

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

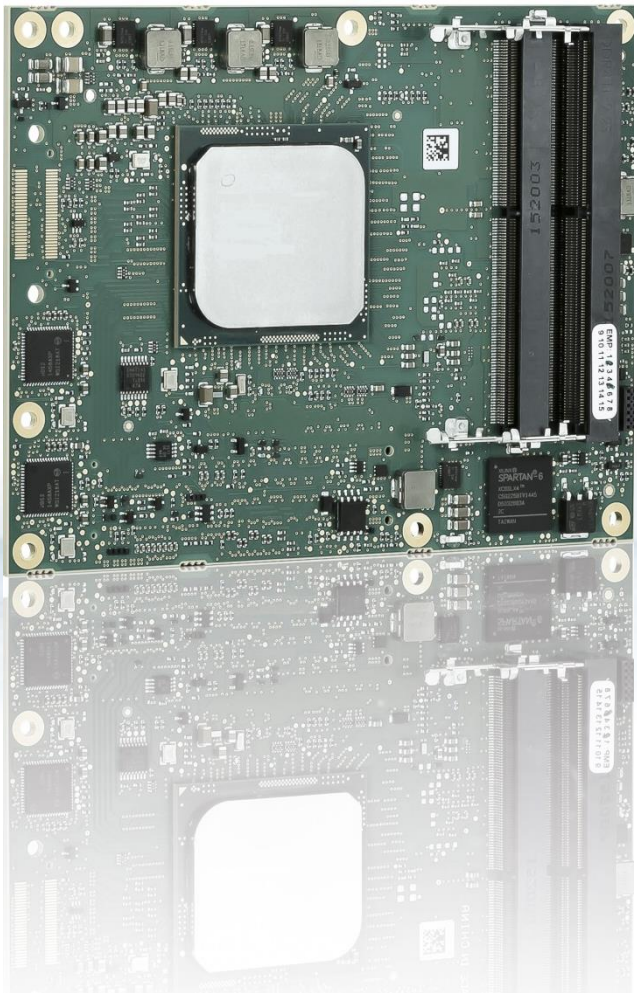
- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

USER GUIDE



COMe-bBD6

User Guide Rev 1.94

Doc-ID: 1067-1292

This page has been intentionally left blank

COME-BBD6 – USER GUIDE

Disclaimer

Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This manual is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this manual is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this manual only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2023 by Kontron Europe GmbH

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "HIGH RISK APPLICATIONS").

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.

⚠CAUTION

Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled. Please follow the "General Safety Instructions" supplied with the system.

NOTICE

You find the most recent version of the "General Safety Instructions" online in the download area of this product.

NOTICE

This product is not suited for storage or operation in corrosive environments, in particular under exposure to sulfur and chlorine and their compounds. For information on how to harden electronics and mechanics against these stress conditions, contact Kontron Support.

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
1.0	Initial issue	2016-May-26	
1.1	Figure 5 and 7 updated, table 4 corrected	2016-Jul-21	
1.2	Table 16 updated with new part numbers for memory modules	2016-Aug-05	
1.3	Table 39 updated: C29 and C30 description corrected	2016-Aut-18	
1.4	Legal and service information updated; table 16: Table header corrected and memory part numbers replaced by speaking P/Ns	2017-Feb-18	
1.5	IntelRCSetup BIOS description corrected, Table 10 corrected	2017-Jul-17	
1.6	layout renewed, content updated	2020-Apr-07	
1.7	Update the Accessories List	2020-Jul-23	
1.8	new memory in table Table 16	2020-Nov-23	hjs
1.9	W2016 issues, new PNs in Accessories list	2021-Mar-29	hjs
1.91	Port x8 deleted in chapter 2.2.5.3, block diagram updated	2021-May-06	hjs
1.92	Minor modifications	2021-May-24	hjs
1.93	Update block diagram, update accessories list	2022-July-22	ih
1.94	New Kontron logo, added RTC chapter	2023-April-06	ih

Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit http://www.kontron.com/terms-and-conditions.

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit http://www.kontron.com/terms-and-conditions.

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website CONTACT US.

Customer Support

Find Kontron contacts by visiting: https://www.kontron.com/support-and-services.

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.

For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit https://www.kontron.com/support-and-services.

Customer Comments

If you have any difficulties using this user guide, discover an error, or just want to provide some feedback, contact Kontron support. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.

Symbols

The following symbols may be used in this manual

DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
NOTICE	NOTICE indicates a property damage message.
CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
	**Electric Shock!** This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
	**ESD Sensitive Device!** This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
	**HOT Surface!** Do NOT touch! Allow to cool before servicing.
	**Laser!** This symbol inform of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.
	This symbol indicates general information about the product and the user guide. This symbol also indicates detail information about the specific product configuration.
	This symbol precedes helpful hints and tips for daily use.

For Your Safety

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

⚠CAUTION

Warning

All operations on this product must be carried out by sufficiently skilled personnel only.

⚠CAUTION



Electric Shock!

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.

Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

Special Handling and Unpacking Instruction

NOTICE



ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the battery.

⚠CAUTION

Danger of explosion if the battery is replaced incorrectly.

- Replace only with same or equivalent battery type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this user guide or received from Kontron Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version that must not be exceeded. If batteries are present, their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, only follow the instructions supplied by the present user guide.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to complying with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit http://www.kontron.com/about-kontron/corporate-responsibility/quality-management.

Disposal and Recycling

Kontron's products are manufactured to satisfy environmental protection requirements where possible. Many of the components used are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- Reduce waste arising from electrical and electronic equipment (EEE)
- Make producers of EEE responsible for the environmental impact of their products, especially when the product become waste
- Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE
- Improve the environmental performance of all those involved during the lifecycle of EEE



Environmental protection is a high priority with Kontron.

Kontron follows the WEEE directive

You are encouraged to return our products for proper disposal.

Table of Contents

1/ Introduction 19
1.1 Product Description 19
1.2 Product Naming Clarification 19
1.3 Understanding COM Express® Functionality 19
1.4 COM Express® Documentation 20
1.5 COM Express® Benefits 20
2/ Product Specification 21
2.1 Module Definition 21
2.1.1 Commercial Grade Modules 21
2.1.2 Industrial Temperature Grade Modules 21
2.2 Functional Specification 22
2.2.1 Processor 22
2.2.2 Chipset 24
2.2.3 Storage 24
2.2.4 USB 25
2.2.5 PCI Express Configuration 25
2.2.6 Ethernet 27
2.2.7 Misc Interfaces and Features 29
2.2.8 Kontron Features 29
2.2.9 Additional Features 30
2.2.10 Power Features 30
2.3 Block Diagram COMe-bBD6 31
2.4 Accessories 32
2.4.1 Product Specific Accessories 32
2.4.2 General Accessories 32
2.5 Electrical Specification 34
2.5.1 Supply Voltage 34
2.5.2 Power Supply Rise Time 34
2.5.3 Supply Voltage Ripple 34
2.5.4 Power Consumption 34
2.5.5 ATX Mode 34
2.5.6 Single Supply Mode 35
2.6 Power Control 36
2.6.1 Power Supply 36
2.6.2 Power Button (PWRBTN#) 36
2.6.3 Power Good (PWR_OK) 36
2.6.4 Reset Button (SYS_RESET# Signal) 36
2.6.5 SM-Bus Alert (SMB_ALERT#) 36
2.7 Environmental Specification 37
2.7.1 Temperature Specification 37
2.7.2 Operating with Kontron Heatspreader Plate Assembly 37
2.7.3 Operating without Kontron heatspreader plate assembly 37
2.7.4 Humidity 38
2.8 Standards and Certifications 38
2.8.1 RoHS II 38
2.8.2 Component Recognition UL 60950-1 38
2.8.3 WEEE Directive 38
2.8.4 Conformal Coating 38
2.8.5 Shock & Vibration 38

2.8.6 EMC ... 39
2.9 MTBF ... 39
2.10 Mechanical Specification ... 40
2.10.1 Dimension ... 40
2.10.2 Height ... 41
2.11 Thermal Management, Heatspreader and Cooling Solutions ... 41
2.12 Onboard Fan Connector ... 42
2.13 Onboard Test Connector ... 43
3/ Features and Interfaces ... 44
3.1 S5 Eco Mode ... 44
3.2 Rapid Shutdown ... 44
3.2.1 Overview ... 44
3.2.2 Crowbar implementation details ... 44
3.3 LPC ... 45
3.4 Serial Peripheral Interface (SPI) ... 46
3.5 SPI boot ... 46
3.5.1 Using an external SPI flash ... 46
3.5.2 External SPI flash on Modules with Intel® ME ... 49
3.6 M.A.R.S. ... **Fehler! Textmarke nicht definiert.**
3.7 UART ... 49
3.8 Fast I2C ... 51
3.9 GPIO - General Purpose Input and Output ... 51
3.10 Triple Staged Watchdog Timer ... 52
3.10.1 Basics ... 52
3.10.2 WDT Signal ... 52
3.11 Intel® Fast Flash Standby™/Rapid Start Technology™ ... 52
3.11.1 Requirements ... 53
3.12 Speedstep Technology ... 54
3.13 C-States ... 55
3.14 Hyper Threading ... 55
3.15 ACPI Suspend Modes and Resume Events ... 55
4/ System Resources ... 57
4.1 Interrupt Request (IRQ) Lines ... 57
4.2 Memory Area ... 57
4.3 I/O Address Map ... 58
4.4 Peripheral Component Interconnect (PCI) Devices ... 59
4.5 I2C Bus ... 60
4.6 System Management (SM) Bus ... 60
5/ Pin-out List ... 61
5.1 Connector X1A Row A ... 62
5.2 Connector X1A Row B ... 67
5.3 Connector X1B Row C ... 72
5.4 Connector X1B Row D ... 76
6/ BIOS Operation ... 80
6.1 Determining the BIOS Version ... 80
6.2 BIOS Update ... 80
6.3 Setup Guide ... 81
6.4 POST Codes ... 81
6.4.1 Start AMI® Aptio Setup Utility ... 81
6.5 BIOS Setup ... 84

6.5.1 Main 84
6.5.2 Advanced 86
6.5.3 Intel RC Setup 121
6.5.4 Security 204
6.5.5 Boot 207
6.5.6 Event Logs 208
6.5.7 Save & Exit 211
7/ Technical Support 215
7.1 Warranty 215
7.2 Returning Defective Merchandise 215

List of Tables

Table 1: Pin Assignment 19
Table 2: Commercial Grade Modules (0°C to 60°C operating) 21
Table 3: Industrial Temperature Grade Modules by Design (E2, -40°C to 85°C Operating) 21
Table 4: Intel® Xeon® Processor D-1500 Product Family Specifications 23
Table 5: Memory Features 24
Table 6: PCH Features 24
Table 7: Storage Features 24
Table 8: USB Features 25
Table 9: PCIe Gen 3 Ports 26
Table 10: PCIe Gen 2 Ports 27
Table 11: Ethernet Features 29
Table 12: Misc Interfaces and Features 29
Table 13: Kontron Features 29
Table 14: Power Features 30
Table 15: Product Specific Accessories List 32
Table 16: General Accessories List 32
Table 17: COM Express® connector Electrical Specifications 34
Table 18: ATX Mode 34
Table 19: Single Supply Mode 35
Table 20: Temperature Specification 37
Table 21: Test Specification 37
Table 22: Electrical Characteristics 42
Table 23: Supported BIOS Features 45
Table 24: SPI Boot Pin Configuration 46
Table 25: Supported SPI boot flash types for 8-SOIC package 46
Table 27: GPIO Pins 51
Table 28: Time-out events 52
Table 29: Defined C-States 55
Table 30: List of Interrupt Requests 57
Table 31: Designated Memory Locations 57
Table 32: Designated I/O Port Addresses 58
Table 33: PCI Device list 59
Table 34: I2C Bus Port Addresses 60
Table 35: Designated I/O Port Addresses 60
Table 36: Electrical characteristic 61
Table 37: Connector X1A Row A Pin-out List 62
Table 38: Connector X1A Row B Pin-out List 67
Table 39: Connector X1B Row C Pin-out List 72
Table 40: Connector X1B Row D Pin-out List 76
Table 41: Key Assignment 81
Table 42: Important POST codes during boot-up 81
Table 43: BIOS Setup Screen Sections 82
Table 44: Legend Keys List 82

Table 45: Main Features List 84
Table 46: Trusted Computing Features List 88
Table 47: ACPI Settings Features List 89
Table 48: Miscellaneous Features List 90
Table 49: Generic LPC Decode Ranges Features List 91
Table 50: Smart Battery Configuration Features List 92
Table 51: Watchdog Features List 94
Table 52: FPD UART Serial Port 1 Configuration Features List 96
Table 53: FPD UART Serial Port 2 Configuration Features List 97
Table 54: W83627DHGSEC Serial Port 1 Configuration Features List 99
Table 55: W83627DHGSEC Serial Port 2 Configuration Features List 100
Table 56: W83627DHGSEC Parallel Port Configuration Features List 101
Table 57: H/W Monitor Features List 102
Table 58: Serial Port Console Redirection Features List 104
Table 59: Console Redirection Settings Features List 105
Table 60: Legacy Console Redirection Settings Features List 107
Table 61: Out-of-Band Management Console Redirection Settings Features List 108
Table 62: PCI Subsystem Settings Features List 109
Table 63: PCI Express Settings Features List 111
Table 64: PCI Express Gen 2 Settings Features List 113
Table 65: PCI Hot-Plug Settings Features List 115
Table 66: Network Stack Configuration Features List 116
Table 67: CSM Configuration Features List 117
Table 68: Advanced USB Configuration Features List 120
Table 69: Processor Configuration Features List 122
Table 70: CPU Socket Configuration Features List 125
Table 71: Advanced Power Management Configuration Features List 126
Table 72: CPU P State Control Features List 127
Table 73: XE Ration Limit Features List 129
Table 74: CPU HWPM State Control Features List 130
Table 75: CPU C State Control Features List 131
Table 76: CPU T State Control Features List 132
Table 77: CPU Thermal Management Features List 133
Table 78: Energy Perf BIAS Features List 135
Table 79: Program PowerCTL_MSR Features List 136
Table 80: Program PPO_CURT_CFG_CTRL_MSR Features List 137
Table 81: PSI Config Features List 138
Table 82: Program CSR_ENTRY_CRITERIA Features List 139
Table 83: CPU Advanced PM Turning Features List 140
Table 84: Program CSR_SWLTROVRD Features List 142
Table 85: Program MSR VR_MISC_CONFIG Features List 143
Table 86: Program MSR VR_MISC_CONFIG2 Features List 144
Table 87: DRAM RAPL Configuration Features List 145
Table 88: Socket RAPL Config Features List 146
Table 89: Common RefCode Configuration Features List 148
Table 90: QPI General Configuration Features List 150
Table 91: QPI Per Socket Configuration - CPU Features List 154
Table 92: Memory Configuration Features List 155
Table 93: Memory Thermal Features List 159
Table 94: Memory Power Savings Advanced Options Features List 160
Table 95: Memory Timings & Voltage Override Features List 161
Table 96: Memory Map Features List 162
Table 97: Memory RAS Configuration Features List 163
Table 98: IIO Configuration Features List 164
Table 99: IIO0 Configuration Features List 166
Table 100: Socket 0 PcieD00F0 - Port 0/DMI Features List 167
Table 101: Socket 0 PcieD0XFX – Port XX Features List 169
Table 102: IOAT Configuration Features List 171
Table 103: IIO General Configuration Features List 172

Table 104: Intel VT for Direct I/O (VT-d) Features List 173
Table 105: IIO South Complex Configuration Features List 174
Table 106: PHC Devices Features List 176
Table 107: PCH Express Configuration Features List 178
Table 108: PCH Express Root Port Features List 179
Table 109: PCH SATA Configuration Features List 181
Table 110: SATA Mode Options Features List 183
Table 111: USB Configuration Features List 184
Table 112: Security Configuration Features List 185
Table 113: Azalia Configuration Features List 186
Table 114: Platform Thermal Configuration Features List 187
Table 115: Miscellaneous Configuration Features List 188
Table 116: Server ME General Configuration Features List 191
Table 117: Override ICC Clock Enables Features List 192
Table 118: Override ICC Spectrum Configuration Features List 194
Table 119: NM Configuration Features List 195
Table 120: Server ME Configuration Features List 196
Table 121: Runtime Error Logging Features List 197
Table 122: Whea Settings Features List 198
Table 123: Memory Error Enabling Features List 199
Table 124: IIO Error Enable Features List 200
Table 125: IIO Coherency Interface Error Enable Features List 201
Table 126: PCI/PCI Error Enabling Features List 202
Table 127: Reserved Memory Features List 203
Table 128: Security Features List 204
Table 129: Secure Boot menu Features List 205
Table 130: Key Management Features List 206
Table 131: Boot Features List 207
Table 132: Change Smbios Event Log Settings Features List 209
Table 133: Save & Exit Features List 211
Table 134: PICMG COME.0 Signal Terminology 212

List of Figures

Figure 1: Block Diagram COMe-bBD6 31
Figure 2: RoHS 38
Figure 3: Component Recognition UL 38
Figure 4: MTBF Temperature De-rating 39
Figure 5: Module Dimensions 40
Figure 6: Module Height 41
Figure 7: Location of the FAN Connectors 42
Figure 8: Entering USB Key Partition Name 47
Figure 9: Using kflash help option 48
Figure 10: Programming the Flash Image Drive 48
Figure 11: Main Menu Screen 84
Figure 12: Platform Information Menu Screen 85
Figure 13: Advanced Menu Screen 86
Figure 14: iSCSI Configuration Menu Screen 87
Figure 15: Trusted Computing Menu Screen 88
Figure 16: ACPI Settings Menu Screen 89
Figure 17: Miscellaneous Menu Screen 90
Figure 18: Generic LPC Decode Ranges Menu Screen 91
Figure 19: Smart Battery Configuration Menu Screen 92
Figure 20: Battery Information Menu Screen 93
Figure 21: Watchdog Menu Screen 94
Figure 22: FPD UART Super IO Configuration Menu Screen 95
Figure 23: FPD UART Serial Port 1 Configuration Menu Screen 96

Figure 24: FPD UART Serial Port 2 Configuration Menu Screen 97
Figure 25: W83627DHGSEC Super IO Configuration Menu Screen 98
Figure 26: W83627DHGSEC Serial Port 1 Configuration Menu Screen 99
Figure 27: W83627DHGSEC Serial Port 2 Configuration Menu Screen 100
Figure 28: W83627DHGSEC Parallel Port Configuration Menu Screen 101
Figure 29: H/W Monitor Menu Screen 102
Figure 30: Serial Port Console Redirection Menu Screen 104
Figure 31: Console Redirection Settings Menu Screen 105
Figure 32: Legacy Console Redirection Settings Menu Screen 107
Figure 33: Out-of-Band Management Console Redirection Settings Menu Screen 108
Figure 34: PCI Subsystem Settings Menu Screen 109
Figure 35: PCI Express Settings Menu Screen 111
Figure 36: PCI Express Gen 2 Settings Menu Screen 113
Figure 37: PCI Hot-Plug Settings Menu Screen 115
Figure 38: Network Stack Configuration Menu Screen 116
Figure 39: CSM Configuration Menu Screen 117
Figure 40: NVMe Configuration Menu Screen 119
Figure 41: Advanced USB Configuration Menu Screen 120
Figure 42: Intel RC Setup Menu Screen 121
Figure 43: Processor Configuration Menu Screen 122
Figure 44: Pre-Socket Configuration Menu Screen 124
Figure 45: CPU Socket Configuration Menu Screen 125
Figure 46: Advanced Power Management Configuration Menu Screen 126
Figure 47: CPU P State Control Menu Screen 127
Figure 48: XE Ratio Limit Menu Screen 129
Figure 49: CPU HWPM State Control Menu Screen 130
Figure 50: CPU C State Control Menu Screen 131
Figure 51: CPU T State Control Menu Screen 132
Figure 52: CPU Thermal Management Menu Screen 133
Figure 53: CPU Advanced PM Turning Menu Screen 134
Figure 54: Energy Perf BIAS Menu Screen 135
Figure 55: Program PowerCTL_MSR Menu Screen 136
Figure 56: Program PPO_CURT_CFG_CTRL_MSR Menu Screen 137
Figure 57: PSI Config Menu Screen 138
Figure 58: Program CSR_ENTRY_CRITERIA Menu Screen 139
Figure 59: CPU Advanced PM Turning Menu Screen 140
Figure 60: Program CSR_SWLTROVRD Menu Screen 142
Figure 61: Program MSR VR_MISC_CONFIG Menu Screen 143
Figure 62: Program MSR VR_MISC_CONFIG2 Menu Screen 144
Figure 63: DRAM RAPL Configuration Menu Screen 145
Figure 64: Socket RAPL Config Menu Screen 146
Figure 65: Common RefCode Configuration Menu Screen 148
Figure 66: QPI Configuration Menu Screen 149
Figure 67: QPI General Configuration Menu Screen 150
Figure 68: QPI Status Menu Screen 152
Figure 69: QPI Per Socket Configuration Menu Screen 153
Figure 70: QPI Per Socket Configuration - CPU Menu Screen 154
Figure 71: Memory Configuration Menu Screen 155
Figure 72: Memory Topology Menu Screen 158
Figure 73: Memory Thermal Menu Screen 159
Figure 74: Memory Power Savings Advanced Options Menu Screen 160
Figure 75: Memory Timings & Voltage Override Menu Screen 161
Figure 76: Memory Map Menu Screen 162
Figure 77: Memory RAS Configuration Menu Screen 163
Figure 78: IIO Configuration Menu Screen 164
Figure 79: IIO0 Configuration Menu Screen 166
Figure 80: Socket 0 PcieD00F0 - Port 0/DMI Menu Screen 166
Figure 81: Socket 0 PcieD0XFX – Port XX Menu Screen 169
Figure 82: IOAT Configuration Menu Screen 171

Figure 83: IIO General Configuration Menu Screen 172
Figure 84: Intel VT for Directed I/O (VT-d) Menu Screen 173
Figure 85: IIO South Complex Configuration Menu Screen 174
Figure 86: PCH Configuration Menu Screen 175
Figure 87: PCH Devices Menu Screen 176
Figure 88: PCH Express Configuration Menu Screen 178
Figure 89: PCH Express Root Port Menu Screen 179
Figure 90: PCH SATA Configuration Menu Screen 181
Figure 91: SATA Mode Options Menu Screen 183
Figure 92: USB Configuration Menu Screen 184
Figure 93: Security Configuration Menu Screen 185
Figure 94: Azalia Configuration Menu Screen 186
Figure 95: Platform Thermal Configuration Menu Screen 187
Figure 96: Miscellaneous Configuration Menu Screen 188
Figure 97: Server ME Debug Configuration Menu Screen 190
Figure 98: Server ME General Configuration Menu Screen 191
Figure 99: Override ICC Clock Enables Menu Screen 192
Figure 100: Override ICC Spectrum Configuration Menu Screen 194
Figure 101: NM Configuration Menu Screen 195
Figure 102: Server ME Configuration Menu Screen 196
Figure 103: Runtime Error Logging Menu Screen 197
Figure 104: Whea Settings Menu Screen 198
Figure 105: Memory Error Enabling Menu Screen 199
Figure 106: IIO Error Enable Menu Screen 200
Figure 107: IIO Coherency Interface Error Enable Menu Screen 201
Figure 108: PCI/PCI Error Enabling Menu Screen 202
Figure 109: Reserved Memory Menu Screen 203
Figure 110: Security Menu Screen 204
Figure 111: Secure Boot menu Menu Screen 205
Figure 112: Key Management Menu Screen 206
Figure 113: Boot Menu Screen 207
Figure 114: Event Logs Menu Screen 208
Figure 115: Change Smbios Event Log Settings Menu Screen 209
Figure 116: View Smbios Event Log Menu Screen 210
Figure 117: Save & Exit Menu Screen 211

1/ Introduction

1.1 Product Description

Kontron's Computer-on-Module COMe-bBD6 is a COM Express® BASIC TYPE 6 WITH Intel® Xeon® PROCESSOR D-1500 with support for Pin-out Type 6, and an additional communication interface block. Kontron's module covers both the need for latest interface technology and the need to extend life-time. The Intel® Xeon®D1500 Generation increases efficiency and performance per watt ratio, which is a result of the innovative 14nm technology and has up to 16 cores for control, micro server, storage and communication applications in Internet of Things (IoT) and embedded environment. The COMe-bBDi6R is also designed for industrial temperature environment.

- Intel® Xeon® Processor D-1500 System on Chip (SoC), newest member of the Intel® Xeon® Processor family
- DDR4 memory technology up to 32 GByte ECC, 2x SODIMMs
- high-speed connectivity x16 PCIE 3.0 + x8 PCIE2.0, Dual 10GbE interfaces (option)

1.2 Product Naming Clarification

The product names for Kontron COM Express® Computer-on-Modules consist of a short form of the industry standard (COMe-), the form factor (b=basic, c=compact, m=mini), the capital letters for the CPU and Chipset Codenames (XX) and the pin-out type (#) followed by the CPU Name.

COM Express® defines a Computer-On-Module, or COM, with all components necessary for a bootable host computer, packaged as a super component.

- COMe-bXX# modules are Kontron's COM Express® modules in basic form factor (125mm x 95mm)
- COMe-cXX# modules are Kontron's COM Express® modules in compact form factor (95mm x 95mm)

1.3 Understanding COM Express® Functionality

All Kontron COM Express® basic and compact modules contain two 220pin connectors; each of it has two rows called Row A & B on primary connector and Row C & D on secondary connector. The COM Express® Computer-On-Module (COM) features the following maximum amount of interfaces according to the PCI Industrial Computer Manufacturers Group (PICMG) module Pin-out type.

Table 1: Pin Assignment

Feature	Type 6 Pin-Out	COMe-bBD6 Pin-Out
HD Audio	1x	-
Gbit Ethernet	1x	2x, (the second pin-out is non- standard, see 2.2.6 and 5/)
Serial ATA	4x	4x
Parallel ATA	-	-
PCI	-	-
PCI Express x8	1x	1x
PCI Express x16 (PEG)	1x	1x
USB Client	-	-
USB 2.0	8x	4x
USB 3.0	4x	4x
VGA	1x	Not used

Feature	Type 6 Pin-Out	COMe-bBD6 Pin-Out
LVDS	Dual Channel	Not used
DP++ (SDVO/DP/HDMI/DVI)	3x	DDI interface used for 2x 10G interface, (the second pin-out is non- standard, see 2.2.6 and 5/)
LPC	1x	1x
External SMB	1x	1x
External I2C	1x	1x
GPIO	8x	8x
SDIO shared w/GPIO	1x optional	-
UART (2-wire COM)	2x	2x
FAN PWM out	1x	1x

1.4 COM Express® Documentation

The COM Express® Specification defines the COM Express® module form factor, pin-out, and signals. This document is available at the PICMG® website by filling out the order form.

1.5 COM Express® Benefits

COM Express® modules are very compact, highly integrated computers. All Kontron COM Express® modules feature a standardized form factor and a standardized connector layout which carry a specified set of signals. Each COM is based on the COM Express® specification. This standardization allows designers to create a single-system baseboard that can accept present and future COM Express® modules.

The baseboard designer can optimize exactly how each of these functions implements physically. Designers can place connectors precisely where needed for the application on a baseboard designed to optimally fit a system's packaging.

A single baseboard design can use a range of COM Express® modules with different sizes and pin-outs. This flexibility can differentiate products at various price/performance points, or when designing future proof systems that have a built-in upgrade path. The modularity of a COM Express® solution also ensures against obsolescence when computer technology evolves. A properly designed COM Express® baseboard can work with several successive generations of COM Express® modules.

A COM Express® baseboard design has many advantages of a customized computer-board design and, additionally, delivers better obsolescence protection, heavily reduced engineering effort, and faster time to market.

2 / Product Specification

2.1 Module Definition

The COM Express® basic sized Computer-on-Module COMe-bBD6 (bBD6) follows pin-out Type 6 and is compatible to PICMG specification COM.0 Rev 2.1. The COMe-bBD6, based on the latest Grangeville platform, is available in different variants to cover the different demands in performance, price and power.

2.1.1 Commercial Grade Modules

The following is a list of modules for commercial temperature range.

Table 2: Commercial Grade Modules (0°C to 60°C operating)

Product Number	Product Name	Processor	PCH
68002-0000-48-8	COMe-bBD6 D-1548	Intel® Xeon® Processor D-1548	Integrated
68002-0000-37-8	COMe-bBD6 D-1537	Intel® Xeon® Processor D-1537	Integrated
68002-0000-28-6	COMe-bBD6 D-1528	Intel® Xeon® Processor D-1528	Integrated
68002-0000-27-4	COMe-bBD6 D-1527	Intel® Xeon® Processor D-1527	Integrated
68002-0000-18-4	COMe-bBD6 D-1518	Intel® Xeon® Processor D-1518	Integrated
68002-0000-17-4	COMe-bBD6 D-1517	Intel® Pentium® Processor D1517	Integrated
68002-0000-08-4	COMe-bBD6 D-1508	Intel® Xeon® Processor D1508	Integrated

2.1.2 Industrial Temperature Grade Modules

Industrial temperature grade modules are available based on their design. Please contact your local sales or support for further details.

Table 3: Industrial Temperature Grade Modules by Design (E2, -40°C to 85°C Operating)

Product Number	Product Name	Processor	PCH
68003-0000-19-4	COMe-bBDi6R D-1519	Intel® Pentium® Processor D1519	Integrated
68003-0000-39-8	COMe-bBDi6R D-1539	Intel® Xeon® Processor D-1539	Integrated
68003-0000-59-9	COMe-bBDi6R D-1559	Intel® Pentium® Processor D-1559	Integrated

2.2 Functional Specification

2.2.1 Processor

The 14nm Intel® Xeon® processor D-1500 product family with 37.5mm x 37.5mm package size (1667 Ball FCBGA) supports:

- Performance
  - Intel® 64
  - Intel® Turbo Boost Technology 2.0
  - Intel® Advanced Vector Extensions 2 (AVX2)
  - Memory Bandwidth Monitoring
- Xeon Class Reliability Availability Serviceability (RAS) includes:
  - Error-Correcting Code (ECC) Single Device Data Correction (SDDC),
  - Memory Demand and Patrol Scrubbing,
  - Data Scrambling with address,
  - End-to-end Cyclic Redundancy Check (ECRC) on PCIe,
  - PCIe and GbE Advanced Error Reporting (AER),
  - Intel® Corrected Machine Check Interrupt (CMCI) Virtualization.
- Virtualization:
  - Intel® Virtualization Technology (VT-x)
  - Advanced Programmable Interrupt Controller virtualization (APICv)
  - Intel® Virtual Machine Control Structure Shadowing (Intel® VMCS Shadowing)
  - Intel® Virtualization Technology for Directed I/O (VT-d)
  - Extended Page Table Accessed and Dirty bits (A/D bits for EPT)
  - Posted Interrupts,
  - Single-Root Input/Output Virtualization (SR-IOV)
  - VT Cache Quality of Service (QoS) and QoS Monitoring/Enforcement
- Security
  - Intel® Trusted Execution Technology (TXT) (requires custom BIOS)
  - Intel® Advanced Encryption Standard New Instructions (AES-NI)
  - Intel® OS Guard (Supervisor Mode Access Protection (SMAP))
  - Intel® Secure Key (RDSEED)
- Intel® Hyper-Threading Technology
- Configurable Thermal Design Power (cTDP)
- Intel® Thermal Monitoring Technologies
- Node Manager Base Power Management (ME FW)

Table 4 provides a list of processors and specifications of the Intel® Xeon® Processor D-1500 Product Family compatible with COMe-bBD6.

Table 4: Intel® Xeon® Processor D-1500 Product Family Specifications

Intel® Xeon® Processor	D-1548	D-1537	D-1528	D-1527	D-1518	D1517	D1508	D1519	D-1539	D-1559
# of Cores	8	8	6	4	4	4	2	4	8	12
# of Threads	16	16	12	8	8	8	4	8	16	24
Processor Base Frequency	2GHz	1,7GHz	1,9GHz	2,2GHz	2,2GHz	2,2GHz	2,2GHz	1,5GHz	1,6GHz	1,5GHz
Max Turbo Frequency	2,6GHz	2,3GHz	2,4GHz	2,7GHz	2,2GHz	2,6GHz	2,6GHz	TBD	TBD	TBD
Temperature								eTEMP	eTEMP	eTEMP
Thermal Design Power (TDP)	45W	35W	35W	35W	35W	25W	25W	25W	35W	45W
Command	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0	64Bit AVX 2.0
Cache	12MB	12MB	9MB	6MB	6MB	6MB	3MB	6MB	12MB	18MB
Max. Memory Speed	DDR4 2400 MHz	DDR4 2133 MHz	DDR4 2133 MHz	DDR4 2133 MHz	DDR4 2133 MHz	DDR4 2133 MHz	DDR4 1866 MHz	DDR4 2133 MHz	DDR4 2133 MHz	DDR4 2133 MHz
Max Memory Size	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)	64 GB (2x32)
ECC Memory Supported	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCIe Express (COMe PEG) 3.0	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.	16x, 4 Contr.
PCIe Lanes (COMe) 2.0	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.	8x, 8 Contr.
10G KR	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
10G Base-T	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1000 Base-T	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VT-d	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AES-NI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5: Memory Features

Socket	2x DDR4 SO-DIMM
Memory Type	DDR4-2400 non-ECC or ECC
Maximum Size	2x32 GB
Technology	Dual Channel

2.2.2 Chipset

The integrated Platform Controller Hub (PCH) supports:

- PCI Express Revision 3.0
- PCI Express Configurations x1, x4, x8
- Intel® Virtualization Technology for Directed I/O (VT-d)
- Intel® Trusted Execution Technology (TXT)
- Intel® Anti-Theft Technology
- Intel® Rapid Storage Technology
- Intel® Smart Response Technology

Table 6: PCH Features

Feature	PCH
Rapid Storage	YES
USB 3.0	YES
VT-d	YES
TXT	YES (but not supported on COMe-bBD6)

2.2.3 Storage

Table 7: Storage Features

SD Card support	-
onboard SATA NAND drive support	-
IDE Interface	-
Serial-ATA	4x SATA 6 Gb/s
SATA AHCI	NCQ, HotPlug, Staggered Spinup, eSATA, PortMultiplier

2.2.4 USB

Table 8 provides a list of USB connections supported by COMe-bBD6.

Table 8: USB Features

USB 3.0/2.0	4x USB 3.0/2.0
USB Client	-



Due to its internal configuration, the Intel® Xeon® Processor D-1500 Family chipset only supports up to 4 USB Hubs.

2.2.5 PCI Express Configuration

The Xeon D-1500 processor has one x16 and one x8 Gen 3 ports from the integrated I/O and one x8 Gen 2 port from the integrated PCH.

2.2.5.1 Gen 3 PCI-Express Graphic (PEG) port

The x16 PCI Express Graphics (PEG) port is compatible to standard PCI Express (PCIe) devices like Ethernet or RAID controllers. This port is available on the COMe connector. There are four root ports allowing the COMe-bBD6 to support the following port configuration:

- One port x16 (default)
- Two ports x8
- One port x8 plus two ports x4
- Four ports x4

The configuration can be selected by a BIOS option in the IIO menu, refer to 6.5.3.36 IIO Configuration.

Table 9: PCIe Gen 3 Ports

Feature	Configuration 0	Configuration 1	Configuration 2	Configuration 3
Lane 0	x16	x8	x8	x4
Lane 1				
Lane 2				
Lane 3				
Lane 4				x4
Lane 5				
Lane 6				
Lane 7				
Lane 8		x8	x4	x4
Lane 9				
Lane 10				
Lane 11				
Lane 12			x4	x4
Lane 13				
Lane 14				
Lane 15				

2.2.5.2 Gen 3 x8 port

This port is used internally on the bBD6 for connecting the two I210-IT Ethernet controllers and it is not available for the user on the COMe connectors.

2.2.5.3 Gen 2 PCI-Express x8 port

This port is available on the COMe connector. There are eight root ports allowing it to be configured as an 8 x1 interface for connecting up to eight devices. The following configurations are supported by different BIOS binary:

- One port x4 plus 4 ports x1
- Two ports x4
- Eight ports x1

Table 10: PCIe Gen 2 Ports

Feature	Configuration 0	Configuration 1	Configuration 2	Configuration 3
Lane 0	x1	x4	x4	x1
Lane 1	x1			x1
Lane 2	x1			x1
Lane 3	x1			x1
Lane 4	x1	x4	x1	x4
Lane 5	x1		x1	
Lane 6	x1		x1	
Lane 7	x1		x1	

Configuration0 is by (default). Configuration 3 does only work without Ethernet. Other configurations are provided in the BIOS download package available on EMD Customer Section.

2.2.6 Ethernet

The COMe-bBD6 offers the following Ethernet Controllers:

- Two Intel® Ethernet I210 Controllers
- One Intel® Dual-Port Ethernet 10GbE Controller

The I210 controller has the following features:

- Platform Power Efficiency
  - IEEE 802.3az Energy Efficient Ethernet (EEE)
  - Proxy: ECMA-393 and Windows* logo for proxy offload
- Advanced Features:
  - -40 to 85 °C industrial temperature
  - Jumbo frames
  - Interrupt moderation, VLAN support, IP checksum offload
  - PCIe OBFF (Optimized Buffer Flush/Fill) for improved system power management
  - Four transmit and four receive queues
  - RSS and MSI-X to lower CPU utilization in multi-core systems
  - Advanced cable diagnostics, auto MDI-X
  - ECC – error correcting memory in packet buffers
- Manageability:
  - Preboot Execution Environment (PXE) and Internet Small Computer System Interface (iSCSI) boot

For more information on the I210 Controller, refer to the *Intel® Ethernet Controller I210 Datasheet*.

The 10GbE controller has the following features:

- Optimized for Virtualization
  - 128 Tx and Rx queues per port
  - SR-IOV (64 VFs), Virtual Machine Device Queues (VMDq) (64 VMs)
  - Simple Virtual Ethernet Port Aggregator (VEPA), Virtual Ethernet Bridge (VEB)
- Software Defined Networking:
  - Virtual Extensible LAN (VXLAN),
  - Network Virtualization using Generic Routing Encapsulation (NVGRE) Network Overlays
- Broad OS Support and Validation:
  - Windows, VMWare, Linux, and Solaris
- Unified networking:
  - Block Storage (iSCSI boot and Fibre Channel over Ethernet (FCoE) Initiator)
  - DCB up to 8 traffic Classes
- Adaptive Power Management:
  - IEEE 802.3az EEE

The 10G Ethernet controller supports the following operation modes:

- Backplane:
  - 10GBASE-KR for GbE backplane applications (IEEE802.3 clause 72)
  - 10GBASE-KR FEC (IEEE 802.3 Clause 74)
  - 1000BASE-KX for GbE backplane applications (IEEE802.3 clause 70)
  - Auto-negotiation for backplane Ethernet (IEEE 802.3 Clause 73)
- 10Gb SFP+:
  - An external PHY is needed. For more information, contact Kontron.
- 10GBASE-T:

An external PHY is needed. For more information, contact Kontron. An interposer is available from Kontron to test this configuration (see Table 15 and 0

  - Onboard Test Connector)

In order to gain access to the 10GbE Controller and second I210 functionalities, an interposer card is required or specific carrier board support is needed (for more information, contact Kontron). Without an interposer or proper carrier handling, the second I210 is not visible in the PCI device tree and the 10G controller is shown as a "dummy device" and is not usable.

For more information on the 10GbE Controller, refer to the *Intel® Xeon® Processor D-1500 Product Family, Datasheet – Volume 4 of 4: Intel® Xeon® Processor D-1500 Product Family LAN Controller*.

Table 11: Ethernet Features

Ethernet	10/100/1000 Mbit
Ethernet controller	Intel® I210
Optional Ethernet Controller	Intel® 10 GbE

2.2.7 Misc Interfaces and Features

Table 12 provides a list of miscellaneous interfaces and features.

Table 12: Misc Interfaces and Features

Supported BIOS Size/Type	16 MB SPI
Onboard Hardware Monitor	Nuvoton NCT7802Y
Trusted Platform Module (TPM)	Infineon SLB9665XT2.0
Miscellaneous	2x UART / PWM FAN

2.2.8 Kontron Features

Table 13 provides a list of Kontron features.

Table 13: Kontron Features

External I2C Bus	Fast I2C, MultiMaster capable
M.A.R.S. support	YES
Embedded API	KEAPI3
Custom BIOS Settings / Flash Backup	YES
Watchdog support	Triple Staged

2.2.9 Additional Features

- All solid capacitors (aluminum-polymer and ceramic). No tantalum capacitors used.
- Optimized RTC Battery monitoring to secure highest longevity
- Fast I2C with transfer rates up to 400kHz

2.2.10 Power Features

Table 14 provides a list of power features.

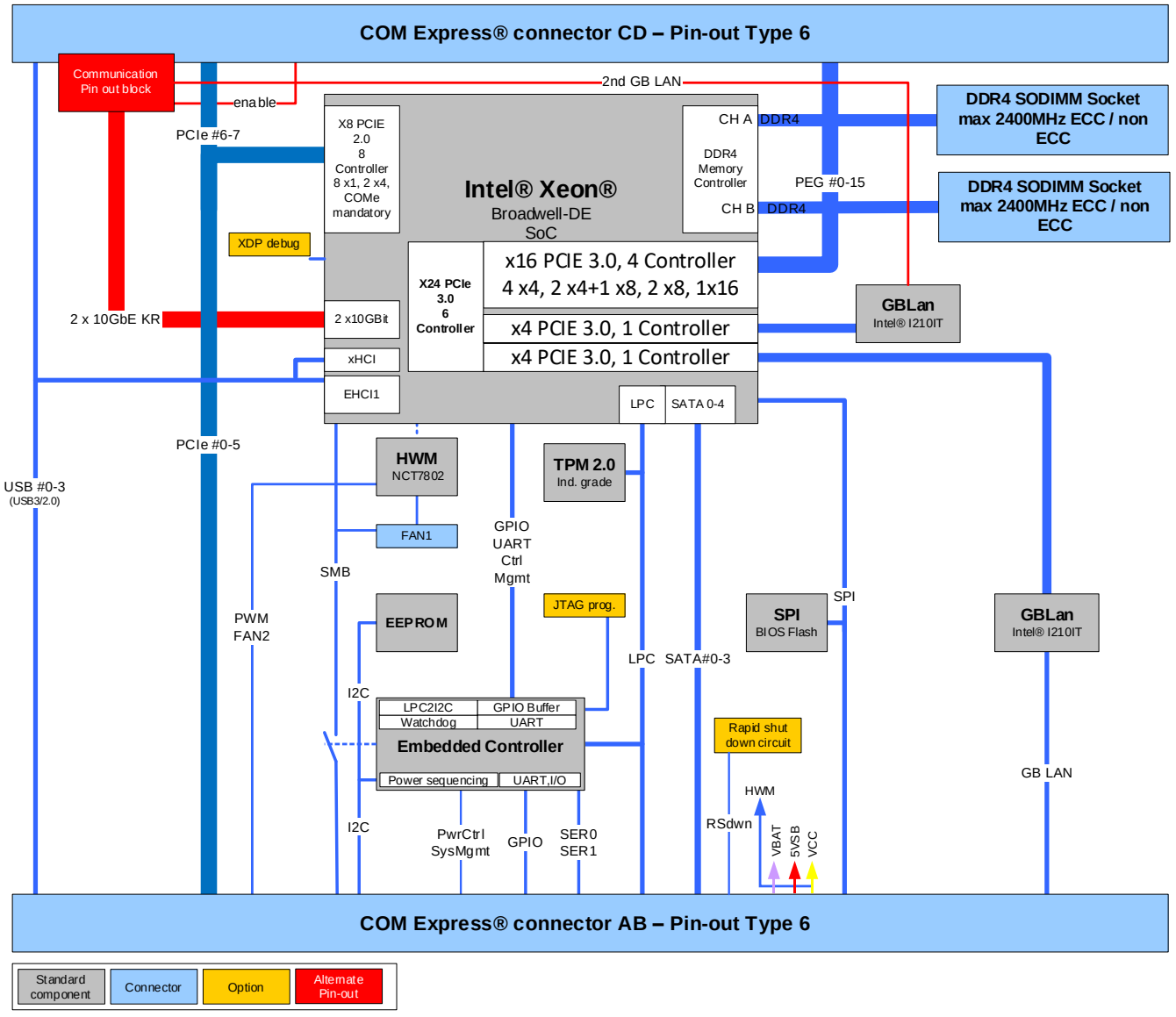
Table 14: Power Features

Singly Supply Support	YES
Supply Voltage	8.5V - 20V
ACPI	ACPI 4.0
S-States	S0, S4, S5
S5 Eco Mode	YES
Misc Power Management	YES

2.3 Block Diagram COMe-bBD6

Figure 1 displays the block diagram applicable to all COMe-bBD6 modules.

Figure 1: Block Diagram COMe-bBD6



2.4 Accessories

2.4.1 Product Specific Accessories

Table 15 provides a list of product accessories specific to COMe-bBD6.

Table 15: Product Specific Accessories List

Product Number	Heatspreader and Cooling Solutions	Comment
68004-0000-99-0	HSP COMe-bBD6/7, thread mounting	Heatspreader with threaded mounting holes
68004-0000-99-1	HSP COMe-bBD6/7, through hole mounting	Heatspreader with through holes
68002-0000-99-0C05	HSK COMe-bBD6/7 active (w/o HSP)	Standard active Cooler for COMe-bBD6 to be mounted on HSP
68002-0000-99-0C06	HSK COMe-bBD6/7 passive (w/o HSP)	Standard passive Cooler for COMe-bBD6 to be mounted on HSP
68200-0000-02-1	ADA-Eval-bBD6 2x 10G, 1x1G LAN COMe-bBD6 Dual 10GBase-T Interposer Card	Interposer Card for COMe-bBD6 based on Intel® Ethernet Connection X557-AT2, for Evaluation only

2.4.2 General Accessories

Table 16 provides a list of general accessories applicable to all COMe pin-out Type 6 products.

Table 16: General Accessories List

Product Number	COMe Carrier	Project Code	Comment
38116-0000-00-5	COM Express® Eval Carrier2 Type 6	ADT6	ATX Carrier with 5mm COMe connector
96006-0000-00-2	COMe POST T6	NFCB	POST Code / Debug Card
Product Number	Mounting	Comment	
38017-0000-00-5	COMe Mount KIT 5mm 1set	Mounting Kit for 1 module including screws for 5mm connectors	
38017-0000-00-0	COMe Mount KIT 8mm 1set	Mounting Kit for 1 module including screws for 8mm connectors	
Product Number	Cables	Comment	
96079-0000-00-0	KAB-HSP 200mm	Cable adapter to connect FAN to module (COMe basic/compact)	
96079-0000-00-2	KAB-HSP 40mm	Cable adapter to connect FAN to module (COMe basic/compact)	
Product Number	Non ECC		
97020-0424-BBD6	DDR4-2400 SODIMM 4GB_BBD6		
97020-0824-BBD6	DDR4-2400 SODIMM 8GB_BBD6		
97020-1624-BBD6	DDR4-2400 SODIMM 16GB_BBD6		
97020-1624-BBD6*	DDR4-2400 SODIMM 32GB_BBD6		
97021-0424-BBD6	DDR4-2400 SODIMM 4GB E2_BBD6		

97021-0824-BBD6	DDR4-2400 SODIMM 8GB E2_BBD6
97021-1624-BBD6	DDR4-2400 SODIMM 16GB E2_BBD6
97021-1624-BBD6*	DDR4-2400 SODIMM 32GB E2_BBD6

* on request

Product Number	ECC
97030-0424-BBD6	DDR4-2400 SODIMM 4GB ECC_BBD6
97030-0824-BBD6	DDR4-2400 SODIMM 8GB ECC_BBD6
97030-1624-BBD6	DDR4-2400 SODIMM 16GB ECC_BBD6
97030-3224-BBD6*	DDR4-2400 SODIMM 32GB ECC_BBD6
97031-0424-BBD6	DDR4-2400 SODIMM 4GB ECC E2_BBD6
97031-0824-BBD6	DDR4-2400 SODIMM 8GB ECC E2_BBD6
97031-1624-BBD6	DDR4-2400 SODIMM 16GB ECC E2_BBD6
97031-3224-BBD6*	DDR4-2400 SODIMM 32GB ECC E2_BBD6

* on request

2.5 Electrical Specification

2.5.1 Supply Voltage

Table 17 provides information regarding the supply voltage specified at the COM Express® connector:

Table 17: COM Express® connector Electrical Specifications

VCC	8.5V - 20V
Standby	5V DC +/- 5%
RTC	2.5V - 3.47V

- 5 V Standby voltage is not mandatory for operation.

2.5.2 Power Supply Rise Time

- The input voltages should rise from ≤10% of nominal to within the regulation ranges within 0.1ms to 20ms.
- There must be a smooth and continuous ramp of each DC input voltage from 10% to 90% of its final set-point following the ATX specification.

2.5.3 Supply Voltage Ripple

Maximum 100 mV peak to peak 0 – 20 MHz.

2.5.4 Power Consumption

The maximum Power Consumption of the different COMe-bBD6 variants is 35 - 70W (100% CPU load on all cores; 90°C CPU temperature).

For Information on Detailed Power Consumption measurements in all states and benchmarks for CPU, Graphics and Memory performance, refer to the Application Note Power&Performance at EMD Customer Section.

2.5.5 ATX Mode

By connecting an ATX power supply with VCC and 5VSB, PWR_OK is set to low level and VCC is off. Press the Power Button to enable the ATX PSU setting PWR_OK to high level and powering on VCC. The ATX PSU is controlled by the PS_ON# signal which is generated by SUS_S3# through inversion. VCC can be 8.5 V – 20 V in ATX Mode. On Computer-on-Modules supporting a wide range input down to 4.75 V the input voltage shall always be higher than 5 V Standby (VCC > 5VSB).

Table 18: ATX Mode

State	PWRBTN#	PWR_OK	V5_StdBy	PS_ON#	VCC
G3	x	x	0 V	x	0 V
S5	high	low	5 V	high	0 V
S5 → S0	PWRBTN Event	low → high	5 V	high →	0 V→ VCC
S0	high	high	5 V	low	VCC

2.5.6 Single Supply Mode

In single supply mode, without 5 V standby the module will start automatically when VCC power is connected and Power Good input is open or at high level (internal PU to 3.3 V). PS_ON# is not used in this mode and VCC can be 8.5 V – 20 V.

To power on the module from S5 state press the power button or reconnect VCC. Suspend/Standby States are not supported in Single Supply Mode.

Table 19: Single Supply Mode

State	PWRBTN#	PWR_OK	V5_StdBy	VCC
G3	0	0	0	0
G3 → S0	high	open / high	OPEN	connecting VCC
S5	high	open / high	OPEN	VCC
S5 → S0	PWRBTN Event	open / high	OPEN	reconnecting VCC



- Signals marked with "x" are not important for the specific power state. There is no difference if connected or open.
- All ground pins have to be tied to the ground plane of the carrier board.
- For more information refer to 2.6 Power Control.

NOTICE

If any of the supply voltages drops below the allowed operating level longer than the specified hold-up time, all the supply voltages should be shut down and left OFF for a time long enough to allow the internal board voltages to discharge sufficiently.
If the OFF time is not observed, parts of the board or attached peripherals may work incorrectly or even suffer a reduction of MTBF. The minimum OFF time depends on the implemented PSU model and other electrical factors and needs to be measured individually for each case.

2.6 Power Control

2.6.1 Power Supply

The COMe-bBD6 supports a power input from 8.5 V – 20 V. The supply voltage is applied through the VCC pins (VCC) of the module connector.

Optionally, 5 V +/- 5% can be applied to the V_5V_STBY pins and allows support for wake-up suspend-to-disk and soft-off state when the VCC power is removed.

Suspend-to-RAM is not supported by the Xeon D-1500.

2.6.2 Power Button (PWRBTN#)

The power button (Pin B12) is available through the module connector described in the pin-out list. To start the module using Power Button the PWRBTN# signal must be at least 50 ms (50 ms ≤ t < 4 s, typical 400 ms) at low level (Power Button Event).

Pressing the power button for at least 4 seconds will turn off power to the module (Power Button Override).

2.6.3 Power Good (PWR_OK)

The COMe-bBD6 provides an external input for a power-good signal (Pin B24). The implementation of this subsystem complies with the COM Express® Specification. PWR_OK is internally pulled up to 3.3V and must be high level to power on the module.

- This is typically driven by the ATX power supply PWR_OK signal.
- This can be driven low to hold the module from powering up as long as needed. The carrier needs to release the signal when ready.

2.6.4 Reset Button (SYS_RESET# Signal)

When the SYS_RESET# pin is detected active, it allows the processor to perform a "graceful" reset, by waiting up to 25 ms for the SMBus to go idle before forcing a reset even though activity is still occurring. Once the reset is asserted, it remains asserted for 5 to 6 ms regardless of whether the SYS_RESET# input remains asserted or not. For more information, refer to the *Intel® Xeon® D-1500 Product Family Datasheet, Vol. 1*.

Modules with Intel® Chipset and active Management Engine do not allow to hold the module in Reset out of S0 for a long time. At about 10 s holding the reset button the ME will reboot the module automatically.

2.6.5 SM-Bus Alert (SMB_ALERT#)

With an external battery manager present and SMB_ALERT# (Pin B15) connected the module always powers on even if BIOS switch "After Power Fail" is set to "Stay Off".

2.7 Environmental Specification

2.7.1 Temperature Specification

Kontron defines following temperature grades for Computer-on-Modules in general. Please see chapter 'Product Specification' for available temperature grades for the COMe-bBD6.

Table 20: Temperature Specification

Temperature Specification	Operating	Non-operating	Validated Input Voltage
Commercial grade	0°C to +60°C	-30°C to +85°C	VCC: 8.5 V – 20 V
Extended Temperature (E1)	-25°C to +75°C	-30°C to +85°C	VCC: 12 V
Industrial grade by Screening (E2S)	-40°C to +85°C	-40°C to +85°C	VCC: 12 V
Industrial grade by Design (E2)	-40°C to +85°C	-40°C to +85°C	VCC: 8.5 V – 20 V

2.7.2 Operating with Kontron Heatspreader Plate Assembly

The operating temperature defines two requirements:

- the maximum ambient temperature with ambient being the air surrounding the module,
- the maximum measurable temperature on any spot on the heatspreader's surface.

Table 21: Test Specification

Temperature Grade	Validation requirements
Commercial grade	at 60°C HSP temperature the CPU @ 100% load needs to run at nominal frequency
Extended Temperature (E1)	at 75°C HSP temperature the CPU @ 75% load is allowed to start speedstepping for thermal protection
Industrial grade by Screening (XT)	at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection
Industrial grade by Design (E2)	at 85°C HSP temperature the CPU @ 50% load is allowed to start throttling for thermal protection

2.7.3 Operating without Kontron heatspreader plate assembly

The operating temperature is the maximum measurable temperature on any spot on the module's surface.

2.7.4 Humidity

Relative Humidity at 40°C is 93%, non-condensing (according to IEC 60068-2-78).

2.8 Standards and Certifications

2.8.1 RoHS II

The COMe-bBD6 is compliant to the directive 2011/65/EU on the Restriction of the use of certain Hazardous Substances (RoHS II) in electrical and electronic equipment.

Figure 2: RoHS



2.8.2 Component Recognition UL 60950-1

The COM Express® basic form factor Computer-on-Modules are Recognized by Underwriters Laboratories Inc.

Representative samples of this component have been evaluated by UL and meet applicable UL requirements.

UL Listings:

- NWGQ2.E304278
- NWGQ8.E304278

Figure 3: Component Recognition UL



2.8.3 WEEE Directive

WEEE Directive 2002/96/EC is not applicable for Computer-on-Modules.

2.8.4 Conformal Coating

Conformal Coating is available for Kontron Computer-on-Modules and for validated SO-DIMM memory modules. Please contact your local sales or support for further details.

2.8.5 Shock & Vibration

The COM Express® basic form factor Computer-on-Modules successfully passed shock and vibration tests according to:

- IEC/EN 60068-2-6 (Non operating Vibration, sinusoidal, 10Hz-4000Hz, +/-0.15mm, 2g)
- IEC/EN 60068-2-27 (Non operating Shock Test, half-sinusoidal, 11ms, 15g)

2.8.6 EMC

Validated in Kontron reference housing for EMC the COMe-bBD6 follows the requirements for electromagnetic compatibility standards:

- EN55022
- EN55024
- 2004/108/EC
- FCC Part 15

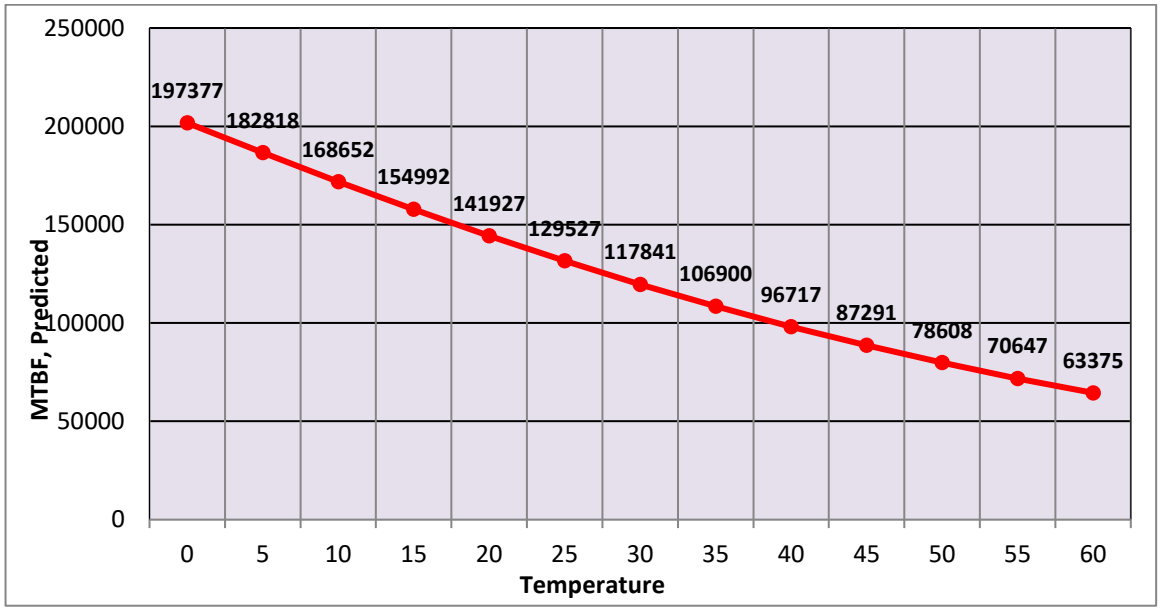
2.9 MTBF

The following MTBF (Mean Time Before Failure) values were calculated using a combination of manufacturer's test data, if the data was available, and the Telcordia (Bellcore) issue 2 calculation for the remaining parts.

The Telcordia calculation used is "Method 1 Case 3" in a ground benign, controlled environment (GB,GC). This particular method takes into account varying temperature and stress data and the system is assumed to have not been burned in.

Figure 4 shows MTBF de-rating for the E1 temperature range in an office or telecommunications environment. Other environmental stresses (such as extreme altitude, vibration, salt water exposure) lower MTBF values. System MTBF(hours) = 117841 @ 30°C

Figure 4: MTBF Temperature De-rating



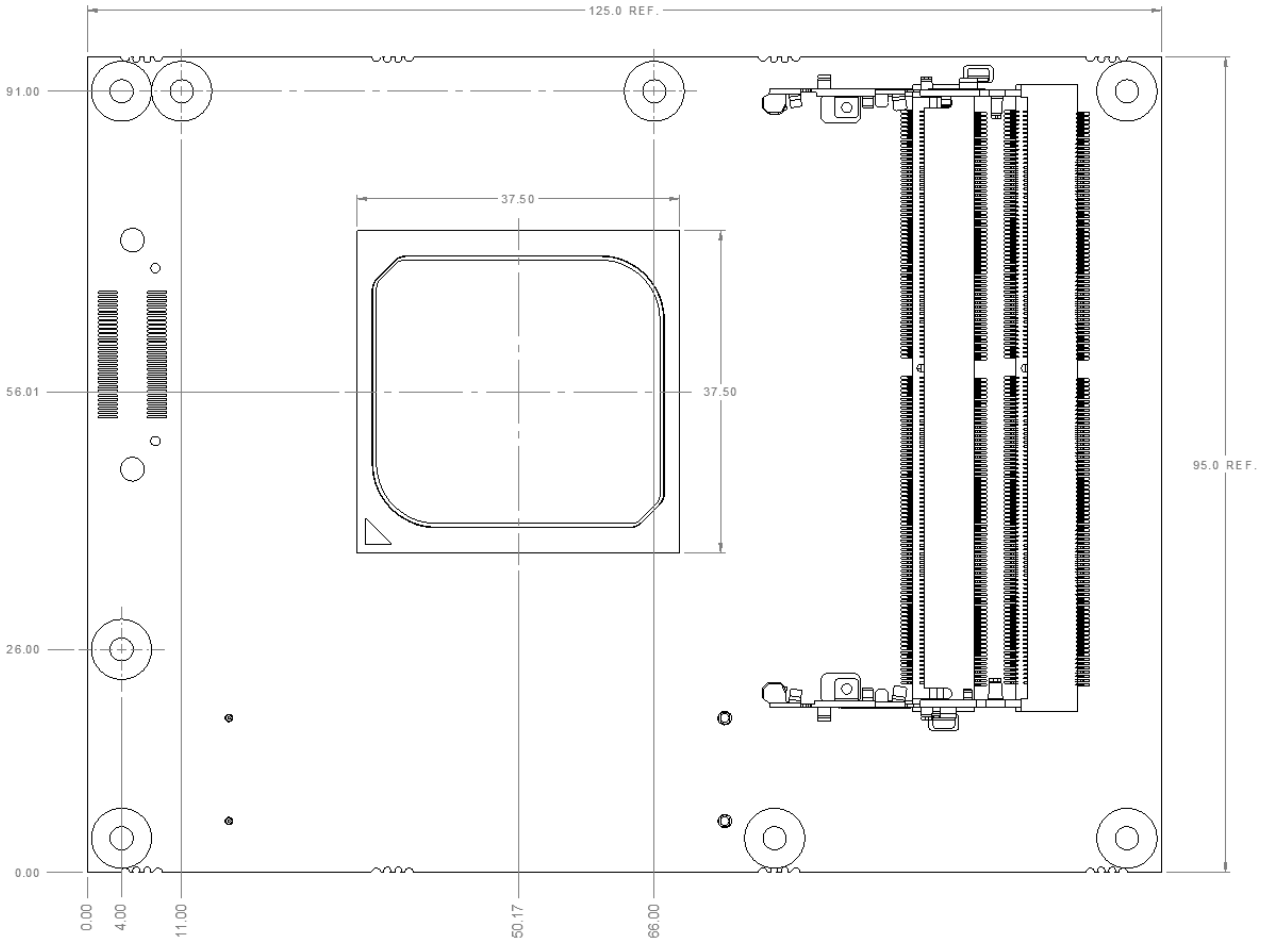
The above estimates assume no fan, but a passive heat sinking arrangement. Estimated RTC battery life (as opposed to battery failures) is not accounted for in the above figure and needs to be considered for separately. Battery life depends on both temperature and operating conditions. When the Kontron unit has external power; the only battery drain is from leakage paths.

