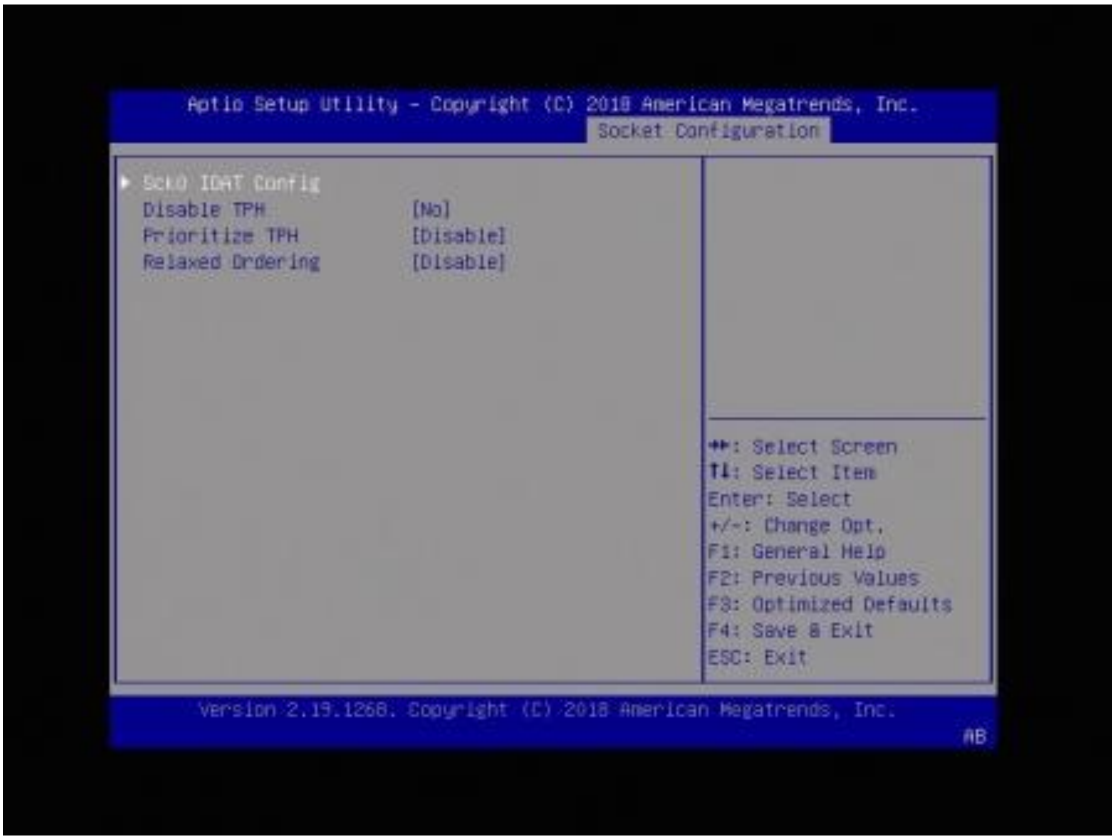


```
       Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration

  Socket 0 PcieBr0D00F0 - Port 0/DMI                  Choose Link Speed for
  ------------------------------------------------    this PCIe port
  ---

  Link Speed                [Auto]
  Override Max Link         [Auto]
  Width
  PCI-E Port DeEmphasis     [-6.0 dB]
  PCI-E Port Link           Linked as x4
  Status
  PCI-E Port Link Max       Max Width x4              ←→: Select Screen
  PCI-E Port Link Speed     Gen 3 (8.0 GT/s)          ↑↓: Select Item
  PCI-E Port Clocking       [Common]                  Enter: Select
  PCI-E Port Max            [Auto]                    +/-: Change Opt.
  Payload Size                                        F1: General Help
  PCI-E Port D-state        [D0]                      F2: Previous Values
  PCI-E ASPM Support        [Disable]                 F3: Optimized Defaults
  MSI                       [Disable]                 F4: Save & Exit
                                                      ESC: Exit

       Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
Link Speed	Choose Link Speed for this PCIe port. Options: Auto, Gen1 (2.5 GT/s), Gen2 (5 GT/s), Gen3 (8 GT/s)
Override Max Link Width	Override the max link width that was set by bifurcation. Options: Auto x1, x2, x4
PCI-E Port DeEmphasis	De-Emphais control (LNKCON2[6]) for this PCIe port. Options: -6.0 dB, -3.5 dB
PCI-E Port Clocking	Configures port clocking via LNKCON[6]. This refers to this components and the down stream component. Options: Distinct, Common
PCI-E Port Max Payload Size	Sets the max. payload size to 256B if possible. Options: 128B, 256B, Auto
PCI-E Port D-state	Sets to D0 for normal operation, D3Hot to be in low-power state. Options: D0, D3Hot
PCI-E ASPM Support	This option enables / disables the ASPM (L1) support for the downstream devices. Options: Auto, L1 only, Diable
MSI	BUS0 DEVx FUN0 OFF 0x5A bit 0, where x is 0-3.

BIOS Setting	Description
PCI-E Extended Sync	Enables / Disables the extended sync mode (D:x F:0 0:7ch B:7) where x is 0-9.
Compliance Mode	Enables / Disables compliance mode for this PCIe port.
EOI	Dev 0,2,3 MISCCTRLSTS (Reg 0x188) Bit 26
Fatal Err Over	Enables / Disables forcing fatal error propogation to the IIO core error logic for this port.
Non-Fatal Err Over	Enables / Disables forcing non-fatal error propogation to the IIO core error logic for this port.
Corr Err Over	Enables / Disables forcing correctable error propogation to the IIO core error logic for this port.
ACPI PME Interrupt	When enabled, ACPI PME Interrupts are generated from this port.
L0s Support	When disabled, IIO never puts its transmitter in L0s state.
P2P Memory Write	Controls Peer2Peer memory write decoding.
P2P Memory Read	Controls Peer2Peer memory read decoding.
PME to ACK	Controls timeout usage for IIO waiting on PME_T0_ACK after a PME_TURN_OFF message.
Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCIe / DMI port.
Alternate TxEq	Enables / Disables TxEq.
SRIS	Enables / Disables SRIS.
ECRC	Enables or Disables ECRC (Error Capabilities and Control Register).
IODC Configuration	Enables / Disables IODC (IODirect Cahe: Generates snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (Cores). Options: KTI Option, Auto, Enable for Remote InvItoM Hybrid Push, InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, Enable fro Remote InvItoM and Remote WViLF.
Non-Transparent Bridge PCIe Port Definition	Configures port as TB, NTB-NTB, or NTB-RP (Don’t select NTP-RP for legacy IIO on A0 Si!) Options: Transparent Bridge, NTB to NTB, NTB to RP
Hide Port?	You can force to hide this root port from OS. Options: No, Yes

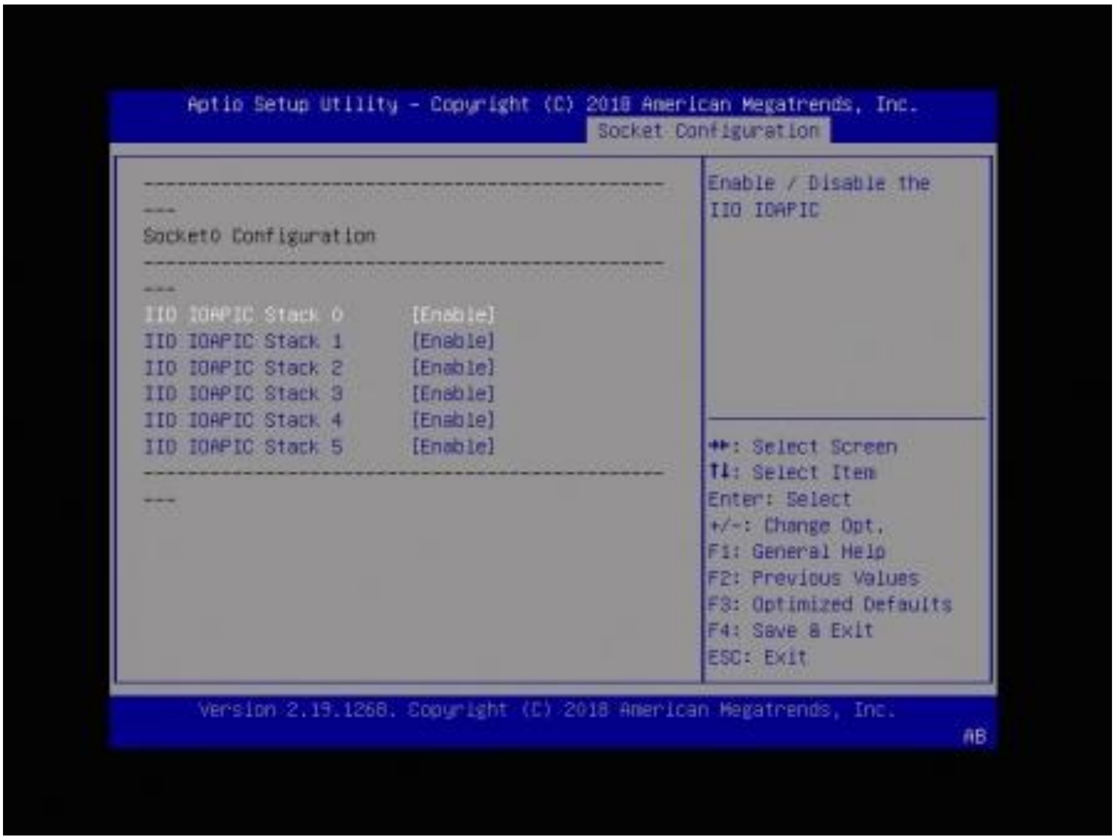
3.6.5.2. IOAT Configuration



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                            Socket Configuration

► Sck0 IOAT Config
  Disable TPH                [No]
  Prioritize TPH             [Disable]
  Relaxed Ordering           [Disable]

                                       ↔: Select Screen
                                       ↑↓: Select Item
                                       Enter: Select
                                       +/-: Change Opt.
                                       F1: General Help
                                       F2: Previous Values
                                       F3: Optimized Defaults
                                       F4: Save & Exit
                                       ESC: Exit

      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Disable TPH	Allows you to choose to disable TLP processing hint or not. Options: No, Yes
Prioritize TPH	Enables / Disables prioritize TPH
Relaxed Ordering	Enables / Disables relaxed ordering.

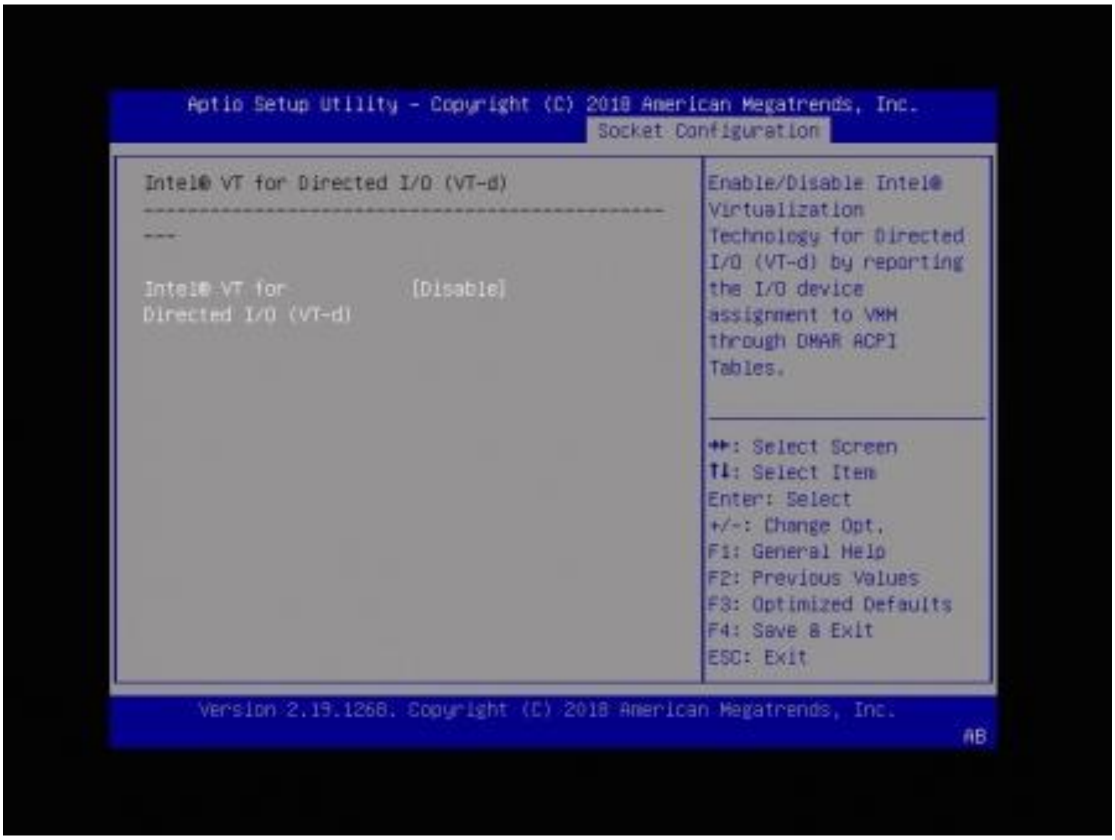
3.6.5.3. IIO General Configuration



