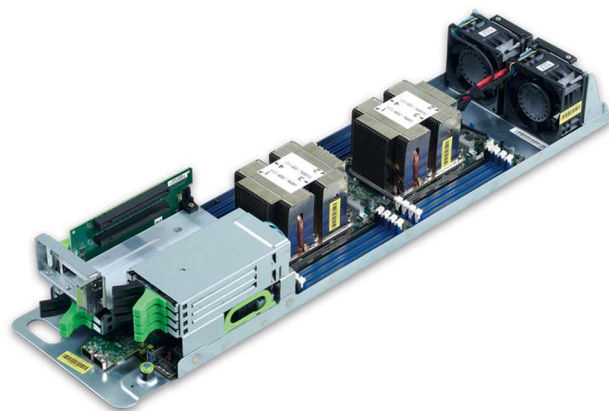


TS2280-E7278P

OCP Computing Sled

User's Manual

Version: 1.1



PREFACE

Copyright

This publication, including all photographs, illustrations, and software, is protected under international copyright laws, with all rights reserved.

Neither this manual, nor any material contained herein, may be reproduced without written consent of manufacturer.

Copyright 2018 MiTAC Computing Technology Corporation. All rights reserved.

Disclaimer

Information contained in this document is furnished by MiTAC Computing Technology Corporation and has been reviewed for accuracy and reliability prior to printing. MiTAC assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of MiTAC products including liability or warranties relating to fitness for a particular purpose or merchantability. MiTAC retains the right to make changes to produce descriptions and/or specifications at any time, without notice. In no event will MiTAC be held liable for any direct or indirect, incidental or consequential damage, loss of use, loss of data or other malady resulting from errors or inaccuracies of information contained in this document.

Trademark Recognition

All registered and unregistered trademarks and company names contained in this manual are property of their respective owners including, but not limited to the following.

Intel® is a trademark of Intel® Corporation.

AMI®, AMIBIOS® and combinations thereof are trademarks of AMI Technologies.

Microsoft®, Windows® are trademarks of Microsoft Corporation.

IBM®, PC®, AT® and PS/2® are trademarks of IBM Corporation.

Winbond® is a trademark of Winbond Electronics Corporation.

About this Manual

This manual is intended for experienced users and integrators with hardware knowledge of personal computers.

It is aimed to provide you with instructions on installing your TS2280-E7278P.

How this guide is organized

This guide contains the following parts:

Chapter 1: Overview

This chapter provides an introduction to the MiTAC OCP TS2280-E7278P server, gives an overview of the product from different angles, describes the installation of components in Sled.

Chapter 2: Setting Up

This chapter introduces how the server is assembled and how users can plugin/remove accessories to the MainBoard.

Chapter 3: Motherboard Information

This chapter includes the detailed information of Main Board including Block Diagram and description of the connectors on the Main Board.

Chapter 4: BIOS Setup

This chapter tells how to change system settings through the BIOS setup menu. Detailed descriptions of the BIOS parameters are also provided.

Chapter 5: BMC

This chapter introduces the basic BMC features and provides a list of sensors that BMC monitored to have better service for the customers.

Chapter 6: Firmware upgrade process

Chapter 7: Trouble Shooting

This is a chapter for reference once you experience errors during operation. Ex: The error-log format and parsing.

Safety and Compliance Information

Before installing and using TS2280-E7278P, take note of the following precautions:

Read all instructions carefully

- Do not place the unit on an unstable surface, cart, or stand.
- Only use the power source indicated on the marking label. If you are not sure, contact the power company.
- The unit uses a three-wire ground cable, which is equipped with a third pin to ground the unit and prevent electric shock. Do not defeat the purpose of this pin. If your outlet does not support this kind of plug, contact your electrician to replace your obsolete outlet.
- Do not place anything on the power cord. Place the power cord where it will not be in the way of foot traffic.
- Follow all warnings and cautions in this manual and on the unit case.
- Do not push objects in the ventilation slots as they may touch high voltage components and result in shock and damage to the components.
- When replacing parts, ensure that you use parts specified by the manufacturer.
- When service or repairs have been done, perform routine safety checks to verify that the system is operating correctly.
- Avoid using the system near water, in direct sunlight, or near a heating device.
- Cover the unit when not in use.

Safety Information

Retain and follow all product safety and operating instructions provided with your equipment. In the event of a conflict between the instructions in this guide and the instructions in equipment documentation, follow the guidelines in the equipment documentation.

Observe all warnings in the operating instructions. To reduce the risk of bodily injury, electric shock, fire and damage to the equipment, observe all precautions included in this guide.

Machine Room Environment

This device is for use only in a machine room or IT room.

Make sure that the area in which you install the system is properly ventilated and climate-controlled.

Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the electrical rating label of the equipment.

Do not install the system in or near a plenum, air duct, radiator, or heat register.

Never use the product in a wet location.

Equipment Chassis

Do not block or cover the openings to the system.

Never push objects of any kind through openings in the equipment. Dangerous voltages might be present.

Conductive foreign objects can produce a short circuit and cause fire, electric shock, or damage to your equipment.

Lift equipment using both hands and with your knees bent.

Revision History

Date	Revision	Explanation of Changes
2018/05/10	0.1	Initial Release
2018/06/27	1.0	Formal Release
2018/12/12	1.1	Update speciation and SKU name

Table of Contents

1.	OVERVIEW	7
1.1	Features	8
1.2	Server Introduction	9
1.3	Sever exploded view	10
2.	SETTING UP	11
2.1	Before you Begin	11
2.1.1	Work Area.....	11
2.1.2	Tools.....	11
2.1.3	Precaution	12
2.2	System SKUs	13
2.2.1	Standard	13
2.2.2	Advanced.....	14
2.2.3	Ultra	14
2.3	Installing Motherboard Components	15
2.3.1	Removing the Chassis Cover	15
2.3.2	Installing the CPU and Heatsink.....	15
2.3.2.1	Install the CPU.....	15
2.3.2.2	Install the heatsink.....	17
2.3.3	Installing the Memory	19
2.3.4	Installing Hard drive (6SSD configuration for example)	20
2.3.5	Release the Hard Drive	21
2.3.6	Install M.2 device.....	21
2.3.7	Install the Add-on cards.....	21
3.	MAINBOARD INFORMATION	26
3.1	Board Introduction	26
3.2	Board I/O	27
3.3	LED Indicators	28
3.4	Block Diagram	29
4.	BIOS/UEFI	30
4.1	BIOS Setup Utility.....	31
4.2	Main Screen	35

4.3	Advanced Screen	37
4.3.1	Intel(R) Virtual RAID on CPU	39
4.3.2	All CPU Information	40
4.3.3	Intel(R) I210 Gigabit Network Connection	41
4.3.3.1	NIC Configuration	42
4.3.4	Driver Health.....	43
4.3.5	Trust Computing	44
4.3.6	ACPI Settings	45
4.3.7	Serial Port Console Redirection	46
4.3.7.1	Console Redirection Settings	48
4.3.7.2	Legacy Console Redirection Settings.....	51
4.3.7.3	Console Redirection Settings (Serial Port for Out-of-Band Management/Windows Emergency Management Services).....	52
4.3.8	SIO Configuration	54
4.3.8.1	[*Active*] Serial Port X.....	55
4.3.9	PCI Subsystem Settings.....	57
4.3.10	Network Stack Configuration	58
4.3.11	CSM Configuration	59
4.3.12	NVME Configuration.....	61
4.3.13	USB Configuration.....	62
4.4	Platform Configuration.....	65
4.4.1	PCH Configuration.....	66
4.4.1.1	PCH Configuration.....	68
4.4.1.2	PCI Express Configuration	70
4.4.1.3	PCH SATA Configuration	79
4.4.1.4	PCH sSATA Configuration	92
4.4.1.5	USB Configuration	98
4.4.1.6	Security Configuration	100
4.4.1.7	Azalia Configuration	101
4.4.1.8	Platform Thermal Configuration.....	102
4.4.1.9	TraceHub Configuration	103
4.4.1.10	PCH DFX Configuration.....	104
4.4.1.11	PCH DWR Configuration	114
4.4.2	Miscellaneous Configuration	116

4.4.2.1	Debug Configuration.....	120
4.4.3	Server ME Configuration	121
4.4.4	Server ME Debug Configuration.....	123
4.4.4.1	Server ME General Configuration	124
4.4.4.2	NM Configuration.....	128
4.4.5	Runtime Error Logging	130
4.4.5.1	eMCA Settings.....	133
4.4.5.2	Whea Settings	135
4.4.5.3	Error Injection Settings	136
4.4.5.4	UPI Error Enabling.....	138
4.4.5.5	Memory Error Enabling.....	139
4.4.5.6	IIO Error Enabling.....	141
4.4.5.7	PCIe Error Enabling.....	145
4.4.6	Reserve Memory	147
4.4.7	Non-Silicon Specific Items.....	148
4.5	Socket Configuration	149
4.5.1	Processor Configuration	150
4.5.1.1	Serial Per-Socket Configuration	157
4.5.2	Common RefCode Configuration	160
4.5.3	UPI Configuration	162
4.5.3.1	UPI General Configuration	163
4.5.3.2	UPI Per Socket Configuration.....	168
4.5.3.3	UPI Dfx Configuration.....	188
4.5.4	Memory Configuration	190
4.5.4.1	Memory Topology.....	199
4.5.4.2	Page Policy.....	201
4.5.4.3	Memory Training.....	202
4.5.4.4	Memory Timings Override	204
4.5.4.5	Memory Map.....	205
4.5.4.6	Memory RAS Configuration.....	207
4.5.4.7	NGN Configuration	209
4.5.4.8	NGNVM DIMM Secure Erase Unit	211
4.5.4.9	Memory Dfx Configuration.....	212
4.5.4.10	BSSA Configuration Menu	214

4.5.4.11	Common RefCode Configuration.....	215
4.5.5	IIO Configuration	217
4.5.5.1	Socket0 Configuration	222
4.5.5.2	IOAT Configuration.....	261
4.5.5.3	IIO General Configuration.....	265
4.5.5.4	Intel® VT for Directed I/O (VT-d).....	266
4.5.5.5	Intel® VMD technology.....	268
4.5.5.6	Intel® AIC Retimer/AIC SSD Technology (non-VMD).....	273
4.5.5.7	IIO DFX Configuration	275
4.5.6	Advanced Power Management Configuration	298
4.5.6.1	CPU P State Control.....	300
4.5.6.2	Hardware PM State Control.....	303
4.5.6.3	Overclocking.....	305
4.5.6.4	CPU C State Control	307
4.5.6.5	Package C State Control	310
4.5.6.6	CPU Thermal Management.....	319
4.5.6.7	CPU - Advanced PM Tuning	322
4.5.6.8	Package Current Configuration	325
4.5.6.9	EPB Override Control	326
4.5.6.10	SOCKET RAPL Configuration	327
4.5.6.11	PMAX CONFIG Configuration	329
4.5.6.12	ACPI Sx State Control	330
4.5.6.13	Memory Power & Thermal Configuration.....	331
4.6	Server Management.....	336
4.6.1	System Event Log	339
4.6.2	BMC Self Test log.....	341
4.6.3	BMC network configuration	342
4.6.4	View System Event Log.....	347
4.6.5	BMC User Settings	348
4.6.5.1	Add User.....	349
4.6.5.2	Delete User.....	350
4.6.5.3	Change User Settings	351
4.7	Security.....	352
4.7.1	Secure Boot.....	354

4.7.1.1	Key Management	355
4.8	Boot Configuration.....	358
4.9	Save & Exit Screen.....	359
5.	BMC	363
5.1	BMC introduction	363
5.2	BMC connectivity.....	363
5.3	Local Serial Console and SOL	363
5.4	BMC sensor list	364
5.4.1	Sensors are listed in the table below.....	364
5.4.2	Threshold for Analog Sensors	369
5.4.3	Event-Only Sensors Table.....	372
5.5	Commands Support.....	379
5.5.1	IPMI commands support.....	379
5.5.1.1	IPMI Global Commands	379
5.5.1.2	BMC Watchdog Timer Commands.....	379
5.5.1.3	IPMI Messaging Support Commands.....	379
5.5.1.4	RMCP+ Support and Payload Commands	380
5.5.1.5	Chassis Device Commands	381
5.5.1.6	Event Commands	381
5.5.1.7	PEF and Alerting Commands	381
5.5.1.8	Sensor Device Commands	381
5.5.1.9	FRU Inventory Area Info.....	382
5.5.1.10	SDR Repository Device Commands.....	382
5.5.1.11	SEL Device Commands.....	382
5.5.1.12	IPMI LAN Commands	383
5.5.1.13	SOL Commands	383
5.5.2	OEM commands support.....	384
5.5.2.1	OEM Commands Synopsis	384
5.5.2.2	Auto BIOS Recovering Command Set	386
5.5.2.3	BIOS Boot Option Command Set	390
5.5.2.4	Other OEM Command Set	391
5.6	Event Logging and Alerting	397
5.7	Chassis Control	397
5.7.1	Power Button Logging	397

5.8	LAN Configuration	398
5.8.1	Get/Set LAN Configuration Parameters	398
5.8.1.1	DHCP	398
5.8.1.2	MAC Address Programming.....	399
5.9	Port 80 POST	400
5.10	LED controlled by BMC	401
5.10.1	BMC Heartbeat LED.....	401
5.10.2	UART Channel LED	401
5.10.3	Power and System Identification LED	401
6.	FIRMWARE UPDATE	402
6.1	BIOS Update	402
6.2	Firmware Update	402
6.2.1	BIOS update	402
6.2.2	BMC update.....	404
APPENDIX A		405

1. OVERVIEW

About the MiTAC TS2280-E7278P

Congratulations on your purchase of the MiTAC TS2280-E7278P OCP system, TS2280-E7278P is a highly optimized OCP system. It is based on Intel® Xeon® Scalable Processor Family 3 (Skylake-SP processor) product family CPU architecture. It supports up to 16 DIMMs.

TS2280-E7278P motherboard is designed to work with Open Rack V2 (Orv2) described in the following chapter.

1.1 Features

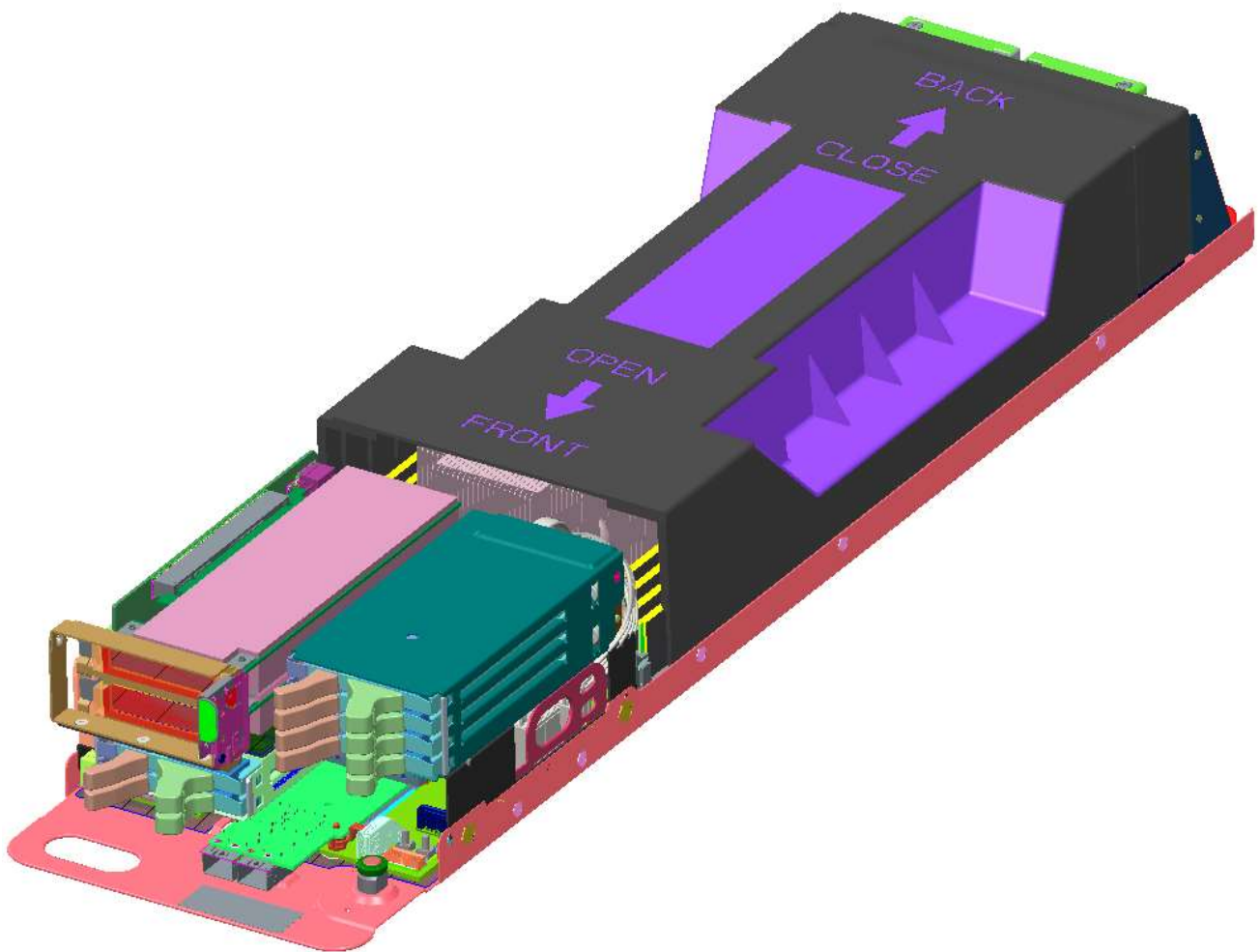
SKU List

SKU	PCI-E slot	HDD Bay
Standard-L	(2) FHHL PCIe x16	(1) 3.5" HDD
Standard-S	(2) FHHL PCIe x16	(1) 2.5" SSD
Advanced	(2) HHHL PCIe x16	(6) 2.5" SSD
Ultra	(1) FHHL PCIe x16	(4) U.2 + (1) 2.5" SSD

Specification

	Standard- L(S)	Advanced	Ultra
Processor	Intel Xeon Scalable Processor Family, Sky Lake/ Cascade lake		
Memory	Up to 512GB RDIMM ; 16 DIMM slots/ 6channels		
Storage and I/O			
Front I/O ports	(1) PW BTN/ (1) PW LED / (1) RST BTN /(1) HDD ACT LED / (1) Error LED (1) Type A USB 3.0/ (1) Type C USB 3.0		
Storage	3.5" or 2.5" SATA swappable bay	6 x 2.5" hot swappable SSD bay	4 x 2.5" hot swappable SATA/SAS/ U.2 bay + 7mm SSD option
On Board Storage	M.2 (SATA or PCI-E)		
PCIE Expansion Slots	2 x FHHL PCI-E x16 Slots	2 x HHHL PCI-E x16 Slots	1 x FHHL PCI-E x16 Slots
Mezzanine Slots	OCP V2.0 NIC mezz compatible		
Server Management	IPMI 2.0 compliant baseboard management controller (BMC) Web interface support Onboard Aspeed AST2500		
LAN	GbE BMC port w/ NCSI		
System Cooling	(2) 8cm fans		
Dimension /Weight	28.46" x 6.87" X 3.5"(723x 174.5x 89mm) / 6~ 8.5kg		
Power Supply	Externally through centralized 12V DC bus bar		

1.2 Server Introduction



Server isometric view

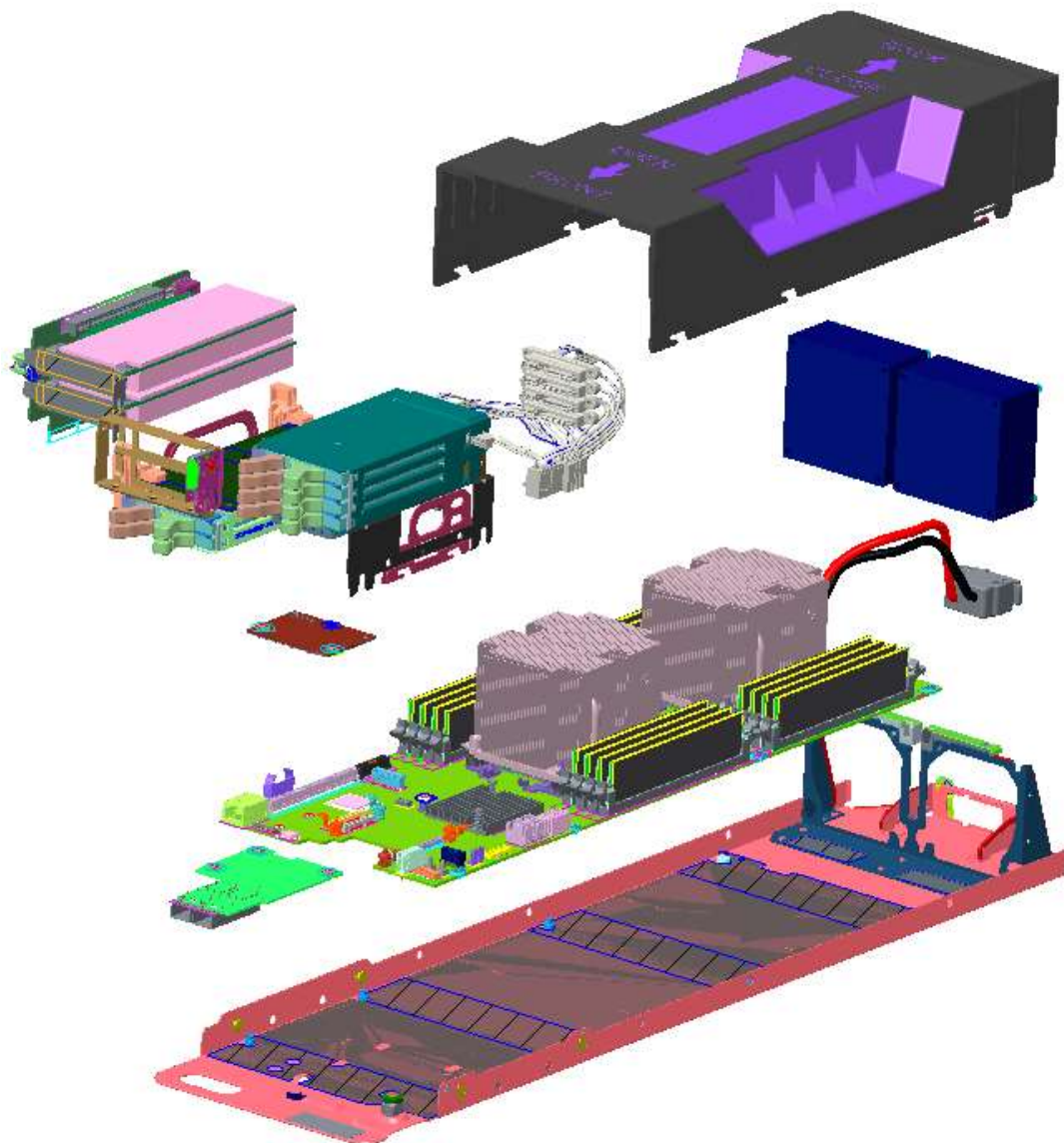
This is an isometric view of TS2280-E7278P server. There are two PCIe slots/Drive bays/IO connections in the front. On the rear end, there is a floating connector that fit into bus bar providing power to this sled.

Be sure to pull the lock button up and push the sled into rack shelf all the way down, then release the lock button.



There are sharp edges on the metal parts. This is generic to the low-cost OCP design. Be sure to wear gloves when you assemble/disassemble any mechanical components. For example, PCIe bracket, PCIe cards and installing cables...etc.

1.3 Server exploded view



This exploded view explains how the TS2280-E7278P sled is assembled. Refer to Chapter 2 for detailed installation guide.

2. Setting Up

2.1 Before you Begin

This chapter explains how to install the CPUs, CPU heatsinks, memory modules, and hard drives. Instructions on inserting add-on cards are also given.

2.1.1 Work Area

Make sure you have a stable, clean working environment. Dust and dirt can get into components and cause malfunctions. Use containers to keep small components separated. Putting all small components in separate containers prevents them from becoming lost. Adequate lighting and proper tools can prevent you from accidentally damaging the internal components.

2.1.2 Tools

The following procedures require only a few tools, including the following:

- A cross head (Phillips) screwdriver
- A grounding strap or an anti-static pad

Most of the electrical and mechanical connections can be disconnected with your hands. It is recommended that you do not use pliers to remove connectors as it may damage the soft metal or plastic parts of the connectors.



Caution!

1. To avoid damaging the motherboard and associated components, do not use torque force greater than 7kgf/cm (6.09 lb/in) on each mounting screw for motherboard installation.
2. Do not apply power to the board if it has been damaged.

2.1.3 Precaution

Components and electronic circuit boards can be damaged by discharges of static electricity. Working on a system that is connected to a power supply can be extremely dangerous. Follow the guidelines below to avoid damage to TA80-B7071 or injury to yourself.

Ground yourself properly before removing the top cover of the system. Unplug the power from the power supply and then touch a safely grounded object to release static charge (i.e. power supply case). If available, wear a grounded wrist strap. Alternatively, discharge any static electricity by touching the bare metal chassis of the unit case, or the bare metal body of any other grounded appliance.

- Avoid touching motherboard components, IC chips, connectors, memory modules, and leads.
- The motherboard is pre-installed in the system. When removing the motherboard, always place it on a grounded anti-static surface until you are ready to reinstall it.
- Hold electronic circuit boards by the edges only. Do not touch the components on the board unless it is necessary to do so. Do not flex or stress circuit boards.
- Leave all components inside the static-proof packaging that they ship with until they are ready for installation.
- After replacing optional devices, make sure all screws, springs, or other small parts are in place and are not left loose inside the case. Metallic parts or metal flakes can cause electrical shorts.



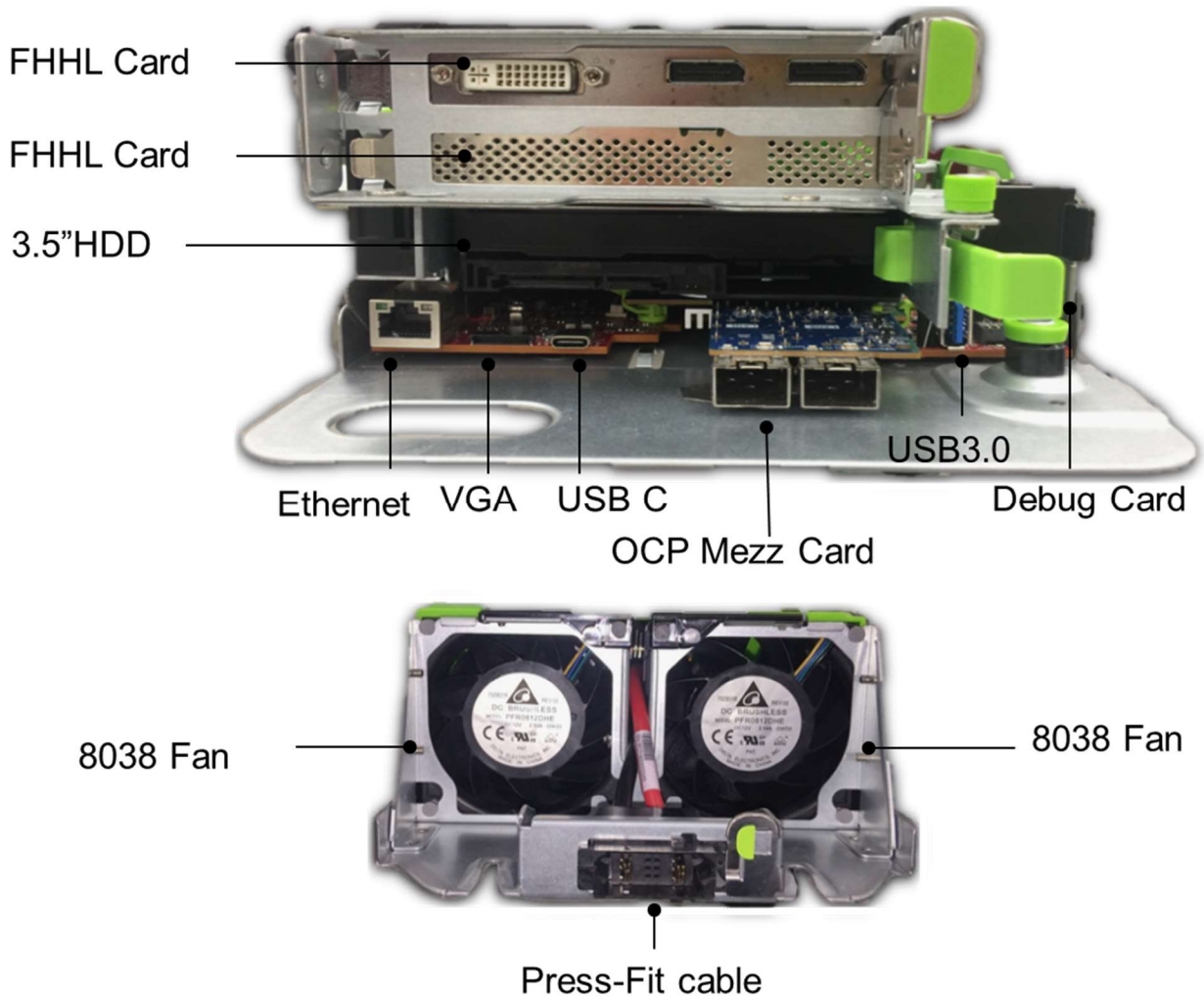
NOTE

All connectors are keyed to only attach one way.

2.2 System SKUs

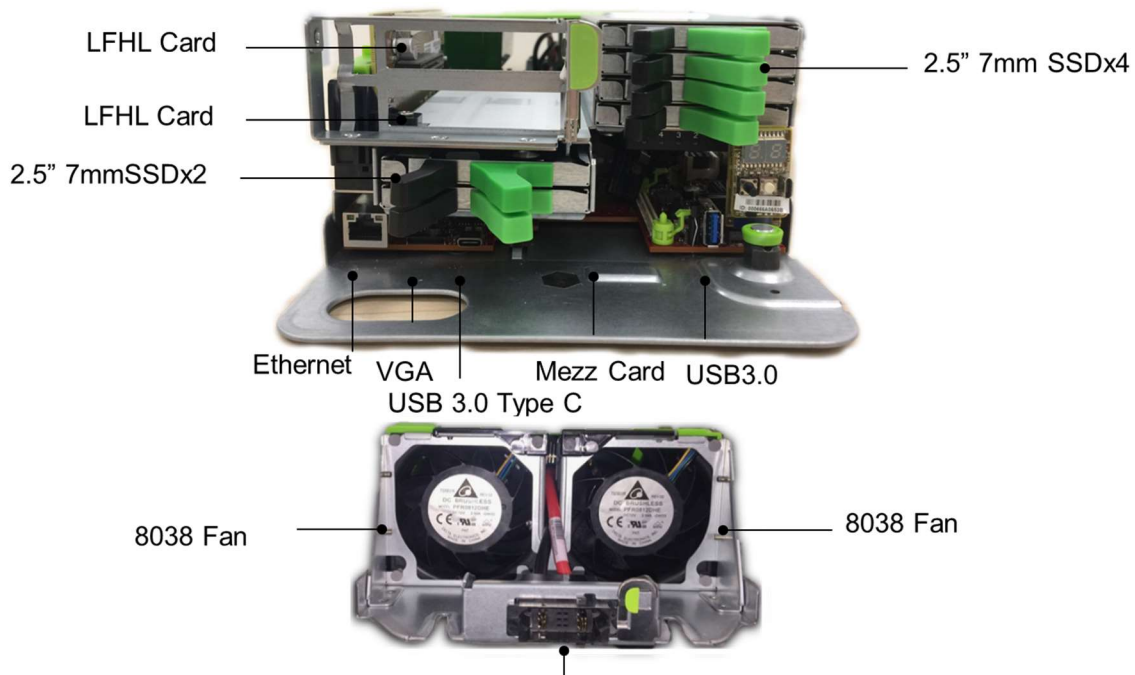
MiTAC TS2280-E7278P servers following 3 HW configurations

2.2.1 Standard



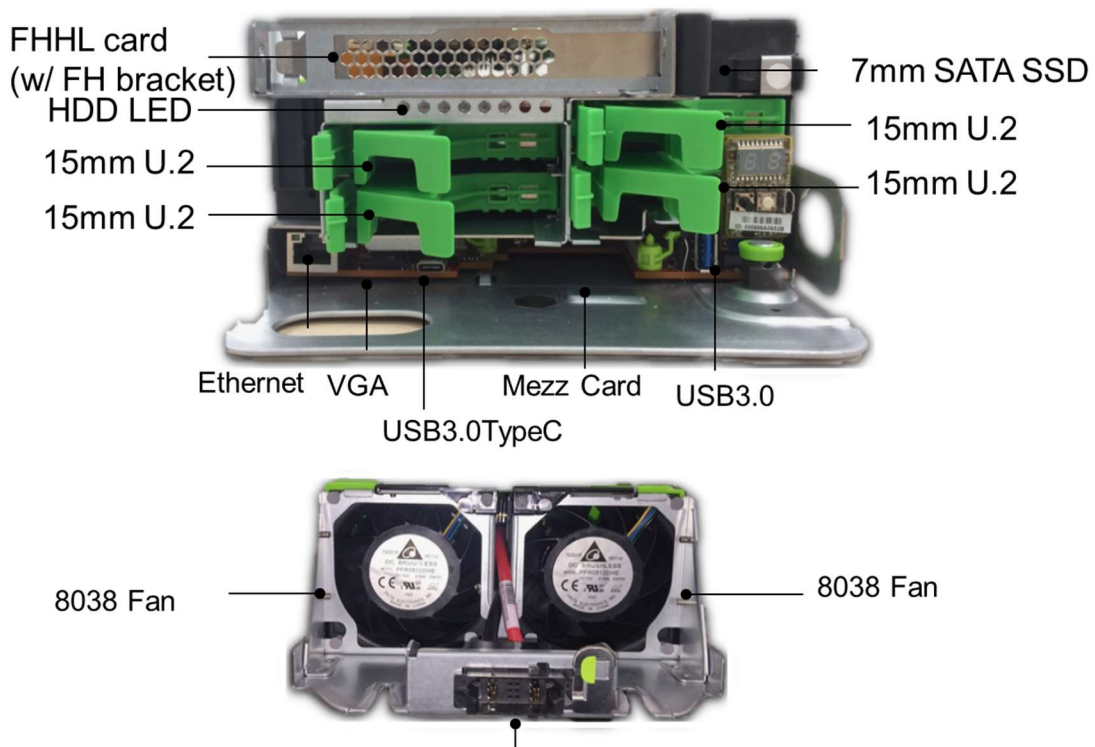
Note: Support 2x FHHL PCIe cards. One 3.5" SATA HDD.

2.2.2 Advanced



Note: Support 6x 7mm thickness SSD SATA drives using PCH SATA or a HBA card. 2x LFHL PCIe cards.

2.2.3 Ultra



Note: 4x U.2 drives. One FHHL PCIe card.

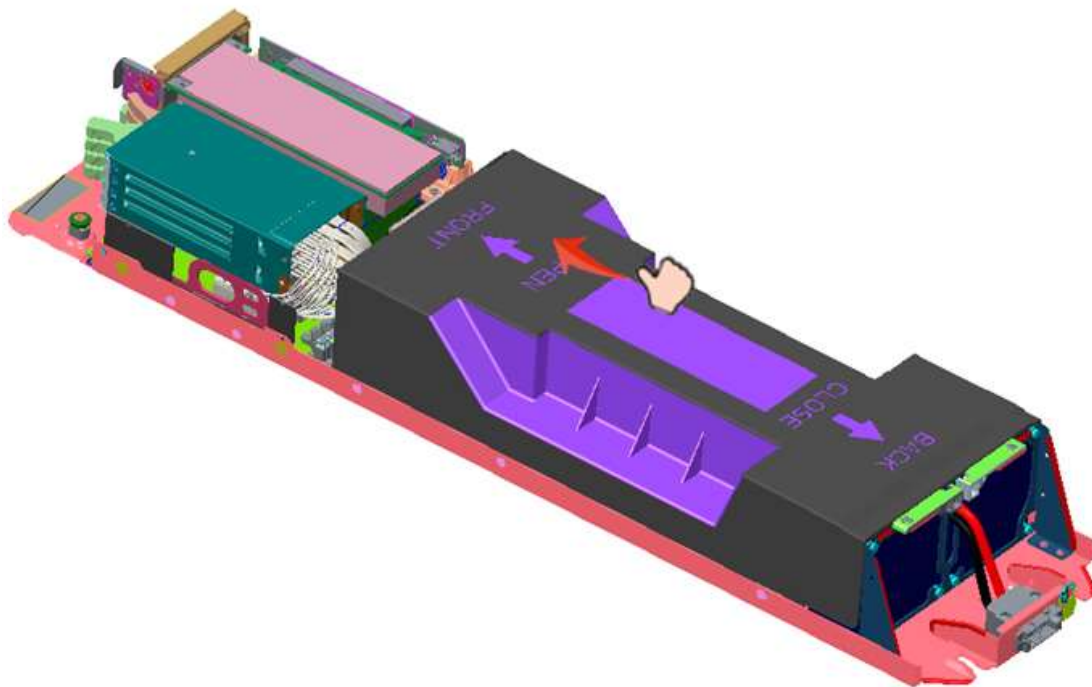
2.3 Installing Motherboard Components

This section describes how to install components on to the mainboard, including CPUs, memory modules, adapter Card, HDD and Add On cards.

2.3.1 Removing the Chassis Cover

Follow these instructions to remove chassis cover.

- Push the top cover in the arrow direction.

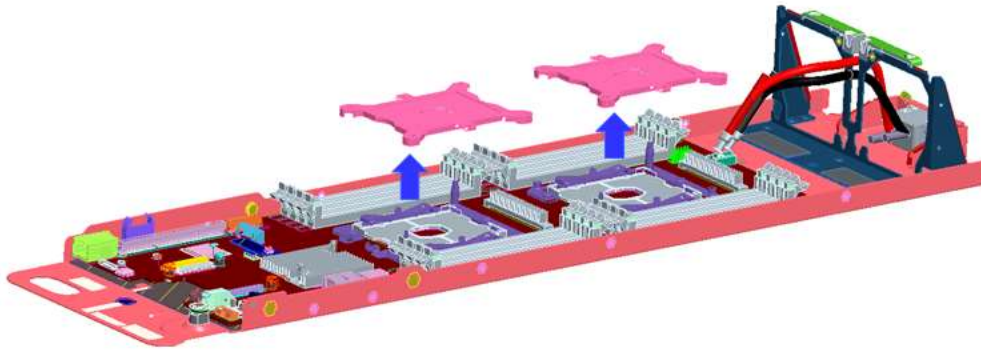


2.3.2 Installing the CPU and Heatsink

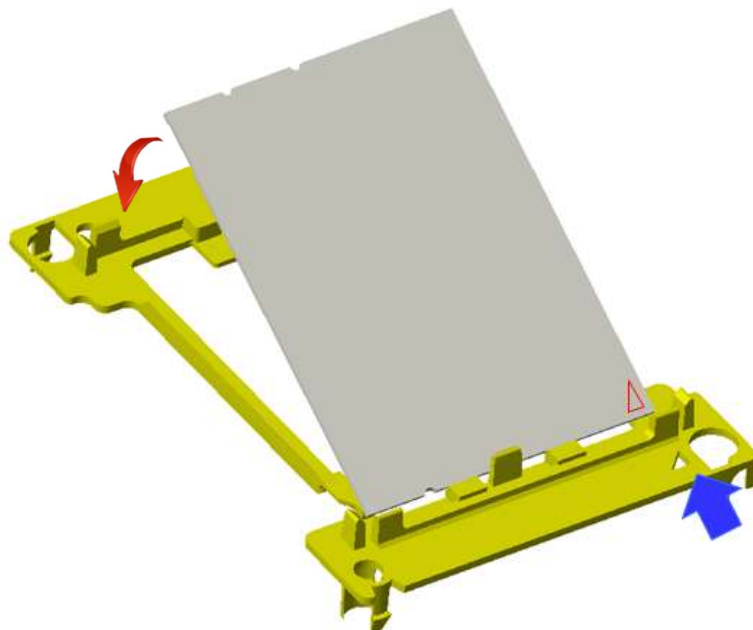
Follow the steps below to install the processor and heatsink.

2.3.2.1 Install the CPU

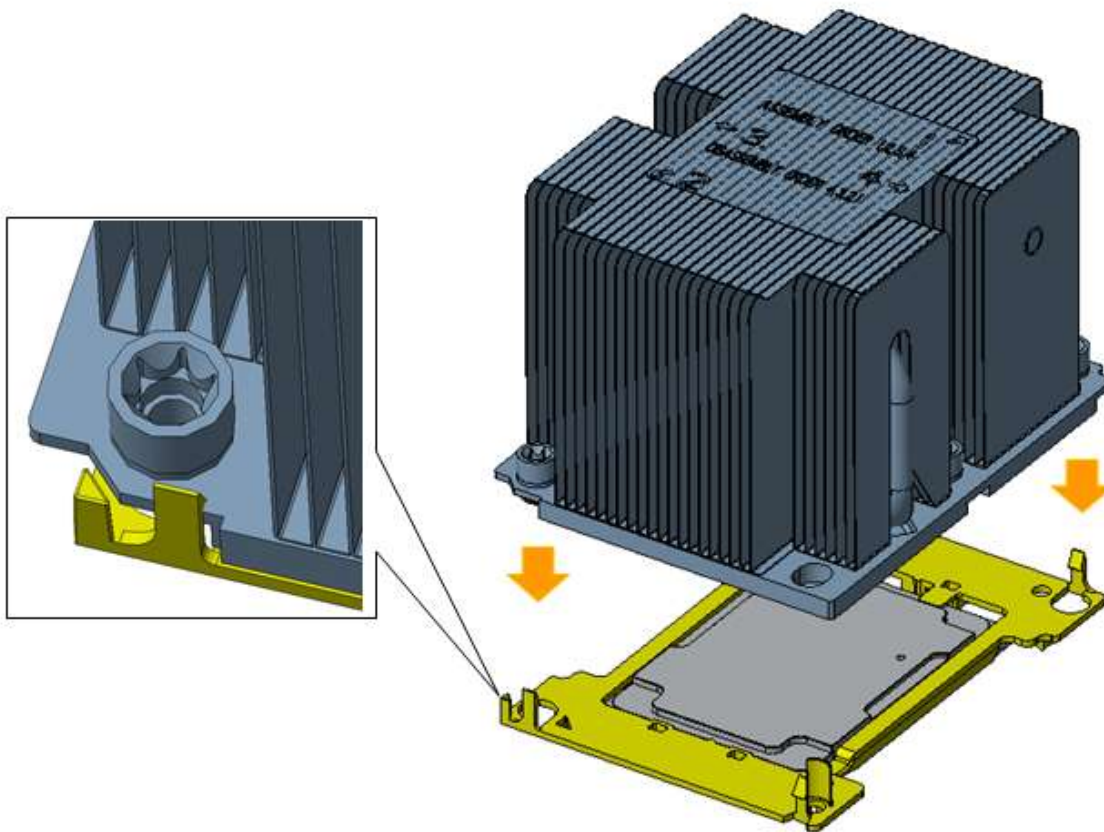
- A. Remove the dust cover.



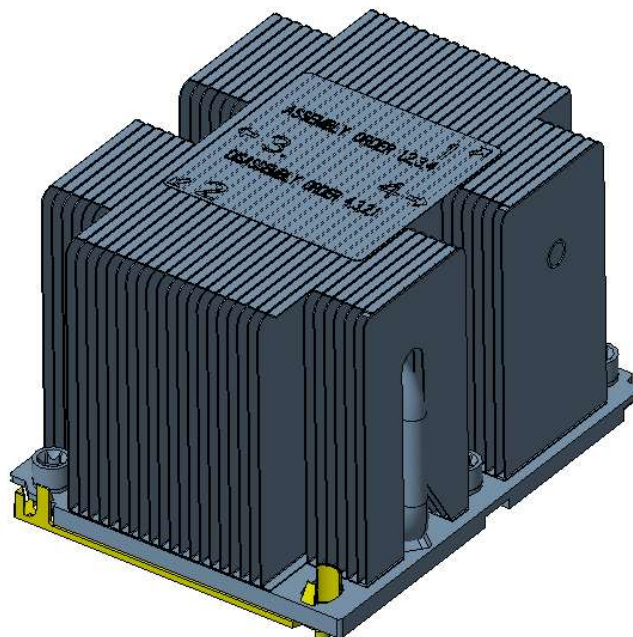
B. Put the processor in the CPU Carrier. and Pin1 need to be aligned with the triangle mark.



C. Install the CPU HS to the carrier, pay attention the foolproof feature
If wrongly installed, it will interfere with HS



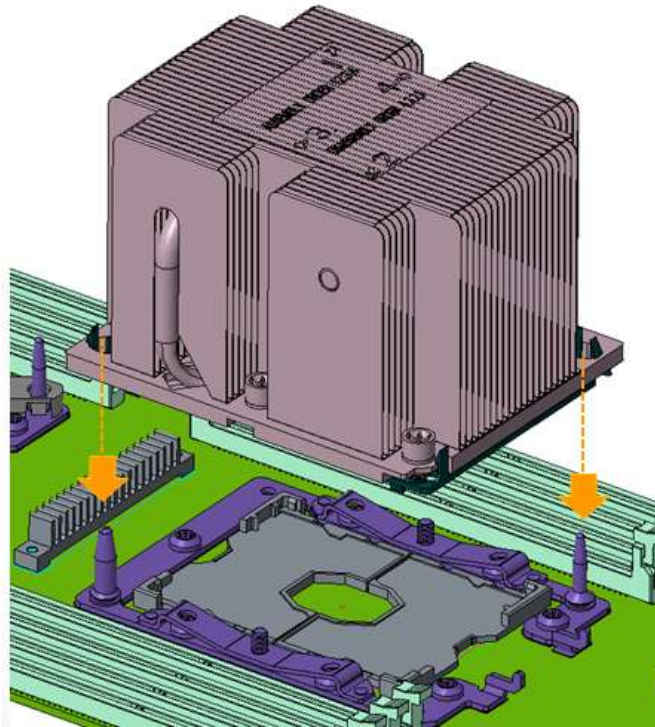
D. Place the CPU in the CPU socket. Make sure the arrow mark on CPU is located in the corresponding location of socket.



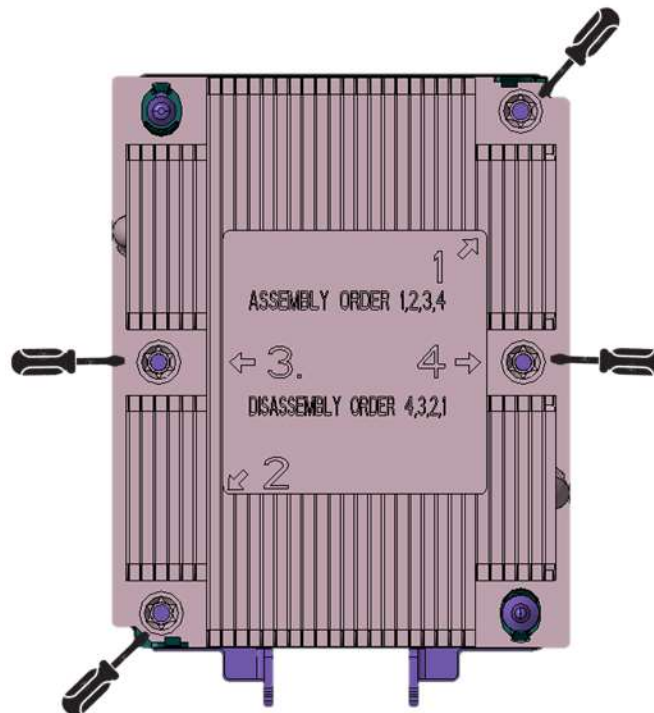
2.3.2.2 Install the

heatsink

A. Place the heatsink on top of the CPU and secure it with 4 screws



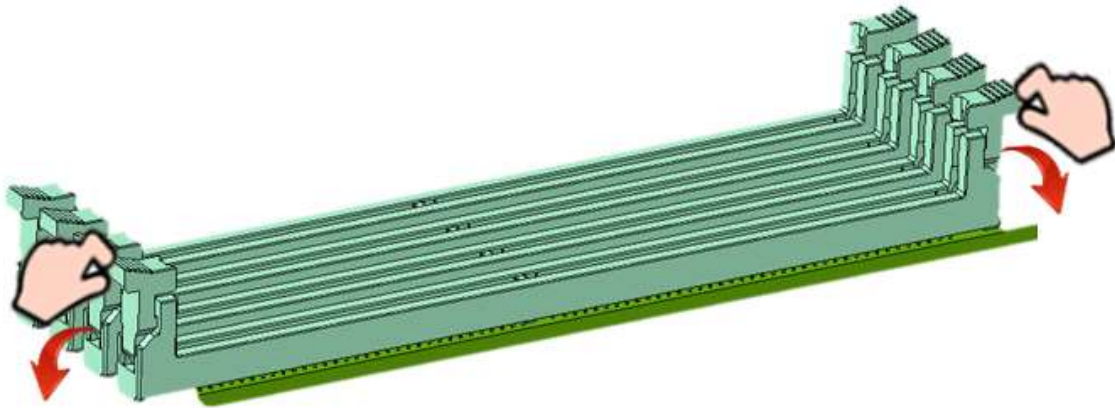
B. Secure the heatsink with 4 screws. To make the pressure even, please tighten these 4 screws in a diagonal way. Use a torque screw driver to make sure you apply a proper torque to the screws.



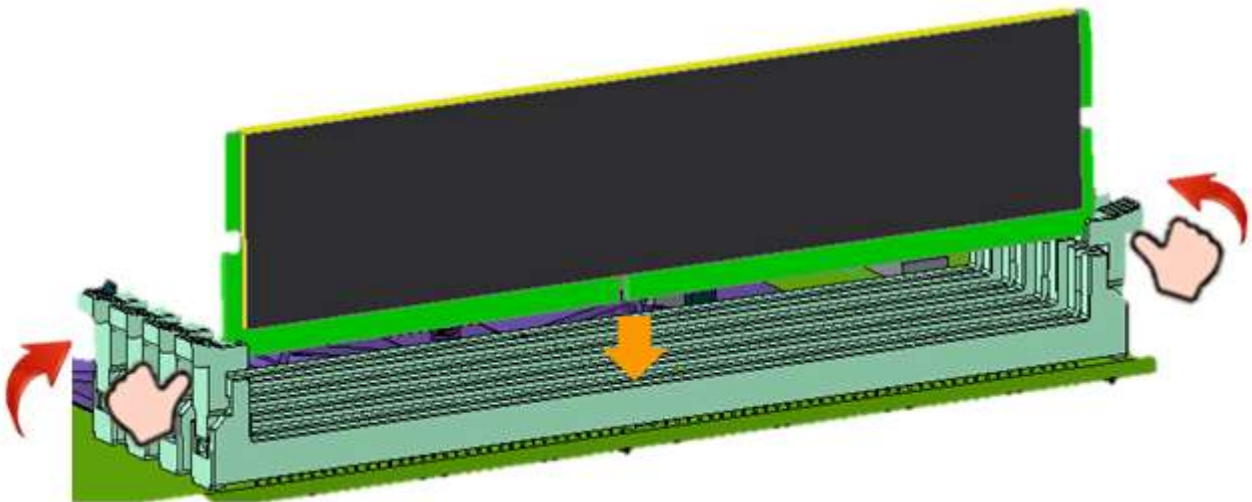
2.3.3 Installing the Memory

Follow these instructions to install the memory modules onto the motherboard.

A. Press the memory slot latch outward.



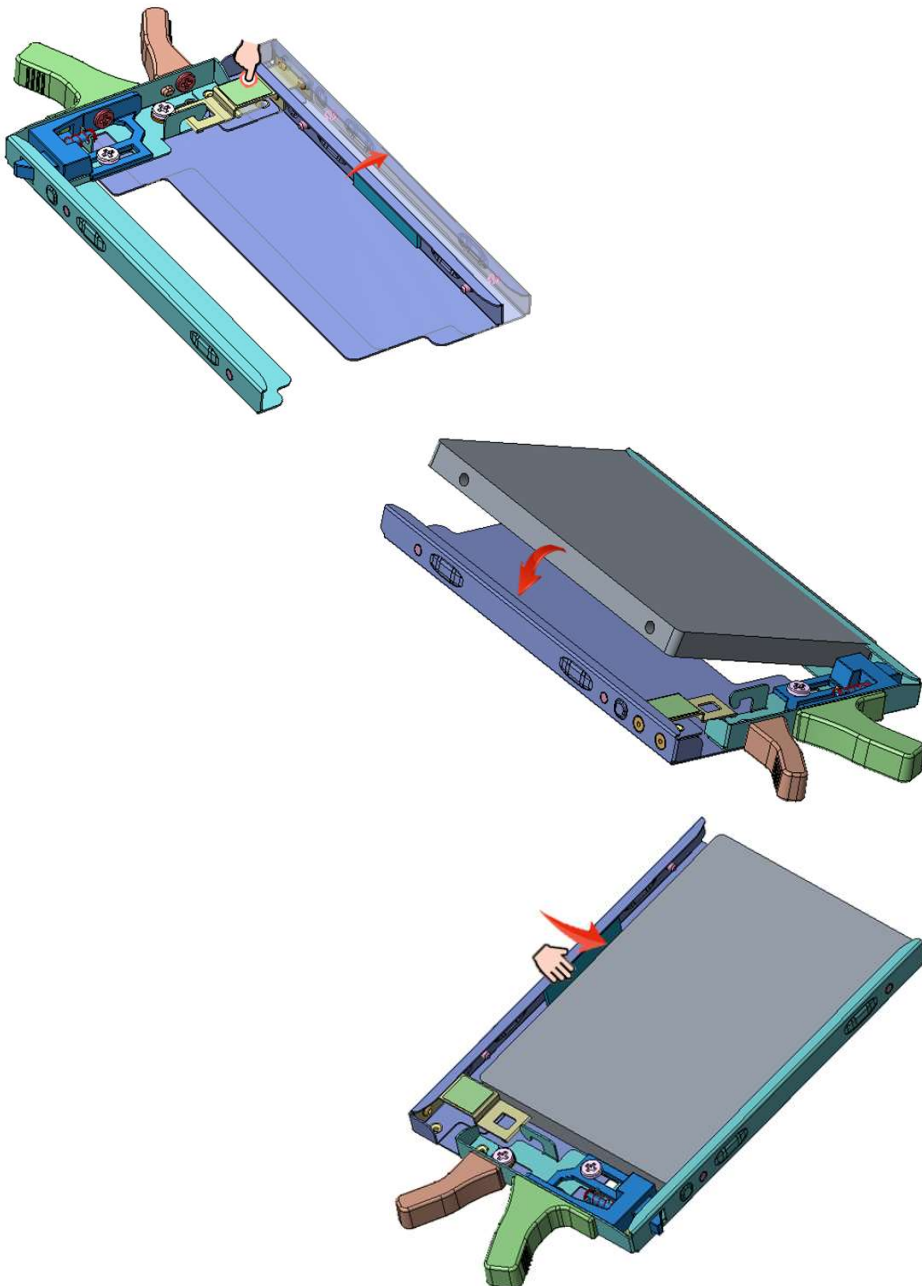
B. Align the memory module with the slot. When insert properly, the memory slot latches automatically onto the indentations at two ends of the module.



2.3.4 Installing Hard drive (6SSD configuration for example)

An OCP TS2280-E7278P supports SSD 2.5" hard drive. Follow these instructions to install a hard drive.

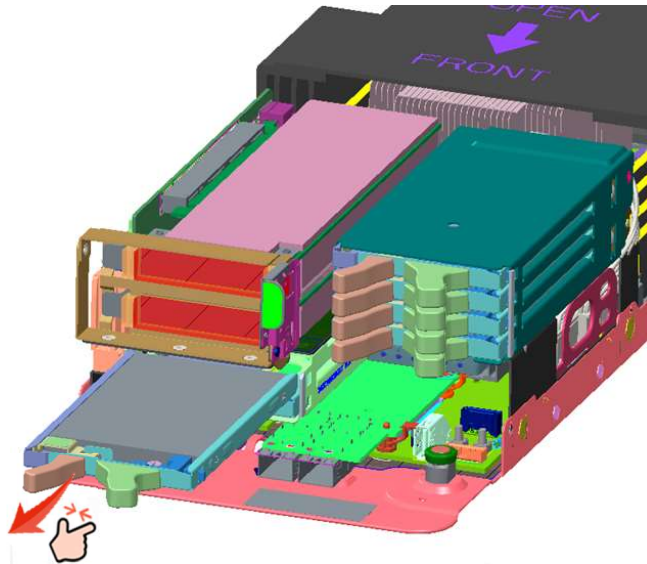
- A. Insert the HDD into the HDD bracket in the direction of arrow until you hear a click.



2.3.5 Release the Hard Drive

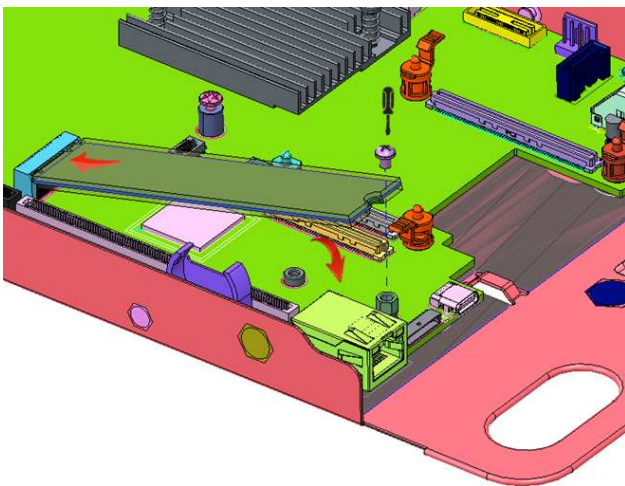
A. Pull the locking HDD lever open in the direction of arrow

B. Take out HDD



2.3.6 Install M.2 device

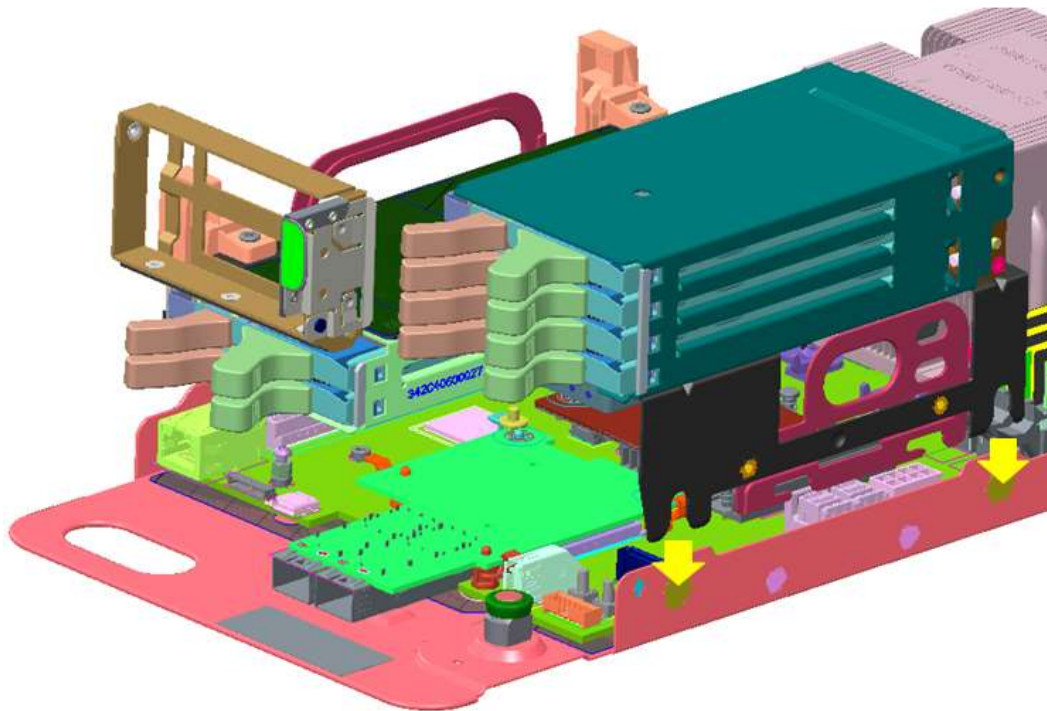
Insert the M.2 device into the connector and push down.



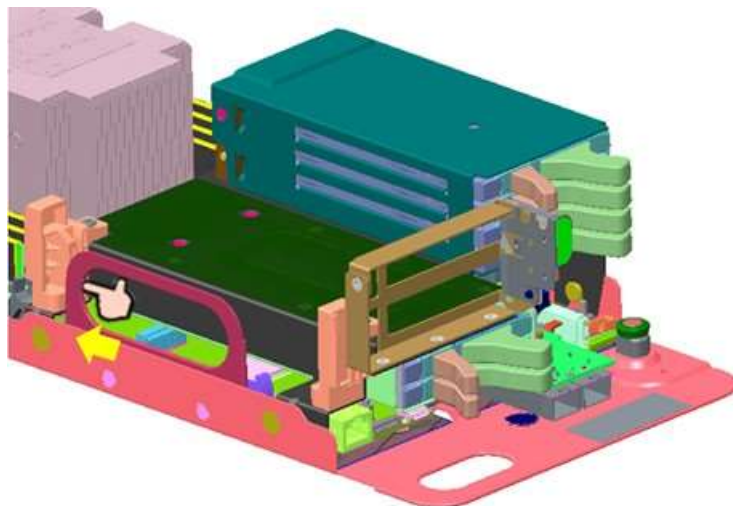
2.3.7 Install the Add-on cards

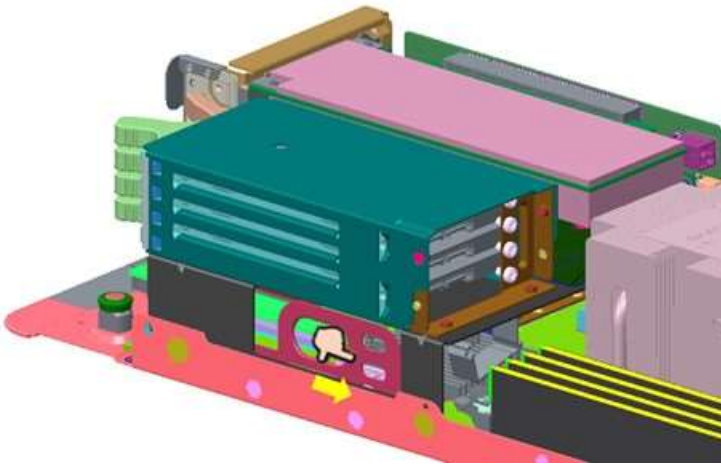
There are two PCIe slots available on PCIe riser board. You can install the add-on cards into the expansion slot of riser which is integrated with the bracket. The following instructions are for add-on card installation.

A. The HDD cage align to the sled and install it

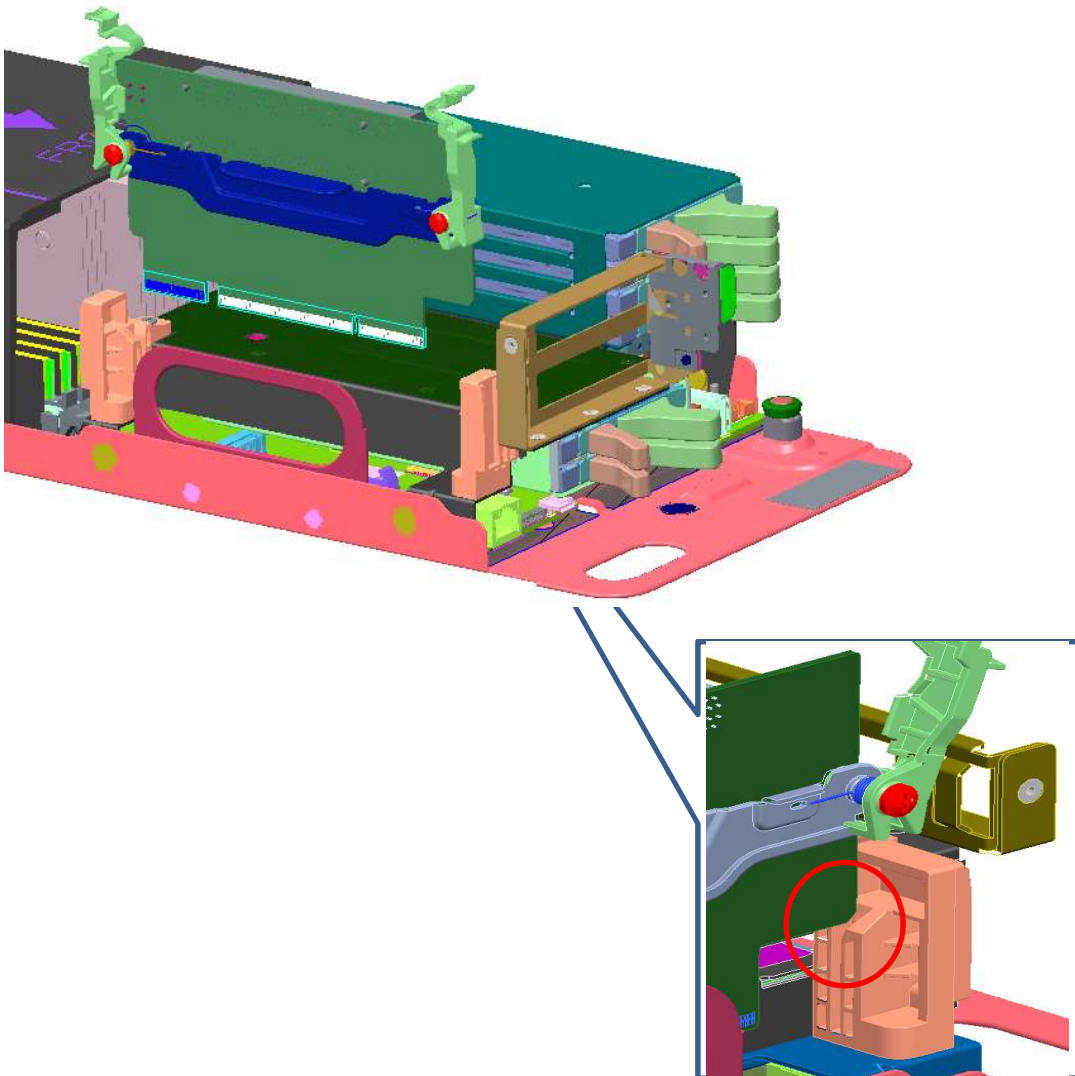


B. Push the Right / Left handle bar to lock the HDD Cage

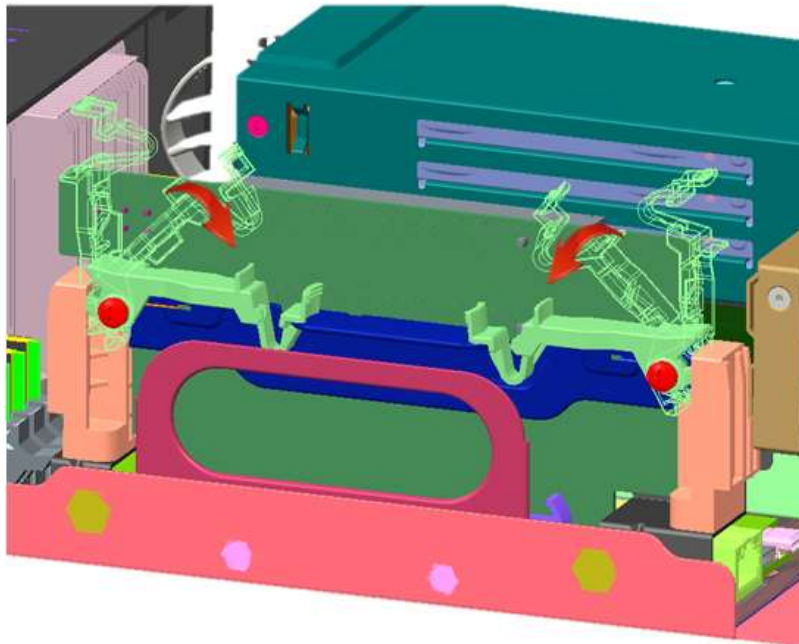




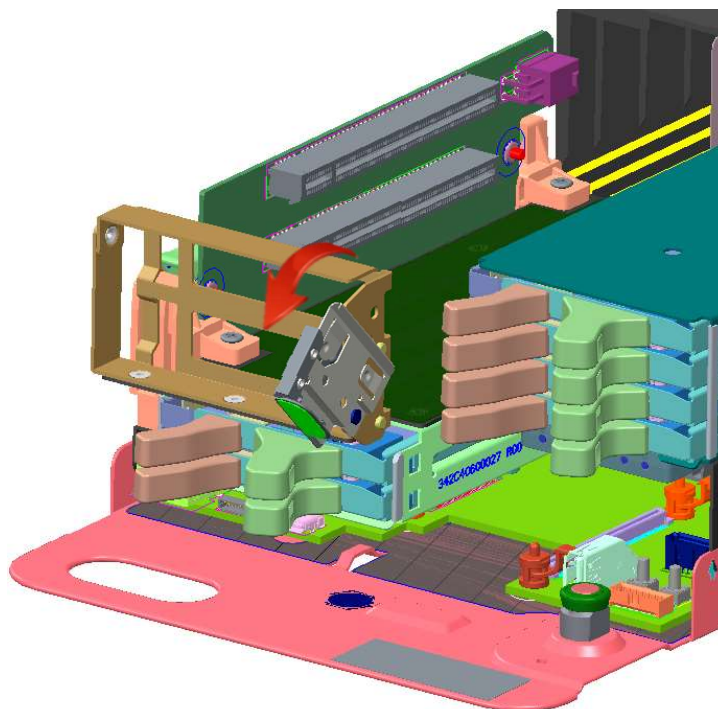
C. Insert the Riser Card



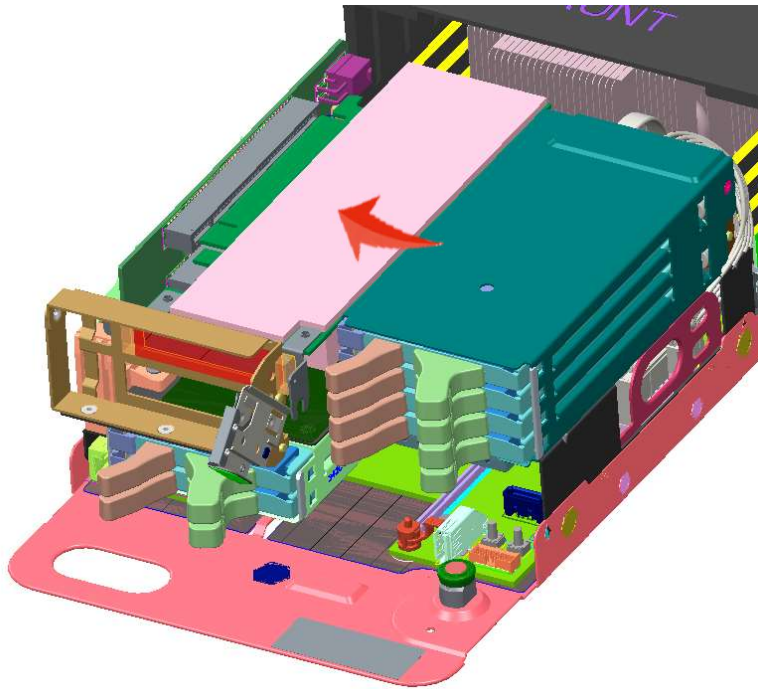
D. Fasten the latch to lock the riser card



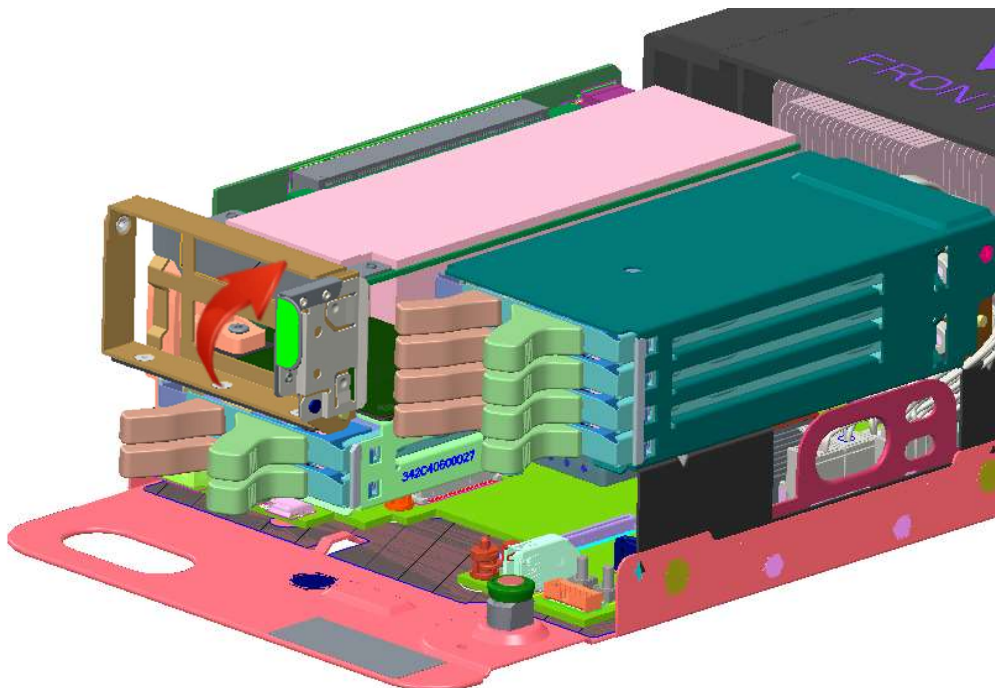
E. Open the retainer as shown



F. Insert the PCI card into the slot of riser board as shown



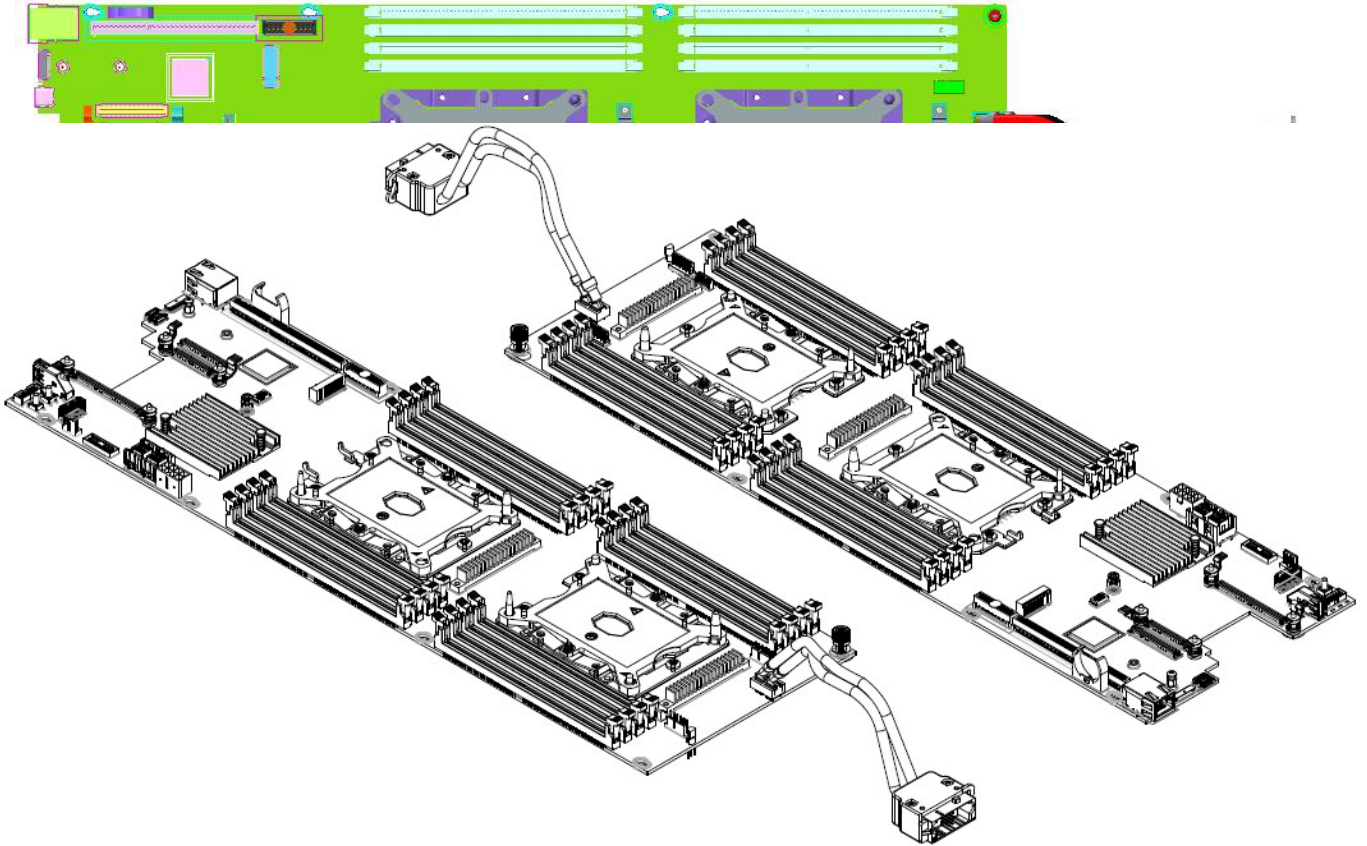
G. Close the retainer to fully secure the PCIe card



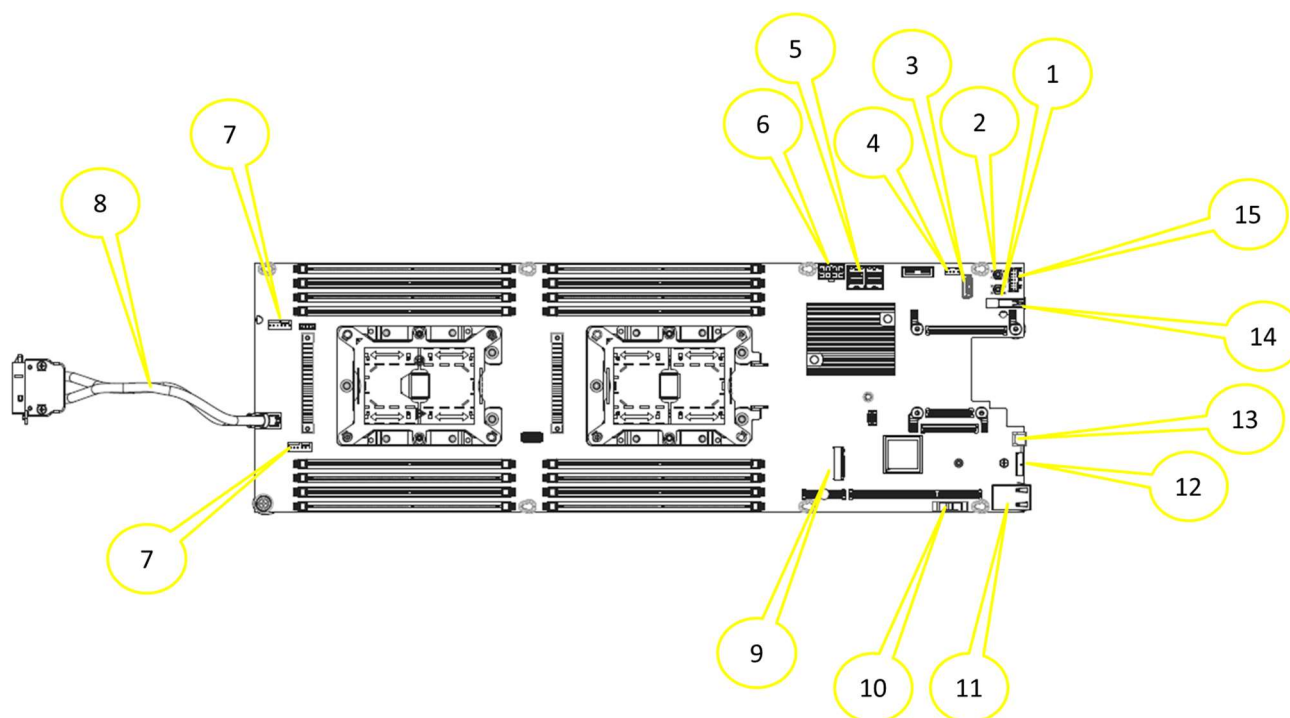
3. MainBoard Information

3.1 Board Introduction

Here are different views of the main board.

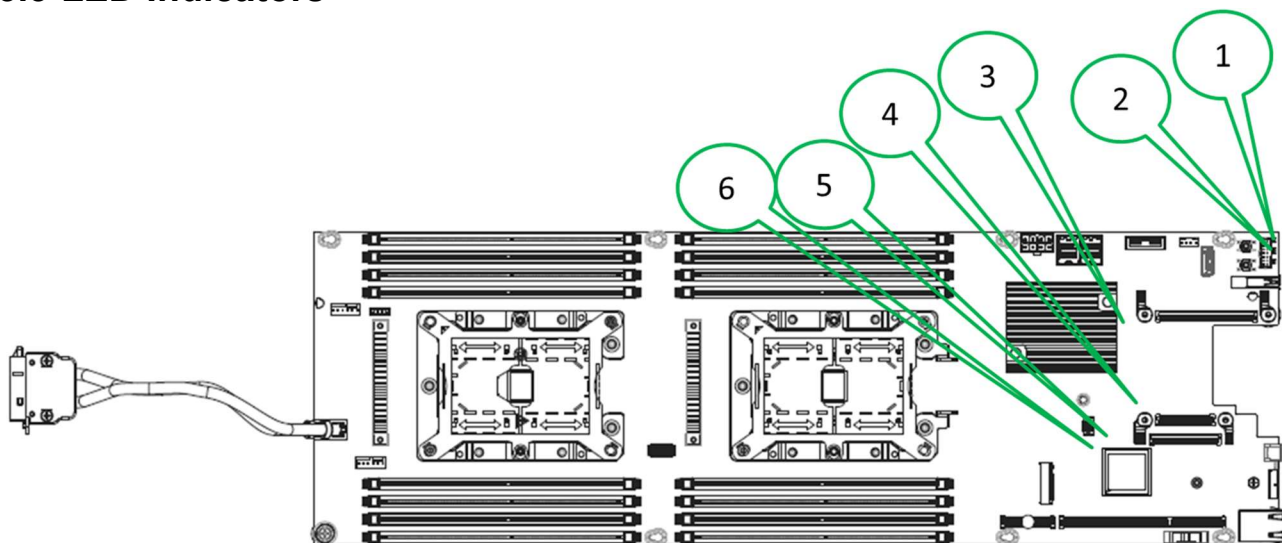


3.2 Board I/O



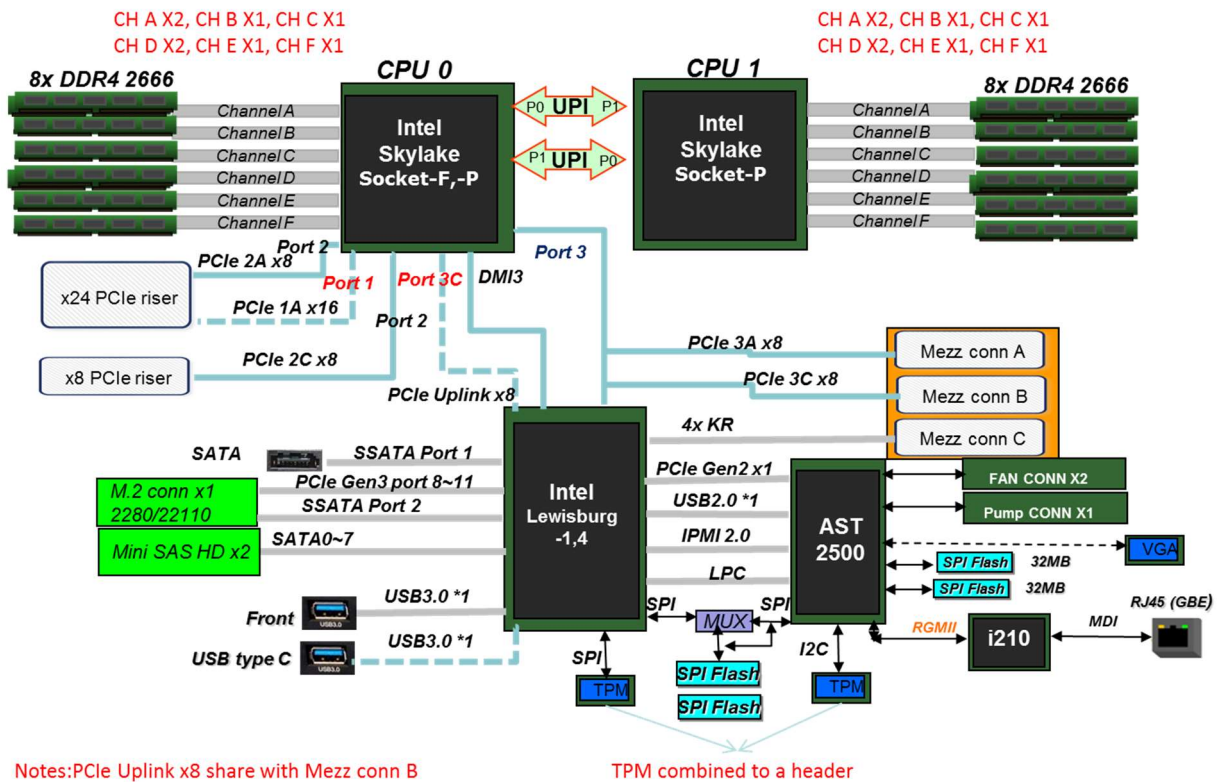
Item	Description	Item	Description
1	Power button	11	RJ45 of Intel® I210
2	Reset button	12	Connector for VGA
3	SATA port for SATA drive	13	Type C USB
4	Power for SATA drive	14	Type A USB
5	Two miniSASHD ports for external SATA drives	15	Connector for debug board(optional)
6	Power for external SATA drives		
7	Fan connector		
8	Power cable		
9	M.2 slot		
10	Battery		

3.3 LED Indicators



	LED	LED Color	Behavior	LED Location
1	Power LED	Blue	Power on	U31
2	HDD LED	Green	Twinkling as SATA device active	U45
3	CPLD Heartbeat	Green	CPLD FW initialize	LED4
4	BMC Heartbeat	Orange	BMC FW initialize	LED3
5	CPU CATERR	Yellow	CPU CATERR	LED28
6	BMC Fail	Orange	BMC fails	U83

3.4 Block Diagram



4. BIOS/uEFI

The TS2280-E7278P BIOS is based on uEFI v2.3.1 specification. The BIOS supports uEFI and legacy modes for different OS. The BIOS provided an interface for user to change system setting for application. Detailed BIOS settings are listed below.

4.1 BIOS Setup Utility

The BIOS Setup utility is a text-based utility that allows the user to configure the system and view current settings and environment information for the platform devices. The Setup utility controls the platform's built-in devices, the boot manager, and error manager.

The BIOS Setup interface consists of a number of pages or screens. Each page contains information or links to other pages. The advanced tab in Setup displays a list of general categories as links. These links lead to pages containing a specific category's configuration.

Console Redirection – BIOS Setup is functional via Console Redirection over various terminal emulation standards. When Console Redirection is enabled, the POST display out is in Text Mode due to Redirection data transfer in a serial port data terminal emulation mode.

Entering BIOS Setup

To enter the BIOS Setup using a keyboard (or emulated keyboard), press the <Del> or <F2> function key during boot time when the POST Diagnostic Screen is displayed.

The following instructional message is displayed on the Diagnostic Screen.

- **Press <DEL> or <F2> to enter setup.**
- **Press <F11> to boot popup menu.**
- **Press <F12> to PXE boot.**

When the Setup Utility is entered, the Main screen is displayed initially.

Setup Navigation Keyboard Commands

The bottom right portion of the Setup screen provides a list of commands that are use of navigate through the Setup utility. These commands are displayed at all times.

Key	Option	Description
→←	Select Screen	The Right/Left arrow is used to select the submenu in the main menu screen.
↑↓	Select item	The up arrow/down arrow is used to select the previous/next value in a pick list or the previous option is a menu item's option list. The selected item must then be activated by pressing the <Enter> key.

<Enter>	Execute Command	The <Enter> key is used to activate submenus when the selected feature is a submenu, or to display a pick list if a selected option has a value field, or to select a subfield for multi-valued features like time and date,. If a pick list is displayed, the <Enter> key selects the currently highlighted item, undoes the pick list, and returns the select item.																																																			
+/-	Change value	The plus/minus key on the keypad is used to change the value of the current item to the next/previous value. This key scrolls through the values in the associated pick list without displaying the full list.																																																			
<F1>	General Help	Pressing the <F1> key cause the following message to display: <table><tr><td>↑↓→←</td><td>:</td><td>Move</td></tr><tr><td>Enter</td><td>:</td><td>Select</td></tr><tr><td>+/-</td><td>:</td><td>Value</td></tr><tr><td>ESC</td><td>:</td><td>Exit</td></tr><tr><td>F1</td><td>:</td><td>General</td></tr><tr><td>Help</td><td></td><td></td></tr><tr><td>F8</td><td>:</td><td>Previous</td></tr><tr><td>Values</td><td></td><td></td></tr><tr><td>F9</td><td>:</td><td>Optimized</td></tr><tr><td>Defaults</td><td></td><td></td></tr><tr><td>F10</td><td>:</td><td>Save & Exit</td></tr><tr><td>Setup</td><td></td><td></td></tr><tr><td><K></td><td>:</td><td>Scroll help</td></tr><tr><td>area upwards</td><td></td><td></td></tr><tr><td><M></td><td>:</td><td>Scroll help</td></tr><tr><td>are downwards</td><td></td><td></td></tr><tr><td colspan="3">OK</td></tr></table> If the <Enter> key is pressed, or the <ESC> key is pressed, the user is returned to where they were before <F1> was pressed without affecting any existing field values.	↑↓→←	:	Move	Enter	:	Select	+/-	:	Value	ESC	:	Exit	F1	:	General	Help			F8	:	Previous	Values			F9	:	Optimized	Defaults			F10	:	Save & Exit	Setup			<K>	:	Scroll help	area upwards			<M>	:	Scroll help	are downwards			OK		
↑↓→←	:	Move																																																			
Enter	:	Select																																																			
+/-	:	Value																																																			
ESC	:	Exit																																																			
F1	:	General																																																			
Help																																																					
F8	:	Previous																																																			
Values																																																					
F9	:	Optimized																																																			
Defaults																																																					
F10	:	Save & Exit																																																			
Setup																																																					
<K>	:	Scroll help																																																			
area upwards																																																					
<M>	:	Scroll help																																																			
are downwards																																																					
OK																																																					
<F8>	Previous values	Pressing the <F8> key cause the following message to display: <table><tr><td colspan="2">Load Previous Values?</td></tr><tr><td>Yes</td><td>No</td></tr></table>	Load Previous Values?		Yes	No																																															
Load Previous Values?																																																					
Yes	No																																																				

		If “Yes” is highlighted and <Enter> is pressed, all changed fields are discarded to the values were saved before. If “No” is highlighted and <Enter> is pressed, or if the <ESC> key is pressed, the user is returned to where they were before <F8> was pressed without affecting any existing field values.				
<F9>	Optimized Defaults	Pressing the <F9> key causes the following message to display: <table><tr><td colspan="2">Load Optimized Defaults?</td></tr><tr><td>Yes</td><td>No</td></tr></table> If “Yes” is highlighted and <Enter> is pressed, all Setup fields are set to their default values. If “No” is highlighted and <Enter> is pressed, or if the <ESC> key is pressed, the user is returned to where they were before <F9> was pressed without affecting any existing field values.	Load Optimized Defaults?		Yes	No
Load Optimized Defaults?						
Yes	No					
<F10>	Save and Exit	Pressing the <F10> key causes the following message to display: <table><tr><td colspan="2">Save configuration and exit?</td></tr><tr><td>Yes</td><td>No</td></tr></table> If “Yes” is highlighted and <Enter> is pressed, all changes are saved and the Setup is exited. If “No” is highlighted and <Enter> is pressed, or if the <ESC> key is pressed, the user is returned to where they were before <F10> was pressed without affecting any existing values.	Save configuration and exit?		Yes	No
Save configuration and exit?						
Yes	No					
<ESC>	Exit	The <ESC> key provides a mechanism for backing out of any field. When the <ESC> key is pressed while editing any field or selecting features of a menu, the parent menu is re-entered. When the <ESC> key is pressed in any submenu, the parent menu is re-entered. When the <ESC> key is pressed in any major menu, the exit confirmation windows is displayed and the user is asked whether changes can be discarded. If “No” is selected and the <Enter> key is pressed, or if the <ESC> is pressed, the				

		user is returned to where they were before <ESC> was pressed, without affecting any existing settings. If “Yes” is selected and the <Enter> key is pressed, the setup is exited and the BIOS reset the system.
--	--	--

BIOS Setup Utility Screens

Setup Menu Screen contains the entire BIOS Setup collection and organizes them into many categories. Each category has a hierarchy with a top-level screen from which lower-level screens may be selected. The default setting of option is marked by blue color and star sign.