2.10 Mechanical Specification

2.10.1 Dimension

The dimensions of the module (see Figure 5) are 95.0 mm x 125.0 mm.

Figure 5: Module Dimensions

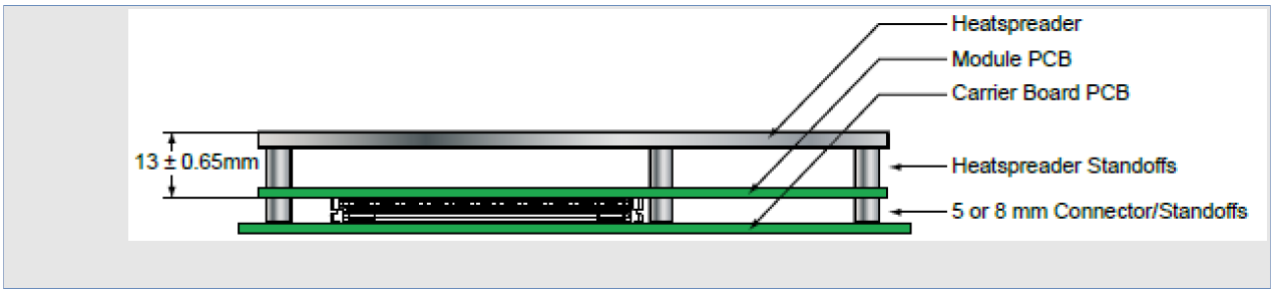


CAD drawings are available at EMD Customer Section.

2.10.2 Height

The COM Express® specification defines a module height of 13mm from module PCB bottom to heatspreader top (see Figure 6).

Figure 6: Module Height



Cooling solutions provided from Kontron for basic sized Computer-on-Modules are 27mm in height from module bottom to Heatsink top.

Universal Cooling solutions to be mounted on the HSP (36099-0000-00-x) are 14.3mm in height for an overall height of 27.3mm from module bottom to Heatsink top.



HOT Surface!
Do NOT touch! Allow to cool before servicing.

2.11 Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron for the COMe-bBD6. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a COM Express®-standard thermal interface to use with a heat sink or external cooling devices.

External cooling must be provided to maintain the heatspreader plate at proper operating temperatures. Under worst case conditions, the cooling mechanism must maintain an ambient air and heatspreader plate temperature on any spot of the heatspreader's surface according the module specifications:

- 60°C for commercial grade modules
- 75°C for extended temperature grade modules (E1)
- 85°C for industrial temperature grade modules (E2)

You can use many thermal-management solutions with the heatspreader plates, including active and passive approaches.

The optimum cooling solution varies, depending on the COM Express® application and environmental conditions. Active or passive cooling solutions provided from Kontron for the COMe-bBD6 are usually designed to cover the power and thermal dissipation for a commercial grade temperature range used in a housing with proper air flow.



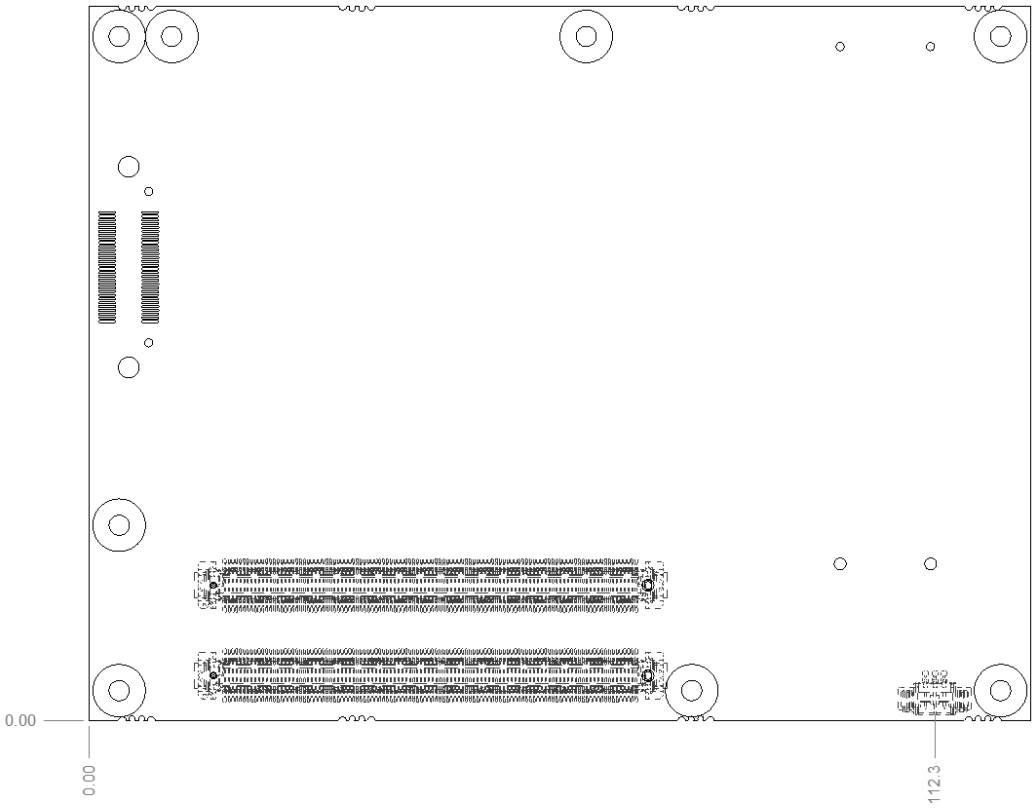
HOT Surface!
Do NOT touch! Allow to cool before servicing.

Documentation and CAD drawings of COMe-bBD6 heatspreader and cooling solutions are provided at EMD Customer Section.

2.12 Onboard Fan Connector

Figure 7 displays an overhead view of the circuit board with the location of the fan connectors (shown in red). The fan connectors are located underneath the circuit board.

Figure 7: Location of the FAN Connectors



Specification of the FAN Connector:

- Part number (Molex) J8: 53261-0371, Mates with: 51021-0300, Crimp terminals: 50079-8100

Pin assignment:

- Pin1: Tacho, Pin2: VCC, Pin3: GND

Table 22: Electrical Characteristics

Module Input Voltage	8.5 – 13 V	>13 V
FAN Output Voltage	8.5 – 13 V	13 V
Max. FAN Output Current	350 mA	150 mA

To connect a standard fan with 3-pin connector to the module please use adapter cable KAB-HSP 200mm (96079-0000-00-0) or KAB-HSP 40mm (96079-0000-00-2).

NOTICE Always check the fan specifications according the output current limitation.

2.13 Onboard Test Connector

The onboard test connector is a 60-pin ITP60c processor debug port used for debugging the CPU complex and the code that is running on it. To debug the board through the processor debug port, the compressed adapter ITP60CADAPTER is required. For more information on the ITP60CADAPTER, refer to http://designintools.intel.com/product_p/itp60cadapter.htm.

3/ Features and Interfaces

3.1 S5 Eco Mode

Kontron's new high-efficient power-off state S5 Eco enables lowest power-consumption in soft-off state – less than 1 mA compared to the regular S5 state. This means a reduction by a factor of at least 200.

In the "normal" S5 mode the board is supplied by 5 V_Stb and needs around 300 mA just to stay off. This mode allows to be switched on by power button, RTC event and WakeOnLan, even when it is not necessary. The new S5 Eco mode reduces the current enormous.

The S5 Eco Mode can be enabled in BIOS Setup, when the BIOS supports this feature.

Following prerequisites and consequences occur when S5 Eco Mode is enabled

- Wake using Power button only.
- "Power On After Power Fail"/"State after G3": only "stay off" is possible

3.2 Rapid Shutdown

3.2.1 Overview

Kontron has implemented a rapid shutdown function. It works as follows:

1. An active-high shutdown signal is asserted by the COM Express Eval Type 6 carrier board through pin C67 of the COM Express connector. The characteristics of the shutdown signal are as follows:

- Amplitude 5.0 V +/- 5%
- Source impedance < = 50 ohms
- Rise time ⇐ 1 µS
- Duration >= 20 µS

The assertion of this signal causes all power regulators to be disabled and the internal power supply rails to be discharged by crowbar circuits. The shutdown circuitry provides internal energy storage that maintains crowbar activation for at least 2mS following the de-assertion of the shutdown signal. The circuit also incorporates a weak input pulldown resistor so that the module will operate normally in systems where the rapid shutdown functionality is not used and pin C67 of the COM Express is left unconnected.

2. Simultaneously with the leading edge of shutdown, the 12V (main) input power to the module is removed and these input power pins are externally clamped to ground though a crowbar circuit located on the COM Express carrier board. This external clamping circuit must maintain a maximum resistance of approximately 1 ohm and be activated for a minimum of 2mS.
3. Simultaneously with the leading edge of shutdown, the 5V (standby) input power to the module is removed, if present. External clamping on these pins is not necessary (but recommended) because it is clamped through the module by the main 12V rail.

3.2.2 Crowbar implementation details

The crowbar circuits are designed to meet the following criteria on each rail. Upon assertion of the shutdown signal:

- Voltage decay to 37% of initial value (equivalent to one RC time constant) within 400 µS.
- Voltage is below 1.5V within 2ms.

It is expected that the carrier's crowbar on the 12V and 5V rails are design based on similar criteria.

3.3 LPC

The Low Pin Count (LPC) Interface signals are connected to the LPC Bus bridge located in the CPU or chipset. The LPC low speed interface can be used for peripheral circuits such as an external Super I/O Controller, which typically combines legacy-device support into a single IC. The implementation of this subsystem complies with the COM Express® Specification. Implementation information is provided in the COM Express® Design Guide maintained by PICMG. Please refer to the official PICMG documentation for additional information.

The LPC bus does not support DMA (Direct Memory Access) and a zero delay clock buffer is required when more than one device is used on LPC. This leads to limitations for ISA bus and SIO (standard I/O´s like Floppy or LPT interfaces) implementations.

All Kontron COM Express® Computer-on-Modules imply BIOS support for following external baseboard LPC Super I/O controller features for the Winbond/Nuvoton 3.3 V 83627DHG-P:

Table 23: Supported BIOS Features

3.3V 83627DHG-P	AMI EFI APTIO V
PS/2	YES
COM1/COM2	YES
LPT	YES
HWM	NO
Floppy	NO
GPIO	NO

Features marked as not supported do not exclude OS support (e.g. HWM can be accessed by SMB). For any other LPC Super I/O additional BIOS implementations are necessary. Please contact your local sales or support for further details.

3.4 Real Time Clock (RTC)

The RTC keeps track of the current time accurately. The RTC's low power consumption enables the RTC to continue operation and keep time using a lower secondary source of power while the primary source of power is switched off or unavailable.

The COMe-bBD7 supports typical RTC values of 3 V and less than 10 µA. When powered by the mains power supply on-module regulators generate the RTC voltage, to reduce RTC current draw. The RTC's battery voltage range is 2.8 V to 3.47 V.



It is not recommended to run a system without a RTC battery on the carrier board. Even if the RTC battery is not required to keep the actual time and date when main power is off, a missing RTC battery will cause other side effects such as longer boot times. Intel processor environments are generally designed to rely on RTC battery voltage.

3.5 Serial Peripheral Interface (SPI)

The Serial Peripheral Interface Bus or SPI bus is a synchronous serial data link standard named by Motorola. Devices communicate in master/slave mode where the master device initiates the data frame. Multiple slave devices are allowed with individual slave select (chip select) lines. Sometimes SPI is called a "four wire" serial bus, contrasting with three, two, and one wire serial buses.



The SPI interface can only be used with a SPI flash device to boot from external BIOS on the baseboard.

3.6 SPI boot

The COMe-bBD6 supports boot from an external SPI Flash. It can be configured by pin A34 (BIOS_DIS0#) and pin B88 (BIOS_DIS1#) in following configuration:

Table 24: SPI Boot Pin Configuration

Configuration	BIOS_DIS0#	BIOS_DIS1#	Function
1	open	open	Boot on module BIOS
2	GND	open	Boot on LPC firmware hub (FWH)
3	open	GND	Boot on carrier SPI
4	GND	GND	Boot on module SPI



By default, only the primary SPI Boot Device (chip select 0) is used in configuration 3 & 4. To access the secondary SPI device (chip select 1), the BIOS must be customized.

Table 25: Supported SPI boot flash types for 8-SOIC package

Size	Manufacturer	Part Number	Device ID
128Mbit	Macronix	MX25L12805D	0xC22018
128Mbit	Micron	N25Q128	0x20BA18
128Mbit	Winbond	W25Q128FV	0xEF4018

3.6.1 Using an external SPI flash

The Kflash utility is available on version 0.06. The "v" verify parameter of this command is not implemented yet, however a check on the size between the binary file and the spi flash is performed before the writing and/or saving operation. First of all, you need to boot on the EFI Shell with an USB key containing the binary we want to flash the SPI with, plugged on the system.

Depending on which SPI you would like to flash, you will need to use one jumper in particular (BIOS_DIS1) located on the carrier Topanga Canyon Type 6 (J27).

To flash the carrier or module Flash chip:

1. Connect a SPI flash with the correct size (similar to BIOS ROM file size) to the module SPI interface.
2. Open pin A34 (BIOS_DIS0#) and B88 (BIOS_DIS1#) to boot from the module BIOS.
3. Turn on the system and make sure your boot your USB is connected and boot on the EFI shell (you need to boot with a BIOS binary that supports kflash utility in order to use it so version should be ≥ SPI_COMe_bBD6_0_06.bin).
4. Connect pin B88 (BIOS_DIS1#) to ground to enable the external SPI flash.
5. From the EFI shell, (see Figure 8) enter the name of the partition of your USB Key in this example:

   FS0: then enter.

Figure 8: Entering USB Key Partition Name



6. If you want to see a help guide regarding "kflash" usage, enter:

   kflash -h

Figure 9: Using kflash help option

```
FSO:\> kflash -h
Kontron SPI flasher
kflash -p filename
kflash -s filename
kflash -v filename
kflash -ver
kflash -h|-?
  -p : program flash image file
  -s : read flash and save content to a file
  -v : verify flash image file and check flash CRC
  -ver : display BIOS version of current flash
  -h|-? : display this help
Program/Manage SPI flash on Kontron board.
To save current BIOS flash content to file named image.bin:
  Shell> kflash -s image.bin
To program file image.bin:
  Shell> kflash -p image.bin
To display current BIOS version in SPI flash:
  Shell> kflash -ver
FSO:\>
```

7. On your terminal, enter the following command:

   ***kflash** -p "binary_name.bin"*

   The following is displayed (see Figure 10):

Figure 10: Programming the Flash Image Drive

```
FSO:\> kflash -p SPI_COMe_bBD6_0_06.bin
Reading data from file 'SPI_COMe_bBD6_0_06.bin'
Done.           [   OK   ]
Flash controller: "Intel(r) C224 Series Chipset Family Server Standard SKU"
Flash chip:       "Winbond W25Q128 series"
Flash size:       0x01000000
Sector size:      0x00001000
Erasing flash...
Done.           [   OK   ]
Writing data to flash...
Done.           [   OK   ]
Flash updated. Verifying flash...
Flash controller: "Intel(r) C224 Series Chipset Family Server Standard SKU"
Flash chip:       "Winbond W25Q128 series"
Flash size:       0x01000000
Sector size:      0x00001000
Reading data from flash...
Done.           [   OK   ]
Flashed image and given image are equal.          [   OK   ]
NVRAM inconsistency detected. Reinitializing.
FSO:\>
```

8. When process is finished, power cycle the whole system.

Your system has now been updated.



For more information, visit the EMD Customer Section.

3.6.2 External SPI flash on Modules with Intel® ME

If booting from the external (baseboard mounted) SPI flash then exchanging the COM Express® module for another one of the same type will cause the Intel® Management Engine to fail during next start. This is by design of the ME because it bounds itself to the very module it has been flashed to. In the case of an external SPI flash this is the module present at flash time.

To avoid this issue please make sure to conduct a complete flash of the external SPI flash device after changing the COMexpress module for another one. If disconnecting and reconnecting the same module again this step is not necessary.

3.7 UART

The COMe-bBD6 supports two Serial RX/TX only Ports defined in COM Express® specification on Pins A98/A99 for UART0 and Pins A101/A102 for UART1. The implementation of the UART is compatible with 16C550 and is supported by default by most operating systems. Resources are available to other UARTS such as from external LPC Super I/O.

UART features:

- Hardware and software register compatible with all standard 16450 and 16550 UARTs
- Implements all standard serial interface protocols
  - 5, 6, 7 or 8 bits per character
  - Odd, Even or no parity detection and generation
- 1, 1.5 or 2 stop bit detection and generation
- Internal baud rate generator and separate receiver clock input
  - Modem control functions
  - Prioritized transmit, receive, line status and
- modem control interrupts
  - False start bit detection and recover
  - Line break detection and generation
  - Internal loop back diagnostic functionality
  - 16 byte transmit and receive FIFOs
- Implements only RX and TX signals.
  - RTS and DTR are not connected
  - CTS, DCD and DSR are tied to active
  - RI is tied to inactive

The UART clock is generated by the 33MHz LPC clock which results in an accuracy of 0.5% on all UART timings.

The First In First Out (FIFO) buffer memory within the UART between the receiver shift register and the host system interface provides the host processor additional time to handle an interrupt from the UART and prevents loss of received data at high rates.

3.8 Fast I2C

The COMe-bBD6 supports FPGA implemented LPC to I2C bridge. The I2C Interface supports clock from 127Hz to 400kHz (limited by on board devices and capacitive loading) and can be configured in Setup.

Specification for external I2C:

- Speed up to 400 kHz
- Compatible to Philips I2C bus standard
- Multi-Master capable
- Clock stretching support and wait state generation
- Interrupt or bit-polling driven byte-by-byte data-transfers
- Arbitration lost interrupt with automatic transfer cancellation
- Start/Stop signal generation/detection
- Bus busy detection

3.9 GPIO - General Purpose Input and Output

The COMe-bBD6 offers four General Purpose Input (GPI) pins and four General Purpose Output (GPO) pins. On a 3.3 V level, digital inputs and outputs are available.

Table 26: GPIO Pins

Signal	Pin	Description
GPI0	A54	General Purpose Input 0
GPI1	A63	General Purpose Input 1
GPI2	A67	General Purpose Input 2
GPI3	A85	General Purpose Input 3
GPO0	A93	General Purpose Output 0
GPO1	B54	General Purpose Output 1
GPO2	B57	General Purpose Output 2
GPO3	B63	General Purpose Output 3

3.10 Triple Staged Watchdog Timer

3.10.1 Basics

A watchdog timer (or computer operating properly (COP) timer) is a computer hardware or software timer that triggers a system reset or other corrective action if the main program, due to some fault condition, such as a hang, neglects to regularly service the watchdog (writing a "service pulse" to it, also referred to as "kicking the dog", "petting the dog", "feeding the watchdog" or "triggering the watchdog"). The intention is to bring the system back from the nonresponsive state into normal operation.

The COMe-bBD6 offers a watchdog which works with three stages that can be programmed independently and used one by one.

Table 27: Time-out events

0000b	No action	The stage is off and will be skipped.
0001b	Reset	A reset will restart the module and starts POST and operating system new.
0010b	NMI	A non-maskable interrupt (NMI) is a computer processor interrupt that cannot be ignored by standard interrupt masking techniques in the system. It is typically used to signal attention for non-recoverable hardware errors.
0011b	SMI	A system management interrupt (SMI) makes the processor entering the system management mode (SMM). As such, specific BIOS code handles the interrupt. The current BIOS handler for the watchdog SMI currently does nothing. For particular needs, contact Kontron customer support.
0100b	SCI	A system control interrupt (SCI) is a OS-visible interrupt to be handled by the OS using AML code
0101b	Delay -> No action*	Might be necessary when an operating system must be started and the time for the first trigger pulse must extended. (Only available in the first stage).
1000b	WDT Only	This setting triggers the WDT Pin on baseboard connector (COM Express® Pin B27) only.
1001b	Reset + WDT	
1010b	NMI + WDT	
1011b	SMI + WDT	
1100b	SCI + WDT	
1101b	DELAY + WDT -> No action*	

* After expiring the counter or triggering the stage action will be set to "No action". The purpose is to allow a one-time delay before starting the actual time. WDT signal (mode 1101b) asserted after stage timeout, not after stage triggering.

3.10.2 WDT Signal

Pin B27 on COM Express® Connector offers a signal that can be asserted when a watchdog timer has not been triggered within time. It can be configured to any of the three stages. Deassertion of the signal is done automatically after reset. If deassertion during runtime is necessary, please ask your Kontron technical support for further help.

3.11 Intel® Fast Flash Standby™/Rapid Start Technology™

The target of Intel® Fast Flash Standby™ (iFFS) (also known as Intel® Rapid Start Technology™ iRST) is to get a wake-up time from S4. Normally, S4 is caused by the OS, which stores its information to the hard disk and then does a

normal shutdown. S4 resume takes quite long as the system does a normal BIOS POST and OS restores its information from the hard disk.

IFFS does it in a different way. The Operating System initiates an S4 and stores its information in memory. After that, the BIOS copies this OS information from DRAM to SSD and does a sleep state similar to S4 with nearly zero power. If the system is resumed by the power button, the BIOS restores the memory content from the SSD to the DRAM and does an S4 resume which is much faster.

3.11.1 Requirements

- SATA Solid State Disk in AHCI mode
- Free disk space on the SSD with at least the DRAM size
- Operating System with disk partition tool to allocate the hibernation partition (e.g. Windows 7/8)
- BIOS supporting iFFS feature

How to setup the Intel® Rapid Start Technology once the operating system is installed:

1. Prepare a free disk space on your onboard or external SSD with at least the size of DRAM.
2. Open cmd.exe in Administrator Mode and type diskpart.exe to open the Windows disk partition tool.
3. DISKPART> list disk
4. DISKPART> select disk X (X is disk number where you want to create the store partition. Refer to results from "list disk" for exact disk number)
5. DISKPART> create partition primary
6. DISKPART> detail disk
7. DISKPART> select Volume X (X is Volume of your store partition. Refer to results from "detail disk" for exact volume number)
8. DISKPART> set id=84 override (ID 84 marks the partition as hibernate partition)
9. DISKPART> exit

   Now there should be a Hibernate Partition visible in your disk management.
10. Reboot and enable iFFS in BIOS

Usage:

1. Move system to Sleep/Standby (→S4).
2. After configured period of time in Setup the system powers on automatically and information in DRAM moves to non-volatile memory (default is 'immediately').
3. System switches off again to iFFS (Power Supply can now be disconnected).
4. When System is powered on, information moved back to DRAM (No display output during copy process).
5. System resumes same as Sleep/Standby S4.

Depending on the platform iFFS enabled may disable the hibernate function in Windows automatically.

Benefits:

- Up to 6x battery life compared to Standby
- Resume time reduced up to 75%

Measured resume times from Power-on to Win7 Log-on Screen on COMe-mCT10:

- 2.5" SATA II HDD 5400rpm: Hibernate: 22s, iFFs on onboard NANDrive: 17s
- 2.5" SATA III SSD: Hibernate: 18s, iFFS on SSD: 10s

3.12 Speedstep Technology

The Intel® processors offer the Intel® Enhanced SpeedStep™ technology that automatically switches between maximum performance mode and battery-optimized mode, depending on the needs of the application being run. It enables you to adapt high performance computing on your applications. When powered by a battery or running in idle mode, the processor drops to lower frequencies (by changing the CPU ratios) and voltage, conserving battery life while maintaining a high level of performance. The frequency is set back automatically to the high frequency, allowing you to customize performance.

In order to use the Intel® Enhanced SpeedStep™ technology the operating system must support SpeedStep™ technology.

By deactivating the SpeedStep feature in the BIOS, manual control/modification of CPU performance is possible. Setup the CPU Performance State in the BIOS Setup or use 3rd party software to control CPU Performance States.

3.13 C-States

New generation platforms include power saving features like SuperLFM, EIST (P-States) or C-States in O/S idle mode.

Activated C-States are able to dramatically decrease power consumption in idle mode by reducing the Core Voltage or switching of parts of the CPU Core, the Core Clocks or the CPU Cache.

Table 28: Defined C-States

C-State	Description	Function
C0	Operating	CPU fully turned on
C1	Halt State	Stops CPU main internal clocks through software
C1E	Enhanced Halt	Similar to C1, additionally reduces CPU voltage
C2	Stop Grant	Stops CPU internal and external clocks through hardware
C2E	Extended Stop Grant	Similar to C2, additionally reduces CPU voltage
C3	Deep Sleep	Stops all CPU internal and external clocks
C3E	Extended Stop Grant	Similar to C3, additionally reduces CPU voltage
C4	Deeper Sleep	Reduces CPU voltage
C4E	Enhanced Deeper Sleep	Reduces CPU voltage even more and turns off the memory cache
C6	Deep Power Down	Reduces the CPU internal voltage to any value, including 0V
C7	Deep Power Down	Similar to C6, additionally LLC (LastLevelCache) is switched off

C-States are usually enabled by default for low power consumption, but active C-States my influence performance sensitive applications or real-time systems.

- Active C6-State may influence data transfer on external Serial Ports
- Active C7-State may cause lower CPU and Graphics performance

It is recommended to disable C-States / Enhanced C-States in BIOS Setup if any problems occur.

3.14 Hyper Threading

Hyper Threading (officially termed Hyper Threading Technology or HTT) is an Intel®-proprietary technology used to improve parallelization of computations performed on PC´s. Hyper-Threading works by duplicating certain sections of the processor—those that store the architectural state but not duplicating the main execution resources. This allows a Hyper- Threading equipped processor to pretend to be two "logical" processors to the host operating system, allowing the operating system to schedule two threads or processes simultaneously. Hyper Threading Technology support always relies on the Operating System.

3.15 ACPI Suspend Modes and Resume Events

The COMe-bBD6 supports the S-states S0, S4, S5. and S5ECO (see 3.1 S5 Eco Mode)

The following events resume the system from S4:

- Power Button
- WakeOnLan (2)

The following events resume the system from S5:

- Power Button

- WakeOnLan (2)

The following events resume the system from S5Eco:

- Power Button



1. OS must support wake up by USB devices and baseboard must power the USB Port with StBy-Voltage.
2. Depending on the Used Ethernet MAC/Phy WakeOnLan must be enabled in BIOS setup and driver options.

4/System Resources

4.1 Interrupt Request (IRQ) Lines

Table 29: List of Interrupt Requests

IRQ#	Used For	Available	Comment
0	Timer	No	-
1	Keyboard	No	-
2	Cascade	No	-
3	COM2	No	Onboard UART
4	COM1	No	Onboard UART
5	LPT	No	External SIO Winbond 83627DHG
6	-	Yes	-
7	-	Yes	-
8	RTC	No	-
9	ACPI	No	-
10	COM3 & COM4	No	External SIO Winbond 83627DHG
11	-	Yes	-
12	PS/2 Mouse	No	External SIO Winbond 83627DHG
13	FPU	No	-
14	-	Yes	-
15	-	Yes	-

4.2 Memory Area

The first 640 kB of DRAM are used as main memory. Using DOS, you can address 1 MB of memory directly. Memory area above 1 MB (high memory, extended memory) is accessed under DOS by special drivers such as HIMEM.SYS and EMM386.EXE, which are part of the operating system. Please refer to the operating system documentation or special textbooks for information about HIMEM.SYS and EMM386.EXE. Other operating systems (Linux or Windows versions) allow you to address the full memory area directly.

Table 30: Designated Memory Locations

Upper Memory	Used for	Available	Comment
C0000h-CFFFFh	Video ROM	No	-
E0000h-FFFFFh	System ROM	No	-
90000000h-FBFFBFFFh	PCIe Config Space	No	-
FBFFC000h-FBFFCFFFh	dmar0	No	-
FEC00000h-FEC003FFh	IOAPIC 0	No	-
FEC01000h-FEC013FFh	IOAPIC 1	No	-
FED00000h-FED003FFh	HPET 0	No	-
FF000000h-FFFFFFFFh	BIOS Flash	No	-

4.3 I/O Address Map

The I/O-port addresses of the bBD6 are functionally identical to a standard PC/AT. All addresses not mentioned in this table should be available. We recommend that you do not use I/O addresses below 0100h with additional hardware for compatibility reasons, even if available.

Table 31: Designated I/O Port Addresses

I/O Address	Used for	Available	Comment
0000-001F	DMA Controller	No	Fixed
0020-002D	Interrupt Controller	No	Fixed
0002E-002F	Onboard UART	No	Fixed
0030-003D	Interrupt Controller	No	Fixed
0040-0042	Timer/Counter	No	Fixed
004E-004F	Winbond 83627DHG	No	When SIO present on carrier
0050-0052	Timer/Counter	No	Fixed
0060-0064	Keyboard Controller	No	Fixed
0071-0077	RTC Controller	No	Fixed
0080	BIOS Post Code	No	Fixed
0081-0091	DMA Controller	No	Fixed
0092	Reset Generator	No	Fixed
0093-009F	DMA Controller	No	Fixed
00A0-00BD	Interrupt Controller	No	Fixed
00C0-00D1	DMA Controller	No	Fixed
00DE-00DF	DMA Controller	No	Fixed
00F0	FERR# / Interrupt Controller	No	Fixed
0240-0247	Winbond 83627DHG Serial Port 1	No	When SIO present on carrier
0248-024F	Winbond 83627DHG Serial Port 2	No	When SIO present on carrier
04D0-04D1	Interrupt Controller	No	Fixed
0A80-0AFF	FPGA	No	Fixed
0CF9	Reset Generator	No	Fixed

Other I/O addresses are dynamically allocated for PCI devices and not listed here. Refer to your OS documentation on how to determine I/O addresses usage.

4.4 Peripheral Component Interconnect (PCI) Devices

All devices follow the Peripheral Component Interconnect 2.3 (PCI 2.3) respectively the PCI Express Base 1.0a specification. The BIOS and OS control memory and I/O resources. Please see the PCI 2.3 specification for details.

Table 32: PCI Device list

PCI Device	B:D.F*	Interface	Comment
Host bridge: Intel Corporation Broadwell DMI2 (rev 02)	00:00.0	Internal	Chipset
PCI bridge: Intel Corporation Broadwell PCI Express Root Port 1 (rev 02)	00:01.0	Internal	Chipset
PCI bridge: Intel Corporation Broadwell PCI Express Root Port 1 (rev 02)	00:01.1	Internal	Chipset
PCI bridge: Intel Corporation Broadwell PCI Express Root Port 2 (rev 02)	00:02.0	Internal	Chipset
PCI bridge: Intel Corporation Broadwell PCI Express Root Port 2 (rev 02)	00:02.2	Internal	Chipset
PCI bridge: Intel Corporation Broadwell PCI Express Root Port 3 (rev 02)	00:03.0	Internal	Chipset
System peripheral: Intel Corporation Broadwell Adress Map/VTd_Misc/System Management (rev 02)	00:05.0	Internal	Chipset
System peripheral: Intel Corporation Broadwell IIO Hot Plug (rev 02)	00:05.1	Internal	Chipset
System peripheral: Intel Corporation Broadwell IIO RAS/Control Status/Global Errors (rev 02)	00:05.2	Internal	Chipset
PIC: Intel Corporation Broadwell I/O APIC (rev 02)	00:05.4	Internal	Chipset
Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller	00:16.0	Internal	Chipset
Communication controller: Intel Corporation 8 Series/C220 Series Chipset Family MEI Controller	00:16.1	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #1	00:1c.0	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #2	00:1c.1	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #3	00:1c.2	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #4	00:1c.3	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #5	00:1c.4	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #6	00:1c.5	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #7	00:1c.6	Internal	Chipset
PCI bridge: Intel Corporation 8 Series/C220 Series Chipset Family PCI Express Root Port #8	00:1c.7	Internal	Chipset
USB controller: Intel Corporation 8 Series/C220 Series Chipset Family USB EHCI #1 (rev 05)	00:1d.0	Internal	Chipset
ISA bridge: Intel Corporation C224 Series Chipset Family Server Standard SKU LPC Controller	00:1f.0	Internal	Chipset

SATA controller: Intel Corporation 8 Series/C220 Series Chipset Family 6-port SATA Controller 1	00:1f.2	Internal	Chipset
SMBus: Intel Corporation 8 Series/C220 Series Chipset Family SMBus Controller (rev 05)	00:1f.3	Internal	Chipset
Ethernet controller: Intel Corporation I210 Gigabit Network Connection (rev 03)	01:00.0	Internal	On board LAN
Ethernet controller: Intel Corporation I210 Gigabit Network Connection (rev 03)	02:00.0	Internal	On board LAN
Xeon Processor D Family QuickData Technology Register DMA Channel 0	03:00.0	Internal	Chipset
Xeon Processor D Family QuickData Technology Register DMA Channel 1	03:00.1	Internal	Chipset
Xeon Processor D Family QuickData Technology Register DMA Channel 2	03:00.2	Internal	Chipset
Xeon Processor D Family QuickData Technology Register DMA Channel 3	03:00.3	Internal	Chipset
Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane	04:00.0	Internal	Chipset
Ethernet controller: Intel Corporation Ethernet Connection X552 10 GbE Backplane	04:00.1	Internal	Chipset

* Bus:Device.Function

4.5 I2C Bus

Table 33: I2C Bus Port Addresses

I2C Address	Used For	Available	Comment
58h	S5 Eco	No	S5 Eco Resistor
A0h	JIDA-EEPROM	No	Module EEPROM
AEh	FRU-EEPROM	No	Recommended for Baseboard EEPROM

4.6 System Management (SM) Bus

The 8-bit SMBus addresses uses the LSB (Bit 0) for the direction. Bit0 = 0 defines the write address, Bit0 = 1 defines the read address for the device. The 8-bit addresses listed below shows the write address for all devices. 7-bit SMBus addresses shows the device address without Bit0.

Table 34: Designated I/O Port Addresses

8-bit Address	7-bit Address	Device	Comment	SMBus
58h	0x2C	HWM NCT7802Y (non ECC Design)	Do not use under any circumstances	SMB



A JIDA Bus No. like in former Modules cannot be provided because the EAPI driver implementation enumerates the I2C busses dynamically. Please follow the initialization process as provided in the EAPI specification.

5/ Pin-out List

The pins of the connectors are listed in the following tables:

- Table 36: Connector X1A Row A Pin-out List
- Table 37: Connector X1A Row B Pin-out List
- Table 38: Connector X1B Row C Pin-out List
- Table 39: Connector X1B Row D Pin-out List

These tables list the pins and signals according to the PICMG specification COM.0 Rev 2.1 Type 6 standard. The descriptions of the pins found in these tables are brief. For a more detailed description of each pin, refer to the COM.0 Rev 2.1 Type 6 standard. The information provided under types, module terminations and comments are complimentary information and for a list of terms used within these columns, refer to

Table 35 and Table 133.

Row C and D have pins safely reused per pin COM.0 Rev 2.1 Type 6 standard characteristics to provide additional Ethernet capabilities, see Chapter 2.2.6. For more information, contact Kontron.

Table 35: Electrical characteristic

Type	Description
NC	Not connected (on this product)
I/O-3,3	Bi-directional 3,3 V IO-Signal
I/O-5T	Bi-dir. 3,3V I/O (5V Tolerance)
I/O-5	Bi-directional 5V I/O-Signal
I-3,3	3,3V Input
I/OD	Bi-directional Input/Output Open Drain
I-5T	3,3V Input (5V Tolerance)
OA	Output Analog
OD	Output Open Drain
O-1,8	1,8V Output
O-3,3	3,3V Output
O-5	5V Output
DP-I/O	Differential Pair Input/Output
DP-I	Differential Pair Input
DP-O	Differential Pair Output
PU	Pull-Up Resistor
PD	Pull-Down Resistor
PWR	Power Connection

NOTICE

To protect external power lines of peripheral devices, make sure that: the wires have the right diameter to withstand the maximum available current the enclosure of the peripheral device fulfills the fire-protection requirements of IEC/EN60950.

5.1 Connector X1A Row A

Table 36 lists the pin-outs for Connector X1A Row A.

Table 36: Connector X1A Row A Pin-out List

Pin	COME Signal	Description	Type	Termination	Comment
A1	GND_1	Power Ground	PWR	-	
A2	GBE0_MDI3-	Gigabit Ethernet Media Dependent Interface	DP-I/O	-	
A3	GBE0_MDI3+				
A4	GBE0_LINK100#	100BT Ethernet controller speed indicator	OD-3.3	-	
A5	GBE0_LINK1000#	1G BT Ethernet controller speed indicator	OD-3.3	-	
A6	GBE0_MDI2-	Gigabit Ethernet Media Dependent Interface	DP-I/O	-	
A7	GBE0_MDI2+				
A8	GBE0_LINK#	Ethernet Controller Link Indicator	OD-3.3	-	
A9	GBE0_MDI1-	Gigabit Ethernet Media Dependent Interface	DP-I/O	-	
A10	GBE0_MDI1+				
A11	GND_2	Power Ground	PWR	-	
A12	GBE0_MDI0-	Gigabit Ethernet Media Dependent Interface	DP-I/O	-	
A13	GBE0_MDI0+				
A14	GBE0_CTREF	Reference voltage for Carrier Board Ethernet magnetics center tap. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0V and as high as 3.3V.	PWR	-	NC
A15	SUS_S3#	Indicates system is in Suspend to RAM state. An inverted copy of SUS_S3# on the Carrier Board may be used to enable the non-standby power on a typical ATX supply.	O-3.3	PD 244	
A16	SATA0_TX+	Serial ATA or SAS transmit data	DP-O	-	
A17	SATA0_TX-				
A18	SUS_S4#	Indicates system is in Suspend to Disk state.	O-3.3	PD 10k	
A19	SATA0_RX+	Serial ATA or SAS receive data	DP-I	-	
A20	SATA0_RX-				
A21	GND_3	Power Ground	PWR	-	
A22	SATA2_TX+	Serial ATA or SAS transmit data	DP-O	-	
A23	SATA2_TX-				

Pin	COME Signal	Description	Type	Termina-tion	Comment
A24	SUS_S5#	Indicates system is in Soft Off state.	O-3.3	-	Connected to SUS_S4#, No S5# on BW-DE SOC
A25	SATA2_RX+	Serial ATA or SAS receive data	DP-I	-	
A26	SATA2_RX-				
A27	BATLOW#	Indicates that external battery is low. This port provides a battery-low signal to the Module.	I-3.3	PU 5.1k 3.3V (S5)	
A28	SATA_ACT#	PATA/SATA or SAS activity indicator	OD-3.3	PU 10k 3.3V (S0)	
A29	AC/HDA_SYNC	Sample-synchronization signal to the CODEC(s).	O-3.3	-	GND
A30	AC/HDA_RST#	Reset output to CODEC.	O-3.3	-	GND
A31	GND_4	Power Ground	PWR	-	
A32	AC/HDA_BITCLK	Serial data clock generated by the external CODEC(s).	I/O-3.3	-	NC
A33	AC/HDA_SDOUT	Serial TDM data output to the CODEC.	O-3.3	-	GND
A34	BIOS_DIS0#	Selection straps to determine the BIOS boot device. The Carrier should only float these or pull them low, please refer to COME.0 specification Table 4.13 for strapping options of BIOS disable signals.	I-3.3	PU 6.6k to 16.5k 3.3V (S5)	Refer to chapter SPI boot
A35	THRMTRIP#	Indicates the CPU has entered thermal shutdown.	O-3.3	-	
A36	USB6-	USB differential pairs (host)	DP-I/O	-	NC
A37	USB6+				
A38	USB_6_7_OC#	USB over-current sense.	I-3.3	-	NC
A39	USB4-	USB differential pairs (host)	DP-I/O	-	NC
A40	USB4+				
A41	GND_5	Power Ground	PWR	-	
A42	USB2-	USB differential pairs (host)	DP-I/O	-	
A43	USB2+				
A44	USB_2_3_OC#	USB over-current sense. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.	I-3.3	PU 5.1k 3.3V (S5)	
A45	USB0-	USB differential pairs (host)	DP-I/O	-	
A46	USB0+				
A47	VCC_RTC	V_BAT	PWR	-	
A48	EXCD0_PERST#	PCI ExpressCard expansion, reset	O-3.3	-	

Pin	COME Signal	Description	Type	Termina-tion	Comment
A49	EXCD0_CPPE#	PCI ExpressCard expansion, capable card request	I-3.3	PU 10k 3.3V (S0)	
A50	LPC_SERIRQ	LPC Serial Interrupt	I/O-3.3	PU 10k 3.3V (S0)	
A51	GND_6	Power Ground	PWR	-	
A52	PCIE_TX5+	PCI Express Transmit	DP-O	-	
A53	PCIE_TX5-				
A54	GPI0	General purpose input pins.	I-3.3	PD 6.6k to 16.5k 3.3V (S5)	
A55	PCIE_TX4+	PCI Express Transmit	DP-O	-	
A56	PCIE_TX4-				
A57	GND_7	Power Ground	PWR	-	
A58	PCIE_TX3+	PCI Express Transmit	DP-O	-	
A59	PCIE_TX3-				
A60	GND_8	Power Ground	PWR	-	
A61	PCIE_TX2+	PCI Express Transmit	DP-O	-	
A62	PCIE_TX2-				
A63	GPI1	General purpose input pins.	I-3.3	PD 6.6k to 16.5k 3.3V (S5)	
A64	PCIE_TX1+	PCI Express Transmit	DP-O	-	
A65	PCIE_TX1-				
A66	GND_9	Power Ground	PWR	-	
A67	GPI2	General purpose input pins.	I-3.3	PD 6.6k to 16.5k 3.3V (S5)	
A68	PCIE_TX0+	PCI Express Transmit	DP-O	-	
A69	PCIE_TX0-				
A70	GND_10	Power Ground	PWR	-	
A71	LVDS_A0+/eDP_TX2+	LVDS or DP transmit	DP-O	-	NC
A72	LVDS_A0-/eDP_TX2-				
A73	LVDS_A1+/eDP_TX1+	LVDS or DP transmit	DP-O	-	NC
A74	LVDS_A1-/eDP_TX1-				
A75	LVDS_A2+/eDP_TX0+	LVDS or DP transmit	DP-O	-	NC

Pin	COME Signal	Description	Type	Termina-tion	Comment
A76	LVDS_A2-/eDP_TX0-				
A77	LVDS/eDP_VDD_EN	LVDS or DP panel power enable	O-3.3	-	GND
A78	LVDS_A3+	LVDS transmit	DP-O	-	NC
A79	LVDS_A3-				
A80	GND_11	Power Ground	PWR	-	
A81	LVDS_A_CK+/eDP_TX3+	LVDS clock or DP transmit	DP-O	-	NC
A82	LVDS_A_CK-/eDP_TX3-				
A83	LVDS_I2C_CK/eDP_AUX+	I2C Clock for LVDS display use or eDP AUX differential pair +	I/O-3.3	PU 2k21 3.3V (S0)	Not used
A84	LVDS_I2C_DAT/eDP_AUX-	I2C Data line for LVDS display use or eDP AUX differential pair -	I/O-3.3	PU 2k21 3.3V (S0)	Not used
A85	GPI3	General Purpose Input	I-3.3	PD 6.6k to 16.5k 3.3V (S5)	
A86	RSVD1	NC	NC	-	
A87	eDP_HPD	Detection of Hot Plug / Unplug and notification of the link layer	I-3.3	-	NC
A88	PCIE_CLK_REF+	Reference clock output for all PCI Express and PCI Express Graphics lanes.	DP-O	-	
A89	PCIE_CLK_REF-				
A90	GND_12	Power Ground	PWR	-	
A91	SPI_POWER	Power supply for Carrier Board SPI – sourced from Module – nominally 3.3V. The Module shall provide a minimum of 100mA on SPI_POWER. Carriers shall use less than 100mA of SPI_POWER. SPI_POWER shall only be used to power SPI devices on the Carrier Board.	O-3.3	-	
A92	SPI_MISO	Data in to Module from Carrier SPI	I-3.3	-	
A93	GPO0	General Purpose Output	O-3.3	PD 6.6k to 16.5k 3.3V (S5)	
A94	SPI_CLK	Clock from Module to Carrier SPI	O-3.3	-	
A95	SPI_MOSI	Data out from Module to Carrier SPI	O-3.3	-	
A96	TPM_PP	TPM Physical Presence	I-3.3	PD 10k	
A97	TYPE10#/OLD_12V	Dual use pin. Indicates to the Carrier Board that a Type 10 Module is installed. Indicates to the Carrier that a Rev 1.0/2.0 Module is installed: TYPE10# NC Pin-out R2.0	Strap	-	NC for type 6 module

Pin	COME Signal	Description	Type	Termina-tion	Comment
A98	SER0_TX/OLD_12V	serial port 0 TXD	O-3.3	-	
A99	SER0_RX/OLD_12V	serial port 0 RXD	I-3.3	PU 3.3k 2.2V (S0)	
A100	GND_13	Power Ground	PWR	-	
A101	SER1_TX/OLD_12V	serial port 1 TXD	O-3.3	-	
A102	SER1_RX/OLD_12V	serial port 1 RXD	I-3.3	PU 3.3k 2.2V (S0)	
A103	LID#/OLD_12V	LID switch input	I-3.3	PU 5.1K 3.3V (S5)	
A104	VCC_12V_1	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A105	VCC_12V_2	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A106	VCC_12V_3	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A107	VCC_12V_4	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A108	VCC_12V_5	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A109	VCC_12V_6	main input voltage (8.5-20V)	PWR 8.5-20V	-	
A110	GND_14	Power Ground	PWR	-	

Active low
+ and - Differential pair differentiator

5.2 Connector X1A Row B

Table 37 lists the pin-outs for Connector X1A Row B.

Table 37: Connector X1A Row B Pin-out List

Pin	COME Signal	Description	Type	Termination	Comment
B1	GND_15	Power Ground	PWR	-	
B2	GBE0_ACT#	Gigabit Ethernet Controller activity indicator	OD	-	
B3	LPC_FRAME#	LPC frame indicates the start of an LPC cycle	O-3.3	-	
B4	LPC_AD0	LPC multiplexed address, command and data bus	I/O-3.3	-	
B5	LPC_AD1				
B6	LPC_AD2				
B7	LPC_AD3				
B8	LPC_DRQ0#	LPC serial DMA request	I-3.3	PU 15k to 40k 3.3V (S0)	
B9	LPC_DRQ1#			PU 15k to 40k 3.3V (S0)	
B10	LPC_CLK	LPC 33MHz clock output	O-3.3	-	
B11	GND_16	Power Ground	PWR	-	
B12	PWRBTN#	A falling edge creates a power button event. Power button events can be used to bring a system out of S5 soft off and other suspend states, as well as powering the system down.	I-3.3	PU 20k 3.3V (S5eco) PU 6.6k to 16.5k 3.3V (S5)	
B13	SMB_CK	SMB bidirectional clock line.	I/OD-3.3	PU 2.2k 3.3V (S5)	
B14	SMB_DAT	SMB bidirectional data line.	I/OD-3.3	PU 2.2k 3.3V (S5)	
B15	SMB_ALERT#	SMB Alert can be used to generate an SMI# or to wake the system.	I-3.3	PU 2.2k 3.3V (S5)	
B16	SATA1_TX+	Serial ATA or SAS transmit data	DP-O	-	
B17	SATA1_TX-				
B18	SUS_STAT#	Indicates imminent suspend operation; used to notify LPC devices	O-3.3	-	
B19	SATA1_RX+	Serial ATA or SAS receive data	DP-I	-	
B20	SATA1_RX-				
B21	GND_17	Power Ground	PWR	-	
B22	SATA3_TX+	Serial ATA or SAS transmit data	DP-O	-	
B23	SATA3_TX-				

Pin	COME Signal	Description	Type	Termina-tion	Comment
B24	PWR_OK	Power OK from main power supply. A high value indicates that the power is good. This signal can be used to hold off Module startup to allow Carrier based FPGAs or other configurable devices time to be programmed.	I-3.3	PU 6.6k to 16.5k 3.3V (S5)	
B25	SATA3_RX+	Serial ATA or SAS receive data.	DP-I	-	
B26	SATA3_RX-				
B27	WDT	A watchdog time-out event has occurred.	O-3.3	-	
B28	AC/HDA_SDIN2	Serial TDM data inputs from up to 3 CODECs.	I/O-3.3	-	NC
B29	AC/HDA_SDIN1				
B30	AC/HDA_SDIN0				
B31	GND_18	Power Ground	PWR	-	
B32	SPKR	Output for audio enunciator - the "speaker" in PC-AT systems. This port provides the PC beep signal and is mostly intended for debugging purposes.	O-3.3	-	
B33	I2C_CK	General purpose I2C port clock output.	I/O-3.3	PU 2k21 3.3V (S5)	
B34	I2C_DAT	General purpose I2C port data I/O line.	I/O-3.3	PU 2k21 3.3V (S5)	
B35	THRM#	Input from off-Module temp sensor indicating an over-temp situation.	I-3.3	PU 6.6k to 16.5k 3.3V (S5)	
B36	USB7-	USB differential pairs (host and/or USB Client)	DP-I/O	-	NC
B37	USB7+				
B38	USB_4_5_OC#	USB over-current sense.	I-3.3	-	NC
B39	USB5-	USB differential pairs (host)	DP-I/O	-	NC
B40	USB5+				
B41	GND_19	Power Ground	PWR	-	
B42	USB3-	USB differential pairs (host)	DP-I/O	-	
B43	USB3+				
B44	USB_0_1_OC#	USB over-current sense. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.	I-3.3	PU 5.1k 3.3V (S5)	
B45	USB1-	USB differential pairs (host)	DP-I/O	-	
B46	USB1+				
B47	EXCD1_PERST#	PCI ExpressCard expansion, reset	O-3.3	-	
B48	EXCD1_CPPE#	PCI ExpressCard expansion, capable card request	I-3.3	PU 10k 3.3V (S0)	

Pin	COME Signal	Description	Type	Termina-tion	Comment
B49	SYS_RESET#	Reset button input.	I-3.3	PU 6.6k to 16.5k 3.3V (S5)	
B50	CB_RESET#	Reset output from Module to Carrier Board.	O-3.3	PU 10k 3.3V (S5)	
B51	GND_20	Power Ground	PWR	-	
B52	PCIE_RX5+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B53	PCIE_RX5-				
B54	GPO1	General Purpose Output	O-3.3	PD 6.6k to 16.5k 3.3V (S5)	
B55	PCIE_RX4+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B56	PCIE_RX4-				
B57	GPO2	General Purpose Output	O-3.3	PD 6.6k to 16.5k 3.3V (S5)	
B58	PCIE_RX3+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B59	PCIE_RX3-				
B60	GND_21	Power Ground	PWR	-	
B61	PCIE_RX2+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B62	PCIE_RX2-				
B63	GPO3	General Purpose Output	O-3.3	PD 6.6k to 16.5k 3.3V (S5)	
B64	PCIE_RX1+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B65	PCIE_RX1-				
B66	WAKE0#	PCI Express wake up signal.	I-3.3	PU 1k 3.3V (S5)	
B67	WAKE1#	General purpose wake up signal. May be used to implement wake-up on PS2 keyboard or mouse activity.	I-3.3	PU 5.1k 3.3V (S5)	
B68	PCIE_RX0+	PCI Express receive lane. AC coupled off module.	DP-I	-	
B69	PCIE_RX0-				
B70	GND_22	Power Ground	PWR	-	
B71	LVDS_B0+	LVDS Channel	DP-O	-	NC
B72	LVDS_B0-				
B73	LVDS_B1+	LVDS Channel	DP-O	-	NC
B74	LVDS_B1-				
B75	LVDS_B2+	LVDS Channel	DP-O	-	NC
B76	LVDS_B2-				

Pin	COME Signal	Description	Type	Termina-tion	Comment
B77	LVDS_B3+	LVDS Channel	DP-O	-	NC
B78	LVDS_B3-				
B79	LVDS/eDP_BKLT_EN	LVDS or eDP panel backlight enable	DP-O	-	NC
B80	GND_23	Power Ground	PWR	-	GND
B81	LVDS_B_CK+	LVDS Channel	DP-O	-	NC
B82	LVDS_B_CK-				
B83	LVDS/eDP_BKLT_CTRL	LVDS or eDP panel backlight brightness control.	I/O-3.3	-	GND
B84	VCC_5V_SBY_1	5V Standby	PWR	-	
B85	VCC_5V_SBY_2				
B86	VCC_5V_SBY_3				
B87	VCC_5V_SBY_4				
B88	BIOS_DIS1#	Selection straps to determine the BIOS boot device. The Carrier should only float these or pull them low, please refer to COME.0 specification Table 4.13 for strapping options of BIOS disable signals.	I-3.3	PU 6.6k to 16.5k	Refer to chapter SPI boot
B89	VGA_RED	Red for monitor. Analog DAC output, designed to drive a 37.5Ω equivalent load.	Analog	-	NC
B90	GND_24	Power Ground	PWR	-	
B91	VGA_GRN	Green for monitor. Analog DAC output, designed to drive a 37.5Ω equivalent load.	Analog	-	NC
B92	VGA_BLU	Blue for monitor. Analog DAC output, designed to drive a 37.5Ω equivalent load.	Analog	-	NC
B93	VGA_HSYNC	Horizontal sync output to VGA monitor	O-3.3	-	NC
B94	VGA_VSYNC	Vertical sync output to VGA monitor	O-3.3	-	NC
B95	VGA_I2C_CK	DDC clock line (I2C port dedicated to identify VGA monitor capabilities).	OD-3.3	PU 2.21k 3.3V (S0)	Not used
B96	VGA_I2C_DAT	DDC data line.	I-3.3	PU 2.21k 3.3V (S0)	Not used
B97	SPI_CS#	Chip select for Carrier Board SPI.	NC	-	NC
B98	RSVD3	NC	NC	-	
B99	RSVD4	NC	NC	-	
B100	GND_25	Power Ground	PWR	-	
B101	FAN_PWMOUT/OLD_12V	Fan speed control by PWM Output.	OD	-	
B102	FAN_TACHIN/OLD_12V	Fan tachometer input for a fan with a two pulse output.	I-3.3	PU 47K 3.3V (S0)	

Pin	COME Signal	Description	Type	Termina-tion	Comment
B103	SLEEP#/OLD_12V	Sleep button signal used by the ACPI operating system to bring the system to sleep state or to wake it up again.	I-3.3	PU 5.1K 3.3V (S5)	
B104	VCC_12V_7	Main input voltage (8.5-20V)	PWR 8.5-20V	-	
B105	VCC_12V_8				
B106	VCC_12V_9				
B107	VCC_12V_10				
B108	VCC_12V_11				
B109	VCC_12V_12				
B110	GND_26	Power Ground	PWR	-	

Active low
+ and - Differential pair differentiator

5.3 Connector X1B Row C

Table 38 lists the pin-outs for Connector X1B Row C.

Table 38: Connector X1B Row C Pin-out List

Pin	COME Signal	Description	Type	Termination	Comment
C1	GND_27	Power Ground	PWR	-	
C2	GND_28				
C3	USB_SSRX0-	Additional receive signal for the SuperSpeed USB data path. AC coupled off module.	DP-I	-	
C4	USB_SSRX0+				
C5	GND_29	Power Ground	PWR	-	
C6	USB_SSRX1-	Additional receive signal for the SuperSpeed USB data path. AC coupled off module.	DP-I	-	
C7	USB_SSRX1+				
C8	GND_30	Power Ground	PWR	-	
C9	USB_SSRX2-	Additional receive signal for the SuperSpeed USB data path. AC coupled off module.	DP-I	-	
C10	USB_SSRX2+				
C11	GND_31	Power Ground	PWR	-	
C12	USB_SSRX3-	Additional receive signal for the SuperSpeed USB data path. AC coupled off module.	DP-I	-	
C13	USB_SSRX3+				
C14	GND_32	Power Ground	PWR	-	
C15	DDI1_PAIR6+	GBE1_CTREF / Reference voltage for Carrier Board Ethernet magnetics center tap. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0V and as high as 3.3V.	PWR	-	**
C16	DDI1_PAIR6-	GBE1_ACT# / Gigabit ethernet controller activity indicator	OD-3.3	-	**
C17	RSVD1	NC	NC	-	
C18	RSVD2	NC	NC	-	
C19	PCIE_RX6+	PCI Express receive lane. AC coupled off module.	DP-I	-	
C20	PCIE_RX6-				
C21	GND_33	Power Ground	PWR	-	
C22	PCIE_RX7+	PCI Express receive lane. AC coupled off module.	DP-I	-	
C23	PCIE_RX7-				
C24	DDI1_HPD	DDI Hotplug Detect	I-3.3	-	NC (3)
C25	DDI1_PAIR4+	GBE1_MDI1- / Gigabit Ethernet Media Dependent Interface GBE1_MDI1+	DP-I/O	-	**
C26	DDI1_PAIR4-				
C27	RSVD3	NC	NC	-	
C28	RSVD4	NC	NC	-	

Pin	COME Signal	Description	Type	Termination	Comment
C29	DDI1_PAIR5+	GBE1_MDI0- / Gigabit Eth. Media Dependent Interface GBE1_MDI0+	DP-I/O	-	**
C30	DDI1_PAIR5-				
C31	GND_34	Power Ground	PWR	-	
C32	DDI2_CTRLCLK_AUX+	GBE1_LINK# / Ethernet Controller Link Indicator	OD-3.3	-	* (2)
C33	DDI2_CTRLDATA_AUX-	GBE1_LINK100# / 100 BT Ethernet controller speed indicator	OD-3.3	-	* (2)
C34	DDI2_DDC_AUX_SEL	GBE1_LINK1000# / 1G BT Ethernet controller speed indicator	OD-3.3	-	* (1)
C35	RSVD5	NC	NC	-	
C36	DDI3_CTRLCLK_AUX+	LAN_I2C_SCL / I2C Data line for LAN use	I/O-3.3	-	* (2)
C37	DDI3_CTRLDATA_AUX-	LAN_I2C_SDA / I2C Clock for LAN use	I/O-3.3	-	* (2)
C38	DDI3_DDC_AUX_SEL	GND	I-3.3	-	(1)
C39	DDI3_PAIR0+	LAN0_KR_RX+ / 10G KR Ethernet Interface LAN0_KR_RX-	DP-I	-	**
C40	DDI3_PAIR0-				
C41	GND_35	Power Ground	PWR	-	
C42	DDI3_PAIR1+	LAN_MDC0_LED0_1 / Management interface clock or LED output	O-1.05	-	**
C43	DDI3_PAIR1-	LAN_MDIO0_LED0_0 / Management interface data or LED output	I/O-1.05	-	**
C44	DDI3_HPD	DDI Hotplug Detect	I-3.3	-	NC (3)
C45	RSVD6	NC	NC	-	GND
C46	DDI3_PAIR2+	LAN1_KR_RX+ / 10G KR Ethernet Interface LAN1_KR_RX-	DP-I	-	**
C47	DDI3_PAIR2-				
C48	RSVD7	GND	NC	-	
C49	DDI3_PAIR3+	LAN_MDC1_LED1_1 / Management interface clock or LED output	O-1.05	-	**
C50	DDI3_PAIR3-	LAN_MDIO1_LED1_0 / Management interface data or LED output	I/O-1.05	-	**
C51	GND_36	Power Ground	PWR	-	
C52	PEG_RX0+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C53	PEG_RX0-				
C54	TYPE0#	Indicate to the Carrier Board the Pin-out Type that is implemented on the Module: TYPE2# TYPE1# TYPE0# GND NC NC Type 6	Strap	-	NC for type 6 module

Pin	COME Signal	Description	Type	Termination	Comment
C55	PEG_RX1+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C56	PEG_RX1-				
C57	TYPE1#	refer to C54	Strap	-	NC for type 6 module
C58	PEG_RX2+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C59	PEG_RX2-				
C60	GND_37	Power Ground	PWR	-	
C61	PEG_RX3+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C62	PEG_RX3-				
C63	RSVD8	NC	NC	-	
C64	RSVD9	NC	NC	-	
C65	PEG_RX4+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C66	PEG_RX4-				
C67	RSVD10	NC	NC	-	refer to 3.2
C68	PEG_RX5+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C69	PEG_RX5-				
C70	GND_38	Power Ground	PWR	-	
C71	PEG_RX6+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C72	PEG_RX6-				
C73	GND_39	Power Ground	PWR	-	
C74	PEG_RX7+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C75	PEG_RX7-				
C76	GND_40	Power Ground	PWR	-	
C77	RSVD11	NC	NC	-	
C78	PEG_RX8+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C79	PEG_RX8-				
C80	GND_41	Power Ground	PWR	-	
C81	PEG_RX9+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C82	PEG_RX9-				
C83	RSVD12	NC	NC	-	
C84	GND_42	Power Ground	PWR	-	
C85	PEG_RX10+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C86	PEG_RX10-				
C87	GND_43	Power Ground	PWR	-	
C88	PEG_RX11+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C89	PEG_RX11-				

Pin	COME Signal	Description	Type	Termination	Comment
C90	GND_44	Power Ground	PWR	-	
C91	PEG_RX12+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C92	PEG_RX12-				
C93	GND_45	Power Ground	PWR	-	
C94	PEG_RX13+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C95	PEG_RX13-				
C96	GND_46	Power Ground	PWR	-	
C97	RSVD13	NC	NC	-	
C98	PEG_RX14+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C99	PEG_RX14-				
C100	GND_47	Power Ground	PWR	-	
C101	PEG_RX15+	PCI Express Graphics receive. AC coupled off Module.	DP-I	-	
C102	PEG_RX15-				
C103	GND_48	Power Ground	PWR	-	
C104	VCC_12V_13	main input voltage (8.5-20V)	PWR 8.5-20V	-	
C105	VCC_12V_14				
C106	VCC_12V_15				
C107	VCC_12V_16				
C108	VCC_12V_17				
C109	VCC_12V_18				
C110	GND_49	Power Ground	PWR	-	

#	Active low
+ and -	Differential pair differentiator
*	Module drives low or open drain. Module tolerates possible PU from type 6 carrier.
**	Safe, AC coupled on DDI carrier
(1)	100K PU to 3.3V or 1Meg PD on Topanga Canyon
(2)	2.2K PU to 3.3V on DDI carrier
(3)	Carrier includes a blocking FET to avoid backfeeding. However, Topanga drives push-pull on this, so not used.