```
           Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                 Socket Configuration
 ------------------------------------------------ Enable / Disable the
 ---                                              IIO IOAPIC
 Socket0 Configuration
 ------------------------------------------------
 ---
 IIO IOAPIC Stack 0        [Enable]
 IIO IOAPIC Stack 1        [Enable]
 IIO IOAPIC Stack 2        [Enable]
 IIO IOAPIC Stack 3        [Enable]
 IIO IOAPIC Stack 4        [Enable]
 IIO IOAPIC Stack 5        [Enable]               ++: Select Screen
 ------------------------------------------------ ↑↓: Select Item
 ---                                              Enter: Select
                                                  +/-: Change Opt.
                                                  F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit
           Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                          AB
```

BIOS Setting	Description
IIO IOAPIC Stack 0/1/2/3/4/5	Enables / Disables the IIO IOAPIC.

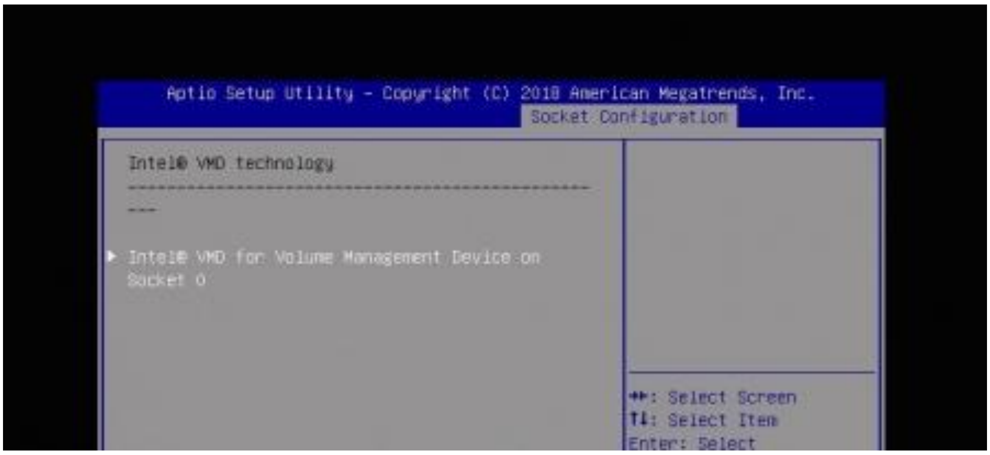
3.6.5.4. Intel® VT for Directed I/O (VT-d)



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                   Socket Configuration

Intel® VT for Directed I/O (VT-d)               Enable/Disable Intel®
------------------------------------------------ Virtualization
---                                             Technology for Directed
                                                I/O (VT-d) by reporting
Intel® VT for              [Disable]            the I/O device
Directed I/O (VT-d)                             assignment to VMM
                                                through DMAR ACPI
                                                Tables.

                                                ↔: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/-: Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

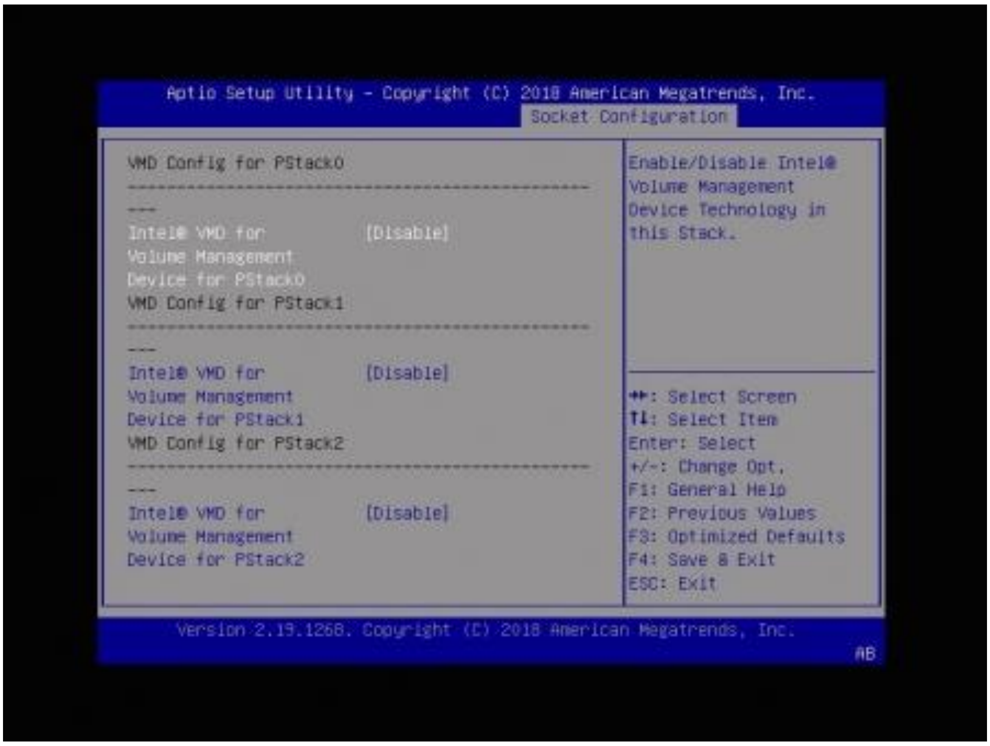
BIOS Setting	Description
Intel® VT for Directed I/O (VT-d)	Enables / Disables Intel® Virtualization Technology for directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI tables.

3.6.5.5. Intel® VMD Technology



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration

 Intel® VMD technology
 ---------------------------------------------------
 ---

▸ Intel® VMD for Volume Management Device on
 Socket 0

                                                   ↔: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
```

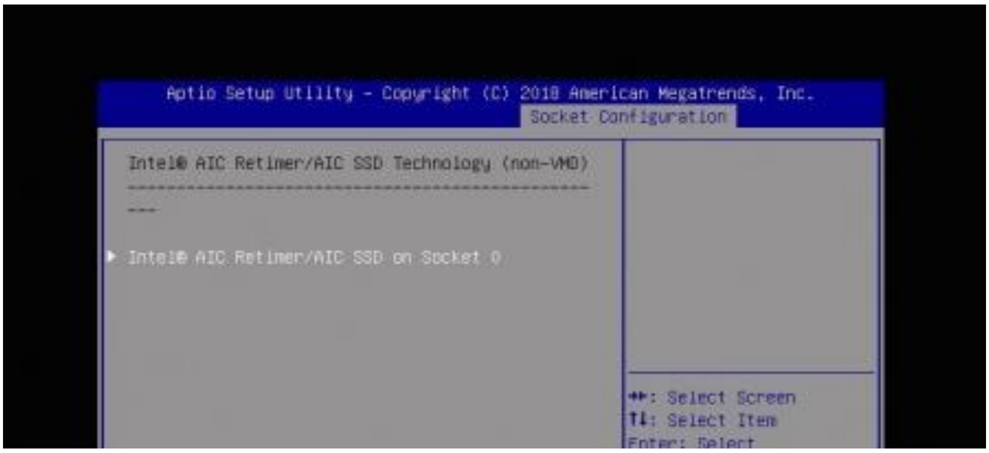
BIOS Setting	Description
Intel® VMD for Volume Management Device on Socket 0	Configures Intel® VMD for PStack(s).



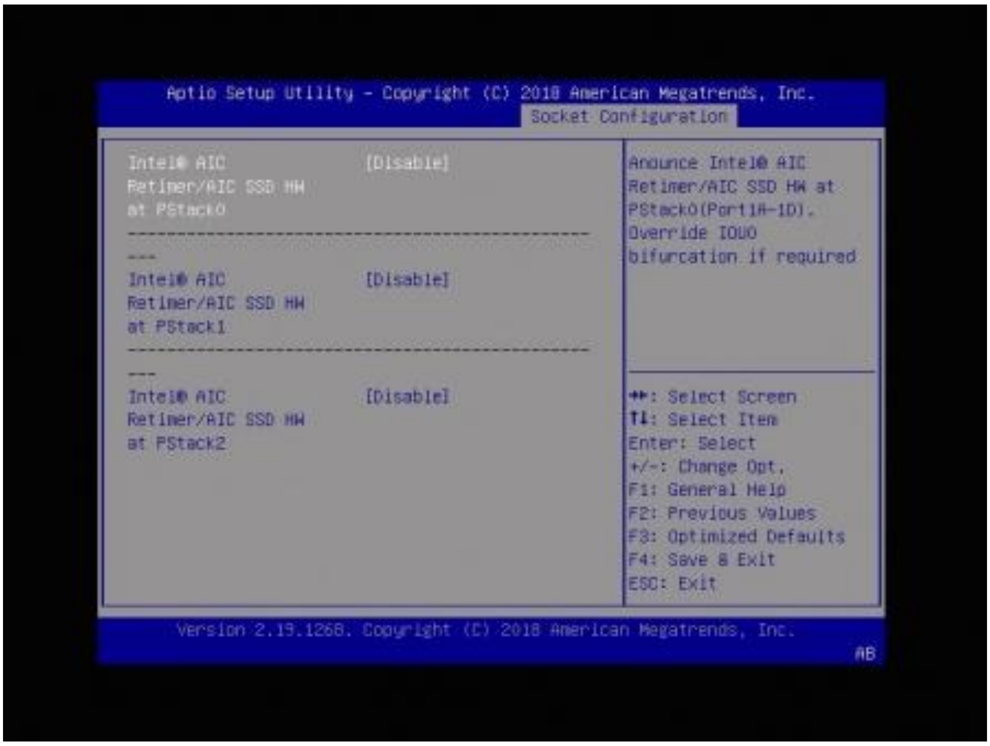
```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration

 VMD Config for PStack0                            Enable/Disable Intel®
 ---------------------------------------------     Volume Management
 ---                                               Device Technology in
 Intel® VMD for           [Disable]                this Stack.
 Volume Management
 Device for PStack0
 VMD Config for PStack1
 ---------------------------------------------
 ---
 Intel® VMD for           [Disable]                ↔: Select Screen
 Volume Management                                 ↑↓: Select Item
 Device for PStack1                                Enter: Select
 VMD Config for PStack2                            +/-: Change Opt.
 ---------------------------------------------     F1: General Help
 ---                                               F2: Previous Values
 Intel® VMD for           [Disable]                F3: Optimized Defaults
 Volume Management                                 F4: Save & Exit
 Device for PStack2                                ESC: Exit

      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                   AB
```

BIOS Setting	Description
Intel® VMD for Volume Management Device for PStack 0 / 1 / 2	Enables / Disables Intel® Volume Management Device Technology in this Stack.

3.6.5.6. Intel® AIC Retimer / AIC SSD Technology (non-VMD)



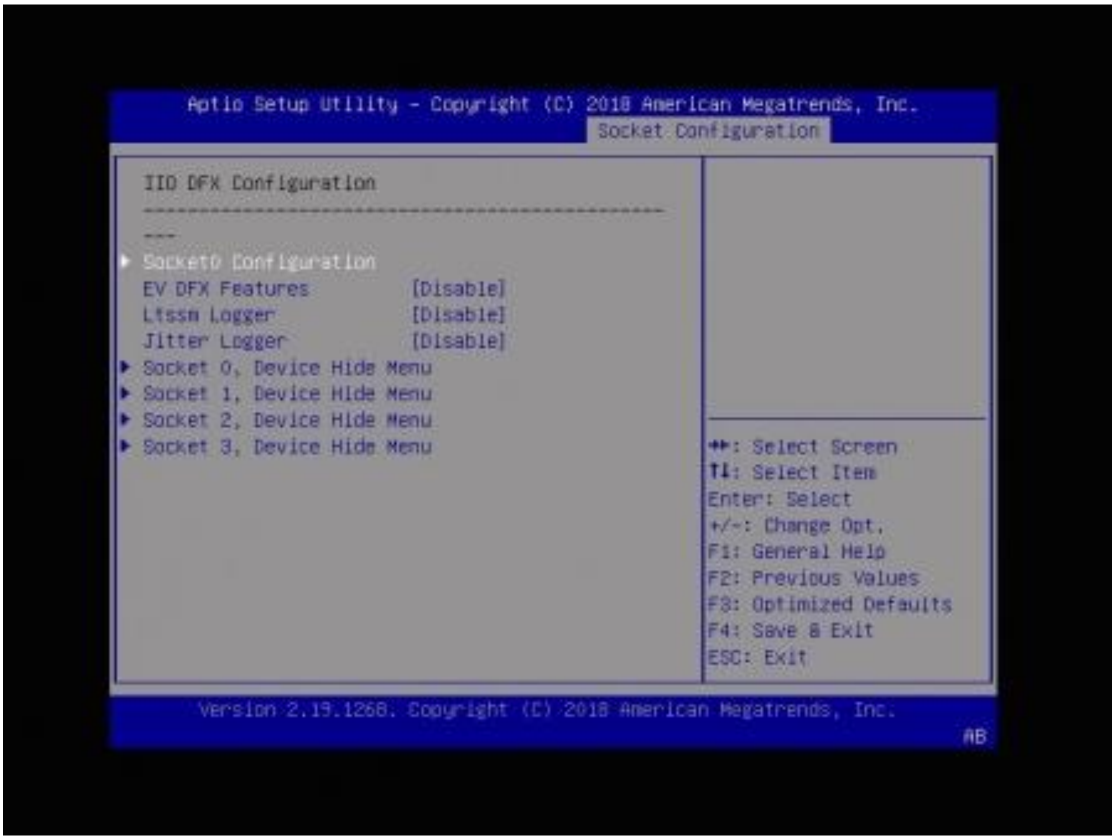
```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                      Socket Configuration

Intel® AIC Retimer/AIC SSD Technology (non-VMD)
--------------------------------------------------
---

▶ Intel® AIC Retimer/AIC SSD on Socket 0

                                                   ↔: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
```



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                      Socket Configuration

Intel® AIC                [Disable]      Anounce Intel® AIC
Retimer/AIC SSD HW                       Retimer/AIC SSD HW at
at PStack0                               PStack0(Port1A-1D).
--------------------------------------   Override IOU0
---                                      bifurcation if required
Intel® AIC                [Disable]
Retimer/AIC SSD HW
at PStack1
--------------------------------------
---                                      ↔: Select Screen
Intel® AIC                [Disable]      ↑↓: Select Item
Retimer/AIC SSD HW                       Enter: Select
at PStack2                               +/-: Change Opt.
                                         F1: General Help
                                         F2: Previous Values
                                         F3: Optimized Defaults
                                         F4: Save & Exit
                                         ESC: Exit