NOTE: The following pages provide the details of BIOS menu. Please be noticed that the BIOS menu are continually changing due to the BIOS updating. The BIOS menu provided are the most updated ones when this manual is written. Please contact us for the information of BIOS.

4.2 Main Screen

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

Main Advanced Platform Configuration Socket Configuration Server Mgmt ►

Checksum	Seed	▲ Choose the system default language
BIOS Information		
BIOS Vendor	American Megatrends	
Core Version	5.12	
Compliance	UEFI 2.5; PI 1.4	
Project Version	V1.000	
Build Date and Time	05/25/2018 17:38:15	
Access Level	Administrator	
Platform Information		
Board ID	0x9	
FAB ID	R02	⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Platform	TiogaPass	
Processor	50654 - SKX H0	
PCH	LBG QS/PRQ - 1G - S1	
RC Revision	151.R03	
Memory Information		
Available Memory		
Total Memory		
Speed		
System Language		
System Date		
System Time		

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

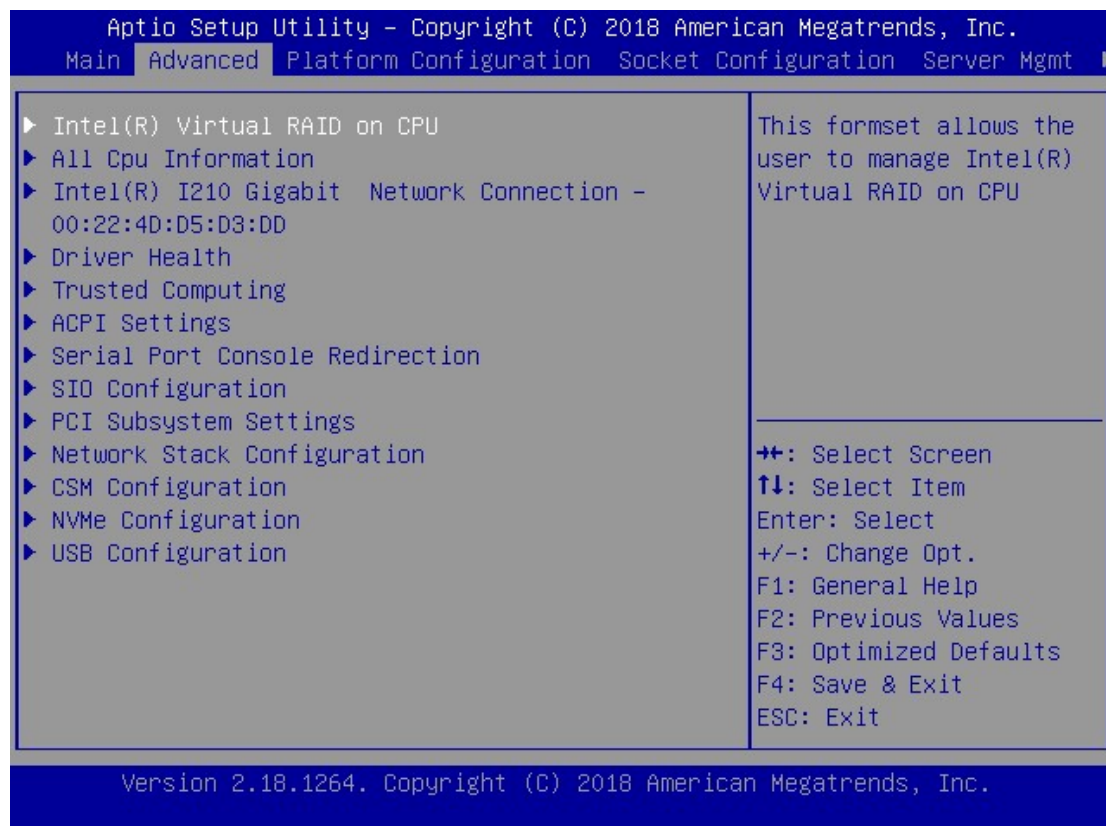
Main Advanced Platform Configuration Socket Configuration Server Mgmt ►

Platform Information		▲ Set the Time. Use Tab to switch between Time elements.
Board ID	0x9	
FAB ID	R02	
Platform	TiogaPass	
Processor	50654 - SKX H0	
PCH	LBG QS/PRQ - 1G - S1	
RC Revision	151.R03	
Memory Information		
Available Memory	16384 MB	
Total Memory	16384 MB	
Speed	2400 MT/S	⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
System Language		
System Date		
System Time		

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
Checksum	static text		BIOS Image checksum
BIOS Information	Static text	N/A	
BIOS Vendor	Static text	ASCII string	
Core Version	Static text	ASCII string	
Compliance	Static text	ASCII string	
Project Version	Static text	4-character string.	
Build Date and Time	Static text	String format MM/DD/YYYY HH:MM:SS	
Access Level	Static text	Administrator	
Platform Information	Static text	N/A	
Board ID	Dynamic text		Board model
FAB ID	Dynamic text		FAB model
Platform	Dynamic text		
Processor	Dynamic text	ASCII string	
PCH	Dynamic text	ASCII string	
RC Revision	Dynamic text	ASCII string	RC revision
Memory Information	Static text	N/A	
Available Memory	Dynamic text	YYYYYY MB	
Total Memory	Dynamic text	YYYYYY MB	
Speed	Dynamic text	XXXX MT/s	
System Language	Multipart item	[English]	Select the default system language
System Date	Dynamic text	[xxx mm/dd/yyyy]	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 2005-2099 Months: 1-12 Days: dependent on month
System Time	Dynamic text	[hh:mm:ss]	Set the Time. Use Tab to switch between Time elements.

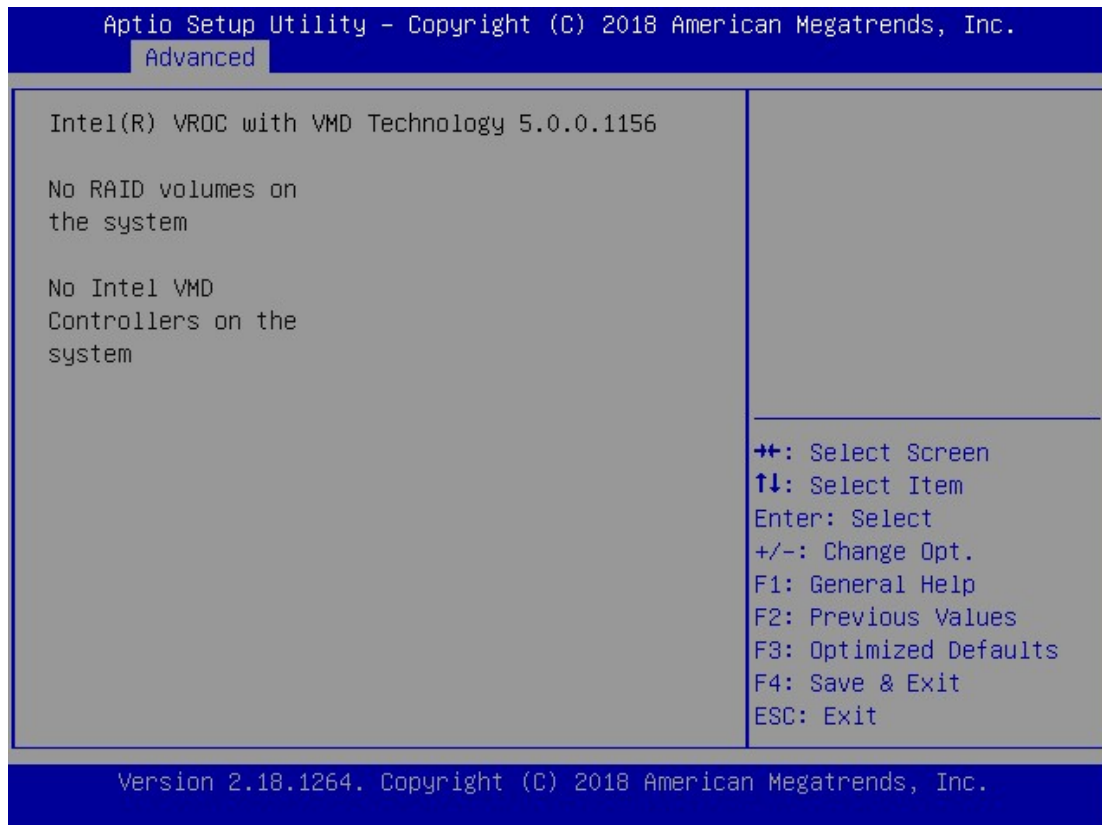
4.3 Advanced Screen



Item	Type	Options	Function description
Intel(R) Virtual RAID on CPU	Submenu	N/A	This formset allows the user to manage Intel(R) Virtual RAID on CPU
All Cpu Information	Submenu	N/A	Display all cpu information
Intel(R) I210 Gigabit Network Connection -	Submenu	N/A	Configure Gigabit Ethernet device parameters
Driver Health	Submenu	N/A	Provides Health Status for the Drivers/Controllers
Trusted Computing	Submenu	N/A	Trusted Computing Settings
ACPI Settings	Submenu	N/A	System ACPI Parameters.

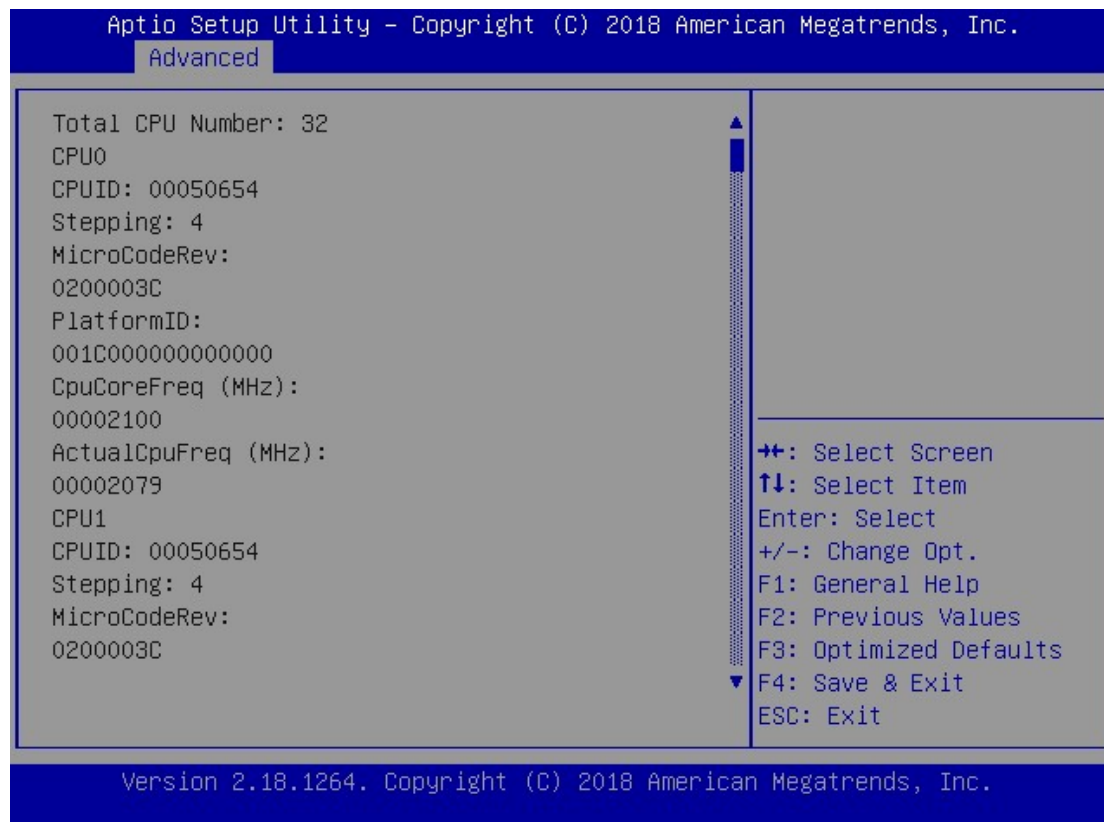
Serial Port Console Redirection	Submenu	N/A	Serial Port Console Redirection
SIO Configuration	Submenu	N/A	SIO Configuration
PCI Subsystem Settings	Submenu	N/A	PCI, PCI-X and PCI Express Settings
Network Stack Configuration	Submenu	N/A	Network Stack Settings
CSM Configuration	Submenu	N/A	CSM configuration: Enable/Disable, option ROM execution settings, etc.
NVMe Configuration	Submenu	N/A	NVMe Device Options Settings
USB Configuration	Submenu	N/A	USB Configuration Parameters

4.3.1 Intel(R) Virtual RAID on CPU



Item	Type	Options	Function description
Intel(R) VROC with VMD Technology	Dynamic text		
RAID volumes info	Dynamic text	N/A	
Intel VMD Controller info	Dynamic text	N/A	

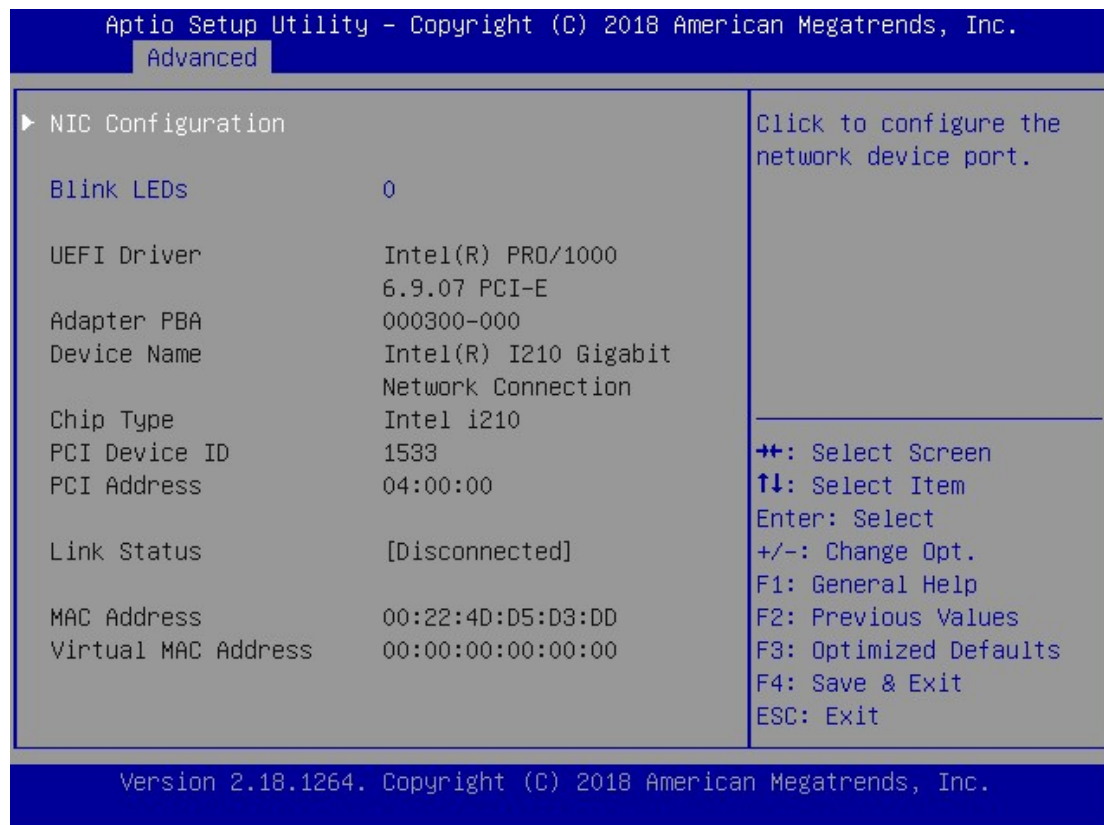
4.3.2 All CPU Information



Item	Type	Options	Function description
Total CPU Number:	Dynamic text	N/A	
CPUX:	Dynamic text	N/A	
CPUID:	Dynamic text	N/A	
Stepping:	Dynamic text	N/A	
MicroCodeRev:	Dynamic text	N/A	
Platform ID:	Dynamic text	N/A	
CpuCoreFreq (MHz)	Dynamic text	N/A	
ActualCpuFreq MHz)	Dynamic text	N/A	

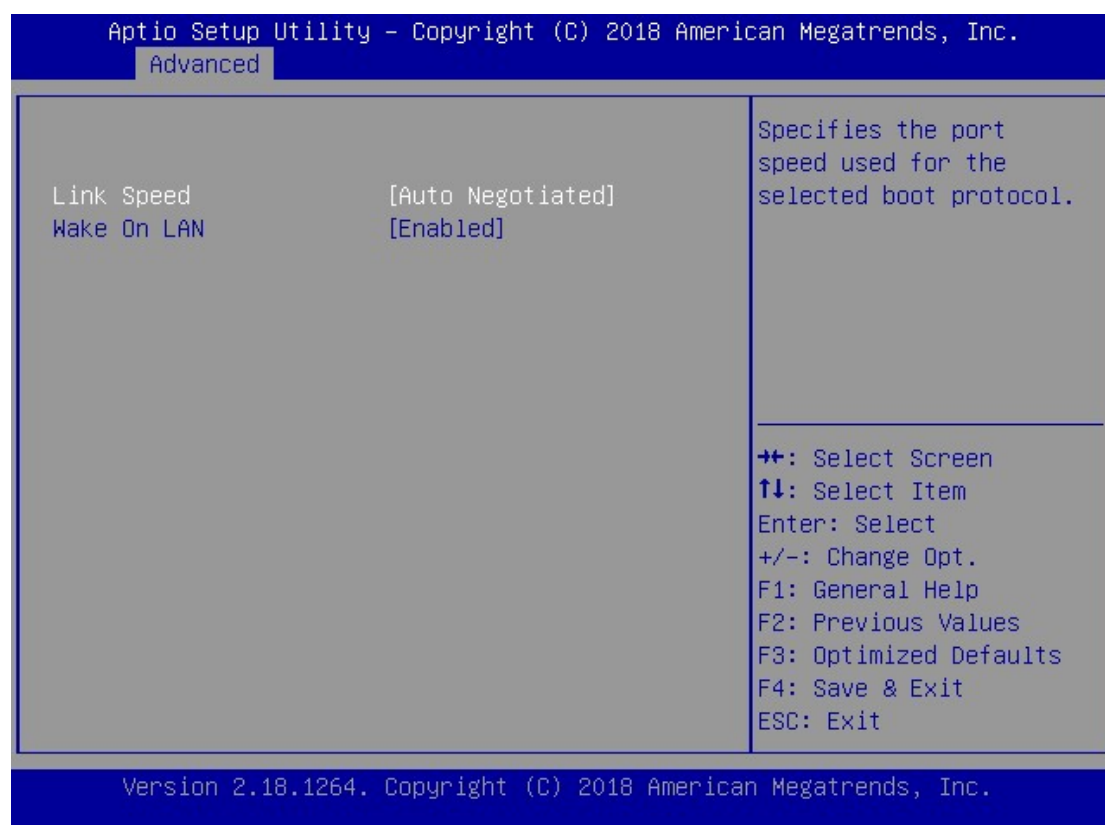
Note : X= 0, 1,2, ...

4.3.3 Intel(R) I210 Gigabit Network Connection



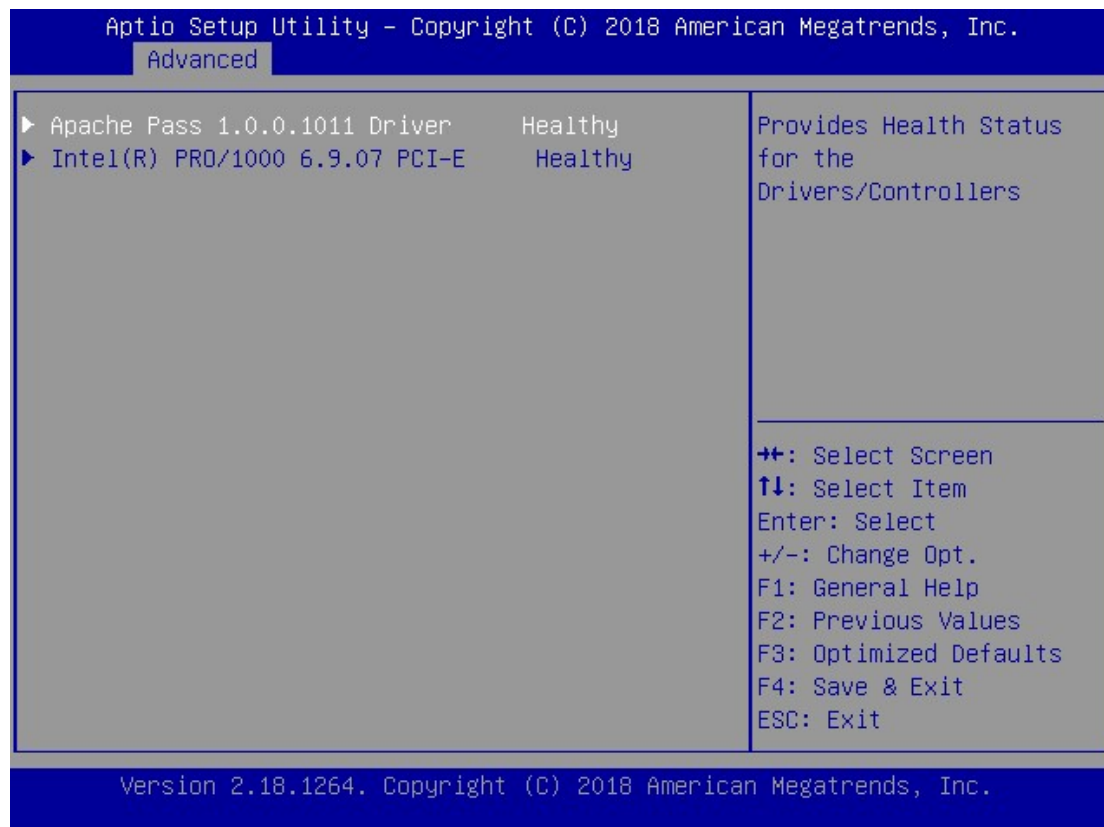
Item	Type	Options	Function description
Link Speed	Multipart item	<Auto Negotiated>* <10 Mbps Half> <10 Mbps Full> <100 Mbps Half> <100 Mbps Full>	Specifies the port speed used for the selected boot protocol.
Wake On LAN	Multipart item	<Disabled> <Enabled>*	Enables the server to be powered on using an in-band magic packet.

4.3.3.1 NIC Configuration



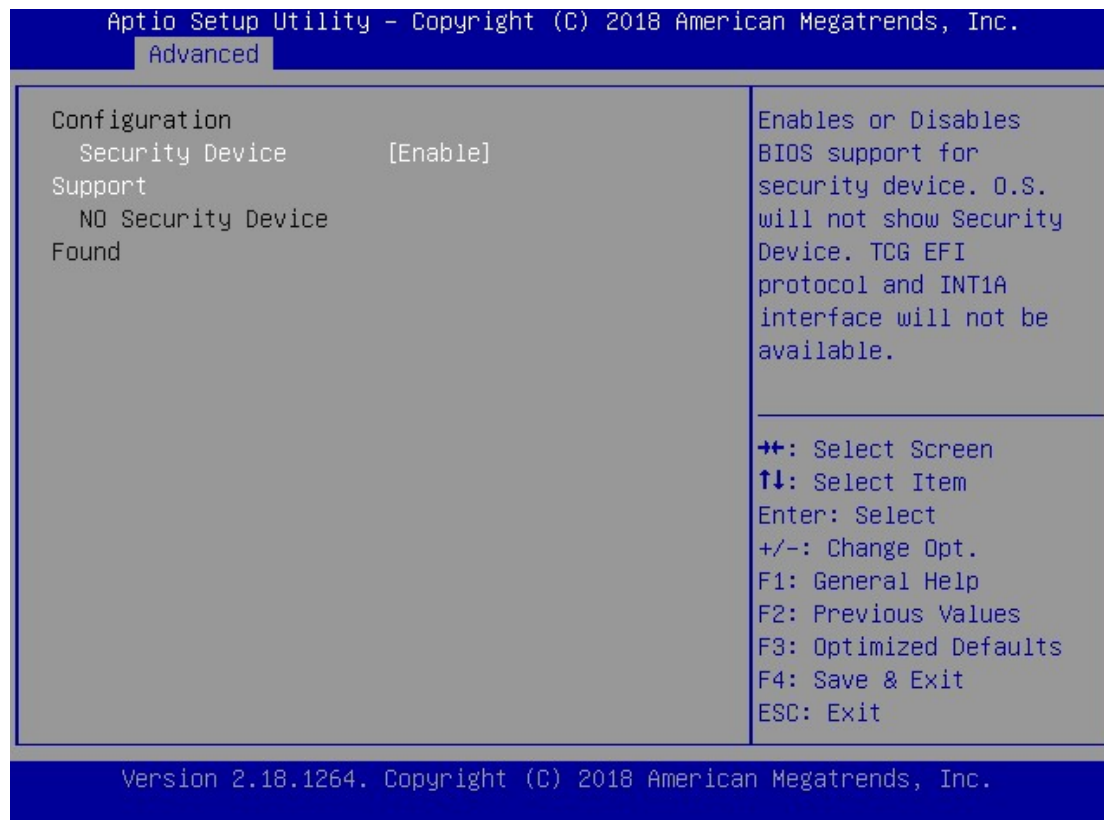
Item	Type	Options	Function description
Link Speed	Multipart item	<Auto Negotiated>* <10 Mbps Half> <10 Mbps Full> <100 Mbps Half> <100 Mbps Full>	Specifies the port speed used for the selected boot protocol.
Wake On LAN	Multipart item	<Disabled> <Enabled>*	Enables the server to be powered on using an in-band magic packet.

4.3.4 Driver Health



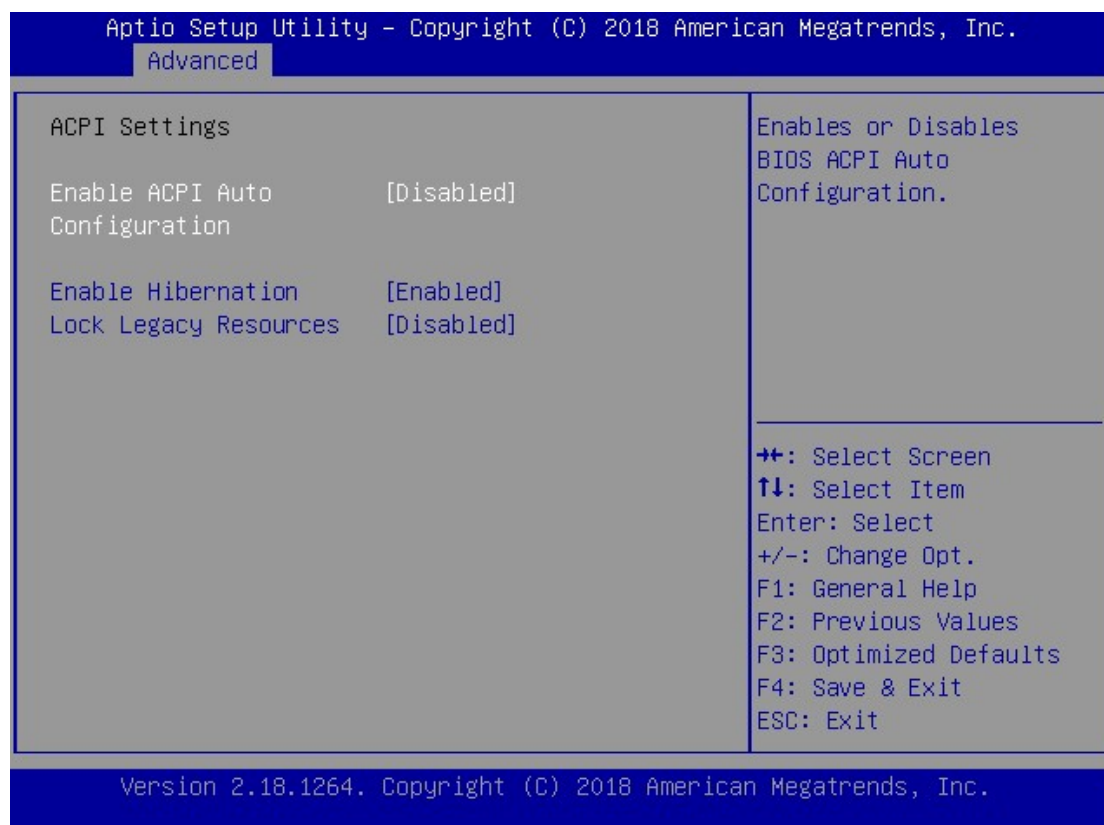
Item	Type	Options	Function description
Apache Pass Driver	Submenu	Drivers/Controllers Health Status	Provides Health Status for the Drivers/Controllers
Intel(R) PRO/1000 PCI-E	Submenu	Drivers/Controllers Health Status	Provides Health Status for the Drivers/Controllers

4.3.5 Trust Computing



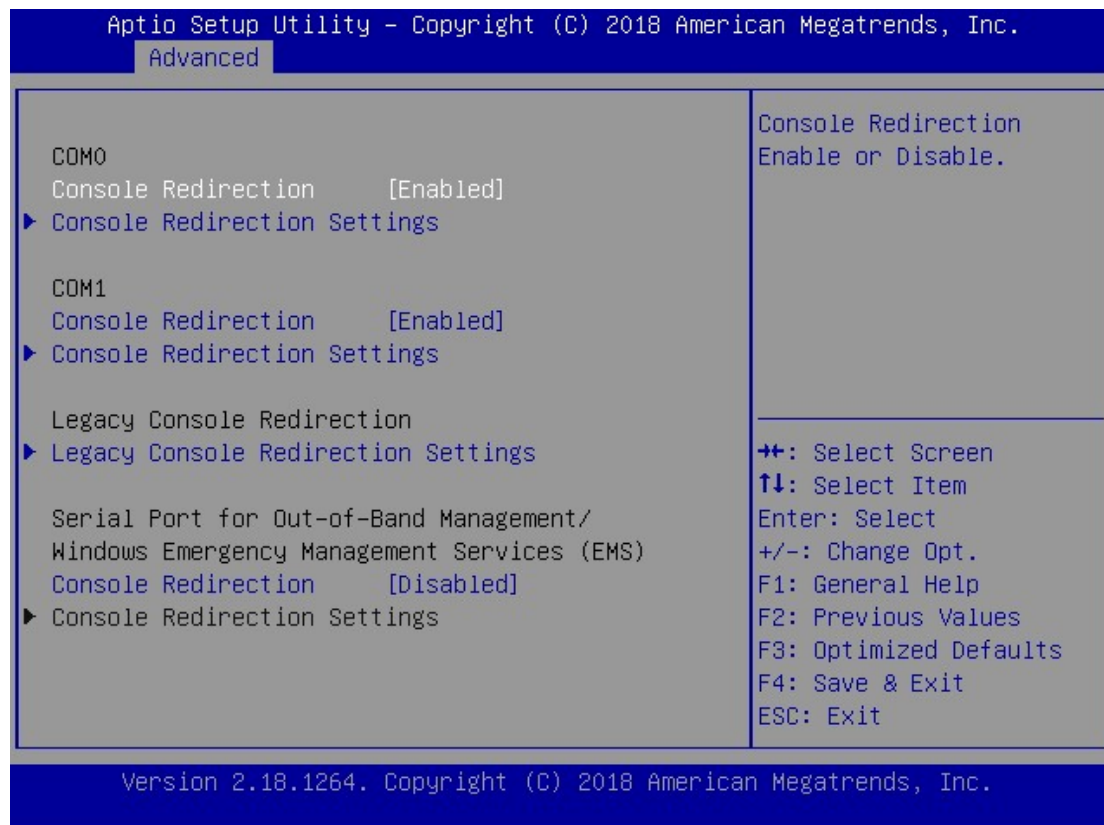
Item	Type	Options	Function description
Configuration	Static text	N/A	
Security Device Support	Multipart item	<Disable> <Enable>*	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
NO Security Device Found	Dynamic text	N/A	

4.3.6 ACPI Settings



Item	Type	Options	Function description
ACPI Settings	Static text	N/A	
Enable ACPI Auto Configuration	Multipart item	<Disable>* <Enable>	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Multipart item	<Disable> <Enable>*	Enables or Disables System ability to Hibernation (OS/S4 Sleep State). This option may not be effective with some operating systems.
Lock Legacy Resources	Multipart item	<Disable>* <Enable>	Enables or Disables Lock of Legacy Resources

4.3.7 Serial Port Console Redirection



Item	Type	Options	Function description
COMX	Static text	N/A	
Console Redirection	Multipart item	<Disable> <Enable>*	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	N/A	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
Legacy Console Redirection	Static text	N/A	
Legacy Console Redirection Settings	Submenu	N/A	Legacy Console Redirection Settings
Serial Port for Out-of-Band Management/Win	Static text	N/A	

dows Emergency Management Services			
Console Redirection	Multipart item	<Disable>* <Enable>	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	N/A	

Note : X= 0, 1

4.3.7.1 Console Redirection Settings

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

Advanced

COM0		▲ Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode
Console Redirection Settings		
Terminal Type	[VT100]	▼ ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Bits per second	[57600]	
Data Bits	[8]	
Parity	[None]	
Stop Bits	[1]	
Flow Control	[None]	
VT-UTF8 Combo Key	[Enabled]	
Support		
Recorder Mode	[Disabled]	
Resolution 100x31	[Disabled]	
Legacy OS	[80x24]	
Redirection		
Resolution		
Putty KeyPad	[VT100]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Advanced

Terminal Type		▲ When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is
Console Redirection Settings		
Terminal Type	[VT100]	▼ ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Bits per second	[57600]	
Data Bits	[8]	
Parity	[None]	
Stop Bits	[1]	
Flow Control	[None]	
VT-UTF8 Combo Key	[Enabled]	
Support		
Recorder Mode	[Disabled]	
Resolution 100x31	[Disabled]	
Legacy OS	[80x24]	
Redirection		
Resolution		
Putty KeyPad	[VT100]	
Redirection After BIOS POST	[Always Enable]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
COMX	Static text	N/A	
Console Redirection Settings	Static text	N/A	
Terminal Type	Multipart item	<VT100>* <VT100+> <VT-UTF8> <ANSI>	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	Multipart item	<9600> <19200> <38400> <57600>* <115200>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	Multipart item	<7> <8>*	Data Bits
Parity	Multipart item	<None>* <Even> <Odd> <Mark> <Space>	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	Multipart item	<1>* <2>	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	Multipart	<None>*	Flow control can prevent data

	item	<Hardware RTS/CTS>	loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	Multipart item	<Disabled> <Enabled>*	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Multipart item	<Disabled>* <Enabled>	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Multipart item	<Disabled>* <Enabled>	Enables or disables extended terminal resolution
Legacy OS Redirection	Multipart item	<80x24>* <80x25>	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	Multipart item	<VT100>* <LINUX> <XTMR6> <SCO> <ESCN> <VT400>	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	Multipart item	<Always Enable>* <BootLoader>	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

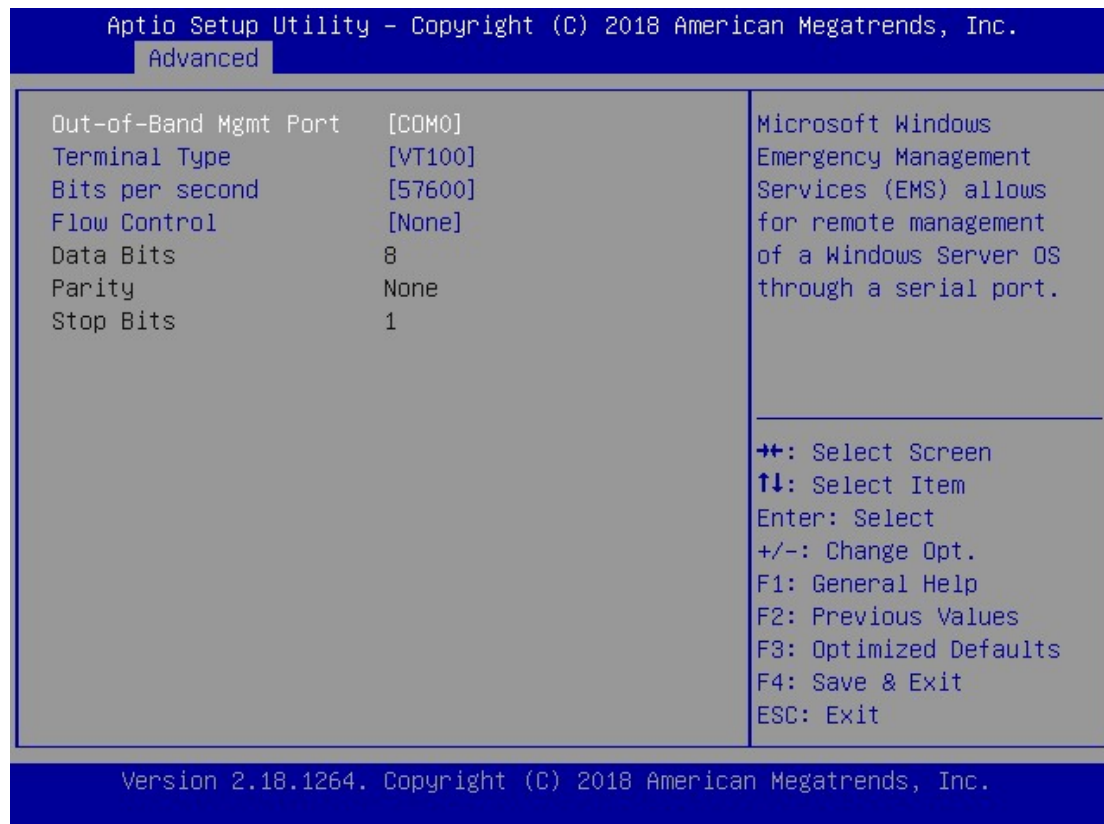
Note : X= 0, 1

4.3.7.2 Legacy Console Redirection Settings



Item	Type	Options	Function description
Legacy Serial Redirection Port	Multipart item	<COM0>* <COM1>	Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages

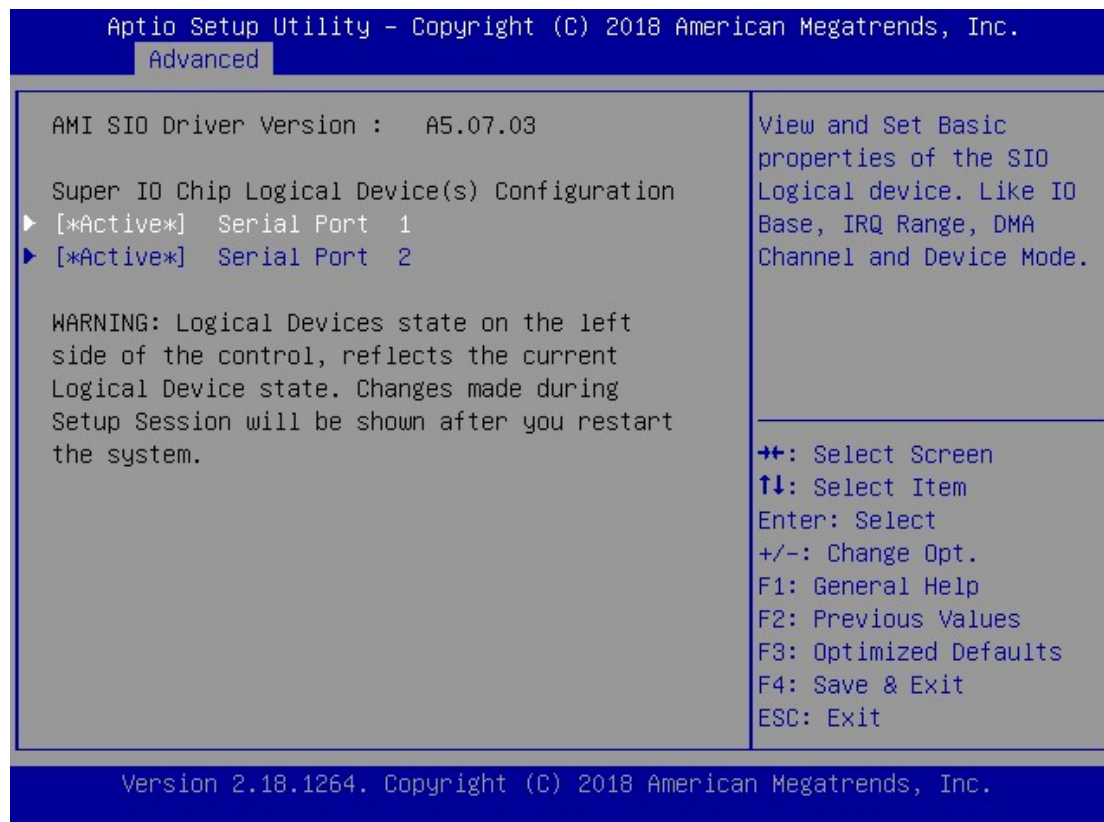
4.3.7.3 Console Redirection Settings (Serial Port for Out-of-Band Management/Windows Emergency Management Services)



Item	Type	Options	Function description
Out-of-Band Mgmt Port	Multipart item	<COM0>*	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.
Terminal Type	Multipart item	<VT100>* <VT100+> <VT-UTF8> <ANSI>	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	Multipart item	<9600> <19200> <38400> <57600>*	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower

		<115200>	speeds.
Flow Control	Multipart item	<None>* <Hardware RTS/CTS>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
Data Bits	Static text	<8>*	
Parity	Static text	<None>*	
Stop Bits	Static text	<1>	

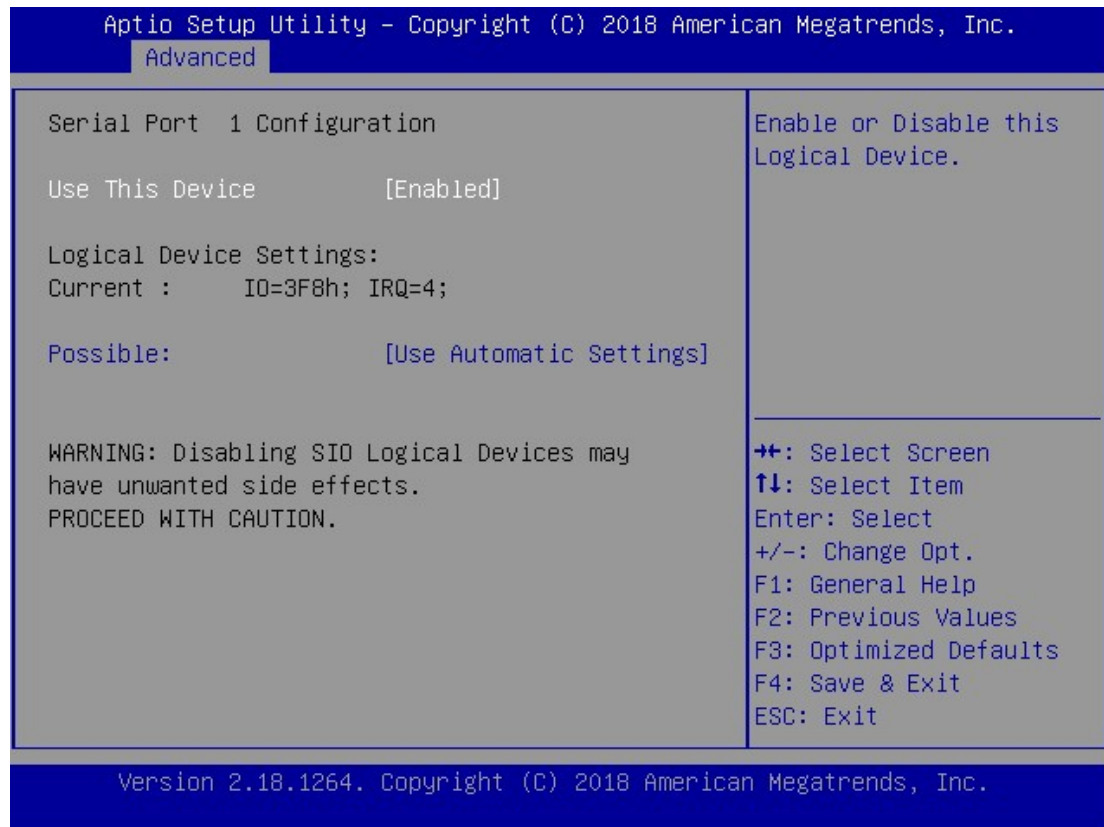
4.3.8 SIO Configuration



Item	Type	Options	Function description
AMI SIO Driver Version:	Dynamic text	N/A	
Super IO Chip Logical Devices(s) Configuration	Static text		
[*Active*] Serial Port X	Dynamic text	1	View and Set Basic properties of the SIO Logical device. Like IO Base, IRQ Range, DMA Channel and Device Mode.
WARNING: Logical Devices state on the left side of the control, reflects the current Logical Device state. Changes made during Setup Session will be shown after you restart the system.	Static text	N/A	

Note : X= 1, 2

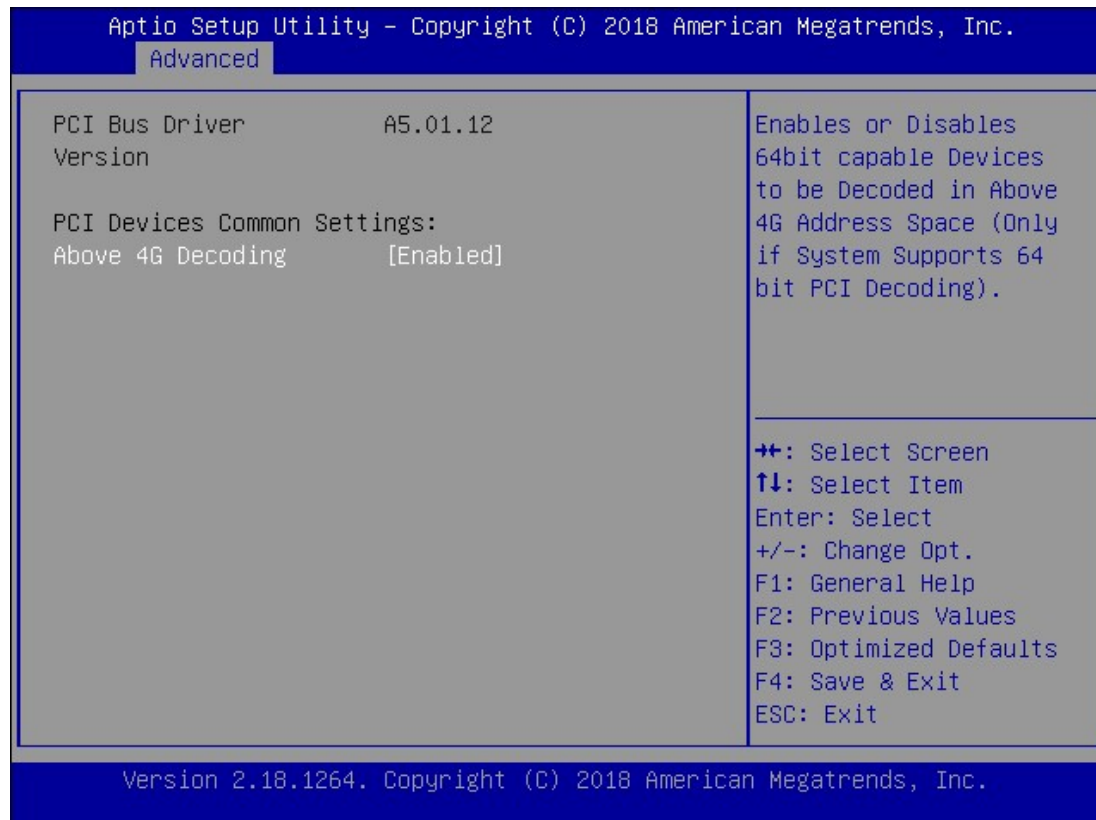
4.3.8.1 [*Active*] Serial Port X



Item	Type	Options	Function description
Serial Port X Configuration	Static text	N/A	
Use This Device	Multipart item	<Disabled> <Enabled>*	Enable or Disable this Logical Device.
Logical Device Settings:	Static text	N/A	
Current:	Dynamic text	N/A	
Possible:		<Use Automatic Settings>* <IO=3F8h; IRQ=4; DMA;> <IO=3F8h; IRQ=3,4,5,7,9,10,11,12; DMA;> <IO=2F8h; IRQ=3,4,5,7,9,10,11,12; DMA;>	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.

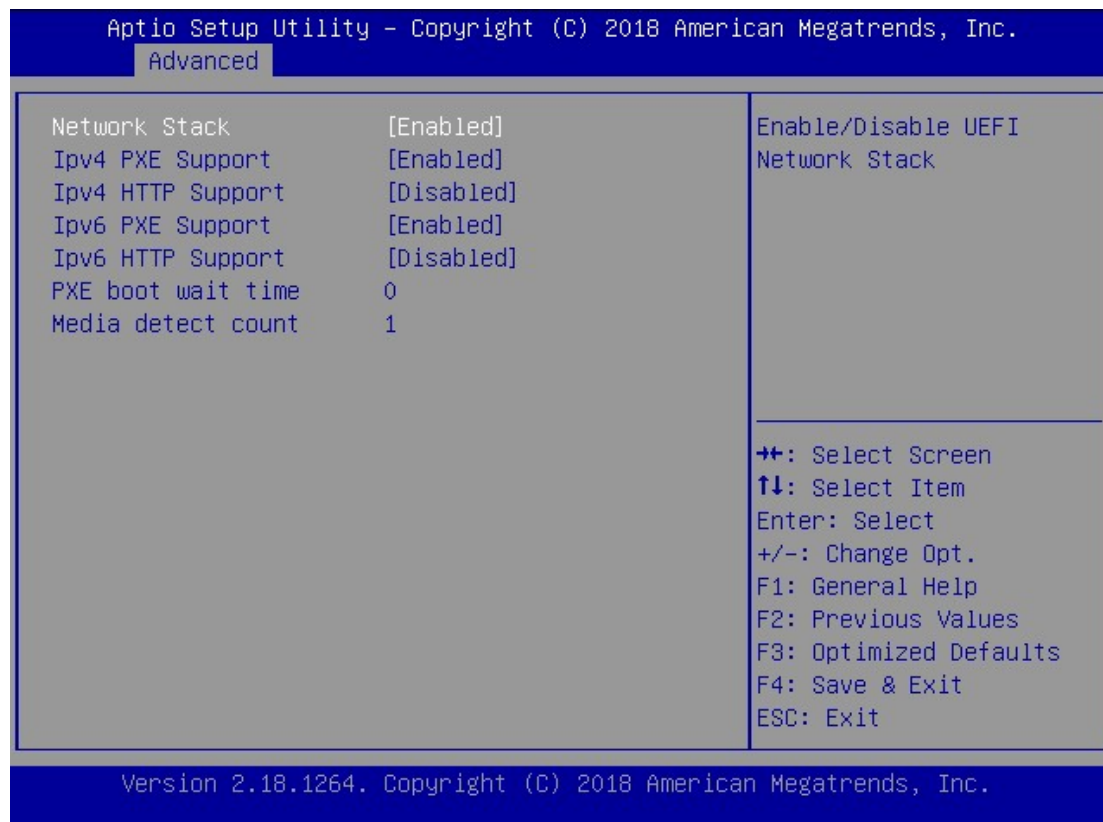
		<IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA;> <IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA;>	
WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	Static text	N/A	

4.3.9 PCI Subsystem Settings



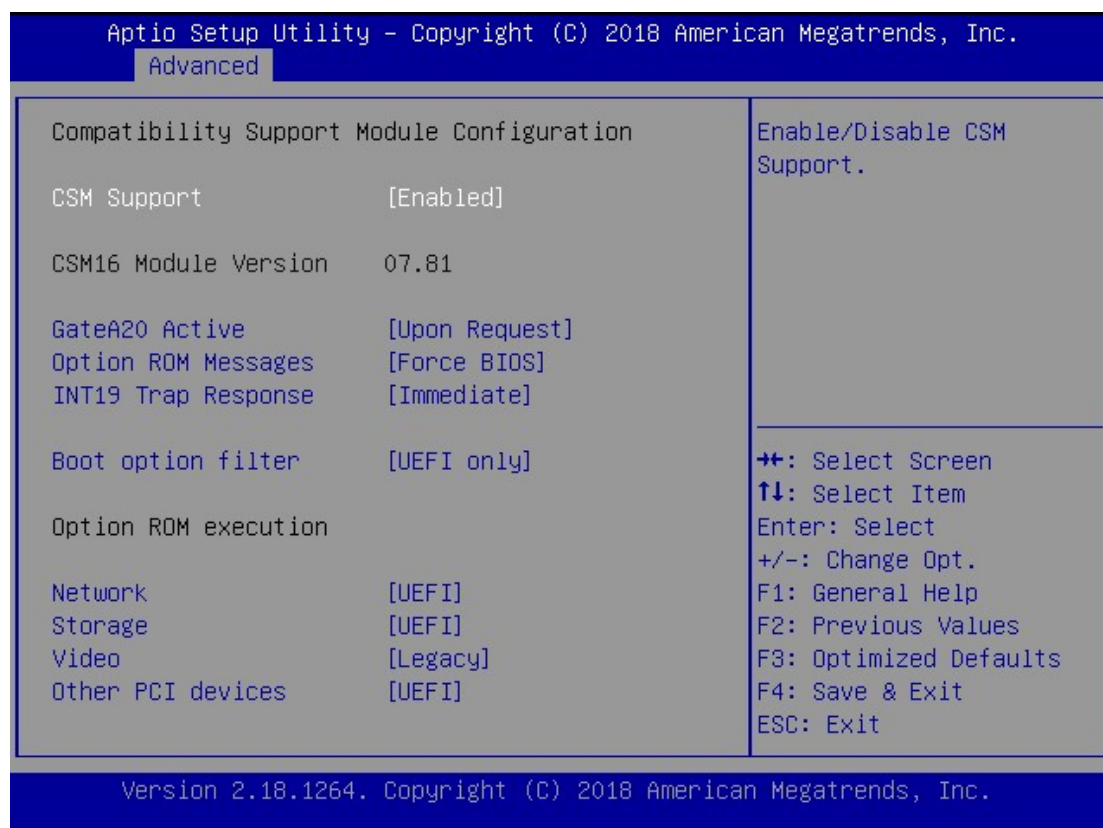
Item	Type	Options	Function description
PCI Bus Driver Version	Dynamic text	A5.01.12	
PCI Devices Common Settings	Static text	N/A	
Above 4G Decoding	Multipart item	<Disabled> <Enabled>*	Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).

4.3.10 Network Stack Configuration



Item	Type	Options	Function description
Network Stack	Multipart item	<Disabled> <Enabled>*	Enable/Disable UEFI Network Stack
Ipv4 PXE Support	Multipart item	<Disabled> <Enabled>*	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created
Ipv4 HTTP Support	Multipart item	<Disabled>* <Enabled>	Enable Ipv4 HTTP Boot Support. If disabled IPV4 HTTP boot option will not be created
Ipv6 PXE Support	Multipart item	<Disabled> <Enabled>*	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created
Ipv6 HTTP Support	Multipart item	<Disabled>* <Enabled>	Enable Ipv6 HTTP Boot Support. If disabled IPV6 HTTP boot option will not be created
PXE boot wait time	Numeric item	0* 0-5	Wait time to press ESC key to abort the PXE boot
Media detect count	Numeric item	1* 1-50	Number of times presence of media will be checked

4.3.11 CSM Configuration



Item	Type	Options	Function description
Compatibility Support Module Configuration	Static text	N/A	
CSM Support	Multipart item	<Disabled> <Enabled>*	Enable/Disable CSM Support.
CSM16 Module Version	Dynamic text	07.81	
GateA20 Active	Multipart item	< Upon Request >* < Always >	UPON REQUEST - GA20 can be disabled using BIOS services. ALWAYS - do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	Multipart item	< Force BIOS >*	Set display mode for Option ROM

		< Keep Current >	
INT19 Trap Response	Multipart item	< Immediate >* < Postponed >	BIOS reaction on INT19 trapping by Option ROM: IMMEDIATE - execute the trap right away; POSTPONED - execute the trap during legacy boot.
Boot option filter	Multipart item	< UEFI and Legacy > < Legacy only > >< UEFI only >*	This option controls Legacy/UEFI ROMs priority
Option ROM execution	Static text	N/A	
Network	Multipart item	< UEFI >* < Legacy >	Controls the execution of UEFI and Legacy PXE OpROM
Storage	Multipart item	< UEFI >* < Legacy >	Controls the execution of UEFI and Legacy Storage OpROM
Video	Multipart item	< UEFI > < Legacy >*	Controls the execution of UEFI and Legacy Video OpROM
Other PCI devices	Multipart item	< UEFI >* < Legacy >	Determines OpROM execution policy for devices other than Network, Storage, or Video

4.3.12 NVME Configuration



Item	Type	Options	Function description
NVMe Configuration	Static text	N/A	

4.3.13 USB Configuration

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Advanced		
USB Configuration		▲ Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
USB Module Version	17	
USB Controllers:		⇐ Select Screen ↑↓ Select Item Enter Select +/- Change Opt. F1 General Help F2 Previous Values F3 Optimized Defaults ▼ F4 Save & Exit ESC Exit
1 XHCI		
USB Devices:		
1 Drive, 1 Keyboard, 1 Mouse		
Legacy USB Support	[Enabled]	
XHCI Hand-off	[Enabled]	
USB Mass Storage	[Enabled]	
Driver Support		
Port 60/64 Emulation	[Enabled]	
USB hardware delays and time-outs:		
USB transfer time-out	[20 sec]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Advanced		
1 Drive, 1 Keyboard, 1 Mouse		▲ Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated
Legacy USB Support	[Enabled]	⇐ Select Screen ↑↓ Select Item Enter Select +/- Change Opt. F1 General Help F2 Previous Values F3 Optimized Defaults ▼ F4 Save & Exit ESC Exit
XHCI Hand-off	[Enabled]	
USB Mass Storage	[Enabled]	
Driver Support		
Port 60/64 Emulation	[Enabled]	
USB hardware delays and time-outs:		
USB transfer time-out	[20 sec]	
Device reset time-out	[20 sec]	
Device power-up delay	[Auto]	
Mass Storage Devices:		
JetFlashTranscend	[Auto]	
16GB 1100		

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
USB Configuration	Static text	N/A	
USB Module Version	Dynamic text	17	
USB Controllers:	Dynamic text	1 XHCI	
USB Devices:	Dynamic text	1 Drive, 1 Keyboard, 1 Mouse	
Legacy USB Support	Multipart item	<Auto> <Disabled> <Enabled>*	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	Multipart item	<Disabled> <Enabled>*	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	Multipart item	<Disabled> <Enabled>*	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation	Multipart item	<Disabled> <Enabled>*	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
USB hardware delays and time-outs:	Static text	N/A	
USB transfer time-out	Multipart item	<1 sec> <5 sec> <10 sec> <20 sec>*	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	Multipart item	<1 sec> <5 sec> <10 sec>	USB mass storage device Start Unit command time-out.

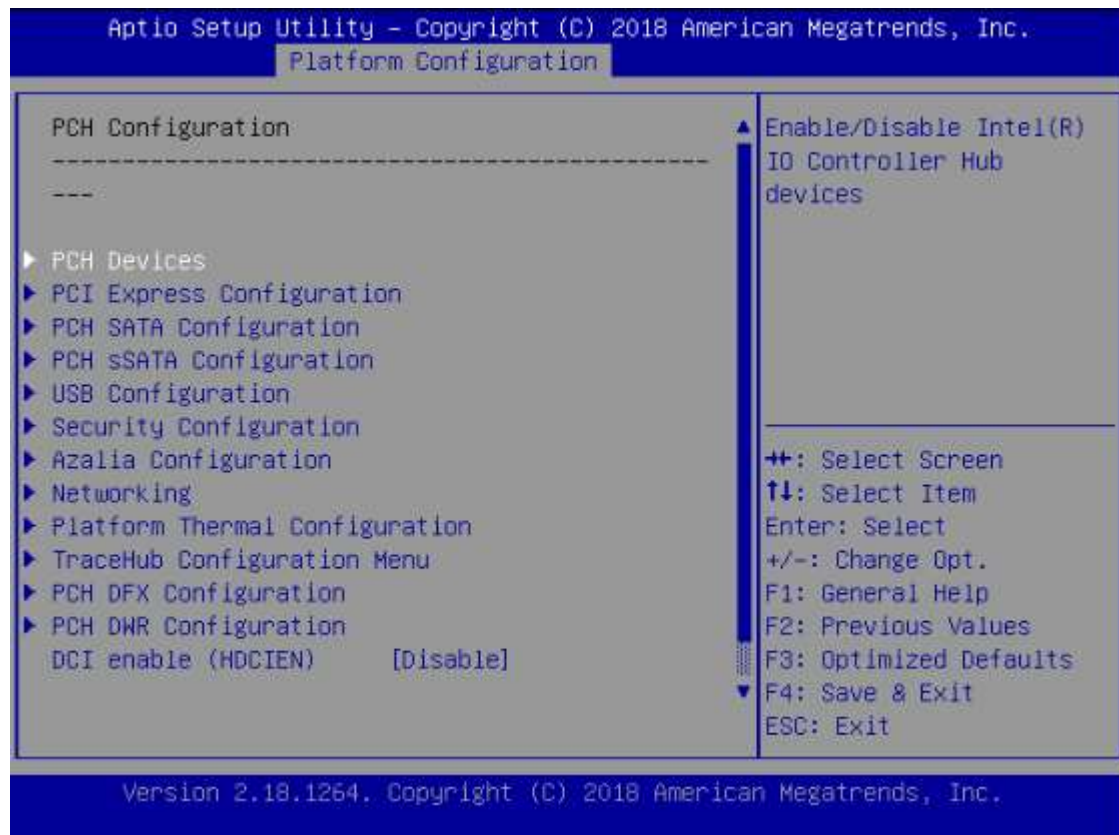
		<20 sec>*	
Device power-up delay	Multipart item	<Auto>* < Manual >	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.
Mass Storage Devices:	Static text	N/A	

4.4 Platform Configuration



Item	Type	Options	Function description
PCH Configuration	Submenu	N/A	Displays and provides option to change the PCH Settings
Miscellaneous Configuration	Submenu	N/A	
Server ME Configuration	Submenu	N/A	Configure Server ME Technology Parameters
Server ME Debug Configuration	Submenu	N/A	Server ME firmware debug parameters configuration
Runtime Error Logging	Submenu	N/A	Press <Enter> to view or change the runtime error log configuration.
Reserve Memory	Submenu	N/A	Reserve Memory
Non-Silicon Specific Items	Submenu	N/A	Non-Silicon Specific Menu
Setup Warning:	Static text	N/A	
Setting items on this Screen to incorrect values	Static text	N/A	
may cause system to malfunction!	Static text	N/A	

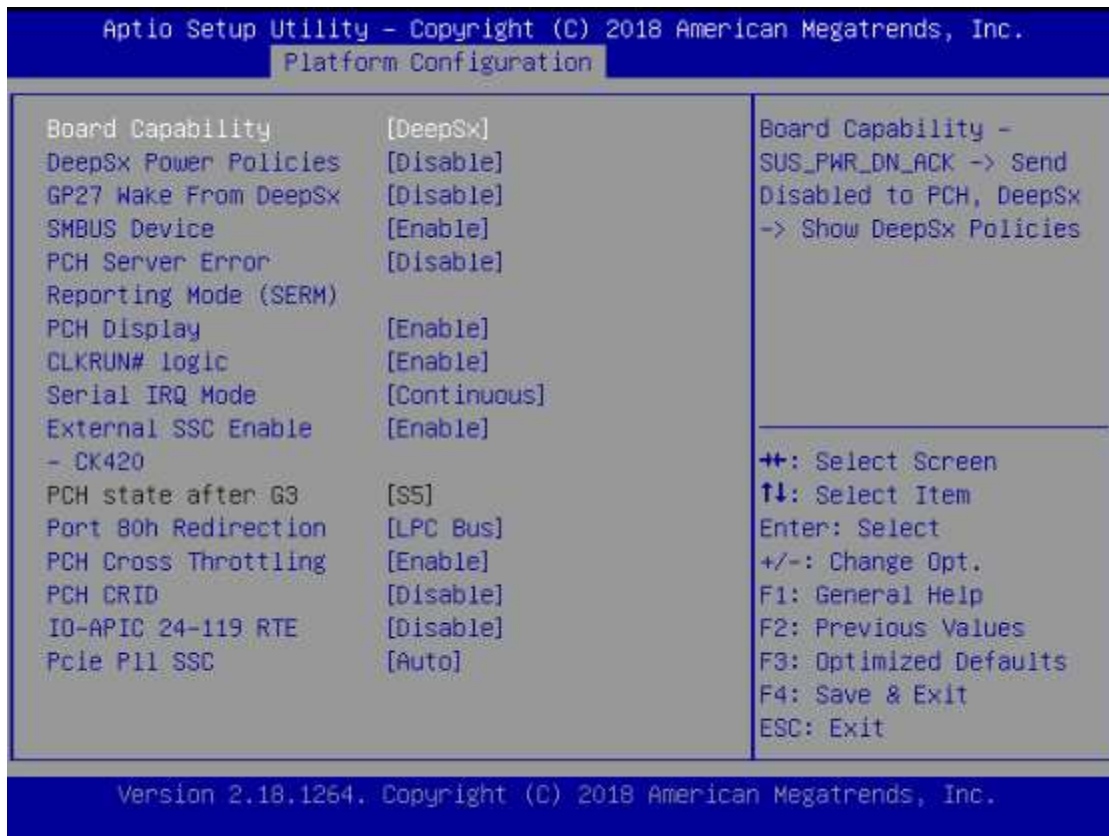
4.4.1 PCH Configuration



Item	Type	Options	Function description
PCH Configuration	Static text	N/A	
PCH Devices	Submenu	N/A	Enable/Disable Intel(R) IO Controller Hub devices
PCI Express Configuration	Submenu	N/A	PCI Express Configuration settings
PCH SATA Configuration	Submenu	N/A	SATA devices and settings
PCH sSATA Configuration	Submenu	N/A	sSATA devices and settings
USB Configuration	Submenu	N/A	USB Configuration Settings
Security Configuration	Submenu	N/A	Security Configuration settings
<u>Azalia</u> Configuration	Submenu	N/A	<u>Azalia</u> related configuration options

Networking	Submenu	N/A	Network devices and settings
Platform Thermal Configuration	Submenu	N/A	Platform Thermal Configuration options
TraceHub Configuration Menu	Submenu	N/A	TraceHub Configuration Settings
PCH DFX Configuration	Submenu	N/A	PCH DFX Configuration Options
PCH DWR Configuration	Submenu	N/A	PCH Dirty Warm Reset Configuration
DCI enable (HDCIEN)	Multipart item	<Disabled> * <Enabled>	When DCI is Enabled, it is taken as user consent to enable the DCI which allows debug over the USB3 interface. When Disabled, the host control is not enabling DCI feature.
DCI Auto Detect Enable	Multipart item	<Disabled> * <Enabled>	When set to Auto Detect, it detects DCI being connected during BIOS post time and enables DCI. Else it disables DCI.

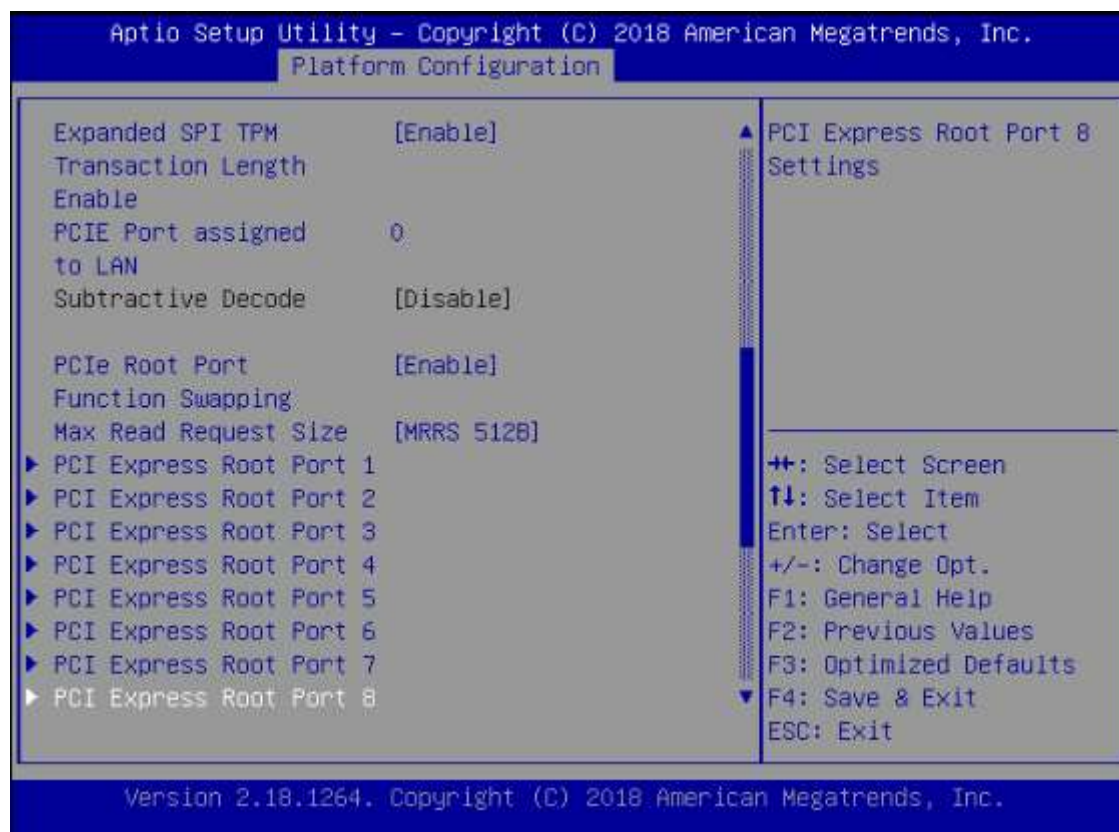
4.4.1.1 PCH Configuration



Item	Type	Options	Function description
Board Capability	Multipart item	<DeepSx>* <SUS_PWR_DN_ACK>	Board Capability - SUS_PWR_DN_ACK -> Send Disabled to PCH, DeepSx -> Show DeepSx Policies
DeepSx Power Policies	Multipart item	<Disabled>* <Enabled in S5> <Enabled in S4-S5> <Enabled in S3-S4-S5>	configure the DeepSx Mode configuration.
GP27 Wake From DeepSx	Multipart item	<Disabled>* <Enabled>	Wake from DeepSx by the assertion of GP27 pin
SMBUS Device	Multipart item	<Disabled> <Enabled>* *	Enable/Disable SMBUS Device.

PCH Server Error Reporting Mode (SERM)	Multipart item	<Disabled> * <Enabled>	When enabled MCH is the final target of all errors otherwise SPCH is the final target to all errors
PCH Display	Multipart item	<Disabled> <Enabled> *	Enables/Disables PCH Display
CLKRUN# logic	Multipart item	<Disabled> <Enabled> *	Enable the CLKRUN# logic to stop the PCI clocks.
Serial IRQ Mode	Multipart item	<Quiet> <Continuous>*	Configure Serial IRQ Mode.
External SSC Enable - CK420	Multipart item	<Disabled> <Enabled> *	Enable Spread Spectrum - only affects external clock generator
PCH state after G3	Multipart item	<S0> <S5>*	Select S0/S5 for ACPI state after a G3
Port 80h Redirection	Multipart item	<LPC Bus>* <PCI Bus>	Control where the Port 80h cycles are sent.
PCH Cross Throttling	Multipart item	<Disabled> <Enabled> *	Enable/Disable the PCH Cross Throttling feature. Only ULT support this feature.
PCH CRID	Multipart item	<Disabled> * <Enabled>	Enable/Disable PCH's CRID
IO-APIC 24-119 RTE	Multipart item	<Disabled> * <Enabled>	Enable/Disable IO APIC entries 24-119
Pcie Pll SSC	Multipart item	<Auto>* <Disabled> <0.5%>	Pcie Pll SSC percentage or Disable SSC. Range is 0.0%-1.9%. Last once is the POR for LBG

4.4.1.2 PCI Express Configuration





Item	Type	Options	Function description
PCI Delay Optimization	Multipart item	<Disabled>* <Enabled>	Experimental ACPI additions for FW latency optimizations
Compliance Test Mode	Multipart item	<Disabled>* <Enabled>	Enable when using Compliance Load Board
PCI-E ASPM Support (Global)	Multipart item	<Disabled>* <Enabled>	This option allows setting ASPM support for all downstream devices.
CTO for Uplink x16	Multipart item	<40-50ms(spec 50us-50ms)>* <40-50ms(spec 16ms-55ms)> <160-170ms(spec 65ms-210ms)> <400-500ms(spec 260ms-900ms)> <1.6-1.7s(spec 1s-3.5s)> <Disable>	PCI Express Completion Timer TO settings for Uplink x16
CTO for	Multipart	<40-50ms(spec	PCI Express Completion Timer

Uplink x8	item	50us-50ms)* <40-50ms(spec 16ms-55ms)> <160-170ms(spec 65ms-210ms)> <400-500ms(spec 260ms-900ms)> <1.6-1.7s(spec 1s- 3.5s)> <Disable>	TO settings for Uplink x8
MPL for Uplink x16	Multipart item	<MPL 128B> <MPL 256B> <MPL 512B>*	PCI Express Max Payload Size settings for Uplink x16
MPL for Uplink x8	Multipart item	<MPL 128B> <MPL 256B> <MPL 512B>*	PCI Express Max Payload Size settings for Uplink x8
PCIE Clock Gating	Multipart item	<Disabled>* <Enabled>	PCIE Clock Gating Enable/Disable for all PCH PCIE Ports.
PCH DMI ASPM	Multipart item	<Platform-POR>* <ASPM L1> <Disable>	PCH DMI ASPM Setting
DMI Link Extended Synch Control	Multipart item	<Disabled>* <Enabled>	The control of Extended Synch on SB side of the DMI Link.
Stop and Scream	Multipart item	<Disabled>* <Enabled>	When Enabled DS packets on DMI with the EP bit set, will have their UT bit set
Expanded SPI TPM Transaction Length Enable	Multipart item	<Disabled> <Enabled>*	When Enabled allows SPI TPM transactions up to 64 bytes
PCIE Port assigned to LAN	Numeric item	0*~20	If Port number is 0, GbE communication is not Enabled over PCIe
Subtractive Decode	Multipart item	<Disabled>* <Enabled>	PCI Express Root Port Subtractive Decode Enable/Disable.
PCIe Root	Multipart	<Disabled>	Enable PCIe root port function

Port Function Swapping	item	<Enabled>*	swapping feature to dynamically assign function 0 to enabled root port.
Max Read Request Size	Multipart item	<MRRS 128B> <MRRS 256B> <MRRS 512B>* <MRRS 1024B> <MRRS 2048B> <MRRS 4096>	PCIe Max Read Request Size Selection.
PCI Express Root Port 1	Submenu	N/A	PCI Express Root Port 1 Settings
PCI Express Root Port 2	Submenu	N/A	PCI Express Root Port 2 Settings
PCI Express Root Port 3	Submenu	N/A	PCI Express Root Port 3 Settings
PCI Express Root Port 4	Submenu	N/A	PCI Express Root Port 4 Settings
PCI Express Root Port 5	Submenu	N/A	PCI Express Root Port 5 Settings
PCI Express Root Port 6	Submenu	N/A	PCI Express Root Port 6 Settings
PCI Express Root Port 7	Submenu	N/A	PCI Express Root Port 7 Settings
PCI Express Root Port 8	Submenu	N/A	PCI Express Root Port 8 Settings
PCI Express Root Port 9	Submenu	N/A	PCI Express Root Port 9 Settings
PCI Express Root Port 10	Submenu	N/A	PCI Express Root Port 10 Settings
PCI Express Root Port 11	Submenu	N/A	PCI Express Root Port 11 Settings
PCI Express Root Port 12	Submenu	N/A	PCI Express Root Port 12 Settings
PCI Express Root Port 13	Submenu	N/A	PCI Express Root Port 13 Settings
PCI Express Root Port 14	Submenu	N/A	PCI Express Root Port 14 Settings
PCI Express Root Port 15	Submenu	N/A	PCI Express Root Port 15 Settings

PCI Express Root Port 16	Submenu	N/A	PCI Express Root Port 16 Settings
PCI Express Root Port 17	Submenu	N/A	PCI Express Root Port 17 Settings
PCI Express Root Port 18	Submenu	N/A	PCI Express Root Port 18 Settings
PCI Express Root Port 19	Submenu	N/A	PCI Express Root Port 19 Settings
PCI Express Root Port 20	Submenu	N/A	PCI Express Root Port 20 Settings

4.4.1.2.1 PCI Express Root Port X (X=1~20)

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Platform Configuration		
PCI Express Root Port 1	[Enabled]	▲ Control the PCI Express Root Port.
PCIE ASPM	[Disable ASPM]	
L1 Substates	[L1.1 & L1.2]	
Gen3 Eq Phase3 Method	[Hardware]	
ACS	[Enable]	
URR	[Disable]	
FER	[Disable]	
NFER	[Disable]	
CER	[Disable]	
SEFE	[Disable]	++: Select Screen
SECE	[Disable]	↑↓: Select Item
PME SCI	[Disable]	Enter: Select
Hot Plug	[Disable]	+/-: Change Opt.
Advanced Error Reporting	[Enable]	F1: General Help
PCIE Speed	[Auto]	F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Platform Configuration		
PCIE Speed	[Auto]	▲ PCIE LTR Configuration Lock
MSI	[Enable]	
PCIE Lane Topology	[Unknown]	
Max Payload Size	[MPL 128B]	
Compl. Timeout	[40-50ms(spec 50us-50ms)]	
Current speed for this RP is:	Unknown	
Current width for this RP is:	Unknown	
PCH PCIE LTR Configuration		++: Select Screen
PCH PCIE1 LTR	[Enable]	↑↓: Select Item
Snoop Latency	[Auto]	Enter: Select
Override		+/-: Change Opt.
Non Snoop Latency	[Auto]	F1: General Help
Override		F2: Previous Values
PCIE1 LTR Lock	[Disable]	F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit

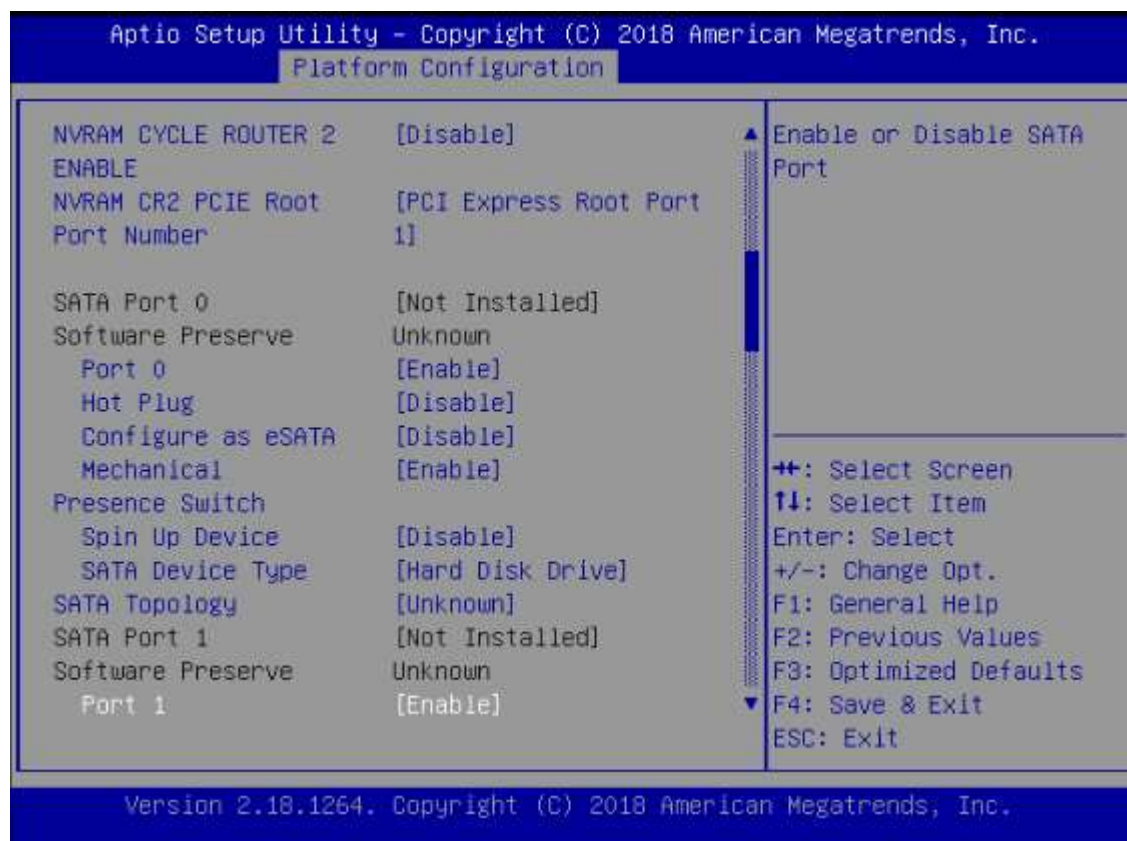
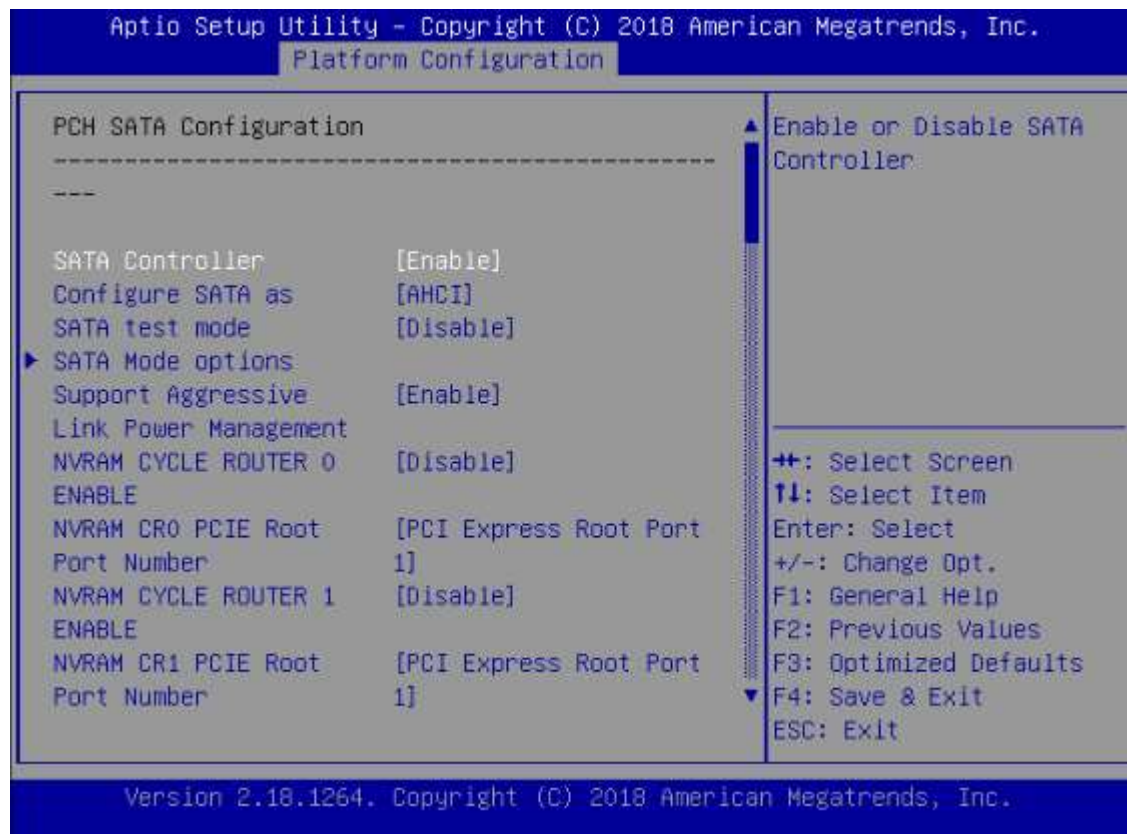
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

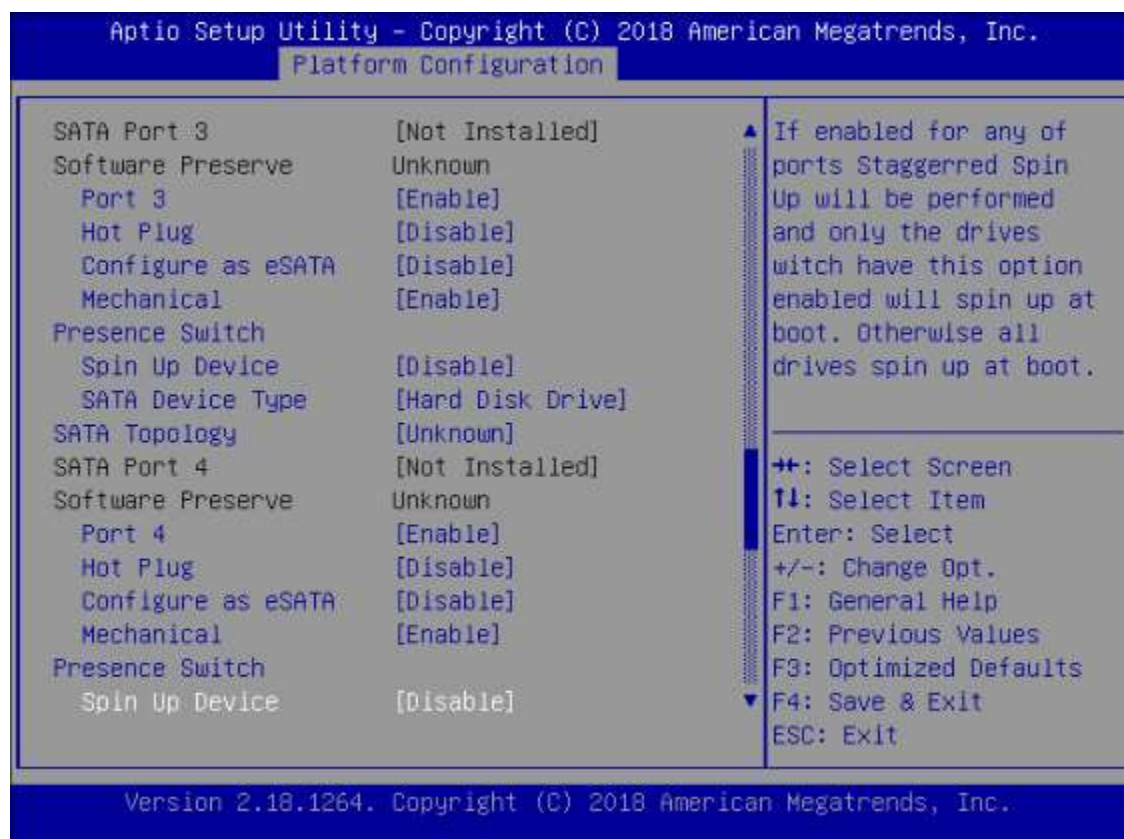
Item	Type	Options	Function description
PCI Express Root Port X (X=1~20)	Multipart item	<Disabled> <Enabled>*	Control the PCI Express Root Port.
PCIE ASPM	Multipart item	<Disable ASPM>* <ASPM L1> <Auto>	PCI Express Root port ASPM Setting
L1 Substates	Multipart item	<Disabled> <L1.1> <L1.2> <L1.1 & L1.2>*	PCI Express L1 Substates settings.
Gen3 Eq Phase3 Method	Multipart item	<Hardware> * <Static Coeff.> <Software Search>	PCIe Gen3 Equalization Phase 3 Method
ACS	Multipart item	<Disabled> <Enabled>*	Enable/Disable Access Control Services Extended Capability
URR	Multipart item	<Disabled>* <Enabled>	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Multipart item	<Disabled>* <Enabled>	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Multipart item	<Disabled>* <Enabled>	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Multipart item	<Disabled>* <Enabled>	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	Multipart item	<Disabled>* <Enabled>	Root PCI Express System Error on Fatal Error Enable/Disable.
SENF	Multipart item	<Disabled>* <Enabled>	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	Multipart item	<Disabled>* <Enabled>	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Numeric item	<Disabled>* <Enabled>	PCI Express PME SCI Enable/Disable.
Hot Plug	Multipart item	<Disabled>* <Enabled>	PCI Express Hot Plug Enable/Disable.
Advanced Error	Multipart	<Disabled>	Advanced Error Reporting

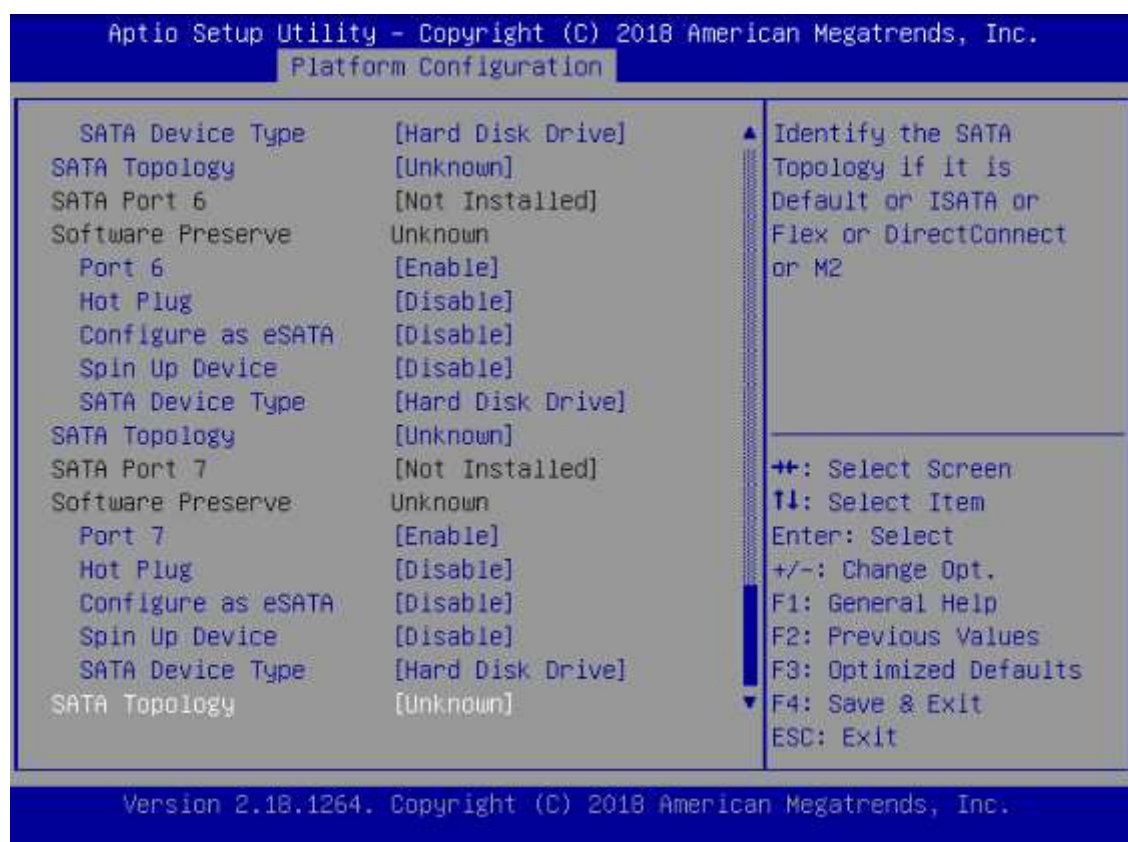
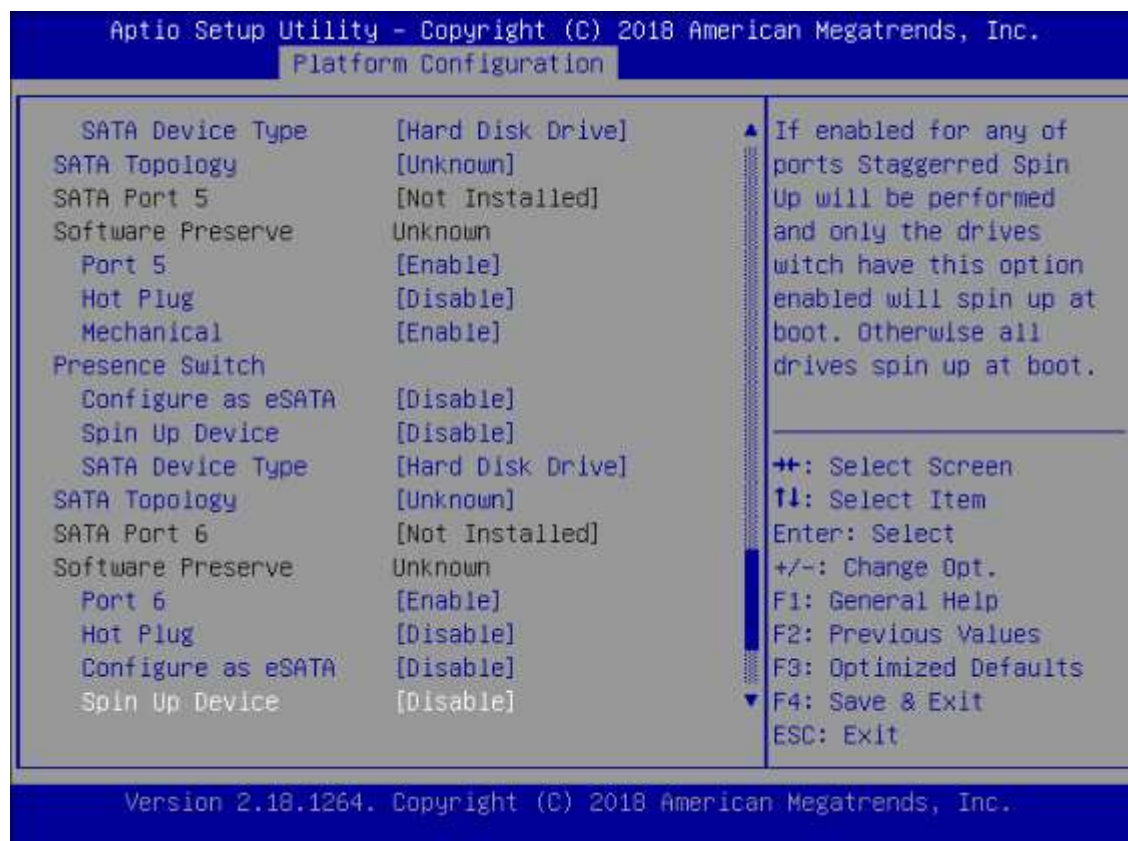
Reporting	item	<Enabled>*	Enable/Disable.
PCIe Speed	Multipart item	<Auto>* <Gen1> <Gen2> <Gen3>	Configure PCIe Speed
MSI	Multipart item	<Disabled> <Enabled>*	PCIE MSI Enable/Disable.
PCIE Lane Topology	Multipart item	<Unknown>* <x1> <x4> <Sata Express> <M2>	Identify the PCIE Lane Topology if it is x1 or x4 or SATA Express or M2
Max Payload Size	Multipart item	<MPL 128B>* <MPL 256B>	PCIE Max Payload Size Selection.
Compl. Timeout	Numeric item	<40-50ms(spec 50us-50ms)>* <40-50ms(spec 16ms-55ms)> <160-170ms(spec 65ms-210ms)> <400-500ms(spec 260ms-900ms)> <1.6-1.7s(spec 1s-3.5s)> <Disable>	PCI Express Root Port Completion Timer TO settings
Current speed for this RP is:	Static text	N/A	Unknown

Current width for this RP is:	Static text	N/A	Unknown
PCH PCIe LTR Configuration	Static text	N/A	
PCH PCIe1 LTR	Multipart item	<Disabled> <Enabled>*	PCH PCIe Latency Reporting Enable/Disable
Snoop Latency Override	Multipart item	<Disabled>* <Manual> <Auto>	Snoop Latency Override for PCH PCIe. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Multipart item		Non Snoop Latency Override for PCH PCIe. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
PCIe1 LTR Lock	Multipart item	<Disabled>* <Enabled>	PCIe LTR Configuration Lock

4.4.1.3 PCH SATA Configuration







Item	Type	Options	Function description
PCH SATA Configuration	Static text	N/A	
SATA Controller	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Controller
Configure SATA as	Multipart item	<AHCI>* <RAID>	This will configure SATA as IDE ,RAID or AHCI.
SATA test mode	Multipart item	<Enable> <Disable>*	Enable/Disable SATA test mode
SATA Mode options	Submenu	N/A	SATA mode related options
Support Aggressive Link Power Management	Multipart item	<Disable> <Enable>*	Enables/Disables SALP
NVRAM CYCLE ROUTER 0 ENABLE	Multipart item	<Disable>* <Enable>	Enable/disable cycle router X for NVRAM Remapping engine (X = 0~2)
NVRAM CRO PCIE Root Port Number	Multipart item	<PCI Express Root Port 1>* <PCI Express Root Port 2> <PCI Express Root Port 3> <PCI Express Root Port 4> <PCI Express Root Port 5> <PCI Express Root Port 6> <PCI Express Root Port 7> <PCI Express Root Port 8> <PCI Express Root Port 9> <PCI Express Root Port 10> <PCI Express Root Port 11> <PCI Express Root Port 12> <PCI Express Root Port 13> <PCI Express Root Port 14> <PCI Express Root Port 15> <PCI Express Root Port 16> <PCI Express Root Port 17> <PCI Express Root Port 18>	Choose one of the RootPorts which will be enabled for Cycle Router 0 for NVRAM engine

		<PCI Express Root Port 19> <PCI Express Root Port 20> <None PCI Express Root Port>	
NVRAM CYCLE ROUTER 1 ENABLE	Multipart item	<Disable>* <Enable>	Enable/disable cycle router 1 for NVRAM Remapping engine
NVRAM CR1 PCIE Root Port Number	Multipart item	<PCI Express Root Port 1>* <PCI Express Root Port 2> <PCI Express Root Port 3> <PCI Express Root Port 4> <PCI Express Root Port 5> <PCI Express Root Port 6> <PCI Express Root Port 7> <PCI Express Root Port 8> <PCI Express Root Port 9> <PCI Express Root Port 10> <PCI Express Root Port 11> <PCI Express Root Port 12> <PCI Express Root Port 13> <PCI Express Root Port 14> <PCI Express Root Port 15> <PCI Express Root Port 16> <PCI Express Root Port 17> <PCI Express Root Port 18> <PCI Express Root Port 19> <PCI Express Root Port 20> <None PCI Express Root Port>	Choose one of the RootPorts which will be enabled for Cycle Router 1 for NVRAM engine
NVRAM CYCLE ROUTER 2 ENABLE	Multipart item	<Disable>* <Enable>	Enable/disable cycle router 2 for NVRAM Remapping engine
NVRAM CR2 PCIE Root Port Number	Multipart item	<PCI Express Root Port 1>* <PCI Express Root Port 2> <PCI Express Root Port 3> <PCI Express Root Port 4> <PCI Express Root Port 5> <PCI Express Root Port 6> <PCI Express Root Port 7>	Choose one of the RootPorts which will be enabled for Cycle Router 2 for NVRAM engine

		<PCI Express Root Port 8> <PCI Express Root Port 9> <PCI Express Root Port 10> <PCI Express Root Port 11> <PCI Express Root Port 12> <PCI Express Root Port 13> <PCI Express Root Port 14> <PCI Express Root Port 15> <PCI Express Root Port 16> <PCI Express Root Port 17> <PCI Express Root Port 18> <PCI Express Root Port 19> <PCI Express Root Port 20> <None PCI Express Root Port>	
SATA Port 0	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 0	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State

			Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 1	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 1	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 2	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown

Port 2	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 3	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 3	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch.