5.4 Connector X1B Row D

Table 39 lists the pin-outs for Connector X1B Row D.

Table 39: Connector X1B Row D Pin-out List

Pin	COME Signal	Description	Type	Termination	Comment
D1	GND_50	Power Ground	PWR	-	
D2	GND_51				
D3	USB_SSTX0-	Additional transmit signal for the SuperSpeed USB data path.	DP-O	-	
D4	USB_SSTX0+				
D5	GND_52	Power Ground	PWR	-	
D6	USB_SSTX1-	Additional transmit signal for the SuperSpeed USB data path.	DP-O	-	
D7	USB_SSTX1+				
D8	GND_53	Power Ground	PWR	-	
D9	USB_SSTX2-	Additional transmit signal for the SuperSpeed USB data path.	DP-O	-	
D10	USB_SSTX2+				
D11	GND_54	Power Ground	PWR	-	
D12	USB_SSTX3-	Additional transmit signal for the SuperSpeed USB data path.	DP-O	-	
D13	USB_SSTX3+				
D14	GND_55	Power Ground	PWR	-	
D15	DDI1_CTRLCLK_AUX+	HDMI/DVI I2C CTRLCLK or DP AUX+ function.	I/O-3.3	-	NC (2)
D16	DDI1_CTRLDATA_AUX-	HDMI/DVI I2C CTRLDATA or DP AUX- function	I/O-3.3	-	NC (2)
D17	RSVD14	NC	NC	-	
D18	RSVD15	NC	NC	-	
D19	PCIE_TX6+	PCI Express Transmit	DP-O	-	
D20	PCIE_TX6-				
D21	GND_56	Power Ground	PWR	-	
D22	PCIE_TX7+	PCI Express Transmit	DP-O	-	
D23	PCIE_TX7-				
D24	RSVD16	NC	NC	-	
D25	RSVD17	NC	NC	-	
D26	DDI1_PAIR0+	GBE1_MDI3- / Gigabit Eth. Media Dependent Interface GBE1_MDI3+	DP-O	-	**
D27	DDI1_PAIR0-				
D28	RSVD18	NC	NC	-	
D29	DDI1_PAIR1+	GBE1_MDI2- / Gigabit Eth. Media Dependent Interface GBE1_MDI2+	DP-O	-	**
D30	DDI1_PAIR1-				

Pin	COME Signal	Description	Type	Termination	Comment
D31	GND_57	Power Ground	PWR	-	
D32	DDI1_PAIR2+	LAN_SPI_CLK / LAN firmware SPI flash clock	O-3.3	-	**
D33	DDI1_PAIR2-	LAN_SPI_CS# / LAN firmware SPI flash chip select	O-3.3	-	**
D34	DDI1_DDC_AUX_SEL	LAN_SPI_HOLD / LAN firmware SPI flash hold	I-3.3	-	* (1)
D35	RSVD19	LAN_DETECT# / When grounded indicates the carrier implements the custom pinout for GBE2 and 10G LAN	I-3.3	-	
D36	DDI1_PAIR3+	LAN_SPI_MISO / LAN firmware SPI data output	I-3.3	-	**
D37	DDI1_PAIR3-	LAN_SPI_MOSI / LAN firmware SPI data input	O-3.3	-	**
D38	RSVD20	GND	NC	-	
D39	DDI2_PAIR0+	LAN0_KR_TX+ / 10G KR Ethernet Interface	DP-O	-	**
D40	DDI2_PAIR0-	LAN0_KR_TX			
D41	GND_58	Power Ground	PWR	-	
D42	DDI2_PAIR1+	LAN_SDP0_0 / Software defined pin	OD-3.3	-	**
D43	DDI2_PAIR1-	LAN_SDP0_1 / Software defined pin	I-3.3	-	**
D44	DDI2_HPD	DDI Hotplug Detect	I-3.3	-	NC (3)
D45	RSVD21	NC	NC	-	GND
D46	DDI2_PAIR2+	LAN1_KR_TX+ / 10G KR Ethernet Interface	DP-O	-	**
D47	DDI2_PAIR2-	LAN1_KR_TX-			
D48	RSVD22	NC	NC	-	GND
D49	DDI2_PAIR3+	LAN_SDP1_0 / Software defined pin	OD-3.3	-	**
D50	DDI2_PAIR3-	LAN_SDP1_1 / Software defined pin	I-3.3	-	**
D51	GND_59	Power Ground	PWR	-	
D52	PEG_TX0+	PCI Express Graphics transmit.	DP-O	-	
D53	PEG_TX0-				
D54	PEG_LANE_RV#	PCIexpress Graphics Lane Reversal	I-3.3	PU 10k 3.3V (S0)	
D55	PEG_TX1+	PCI Express Graphics transmit.	DP-O	-	
D56	PEG_TX1-				
D57	TYPE2#	refer to C54	Strap	-	GND for type 6 module
D58	PEG_TX2+	PCI Express Graphics transmit.	DP-O	-	
D59	PEG_TX2-				
D60	GND_60	Power Ground	PWR	-	
D61	PEG_TX3+	PCI Express Graphics transmit.	DP-O	-	

Pin	COME Signal	Description	Type	Termination	Comment
D62	PEG_TX3-				
D63	RSVD23	NC	NC	-	
D64	RSVD24	NC	NC	-	
D65	PEG_TX4+	PCI Express Graphics transmit.	DP-O	-	
D66	PEG_TX4-				
D67	GND_61	Power Ground	PWR	-	
D68	PEG_TX5+	PCI Express Graphics transmit.	DP-O	-	
D69	PEG_TX5-				
D70	GND_62	Power Ground	PWR	-	
D71	PEG_TX6+	PCI Express Graphics transmit.	DP-O	-	
D72	PEG_TX6-				
D73	GND_63	Power Ground	PWR	-	
D74	PEG_TX7+	PCI Express Graphics transmit.	DP-O	-	
D75	PEG_TX7-				
D76	GND_64	Power Ground	PWR	-	
D77	RSVD25	NC	NC	-	
D78	PEG_TX8+	PCI Express Graphics transmit.	DP-O	-	
D79	PEG_TX8-				
D80	GND_65	Power Ground	PWR	-	
D81	PEG_TX9+	PCIexpress Graphics Transmit + (9)	DP-O	-	
D82	PEG_TX9-				
D83	RSVD26	NC	NC	-	
D84	GND_66	Power Ground	PWR	-	
D85	PEG_TX10+	PCI Express Graphics transmit.	DP-O	-	
D86	PEG_TX10-				
D87	GND_67	Power Ground	PWR	-	
D88	PEG_TX11+	PCI Express Graphics transmit.	DP-O	-	
D89	PEG_TX11-				
D90	GND_68	Power Ground	PWR	-	
D91	PEG_TX12+	PCI Express Graphics transmit.	DP-O	-	
D92	PEG_TX12-				
D93	GND_69	Power Ground	PWR	-	
D94	PEG_TX13+	PCI Express Graphics transmit.	DP-O	-	
D95	PEG_TX13-				
D96	GND_70	Power Ground	PWR	-	

Pin	COME Signal	Description	Type	Termination	Comment
D97	RSVD27	NC	NC	-	
D98	PEG_TX14+	PCI Express Graphics transmit.	DP-O	-	
D99	PEG_TX14-				
D100	GND_71	Power Ground	PWR	-	
D101	PEG_TX15+	PCI Express Graphics transmit.	DP-O	-	
D102	PEG_TX15-				
D103	GND_72	Power Ground	PWR	-	
D104	VCC_12V_19	main input voltage (8.5-20V)	PWR 8.5-20V	-	
D105	VCC_12V_20				
D106	VCC_12V_21				
D107	VCC_12V_22				
D108	VCC_12V_23	main input voltage (8.5-20V)	PWR 8.5-20V	-	
D109	VCC_12V_24				
D110	GND_73	Power Ground	PWR	-	

#	Active low
+ and -	Differential pair differentiator
*	Module drives low or open drain. Module tolerates possible PU from type 6 carrier.
**	Safe, AC coupled on DDI carrier
(1)	100K PU to 3.3V or 1Meg PD on Topanga Canyon
(2)	2.2K PU to 3.3V on DDI carrier
(3)	Carrier includes a blocking FET to avoid backfeeding. However, Topanga drives push-pull on this, so not used.

6 / BIOS Operation

The module is equipped with AMI® Aptio V, which is located in an onboard SPI serial flash memory.



The BIOS version covered in this document might not be the latest version. The latest version might have certain differences to the BIOS options and features described in this chapter.

6.1 Determining the BIOS Version

The AMI® Aptio version is displayed in the main menu of the setup utility.

- BIOS Vendor: American Megatrends
- Core Version: x.x.x.x
- Project Version: COMe_bBD6_Rx.xx x64
- Build Date and Time: mm/dd/yyyy hh:mm:ss

6.2 BIOS Update

Kontron provides continuous BIOS updates for Computer-on-Modules. The updates are provided for download on http://emdcustomersection.kontron.com with a detailed change description within the according Product Change Notification (PCN).



Please register for the EMD Customer Section to get access to BIOS downloads and PCN service.

Therefore, it is strongly recommended to use the "Kflash" shell utility available from version 0.06 with the BIOS binary update to flash the whole SPI region (16MB).

1. Boot the module to EFI Shell with access to the BIOS image.
2. Execute "kflash " shell utility as described in 3.5.1.

Backup the BIOS / Create a BIOS with custom defaults:

1. Change your BIOS settings according to your needs and backup your customized binary onto a USB storage device.
2. Save and Exit Setup to EFI Shell.
3. On your terminal, make sure to navigate to the USB key.
4. Enter the following command to read SPI and save content to file "**binary_name.bin**" in USB storage:

   kflash -s binary_name.bin

Now you can clone the BIOS with your customized default settings to other modules or external SPI flashes with the above "kflash" Shell utility and the new customized and saved binary ("binary_name.bin").

NOTICE Any modification of the update process may damage your module.

6.3 Setup Guide

The Aptio Setup Utility changes system behavior by modifying the Firmware configuration. The setup program uses a number of menus to make changes and turn features on or off.

Functional keystrokes in POST:

Table 40: Key Assignment

Key	Function
DEL	Enter Setup
F2	Enter Setup
F7	Boot Menu

6.4 POST Codes

Table 41: Important POST codes during boot-up

Key	Function
AB	BIOS Setup
AD	EFI Shell
AE	Windows

6.4.1 Start AMI® Aptio Setup Utility

To start the AMI® BIOS setup utility, press <DEL> or <F2> when the following string appears during bootup:

Press <DEL> to enter Setup

The setup utility screen appears.

The Setup Screen is composed of several sections:

Table 42: BIOS Setup Screen Sections

Setup Screen	Location	Function
Menu Bar	Top	Lists and selects all top level menus.
Legend Bar	Right side Bottom	Lists setup navigation keys.
Item Specific Help Window	Right side Top	Help for selected item.
Menu Window	Left Center	Selection fields for current menu.

6.4.1.1 Menu Bar

The menu bar at the top of the window lists different menus. Use the left/right arrow keys to make a selection.

6.4.1.2 Legend Bar

Use the keys listed in the legend bar on the bottom to make your selections or exit the current menu. The table below describes the legend keys and their alternates.

Table 43: Legend Keys List

Key	Function
← or → Arrow key	Select a menu.
↑ or ↓ Arrow key	Select fields in current menu.
<Home> or <End>	Move cursor to top or bottom of current window.
<PgUp> or <PgDn>	Move cursor to next or previous page.
+/-	Change Option
<Enter>	Execute command or select submenu.
<F1>	General Help window.
<F2>	Previous Values
<F3>	Load the optimized default configuration.
<F4>	Save and exit.
<Esc>	Exit menu.

6.4.1.3 Selecting an Item

Use the ↑ or ↓ key to move the cursor to the field you want. Then use the + and – keys to select a value for that field. The Save Value commands in the Exit menu save the values displayed in all the menus.

6.4.1.4 Displaying Submenus

Use the ←or →key to move the cursor to the submenu you want. Then press <Enter>. A pointer ▶ marks all submenus.

6.4.1.5 Item Specific Help Window

The Help window on the right side of each menu displays the Help text for the selected item. It updates as you move the cursor to each field.

6.4.1.6 General Help Window

Pressing <F1> on a menu brings up the General Help window that describes the legend keys and their alternates. Press <Esc> to exit the General Help window.

6.5 BIOS Setup

6.5.1 Main

Figure 11: Main Menu Screen

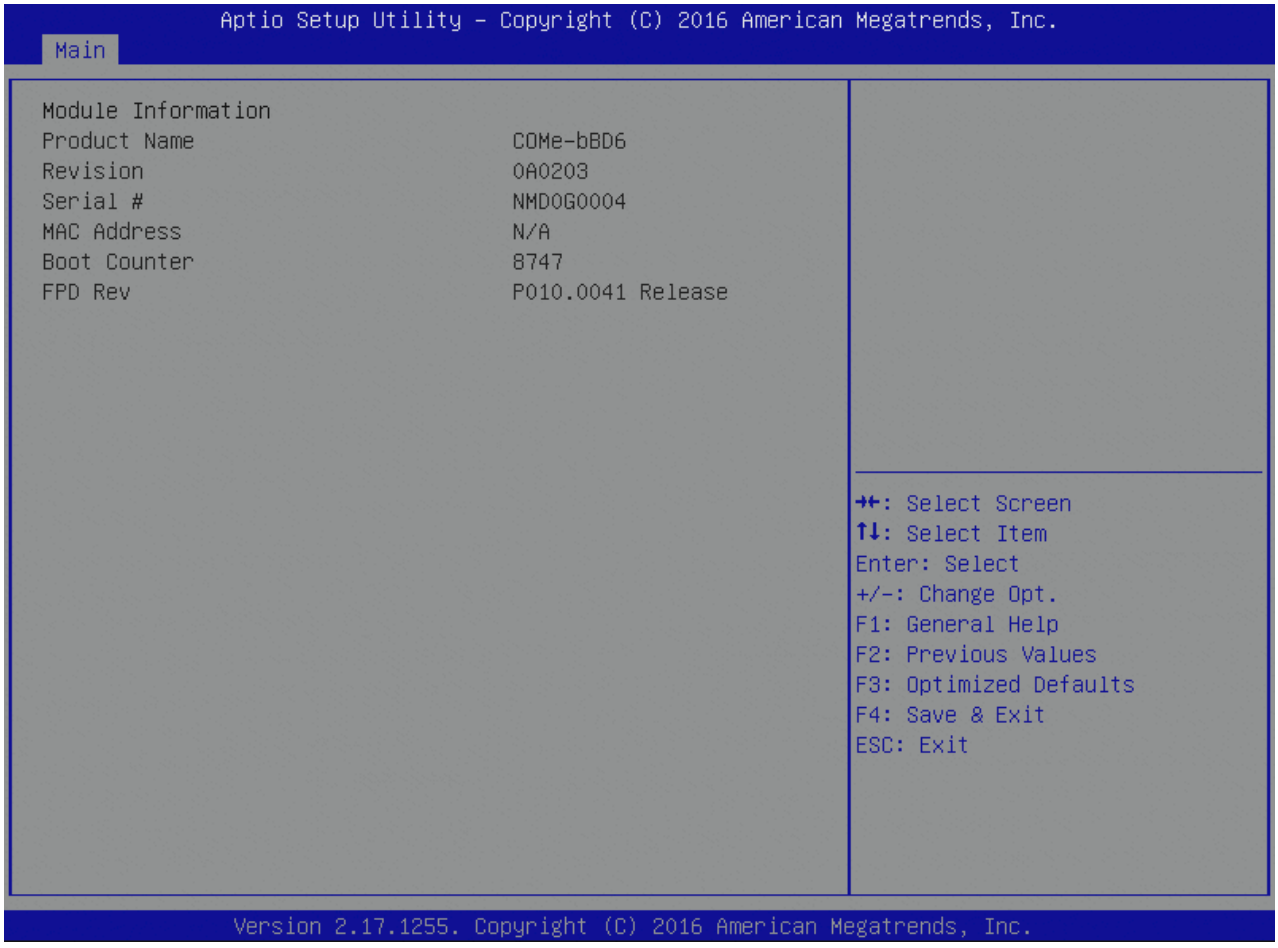


Table 44: Main Features List

Feature	Options	Description
System Language	English	Choose the system default language.
System Date	[mm/dd/yyyy]	Set the Date. Use Tab to switch between Date elements.
System Time	[hh:mm:ss]	Set the Time. Use Tab to switch between Time elements.

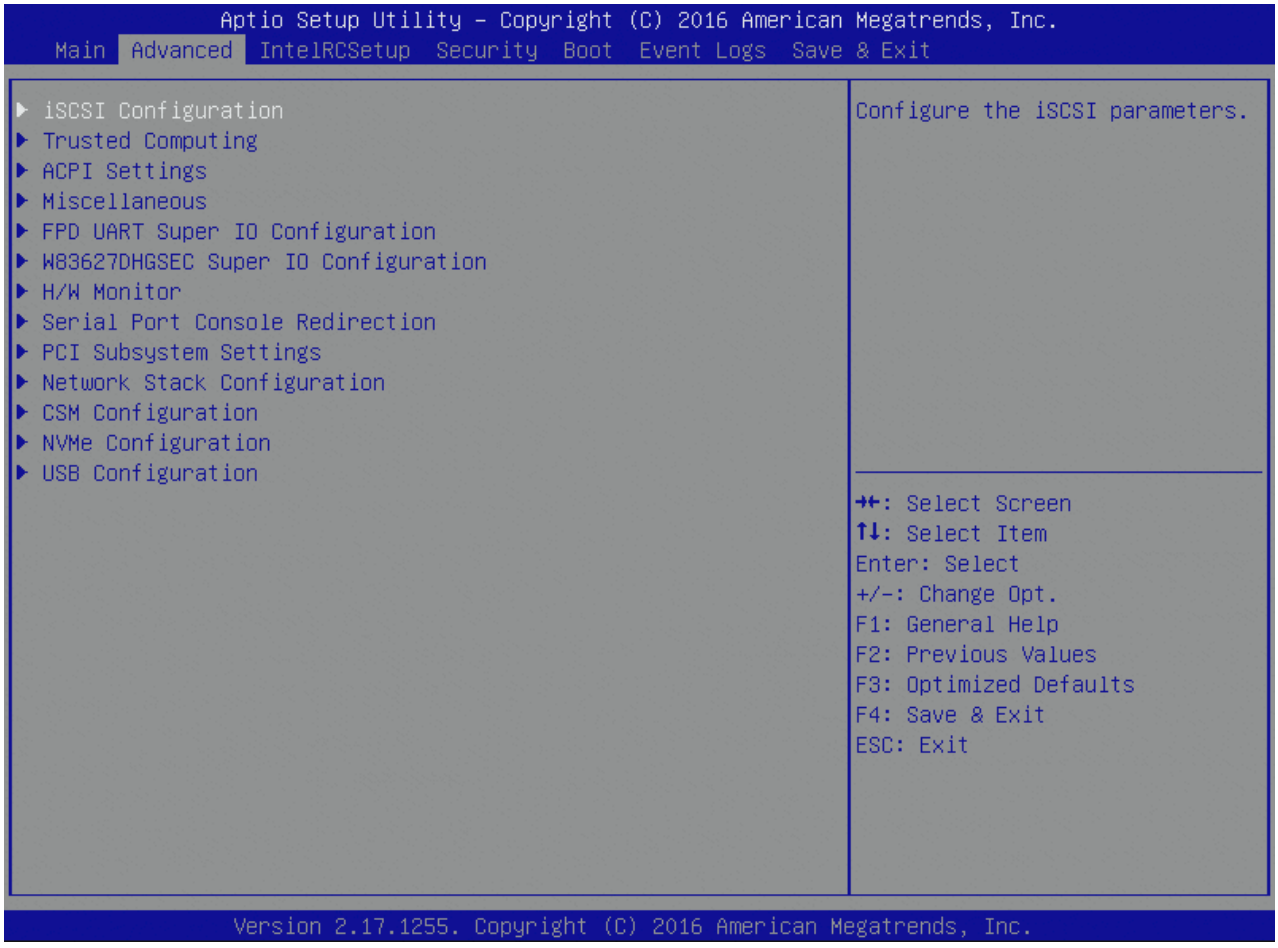
6.5.1.1 Platform Information

Figure 12: Platform Information Menu Screen



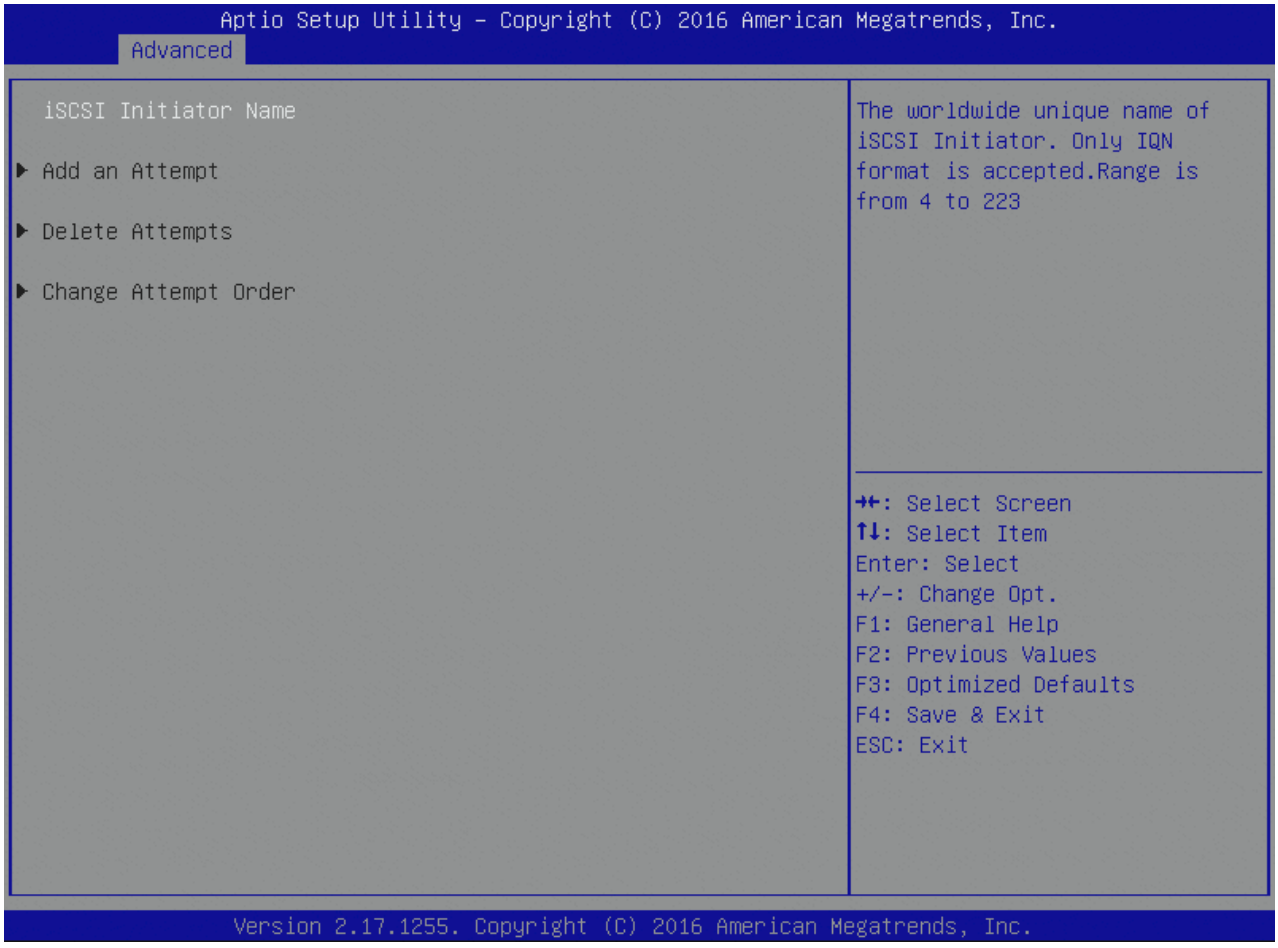
6.5.2 Advanced

Figure 13: Advanced Menu Screen



6.5.2.1 iSCSI Configuration

Figure 14: iSCSI Configuration Menu Screen



6.5.2.2 Trusted Computing

Figure 15: Trusted Computing Menu Screen

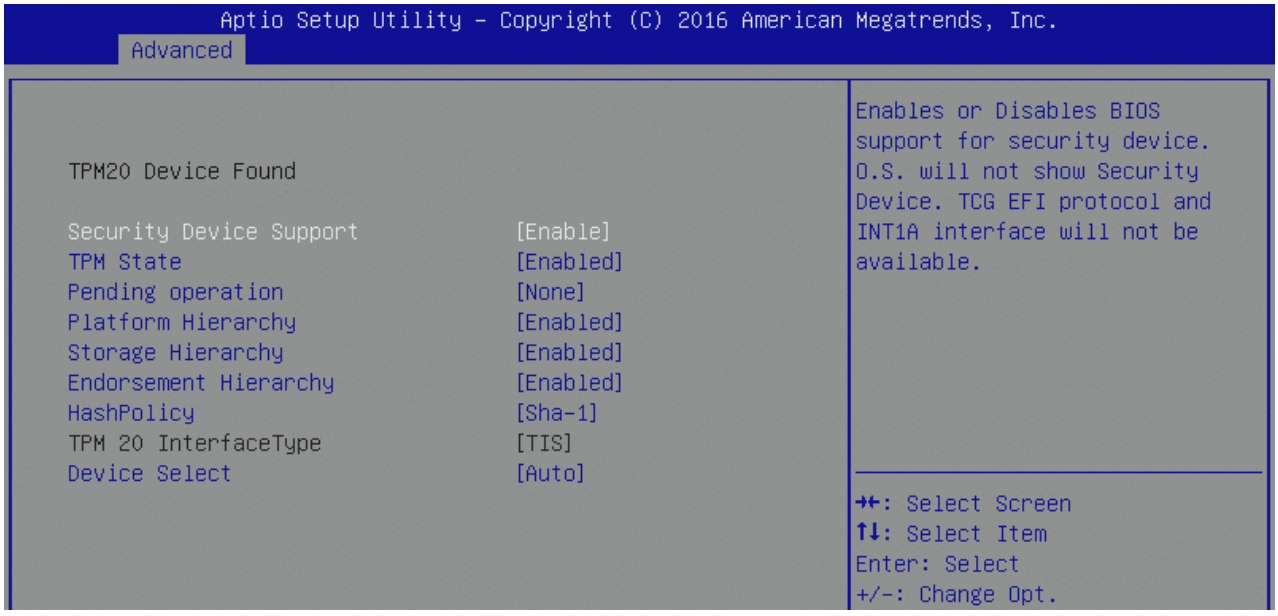


Table 45: Trusted Computing Features List

Feature	Options	Description
Security Device Support	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.
TPM State	Disabled **Enabled**	Enable/Disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
Pending operation	**None** TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
Platform Hierarchy	Disabled **Enabled**	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disabled **Enabled**	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disabled **Enabled**	Enable or Disable Endorsement Hierarchy
HashPolicy	Sha-1 Sha-2	Select the Hash policy to use. SHA-2 is most secure but might not be supported by all Operating Systems
Device Select	TPM 1.2 TPM 2.0 **Auto**	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

6.5.2.3 ACPI Settings

Figure 16: ACPI Settings Menu Screen

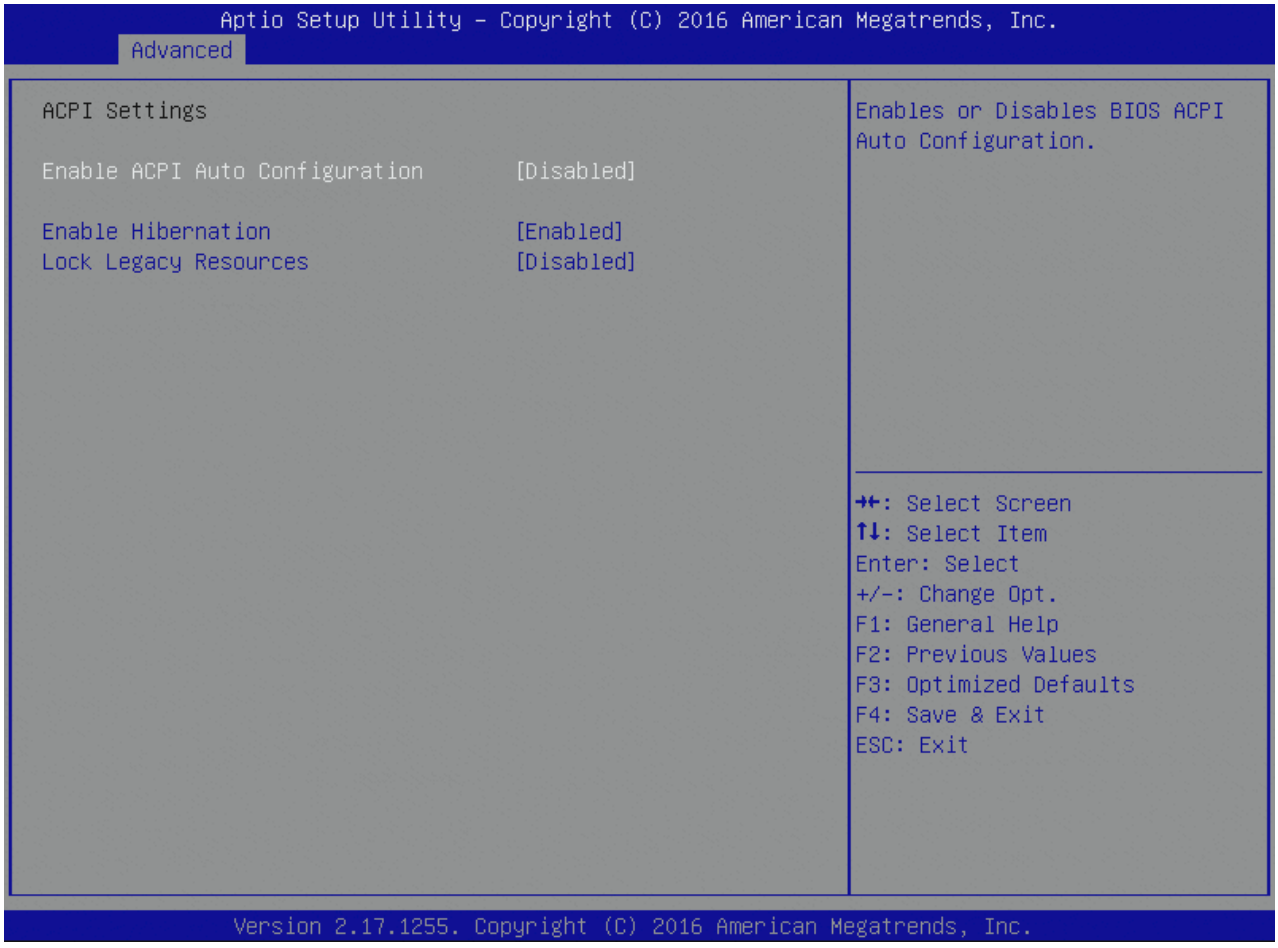


Table 46: ACPI Settings Features List

Feature	Options	Description
Enable ACPI Auto Configuration	**Disabled** Enabled	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled **Enabled**	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.
Lock Legacy Resources	**Disabled** Enabled	Enables or Disables Lock of Legacy Resources

6.5.2.4 Miscellaneous

Figure 17: Miscellaneous Menu Screen

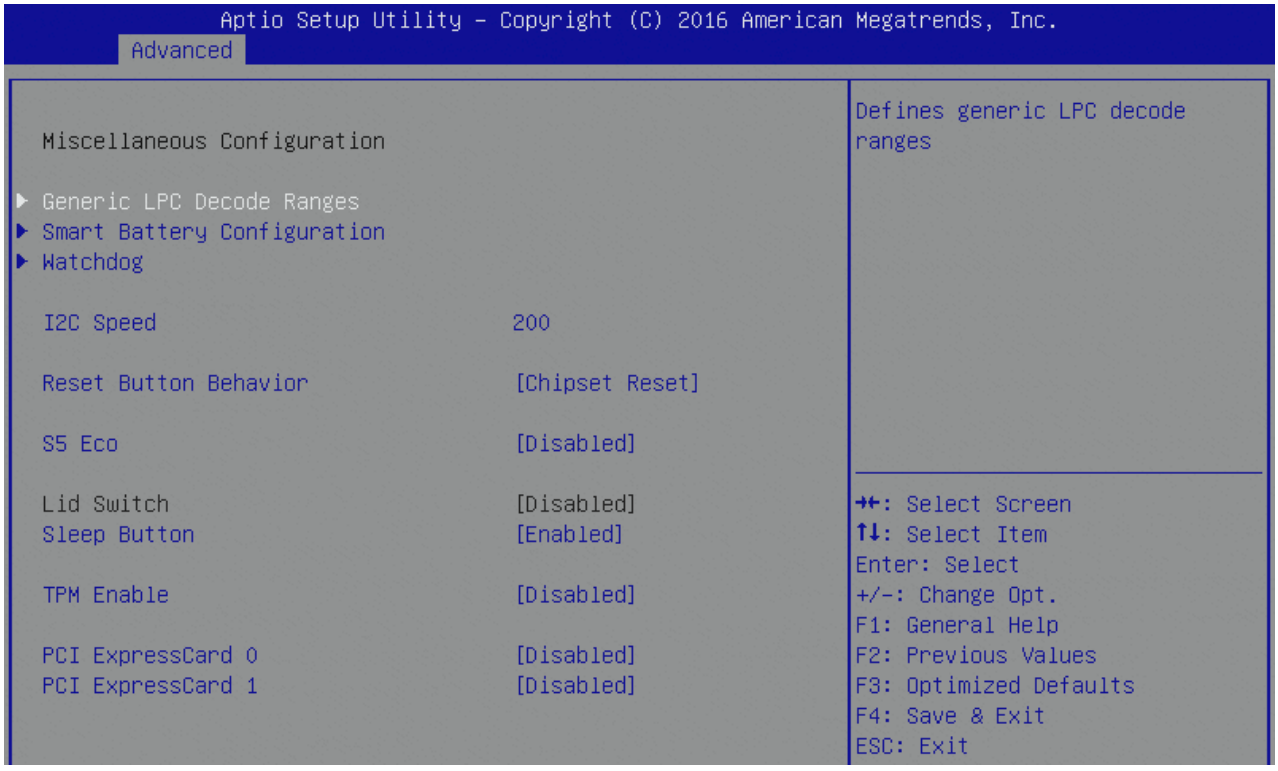


Table 47: Miscellaneous Features List

Feature	Options	Description
I2C Speed	200	Select I2C Bus Speed in kHz, min. 1kHz, max. 400kHz. For a default system 200kHz should be an appropriate value.
Reset Button Behavior	Chipset Reset Power Cycle	Select Reset Button Behavior: Chipset Reset, Power Cycle
S5 Eco	**Disabled** Enabled	Reduce supply current in Soft Off (S5) to less than 1mA. If enabled, power button is the only wakeup source in S5! See manual for restrictions in S5 Eco.
Sleep Button	Disabled **Enabled**	Shows or hides Sleep Button inside ACPI OS
TPM Enable	Disabled Enabled	Enable/Disable TPM (Trusted Platform Module)
PCI ExpressCard 0	Port 1 … Port 8 **Disabled**	Controls PCIe Port for ExpressCard support.
PCI ExpressCard 1	Port 1 … Port 8 **Disabled**	Controls PCIe Port for ExpressCard support.

6.5.2.5 Generic LPC Decode Ranges

Figure 18: Generic LPC Decode Ranges Menu Screen

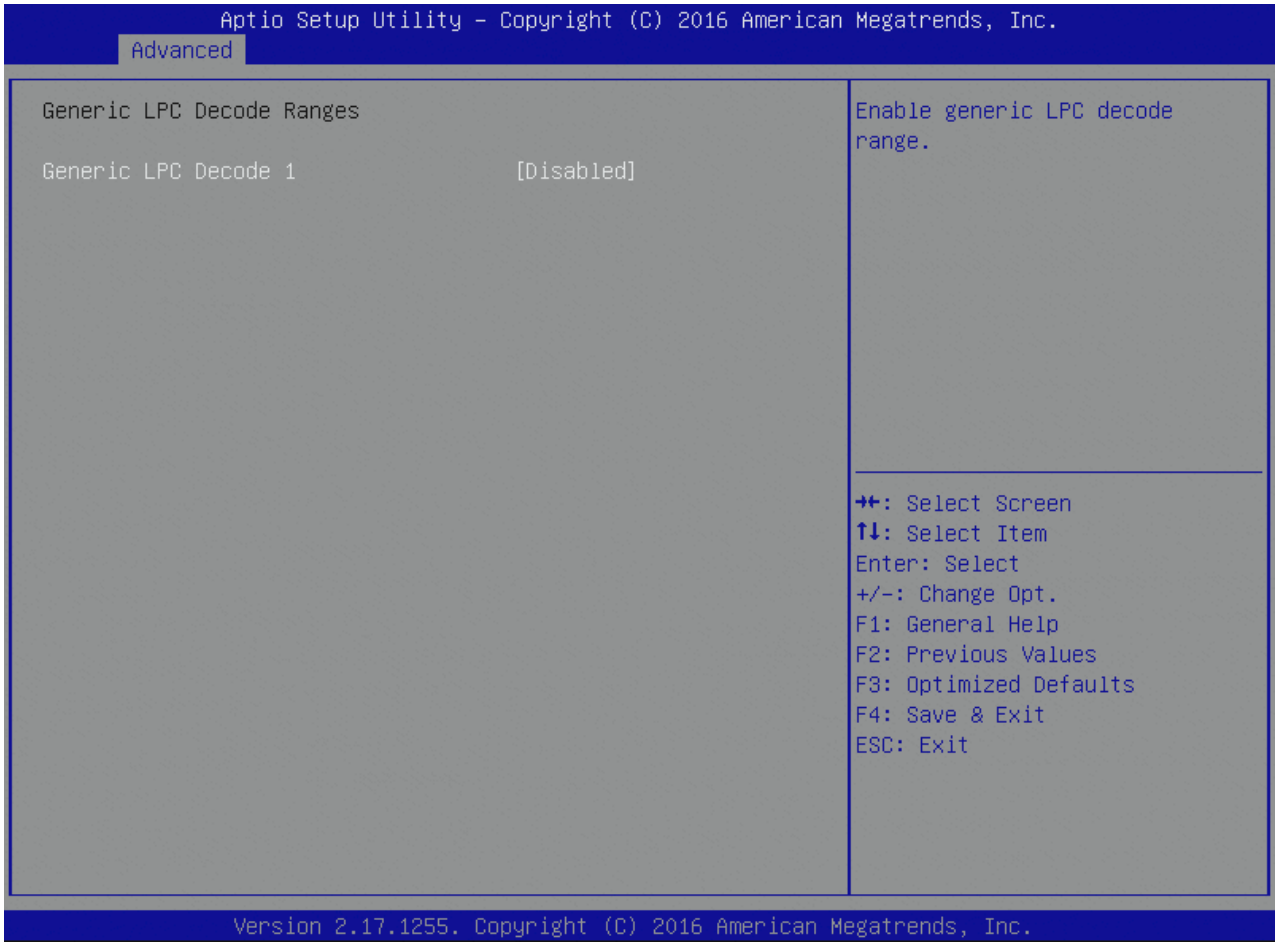


Table 48: Generic LPC Decode Ranges Features List

Feature	Options	Description
Generic LPC Decode 1	**Disabled** Enabled	Enable generic LPC decode range.

6.5.2.6 Smart Battery Configuration

Figure 19: Smart Battery Configuration Menu Screen

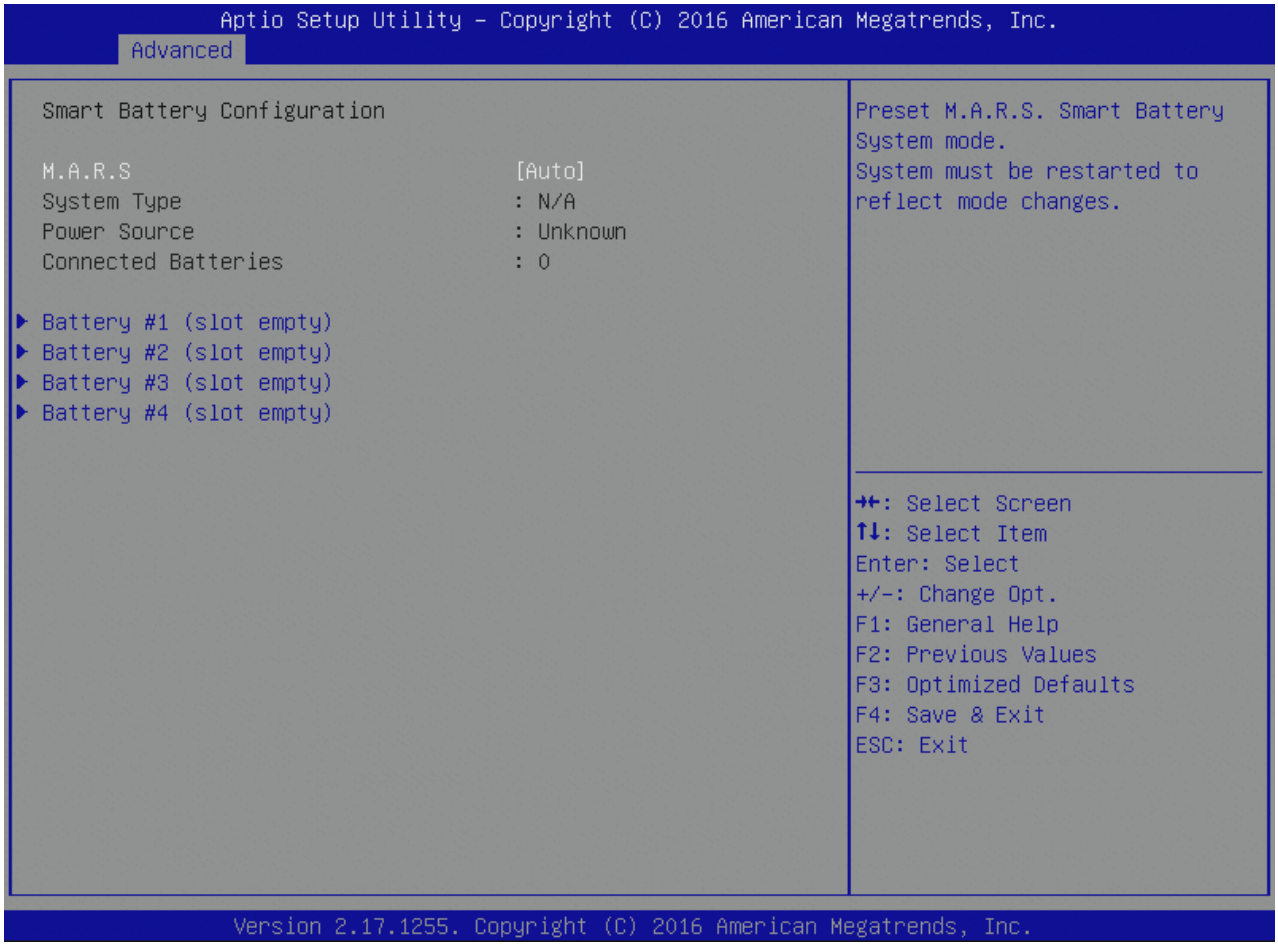
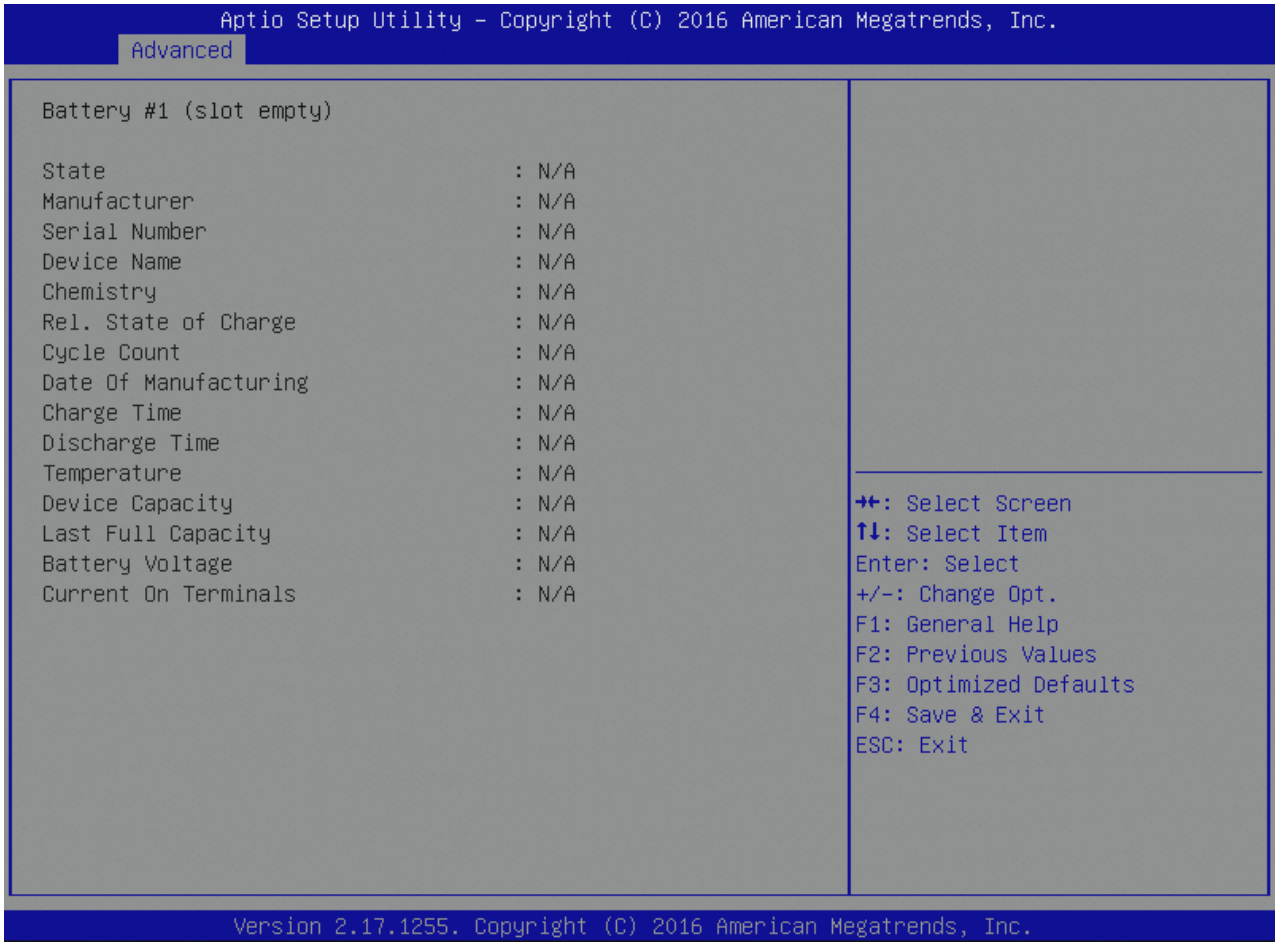


Table 49: Smart Battery Configuration Features List

Feature	Options	Description
M.A.R.S.	Disabled **Auto** Charger Manager	Preset M.A.R.S. Smart Battery System mode. System must be restarted to reflect mode changes.

6.5.2.7 Battery Information

Figure 20: Battery Information Menu Screen



6.5.2.8 Watchdog

Figure 21: Watchdog Menu Screen

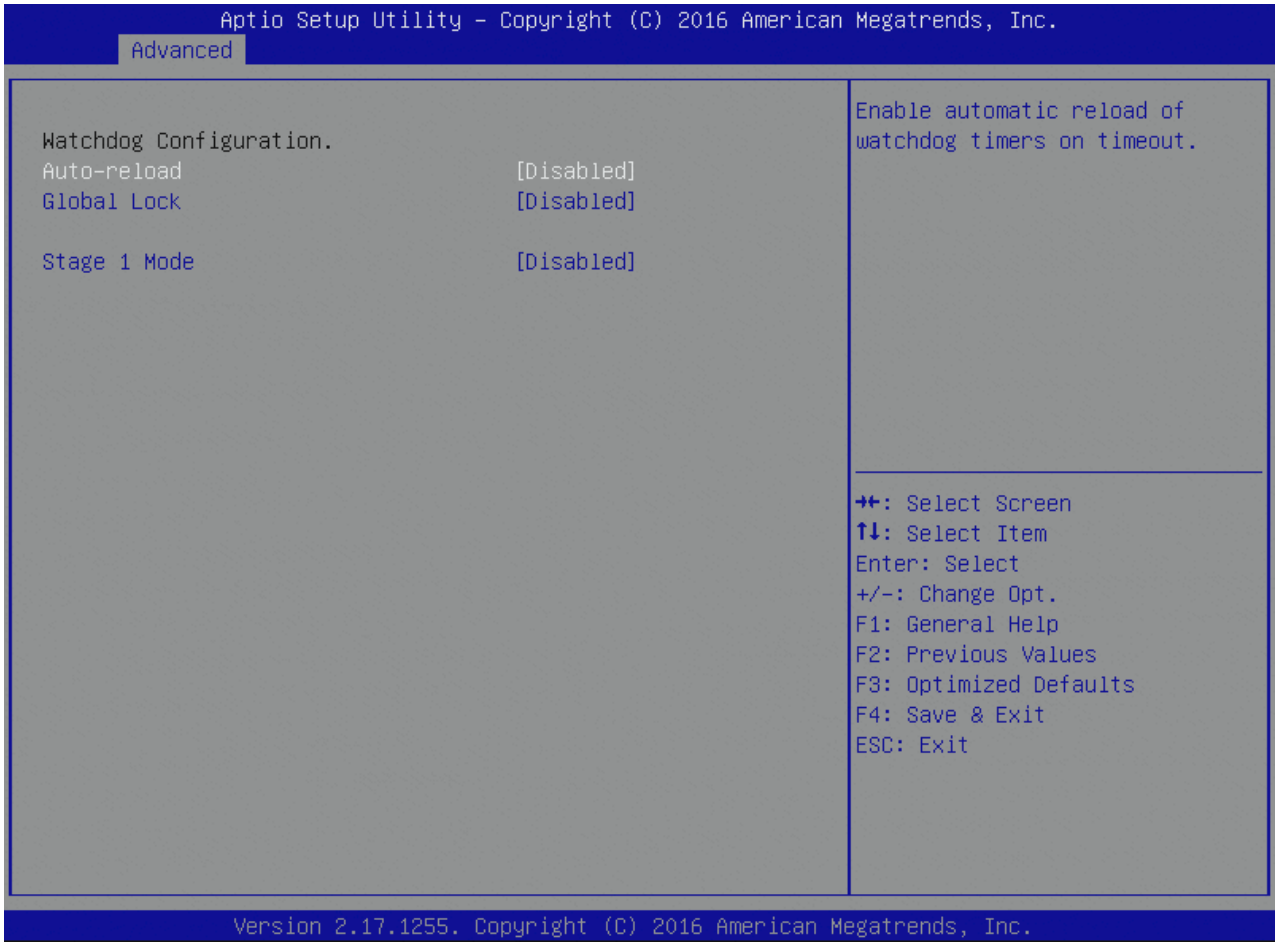


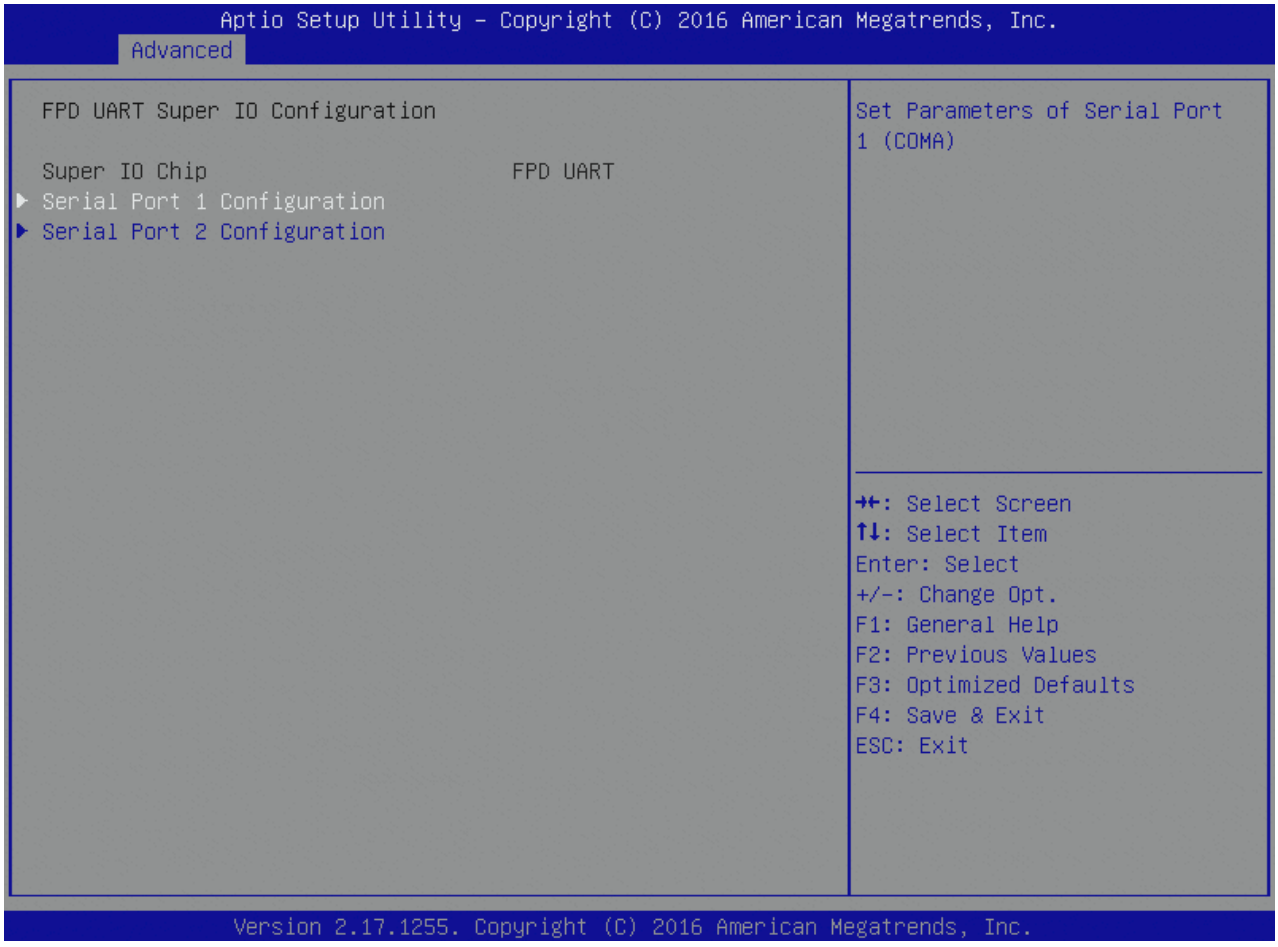
Table 50: Watchdog Features List

Feature	Options	Description
Auto-reload	**Disabled** Enabled	Enable automatic reload of watchdog timers on timeout.
Global Lock	**Disabled** Enabled	If set to enabled, all Watchdog registers (except WD_KICK) become read only until the board is reset.
Stage 1 Mode	**Disabled** Reset NMI SMI SCI Delay WDT Signal only	Select Action for this Watchdog stage

6.5.2.9 FPD UART Super IO Configuration

This setup option is available if a LPC SuperI/O Nuvoton 83627 is present on the baseboard. By default the COMe-bBD6 supports the legacy interfaces of 3.3V 83627DHG-P on external LPC. The SIO hardware monitor is not supported in the setup.