      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                   AB
```

BIOS Setting	Description
Intel® AIC Retimer/AIC SSD HW at PStack 0 / 1 / 2	Anounce Intel® AIC Retimer/AIC SSD HW at PStack0 / 1 / 2 (Port1A-1D / Port2A-2D / Port3A-3D). Override IOU0 bifurcation if required.

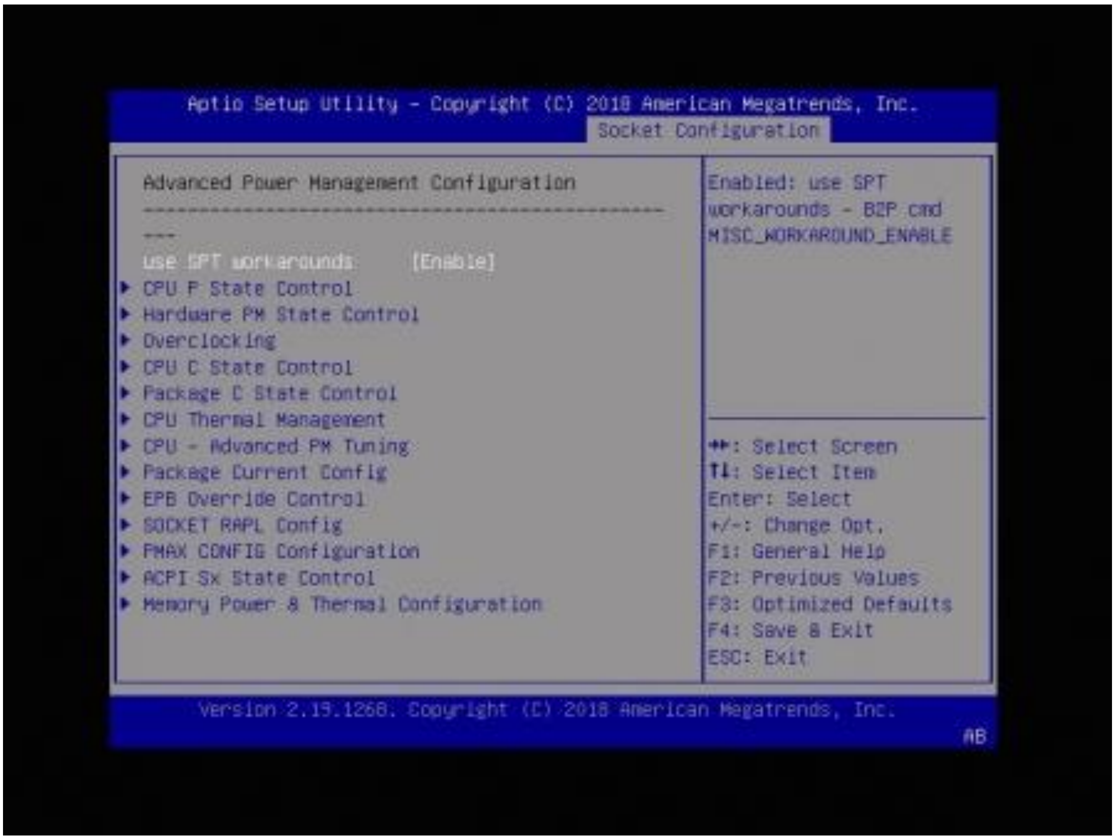
3.6.5.7. IIO DFX Configuration



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                             Socket Configuration
   IIO DFX Configuration
   ----------------------------------------------
   ---
 ► Socket0 Configuration
   EV DFX Features            [Disable]
   Ltssm Logger               [Disable]
   Jitter Logger              [Disable]
 ► Socket 0, Device Hide Menu
 ► Socket 1, Device Hide Menu
 ► Socket 2, Device Hide Menu
 ► Socket 3, Device Hide Menu
                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit
         Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
Socket 0 Configuration	Configures Socket 0 DFX PCIe ports.
EV DFX Features	Exposes IIO DFX devices and other CPU devices like PMON.
Ltssm Logger	Enables / Disables Ltssm Logger for PCIe functionality.
Jitter Logger	Enables / Disable Jitter Logger for PCIe functionality.
Socket 0 / 1 / 2 / 3, Device Hide Menu	Displays Socket 0/1/2/3 device hide menu.

3.6.6 Advanced Power Management Configuration

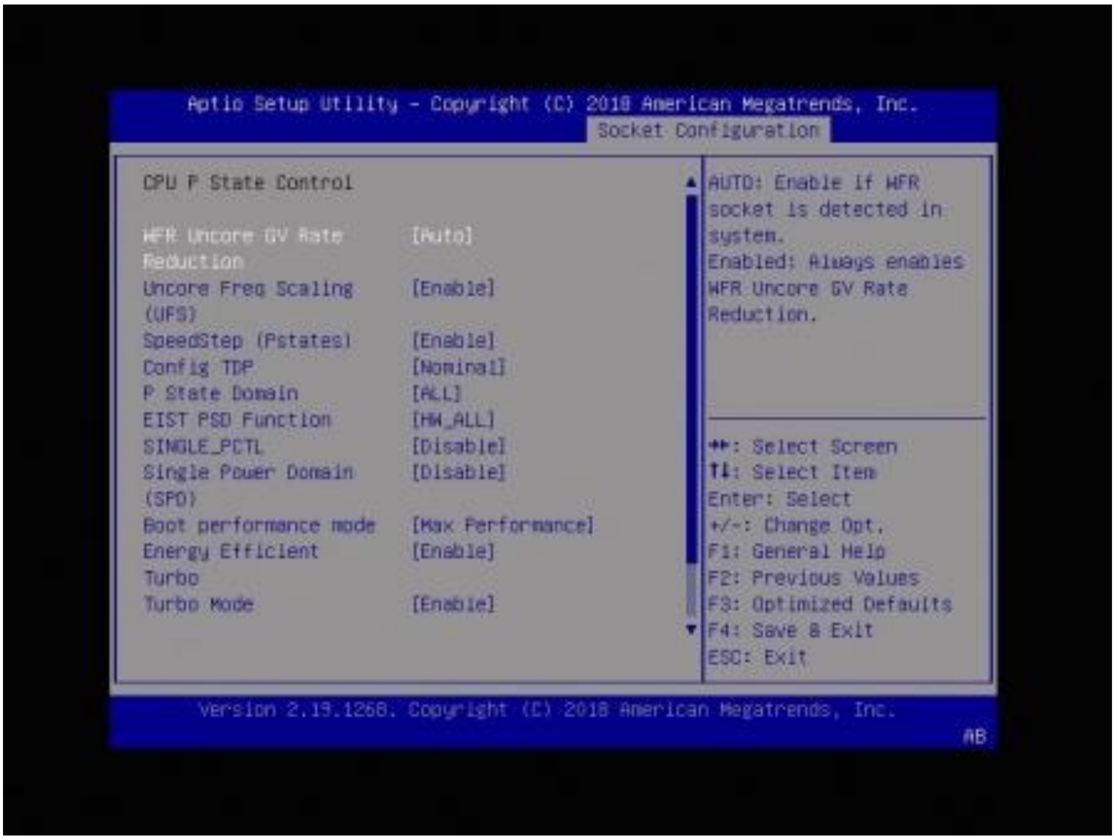


```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                Socket Configuration
 Advanced Power Management Configuration      | Enabled: use SPT
 -------------------------------------------- | workarounds - B2P cmd
 ---                                          | MISC_WORKAROUND_ENABLE
 Use SPT workarounds        [Enable]          |
▶ CPU P State Control                         |
▶ Hardware PM State Control                   |
▶ Overclocking                                |
▶ CPU C State Control                         |
▶ Package C State Control                     |
▶ CPU Thermal Management                      |--------------------------
▶ CPU - Advanced PM Tuning                    | →←: Select Screen
▶ Package Current Config                      | ↑↓: Select Item
▶ EPB Override Control                        | Enter: Select
▶ SOCKET RAPL Config                          | +/-: Change Opt.
▶ PMAX CONFIG Configuration                   | F1: General Help
▶ ACPI Sx State Control                       | F2: Previous Values
▶ Memory Power & Thermal Configuration        | F3: Optimized Defaults
                                              | F4: Save & Exit
                                              | ESC: Exit
      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                     AB
```

BIOS Setting	Description
Use SPT workarounds	Enable – Use SPT workarounds – B2P cmd MISC_WORKAROUND_ENABLE
CPU P State Control	P state control configuration sub menu, including Turbo, XE, etc.
Hardware PM State Control	Controls the hardware PM state.
Overclocking	Provide manual XE Ratio Limit setting.
CPU C State Control	Sets the CPU C state setting.
Package C State Control	Configures the C state setting.
CPU Thermal Management	Manages the CPU thermal conditions.
CPU – Advanced PM Tuning	Sets the energy per Bias, Pwr_Ctl, PP0 Current SWLTD, SAPM, etc.
Package Current Config	Programs PRI_PLANE_CURT_CFG_CTRL_MSR 0x601 sub menu.

BIOS Setting	Description
EPB Override Control	Programs CSR_DYNAMIC_PERF_POWER_CTL 1:10:2:0x64 sub menu.
SOCKET RAPL Config	Socket RAPL configuration sub menu – TURBO_POWER_LIMIT CSR & MSR.
PMAX CONFIG Configuration	Displays the PMAX configuration control sub menu.
ACPI Sx State Control	Controls the ACPI Sx State individually.
Memory Power & Thermal Configuration	Displays and provides option to change the memory settings.

3.6.6.1. CPU P State Control

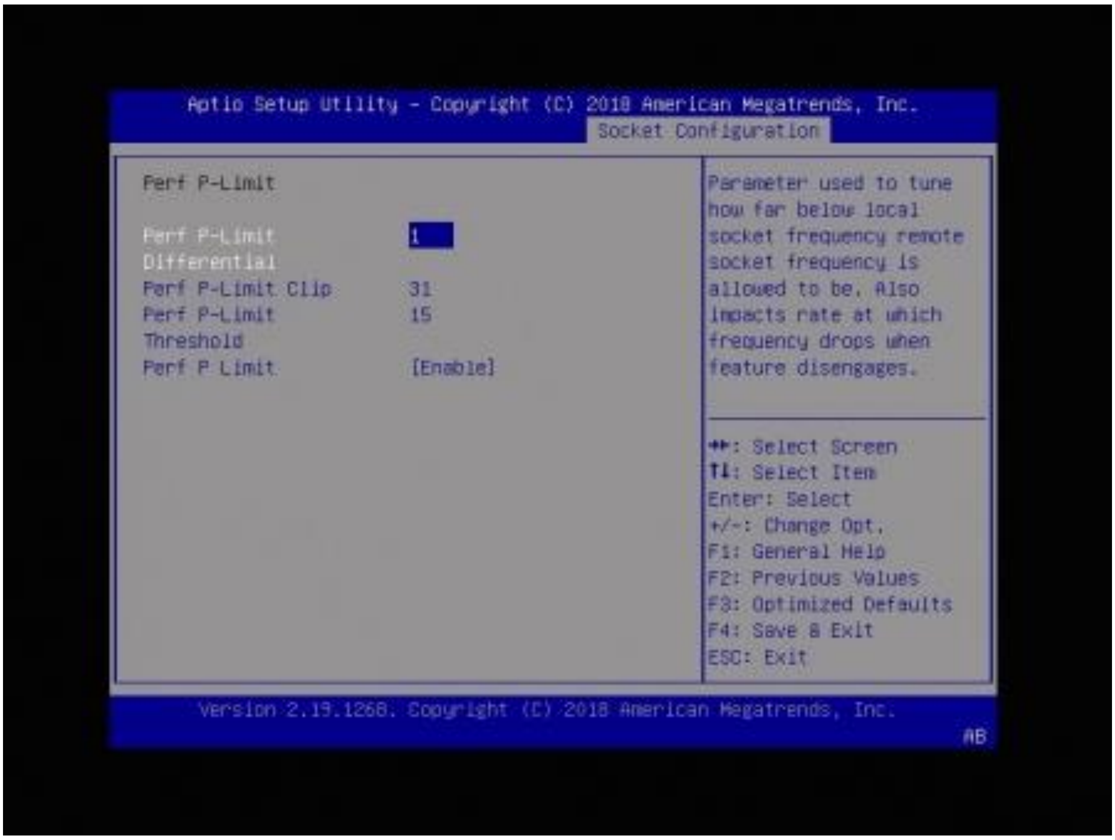


```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration
  CPU P State Control                                 AUTO: Enable if WFR
                                                      socket is detected in
  WFR Uncore GV Rate         [Auto]                   system.
  Reduction                                           Enabled: Always enables
  Uncore Freq Scaling        [Enable]                 WFR Uncore GV Rate
  (UFS)                                               Reduction.
  SpeedStep (Pstates)        [Enable]
  Config TDP                 [Nominal]
  P State Domain             [ALL]
  EIST PSD Function          [HW_ALL]
  SINGLE_PCTL                [Disable]                ↔: Select Screen
  Single Power Domain        [Disable]                ↑↓: Select Item
  (SPD)                                               Enter: Select
  Boot performance mode      [Max Performance]        +/-: Change Opt.
  Energy Efficient           [Enable]                 F1: General Help
  Turbo                                               F2: Previous Values
  Turbo Mode                 [Enable]                 F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                          AB
```

BIOS Setting	Description
WFR Uncore GV Rate Reduction	Auto – Enables the feature if WFT socket is detected in system. Enable – Always enables WFR Uncore GV rate reduction.

BIOS Setting	Description
Uncore Freq Scaling (UFS)	Enables / Disables automous uncore frequency scaling.
SpeedStep (Pstates)	Enables / Disables EIST (P-States).
Config TDP	Config TDP level selection. Options: Normal, Level 1, Level 2
P State Domain	Per Logical (ONE): indicates the P-state domain for each logical proc in the system. Per Package (ALL): all procs indicate the same domai in the same package.
EIST PSD Function	Chooses HW_ALL, SW_ALL, SW_ANY in _PSD return.
SINGLE_PCTL	Single PCTL mode makes all cores in the processor go to the most recent ratio request.
Single Power Domain (SPD)	Single power domain aggregates the request from all cores and the highest request ratio is applied to all cores on the processor.
Boot Performance Mode	Select the performance state that the BIOS Will set before OS hand off. Options: Max Performance, Max Efficient, Set by Intel Node Manager
Energy Efficient Turbo	Enables / Disables Energy efficient turbo, MSR 0x1FC [19].
Turbo Mode	Enables / Disables processor turbo mode (requires EMTTM enabled too).
CPU Flex Ratio Override	Enables / Disables CPU flex ratio programming.
Perf P-Limit	Program PERF _P _LIMIT 1:30:2:0xe4 sub menu.

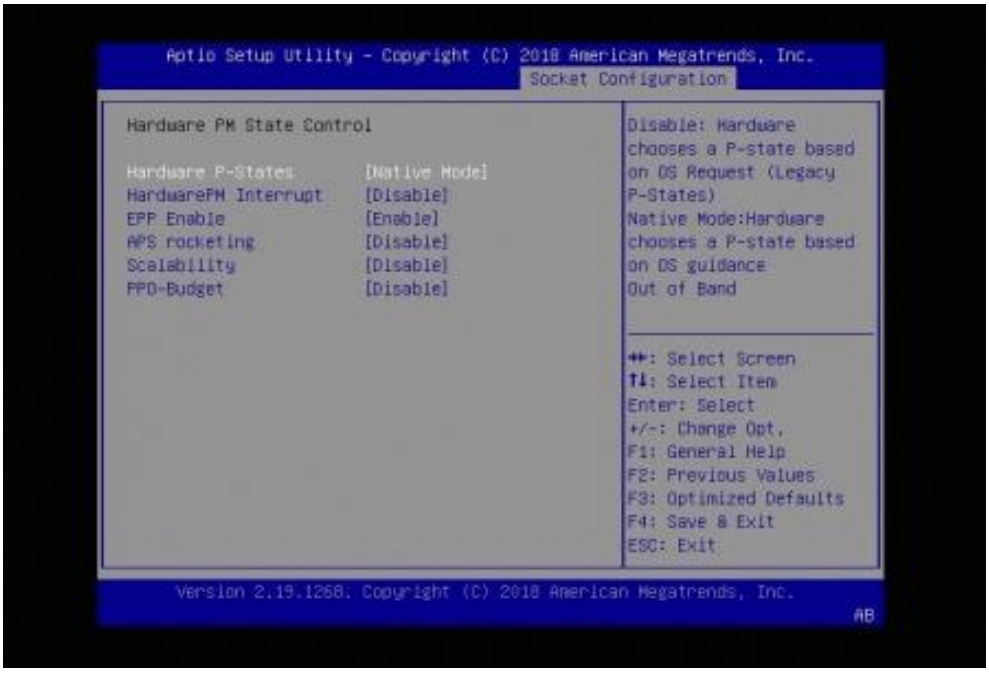
Perf P-Limit



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                Socket Configuration

Perf P-Limit                                     Parameter used to tune
                                                 how far below local
Perf P-Limit            1                        socket frequency remote
Differential                                     socket frequency is
Perf P-Limit Clip       31                       allowed to be. Also
Perf P-Limit            15                       impacts rate at which
Threshold                                        frequency drops when
Perf P Limit            [Enable]                 feature disengages.

                                                 ↔: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                  AB
```