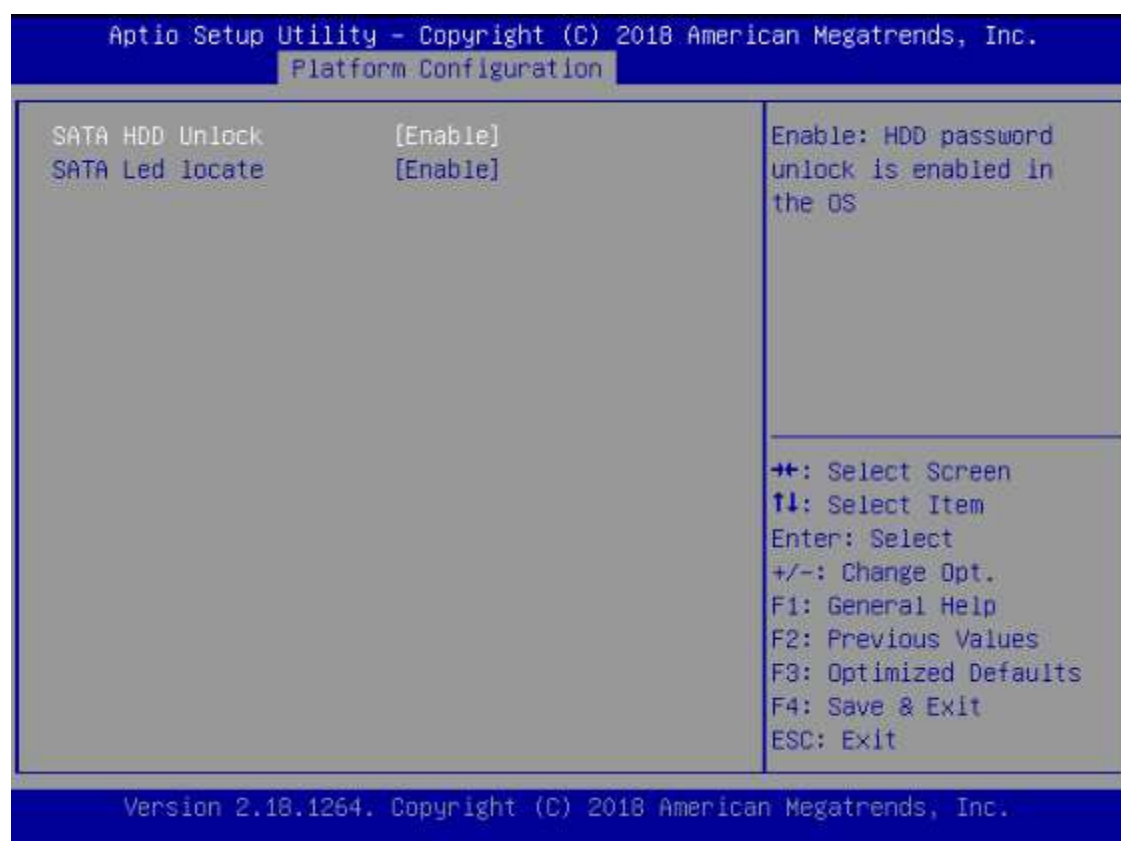
			Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 4	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 4	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all

			drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 5	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 5	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2

SATA Port 6	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 6	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 7	Static text	N/A	[Not Installed]
Software Preserve	Static text	N/A	Unknown
Port 7	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)

Mechanical Presence Switch	Multipart item	<Disable> <Enable>*	Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support.
Spin Up Device	Multipart item	<Disable>* <Enable>	If enabled for any of ports Staggered Spin Up will be performed and only the drives witch have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2

4.4.1.3.1 SATA Mode options



Item	Type	Options	Function description
SATA HDD Unlock	Multipart item	<Disable> <Enable>*	Enable: HDD password unlock is enabled in the OS
SATA Led locate	Multipart item	<Disable> <Enable>*	If enabled LED/SGPIO hardware is attached

4.4.1.4 PCH sSATA Configuration

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

Platform Configuration

PCH sSATA Configuration

sSATA Controller [Enable]

Configure sSATA as [AHCI]

SATA test mode [Disable]

► SATA Mode options

Support Aggressive [Enable]

Link Power Management

sSATA Port 0 [Not Installed]

Port 0 [Enable]

Hot Plug [Disable]

Configure as eSATA [Disable]

Spin Up Device [Disable]

sSATA Device Type [Hard Disk Drive]

SATA Topology [Unknown]

▲ Enable or Disable SATA Controller

++: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous Values

F3: Optimized Defaults

▼ F4: Save & Exit

ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Platform Configuration

sSATA Port 1 [Not Installed]

Port 1 [Enable]

Hot Plug [Disable]

Configure as eSATA [Disable]

Spin Up Device [Disable]

sSATA Device Type [Hard Disk Drive]

SATA Topology [Unknown]

sSATA Port 2 [Not Installed]

Port 2 [Enable]

Hot Plug [Disable]

Configure as eSATA [Disable]

Spin Up Device [Disable]

sSATA Device Type [Hard Disk Drive]

SATA Topology [Unknown]

sSATA Port 3 [Not Installed]

Port 3 [Enable]

Hot Plug [Disable]

Configure as eSATA [Disable]

▲ Configures port as External SATA (eSATA)

++: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

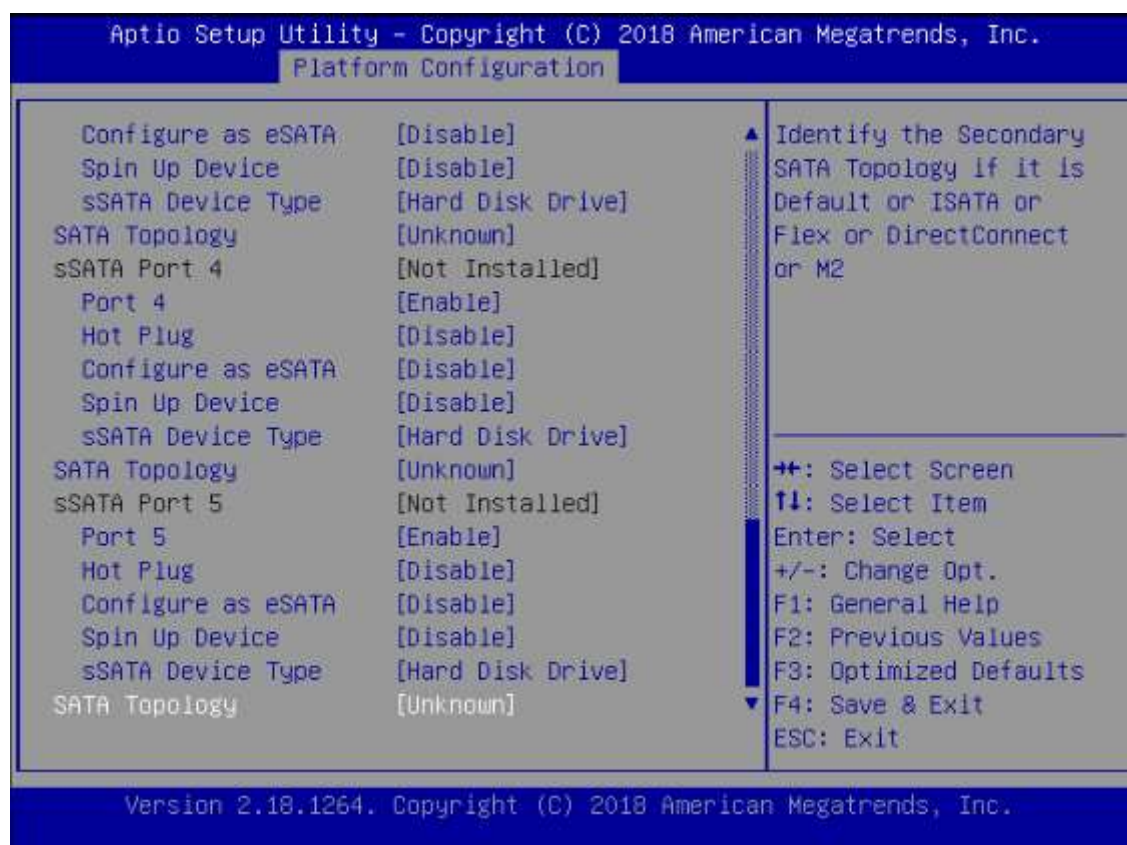
F2: Previous Values

F3: Optimized Defaults

▼ F4: Save & Exit

ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.



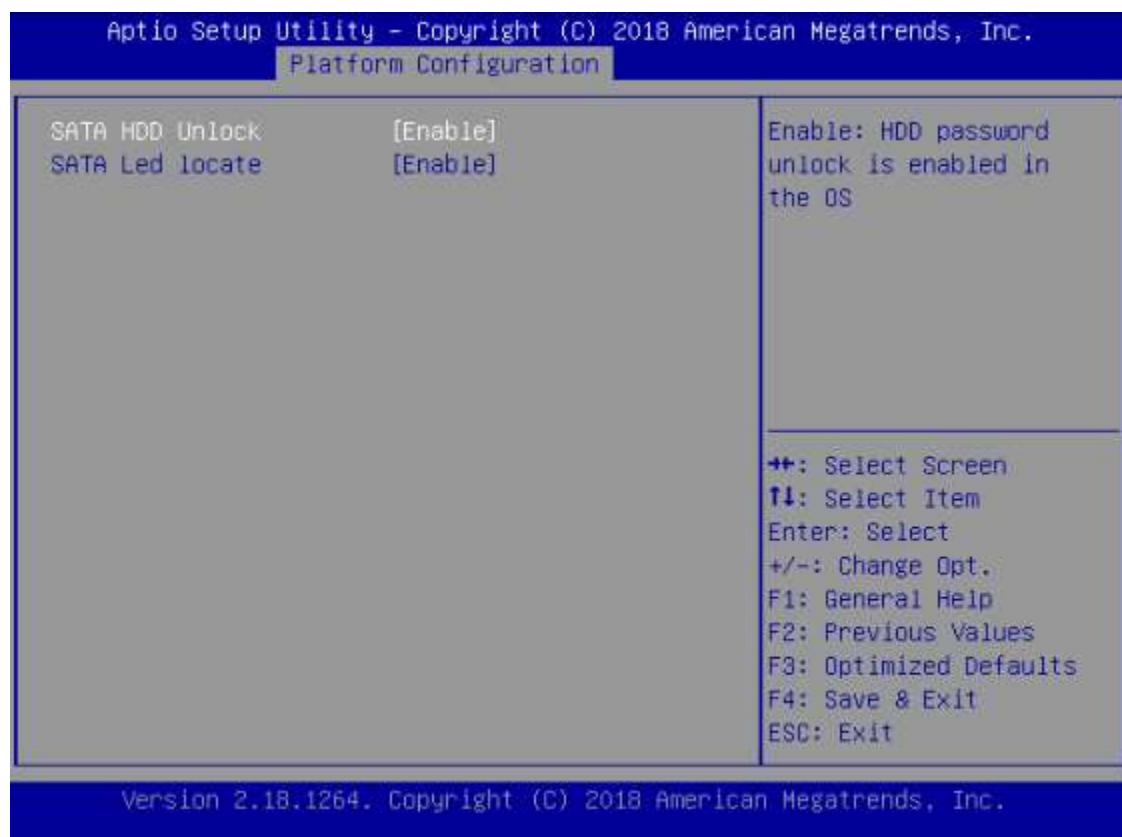
Item	Type	Options	Function description
PCH sSATA Configuration	Static text	N/A	
sSATA Controller	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Controller
Configure sSATA as	Multipart item	<AHCI>* <RAID>	This will configure sSATA as IDE ,RAID or AHCI.
SATA test mode	Multipart item	<Enable> <Disable>*	Enable/Disable SATA test mode
SATA Mode options	Submenu	N/A	SATA mode related options
Support Aggressive Link Power Management	Multipart item	<Disable> <Enable>*	Enables/Disables SALP
sSATA Port 0	Static text	N/A	[Not Installed]
Port 0	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.

Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
sSATA Port 1	Static text	N/A	[Not Installed]
Port 1	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
sSATA Port 2	Static text	N/A	[Not Installed]
Port 2	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart	<Hard Disk	Identify the SATA port is

	item	Drive>* <Solid State Drive>	connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
sSATA Port 3	Static text	N/A	[Not Installed]
Port 3	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
sSATA Port 4	Static text	N/A	[Not Installed]
Port 4	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

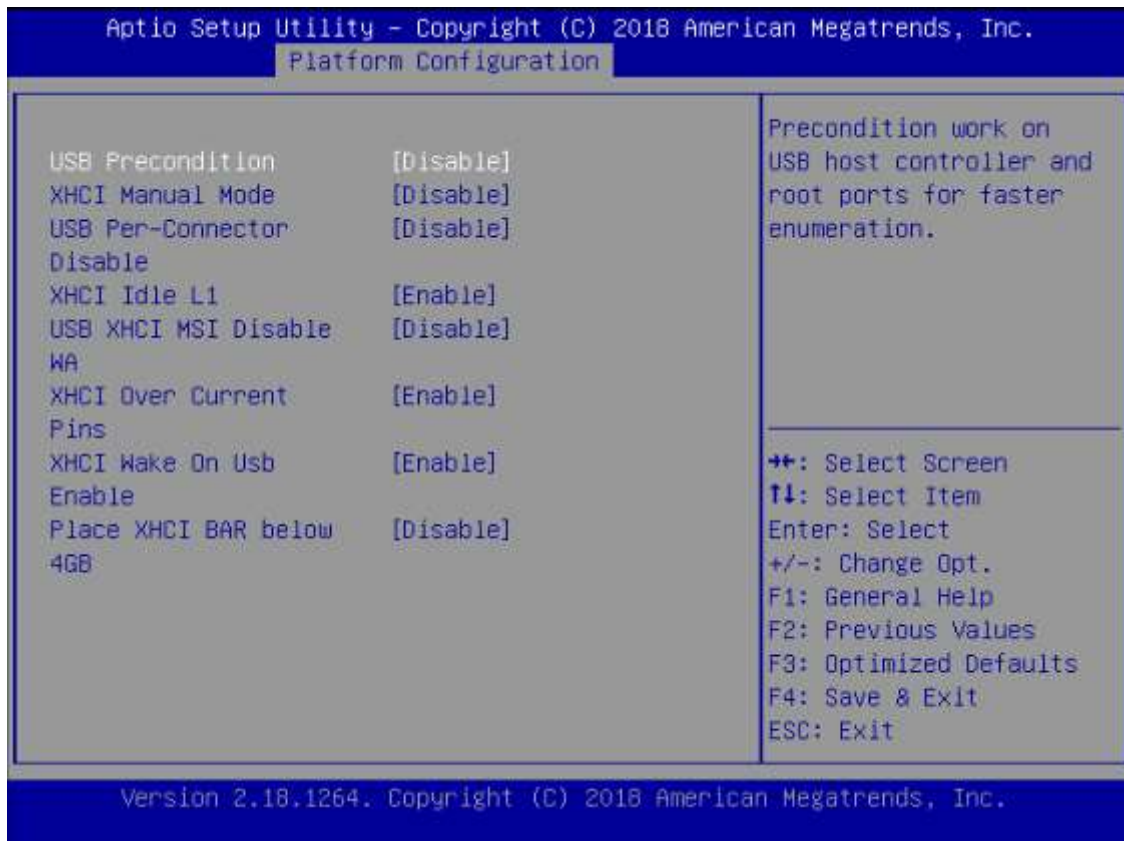
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
sSATA Port5	Static text	N/A	[Not Installed]
Port 5	Multipart item	<Disable> <Enable>*	Enable or Disable SATA Port
Hot Plug	Multipart item	<Disable>* <Enable>	Designates this port as Hot Pluggable.
Configure as eSATA	Multipart item	<Disable>* <Enable>	Configures port as External SATA (eSATA)
sSATA Device Type	Multipart item	<Hard Disk Drive>* <Solid State Drive>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA Topology	Multipart item	<Unknown>* <ISATA> <Direct Connect> <Flex> <M2>	Identify the Secondary SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2

4.4.1.4.1 SATA Mode options



Item	Type	Options	Function description
SATA HDD Unlock	Multipart item	<Disable> <Enable>*	Enable: HDD password unlock is enabled in the OS
SATA Led locate	Multipart item	<Disable> <Enable>*	If enabled LED/SGPIO hardware is attached

4.4.1.5 USB Configuration



Item	Type	Options	Function description
USB Precondition	Multipart item	<Disable>* <Enable>	Precondition work on USB host controller and root ports for faster enumeration.
XHCI Manual Mode	Multipart item	<Disable>* <Enable>	Use by validation, not for end-user.
USB Per-Connector Disable	Multipart item	<Disable>* <Enable>	Selectively Enable/Disable each of the USB Physical Connector (physical port). Once a connector is disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
XHCI Idle L1	Multipart item	<Disable> <Enable>*	Enabled XHCI Idle L1. Disabled to work around 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	Multipart item	<Disable>* <Enable>	Enable/Disable USB XHCI MSI Disable WA. ENABLE = hides MSI capability on XHCI
XHCI Over Current Pins	Multipart item	<Disable> <Enable>*	Enables/Disables support for XHCI Over Current Pin Mapping

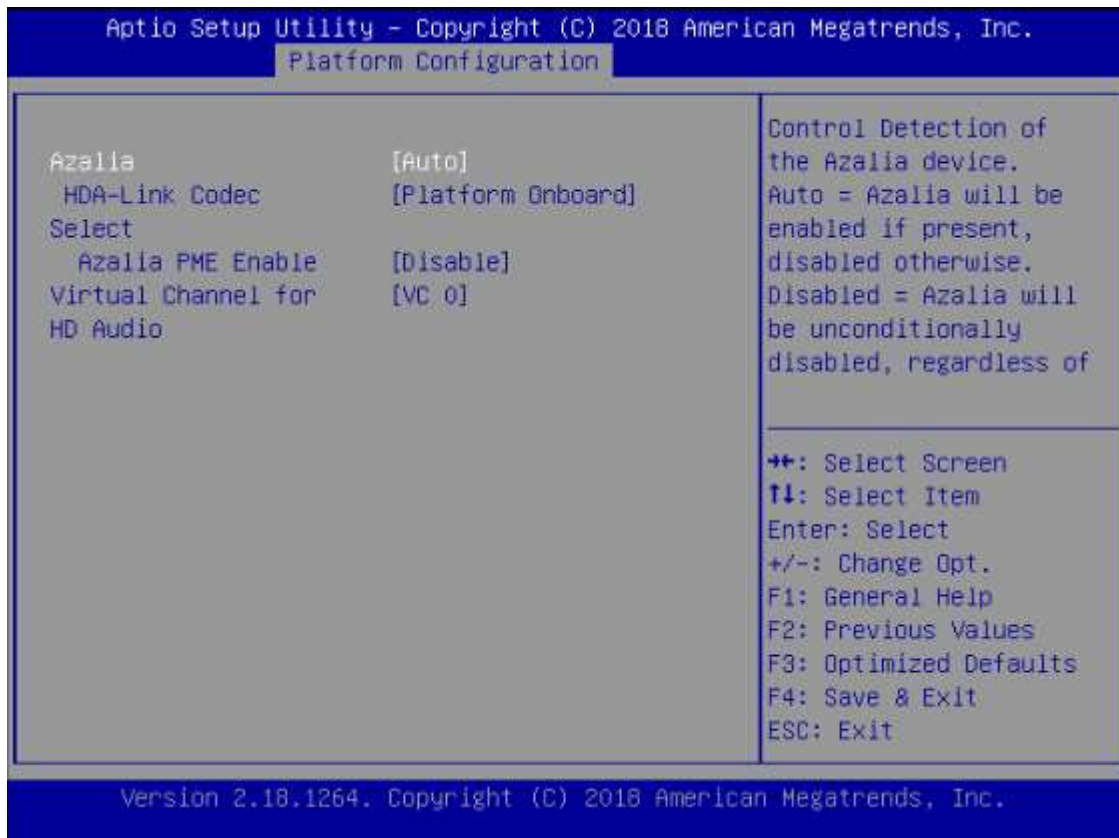
XHCI Wake On Usb Enable	Multipart item	<Disable> <Enable>*	Enables/Disables support for XHCI Wake on USB on connect/disconnect.
Place XHCI BAR below 4GB	Multipart item	<Disable>* <Enable>	Enable to work around WS2K12 KDUSB 64-bit BAR issue.

4.4.1.6 Security Configuration



Item	Type	Options	Function description
Security Configuration	Static text	N/A	Security Configuration settings
SMM BIOS Write Protect	Multipart item	<Disable> <Enable>*	Enable/Disable SMM BIOS Write-Protect feature

4.4.1.7 Azalia Configuration



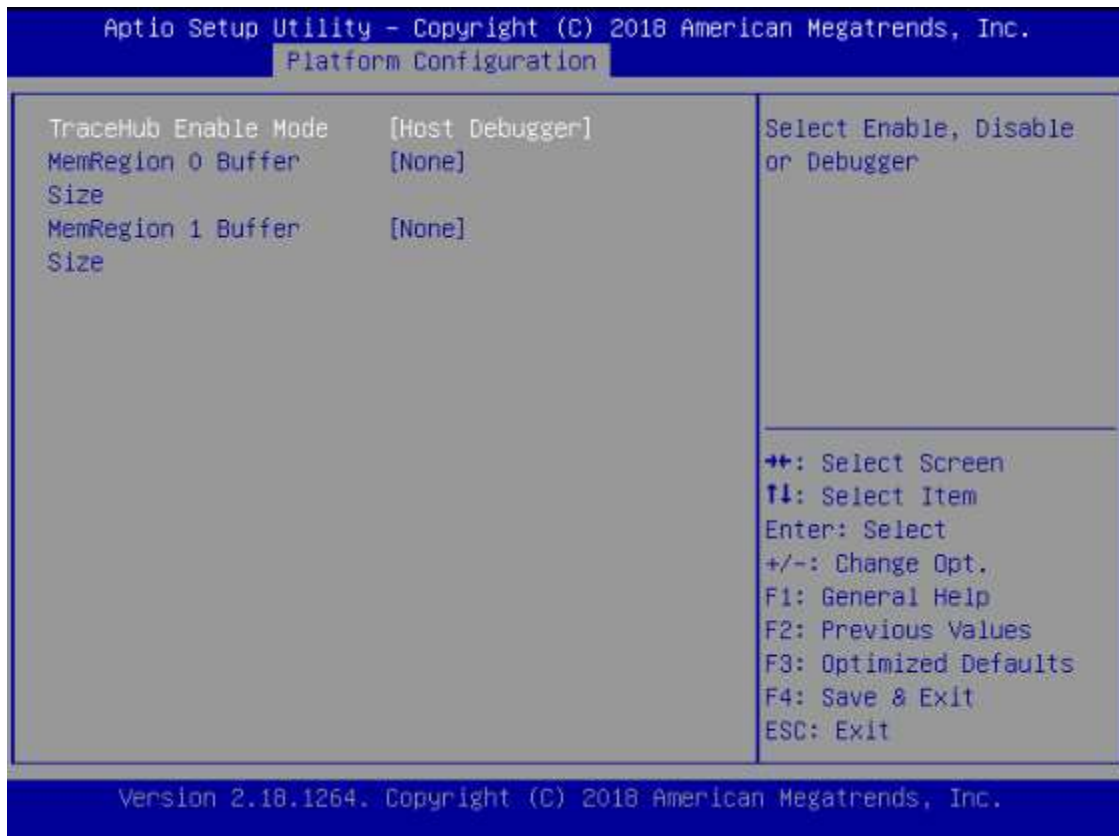
Item	Type	Options	Function description
Azalia	Multipart item	<Disable> <Enable> <Auto>*	Control Detection of the <u>Azalia</u> device. Auto = <u>Azalia</u> will be enabled if present, disabled otherwise. Disabled = <u>Azalia</u> will be unconditionally disabled, regardless of presence.
HDA-Link Codec Select	Multipart item	<Platform Onboard>* <External Kit>	Selects whether Platform Onboard Codec (single Verb Table installed) or External Codec Kit (multiple Verb Tables installed) will be used.
<u>Azalia</u> PME Enable	Multipart item	<Disable>* <Enable>	Enable/Disable PME for <u>Azalia</u> .
Virtual Channel for HD Audio	Multipart item	<VC 0>* <VC 1>	Virtual Channel assigned to Traffic Class of HD Audio controller

4.4.1.8 Platform Thermal Configuration



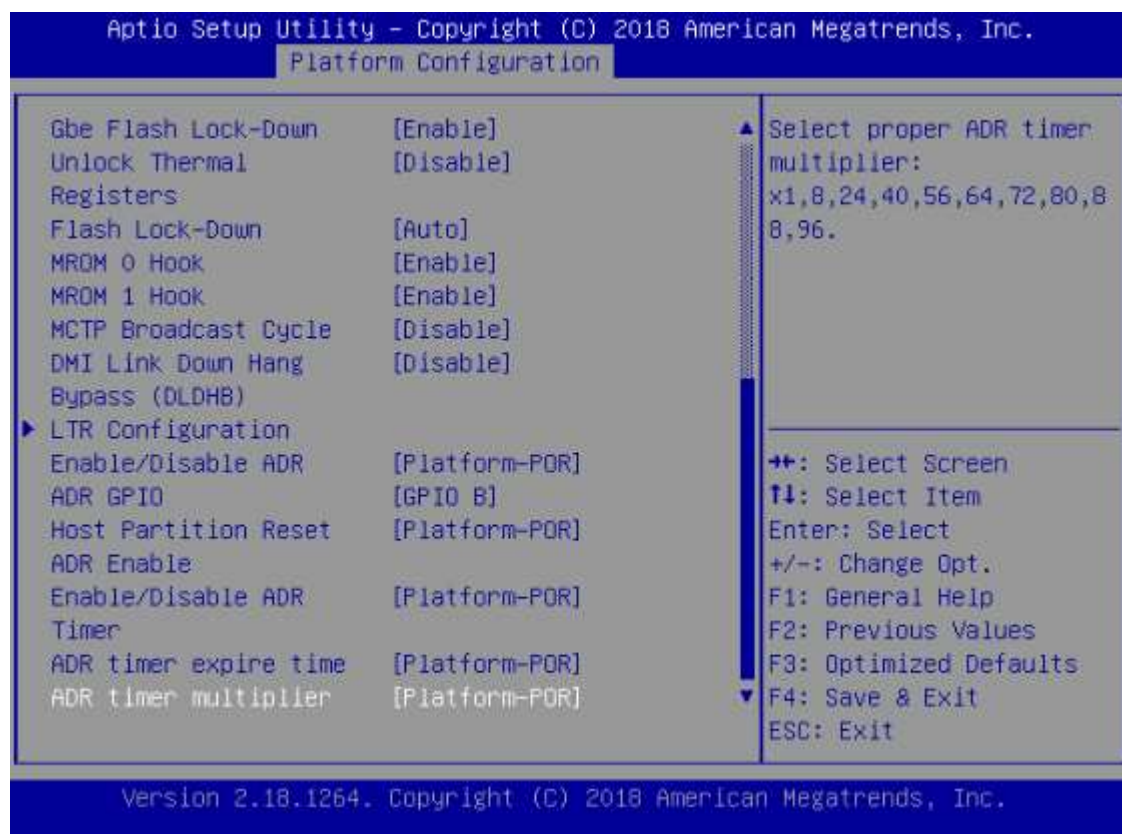
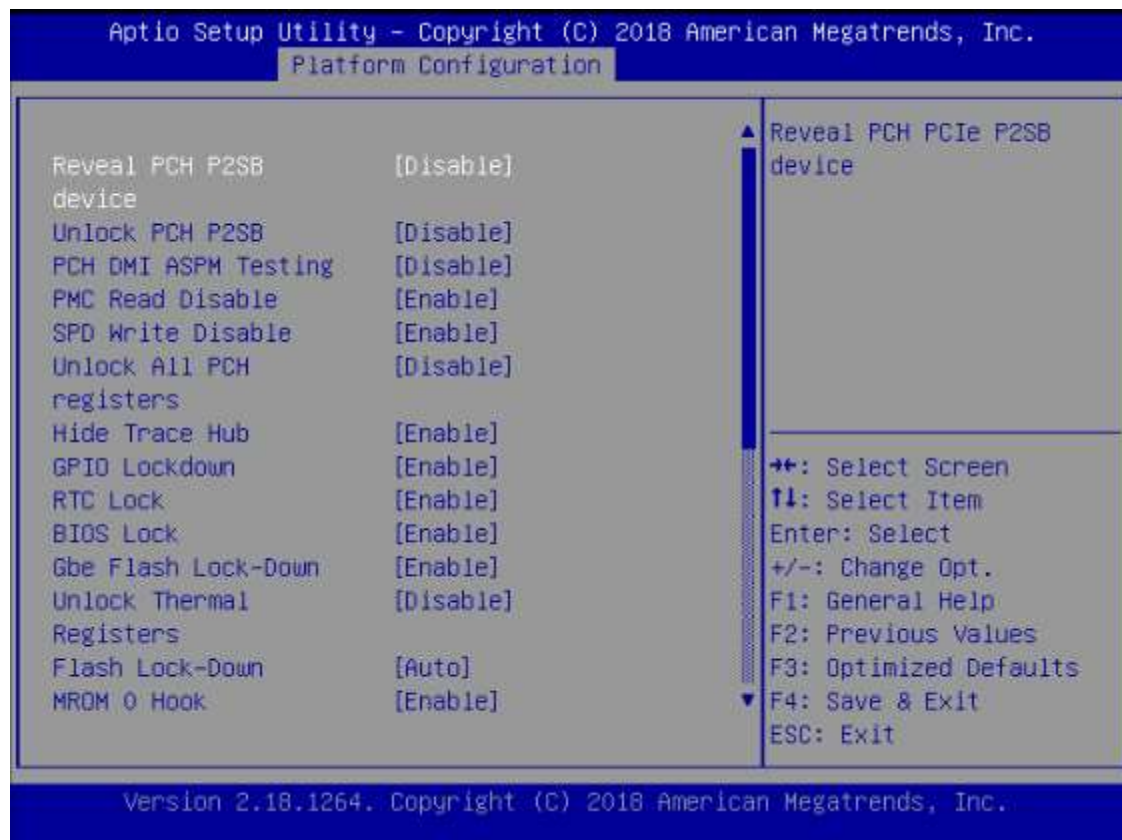
Item	Type	Options	Function description
PCH Thermal Device	Multipart item	<Disable> <Enabled in PCI mode> <Enabled in ACPI mode> <Auto>*	Enable/Disable PCH Thermal Device(D20:F2)

4.4.1.9 TraceHub Configuration



Item	Type	Options	Function description
TraceHub Enable Mode	Multipart item	<Disable> <Target Debugger> <Host Debugger> *	Select Enable, Disable or Debugger
MemRegion 0 Buffer Size	Multipart item	<None>* <1MB> <8MB> <64MB>	Select size of mem region 0 buffer
MemRegion 1 Buffer Size	Multipart item	<None>* <1MB> <8MB> <64MB>	Select size of mem region 1 buffer

4.4.1.10 PCH DFX Configuration



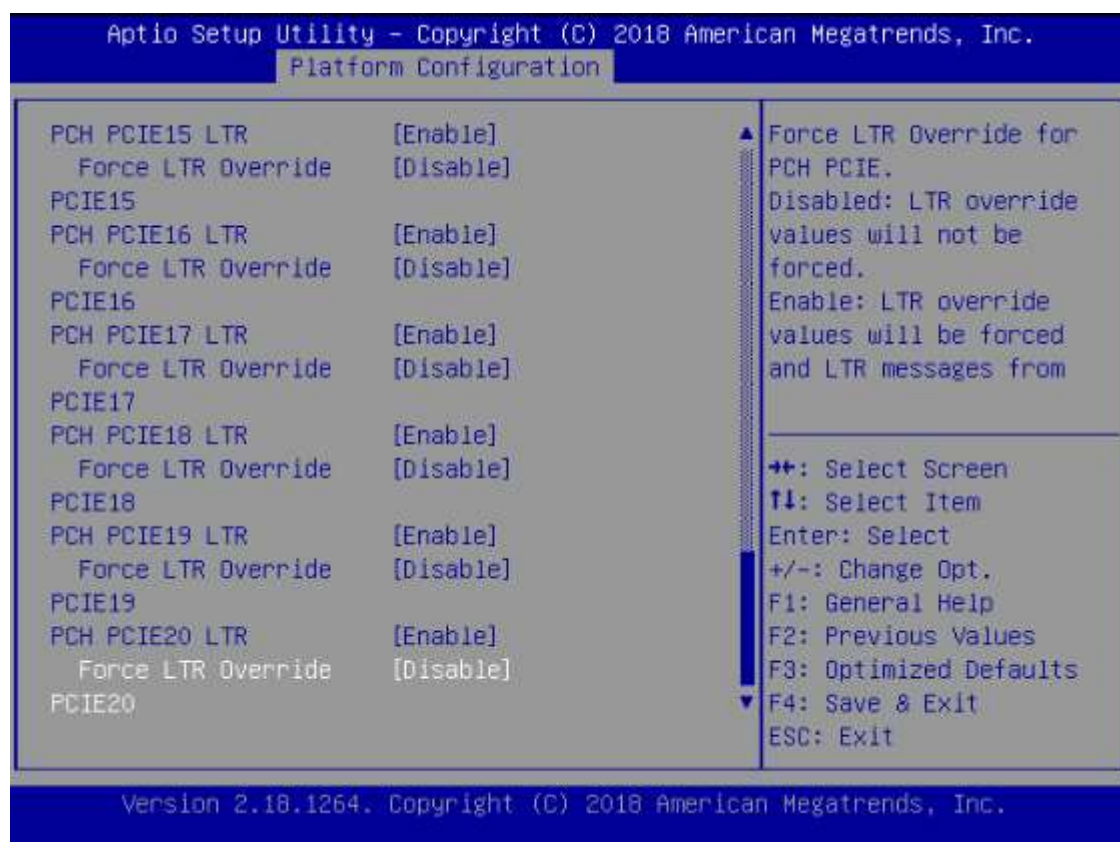
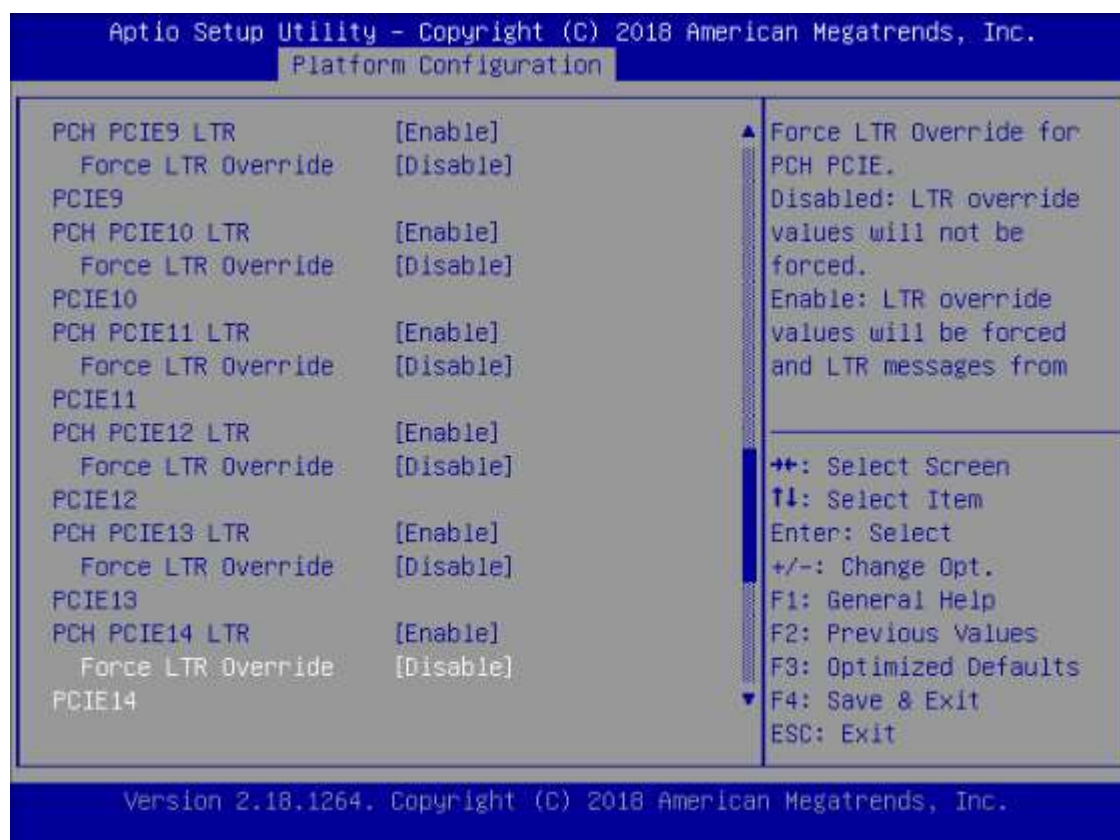
Item	Type	Options	Function description
Reveal PCH P2SB device	Multipart item	<Disable>* <Enable>	Reveal PCH PCIe P2SB device
Unlock PCH P2SB	Multipart item	<Disable>* <Enable>	Unlock PCH P2SB SBI and Configuration space by PSF
PCH DMI ASPM Testing	Multipart item	<Disable>* <ASPM L1>	Allow DMI enter to L1 besides PCIe Root Ports support
PMC Read Disable	Multipart item	<Disable> <Enable>*	Disables host to read to PMC XRAM
SPD Write Disable	Multipart item	<Disable> <Enable>*	Enable/Disable setting SPD Write Disable
Unlock All PCH registers	Multipart item	<Disable>* <Enable>	Unlocks all PCH RW-L and RW-KL registers
Hide Trace Hub	Multipart item	<Disable> <Enable>*	Hide Trace Hub
GPIO Lockdown	Multipart item	<Disable> <Enable>*	Locks configuration and/or state of vendor-defined set of GPIOs.
RTC Lock	Multipart item	<Disable> <Enable>*	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM
BIOS Lock	Multipart item	<Disable> <Enable>*	Enable/Disable the PCH BIOS Lock Enable feature.
Gbe Flash Lock-Down	Multipart item	<Disable> <Enable>*	Enable/Disable <u>Gbe</u> Flash Lock-Down
Unlock Thermal Registers	Multipart item	<Disable>* <Enable>	Do not lock all thermal related registers
Flash Lock-Down	Multipart item	<Auto>* <Disable> <Enable>	Enable/Disable Flash Lock-Down
MROM 0 Hook	Multipart item	<Disable> <Enable>*	Enables special handling of MROM OpROM for DFX.
MROM 1 Hook	Multipart item	<Disable> <Enable>*	Enables special handling of MROM 1 OpROM for DFX. For MROM 1 this option will also enable/disable the MROM 0 device.
MCTP Broadcast Cycle	Multipart item	<Disable>* <Enable>	Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner
DMI Link	Multipart	<Disable>*	Set DLDHB bit

Down Hang Bypass (DLDHB)	item	<Enable>	
LTR Configuration	Submenu	N/A	LTR Configuration Options
Enable/Disable ADR	Multipart item	<Platform-POR>* <Disable> <Enable>	Enable or disable Automatic DIMM Refresh (ADR)
ADR GPIO	Multipart item	<GPIO B>* <GPIO C>	Select between GPIO_B or GPIO_C.
Host Partition Reset ADR Enable	Multipart item	<Platform-POR>* <Disable> <Enable>	Enables/Disables ADR on Host Partition Reset
Enable/Disable ADR Timer	Multipart item	<Platform-POR>* <Disable> <Enable>	Held-off for DEBUG PURPOSES ONLY!
ADR timer expire time	Multipart item	<Platform-POR>* <25 uS> <50 uS> <100 uS> <0 uS>	Select proper ADR timer value: 25uS, 50uS, 100uS or 0.
ADR timer multiplier	Multipart item	<Platform-POR>* <x1> <x8> <x24> <x40> <x56> <x64> <x72> <x80> <x88> <x96>	Select proper ADR timer multiplier: x1,8,24,40,56,64,72,80,88,96.

4.4.1.10.1 LTR Configuration

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Platform Configuration	
PCH SATA LTR Configuration	
PCH SATA LTR	[Enable]
SATA LTR Override	[Disable]
SATA LTR Lock	[Enable]
PCH sSATA LTR Configuration	
PCH sSATA LTR	[Enable]
sSATA LTR Override	[Disable]
sSATA LTR Lock	[Enable]
CPU PCIe LTR Override	
PCH PCIE1 LTR	[Enable]
Force LTR Override	[Disable]
PCIE1	
PCH PCIE2 LTR	[Enable]
Force LTR Override	[Disable]
PCIE2	
▲ PCH SATA Latency Reporting Enable/Disable ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Platform Configuration	
PCH PCIE3 LTR	
Force LTR Override	[Disable]
PCIE3	
PCH PCIE4 LTR	
Force LTR Override	[Disable]
PCIE4	
PCH PCIE5 LTR	
Force LTR Override	[Disable]
PCIE5	
PCH PCIE6 LTR	
Force LTR Override	[Disable]
PCIE6	
PCH PCIE7 LTR	
Force LTR Override	[Disable]
PCIE7	
PCH PCIE8 LTR	
Force LTR Override	[Disable]
PCIE8	
▲ Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
PCH SATA LTR Configuration	Static text	N/A	
PCH SATA LTR	Multipart item	<Disable> <Enable>*	PCH SATA Latency Reporting Enable/Disable
SATA LTR Override	Multipart item	<Enable> <Disable>*	PCH SATA LTR Override Enable/Disable.
SATA LTR Lock	Multipart item	<Enable>* <Disable>	Enable/Disable SATA LTR lock.
PCH sSATA LTR Configuration	Static text	N/A	
PCH sSATA LTR	Multipart item	<Disable> <Enable>*	PCH sSATA Latency Reporting Enable/Disable
sSATA LTR Override	Multipart item	<Disable>* <Enable>	PCH sSATA LTR Override Enable/Disable.
sSATA LTR Lock	Multipart item	<Disable> <Enable>*	Enable/Disable sSATA LTR lock.
CPU PCIe LTR Override	Static text	N/A	
PCH PCIE1 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE1	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE2 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE2	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE3 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable

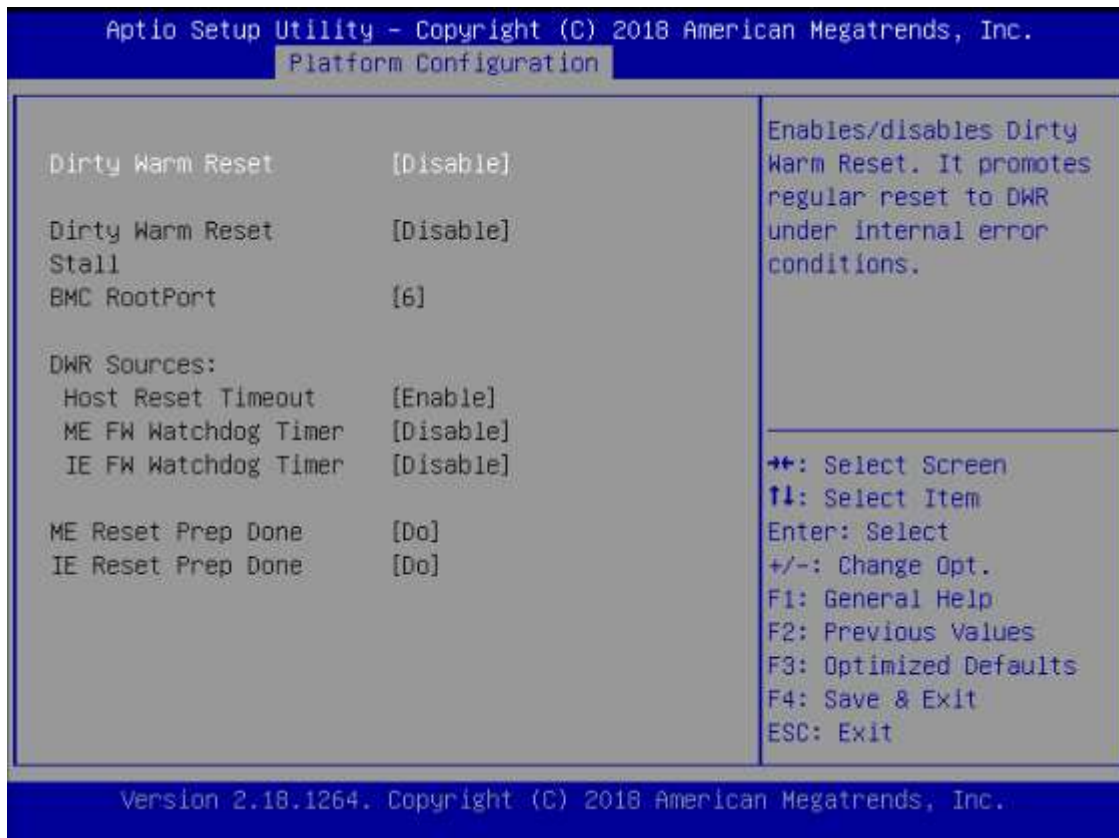
Force LTR Override PCIE3	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE4 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE4	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE5 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE5	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE6 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE6	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE7 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE7	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE8	Multipart	<Disable>	PCH PCIE Laten-UScy Reporting en-

LTR	item	<Enable>*	USable/Disable
Force LTR Override PCIE8	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE9 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE9	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE10 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE10	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE11 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE11	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE12 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE12	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.

PCH PCIE13 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE13	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE14 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE14	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE15 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE15	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE16 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE16	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE17 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE17	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be

			ignored.
PCH PCIE18 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE18	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE19 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE19	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
PCH PCIE20 LTR	Multipart item	<Disable> <Enable>*	PCH PCIE Laten-UScy Reporting en-USable/Disable
Force LTR Override PCIE20	Multipart item	<Disable>* <Enable>	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.

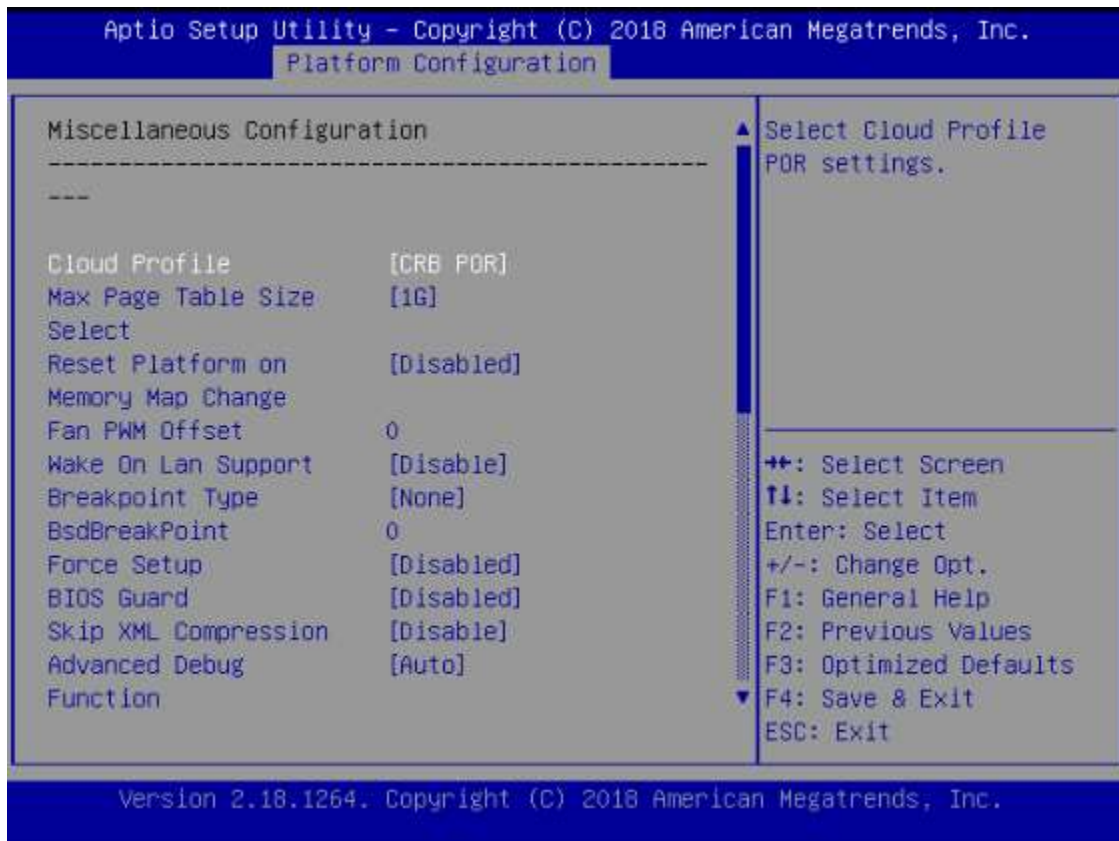
4.4.1.11 PCH DWR Configuration



Item	Type	Options	Function description
Dirty Warm Reset	Multipart item	<Disable>* <Enable>	Enables/disables Dirty Warm Reset. It promotes regular reset to DWR under internal error conditions.
Dirty Warm Reset Stall	Multipart item	<Disable>* <Enable>	When enabled, system will enter spin loop during dirty warm reset allowing manual error collection
BMC RootPort	Multipart item	<6>* <12 >	RootPort that BMC is connected to
DWR Sources:	Static text	N/A	
Host Reset Timeout	Multipart item	<Disable> <Enable>*	Global to Host reset promotion on PMC FW-Initiated Host Reset Timeout
ME FW Watchdog Timer	Multipart item	<Disable>* <Enable>	Global to Host reset promotion on ME FW Watchdog Timer
IE FW Watchdog Timer	Multipart item	<Disable>* <Enable>	Global to Host reset promotion on IE FW Watchdog Timer

ME Reset Prep Done	Multipart item	<Skip> <Do>*	ME Reset Prep Done (ETR3 bit 17)
IE Reset Prep Done	Multipart item	<Skip> <Do>*	IE Reset Prep Done (ETR3 bit 16)

4.4.2 Miscellaneous Configuration



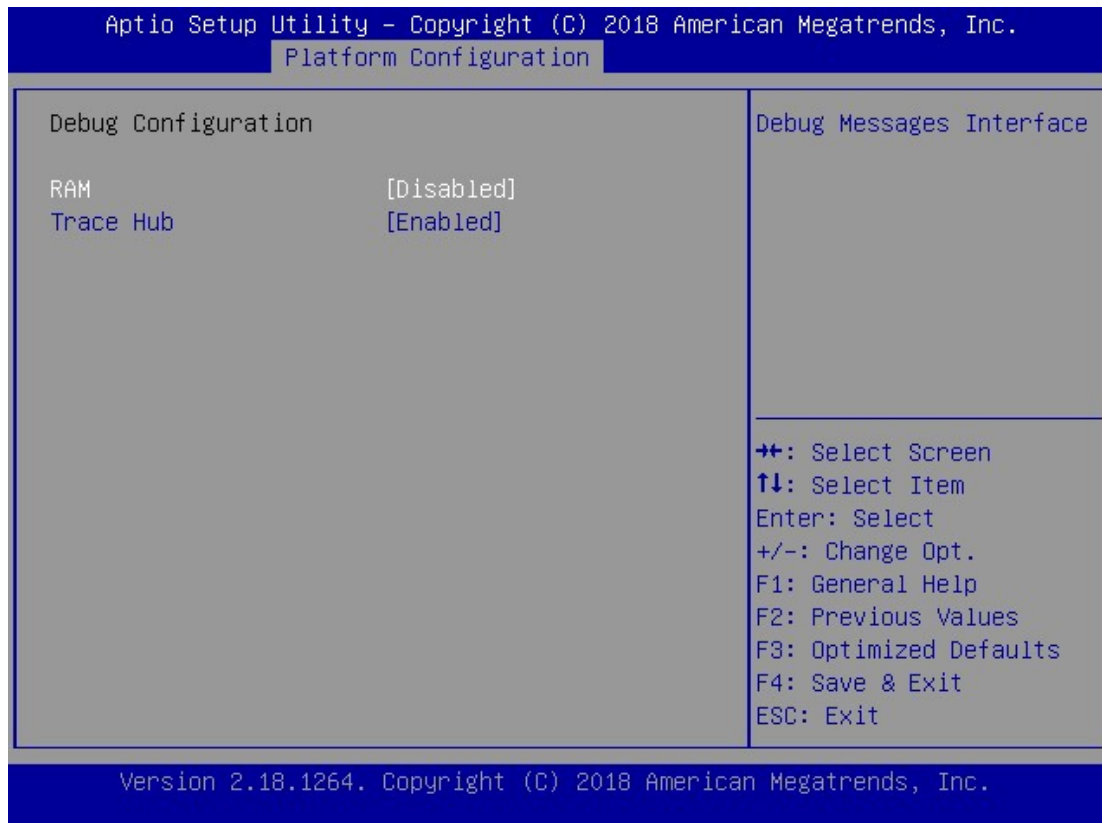


Item	Type	Options	Function description
Miscellaneous Configuration	Static text	N/A	
Cloud Profile	Multipart item	<CRB POR>* <Cloud Profile 1 POR>	Select Cloud Profile POR settings.
Max Page Table Size Select	Multipart item	<2M>* <1G>*	Select the max page size to use. If 1G size is used, it may cause problems with older OSes."
Reset Platform on Memory Map Change	Multipart item	<Disabled>* <Enabled>	Causes a platform reset if the memory map has changed. Required for S4 resume to function at first boot.
Fan PWM Offset	Numeric item	0*~100	Valid Offset 0-100. This number is added to the calculated PWM value to increase Fan Speed
Wake On Lan Support	Multipart item	<Disable>* <Enable>	Enable or Disable Wake On Lan Support
Breakpoint	Multipart	<None>*	Halt at specified points in BIOS

Type	item	<After MRC> <After QPIRC> <After Resource Allocation> <After POST> <After Full Speed Setup> <Ready for IBIST>	
BsdBreakPoint	Numeric item	0*~0xFFFF	Create initial stallpoint 0 - 0xFFFF
Force Setup	Multipart item	<Disabled>* <Enabled>	Enable/Disable loading setup without pressing F2
BIOS Guard	Multipart item	<Disabled>* <Enabled>	Enable/Disable BIOS Guard Platform Protection Technology
Skip XML Compression	Multipart item	<Disable>* <Enable>	If enabled the XML Compression will be skipped
Advanced Debug Function	Multipart item	<Auto>* <Disable> <Enable>	Advanced Debug Function (Dfx Knob)
Additional Post Codes	Multipart item	<Disable>* <Enable>	Enables or Disables Additional Post Codes
Debug Configuration	Submenu	N/A	Debug Message Settings
Serial Debug Message Level	Multipart item	<Disable>* <Minimum> <Normal> <Maximum> <Auto>	Disable = no messages, Minimum = critical messages, Normal = critical & informational messages, Maximum = all messages, Auto = Minimum (default) or Normal (Advanced Debug mode)
Trace Messages	Multipart item	<Disable>* <Enable> <Enabled for registry writes only.>	Enables display of every IO access
Training Messages	Multipart item	<Disable>* <Enable>	Enabled = set to display the training results. Training results also get

			displayed if debug messages is set to Maximum.
Active Video	Multipart item	<Auto>* <Onboard> <PCIE Device>	Select active Video type
PMTT ACPI Table	Multipart item	<Disable>* <Enable>	Enable/Disable PMTT ACPI Table for DDR4 only
PS2 Port Swap	Multipart item	<Disable>* <Enable>	Enables or Disables the PS2 port swap
NumLock	Multipart item	<Disable>* <Enable>	Enables or Disables NumLock
Wake On Lan from S5	Multipart item	<Disable>* <Enable>	Enables or Disables Wake on Lan from S5
Boot to Network	Multipart item	<Disable>* <Enable>	Enables or Disables Boot to Network.
ARI Forwarding	Multipart item	<Disable> <Enable>*	Enable or disable the ARI Forwarding
ARI Forward	Multipart item	<Disable>* <Enable>	Enable or disable the ARI Forward
RTC Wake system from S4/S5	Multipart item	<Disable>* <Enable>	Enable or disable System wake on alarm event. When enabled, System will wake on the day::hr::min::sec specified
Firmware Configuration	Multipart item	<Production>* <Debug>	Firmware Configuration options

4.4.2.1 Debug Configuration



Item	Type	Options	Function description
Debug Configuration	Static text	N/A	
RAM	Multipart item	<Disabled>* <Enabled>	Debug Messages Interface
Trace Hub	Multipart item	<Disabled> <Enabled>*	Debug Messages Interface

4.4.3 Server ME Configuration

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

Platform Configuration

General ME Configuration		▲ The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Oper. Firmware Version	0A:4.0.4.313	
Backup Firmware Version	N/A	
Recovery Firmware Version	0A:4.0.4.313	
ME Firmware Status #1	0x000F0245	
ME Firmware Status #2	0x88116826	
ME ODM Revision	C439000A	
Current State	Operational	
Error Code	No Error	
Recovery Cause	N/A	
PTT Support	[Disable]	
Altitude	12c	
MCTP Bus Owner	0	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

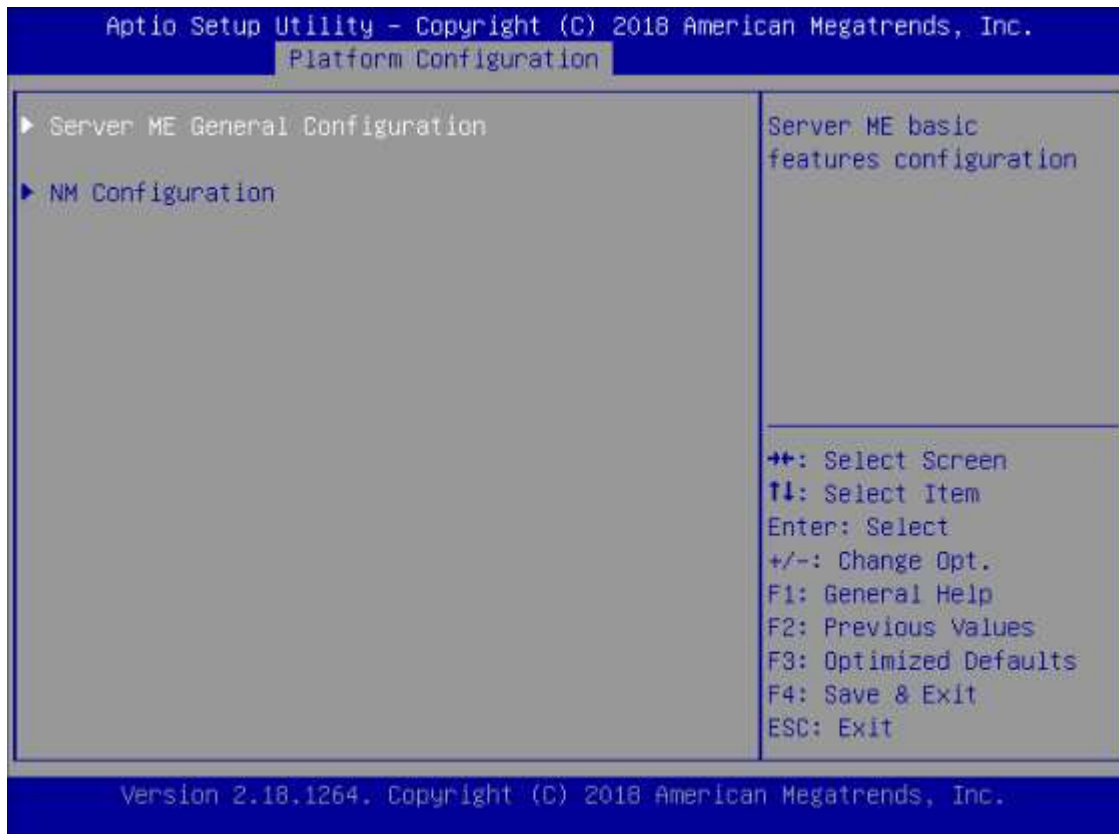
Platform Configuration

ME Firmware Status #1	0x000F0245	▲ MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled. ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
ME Firmware Status #2	0x88116826	
ME ODM Revision	C439000A	
Current State	Operational	
Error Code	No Error	
Recovery Cause	N/A	
PTT Support	[Disable]	
Altitude	12c	
MCTP Bus Owner	0	
ME Firmware Features	SiEn+NM+ICC+MeStorageServices+BootGuard+CpuHotPlug+ThermalReport+HSIO+PECIOverDMI+PCHDebug+PowerThermalUtility+PCHThermalSensorInit+DeepSx+DirectMeUpdate+CUPS+TurboStateLimiting+TelemetryHub	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

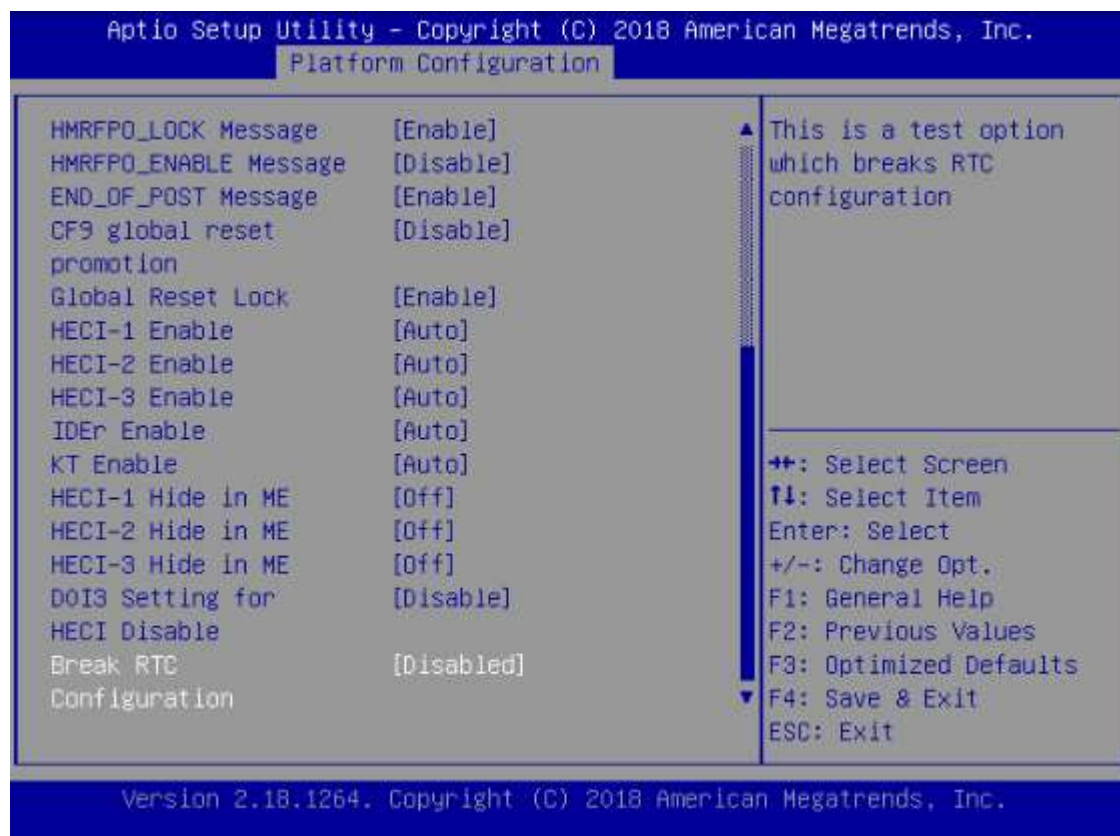
Item	Type	Options	Function description
General ME Configuration	Static text	N/A	
<u>Oper.</u> Firmware Version	Dynamic text		Version of operational firmware selected to run.
Backup Firmware Version	Dynamic text		Version of backup operational firmware if present (optional).
Recovery Firmware Version	Dynamic text		Version of recovery firmware - runs when ME is in recovery mode.
ME Firmware Status #1	Dynamic text		ME Firmware Status #1 register in HECI-1 configuration space.
ME Firmware Status #2	Dynamic text		ME Firmware Status #2 register in HECI-1 configuration space.
ME ODM Revision	Dynamic text		Get ME ODM Revision
Current State	Dynamic text		ME firmware Current State, bits [3:0] in MEFS1.
Error Code	Dynamic text		ME firmware Error Code, bits [15:12] in MEFS1.
Recovery Cause	Dynamic text		Server ME firmware recovery cause, bits [10:8] in MEFS2.
PTT Support	Dynamic text		Enable/disable Platform Trusted Technology (PTT) support
Altitude	Numeric item	0~0xFFFF [0x12c]*	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 8000h value if the altitude is unknown.
MCTP Bus Owner	Numeric item	0*~0xFFFF	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.
ME Firmware Features	Dynamic text		Server ME firmware features list.

4.4.4 Server ME Debug Configuration



Item	Type	Options	Function description
Server ME General Configuration	Submenu	N/A	Server ME basic features configuration
NM Configuration	Submenu	N/A	Options to configure NM features

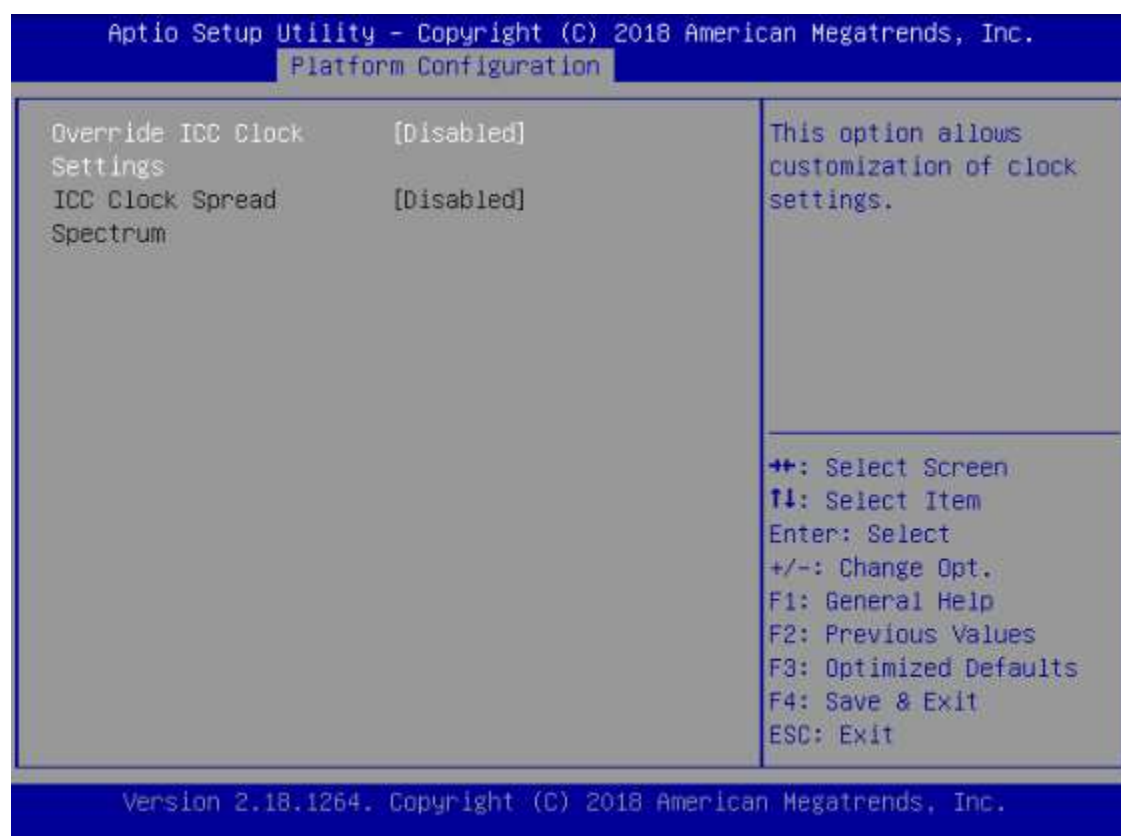
4.4.4.1 Server ME General Configuration



Item	Type	Options	Function description
ME Initialization Complete Timeout	Numeric item	0~12 [2]*	This option defines how long BIOS waits for ME to initialize.
Enable HSIO Messaging	Multipart item	<Disable> <Enable>*	Enable/Disable HSIO messaging
DRAM Init Done Enable	Multipart item	<Disabled> <Enabled>*	Enable/Disable notifying ME about DRAM initialization. (It Enables/Disables UMA functionality.)
DRAM Initialization Status	Multipart item	<Auto - true status>* <0 - Success> <1 - No Memory in Channels> <2 - Memory Init Error>	Override the DRAM initialization status value.
Host Reset Warning	Multipart item	<Disabled> <Enabled>*	Enable/Disable sending Host Reset Warning to ME
<u>Pre</u> -DramInitDone ME Reset	Multipart item	<Disabled>* <Enabled>	When ME is in recovery because of internal error try to reset it.
Override ICC Clock Settings	Submenu	N/A	Override the default ICC Set Clock Settings.
HMRFPPO_LOCK Message	Multipart item	<Disable> <Enable>*	Enable/Disable sending HMRFPPO_LOCK message to ME
HMRFPPO_ENABLE Message	Multipart item	<Disable>* <Enable>	Enable/Disable sending HMRFPPO_ENABLE message to ME
END_OF_POST Message	Multipart item	<Disable> <Enable>*	Enable/Disable sending END_OF_POST message to ME
CF9 global reset promotion	Multipart item	<Disable>* <Enable>	Enable/Disable promoting CF9 reset to global
Global Reset Lock	Multipart item	<Disable> <Enable>*	Enable/Disable locking the joint ME and host reset capability
HECI-1 Enable	Multipart	<Disable>	Override HECI-1 status on PCI, or let

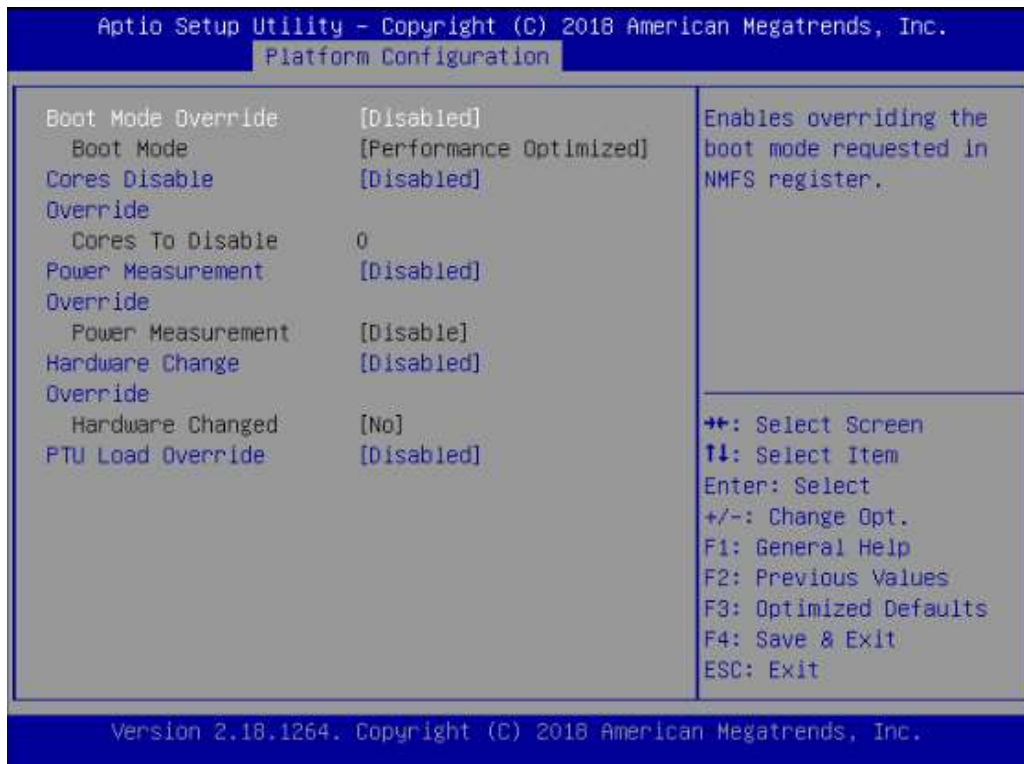
	item	<Enable> <Auto>*	firmware decide based on ME type (auto)
HECI-2 Enable	Multipart item	<Disable> <Enable> <Auto>*	Override HECI-2 status on PCI, or let firmware decide based on ME type (auto)
HECI-3 Enable	Multipart item	<Disable> <Enable> <Auto>*	Override HECI-3 status on PCI, or let firmware decide based on ME type (auto)
IDEr Enable	Multipart item	<Disable> <Enable> <Auto>*	Override IDEr status on PCI, or let firmware decide based on ME type (auto)
KT Enable	Multipart item	<Disable> <Enable> <Auto>*	Override KT status on PCI, or let firmware decide based on ME type (auto)
HECI-1 Hide in ME	Multipart item	<Off>* <Hide> < Disable >	Enables sending request to ME to hide or disable HECI-1 on host PCI
HECI-2 Hide in ME	Multipart item	<Off>* <Hide> < Disable >	Enables sending request to ME to hide or disable HECI-2 on host PCI
HECI-3 Hide in ME	Multipart item	<Off>* <Hide> < Disable >	Enables sending request to ME to hide or disable HECI-3 on host PCI
D0I3 Setting for HECI Disable	Multipart item	<Disable>* <Enable>	Setting this option disables setting D0I3 bit for all HECI devices
Break RTC Configuration	Multipart item	<Disabled>* <Enabled>	This is a test option which breaks RTC configuration

4.4.4.1.1 Override ICC Clock Settings



Item	Type	Options	Function description
Override ICC Clock Settings	Multipart item	<Disabled>* <Enabled>	This option allows customization of clock settings.
ICC Clock Spread Spectrum	Multipart item	<Disabled>* <Enabled>	Turn on / off Spread Spectrum Setting for IsCLK

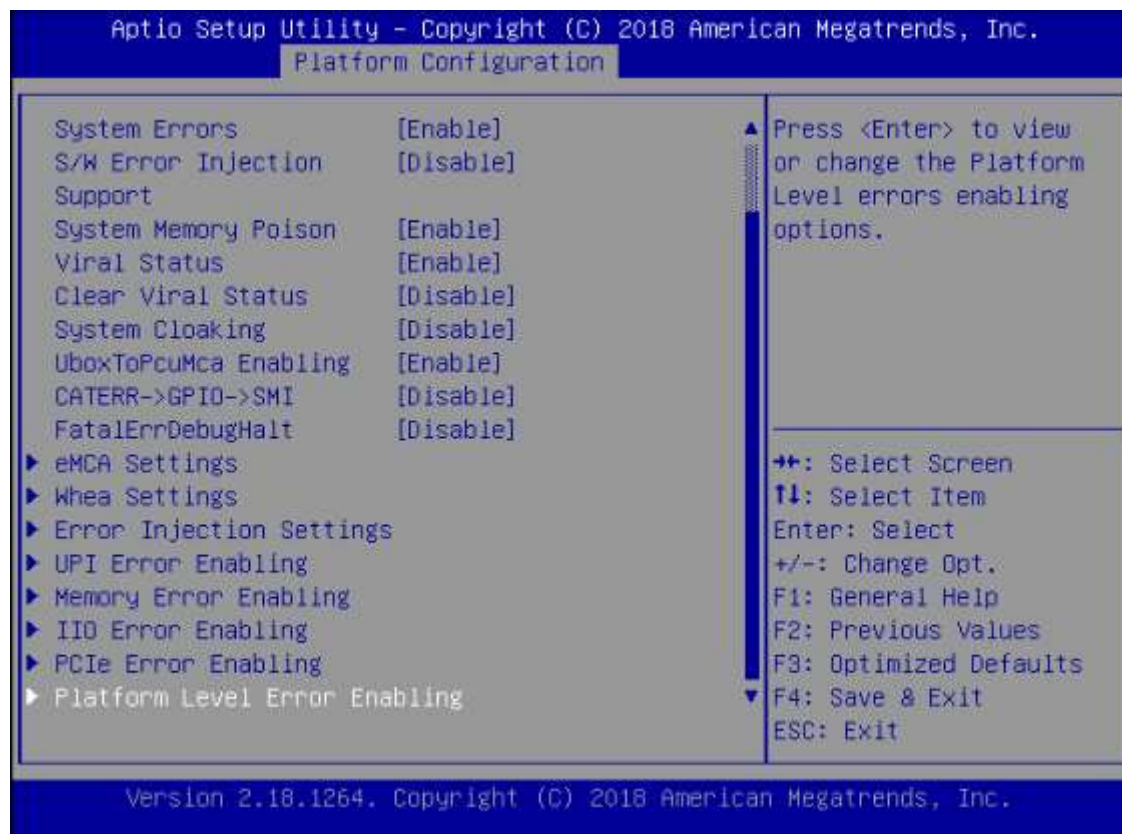
4.4.4.2 NM Configuration



Item	Type	Options	Function description
Boot Mode Override	Multipart item	<Disabled>* <Enabled>	Enables overriding the boot mode requested in NMFS register.
Boot Mode	Multipart item	<Performance Optimized>* <Power Optimized>	The boot mode to use instead of the mode requested in NMFS register.
Cores Disable Override	Multipart item	<Disabled>* <Enabled>	Enables overriding the value of the number of cores to disable requested in NMFS register.
Cores To Disable	Numeric item	0*~0x7F	The number of cores to disable instead of the number requested in NMFS register.
Power Measurement Override	Multipart item	<Disabled>* <Enabled>	Override power measurement support status reported to ME
Power Measurement	Multipart item	<Disable>* <Enable>	Override power measurement support status reported to ME
Hardware	Multipart	<Disabled>*	Override hardware change detection

Change Override	item	<Enabled>	status reported to ME
Hardware Changed	Multipart item	<No>* <Yes>	Override hardware change detection status reported to ME
PTU Load Override	Multipart item	<Disabled>* <Enabled>	In MROM-less system force loading PTU regardless of ME request

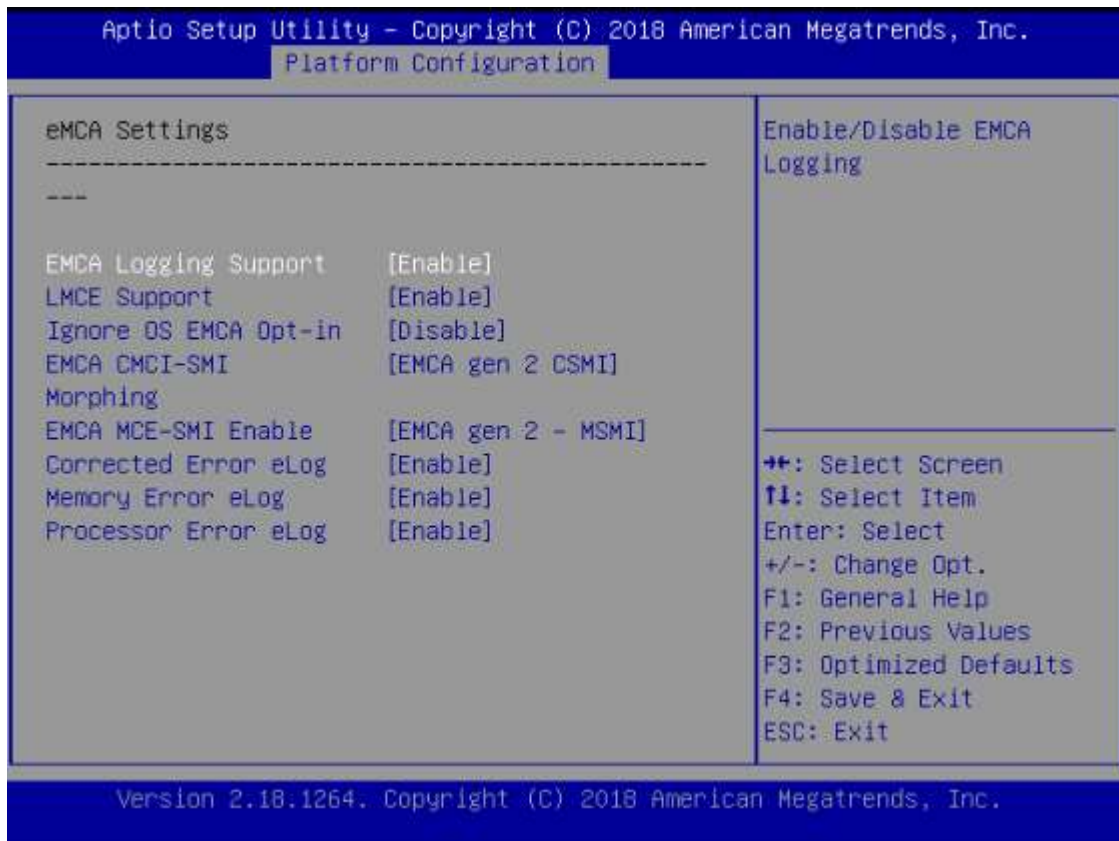
4.4.5 Runtime Error Logging



Item	Type	Options	Function description
Runtime Error Logging	Static text	N/A	
System Errors	Multipart item	<Disable> <Enable>*	System Error Enable/Disable setup options.
S/W Error Injection Support	Multipart item	<Disable>* <Enable>	When Enabled S/W Error Injection is supported by unlocking MSR 0x790
System Memory Poison	Multipart item	<Disable> <Enable>*	Enable/Disable System Memory Poison
Viral Status	Multipart item	<Disable> <Enable>*	Enable/Disable Viral
Clear Viral Status	Multipart item	<Disable>* <Enable>	Enable/Disable Clear Viral Status
System Cloaking	Multipart item	<Disable>* <Enable>	When enabled, Corrected and UCNA errors are masked from OS/SW visibility
UboxToPcuMca Enabling	Multipart item	<Disable> <Enable>*	<u>Enables</u> or disables <u>Ubox</u> Local errors to cause MCA.
CATERR->GPIO->SMI	Multipart item	<Disable>* <Enable>	Enable/Disable PCH GPIO to trigger SMI on CATERR
FatalErrDebug Halt	Multipart item	<Disable>* <Enable>	DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in <u>conjunction</u> with ITP as thread will halt in Fatal error flow
eMCA Settings	Submenu	N/A	Press <Enter> to view or change the eMCA configuration.
<u>Whea</u> Settings	Submenu	N/A	Press <Enter> to view or change the WHEA configuration.
Error Injection Settings	Submenu	N/A	Press <Enter> to view or change the Error Injection configuration.
UPI Error Enabling	Submenu	N/A	Press <Enter> to view or change the UPI errors enabling options.
Memory Error Enabling	Submenu	N/A	Press <Enter> to view or change the Memory errors enabling options.
IIO Error Enabling	Submenu	N/A	Press <Enter> to view or change the IIO errors enabling options.
PCIe Error	Submenu	N/A	Press <Enter> to view or change the

Enabling			PCIe errors enabling options.
Platform Level Error Enabling	Submenu	N/A	Press <Enter> to view or change the Platform Level errors enabling options.