Figure 22: FPD UART Super IO Configuration Menu Screen



6.5.2.10 FPD UART Serial Port 1 Configuration

Figure 23: FPD UART Serial Port 1 Configuration Menu Screen

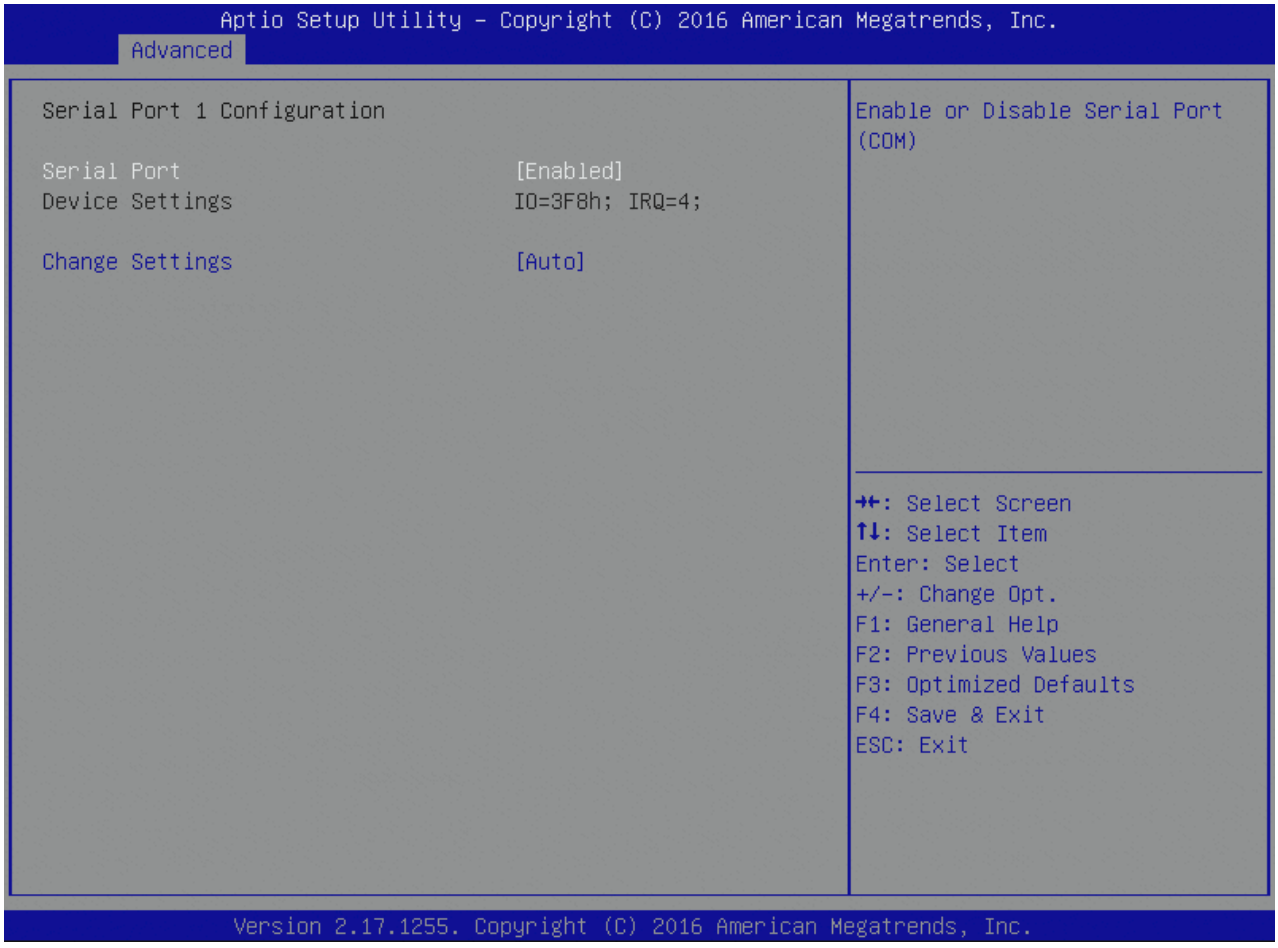


Table 51: FPD UART Serial Port 1 Configuration Features List

Feature	Options	Description
Serial Port	Disabled **Enabled**	Enable or Disable Serial Port (COM)
Change Settings	**AUTO** IO=3F8h; IRQ=4; IO=3F8h, IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h, IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h, IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h, IRQ=3,4,5,6,7,9,10,11,12;	Select an optimal setting for Super IO Device

6.5.2.11 FPD UART Serial Port 2 Configuration

Figure 24: FPD UART Serial Port 2 Configuration Menu Screen

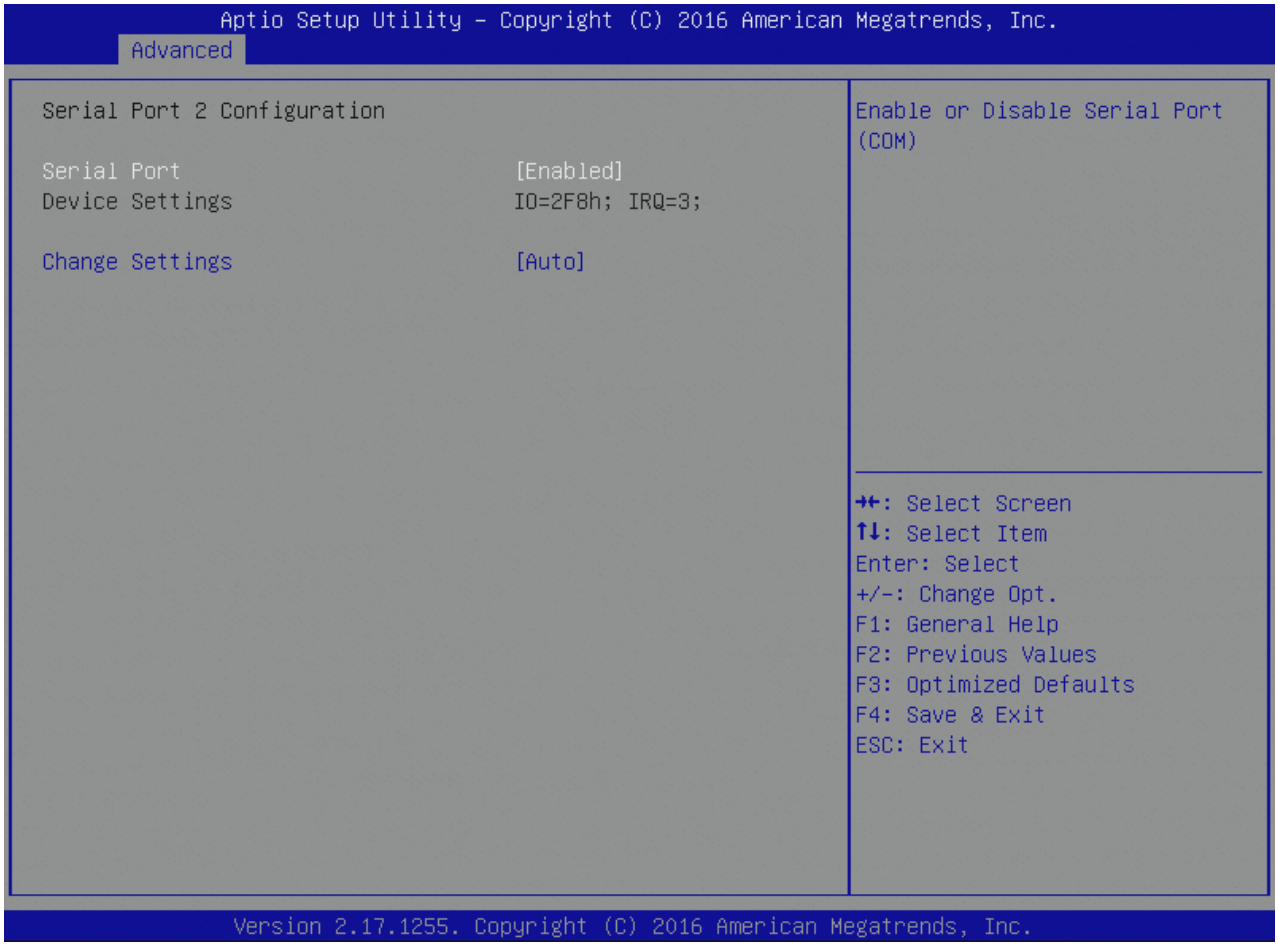
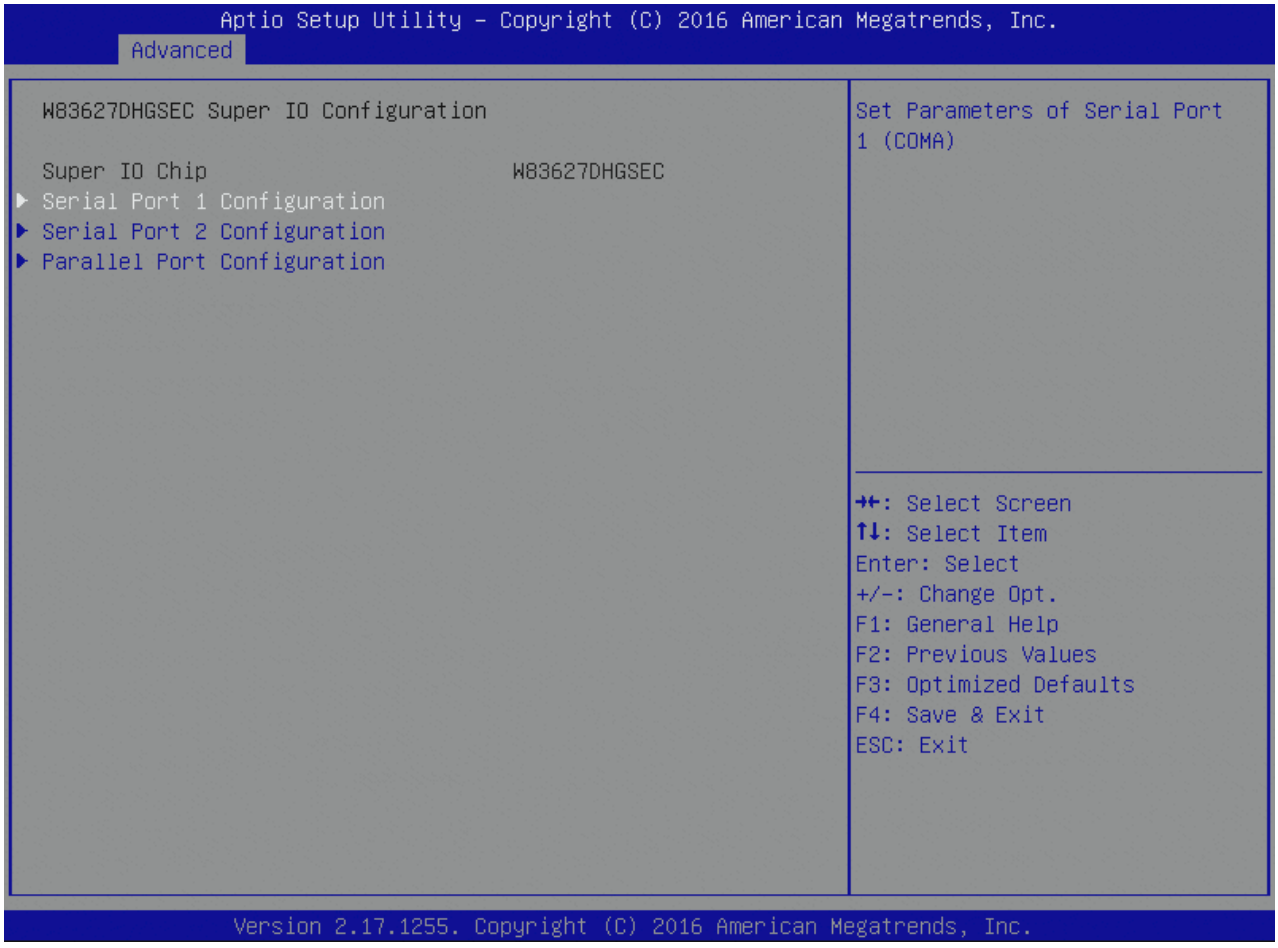


Table 52: FPD UART Serial Port 2 Configuration Features List

Feature	Options	Description
Serial Port	Disabled **Enabled**	Enable or Disable Serial Port (COM)
Change Settings	**AUTO** IO=2F8h; IRQ=3; IO=3F8h, IRQ=3,4,5,6,7,9,10,11,12; IO=2F8h, IRQ=3,4,5,6,7,9,10,11,12; IO=3E8h, IRQ=3,4,5,6,7,9,10,11,12; IO=2E8h, IRQ=3,4,5,6,7,9,10,11,12;	Select an optimal setting for Super IO Device

6.5.2.12 W83627DHGSEC Super IO Configuration

Figure 25: W83627DHGSEC Super IO Configuration Menu Screen



6.5.2.13 W83627DHGSEC Serial Port 1 Configuration

Figure 26: W83627DHGSEC Serial Port 1 Configuration Menu Screen

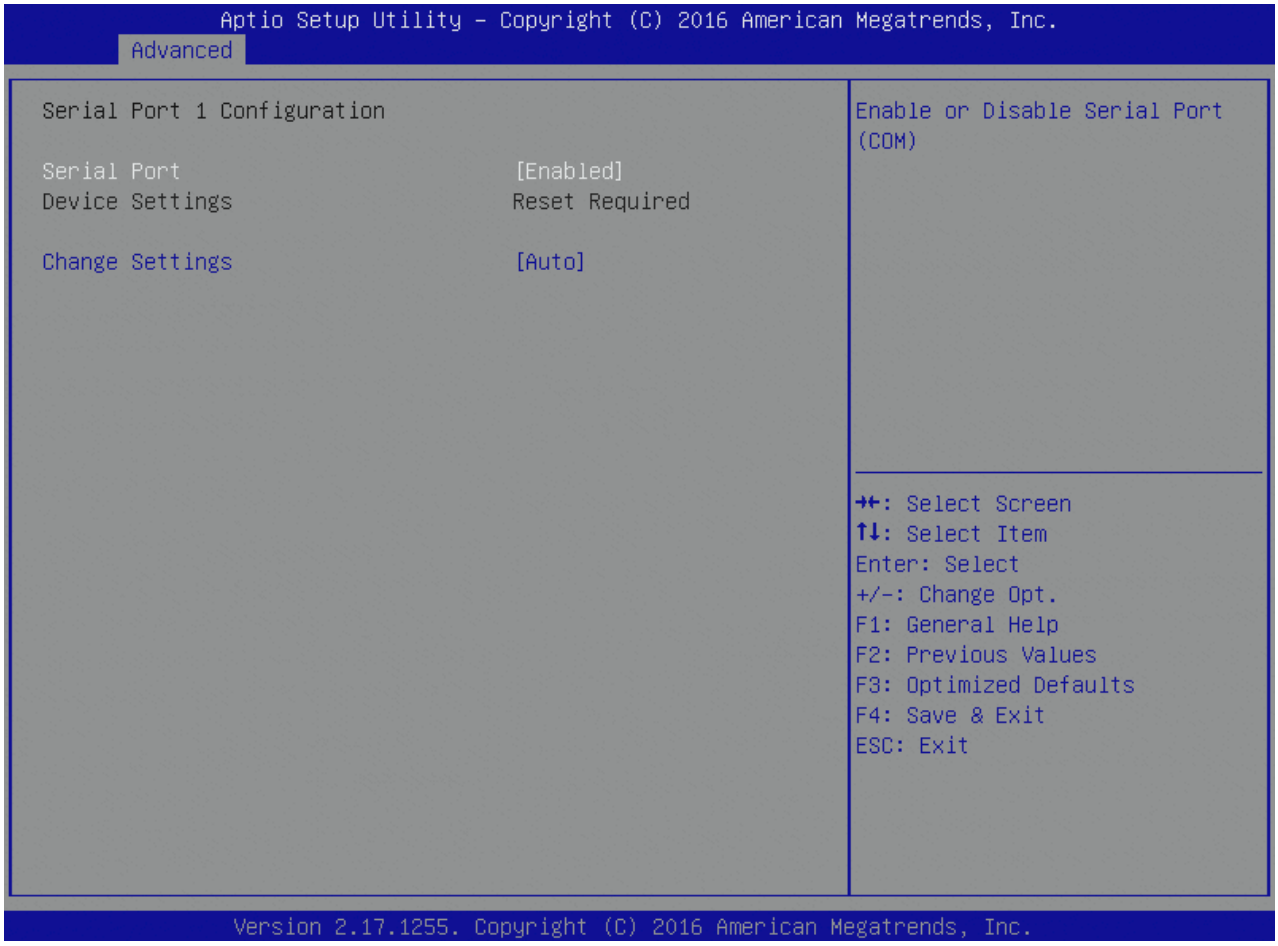


Table 53: W83627DHGSEC Serial Port 1 Configuration Features List

Feature	Options	Description
Serial Port	Disabled **Enabled**	Enable or Disable Serial Port (COM)
Change Settings	**Auto** IO=240h; IRQ=10; IO=240h, IRQ=3,4,5,6,7,10,11,12; IO=248h, IRQ=3,4,5,6,7,10,11,12; IO=250h, IRQ=3,4,5,6,7,10,11,12; IO=258h, IRQ=3,4,5,6,7,10,11,12; IO=260h, IRQ=3,4,5,6,7,10,11,12; IO=268h, IRQ=3,4,5,6,7,10,11,12;	Select an optimal settings for Super IO Device

6.5.2.14 W83627DHGSEC Serial Port 2 Configuration

Figure 27: W83627DHGSEC Serial Port 2 Configuration Menu Screen

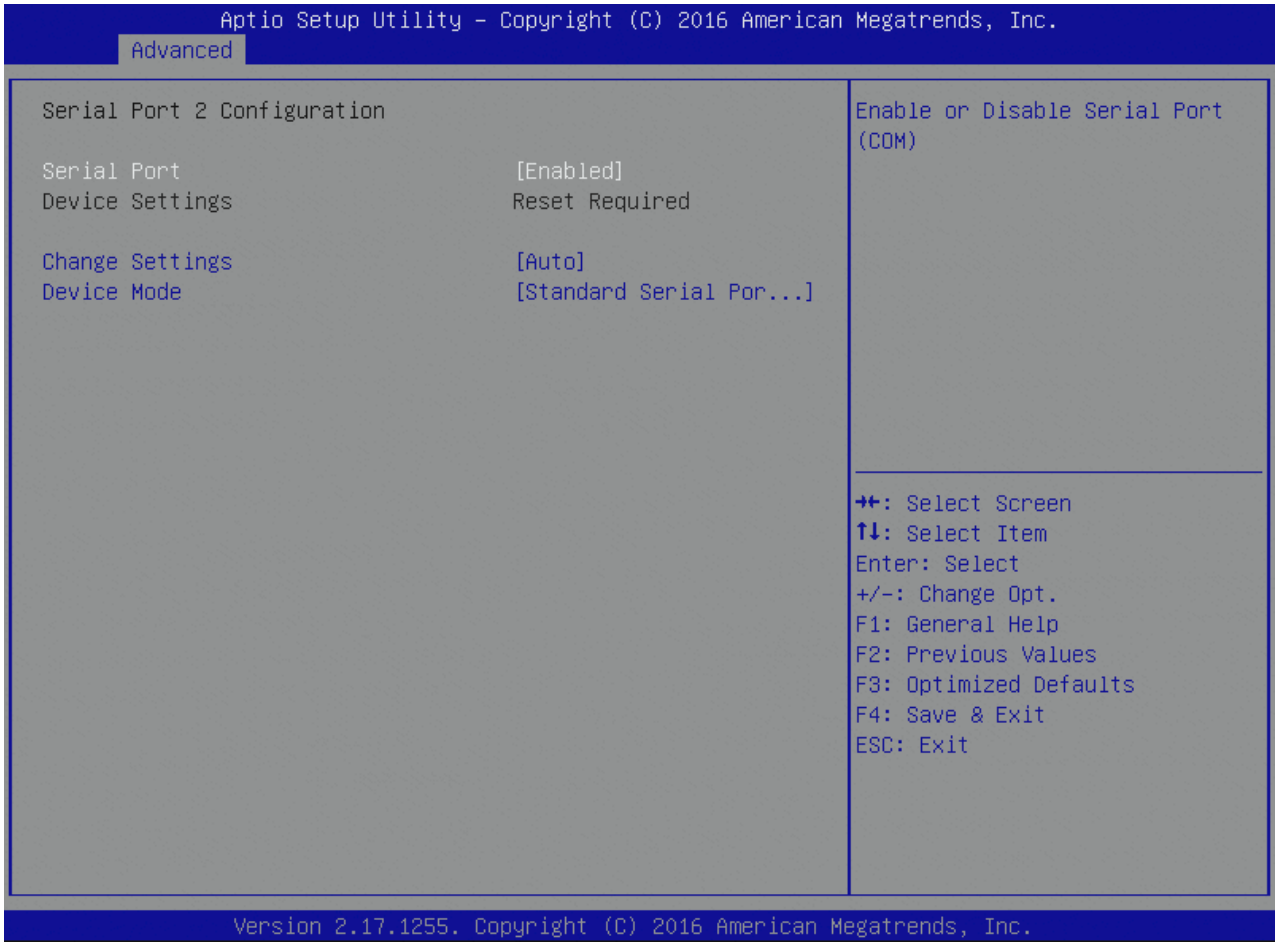


Table 54: W83627DHGSEC Serial Port 2 Configuration Features List

Feature	Options	Description
Serial Port	Disabled **Enabled**	Enable or Disable Serial Port (COM)
Change Settings	**Auto** IO=248h; IRQ=10; IO=240h, IRQ=3,4,5,6,7,10,11,12; IO=248h, IRQ=3,4,5,6,7,10,11,12; IO=250h, IRQ=3,4,5,6,7,10,11,12; IO=258h, IRQ=3,4,5,6,7,10,11,12; IO=260h, IRQ=3,4,5,6,7,10,11,12; IO=268h, IRQ=3,4,5,6,7,10,11,12;	Select an optimal setting for Super IO Device
Device Mode	**Standard Serial Port Mode** IrDA Active pulse 1.6 µS IrDA Active pulse 3/16 bit time ASKIR Mode	Change the Serial Port mode.

6.5.2.15 W83627DHGSEC Parallel Port Configuration

Figure 28: W83627DHGSEC Parallel Port Configuration Menu Screen

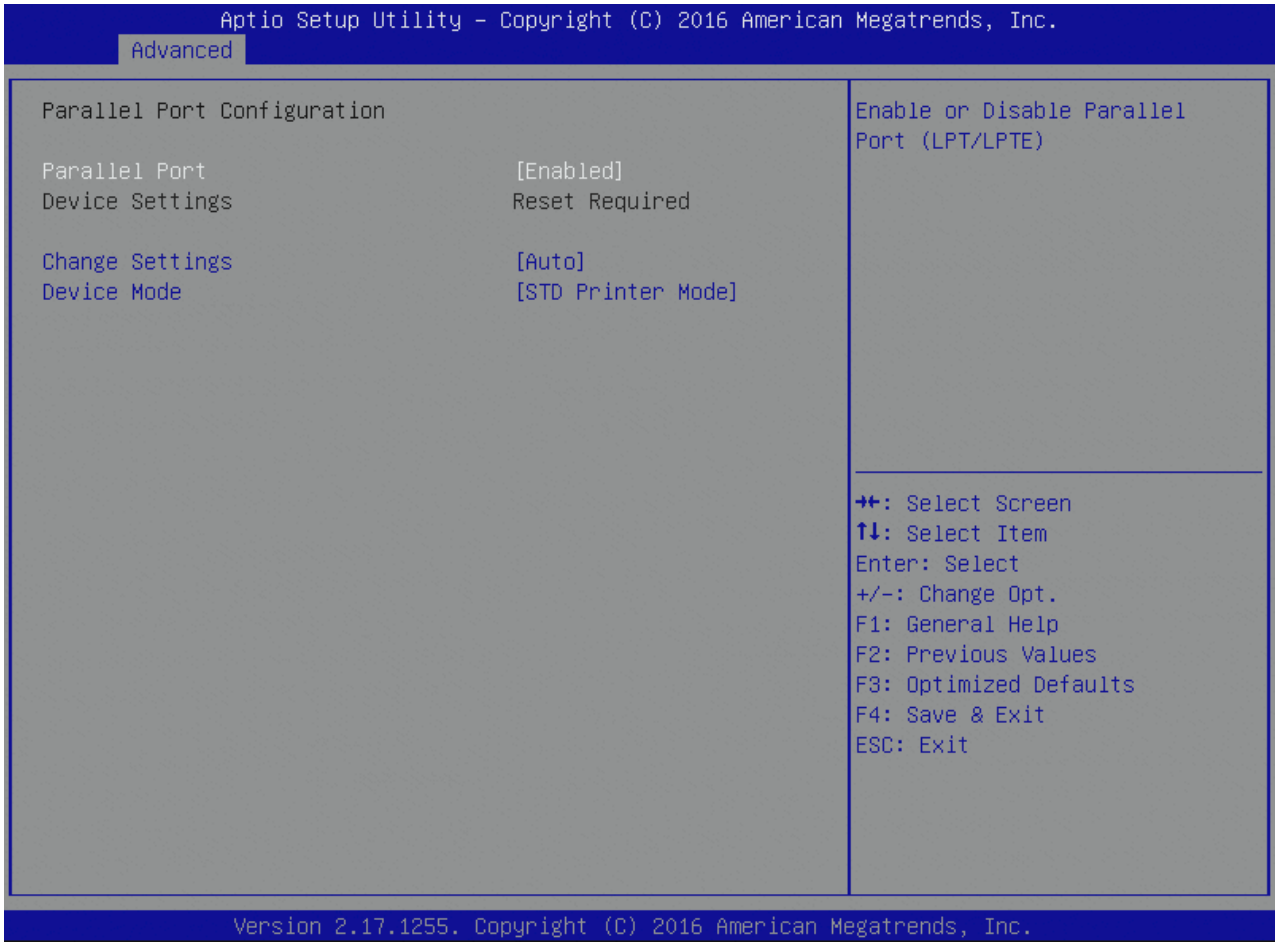


Table 55: W83627DHGSEC Parallel Port Configuration Features List

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

6.5.2.16 H/W Monitor

Hardware Monitor measurements and configuration for the onboard Nuvoton NCT7802Y.

Figure 29: H/W Monitor Menu Screen

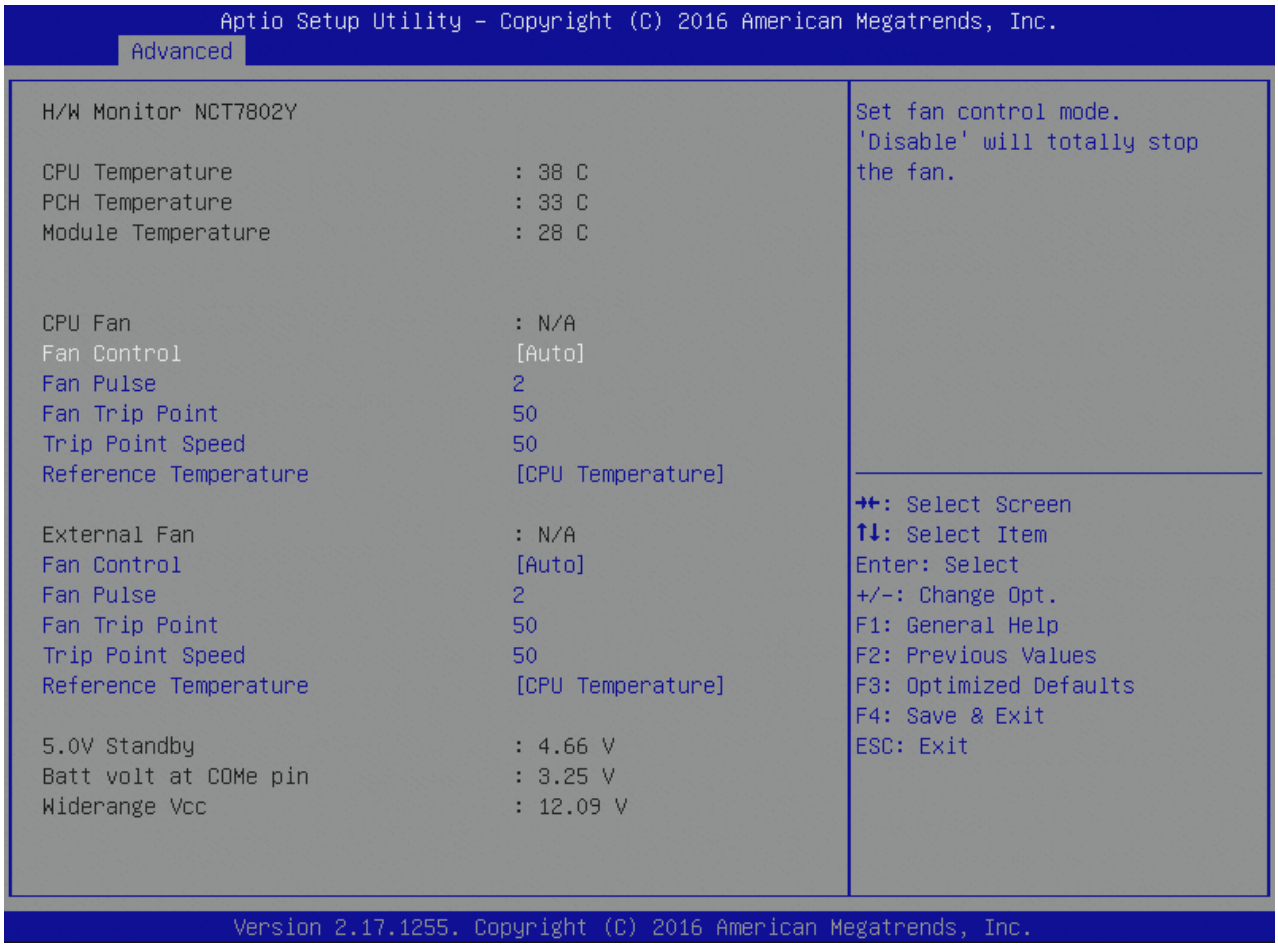


Table 56: H/W Monitor Features List

Feature	Options	Description
CPU Temperature	xx°C	Shows the measured temperature of the CPU Diode with onboard HWM.
PCH Temperature	xx°C	Shows the internal Platform Controller Hub temperature.
Module Temperature	xx°C	Shows the internal hardware monitor temperature.
CPU FAN	xxxx rpm	Shows the fan speed of onboard FAN connector.
FAN Control	Disabled Manual **Auto**	Set fan control mode. 'Disable' will totally stop the fan.
Fan Pulse	2	Number of pulses the fan produces during one revolution. Range 1-4
Fan Trip Point	50	Temperature where fan accelerates. Range: 20 – 80 C.
Trip Point Speed	50	Fan speed at trip point in %. Minimum value is 30. Fan always runs at 100% at TJmax – 10 C.

Feature	Options	Description
Reference Temperature	PCH Temperature Module Temperature **CPU Temperature**	Determines the temperature source which is used for automatic fan control
External FAN	xxxx rpm	Shows the fan speed of external COMe FAN.
FAN Control	Disabled Manual **Auto**	Set fan control mode. 'Disable' will totally stop the fan.
Fan Pulse	2	Number of pulses the fan produces during one revolution. Range 1-4
Fan Trip Point	50	Temperature where fan accelerates. Range 20 – 80 C
Trip Point Speed	50	Fan speed at trip point in %. Minimum value is 30. Fan always runs at 100% at TJmax – 10 C.
Reference Temperature	PCH Temperature Module Temperature **CPU Temperature**	Determines the temperature source which is used for automatic fan control.
5.0V Standby	x.xx V	Shows the 5V Standby Voltage input.
Batt volt at COMe pin	x.xx V	Shows the RTC Battery Voltage input measured at COMe connector.
Widerange Vcc	x.xx V	Shows the Module Main Input Voltage.

6.5.2.17 Serial Port Console Redirection

Figure 30: Serial Port Console Redirection Menu Screen

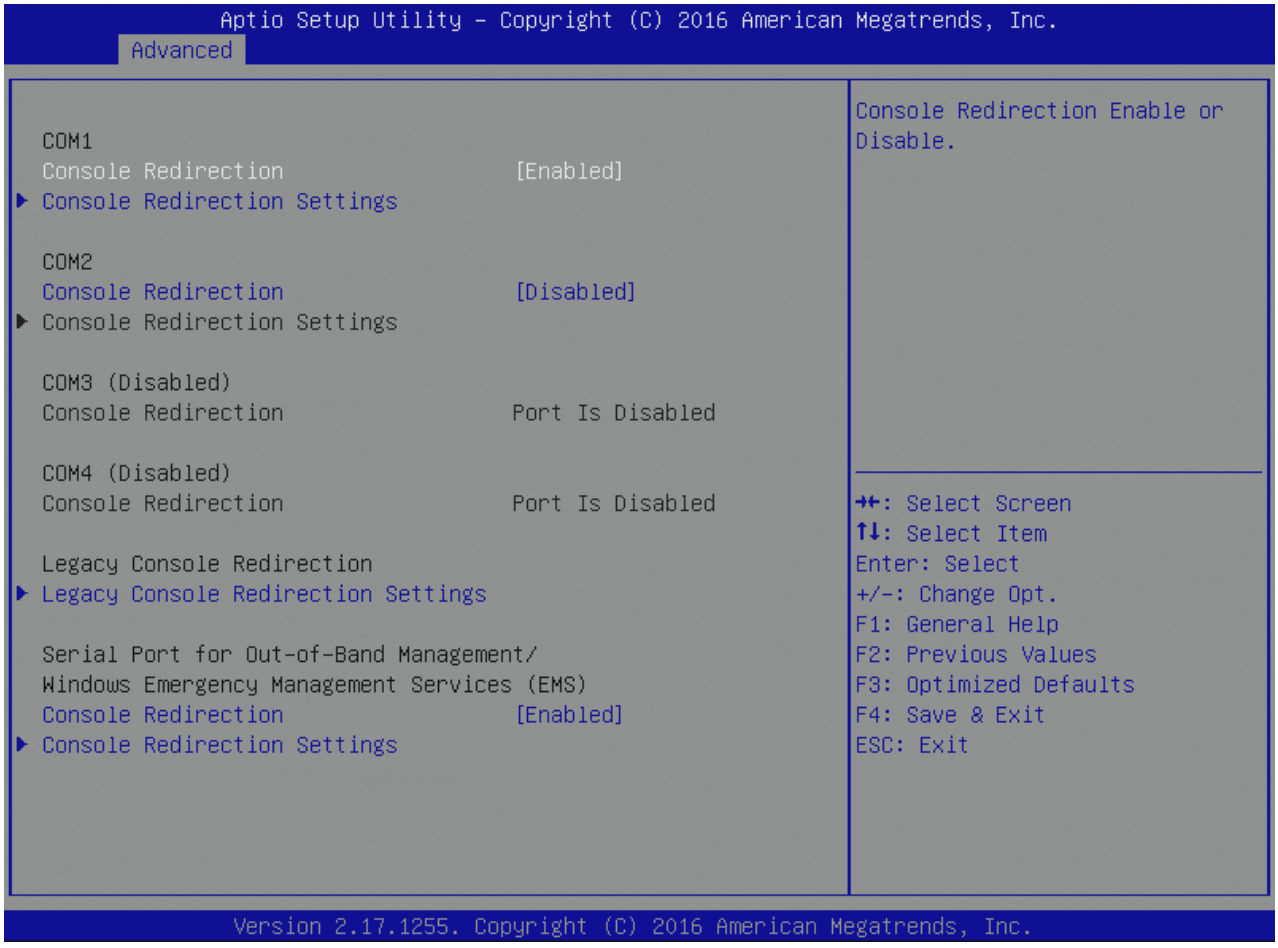


Table 57: Serial Port Console Redirection Features List

Feature	Options	Description
COM1 Console Redirection	Disabled **Enabled**	Console Redirection Enable or Disable.
COM2 Console Redirection	**Disabled** Enabled	Console Redirection Enable or Disable.
COM3 Console Redirection	**Disabled** Enabled	Console Redirection Enable or Disable.
COM4 Console Redirection	**Disabled** Enabled	Console Redirection Enable or Disable.
Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS) Console Redirection	Disabled **Enabled**	Console Redirection Enable or Disable.

6.5.2.18 Console Redirection Settings

Figure 31: Console Redirection Settings Menu Screen



Table 58: Console Redirection Settings Features List

Feature	Options	Description
Terminal Type	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	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	7 8	Data Bits
Parity	**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.

Feature	Options	Description
Stop Bits	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	**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 restart the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Sup	Disabled Enabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100×31	Disabled Manual	Enables or disables extended terminal resolution
Legacy OS Redirection Resolution	80x24 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIO	Always Enable BootLoader	The Settings specify if Bootloader is selected then legacy console redirection is disabled before booting to legacy OS. Default value is Always Enable which means Legacy console Redirection is enabled for Legacy OS.

6.5.2.19 Legacy Console Redirection Settings

Figure 32: Legacy Console Redirection Settings Menu Screen

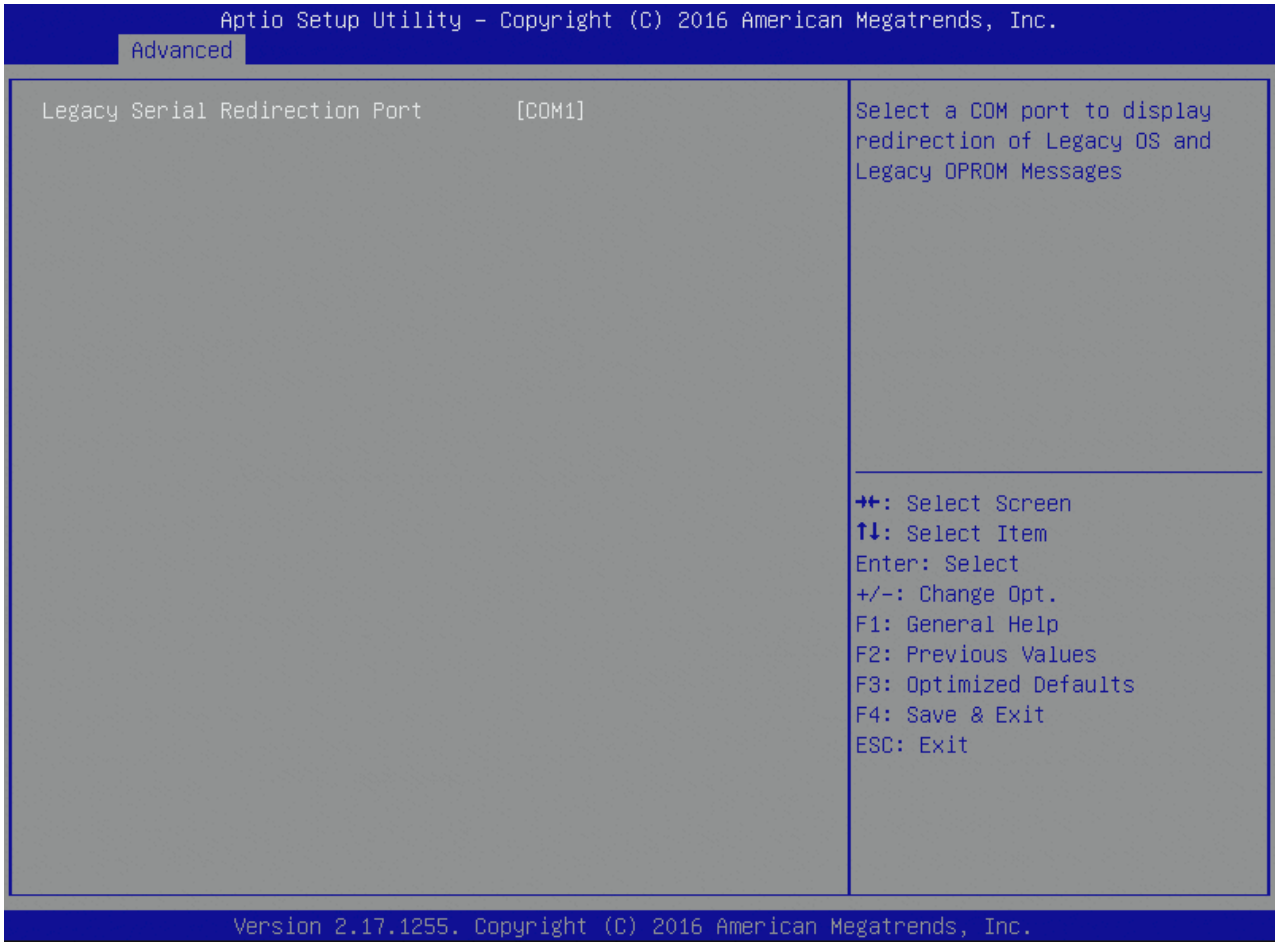


Table 59: Legacy Console Redirection Settings Features List

Feature	Options	Description
Legacy Serial Redirection Port	**COM1** COM2 COM3 (Disabled) COM4 (Disabled)	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages

6.5.2.20 Out-of-Band Management Console Redirection Settings

Figure 33: Out-of-Band Management Console Redirection Settings Menu Screen

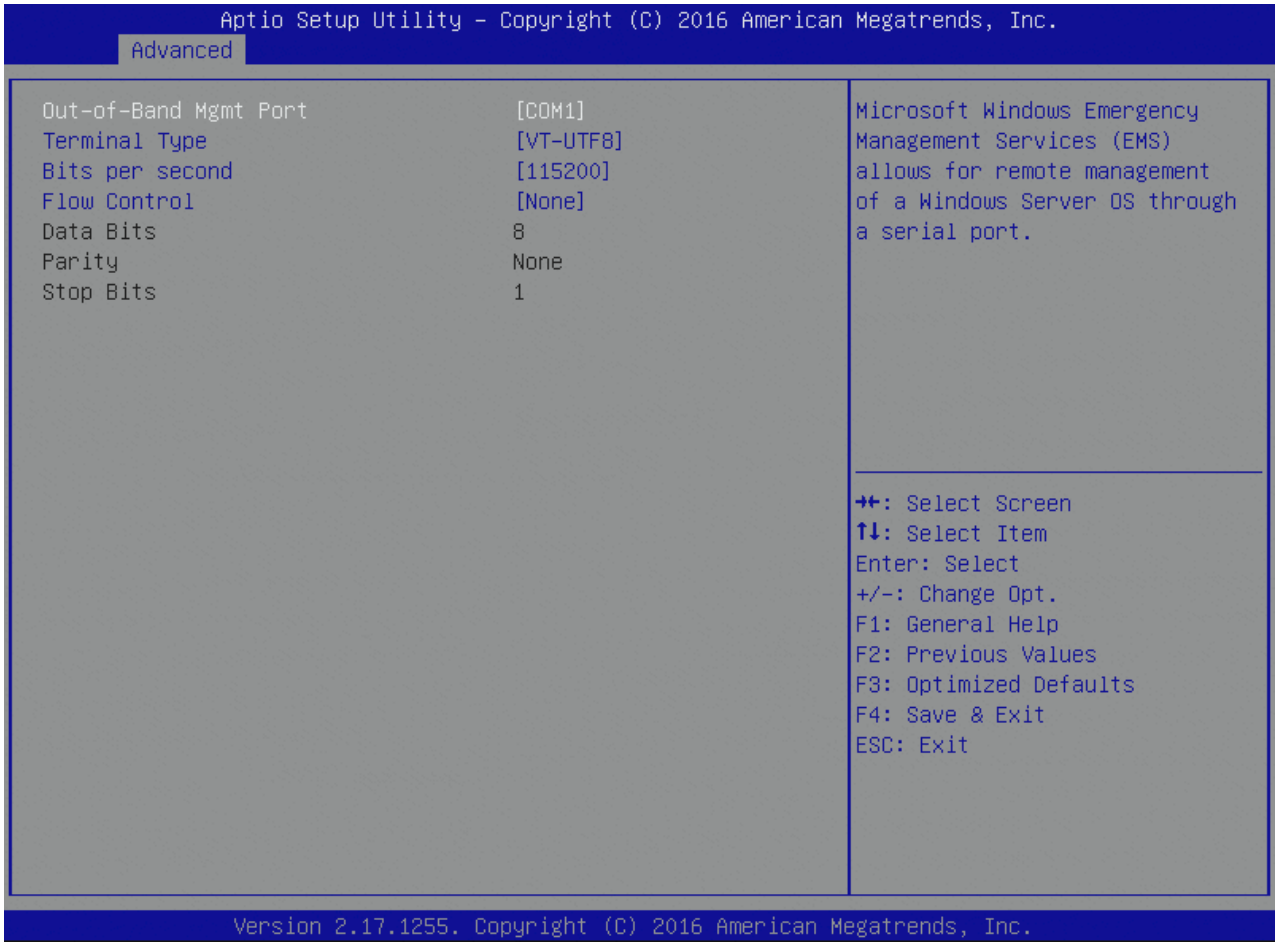


Table 60: Out-of-Band Management Console Redirection Settings Features List

Feature	Options	Description
Out-of-Band Mgmt Port	**COM1** COM2 COM3 (Disabled) COM4 (Disabled)	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.
Terminal Type	VT100 VT100+ **VT-UTF8** ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per second	9600 19200 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	None Hardware RTS/CTS Software Xon/Xoff	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 restart the flow. Hardware flow control uses two wires to send start/stop signals.

6.5.2.21 PCI Subsystem Settings

Figure 34: PCI Subsystem Settings Menu Screen

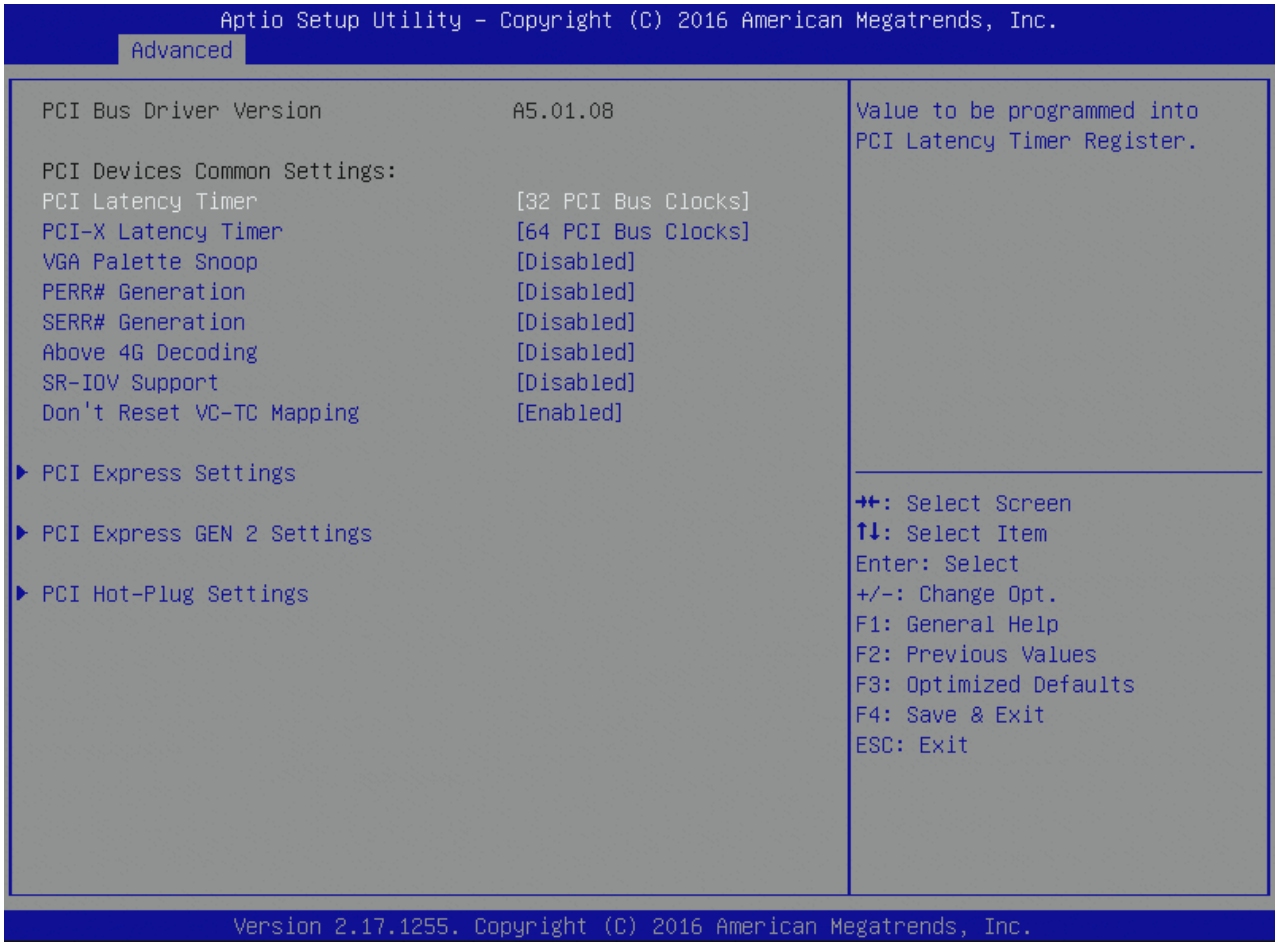


Table 61: PCI Subsystem Settings Features List

Feature	Options	Description
PCI Latency Timer	**32 PCI Bus Clocks** ... 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
PCI-X Latency Timer	... **64 PCI Bus Clocks** ... 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
VGA Palette Snoop	**Disabled** Enabled	Enables or Disables VGA Palette Registers Snooping.
PERR# Generation	**Disabled** Enabled	Enables or Disables PCI Device to Generate PERR#.
SERR# Generation	**Disabled** Enabled	Enables or Disables PCI Device to Generate SERR#.
Above 4G Decoding	Disabled Enabled	Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64bit PCI Decoding).

Feature	Options	Description
SR-IOV Support	Disabled Enabled	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.
Don't Reset VC-TC Mapping	Disabled **Enabled**	If system has Virtual Channels, Software can reset Traffic Class mapping through Virtual Channels, to it's default state. Setting this option to Enabled will not modify VC Resources.

6.5.2.22 PCI Express Settings

Figure 35: PCI Express Settings Menu Screen

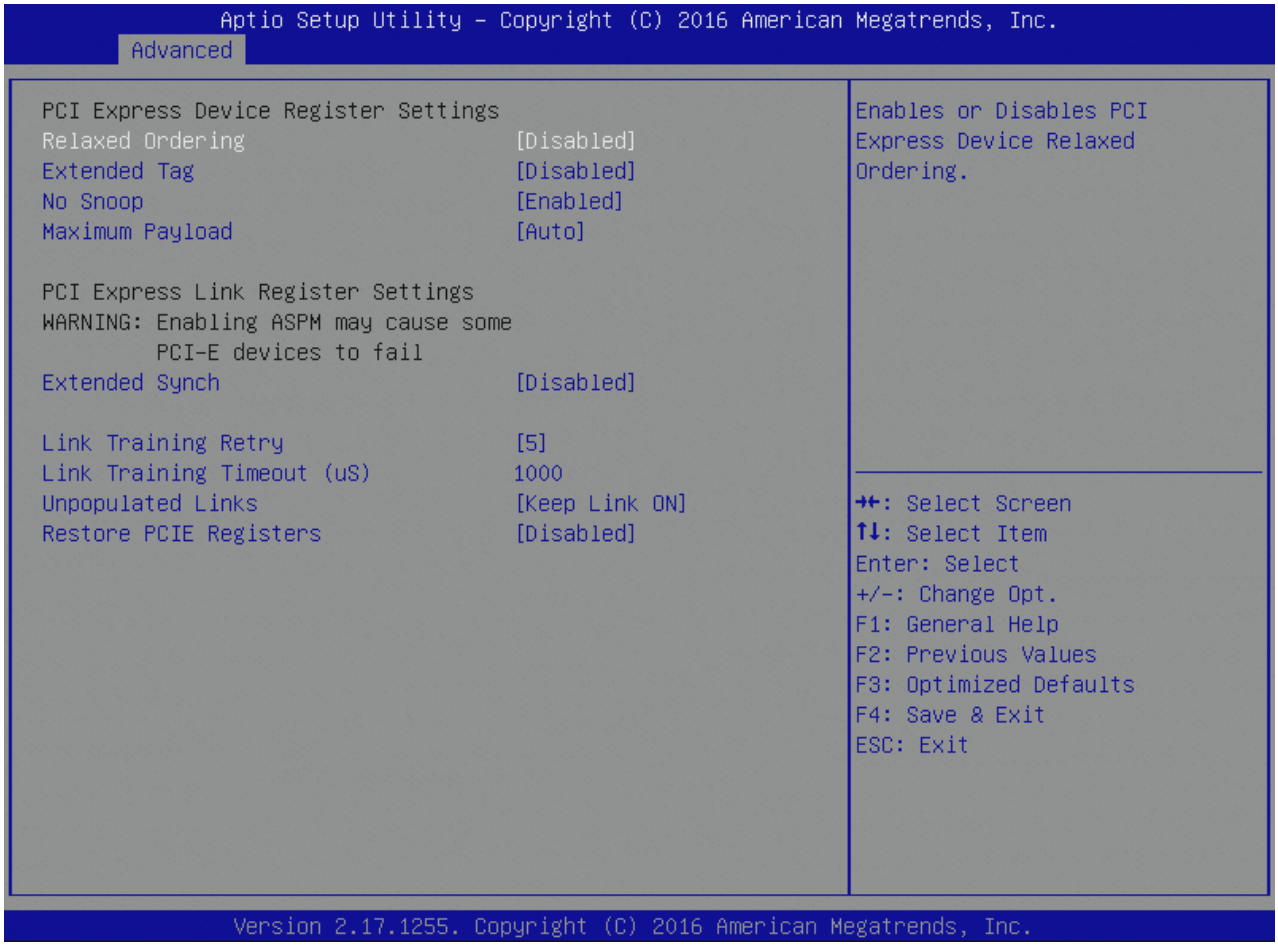


Table 62: PCI Express Settings Features List

Feature	Options	Description
Relaxed Ordering	**Disabled** Enabled	Enables or Disables PCI Express Device Relaxed Ordering.
Extended Tag	**Disabled** Enabled	If ENABLED allows Device to use 8-bit Tag field as a requester.
No Snoop	Disabled **Enabled**	Enables or Disables PCI Express No Snoop option.
Maximum Payload	**Auto** 128 Bytes … 2048 Bytes 4096 Bytes	Set Maximum Payload of PCI Express Device or allow System BIOS to select the value.
Extended Synch	Disabled Enabled	If ENABLED allows generation of Extended Synchronization patterns.
Link Training Retry	Disabled 2	Defines number of Retry Attempts software will take to retrain the link if previous training attempt was unsuccessful.

Feature	Options	Description
	3 **5**	
Link Training Timeout (µS)	1000	Defines number of Microseconds software will wait before polling 'Link Training' bit in Link Status register. Value range from 10 to 10000 µS.
Unpopulated Links	Keep Link ON Disable Link	In order to save power, software will disable unpopulated PCI Express links, if this option set to 'Disable Link'.
Restore PCIE Registers	**Disabled** Enabled	On non-PCI Express aware OS's (Pre Windows Vista) some devices may not be correctly reinitialized after S3. Enabling this restors PCI Express device configurations on S3 resume. Warning: Enabling this may cause issues with other hardware after S3 resume.

6.5.2.23 PCI Express Gen 2 Settings

Figure 36: PCI Express Gen 2 Settings Menu Screen

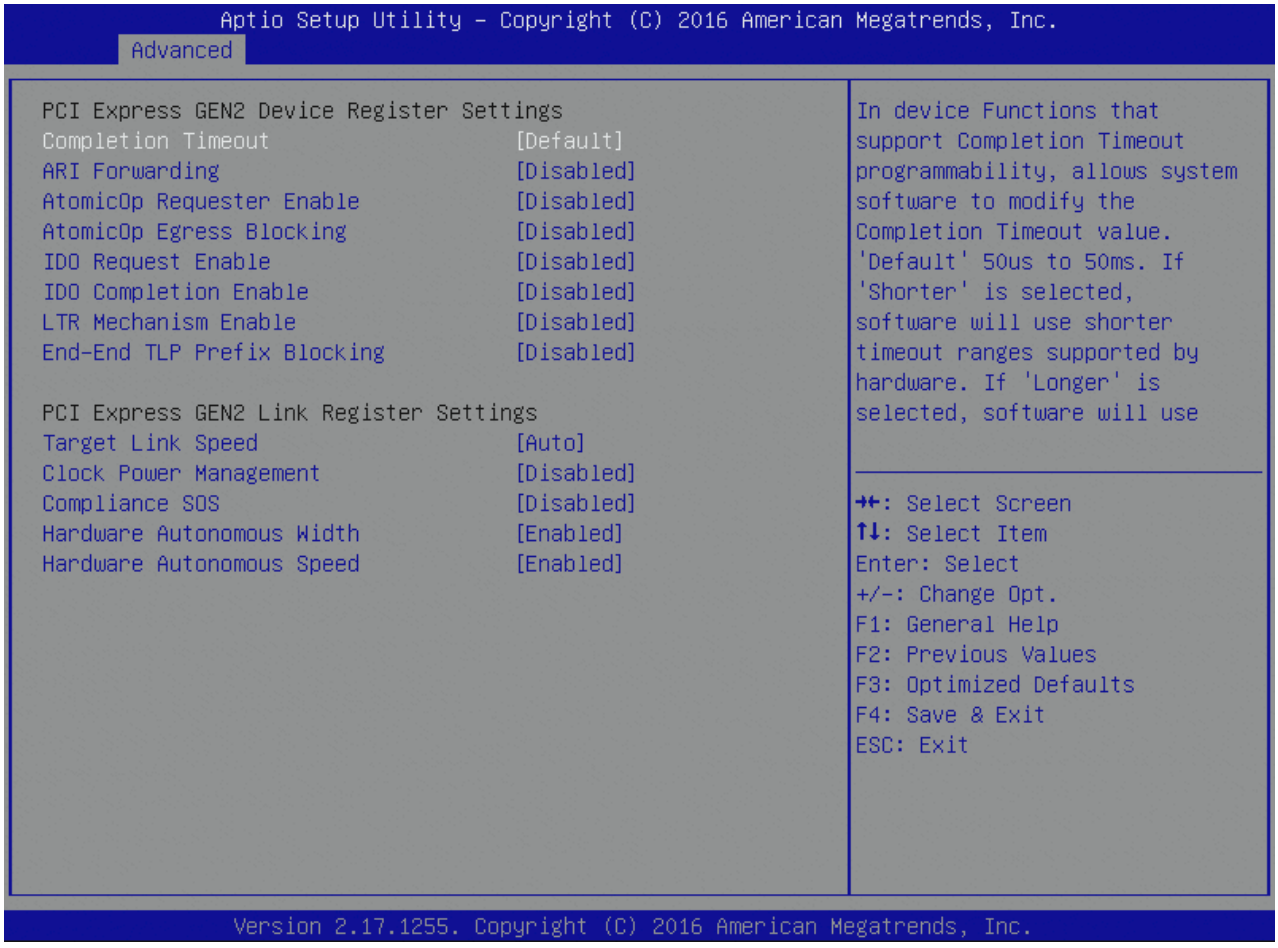


Table 63: PCI Express Gen 2 Settings Features List

Feature	Options	Description
Completion Timeout	**Default** Shorter Longer Disabled	In device Functions that support Completion Timeout programmability, allows system software to modify the Completion Timeout value. 'Default' 50us to 50ms. If 'Shorter' is selected, software will use shorter timeout ranges supported by hardware. If 'Longer' is selected, software will use longer timeout ranges.
ARI Forwarding	**Disabled** Enabled	If supported by hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number field being 0 enforcement when turning a type1 Configuration Request into a type0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port. Default value: Disabled
AtomicOp Requester Enable	Disabled Enabled	If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if Bus Master Enable bit is in the Command Register Set.
AtomicOp Egress Blocking	Disabled Enabled	If supported by hardware and set to 'Enabled', outbound AtomicOp Requests via Egress Ports will be blocked.

Feature	Options	Description
IDO Request Enable	Disabled Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated.
IDO Completion Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated.
LTR Mechanism Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this enables the Latency Tolerance Reporting (LTR) Mechanism.
End-End TLP Prefix Blocking	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this function will block forwarding of TLPs containing End-End TLP Prefixes.
Target Link Speed	**Auto** Force to 2.5 GT/s Force to 5.0 GT/s	If supported by hardware and set to 'Force to 2.5 GT/s' for Downstream Ports, this sets an upper limit on Link operational speed by restricting the values advertised by the Upstream component in its training sequences. When 'Auto' is selected HW initialized data will be used.
Clock Power Management	**Disabled** Enabled	If supported by hardware and set to 'Enabled', the device is permitted to use CLKREQ# signal for power management of Link clock in accordance to protocol defined in appropriate for factor specification.
Compliance SOS	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this will force LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern.
Hardware Autonomous Width	**Enabled** Disabled	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation.
Hardware Autonomous Speed	**Enabled** Disabled	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link speed except speed rate reduction for the purpose of correcting unstable link operation.

6.5.2.24 PCI Hot-Plug Settings

Figure 37: PCI Hot-Plug Settings Menu Screen

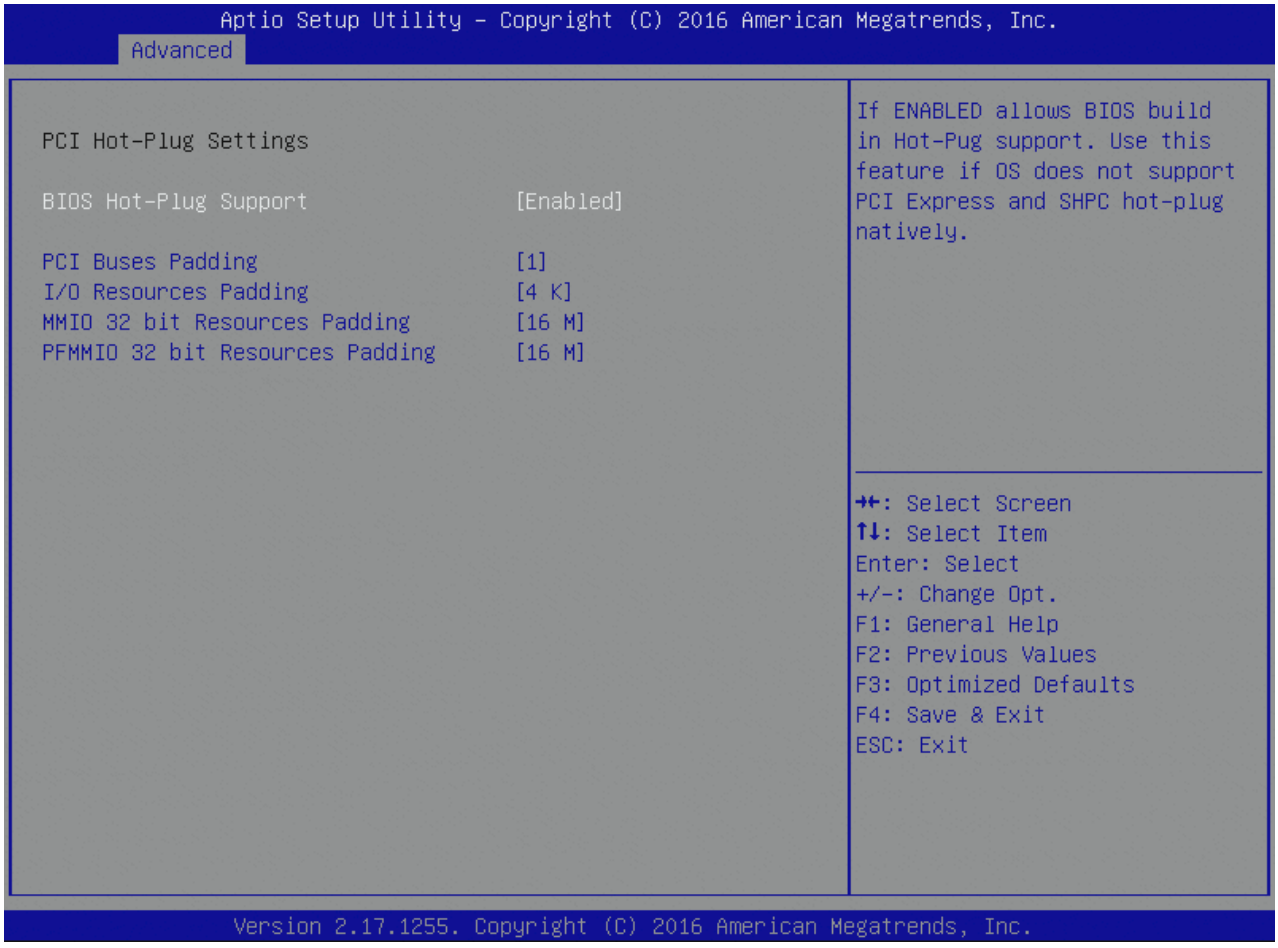


Table 64: PCI Hot-Plug Settings Features List

Feature	Options	Description
BIOS Hot-Plug Support	Disabled **Enabled**	If ENABLED allows BIOS build in Hot-Pug support. Use this feature if OS does not support PCI Express and SHPC hot-plug natively.
PCI Buses Padding	**1** 2 3 4 5	Padd PCI Buses behind the bridge for Hot-Plug.
I/O Resources Padding	**4 K** 8 K 16 K 32 K	Padd PCI I/O Resources behind the bridge for Hot-Plug.
MMIO 32 bit Resources Padding	… 16 M …	Padd PCI MMIO 32-bit Resources behind the bridge for Hot-Plug.
PFMMIO 32 bit Resources Padding	… 16 M …	Padd PCI MMIO 32-bit Prefetchable Resources behind the bridge for Hot-Plug.