BIOS Setting	Description
Perf P-Limit Differential	Parameter used to tune how far bellow local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.
Perf P-Limit Clip	Maximum value the floor is allowed to be set to for perf P-Limit.
Perf P-Limit Threshold	Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.
Perf P Limit	Enables / Disables performance P-Limit.

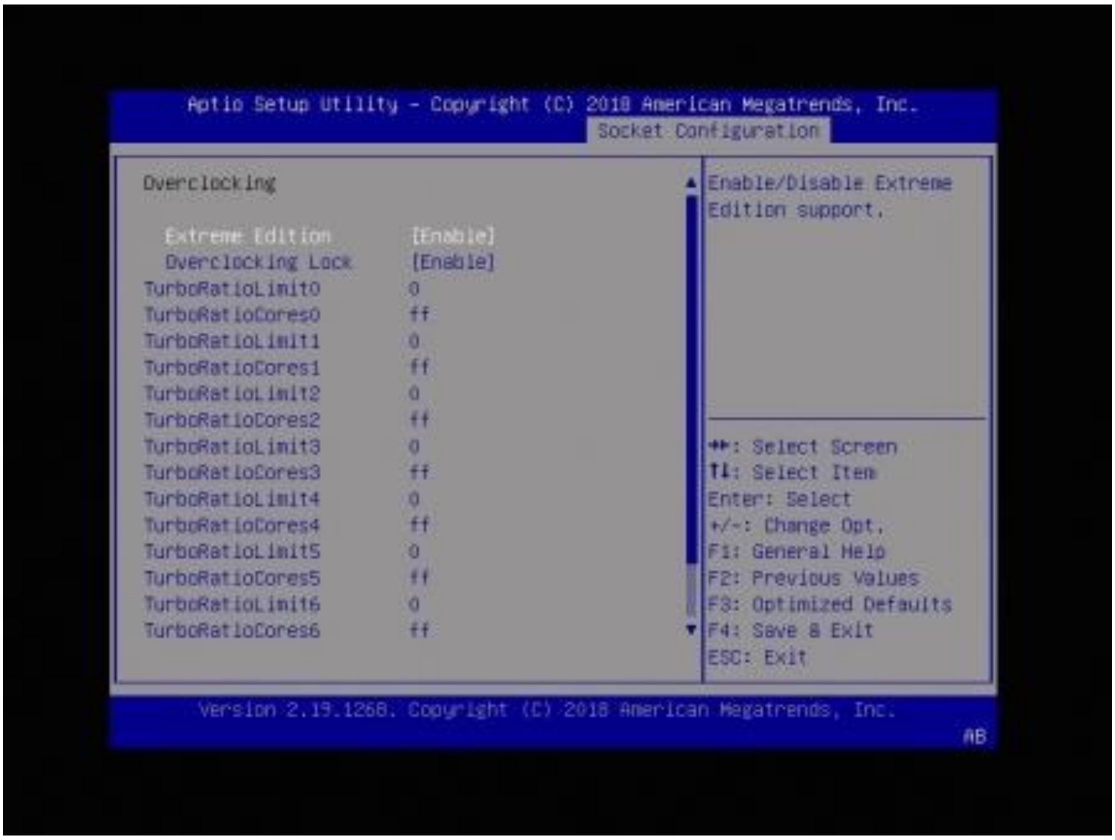
3.6.6.2. Hardware PM State Control



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration
 Hardware PM State Control                             Disable: Hardware
                                                       chooses a P-state based
 Hardware P-States          [Native Mode]              on OS Request (Legacy
 HardwarePM Interrupt       [Disable]                  P-States)
 EPP Enable                 [Enable]                   Native Mode:Hardware
 APS rocketing              [Disable]                  chooses a P-state based
 Scalability                [Disable]                  on OS guidance
 PPO-Budget                 [Disable]                  Out of Band

                                                       ↔: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit
           Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
Hardware P-States	Disable: Hardware chooses a P-state based on OS request (Legacy P-States). Native Mode: Hardware chooses a P-state based on OS guidance. Options: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support
HardwarePM Interrupt	Enables / Disables hardware PM interruption.
EPP Enable	When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP.APS
APS Rocketing	Enables / Disables the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to Jump to max. turbo instantaneously.
Scalability	Enables / Disables the use of scalability in HMP pcode power efficiency algorithms. Scalability is the measure of estimated performance improvement for a given increase in core.
PP0-Budget	Enables / Disables core parameter based per core power budgeting. PP-=Budget allocates power budget to cores based on their scalability/EPP.

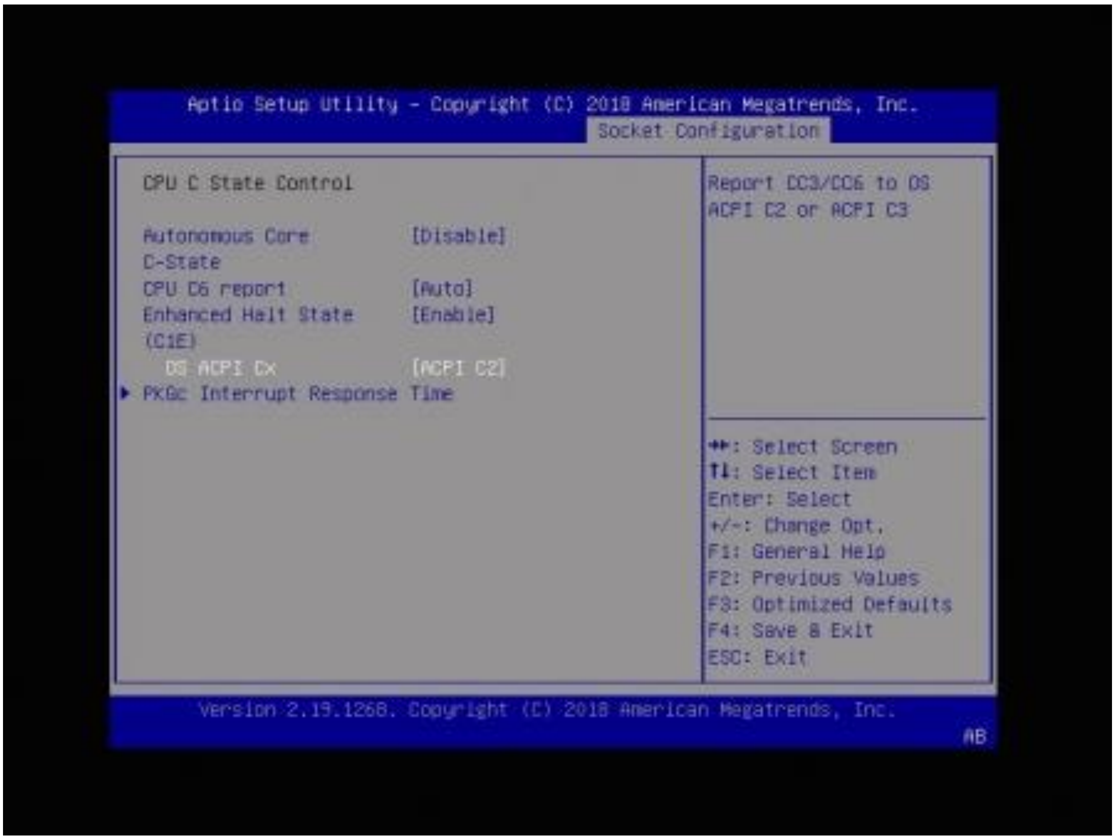
3.6.6.3. Overclocking



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                        Socket Configuration

Overclocking                                  Enable/Disable Extreme
                                              Edition support.
  Extreme Edition         [Enable]
  Overclocking Lock       [Enable]
TurboRatioLimit0          0
TurboRatioCores0          ff
TurboRatioLimit1          0
TurboRatioCores1          ff
TurboRatioLimit2          0
TurboRatioCores2          ff
TurboRatioLimit3          0                   ↔: Select Screen
TurboRatioCores3          ff                  ↑↓: Select Item
TurboRatioLimit4          0                   Enter: Select
TurboRatioCores4          ff                  +/-: Change Opt.
TurboRatioLimit5          0                   F1: General Help
TurboRatioCores5          ff                  F2: Previous Values
TurboRatioLimit6          0                   F3: Optimized Defaults
TurboRatioCores6          ff                  F4: Save & Exit
                                              ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                              AB
```

BIOS Setting	Description
Extreme Edition	Enables / Disables Extreme Edition support.
Overclocking Lock	Enables / Disables Overclocking.
LOT26 Enable	For HEDT *only*, select whether VR power is turned off to empty DIMM channels.

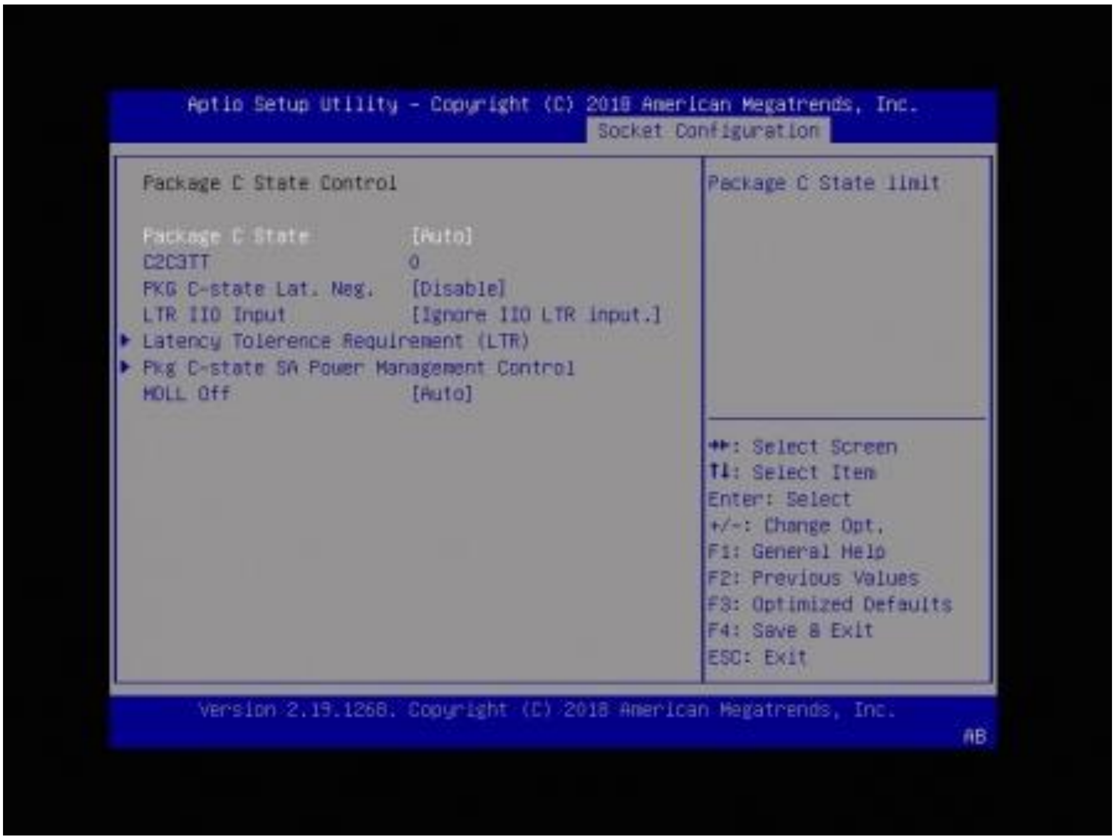
3.6.6.4. CPU C State Control