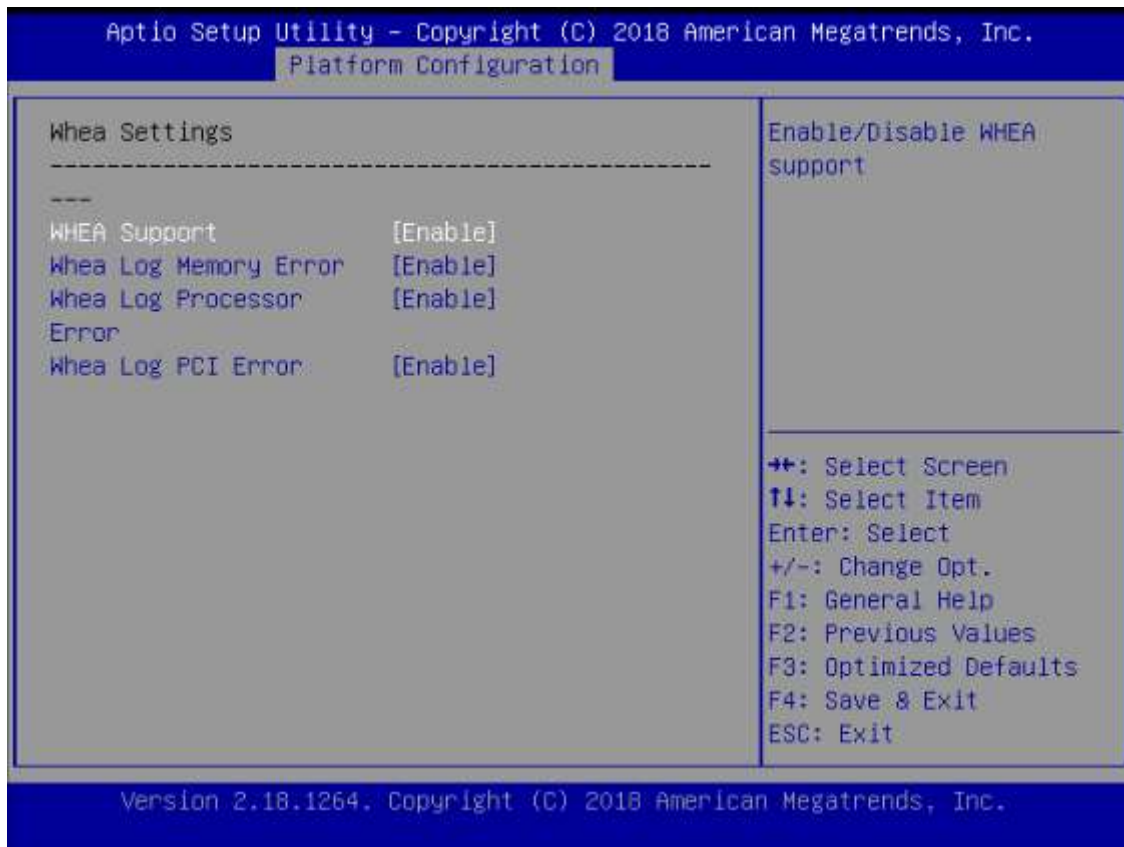
4.4.5.1 eMCA Settings



Item	Type	Options	Function description
eMCA Settings	Static text	N/A	
EMCA Logging Support	Multipart item	<Disable> <Enable>*	Enable/Disable EMCA Logging
LMCE Support	Multipart item	<Disable> <Enable>*	Enable/Disable Local MCE firmware support
Ignore OS EMCA Opt-in	Multipart item	<Disable>* <Enable>	Enable/Disable Ignore OS EMCA Opt-in and log
EMCA CMCI-SMI Morphing	Multipart item	<Disable> <EMCA <u>gen</u> 1 <u>Lite</u> > <EMCA <u>gen</u> 2 CSMI>*	Enable/Disable EMCA CSMI
EMCA MCE-SMI Enable	Multipart item	< Disable> <EMCA <u>gen</u> 1 Dual Mode>	Enable/Disable EMCA Uncorrected SMI for gen1 and gen2

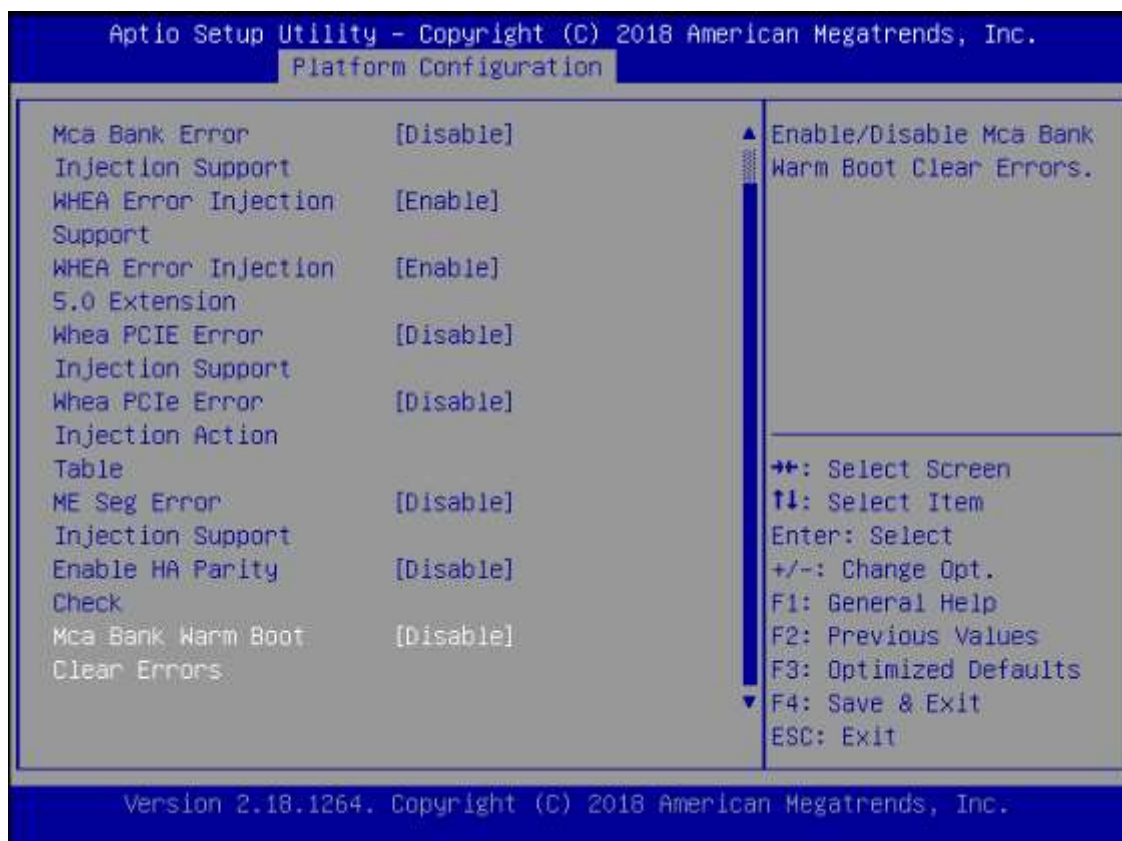
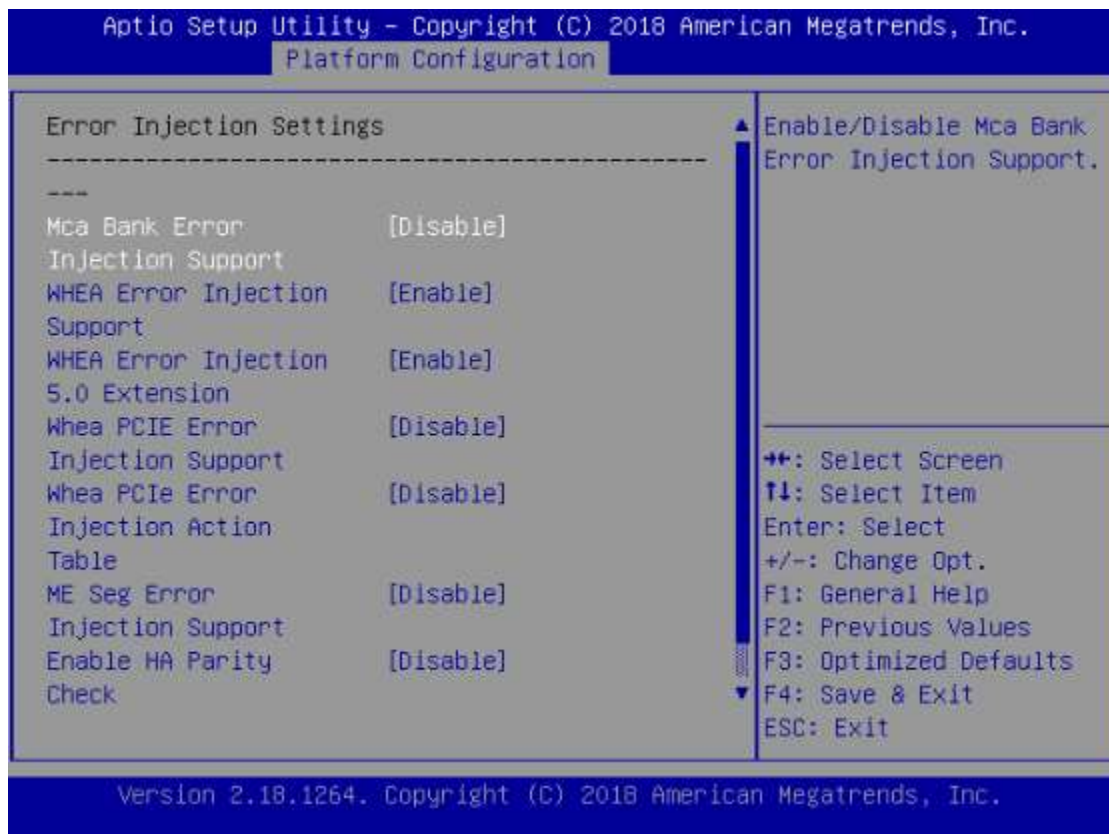
		<EMCA <u>gen</u> 2 - MSMI>*	
Corrected Error eLog	Multipart item	<Disabled> <Enabled>*	Enable/Disable Corrected Error eLog
Memory Error eLog	Multipart item	<Disabled> <Enabled>*	Enable/Disable Memory Error eLog
Processor Error eLog	Multipart item	<Disabled> <Enabled>*	Enable/Disable Processor Error eLog

4.4.5.2 Whea Settings



Item	Type	Options	Function description
<u>Whea</u> Settings	Static text	N/A	
WHEA Support	Multipart item	<Disable> <Enable>*	Enable/Disable WHEA support
<u>Whea</u> Log Memory Error	Multipart item	<Disable> <Enable>*	Enable/Disable <u>Whea</u> Log Memory Error
<u>Whea</u> Log Processor Error	Multipart item	<Disable> <Enable>*	Enable/Disable <u>Whea</u> Log Processor Error
<u>Whea</u> Log PCI Error	Multipart item	<Disable> <Enable>*	Enable/Disable <u>Whea</u> Log PCI Error

4.4.5.3 Error Injection Settings



Item	Type	Options	Function description
Error Injection Settings	Static text	N/A	
<u>Mca</u> Bank Error Injection Support	Multipart item	<Disable>* <Enable>	Enable/Disable <u>Mca</u> Bank Error Injection Support.
WHEA Error Injection Support	Multipart item	<Disable> <Enable>*	Enable/Disable WHEA Error Injection Support. Please disable DIRECTORY MODE for Memory Error Injection
WHEA Error Injection 5.0 Extension	Multipart item	<Disable> <Enable>*	<u>Whea</u> EINJ ACPI 5.0 support for set error type with address and vendor extensions.
Whea PCIE Error Injection Support	Multipart item	<Disable>* <Enable>	Enable/Disable Whea PCIE Error Injection Support.
Whea PCIe Error Injection Action Table	Multipart item	<Disable>* <Enable>	Use Action Table for Whea PCIe Error Injection
ME Seg Error Injection Support	Multipart item	<Disable>* <Enable>	Enable/Disable ME Seg Error Injection Support.
Enable HA Parity Check	Multipart item	<Disable>* <Enable>	Enable/Disable HA Parity Check.
<u>Mca</u> Bank Warm Boot Clear Errors	Multipart item	<Disable>* <Enable>	Enable/Disable <u>Mca</u> Bank Warm Boot Clear Errors.

4.4.5.4 UPI Error Enabling



Item	Type	Options	Function description
UPI Error Enabling	Static text	N/A	
SMI UPI Lane Failover	Multipart item	<Disable> <Enable>*	Enable/disable SMI when clock/data failover is set

4.4.5.5 Memory Error Enabling

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

Platform Configuration

Memory Error Enabling		▲ Enable/Disable Memory Error

Memory Error	[Enable]	
Memory Corrected Error	[Enable]	
Memory Leaky Bucket Value	0	
Spare Interrupt	[SMI]	
NVMCTLR Errors	[Disable]	
NVMCTLR Low Priority Error Signaling	[Disable]	
NVMCTLR High Priority Error Signaling	[Disable]	
Set NGN Address Range Scrub	[Disable]	
		⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Platform Configuration

Memory Error		▲ Configures to signal Poison or Viral upon receiving DIMM Physical Address Error
Memory Error	[Enable]	
Memory Corrected Error	[Enable]	
Memory Leaky Bucket Value	0	
Spare Interrupt	[SMI]	
NVMCTLR Errors	[Disable]	
NVMCTLR Low Priority Error Signaling	[Disable]	
NVMCTLR High Priority Error Signaling	[Disable]	
Set NGN Address Range Scrub	[Disable]	
Set NGN Host Alert Policy for AIT Error	[Poison]	
Set NGN Host Alert Policy for DPA Error	[Poison]	
		⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
Memory Error Enabling	Static text	N/A	
Memory Error	Multipart item	<Disable> <Enable>*	Enable/Disable Memory Error
Memory Corrected Error	Multipart item	<Disable> <Enable>*	Enable/Disable Memory Corrected Error
Memory Leaky Bucket Value	Numeric item	0* ~ 0xFFFF	0x0000 - 0xffff
Spare Interrupt	Multipart item	<Disable> <SMI>* <Error Pin> <CMCI>	Spare Interrupt Selection
NVMCTLR Errors	Multipart item	<Disable>* <Enable>	Enable/Disabled NVMCTLR Error Reporting & Logging
NVMCTLR Low Priority Error Signaling	Multipart item	<Disable>* <Enable>	Selection of signaling for errors bucketed as Low Priority
NVMCTLR High Priority Error Signaling	Multipart item	<Disable>* <Enable>	NVMCTLR High Priority Error Signaling
Set NGN Address Range Scrub	Multipart item	<Disable>* <Enable>	Enable/Disable NGN DIMM Physical Address Range scrub
Set NGN Host Alert Policy for AIT Error	Multipart item	<Poison>* <Viral>	Configures to signal Poison or Viral upon receiving Address Indirection Table Error
Set NGN Host Alert Policy for DPA Error	Multipart item	<Poison>* <Viral>	Configures to signal Poison or Viral upon receiving DIMM Physical Address Error

4.4.5.6 IIO Error Enabling



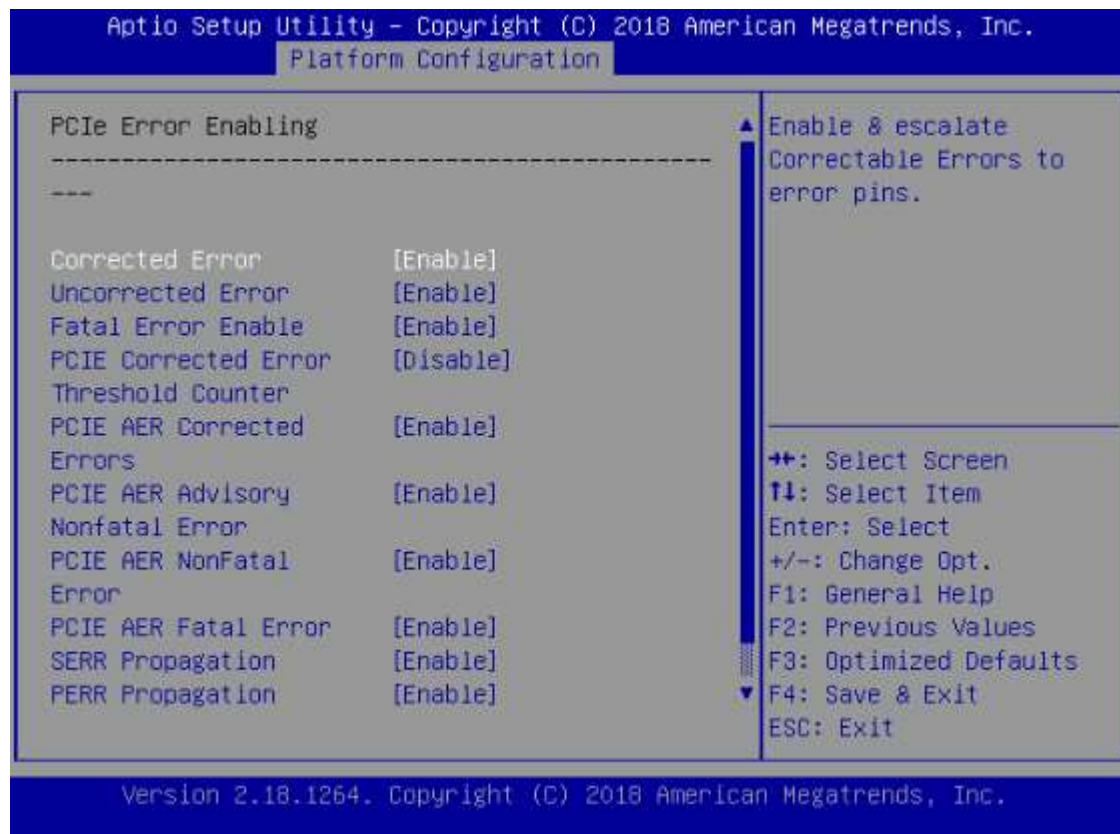


Item	Type	Options	Function description
IIO Error Enabling	Static text	N/A	
IIO/PCH Global Error Support	Multipart item	<Disable> <Enable>*	Enable/Disable IIO/PCH Error Support.
IIO MCA Support	Multipart item	<Disable>* <Enable>	Enable/Disable IIO MCA Support
IIO Error Pin Programming	Multipart item	<Disable>* <Enable>	Enable/Disable IIO Error Pin Programming
IIO Error Registers Clear	Multipart item	<Disable> <Enable>*	Enable/Disable Clear IIO Error Registers
IIO LER Support	Multipart item	<Disable>* <Enable>	Enable/Disable IIO LER Support
IIO Coherent Interface Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO Coherent Interface Error
IIO IRPO protocol	Multipart item	<Disable> <Enable>*	Enable or disable Coherent Interface protocol IIO parity error reporting

parity error			
IIO IRP0 protocol qt overflow underflow error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting
IIO IRP0 protocol rcvd unexprsp	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting
IIO IRP0 csr acc 32b unaligned	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting
IIO IRP0 wrcache uncecccs0 error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting
IIO IRP0 wrcache uncecccs1 error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting
IIO IRP0 protocol rcvd poison error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting
IIO IRP0 wrcache correcccs0 error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting
IIO IRP0 wrcache correcccs1 error	Multipart item	<Disable> <Enable>*	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting
IIO Misc. Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO Misc. Error
IIO Vtd Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO Vtd Error
IIO Dma Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO Dma Error
IIO Dmi Error	Multipart item	<Disable>* <Enable>	Enable/Disable IIO Dmi Error

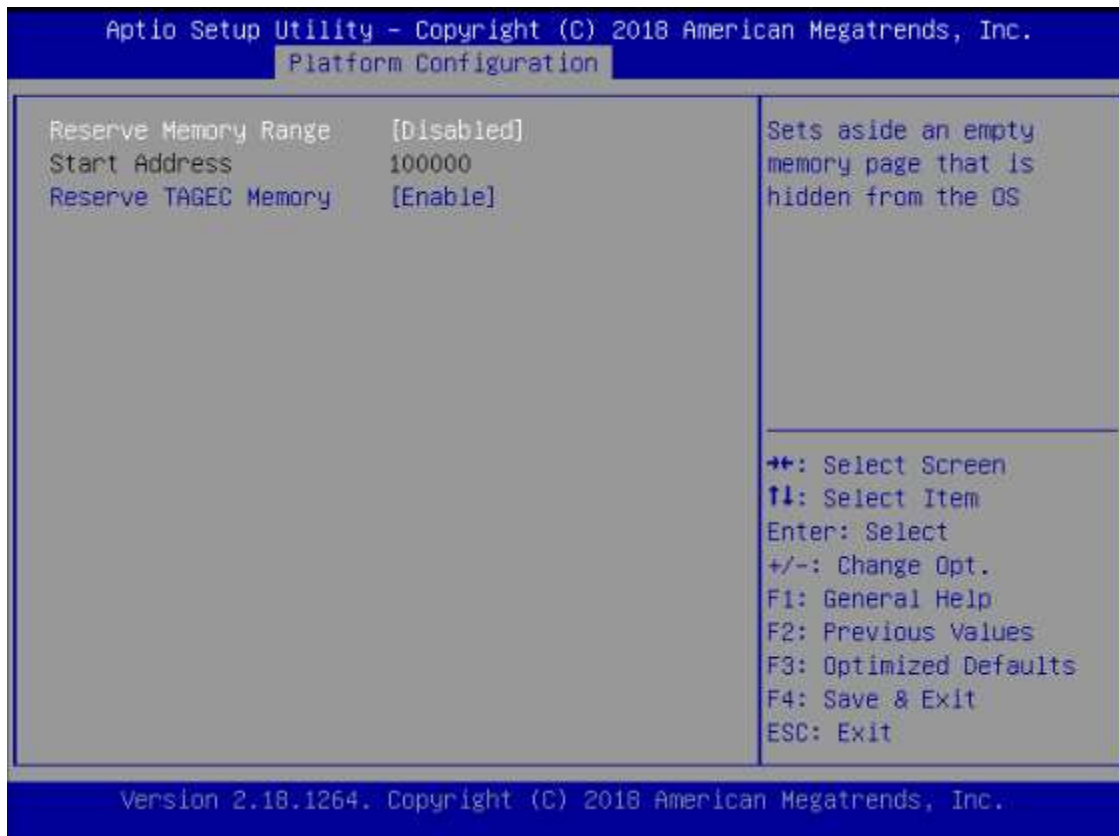
PCIE Error	Multipart item	<Disable> <Enable>*	Enable/Disable PCIE Error
IIO PCIE Additional Corrected Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO PCIE Additional Corrected Error
IIO PCIE Additional Uncorrected Error	Multipart item	<Disable> <Enable>*	Enable/Disable IIO PCIE Additional Uncorrected Error
IIO PCIE AER Spec Compliant	Multipart item	<Disable>* <Enable>	Enable/Disable IIO PCIE AER Spec Compliant

4.4.5.7 PCIe Error Enabling



Item	Type	Options	Function description
I/O Error Enabling	Static text	N/A	
Corrected Error	Multipart item	<Disable> <Enable>*	Enable & escalate Correctable Errors to error pins.
Uncorrected Error	Multipart item	<Disable> <Enable>*	Enable & escalate Uncorrectable/Recoverable to error pins.
Fatal Error Enable	Multipart item	<Disable> <Enable>*	Enable & escalate fatal errors to error pins.
PCIe Corrected Error Threshold Counter	Multipart item	<Disable>* <Enable>	Enable/Disable PCIe Corrected Error Counter
PCIe AER Corrected Errors	Multipart item	<Disable> <Enable>*	Enable/Disable PCIe AER Corrected Errors
PCIe AER Advisory Nonfatal Error	Multipart item	<Disable> <Enable>*	Enable/Disable PCIe AER Advisory Nonfatal Error
PCIe AER NonFatal Error	Multipart item	<Disable> <Enable>*	Enable/Disable PCIe AER NonFatal Error
PCIe AER Fatal Error	Multipart item	<Disable> <Enable>*	Enable/Disable PCIe AER Fatal Error
SERR Propagation	Multipart item	<Disable> <Enable>*	Enable/Disable SERR propagation
PERR Propagation	Multipart item	<Disable> <Enable>*	Enable/Disable PERR propagation
Signal to OS on SERR	Multipart item	<Disable> <Enable>*	Enable/Disable Signal to OS on SERR
Signal to OS on PERR	Multipart item	<Disable> <Enable>*	Enable/Disable Signal to OS on PERR

4.4.6 Reserve Memory



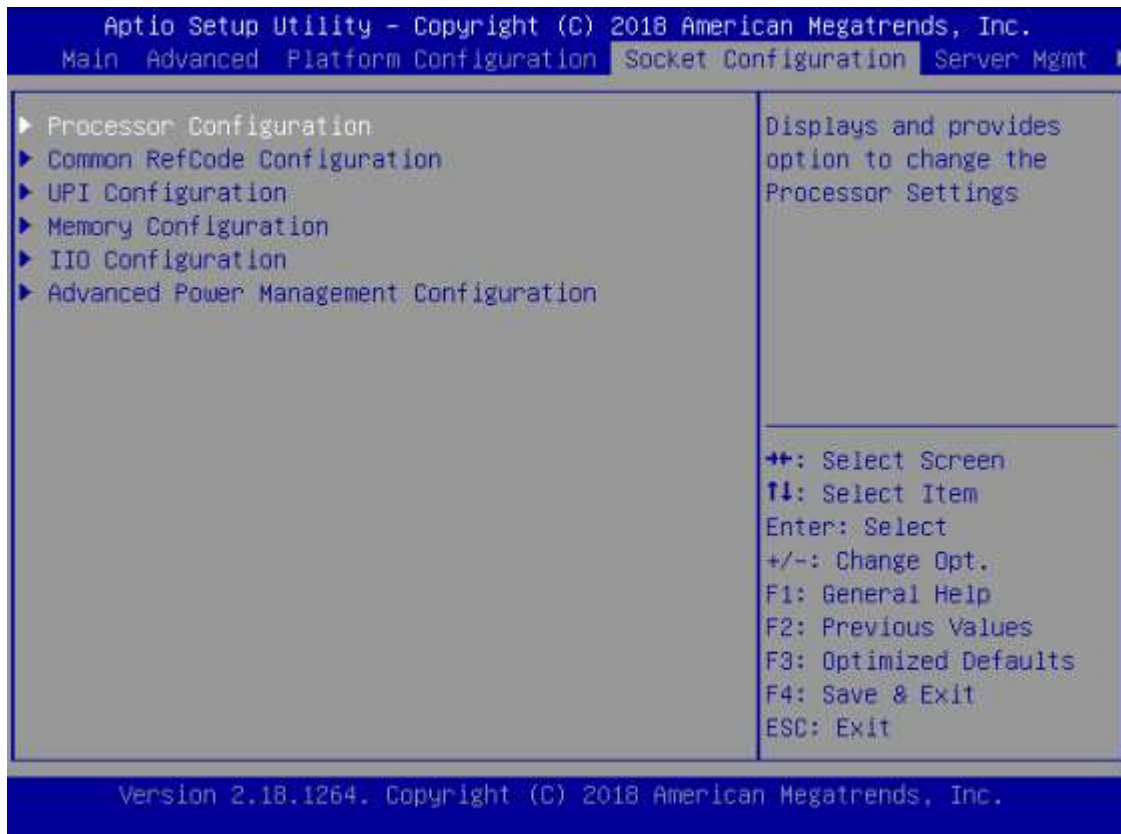
Item	Type	Options	Function description
Reserve Memory Range	Multipart item	<Disabled>* <Enabled>	Sets aside an empty memory page that is hidden from the OS
Start Address	Numeric item	0x100000* ~ 0xFFFFFFFF FFFFFFF	Address that reserved memory page starts at
Reserve TAGEC Memory	Multipart item	<Disable> <Enable>*	Reserve 16M for TAGEC

4.4.7 Non-Silicon Specific Items



Item	Type	Options	Function description
ResetTesting	Static text	N/A	All SV reset testing options
Reset Type	Multipart item	<None>* <Power Good S-S> <Normal S-F (F-F) HRDRST>	Option for forcing reset testing based on reset type selected

4.5 Socket Configuration



Item	Type	Options	Function description
Processor Configuration	Submenu	N/A	Displays and provides option to change the Processor Settings
Common RefCode Configuration	Submenu	N/A	Displays and provides option to change the Common RefCode Settings
UPI Configuration	Submenu	N/A	Displays and provides option to change the UPI Settings
Memory Configuration	Submenu	N/A	Displays and provides option to change the Memory Settings
IIO Configuration	Submenu	N/A	Displays and provides option to change the IIO Settings
Advanced Power Management Configuration	Submenu	N/A	Displays and provides option to change the Power Management Settings

4.5.1 Processor Configuration

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

Socket Configuration

Processor Configuration		Change Per-Socket Settings	

▶ Per-Socket Configuration			
Processor BSP	50654 - SKX H0		
Revision			
Processor Socket	Socket 0	Socket 1	
Processor ID	00050654*	N/A	
Processor Frequency	2.100GHz	N/A	
Processor Max Ratio	15H	N/A	
Processor Min Ratio	0AH	N/A	
Microcode Revision	0200003C	N/A	
L1 Cache RAM	64KB	N/A	
L2 Cache RAM	1024KB	N/A	
L3 Cache RAM	22528KB	N/A	
Processor 0 Version	Intel(R) Xeon(R) Gold 6130T CPU @ 2.10GHz		
Processor 1 Version	Not Present		

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Socket Configuration

Processor Configuration		Change Per-Socket Settings	

▶ Per-Socket Configuration			
Processor BSP	50654 - SKX H0		
Revision			
Processor Socket	Socket 0	Socket 1	
Processor ID	00050654*	N/A	
Processor Frequency	2.100GHz	N/A	
Processor Max Ratio	15H	N/A	
Processor Min Ratio	0AH	N/A	
Microcode Revision	0200003C	N/A	
L1 Cache RAM	64KB	N/A	
L2 Cache RAM	1024KB	N/A	
L3 Cache RAM	22528KB	N/A	
Processor 0 Version	Intel(R) Xeon(R) Gold 6130T CPU @ 2.10GHz		
Processor 1 Version	Not Present		

▲ Enables the Vanderpool Technology, takes effect after reboot.
 ⇐+: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
Enable SMX	[Disable]	▲ Enable/disable AES-NI support ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Lock Chipset	[Enable]	
MSR Lock Control	[Enable]	
PPIN Control	[Unlock/Enable]	
DEBUG INTERFACE	[Disable]	
Hardware Prefetcher	[Enable]	
Adjacent Cache Prefetch	[Enable]	
DCU Streamer Prefetcher	[Enable]	
DCU IP Prefetcher	[Enable]	
LLC Prefetch	[Disable]	
DCU Mode	[32KB 8Way Without ECC]	
Bsp Selection	[Auto]	
MTRR Default as uncacheable.	[Enable]	
Extended APIC	[Disable]	
AES-NI	[Enable]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
Down Stream PECI	[Enable]	▲ Enable or Disable OC Detect ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
PECI IN TRUST BIT	[Enable]	
ENABLE		
IIO LLC Ways	0	
[19:0] (Hex)		
Expanded IIO LLC	0	
Ways [10:0] (Hex)		
Remote Ways	0	
[22:12] (Hex)		
QLRU Config	0	
[63:32] (Hex)		
QLRU Config	0	
[31:0] (Hex)		
Targeted Smi	[Disable]	
eSMM Save State	[Disable]	
Smbus Error Recovery	[Disable]	
OC Detect	[No change]	
Fast Prochot	[Disable]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
Processor Configuration	Static text	ASCII string	
Per-Socket Configuration	Submenu	N/A	Change Per-Socket settings
Processor BSP Revision	Static text	N/A	
Processor Socket	Static text	ASCII string	
Processor ID	Dynamic text	ASCII string	
Processor Frequency	Dynamic text	X.XXX Ghz	
Processor Max Ratio	Dynamic text	Hex number	
Processor Min Ratio	Dynamic text	Hex number	
Microcode Revision	Dynamic text	ASCII string	
L1 Cache RAM	Dynamic text	YYYY KB	
L2 Cache RAM	Dynamic text	ZZZZ KB	
L3 Cache RAM	Dynamic text	QQQQQ KB	
Processor 0 Version	Dynamic text	ASCII string	
Processor 1 Version	Dynamic text	ASCII string	
TRACE HUB STH ACPIBAR BASE	Multipart item	<Disable>* <Enable>	Enable: Set PCH_TRACE_HUB_FW_BASE_ADDRESS in MSR_TRACE_HUB_STH_ACPIBAR_BASE (MSR 80h).
Hyper-Threading [All]	Multipart item	<Disable> <Enable>*	Enables Hyper Threading (Software Method to Enable/Disable Logical

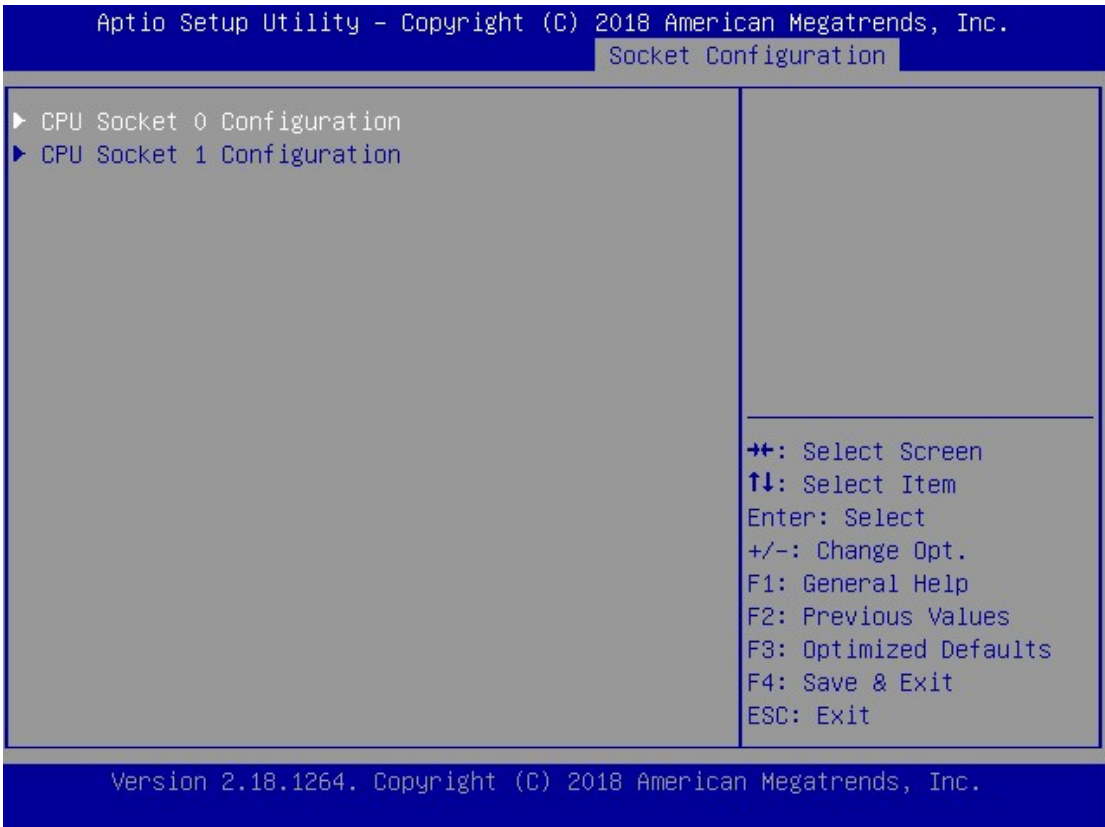
			Processor threads
Intel Enhanced Debug	Multipart item	<Disable> <4096K>*	Option to disable/enable Intel Enhanced Debug support
IED Trace memory	Multipart item	<Disable>* <4> <8> <16> <32> <64> <128> <256> <512> <1G>	Option to allocate memory for PSMI trace
TSEG Smram Size	Multipart item	<4M> <8M> <16M> <32M> <64M> <128M>	Option to change the size of SMRAM for TSEG
Allow mixed freq among CPUs	Multipart item	<Disable> <Enable>*	Keep (mixed) power-on freq of each CPU socket. Caution: This is for Intel PPV test only
Check CPU BIST Result	Multipart item	<Disable> <Enable>*	Disable failed BIST core when enable, otherwise, ignore BIST result
3StrikeTimer	Multipart item	<Disable> <Enable>*	The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT(MSR 0x01a4).
Fast String	Multipart item	<Disable> <Enable>*	When enabled, enable fast strings for REP MOVSB/STOS
Machine Check	Multipart item	<Disable> <Enable>*	Enable or Disable the Machine Check
Max CPUID Value Limit	Multipart item	<Disable>* <Enable>	This should be enabled in order to boot legacy OSes that cannot support CPUs with extended CPUID functions.

Execute Disable Bit	Multipart item	<Disable> <Enable>*	When disabled, forces the XD feature flag to always return 0.
Enable Intel® TXT Support	Multipart item	<Disable>* <Enable>	Enables Intel® Trusted Execution Technology Configuration. Please disable "EV DFX Features" when TXT is enabled.
VMX	Multipart item	<Disable> <Enable>*	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	Multipart item	<Disable>* <Enable>	Enables Safer Mode Extensions.
Lock Chipset	Multipart item	<Disable> <Enable>*	
MSR Lock Control	Multipart item	<Disable> <Enable>*	Enable - MSR 3Ah, MSR 0E2h and CSR 80h will locked. Power Good reset is needed to remove lock bits.
PPIN Control	Multipart item	<Unlock/Disabled> <Unlock/Enabled>*	Unlock and Enabled/Disable PPIN Control
DEBUG INTERFACE	Multipart item	<Disable>* <Enable>	MSR 0C80h bit[0], When set enables the debug features.
Hardware Prefetcher	Multipart item	<Disable> <Enable>*	MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetcher	Multipart item	<Disable> <Enable>*	MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	Multipart item	<Disable> <Enable>*	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2])
DCU IP Prefetcher	Multipart item	<Disable> <Enable>*	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3])
LLC Prefetch	Multipart item	<Disable>* <Enable>	Enable/Disable LLC Prefetch on all threads
DCU Mode	Multipart item	<32KB 8Way Without ECC>*	MSR 31h Bit[0] - A write of 1 selects the DCU mode as 16KB

		<16KB 4Way With ECC>	4-way with ECC.
Bsp Selection	Multipart item	<Socket0> < Socket1> < Socket2> < Socket3> <Auto>*	Choose the method to select BSP
MTRR Default as uncacheable.	Multipart item	<Disable> <Enable>*	EFI_CACHE_IA32_MTRR_DEF_T YPE msr(2FF) as uncacheable
Extended APIC	Multipart item	<Disable>* <Enable>	Enable/disable extended APIC support
AES-NI	Multipart item	<Disable> <Enable>*	Enable/Disable AES-NI support
APIC Physical Mode	Multipart item	<Disable>* <Enable>	Enalbe/Disable the APIC physical destination mode
Virtual Wire Mode	Multipart item	< Virtual Wire A >* < Virtual Wire B >	Select virtual wire interrupt mode
Down Stream PECI	Multipart item	<Disable> <Enable>*	Enable PCIe Down Stream PECI Write
PECI IN TRUST BIT ENABLE	Multipart item	<Disable> <Enable>*	PECI IN TRUST BIT ENABLE
IIO LLC Ways [19:0](Hex)	Multipart item	0*- 0x7fffff	MSR CBO_SLICE0_CR_IIO_LLC_WAYS bitmask
Expanded IIO LLC Ways [10:0](Hex)	Multipart item	0*- 0x7ff	MSR INGRESS_SPARE bitmask[10:0]
Remote Ways [22:12](Hex)	Multipart item	0*- 0x7ff	MSR INGRESS_SPARE bitmask[26:16], Value 0 means no override
QLRU Config [63:32](Hex)	Multipart item	0*- 0xffffffff	VIRTUAL_MSR_CR_QLRU_CONFIG bitmask
QLRU Config [31:0](Hex)	Multipart item	0*- 0xffffffff	VIRTUAL_MSR_CR_QLRU_CONFIG bitmask
Targeted SMI	Multipart item	<Disable>* <Enable>	Enable or disable targeted SMI feature

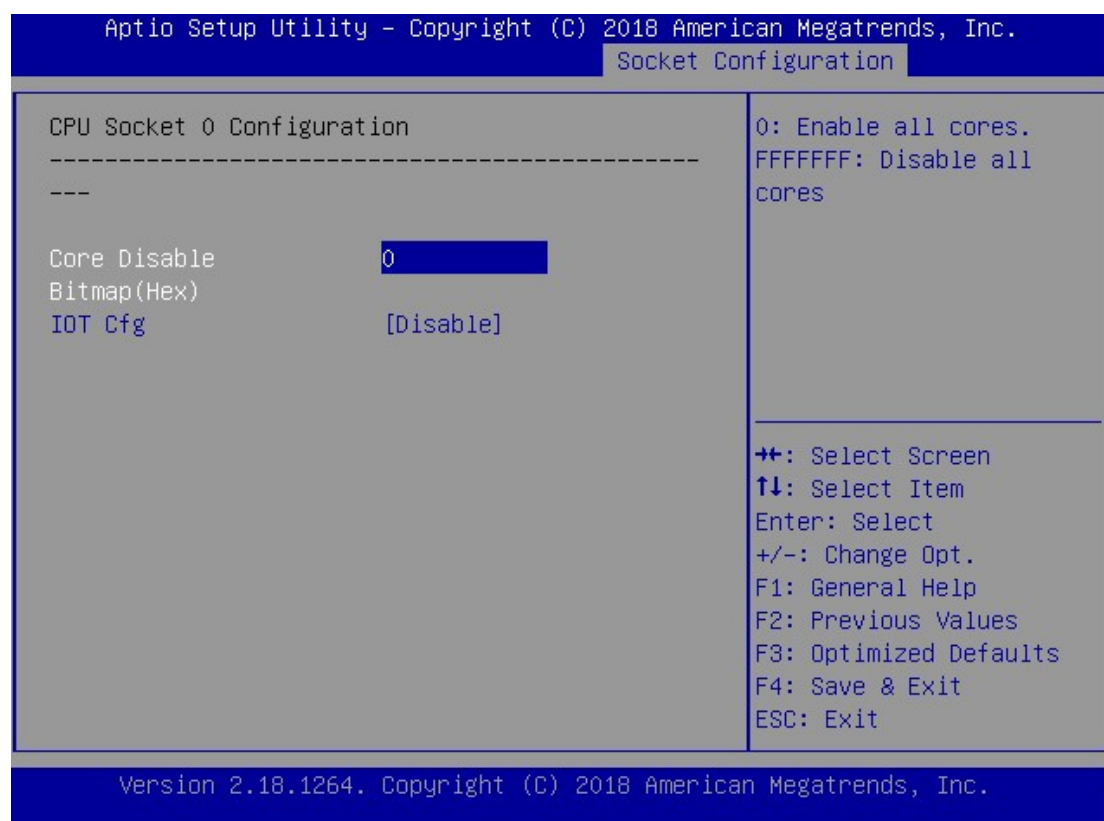
eSMM Save State	Multipart item	<Disable>* <Enable>	Enable or Disable the eSMM Save State Feature
Smbus Error Recovery	Multipart item	<Disable>* <Enable>	Enable or Disable Smbus Error Recovery
OC Detect	Multipart item	<Disable> <Enable> <No Change>*	Enable or Disable OC Detect
Fast Prochot	Multipart item	<Disable>* <Enable>	Enable/Disable/No change Fast Prochot#

4.5.1.1 Serial Per-Socket Configuration



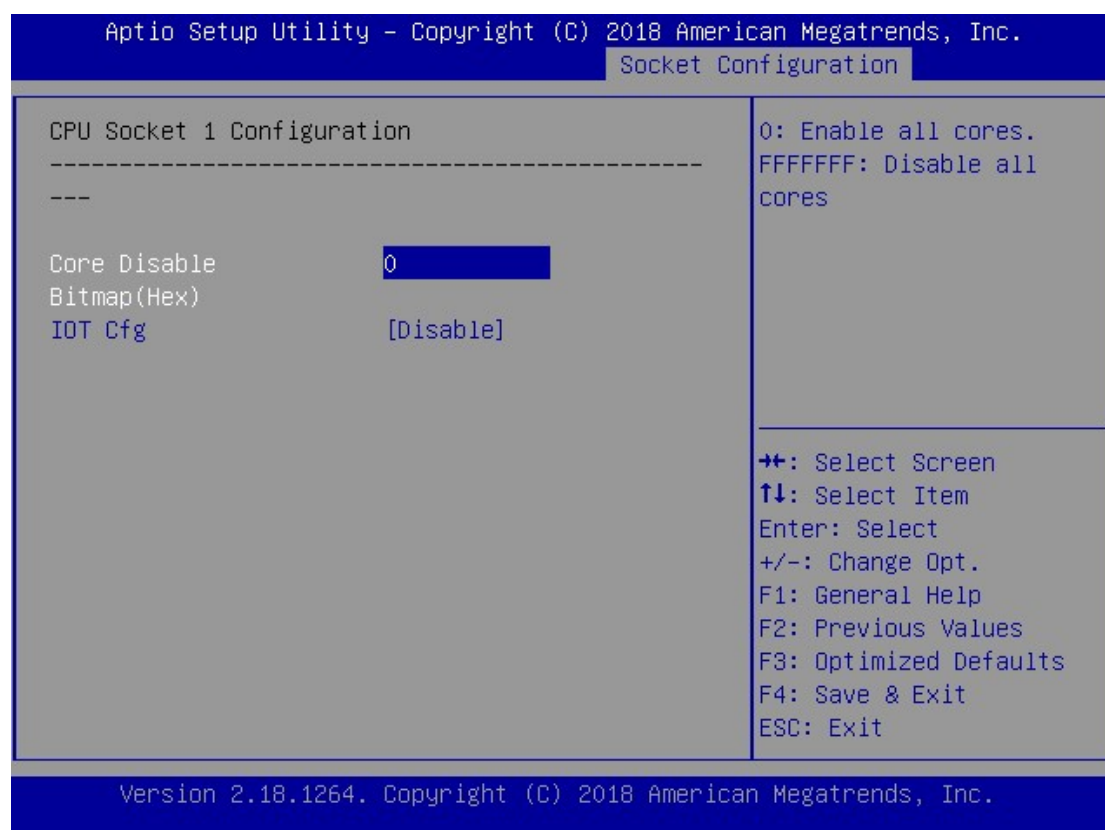
Item	Type	Options	Function description
CPU Socket 0 Configuration	Submenu	N/A	Options for CPU socket0
CPU Socket 1 Configuration	Submenu	N/A	Options for CPU socket1

4.5.1.1.1 CPU Socket 0 Configuration



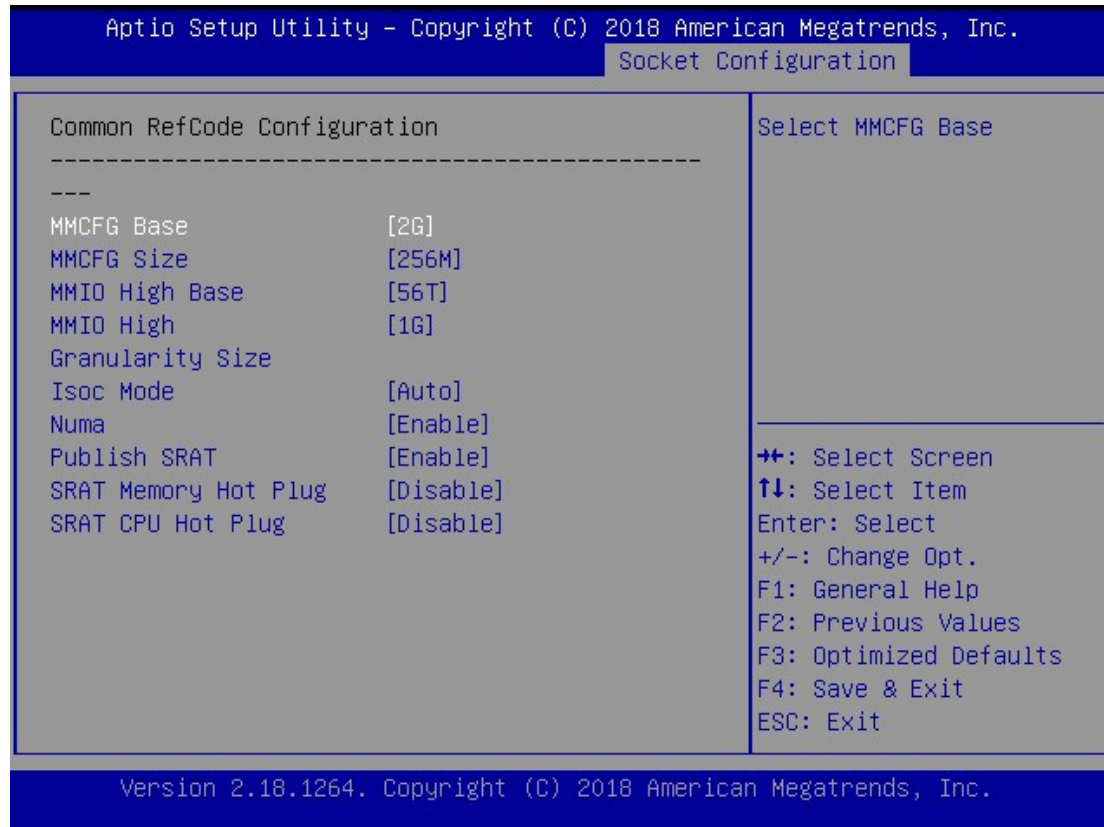
Item	Type	Options	Function description
Core Disable Bitmap(Hex)	Numeric item	0* ~ X	0: Enable all cores. ffffffff: Disable all cores
IOT Cfg	Multipar t item	<Disable>* <Enable>	Each bit enables IOT/OCLA for a CBo

4.5.1.1.2 CPU Socket 1 Configuration



Item	Type	Options	Function description
Core Disable Bitmap(Hex)	Numeric item	0* ~ X	0: Enable all cores. fffffff: Disable all cores
IOT Cfg	Multipar t item	<Disable>* <Enable>	Each bit enables IOT/OCLA for a CBo

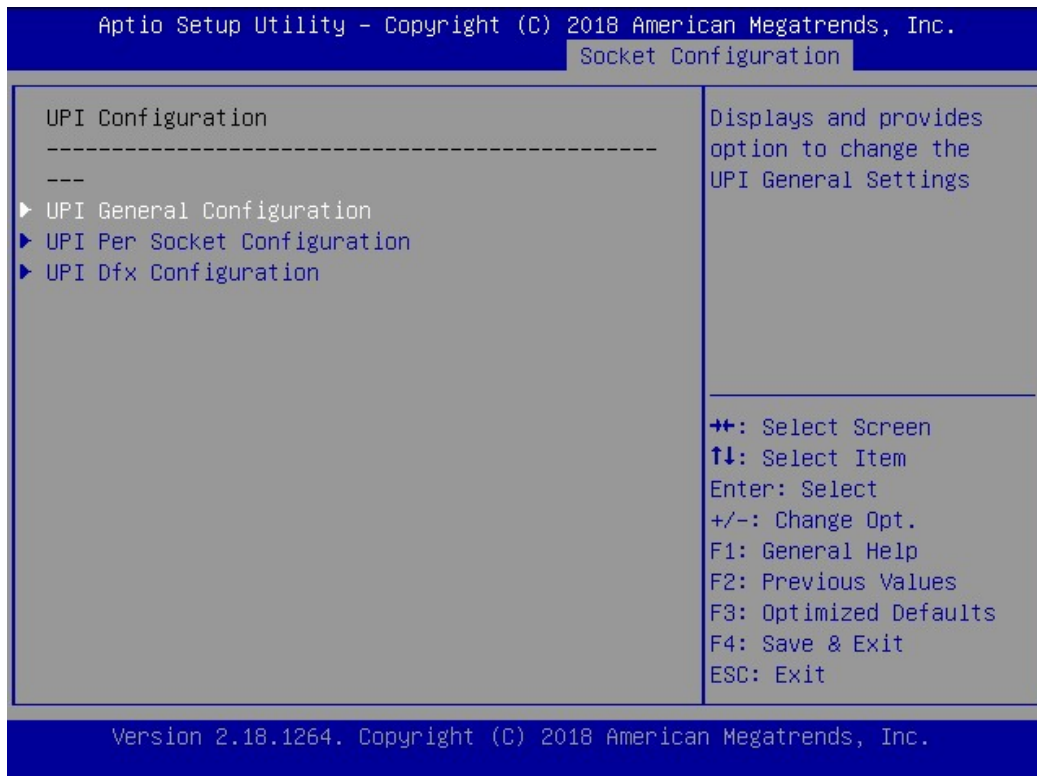
4.5.2 Common RefCode Configuration



Item	Type	Options	Function description
MMCFG Base	Multipart item	<1G> <1.5G> <1.75G> <2G>* <2.25G> <3G>	Select MMCFG Base
MMCFG Size	Multipart item	< 64M > <128M> <256M>* <512M> <1G> <2G>	Select MMCFG Size
MMIO High Base	Multipart item	< 56T >* <40T> <24T> <16T> <4T>	Select MMIO High Base

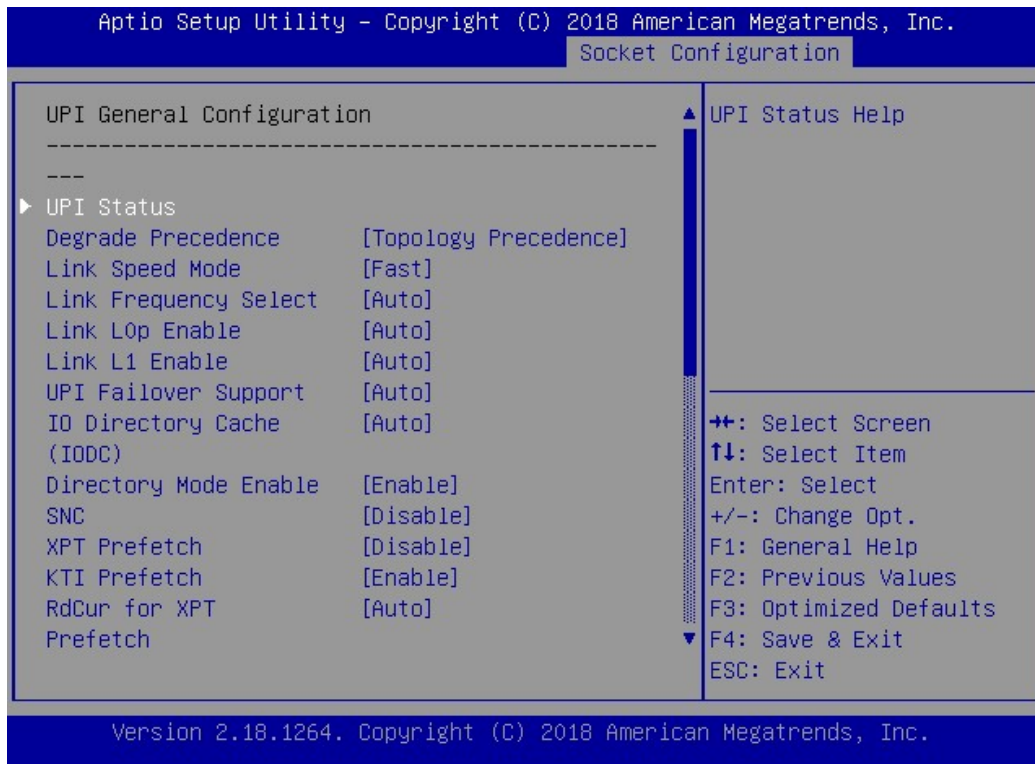
		<1T>	
MMIO High Granularity Size	Multipart item	<1G> <4G> <16G> <64G> <256G> <1024G>	Selects the allocation size used to assign mmioh resources.\nTotal mmioh space can be up to 32xgranularity.\nPer stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.
Isoc Mode	Multipart item	<Auto>* <Disable> <Enable>	Isoc: Disable,Enable
Numa	Multipart item	<Disable>* <Enable>	Enable or Disable Non uniform Memory Access (NUMA).
Publish SRAT	Multipart item	<Disable> <Enable>*	Publish the SRAT ACPI table to the OS.
SRAT Memory Hot Plug	Multipart item	<Disable>* <Enable>	Fix for OS that does not support memory hot plug.\nEx: SuSE SLES10 SP2. \n \nEnable by default. \nDisable will clear all hot plug bits and remove the hot plug entries in SRAT table.
SRAT CPU Hot Plug	Multipart item	<Disable>* <Enable>	Set Processor Flag to Enabled for all processor entries in SRAT.

4.5.3 UPI Configuration



Item	Type	Options	Function description
UPI Configuration	Static text	N/A	
UPI General Configuration	Submenu	N/A	Displays and provides option to change the UPI General Settings
UPI Per Socket Configuration	Submenu	N/A	UPI Per Socket Configuration
UPI Dfx Configuration	Submenu	N/A	Displays and provides option to change the UPI Dfx Settings

4.5.3.1 UPI General Configuration



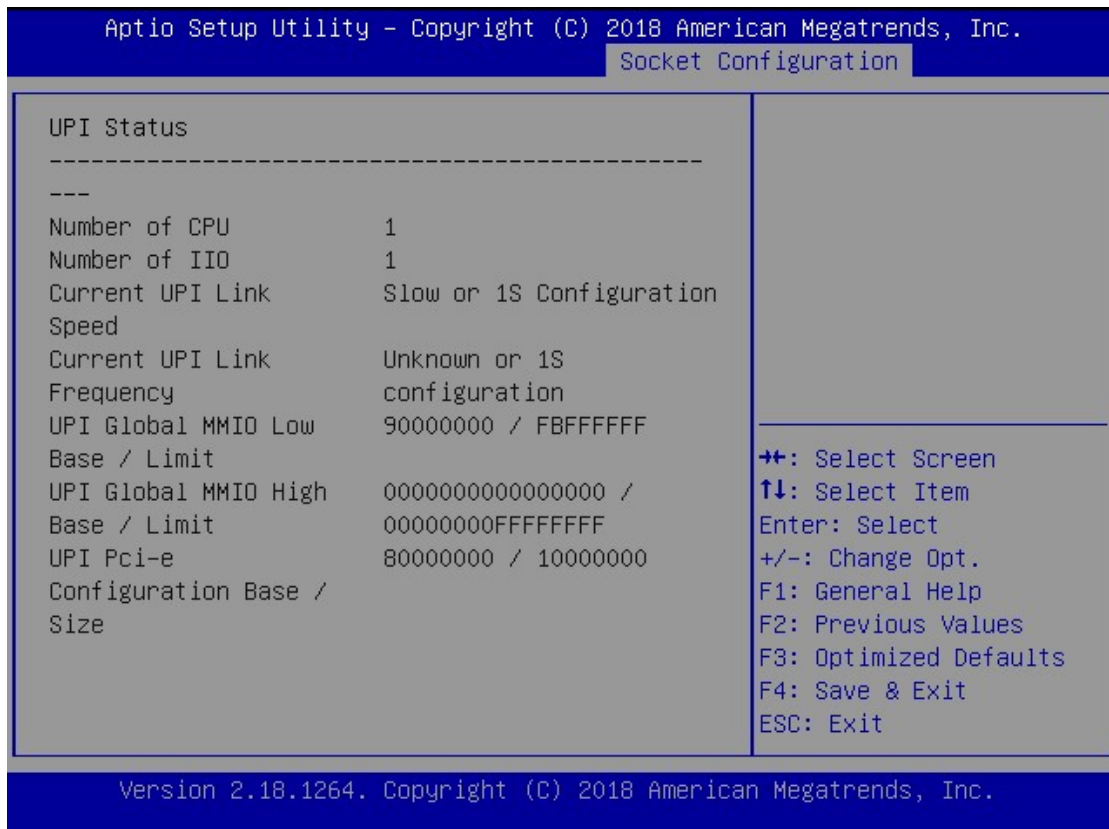
Item	Type	Options	Function description
UPI General Configuration	Static text	N/A	
UPI Status	Submenu	N/A	UPI Status
Degrade Precedence	Multipart item	<Topology Precedence>* <Feature Precedence>	Choose Topology Precedence to degrade features if system options are in conflict or choose Feature Precedence to degrade topology if system options are in conflict
Link Speed Mode	Multipart item	<Slow> <Fast>*	Select the UPI link speed as either the POR speed (Fast) or default speed (Slow)
Link Frequency Select	Multipart item	<9.6GB/s> <10.4GB/s> <Auto>* < Use Per Link Setting >	Allows for selecting the UPI Link Frequency
Link L0p Enable	Multipart item	<Disable> <Enable>	Enable - Set the c_l0p_en, Disable - Reset it, Auto - Auto decides based

		<Auto>*	on Si Compatibility
Link L1 Enable	Multipart item	<Disable> <Enable> <Auto>*	Enable - Set the c_l1_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility
UPI Failover Support	Multipart item	<Disable> <Enable> <Auto>*	Enable - Set the c_failover_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility
IO Directory Cache (IODC)	Multipart item	<Disable> <Auto>* <Enable for Remote Invltom Hybrid Push> <Invltom AllocFlow> <Enable for Remote Invltom Hybrid AllocNonAlloc> <Enable for Remote Invltom and Remote WViLF>	IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote Invltom (IIO) and/or WViLF (cores), Auto - Auto sets to WViLF
Directory Mode Enable	Multipart item	<Disable> <Enable>*	Directory Mode Enable
SNC	Multipart item	<Disable>* <Enable> <Auto>	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. SNC Enable supports Full SNC (2 clusters) and 1-way IMC interleave
XPT Prefetch	Multipart item	<Disable>* <Enable>	XPT Prefetch
KTI Prefetch	Multipart item	<Disable> <Enable>*	KTI Prefetch
RdCur for XPT Prefetch	Multipart item	<Disable> <Enable> <Auto>*	Enable - Set the suppress_mem_rd_prefetch_rdcu, Disable - Reset it, Auto - Auto

			decides based on Si Compatibility
UPI VNA Credit Override	Multipart item	<Maximum>* <Minimum> <Per Link>	Global option UPI VNA credit override: Max, Min, Per Link
CRC Mode	Multipart item	<16 Bit CRC> <32 Bit rolling CRC > <Auto>*	Select UPI CRC Mode: Auto sets this to 16-bit
UPI Load Board for Failed Links	Multipart item	<Disable>* <Enable>	For debugging purposes, UPI link will remain enabled for h/w continuous training in spite of previous failure
Legacy VGA Socket	Numeric item	0*~3	Socket that claims the legacy VGA range; valid values are 0-3; 0 is default
Legacy VGA Stack	Numeric item	0*~3	Stack that claims the legacy VGA range; valid values are 0-3; 0 is default
MMIO P2P Disable	Multipart item	<No>* <Yes>	To disable MMIO P2P traffic across Sockets. Default is NO to not disable
CPU Hot Plug	Multipart item	<Disable>* <Enable>	To enable CPU Hot Plug
CPU Hot Plug Topology	Multipart item	<4 SOCKETS MAX>* <8 SOCKETS MAX>	CPU Hot Plug Max Sockets has to be chosen before hands in order to use either 4 or 8 sockets topology
CPU SKU Type Mismatch check	Multipart item	<No> <Yes>*	Yes or No to do CPU SKU Type Mismatch check
UPI Debug Print Level	Multipart item	<Fatal> <Warning> <Summary> <Detail> <All>*	UPI Debug Print Level Enable-Disable
Local/Remote Threshold	Multipart item	<Disable> <Auto>* <Low> <Medium> <High>	Local/Remote Threshold setting

TSC Sync support	Multipart item	<Disable> <Enable> <Auto>*	TSC Sync support for all processors
Stale AtoS	Multipart item	<Disable>* <Enable> <Auto>	Stale A to S Dir optimization
LLC dead line alloc	Multipart item	<Disable> <Enable>* <Auto>	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC

4.5.3.1.1 UPI Status



Item	Type	Options	Function description
UPI Status	Static text	N/A	
Number of CPU	Dynamic text	Dec number	
Number of IIO	Dynamic text	Dec number	
Current UPI Link Speed	Dynamic text	Uni string	
Current UPI Link Frequency	Dynamic text	Uni string	
UPI Global MMIO Low Base / Limit	Dynamic text	Hex number/ Hex number	
UPI Global MMIO High Base / Limit	Dynamic text	Hex number/ Hex number	
UPI Pci-e Configuration Base / Size	Dynamic text	Hex number/ Hex number	

4.5.3.2 UPI Per Socket Configuration



Item	Type	Options	Function description
UPI Per Socket Configuration	Static text	N/A	
CPU 0	Submenu	N/A	CPU 0 Configuration Silk Screen Equivalent->CPU 1
CPU 1	Submenu	N/A	CPU 1 Configuration Silk Screen Equivalent->CPU 2

4.5.3.2.1 CPU 0



Item	Type	Options	Function description
CPU 0	Static text	N/A	
CPU 0 UPI Port 0	Submenu	N/A	CPU 0 UPI Port 0 Configuration
CPU 0 UPI Port 0 DFX	Submenu	N/A	CPU 0 UPI Port 0 DFX Configuration
CPU 0 UPI Port 1	Submenu	N/A	CPU 0 UPI Port 1 Configuration
CPU 0 UPI Port 1 DFX	Submenu	N/A	CPU 0 UPI Port 1 DFX Configuration
CPU 0 UPI Port 2	Submenu	N/A	CPU 0 UPI Port 2 Configuration
CPU 0 UPI Port 2 DFX	Submenu	N/A	CPU 0 UPI Port 2 DFX Configuration
Bus Resources Allocation Ratio	Numeric item	0,1*,2~8	Bus resources allocation ratio, range 0 to 8

4.5.3.2.1.1 CPU 0 UPI Port 0



Item	Type	Options	Function description
CPU 0 UPI Port 0	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

4.5.3.2.1.2 CPU 0 UPI Port 0 DFX



Item	Type	Options	Function description
CPU 0 UPI Port 0 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the

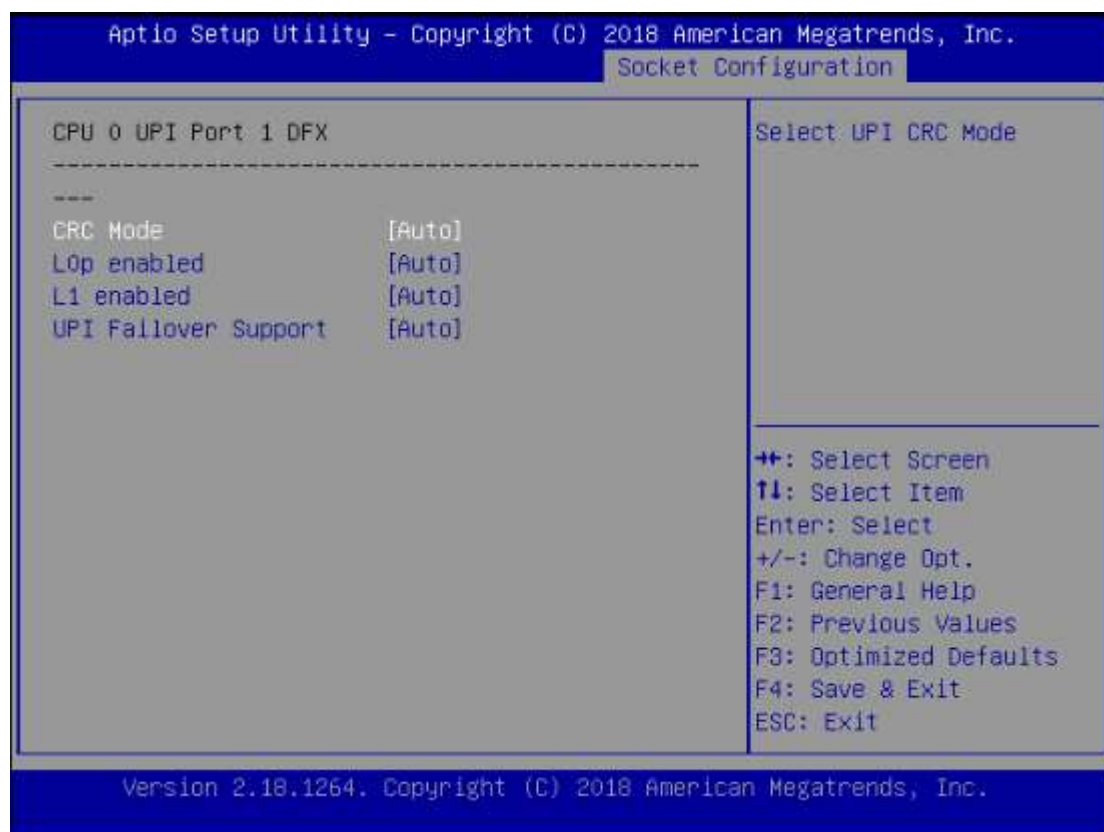
			connected port to determine if the link may enter L1.
UPI Failover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Failover

4.5.3.2.1.3 CPU 0 UPI Port 1



Item	Type	Options	Function description
CPU 0 UPI Port 1	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

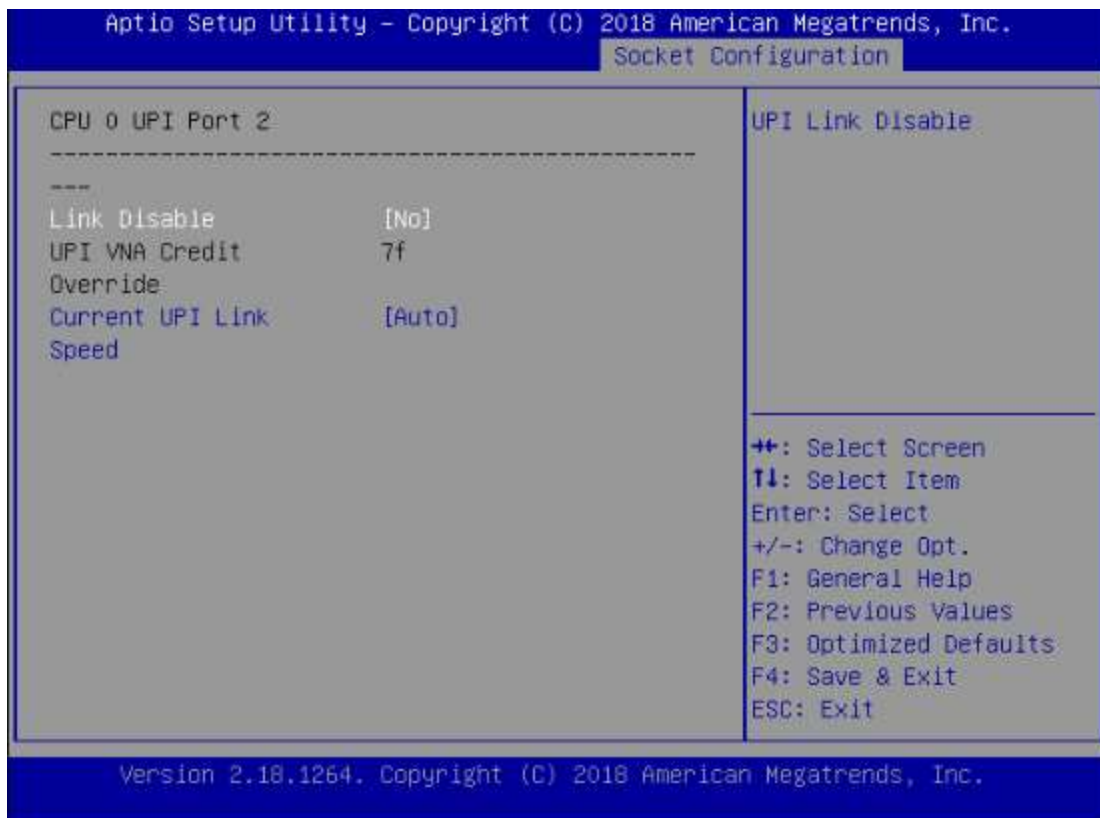
4.5.3.2.1.4 CPU 0 UPI Port 1 DFX



Item	Type	Options	Function description
CPU 0 UPI Port 1 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the

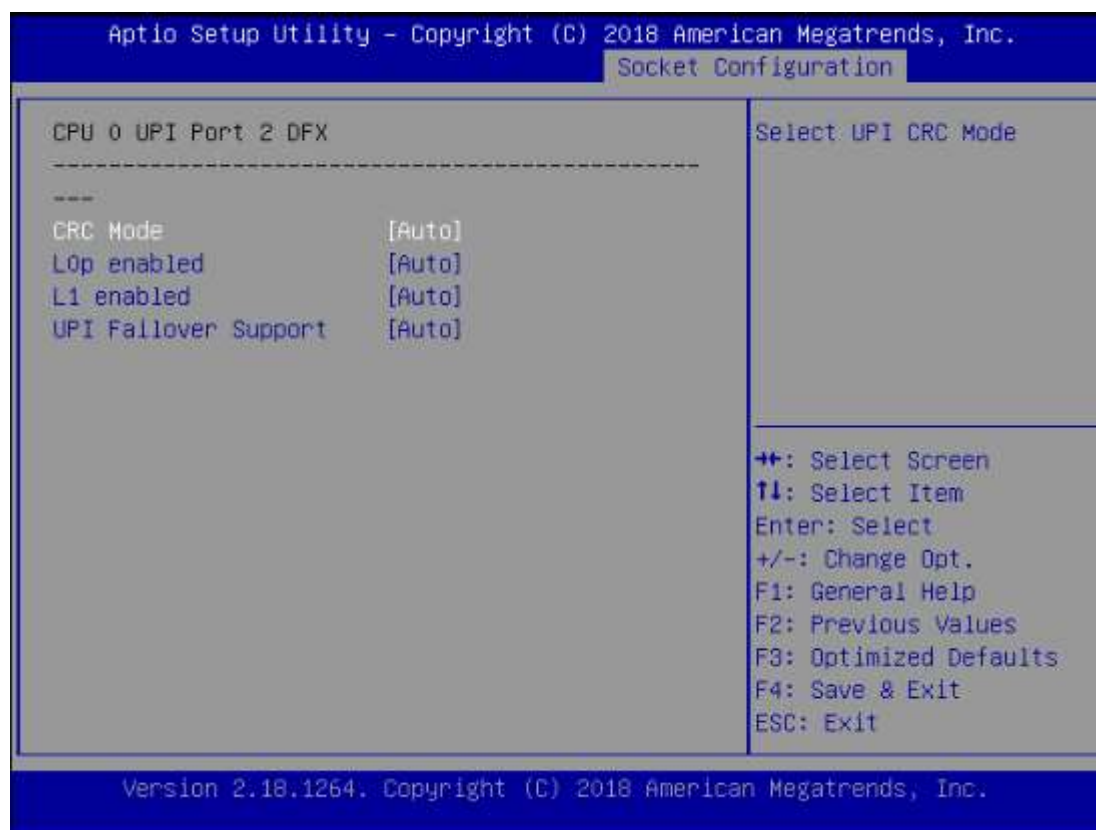
			connected port to determine if the link may enter L1.
UPI Failover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Failover

4.5.3.2.1.5 CPU0 UPI Port 2



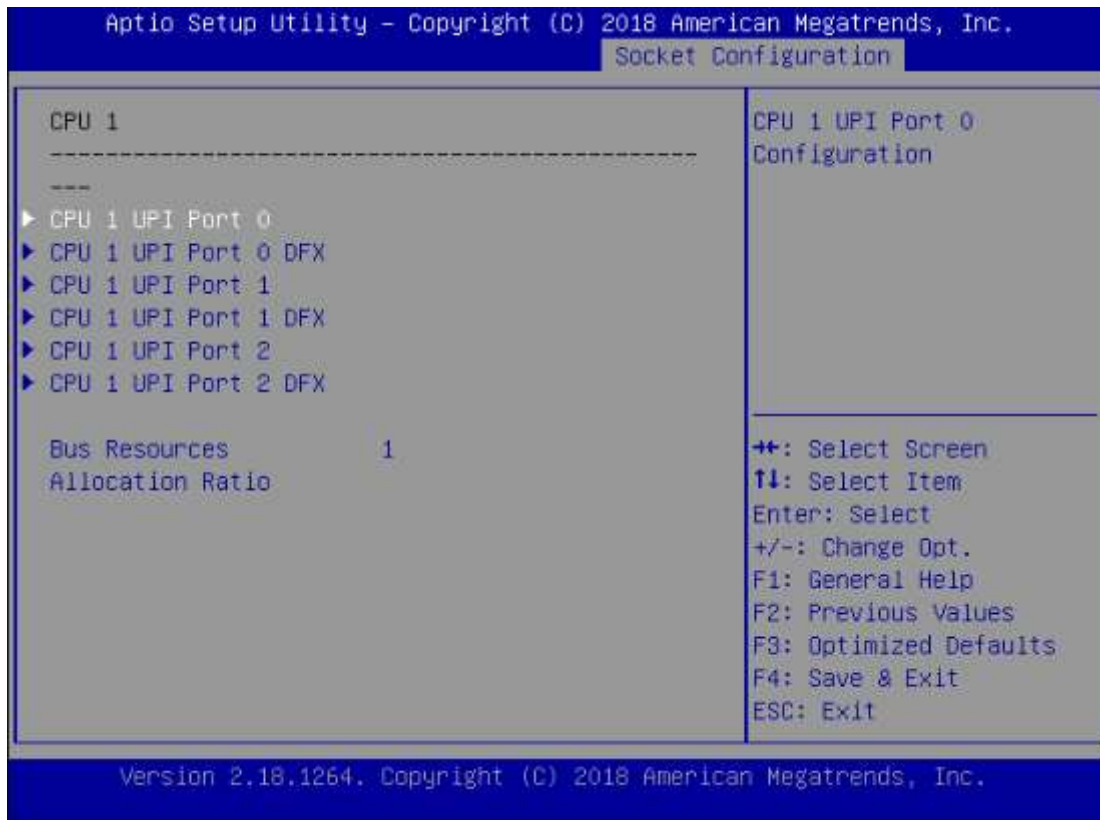
Item	Type	Options	Function description
CPU 0 UPI Port 2	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

4.5.3.2.1.6 CPU 0 UPI Port 2 DFX



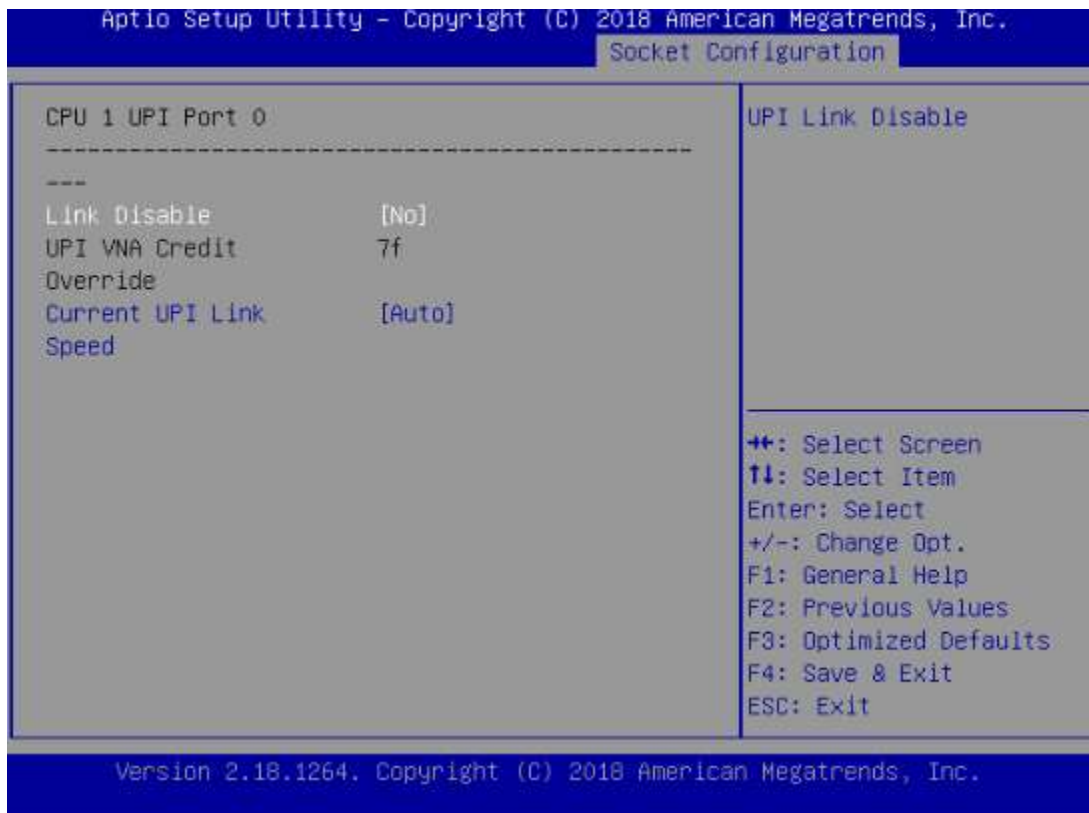
Item	Type	Options	Function description
CPU 0 UPI Port 2 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L1.
UPI Fallover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Fallover

4.5.3.2.2 CPU 1



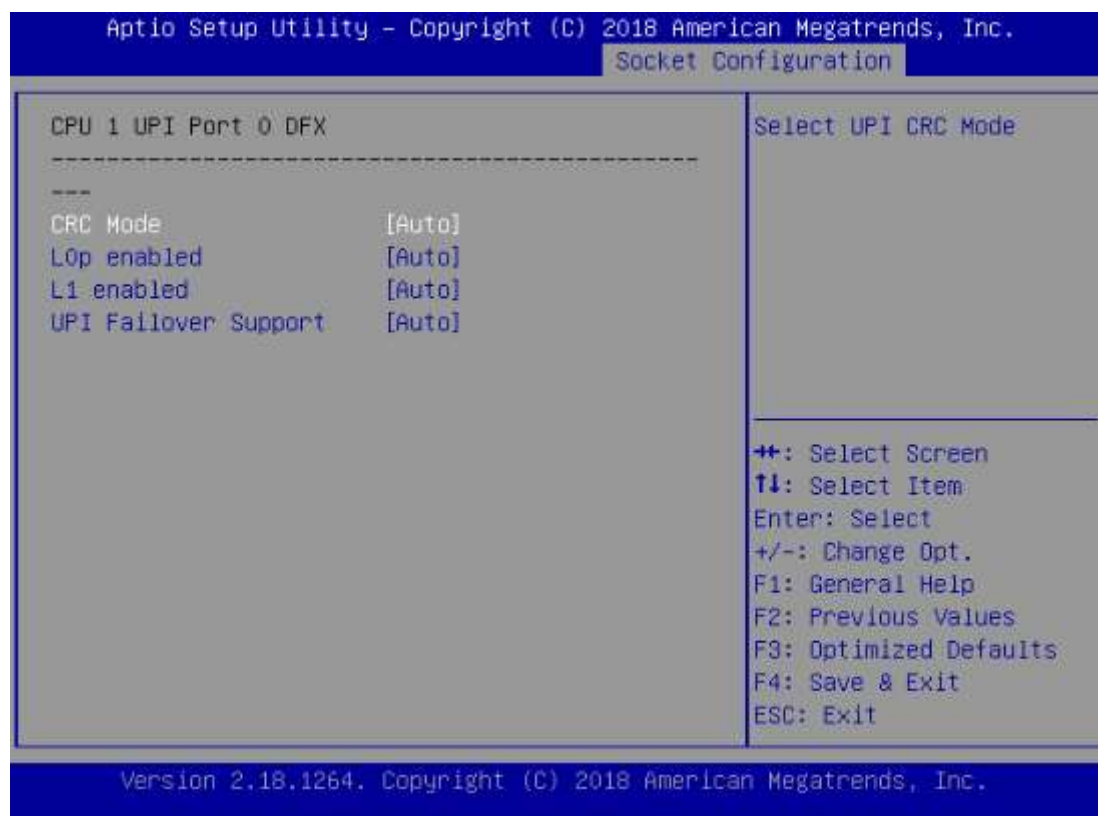
Item	Type	Options	Function description
CPU 1	Static text	N/A	
CPU 1 UPI Port 0	Submenu	N/A	CPU 1 UPI Port 0 Configuration
CPU 1 UPI Port 0 DFX	Submenu	N/A	CPU 1 UPI Port 0 DFX Configuration
CPU 1 UPI Port 1	Submenu	N/A	CPU 1 UPI Port 1 Configuration
CPU 1 UPI Port 1 DFX	Submenu	N/A	CPU 1 UPI Port 1 DFX Configuration
CPU 1 UPI Port 2	Submenu	N/A	CPU 1 UPI Port 2 Configuration
CPU 1 UPI Port 2 DFX	Submenu	N/A	CPU 1 UPI Port 2 DFX Configuration
Bus Resources Allocation Ratio	Numeric item	0,1*,2~8	Bus resources allocation ratio, range 0 to 8

4.5.3.2.2.1 CPU 1 UPI Port 0



Item	Type	Options	Function description
CPU 1 UPI Port 0	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

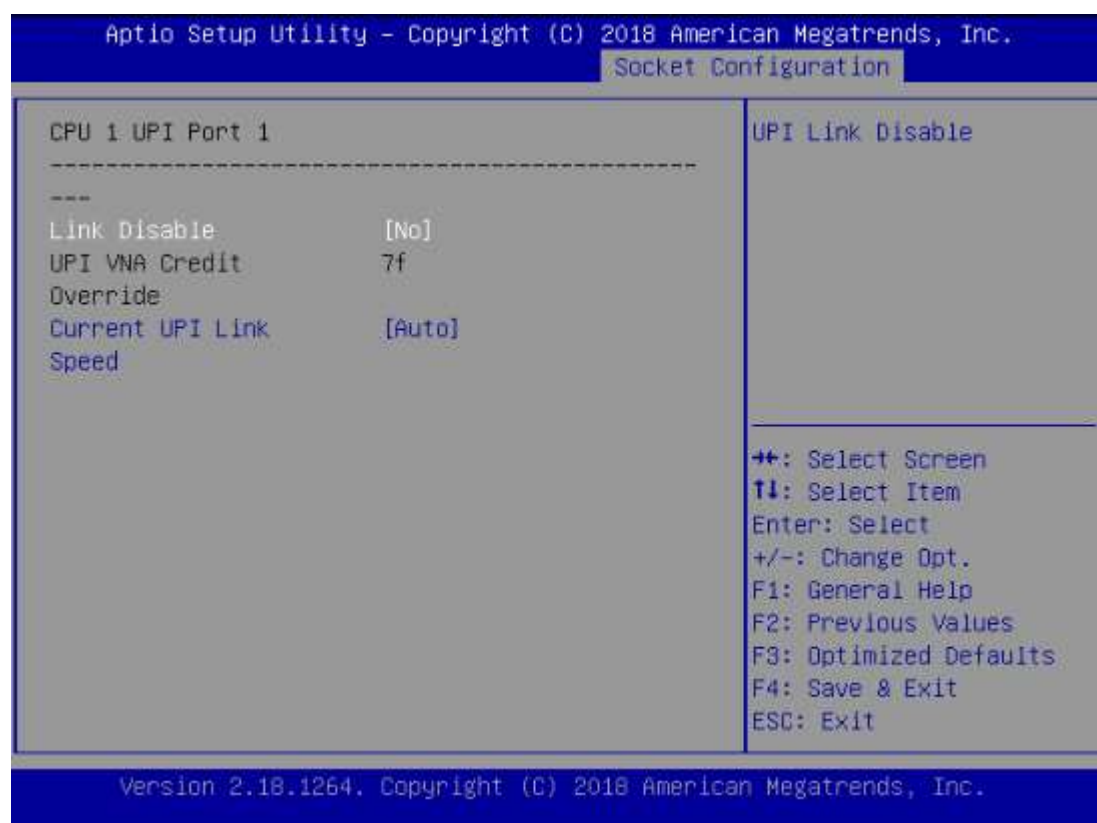
4.5.3.2.2.2 CPU 1 UPI Port 0 DFX



Item	Type	Options	Function description
CPU 1 UPI Port 0 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L1.