6.5.2.25 Network Stack Configuration

Figure 38: Network Stack Configuration Menu Screen

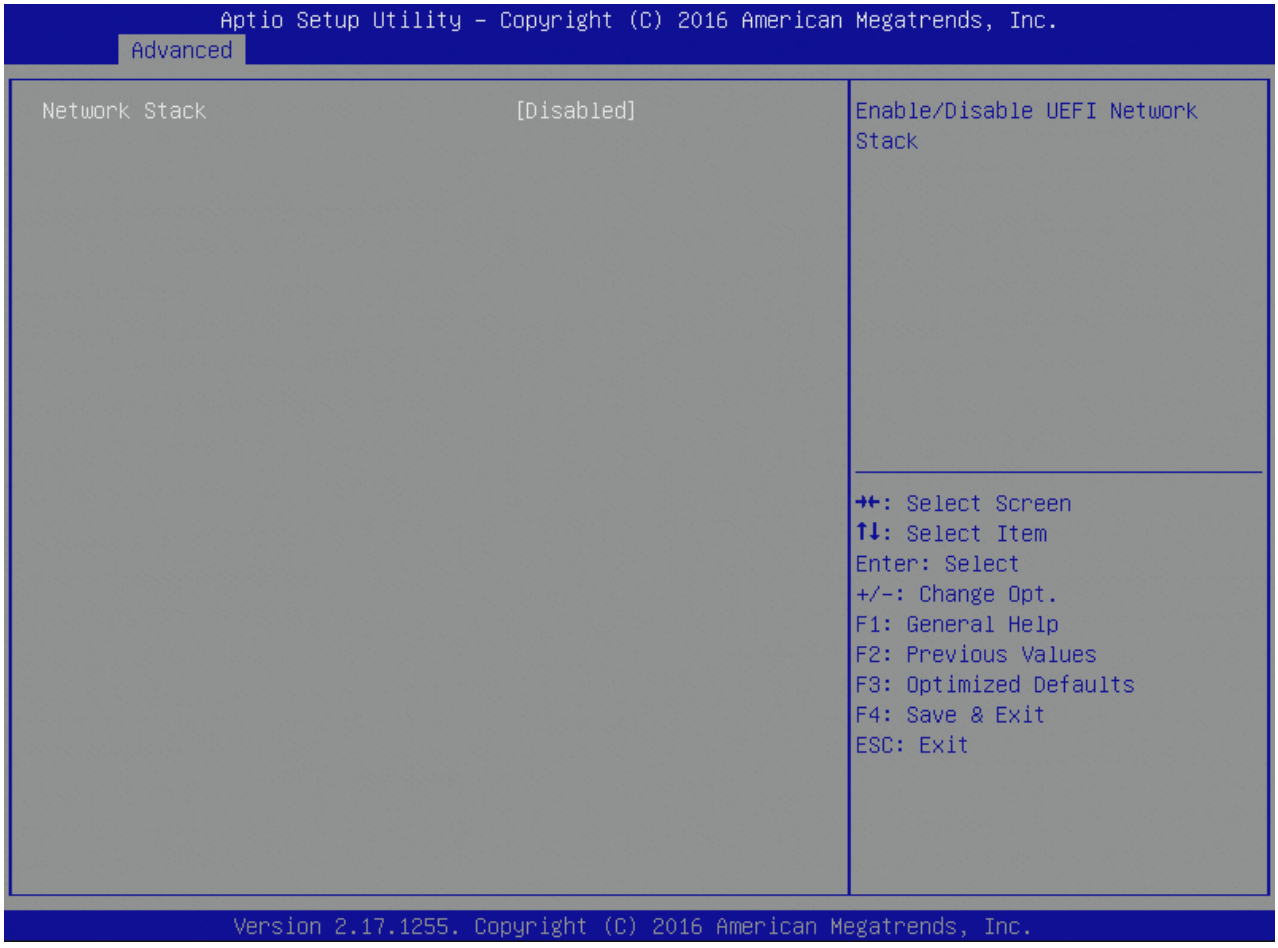


Table 65: Network Stack Configuration Features List

Feature	Options	Description
Network Stack	**Disabled** Enabled	Enable/Disable UEFI Network Stack

6.5.2.26 CSM Configuration

Figure 39: CSM Configuration Menu Screen

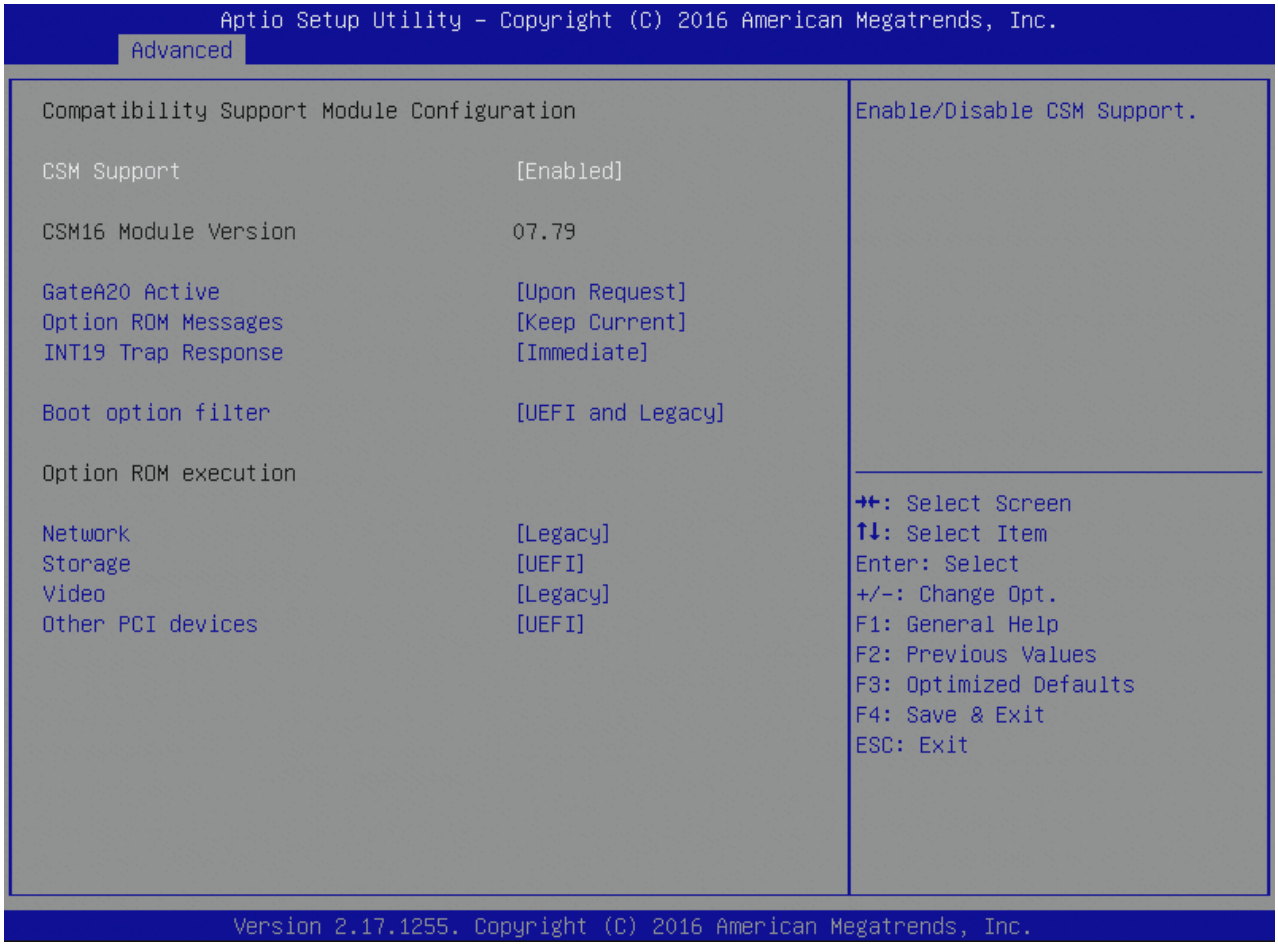


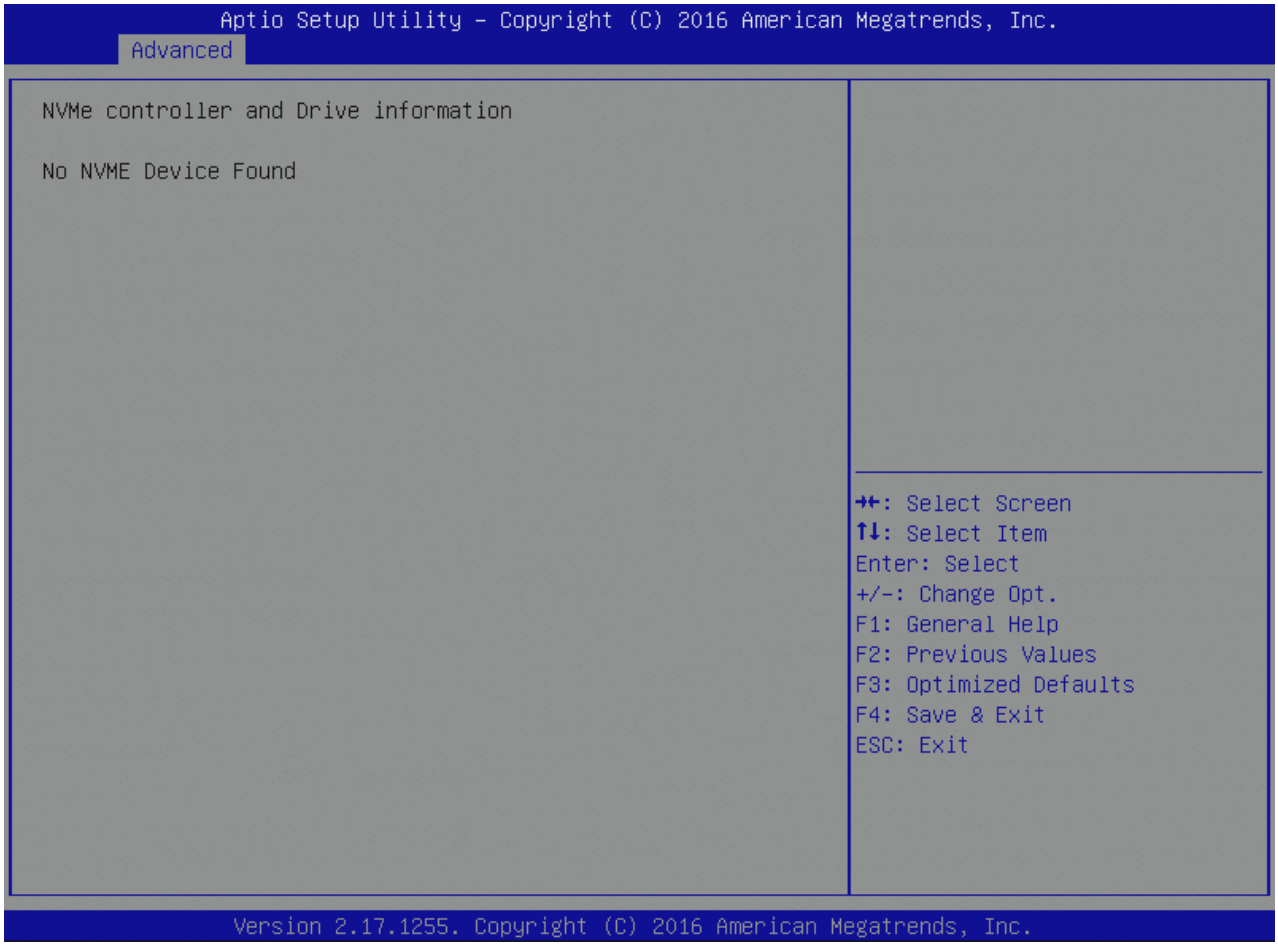
Table 66: CSM Configuration Features List

Feature	Options	Description
CSM Support	Disabled **Enabled**	Enables/Disables CSM Support.
GateA20 Active	Upon Request Always	UPN 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	Keep Current Force BIOS	Set display mode for Option ROM
INT19 Trap Response	**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	**UEFI and Legacy** Legacy only UEFI only	This option controls Legacy/UEFI ROMs priority
Network	Do not launch UEFI **Legacy**	Controls the execution of UEFI and Legacy PXE OpROM

Feature	Options	Description
Storage	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy Storage OpROM
Video	Do not launch UEFI **Legacy**	Controls the execution of UEFI and Legacy Video OpROM
Other PCI devices	Do not launch **UEFI** Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video

6.5.2.27 NVMe Configuration

Figure 40: NVMe Configuration Menu Screen



6.5.2.28 Advanced USB Configuration

Figure 41: Advanced USB Configuration Menu Screen

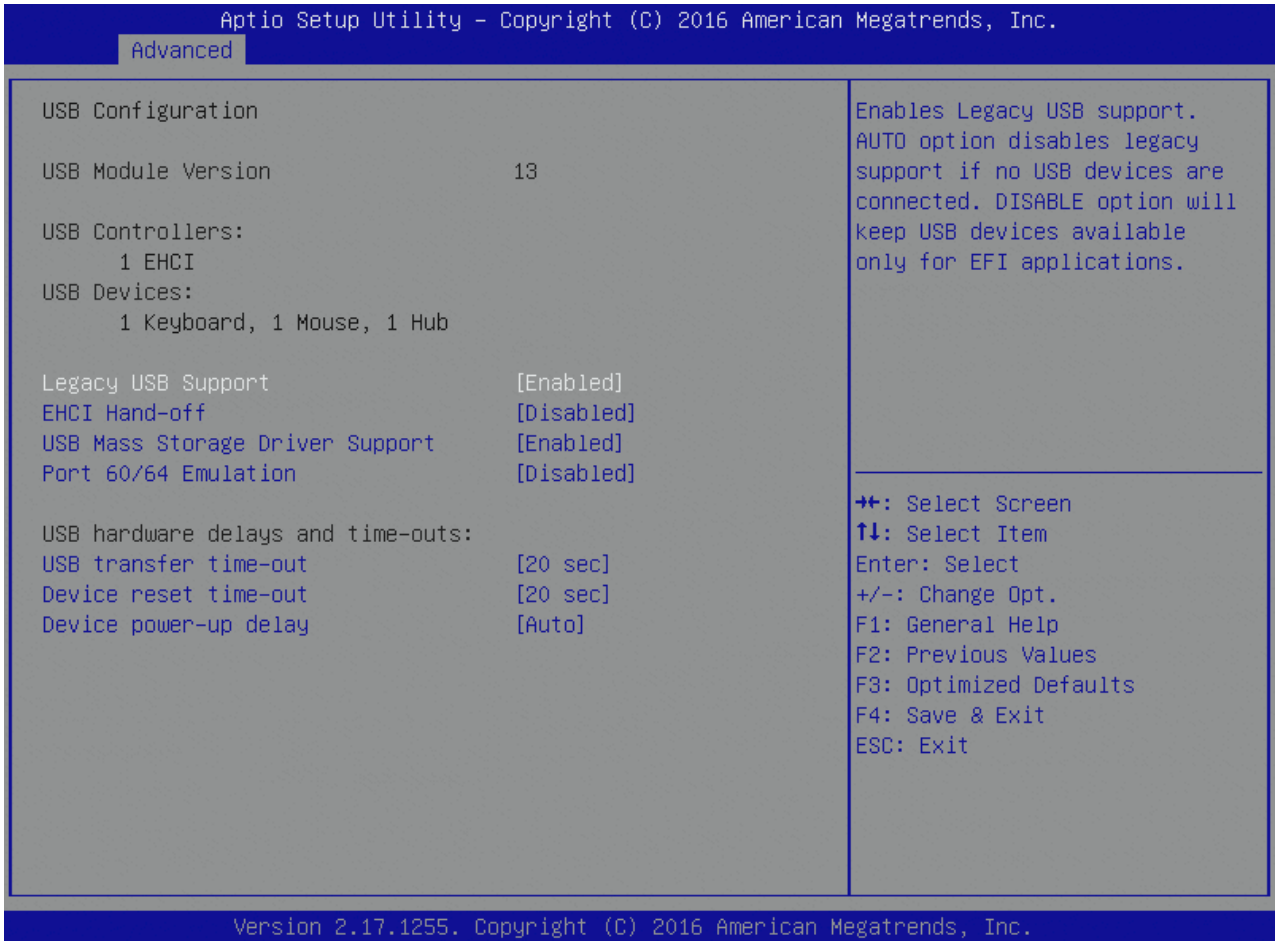
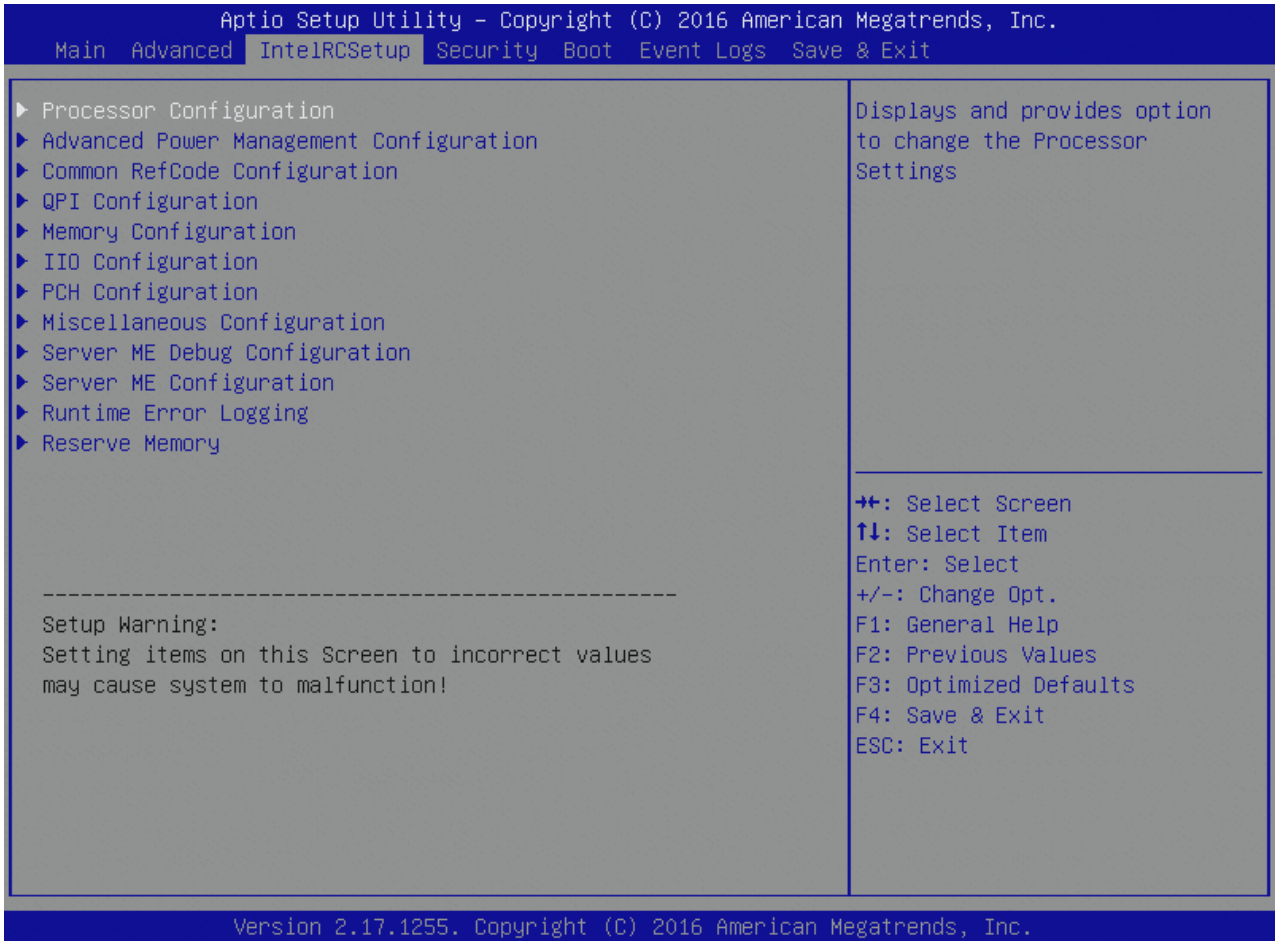


Table 67: Advanced USB Configuration Features List

Feature	Options	Description
Legacy USB Support	**Enabled** Disabled AUTO	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.
EHCI Hand-off	Disabled Enabled	This is a workaround for OSes without EHCI hand-off Support. The EHCI ownership change should be claimed by EHCI driver.
USB Mass Storage Driver Support	Disabled Enabled	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation	**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 transfer time-out	1sec … **20sec**	The time-out value for Control, Bulk and Interrupt transfers.
Device reset time-out	10sec **20sec** …	USB mass storage device Start Unit command time-out.
Device power-up delay	**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 100ms, for a Hub port the delay is taken from Hub descriptor.

6.5.3 Intel RC Setup

Figure 42: Intel RC Setup Menu Screen



6.5.3.1 Processor Configuration

Figure 43: Processor Configuration Menu Screen

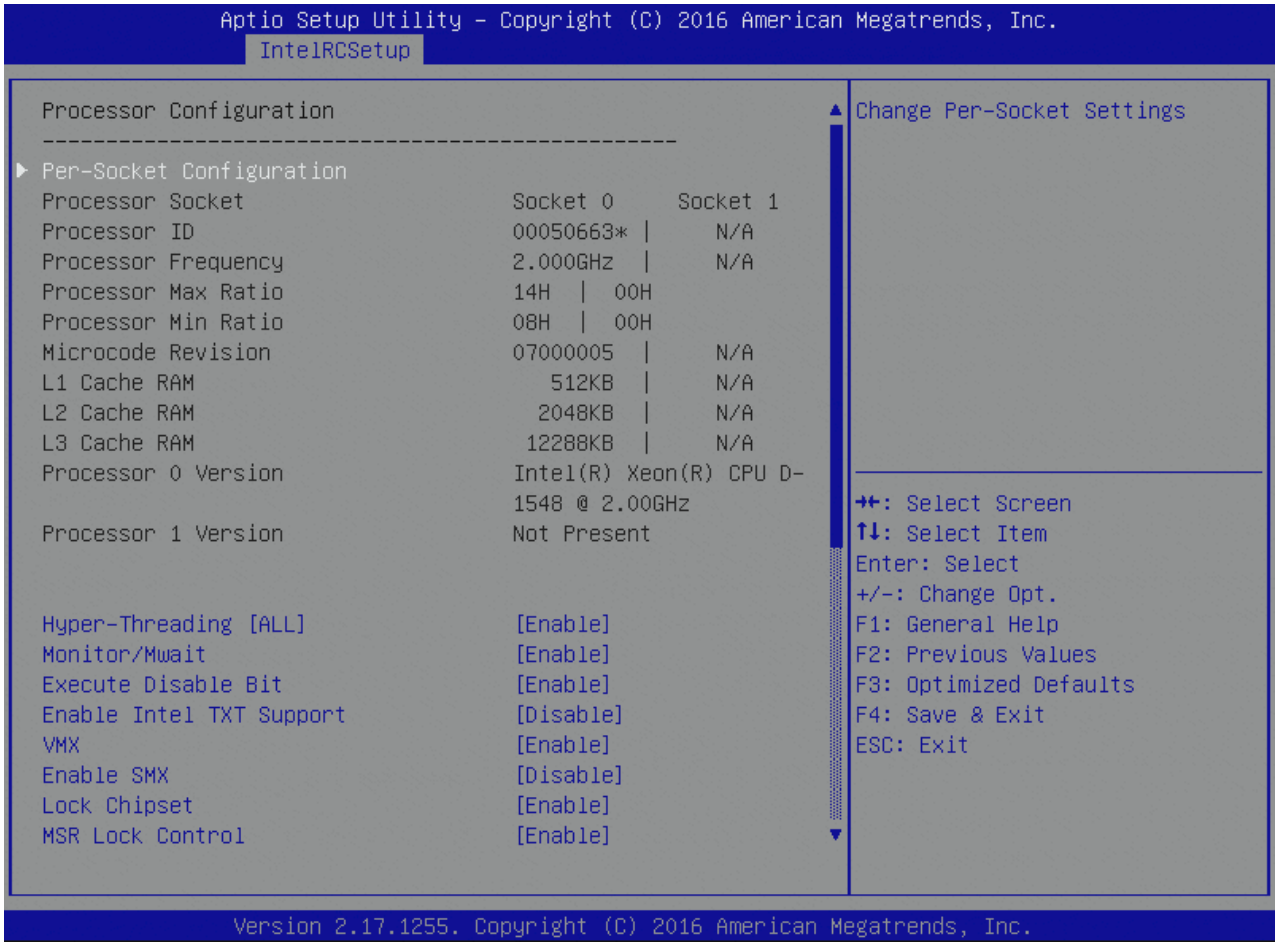


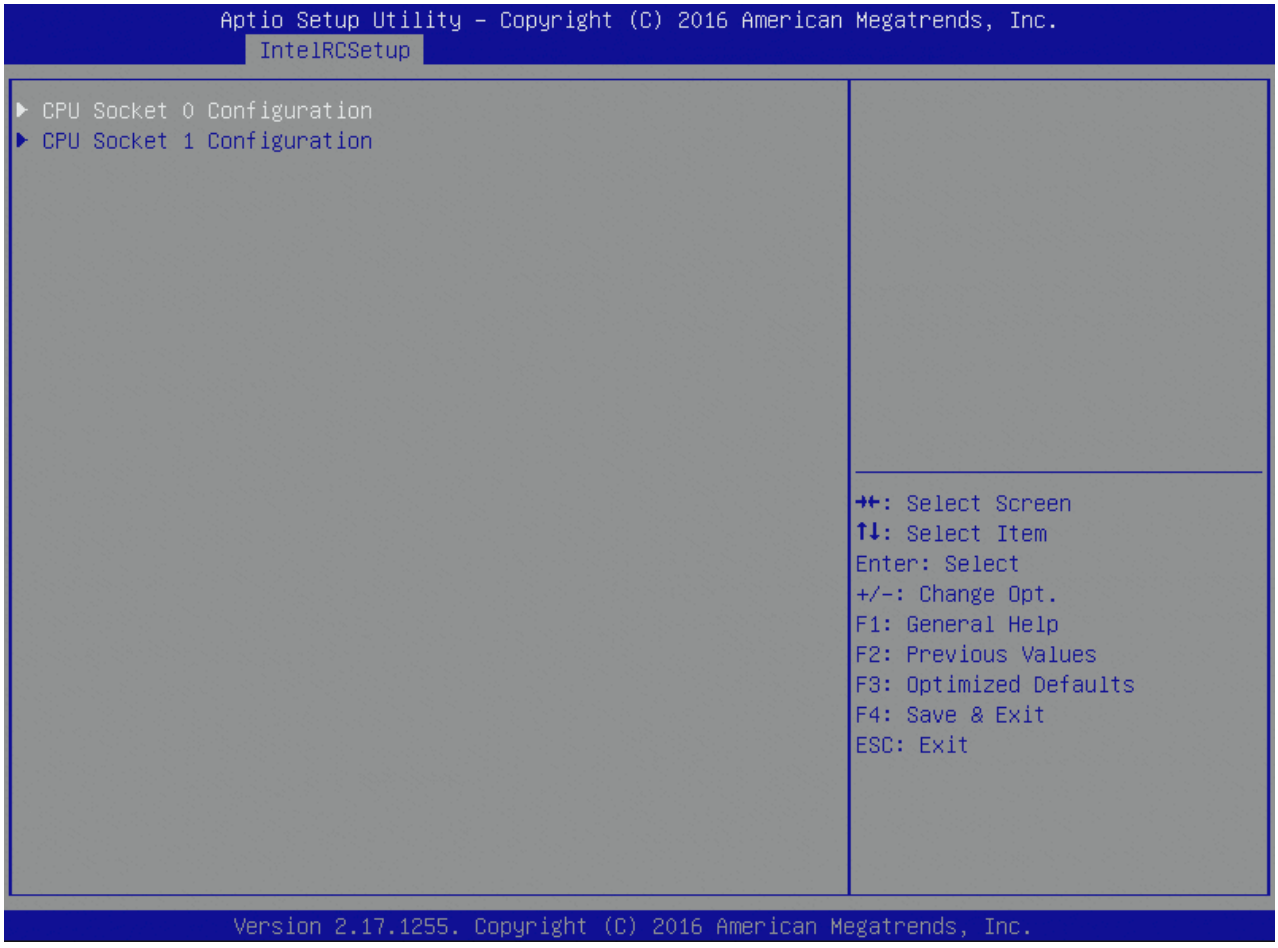
Table 68: Processor Configuration Features List

Feature	Options	Description
Hyper-Threading (ALL)	Disabled **Enabled**	Enables Hyper Threading (software Method to Enable/Disable Logical Processor threads.
Monitor/Mwait	Disabled **Enabled**	Enable or Disable the Monitor/Mwait instruction
Execute Disable Bit	Disabled **Enabled**	When disabled, forces the XD feature flag to always return 0.
Enable Intel TXT Support	**Disabled** Enabled	Enables Intel Trusted Execution Technology Configuration. Please disable "EV DFX Features" when TXT is enabled.
VMX	Disabled **Enabled**	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	**Disabled** Enabled	Enables Safer Mode Extensions.
Lock Chipset	Disabled **Enabled**	Lock or Unlock chipset

Feature	Options	Description
MSR Lock Control	Disabled **Enabled**	Enable – MSR 3Ah, MSR 0E2h and CSR 80h will locked. Power Good reset os needed to remove lock bits.
PPIN Control	Unlock/Disabled **Unlock/Enabled**	Unlock and Enable/Disable PPIN Control
DEBUG INTERFACE	Disable Enable **Auto**	MSR 0C80h bit[0], When set enables the debug features.
Hardware Prefetcher	**Enable** Disable	= MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetch	**Enable** Disable	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	**Enable** Disable	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[2]).
DCU IP Prefetcher	**Enable** Disable	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[3]).
DCU Mode	32KB 8Way Without ECC 16KB 4Way With ECC	MSR 31h Bit[0] – A write of 1 selects the DCU mode as 16KB 4-way with ECC.
Direct Cache Access (DCA)	Disable Enable **Auto**	Enables Direct Cache Access
DCA Prefetch Delay	… **32** …	DCA Prefetch Delay Help
X2aPIC	**Disable** Enable	Enable/disable extended APIC support
X2aPIC_OPT_OUT Flag	Disabled Enabled	Enable/disable X2aPIC_OPT_OUT support flag
AES-NI	**Disabled** Enabled	
Down Stream PECI	**Disabled** Enabled	Enable PCIe Down Stream PECI Write
IIO LLC Ways [19:0] (Hex)	0	MSR CBO_SLICEO_CR_IIO_LLC_WAYS bitmask
QLRU Config [63:32] (Hex)	0	VIRTUAL_MSR _CR_QLRU_CONFIG bitmask
QLRU Config [31:0] (Hex)	0	VIRTUAL_MSR _CR_QLRU_CONFIG bitmask
SMM Save State	Enable **Disable**	Enable or Disable the SMM Save State Feature
Targeted Smi	Enable **Disable**	Enable or Disable Targeted Smi Feature

6.5.3.2 Pre-Socket Configuration

Figure 44: Pre-Socket Configuration Menu Screen



6.5.3.3 CPU Socket Configuration

Figure 45: CPU Socket Configuration Menu Screen

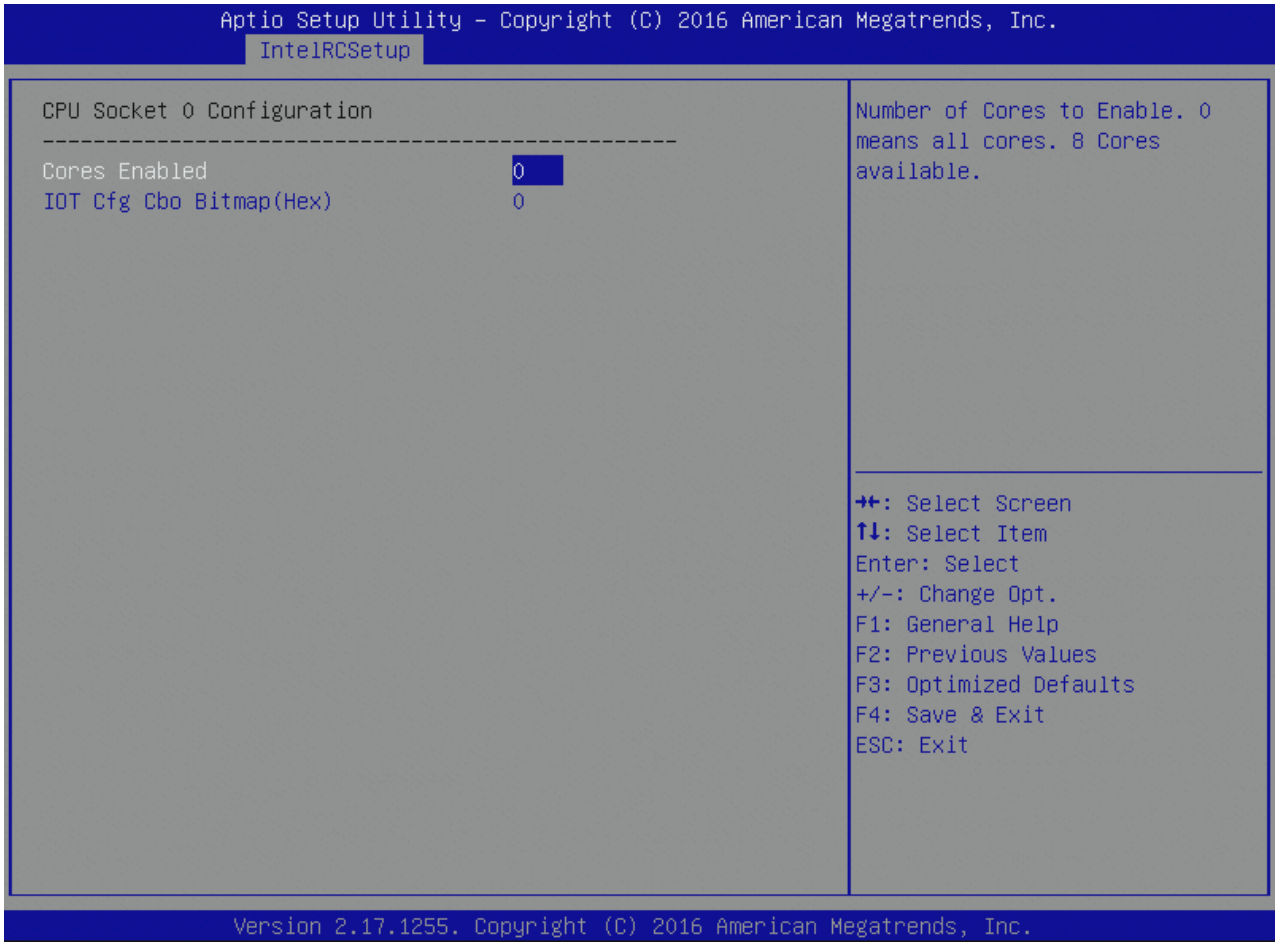


Table 69: CPU Socket Configuration Features List

Feature	Options	Description
Cores Enabled	0	Number of Cores to Enable. 0 means all cores. 8 Cores available.
IOT Cfg Cbo Bitmap(Hex)	0	Each bit enables IOT/OCLA for a CBo.

6.5.3.4 Advanced Power Management Configuration

Figure 46: Advanced Power Management Configuration Menu Screen

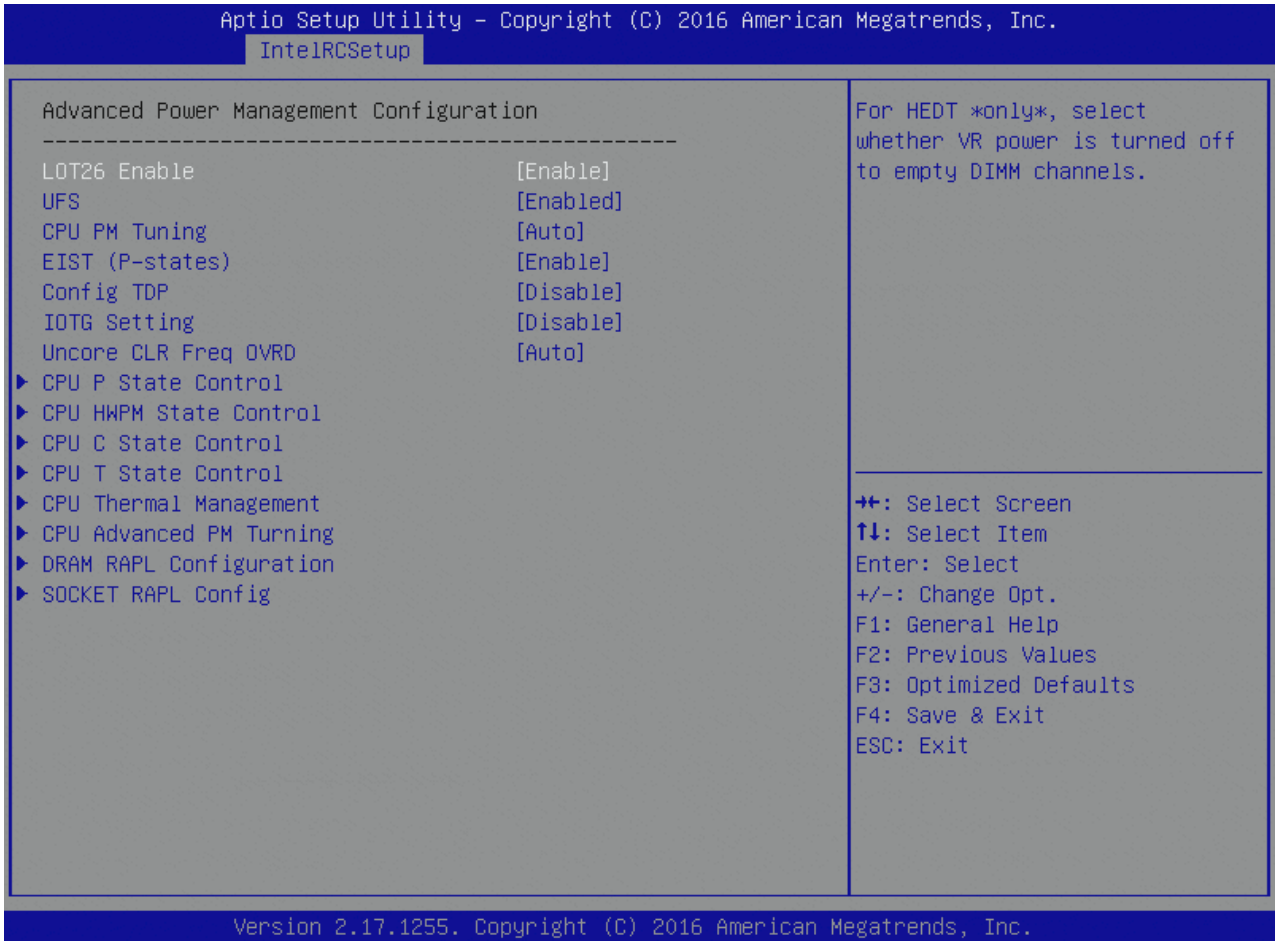


Table 70: Advanced Power Management Configuration Features List

Feature	Options	Description
LOT26 Enable	Disable **Enable**	For HEDT *only*, select whether VR power is turned off to empty DIMM channels.
UFS	**Enabled** Disabled	Setting in PCU_MISC_CONFIG Bit[28]
CPU PM Tuning	**Auto** Manual	If selected as 'AUTO', all bits in MSR 1FCh keeping value as PO.
EIST (P-states)	Disable **Enable**	When enabled, OS sets CPU frequency according load. When disabled, CPU frequency is set at max non-turbo.
Config TDP	**Disable** Enable	Option to disable/enable Config TDP
IOTG Setting	**Disable** Enable	IOTG Setting via sticky scratch pad register
Uncore CLR Freq OVRD	**Auto** Manual	Override Uncore max CLR Freq ratio programming to MSR 0x620 bits[6:0]

6.5.3.5 CPU P State Control

Figure 47: CPU P State Control Menu Screen

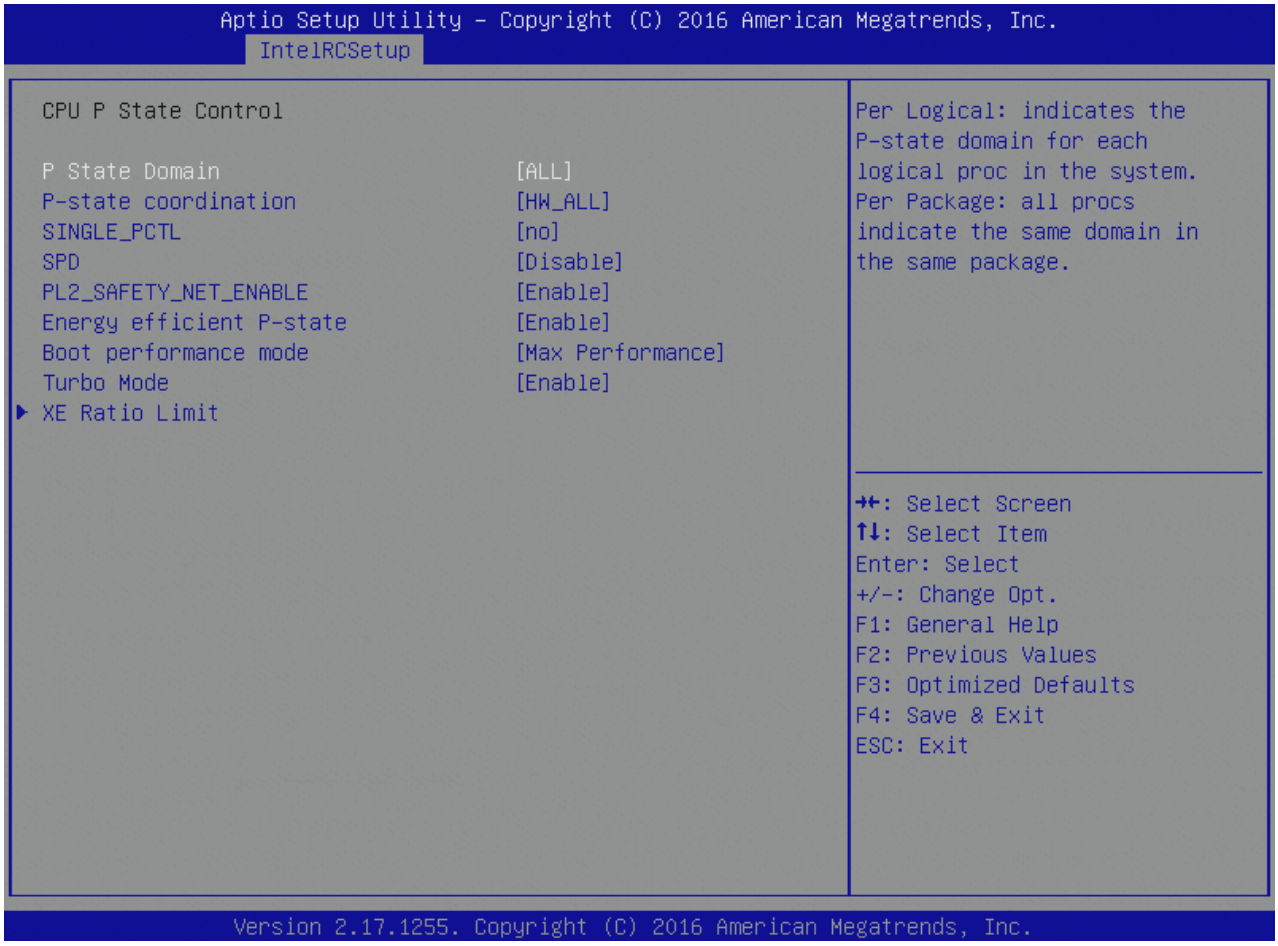


Table 71: CPU P State Control Features List

Feature	Options	Description
P State Domain	**ALL** ONE	Per Logical: indicates the P-state domain for each logical proc in the system. Per Package: all procs indicate the same domain in the same package.
P-state coordination	**HW_ALL** SW_ALL SW_ANY	HW_ALL (hardware) coordination is recommended over SW_ALL an SW_ANY (software coordination).
SINGLE_PCTL	**no** yes	MSR_CR_MISC_PWR_MGMT 0x1AA Bit[0]: SINGLE_PCTL_EN
SPD	**Disable** Enable	PCU_MISC_CONFIG Bit[30]: SPD
PL2_SAFETY_NET_ENABLE	Disable **Enable**	PCU_MISC_CONFIG Bit[1]: PL2_SAFETY_NET_ENABLE
Energy efficient P-state	Disable **Enable**	Enable/Disable Energy efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 EAX[3] will read 0 indicating nosupport for Energy Efficient policy setting. When set to 1 willenable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Function 6

Feature	Options	Description
		EAX[3] will read 1 indicating Energy EfficientPolicy setting is supported.
Boot performance mode	Max Performance Max Efficient	Select the performance state that the BIOS will set before OS handoff.
Turbo Mode	Disable **Enable**	Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceed CPU defined limits.

6.5.3.6 XE Ratio Limit

Figure 48: XE Ratio Limit Menu Screen

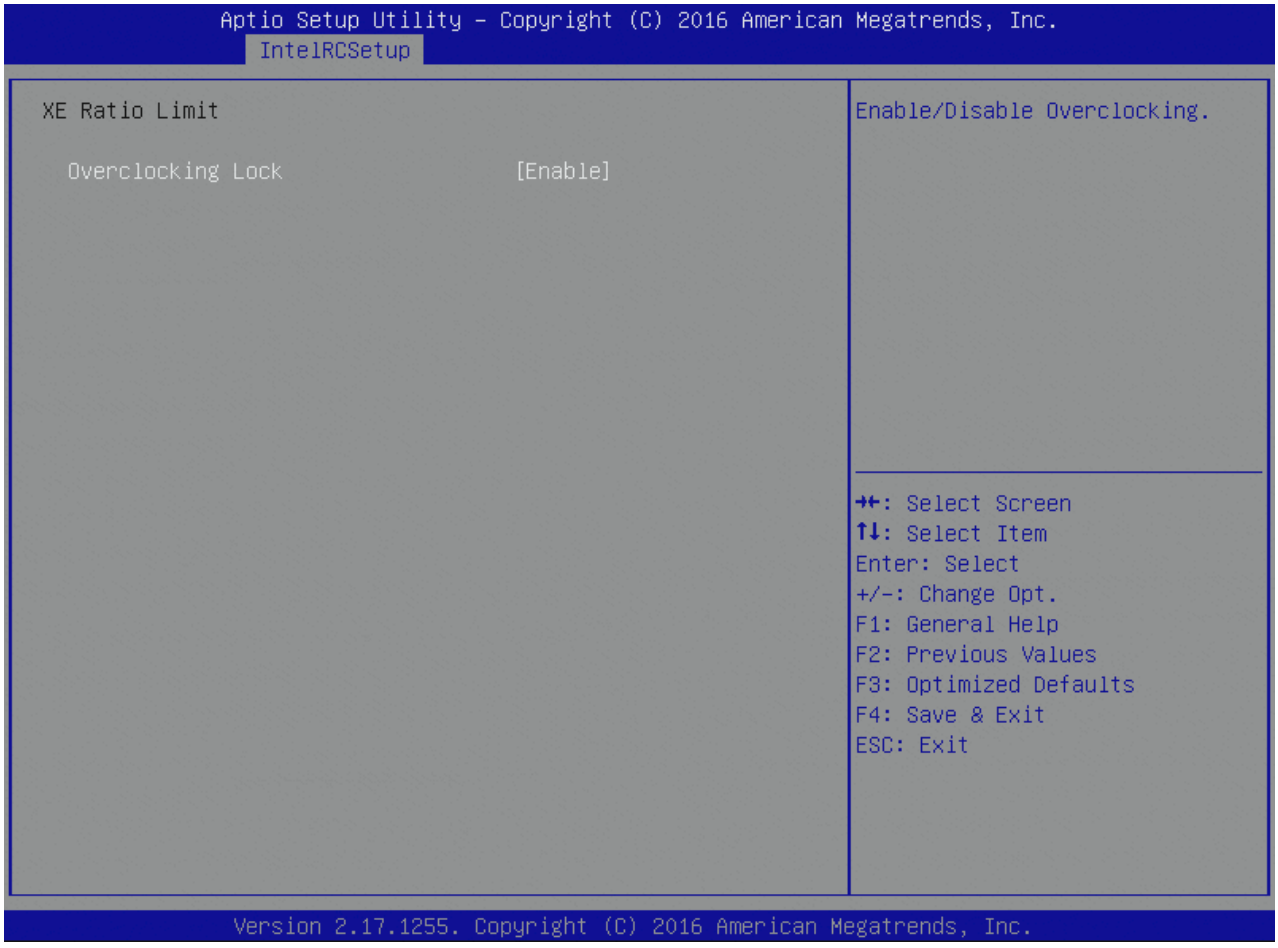


Table 72: XE Ration Limit Features List

Feature	Options	Description
Overclocking Lock	Disable **Enable**	Enable/Disable Overclocking.

6.5.3.7 CPU HWPM State Control

Figure 49: CPU HWPM State Control Menu Screen

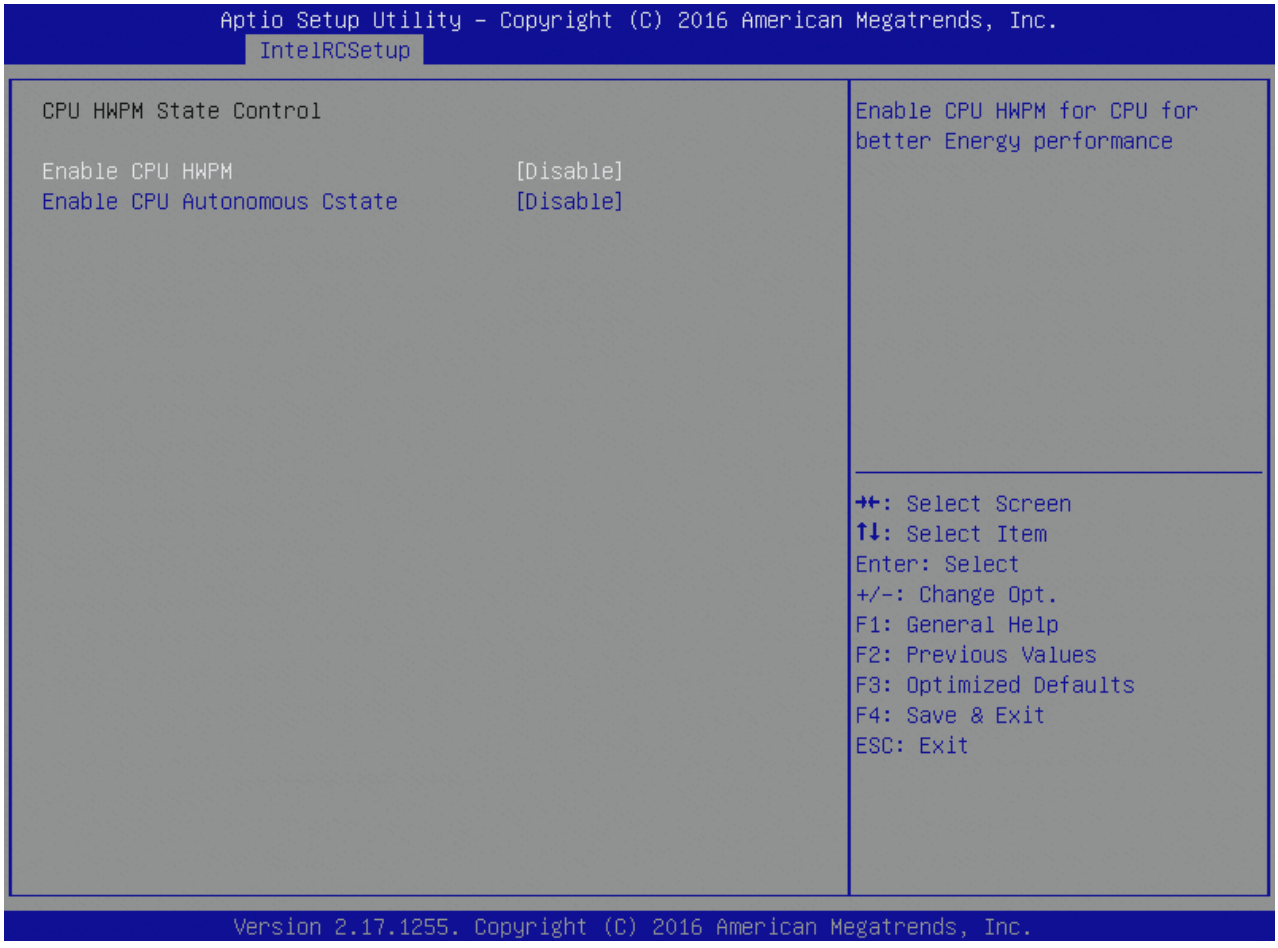


Table 73: CPU HWPM State Control Features List

Feature	Options	Description
Enable CPU HWPM	**Disable** HWPM NATIVE MODE HWPM OOB MODE	Enable CPU HWPM for CPU for better Energy performance
Enable CPU Autonomous Cstate	**Disable** Enable	Enable CPU Autonomous Cstate which is CPU converst HALT instruction to MWAIT

6.5.3.8 CPU C State Control

Figure 50: CPU C State Control Menu Screen

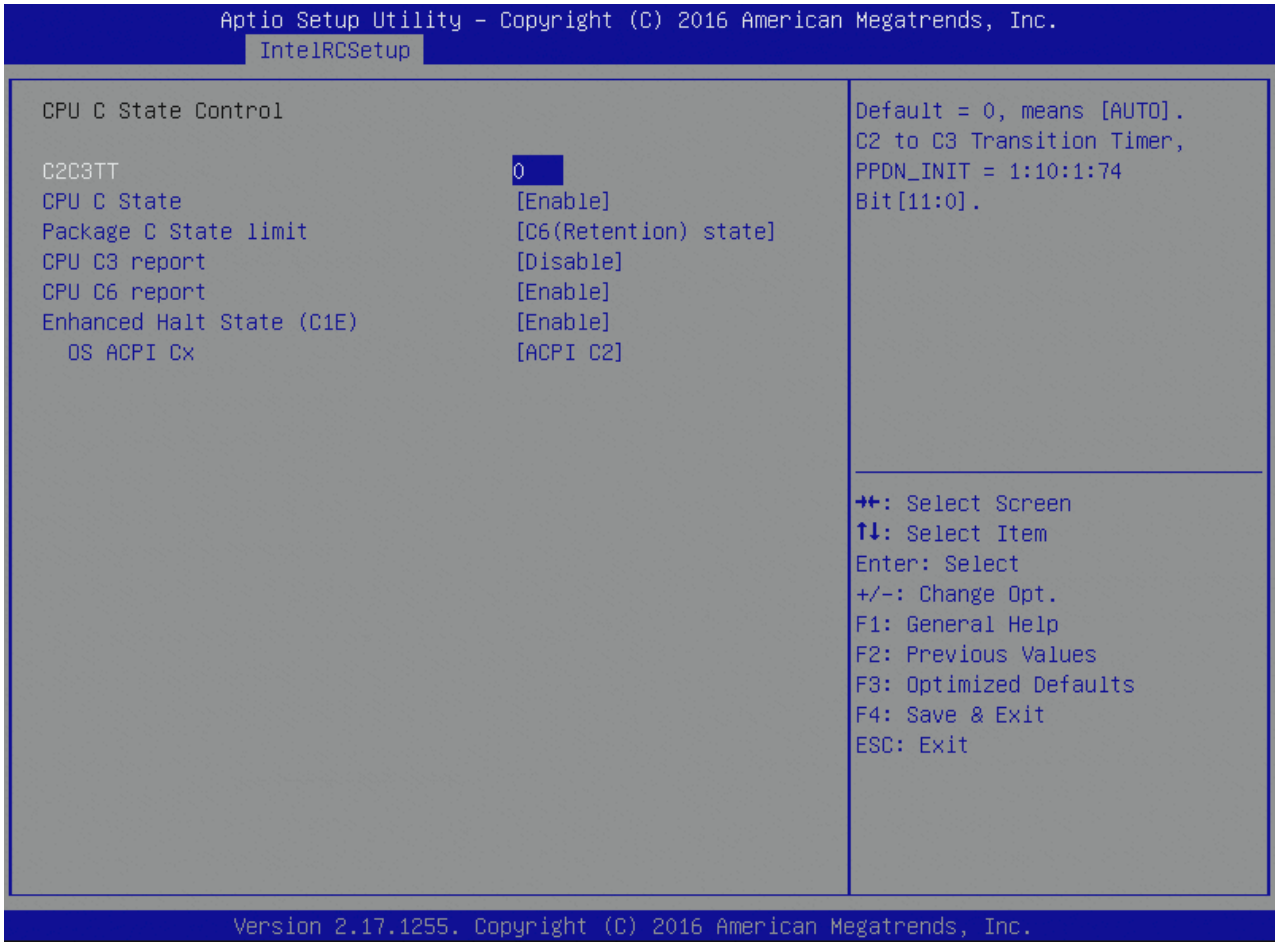


Table 74: CPU C State Control Features List

Feature	Options	Description
C2C3TT	0	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].
CPU C State	Disable **Enable**	Enables the Enhanced Cx state of the CPU, takes effect after reboot.
Package C State limit	C0/C1 state C2 state C6(non Retention) state **C6(Retention) state** No Limit	Package C State limit
CPU C3 report	**Disable** Enable	Enable/Disable CPU C3(ACPI C2) report to OS. Recommended to be disabled.
CPU C6 report	Disable **Enable**	Enable/Disable CPU C6(ACPI C2) report to OS Recommended to be enabled.
Enhanced Halt State (C1E)	Disable **Enable**	Enables the Enhanced C1E state of the CPU, takes effect after reboot.
OS ACPI Cx	ACPI C2	Report CC3/CC6 to OS ACPI C2 or ACPI C3

6.5.3.9 CPU T State Control

Figure 51: CPU T State Control Menu Screen

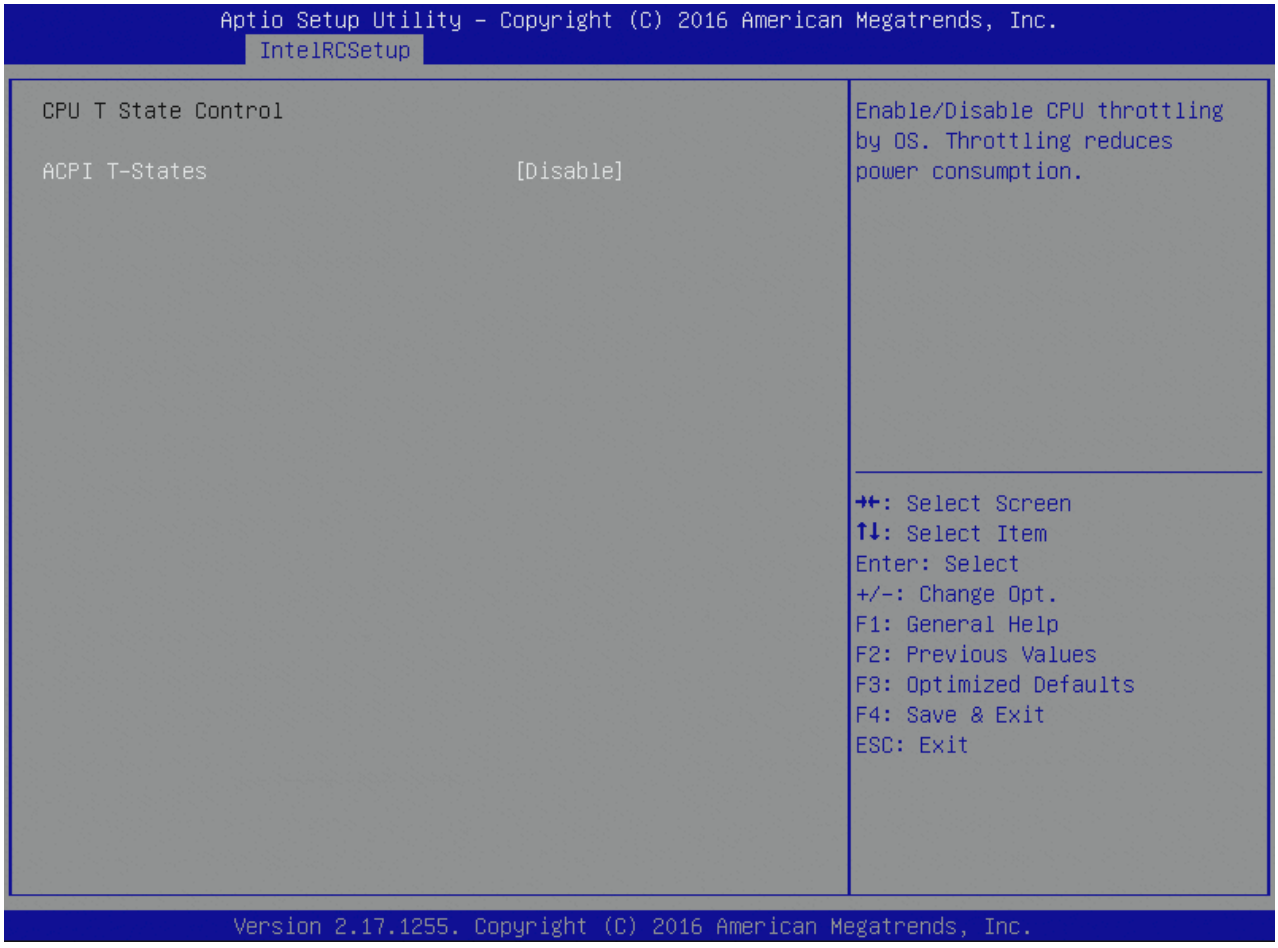


Table 75: CPU T State Control Features List

Feature	Options	Description
ACPI T-States	**Disable** Enable	Enable/Disable CPU throttling by OS. Throttling reduces power consumption.