```
         Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                   Socket Configuration
  CPU C State Control                              Report CC3/CC6 to OS
                                                   ACPI C2 or ACPI C3
  Autonomous Core          [Disable]
  C-State
  CPU C6 report            [Auto]
  Enhanced Halt State      [Enable]
  (C1E)
    OS ACPI Cx             [ACPI C2]
▶ PKGc Interrupt Response Time
                                                   ↔: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit
          Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                         AB
```

BIOS Setting	Description
Autonomous Core C-State	Controls the autonomous core C-state.
CPU C6 report	Enables / Disables CPU C6 (ACPI C3) report to OS.
Enahnced Halt State (C1E)	Enables / Disables core C1E auto promotion control. Takes effect after reboot.
OS ACPI Cx	Report CC3/CC6 to OS ACPI C2 or ACPI C3.
PKGc Interrupt Response Time	Programmable package C-state interruption resonse time setup control.

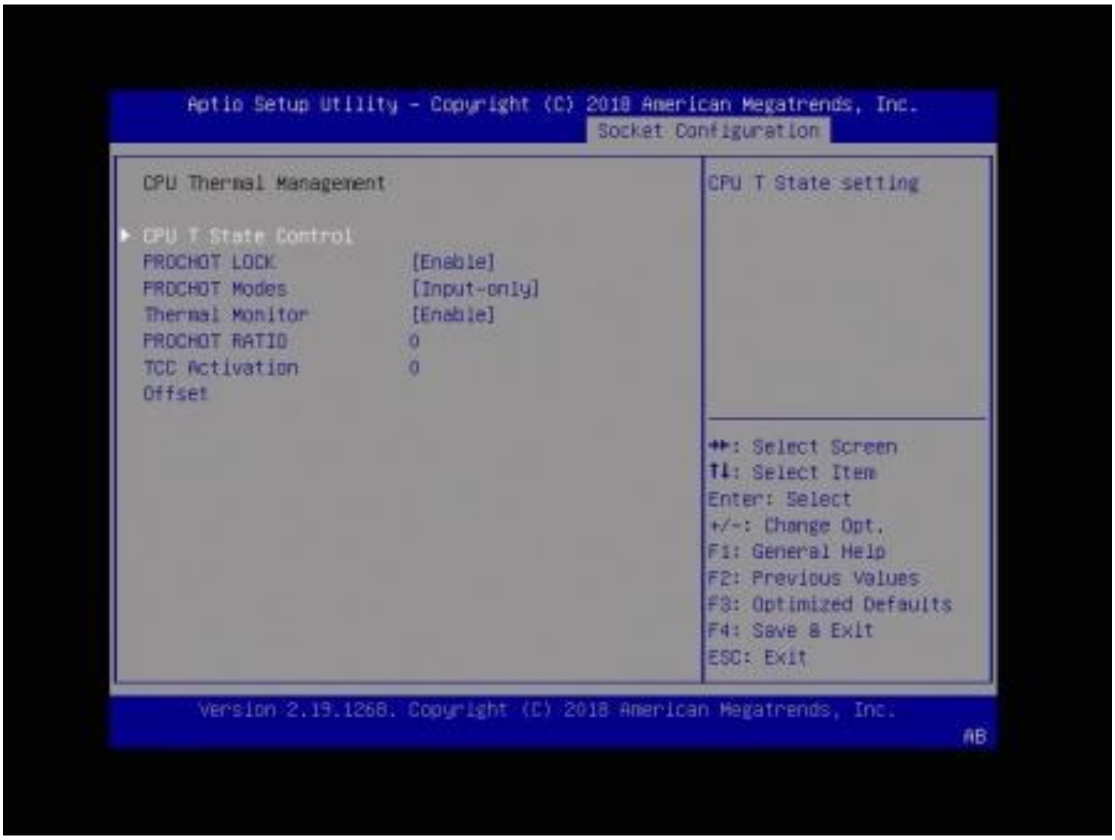
3.6.6.5. Package C State Control



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                                  Socket Configuration
  Package C State Control                             Package C State limit

  Package C State            [Auto]
  C2C3TT                     0
  PKG C-state Lat. Neg.      [Disable]
  LTR IIO Input              [Ignore IIO LTR input.]
▶ Latency Tolerence Requirement (LTR)
▶ Pkg C-state SA Power Management Control
  MDLL Off                   [Auto]
                                                      ↔: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                         AB
```

BIOS Setting	Description
Package C State	Configures the package C state limit. Options: C0/C1 state, C2 state, C6 (non Retention) state, C6 (Retention) state, No Limit, Auto
C2C3TT	Default = 0, means [Auto]. C2 to C3 Transition Timer, PPDN_INIT – 1:10:1:74 Bit [11:0].
PKG C-state Lat. Neg.	MSR 1FCh Bit [30] = PCH_NEG_DISABLE
LTR IIO Input	MSR 1FCh Bit [29] = LTR_IIO_DISABLE. Disable – Innores IIO LTR input. Options: Take IIO LTR input, Ingore IIO LTR input
Latency Tolerence Requirement (LTR)	Program CSR_SWLTROVRD 1:10:1:0x78 sub menu.
Plg C-state SA Power Management Control MDLL Off	Programs CSR_SAPMCTL 1:30:1:0xb0 sub menu.
MDLL Off	Enables / Disables to shut down MDLL during SR.

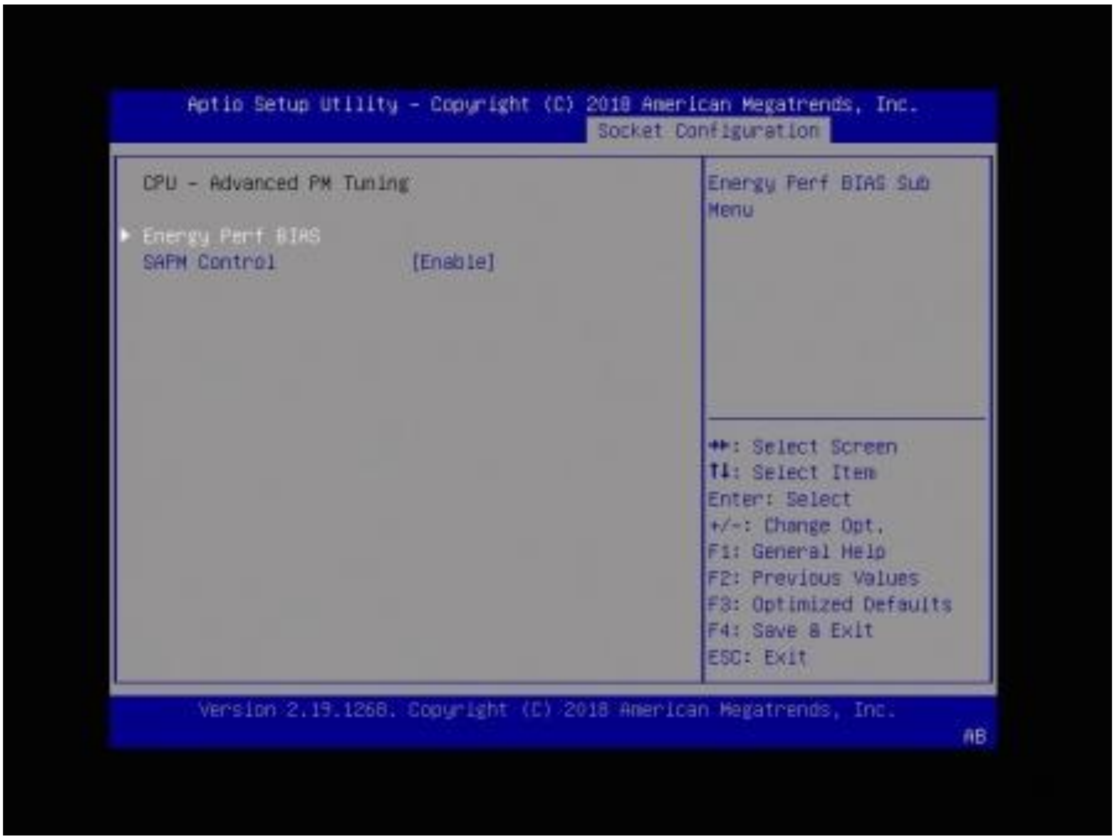
3.6.6.6. CPU Thermal Management



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                         Socket Configuration
  CPU Thermal Management                              CPU T State setting

▶ CPU T State Control
  PROCHOT LOCK                [Enable]
  PROCHOT Modes               [Input-only]
  Thermal Monitor             [Enable]
  PROCHOT RATIO               0
  TCC Activation              0
  Offset
                                                      ↔: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                        AB
```

BIOS Setting	Description
CPU T State Control	CPU T State setting.
PROCHOT LOCK	Setting this bit will lock in xxPROCHOT# response configurations including ENABLE_BIDR_PROCHOT, DIS_PROCHOT_OUT, VR_THERM_ALERT_DISABLE, and PROCHOT_LOCK.
PROCHOT Modes	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. Options: Output-only, Disable, Both Input and Output, Input-only
Thermal Monitor	Enables / Disables thermal monitor.

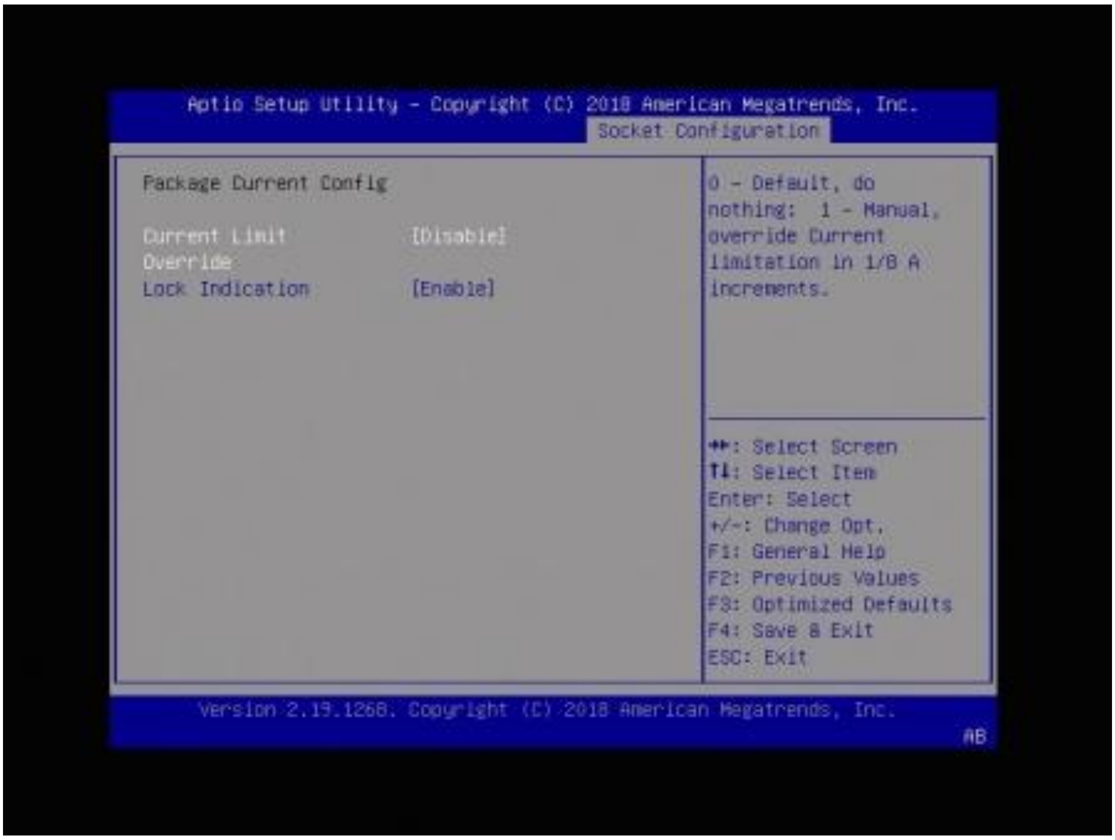
3.6.6.7. CPU – Advanced PM Tuning



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                           Socket Configuration

CPU - Advanced PM Tuning                      Energy Perf BIAS Sub
                                              Menu
▶ Energy Perf BIAS
  SAPM Control             [Enable]

                                              ↔: Select Screen
                                              ↑↓: Select Item
                                              Enter: Select
                                              +/-: Change Opt.
                                              F1: General Help
                                              F2: Previous Values
                                              F3: Optimized Defaults
                                              F4: Save & Exit
                                              ESC: Exit

      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Energy Perf BIAS	Displays the Energy Perf BIAS sub menu.
SAPM Control	MAR 1FCh Bit [22] = PWR_PERF_TUNING_DISABLE_SAPM_CTRL.

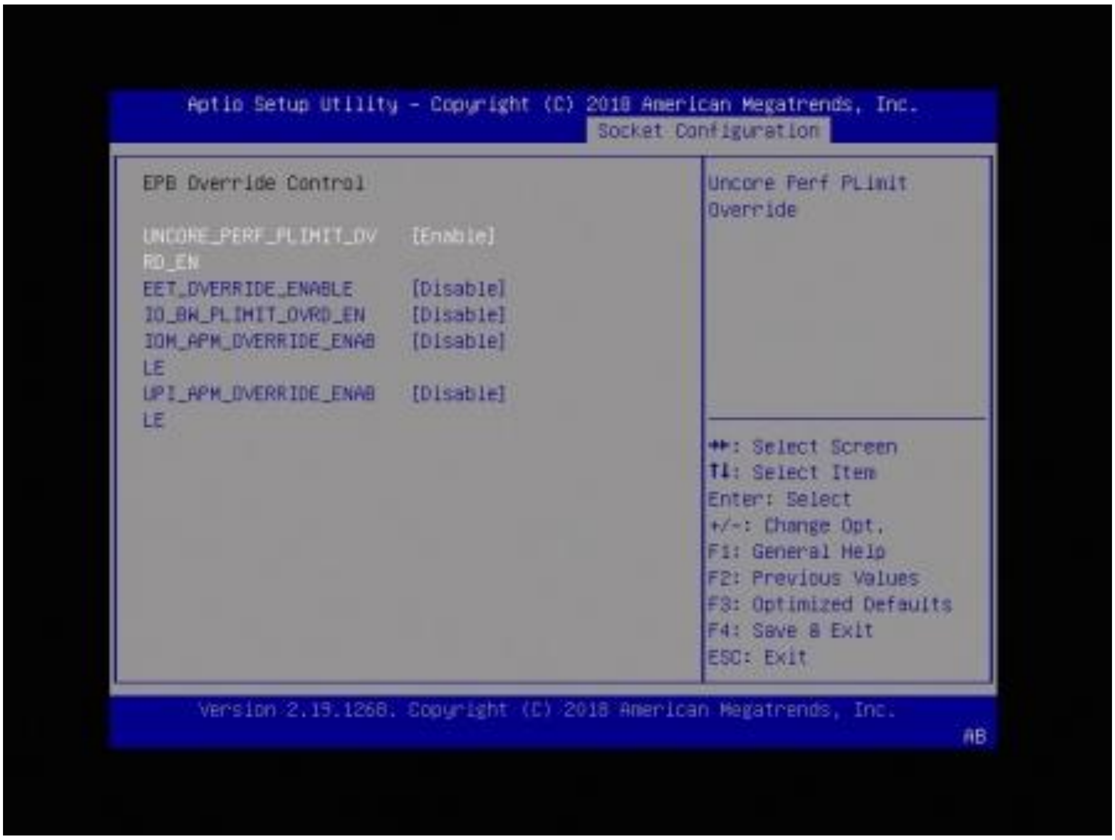
3.6.6.8. Package Current Config



```
        Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration
 Package Current Config                        0 - Default, do
                                               nothing:  1 - Manual,
 Current Limit          [Disable]              override Current
 Override                                      limitation in 1/8 A
 Lock Indication        [Enable]               increments.