UPI Failover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Failover
----------------------	----------------	-------------------------------------	-------------------

4.5.3.2.2.3 CPU 1 UPI Port 1



Item	Type	Options	Function description
CPU 1 UPI Port 1	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

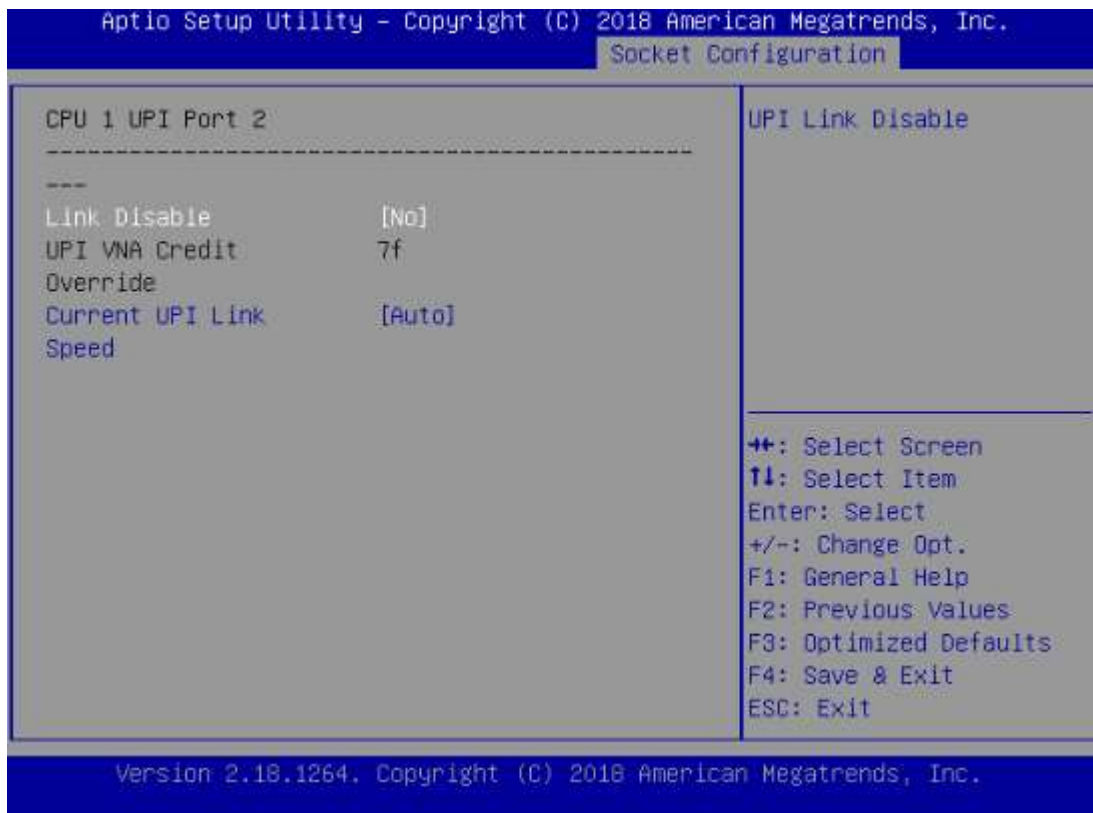
4.5.3.2.2.4 CPU 1 UPI Port 1 DFX



Item	Type	Options	Function description
CPU 1 UPI Port 1 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the

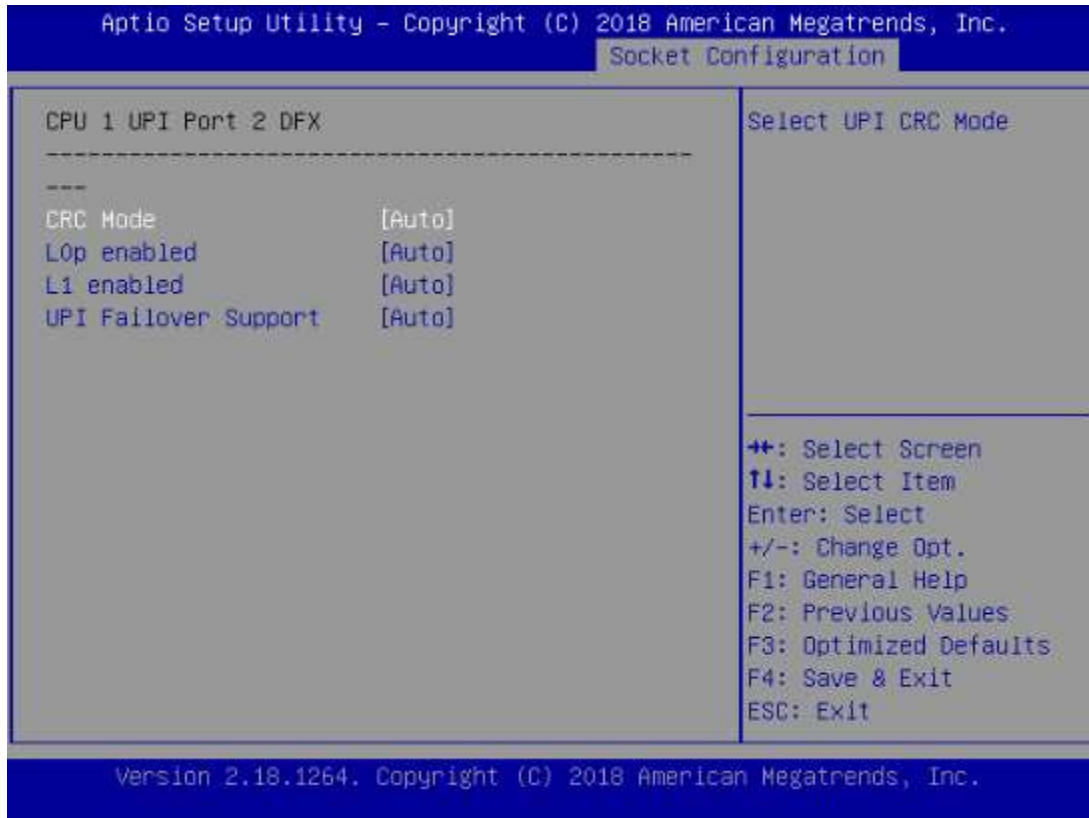
			connected port to determine if the link may enter L1.
UPI Failover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Failover

4.5.3.2.2.5 CPU 1 UPI Port 2



Item	Type	Options	Function description
CPU 1 UPI Port 2	Static text	N/A	
Link Disable	Multipart item	<No>* <Yes>	UPI Link Disable
UPI VNA Credit Override	Static text	7f	
Current UPI Link Speed	Multipart item	< 9.6GB/s> < 10.4GB/s> < Auto>*	Allows for selecting the UPI Link Frequency

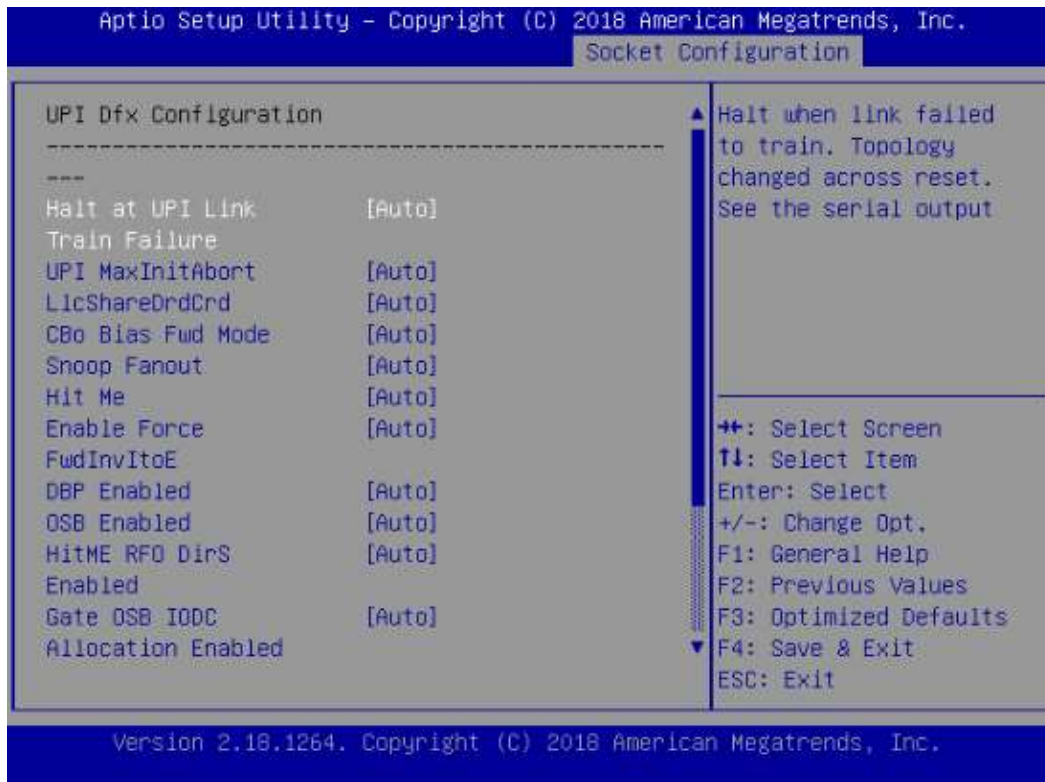
4.5.3.2.2.6 CPU 1 UPI Port 2 DFX



Item	Type	Options	Function description
CPU 1 UPI Port 2 DFX	Static text	N/A	
CRC Mode	Multipart item	<16 Bit CRC > <32 Bit Rolling CRC> <Auto>*	Select UPI CRC Mode
L0p enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L0p mode at transmitter which will be ANDed together with the exchanged value of the connected port to determine if the link may enter L0p.
L1 enabled	Multipart item	< Disable> < Enable> < Auto>*	Enable/Disable per port L1 which will be ANDed together with the exchanged value of the

			connected port to determine if the link may enter L1.
UPI Failover Support	Multipart item	< Disable> < Enable> < Auto>*	UPI Data Failover

4.5.3.3 UPI Dfx Configuration



Item	Type	Options	Function description
UPI Dfx Configuration	Static text	N/A	
Halt at UPI Link Train Failure	Multipart item	< Disable> < Enable> < Auto>*	Halt when link failed to train. Topology changed across reset. See the serial output
UPI MaxInitAbort	Multipart item	< Disable> < Enable> < Auto>*	UPI MaxInitAbort
LlcShareDrdCrd	Multipart item	< Disable> < Enable> < Auto>*	Enable migration from SF to LLC and to leave shared lines in the LLC for <u>Drd</u> and <u>Crd</u> : Enable (1), Disable (0), Auto
CBo Bias <u>Fwd</u> Mode	Multipart item	< Mode0> < Mode1> < Mode2> < Mode3> < Mode4> < Auto>*	0 - Mode 0 (<u>Fwd</u> only when <u>Hom</u> != <u>Req</u> , Default); 1 - Mode 1 (<u>Fwd</u> when <u>Hom</u> != <u>Req</u> & <u>Hom</u> != Local); 2 - Mode 2 (Disable Bias <u>Fwd</u>)

Snoop <u>Fanout</u>	Multip art item	< Disable> < Enable> < Auto>*	Snoop <u>Fanout</u>
Hit Me	Multip art item	< Disable> < Enable> < Auto>*	CHA HitME Cache Enable
Enable Force FwdInvltoE	Multip art item	< Disable> < Enable> < Auto>*	Enable Force FwdInvltoE
DBP Enabled	Multip art item	< Disable> < Enable> < Auto>*	DBP Enabled
OSB Enabled	Multip art item	< Disable> < Enable> < Auto>*	OSB Enabled
HitME RFO DirS Enabled	Multip art item	< Disable> < Enable> < Auto>*	Enable HitME DIR=S RFO optimization
Gate OSB IODC Allocation Enabled	Multip art item	< Disable> < Enable> < Auto>*	When OSB indicates that there aren't enough snoop credits don't allocate IODC entry.
Dual Link Interleave Mode	Multip art item	< Enable CHA interleaving (disable SNC, XOR-based Intlv)> < Disable D2C> < Auto>*	Only valid in 2 Socket 2 Link Topology
DfxSystemDe gradeMode	Multip art item	< Degrade_to_1S> <Degrade_to_Supported>* < No_Degrade>	System topology degrade mode options.
VN1	Multip art item	< Disable> < Enable> < Auto>*	VN1
Direct To Core (D2C)	Multip art item	< Disable> < Enable> < Auto>*	Direct To Core (D2C)
Direct To UPI (D2K)	Multip art item	< Disable> < Enable> < Auto>*	Direct To UPI (D2K)

4.5.4 Memory Configuration

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
<pre> ----- --- Integrated Memory Controller (iMC) ----- ---</pre>	
Enforce POR	[Auto]
PPR Type	[Auto]
PPR Error Injection test	[Disable]
Memory Frequency	[Auto]
IMC BCLK	[Auto]
MRC Promote Warnings	[Enable]
Promote Warnings	[Enable]
Halt on mem Training Error	[Enable]
Multi-Threaded MRC	[Auto]
▲ Enable - Enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

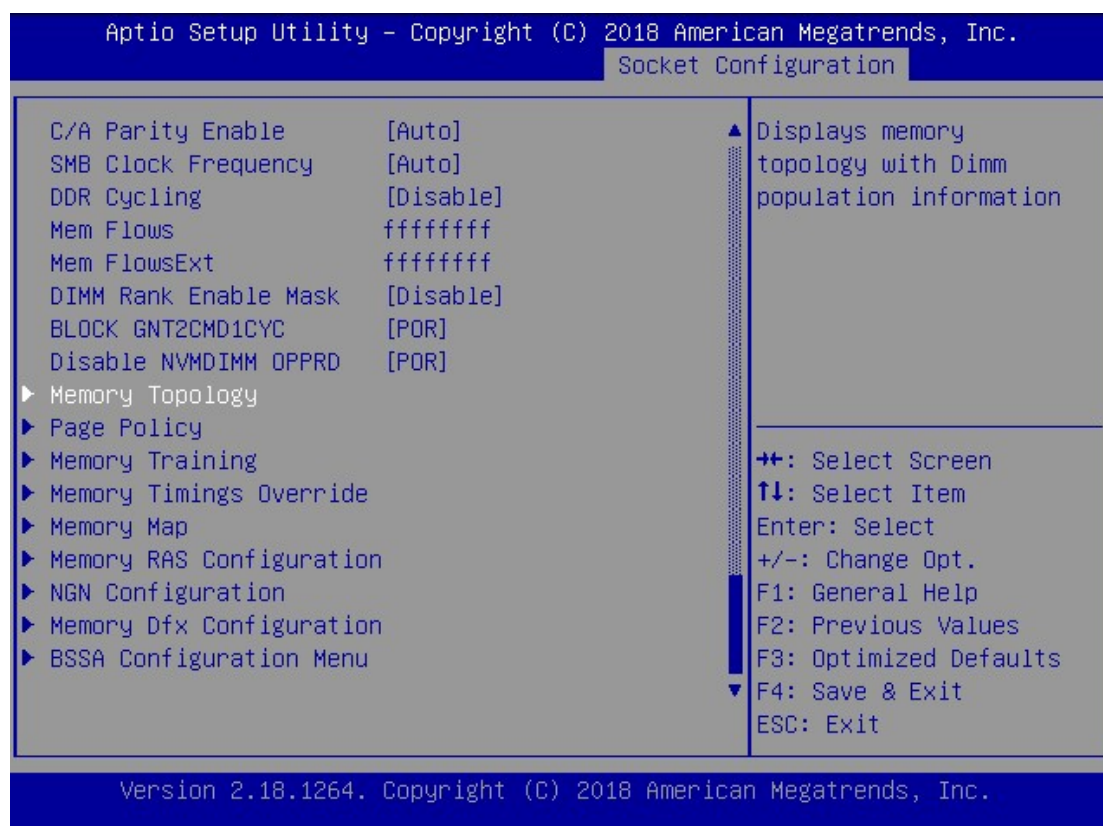
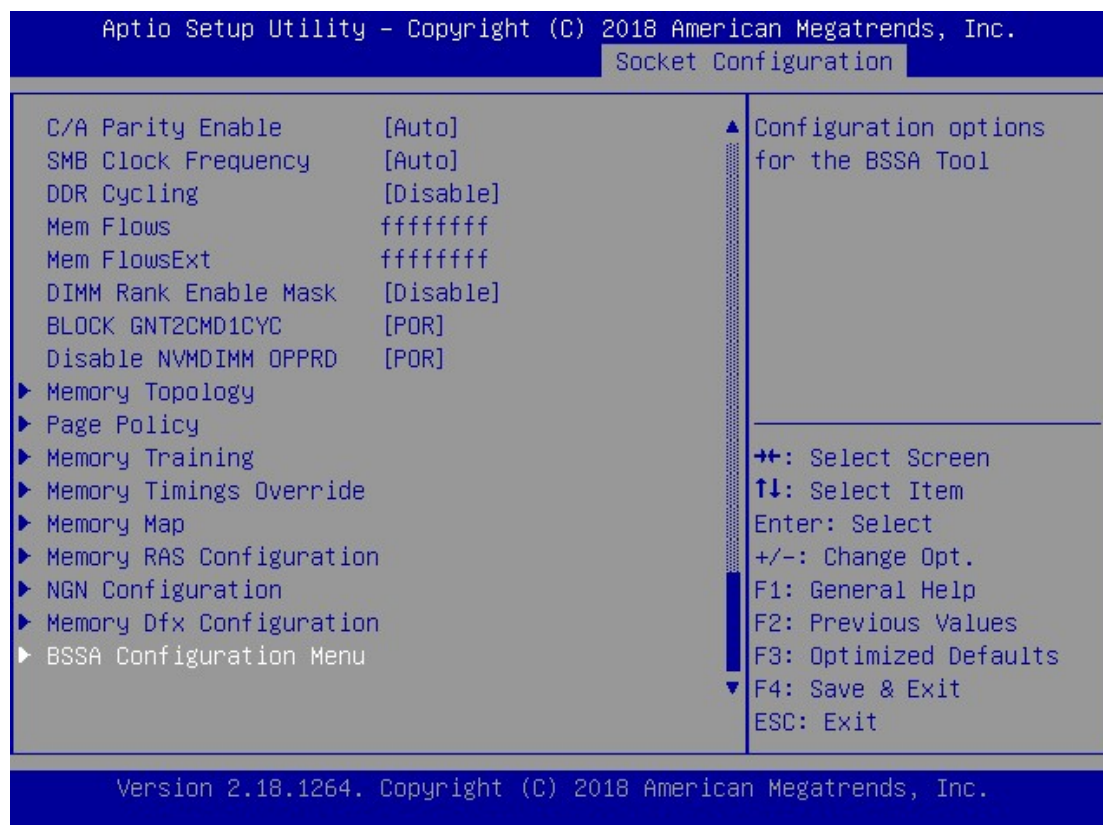
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
SPD CRC Check	[Auto]
Enhanced Log Parsing	[Disable]
LRDIMM Module Delay	[Auto]
MemTest	[Auto]
MemTestLoops	1
Memory Type	[UDIMMs and RDIMMs]
Rank Margin Tool	[Disable]
Backside RMT	[Auto]
Backside CMD RMT	[Disable]
RMT Pattern Length	32767
RMT Pattern Length	32767
CMD CTL VREF	
Per Bit Margin	[Auto]
NVMDIMM BCOM	[Disable]
Margining Support	
Attempt Fast Boot	[Auto]
Attempt Fast Cold Boot	[Auto]
▲ Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
MemTest On Fast Boot	[Auto]	▲ Enables/Disables Automatic resotring of NVDIMMs
RMT On Cold Fast Boot	[Auto]	
BDAT	[Disable]	
Data Scrambling for NVMDIMM	[Enable]	
Data Scrambling for DDR4	[Auto]	
Allow Correctables	[Auto]	
WR CRC feature Control	[Auto]	
DIMM Isolation Enable	[Auto]	
Scrambling Seed Low	41003	
Scrambling Seed High	54165	
Enable ADR	[Enable]	⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Legacy ADR Mode	[Disable]	
ADR Data Save Mode	[NVDIMMs]	
Erase-Arm NVDIMMs	[Enable]	
Restore NVDIMMs	[Enable]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
Interleave NVDIMMs	[Disable]	▲ DDR4 training options
Custom Refresh Enable	[Disable]	
MC BGF threshold	0	
DLL Reset Test	0	
Opp read during WMM	[Auto]	
Normal Operation	400	
Duration		
C/A Parity Enable	[Auto]	
SMB Clock Frequency	[Auto]	
DDR Cycling	[Disable]	
Mem Flows	ffffffff	⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Mem FlowsExt	ffffffff	
DIMM Rank Enable Mask	[Disable]	
BLOCK GNT2CMD1CYC	[POR]	
Disable NVMDIMM OPPRD	[POR]	
▶ Memory Topology		
▶ Page Policy		
▶ Memory Training		

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.



Item	Type	Options	Function description
Integrated Memory Controller (iMC)	Static text	N/A	
Enforce POR	Multipart item	<Auto>* <Enforce POR> <Disable>	Enable - Enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
PPR Type	Multipart item	<Auto>* <Hard PPR> <Soft PPR> <PPR Disabled>*	Selects Post Package Repair Type - Hard / Soft / Disabled. Auto - Sets it to the MRC default setting; current default is Disabled.
PPR Error Injection test	Multipart item	<Disable>* <Enable>	Enable / Disable support for c-script err inj test
Memory Frequency	Multipart item	<Auto>* <800> <1066> <1200> <1333> <1400> <1600> <1800> <1866> <2000> <2133> <2200> <2400> <2600> <2666> <2800-OvrClk> <2933-OvrClk> <3000-OvrClk> <3200-OvrClk> <3400-OvrClk>	Maximum Memory Frequency Selections in Mhz. Do not select Reserved

		<3466-OvrClk> <3600-OvrClk> <3733-OvrClk> <3800-OvrClk> <4000-OvrClk> <4200-OvrClk> <4266-OvrClk> <4400-OvrClk>	
IMC BCLK	Multipar t item	<Auto>* <100MHz> <133MHz>	Auto, 100MHz or 133MHz
MRC Promote Warnings	Multipar t item	<Disable> <Enable>*	Determines if MRC warnings are promoted to system level
Promote Warnings	Multipar t item	<Disable> <Enable>*	Determines if warnings are promoted to system level
Halt on mem Training Error	Multipar t item	<Disable> <Enable>*	Halt on mem Training Error Disable/Enable
Multi-Threaded MRC	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Executes the Memory Reference Code multi-threaded. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable.
SPD CRC Check	Multipar t item	<Auto>* <Disable> <Enable>	Enable to turn on checking the SPD CRC
Enhanced Log Parsing	Multipar t item	<Disable>* <Enable>	Enables additional output in debug log for easier machine parsing
LRDIMM Module Delay	Multipar t item	<Disable> <Auto>*	When Disabled, MRC will not use SPD bytes 90-95 for LRDIMM Module Delay. When Auto, MRC will boundary check the values and use default values, if SPD is 0 or out of range
MemTest	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables memory test during normal boot. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable.
MemTestLoops	Dynamic text	1* 0-65535	Number of memory test loops during normal boot, set to 0 to run memtest

			infinitely
Memory Type	Multipar t item	< RDIMMs only > < UDIMMs only > < UDIMMs and RDIMMs >*	Selects the Memory type supported by this platform.
Rank Margin Too	Multipar t item	<Disable>* <Enable>	Enable - Enables the legacy rank margin tool to run after DDR4 memory training. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable. Should be disabled in production releases.
Backside RMT	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables the legacy Backside Rank Margin Tool. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable. Should be disabled for production releases.
Backside CMD RMT	Multipar t item	<Disable>* <Enable>	Enables the Backside CMD RMT
RMT Pattern Length	Dynamic text	32767* 1-9000000	Sets the pattern length for the Rank Margin Tool
RMT Pattern Length CMD CTL VREF	Dynamic text	32767* 1-9000000	Sets the pattern length for the Rank Margin Tool (CMD CTL VREF step)
Per Bit Margin	Multipar t item	<Auto>* <Disable> <Enable>	Sets the pattern length for the Rank Margin Tool (CMD CTL VREF step)
NVMDIMM BCOM Margining Support	Multipar t item	<Disable>* <Enable>	Enables NVMDIMM BCOM margining support for RMT and BSSA
Attempt Fast Boot	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature. Auto - Sets it to the MRC

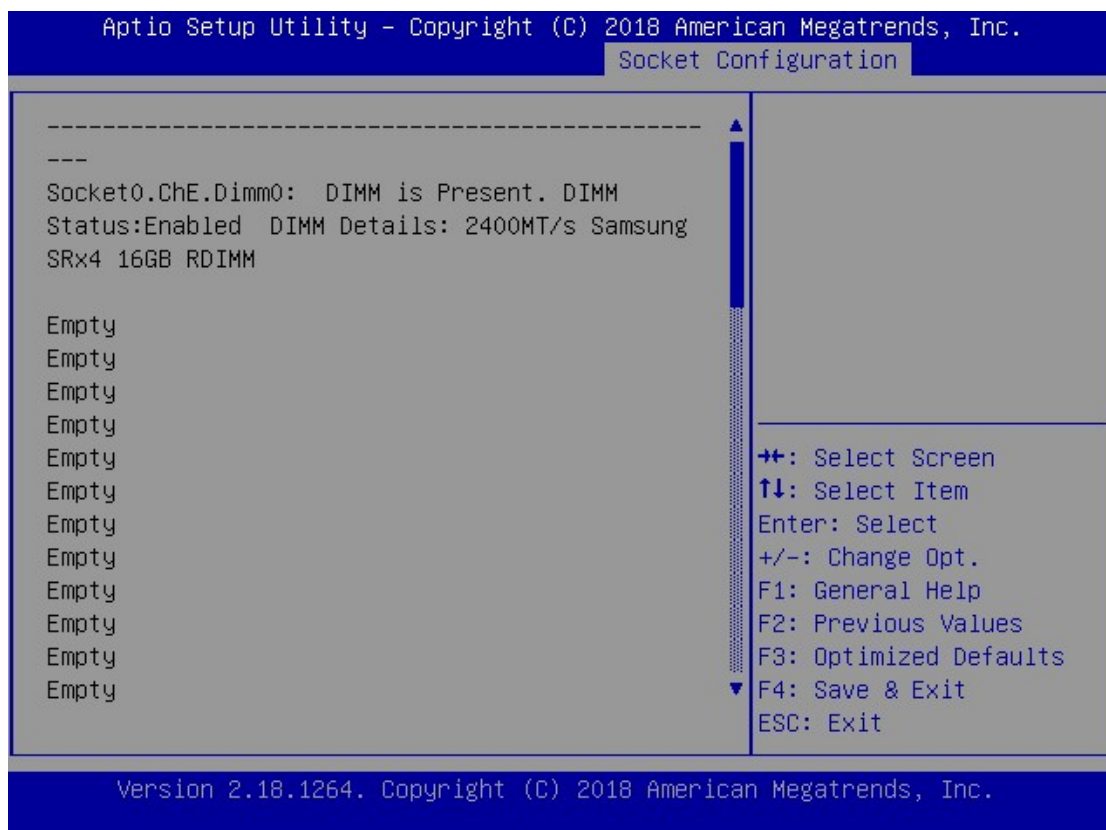
			default setting; current default is Disable.
Attempt Fast Cold Boot	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Disable.
MemTest On Fast Boot	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables memory test during fast boot. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Disable.
RMT On Cold Fast Boot	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables Rank Margin Tool on Cold Fast Boot. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable. Should be disabled in production releases.
BDAT	Multipar t item	<Disable>* <Enable>	Enable Disables BDAT
Data Scrambling for NVMDIMM	Multipar t item	<Auto> <Disable> <Enable>*	Enable - Enables data scrambling for NVMDIMM. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
Data Scrambling for DDR4	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables data scrambling for DDR4. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
Allow Correctables	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Allows correctable errors during memory training. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
WR CRC feature Control	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables Write CRC. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current

			default is Disable.
DIMM Isolation Enable	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables DIMM Isolation for Command/Address Parity and Write CRC. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
Scrambling Seed Low	Dynamic text	41003* 0-65535	Low 32 bits of the scrambling seed
Scrambling Seed High	Dynamic text	54165* 0-65535	High 32 bits of the scrambling seed
Enable ADR	Multipar t item	<Disable> <Enable>*	Enables the detecting and enabling of ADR
Legacy ADR Mode	Multipar t item	<Disable>* <Enable>	Enable/Disable Legacy ADR Mode
ADR Data Save Mode	Multipar t item	<Disable> <Batterybacked DIMMs> <NVDIMMs>	Data Save Mode for ADR. Batterybacked or Type 01 NVDIMM
Erase-Arm NVDIMMs	Multipar t item	<Disable> <Enable>*	Enables/Disables Erasing and Arming NVDIMMs
Restore NVDIMMs	Multipar t item	<Disable> <Enable>*	Enables/Disables Automatic resotring of NVDIMMs
Interleave NVDIMMs	Multipar t item	<Disable>* <Enable>	Controls if NVDIMMs are interleaved together or not
Custom Refresh Enable	Multipar t item	<Disable>* <Enable>	Enable/disable a custom memory refresh rate
MC BGF threshold	Dynamic text	0* 0-15	The HA to MC BGF threshold is used for scheduling MC request in bypass condition.
DLL Reset Test	Dynamic text	0* 0-0xFF	Set this to the number of loops to execute the DDL reset test. The test will execute RMT for the provided number of loops without DLL resets and then it will exectue RMT for the same number of loops with DLL resets.
Opp read during WMM	Multipar t item	<Auto>* <Disable>	Enable - Enables issuing read commands opportunistically during

		<Enable>	Write Major Mode. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
Normal Operation Duration	Dynamic text	1024 0-0xFFFF	Set normal operation duration interval (0 - 65535)
C/A Parity Enable	Multipar t item	<Auto>* <Disable> <Enable>	Enable - Enables DDR4 Command Address Parity. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.
SMB Clock Frequency	Multipar t item	<Auto>* <100 Khz> <400 Khz> <1 Mhz>	Sets DDR4 SMBus Clock Frequencies For SPD Access. Auto - Sets it to the MRC default setting; current default is 400K.
DDR Cycling	Multipar t item	<Disable>* <Enable>	When enabled, MRC will train the memory and then power cycle over and over to stress MRC
Mem Flows	Dynamic text	0xFFFFFFFF 0-0xFFFFFFFF	Enable(1)/Disable(0) memory training steps in MRC flow; X_OVER-BIT0; SENSE_AMP-BIT1; E_CMDCLK-BIT2; REC_EN-BIT3; RD_DQS-BIT4; WR_LVL-BIT5; WR_FLYBY-BIT6; WR_DQ-BIT7; CMDCLK-BIT8; RD_ADV-BIT9; WR_ADV-BIT10; RD_VREF-BIT11; WR_VREF-BIT12; RT_OPT-BIT13; RX_DESKEW-BIT14; TX_DESKEW-BIT14; TX_EQ-BIT15; IMODE-BIT16; EARLY_RID-BIT17; DQ_SWIZ-BIT18; LRBUF_RD-BIT19; LRBUF_WR-BIT20; RANK_MARGIN-BIT21; EARLY_WR_VREF-BIT22; EARLY_RD_VREF-BIT23; LR_RD_VREF-BIT24; MEM_INIT-BIT25; FNVSIMICSSIM_EN-BIT26; NORMAL_MODE-BIT27; CMD_VREF-BIT28; LR_WR_VREF-BIT29; MEMTEST-BIT30; E_CTLCLK-BIT31

Mem FlowsExt	Dynamic text	0xFFFFFFFF 0-0xFFFFFFFF	Enable(1)/Disable(0) memory training steps in MRC flow; RX_CTL-BIT0; PXC-BIT1; CMD_NORM-BIT2; BIOS_SSA_RMT-BIT3; MC_ODT-BIT4; MC_RON-BIT5; DIMM_RON-BIT6; RTT_WRT-BIT7; NONTGT_ODT-BIT8
DIMM Rank Enable Mask	Multipart item	<Disable>* <Enable>	Selects ranks to enable/disable per DIMM
BLOCK GNT2CMD1CYC	Multipart item	<PO Safe Value> <POR>*	Enable\Disable BLOCK GNT2CMD1CYC
Disable NVMDIMM OPPRD	Multipart item	<PO Safe Value> <POR>*	Enable\Disable Disable NVMDIMM OPPRD
Memory Topology	Submenu	N/A	Displays memory topology with Dimm population information
Page Policy	Submenu	N/A	Set memory page policy parameters
Memory Training	Submenu	N/A	DDR4 training options
Memory Timings Override	Submenu	N/A	Selects the XMP profile to use
Memory Map	Submenu	N/A	Set memory mapping settings
Memory RAS Configuration	Submenu	N/A	Displays and provides option to change the Memory Ras Settings
NGN Configuration	Submenu	N/A	Displays and provides option to change the NGN settings
Memory Dfx Configuration	Submenu	N/A	Displays and provides option to change the Memory Dfx Settings
BSSA Configuration Menu	Submenu	N/A	Configuration options for the BSSA Tool

4.5.4.1 Memory Topology



Show DIMM Topology information

4.5.4.2 Page Policy

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

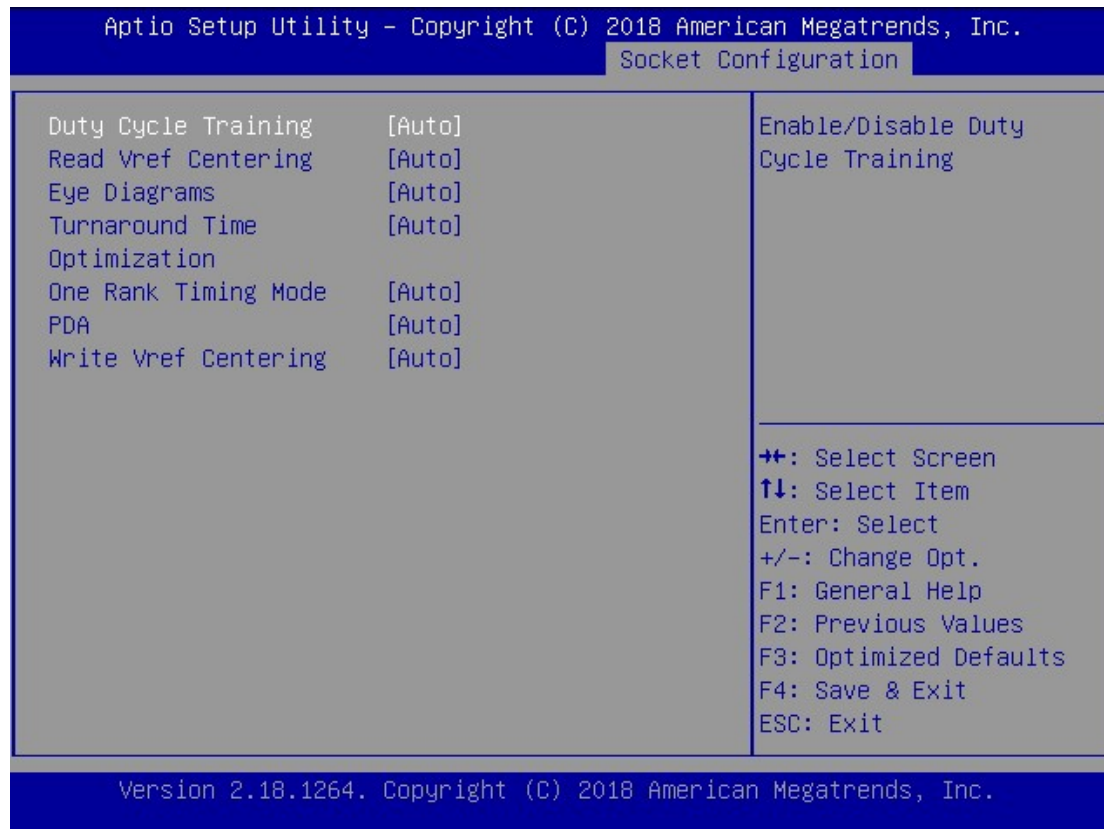
Socket Configuration

Page Policy	[Auto]	Select Page Policy
		⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
Page Policy	Multipart item	<Auto> < Closed > < Adaptive >	Select Page Policy

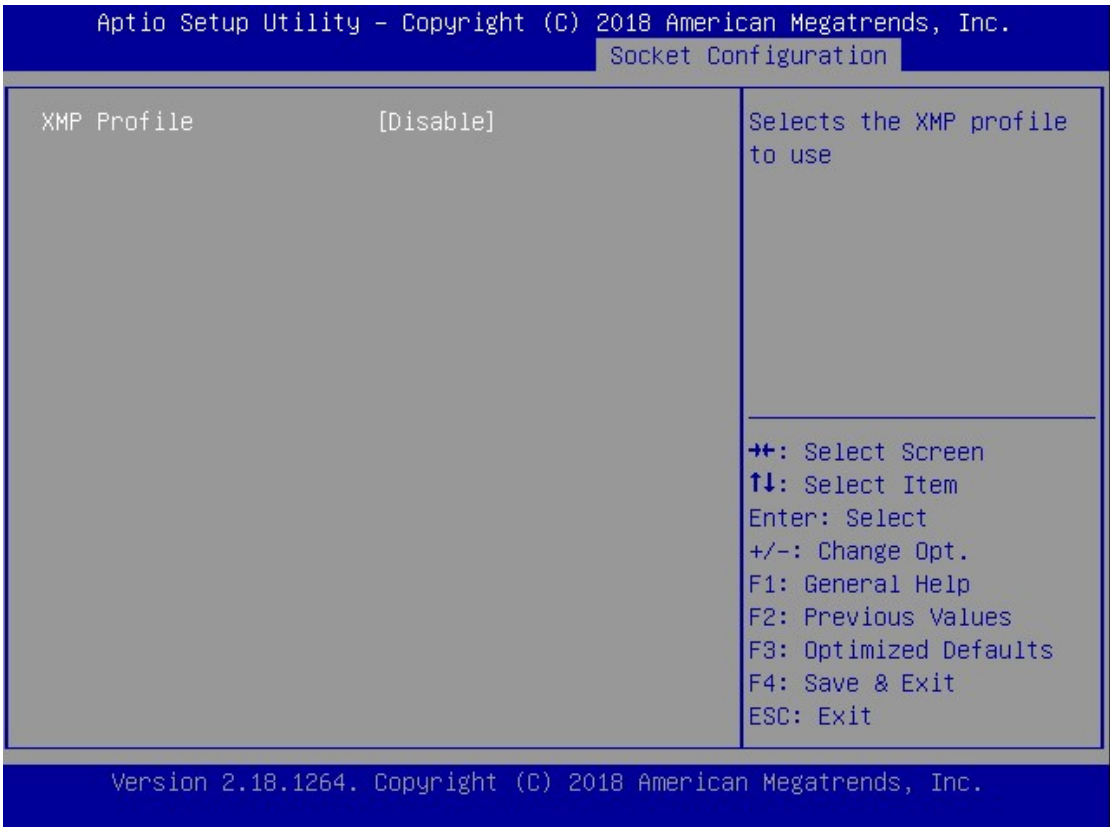
4.5.4.3 Memory Training



Item	Type	Options	Function description
Duty Cycle Training	Multipart item	<Auto>* < Disable > < Enable >	Enable/Disable Duty Cycle Training
Read Vref Centering	Multipart item	<Auto>* < Disable > < Enable >	Read Vref Centering Disable/Enable
Eye Diagrams	Multipart item	<Auto>* < Disable > < Enable >	Enables Rx and Tx Dq eye diagrams for each rank
Turnaround Time Optimization	Multipart item	<Auto>* < Disable > < Enable >	Enables optimal turnaround times
One Rank Timing Mode	Multipart item	<Auto>* < Disable > < Enable >	LRDIMM One Rank Timing Mode turnaround time optimization
PDA	Multipart item	<Auto>* < Disable >	Enables Per DRAM Addressing

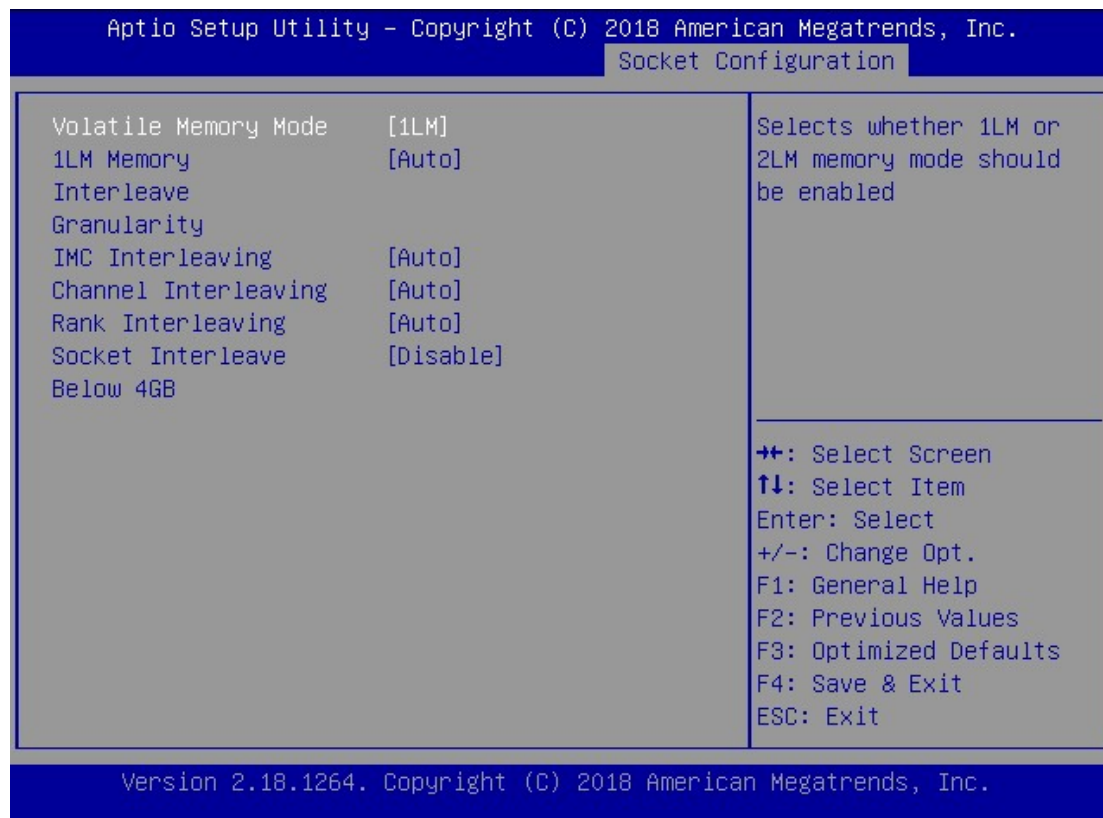
		< Enable >	
Write Vref Centering	Multipart item	<Auto>* < Disable > < Enable >	Write Vref Centering Disable/Enable

4.5.4.4 Memory Timings Override



Item	Type	Options	Function description
XMP Profile	Multipart item	< Disable >* < Enable >	Selects the XMP profile to use

4.5.4.5 Memory Map



Item	Type	Options	Function description
Volatile Memory Mode	Multipart item	< 1LM >* < 2LM > <AUTO>	Selects whether 1LM or 2LM memory mode should be enabled
1LM Memory Interleave Granularity	Multipart item	<AUTO>* <256B Target, 256B Channel> <64B Target, 64B Channel>	Selects the 1LM memory interleave granularity
IMC Interleaving	Multipart item	<AUTO>* <1-way Interleave> <2-way Interleave>	Select IMC Interleaving setting
Channel Interleaving	Multipart item	<AUTO>* <1-way Interleave> <2-way Interleave> <3-way Interleave>	Select Channel Interleaving setting
Rank Interleaving	Multipart item	<AUTO>* <1-way Interleave>	Select Rank Interleaving setting

		<2-way Interleave> <4-way Interleave> <8-way Interleave>	
Socket Interleave Below 4GB	Multipart item	< Disable > * < Enable >	Splits the 0-4GB address space between two sockets, so that both sockets get a chunk of local memory below 4GB

4.5.4.6 Memory RAS Configuration

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

Socket Configuration

 Memory RAS Configuration Setup

Static Virtual Lockstep Mode	[Disable]	▲ Enable Static Virtual Lockstep mode
Mirror mode	[Disable]	
Mirror TADO	[Disable]	
Enable Partial Mirror	[Disable]	
UEFI ARM Mirror	[Disable]	
Memory Rank Sparing	[Disable]	
ECC Error Threshold	[1000]	
ECC Error Event Log Threshold	[10]	
SDDC Plus One	[Disable]	▼

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Socket Configuration

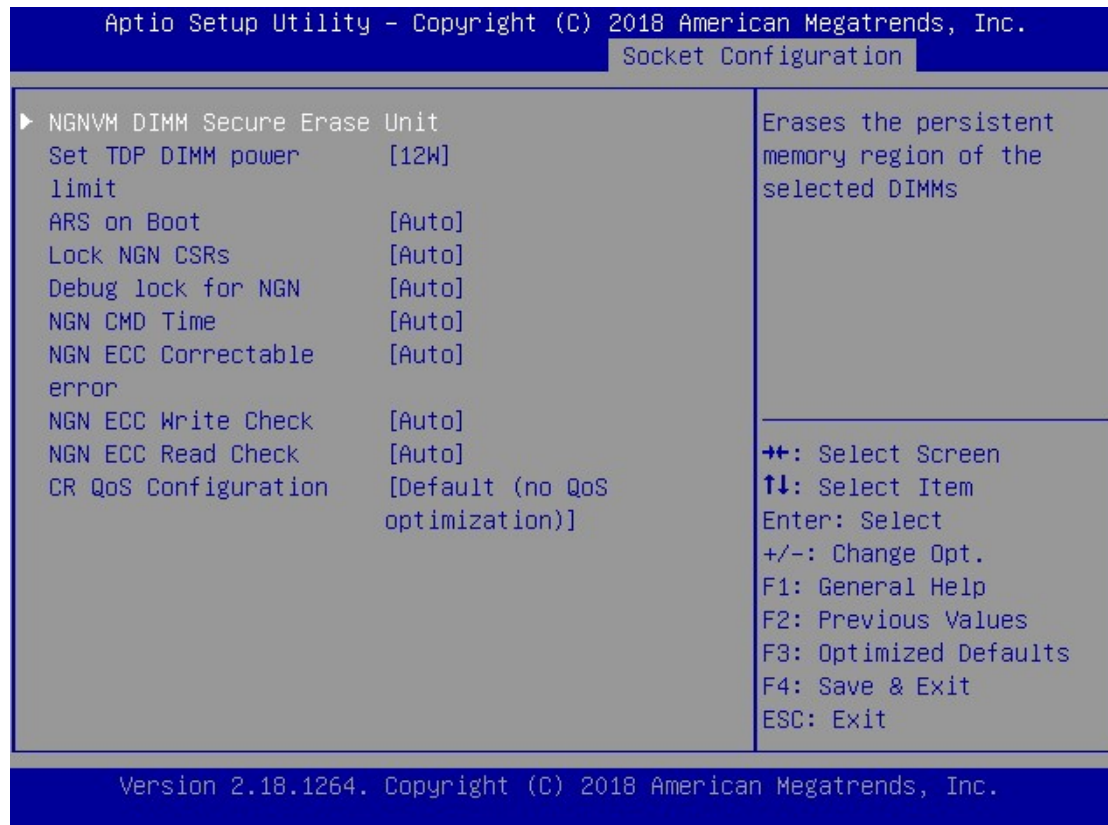
Mirror mode	[Disable]	▲ Selects the address mode between System Physical Address (or) Reverse Address
Mirror TADO	[Disable]	
Enable Partial Mirror	[Disable]	
UEFI ARM Mirror	[Disable]	
Memory Rank Sparing	[Disable]	
ECC Error Threshold	[1000]	
ECC Error Event Log Threshold	[10]	
SDDC Plus One	[Disable]	
ADDDC Sparing	[Disable]	
Set NGN Die Sparing	[Enable]	
NGN Die Sparing	128	
Aggressiveness		
Patrol Scrub	[Enable]	
Patrol Scrub Interval	24	
Patrol Scrub Address Mode	[System Physical Address]	▼

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
Static Virtual Lockstep Mode	Multipart item	< Disable >* < Enable >	Enable Static Virtual Lockstep mode
Mirror mode	Multipart item	< Disable >* < Mirror Mode 1LM> < Mirror Mode 2LM>	Mirror Mode will set entire 1LM/2LM memory in system to be mirrored, consequently reducing the memory capacity by half. Mirror Enable will disable XPT Prefetch
Mirror TAD0	Multipart item	< Disable >* < Enable >	Enable Mirror on entire memory for TAD0
Enable Partial Mirror	Multipart item	< Disable >* < Partial Mirror mode 1LM> < Partial Mirror mode 2LM>	Partial mirror mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Mirror Enable will disable XPT Prefetch
UEFI ARM Mirror	Multipart item	< Disable >* < Enable>	Imitate behavior of UEFI based Address Range Mirror with setup option
Memory Rank Sparing	Multipart item	< Disable >* < Enable>	Enable/Disable Memory Rank Sparing
ECC Error Threshold	Multipart item	<1> <4> <10> <1000>*	Threshold value for logging ECC Error - threshold of 1(default) logs the first ECC error,"1" logs every ECC error.
ECC Error Event Log Threshold	Multipart item	<Disable> <10>* <50> <100>	ECC Error event log threshold in one boot time.
SDDC Plus One	Multipart item	< Disable >* < Enable>	Enable/Disable SDDC Plus One
ADDDC Sparing	Multipart item	< Disable >* < Enable>	Enable/Disable ADDDC Sparing

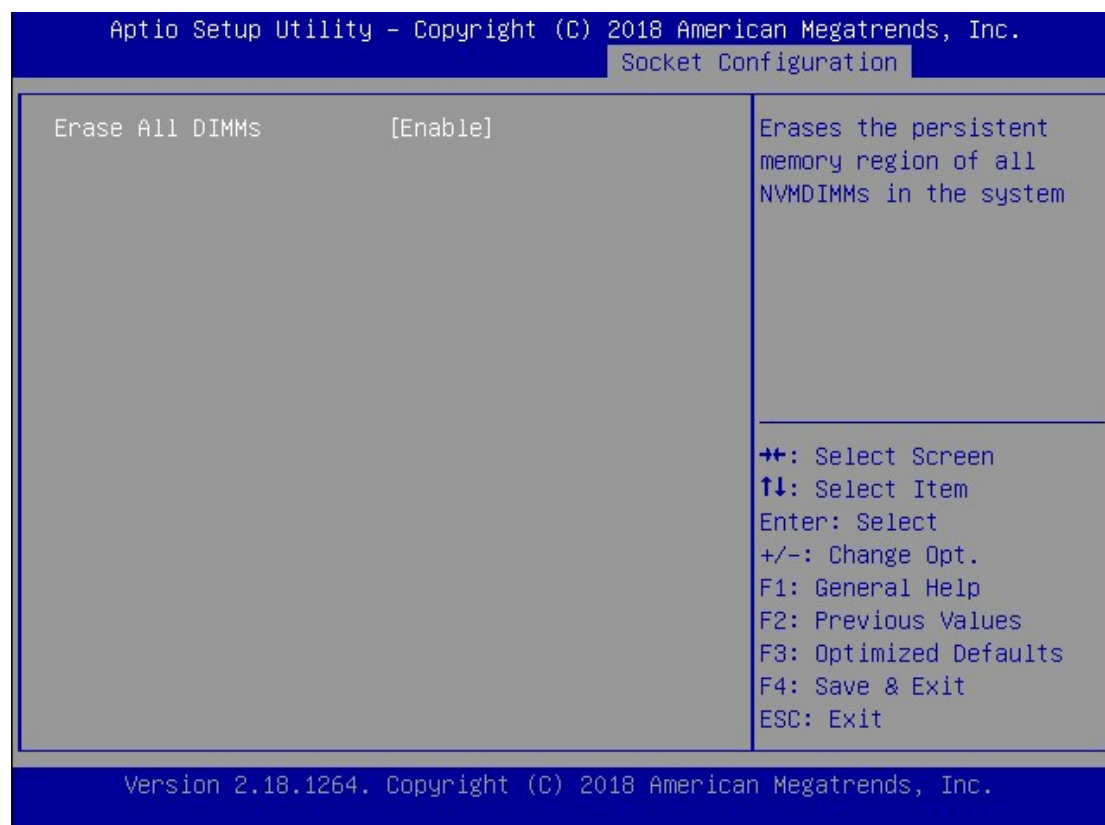
4.5.4.7 NGN Configuration



Item	Type	Options	Function description
NGNVM DIMM Secure Erase Unit	Submenu	N/A	Erases the persistent memory region of the selected DIMMs
Set TDP DIMM power limit	Multipart item	< 10W > < 12W >* < 15W > < 18W >	Sets the current total dissipated DIMM power limit
ARS on Boot	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable Address Range Scrub during boot time
Lock NGN CSRs	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable Lock NGN CSRs
Debug lock for NGN	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable Debug lock for NGN
NGN CMD	Multipart	<Auto>*	Select 1N\2N NGN Command

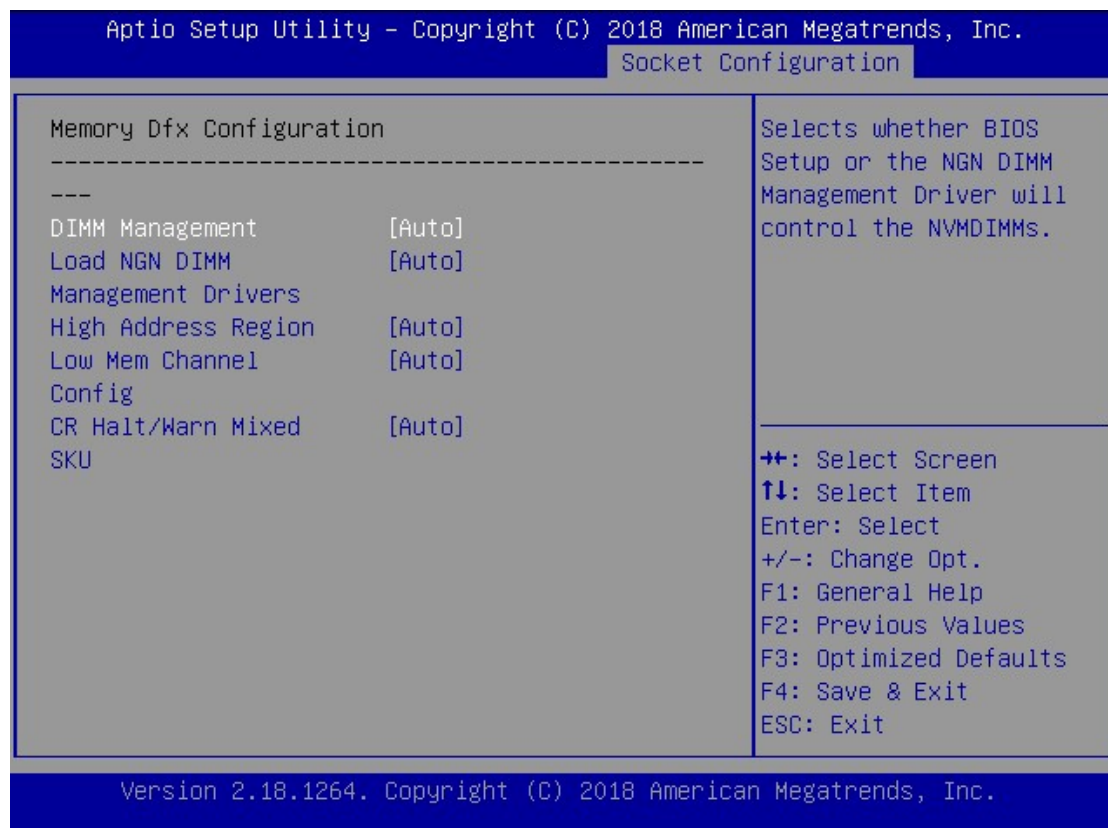
Time	item	<Disable> <Enable>	time
NGN ECC Correctable error	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable NGN ECC Correctable error
NGN ECC Write Check	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable NGN ECC Write Check
NGN ECC Read Chec	Multipart item	<Auto>* <Disable> <Enable>	Enable\Disable NGN ECC Read Check
CR QoS Configuration	Multipart item	<Default (no QoS optimization >* <Option 1> <Option 2> <Option 3> <Option 4> <Option 5>	Select CR QoS Configuration Profiles

4.5.4.8 NGNVM DIMM Secure Erase Unit



Item	Type	Options	Function description
Erase All DIMMs	Multipart item	<Disable>* <Enable>	Erases the persistent memory region of all NVMDIMMs in the system
SxCHy, x=0-3, y=0-5	Multipart item	<Disable>* <Enable>	Erases the persistent memory region of NVMDIMM in Channel 0-2, Memory controller 0-1, Socket 0-7

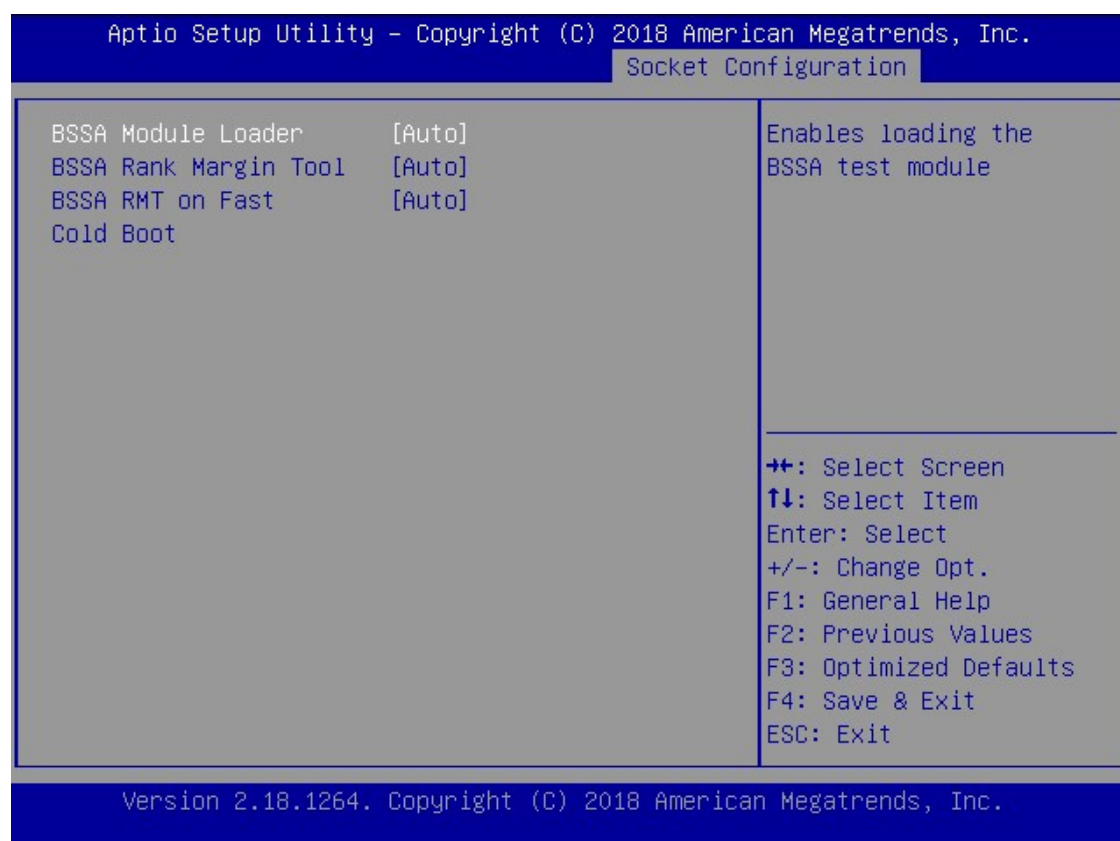
4.5.4.9 Memory Dfx Configuration



Item	Type	Options	Function description
DIMM Management	Multipart item	<Auto>* <BIOS Setup> <NGN DIMM Management Driver>	Selects whether BIOS Setup or the NGN DIMM Management Driver will control the NVMDIMMs.
Load NGN DIMM Management Drivers	Multipart item	<Auto>* <Disable> <Enable>	Enable/Disable to load the NGN DIMM Management Drivers for NVMDIMMs(install the gNfitBindingProtocolGuid).
High Address Region	Multipart item	<Bit Position 33>* <Bit Position 33-45>	High Address Region starting bit position. Auto - 0 (not enabled). Note that the actual start of the region is 2*N - 64MB, where N is the selected bit position.
Low Mem	Multipart	<Auto>*	Select Channel for low

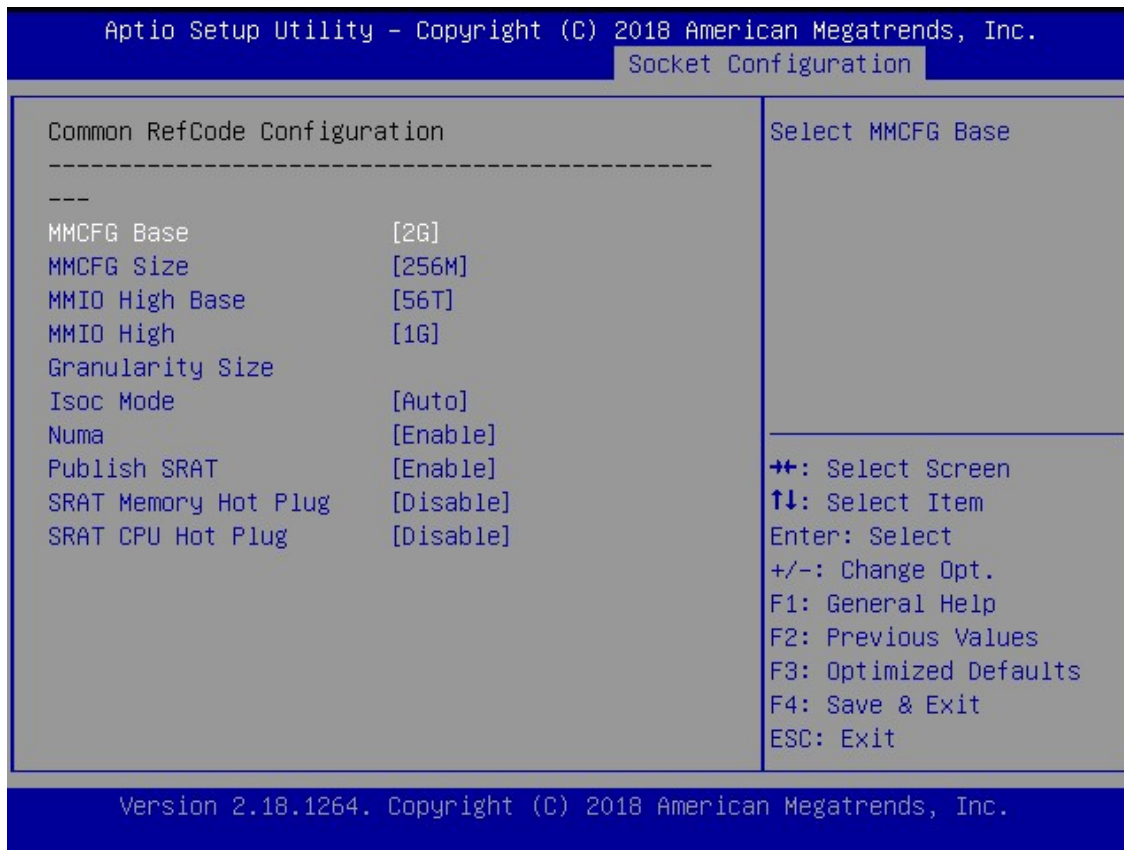
Channel Config	item	< Channel 0 > < Channel 1 > < Channel 2 > < Channel 3 >	memory, Auto - 0 (BIOS select)
CR Halt/Warn Mixed SKU	Multipart item	<Auto>* <Disable> <Enable>	Enable will raise Fatal error and halt the system; Disable will log warning and continue booting to shell/OS

4.5.4.10 BSSA Configuration Menu



Item	Type	Options	Function description
BSSA Module Loader	Multipart item	<Auto>* <Enable> <Disable>	Enables loading the BSSA test module
BSSA Rank Margin Tool	Multipart item	<Auto>* <Enable> <Disable>	Enables the BSSA Rank Margin Tool
BSSA RMT on Fast Cold Boot	Multipart item	<Auto>* <Enable> <Disable>	Enable/Disable the BSSA Rank Margin Tool on a Fast Cold Boot

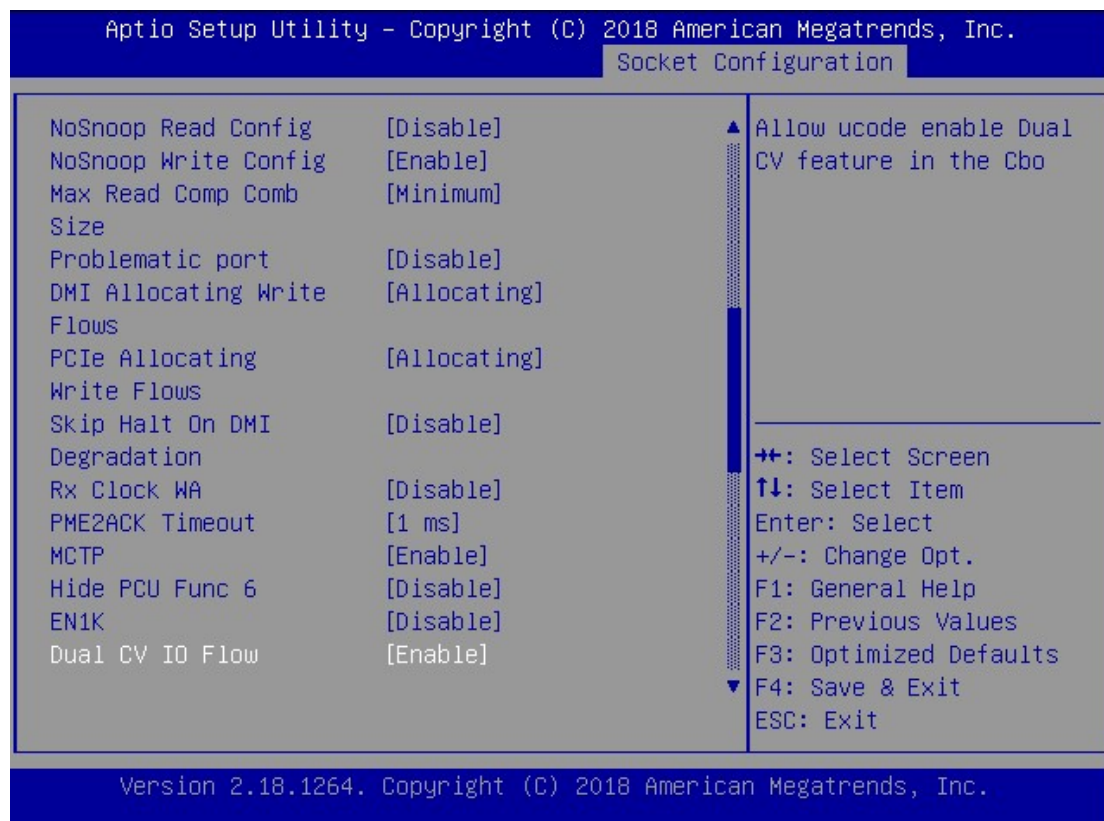
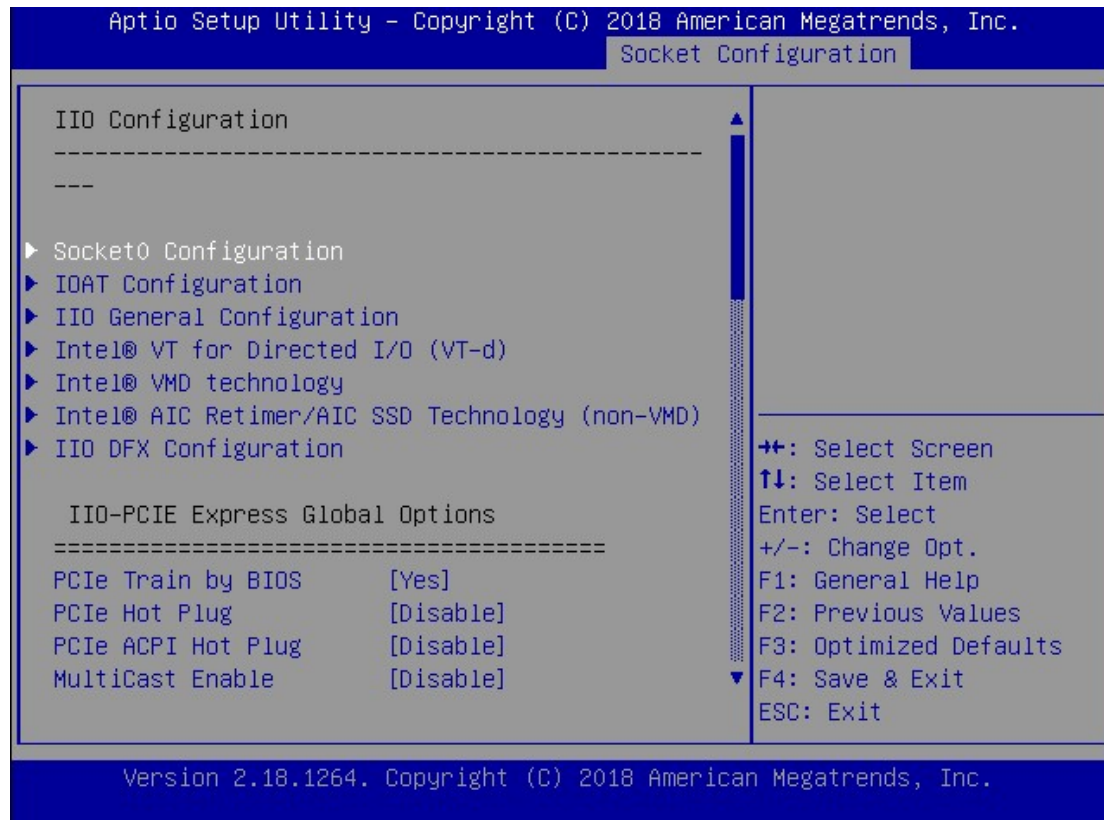
4.5.4.11 Common RefCode Configuration



Item	Type	Options	Function description
MMCFG Base	Multipart item	<1G> <1.5G> <1.75G> <2G>* <2.25G> <3G>	Select MMCFG Base
MMCFG Size	Multipart item	< 64M > <128M> <256M>* <512M> <1G> <2G>	Select MMCFG Size
MMIO High Base	Multipart item	< 56T >* <40T> <24T> <16T> <4T>	Select MMIO High Base

		<1T>	
MMIO High Granularity Size	Multipart item	<1G> <4G> <16G> <64G> <256G> <1024G>	Selects the allocation size used to assign mmioh resources.\nTotal mmioh space can be up to 32xgranularity.\nPer stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.
Isoc Mode	Multipart item	<Auto>* <Disable> <Enable>	Isoc: Disable,Enable
Numa	Multipart item	<Disable>* <Enable>	Enable or Disable Non uniform Memory Access (NUMA).
Publish SRAT	Multipart item	<Disable> <Enable>*	Publish the SRAT ACPI table to the OS.
SRAT Memory Hot Plug	Multipart item	<Disable>* <Enable>	Fix for OS that does not support memory hot plug.\nEx: SuSE SLES10 SP2. \n \nEnable by default. \nDisable will clear all hot plug bits and remove the hot plug entries in SRAT table.
SRAT CPU Hot Plug	Multipart item	<Disable>* <Enable>	Set Processor Flag to Enabled for all processor entries in SRAT.

4.5.5 IIO Configuration



Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
PCIE Coherent Read Partial	[PCIRdCur Setting]	▲ 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 Coherent Read Full	[PCIRdCur Setting]	
PCI-E Completion Timeout (Global)	[No]	
Disable		
PCI-E Global Timeout Value	[260ms to 900ms]	
PCI-E ASPM Support (Global)	[Per-Port]	
PCIE Stop & Scream Support	[Disable]	
Snoop Response Hold Off	9	
PCIE Latency Tolerance Reporting	[Auto]	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
PCI-E ASPM Support (Global)	[Per-Port]	▲ PCIe PHY test mode Enable/Disable
PCIE Stop & Scream Support	[Disable]	
Snoop Response Hold Off	9	
PCIE Latency Tolerance Reporting	[Auto]	
PCIe Extended Tag Enable	[Enable]	
PCIe Atomic Operation Request Support	[Disable]	
PCIe Max Read Request Size	[Auto]	
Pcie Relaxed Ordering	[Enable]	
PCIe PHY test mode	[Disable]	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Item	Type	Options	Function description
IIO configuration	Static text	N/A	option to change the IIO General Settings
Socket0 Configuration	Submenu	N/A	Displays and provides option to change the IIO Settings
IOAT Configuration	Submenu	N/A	All IOAT configuration options
Intel® VT for Directed I/O (VT-d)	Submenu	N/A	Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.
Intel® VMD technology	Submenu	N/A	Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.
Intel® AIC Retimer/AIC SSD Technology (non-VMD)	Submenu	N/A	Press <Enter> to bring up the Intel® AIC Retimer/AIC SSD Configuration menu.
IIO DFX Configuration	Submenu	N/A	Enable/Disable DFX Configuration
IIO-PCIE Express	Static text	N/A	
PCIE Train by BIOS	Multipart item	<No> <Yes>*	Assume IIO is strapped for Wait-for-BIOS because straps are unreliable in A-0 Silicon
PCIE Hot Plug	Multipart item	<Disable>* <Enable>	Enable/Disable PCIE Hot Plug globally
PCIE ACPI Hot Plug	Multipart item	<Disable>* <Enable>	Enable/Disable PCIE ACPI Hot Plug globally, or allow per-port control. When Disabled, MSI is generated on HP event. When Enabled, _HPGPE message is generated.
MultiCast Enable	Multipart item	<Disable>* <Enable>	Enable MultiCast (for validation use)
NoSnoop Read Config	Multipart item	<Disable>* <Enable>	NoSnoop Read Configuration
Max Read Comp Comb Size	Multipart item	<Maximum> <Minimum>*	Minimum or Maximum size

Problematic port	Multipart item	<Disable>* <Enable>	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.
DMI Allocating Write Flows	Multipart item	<Non-Allocating> <Allocating>*	Selects DMI Vc0/VCp writes selection as either allocating or non-allocating. Auto enables POR setting.
PCIe Allocating Write Flows	Multipart item	<Non-Allocating> <Allocating>*	Selects Vc0/VCp writes selection for all CPU PCIe ports as either allocating or non-allocating. Auto enables POR setting.
Skip Halt On DMI Degradation	Multipart item	<Disable>* <Enable>	Enable this option to avoid the system to be halted on DMI width/link degradation.
Rx Clock WA	Multipart item	<Disable>* <Enable>	HSX HSD# 4166557
PME2ACK Timeout	Multipart item	<1 ms>* <10 ms> <50 ms> <Test Mode>	Controls duration to wait between PME_TURN_OFF and PME_TO_ACK
Hide PCU Func 6	Multipart item	<Disable>* <Enable>	Hide Power Control Unit Device 30 Function 6
EN1K	Multipart item	<Disable>* <Enable>	Enables 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	Multipart item	<Disable> <Enable>*	Allow ucode enable Dual CV feature in the Cbo
PCIe Coherent Read Partial	Multipart item	<PCIRdCur Setting>* <PRd Setting>	Configures Coherent Reads for Available Settings
PCIe Coherent Read Full	Multipart item	<PCIRdCur Setting>* <PRd Setting>	Configures Coherent Reads for Available Settings
PCI-E Completion Timeout (Global)	Multipart item	<No>* <Yes>	Enable / disable the Completion Timeout (D:x F:0 O:B8h B:4) where x is 0-3

Disable			
PCI-E Global Timeout Value	Multipart item	< 50µs to 10ms> < 16ms to 55ms> <65ms to 210ms> <260ms to 900ms>* <1s to 3.5s> <4s to 13s> <17s to 64s>	Program the Completion Timeout Value (D:x F:0 O:B8h B:3-0) where x is 0-3
PCI-E ASPM Support (Global)	Multipart item	<Disable> <Per-Port>* <L1 Only>	This option enables / disables the ASPM support for all downstream devices.
PCIE Stop & Scream Support	Multipart item	<Disable>* <Enable>	This option enables / disables PCIE Stop & Scream Support.
Snoop Response Hold Off	Numeric	0~9*~F	Sets Snoop Response Hold Off value, 256 cycles as Default
PCle Latency Tolerance Reporting	Multipart item	<Enable> <Disable> <Auto>*	Auto/Disable - Turns off the Latency Tolerance Report feature of the Pcie Root port and endpoint. Enable - Turns on the Latency Tolerance Report feature.
PCle Extended Tag Enable	Multipart item	<Enable>* <Disable>	Auto/Enable - BIOS sets 8-bit Tag Field for PCle Root Port/EndPoint. Disable - BIOS sets 5-bit Tag Field for PCle Root Port/EndPoint.
PCle Atomic Operation Request Support	Multipart item	<Enable> <Disable>*	Enable or Disable Atomic Operation feature in PCle Device Control2 register of IIO Root Ports and Endpoints
PCle Max Read Request Size	Multipart item	<Auto>* <128B> <256B> <512B> <1024B> <2048B> <4096B>	Set Max Read Request Size in EndPoints

4.5.5.1 Socket0 Configuration

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
IOU0 (IIIO PCIe Br1)	[x16]	▲ Selects PCIe port Bifurcation for selected slot(s)
IOU1 (IIIO PCIe Br2)	[x16]	
IOU2 (IIIO PCIe Br3)	[x8x8]	
MCP0 (IIIO PCIe Br4)	[Auto]	
MCP1 (IIIO PCIe Br5)	[Auto]	
PCI-E Completion Timeout Disable		
PCI-E Completion Timeout Value	[260ms to 900ms]	
Sck0 RP Correctable Err	[Disable]	
Sck0 RP NonFatal Uncorrectable Err	[Disable]	
Sck0 RP Fatal Uncorrectable Err	[Disable]	
▶ Socket 0 PcieBr0D00F0 - Port 0/DMI		
▶ Socket 0 PcieBr1D00F0 - Port 1A		
▶ Socket 0 PcieBr2D00F0 - Port 2A		
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
MCP1 (IIIO PCIe Br5)	[Auto]	▲ Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
PCI-E Completion Timeout Disable		
PCI-E Completion Timeout Value	[260ms to 900ms]	
Sck0 RP Correctable Err	[Disable]	
Sck0 RP NonFatal Uncorrectable Err	[Disable]	
Sck0 RP Fatal Uncorrectable Err	[Disable]	
▶ Socket 0 PcieBr0D00F0 - Port 0/DMI		
▶ Socket 0 PcieBr1D00F0 - Port 1A		
▶ Socket 0 PcieBr2D00F0 - Port 2A		
▶ Socket 0 PcieBr3D00F0 - Port 3A		
▶ Socket 0 PcieBr3D02F0 - Port 3C		⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
▶ Socket 0 PcieBr4D00F0 - MCP 0		
▶ Socket 0 PcieBr5D00F0 - MCP 1		
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Item	Type	Options	Function description
IOU0 (IIO PCIe Br1)	Multipart item	<x4x4x4x4> <x4x4x8> <x8x4x4> <x8x8> <x16>* <Auto>	Selects PCIe port Bifurcation for selected slot(s)
IOU1 (IIO PCIe Br2)	Multipart item	<x4x4x4x4> <x4x4x8> <x8x4x4> <x8x8> <x16>* <Auto>	Selects PCIe port Bifurcation for selected slot (s)
IOU2 (IIO PCIe Br3)	Multipart item	<x4x4x4x4> <x4x4x8> <x8x4x4> <x8x8>* <x16> <Auto>	Selects PCIe port Bifurcation for selected slot (s)
MCP0 (IIO PCIe Br4)	Multipart item	<x4x4x4x4> <x4x4x8> <x8x4x4> <x8x8> <x16> <Auto>*	Selects PCIe port Bifurcation for selected slot (s)
MCP1 (IIO PCIe Br5)	Multipart item	<x4x4x4x4> <x4x4x8> <x8x4x4> <x8x8> <x16> <Auto>*	Selects PCIe port Bifurcation for selected slot (s)
PCI-E Completion Timeout Disable	Multipart item	<No>* <Yes>	Enable / disable the Completion Timeout (D:x F:0 O:B8h B:4) where x is 0-3
PCI-E Completion Timeout	Multipart item	< 50μs to 10ms> < 16ms to	Program the Completion Timeout Value (D:x F:0 O:B8h B:3-0) where x is 0-3

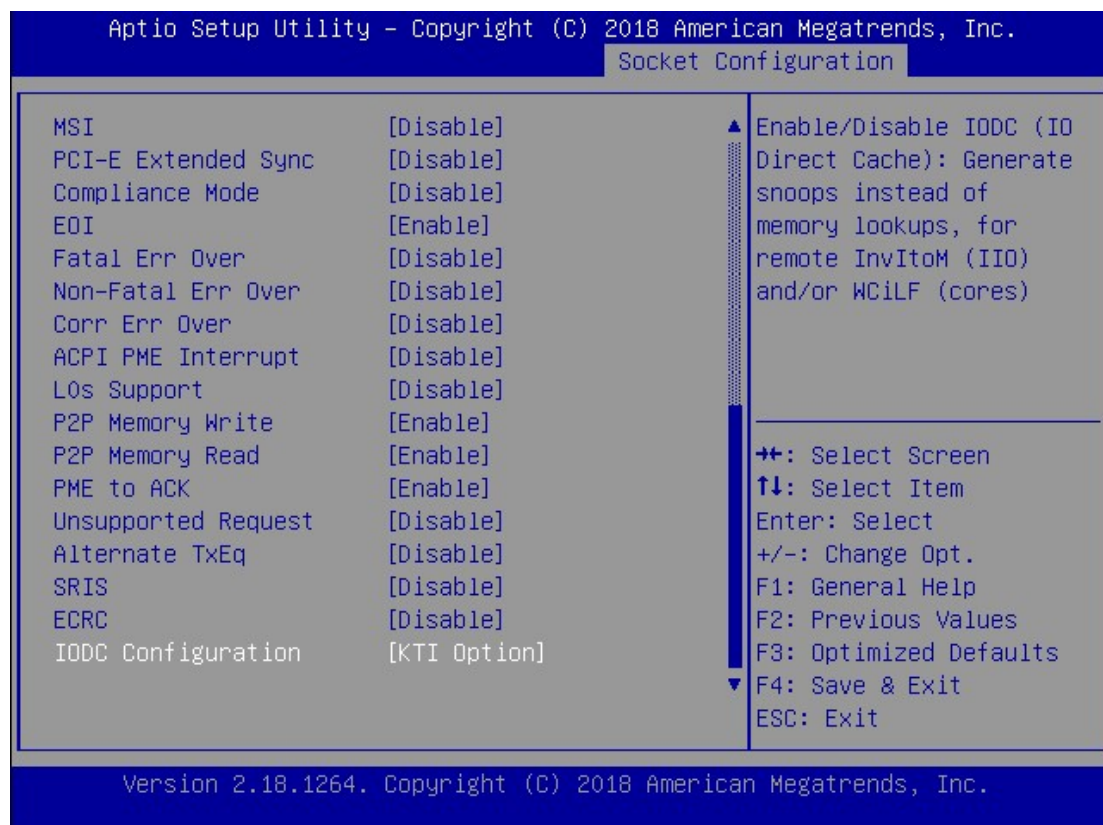
Value		55ms> <65ms to 210ms> <260ms to 900ms>* <1s to 3.5s> <4s to 13s> <17s to 64s>	
Sck0 RP Correctable Err	Multipart item	<Disable>* <Enable>	Applies to root ports only. Enable interrupt on correctable errors
Sck0 RP NonFatal Uncorrectable Err	Multipart item	<Disable>* <Enable>	Applies to root ports only. Enable interrupt on a non-fatal error
Sck0 RP Fatal Uncorrectable Err	Multipart item	<Disable>* <Enable>	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors
Socket 0 PcieBr0D00F0 - Port 0/DMI	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr1D00F0 - Port 1A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr2D00F0 - Port 2A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr3D00F0 - Port 3A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr3D02F0 - Port 3C	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr4D00F0 - MCP 0	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr5D00F0 - MCP 1	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)

4.5.5.1.1 Socket 0 PcieBr0D00F0 – Port 0/DMI

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr0D00F0 - Port 0/DMI	

Link Speed	[Auto]
Override Max Link Width	[Auto]
PCI-E Port DeEmphasis	[-6.0 dB]
PCI-E Port Link Status	Linked as x4
PCI-E Port Link Max	Max Width x4
PCI-E Port Link Speed	Gen 3 (8.0 GT/s)
PCI-E Port Clocking	[Common]
PCI-E Port Max Payload Size	[Auto]
PCI-E Port D-state	[D0]
PCI-E ASPM Support	[L1 Only]
▲ Choose Link Speed for this PCIe port +←: Select Screen ↑↓: Select Item Enter: Select +/=: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port L0s Exit Latency	[4uS - 8uS]
PCI-E Port L1 Exit Latency	[8uS - 16uS]
MSI	[Disable]
PCI-E Extended Sync Compliance Mode	[Disable]
EOI	[Enable]
Fatal Err Over	[Disable]
Non-Fatal Err Over	[Disable]
Corr Err Over	[Disable]
ACPI PME Interrupt	[Disable]
L0s Support	[Disable]
P2P Memory Write	[Enable]
P2P Memory Read	[Enable]
PME to ACK	[Enable]
Unsupported Request	[Disable]
Alternate TxEq	[Disable]
▲ Enable or Disable TxEq +←: Select Screen ↑↓: Select Item Enter: Select +/=: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
Socket 0 PcieBr0D00F0 -Port 0/DMI	Static text	N/A	
Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB> <-6.0 dB>*	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Linked as x4	
PCI-E Port	Dynamic	Max Width x4	

Link Max	text		
PCI-E Port Link Speed	Dynamic text	Gen 3 (8.0 GT/s)	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1 Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L1 to L0
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart	<Disable>*	Enables forcing fatal error

	item	<Enable>	propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote Invltom Hybrid Push> <Invltom AllocFlow> <Enable for Remote Invltom Hybrid AllocNonAlloc>	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote Invltom (IIO) and/or WCiLF (cores)

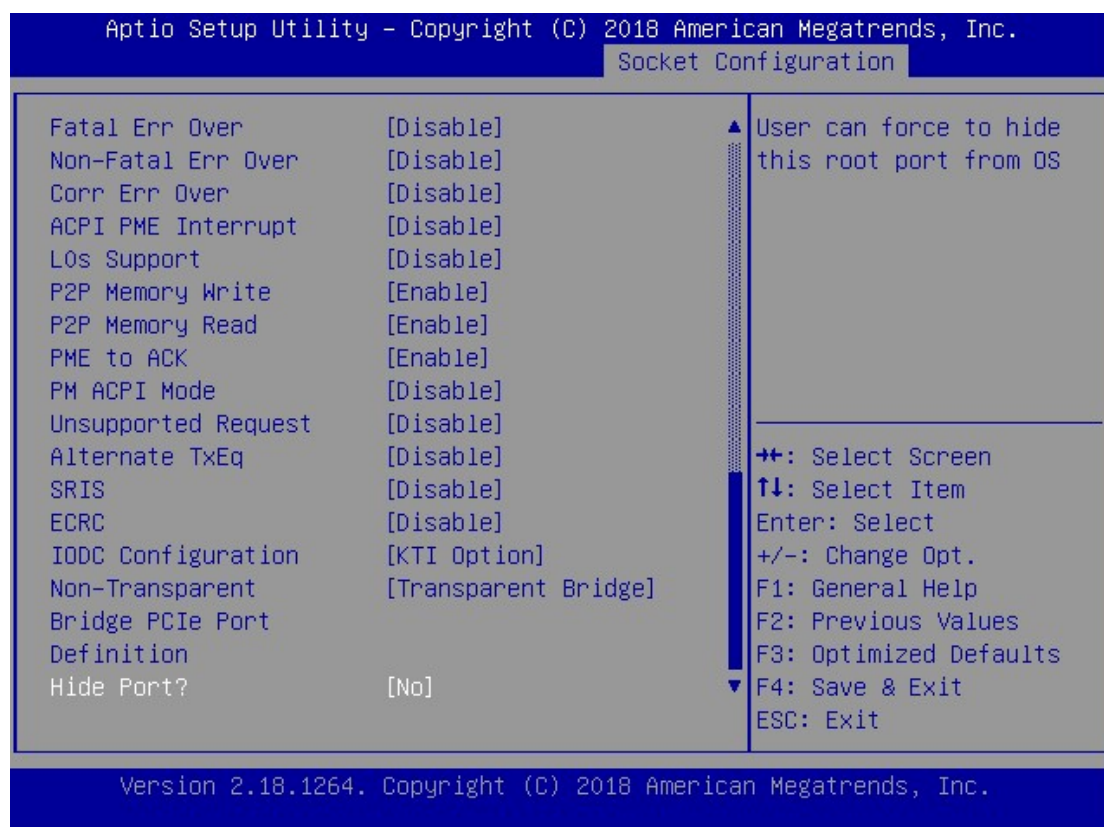
		<Enable for Remote InvltoM and Remote WViLF> <KTI Option>*	
--	--	--	--

4.5.5.1.2 Socket 0 PcieBr1D00F0 – Port 1A

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr1D00F0 - Port 1A	

PCI-E Port	[Auto]
Hot Plug Capable	[Disable]
Surprise Hot Plug Capable	[Disable]
PCI-E Port Link	[Enable]
Link Speed	[Auto]
Override Max Link Width	[Auto]
PCI-E Port DeEmphasis	[-3.5 dB]
PCI-E Port Link Status	Link Did Not Train
PCI-E Port Link Max	Max Width x16
PCI-E Port Link Speed	Link Did Not Train
PCI-E Port Clocking	[Common]
▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the --- ▲+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port Max Payload Size	[Auto]
PCI-E Port D-state	[D0]
PCI-E ASPM Support	[L1 Only]
PCI-E Port L0s Exit Latency	[4uS - 8uS]
PCI-E Port L1 Exit Latency	[8uS - 16uS]
MSI	[Disable]
PCI-E Extended Sync Compliance Mode	[Disable]
EOI	[Disable]
Fatal Err Over	[Disable]
Non-Fatal Err Over	[Disable]
Corr Err Over	[Disable]
ACPI PME Interrupt	[Disable]
L0s Support	[Disable]
P2P Memory Write	[Enable]
▲ Controls Peer2Peer Memory Write Decoding --- ▲+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
Socket 0 PcieBr1D00F0 –Port 1A	Static text	N/A	
PCI-E Port	Multipart item	<Auto>* <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port Link	Multipart item	<Disable> <Enable>*	This option disables the link so that the no training occurs but the CFG space is still active.

Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Max Width x16	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1	Multipart	<<1uS>	The length of time this port

Exit Latency	item	<1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When

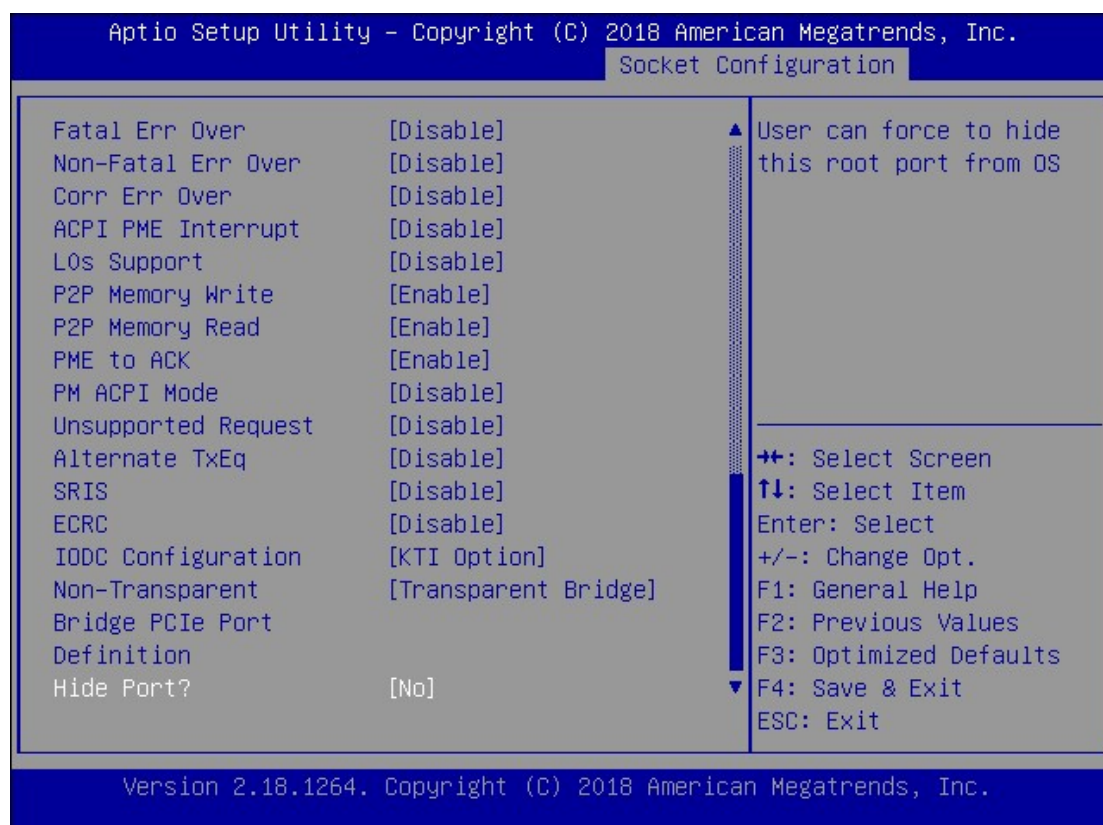
			Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote InvltoM Hybrid Push> <InvltoM AllocFlow> <Enable for Remote InvltoM Hybrid AllocNonAlloc> <Enable for Remote InvltoM and Remote WViLF> <KTI Option>*	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvltoM (IIO) and/or WViLF (cores)
Non-Transparent Bridge PCIe Port Definition	Multipart item	<Transparent Bridge>* <NTB to NTB> <NTB to RP>	[EMBAR1XBASE, EMBAR2XBASE] Configures port as TB, NTB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy IIO on A0 Si!)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.1.3 Socket 0 PcieBr2D00F0 – Port 2A

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr2D00F0 - Port 2A	

PCI-E Port	[Auto]
Hot Plug Capable	[Disable]
Surprise Hot Plug Capable	[Disable]
PCI-E Port Link	[Enable]
Link Speed	[Auto]
Override Max Link Width	[Auto]
PCI-E Port DeEmphasis	[-3.5 dB]
PCI-E Port Link Status	Link Did Not Train
PCI-E Port Link Max	Max Width x16
PCI-E Port Link Speed	Link Did Not Train
PCI-E Port Clocking	[Common]
▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the →+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port Max Payload Size	[Auto]
PCI-E Port D-state	[D0]
PCI-E ASPM Support	[L1 Only]
PCI-E Port L0s Exit Latency	[4uS - 8uS]
PCI-E Port L1 Exit Latency	[8uS - 16uS]
MSI	[Disable]
PCI-E Extended Sync Compliance Mode	[Disable]
E0I	[Disable]
Fatal Err Over	[Disable]
Non-Fatal Err Over	[Disable]
Corr Err Over	[Disable]
ACPI PME Interrupt	[Disable]
L0s Support	[Disable]
P2P Memory Write	[Enable]
▲ Controls Peer2Peer Memory Write Decoding →+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
Socket 0 PcieBr2D00F0 –Port 2A	Static text	N/A	
PCI-E Port	Multipart item	<Auto> <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable> <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable> <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port Link	Multipart item	<Disable> <Enable>	This option disables the link so that the no training occurs but the CFG space is still active.

Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Max Width x16	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1	Multipart	<<1uS>	The length of time this port

Exit Latency	item	<1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When

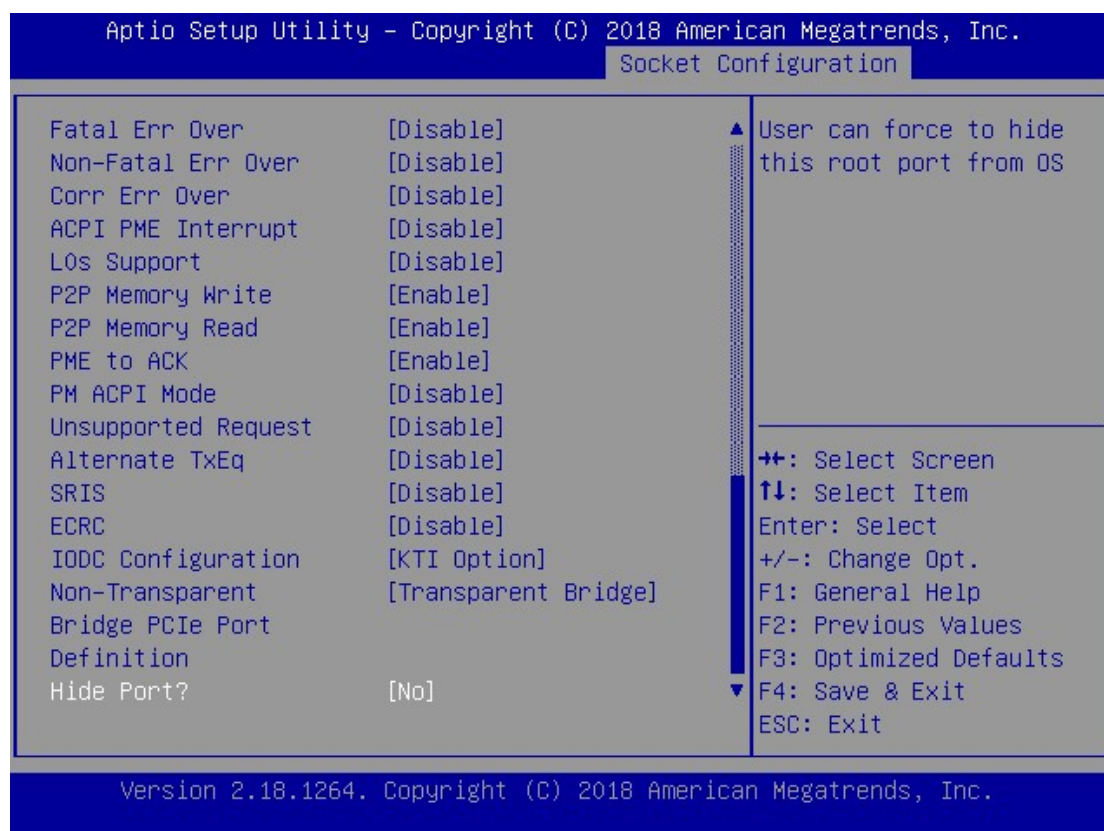
			Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote InvltoM Hybrid Push> <InvltoM AllocFlow> <Enable for Remote InvltoM Hybrid AllocNonAlloc> <Enable for Remote InvltoM and Remote WViLF> <KTI Option>*	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvltoM (IIO) and/or WCiLF (cores)
Non-Transparent Bridge PCIe Port Definition	Multipart item	<Transparent Bridge>* <NTB to NTB> <NTB to RP>	[EMBAR1XBASE, EMBAR2XBASE] Configures port as TB, NTB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy IIO on A0 Si!)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.1.4 Socket 0 PcieBr3D00F0 – Port 3A

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.			
Socket Configuration			
Socket 0 PcieBr3D00F0 - Port 3A		▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the	

PCI-E Port	[Auto]	▼	
Hot Plug Capable	[Disable]		
Surprise Hot Plug Capable	[Disable]		
PCI-E Port Link	[Enable]		
Link Speed	[Auto]		
Override Max Link Width	[Auto]		
PCI-E Port DeEmphasis	[-3.5 dB]		
PCI-E Port Link Status	Link Did Not Train		
PCI-E Port Link Max	Max Width x8		
PCI-E Port Link Speed	Link Did Not Train		
PCI-E Port Clocking	[Common]		
			↔: Select Screen
			↑↓: Select Item
			Enter: Select
			+/-: Change Opt.
		F1: General Help	
		F2: Previous Values	
		F3: Optimized Defaults	
		F4: Save & Exit	
		ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.			

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.			
Socket Configuration			
PCI-E Port Max Payload Size	[Auto]	▲ Controls Peer2Peer Memory Write Decoding	
PCI-E Port D-state	[D0]		
PCI-E ASPM Support	[L1 Only]	▼	
PCI-E Port L0s Exit Latency	[4uS - 8uS]		
PCI-E Port L1 Exit Latency	[8uS - 16uS]		
MSI	[Disable]		
PCI-E Extended Sync	[Disable]		
Compliance Mode	[Disable]		
E0I	[Disable]		
Fatal Err Over	[Disable]		
Non-Fatal Err Over	[Disable]		
Corr Err Over	[Disable]		
ACPI PME Interrupt	[Disable]		
L0s Support	[Disable]		
P2P Memory Write	[Enable]		
			↔: Select Screen
			↑↓: Select Item
		Enter: Select	
		+/-: Change Opt.	
		F1: General Help	
		F2: Previous Values	
		F3: Optimized Defaults	
		F4: Save & Exit	
		ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.			



Item	Type	Options	Function description
Socket 0 PcieBr3D00F0 -Port 3A	Static text	N/A	
PCI-E Port	Multipart item	<Auto>* <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port	Multipart	<Disable>	This option disables the

Link	item	<Enable>*	link so that the no training occurs but the CFG space is still active.
Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Max Width x16	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS>	The length of time this port requires to complete

		<2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	transition from L0s to L0
PCI-E Port L1 Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propogation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propogation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propogation to the IIO core error logic for this port
ACPI PME	Multipart	<Disable>*	When enabled, ACPI PME

Interrupt	item	<Enable>	Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote InvltoM Hybrid Push> <InvltoM AllocFlow> <Enable for Remote InvltoM Hybrid AllocNonAlloc> <Enable for Remote InvltoM and Remote WViLF>	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvltoM (IIO) and/or WViLF (cores)

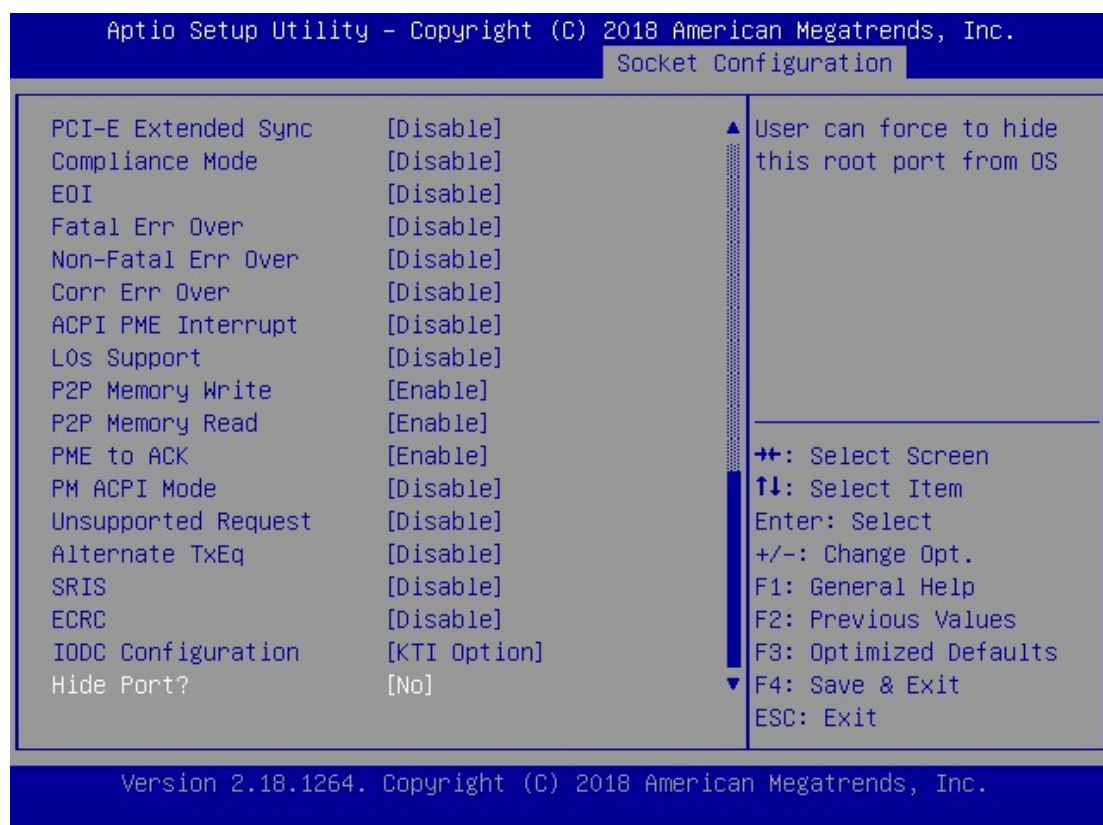
		<KTI Option>*	
Non-Transparent Bridge PCIe Port Definition	Multipart item	<Transparent Bridge>* <NTB to NTB> <NTB to RP>	[EMBAR1XBASE, EMBAR2XBASE] Configures port as TB, NTB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy IIO on A0 Si!)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.1.5 Socket 0 PcieBr3D02F0 – Port 3C

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr3D02F0 - Port 3C	

PCI-E Port	[Auto]
Hot Plug Capable	[Disable]
Surprise Hot Plug Capable	[Disable]
PCI-E Port Link	[Enable]
Link Speed	[Auto]
Override Max Link Width	[Auto]
PCI-E Port DeEmphasis	[-3.5 dB]
PCI-E Port Link Status	Link Did Not Train
PCI-E Port Link Max	Max Width x8
PCI-E Port Link Speed	Link Did Not Train
PCI-E Port Clocking	[Common]
▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the --- ▲+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port Max Payload Size	[Auto]
PCI-E Port D-state	[D0]
PCI-E ASPM Support	[L1 Only]
PCI-E Port L0s Exit Latency	[4uS - 8uS]
PCI-E Port L1 Exit Latency	[8uS - 16uS]
MSI	[Disable]
PCI-E Extended Sync Compliance Mode	[Disable]
EOI	[Disable]
Fatal Err Over	[Disable]
Non-Fatal Err Over	[Disable]
Corr Err Over	[Disable]
ACPI PME Interrupt	[Disable]
L0s Support	[Disable]
P2P Memory Write	[Enable]
▲ Controls Peer2Peer Memory Write Decoding --- ▲+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
Socket 0 PcieBr3D02F0 –Port 3C	Static text	N/A	
PCI-E Port	Multipart item	<Auto>* <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port Link	Multipart item	<Disable> <Enable>*	This option disables the link so that the no training occurs but the CFG space is still active.

Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Max Width x16	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1	Multipart	<<1uS>	The length of time this port

Exit Latency	item	<1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When

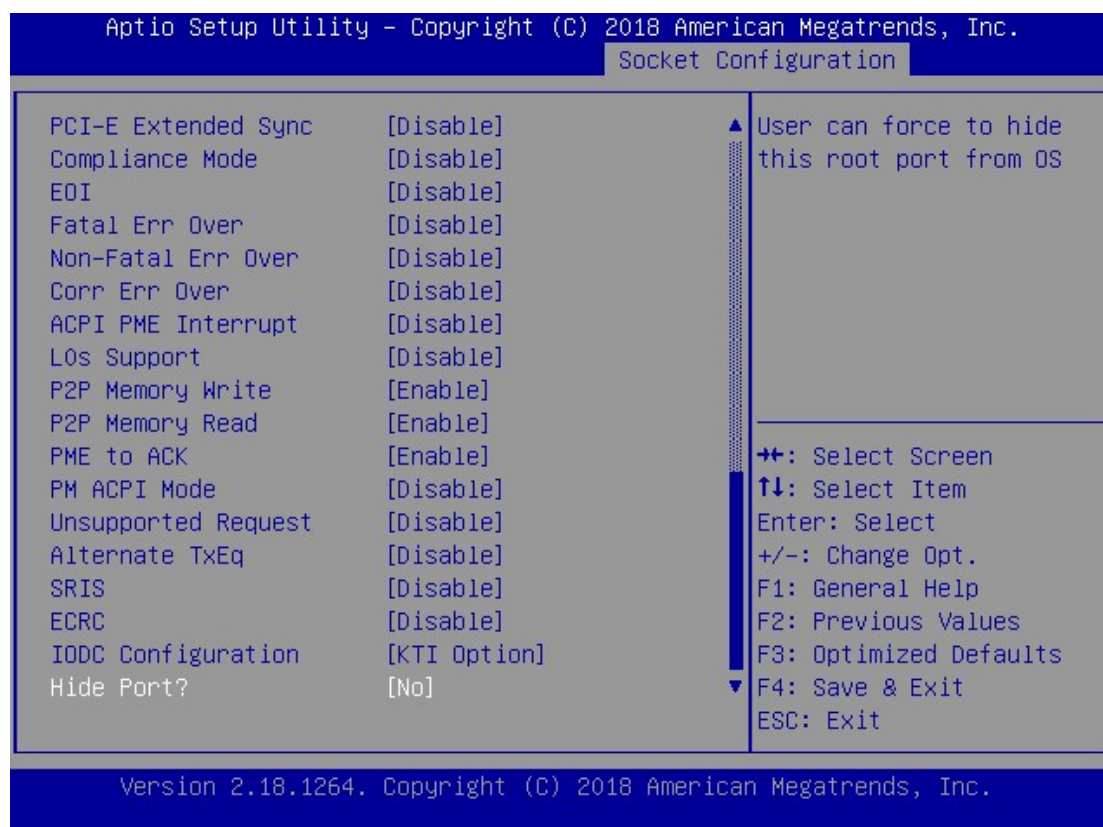
			Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote InvltoM Hybrid Push> <InvltoM AllocFlow> <Enable for Remote InvltoM Hybrid AllocNonAlloc> <Enable for Remote InvltoM and Remote WViLF> <KTI Option>*	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvltoM (IIO) and/or WViLF (cores)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.1.6 Socket 0 PcieBr4D00F0 – MCP 0

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr4D00F0 - MCP 0	

PCI-E Port	[Auto]
Hot Plug Capable	[Disable]
Surprise Hot Plug Capable	[Disable]
PCI-E Port Link	[Enable]
Link Speed	[Auto]
Override Max Link Width	[Auto]
PCI-E Port DeEmphasis	[-3.5 dB]
PCI-E Port Link Status	Link Did Not Train
PCI-E Port Link Max	ERROR: Not Available
PCI-E Port Link Speed	Link Did Not Train
PCI-E Port Clocking	[Common]
▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port Max Payload Size	[Auto]
PCI-E Port D-state	[D0]
PCI-E ASPM Support	[L1 Only]
PCI-E Port L0s Exit Latency	[4uS - 8uS]
PCI-E Port L1 Exit Latency	[8uS - 16uS]
MSI	[Disable]
PCI-E Extended Sync Compliance Mode	[Disable]
EOI	[Disable]
Fatal Err Over	[Disable]
Non-Fatal Err Over	[Disable]
Corr Err Over	[Disable]
ACPI PME Interrupt	[Disable]
L0s Support	[Disable]
P2P Memory Write	[Enable]
▲ Controls Peer2Peer Memory Write Decoding ↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



Item	Type	Options	Function description
Socket 0 PcieBr4D00F0 -MCP 0	Static text	N/A	
PCI-E Port	Multipart item	<Auto>* <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port Link	Multipart item	<Disable> <Enable>*	This option disables the link so that the no training occurs but the CFG space is still active.

Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Error: Not Available	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1	Multipart	<<1uS>	The length of time this port

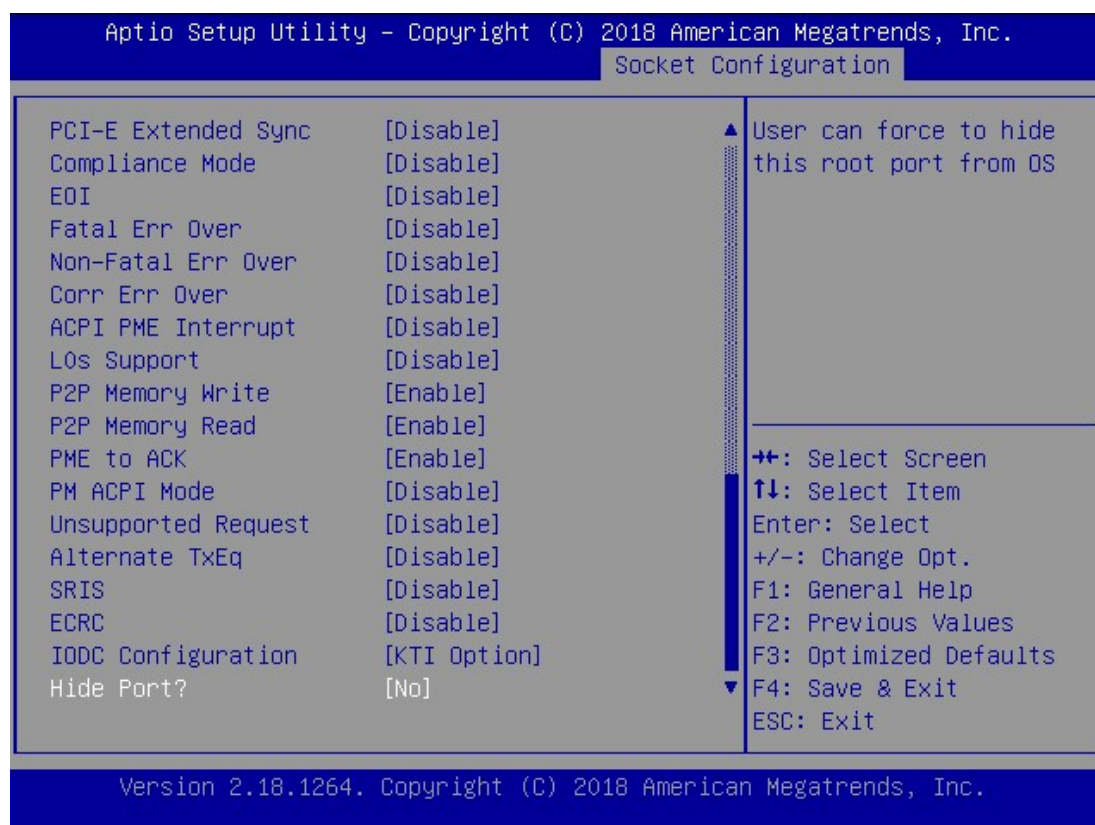
Exit Latency	item	<1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When

			Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote InvltoM Hybrid Push> <InvltoM AllocFlow> <Enable for Remote InvltoM Hybrid AllocNonAlloc> <Enable for Remote InvltoM and Remote WViLF> <KTI Option>*	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvltoM (IIO) and/or WViLF (cores)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.1.7 Socket 0 PcieBr5D00F0 – MCP 1

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
Socket 0 PcieBr5D00F0 - MCP 1 ----- ---	
PCI-E Port [Auto] Hot Plug Capable [Disable] Surprise Hot Plug Capable [Disable] PCI-E Port Link [Enable] Link Speed [Auto] Override Max Link Width [Auto] PCI-E Port DeEmphasis [-3.5 dB] PCI-E Port Link Status Link Did Not Train PCI-E Port Link Max ERROR: Not Available PCI-E Port Link Speed Link Did Not Train PCI-E Port Clocking [Common]	▲ In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the ----- ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit ▼
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.	
Socket Configuration	
PCI-E Port Max [Auto] Payload Size PCI-E Port D-state [D0] PCI-E ASPM Support [L1 Only] PCI-E Port L0s Exit Latency [4uS - 8uS] PCI-E Port L1 Exit Latency [8uS - 16uS] MSI [Disable] PCI-E Extended Sync [Disable] Compliance Mode [Disable] EOI [Disable] Fatal Err Over [Disable] Non-Fatal Err Over [Disable] Corr Err Over [Disable] ACPI PME Interrupt [Disable] L0s Support [Disable] P2P Memory Write [Enable]	▲ Controls Peer2Peer Memory Write Decoding ----- ++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit ▼
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.	



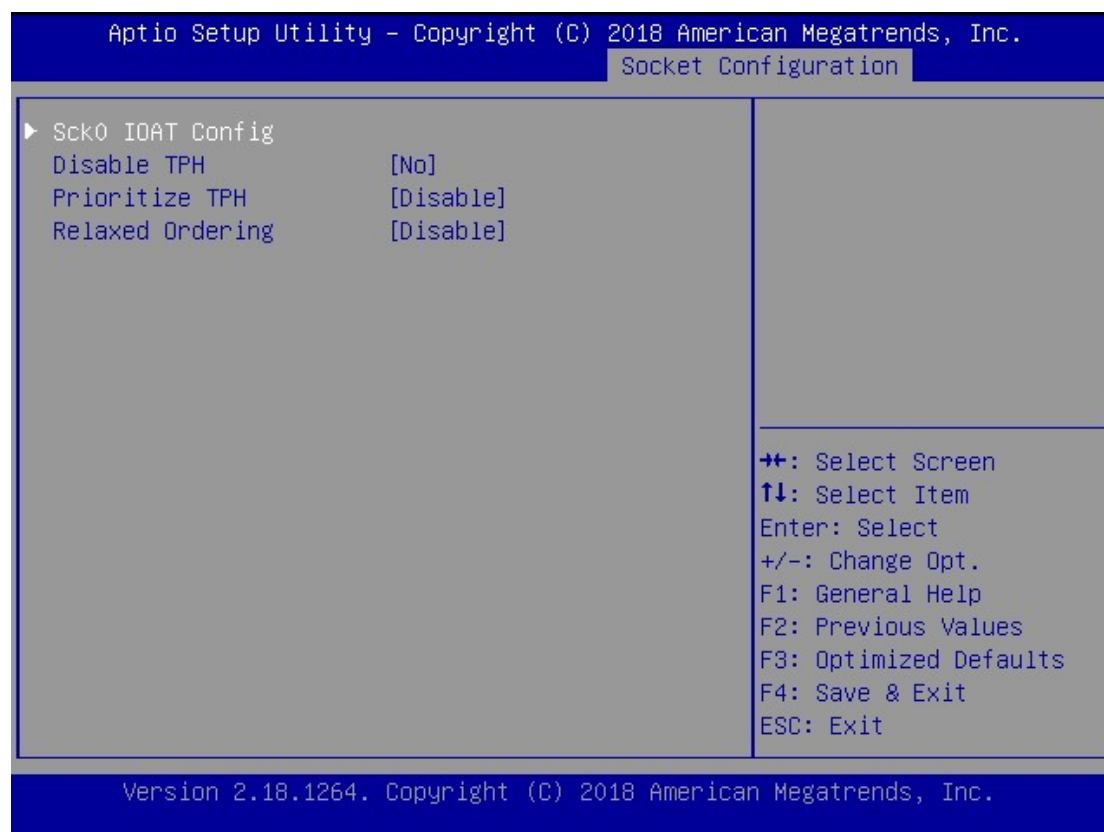
Item	Type	Options	Function description
Socket 0 PcieBr4D00F0 -MCP 0	Static text	N/A	
PCI-E Port	Multipart item	<Auto>* <Disable> <Enable>	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Hot Plug capable.
Surprise Hot Plug Capable	Multipart item	<Disable>* <Enable>	This option specifies if the link is considered Surprise Hot Plug capable.
PCI-E Port Link	Multipart item	<Disable> <Enable>*	This option disables the link so that the no training occurs but the CFG space is still active.

Link Speed	Multipart item	<Auto>* <Gen 1 (2.5 GT/s)> <Gen 2 (5 GT/s)> <Gen 3 (8 GT/s)>	Choose Link Speed for this PCIe port
Override Max Link Width	Multipart item	<Auto>* <x1> <x2> <x4> <x8> <x16>	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	Multipart item	<-3.5 dB>* <-6.0 dB>	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Dynamic text	Link Did Not Train	
PCI-E Port Link Max	Dynamic text	Error: Not Available	
PCI-E Port Link Speed	Dynamic text	Link Did Not Train	
PCI-E Port Clocking	Multipart item	<Common>* <Distinct>	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.
PCI-E Port Max Payload Size	Multipart item	<128B> <256B> <Auto>*	Set Maxpayload size to 256B if possible
PCI-E Port D-state	Multipart item	<D0>* <D3Hot>	Set to D0 for normal operation, D3Hot to be in low-power state
PCI-E ASPM Support	Multipart item	<Auto> <L1 Only>* <Disable>	This option enables / disables the ASPM (L1) support for the downstream devices.
PCI-E Port L0s Exit Latency	Multipart item	<<1uS> <1uS - 2uS> <2uS - 4uS> <4uS - 8uS>* <8uS - 16uS> <16uS - 32uS> <32uS - 64uS> <>64uS>	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1	Multipart	<<1uS>	The length of time this port

Exit Latency	item	<1uS - 2uS> <2uS - 4uS> <4uS - 8uS> <8uS - 16uS>* <16uS - 32uS> <32uS - 64uS> <>64uS>	requires to complete transition from L1 to L0
MSI	Multipart item	<Disable>* <Enable>	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3
PCI-E Extended Sync	Multipart item	<Disable>* <Enable>	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9
Compliance Mode	Multipart item	<Disable>* <Enable>	Disable/Enable Compliance Mode for this PCIe port
EOI	Multipart item	<Disable>* <Enable>	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26
Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	Multipart item	<Disable>* <Enable>	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	Multipart item	<Disable>* <Enable>	Enables forcing correctable error propagation to the IIO core error logic for this port
ACPI PME Interrupt	Multipart item	<Disable>* <Enable>	When enabled, ACPI PME Interrupts are generated from this port
L0s Support	Multipart item	<Disable>* <Enable>	When disabled, IIO never puts its transmitter in L0s state
P2P Memory Write	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Write Decoding
P2P Memory Read	Multipart item	<Disable> <Enable>*	Controls Peer2Peer Memory Read Decoding
PME to ACK	Multipart item	<Disable> <Enable>*	Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message
PM ACPI Mode	Multipart item	<Disable>* <Enable>	When Disabled, MSI is generated on PM event. When

			Enabled, _HPGPE message is generated
Unsupported Request	Multipart item	<Disable>* <Enable>	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
Alternate TxEq	Multipart item	<Disable>* <Enable>	Enable or Disable TxEq
SRIS	Multipart item	<Disable>* <Enable>	Enable or Disable SRIS
ECRC	Multipart item	<Disable>* <Enable>	Enable or Disable ECRC (Error Capabilities and Control Register)
IODC Configuration	Multipart item	<Auto> <Enable for Remote Invltom Hybrid Push> <Invltom AllocFlow> <Enable for Remote Invltom Hybrid AllocNonAlloc> <Enable for Remote Invltom and Remote WViLF> <KTI Option>*	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote Invltom (IIO) and/or WViLF (cores)
Hide Port?	Multipart item	<No>* <Yes>	User can force to hide this root port from OS

4.5.5.2 IOAT Configuration



Item	Type	Options	Function description
Sck0 IOAT Config	Submenu	N/A	All IOAT configuration options
Disable TPH	Multipart item	<No>* <Yes>	TLP Processing Hint disable
Prioritize TPH	Multipart item	<Disable>* <Enable>	STR_PRIORITIZE_TPH
Relaxed Ordering	Multipart item	<Disable>* <Enable>	Relaxed Ordering Enable/Disable

4.5.5.2.1 Sck0 IOAT Config

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

Socket Configuration

DCA	[Enable]	▲ DCA Enable/Disable for this specific socket
IOAT Function 0 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 1 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 2 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 3 Items		
=====		

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

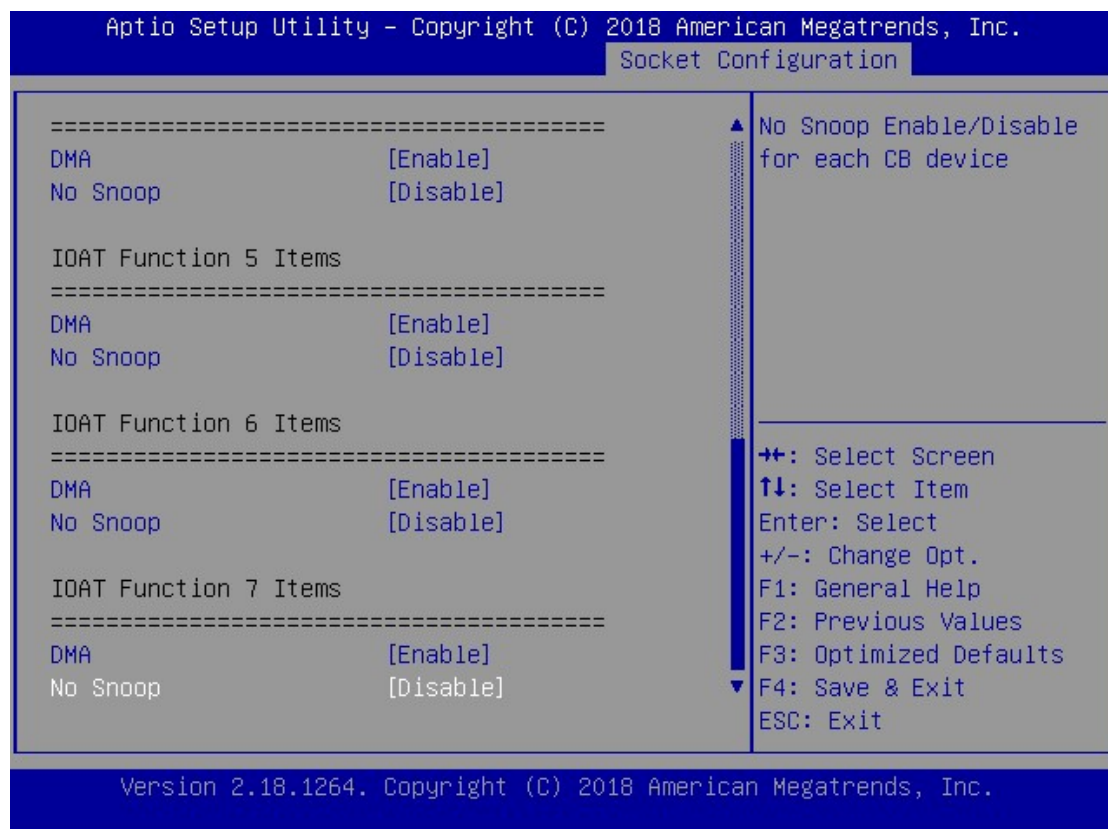
Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.

Socket Configuration

=====		▲ No Snoop Enable/Disable for each CB device
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 4 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 5 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	
IOAT Function 6 Items		
=====		
DMA	[Enable]	
No Snoop	[Disable]	

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

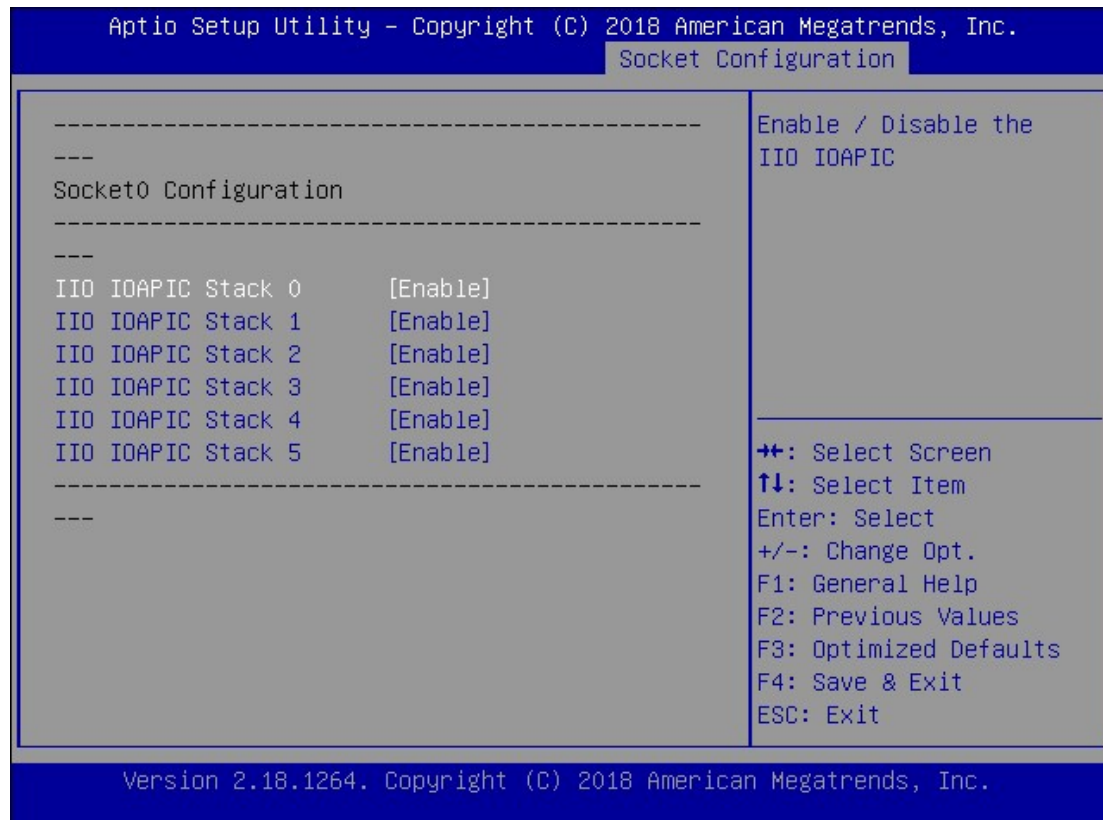
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.



Item	Type	Options	Function description
DCA	Multipart item	<Disable> <Enable>*	DCA Enable/Disable for this specific socket
IOAT Function 0 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 1 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 2 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device

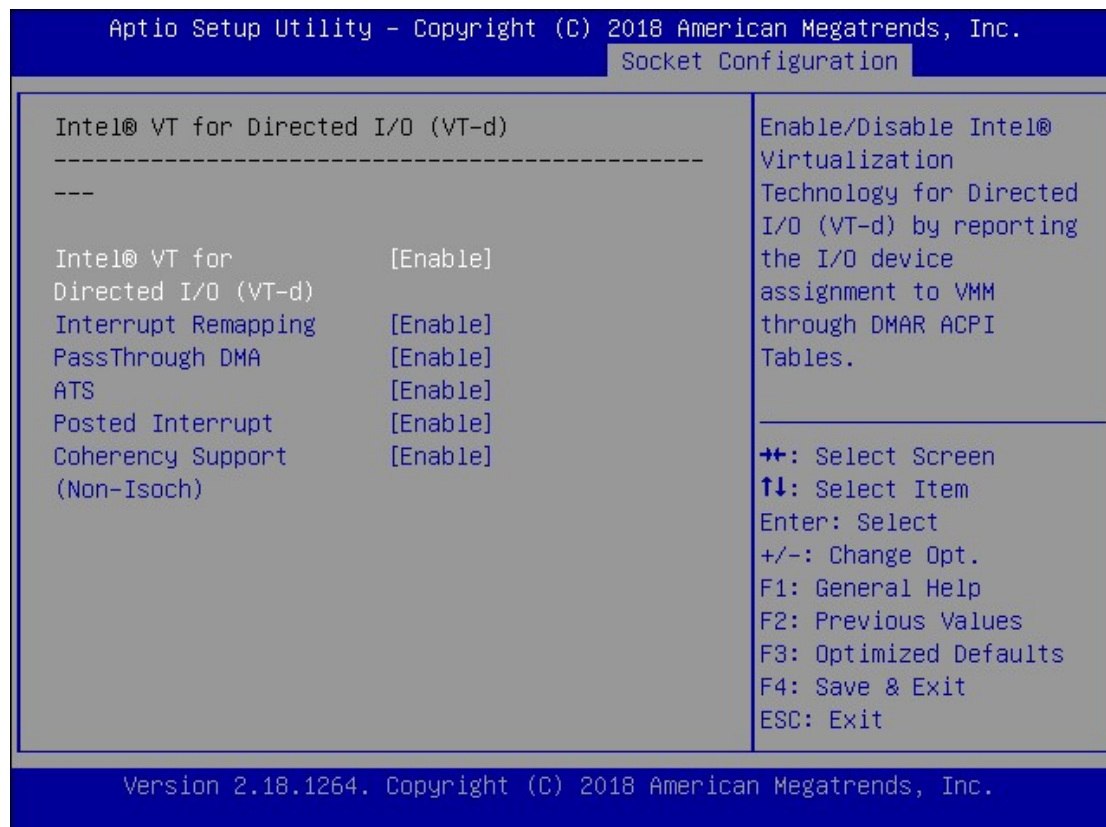
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 3 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 4 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 5 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 6 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device
IOAT Function 7 Items	Static text	N/A	
DMA	Multipart item	<Disable> <Enable>*	Select Dma Enable/Disable for each CB device
No Snoop	Multipart item	<Disable>* <Enable>	No Snoop Enable/Disable for each CB device

4.5.5.3 IIO General Configuration



Item	Type	Options	Function description
Socket0 Configuration	Static text	N/A	
IIO IOAPIC Stack 0	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC
IIO IOAPIC Stack 1	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC
IIO IOAPIC Stack 2	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC
IIO IOAPIC Stack 3	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC
IIO IOAPIC Stack 4	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC
IIO IOAPIC Stack 5	Multipart item	<Disable> <Enable>*	Enable / Disable the IIO IOAPIC

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



Item	Type	Options	Function description
Intel® VT for Directed I/O (VT-d)	Static text	N/A	Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.
Intel® VT for Directed I/O (VT-d)	Multipart item	<Disable> <Enable>*	Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
Interrupt Remapping	Multipart item	<Disable> <Enable>*	Enable/Disable VT_D Interrupt Remapping Support
PassThrough DMA	Multipart item	<Disable> <Enable>*	Enable/Disable Non-Isoch VT_D Engine Pass Through DMA support
Posted Interrupt	Multipart item	<Disable> <Enable>*	Enable/Disable VT_D posted interrupt
ATS	Multipart item	<Disable> <Enable>*	Enable/Disable Non-Isoch VT_D Engine ATS support
Posted Interrupt	Multipart item	<Disable> <Enable>*	Enable/Disable VT_D posted interrupt

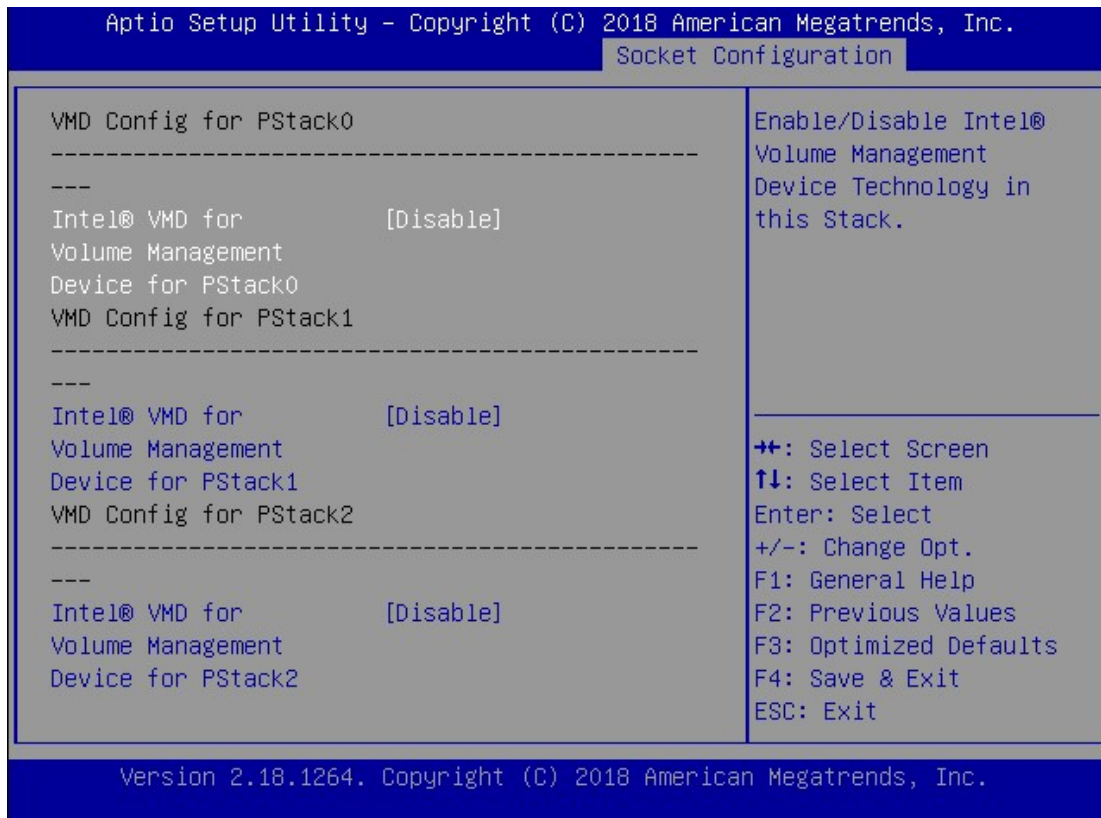
Coherency Support (Non-Isoch)	Multipart item	<Disable> <Enable>*	Enable/Disable Non-Isoch VT_D Engine Coherency support
-------------------------------	----------------	------------------------	--

4.5.5.5 Intel® VMD technology



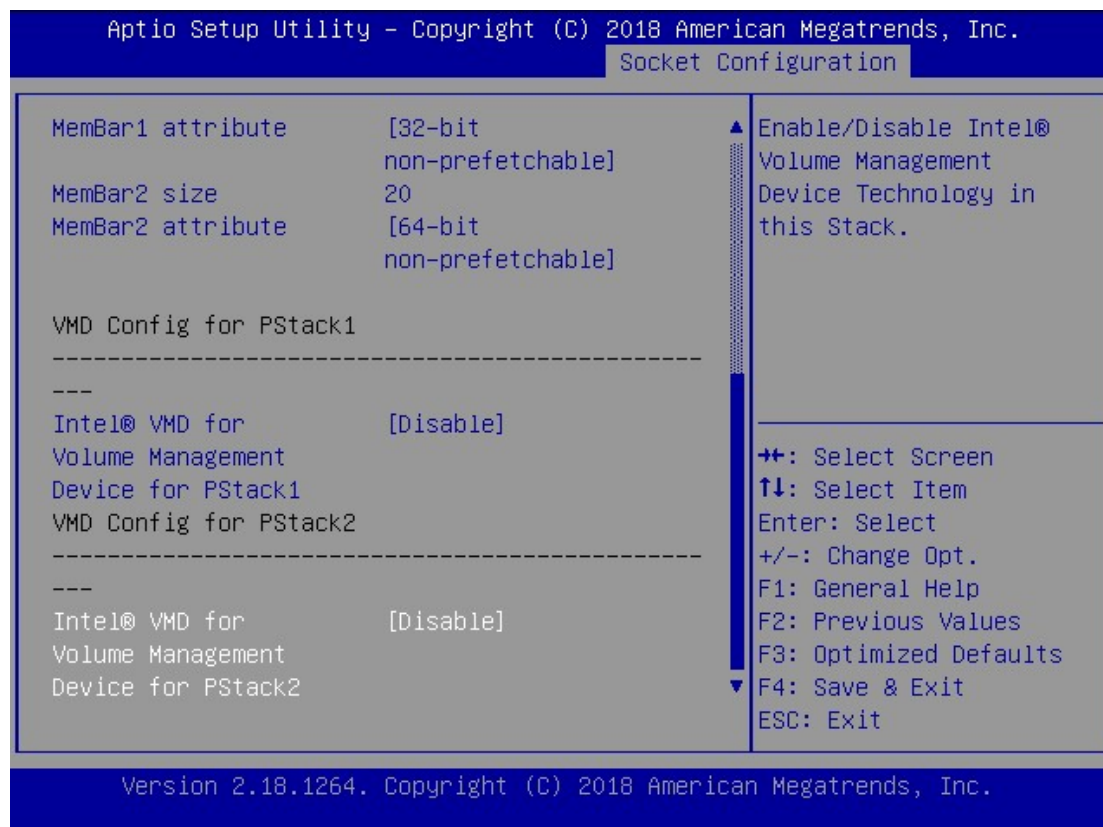
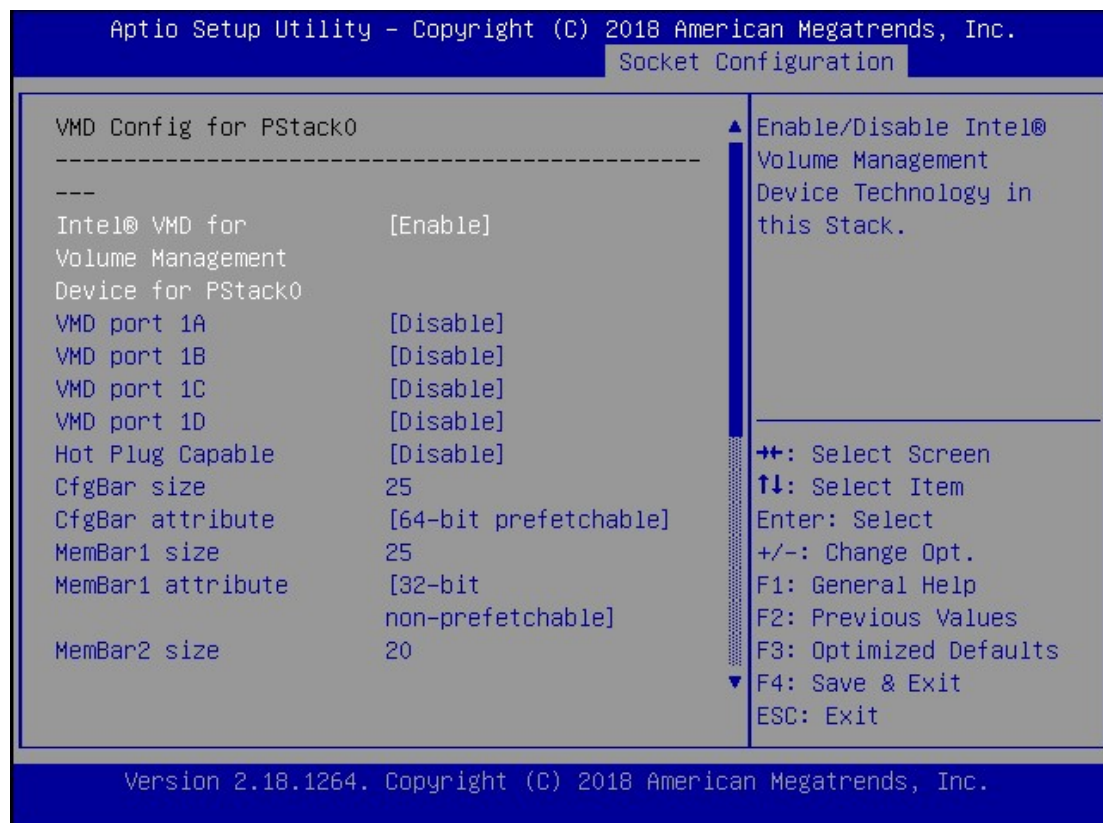
Item	Type	Options	Function description
Intel® VMD for Volume Management Device on Socket 0	Submenu	N/A	
Intel® VMD for Volume Management Device on Socket 1	Submenu	N/A	

4.5.5.5.1 Intel® VMD for Volume Management Device on Socket 0



Item	Type	Options	Function description
VMD Config for PStack0	Static text	N/A	
Intel® VMD for Volume Management Device for PStack0	Multipart item	<Disable> <Enable>*	Enable/Disable Intel® Volume Management Device Technology in this Stack.
VMD Config for PStack1	Static text	N/A	
Intel® VMD for Volume Management Device for PStack1	Multipart item	<Disable> <Enable>*	Enable/Disable Intel® Volume Management Device Technology in this Stack.
VMD Config for PStack2	Static text	N/A	
Intel® VMD for Volume Management Device for PStack2	Multipart item	<Disable> <Enable>*	Enable/Disable Intel® Volume Management Device Technology in this Stack.

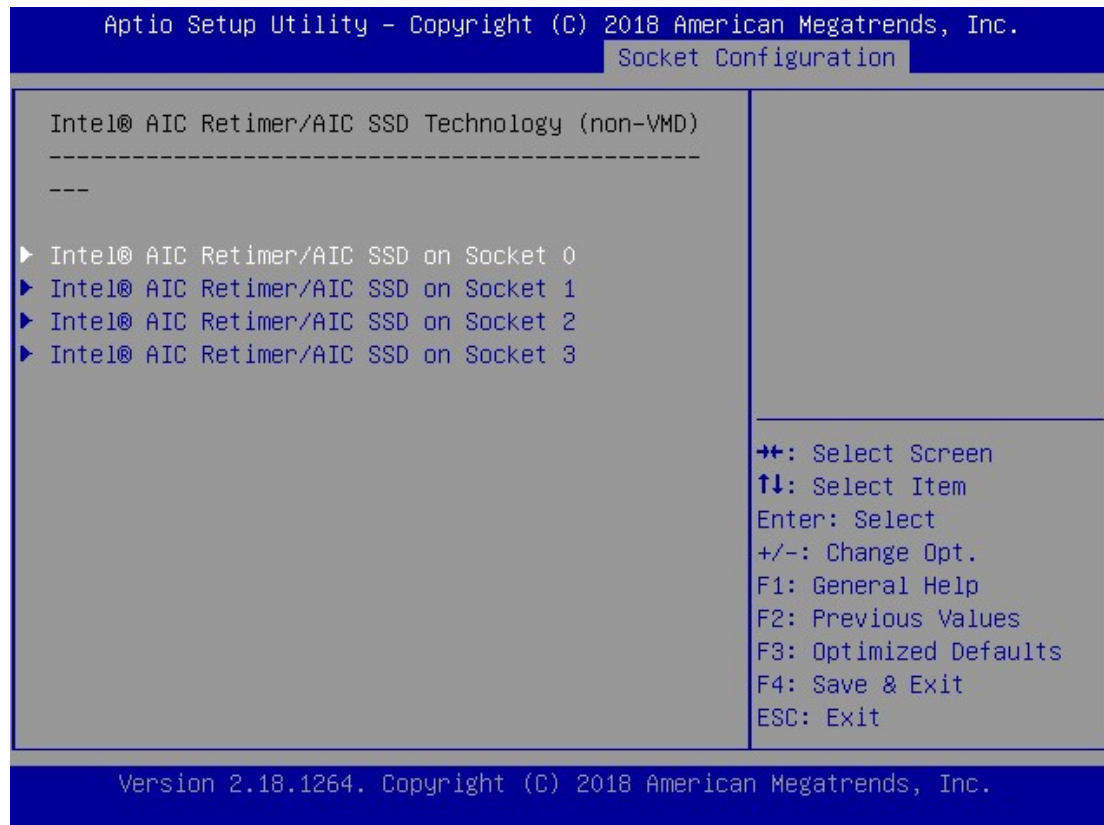
4.5.5.5.2 Intel® VMD for Volume Management Device for PStack0



Item	Type	Options	Function description
VMD Config for PStack0	Multipart item	<Disable> <Enable>*	
VMD port 1A	Multipart item	<Disable>* <Enable>	Enable/Disable Intel® Volume Management Device Technology on specific root port
VMD port 1B	Multipart item	<Disable>* <Enable>	Enable/Disable Intel® Volume Management Device Technology on specific root port
VMD port 1C	Multipart item	<Disable>* <Enable>	Enable/Disable Intel® Volume Management Device Technology on specific root port
VMD port 1D	Multipart item	<Disable>* <Enable>	Enable/Disable Intel® Volume Management Device Technology on specific root port
Hot Plug Capable	Multipart item	<Disable>* <Enable>	Enable/Disable Hot Plug for PCIe Root Ports 1A-1D
CfgBar size	Numeric	20~25*~27	Setup VMD Config BAR size (in bits Min=20, Max=27), ex: 20bits=1MB, 27bits=128MB
CfgBar attribute	Multipart item	<32-bit non-prefetchable> <64-bit non-prefetchable> <64-bit prefetchable >*	Set up VMD Config BAR attribute, like 64-bit or prefetchable
MemBar1 size	Numeric	20~25*~39	Setup VMD Memory BAR1 size (in bits Min=20), ex: 20bits=1MB, 22bits=4MB, 26bits=64MB
MemBar1 attribute	Multipart item	<32-bit non-prefetchable>* <64-bit non-prefetchable> <64-bit prefetchable >	Set up VMD Config BAR attribute, like 64-bit or prefetchable
MemBar2 size	Numeric	20*~39	Setup VMD Memory BAR2 size (in bits Min=20), ex:

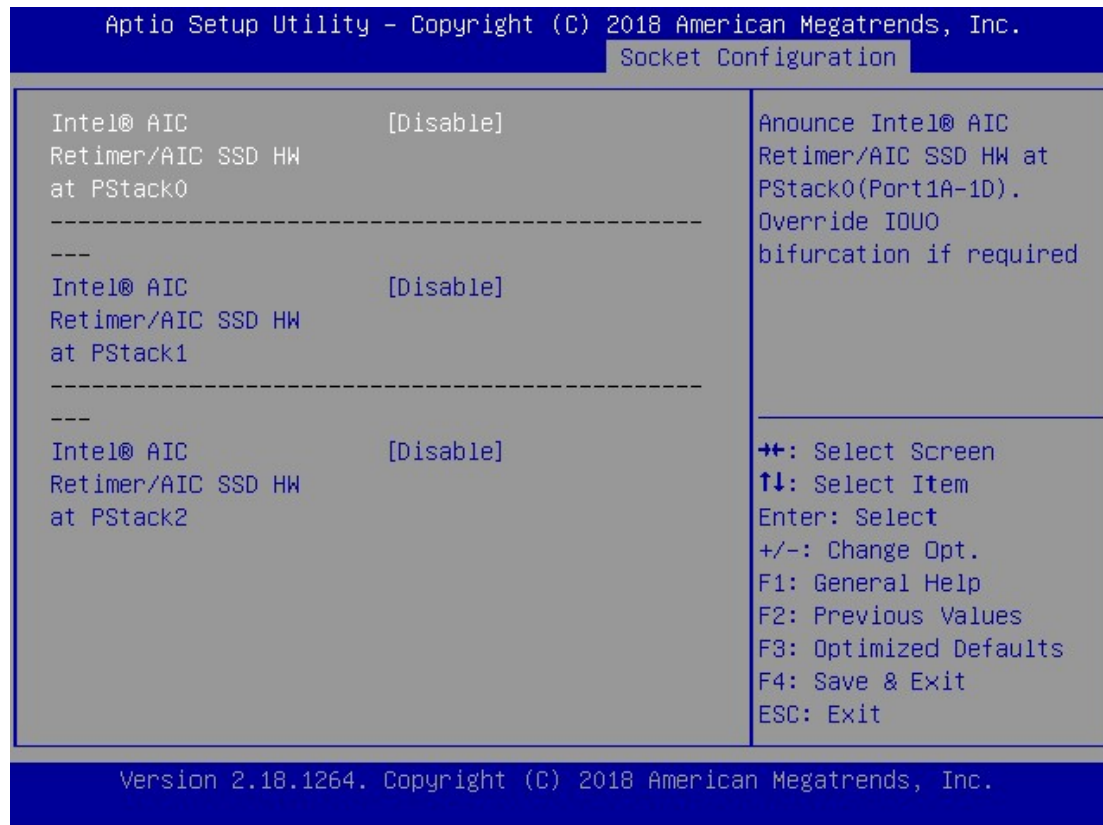
			20bits=1MB, 22bits=4MB, 26bits=64MB
MemBar2 attribute	Multipart item	<32-bit non- prefetchable> <64-bit non- prefetchable>* <64-bit prefetchable >	Set up VMD Config BAR attribute, like 64-bit or prefetchable

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



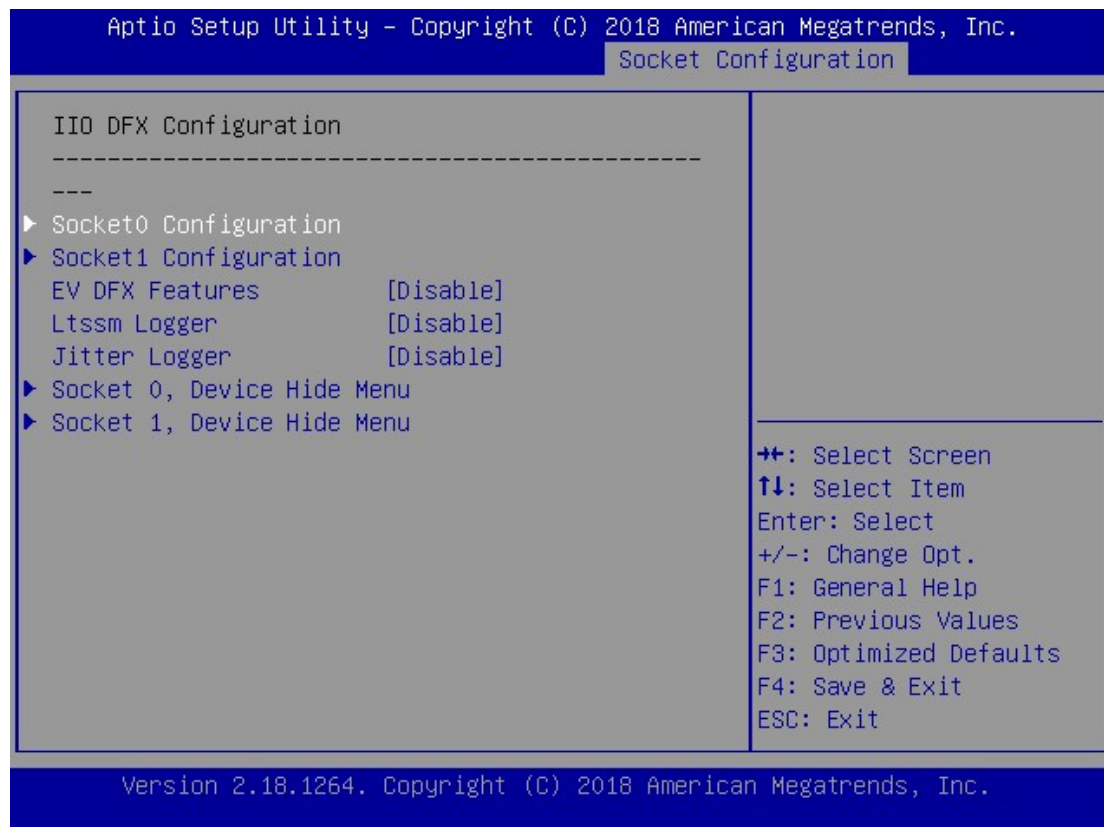
Item	Type	Options	Function description
Intel® AIC Retimer/AIC SSD Technology (non-VMD)	Static text	N/A	
Intel® AIC Retimer/AIC SSD on Socket 0	Submenu	N/A	
Intel® AIC Retimer/AIC SSD on Socket 1	Submenu	N/A	
Intel® AIC Retimer/AIC SSD on Socket 2	Submenu	N/A	
Intel® AIC Retimer/AIC SSD on Socket 3	Submenu	N/A	

4.5.5.6.1 Intel® AIC Retimer/AIC SSD on Socket x (x=0~3)



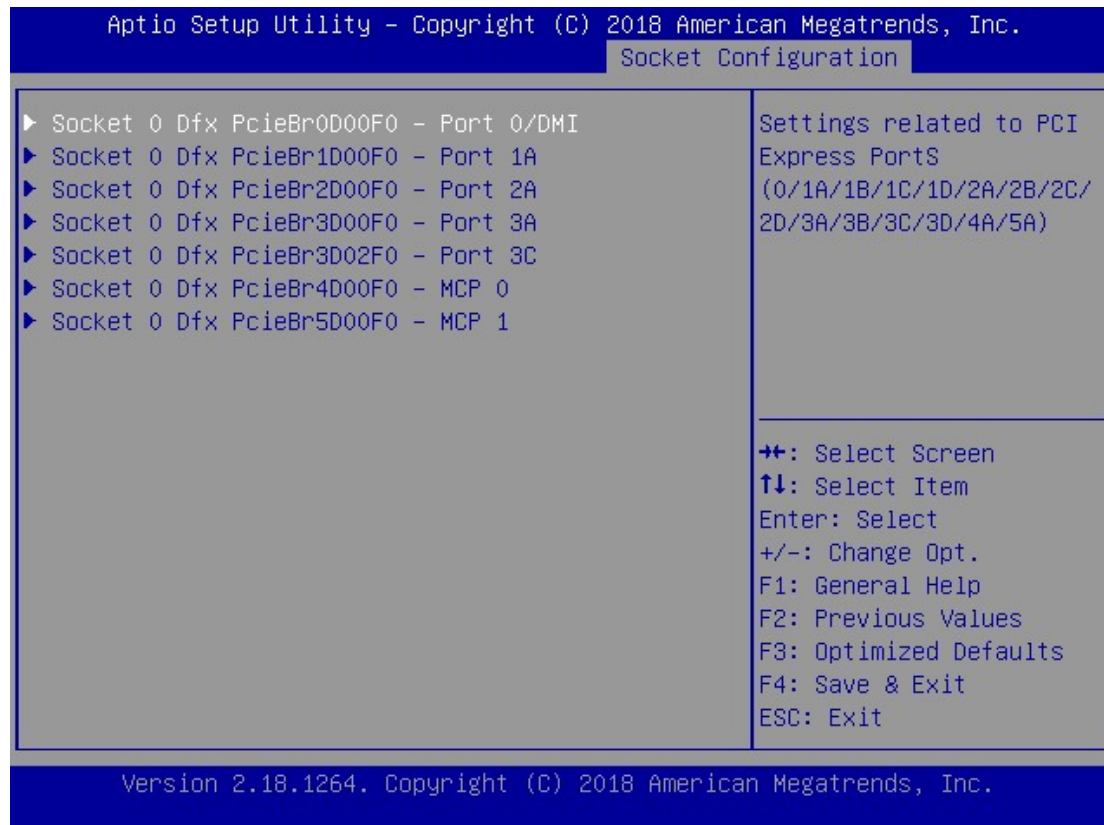
Item	Type	Options	Function description
Intel® AIC Retimer/AIC SSD HW at PStack0	Multipart item	<Disable>* <Enable>	Anounce Intel® AIC Retimer/AIC SSD HW at PStack0(Port1A-1D). Override IOU0 bifurcation if required
Intel® AIC Retimer/AIC SSD HW at PStack1	Multipart item	<Disable>* <Enable>	Anounce Intel® AIC Retimer/AIC SSD HW at PStack1(Port2A-2D). Override IOU0 bifurcation if required
Intel® AIC Retimer/AIC SSD HW at PStack2	Multipart item	<Disable>* <Enable>	Anounce Intel® AIC Retimer/AIC SSD HW at PStack2(Port3A-3D). Override IOU0 bifurcation if required

4.5.5.7 IIO DFX Configuration



Item	Type	Options	Function description
IIO DFX Configuration	Static text	N/A	
Socket0 Configuration	Submenu	N/A	
Socket1 Configuration	Submenu	N/A	
EV DFX Features	Multipart item	<Disable>* <Enable>	Expose IIO DFX devices and other CPU devices like PMON
Ltssm Logger	Multipart item	<Disable>* <Enable>	Enable/Disable Ltssm Logger for PCIE functionality
Jitter Logger	Multipart item	<Disable>* <Enable>	Enable/Disable Jitter Logger for PCIE functionality
Socket 0, Device Hide Menu	Submenu	N/A	Socket 0, Device Hide Menu
Socket 1, Device Hide Menu	Submenu	N/A	Socket 1, Device Hide Menu

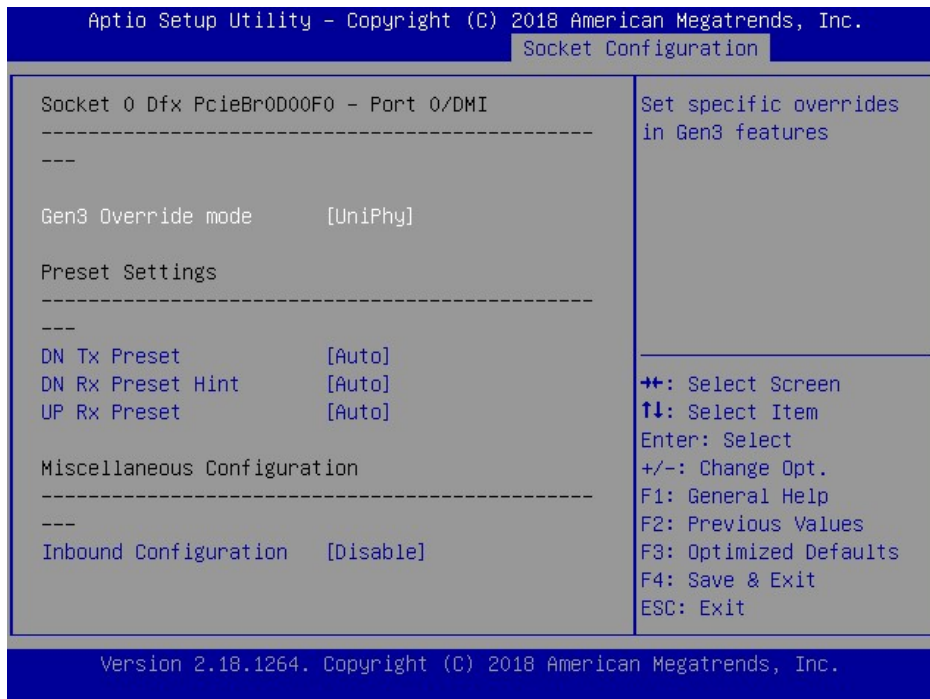
4.5.5.7.1 Socket0 Configuration



Item	Type	Options	Function description
Socket 0 Dfx PcieBr0D00F0 - Port 0/DMI	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr1D00F0 - Port 1A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr2D00F0 - Port 2A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr3D00F0 - Port 3A	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/5A)
Socket 0	Submenu	N/A	Settings related to PCI

PcieBr3D02F0 - Port 3C			Express PortS (0/1A/1B/1C/1D/2A/2B/2C /2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr4D00F0 - MCP 0	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C /2D/3A/3B/3C/3D/4A/5A)
Socket 0 PcieBr5D00F0 - MCP 1	Submenu	N/A	Settings related to PCI Express PortS (0/1A/1B/1C/1D/2A/2B/2C /2D/3A/3B/3C/3D/4A/5A)

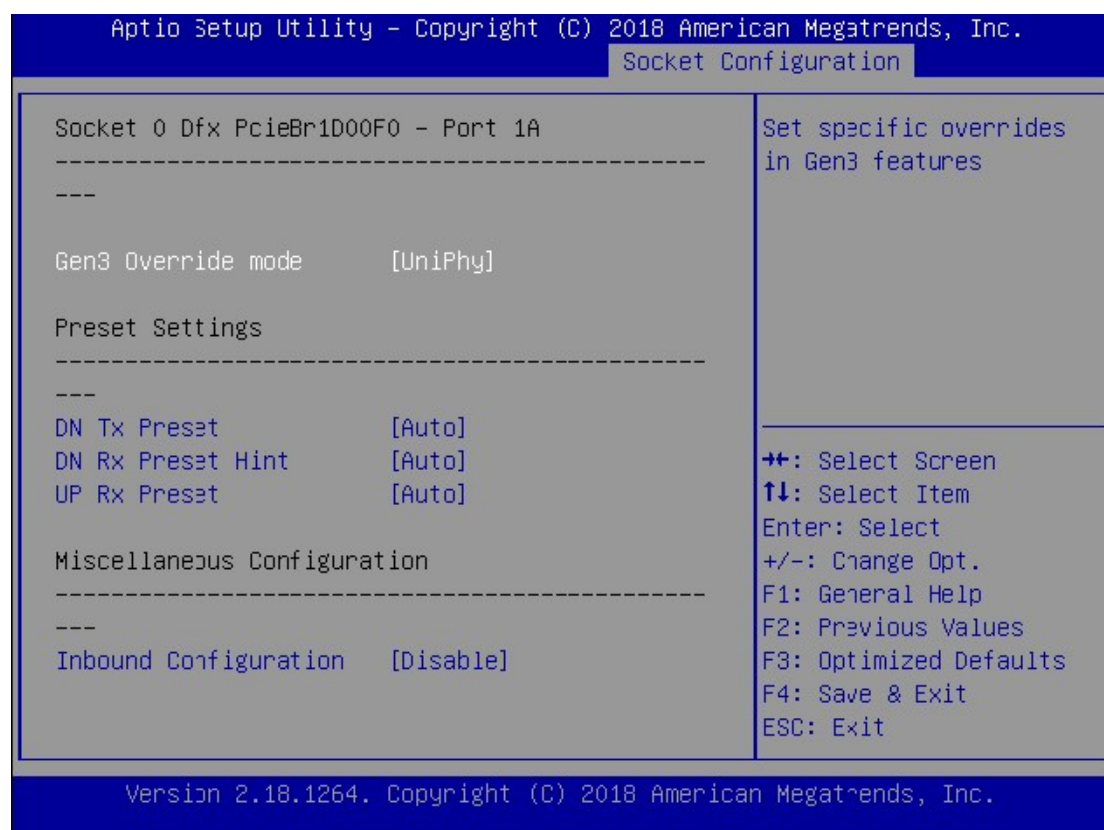
4.5.5.7.2 Socket 0 Dfx PcieBr0D00F0 - Port 0/DMI



Item	Type	Options	Function description
Socket 0 Dfx PcieBr0D00F0 - Port 0/DMI	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Downstream Tx Preset
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)>	PCIe Downstream Rx Preset Hint

		<P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

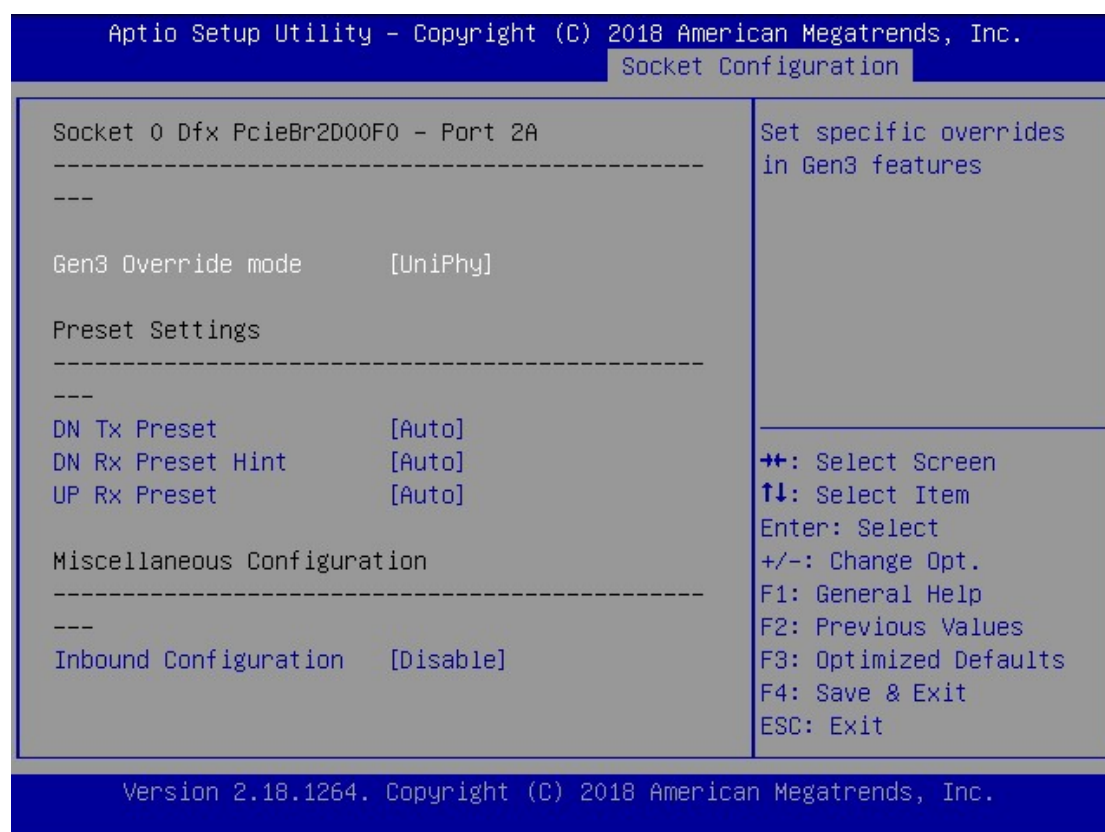
4.5.5.7.3 Socket 0 PcieBr1D00F0 - Port 1A



Item	Type	Options	Function description
Socket 0 PcieBr1D00F0 - Port 1A	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

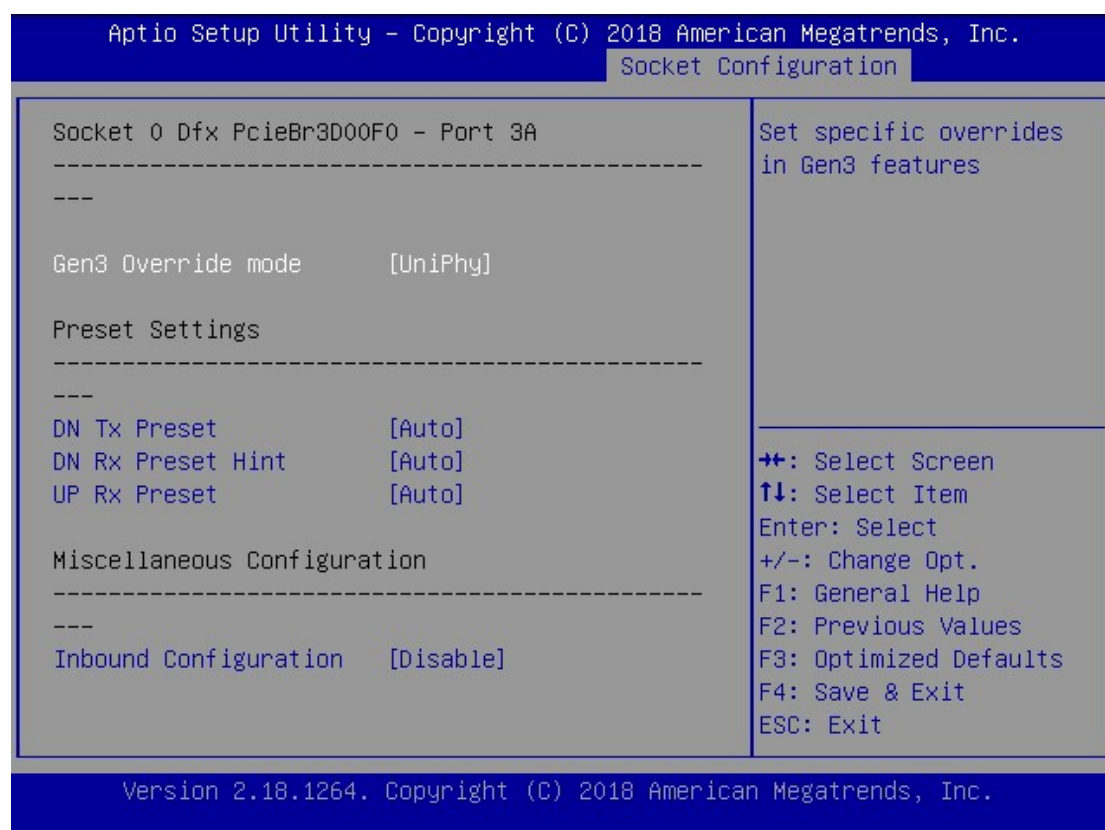
4.5.5.7.4 Socket 0 PcieBr2D00F0 - Port 2A



Item	Type	Options	Function description
Socket 0 PcieBr2D00F0 - Port 2A	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

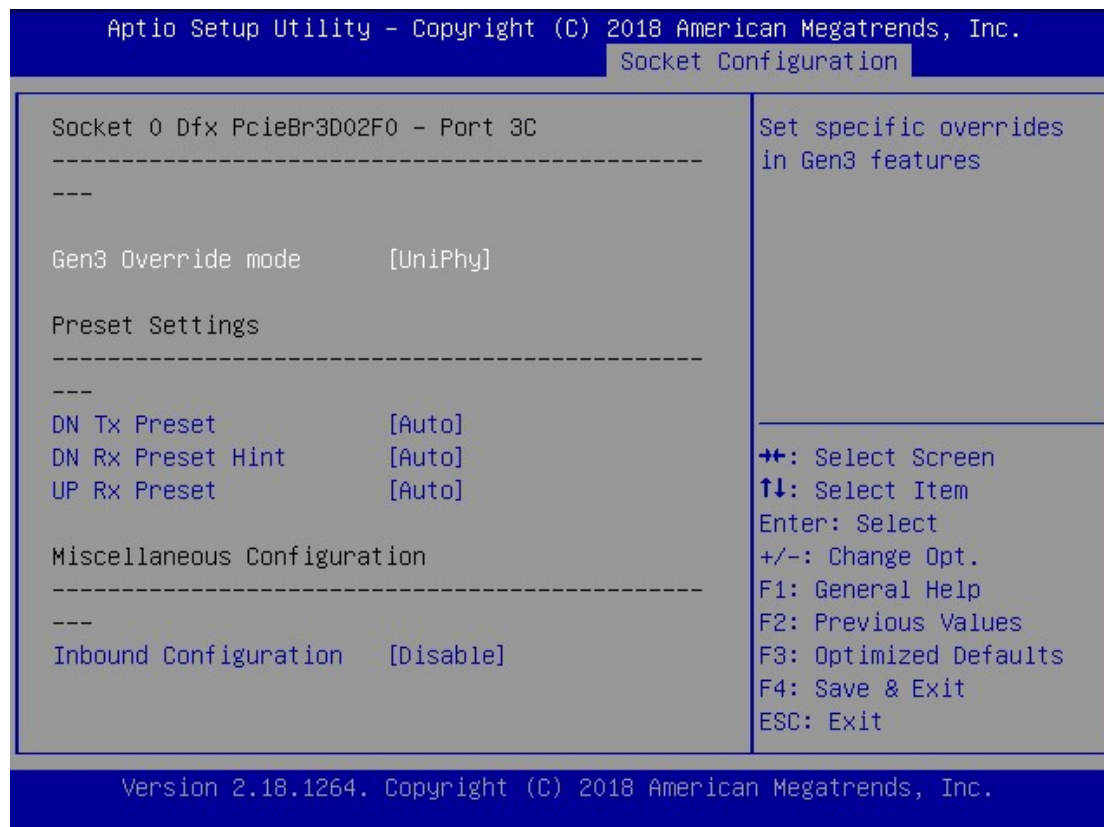
4.5.5.7.5 Socket 0 PcieBr3D00F0 - Port 3A



Item	Type	Options	Function description
Socket 0 PcieBr3D00F0 - Port 3A	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

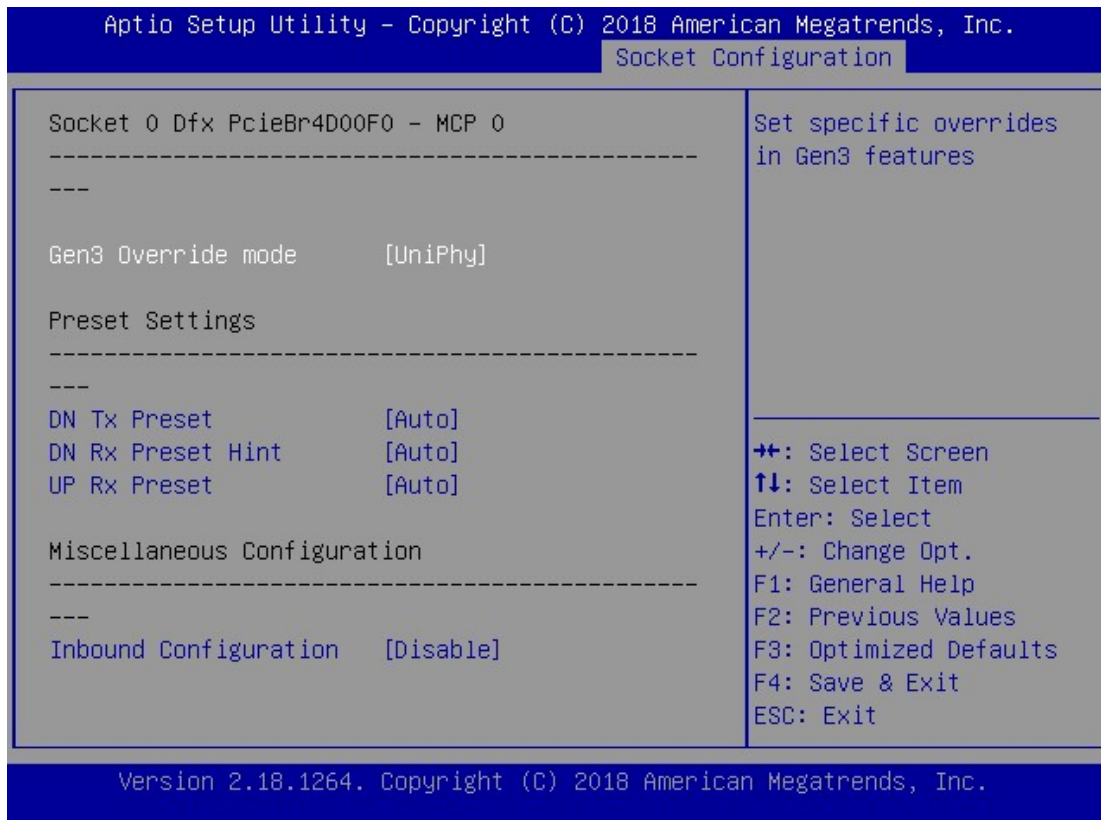
4.5.5.7.6 Socket 0 PcieBr3D02F0 - Port 3C



Item	Type	Options	Function description
Socket 0 PcieBr3D00F0 - Port 3C	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

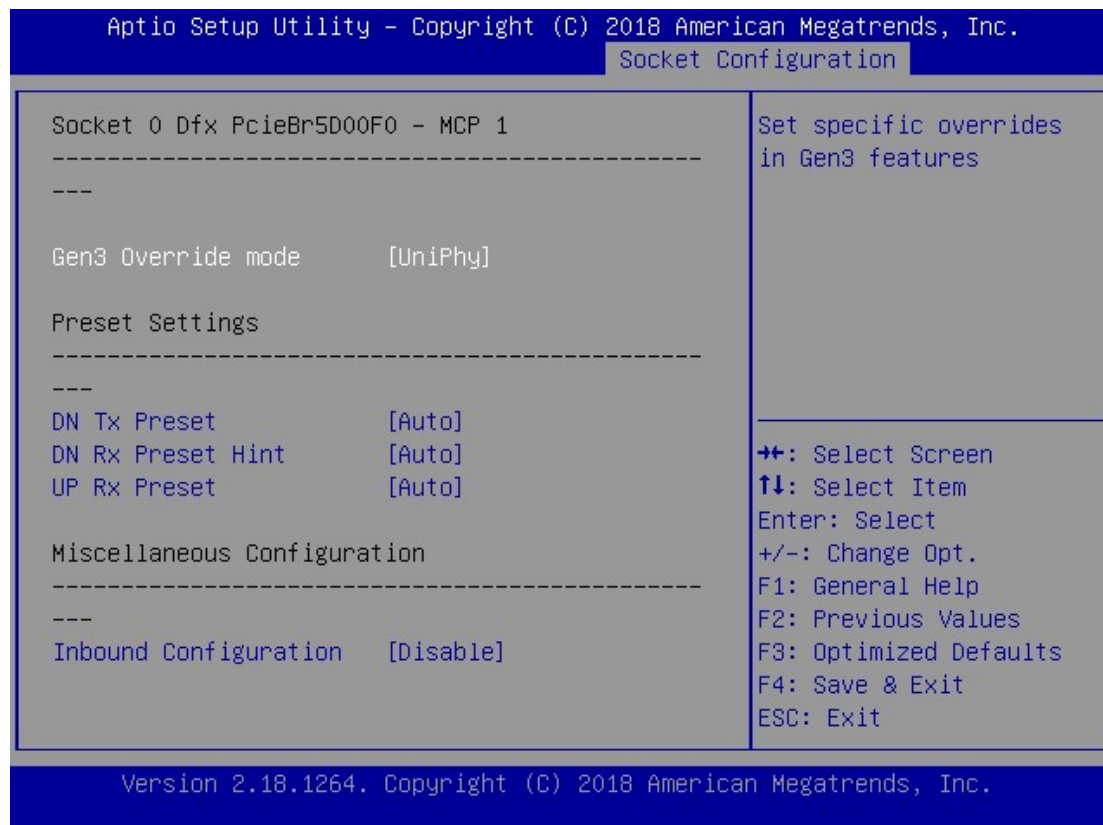
4.5.5.7.7 Socket 0 PcieBr4D00F0 - MCP 0



Item	Type	Options	Function description
Socket 0 PcieBr4D00F0 – MCP 0	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

4.5.5.7.8 Socket 0 PcieBr5D00F0 - MCP 1



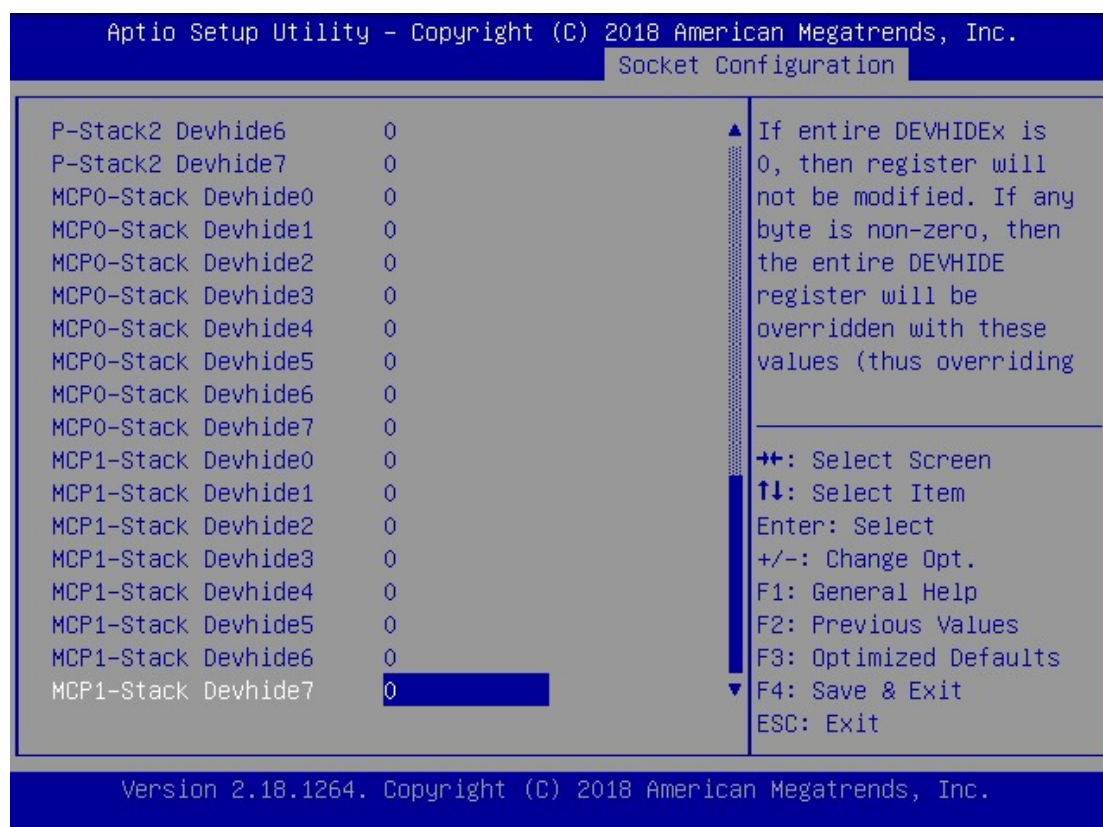
Item	Type	Options	Function description
Socket 0 PcieBr5D00F0 - MCP 1	Static text	N/A	
Gen3 Override mode	Multipart item	<UniPhy>* <Manual> <Test Card>	Set specific overrides in Gen3 features
Preset Setting	Static text	N/A	
DN Tx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)>	PCIe Downstream Tx Preset

		<P9 (0.0/3.5 dB)>	
DN Rx Preset Hint	Multipart item	<Auto>* <P0 (-6.0 dB)> <P1 (-7.0 dB)> <P2 (-8.0 dB)> <P3 (-9.0 dB)> <P4 (-10.0 dB)> <P5 (-11.0 dB)> <P6 (-12.0 dB)>	PCIe Downstream Rx Preset Hint
UP Rx Preset	Multipart item	<Auto>* <P0 (-6.0/0.0 dB)> <P1 (-3.5/0.0 dB)> <P2 (-4.5/0.0 dB)> <P3 (-2.5/0.0 dB)> <P4 (0.0/0.0 dB)> <P5 (0.0/2.0 dB)> <P6 (0.0/2.5 dB)> <P7 (-6.0/3.5 dB)> <P8 (-3.5/3.5 dB)> <P9 (0.0/3.5 dB)>	PCIe Upstream Tx Prese
Miscellaneous Configuration	Static text	N/A	
Inbound Configuration	Multipart item	<Disable>* <Enable>	Enable Inbound configuration

4.5.5.7.9 Socket 0, Device Hide Menu

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Socket Configuration		
C-Stack Devhide0	0	▲ If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding ⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit
C-Stack Devhide1	0	
C-Stack Devhide2	0	
C-Stack Devhide3	0	
C-Stack Devhide4	0	
C-Stack Devhide5	0	
C-Stack Devhide6	0	
C-Stack Devhide7	0	
P-Stack0 Devhide0	0	
P-Stack0 Devhide1	0	
P-Stack0 Devhide2	0	
P-Stack0 Devhide3	0	
P-Stack0 Devhide4	0	
P-Stack0 Devhide5	0	
P-Stack0 Devhide6	0	
P-Stack0 Devhide7	0	
P-Stack1 Devhide0	0	
P-Stack1 Devhide1	0	
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.			
Socket Configuration			
P-Stack1 Devhide2	0	▲ If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding ⇐: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
P-Stack1 Devhide3	0		
P-Stack1 Devhide4	0		
P-Stack1 Devhide5	0		
P-Stack1 Devhide6	0		
P-Stack2 Devhide7	0		
P-Stack2 Devhide0	0		
P-Stack2 Devhide1	0		
P-Stack2 Devhide2	0		
P-Stack2 Devhide3	0		
P-Stack2 Devhide4	0		
P-Stack2 Devhide5	0		
P-Stack2 Devhide6	0		
P-Stack2 Devhide7	0		
MCP0-Stack Devhide0	0		
MCP0-Stack Devhide1	0		
MCP0-Stack Devhide2	0		
MCP0-Stack Devhide3	0		
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.			