6.5.3.10 CPU Thermal Management

Figure 52: CPU Thermal Management Menu Screen



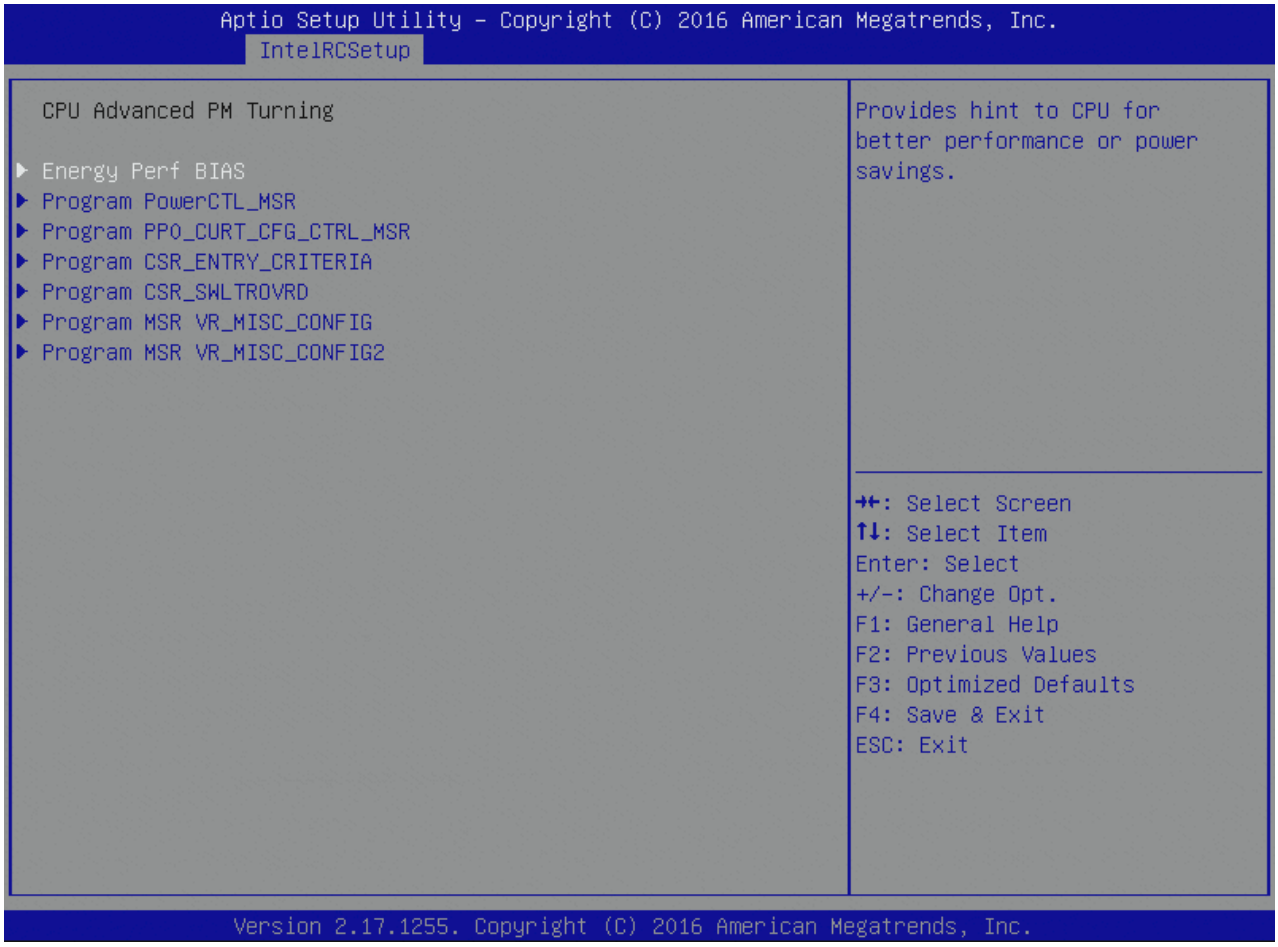
Table 76: CPU Thermal Management Features List

Feature	Options	Description
Bi-directional PROCHOT#	Output-only Disable Bidirectional (normal input response) **Input-only**	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
Thermal Monitor	Disable Enabled	Enable/Disable Thermal Monitor
PROCHOT RESPONSE	Pn clamping Pm clamping	Force CPU to throttle to a lower power condition such as Pn/Pm by asserting PROCHOT#. MSR 0x1FC [26] =1: go to Pm(min freq) on PROCHOT; =0 go to Pn (max efficient freq).
Use PCH_HOT	Disable Enabled	Pcode is allowed to use PCH_HOT pin information for thermal management
Use PCH Temp From ME	Disable Enabled	Pcode is allowed to use PCH Temperature provided by ME

CPU to PCH Throttle	Disable Enabled	Enable Pcode to throttle PCH

6.5.3.11 CPU Advanced PM Turning

Figure 53: CPU Advanced PM Turning Menu Screen



6.5.3.12 Energy Perf BIAS

Figure 54: Energy Perf BIAS Menu Screen

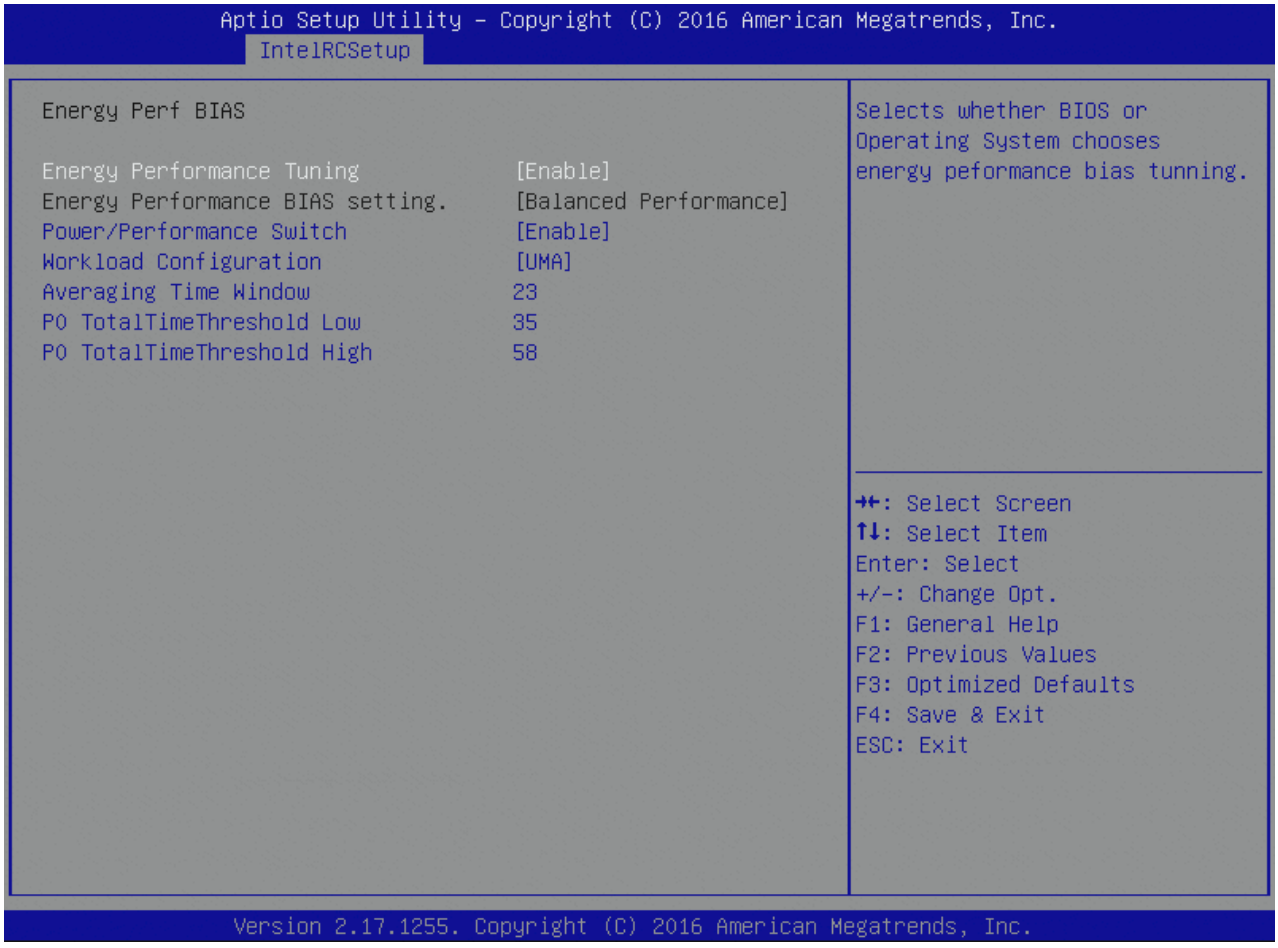


Table 77: Energy Perf BIAS Features List

Feature	Options	Description
Energy Performance Tuning	**Enable** Disable	Selects whether BIOS or Operating System chooses energy performance bias tunning.
Energy Performance BIAS setting.	Performance **Balance Performance** Balance Power Power	
Power/Performance Switch	Disable Enabled	MSR 1FCh Bit[24] = PWR_PERF_TUNING_ENABLE_DYN_SWITCHING
Workload Configuration	**UMA** NUMA	Optimization for the workload characterization. Balanced is recommended.
Averaging Time Window	23	This is used to control the effective window of the average for C0 and P0 time
P0 TotalTimeThreshold Low	35	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than this threshhold

P0 TotalTimeThreshold High	58	The HW switching mechanism ENABLES the performance setting (0) when the total P0 time is greater than this threshhold

6.5.3.13 Program PowerCTL_MSR

Figure 55: Program PowerCTL_MSR Menu Screen

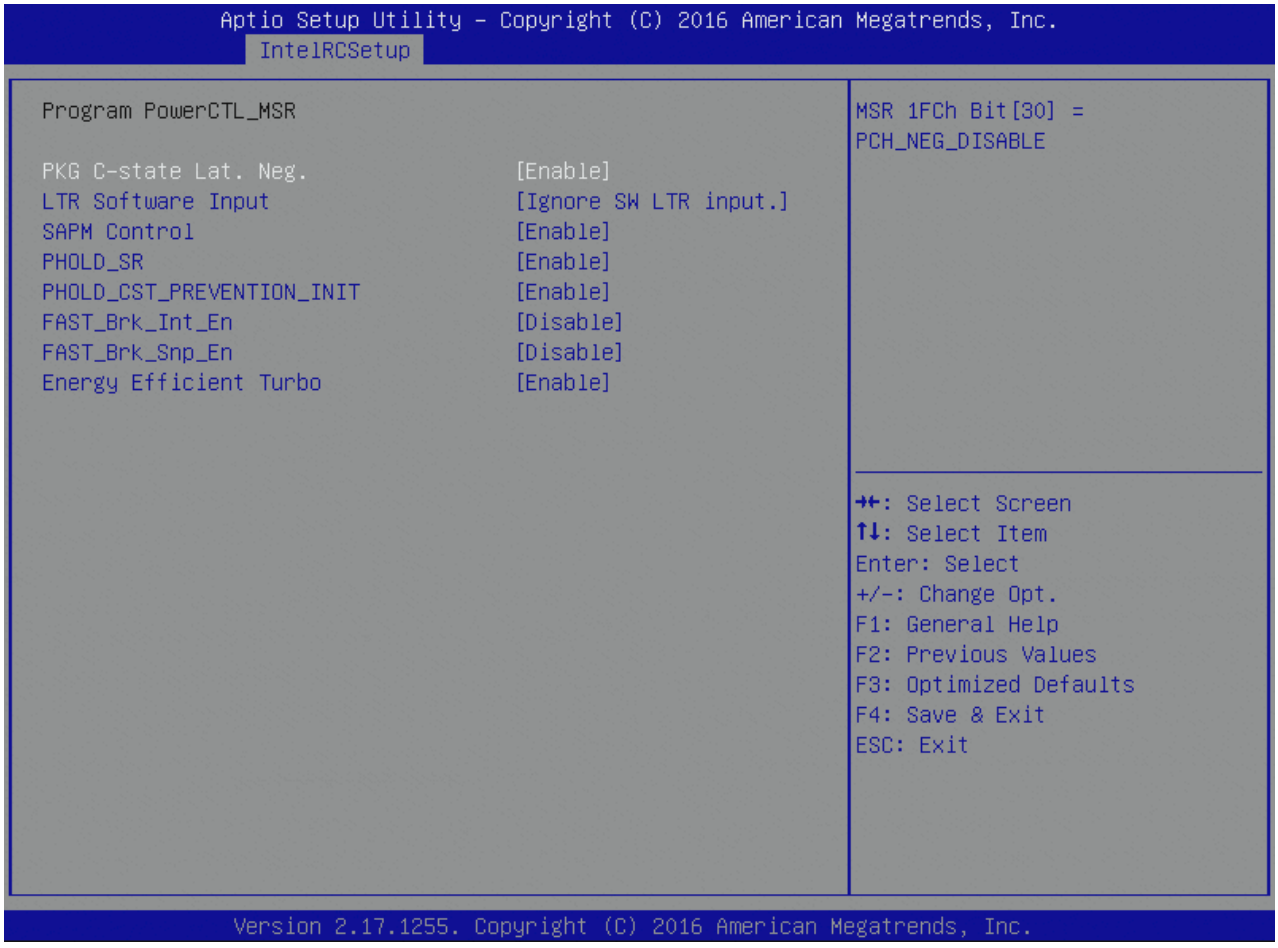


Table 78: Program PowerCTL_MSR Features List

Feature	Options	Description
PKG C-state Lat. Neg.	**Enable** Disable	MSR 1FCh Bit[30] = PCH_NEG_DISABLE
LTR Software Input	Take SW LTR input. Ignore SW LTR input.	MSR 1FCh Bit[28] = LTR_SW_DISABLE. Disable = Ignore SW LTR input.
SAPM Control	**Enable** Disable	MSR 1FCh Bit[22] = PWR_PERF_TUNING_DISABLE_SAPM_CTRL
PHOLD_SR	**Enable** Disable	MSR 1FCh Bit[17] = PHOLD_SR_Disable
PHOLD_CST_PREVENTION_INIT	**Enable** Disable	MSR 1FCh Bit[16] = PHOLD_CST_PREVENTION_INIT
FAST_Brk_Int_En	Enable Disable	MSR 1FCh Bit[4] = FAST_Brk_Int_En. Disable = Use 'fast' VID swing rate.

FAST_Brk_Snp_En	Enable Disable	MSR 1FCh Bit[3] = FAST_Brk_Snp_En. Disable = Use 'fast' VID swing rate.
Energy Efficient Turb	**Enable** Disable	Energy Efficient Turbo Disable, MSR 0x1FC [19]

6.5.3.14 Program PPO_CURT_CFG_CTRL_MSR

Figure 56: Program PPO_CURT_CFG_CTRL_MSR Menu Screen

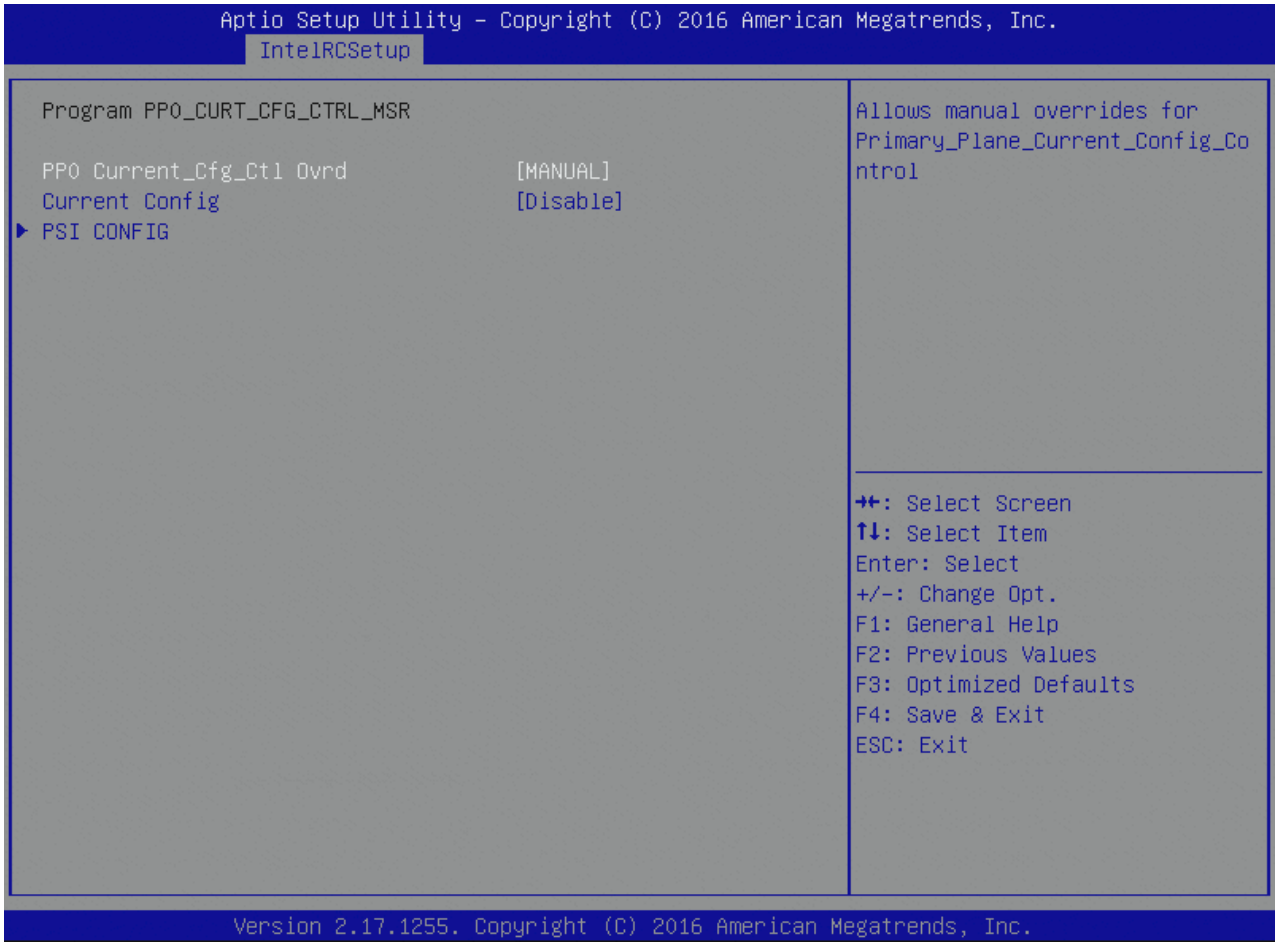


Table 79: Program PPO_CURT_CFG_CTRL_MSR Features List

Feature	Options	Description
PPO Current_Cfg_Ctl Ovrd	Auto Manual	Allows manual overrides for Primary_Plane_Current_Config_Control
Current Config	Disabled Enable	0 – Deafult, do nothing; 1 – Manual, override Current limitation in 1/8 A increments.

6.5.3.15 PSI Config

Figure 57: PSI Config Menu Screen

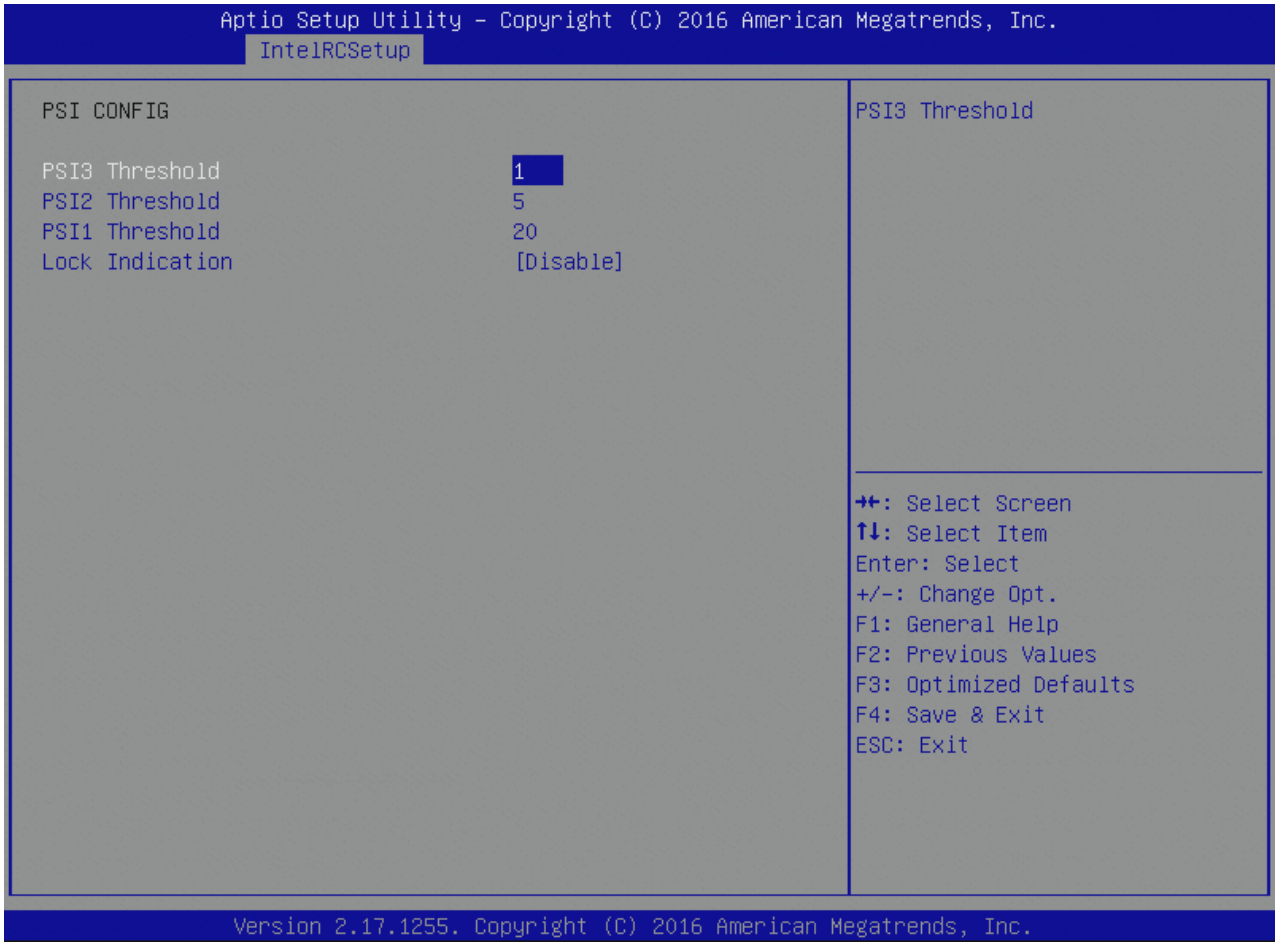


Table 80: PSI Config Features List

Feature	Options	Description
PSI3 Threshold	1	PSI3 Threshold
PSI2 Threshold	5	PSI2 Threshold
PSI1 Threshold	20	PSI1 Threshold
Lock Indication	Disable Enable	This bit will lock the CURRENT_LIMIT settings in this register and will also lock this setting

6.5.3.16 Program CSR_ENTRY_CRITERIA

Figure 58: Program CSR_ENTRY_CRITERIA Menu Screen

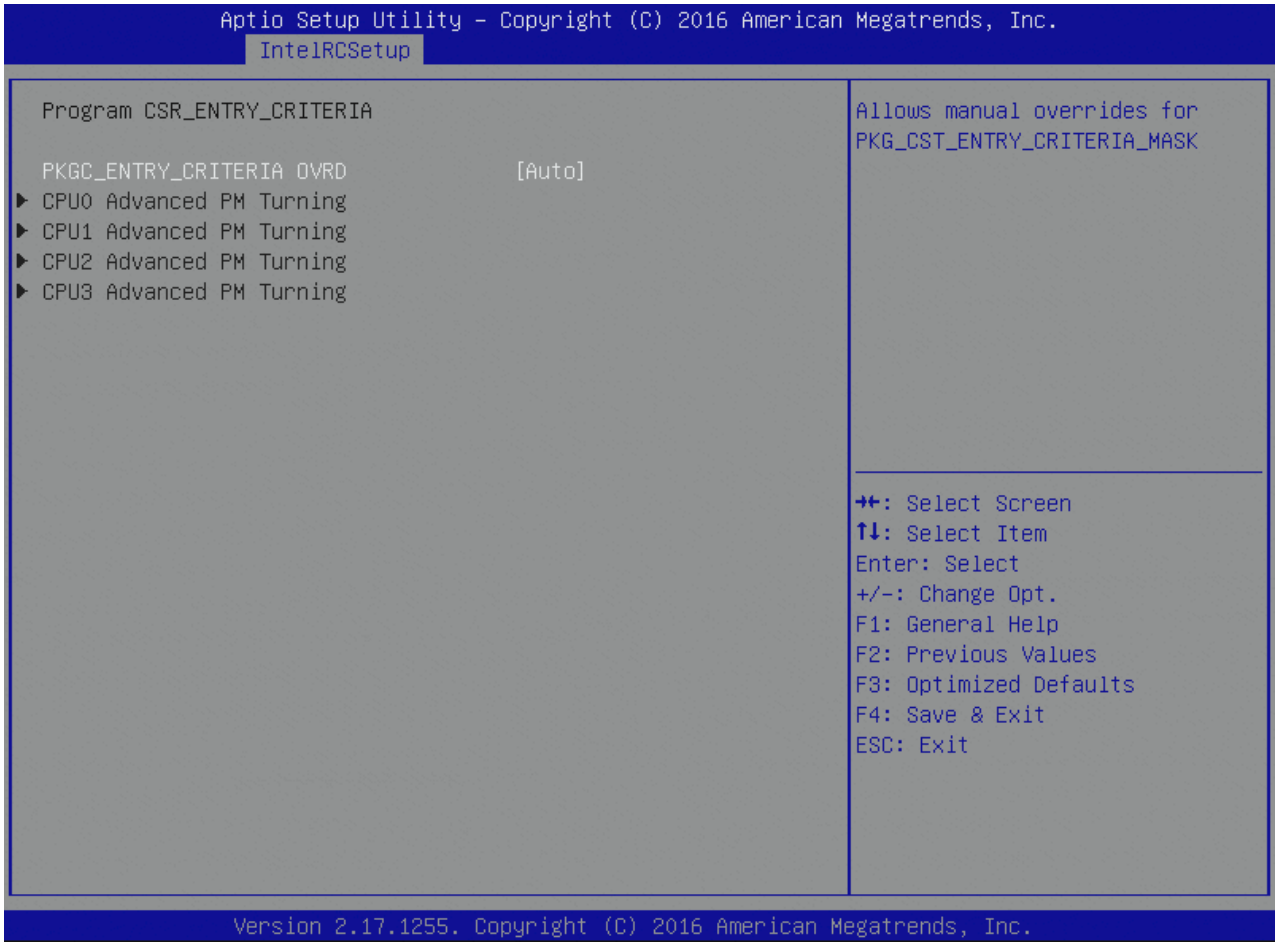


Table 81: Program CSR_ENTRY_CRITERIA Features List

Feature	Options	Description
PKG_CST_ENTRY_CRITERIA OVRD	**Auto** Manual	Allows manual overrides for PKG_CST_ENTRY_CRITERIA_MASK

6.5.3.17 CPU Advanced PM Turning

Figure 59: CPU Advanced PM Turning Menu Screen

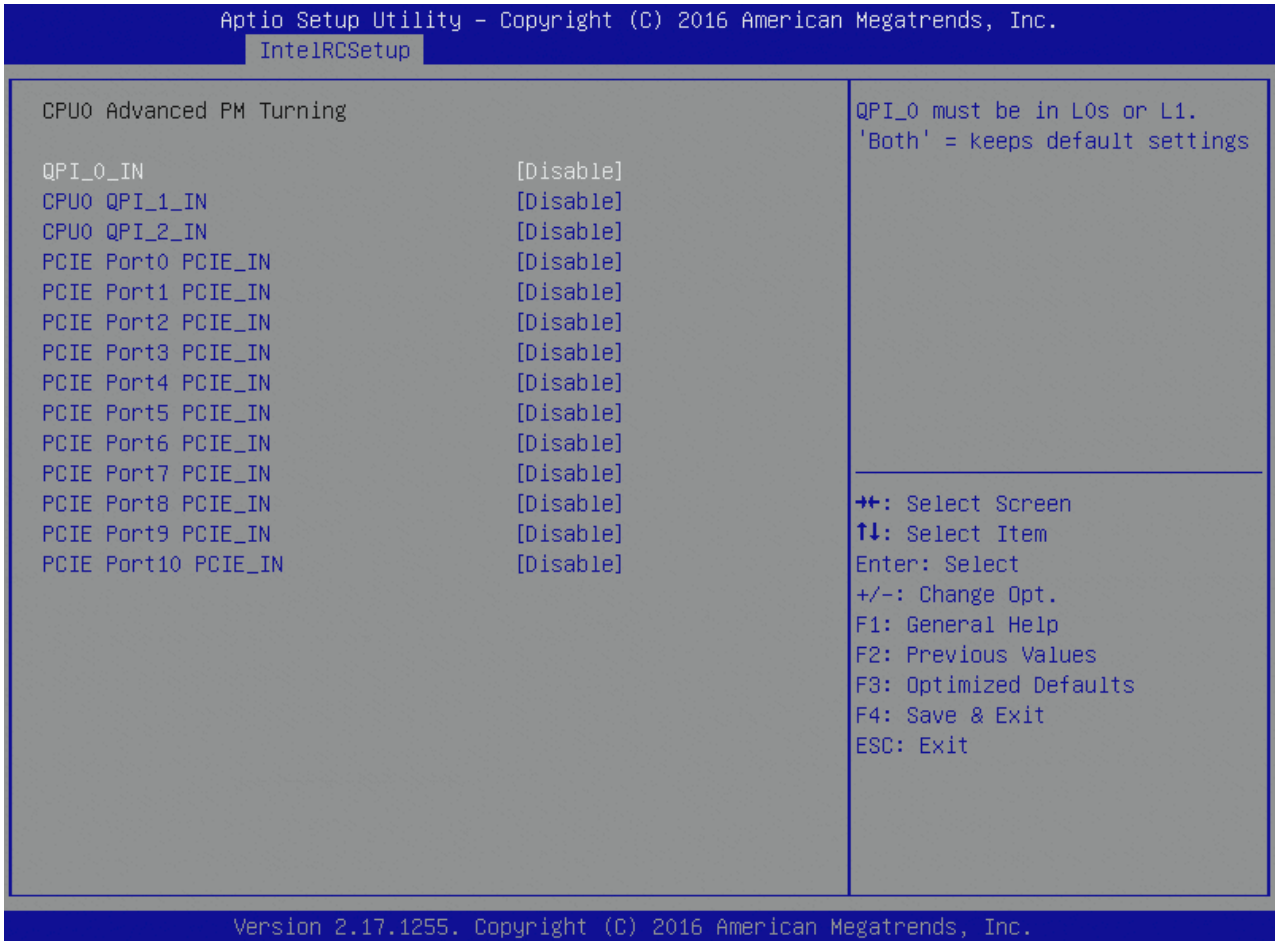


Table 82: CPU Advanced PM Turning Features List

Feature	Options	Description
QPI_0_IN	Disable IN_L1	QPI_0 must be in L0s or L1. 'Both' = keeps default settings
CPU0 QPI_1_IN	Disable IN_L1	QPI_1 must be in L0s or L1. 'Both' = keeps default settings
CPU0 QPI_2_IN	Disable IN_L1	QPI_2 must be in L0s or L1. 'Both' = keeps default settings
PCIE Port0 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port1 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port2 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port3 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.

Feature	Options	Description
PCIE Port4 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port5 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port6 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port7 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port8 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port9 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.
PCIE Port10 PCIE_IN	Disable IN_L1	If IN_L1, MSB = PCIe10. LSB-PCIe_10. LSB = PCIe_0.

6.5.3.18 Program CSR_SWLTROVRD

Figure 60: Program CSR_SWLTROVRD Menu Screen

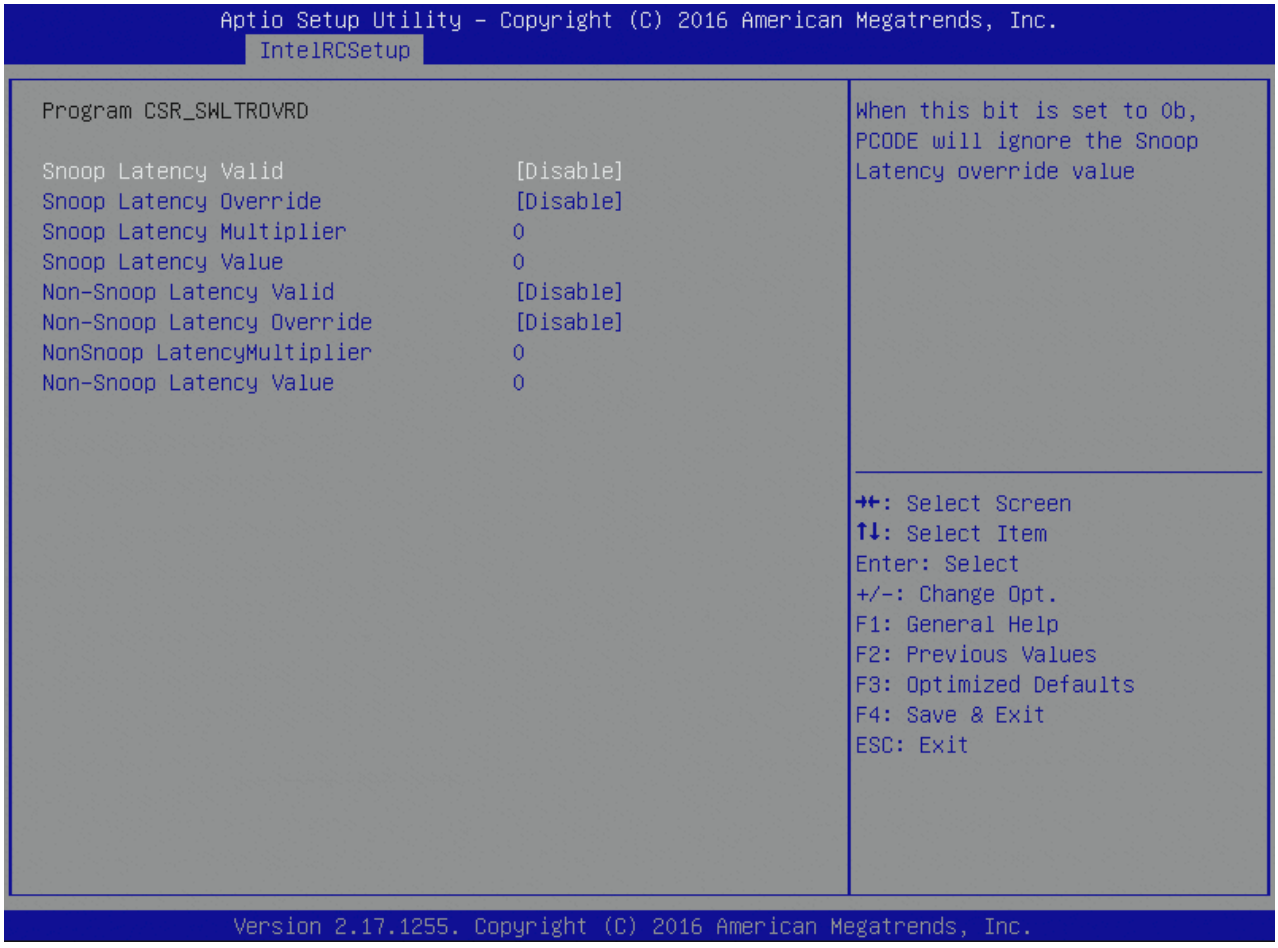


Table 83: Program CSR_SWLTROVRD Features List

Feature	Options	Description
Snoop Latency Valid	Disable Enable	When this bit is set to 0b, PCODE will ignore the Snoop Latency override value
Snoop Latency Override	Disable Enable	Force PCODe to always use values provided in SW_LTR_OVRD
Snoop Latency Multiplier	0	Value is multipled by to yield a time value
Snoop Latency Value	0	Latency requirement for Snoop requests
Non-Snoop Latency Value	Disable Enable	When this bit is set to 0b, PCODE will ignore the Non-Snoop Latency override value
Non-Snoop Latency Override	Disable Enable	Force PCODe to always use values provided in SW_LTR_OVRD
NonSnoop LatencyMultiplier	0	Value is multipled by to yield a time value
Non-Snoop Latency Value	0	Latency requirement for Non-Snoop requests

6.5.3.19 Program MSR VR_MISC_CONFIG

Figure 61: Program MSR VR_MISC_CONFIG Menu Screen

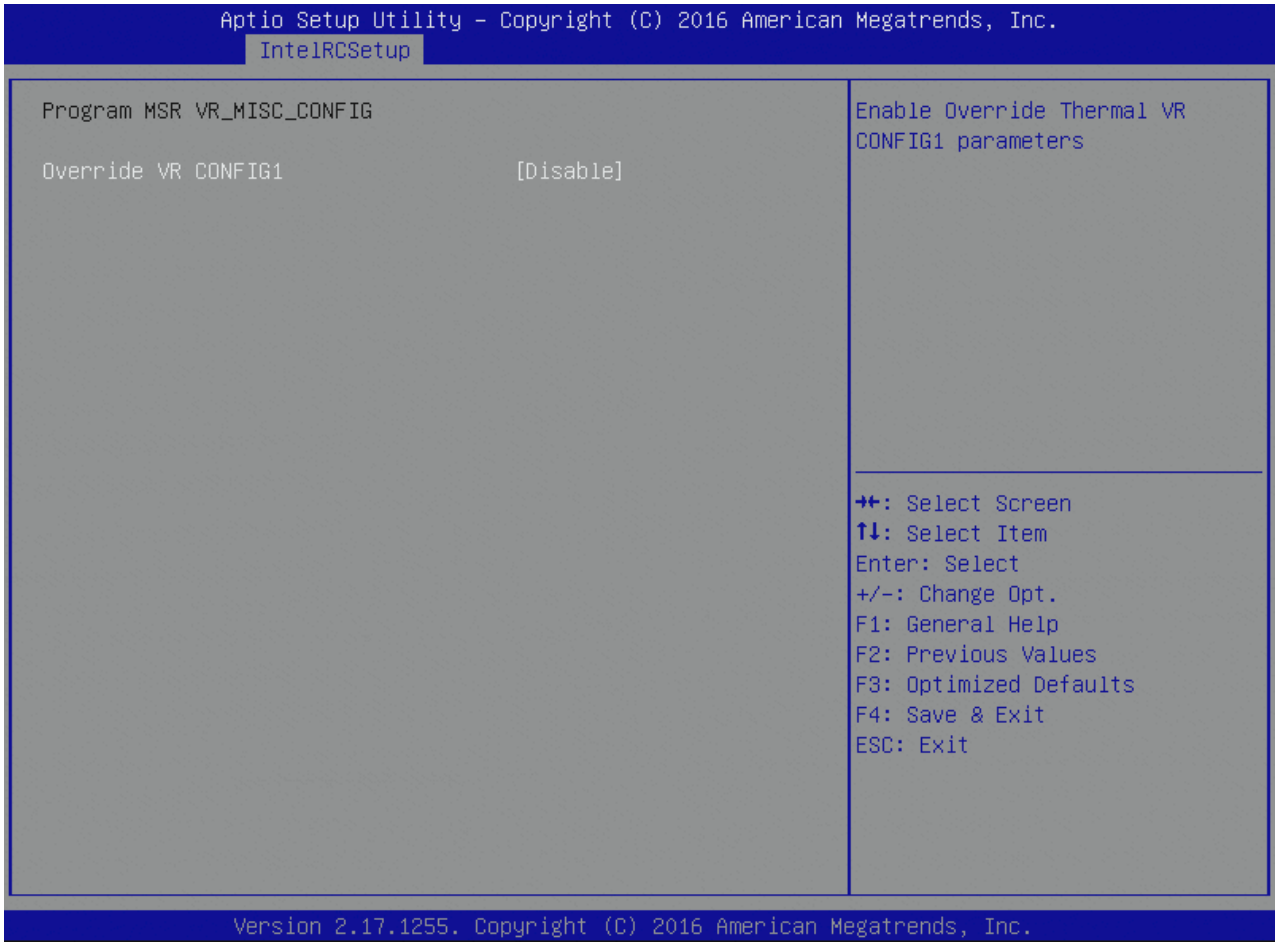


Table 84: Program MSR VR_MISC_CONFIG Features List

Feature	Options	Description
Override VR CONFIG1	Disable Enable	Enable Override Thermal VR CONFIG1 parameters

6.5.3.20 Program MSR VR_MISC_CONFIG2

Figure 62: Program MSR VR_MISC_CONFIG2 Menu Screen

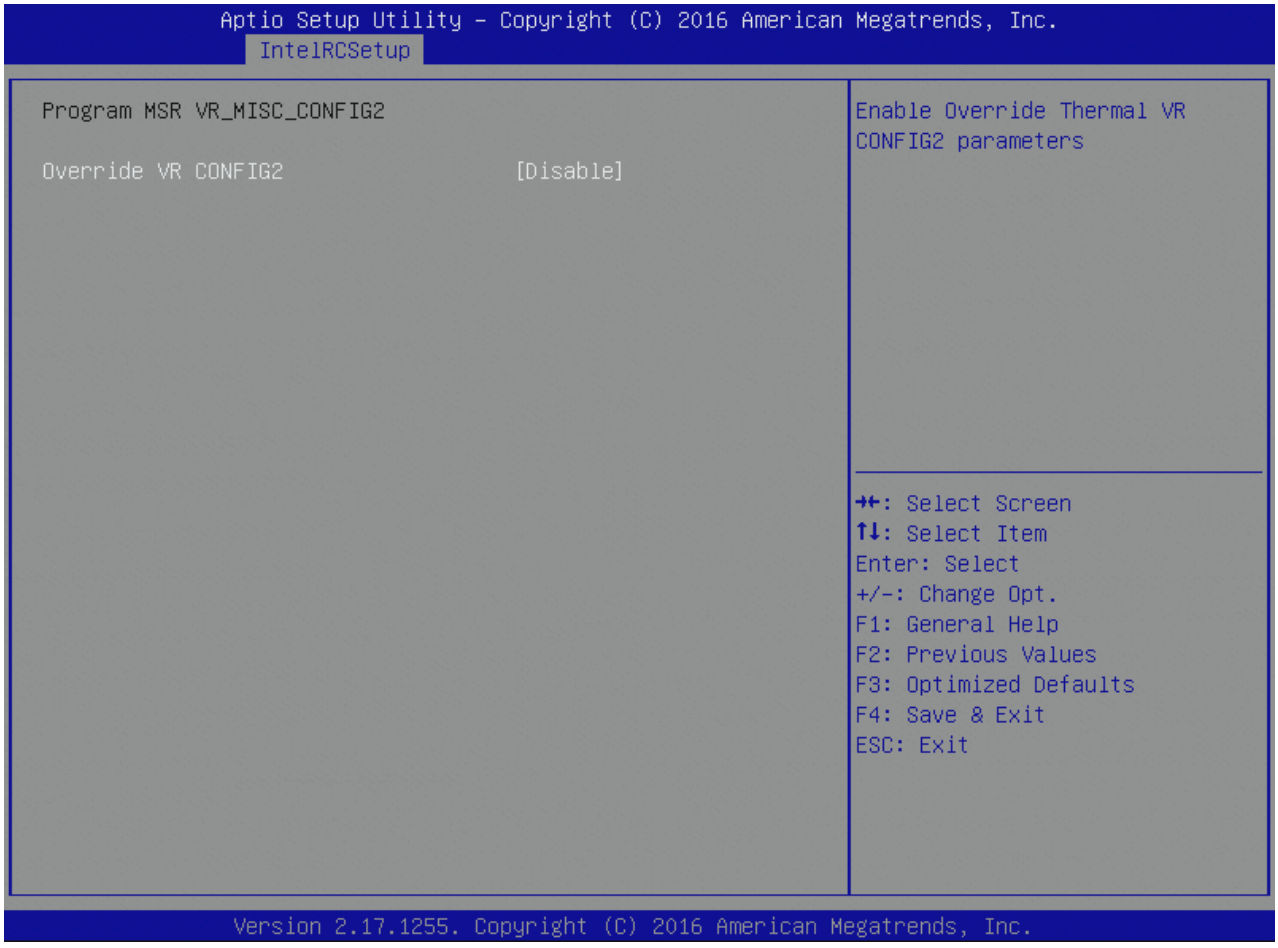


Table 85: Program MSR VR_MISC_CONFIG2 Features List

Feature	Options	Description
Override VR CONFIG2	Disable Enable	Enable Override Thermal VR CONFIG2 parameters

6.5.3.21 DRAM RAPL Configuration

Figure 63: DRAM RAPL Configuration Menu Screen

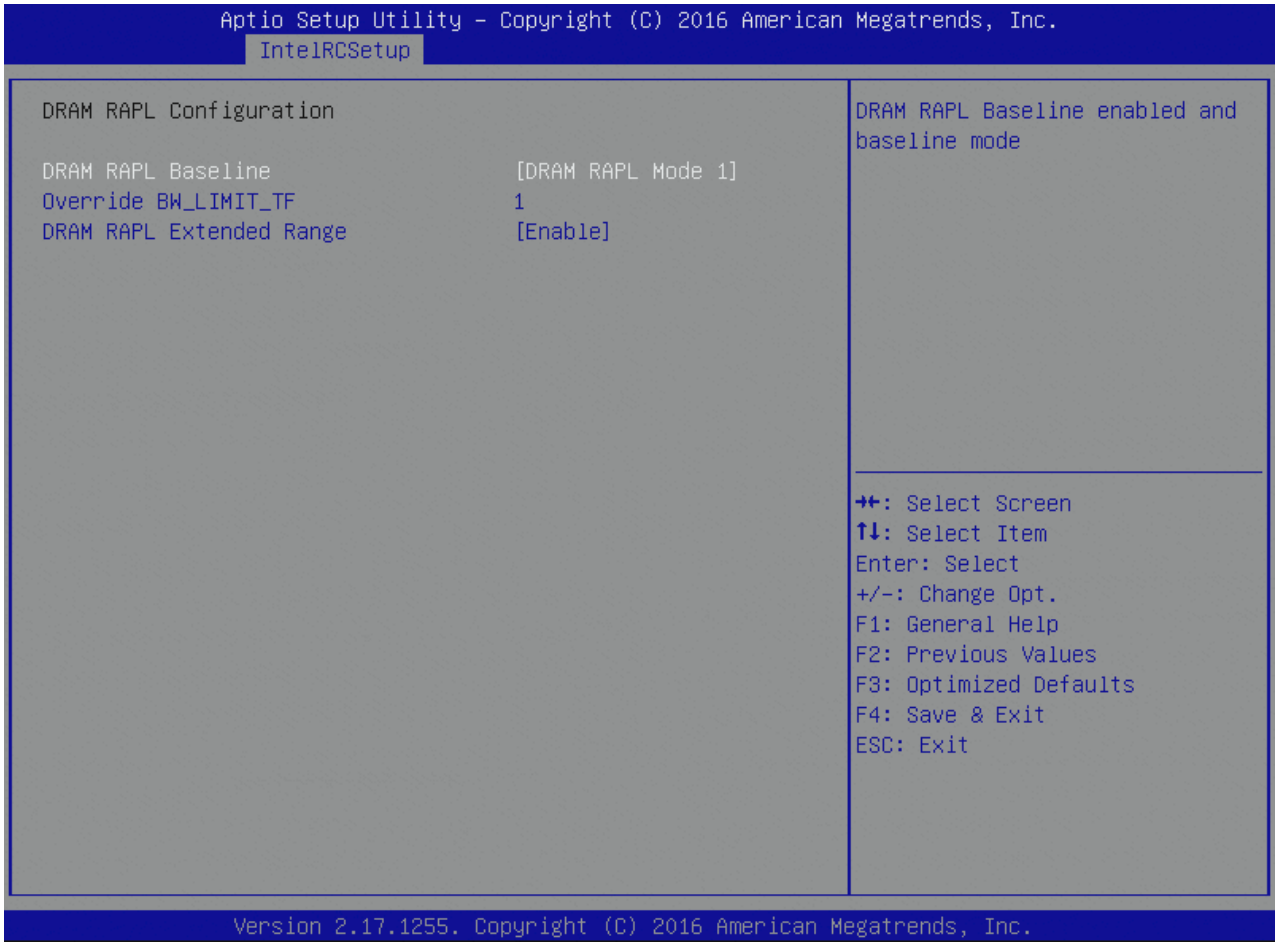


Table 86: DRAM RAPL Configuration Features List

Feature	Options	Description
DRAM RAPL Baseline	Disable DRAM RAPL Mode 0 **DRAM RAPL Mode 1**	DRAM RAPL Baseline enabled and baseline mode
Override BW_LIMIT_TF	1	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled
DRAM RAPL Extended Range	Disable Enable	Select DRAM RAPL Extended Range

6.5.3.22 Socket RAPL Config

Figure 64: Socket RAPL Config Menu Screen

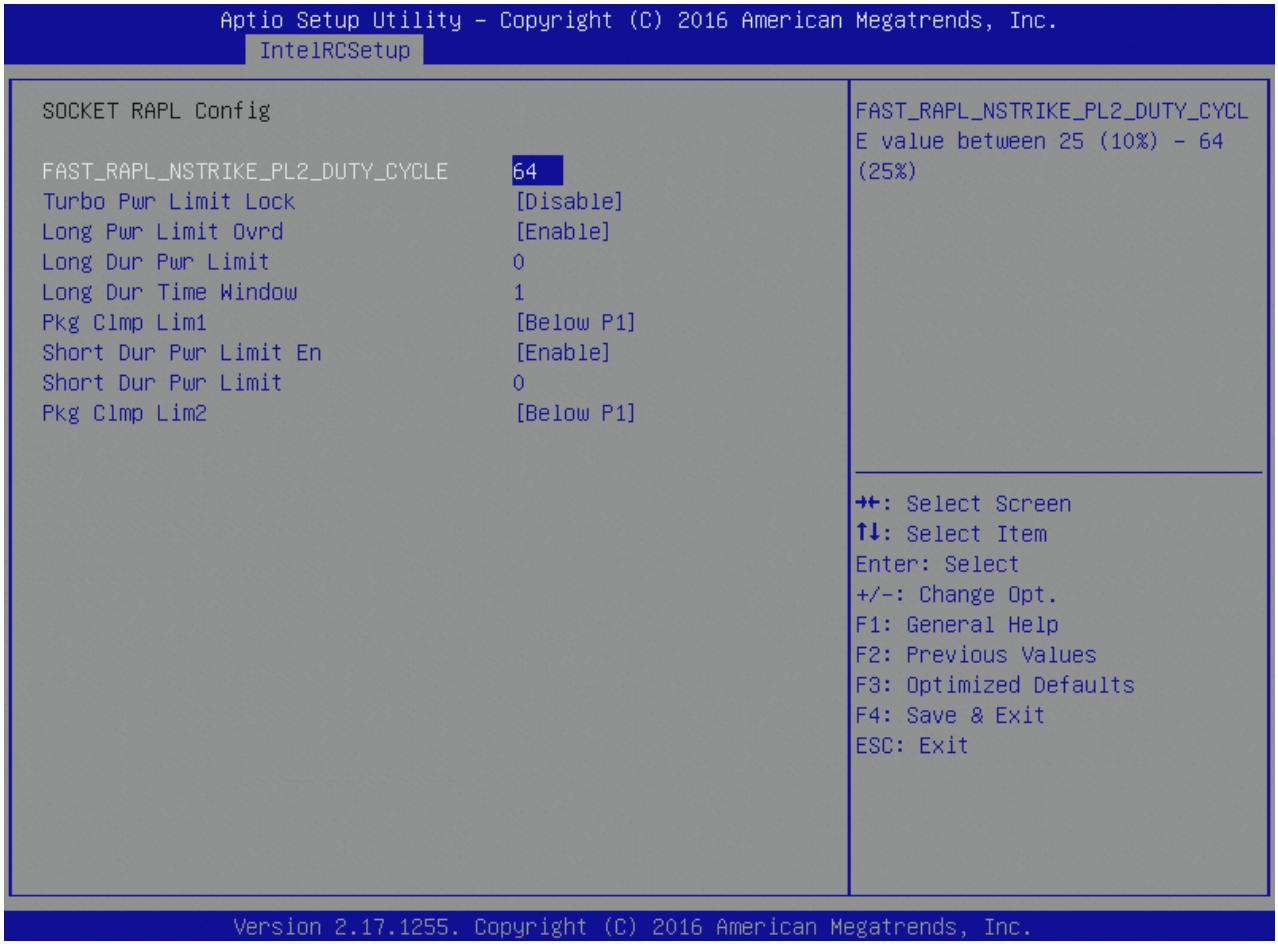


Table 87: Socket RAPL Config Features List

Feature	Options	Description
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	64	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) – 64 (25%)
Turbo Pwr Limit Lock	Disable Enable	Enable/Disable locking of turbo settings. When enabled, TURBO_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
Long Pwr Limit Ovrd	Disable Enable	Enable/Disable Long Term Power Limit override. If this option is disabled, BIOS will program the deafult values for Long Term Power Limit and Long Term Power Limit Time Window.
Long Dur Pwr Limit	0	Turbo Mode Long Duration Power Limit (aka Power Limit 1) 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.
Long Dur Time Window	1	Long Duration Time Window (aka Power Limit 1 Time) value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value

Feature	Options	Description
		should be maintained. If the value is 0, the fused value will be programmed.
Pkg Clmp Lim1	Bewtee P1/P0 **Below P1**	Pkg Clamping limit 1, Allow going below P1. 0: PBBM limited between P1 and P0, 1: PBM can go below P1
Short Dur Pwr Limit En	Disable **Enable**	Enable/Disable Short Duration Power Limit (aka Power Limit 2)
Short Dur Pwr Limit	0	Short Duration Power Limit (aka Power Limit 2) value in Watts. The value may vary from 0 to 32767. If the value is 0, BIOS will program this value as 125%TDP. Processor applies control policies such that the package power does not exceed this limit.
Pkg Clmp Lim2	Bewtee P1/P0 **Below P1**	Pkg Clamping limit 2, Allow going below P1. 0: PBBM limited between P1 and P0, 1: PBM can go below P1

6.5.3.23 Common RefCode Configuration

Figure 65: Common RefCode Configuration Menu Screen

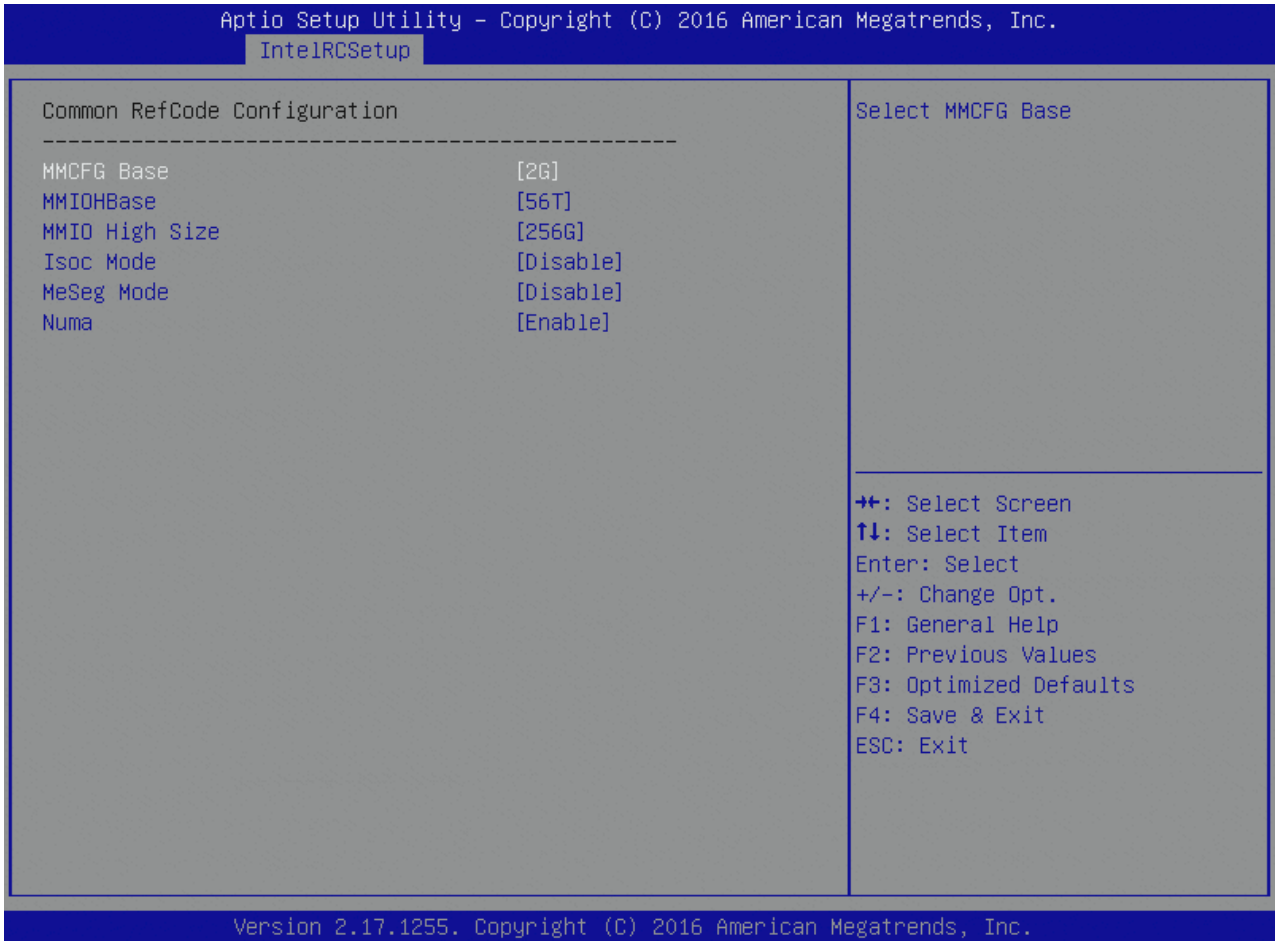
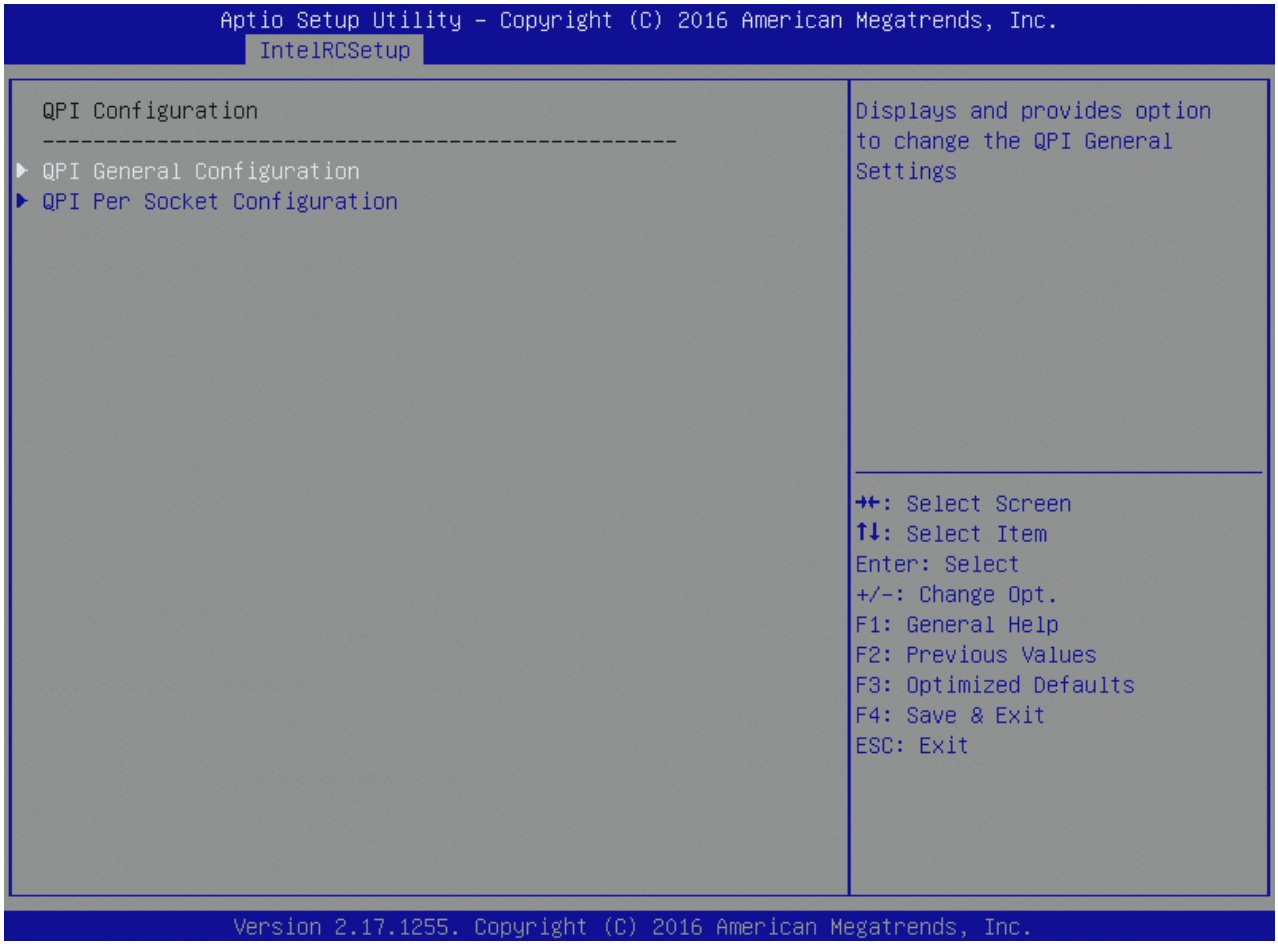


Table 88: Common RefCode Configuration Features List

Feature	Options	Description
MMCFG Base	**2G** 1G 3G	Select MMCFG Base
MMIOBase	**56T** 48T … 1T	MMIOH Base [63:32]; must be between 4032 – 4078
MMIO High Size	**256G** 128G 512G 1024G	Select MMIOH High Size
Isoc Mode	Disable	Isoc: Disable,Enable
MeSeg Mode	**Disable** Enable Auto	MeSeg: Disable,Enable
Numa	Disable **Enable**	Enable or Disable Non uniform Memory Access (NUMA).