                                               ↔: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit
         Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
Current Limit Override	0 – Default, do nothing. 1 – Manual, override Current limitation in 1/8 A increments.
Lock Indication	Enables / Disables lock for CURRENT_LIMIT settings.

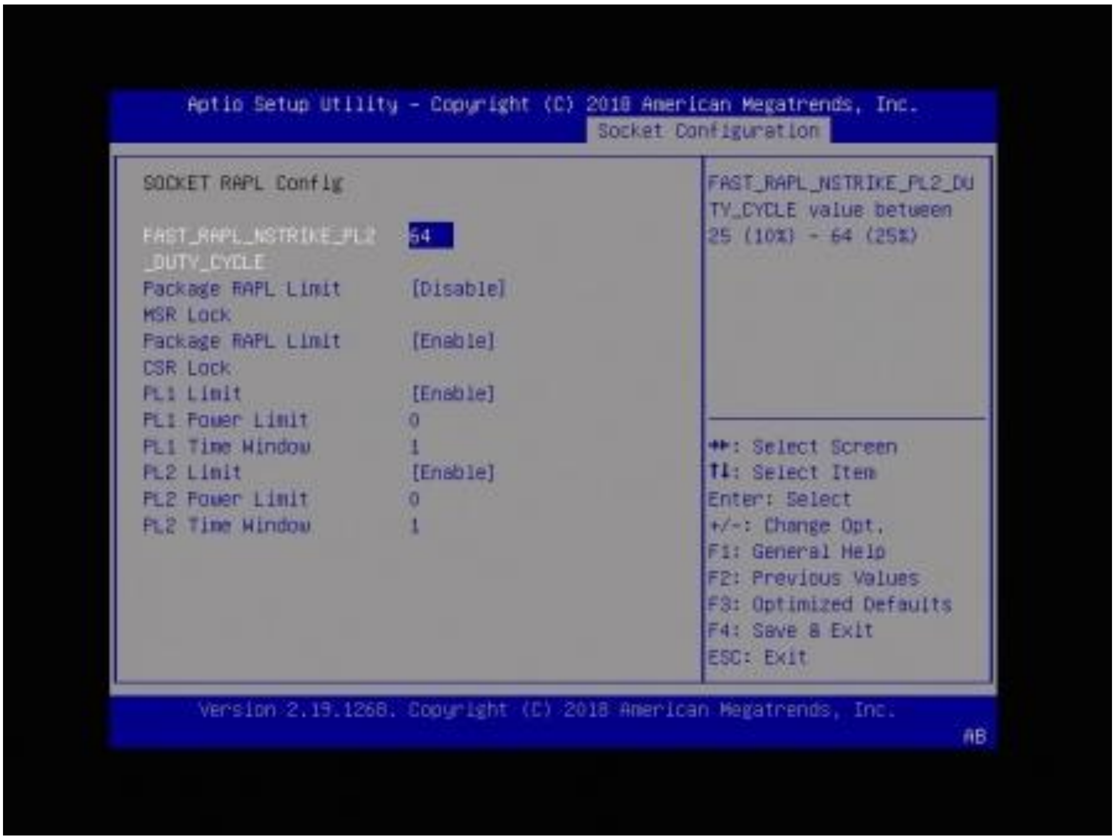
3.6.6.9. EPB Override Control



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                          Socket Configuration

EPB Override Control                                Uncore Perf PLimit
                                                    Override
UNCORE_PERF_PLIMIT_OV      [Enable]
RD_EN
EET_OVERRIDE_ENABLE        [Disable]
IO_BW_PLIMIT_OVRD_EN       [Disable]
IOM_APM_OVERRIDE_ENAB      [Disable]
LE
UPI_APM_OVERRIDE_ENAB      [Disable]
LE
                                                    ←→: Select Screen
                                                    ↑↓: Select Item
                                                    Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
                                                    F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                 AB
```

BIOS Setting	Description
UNCORE_PERF_PLIMIT_0VRD_EN	Uncore Perf PLimit Override
EET_OVERRIDE_ENABLE	Enables / Disables EET override
IO_BW_PLIMIT_OVRD_EN	Enables / Disables IO BW PLimit override
IOM_APM_OVERRIDE_ENABLE	Enables / Disables IOM APM override
UPI_APM_OVERRIDE_ENABLE	Enables / Disables UPI APM override

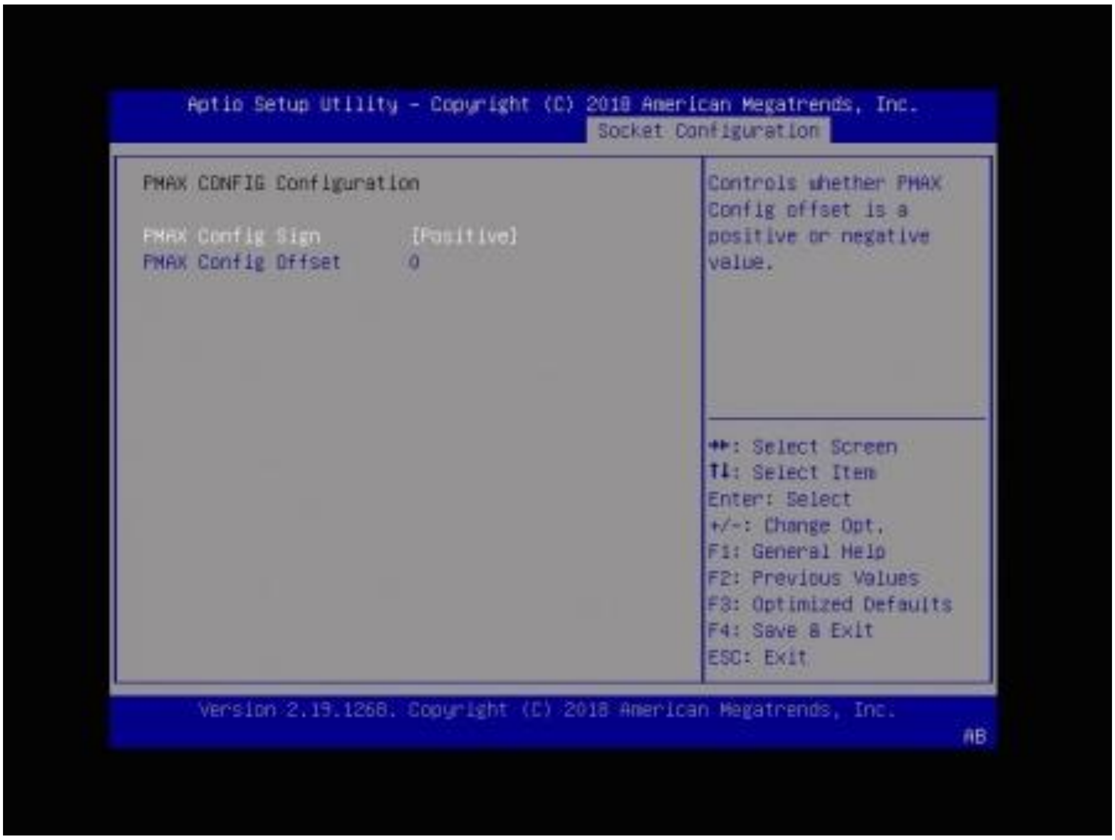
3.6.6.10. SOCKET RAPL Config



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                    Socket Configuration

SOCKET RAPL Config                              FAST_RAPL_NSTRIKE_PL2_DU
                                                TY_CYCLE value between
FAST_RAPL_NSTRIKE_PL2      64                   25 (10%) - 64 (25%)
_DUTY_CYCLE
Package RAPL Limit         [Disable]
MSR Lock
Package RAPL Limit         [Enable]
CSR Lock
PL1 Limit                  [Enable]
PL1 Power Limit            0
PL1 Time Window            1
PL2 Limit                  [Enable]
PL2 Power Limit            0
PL2 Time Window            1

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) ~ 64 (25%)
Package RAPL Limit MSR Lock	Enables / Disables locking of package RAPL Limit MSR and a reset will be required to unlock the register.
Package RAPL Limit CSR Lock	Enables / Disables locking of package RAPL Limit MSR and a reset will be required to unlock the register.
PL1 Limit / PL1 Power Limit / PL1 Time Window	Enables / Disables PL1. If this option is disabled, BIOS will program the default values for PL1 power limit and PL1 time window.
PL2 Limit / PL2 Power Limit / PL2 Time Window	Enables / Disables PL2. If this option is disabled, BIOS will program the default values for PL2 power limit and PL2 time window.

3.6.6.11. PMAX CONFIG Configuration



Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Socket Configuration

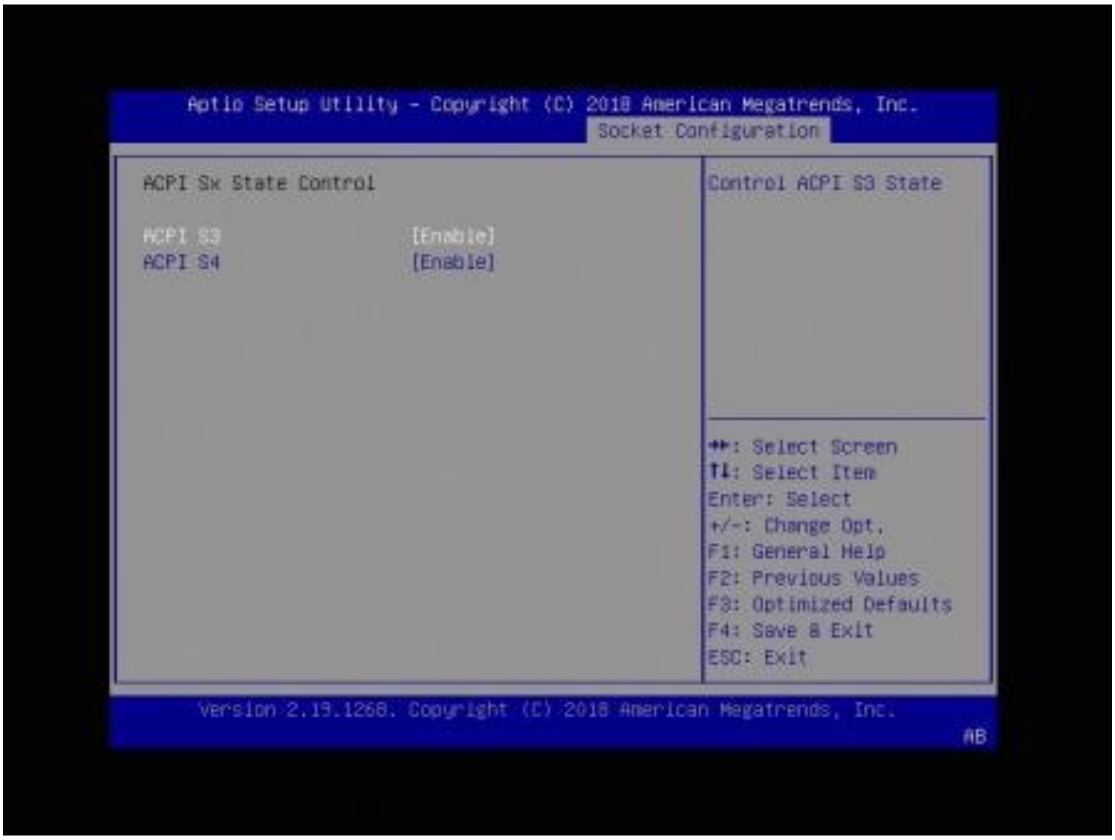
PMAX CONFIG Configuration

PMAX Config Sign [Positive]
PMAX Config Offset 0

Controls whether PMAX Config offset is a positive or negative value.

BIOS Setting	Description
PMAX Config Sign	Controls whether PMAX config offset is a positive or negative value.
PMAX Config Offset	Input decimal correction factor to program. Valid input values are 0 to 15. Will be positive or negative based on PMAX Config Sign value.

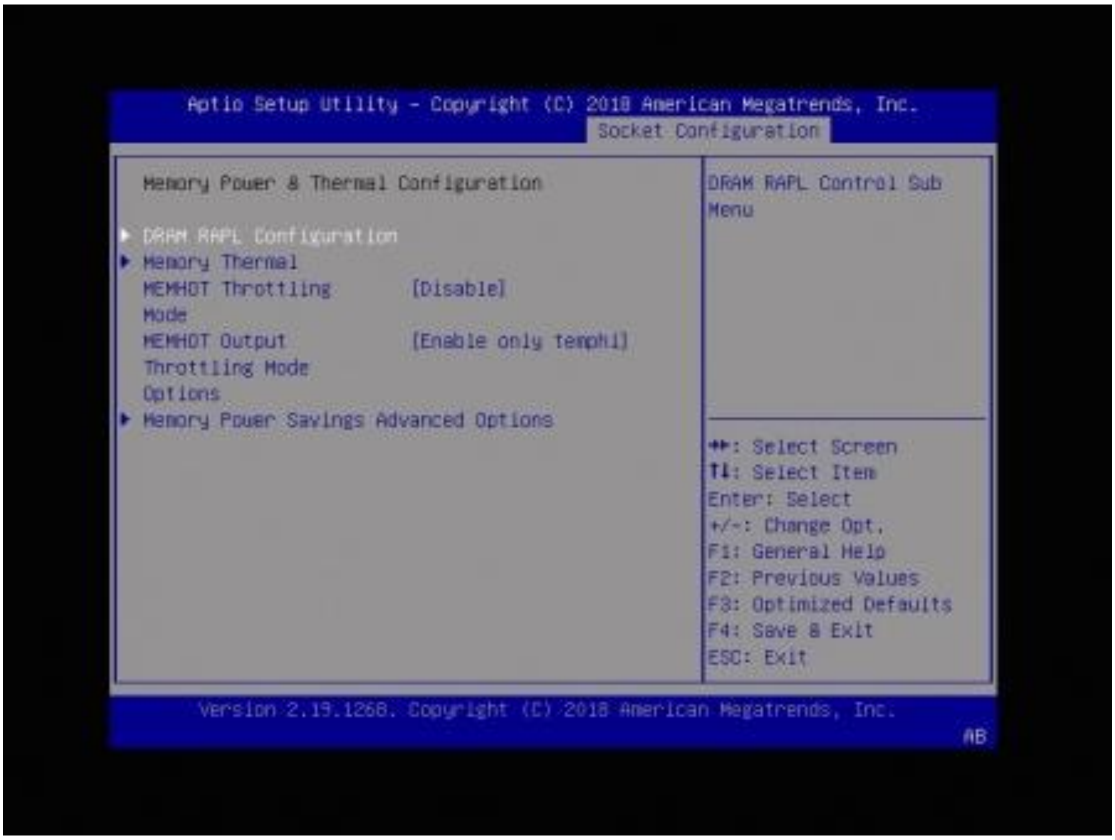
3.6.6.12. ACPI Sx State Control



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                              Socket Configuration

ACPI Sx State Control                          Control ACPI S3 State

ACPI S3                    [Enable]
ACPI S4                    [Enable]

                                               ↔: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit

     Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                   AB
```

BIOS Setting	Description
ACPI S3	Controls ACPI S3 state.
ACPI S4	Controls ACPI S4 state.