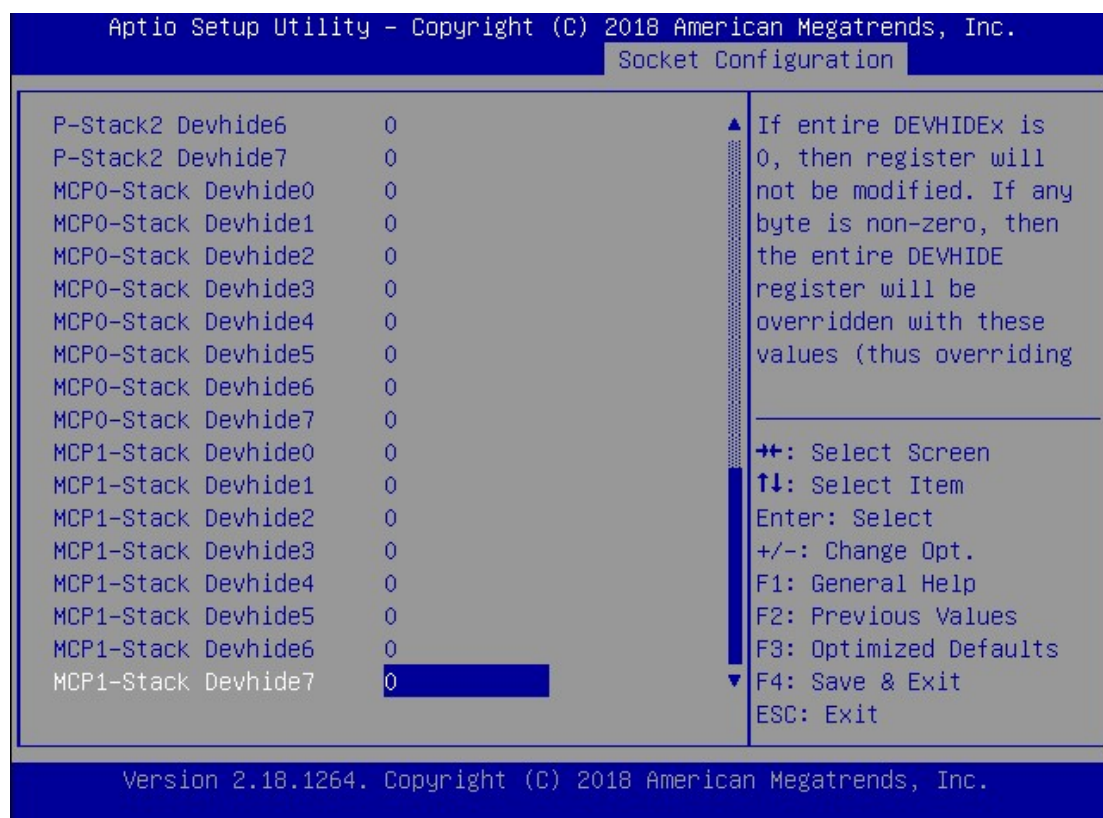
Item	Type	Options	Function description
C-Stack DevhideX X=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDE _X is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack0 DevhideY Y=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDE _X is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack1 DevhideZ Z=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDE _X is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these

			values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack2 DevhideA A=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
MCP0-Stack DevhideB B=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
MCP1-Stack DevhideC C=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).

4.5.5.7.10 Socket 1, Device Hide Menu

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.			
Socket Configuration			
C-Stack Devhide0	0	▲ If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding →+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
C-Stack Devhide1	0		
C-Stack Devhide2	0		
C-Stack Devhide3	0		
C-Stack Devhide4	0		
C-Stack Devhide5	0		
C-Stack Devhide6	0		
C-Stack Devhide7	0		
P-Stack0 Devhide0	0		
P-Stack0 Devhide1	0		
P-Stack0 Devhide2	0		
P-Stack0 Devhide3	0		
P-Stack0 Devhide4	0		
P-Stack0 Devhide5	0		
P-Stack0 Devhide6	0		
P-Stack0 Devhide7	0		
P-Stack1 Devhide0	0		
P-Stack1 Devhide1	0		
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.			

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.			
Socket Configuration			
P-Stack1 Devhide2	0	▲ If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding →+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults ▼ F4: Save & Exit ESC: Exit	
P-Stack1 Devhide3	0		
P-Stack1 Devhide4	0		
P-Stack1 Devhide5	0		
P-Stack1 Devhide6	0		
P-Stack1 Devhide7	0		
P-Stack2 Devhide0	0		
P-Stack2 Devhide1	0		
P-Stack2 Devhide2	0		
P-Stack2 Devhide3	0		
P-Stack2 Devhide4	0		
P-Stack2 Devhide5	0		
P-Stack2 Devhide6	0		
P-Stack2 Devhide7	0		
MCP0-Stack Devhide0	0		
MCP0-Stack Devhide1	0		
MCP0-Stack Devhide2	0		
MCP0-Stack Devhide3	0		
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.			



Item	Type	Options	Function description
C-Stack DevhideX X=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack0 DevhideY Y=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack1 DevhideZ Z=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these

			values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
P-Stack2 DevhideA A=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
MCP0-Stack DevhideB B=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).
MCP1-Stack DevhideC C=0~7	Numeric	0*~0xFFFFFFFF	If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).

4.5.6 Advanced Power Management Configuration



Item	Type	Options	Function description
Advanced Power Management Configuration	Static text	N/A	
use SPT workarounds	Multipart item	<Disable> <Enable>*	Enabled: use SPT workarounds - B2P cmd MISC_WORKAROUND_ENABLE
CPU P State Control	Submenu	N/A	P State Control Configuration Sub Menu, include Turbo, XE and etc.
Hardware PM State Control	Submenu	N/A	Hardware P-State setting
Overclocking	Submenu	N/A	Provide manual XE Ratio Limit setting
CPU C State Control	Submenu	N/A	CPU C State setting
Package C State Control	Submenu	N/A	Package C State setting
CPU Thermal Management	Submenu	N/A	CPU Thermal Related setting

CPU - Advanced PM Tuning	Submenu	N/A	Setting Energy Per Bias, Pwr_Ctl, PPO Current SWLTD, SAPM etc
Package Current Config	Submenu	N/A	Program PRI_PLANE_CURT_CFG_CTRL_MSR 0x601 Sub Menu
EPB Override Control	Submenu	N/A	Program CSR_DYNAMIC_PERF_POWER_CTL 1:10:2:0x64 Sub Menu
SOCKET RAPL Config	Submenu	N/A	SOCKET RAPL Configuration Sub Menu - TURBO_POWER_LIMIT CSR & MSR
PMAX CONFIG Configuration	Submenu	N/A	PMAX CONFIG Control Sub Menu
ACPI Sx State Control	Submenu	N/A	ACPI Sx State Control individually
Memory Power & Thermal Configuration	Submenu	N/A	Displays and provides option to change the Memory Settings

4.5.6.1 CPU P State Control



Item	Type	Options	Function description
CPU P State Control	Static text	N/A	
WFR Uncore GV Rate Reduction	Multipart item	< Disable >* < Enable > <Auto>	AUTO: Enable if WFR socket is detected in system. Enabled: Always enables WFR Uncore GV Rate Reduction.
Uncore Freq Scaling (UFS)	Multipart item	< Enable >* < Disable >	Enable/Disable autonomous uncore frequency scaling
SpeedStep (Pstates)	Multipart item	< Disable > < Enable >*	Enable/Disable EIST (P-States)
Config TDP	Multipart item	< Nominal>* < Level 1> < Level 2>	Config TDP level selection
P State Domain	Multipart item	< ALL>* < ONE>	Per Logical (ONE): indicates the P-state domain for each logical proc in the system. Per Package (ALL): all procs indicate the same

			domain in the same package.
EIST PSD Function	Multipart item	< HW_ALL>* < SW_ALL> < SW_ANY>	Choose HW_ALL/SW_ALL/SW_ANY in _PSD return
SINGLE_PCTL	Multipart item	< Disable >* < Enable >	Single PCTL Mode makes all cores in the processor go to the most recent ratio request
Single Power Domain (SPD)	Multipart item	< Disable >* < Enable >	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	Multipart item	< Max Performance>* < Max Efficient> < Set by Intel Node Manager>	Select the performance state that the BIOS will set before OS hand off.
Energy Efficient Turbo	Multipart item	< Enable >* < Disable >	Energy Efficient Turbo Disable, MSR 0x1FC [19]
Turbo Mode	Multipart item	< Disable > < Enable >*	Enable/Disable processor Turbo Mode (requires EMTTM enabled too).
CPU Flex Ratio Override	Multipart item	< Disable >* < Enable >	Enable/Disable CPU Flex Ratio Programming
CPU Core <u>Flex</u> Ratio	Numeric item	0-22,23*,24-100	Non-Turbo Mode Processor Core Ratio Multiplier
Perf P-Limit	Submenu	N/A	Program PERF_P_LIMIT 1:30:2:0xe4 Sub Menu

4.5.6.1.1 Perf P-Limit



Item	Type	Options	Function description
Perf P-Limit	Static text	N/A	
Perf P-Limit Differential	Numeric item	0,1*,2-7	Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.
Perf P-Limit Clip	Numeric item	0-30,31*	Maximum value the floor is allowed to be set to for perf P-limit.
Perf P-Limit Threshold	Numeric item	0-14,15*,16-31	Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.
Perf P Limit	Multipart item	< Disable > < Enable >*	Enable/Disable Performance P-Limit

4.5.6.2 Hardware PM State Control



Item	Type	Options	Function description
Hardware PM State Control	Static text	N/A	
Hardware P-States	Multipart item	< Disable > < Native Mode >* < Out of Band Mode> < Native Mode with No Legacy Support>	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States)\nNative Mode: Hardware chooses a P-state based on OS guidance\nOut of Band Mode: Hardware autonomously chooses a P-state (no OS guidance)
HardwarePM Interrupt	Multipart item	< Disable >* < Enable>	Enable/Disable Hardware PM Interrupt
EPP Enable	Multipart item	< Disable > < Enable>*	When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP
EPP profile	Multipart item	< Performance> < Balanced	Choose an HWPM Profile (EPP)

		Performance>* < Balanced Power> < Power>	
APS rocketing	Multipart item	< Enable> < Disable >*	Enable/Disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up
Scalability	Multipart item	< Enable> < Disable >*	Enable/Disable the use of scalability in HWP pcode power efficiency algorithms. Scalability is the measure of estimated performance improvement for a given increase in core frequency
PPO-Budget	Multipart item	< Enable> < Disable >*	Enable/disable core parameter based per core power budgeting. PPO-Budget allocates power budget to cores based on their scalability/EPP

4.5.6.3 Overclocking



Item	Type	Options	Function description
Overclocking	Static text	N/A	
Extreme Edition	Multipart item	< Disable > < Enable>*	Enable/Disable Extreme Edition support.
Overclocking Lock	Multipart item	< Disable > < Enable>*	Enable/Disable Overclocking.
TurboRatioLimit0	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCores0	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLimit1	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCores1	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLimit2	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)

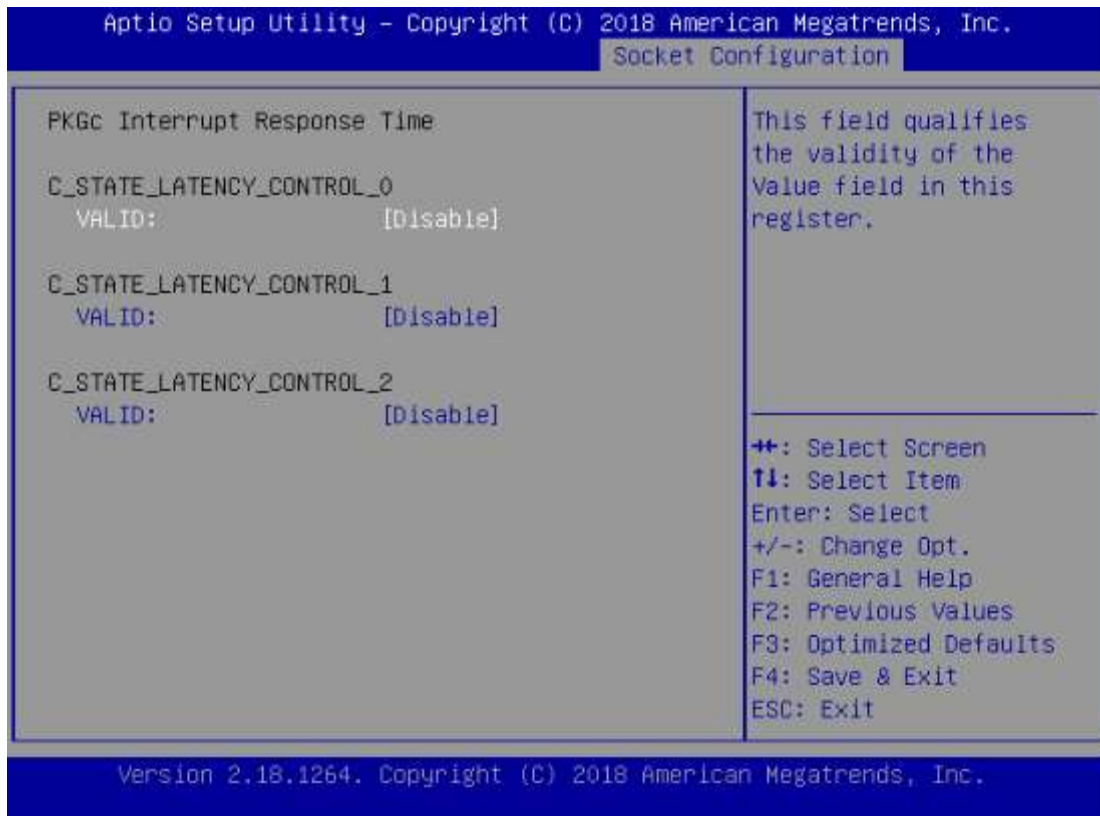
TurboRatioCo res2	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLi mit3	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCo res3	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLi mit4	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCo res4	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLi mit5	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCo res5	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLi mit6	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCo res6	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
TurboRatioLi mit7	Numeric item	0*,1-80	User defined Ratio for TurboRatioLimits Msr(0x1AD)
TurboRatioCo res7	Numeric item	0*,1-ff	User defined core# for TurboRatioLimits Msr(0x1AE)
LOT26 Enable	Multipart item	< Disable > < Enable>*	For HEDT *only*, select whether VR power is turned off to empty DIMM channels.

4.5.6.4 CPU C State Control



Item	Type	Options	Function description
CPU C State Control	Static text	N/A	
Autonomous Core C-State	Multipart item	< Disable >* < Enable>	Autonomous Core C-State Control
CPU C6 report	Multipart item	< Disable >* < Enable> <Auto>	Enable/Disable CPU C6(ACPI C3) report to OS
Enhanced Halt State (C1E)	Multipart item	< Disable > < Enable>*	Core C1E auto promotion Control. Takes effect after reboot.
OS ACPI Cx	Multipart item	< ACPI C2>* < ACPI C3>	Report CC3/CC6 to OS ACPI C2 or ACPI C3
PKGc Interrupt Response Time	Submenu	N/A	Programmable Package C-state interrupt response time setup control

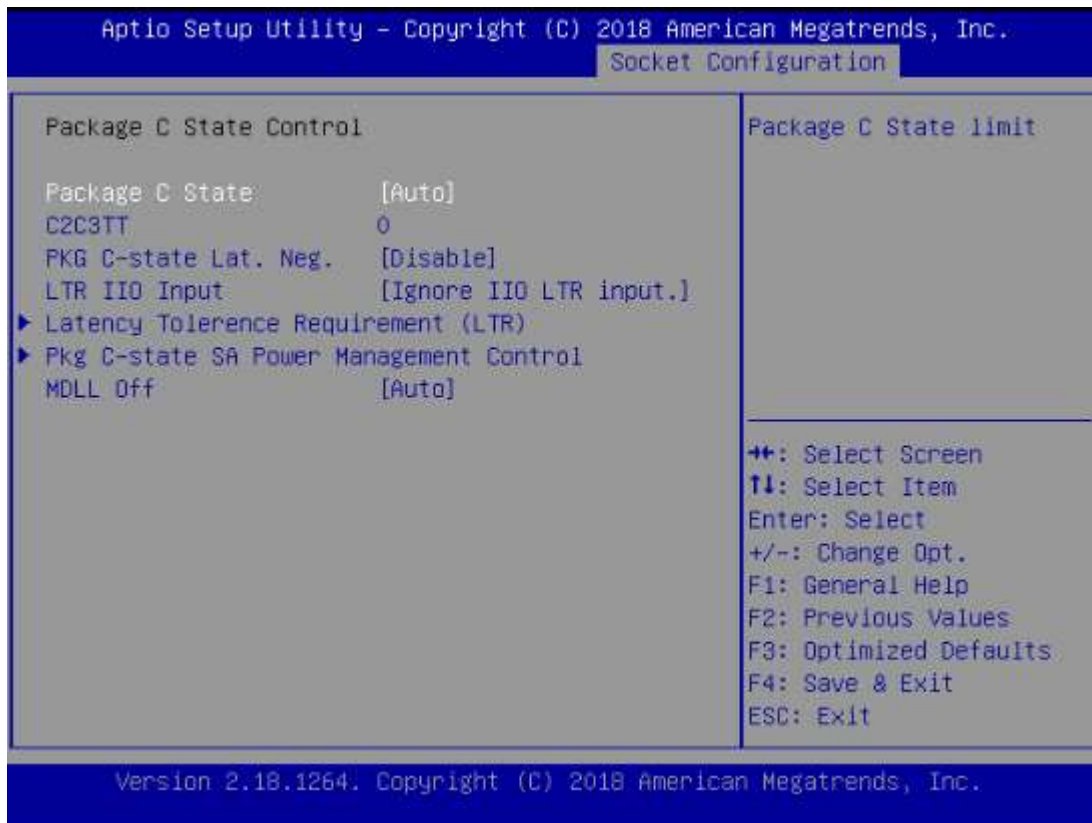
4.5.6.4.1 PKGc Interrupt Response Time



Item	Type	Options	Function description
PKGc Interrupt Response Time	Static text	N/A	
C_STATE_LATENCY_CONTROL_0	Static text	N/A	
VALID:	Multipart item	< Disable >* < Enable>	This field qualifies the validity of the Value field in this register.
MULTIPLIER:	Numeric item	0*,1-7	This field indicates the unit of measurement that is defined for the Value field in this register.
VALUE:	Numeric item	0*,1-0x1023	The Interrupt Response Time Limit is given in units defined in the Multiplier field of this register.
C_STATE_LATENCY_CONTROL_1	Static text	N/A	
VALID:	Multipart item	< Disable >* < Enable>	This field qualifies the validity of the Value field in this register.

MULTIPLIER:	Numeric item	0*,1-7	This field indicates the unit of measurement that is defined for the Value field in this register.
VALUE:	Numeric item	0*,1-0x1023	The Interrupt Response Time Limit is given in units defined in the Multiplier field of this register.
C_STATE_LATENCY_CONTROL_2	Static text	N/A	
VALID:	Multipart item	< Disable >* < Enable>	This field qualifies the validity of the Value field in this register.
MULTIPLIER:	Numeric item	0*,1-7	This field indicates the unit of measurement that is defined for the Value field in this register.
VALUE:	Numeric item	0*,1-0x1023	The Interrupt Response Time Limit is given in units defined in the Multiplier field of this register.

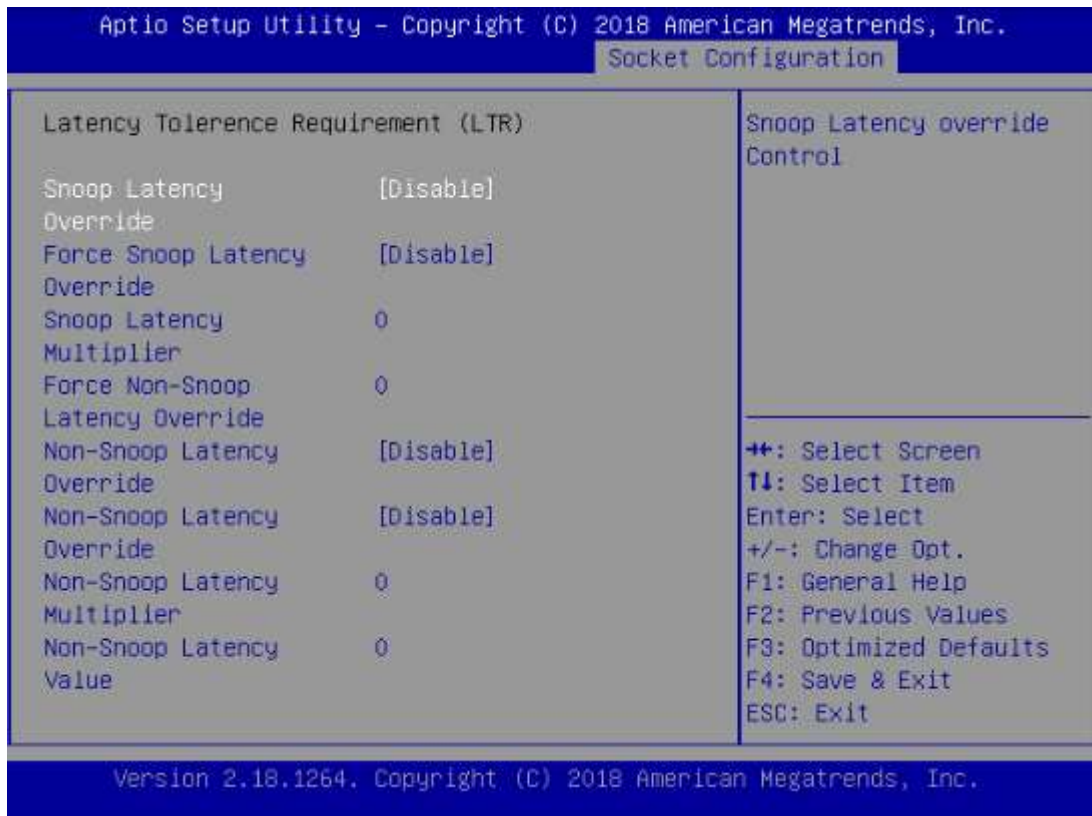
4.5.6.5 Package C State Control



Item	Type	Options	Function description
Package C State Control	Static text	N/A	
Package C State	Multipart item	< C0/C1 state > < C2 state > < C6(non Retention) state> < C6(Retention) state> < No Limit> <Auto>*	Package C State limit
C2C3TT	Numeric item	0*,1-255	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].
PKG C-state Lat. Neg.	Multipart item	< Disable >* < Enable>	MSR 1FCh Bit[30] = PCH_NEG_DISABLE
LTR IIO Input	Multipart	< Take IIO LTR	MSR 1FCh Bit[29] =

	item	input.> < Ignore IIO LTR input.>*	LTR_IIO_DISABLE. Disable = Ignore IIO LTR input.
Latency Tolerance Requirement (LTR)	Submenu	N/A	Program CSR_SWLTROVRD 1:10:1:0x78 Sub Menu
Pkg C-state SA Power Management Control	Submenu	N/A	Program CSR_SAPMCTL 1:30:1:0xb0 Sub Menu
MDLL Off	Multipart item	<Auto>* < Disable > < Enable>	Enable to shut down MDLL during SR

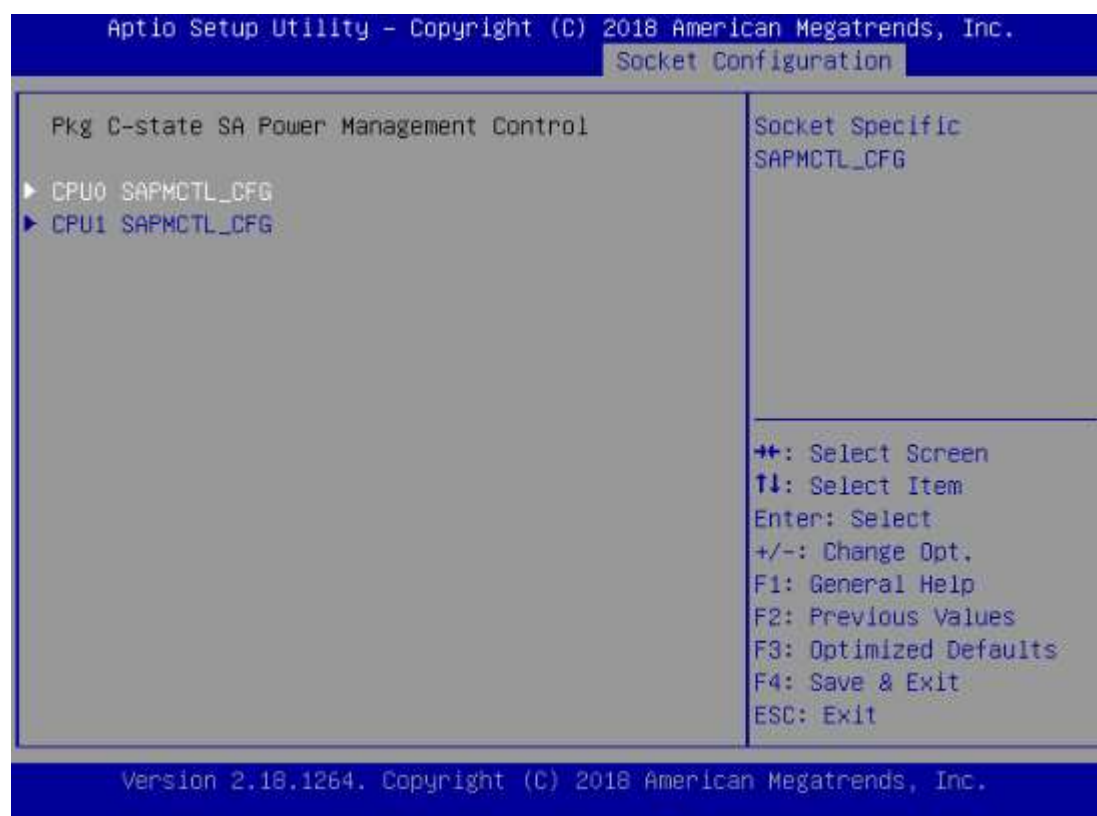
4.5.6.5.1 Latency Tolerance Requirement (LTR)



Item	Type	Options	Function description
Latency Tolerance Requirement (LTR)	Static text	N/A	
Snoop Latency Override	Multipart item	< Disable >* < Enable>	Snoop Latency override Control
Force Snoop Latency Override	Multipart item	< Disable >* < Enable>	Control to ignore PCIe LTR, and force the Snoop Latency value
Snoop Latency Multiplier	Numeric item	0*,1-7	Override Value is multiplied by this field to yield a time value
Force Non-Snoop Latency Override	Numeric item	0*,1-0x3ff	Control to ignore PCIe LTR, and force the Non-Snoop Latency value

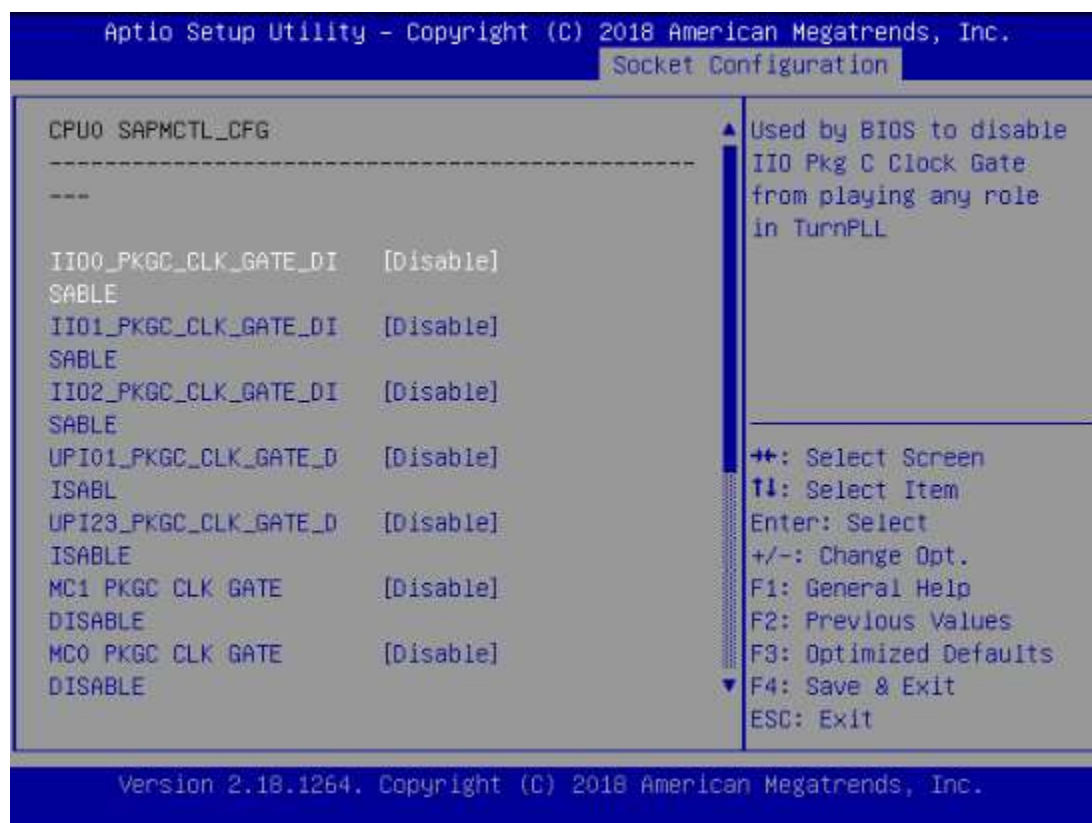
Non-Snoop Latency Override	Multipart item	< Disable >* < Enable>	Non-Snoop Latency override Control
Non-Snoop Latency Override	Multipart item	< Disable >* < Enable>	Force PCODE to always use values provided in SW_LTR_OVRD
Non-Snoop Latency Multiplier	Numeric item	0*,1-7	Override Value is multiplied by this field to yield a time value
Non-Snoop Latency Value	Numeric item	0*,1-0x3ff	Latency requirement for Non-Snoop requests

4.5.6.5.2 Pkg C-state SA Power Management Control



Item	Type	Options	Function description
Pkg C-state SA Power Management Control	Static text	N/A	
CPU0 SAPMCTL_CFG	Submenu	N/A	Socket Specific SAPMCTL_CFG
CPU1 SAPMCTL_CFG	Submenu	N/A	Socket Specific SAPMCTL_CFG

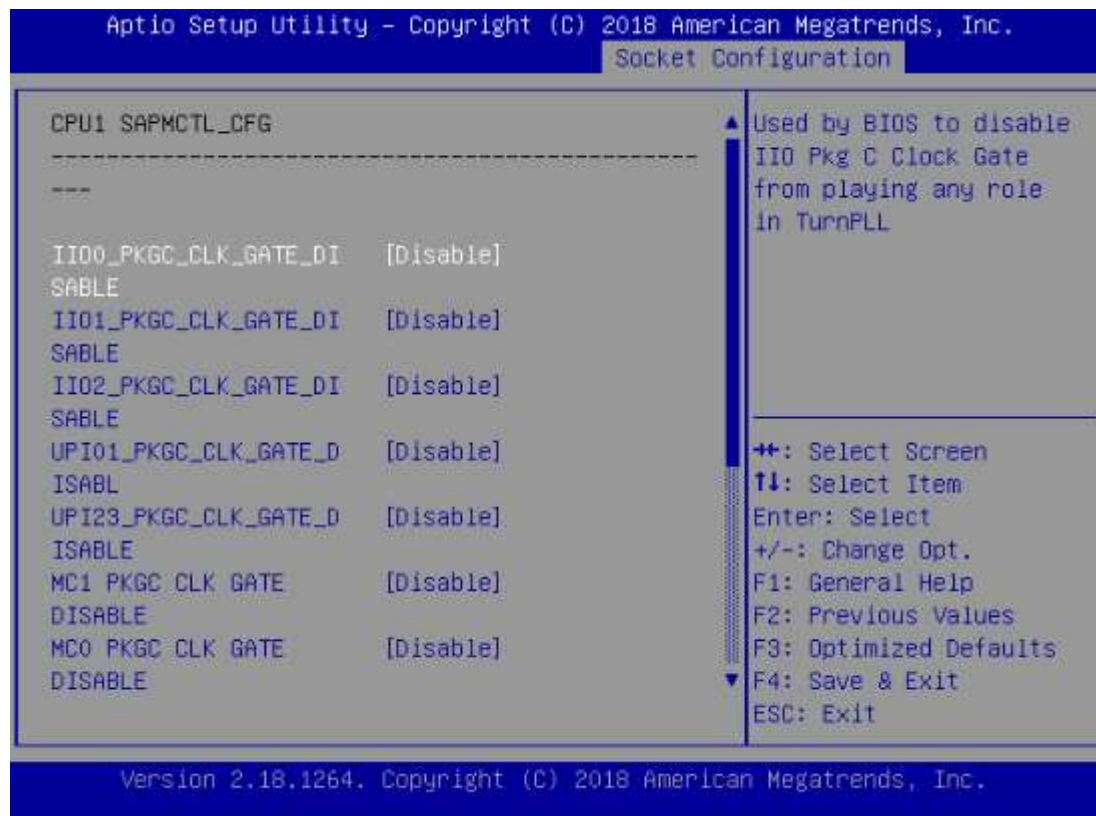
4.5.6.5.2.1 CPU0 SAPMCTL_CFG



Item	Type	Options	Function description
CPU0 SAPMCTL_CFG	Static text	N/A	
IIO0_PKGC_CLK_GATE_DISABLE	Multipart item	< Disable >* < Enable>	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
IIO1_PKGC_CLK_GATE_DISABLE	Multipart item	< Disable >* < Enable>	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
IIO2_PKGC_CLK_GATE_DISABLE	Multipart item	< Disable >* < Enable>	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
UPI01_PKGC_CLK_GATE_DISABLE	Multipart item	< Disable >* < Enable>	Used by BIOS to disable QPI01 Pkg C Clock Gate from playing any role in TurnPLL
UPI23_PKGC_CLK_GATE_DISABLE	Multipart item	< Disable >* < Enable>	Used by BIOS to disable QPI2 Pkg C Clock Gate from playing any role in TurnPLL

MC1 PKGC CLK GATE DISABLE	Multipart item	< Disable >* < Enable>	MC1 PKGC CLK GATE is Disabled when in PKG-C6 state
MC0 PKGC CLK GATE DISABLE	Multipart item	< Disable >* < Enable>	MC0 PKGC CLK GATE is Disabled in PKG-C6 state
UPI01 PLL Shutdown <u>En</u>	Multipart item	< Disable > < Enable>*	UPI01 PLL Shutdown Enable
UPI23 PLL Shutdown <u>En</u>	Multipart item	< Disable > < Enable>*	UPI23 PLL Shutdown Enable
PCIe IIO0 PLL Shutdown En	Multipart item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
PCIe IIO1 PLL Shutdown En	Multipart item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
PCIe IIO2 PLL Shutdown En	Multipart item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
MC0 PLLs Shutdown En	Multipart item	< Disable > < Enable>*	Memory PLLs Shutdown Enable
MC1 PLLs Shutdown En	Multipart item	< Disable > < Enable>*	Memory PLLs Shutdown Enable
SetVID Decay Disable	Multipart item	< Disable >* < Enable>	Used by BIOS to disable SETVID Decay to enable use of VR12. NOTE: Socket 0 setting will be applied for all sockets.
SAPMCTL_CFG LOCK	Multipart item	< Disable > < Enable>*	When set locks various PM registers

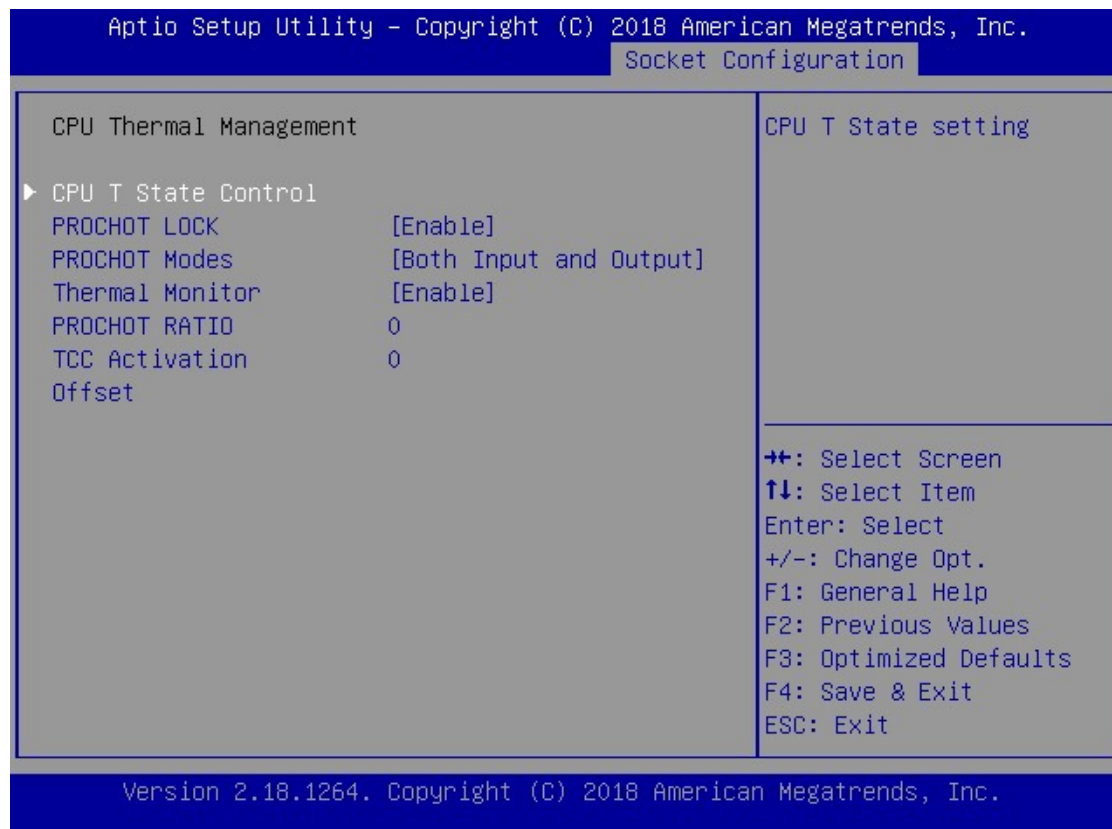
4.5.6.5.2.2 CPU1 SAPMCTL_CFG



Item	Type	Options	Function description
CPU1 SAPMCTL_CFG	Static text	N/A	
IIO0_PKGC_CLK_GATE_DISABLE	Multipar t item	< Disable > * < Enable >	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
IIO1_PKGC_CLK_GATE_DISABLE	Multipar t item	< Disable > * < Enable >	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
IIO2_PKGC_CLK_GATE_DISABLE	Multipar t item	< Disable > * < Enable >	Used by BIOS to disable IIO Pkg C Clock Gate from playing any role in TurnPLL
UPI01_PKGC_CLK_GATE_DISABLE	Multipar t item	< Disable > * < Enable >	Used by BIOS to disable QPI01 Pkg C Clock Gate from playing any role in TurnPLL
UPI23_PKGC_CLK_GATE_DISABLE	Multipar t item	< Disable > * < Enable >	Used by BIOS to disable QPI2 Pkg C Clock Gate from playing any role in TurnPLL

MC1 PKGC CLK GATE DISABLE	Multipar t item	< Disable >* < Enable>	MC1 PKGC CLK GATE is Disabled when in PKG-C6 state
MC0 PKGC CLK GATE DISABLE	Multipar t item	< Disable >* < Enable>	MC0 PKGC CLK GATE is Disabled in PKG-C6 state
UPI01 PLL Shutdown <u>En</u>	Multipar t item	< Disable > < Enable>*	UPI01 PLL Shutdown Enable
UPI23 PLL Shutdown <u>En</u>	Multipar t item	< Disable > < Enable>*	UPI23 PLL Shutdown Enable
PCIe IIO0 PLL Shutdown En	Multipar t item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
PCIe IIO1 PLL Shutdown En	Multipar t item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
PCIe IIO2 PLL Shutdown En	Multipar t item	< Disable > < Enable>*	PCIe PLL Shutdown Enable
MC0 PLLs Shutdown En	Multipar t item	< Disable > < Enable>*	Memory PLLs Shutdown Enable
MC1 PLLs Shutdown En	Multipar t item	< Disable > < Enable>*	Memory PLLs Shutdown Enable
SetVID Decay Disable	Multipar t item	< Disable >* < Enable>	Used by BIOS to disable SETVID Decay to enable use of VR12. NOTE: Socket 0 setting will be applied for all sockets.
SAPMCTL_CFG LOCK	Multipar t item	< Disable > < Enable>*	When set locks various PM registers

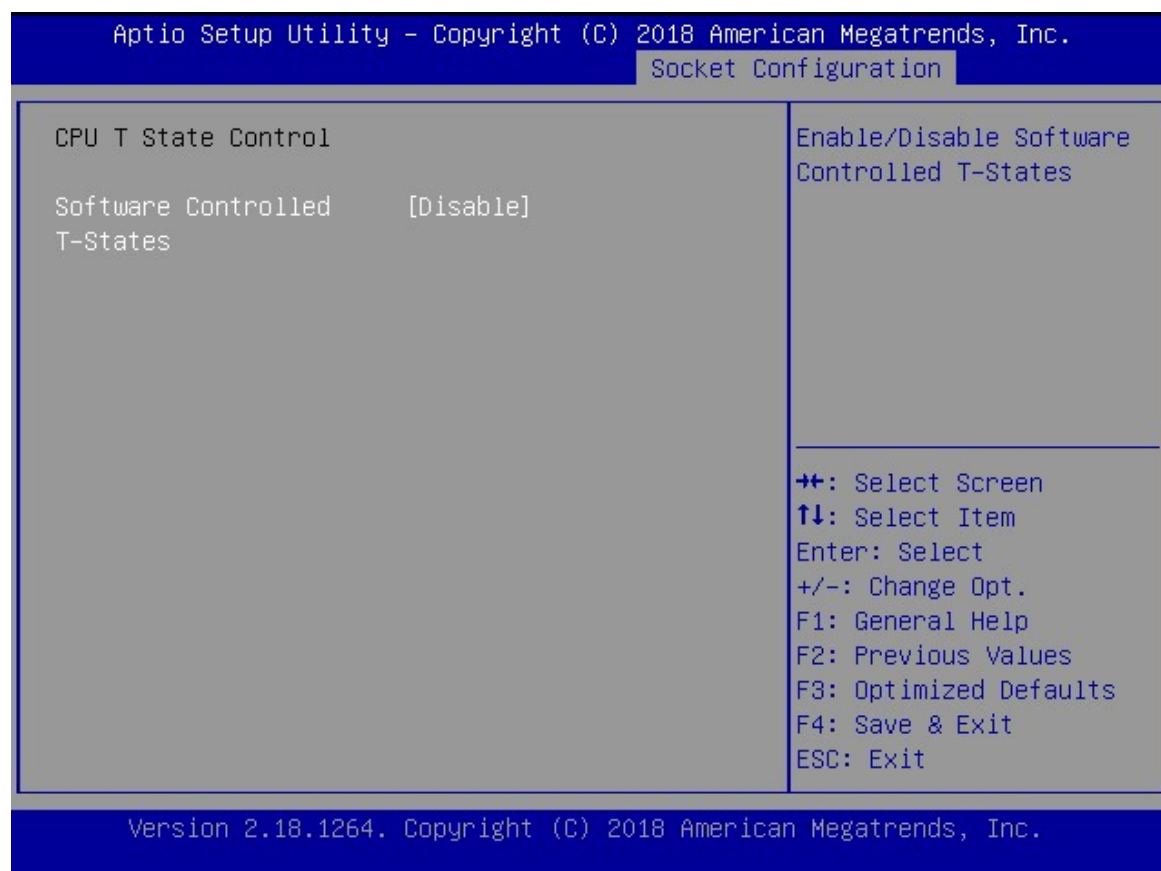
4.5.6.6 CPU Thermal Management



Item	Type	Options	Function description
CPU Thermal Management	Static text	N/A	
CPU T State Control	Submenu	N/A	
PROCHOT LOCK	Multipart item	<Disable> <Enable>*	Setting this bit will lock in xxPROCHOT# response configurations including ENABLE_BIDIR_PROCHOT, DIS_PROCHOT_OUT, VR_THERM_ALERT_DISABLE, and PROCHOT_LOCK.
PROCHOT Modes	Multipart item	< Output-only > < Input-only > <Disable> < Both Input and Output >*	When a processor thermal sensor trips (either core), the PROCHOT# will be driven.\nIf bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.

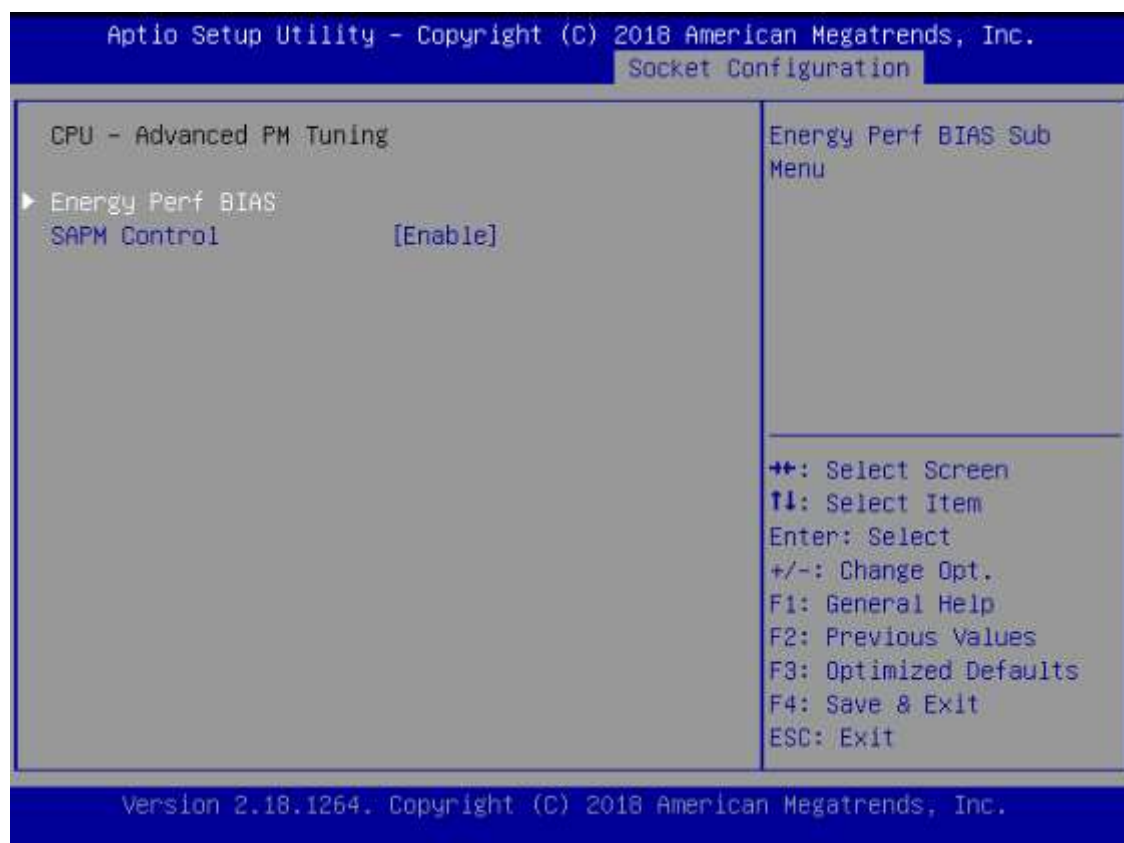
Thermal Monitor	Multipart item	<Disable> <Enable>*	Enable/Disable Thermal Monitor
PROCHOT RATIO	Numeric item	0* 0-0xFF	Controls the CPU response to an inbound platform assertion of xxPROCHOT# by capping to the programmed ratio. Default value 0 will allow ME to control this value. If ME does not set ratio, default 0 equates to Pn. A non-zero value will override ME setting. The min allowed ratio is defined by PLATFORM_INFO[MIN_OPERATING_RATIO]
TCC Activation Offset	Numeric item	0* 0-0xF	Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated.

4.5.6.6.1 CPU T State Control



Item	Type	Options	Function description
CPU T State Control	Static text	N/A	
Software Controlled T-States	Multipart item	<Disable>* <Enable>	Enable/Disable Software Controlled T-States

4.5.6.7 CPU - Advanced PM Tuning



Item	Type	Options	Function description
CPU - Advanced PM Tuning	Static text	N/A	
Energy Perf BIAS	Submenu	N/A	Energy Perf BIAS Sub Menu
SAPM Control	Multipart item	<Disable> <Enable>*	MSR 1FCh Bit[22] = PWR_PERF_TUNING_DISABLE_S APM_CTRL

4.5.6.7.1 Energy Perf BIAS



Item	Type	Options	Function description
Energy Perf BIAS	Static text	N/A	
Power Performance Tuning	Multipart item	<OS Controls EPB>* <BIOS Controls EPB>	MSR 1FCh Bit[25] = PWR_PERF_TUNING_CFG_MODE E. Enable - Use IA32_ENERGY_PERF_BIAS input from the core; Disable - Use alternate perf BIAS input from ENERGY_PERF_BIAS_CONFIG
PECI PCS EPB	Multipart item	<OS controls EPB>* <PECI controls EPB using PCS>	Controls whether Peci has control over EPB
ENERGY_PERF_BIAS_CFG mode	Multipart item	<Performance>* <Balanced Performance>	Use input from ENERGY_PERF_BIAS_CONFIG mode selection. PERF/Balanced

		<Balanced Power> <Power>	Perf/Balanced Power/Power
Dynamic Loadline Switch	Multipart item	<Disable> <Enable>*	Dynamic Loadline Switch control. MSR 0x1FC[Bit24]
Workload Configuration	Multipart item	<UMA>* <NUMA>	This allows optimization for the workload characterization. The three options for selection
Averaging Time Window	Numeric item	0~0xFF [0x17]*	This is used to control the effective window of the average for C0 an P0 time
P0 TotalTimeThreshold Low	Numeric item	0~0x3F [0x23]*	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than this threshold
P0 TotalTimeThreshold High	Numeric item	0~0x3F [0x3A]*	The HW switching mechanism ENABLES the performance setting (0) when the total P0 time is greater than this threshold

4.5.6.8 Package Current Configuration

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

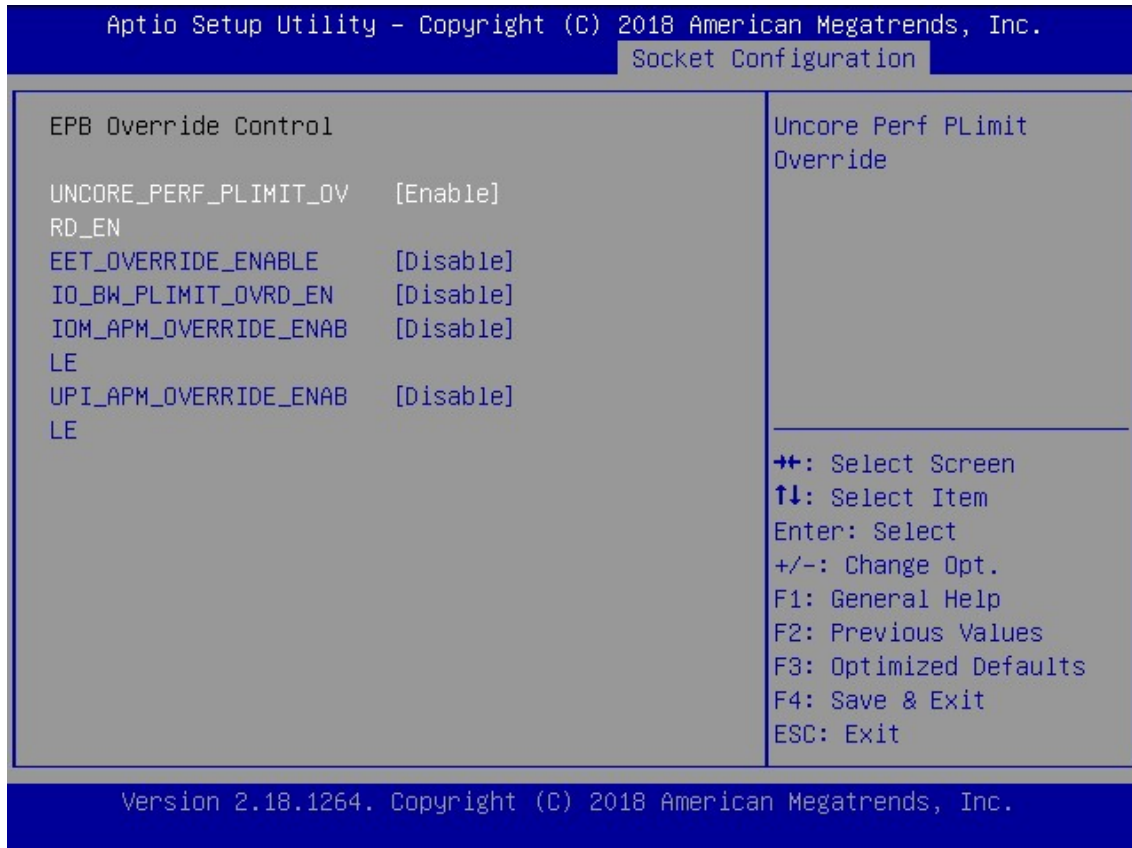
Socket Configuration

Package Current Config		0 - Default, do nothing; 1 - Manual, override Current limitation in 1/8 A increments. ⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Current Limit	[Disable]	
Override		
Lock Indication	[Enable]	

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

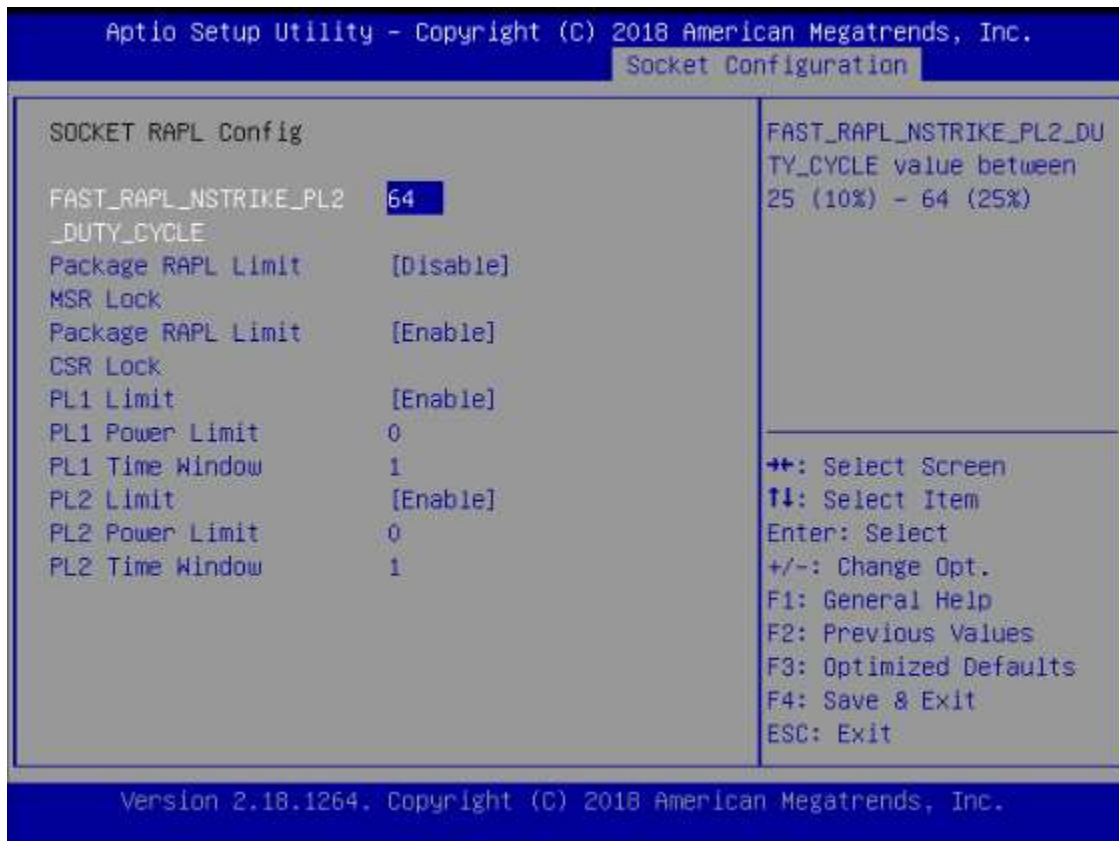
Item	Type	Options	Function description
Package Current config	Static text	N/A	
Current Limit Override	Multipart item	<Disable>* <Enable>	0 - Default, do nothing; 1 - Manual, override Current limitation in 1/8 A increments.
Lock Indication	Multipart item	<Disable> <Enable>*	Lock for CURRENT_LIMIT settings\ Move this into the Config Above

4.5.6.9 EPB Override Control



Item	Type	Options	Function description
EPB Override Control	Static text	N/A	
UNCORE_PERF_PLIMIT_OVRD_EN	Multipart item	<Disable> <Enable>*	Uncore Perf PLimit Override
EET_OVERRIDE_ENABLE	Multipart item	<Disable>* <Enable>	EET override
IO_BW_PLIMIT_OVRD_EN	Multipart item	<Disable>* <Enable>	IO BW PLimit Override
IOM_APM_OVERRIDE_ENABLE	Multipart item	<Disable>* <Enable>	IOM APM Override
UPI_APM_OVERRIDE_ENABLE	Multipart item	<Disable>* <Enable>	UPI APM Override

4.5.6.10 SOCKET RAPL Configuration



Item	Type	Options	Function description
SOCKET RAPL Config	Static text	N/A	
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	Numeric item	0~255 [64]*	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) - 64 (25%)
Package RAPL Limit MSR Lock	Multipart item	<Disable>* <Enable>	Enable/Disable locking of Package RAPL Limit MSR and a reset will be required to unlock the register.
Package RAPL Limit CSR Lock	Multipart item	<Disable> <Enable>*	Enable/Disable locking of Package RAPL Limit CSR and a reset will be required to unlock the register.
PL1 Limit	Multipart item	<Disable> <Enable>*	Enable/Disable PL1. If this option is disabled, BIOS will program the default values for PL1 Power Limit and PL1 Time Window.
PL1 Power Limit	Numeric item	0*~32767	PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is

			0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.
PL1 Time Window	Numeric item	0~56 [1]*	PL1 value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value should be maintained. If the value is 0, the fused value will be programmed.
PL2 Limit	Multipart item	<Disable> <Enable>*	Enable/Disable PL2. If this option is disabled, BIOS will program the default values for PL2 Power Limit and PL2 Time Window.
PL2 Power Limit	Numeric item	0*~32767	PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 125% * TDP
PL2 Time Window	Numeric item	0~56 [1]*	PL2 value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value should be maintained. If the value is 0, the fused value will be programmed.

4.5.6.11 PMAX CONFIG Configuration



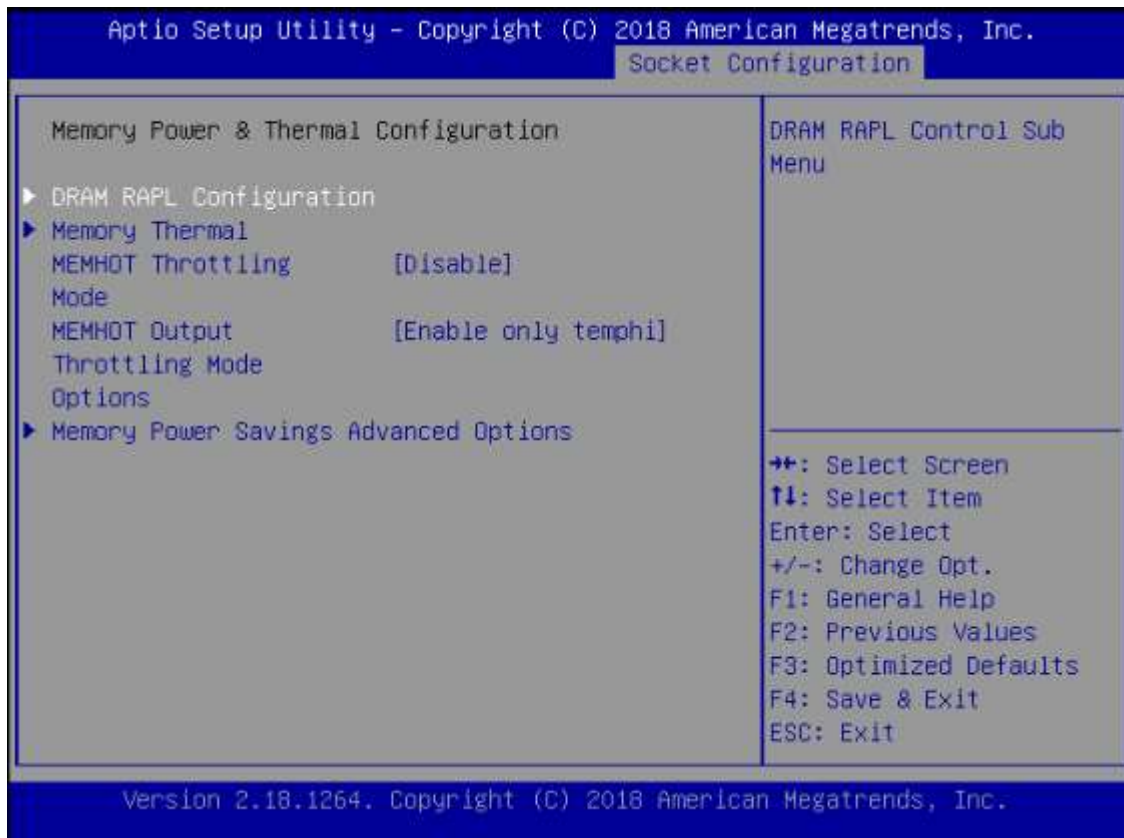
Item	Type	Options	Function description
PMAX CONFIG Configuration	Static text	N/A	
PMAX Config Sign	Multipart item	<Positive>* <Negative>	Controls whether PMAX Config offset is a positive or negative value.
PMAX Config Offset	Numeric item	0*~F	Input decimal correction factor to program. Valid input values are 0 to 15. Will be positive or negative based on PMAX Config Sign value.

4.5.6.12 ACPI Sx State Control



Item	Type	Options	Function description
ACPI Sx State Control	Static text	N/A	
ACPI S3	Multipart item	<Disable> <Enable>*	Control ACPI S3 State
ACPI S4	Multipart item	<Disable> <Enable>*	Control ACPI S4 State

4.5.6.13 Memory Power & Thermal Configuration



Item	Type	Options	Function description
Memory Power & Thermal Configuration	Static text	N/A	
DRAM RAPL Configuration	Submenu	N/A	DRAM RAPL Control Sub Menu
Memory Thermal	Submenu	N/A	Set memory thermal settings
MEMHOT Throttling Mode	Multipart item	<Disable>* <Output-only> <Input-only> <Input and Output Enabled>	MEMHOT Output Throttling Mode Options
MEMHOT Output Throttling Mode	Multipart item	<Disabled> <Enable only temphi>* <Enable only temphi & mid>	Configure MEMHOT Output Mode options: Enable/Disable the Throt Output high, mid and low

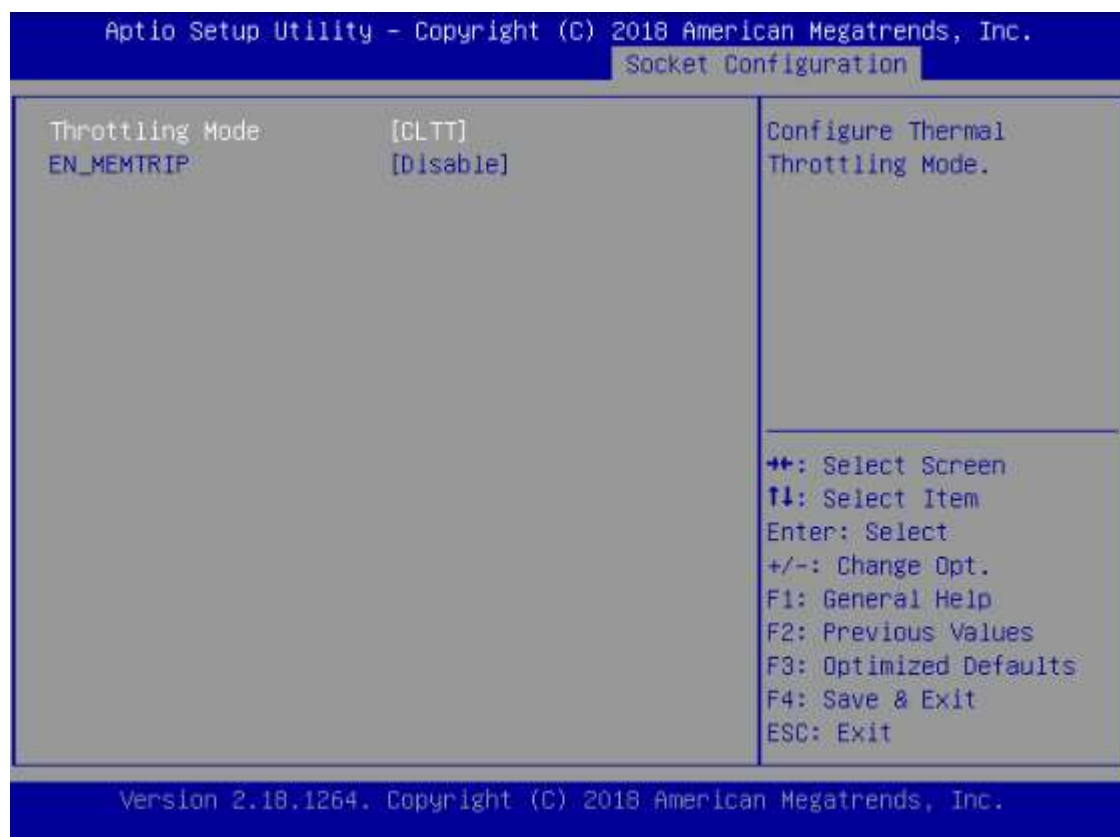
Options		<Enable only temphi, mid and low>	bit fields.
Memory Power Savings Advanced Options	Submenu	N/A	Advanced Settings for CKE and related Memory Power Savings Features

4.5.6.13.1 DRAM RAPL Configuration



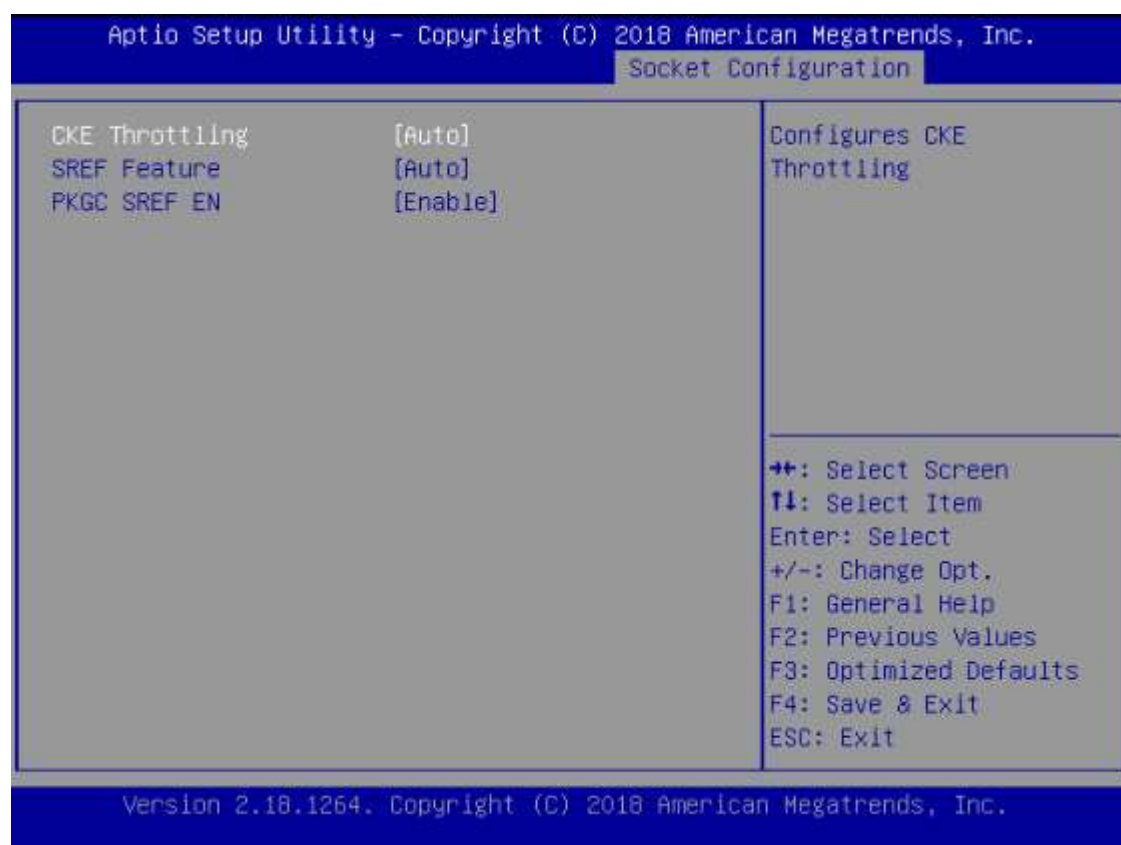
Item	Type	Options	Function description
DRAM RAPL Configuration	Static text	N/A	
Override BW_LIMIT_TF	Numeric item	0*~16	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled
DRAM RAPL Extended Range	Multipart item	<Disable> <Enable>*	Select DRAM RAPL Extended Range
CMS ENABLE DRAM PM	Multipart item	<Disable> <Enable>*	CMS ENABLE DRAM PM

4.5.6.13.2 Memory Thermal



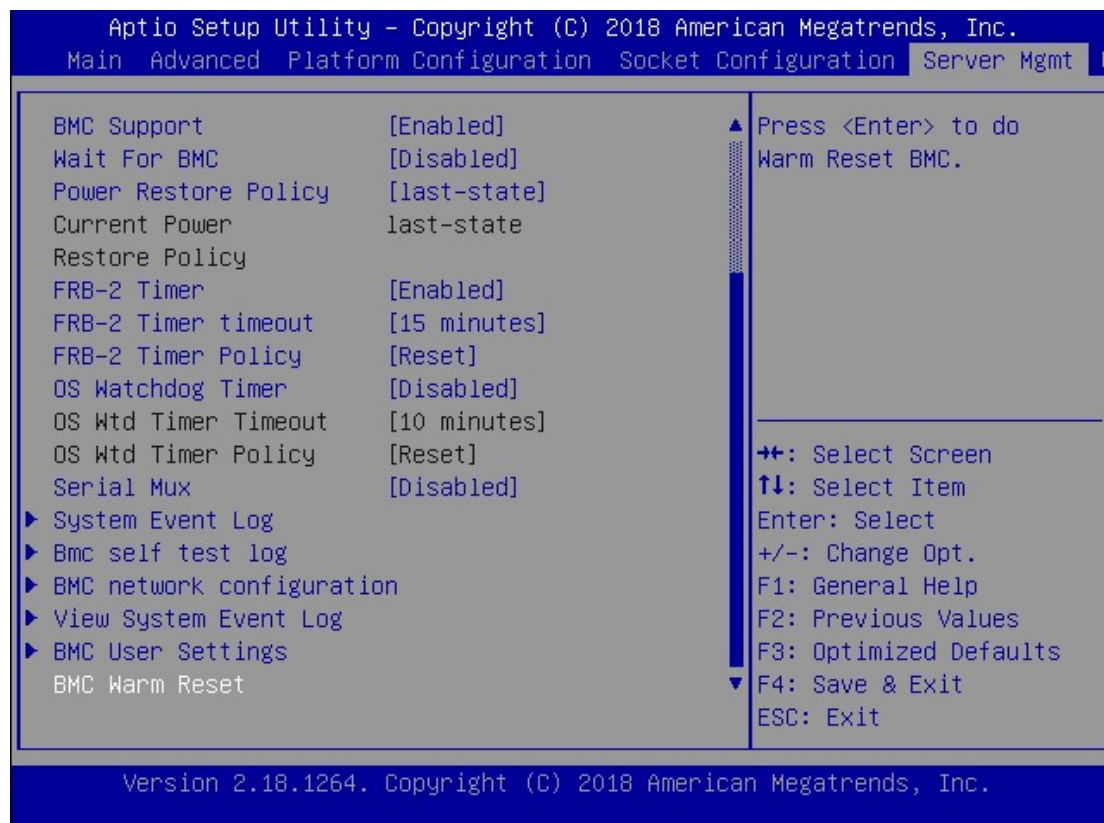
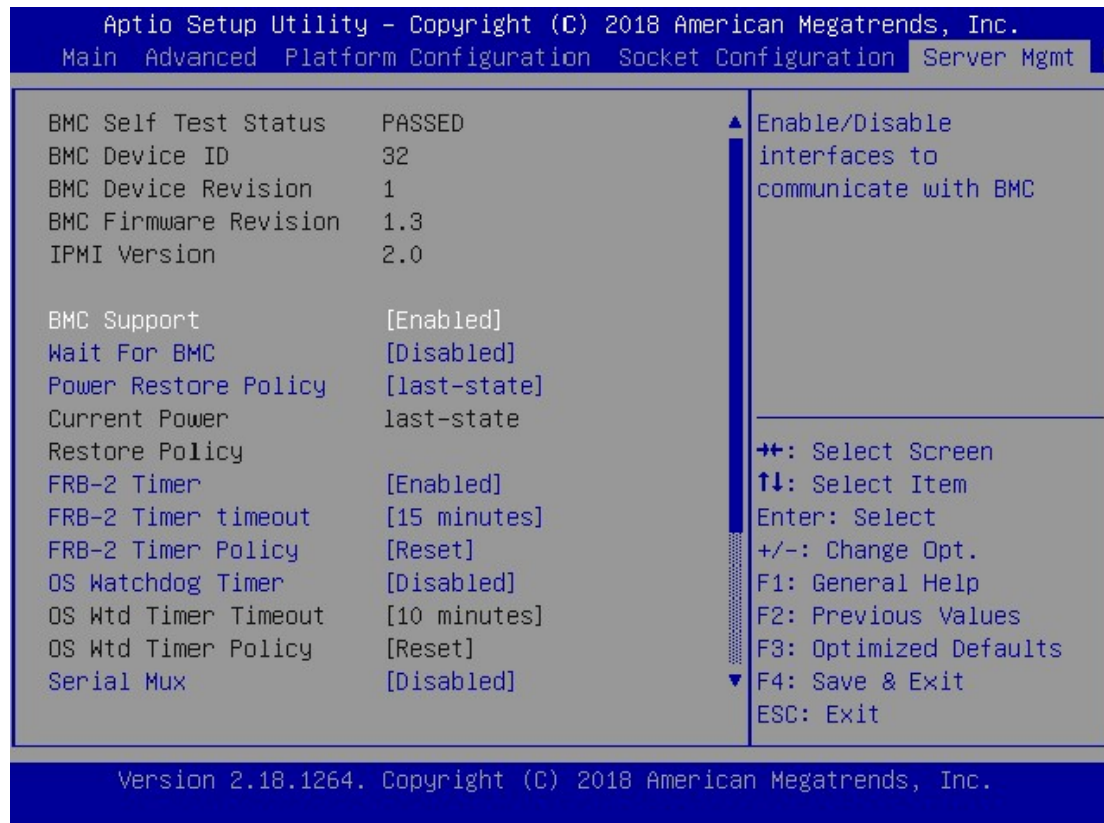
Item	Type	Options	Function description
Throttling Mode	Multipart item	<Disable> <OLTT> <CLTT>* <CLTT with PECI>	Configure Thermal Throttling Mode.
EN_MEMTRIP	Multipart item	<Disable>* <Enable>	If set to 0, processor will ignore MEMtrip. If set to 1 processor will include MEMtrip in ThermTrip tree.

4.5.6.13.3 Memory Power Savings Advanced Options



Item	Type	Options	Function description
CKE Throttling	Multipart item	<Auto>* <Manual>	Configures CKE Throttling
SREF Feature	Multipart item	<Auto>* <Manual>	SREF Feature
PKGC SREF EN	Multipart item	<Disable> <Enable>*	PKGC SREF EN

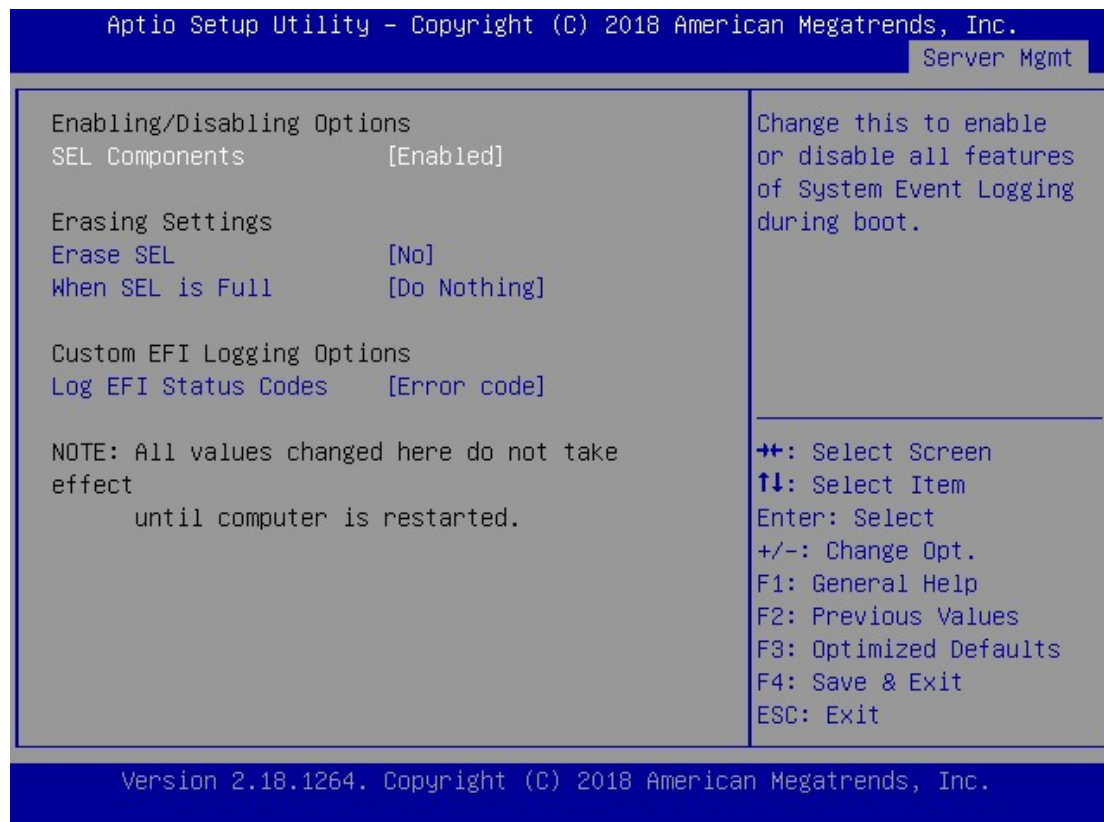
4.6 Server Management



Item	Type	Options	Function description
BMC Self Test Status	Dynamic text	PASSED	Show BMC Self Test status
BMC Device ID	Dynamic text	32	
BMC Device Revision	Dynamic text	1	
BMC Firmware Revision	Dynamic text	x.y	
IPMI Version	Dynamic text	2.0	IPMI spec support
BMC Support	Multipart item	<Enabled>* <Disabled>	Enable/Disable interfaces to communicate with BMC
Wait For BMC	Multipart item	<Enabled> <Disabled>*	Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces
Power Restore Policy	Multipart item	<last state>* < always-on > <always-off>	Select always-on/always-off/last-state for ACPI state after a G3
Current Power Restore Policy	Dynamic text	status	Show current BMC Power Restore Policy
FRB-2 Timer	Multipart item	<Enabled> <Disabled>*	Enable or Disable FRB-2 timer(POST timer)
FRB-2 Timer timeout	Multipart item	<3 minutes> <4 minutes> <5 minutes> <6 minutes> <15 minutes>*	Enter value Between 3 to 15 min for FRB-2 Timer Expiration value
FRB-2 Timer Policy	Multipart item	<Do Nothing> <Reset>* <Power Down> <Power Cycle>	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled
OS Watchdog Timer	Multipart item	<Enabled> <Disabled>*	If enabled, starts a BIOS timer which can only be shut off by Intel® Management Software after the OS loads. Helps

			determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy
OS Wtd Timer Timeout	Multipart item	<5 minutes> <10 minutes>* <15 minutes> <20 minutes>	Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled
OS Wtd Timer Policy	Multipart item	<Do Nothing> <Reset>* <Power Down>	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled
Serial Mux	Multipart item	<Enabled> <Disabled>*	Press <Enter> to enable or disable Serial Mux configuration
System Event Log	Submenu	N/A	Press <Enter> to change the SEL event log configuration.
BMC Self test log	Submenu	N/A	Logs the report returned by BMC self test command
BMC network configuration	Submenu	N/A	Configure BMC network parameters
View System Event Log	Submenu	N/A	Press <Enter> to view the System Event Log Records.
BMC User Settings	Submenu	N/A	Press <Enter> to Add, Delete and Set Privilege level for users.
BMC Warm Reset	Executing item		Press <Enter> to do Warm Reset BMC

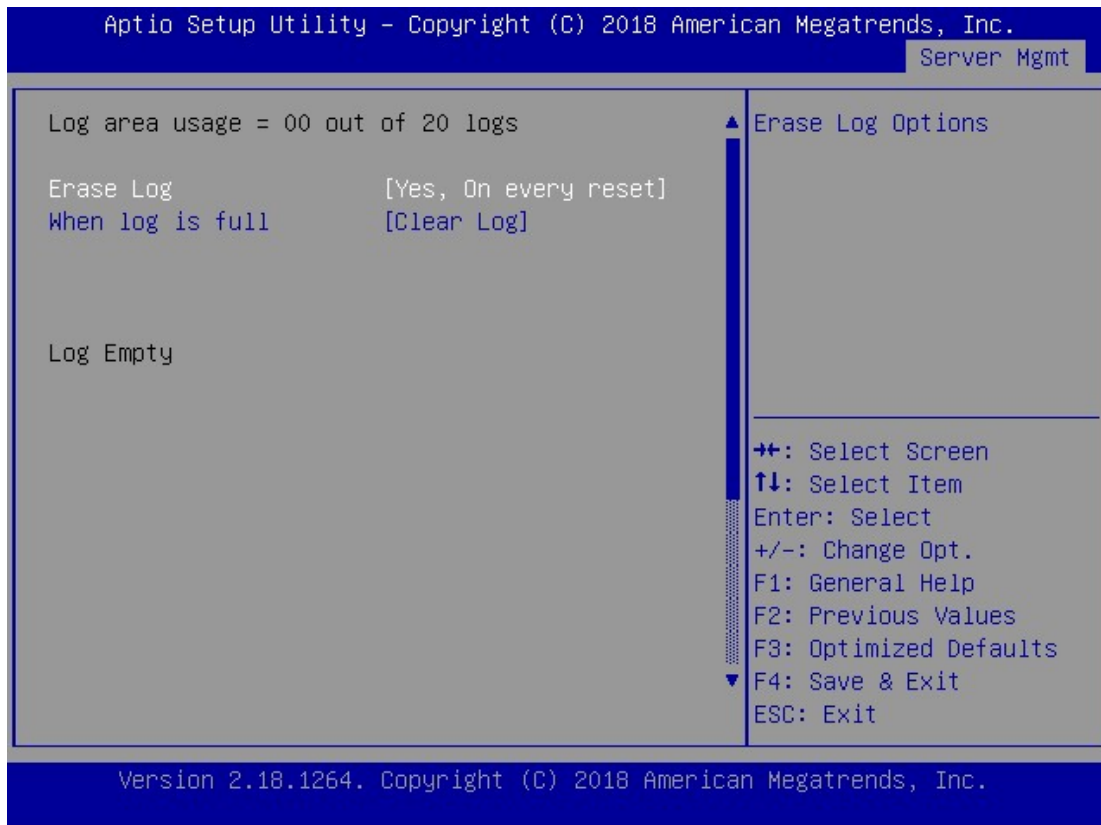
4.6.1 System Event Log



Item	Type	Options	Function description
Enabling/Disabling Options	Static text	N/A	
SEL Components	Multipart item	<Disabled> <Enabled>*	Change this to enable or disable all features of System Event Logging during boot.
Erasing Settings	Static text	N/A	
Erase SEL	Multipart item	<No>* <Yes, On next reset> <Yes, On every reset>	Choose options for erasing SEL.
When SEL is Full	Multipart item	<Do Nothing>* <Erase Immediately>	Choose options for reactions to a full SEL
Customer EFI Logging Options	Static text	N/A	
Log EFI Status Codes	Multipart item	<Disabled> <Both>	Enable or disable the logging of EFI Status Codes (if not already

		<Error Code>* <Progress Code>	converted to legacy).
NOTE: All values changed here do not take effect	Static text	N/A	
until computer is restarted.	Static text	N/A	

4.6.2 BMC Self Test log



Item	Type	Options	Function description
Log area usage	Dynamic text		
Erase Log	Multipart item	<Yes, On every reset>* <No>	Erase Log Options
When log is full	Multipart item	<Clear Log>* <Do not log any more>	Select the action to be taken when log is full
Log info	Dynamic text		

4.6.3 BMC network configuration

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

Server Mgmt

--BMC network configuration--

Configure IPv4 support

Lan channel 1
Configuration [Unspecified]
Address source
Current DynamicAddressBmcDhcp
Configuration
Address source
Station IP address 0.0.0.0
Subnet mask 0.0.0.0
Station MAC address 00-22-4d-d5-d3-de
Router IP address 0.0.0.0
Router MAC address 00-00-00-00-00-00

Lan channel 2

▲ Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

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

Server Mgmt

Configuration [Unspecified]
Address source
Current Unspecified
Configuration
Address source
Station IP address 0.0.0.0
Subnet mask 0.0.0.0
Station MAC address 00-00-00-00-00-00
Router IP address 0.0.0.0
Router MAC address 00-00-00-00-00-00

Configure IPv6 support

Lan channel 1
IPv6 Support [Enabled]

▲ Enable or Disable LAN1 IPV6 Support

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		Server Mgmt
Configuration	[Unspecified]	▲ Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS
Address source		
Current Configuration	DynamicAddressBmcDhcp	
Address source		
Station IPv6 address	::	
Prefix Length	0	
IPv6 Router1 IP Address	::	
IPv6 address status	Active	
IPv6 DHCP Algorithm	DHCPv6	
		▲ Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		Server Mgmt
Station IPv6 address	::	▲ Enable or Disable LAN1 IPv6 Support
Prefix Length	0	
IPv6 Router1 IP Address	::	
IPv6 address status	Active	
IPv6 DHCP Algorithm	DHCPv6	
Lan channel 2		
IPv6 Support	[Disabled]	
IPv6 is not supported in BMC (OR) IPv6 Support is Disabled.		▲ Enable or Disable LAN1 IPv6 Support ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.		