6.5.3.24 QPI Configuration

Figure 66: QPI Configuration Menu Screen



6.5.3.25 QPI General Configuration

Figure 67: QPI General Configuration Menu Screen

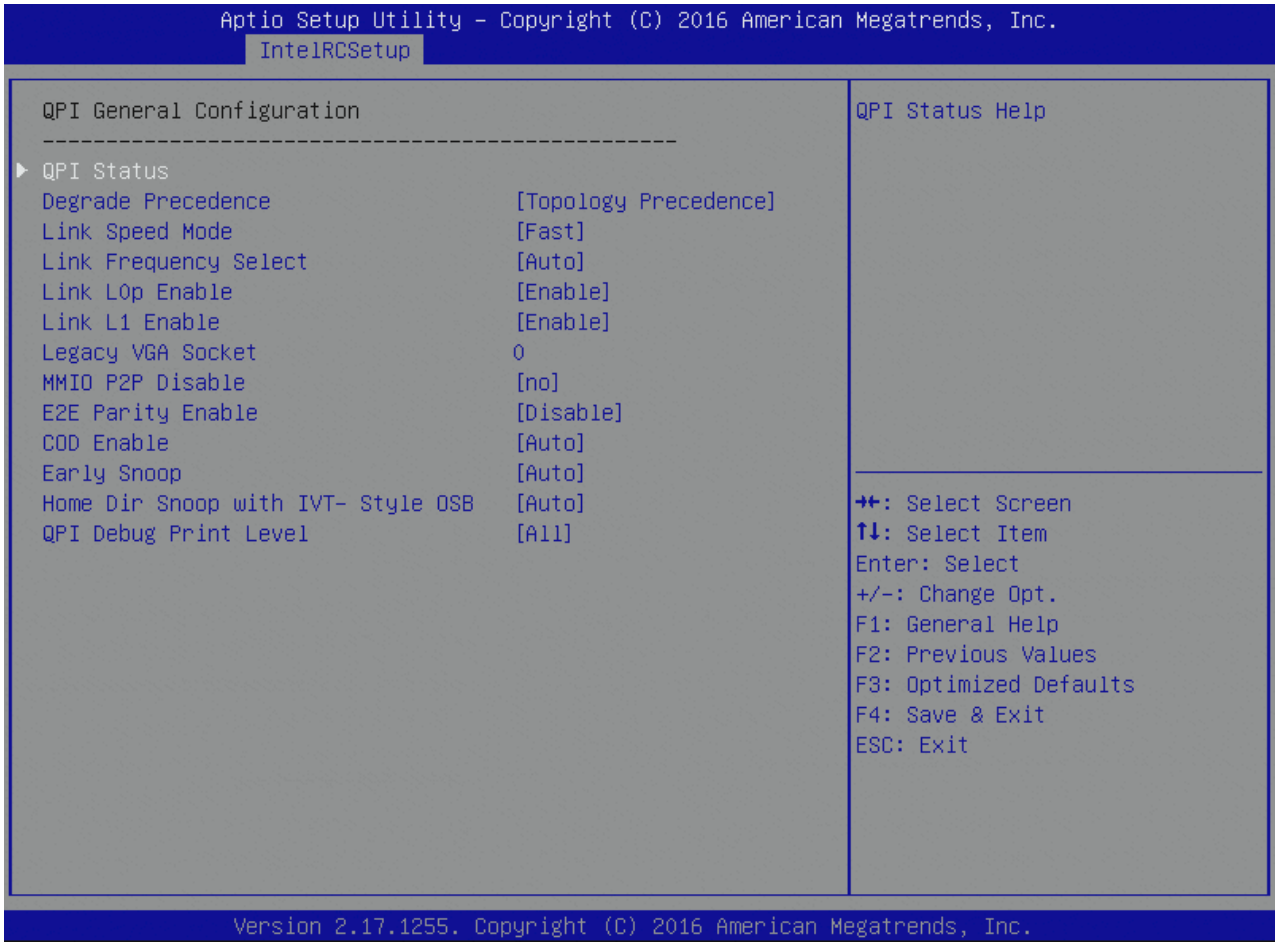


Table 89: QPI General Configuration Features List

Feature	Options	Description
Degrade Precedence	**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	Slow **Fast**	Select the QPI link speed as either the POR speed (Fast) or default speed (Slow)
Link Frequency Select	6.4GB/s 8.0GB/s 9.6GB/s **Auto** Auto Limited	Allows for selecting the QPI Link Frequency
Link L0p Enable	Disable **Enable**	Link L0p Enable:Disable,Enable,Auto(default)
Link L1 Enable	Disable **Enable**	Link L1 Enable:Disable,Enable,Auto(default)
Legacy VGA Socket	0	Socket that claims the legacy VGA range; valid values are 0-7; 0 is default.

Feature	Options	Description
MMIO P2P Disable	no yes	To disable MMIOL P2P traffic across Sockets. Default is NO to not disable.
E2E Parity Enable	Disable Enable	Enable/Disable E2E Parity.
COD Enable	Disable Enable **Auto**	Enable/disable Cluster on Die.
Early Snoop	Disable Enable **Auto**	
Home Dir Snoop with I	Disable Enable **Auto**	Enable/disable Home Dir Snoop with IVT- Style OSB
QPI Debug Print Level	Fatal Warning Summary Detail **All**	QPI Debug Print Level Enable-Disable.

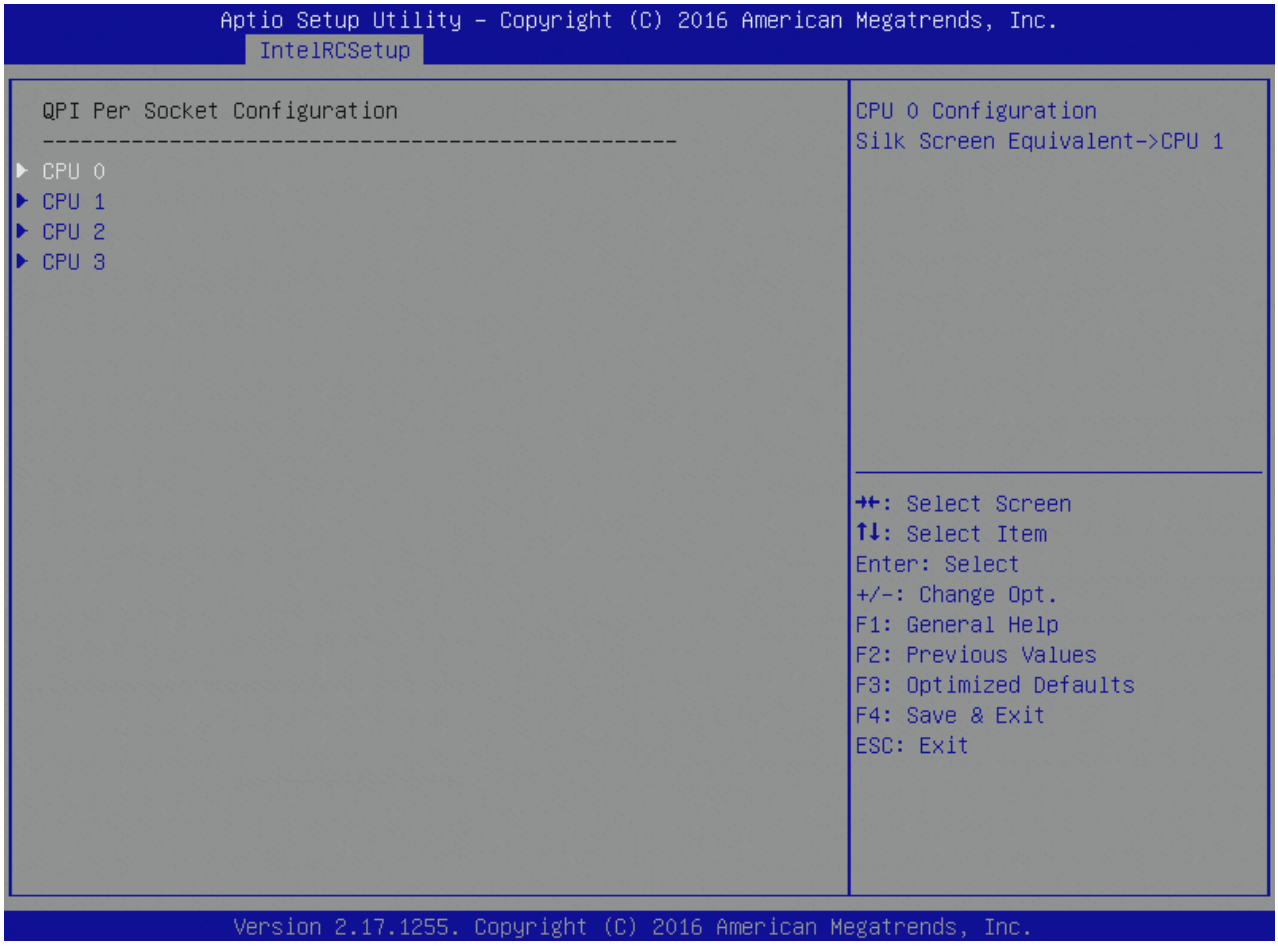
6.5.3.26 QPI Status

Figure 68: QPI Status Menu Screen



6.5.3.27 QPI Per Socket Configuration

Figure 69: QPI Per Socket Configuration Menu Screen



6.5.3.28 QPI Per Socket Configuration - CPU

Figure 70: QPI Per Socket Configuration - CPU Menu Screen

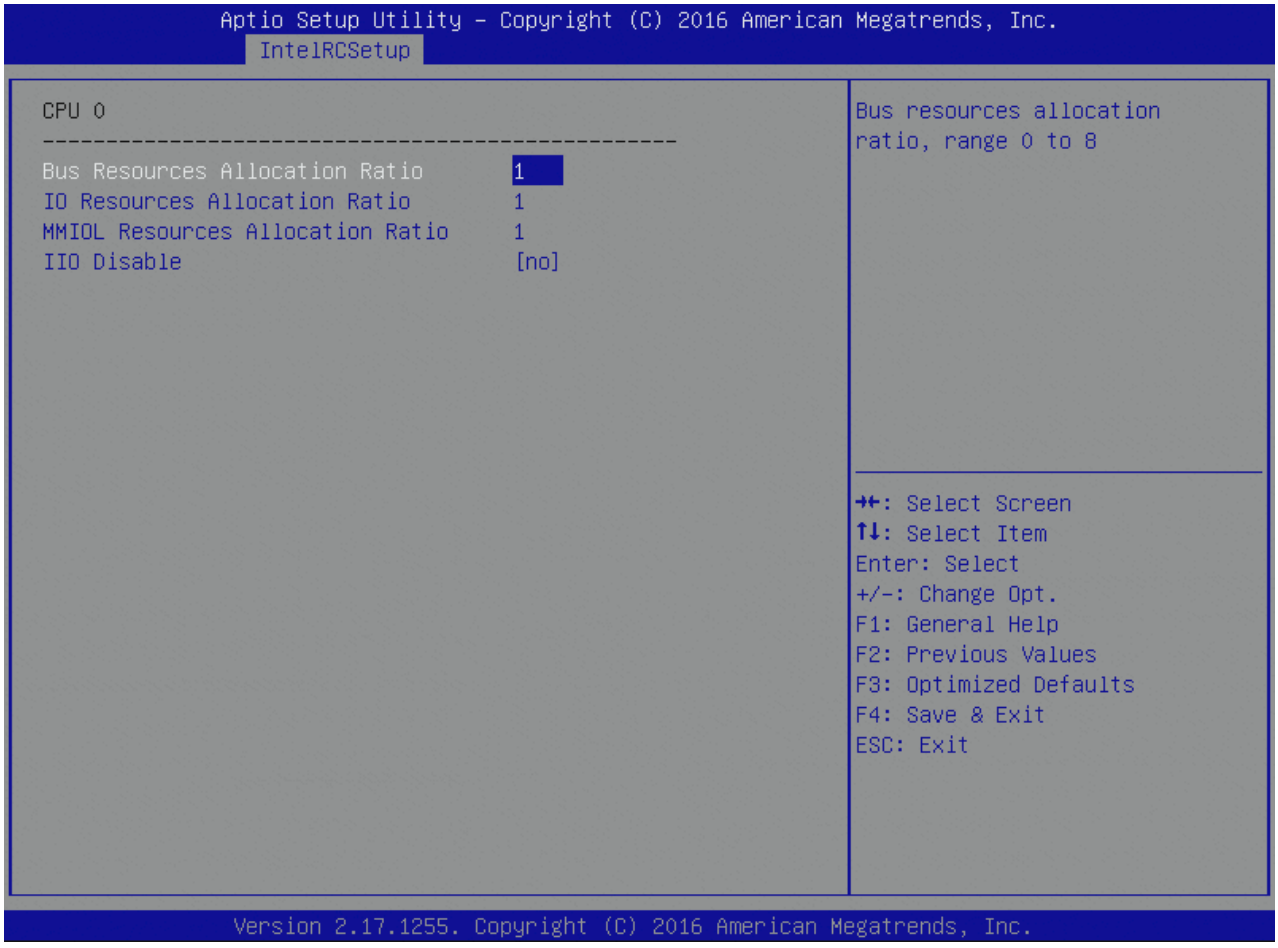


Table 90: QPI Per Socket Configuration - CPU Features List

Feature	Options	Description
Bus Resources Allocation Ration	1	Bus resources allocation ratio, range 0 to 8
IO Resources Allocation Ration	1	IO resources allocation ratio, range 0 to 8
MMIOL:Resources Allocation Ratio	1	MMIOL resources allocation ratio, range 0 to 8
IIO Disable	**no** Disable Ports and IIO without memory hotplug Disable Ports Only with memory hotplug	Disable Ports and Clock Gate IIO

6.5.3.29 Memory Configuration

Figure 71: Memory Configuration Menu Screen

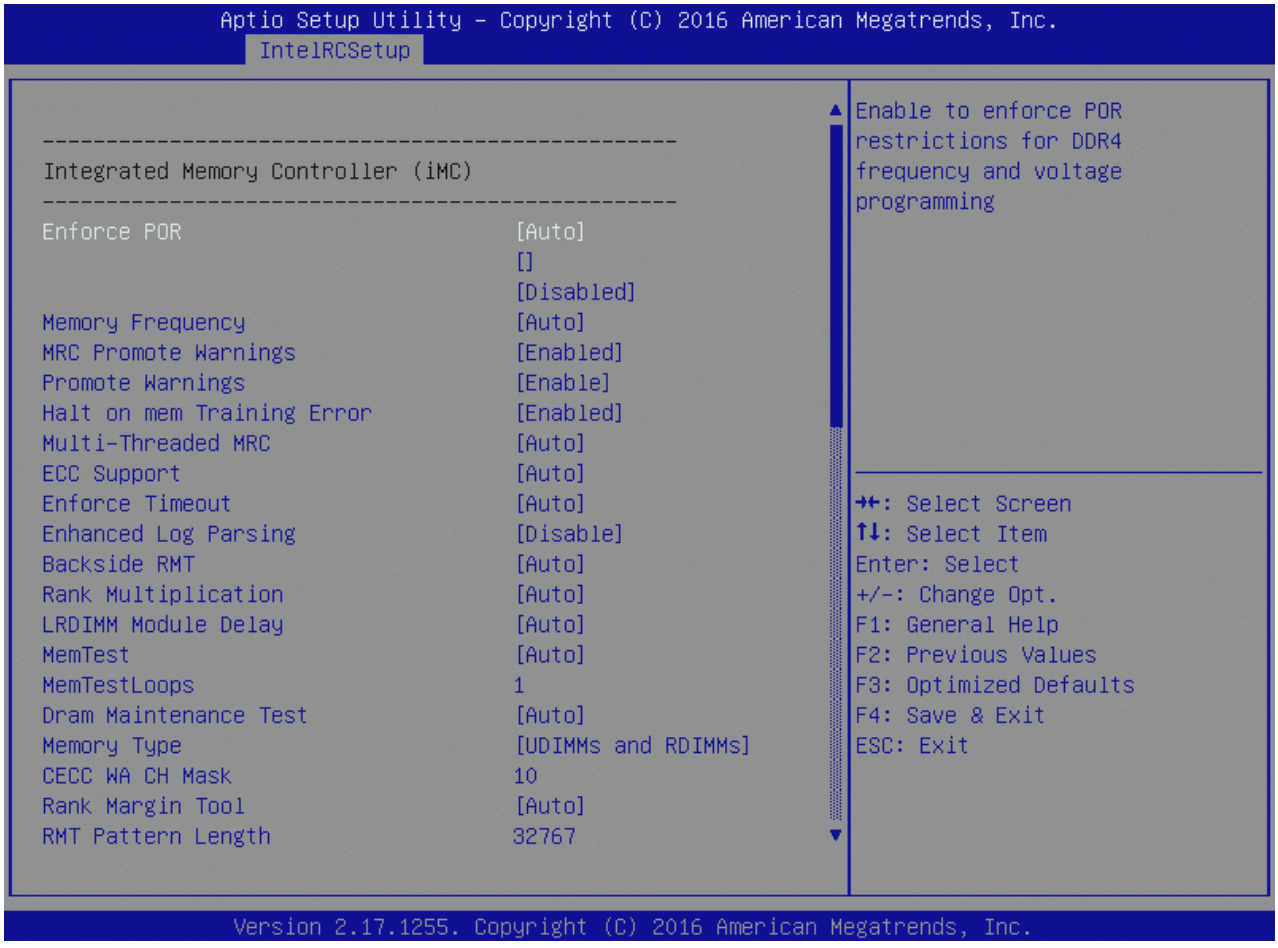


Table 91: Memory Configuration Features List

Feature	Options	Description
Enforce POR	**Auto** Enforce POR Disabled Enforce Stretch Goals	Enable to enforce POR restrictions for DDR4 frequency and voltage programming
Memory Frequency	**Auto** ... Reserved	Maximum Memory Frequency Selections in MHz. Do not select Reserved
MRC Promote Warnings	Disabled **Enabled**	Determines if MRC warnings are promoted to system level
Promote Warnings	Disable **Enable**	Determines if warnings are promoted to system level
Halt on mem Training Error	Disabled **Enabled**	Halt on mem Training Error Disable/Enable
Multi-Threaded MRC	**Auto** Disabled Enabled	Enable to execute the Memory Reference Code multi-threaded

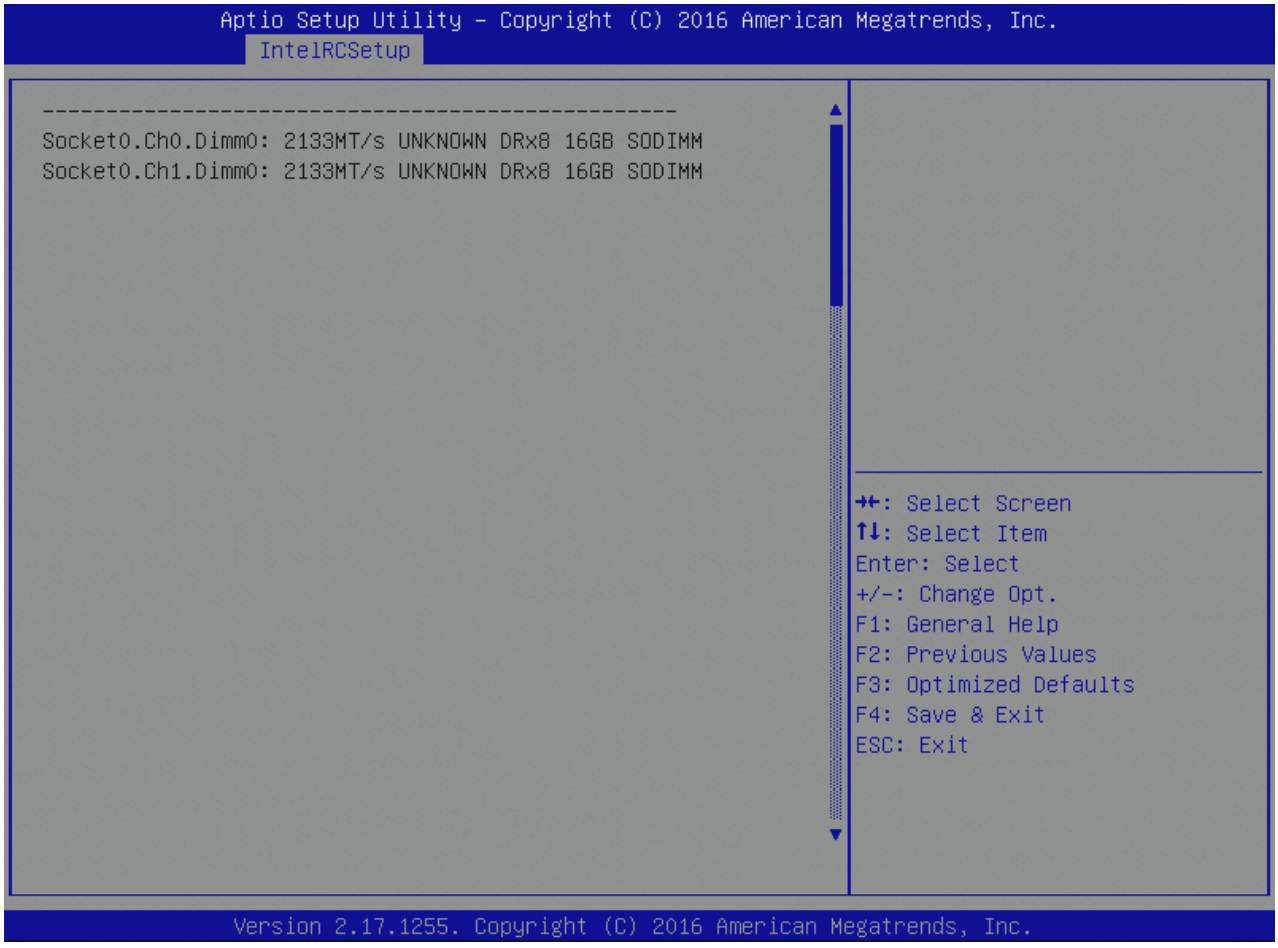
Feature	Options	Description
ECC Support	**Auto** Disable Enable	Enable/disable DDR ECC Support
Enforce Timeout	**Auto** Disable Enable	Enable/disable forcing cold reset after 3 months
Enhanced Log Parsing	**Disable** Enable	Enable additional output in debug log for easier machine parsing
Backside RMT	**Auto** Disable Enable	Enable Backside RMT
Rank Multiplication	**Auto** Enabled	Force the Rank Multiplication factor for LRDIMM
LRDIMM Module Delay	Disabled **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	**Auto** Disable Enable	Enable/disable memory test during normal boot
MemTestLoops	1	Number of Memory test loops during normal boot, set to 0 to run memtest infinitely
Dram Maintenance Test	**Auto** Disabled Enabled	Dram Maintenance Test during normal boot
Memory Type	RDIMMs only UDIMMs only **RDIMMs and UDIMMs**	Selects the Memory type supported by this platform.
CECC WA CH Mask	10	CH bitmask to apply CECC WA. 1 bit per CH. Value 2 applies WA on CH1, 3 on CH0 and 1
Rank Margin Tool	**Auto** Disabled Enabled	Enables the rank margin tool to run after DDR4 memory training
RMT Pattern Length	32767	Sets the pattern length for the Rank Margin Tool
CMD Pattern Length	32767	Sets the pattern length for the Rank Margin Tool
Per Bit Margin	**Auto** Disable Enable	Enables the logging from the serial port of DDR Per Bit Margin Data
Training Result Offset Config	**Auto** Disabled Enabled	Option to offset the final memory training results
Attempt Fast Boot	**Auto** Disable Enable	When enabled, portions of memory reference code will be skipped when possible to increase boot speed
Attempt Fast Cold Boot	**Auto** Disable Enable	When enabled, portions of memory reference code will be skipped when possible to increase boot speed

Feature	Options	Description
MemTest On Fast Boot	**Auto** Disable Enable	Enable/disable memory test during fast boot
RMT on Cold Fast Boot	**Auto** Disable Enable	Enable/Disable Rank Margin Tool on Cold Fast Boot
BDAT	Enabled **Disabled**	Enable Disables BDAT
Data Scrambling	**Auto** Disabled Enabled	Enables data scrambling
Allow SBE during Training	**Auto** Disabled Enabled	Allow SBE during training knob enable/disable
CECC WA Control	**Auto** Disabled Enabled	This knob controls the CECC WA. Disabled by Default on L0 and Later Processor.
CAP ERR LOW feature	**Auto** Disabled Enabled	This knob controls the CAP ERR FLOW feature. Disabled by Default.
Scrambling Seed Low	41003	Low 32 bits of the scrambling seed
Scrambling Seed High	54165	High 32 bits of the scrambling seed
Enable ADR	**Disabled** Hardware Triggered ADR Software Triggered ADR	Enables the detecting and enabling of ADR
MC BGF threshold	0	The HA to MC BGF threshold is used for scheduling MC request in bypass condition.
DLL Reset Test	0	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.
MC ODT Mode	**Auto** 100 OHms 50 OHms	Select MC ODT Mode
Opp read during WMM	**Auto** Disabled Enabled	Enable/Disable issuing read commands opportunistically during WMM
Normal Operation Duration	1024	Set normal operation duration interval (0 – 65535)
Number of Sparing Transaction	4	Set number of sparing transactions interval (0 – 65535)
PSMI Support	Disabled Enabled	PSMI Support Disable/Enable
C/A Parity Enable	**Auto** Disabled Enabled	Enable/Disable DDR4 Command Address Parity

Feature	Options	Description
SMB Clock Frequency	**Auto** 400 kHz 1 MHz	Sets DDR4 SMB Clock Frequencys For SPD ACCESS
DIMM Rank Enable Mask	Disabled Enabled	Selects rank to enable/disable per DIMM

6.5.3.30 Memory Topology

Figure 72: Memory Topology Menu Screen



6.5.3.31 Memory Thermal

Figure 73: Memory Thermal Menu Screen

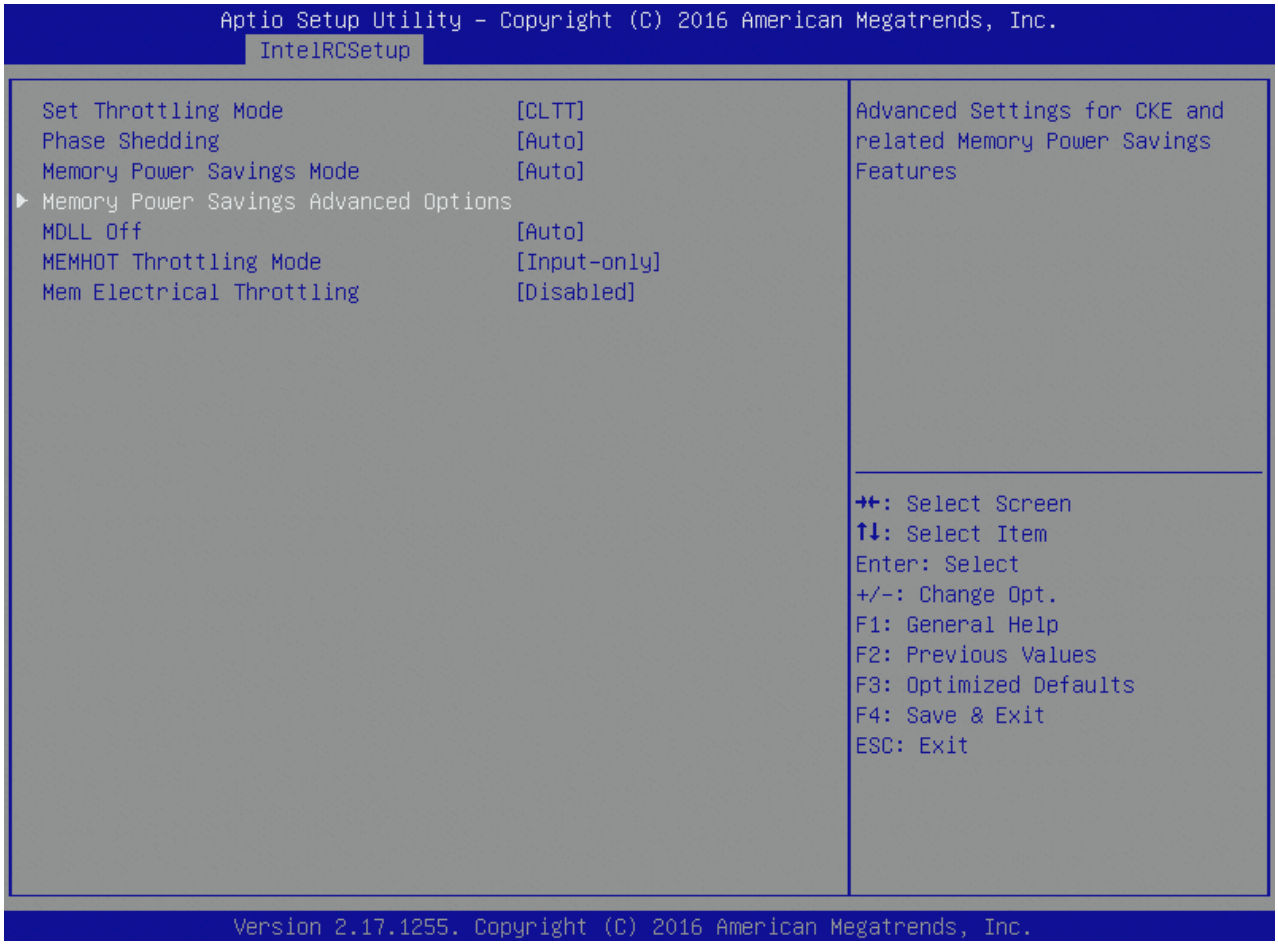


Table 92: Memory Thermal Features List

Feature	Options	Description
Set Throttling Mode	Disabled OLTT **CLTT**	Configure Thermal Throttling Mode. Select OLTT or CLTT mode.
Phase Shedding	**Auto** Disabled Enabled	DDR4 VR Static Phase Shedding Support. PS0: full-phase, PS1: single-phase, typically <18A load, PS2: fixed loss, typically <5A load
Memory Power Savings Mode	**Auto** ... User Defined	Configures CKE and related Memory Power Savings Features
MDLL Off	**Auto** Disabled Enabled	Enable to shut down MDLL during SR
MEMHOT Throttling Mode	Disabled Output-only **Input-only**	Configure MEMHOT Input and Output Mode: Mem Hot Sense Therm Throt or Mem Hot Output Therm Throt.
Mem Electrical Throttling	**Disabled** Enabled Auto	Configure Memory Electrical Throttling

6.5.3.32 Memory Power Savings Advanced Options

Figure 74: Memory Power Savings Advanced Options Menu Screen

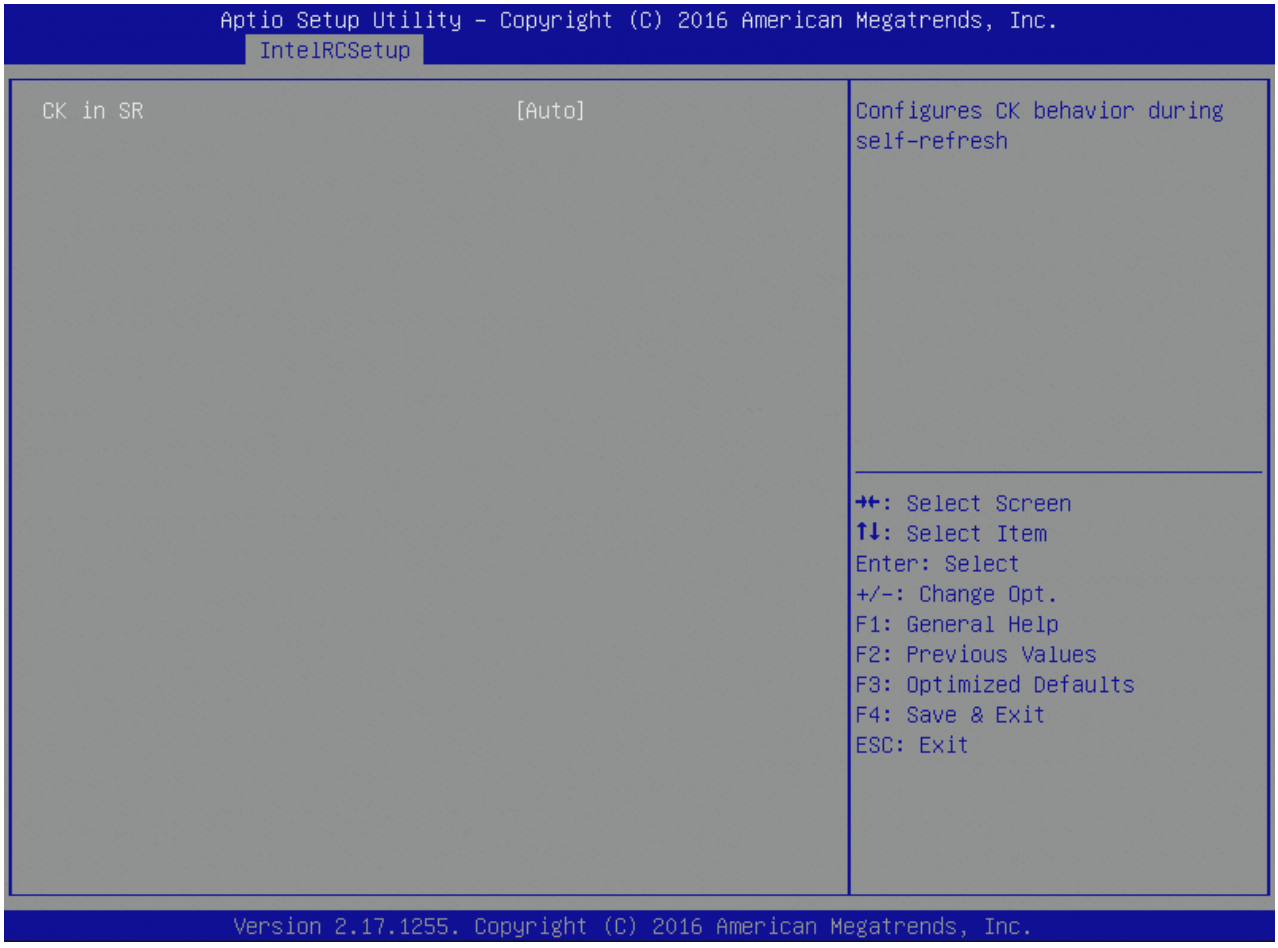


Table 93: Memory Power Savings Advanced Options Features List

Feature	Options	Description
CK in SR	**Auto** Driven Tri-State Pulled Low Pulled High	Configures CK behavior during self-refresh.

6.5.3.33 Memory Timings & Voltage Override

Figure 75: Memory Timings & Voltage Override Menu Screen



Table 94: Memory Timings & Voltage Override Features List

Feature	Options	Description
DIMM profile	Disabled Manual	Selects the XMP profile to use
Memory Frequency	**Auto** 800 …	Maximum Memory Frequency Selections in Mhz. Do not select Reserved

6.5.3.34 Memory Map

Figure 76: Memory Map Menu Screen

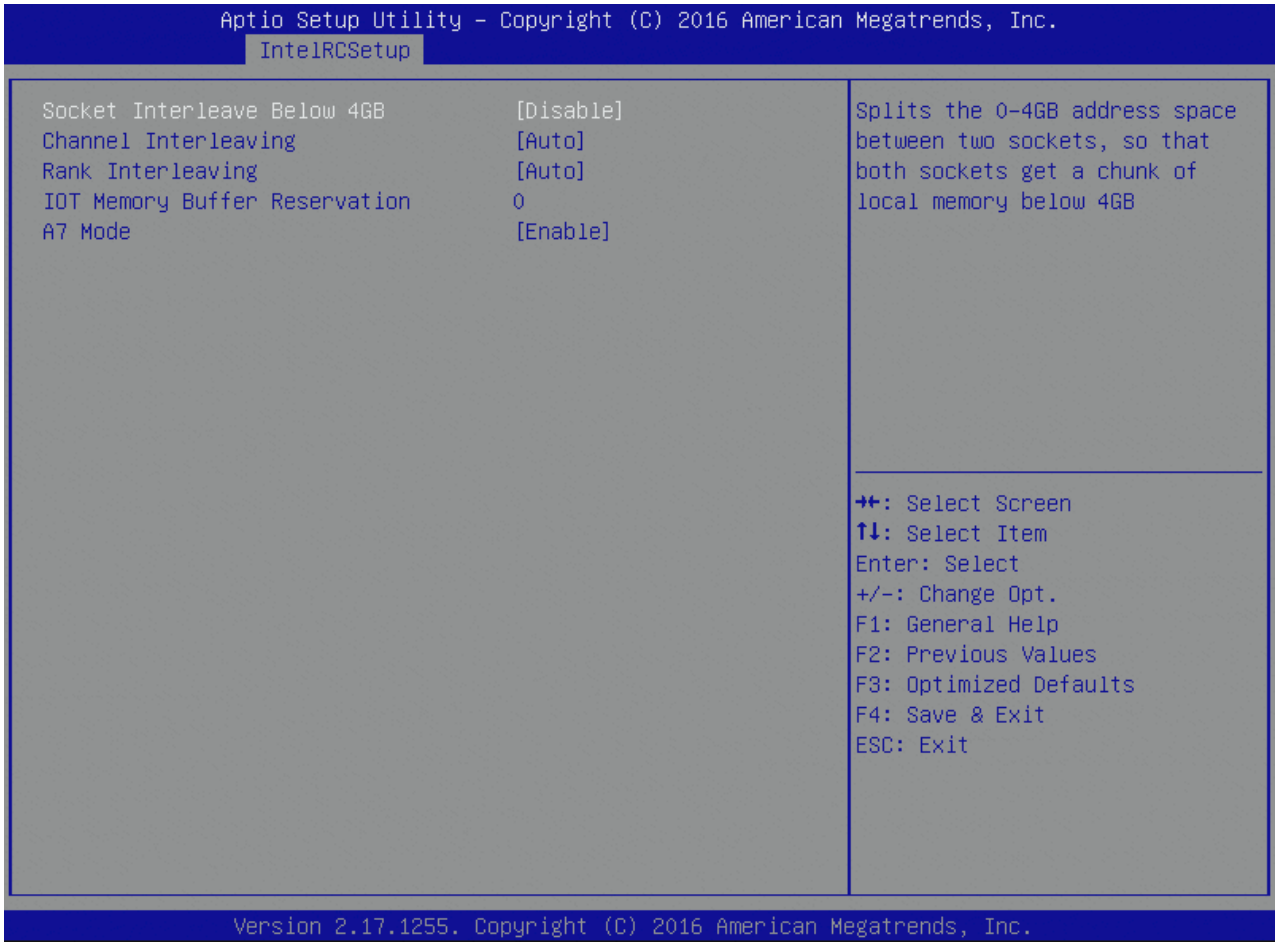


Table 95: Memory Map Features List

Feature	Options	Description
Socket Interleave Below 4GB	Disable Enable	Splits the 0-4GB address space between two sockets, so that both sockets get a chunk of local memory below 4GB
Channel Interleaving	**Auto** 1-way Interleave … 4-way Interleave	Select Channel Interleaving setting
Rank Interleaving	**Auto** 1-way Interleave … 8-way Interleave	Select Rank Interleaving setting
IOT Memory Buffer Reservation	0	Enable/Disable/Select IOT Memory Buffer Reservation
A7 Mode	Disable Enable	A7 Mode Disable/Enable

6.5.3.35 Memory RAS Configuration

Figure 77: Memory RAS Configuration Menu Screen

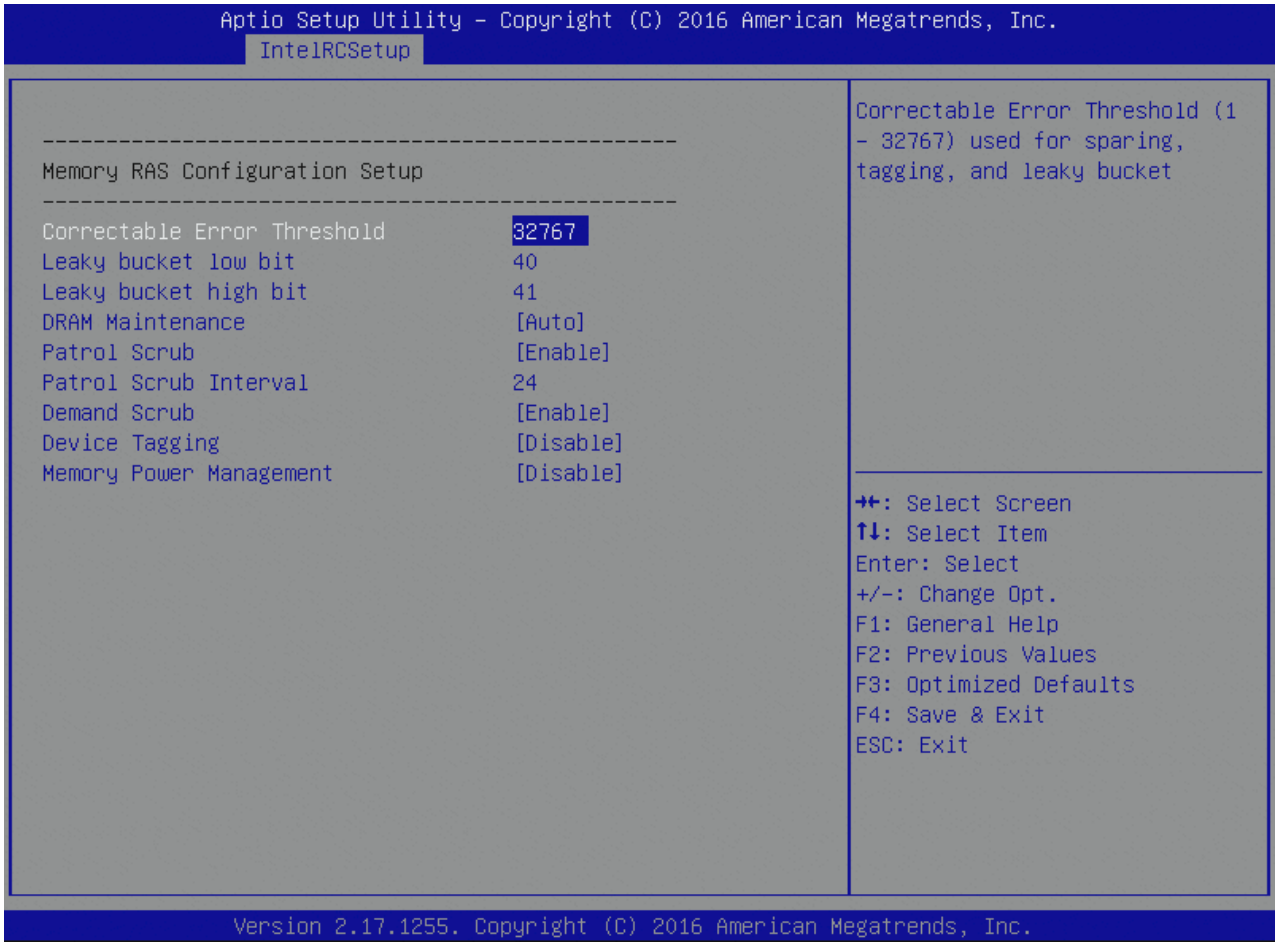


Table 96: Memory RAS Configuration Features List

Feature	Options	Description
Correctable Error Threshold	32767	Correctable Error Threshold (1 – 32767) used for sparing, tagging, and leaky bucket
Leaky bucket low bit	40	Leaky bucket low bit" (1 – 63)
Leaky bucket high bit	41	Leaky bucket high bit" (1 – 63)
DRAM Maintenance	**Auto** MANUAL Disable	Select Manual to customize DRAM Maintenance settings
Patrol Scrub	Disable Enable	Enable/Disable Patrol Scrub
Patrol Scrub Interval	24	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto!
Demand Scrub	Disable **Enable**	Enable/Disable Demand Scrub
Device Tagging	Disable Enable	Enable/Disable Device Tagging

Memory Power Management	Disable Enable	Enable Memory power management for this platform

6.5.3.36 IIO Configuration

Figure 78: IIO Configuration Menu Screen

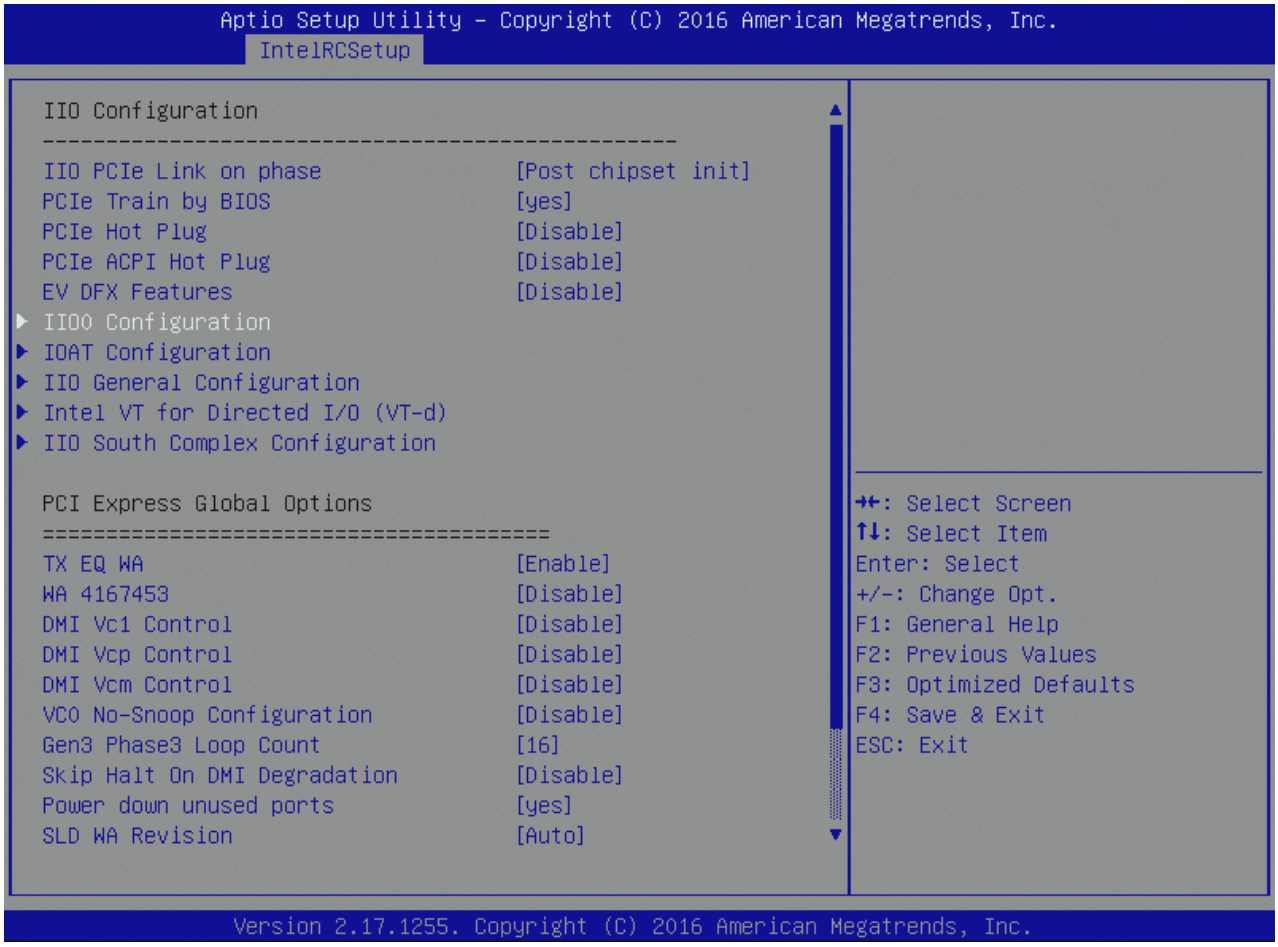


Table 97: IIO Configuration Features List

Feature	Options	Description
IIO PCIe Link on phase	Before memory chipset init **Post chipset init**	Link training can be done either before memory chipset init or post chipset init
PCIe Train by BIOS	no **yes**	Assume IIO is strapped for Wait-for-BIOS because straps are unreliable in A-O Silicon
PCIe Hot Plug	**Disable** Enable Auto MANUAL	Enable/Disable PCIe Hot Plug globally
PCIe ACPI Hot Plug	**Disable** Enable Per-Port	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.

Feature	Options	Description
EV DFX Features	Disable Enable	Set this option to allow DFX Lock Bits to remain clear
TX EQ WA	**Enable** Disable	Use special table for TX_EQ and vendor specific cards
WA 4167453	Disable Enable	Disable IIO VCP, Disable PHC VC1, set IIO VC1 & PCH VCP to TC2, clear irp_misc_dfx0.force_no_snp_on_vc1_vcm
DMI Vc1 Control	Disable Enable	Enable/Disable DMI Vc1
DMI Vcp Control	Disable Enable	Enable/Disable DMI Vcp
DMI Vcm Control	Disable Enable	Enable/Disable DMI Vcm
VC0 No-Snoop Configuration	Disable Enable	Enables No-Snoop on reads and writes for Vc0 traffic.
Gen3 Phase3 Loop Count	1 4 **16** 256	
Skip Halt On DMI Degradation	Disable Enable	Enable this option to avoid the system to be halted on DMI width/link degradation
Power down unused ports	no yes	Power down unused ports
SLD WA Revision	Auto	
Rx Clock WA	Disable Enable	Rx Clock WA
PCI-E ASPM Support (Global)	Disable L1 Only	This option enables / disables the ASPM support for all downstream devices.
PCIE Stop & Scream Support	Disable Enable	This option enables / disables PCIE Stop & Scream Support
Snoop Response Hold Off	6	Sets Snoop Response Hold Off value, 256 cycles as Default

6.5.3.37 IIO0 Configuration

Figure 79: IIO0 Configuration Menu Screen

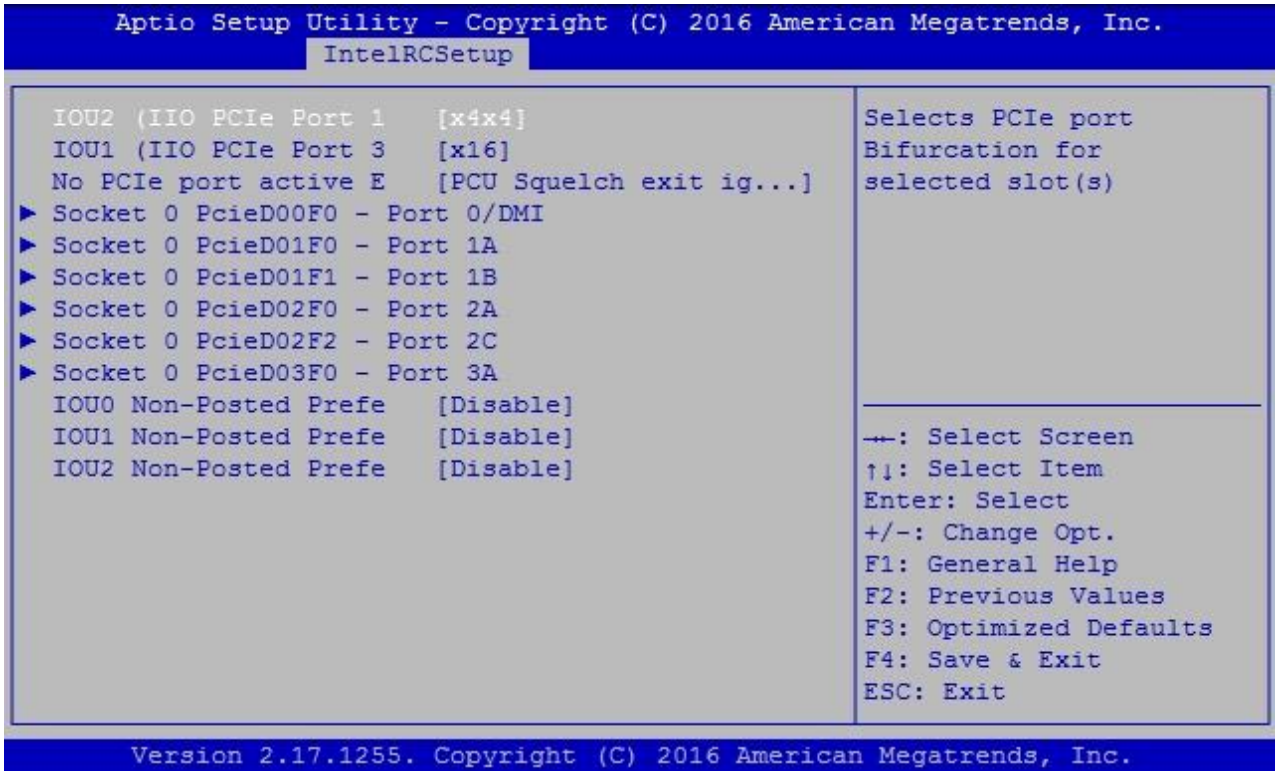


Table 98: IIO0 Configuration Features List

Feature	Options	Description
IOU2 (IIO PCIe Port 1)	**x4x4** x8 Auto	Selects PCIe port Bifurcation for selected slots(s)
IOU1 (IIO PCIe Port 3)	… **x16** Auto	Selects PCIe port Bifurcation for selected slots(s)
No PCIe port active ECOPCIe ACPI Hot Plug	PCU Squelsh exit ignore option Reset the SQ FLOP by CSR option	Workaround settings when no PCIe port active
IOU0 Non-Posted Prefetch	Enable Disable	Enable/Disable IOU0 Non-Posted Prefetch
IOU1 Non-Posted Prefetch	Enable Disable	Enable/Disable IOU1 Non-Posted Prefetch
IOU2 Non-Posted Prefetch	Enable Disable	Enable/Disable IOU2 Non-Posted Prefetch

6.5.3.38 Socket 0 PcieD00F0 - Port 0/DMI

Figure 80: Socket 0 PcieD00F0 - Port 0/DMI Menu Screen

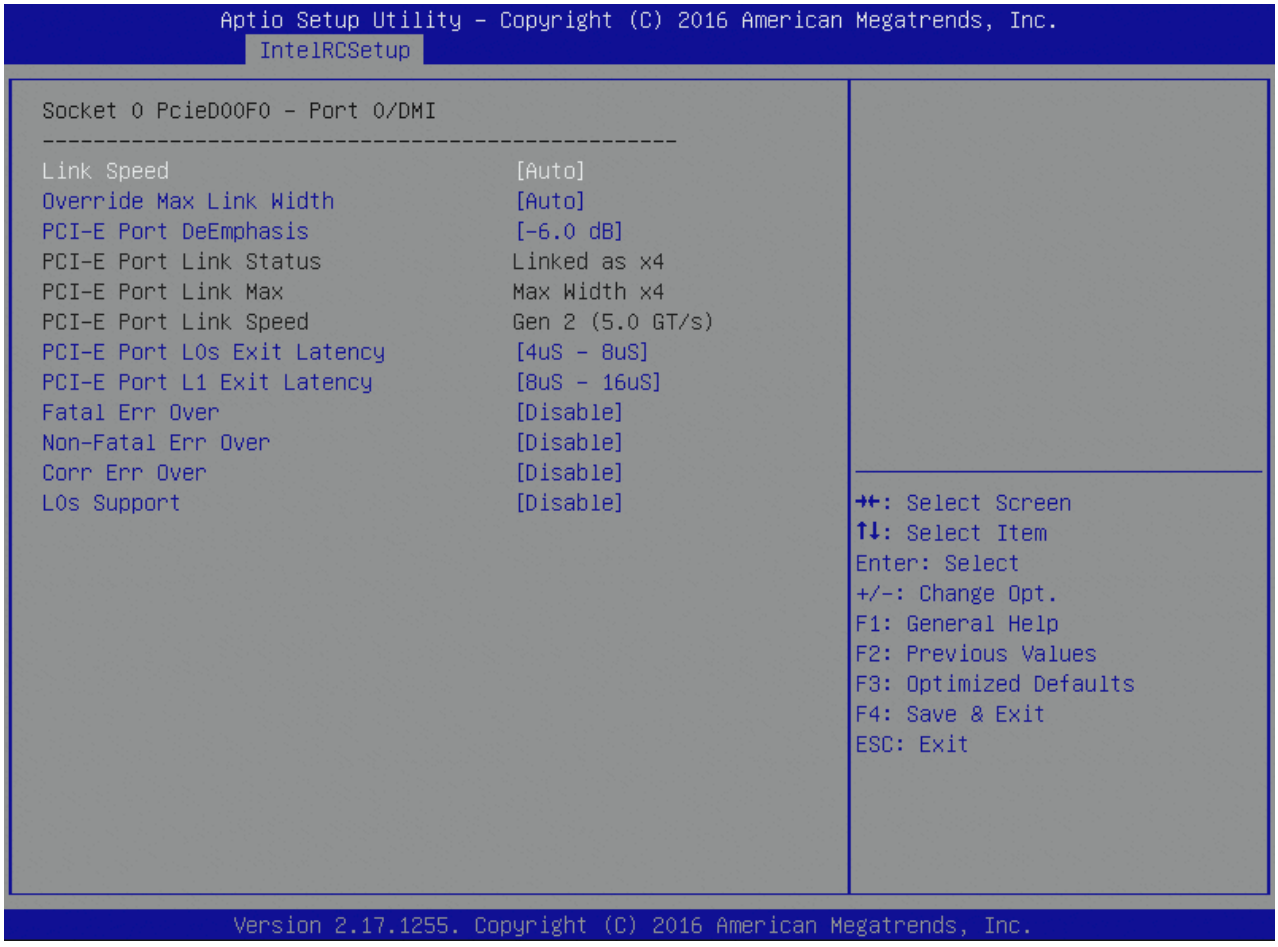


Table 99: Socket 0 PcieD00F0 - Port 0/DMI Features List

Feature	Options	Description
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s)	
Override Max Link Width	**Auto** x1 … x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	-6.0 dB -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port L0s Exit Latency	4uS – 8uS	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1 Exit Latency	<1uS … 8uS – 16uS … >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	Disable Enable	Enables forcing fatal error propogation to the IIO core error logic for this port
Non-Fatal Err Over	Disable Enable	Enable forcing non-fatal error propogation to the IIO core error logic for this port

Feature	Options	Description
Corr Err Over	Disable Enable	Enables forcing correctable error propogation to the IIO core error logic for this port
L0s Support	Disable	When disabled, IIO never puts its transmitter in L0s state

6.5.3.39 Socket 0 PcieD0XFX – Port XX

Figure 81: Socket 0 PcieD0XFX – Port XX Menu Screen

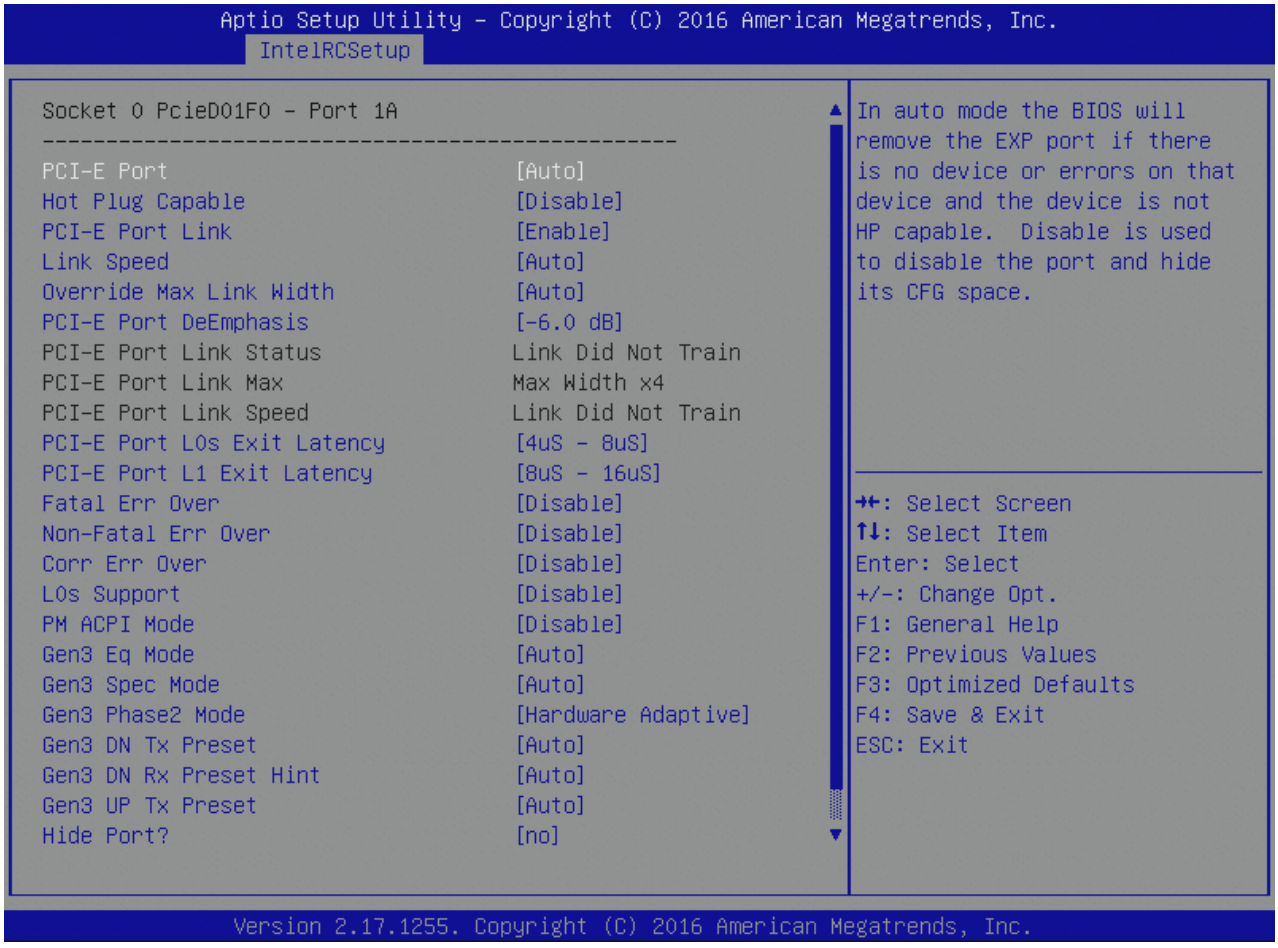


Table 100: Socket 0 PcieD0XFX – Port XX Features List

Feature	Options	Description
PCI-E Port	**Auto** Enable Disable	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	Disable Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	**Enable** Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	
Override Max Link Width	**Auto** x1 … x16	Override the max link width that was set by bifurcation

Feature	Options	Description
PCI-E Port DeEmphasis	-6.0 dB -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port L0s Exit Latency	4uS – 8uS	The length of time this port requires to complete transition from L0s to L0
PCI-E Port L1 Exit Latency	<1uS … 8uS – 16uS … >64uS	The length of time this port requires to complete transition from L1 to L0
Fatal Err Over	Disable Enable	Enables forcing fatal error propogation to the IIO core error logic for this port
Non-Fatal Err Over	Disable Enable	Enable forcing non-fatal error propogation to the IIO core error logic for this port
Corr Err Over	Disable Enable	Enables forcing correctable error propogation to the IIO core error logic for this port
L0s Support	Disable	When disabled, IIO never puts its transmitter in L0s state
PM ACPI Mode	Disable Enable	
Gen3 Eq Mode	**Auto** Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 … Alt Short Channel	PCIe Gen3 Adaptive Equilization Mode
Gen3 Spec Mode	**Auto** 0.70 July 0.70 Sept 0.71 Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	Hardware Adaptive Manual	
Gen3 DN Tx Preset	**Auto** P0 (-6.0/0.0 dB) …	PCIe Gen3 Downstream Tx Preset
Gen3 DN Rx Preset	**Auto** P0 (-6.0/0.0 dB) …	PCIe Gen3 Downstream Rx Preset Hint
Gen3 UP Tx Preset	**Auto** P0 (-6.0/0.0 dB) …	PCIe Gen3 Upstream Tx Preset
Hide Port?	no yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable **Auto**	Enable/Disable Pcie Ercr Support for this port.