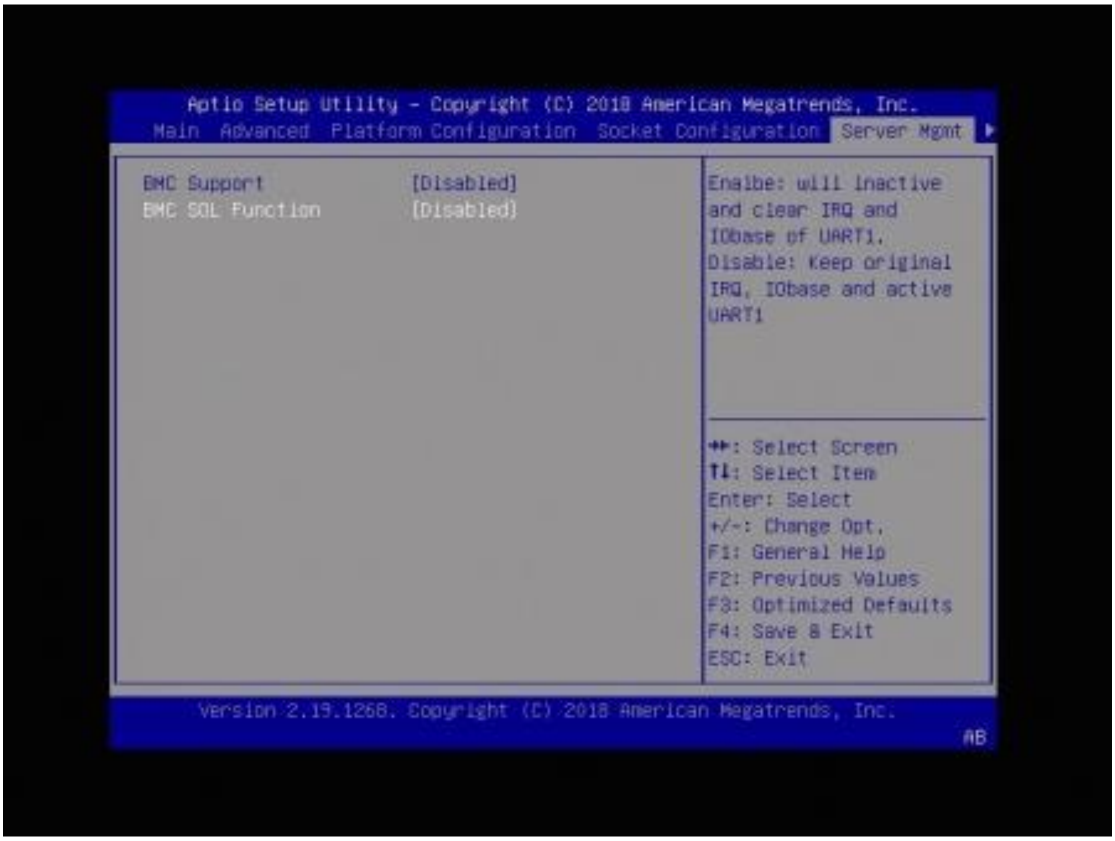
3.6.6.13. Memory Power & Thermal Configuration



```
       Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
                                               Socket Configuration
  Memory Power & Thermal Configuration              DRAM RAPL Control Sub
                                                    Menu
▶ DRAM RAPL Configuration
▶ Memory Thermal
  MEMHOT Throttling         [Disable]
  Mode
  MEMHOT Output             [Enable only temphi]
  Throttling Mode
  Options
▶ Memory Power Savings Advanced Options
                                                    →←: Select Screen
                                                    ↑↓: Select Item
                                                    Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
                                                    F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit
        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                         AB
```

BIOS Setting	Description
DRAM RAPL Configuration	Displays DRAM RAPL control sub menu.
Memory Thermal	Sets memory thermal settings.
MEMHOT Throttling Mode	Configure MEMHOT input and output modes: memhot sense therm throt or memhot output therm throt. Options: Disable, Output-only, Input-only, Input and Output Enabled
MEMHOT Output Throttling Mode Options	Enables / Disables the throt output high and low bit fields. Options: Disable; Enable only temphi; Enable only temphi & mid; Enable only temphi, mid and low
Memory Power Savings Advanced Options	Advanced Settings for CKE and related memory power saving features.

3.7 Server Management

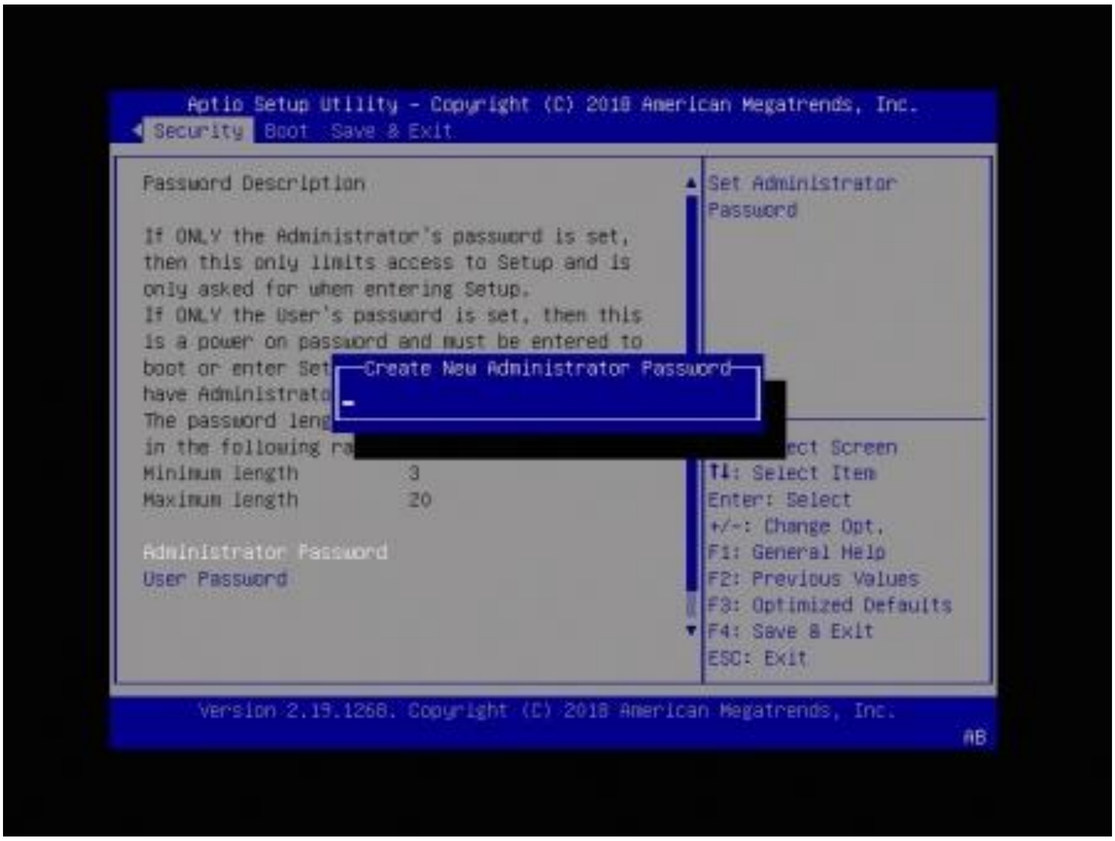

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
Main Advanced Platform Configuration Socket Configuration Server Mgmt ▶
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
AB

```
BMC Support                 [Disabled]
BMC SOL Function            [Disabled]
```

```
Enalbe: will inactive
and clear IRQ and
IObase of UART1.
Disable: Keep original
IRQ, IObase and active
UART1
```

BIOS Setting	Description
BMC Support	Enables / Disables interfaces to communicate with BMC.
BMC SOL Function	Enables / Disables BMC SOL function. **Enable:** will inactive and clear IRQ and IObase of UART1. **Disable:** keep original IRQ, IObase and active UART1

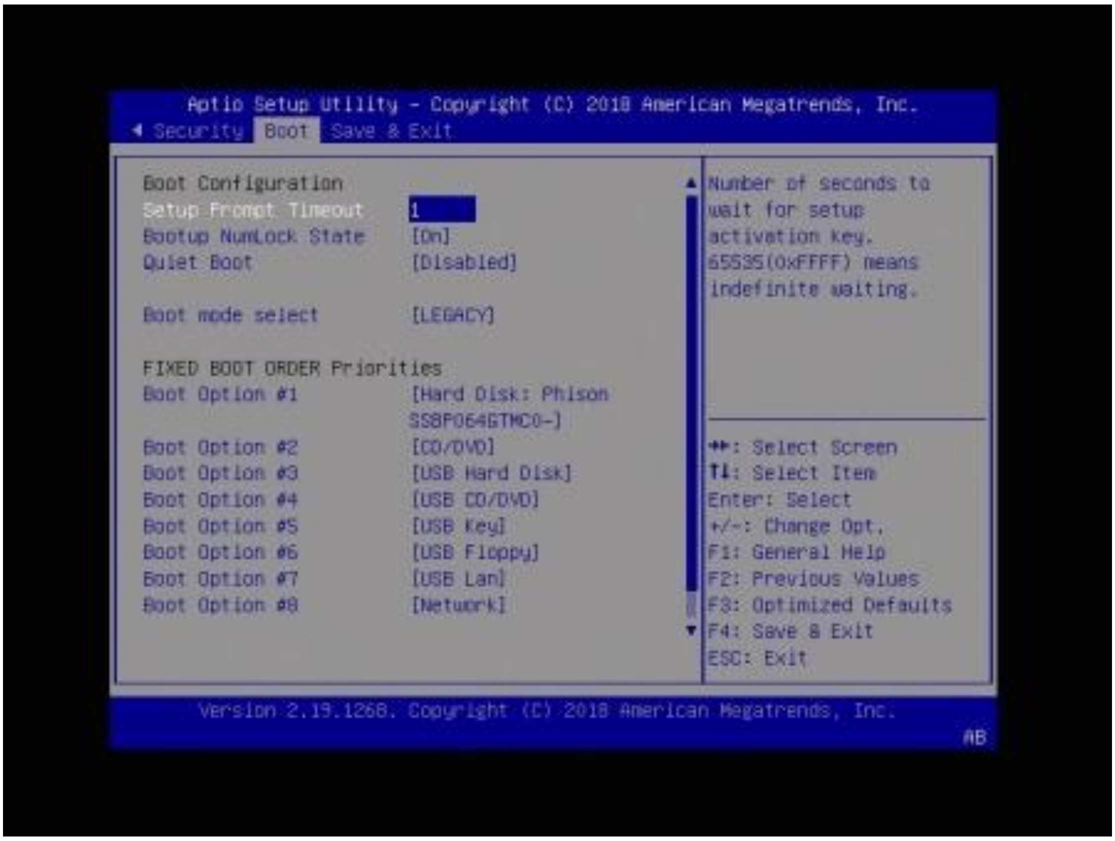
3.8 Security Settings



```
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
◄ Security  Boot  Save & Exit

Password Description                                Set Administrator
                                                    Password
If ONLY the Administrator's password is set,
then this only limits access to Setup and is
only asked for when entering Setup.
If ONLY the User's password is set, then this
is a power on password and must be entered to
boot or enter Set ┌Create New Administrator Password┐
have Administrato │_                                │
The password leng └─────────────────────────────────┘
in the following ra                                    ect Screen
Minimum length          3                           ↑↓: Select Item
Maximum length          20                          Enter: Select
                                                    +/-: Change Opt.
Administrator Password                              F1: General Help
User Password                                       F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

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

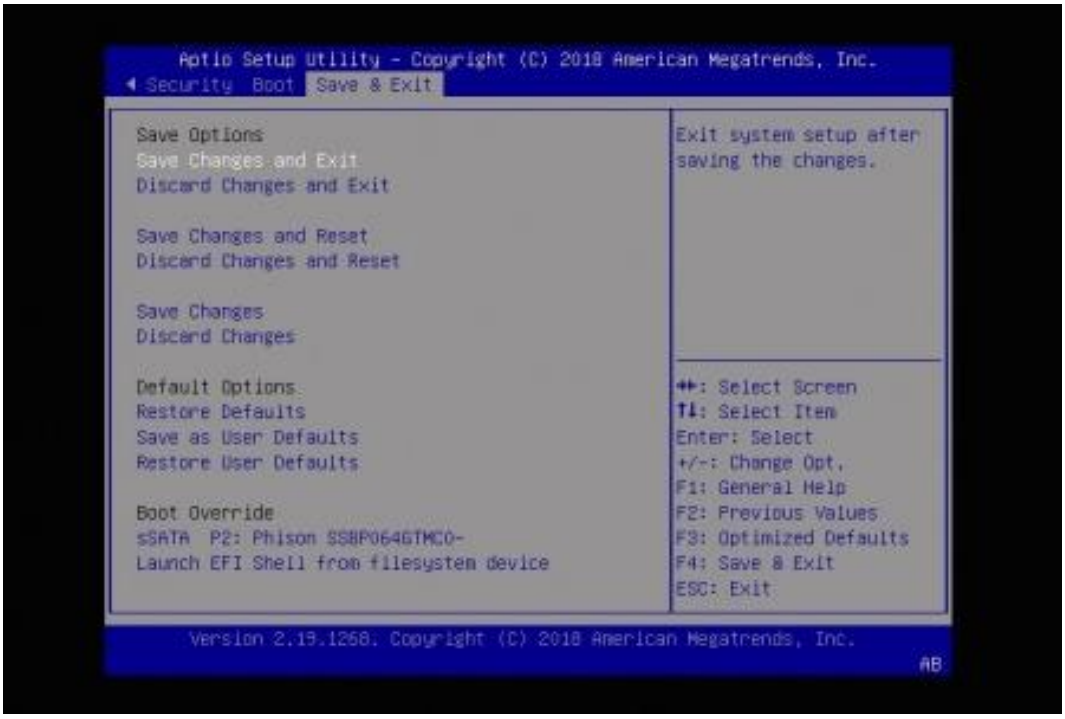
3.9 Boot Settings