Item	Type	Options	Function description
--BMC network configuration--	Static text	N/A	
***** *****	Static text	N/A	
Configure IPV4 support	Static text	N/A	
***** *****	Static text	N/A	
Lan channel 1	Static text		
Configuration Address Source	Multipart item	<Unspecified>* <Static> <DynamicBmcDhcp> <DynamicBmcNonDhcp>	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Current Configuration	Dynamic text	DynamicAddressBmcDhcp	
Address Source	Static text	N/A	
Station IP address	Dynamic text	IP address	
Subnet mask	Dynamic text	IP mask	
Station MAC address	Dynamic text	MAC address	
Router IP address	Dynamic text	IP address	
Router MAC address	Dynamic text	MAC address	
Lan channel 2	static text		
Configuration Address Source	Multipart item	<Unspecified>* <Static> <DynamicBmcDhcp> <DynamicBmcNonDhcp>	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network

			parameters during BIOS phase
Current Configuration	Dynamic text	Unspecified	
Address Source	Static text	N/A	
Station IP address	Dynamic text	IP address	
Subnet mask	Dynamic text	IP mask	
Station MAC address	Dynamic text	MAC address	
Router IP address	Dynamic text	IP address	
Router MAC address	Dynamic text	MAC address	
***** *****	Static text	N/A	
Configure IPV6 support	Static text	N/A	
***** *****	Static text	N/A	
Lan channel 1	Static text	N/A	
IPV6 Support	Multipart item	<Enabled>* <Disabled>	Enable or Disable LAN1 IPV6 Support
Configuration Address Source	Multipart item	<Unspecified>* <Static> <DynamicBmcDhcp> <DynamicBmcNonDhcp>	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Station IPV6 address	Dynamic text	IP address	
Prefix Length	Dynamic text	Prefix	
IPV6 Router 1 IP address	Dynamic text	IP address	

IPV6 address status	Dynamic text		
IPV6 DHCP Algorithm	Dynamic text		
Lan channel 2	Static text	N/A	
IPV6 Support	Multipart item	<Enabled> <Disabled>*	Enable or Disable LAN1 IPV6 Support
IPV6 is not supported in BMC (OR) IPV6 Support is Disabled.	Static text	N/A	

4.6.4 View System Event Log

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

Server Mgmt

No. of log entries in SEL : 592

DATE	TIME	SENSOR TYPE
01/01/00	00:00:53	Event Logging Disabled
01/01/00	00:00:56	Button/Switch
01/01/00	00:00:56	Other Units-Based Sensor
01/01/00	00:00:57	Other Units-Based Sensor
01/01/00	00:00:11	System Event
01/01/00	00:00:11	System Event
01/01/00	00:00:11	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:12	Other Units-Based Sensor
01/01/00	00:00:13	Other Units-Based Sensor

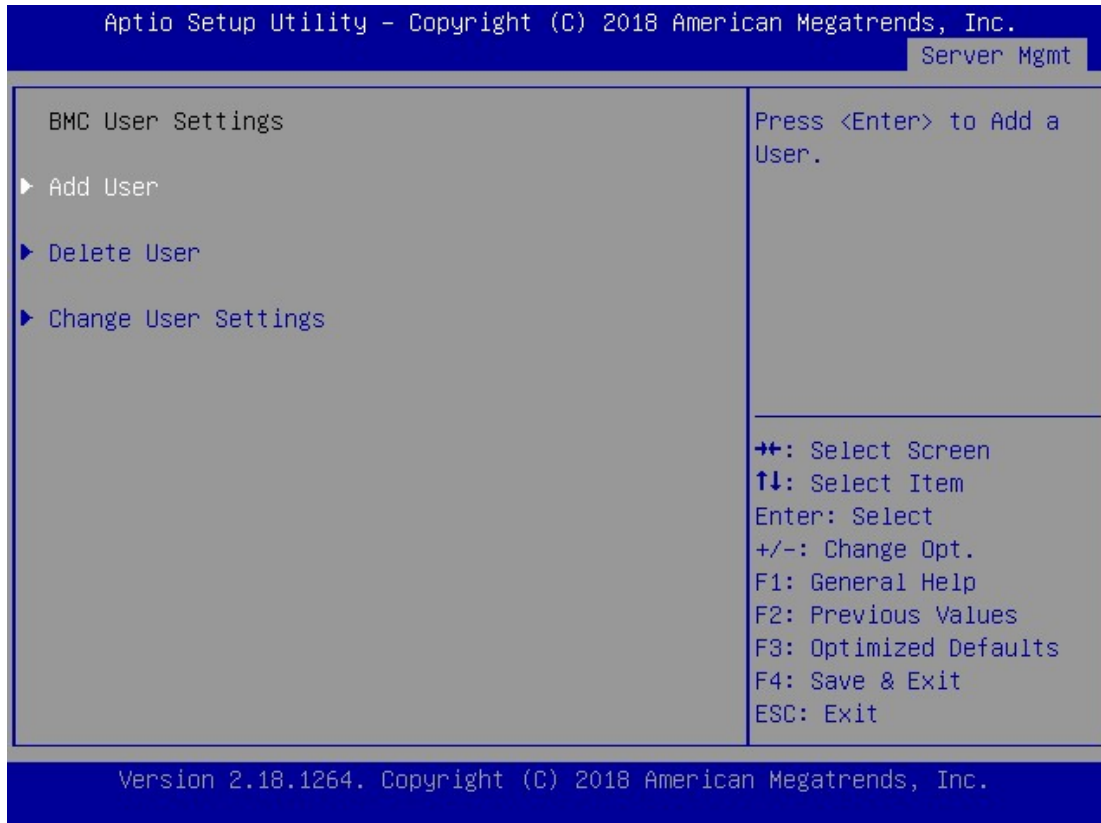
▲ HEX:
 01 00 02 B5 43 6D
 38 20 00 04 10 5F
 6F 02 FF FF
 Generator ID: BMC - LUN
 #0 (Channel #0)
 Sensor Number: 0x5F
 Reserved or Unknown

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
No. of log entries in SEL :	Dynamic text		
Log info	Dynamic text		

4.6.5 BMC User Settings



Item	Type	Options	Function description
BMC User Settings	Static text	N/A	
Add User	Submenu	N/A	Press <Enter> to Add a User.
Delete User	Submenu	N/A	Press <Enter> to Delete a User.
Change User Settings	Submenu	N/A	Press <Enter> to Change User Settings.

4.6.5.1 Add User

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

Server Mgmt

BMC Add User Details

User Name

User Password

Channel No 0

User Privilege Limit [Reserved]

Enter BMC User Name

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
BMC Add User Details	Static text	N/A	
User Name	String item		Enter BMC User Name
User Password	Password item		Enter BMC User Password
Channel No	Numeric item	0*~15	Enter BMC Channel Number
User Privilege Limit	Multipart item	[Reserved]*	Enter BMC User Privilege Limit for Selected Channel

4.6.5.2 Delete User

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.
 Server Mgmt

BMC Delete User Details User Name User Password	Enter BMC User Name ⇐+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
---	---

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
BMC Delete User Details	Static text	N/A	
User Name	String item		Enter BMC User Name
User Password	Password item		Enter BMC User Password

4.6.5.3 Change User Settings

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

Server Mgmt

BMC Change User Settings

User Name

User Password

User [Disable]

Change User Password

Channel No 0

User Privilege Limit [Reserved]

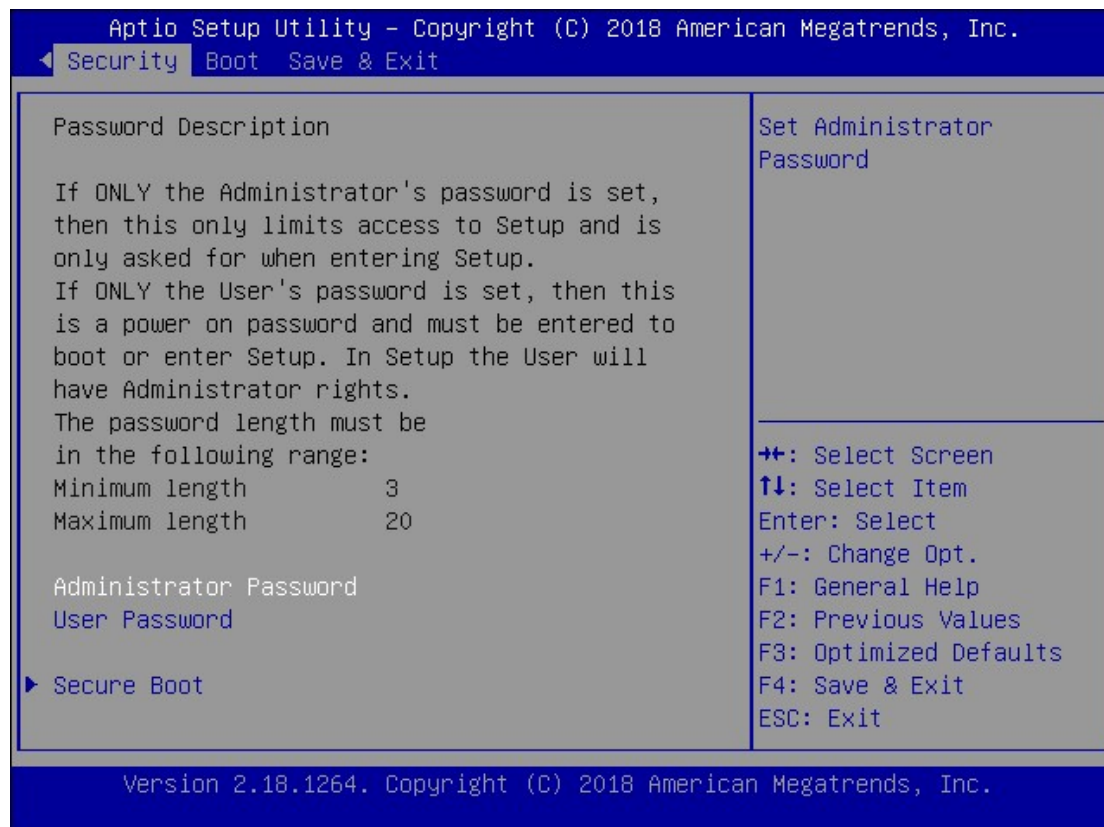
Enter BMC User Name

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

Version 2.18.1264. Copyright (C) 2018 American Megatrends, Inc.

Item	Type	Options	Function description
BMC Add User Details	Static text	N/A	
User Name	String item		Enter BMC User Name
User Password	Password item		Enter BMC User Password
User	Multipart item	<Enabled> <Disabled>*	Enable/Disable the User.
Change User Password	Password item		Enter New Password to change.
Channel No	Numeric item	0*~15	Enter BMC Channel Number
User Privilege Limit	Multipart item	[Reserved]*	Enter BMC User Privilege Limit for Selected Channel

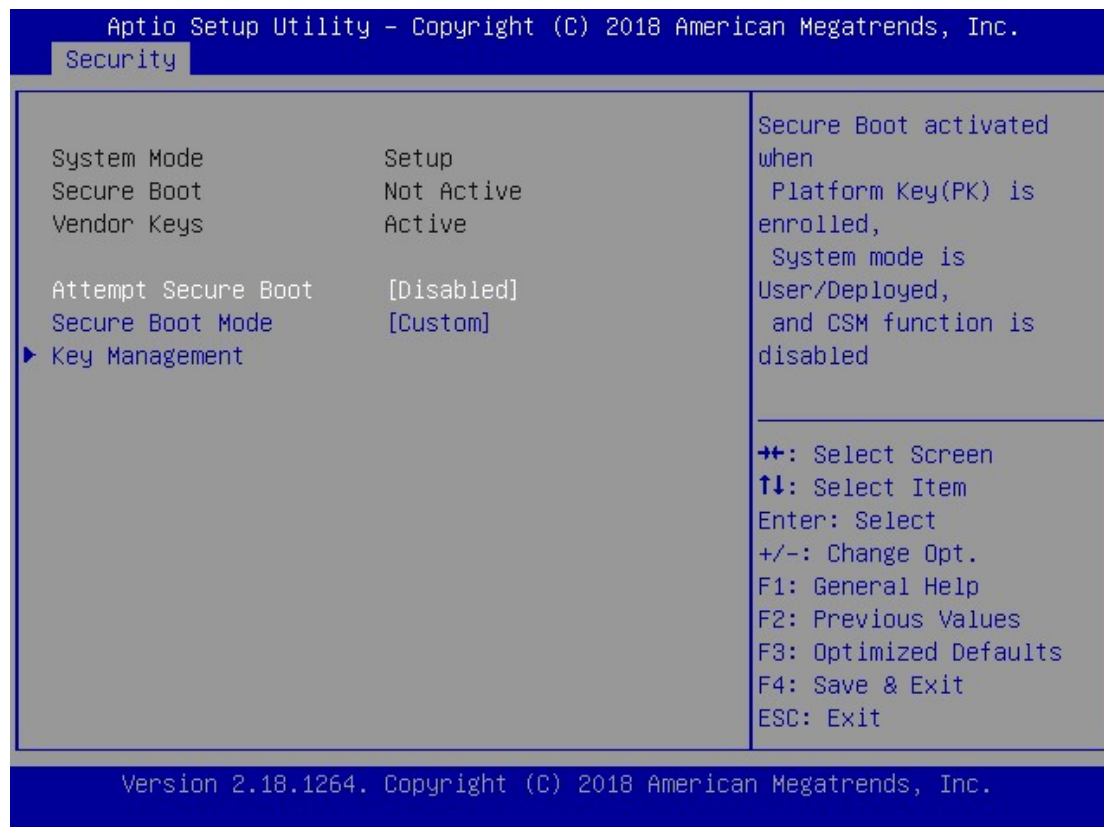
4.7 Security



Item	Type	Options	Function description
Password Description	Static text	N/A	
If ONLY the Administrator's password is set,	Static text	N/A	
then this only limits access to Setup and is	Static text	N/A	
only asked for when entering Setup.	Static text	N/A	
If ONLY the User's password is set, then this	Static text	N/A	
is a power on password and must be entered to	Static text	N/A	
boot or enter Setup. In Setup the User will	Static text	N/A	
have Administrator rights.	Static text	N/A	
in the following range:	Static text	N/A	
Minimum length	Dynamic text		

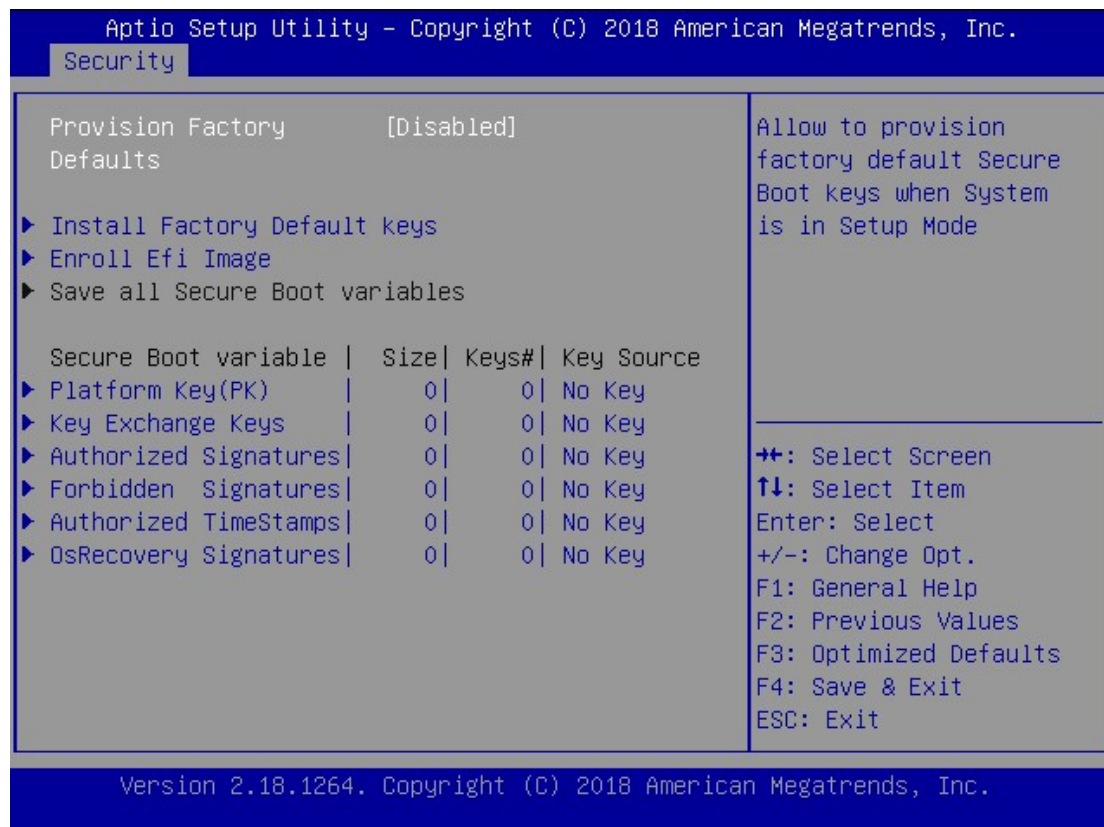
Maximum length	Dynamic text		
Administrator Password	Password item		Set Administrator Password
User Password	Password item		Set User Password
Secure Boot	Submenu	N/A	Customizable Secure Boot settings

4.7.1 Secure Boot



Item	Type	Options	Function description
System Mode	Static text	ASCII string	
Secure Boot	Static text	ASCII string	
Vendor Keys	Static text	ASCII string	
Attempt Secure Boot	Multipart item	<Disabled>* <Enabled>	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User/Deployed, and CSM function is disabled
Secure Boot Mode	Multipart item	<Standard> <Custom>*	Secure Boot mode selector: Standard/Custom. In Custom mode Secure Boot Variables can be configured without authentication
Key Management	Submenu	N/A	Enables expert users to modify Secure Boot Policy variables without full authentication

4.7.1.1 Key Management

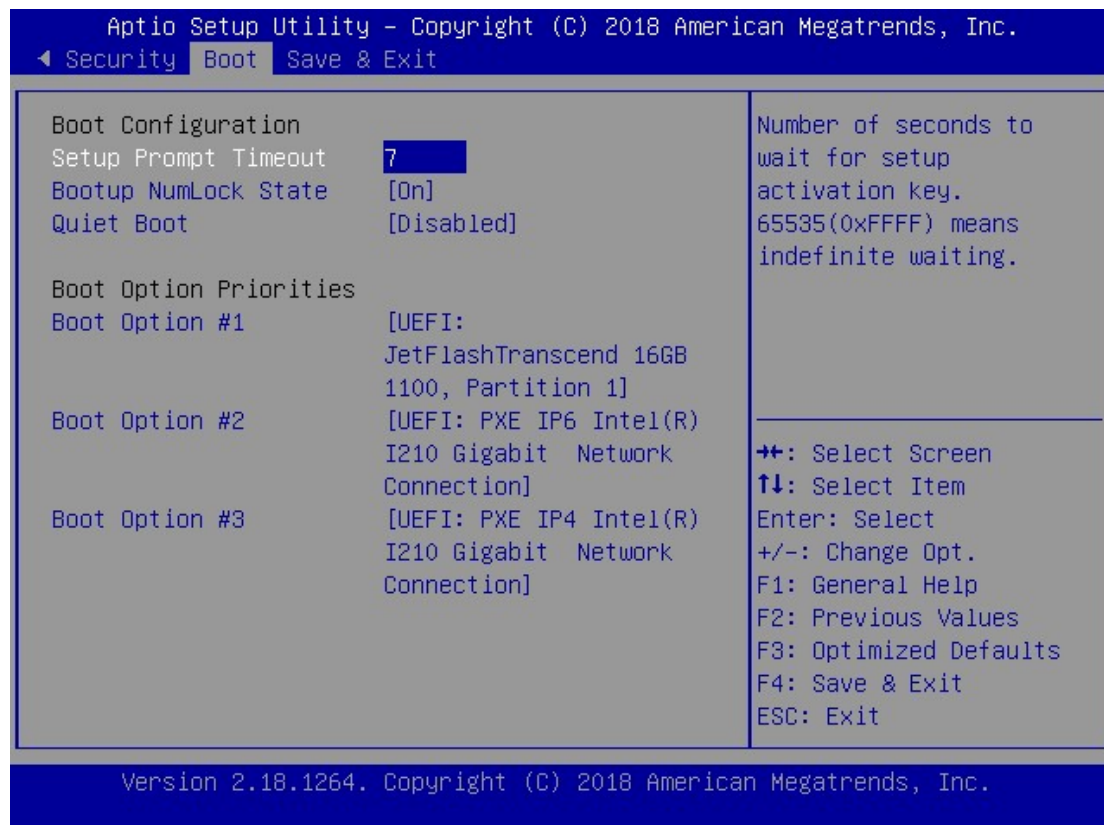


Item	Type	Options	Function description
Provision Factory Defaults	Multipart item	N/A	Allow to provision factory default Secure Boot keys when System is in Setup Mode
Install Factory Default keys	Executing item	Yes / No	Force System to User Mode - install all Factory Default keys
Enroll Efi Image	Executing item	Yes / No	Allow the image to run in Secure Boot mode. Enroll SHA256 hash of the binary into Authorized Signature Database (db)
Save all Secure Boot variables	Executing item	Yes / No	Save NVRAM content of Secure Boot policy variables to the files (EFI_SIGNATURE_LIST data format) in root folder on a target file system device
Security Boot Variable Size Keys# Key Source	Static text	N/A	

Platform Key(PK) Size Keys# Key Source	Executing item /Dynamic text	Save to File / Set New / Erase	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test
Key Exchange Keys Size Keys# Key Source	Executing item /Dynamic text	Save to File / Set New / Append / Erase	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test
Authorized Signatures Size Keys# Key Source	Executing item /Dynamic text	Save to File / Set New / Append / Erase	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test
Forbidden Signatures Size Keys# Key Source	Executing item /Dynamic text	Save to File / Set New / Append / Erase	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin)

			d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test
Authorized TimeStamps Size Keys# Key Source	Executing item /Dynamic text	Set New / Append	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test
OsRecovery Signatures Size Keys# Key Source	Executing item /Dynamic text	Set New / Append	Enroll Factory Defaults or load certificates from a file: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256,384,512 2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256) Key Source: Default,External,Mixed,Test

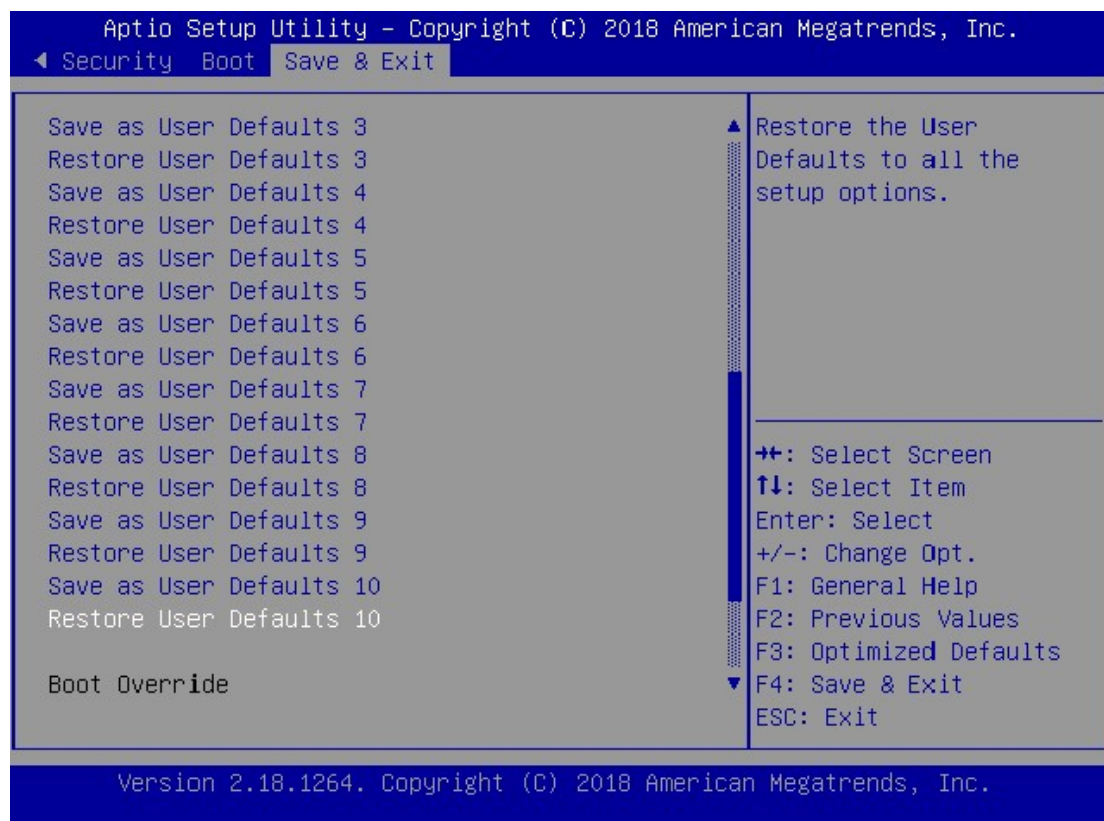
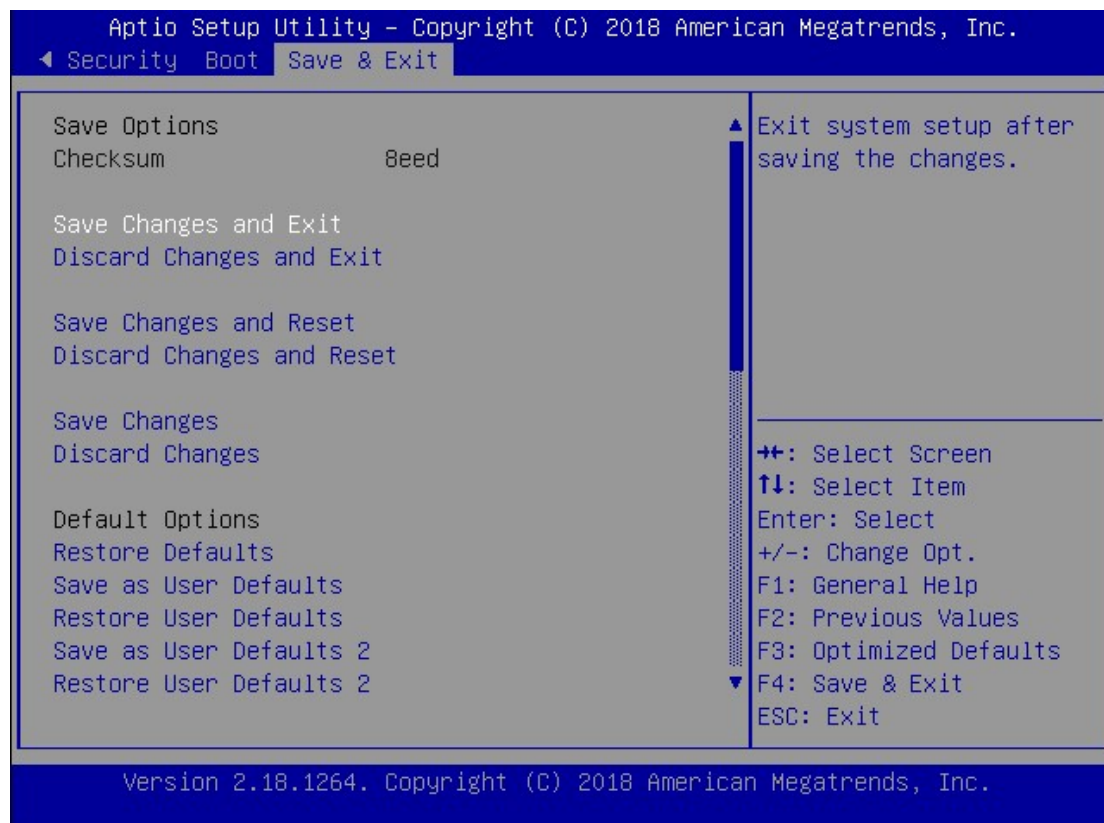
4.8 Boot Configuration

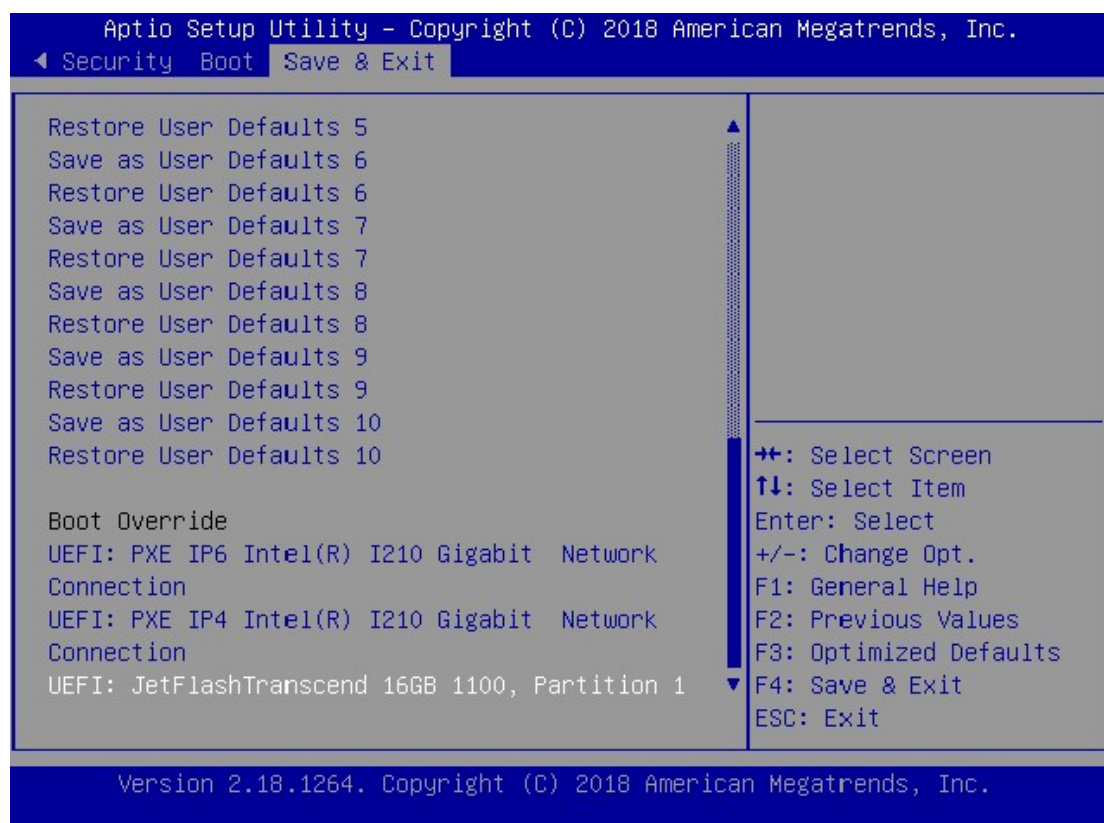


Item	Type	Options	Function description
Boot Configuration	Static text	N/A	
Setup Prompt Timeout	Numeric item	1 ~ 7* ~65535	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting
Bootup NumLock State	Multipart item	<On>* <Off>	Select the keyboard NumLock state
Quiet Boot	Multipart item	<Disabled>* <Enabled>	Enables or disables Quiet Boot option
Boot Option Priorities	Static text		
Boot Option #X1	Dynamic Multipart item	Boot option name	Sets the system boot order

Note : X= 1, 2,3, ...

4.9 Save & Exit Screen





Item	Type	Options	Function description
Save Options	Static text	N/A	
BIOS Checksum	Static text	Check sum	
Save changes and Exit	Executing item	Yes / No	Exit system setup after saving the changes
Discard Changes and Exit	Executing item	Yes / No	Exit system setup without saving any changes
Save Changes and Reset	Executing item	Yes / No	Reset the system after saving the changes
Discard Changes and Reset	Executing item	Yes / No	Reset system setup without saving any changes
Save Changes	Executing item	Yes / No	Save Changes done so far to any of the setup options
Discard Changes	Executing item	Yes / No	Discard Changes done so far to any of the setup options
Default	Static text	N/A	

Options			
Restore Defaults	Executing item	Yes / No	Restore/Load Default values for all the setup options
Save as User Defaults	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 2	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 2	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 3	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 3	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 4	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 4	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 5	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 5	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 6	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 6	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 7	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 7	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 8	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 8	Executing item	Yes / No	Restore the User Defaults to all the setup options
Save as User Defaults 9	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 9	Executing item	Yes / No	Restore the User Defaults to all the setup options

Save as User Defaults 10	Executing item	Yes / No	Save the changes done so far as User Defaults
Restore User Defaults 10	Executing item	Yes / No	Restore the User Defaults to all the setup options
Boot Override	static text	N/A	
Boot options	Dynamic text	Boot option name	Press <Enter> to force BIOS boot from this boot option.

5. BMC

5.1 BMC introduction

TS2280-E7278P uses an ASPEEDR AST2500 BMC for various platform management services and interfaces with hardware, BIOS, Intel® SPS firmware.

BMC is a standalone system in parallel to host (dual processor x86 for TS2280-E7278P). It manages the healthy status of host system.

5.2 BMC connectivity

There are three options for out-of-band BMC access:

Option 1: Shared-NIC uses I2C or RMII/NCSI interfaces to pass management traffic on data network of Mezzanine 10GE NIC.

Option 2: Shared-NIC uses RMII/NCSI interfaces to pass management traffic on data network of Intel® I210-AT. Intel® I210-AT has 10/100/1000 MDI interface to RJ45.

Option 3: Dedicated NIC uses RMII/NCSI interfaces to pass management traffic on data network on Intel® I210-AT. Intel® I210-AT connection to host is disabled.

If Option 2 exists, BMC uses RJ45(on board Intel® I210) as default.

TS2280-E7278P BMC management network firmware and utility supports all features defined in this specification in both IPv4 and IPv6 network environment.

5.3 Local Serial Console and SOL

TS2280-E7278P BMC supports two paths to access serial console:

A local serial console is on debug header.

A remote console, also known as Serial-Over-LAN (SOL) goes through management network.

Both interfaces are functional at all stages of system operation.

During system booting, POST codes will be sent to port 80 and decoded by BMC to drive the LED display. Before the system has first screen, POST codes are dumped to and displayed in SOL console in sequence. For example, display as “[00] [01] [02] [E0]...” etc. BMC also stores up to 256 POST codes for debugging purpose.

After the system has first screen in SOL console, the last POST code received on port 80 is displayed in the lower right corner of SOL console screen.

5.4 BMC sensor list

5.4.1 Sensors are listed in the table below.

Sensor Name	Sensor Number ^[1]	Sensor Type ^[2]	Sensor Reading Type	Sensor Record Type ^[3]	Sensor Owner ID	Entity ID	Entity / Instance	Assertion Event ^[6]
Threshold Sensors								
Outlet Temp	01H	01H	01H	01H	20H	07H	00H	UC
Inlet Temp	07H	01H	01H	01H	20H	07H	00H	UC
PCH Temp	08H	01H	01H	01H	20H	07H	00H	UC
P0 Therm Margin	09H	01H	01H	01H	20H	03H	00H	UC
P1 Therm Margin	0AH	01H	01H	01H	20H	03H	01H	UC
P0 Temp	05H	01H	01H	01H	20H	03H	00H	UC
P1 Temp	06H	01H	01H	01H	20H	03H	01H	UC
P0 VR Temp	02H	01H	01H	01H	20H	14H	00H	UC
P1 VR Temp	03H	01H	01H	01H	20H	14H	01H	UC
P0 DIMM VR0 Temp	0BH	01H	01H	01H	20H	14H	02H	UC
P0 DIMM VR1 Temp	0CH	01H	01H	01H	20H	14H	03H	UC
P1 DIMM VR0 Temp	0DH	01H	01H	01H	20H	14H	04H	UC
P1 DIMM VR1 Temp	0EH	01H	01H	01H	20H	14H	05H	UC
HSC Temp	0FH	01H	01H	01H	20H	07H	00H	UC
P0 core VR PIN	11h	01H	01H	01H	20H	03H	00H	UC
P1 core VR PIN	12h	01H	01H	01H	20H	03H	01H	UC
HSC Input Power	29H	0BH	01H	01H	20H	07H	00H	UC
HSC Output Curr	28H	03H	01H	01H	20H	07H	00H	UC
HSC Input Volt	2AH	02H	01H	01H	20H	07H	00H	LC,UC
P0 Package Power	2CH	0BH	01H	01H	20H	07H	00H	NA
P1 Package Power	2DH	0BH	01H	01H	20H	07H	00H	NA

Sensor Name	Sensor Number [1]	Sensor Type [2]	Sensor Reading Type	Sensor Record Type [3]	Sensor Owner ID	Entity ID	Entity / Instance	Assertion Event[6]
P0 core VR POUT	22H	0BH	01H	01H	20H	14H	00H	UC
P0 core VR Curr	23H	03H	01H	01H	20H	14H	00H	UC
P0 core VR Vol	24H	02H	01H	01H	20H	14H	00H	LC,UC
P1 core VR POUT	25H	0BH	01H	01H	20H	14H	01H	UC
P1 core VR Curr	26H	03H	01H	01H	20H	14H	01H	UC
P1 core VR Vol	27H	02H	01H	01H	20H	14H	01H	LC,UC
P0 DIMM VR0 POUT	32H	0BH	01H	01H	20H	14H	02H	UC
P0 DIMM VR0 Curr	33H	03H	01H	01H	20H	14H	02H	UC
P0 DIMM VR0 Vol	34H	02H	01H	01H	20H	14H	02H	LC,UC
P0 DIMM VR1 POUT	35H	0BH	01H	01H	20H	14H	03H	UC
P0 DIMM VR1 Curr	36H	03H	01H	01H	20H	14H	03H	UC
P0 DIMM VR1 Vol	37H	02H	01H	01H	20H	14H	03H	LC,UC
P1 DIMM VR0 POUT	38H	0BH	01H	01H	20H	14H	04H	UC
P1 DIMM VR0 Curr	39H	03H	01H	01H	20H	14H	04H	UC
P1 DIMM VR0 Vol	3AH	02H	01H	01H	20H	14H	04H	LC,UC
P1 DIMM VR1 POUT	3CH	0BH	01H	01H	20H	14H	05H	UC
P1 DIMM VR1 Curr	3DH	03H	01H	01H	20H	14H	05H	UC
P1 DIMM VR1 Vol	3EH	02H	01H	01H	20H	14H	05H	LC,UC
SYS FAN0	46H	04H	01H	01H	20H	1DH	00H	UC
SYS FAN1	47H	04H	01H	01H	20H	1DH	01H	UC
P0 DTSmax	30H	07H	01H	01H	20H	03H	00H	NA
P1 DTSmax	31H	07H	01H	01H	20H	03H	01H	NA
Airflow	4AH	0BH	01H	01H	20H	07H	00H	NA

Sensor Name	Sensor Number ^[1]	Sensor Type ^[2]	Sensor Reading Type	Sensor Record Type ^[3]	Sensor Owner ID	Entity ID	Entity / Instance	Assertion Event ^[6]
P0 DIMM0 Temp	B4h	01H	01H	01H	20H	0AH	00H	UC
P0 DIMM1 Temp	B5h	01H	01H	01H	20H	0AH	00H	UC
P1 DIMM0 Temp	B6h	01H	01H	01H	20H	0AH	00H	UC
P1 DIMM1 Temp	B7h	01H	01H	01H	20H	0AH	00H	UC
KR_Temp	B8h	01H	01H	01H	20H	0BH	00H	UC
P3V3	D0H	02H	01H	01H	20H	07H	00H	LC,UC
P5V	D1H	02H	01H	01H	20H	07H	00H	LC,UC
P12V_STBY	D2H	02H	01H	01H	20H	07H	00H	LC,UC
P1V05_PCH_STBY	D3H	02H	01H	01H	20H	07H	00H	LC,UC
PVNN_PCH_STBY	D4H	02H	01H	01H	20H	07H	00H	LC,UC
P3V3 AUX	D5H	02H	01H	01H	20H	07H	00H	LC,UC
P5V AUX	D6H	02H	01H	01H	20H	07H	00H	LC,UC
P3V BAT	D7H	02H	01H	01H	20H	07H	00H	LC,UC
Discrete Sensors								
System Status	10H	0BH	6FH	02H	20H	07H	00H	[0]=1b, CPU0 socket occupied [1]=1b, CPU1 socket occupied [2]=1b, CPU0 Thermal trip [3]=1b, CPU1 Thermal trip [4]=1b, CPU0 FIVR FAULT [5]=1b, CPU1 FIVR FAULT [6]=1b, CPU CATERR [7]=1b, System throttle
SEL Status	5FH	0BH	6FH	02H	20H	D0H	00H	02h, SEL Clear. 08h, SEL Rollover.

Sensor Name	Sensor Number ^[1]	Sensor Type ^[2]	Sensor Reading Type	Sensor Record Type ^[3]	Sensor Owner ID	Entity ID	Entity / Instance	Assertion Event ^[6]
DCMI Watchdog	60H	23H	6FH	02H	20H	D0H	01H	[0]=1b, Timer expired [1]=1b, Hard Reset [2]=1b, Power Down [3]=1b, Power Cycle [8]=1b, Timer interrupt
Chassis Pwr Sts	70H	09H	6FH	02H	20H	15H	00H	[0]=1b, Power Off/Power Down [1]=1b, Power Cycle [2]=1b, Power On [3]=1b, Soft-Shutdown [4]=1b, AC Lost [5]=1b, Hard Reset
Sys booting sts	7EH	0BH	6FH	02H	20H	07H	00H	[0]=1b, SLP S4 [1]=1b, SLP S3 [2]=0b, PCH PWROK [3]=0b, SYS PWROK [4]=1b, Platform reset [5]=0b, BIOS post complete
VR HOT	B2H	0BH	6FH	02H	20H	14H	00H	[0]=1b, CPU0 core VR hot [1]=1b, CPU1 core VR hot [2]=1b, CPU0 DIMM VR0 HOT [3]=1b, CPU0 DIMM VR1 HOT [4]=1b, CPU1 DIMM VR0 HOT [5]=1b, CPU1 DIMM VR1 HOT
CPU_DIMM HOT	B3H	0BH	6FH	02H	20H	14H	00H	[0]=1b, CPU0 PROCHOT [1]=1b, CPU1 PROCHOT [2]=1b, CPU0 CH0/1 MEMHOT [3]=1b, CPU0 CH2/3 MEMHOT [4]=1b, CPU1 CH0/1 MEMHOT [5]=1b, CPU1 CH2/3 MEMHOT

Sensor Name	Sensor Number ^[1]	Sensor Type ^[2]	Sensor Reading Type	Sensor Record Type ^[3]	Sensor Owner ID	Entity ID	Entity / Instance	Assertion Event ^[6]
HSC Sts Low	2EH	0BH	6FH	02H	20H	14H	00H	[0]=1b, NONEABOVE_STATUS [1]=1b, CML_FAULT [2]=1b, TEMP_FAULT [3]=1b, VIN UV FAULT [4]=1b, IOUT OC FAULT [5]=1b, VOUT OV FAULT [6]=1b, HOTSWAP_OFF [7]=1b, BUSY
HSC Sts High	2FH	0BH	6FH	02H	20H	14H	01H	[0]=1b, Unknown [1]=1b, Other [2]=1b, Fans [3]=1b, Power Good [4]=1b, MFR Specific [5]=1b, Input [6]=1b, Iout/Pout [7]=1b, Vout
CPU0 Error	91H	0BH	6FH	02H	20H	03H	00H	[0]=CPU FIVR Fault [3]=Thermal Trip
CPU1 Error	92H	0BH	6FH	02H	20H	03H	01H	[[0]=CPU FIVR Fault [3]=Thermal Trip

5.4.2 Threshold for Analog Sensors

Sensor Description	Sensor No.	LC (raw data)	LC (real value)	UC (raw data)	UC (real value)	UNR	Formula[1]
Outlet Temp	01H	—	—	0x4b	75	—	y=x
Inlet Temp	07H	—	—	0x28	40	—	y=x
PCH Temp	08H	—	—	0x53	83	—	y=x
P0 Therm Margin	09H	—	—	0xfe	−2	—	y=x
P1 Therm Margin	0AH	—	—	0xfe	−2	—	y=x
P0 Temp	05H	—	—	Tjmax-2	Tjmax-2	—	y=x
P1 Temp	06H	—	—	Tjmax -2	Tjmax -2	—	y=x
P0 VR Temp	02H	—	—	0x6e	110	—	y=x
P1 VR Temp	03H	—	—	0x6e	110	—	y=x
P0 DIMM VR0 Temp	0BH	—	—	0x64	100	—	y=x
P0 DIMM VR1 Temp	0CH	—	—	0x64	100	—	y=x
P1 DIMM VR0 Temp	0DH	—	—	0x64	100	—	y=x
P1 DIMM VR1 Temp	0EH	—	—	0x64	100	—	y=x
HSC Temp	0FH	—	—	0x64	100	—	y=x
P0 core VR PIN	11h			0xe1	450		y=2x
P1 core VR PIN	12h			0xe1	450		y=2x
HSC Input Power	29H	—	—	0xc8	500	—	y=2.5x
HSC Output Curr	28H	—	—	0xF0	48	—	y=0.2x
HSC Input Volt	2AH	0x71	11.3	0x84	13.2	—	y=0.1x
P0 Package Power	2CH	—	—	N/A	N/A	—	-
P1 Package Power	2DH	—	—	N/A	N/A	—	-
P0 core VR POUT	22H	—	—	0x87	270	—	y=2x
P0 core VR Curr	23H	—	—	0x9E	158	—	y=x
P0 core VR Vol	24H	0x87	1.35	0xc4	1.96	—	y=0.01x
P1 core VR POUT	25H	—	—	0x87	270	—	y=2x

Sensor Description	Sensor No.	LC (raw data)	LC (real value)	UC (raw data)	UC (real value)	UNR	Formula[1]
P1 core VR Curr	26H	—	—	0x9E	158	—	y=x
P1 core VR Vol	27H	0x87	1.35	0xc4	1.96	—	y=0.01x
P0 DIMM VR0 POUT	32H	—	—	0xc8	50	—	y=0.25x
P0 DIMM VR0 Curr	33H	—	—	0x68	41.6	—	y=0.4x
P0 DIMM VR0 Vol	34H	0x72	1.14	0x7e	1.26	—	y=0.01x
P0 DIMM VR1 POUT	35H	—	—	0xc8	50	—	y=0.25x
P0 DIMM VR1 Curr	36H	—	—	0x68	41.6	—	y=0.4x
P0 DIMM VR1 Vol	37H	0x72	1.14	0x7e	1.26	—	y=0.01x
P1 DIMM VR0 POUT	38H	—	—	0xc8	50	—	y=0.25x
P1 DIMM VR0 Curr	39H	—	—	0x68	41.6	—	y=0.4x
P1 DIMM VR0 Vol	3AH	0x72	1.14	0x7e	1.26	—	y=0.01x
P1 DIMM VR1 POUT	3CH	—	—	0xc8	50	—	y=0.25x
P1 DIMM VR1 Curr	3DH	—	—	0x68	41.6	—	y=0.4x
P1 DIMM VR1 Vol	3EH	0x72	1.14	0x7e	1.26	—	y=0.01x
SYS FAN0	46H	0x5	500				y=100x
SYS FAN1	47H	0x5	500				Y=100x
Airflow	4AH	N/A	N/A	N/A	N/A	—	—
P0 DIMM0 Temp	B4h			0x53	83		Y=x
P0 DIMM1 Temp	B5h			0x53	83		Y=x
P1 DIMM0 Temp	B6h			0x53	83		Y=x
P1 DIMM1 Temp	B7h			0x53	83		Y=x
KR_Temp	B8h			0x37	55		Y=x
P3V3	D0H	0xaf	2.993	0xd2	3.591	—	y=0.0171x
P5V	D1H	0xae	4.489	0xd5	5.495	—	y=0.0258x
P12V_STBY	D2H	0x71	11.3	0x84	13.2	—	y=0.1x
P1V05_PCH_STBY	D3H	0x13	0.95	0x17	1.15	—	Y=0.05
PVNN_PCH_STBY	D4H	0x10	0.8	0x16	1.1	—	Y=0.05x

Sensor Description	Sensor No.	LC (raw data)	LC (real value)	UC (raw data)	UC (real value)	UNR	Formula[1]
P3V3 AUX	D5H	0xaf	2.993	0xd2	3.591	—	$y=0.0171x$
P5V AUX	D6H	0xae	4.489	0xd5	5.495	—	$y=0.0258x$
P3V BAT	D7H	0x80	2.701	0xab	3.608	—	$y=0.0211x$

5.4.3 Event-Only Sensors Table

Sensor Name	Sensor Number	Generator ID	Assertion Event
SPS FW Health	0x17	0x602C	Event Data1: [7,6]=10b [5,4]=10b [3..0]=00h ,Firmware Status Event Data2: Follow IntelR SPS FW specification. Event Data3: Follow IntelR SPS FW specification.
NM Exception	0x18	0x602C	Event Data1: [0:2]-Reserved. [3]=1b, Policy Correction Time Exceeded [4:5]=10b-OEM code in byte 3. [6:7]=10b-OEM code in byte 2. Event Data2: 00h: Entire platform 01h: CPU subsystem 02h: Memory subsystem 03h: HW Protection 04h: High Power I/O subsystem. Event Data3: <Policy ID>
NM Health	0x19	0x602C	Event Data1: [0:3]=0010b, Sensor IntelR Node Manager [4:5] =10b-OEM code in byte 3. [6:7] =10b-OEM code in byte 2. Event Data2: Follow IntelR SPS FW specification Event Data3: Follow IntelR SPS FW specification
NM Capabilities	0x1A	0x602C	Event Data1: [0] - Policy interface capability 0 = Not Available. 1 = Available. [1] - Monitoring capability 0 = Not Available. 1 = Available. [2] - Power limiting capability 0 = Not Available. 1 = Available. [4:7] - Reserved. Event Data2: none Event Data3: none
NM Threshold	0x1B	0x602C	Event Data1: [0:1] -Threshold Number. [2] - reserved [3] - 0 = Threshold exceeded 1 = Policy Correction Time Exceeded [4:5] - 10b = OEM code in byte 3. [6:7] - 10b = OEM code in byte 2. Event Data2: 00h: Entire platform 01h: CPU subsystem 02h: Memory subsystem 03h: HW Protection 04h: High Power I/O subsystem. Event Data3: <Policy ID>

Sensor Name	Sensor Number	Generator ID	Assertion Event
CPU0 Therm Statu	0x1C	0x602C	Event Data1: 0h - CPU Critical Temperature. Indicates whether CPU temperature is above critical temperature point. 1h - PROCHOT# Assertions.Indicates whether PROCHOT# signal is asserted. 2h - TCC Activation. Indicates whether CPU thermal throttling functionality is activated due to CPU temperature being above Thermal Circuit Control Activation point. Event Data2: none. Event Data3: none
CPU1 Therm Statu	0x1D	0x602C	Event Data1: 0h - CPU Critical Temperature. Indicates whether CPU temperature is above critical temperature point. 1h - PROCHOT# Assertions.Indicates whether PROCHOT# signal is asserted. 2h - TCC Activation. Indicates whether CPU thermal throttling functionality is activated due to CPU temperature being above Thermal Circuit Control Activation point. Event Data2: none. Event Data3: none
POST Error	0x2B	0x0001	Event Data1: [7:6] 10b or 11b [5:4] 10b [3:0] Offset 0x00 (System Firmware Error) Event Data2: ED1[7:6]= 10b, LSB of POST Error Code. ED1[7:6]= 11b, Per IPMI Spec. Event Data3: MSB of POST Error Code
Pwr Thresh Evt	0x3B	0x602C	Event Data1: 01h, Limit Exceeded Event Data2: none. Event Data3: none
Machine Chk Err	0x40	0x0001	Event Data1: [7:6]=10b [5:4]=10b [3:0]=0Bh, Uncorrectable Or 0Ch, Correctable Event Data2: Machine Check bank Number (Any one of 0 to 21) Event Data3: [7:5] CPU Number [4:0] Core Number
PCle Error	0x41	0x0001	Event Data1: [7:6]=10b [5:4]=10b [3:0]= 04h = PCI PERR 05h = PCI SERR 07h, correctable 08h, uncorrectable 0Ah, Bus Fatal Event Data2: [7:3] Device Number [2:0] Func Number Event Data3: [7:0] Bus No

Sensor Name	Sensor Number	Generator ID	Assertion Event
Other IIO Err	0x43	0x0001	Event Data1: [7:6] 10b [5:4] 10b [3:0] Offset 0x00 (Other IIO) Event Data2: [7:0] Error ID [Refer to Haswell EDS Vol1 Sec 11.1.7 IIO module error codes] Event Data3: [7:5] CPU Number [4:3] Reserved [2:0] Source 000b = IRP0 001b = IRP1 010b = IIO-Core 011b = VT-d 100b = Intel Quick data 101b = Misc Others = Reserved
ProcHot Ext	0x51	0x0020	Event Data1: [7:6]=10b [5:4]=10b [3:0]=0Ah, Processor thermal throttling offset Event Data2: [7:2] Reserved [1:0] 0h = Native, 1h = External (VR), 2h = External(Throttle) Event Data3: [7:5] CPU/VR Number [4:0] Reserved
MemHot Ext	0x52	0x0020	Event Data1: [7:6]=10b [5:4]=10b [3:0] Memory thermal throttling offset (09h) Event Data2: [7:2] Reserved [1:0] 0h = Native, 1h = External (VR), 2h = External(Throttle) Event Data3: [7:5] CPU/VR Number [4:3] Channel Number [2:0] DIMM Number [4:0] Reserved for VR HOT
Power Error	0x56	0x0020	Event Data1: [7:6]=00b [5:4]=00b [3:0]=Event offset: 01h, SYS_PWROK Failure 02h, PCH_PWROK Failure Event Data2: 0xFF Event Data3: 0xFF

Sensor Name	Sensor Number	Generator ID	Assertion Event
Memory ECC Error	0x63	0x0001	Event Data1: [7:6] 10b – OEM Code in Byte2 [5:4] 10b – OEM Code in Byte3 [3:0] 00h – Correctable ECC 01h – Uncorrectable ECC 05h – Correctable ECC error Logging Limit Reached. Event Data2: [7:4] Reserved [3:2] 00b = All info valid 01b = DIMM info invalid 10b = All info invalid [1:0] Logical Rank Event Data3: [7:5] CPU Number [4:2] Channel Number [1:0] DIMM Number
Software NMI	0x90	0x0001	Event Data1: [7:6] 00b – Unspecified byte2 [5:4] 00b – Unspecified byte3 [3:0] 03h – Software NMI Event Data2: FFh - Not Used Event Data3: FFh - Not Used
Button	0xAA	0x0020	Event Data1: [7:4] 0h [3:0] 0h: Power button pressed 2h: Reset button pressed Event Data2: FFh - Not Used Event Data3: FFh - Not Used
Power State	0xAB	0x0020	Event Data1: [7:4] 0h [3:0] 0h: Transition to running 2h: Transition to power off Event Data2: FFh - Not Used Event Data3: FFh - Not Used
Power Policy	0xAC	0x0020	Event Data1: [7:6]=00b [5:4]=00b [3:0]=Event offset: 05h: Soft-power control failure Event Data2: FFh - Not Used Event Data3: FFh - Not Used

Sensor Name	Sensor Number	Generator ID	Assertion Event
ME Status	0xAE	0x0020	Event Data1: [7:6]=00b [5:4]=00b [3:0]=Event offset: 01h: Controller access degraded or unavailable 03h: Management controller unavailable Event Data2: FFh - Not Used Event Data3: FFh - Not Used
Network Status	0xB1	0x0020	Event Data1: [7:6]=00b [5:4]=00b [3:0]=Event offset: 00h, After BMC has IP assigned, and Both IPv4 and IPv6 network cannot ping gateway. BMC in disconnection state 01h, Either IPv4 or IPv6 can ping gateway after disconnection state Event Data2: FFh - Not Used Event Data3: FFh - Not Used
PCH Thermal Trip	0xBF	0x0020	Event Data1: 01h, State Asserted Event Data2: FFh - Not Used Event Data3: FFh - Not Used
ME GI Reset Warn	0xC5	0x602C	Event Data1: A0h Event Data2: If state is asserted: Time for which IntelR ME will delay Global Platform Reset. =00h - FEh - time in unites specified in Event Data 3 =FFh - Infinite delay. For debug purposes, you could configure the delay time as infinity. In this case, the BMC is not required to respond to the event - global reset is suppressed unconditionally. Event Data3: If State is Asserted: Time Units for which IntelR ME will delay Global Platform Reset. =00h - reserved =01h - minutes =02h - FFh - reserved.

Sensor Name	Sensor Number	Generator ID	Assertion Event
System Event	0xE9	0x0020	Event Data1: [7:0]=E5h, Timestamp Clock synch. [7:0]=C4h, PEF Action. Event Data2: if ED1 = E5h: 0x00: event is first of pair 0x80: event is second of pair if ED1 = C4h: 0x1: PEF Action Event Data3: if ED1 = E5h: Cause of time changed: 00h: NTP 01h: Host RTC 02h: Set SEL time command 03h: Set SEL time UTC offset Command FFh: Unknown if ED1 = C4h: FFh
Critical IRQ	0xEA	0x0020	Event Data1: 00h, Front Panel NMI / Diagnostic Interrupt Event Data2: FFh - Not Used Event Data3: FFh - Not Used
CATERR/MS MI	0xEB	0x0020	Event Data1: 00h: IERR (CATERR_N Hold low) 01h: MSMI_N Hold Low 0Bh: MCERR (CATERR_N 16 BCLK pulse) 0Ch: MSMI_N 16 BCLK Pulse Event Data2: FFh - Not Used Event Data3: FFh - Not Used
Dual BIOS Up Sts	0xEf	0x0020	Event Data1: 01h: Auto Recovery 02h: Manual Recovery 03h: OOB Directly Event Data2: if ED1 = 01h 01h: ARB Timer timeout 02h: BIOS Good de-assert (GPIOAA5) if ED1 = 02h 03h: Recovery from Gold to primary 04h: Recovery from Primary to Gold if ED1 = 03h 05h: Primary directly 06h: Gold directly Event Data3: if ED2 = 01h or 02h 01h: Start the progress for recovery 02h: End the progress for recovery

Sensor Name	Sensor Number	Generator ID	Assertion Event
ABR ERR	0x89	0x0020	Event Data1: 00h Primary flash booting fail. #1 Event 07h: Latest BIOS Post Code #1 08h: Latest BIOS Post Code #2 09h: Latest BIOS Post Code #3 10h: Latest BIOS Post Code #4 11h: Latest BIOS Post Code #5 12h: Latest BIOS Post Code #6 13h: Latest BIOS Post Code #7 14h: Latest BIOS Post Code #8 15h: Latest BIOS Post Code #9 16h: Latest BIOS Post Code #10 #1 Event 07h: Latest BIOS Post Code #11 08h: Latest BIOS Post Code #12 09h: Latest BIOS Post Code #13 10h: Latest BIOS Post Code #14 11h: Latest BIOS Post Code #15 12h: Latest BIOS Post Code #16 13h: Latest BIOS Post Code #17 14h: Latest BIOS Post Code #18 15h: Latest BIOS Post Code #19 16h: Latest BIOS Post Code #20

5.5 Commands Support

TS2280-E7278P BMC FW provides a fully-compliant IPMI 2.0 based management of the service processor.

All the mandatory requirements and commands in IPMI 2.0 are supported

5.5.1 IPMI commands support

In addition to the mandatory criteria in IPMI 2.0 specification, TS2280-E7278P BMC FW also supports many optional commands.

The following is a list of commands that currently support to the TS2280-E7278P BMC firmware.

5.5.1.1 IPMI Global Commands

IPM Global Commands
Get Device ID
Cold Reset
Warm Reset
Get Self Test Results
Set ACPI Power State
Get ACPI Power State
Get Device GUID
Get NetFn Support
Get Command Support
Get Command Sub-function Support
Get Configurable
Get Configurable Command Sub-functions

5.5.1.2 BMC Watchdog Timer Commands

BMC Watchdog Timer Commands
Reset Watchdog Timer
Set Watchdog Timer
Get Watchdog Timer

5.5.1.3 IPMI Messaging Support Commands

IPMI Messaging Support Commands
Set BMC Global Enables
Get BMC Global Enables
Clear Message Flags
Get Message Flags

Enable Message Channel Receive
Get Message
Send Message
Read Event Message Buffer
Get System GUID
Get Channel Authentication Capabilities
Get Session Challenge
Activate Session
Set Session Privilege Level
Close Session
Get Session Info
Get AuthCode
Set Channel Access
Get Channel Access
Get Channel Info
Set Channel Security Keys
Set User Access
Get User Access
Set User Name
Get User Name
Set User Password
Master Write-Read
Get Channel Cipher Suites
Get System Interface Capabilities
Set System Info Parameters
Get System Info Parameters

5.5.1.4 RMCP+ Support and Payload Commands

RMCP+ Support and Payload Commands
Activate Payload
Deactivate Payload
Get Payload Activation Status
Get Payload Instance Info
Set User Payload Access
Get User Payload Access
Get Channel Payload Support
Get Channel Payload Version
Get Channel OEM Payload Info
Suspend/Resume Payload Encryption

5.5.1.5 Chassis Device Commands

Chassis Commands
Get Chassis Capabilities
Get Chassis Status
Chassis Control
Chassis Identify
Set Chassis Capabilities
Set Power Restore Policy – disable by default
Get System Restart Cause
Set System Boot Options
Get System Boot Options
Get POH Counter

5.5.1.6 Event Commands

Event Commands
Set Event Receiver
Get Event Receiver
Platform Event

5.5.1.7 PEF and Alerting Commands

PEF and Alerting Commands
Get PEF Capabilities
Arm PEF Postpone Timer
Set PEF Configuration Parameters
Get PEF Configuration Parameters
Set Last Processed Event ID
Get Last Processed Event ID
Alert Immediate
PET Acknowledge

5.5.1.8 Sensor Device Commands

Sensor Device Commands
Get Device SDR Info
Get Sensor Reading Factors
Set Sensor Hysteresis
Get Sensor Hysteresis
Set Sensor Threshold
Get Sensor Threshold
Set Sensor Event Enable
Get Sensor Event Enable

Re-arm Sensor Events
Get Sensor Event Status
Get Sensor Reading
Set Sensor Reading And Event Status
Set Sensor Type

5.5.1.9 FRU Inventory Area Info

FRU Device Commands
Get FRU Inventory Area Info
Read FRU Data
Write FRU Data

5.5.1.10 SDR Repository Device Commands

SDR Repository Device Commands
Get SDR Repository Info
Get SDR Repository Allocation Info
Reserve SDR Repository
Get SDR
Add SDR
Partial Add SDR
Clear SDR Repository
Get SDR Repository Time
Enter SDR Repository Update Mode
Exit SDR Repository Update Mode
Run Initialization Agent

5.5.1.11 SEL Device Commands

SEL Device Commands
Get SEL Info
Get SEL Allocation Info
Reserve SEL
Get SEL Entry
Add SEL Entry
Partial Add SEL Entry
Clear SEL
Get SEL Time
Set SEL Time
Get SEL Time UTC Offset

Set SEL Time UTC Offset

5.5.1.12 IPMI LAN Commands

IPMI LAN Commands
Set LAN Configuration Parameters
Get LAN Configuration Parameters
Suspend BMC ARPs

5.5.1.13 SOL Commands

SOL Commands
SOL Activating
Set SOL Configuration Parameters
Get SOL Configuration Parameters

5.5.2 OEM commands support

Except the Standard and optional commands, TS2280-E7278P provide the system specific OEM commands that dedicated for TS2280-E7278P system, below are all the OEM commands that available for TS2280-E7278P.

The following is a list of OEM commands that planning to support on the TS2280-E7278P BMC firmware.

5.5.2.1 OEM Commands Synopsis

Command Set	Sub command	NetFn	CMD Code
Auto BIOS Recovering command Set	Disable ABR Timer Command	0x3C	0x30
	Set Dual BIOS Mux Command	0x30	0x43
	Get Dual BIOS Status Command	0x30	0x45
	Set Dual BIOS Version Obtain Command	0x30	0x54
	Get Dual BIOS Version Command	0x30	0x50
	Perform BIOS Recovery Command	0x30	0x41
	Perform BIOS Backup Command	0x30	0x42
	Get BIOS Flash Info	0x30	0x55
	Get BIOS Version Command	0x30	0x83
	Set Dual BIOS Recovery Command	0x30	0x44
	Get Auto BIOS Recovery Setting State Command	0x3C	0x27
	Get BIOS Recovery/Backup Progress Command	0x3C	0x23
Auto BIOS Recovering Command Set	Get BIOS Boot Option Status Command	0x3C	0x10
	Get BIOS Boot Option Counter Command	0x3C	0x11
	Get BIOS Boot Order Command	0x30	0x53
	Set BIOS Boot Order Command	0x30	0x52
	Set BIOS Boot Option Status Command	0x3C	0x14
	Set BIOS Boot Mode Command	0x3C	0x15
	Get BIOS Boot Mode Command	0x3C	0x16
	Get BIOS Boot Mode Status Command	0x3C	0x17
	Clean BIOS Boot Mode Status Command	0x3C	0x18
Other OEM Command Set	Restore Factory Default Command	0x32	0x66
	Set Fast PROCHOT Command	0x30	0xD1

Command Set	Sub command	NetFn	CMD Code
	Get Fast PROCHOT Command	0x30	0xD0
	Get 80 Port Record Command	0x30	0x49
	Set DIMM Information Command	0x30	0x1C
	Get DIMM Information Command	0x30	0x1D
	Set VR Monitor Enable Command	0x30	0xD2
	Get VR Monitor Enable Command	0x30	0xD4
	Get CPLD Info Command	0x32	0x88
	Set Network Sequence Command	0x30	0xB0
	Get Network Sequence Command	0x30	0xB1
	Replay SOL Buffer Command	0x30	0x48
	Set PPIN Command	0x30	0x77
	Get PPIN Command	0x30	0x78
	Set Preserve Configuration Command	0x32	0x83
	Get Preserve Configuration Command	0x32	0x84
	Set First Time BIOS Boot Flag Command	0x30	0x40
	Set PHY Reset Status Command	0x30	0x30
	Get PHY Reset Status Command	0x30	0x31
	Set GPIO Command	0x30	0xE0
	Get GPIO Command	0x30	0xE1
	Getting Multiple IPv6 IP Addresses Command	0x32	0x99
	Clear CMOS	0x30	0xA1
	Get PIN	0x30	0xDF

5.5.2.2 Auto BIOS Recovering Command Set

5.5.2.2.1 Set Dual BIOS Mux Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
43h	Set Dual BIOS Mux	Request: Byte 1 – 00h = Set SPI flash bus to PCH. 01h = Set SPI flash bus to BMC. Byte 2 – 01h = Select primary BIOS flash. 02h = Select backup BIOS flash. Response: Byte 1 – Completion code. 00h = Command Completed Normally. D5h = Command could not be executed, BIOS in post/setup mode. C0h = Node Busy. The previous operation not finished yet.	This command could not execution during BIOS post, BIOS setup menu and system reboot. Please note the user should confirm the SPS FW is in the recovery mode before issuing this command. User can send Force ME Recovery Command to achieve this. i.e. ipmitool -t 0x2c -b 6 raw 0x2e 0xdf 0x57 0x01 0x00 0x01

5.5.2.2.2 Set Dual BIOS Recovery Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
44h	Set Dual BIOS Recovery	Request: Byte 1 –Setting of Dual BIOS recovery 00h = Disable 01h = Enable. Response: Byte 1 – Completion code. 00h = Command Completed Normally.	Setting of enable/disable Auto BIOS Recovery after 1st time boot after a BIOS update

5.5.2.2.3 Get Dual BIOS Status Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
45h	Get Dual BIOS Status	Request: N/A Response: Byte 1 – Completion code. Byte 2 – Setting of Dual BIOS recovery 00h = Disabled 01h = Enabled. Byte 3 – 00h = SPI flash bus has been selected to PCH. 01h = SPI flash bus has been selected to BMC. Byte 4 – 01h = The primary flash has been selected.	The default Byte 2 = 0. The default Byte 3 = 0. The default Byte 4 = 1.

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
		02h = The backup flash has been selected. Byte 5 – Recover/Backup status 00h = Nothing to happen 01h = Performing BIOS Recovery 02h = Performing BIOS Backup	

5.5.2.2.4 Set Dual BIOS Version Obtain Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
54h	Set Dual BIOS Version Obtain	Request: N/A Response: Byte 1 – Completion code. D5h = Command could not be executed, BIOS in post/setup mode. C0h = Node Busy. The previous operation not finished yet.	Request BMC to read BIOS version from physical primary and backup SPI flash device, and save in BMC DRAM. Get dual BIOS version reads the same variable in BMC DRAM. This command could not execution during BIOS post - BIOS setup menu and system reboot. If completion code is C0h, please wait for 15 seconds and try this command again.

5.5.2.2.5 Get Dual BIOS Version Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
50h	Get Dual BIOS Version	Request: Byte 1– 01h = Get primary BIOS FW version. 02h = Get backup BIOS FW version. Response: Byte 1 – Completion code. 00h = Command Completed Normally. CBh = Requested Sensor, data, or record not present. CCh = Invalid data field in Request. 82h = Dual BIOS version not ready Byte 2:N – BIOS FW version(ASCII code) (LSB first)	Read BIOS version of primary and backup image from BMC DRAM.

5.5.2.2.6 Perform BIOS Recovery Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
41h	Perform BIOS Recovery	Request: Byte 1 – 72h ('r') Byte 2 – 65h ('e') Byte 3 – 63h ('c') Byte 4 – 6Fh ('o') Byte 5 – 76h ('v') Byte 6 – 65h ('e') Byte 7 – 72h ('r') Response: Byte 1 – Completion code. 00h = Command Completed Normally. C0h = Node Busy. The previous operation not finished yet. D5h = Command could not be executed, BIOS in post/setup mode.	Copy backup BIOS image to primary BIOS image. This command could not execution during BIOS post - BIOS setup menu and system reboot. Please send the below command to execute Global Reset after the recovery is done 'ipmitool power cycle'

5.5.2.2.7 Perform BIOS Backup Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
42h	Perform BIOS Backup	Request: Byte 1 – 62h ('b') Byte 2 – 61h ('a') Byte 3 – 63h ('c') Byte 4 – 6Bh ('k') Byte 5 – 75h ('u') Byte 6 – 70h ('p') Response: Byte 1 – Completion code. 00h = Command Completed Normally. C0h = Node Busy. The previous operation not finished yet. D5h = Command could not be executed, BIOS in post/setup mode	Copy primary BIOS image to backup BIOS image. This command could not execution during BIOS post - BIOS setup menu and system reboot. Please send the below command to execute Global Reset after the backup is done 'ipmitool power cycle'

5.5.2.2.8 Get BIOS Flash Info

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
55h	Get BIOS Flash Info	Request: Byte 1 – 00h = Primary PCH flash 01h = Backup PCH flash Response: Byte 1 – Completion code. 00h = Command Completed Normally. C0h = Node Busy. The previous operation not finished yet. 82h = BIOS flash info not ready. D5h = Command could not be executed, BIOS in post/setup mode. The below data can be respond while the BIOS flash info is ready in the BMC DRAM, Byte 2 – Manufactory ID Byte 3 – Memory type Byte 4 – Memory density/capacity Byte 5 – Status register	Read BIOS SPI Flash JEDEC ID and status register

5.5.2.2.8 Disable ARB Timer Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
0x30	Disable ARB Timer	Request: N/A Response: Byte[1] : Completion code	This command only for BIOS. This command let BIOS to notify BMC to disable ARB timer. The disable conditions are as below: BIOS runs normally and BIOS will send a “disable ARB timer” command to BMC before boot to OS

5.5.2.3 BIOS Boot Option Command Set

5.5.2.3.1 Get BIOS Boot Mode Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
0x16	Get BIOS Boot Mode	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 0x00 = UEFI mode. 0x01 = Legacy mode.	

5.5.2.3.2 Get BIOS Boot Mode Status Command

Net Function = 0x30			
Code	Command	Request/Response Data	Description
0x17	Get BIOS Boot Mode Status.	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 0x00 = No change. 0x01 = The boot mode has been changed by software tool.	

5.5.2.4 Other OEM Command Set

5.5.2.4.1 Restore Factory Default Command

Net Function = 0x32			
Code	Command	Request, Response Data	Description
66h	Restore Factory Default	Request: NA Responses: Byte 1 – Completion code.	When send this command to BMC, the LAN Configuration Parameters will be changed current setting value to default value as following: 1. IP Address Source = 0x00(DHCP) 2. The Network sequence priority default is Mezzanine card for PVT/MP. 3. The MEZZ protocol priority default is NCSI for PVT/MP. 4. User IDs (User/Password/Privilege/Channels). 5. Debug Console Serial Parameters. 6. Product Information - Product ID. - Manufacturer ID Remove all the special settings such as different priority, but SEL will not remove. (Note: The BMC will reset itself after restore to default.)

5.5.2.4.2 Get Over Current Detect Command

Net Function = 0x3C			
Code	Command	Request, Response Data	Description
6Bh	Get Over Current Detect Command	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 00h = Disable Over Current Detect. 01h = Enable Over Current Detect.	Read setting of current based FM_OC_DETECT_EN_N. The Over Current Detect default is disable (FM_OC_DETECT_EN_N = high).

5.5.2.4.3 Get Fast PROCHOT Command

Net Function = 30h (OEM)			
Code	Command	Request, Response Data	Description
D0h	Get Fast PROCHOT	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 00h = Disable Fast PROCHOT.	Read setting of current based FAST_PROCHOT_N. The Fast PROCHOT default is disable (FAST_PROCHOT_N = high).

Net Function = 30h (OEM)			
Code	Command	Request, Response Data	Description
		01h = Enable Fast PROCHOT.	

5.5.2.4.4 Get 80 Port Record Command

Net Function = 30h (OEM)			
Code	Command	Request, Response Data	Description
49h	Get 80 Port Record	Request: N/A Response: Byte 1 – Completion code. Byte 2:N – POST code.	Replay the last port 80 POST codes (up to 256x POST records). N: maximum number = 256

5.5.2.4.5 Get DIMM Information Command

Net Function = 30h (OEM)			
Code	Command	Request, Response Data	Description
1Dh	Get DIMM Information	Request: N/A Response: Byte 1 – Completion code. Byte 2:N – All DIMM information.	Read DIMM Type from BMC.

5.5.2.4.6 Get VR FW Version

30h (OEM)			
Code	Command	Request, Response Data	Description
51h	Get VR FW Version	Request: Byte 1 – The VR controller desired 00: CPU0 VR 01: CPU1 VR 02: CPU0 DIMM0 VR 03: CPU0 DIMM1 VR 04: CPU1 DIMM0 VR 05: CPU1 DIMM1 VR Response: Byte 1 – Completion code. Byte 2:5 – VR checksum (LSB first)	BMC can provide the NVM Checksum stored in the BMC DRAM for the specific VR controller.

5.5.2.4.7 Set First Time BIOS Boot Flag Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
40h	Set First Time BIOS Boot Flag	Request: Byte 1 – 01h = Set First Time BIOS Boot Flag Response: Byte 1 – Completion code.	For inband BIOS update utility to set flag for first time boot after an inband BIOS update action.

5.5.2.4.8 Set Preserve Configuration Command

Net Function = 32h (OEM)			
Code	Command	Request/ Response Data	Description
83h	Set Preserve Configuration	Request: Byte 1 – Selector Byte 2 – 0 = Disable 1 = Enable Response: Byte 1 – Completion code.	Set BMC configuration to be preserved or not after BMC FW update. This command is for YAFU flash update tool.

5.5.2.4.9 Get Preserve Configuration Command

Net Function = 32h (OEM)			
Code	Command	Request/ Response Data	Description
84h	Get Preserve Configuration	Request: Byte 1 – Selector Response: Byte 1 – Completion code. Byte 2 – 00h = Disable 01h = Enable	

5.5.2.4.10 Get CPLD Information Command

Net Function = 32h (OEM)			
Code	Command	Request/ Response Data	Description
88h	Get CPLD Information	Request: N/A Response: Byte 1 – Completion code. Byte 2 – CPLD version number. Byte 3:6 – Device ID(LSB first).	1. Get CPLD version via CPLD SGPIO by BMC. 2. Get CPLD Device ID via JTAG interface by BMC.

5.5.2.4.11 Set Network Sequence Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
B0h	Set Network Sequence	Request: Byte 1 – 00h = LOM (I210) is priority 1. Mezzanine card is priority 2. 01h = Mezzanine card is priority 1. LOM (I210) is priority 2. Response: Byte 1 – Completion code.	Change setting of OOB interface priority between LOM and Mezzanine card. BMC will apply the new priority at next AC reset or cold reset The default setting as following: LOM (I210) is priority 1 Mezzanine card is priority 2.

5.5.2.4.12 Get Network Sequence Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
B1h	Get Network Sequence	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 00h = LOM (I210) is priority 1. Mezzanine card is priority 2. 01h = Mezzanine card is priority 1. LOM (I210) is priority 2.	Read setting of OOB interface priority. The Network sequence priority default is LOM (I210) (Byte 2 = 0).

5.5.2.4.13 Replay SOL Buffer Command

Net Function = 30h			
Code	Command	Request/ Response Data	Description
48h	Replay SOL Buffer	Request: N/A Response: Byte 1 – Completion code.	Replay last 16KB of SOL screen in SOL console. Use this command can display 5x last frames buffer when SOL session is connecting.

5.5.2.4.14 Get PPIN Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
78h	Get PPIN	Request: Byte 1 – CPU number (CPU#0: 00h, CPU#1: 01h) Response:	Read PPIN from BMC. BMC default provides 0xFFFFFFFFFFFFFFFF for CPU 0/1.

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
		Byte 1 – Completion code. Byte 2:9 – VALUE-The 64 bit(bit 63:0) inventory number (MS-byte first).	

5.5.2.4.15 Set PHY Reset Status Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
30h	Set PHY Reset Status	Request: Byte 1 – 00h = Disable PHY reset. 01h = Enable PHY reset. Response: Byte 1 – Completion code.	Change setting to enable/disable shared NIC PHY reset of all shared NICs during system warm reboot and DC cycle. This default setting is 0.

5.5.2.4.16 Get PHY Reset Status Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
31h	Get PHY Reset Status	Request: N/A Response: Byte 1 – Completion code. Byte 2 – 00h = Disable PHY reset. 01h = Enable PHY reset.	Read setting of keep NIC PHY link up feature of all shared NICs. This default setting is 0.

5.5.2.4.17 Get PIN Command

Net Function = 30h (OEM)			
Code	Command	Request/ Response Data	Description
DFh	Get PIN	Request: Byte 1:2 –Duration time (LSB first), resolution of 0.1s. Response: Byte 1:2 –Average power (LSB first), resolution of 0.1W.	Read average PIN in any duration between 0.1 to 60 seconds

5.6 Event Logging and Alerting

All of the system events are logged to an internal 64K bytes flash. However, TS2280-E7278P BMC does not support any alert mechanism based on manufacturer per-configured Alert Policy.

5.7 Chassis Control

BMC has the ability to perform system power on/off and reset functions. These functions will be controlled externally through the IPMI chassis commands that described in the IPMIv2.0 specification. Including Get chassis capabilities, Get chassis status, and chassis control.

- Power down
- Power up
- Power cycle
- Hard Reset

5.7.1 Power Button Logging

BMC has the ability to generate unique events in SEL for the below button response.

Host System State	Button Action
Powered on	Any button press Short press (<=5 sec)
Powered off	Long press (1min> time >5 sec) Button stuck (>1min)

5.8 LAN Configuration

For SNMP Traps related LAN configuration setting, please refer to IPMI v2.0 spec Chapter 23.2 Get LAN Configuration Parameters Command “Table 23-4 LAN Configuration Parameters”, because TS2280-E7278P BMC follows IPMI v2.0 spec definition to implement related functions. So BMC doesn’t allow user to enter host name to set LAN configuration.

Parameter	#	Parameter Data (non-volatile unless otherwise noted) ^[1]
Destination Addresses	19	Sets/Gets the list of IP addresses that a LAN alert can be sent to. This parameter is not present if the Number of Destinations parameter is 0. <u>data 1</u> - Set Selector = Destination Selector. [7:4] - reserved [3:0] - Destination selector. Destination 0 is always present as a volatile destination that is used with the <i>Alert Immediate</i> command. <u>data 2</u> - Address Format [7:4] - Address Format: 0h = IPv4 IP Address followed by DIX Ethernet/802.3 MAC Address [3:0] - reserved For Address Format = 0h: <u>data 3</u> - Gateway selector [7:1] - reserved [0] - 0b = use default gateway 1b = use backup gateway <u>data 4:7</u> - Alerting IP Address (MS-byte first) <u>data 8:13</u> - Alerting MAC Address (MS-byte first)

Following parameters are introduced with IPMI v2.0 / RMCP+

VLAN configuration can be used with IPMI v1.5 and IPMI v2.0 sessions. Parameters labeled “RMCP+” are specific to IPMI v2.0 implementations that implement IPMI v2.0 / RMCP+ sessions.

5.8.1 Get/Set LAN Configuration Parameters

In order to reflect the capabilities provided by the BMC for some of the network settings, the values for some of the parameter data is defined as shown below.

5.8.1.1 DHCP

In addition to the usual methods of obtaining an IP address, the BMC provides a mode where it attempts to obtain an IP address from a DHCP server for a given period of time and if unsuccessful fails over to using a static IP address.

Parameter	#	Parameter Data
IP Address Source	4	<u>data 1</u> [7:4] – reserved [3:0] – address source 0h = unspecified 1h = static address (manually configured) 2h = address obtained by BMC running DHCP 3h = address obtained by BIOS or system software 4h = address obtained by BMC running other address

	assignment protocol. The BMC will use the value 4h to indicate the address mode of DHCP with failover to static.
--	---

5.8.1.2 MAC Address Programming

BMC provides a default MAC Address “00:11:22:33:44:55” for testing purpose use. When BMC initialize in UBoot, BMC will check EEPROM MAC address whether exist. If the MAC address does not exist, BMC will set a default MAC Address “00:11:22:33:44:55” to network configuration setting in RAM.

User can use standard IPMI “Set LAN Configuration Parameters” command to set OEM Parameters to enable set MAC address to change MAC address.

Set “ENABLE SET MAC”, this is defined in OEM Parameters as following:

OEM Parameters: 194(C2h)

Data1: 00h = Set MAC address for BMC MAC0

01h = Set MAC address for BMC MAC1

For example as following:

Step 1: Enable Set MAC address

Ex. ipmitool raw 0x0C 0x01 0x01 0xC2 0x00 ; “Enable Set MAC for BMC MAC0”

Step 2: Set MAC Address by standard IPMI “Set LAN Configuration Parameters” command.

If MAC address = XX XX XX XX XX XX.

Ex. ipmitool raw 0x0C 0x01 0x01 0x05 XX XX XX XX XX XX

Step 3. After about 30 seconds, please use ‘ipmitool lan print’ to check BMC LAN info.

5.9 Port 80 POST

TS2280-E7278P BMC supports port 80 POST code display to drive 8 bit HEX GPIO to debug header described. BMC post function would ready before system BIOS starts to send 1st POST code to port 80.

BMC would access to POST code and record up to 256x POST codes. OOB raw command can be used to retrieve last 20x POST code from BMC.

5.10 LED controlled by BMC

5.10.1 BMC Heartbeat LED

The BMC heartbeat LED will be blinking while BMC is alive, otherwise it must be deactivated while BMC's firmware is out of working.

5.10.2 UART Channel LED

BMC would control UART channel switch signal, and then this signal would direct to LED signal.

UART Channel	UART_LED1	UART_LED0
Host console	OFF	OFF
BMC debug console	OFF	ON
BMC UART2/IE UART	ON	OFF

5.10.3 Power and System Identification LED

The motherboard combines Power LED and System Identification LED to a single blue LED at front side.

Power LED on is defined by the readiness of major run time power rails (P12V, P5V, and P3V3) but NOT the readiness of all run time power rails; for example, CPU core power rail being ready is not required for Power LED on indication.

Power LED blinking is used as system identification. The on time is different during power on and power off.

There are 4 states of Power/system identification LED depending on system power state, and chassis identify status.

Power off, Chassis identify off: LED consistently off

Power off, Chassis identify on: LED on for 0.1sec, off for 0.9sec, and loop

Power on, Chassis identify off: LED consistently on

Power on, Chassis identify on: LED on for 0.9sec, off for 0.1sec, and loop

6. Firmware Update

6.1 BIOS Update

If you experience problems with setting up your system, always contact MiTAC for help.

6.2 Firmware Update

Every BIOS/BMC file is unique for the motherboard it was designed for. For Flash Utilities, image downloads, and information on how to properly use the Flash Utility with your motherboard.

6.2.1 BIOS update

You can do BIOS update via local or OOB.

This is an example of local BIOS update.

```
File Edit View Search Terminal Help
[root@localhost 439A1000]# ./Tioga621_Linux_64.sh
Bin file name is 439A1000.bin

BEGIN

+-----+
|               AMI Firmware Update Utility v5.09.02.1396               |
|               Copyright (C)2017 American Megatrends Inc. All Rights Reserved.               |
+-----+
!!!!!!Please do not remove the AC power!!!!!!
Reading flash ..... done
- ME Data Size checking . ok
- FFS checksums ..... ok
- Check RomLayout ..... Ok.
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
Erasing Main Block ..... done
Updating Main Block ..... done
Verifying Main Block ..... done
Erasing NVRAM Block ..... done
Updating NVRAM Block ..... done
Verifying NVRAM Block ..... done
Erasing NCB Block ..... done
Updating NCB Block ..... done
Verifying NCB Block ..... done
- Update success for FDR
- Update success for DER.
- PTT is locked, skip updating.
- Successful Update Recovery Loader to OPRx!!
- Successful Update MFSB!!-
- Successful Update FTPI!!-
- Successful Update MFS, IVB1 and IVB2!!
- Successful Update FLOG and UTOK!!
- ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!
[root@localhost 439A1000]#
```

Here is the example of OOB BIOS update.

```
[root@localhost C439_TGPSNTT_101]# ./Yafuflash -d 2 -nw -ip 192.168.50.107 -u
admin -p admin C439_TGPSNTT_101.BIN
INFO: Yafu INI Configuration File not found... Default options will not be app
plied...

Creating IPMI session via network with address 192.168.50.107...Done

-----
YAFUFlash - Firmware Upgrade Utility (Version 4.89.0)
-----
(C)Copyright 2016, American Megatrends Inc.
Beginning BIOS Update...
Uploading Image : 100%... done
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
[root@localhost C439_TGPSNTT_101]#
```

IP: Your BMC IP.

C439_TGPSNTT_101.BIN: The BMC image you received.

6.2.2 BMC update

You can do BMC update via local or OOB.

Example of local BMC update:

```
root@localhost:~/Desktop/439A01.I02
File Edit View Search Terminal Help
[root@localhost 439A01.I02]# ./socflash x64 -s 439A01.I02
ASPEED SOC Flash Utility v.1.14.00
Find ASPEED Device 1a03:2000 on 3:0.0
MMIO Virtual Address: a5e69000
Relocate IO Base: 2000
Found ASPEED Device 1a03:2500 rev. 41
Static Memory Controller Information:
CS0 Flash Type is SPI
CS1 Flash Type is SPI
CS2 Flash Type is SPI
CS3 Flash Type is NOR
CS4 Flash Type is NOR
Boot CS is 1
Option Information:
CS: 1
Flash Type: SPI
[Warning] Don't AC OFF or Reboot System During BMC Firmware Update!!
[SOCFLASH] Flash ID : 1920c2
Find Flash Chip #1: MXIC MX25L256/257
Update Flash Chip #1 O.K.
Update Flash Chip O.K.
[root@localhost 439A01.I02]#
```

Example of BMC update via OOB:

```
root@localhost:/home/TiogaPass/FW/BMC/439A01.I03
File Edit View Search Terminal Help
[root@localhost 439A01.I03]# ./YafuFlash -nw -ip 192.168.50.107 -u admin -p admin 439A01.I03
INFO: Yafu INI Configuration File not found... Default options will not be applied...
Creating IPMI session via network with address 192.168.50.107...Done
.....
YAFUFlash - Firmware Upgrade Utility (Version 4.89.0)
.....
(C)Copyright 2016, American Megatrends Inc.
The Module boot major or minor version is different from the one in the image
So,Type (Y/y) to do Full Firmware Upgrade or (N/n) to exit
Enter your Option : y
.....
*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Preserving Env Variables... done
Uploading Firmware Image : 100%... done
Flashing [boot] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [conf] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [bupconf] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [root] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [osimage] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [lww] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [ast2500] Module ...
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Setting Env variables... done
Resetting the firmware.....
[root@localhost 439A01.I03]#
```

Appendix A

BIOS POST ERROR CODE

SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.

0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C	PEI phase BMC self-test failure
0x5C-0x5F	Reserved for future AML error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AML progress codes
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AML error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AML progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AML error codes

DXE PHASE

Status Code	
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started

0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error

0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure

TS2280-E7278P also displays the DIMM error information on debug card.

During the boot sequence the BIOS initialize and test each DIMM module. If a module fails initialization or does not pass the BIOS test the following post codes should flash on the debug card to indicate which DIMM has failed. The first hex character indicates which CPU interfaces the DIMM module; the second hex character indicates the number of the DIMM module. POST code will also display error major code and minor code from Intel memory reference code. The display sequence will be "00", DIMM location, Major code and Minor code with 1 second delay for every code displayed. BIOS repeat the display sequence indefinitely to allow time for a technician to service the system. DIMM location code table is listed below. DIMM number count starts from the furthest DIMM from CPU.

DIMM location code

CPU0 (Channel 0 & 1)	A0
	A1
	A2
	A3
CPU0 (Channel 2 & 3)	A4
	A5
	A6
	A7
CPU1 (Channel 0 & 1)	B0
	B1
	B2
	B3
CPU1 (Channel 2 & 3)	B4
	B5
	B6
	B7

BIOS Memory ERROR CODE

Fatal Errors	Major Code	Minor Code	Error Description
ERR_NO_MEMORY	0E8h		
ERR_NO_MEMORY_MINOR_NO_MEMORY		01h	1. No memory was detected via SPD read. No warning log entries available. 2. Invalid configuration that causes no operable memory.
ERR_NO_MEMORY_MINOR_ALL_CH_DISABLED		02h	Memory on all channels of all sockets is disabled due to hardware memtest error.
ERR_NO_MEMORY_MINOR_ALL_CH_DISABLED_MIXED		03h	No memory installed. All channels are disabled.
ERR_LT_LOCK	0E9h		Memory is locked by LT, inaccessible
ERR_DDR_INIT	0EAh		DDR training did complete successfully
ERR_RD_DQ_DQS		01h	Error on read DQ/DQS init
ERR_RC_EN			Error on Receive Enable
ERR_WR_LEVEL			Error on Write Leveling
ERR_WR_DQ_DQS			Error on write DQ/DQS
ERR_MEM_TEST			Memory test failure
ERR_MEM_TEST_MINOR_SOFTWARE			Software memtest failure
ERR_MEM_TEST_MINOR_HARDWARE			Hardware memtest failure
ERR_MEM_TEST_LOCKSTEP_MODE			Hardware memtest failure in Lockstep channel mode requiring a channel to be disabled. This is a fatal error which requires a reset and calling BIOS with a different RAS mode to retry
ERR_VENDOR_SPECIFIC	0ECh		RDIMMs is present DIMM vendor-specific errors
ERR_DIMM_COMPAT	0Edh		
ERR_MIXED_MEM_TYPE		01h	Different DIMM types are detected installed in the system
ERR_INVALID_POP		02h	Violation of population rules
ERR_INVALID_POP_MINOR_UNSUPPORTED_VOLTAGE		05h	Unsupported DIMM voltage
Reserved	0EEh		Reserved
ERR_INVALID_BOOT_MODE		01h	Boot mode is unknown
ERR_INVALID_SUB_BOOT_MODE		02h	Sub boot mode is unknown