```
      Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
 ◄ Security  Boot  Save & Exit
  Boot Configuration                            ▲ Number of seconds to
  Setup Prompt Timeout       1                    wait for setup
  Bootup NumLock State       [On]                 activation key.
  Quiet Boot                 [Disabled]           65535(0xFFFF) means
                                                  indefinite waiting.
  Boot mode select           [LEGACY]

  FIXED BOOT ORDER Priorities
  Boot Option #1             [Hard Disk: Phison
                             SSBP064GTMC0-]
  Boot Option #2             [CD/DVD]             ↔: Select Screen
  Boot Option #3             [USB Hard Disk]      ↑↓: Select Item
  Boot Option #4             [USB CD/DVD]         Enter: Select
  Boot Option #5             [USB Key]            +/-: Change Opt.
  Boot Option #6             [USB Floppy]         F1: General Help
  Boot Option #7             [USB Lan]            F2: Previous Values
  Boot Option #8             [Network]            F3: Optimized Defaults
                                                ▼ F4: Save & Exit
                                                  ESC: Exit
      Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                    AB
```

BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
Boot Mode Select	Selects boot mode Legacy/UEFI.
Boot Option Priorities	Sets the system boot order.
Hard Disk Drive BBS Priorities	Specifies the Boot Device Priority sequence from available Hard Disk Drives.

3.10 Save & Exit Settings



```
        Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
 ◄ Security  Boot  Save & Exit

 Save Options                                    Exit system setup after
 Save Changes and Exit                           saving the changes.
 Discard Changes and Exit

 Save Changes and Reset
 Discard Changes and Reset

 Save Changes
 Discard Changes

 Default Options                                 ↔: Select Screen
 Restore Defaults                                ↑↓: Select Item
 Save as User Defaults                           Enter: Select
 Restore User Defaults                           +/-: Change Opt.
                                                 F1: General Help
 Boot Override                                   F2: Previous Values
 sSATA  P2: Phison SSBP064GTMC0-                 F3: Optimized Defaults
 Launch EFI Shell from filesystem device         F4: Save & Exit
                                                 ESC: Exit

        Version 2.19.1268. Copyright (C) 2018 American Megatrends, Inc.
                                                                      AB
```

BIOS Setting	Description
Save Changes and Exit	Exits system setup after saving the changes.
Discard Changes and Exit	Exits system setup without saving any changes.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options.
Restore Defaults	Restores / Loads defaults values for all the setup options.
Save as User Defaults	Saves the changes done so far as user defaults.
Restore User Defaults	Restores the user defaults to all the setup options.
sSATA P2: Phison SSBP064GTMC0-	Choose to save the configuration or not.
Launch EFI Shell from Filesystem Device	Attempts to launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

Appendix

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

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

A. I/O Port Address Map

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

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000A20-0x00000A2F	Motherboard resources
0x00000070-0x00000071	System CMOS/real time clock
0x000003F8-0x000003FF	Communications Port (COM1)
0x000003F8-0x000003FF	PCI Express Root Complex
0x000002F8-0x000002FF	Communications Port (COM2)
0x000002F8-0x000002FF	PCI Express Root Complex
0x00000020-0x00000021	Programmable interrupt controller
0x000000A0-0x000000A1	Programmable interrupt controller
0x0000C000-0x0000C01F	Ethernet Controller
0x0000C000-0x0000C01F	PCI Express Root Port
0x00000000-0x000002E7	PCI Express Root Complex
0x00000000-0x000002E7	Direct memory access controller
0x00000300-0x000003AF	PCI Express Root Complex
0x000002E8-0x000002EF	PCI Express Root Complex
0x000003E8-0x000003EF	PCI Express Root Complex
0x00000400-0x00000CF7	PCI Express Root Complex
0x00000400-0x00000CF7	PCI Express Root Complex
0x000003B0-0x000003DF	PCI Express Root Complex
0x000003B0-0x000003DF	PCI Express to PCI/PCI-X Bridge
0x000003B0-0x000003DF	Microsoft Basic Display Adapter
0x000003B0-0x000003DF	PCI Express Root Port
0x0000B000-0x0000BFFF	PCI Express to PCI/PCI-X Bridge
0x0000B000-0x0000BFFF	Microsoft Basic Display Adapter
0x0000B000-0x0000BFFF	PCI Express Root Port
0x000003C0-0x000003DF	PCI Express to PCI/PCI-X Bridge

Address	Device Description
0x000003C0-0x000003DF	Microsoft Basic Display Adapter
0x000003C0-0x000003DF	PCI Express Root Port
0x00000CA2-0x00000CA2	Microsoft Generic IPMI Compliant Device
0x00000CA3-0x00000CA3	Microsoft Generic IPMI Compliant Device
0x00000040-0x00000043	System timer
0x00000010-0x0000001F	Motherboard resources
0x00000022-0x0000003F	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000065-0x00000065	Motherboard resources
0x00000067-0x0000006F	Motherboard resources
0x00000072-0x0000007F	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000084-0x00000086	Motherboard resources
0x00000088-0x00000088	Motherboard resources
0x0000008C-0x0000008E	Motherboard resources
0x00000090-0x0000009F	Motherboard resources
0x000000A2-0x000000BF	Motherboard resources
0x000000B1-0x000000B1	Motherboard resources
0x000000E0-0x000000EF	Motherboard resources
0x000004D0-0x000004D1	Motherboard resources
0x0000040B-0x0000040B	Motherboard resources
0x000004D6-0x000004D6	Motherboard resources
0x00000C00-0x00000C01	Motherboard resources
0x00000C14-0x00000C14	Motherboard resources
0x00000C50-0x00000C51	Motherboard resources
0x00000C52-0x00000C52	Motherboard resources
0x00000C6C-0x00000C6C	Motherboard resources
0x00000C6F-0x00000C6F	Motherboard resources
0x00000CD0-0x00000CD1	Motherboard resources
0x00000CD2-0x00000CD3	Motherboard resources
0x00000CD4-0x00000CD5	Motherboard resources
0x00000CD6-0x00000CD7	Motherboard resources

Address	Device Description
0x00000CD8-0x00000CDF	Motherboard resources
0x00000800-0x0000089F	Motherboard resources
0x00000B00-0x00000B0F	Motherboard resources
0x00000B20-0x00000B3F	Motherboard resources
0x00000900-0x0000090F	Motherboard resources
0x00000910-0x0000091F	Motherboard resources
0x0000FE00-0x0000FEFE	Motherboard resources
0x00000061-0x00000061	System speaker
0x00000081-0x00000083	Direct memory access controller
0x00000087-0x00000087	Direct memory access controller
0x00000089-0x0000008B	Direct memory access controller
0x0000008F-0x0000008F	Direct memory access controller
0x000000C0-0x000000DF	Direct memory access controller

B. Interrupt Request Lines (IRQ)

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

Level	Function
IRQ 4294967286	Standard SATA AHCI Controller
IRQ 7	AMD GPIO Controller
IRQ 4294967291	PCI Express Root Port
IRQ 4294967292	PCI Express Root Port
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 11	Ethernet Controller
IRQ 54 ~ IRQ 204	Microsoft ACPI-Compliant System
IRQ 256 ~ IRQ 511	Microsoft ACPI-Compliant System
IRQ 0	System timer
IRQ 4294967294	PCI Express Root Port
IRQ 4294967293	PCI Express Root Port
IRQ 4294967290	PCI Express Root Port
IRQ 4294967289	PCI Express Root Port
IRQ 4294967288	PCI Express Root Port
IRQ 4294967287	PCI Express Root Port
IRQ 5	PCI Encryption/Decryption Controller
IRQ 4294967285	AMD PSP 3.0 Device
IRQ 4294967284	AMD PSP 3.0 Device
IRQ 43	High Definition Audio Controller
IRQ 4294967283	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967282	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967281	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967280	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967279	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967278	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967277	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967276	AMD USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)

C. Watchdog Timer Configuration

The Watchdog Timer (WDT) is used to generate a variety of output signals after a user programmable count. The WDT is suitable for the use in the prevention of system lock-up, such as when software becomes trapped in a deadlock. Under these sorts of circumstances, the timer will count to zero and the selected outputs will be driven.

Under normal circumstance, you will need to restart the WDT at regular intervals before the timer counts to zero.

1. Sample Code: The file NCT5523D.H

```
//---------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A
PARTICULAR
// PURPOSE.
//
//---------------------------------------------------------------------------
#ifndef __NCT5523D_H
#define __NCT5523D_H                    1
//---------------------------------------------------------------------------
#define     NCT5523D_INDEX_PORT         (NCT5523D_BASE)
#define     NCT5523D_DATA_PORT          (NCT5523D_BASE+1)
//---------------------------------------------------------------------------
#define     NCT5523D_REG_LD             0x07
//---------------------------------------------------------------------------
#define NCT5523D_UNLOCK                 0x87
#define     NCT5523D_LOCK               0xAA
//---------------------------------------------------------------------------
unsigned int Init_NCT5523D(void);
void Set_NCT5523D_LD( unsigned char);
void Set_NCT5523D_Reg( unsigned char, unsigned char);
unsigned char Get_NCT5523D_Reg( unsigned char);
//---------------------------------------------------------------------------
#endif      //__NCT5523D_H
```

2. Sample Code: The file MAIN.CPP

```
//---------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A
PARTICULAR
// PURPOSE.
//
//---------------------------------------------------------------------------
#include <dos.h>
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include "NCT5523D.H"
//---------------------------------------------------------------------------
int main (void);

void WDTInitial(void);
void WDTEnable(unsigned char);
void WDTDisable(void);

//---------------------------------------------------------------------------
int main (void)
{
        char SIO;

        SIO = Init_NCT5523D();
        if (SIO == 0)
        {
                printf("Can not detect Nuvoton NCT5523D, program abort.\n");
                return(1);
        }

        WDTInitial();

        WDTEnable(10);

        WDTDisable();

        return 0;
}
//---------------------------------------------------------------------------
void WDTInitial(void)
{
        unsigned char bBuf;
        Set_NCT5523D_LD(0x08);                          //switch to logic device 8
        bBuf = Get_NCT5523D_Reg(0x30);
        bBuf &= (~0x01);
        Set_NCT5523D_Reg(0x30, bBuf);                   //Enable WDTO
}
//---------------------------------------------------------------------------
```

```
void WDTEnable(unsigned char NewInterval)
{
        unsigned char bBuf;

        Set_NCT5523D_LD(0x08);                          //switch to logic device 8
        Set_NCT5523D_Reg(0x30, 0x01);                   //enable timer

        bBuf = Get_NCT5523D_Reg(0xF0);
        bBuf &= (~0x08);
        Set_NCT5523D_Reg(0xF0, bBuf);                   //count mode is second

        Set_NCT5523D_Reg(0xF1, NewInterval);        //set timer
}
//---------------------------------------------------------------------------
void WDTDisable(void)
{
        Set_NCT5523D_LD(0x08);                          //switch to logic device 8
        Set_NCT5523D_Reg(0xF1, 0x00);                   //clear watchdog timer
        Set_NCT5523D_Reg(0x30, 0x00);                   //watchdog disabled
}
//---------------------------------------------------------------------------
```

3. Sample Code: The file NCT5523D.CPP

```
//---------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR
// PURPOSE.
//
//---------------------------------------------------------------------------
#include "NCT5523D.H"
#include <dos.h>
//---------------------------------------------------------------------------
unsigned int NCT5523D_BASE;
void Unlock_NCT5523D (void);
void Lock_NCT5523D (void);
//---------------------------------------------------------------------------
unsigned int Init_NCT5523D(void)
{
        unsigned int result;
        unsigned char ucDid;

        NCT5523D_BASE = 0x4E;
        result = NCT5523D_BASE;

        ucDid = Get_NCT5523D_Reg(0x20);
        if (ucDid == 0xC4)                              //NCT5523D??
        {       goto Init_Finish; }

        NCT5523D_BASE = 0x2E;
        result = NCT5523D_BASE;

        ucDid = Get_NCT5523D_Reg(0x20);
        if (ucDid == 0xC4)                              //NCT5523D??
        {       goto Init_Finish; }

        NCT5523D_BASE = 0x00;
        result = NCT5523D_BASE;

Init_Finish:
        return (result);
}
//---------------------------------------------------------------------------
void Unlock_NCT5523D (void)
{
        outportb(NCT5523D_INDEX_PORT, NCT5523D_UNLOCK);
        outportb(NCT5523D_INDEX_PORT, NCT5523D_UNLOCK);
}
//---------------------------------------------------------------------------
```

```
void Lock_NCT5523D (void)
{
        outportb(NCT5523D_INDEX_PORT, NCT5523D_LOCK);
}
//---------------------------------------------------------------------------
void Set_NCT5523D_LD( unsigned char LD)
{
        Unlock_NCT5523D();
        outportb(NCT5523D_INDEX_PORT, NCT5523D_REG_LD);
        outportb(NCT5523D_DATA_PORT, LD);
        Lock_NCT5523D();
}
//---------------------------------------------------------------------------
void Set_NCT5523D_Reg( unsigned char REG, unsigned char DATA)
{
        Unlock_NCT5523D();
        outportb(NCT5523D_INDEX_PORT, REG);
        outportb(NCT5523D_DATA_PORT, DATA);
        Lock_NCT5523D();
}
//---------------------------------------------------------------------------
unsigned char Get_NCT5523D_Reg(unsigned char REG)
{
        unsigned char Result;
        Unlock_NCT5523D();
        outportb(NCT5523D_INDEX_PORT, REG);
        Result = inportb(NCT5523D_DATA_PORT);
        Lock_NCT5523D();
        return Result;
}
//-----------------------------------------------------------------------
```