6.5.3.40IOAT Configuration

Figure 82: IOAT Configuration Menu Screen



Table 101: IOAT Configuration Features List

Feature	Options	Description
Enable IOAT	Disable Enable	Control to enable/disable IOAT devices
No Snoop	Disable Enable	No Snoop Enable/Disable for each CB device
Disable TPH	**Enable** Disable	TLP processing Hint disable

6.5.3.41 IIO General Configuration

Figure 83: IIO General Configuration Menu Screen

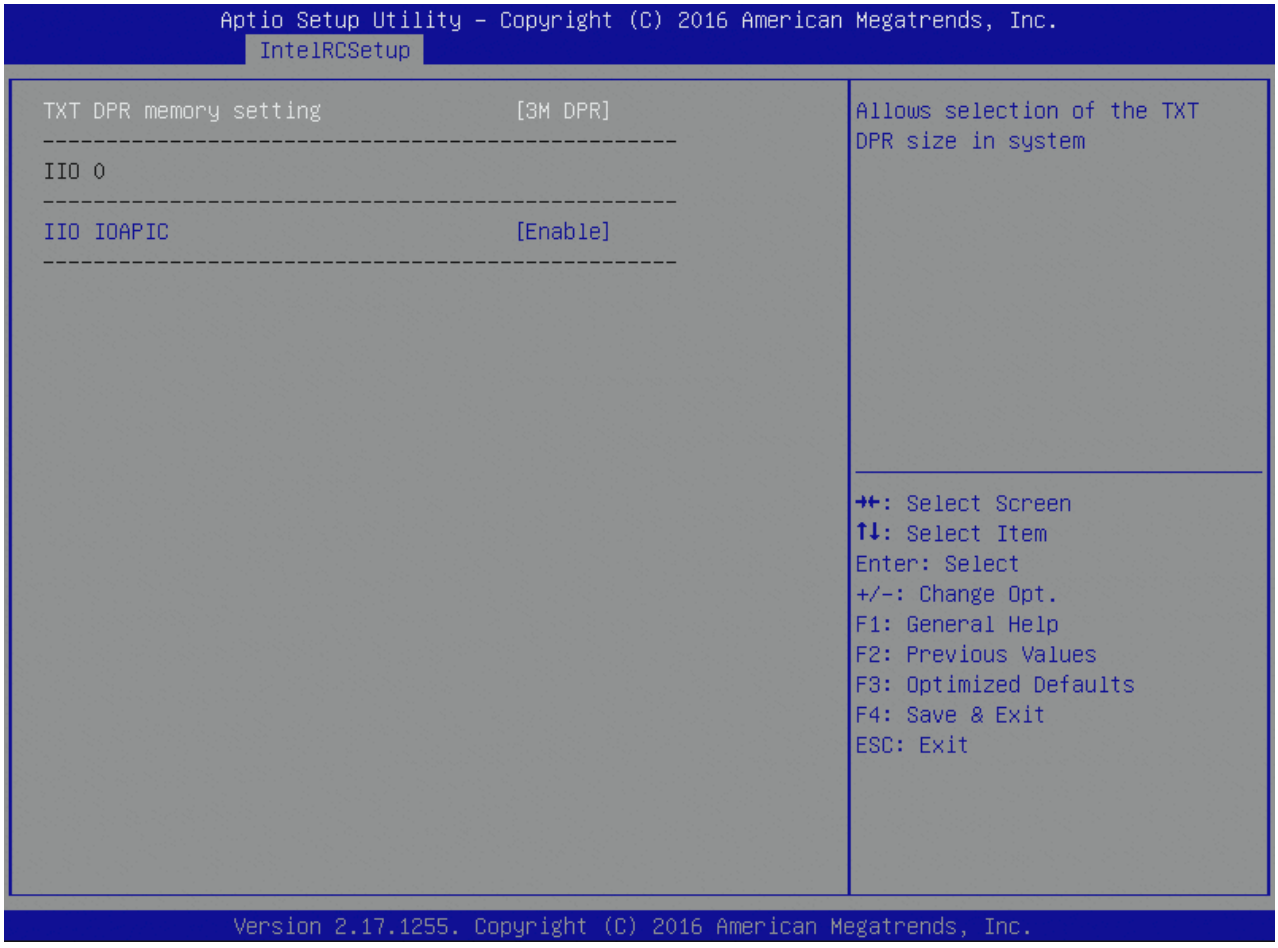


Table 102: IIO General Configuration Features List

Feature	Options	Description
TXT DPR memory setting	1M DPR 3M DPR 64M DPR 128M DPR 255M DPR	Allows selection of the TXT DPR size in system
IIO IOAPIC	Disable **Enable**	Enable / Disable the IIO IOAPIC

6.5.3.42 Intel VT for Directed I/O (VT-d)

Figure 84: Intel VT for Directed I/O (VT-d) Menu Screen

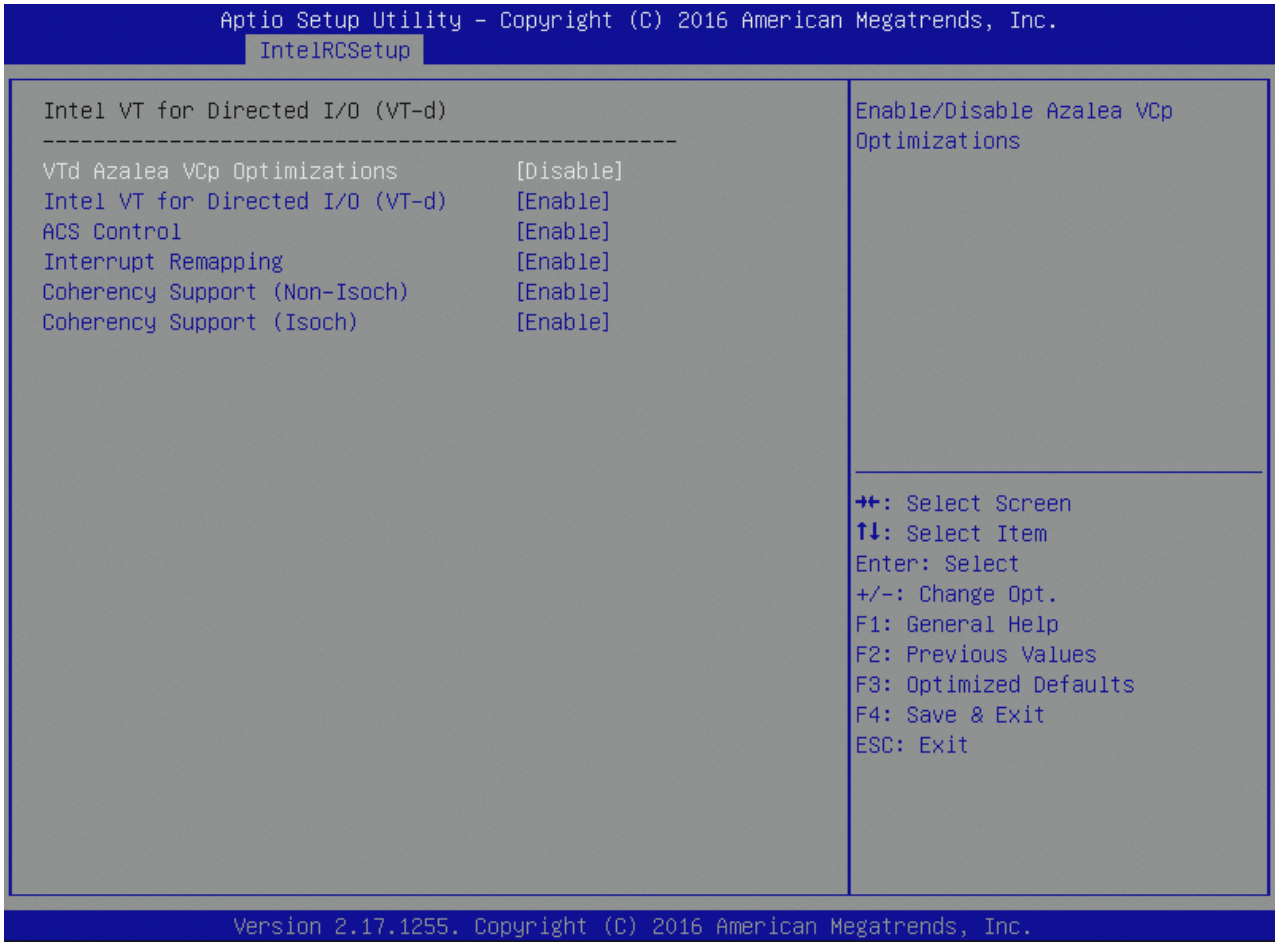


Table 103: Intel VT for Direct I/O (VT-d) Features List

Feature	Options	Description
VTd Azalea VCp Optimizations	Disable Enable	Enable/Disable Azalea VCp Optimizations
Intel VT for Directed I/O (VT-d)	**Enable** Disable	Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
ACS Control	Enable Disable	Enable: Programs ACS only to Chipset Pcie Root Ports Bridges; Disable: Programs ACS to all Pcie bridges
Interrupt Remapping	Enable Disable	Enable/Disable VT_D Interrupt Remapping Support
Coherency Support (Non-Isoch)	Enable Disable	Enable/Disable Non-Isoch VT_D Engine Coherency support
Coherency Support (Isoch)	Enable Disable	Enable/Disable Isoch VT_D Engine Coherency support

6.5.3.43 IIO South Complex Configuration

Figure 85: IIO South Complex Configuration Menu Screen

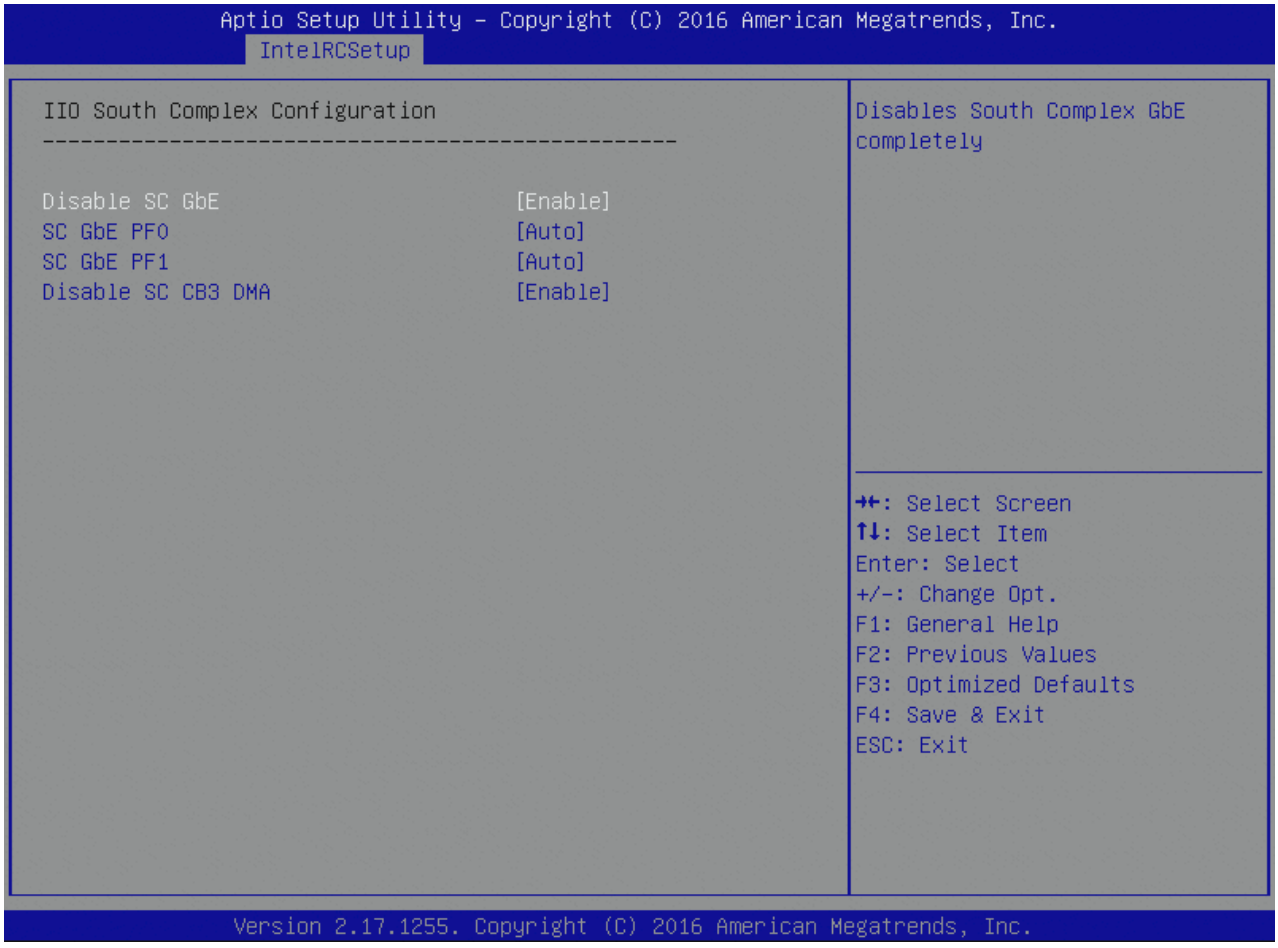
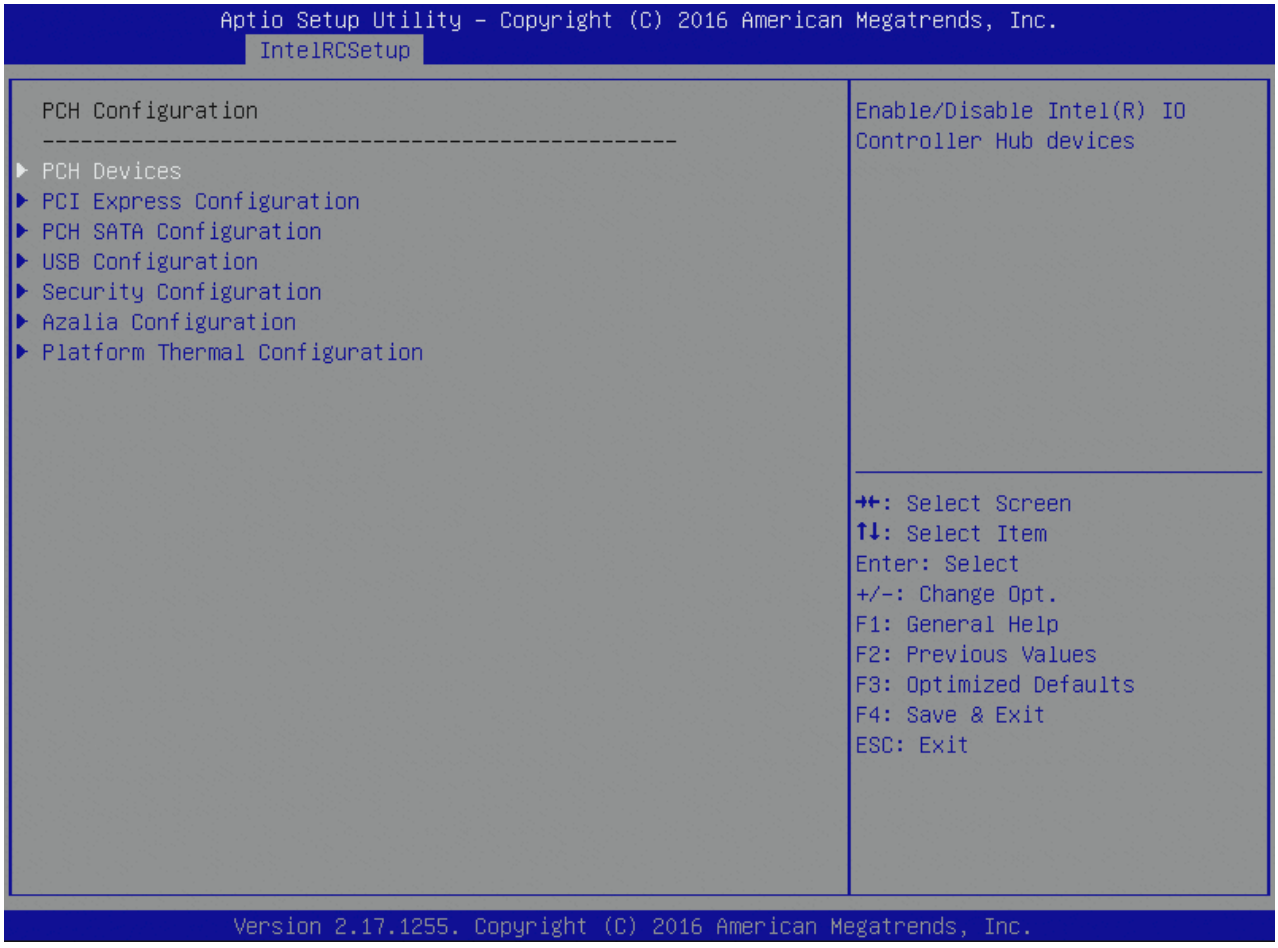


Table 104: IIO South Complex Configuration Features List

Feature	Options	Description
Disable SC GbE	Disable **Enable**	Disables South Complex GbE completely
SC GbE PF0	**Auto** Enable Disable	Force Enable / Disable SC GbE physical function 0
SC GbE PF1	**Auto** Enable Disable	Force Enable / Disable SC GbE physical function 1
Disable SC CB3 DMA	Disable **Enable**	Disables South Complex CB3 DMA completely

6.5.3.44 PCH Configuration

Figure 86: PCH Configuration Menu Screen



6.5.3.45 PCH Devices

Figure 87: PCH Devices Menu Screen

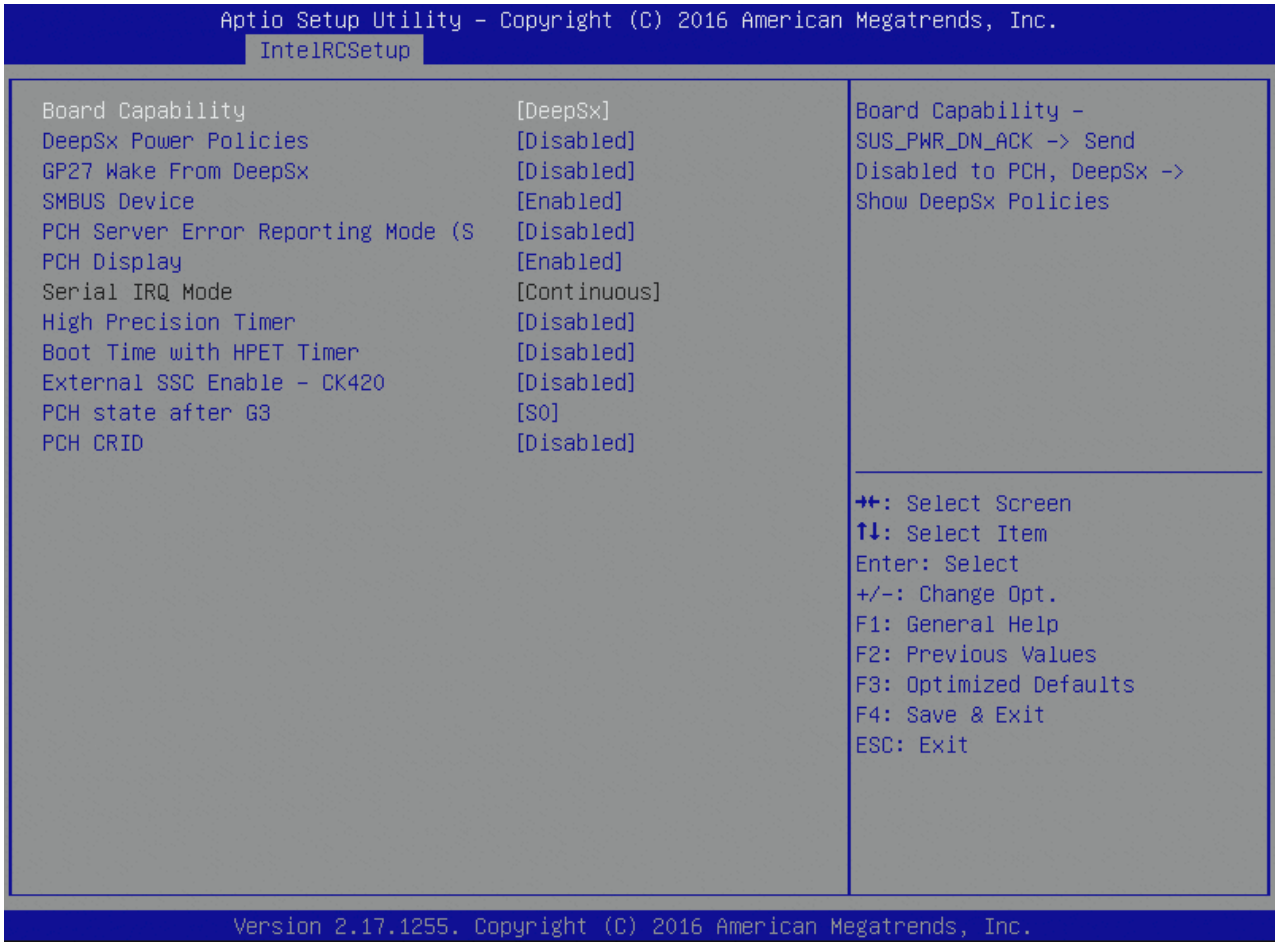


Table 105: PHC Devices Features List

Feature	Options	Description
Board Capacity	SUS_PWR_ON_ACK **DeepSx**	Board Capability – SUS_PWR_DN_ACK -> Send Disabled to PCH, DeepSx -> Show DeepSx Policies
DeepSx Power Policies	**Disabled** Enabled in S5 Enabled in S4-S5 Enabled in S3-S4-S5	configure the DeepSx Mode configuration.
GP27 Wake From DeepSx	Enabled Disabled	Wake from DeepSx by the assertion of GP27 pin
SMBUS Device	Disabled **Enabled**	Enable/Disable SMBUS Device.
PCH Server Error Reporting Mode (S	**Disabled** Enabled	When enabled MCH is the final target of all errors otherwise SPCH is the final target to all errors
PCH Display	Disabled **Enabled**	Enables/Disables PCH Display
High Precision Timer	**Disabled** Enabled	Enable or Disable the High Precision Event Timer.

Feature	Options	Description
Boot Time with HPET Timer	**Disabled** Enabled	Boot time calculation with High Precision Event Timer enabled.
External SSC Enable – CK420	**Disabled** Enabled	Enable Spread Spectrum – only affects external clock generator
PCH state after G3	**S0** S5 Last State	Select S0/S5 for ACPI state after a G3
PCH CRID	**Disabled** Enabled	Enable/Disable PCH's CRID

6.5.3.46 PCI Express Configuration

Figure 88: PCH Express Configuration Menu Screen

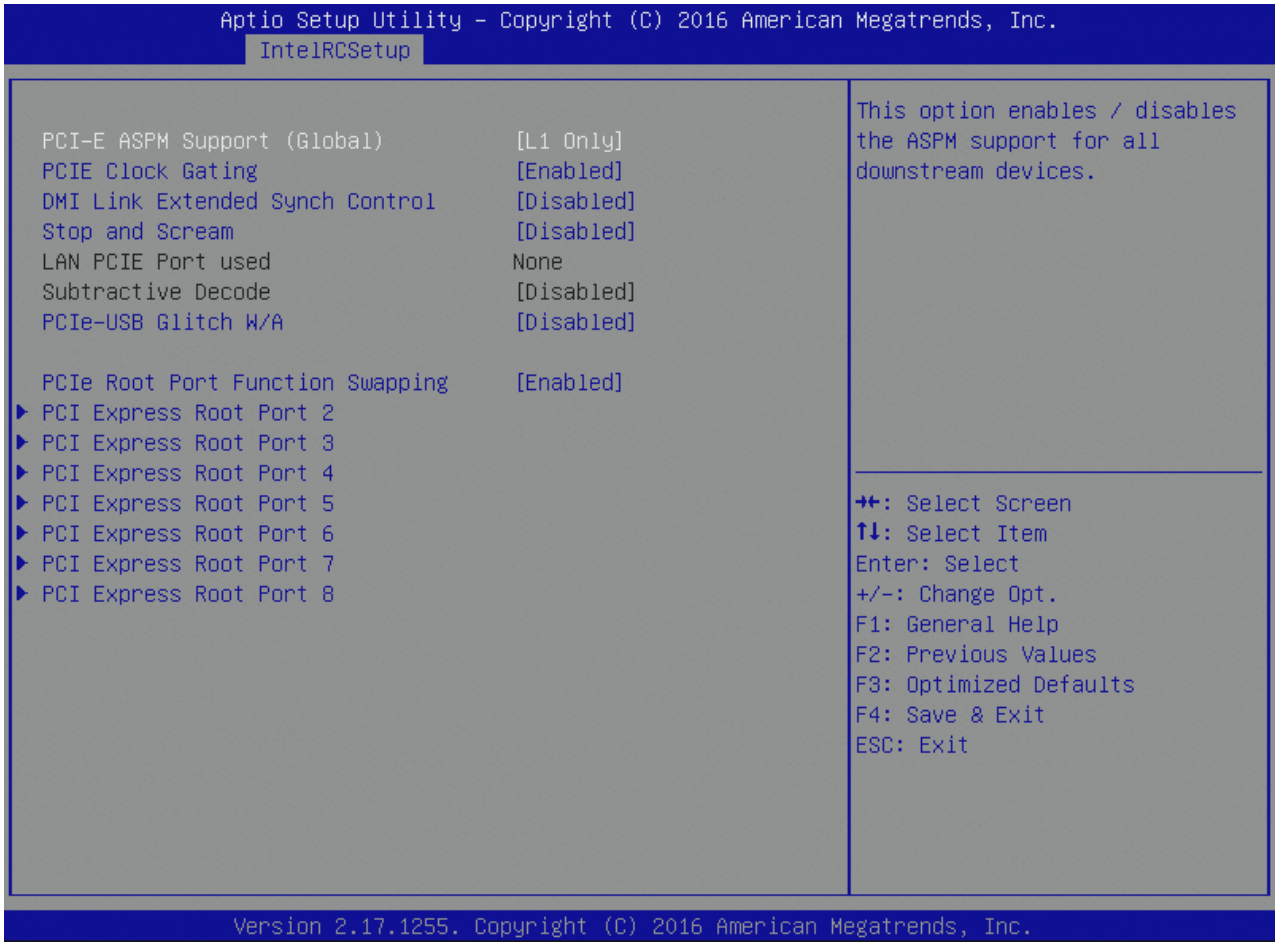


Table 106: PCH Express Configuration Features List

Feature	Options	Description
PCI-E ASPM Support (Global)	Disabled **L1 Only**	This option enables / disables the ASPM support for all downstream devices.
PCI-E Clock Gating	Disabled **Enabled**	PCIE Clock Gating Enable/Disable for all PCH PCIE Ports.
DMI Link Extended Synch Control	Disabled Enabled	The control of Extended Synch on SB slide of the DMI Link.
Stop and Screame	Disabled Enabled	When Enabled DS packets on DMI with the EP bit set, will have their UT bit set.
PCIe-USB Glitch W/A	**Disabled** Enabled	PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port.
PCIe Root Port Function Swapping	Disabled **Enabled**	Enable PCIe root port function swapping feature to dynamically assign function 0 to enabled root port.

6.5.3.47 PCI Express Root Port

Figure 89: PCH Express Root Port Menu Screen

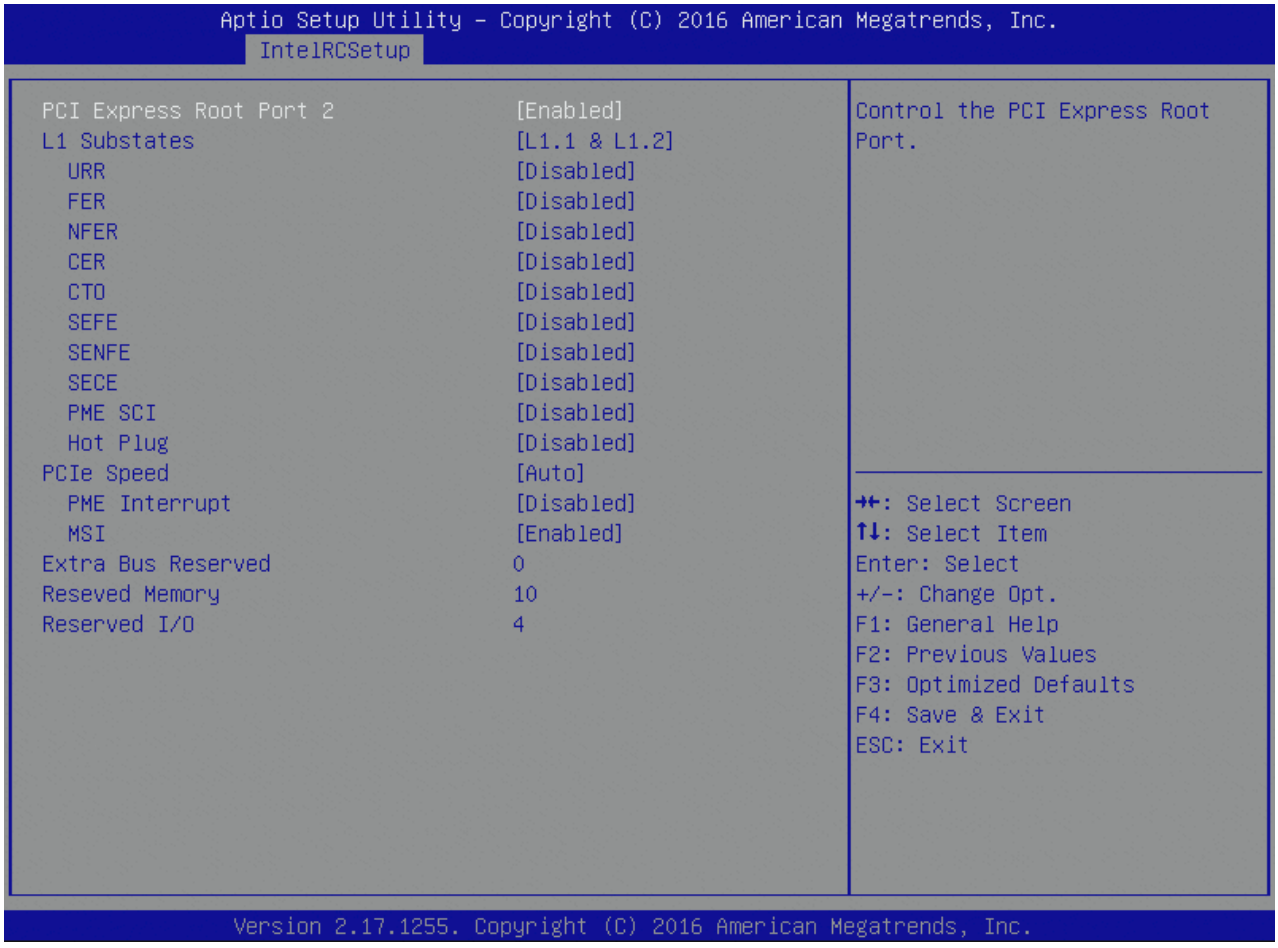


Table 107: PCH Express Root Port Features List

Feature	Options	Description
PCI Express Root Port	Disabled **Enabled**	Control the PCI Express Root Port.
L1 Substates	Disabled … **L1.1 & L1.2**	PCI Express L1 Substates settings.
URR	Disabled Enabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled Enabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled Enabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	**Disabled** Enabled	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	Disabled Enabled	PCI Express Completion Timer T0 Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.

Feature	Options	Description
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	**Disabled** Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled** Enabled	PCI Express Hot Plug Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2	Configure PCIe Speed
PME Interrupt	**Disabled** Enabled	PCI Express PME Interrupt Enable/Disable.
MSI	Disabled **Enabled**	PCIE MSI Enable/Disable.
Extra Bus Reserved	0	Extra Bus Reserved (0-7) for bridges behind this root Bridge.
Reseved Memory	10	Reserved Memory and Prefetchable Memory (1-20MB) Range for this Root Bridge.
Reserved I/O	4	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.

6.5.3.48PCH SATA Configuration

Figure 90: PCH SATA Configuration Menu Screen

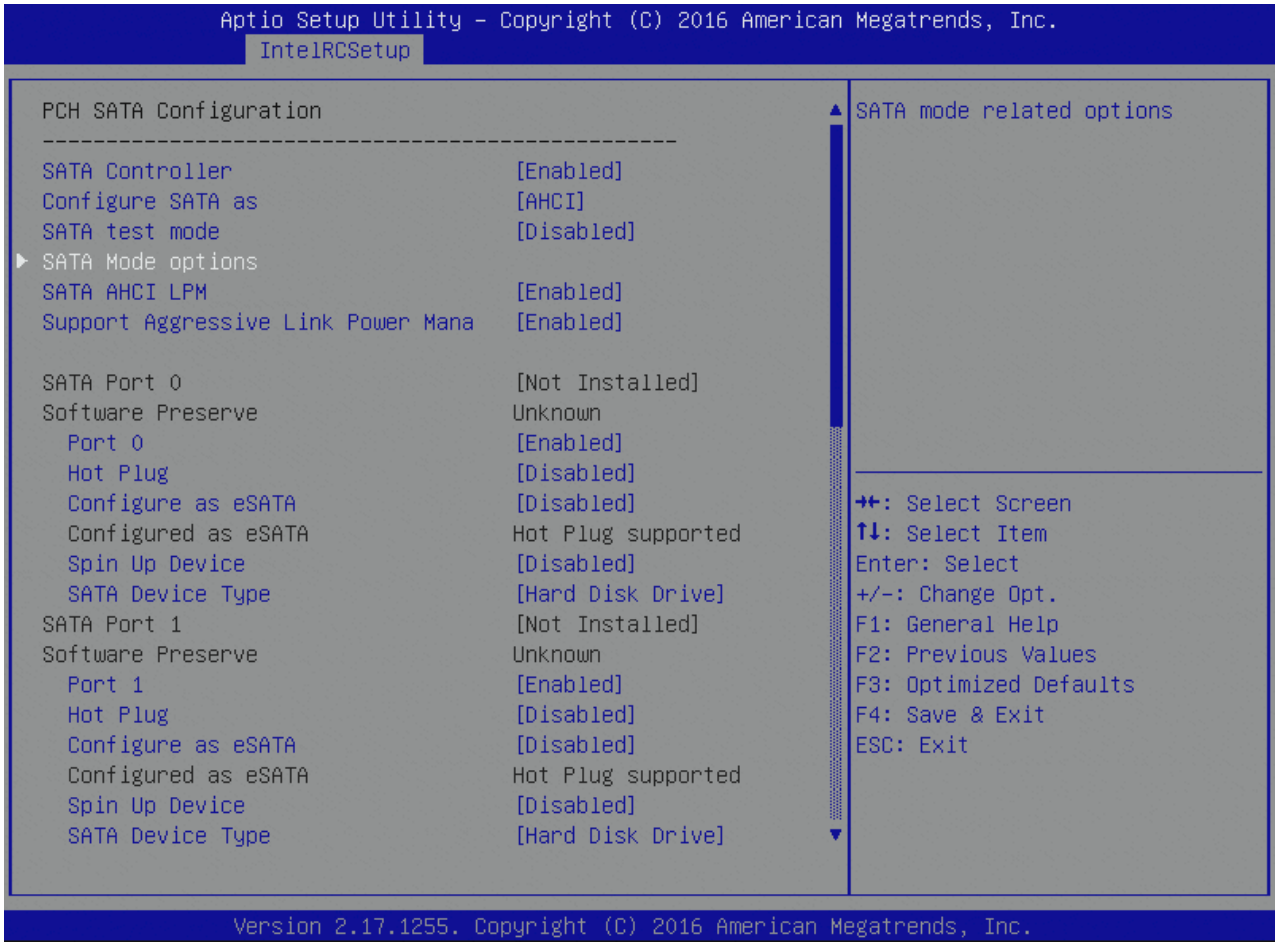


Table 108: PCH SATA Configuration Features List

Feature	Options	Description
SATA Controller	Disabled **Enabled**	Enable or Disable SATA Controller
Configure SATA as	IDE **AHCI**	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
SATA test mode	Enabled Disabled	Enable/Disable SATA test mode
SATA AHCI LPM	Disabled **Enabled**	Enables/Disables Link Power Management
Support Aggressive Link Power Mana	Disabled **Enabled**	Enables/Disables SALP
For each SATA Port:		
Port	Disabled **Enabled**	Enable or Disable SATA Port
Hot Plug	Disabled Enabled	Designates this port as Hot Pluggable.

Feature	Options	Description
Configure as eSATA	**Disabled** Enabled	Configures port as External SATA (eSATA)
Spin Up Device	**Disabled** Enabled	If enabled for any of ports Staggered Spin Up will be performed and only the drivers which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

6.5.3.49 SATA Mode Options

Figure 91: SATA Mode Options Menu Screen



Table 109: SATA Mode Options Features List

Feature	Options	Description
SATA HDD Unlock	Disabled **Enabled**	Enable: HDD password unlock is enabled in the OS
SATA Led locate	Disabled **Enabled**	If enabled LED/SGPIO hardware is attached

6.5.3.50 USB Configuration

Figure 92: USB Configuration Menu Screen

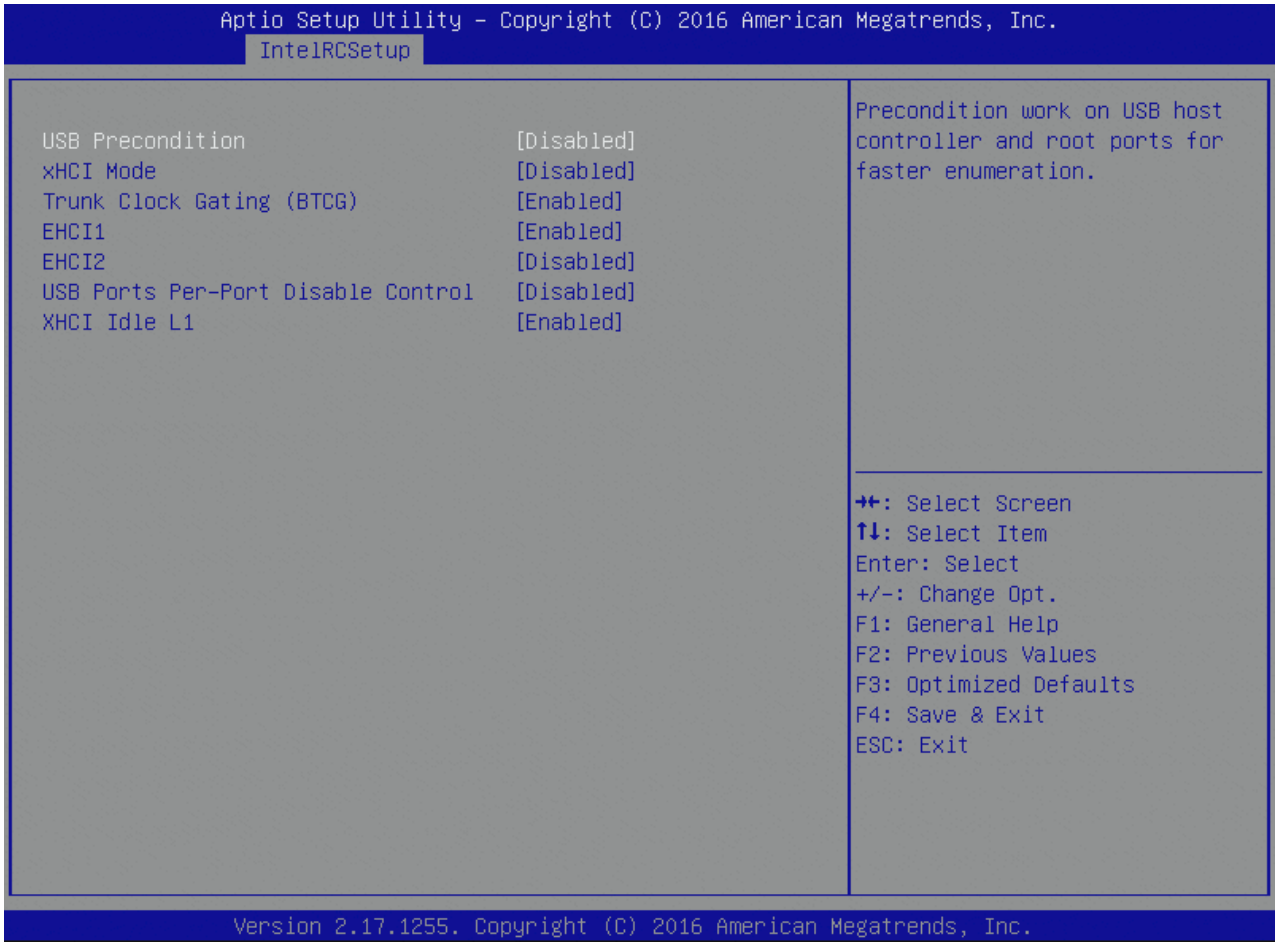


Table 110: USB Configuration Features List

Feature	Options	Description
USB Precondition	Enabled **Disabled**	Precondition work on USB host controller and root ports for faster enumeration.
xHCI Mode	Smart Auto ... **Disabled** Manual	Mode of operation of xHCI controller.
Trunk Clock Gating (BTCG)	**Enabled** Disabled	Enable/Disable BTCG.
EHCI1	Disabled **Enabled**	Control the USB EHCI (USB 2.0) functions. One EHCI controller must always be enabled.
EHCI2	Disabled Enabled	Control the USB EHCI (USB 2.0) functions. One EHCI controller must always be enabled.
USB Per-Port Control	**Disabled** Enabled	Control each of the USB ports (0~13) disabling.
XHCI Idle L1	**Enabled** Disabled	Enabled XHCI Idle L1. Disabled to workaround USB3 hot plug will fall after 1 hot plug removal. Please put the system to G3 for the new settings to take effect.

6.5.3.51 Security Configuration

Figure 93: Security Configuration Menu Screen

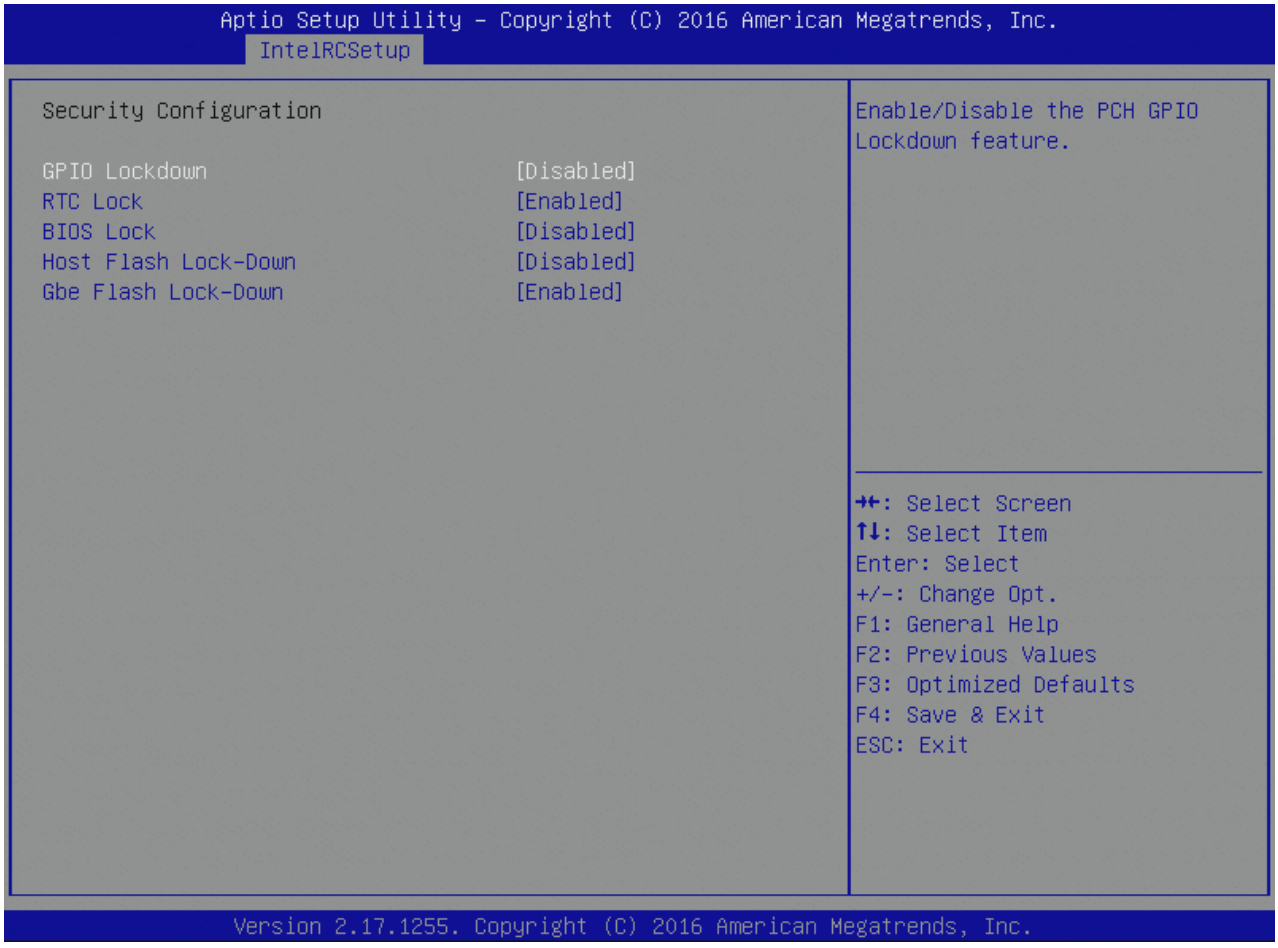


Table 111: Security Configuration Features List

Feature	Options	Description
GPIO Lockdown	**Disabled** Enabled	Enable/Disable the PCH GPIO Lockdown feature.
RTC Lock	Disabled **Enabled**	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank o fRTC RAM
BIOS Lock	Disabled Enabled	Enable/Disable the PCH BIOS Lock Enable feature.
Host Flash Lock-Down	Disabled Enabled	Enable/Disable Host Flash Lock-Down
Gbe Flash Lock-Down	Disabled **Enabled**	Enable/Disable Gbe Flash Lock-Down

6.5.3.52 Azalia Configuration

Figure 94: Azalia Configuration Menu Screen

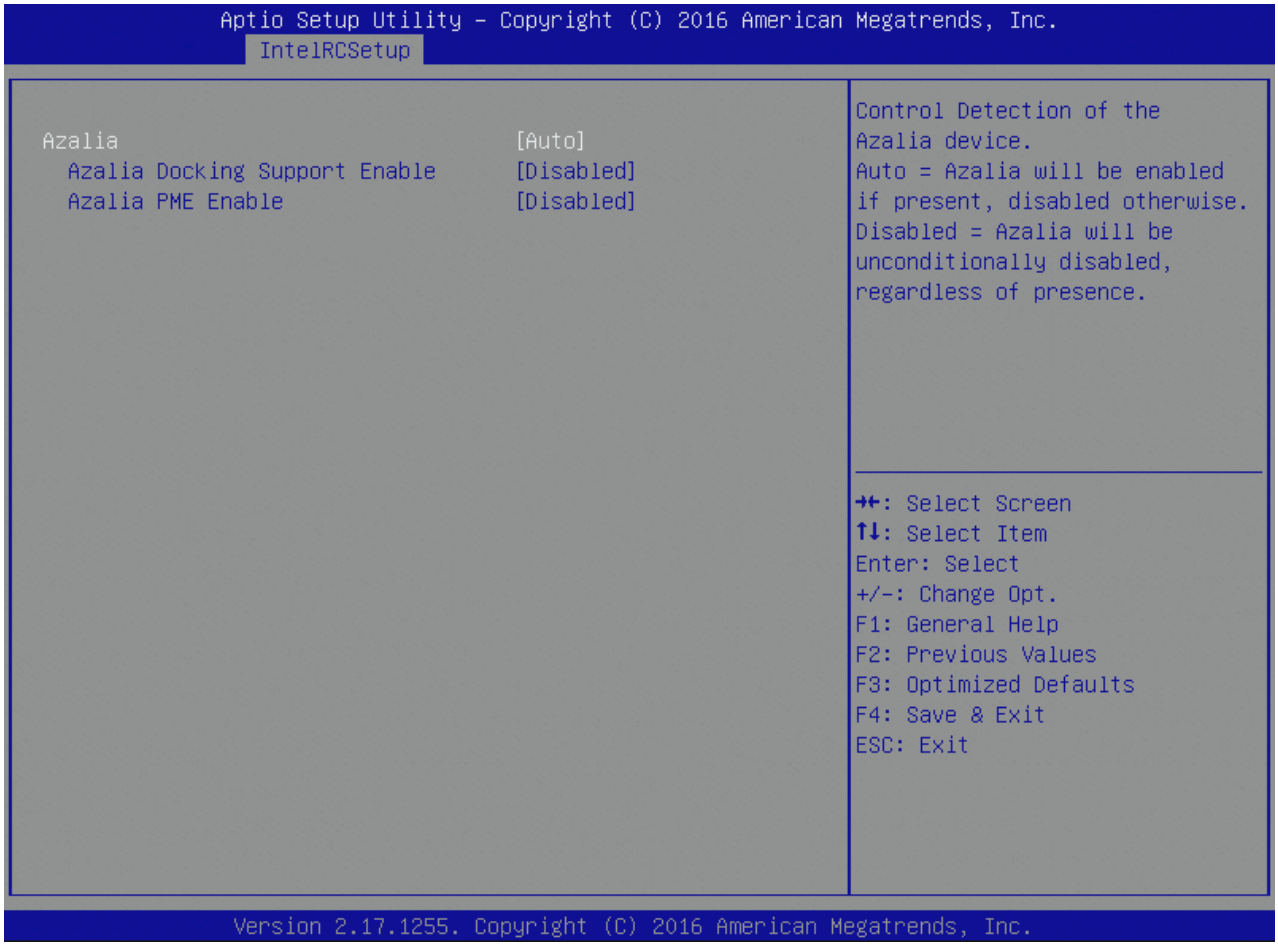


Table 112: Azalia Configuration Features List

Feature	Options	Description
Azalia	Disabled Enabled **Auto**	Control Detection of the Azalia device. Auto = Azalia will be enabled if present, disabled otherwise. Disabled = Azalia will be unconditionally disabled, regardless of presence.
Azalia Docking Support Enable	**Disabled** Enabled	Enable/Disable Azalia Docking Support of Audio Controller.
Azalia PME Enable	Disabled Enabled	Enable/Disable PME for Azalia.

6.5.3.53 Platform Thermal Configuration

Figure 95: Platform Thermal Configuration Menu Screen

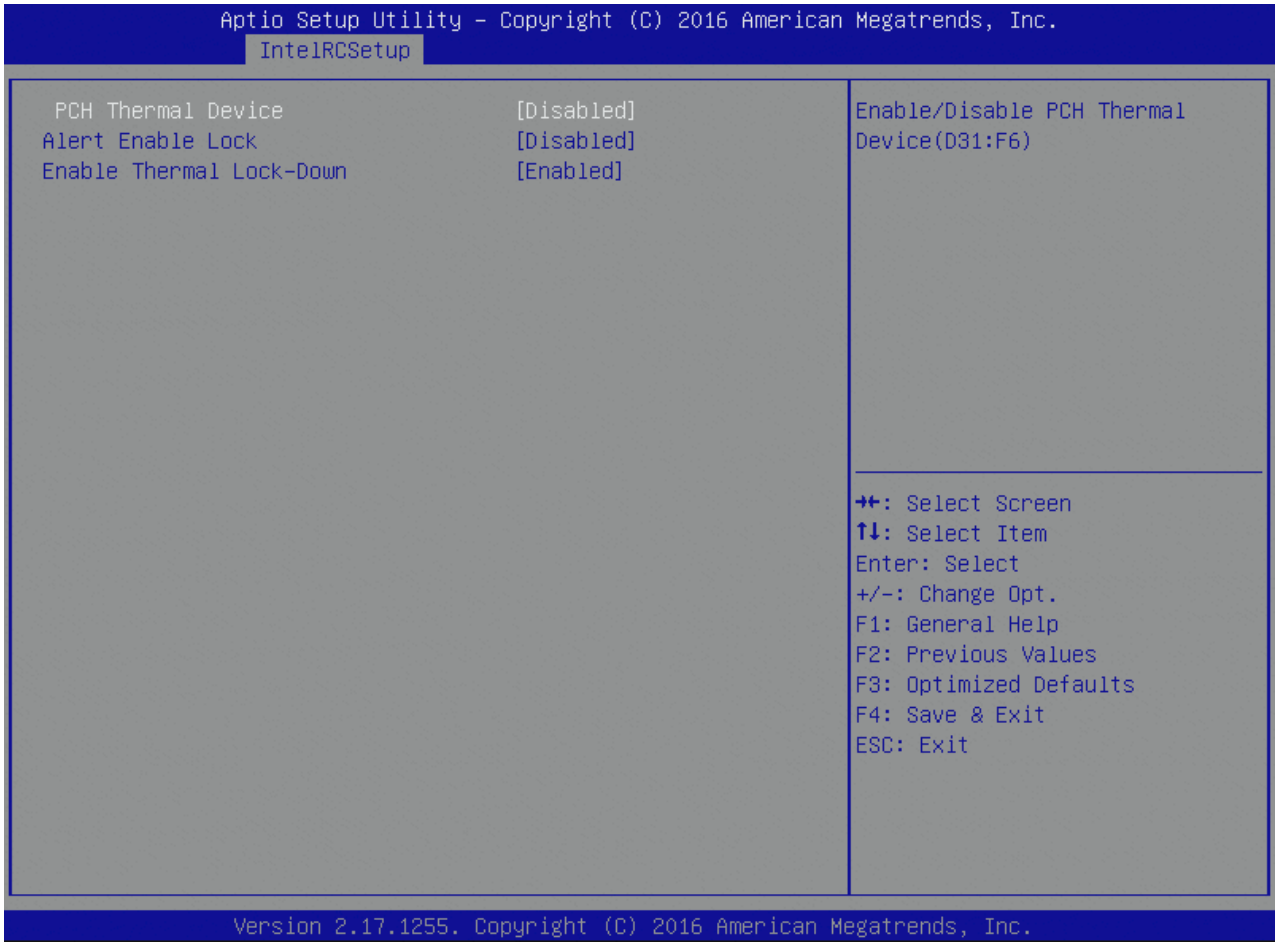


Table 113: Platform Thermal Configuration Features List

Feature	Options	Description
PCH Thermal Device	**Disabled** Enabled Auto	Enable/Disable PCH Thermal Device(D31:F6)
Alert Enable Lock	**Disabled** Enabled	Lock all Alert Enable settings
Enable Thermal Lock-Down	Disabled **Enabled**	Enable will execute thermal programming, use disable as WA for PCHHOT

6.5.3.54 Miscellaneous Configuration

Figure 96: Miscellaneous Configuration Menu Screen

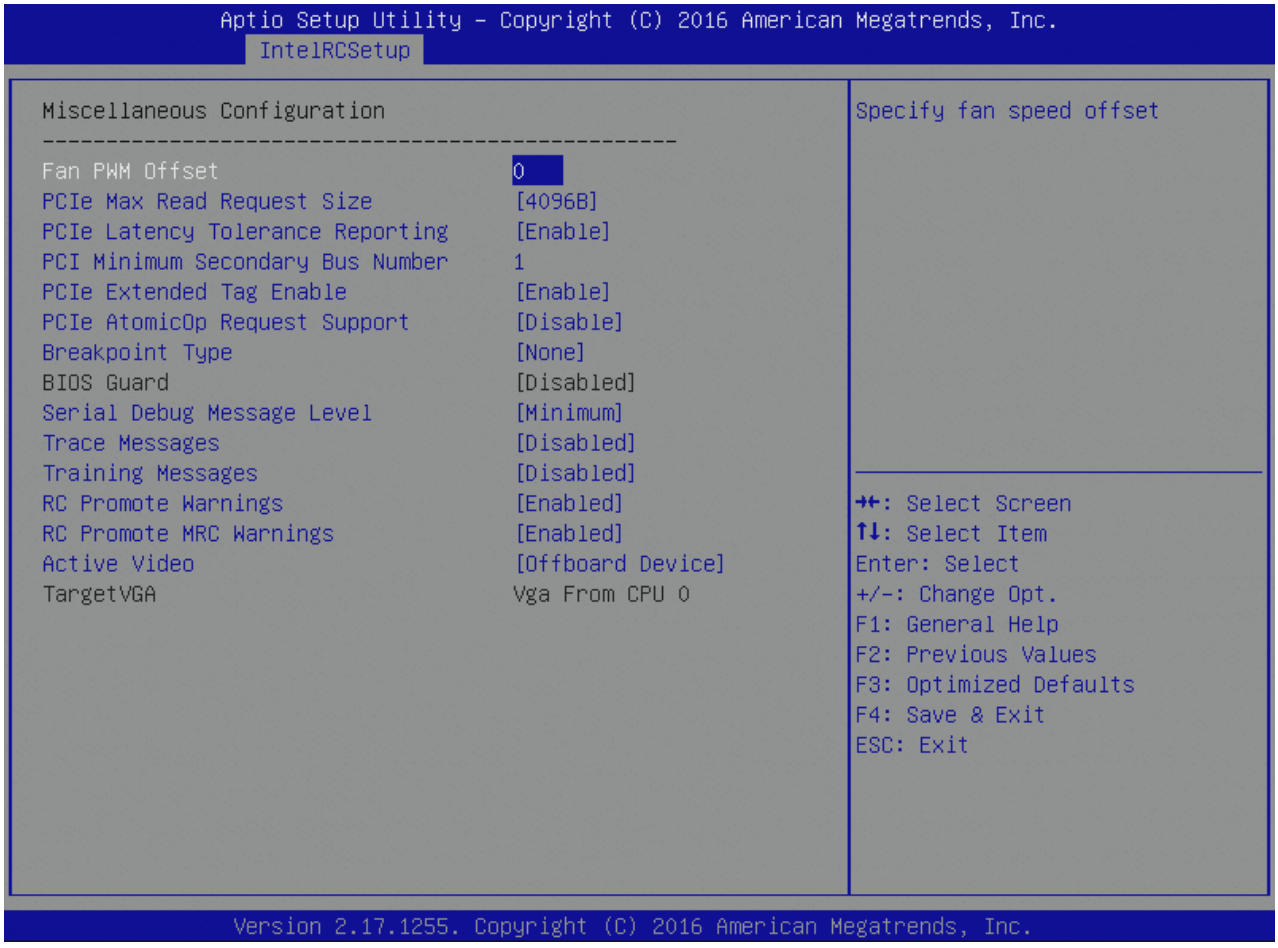


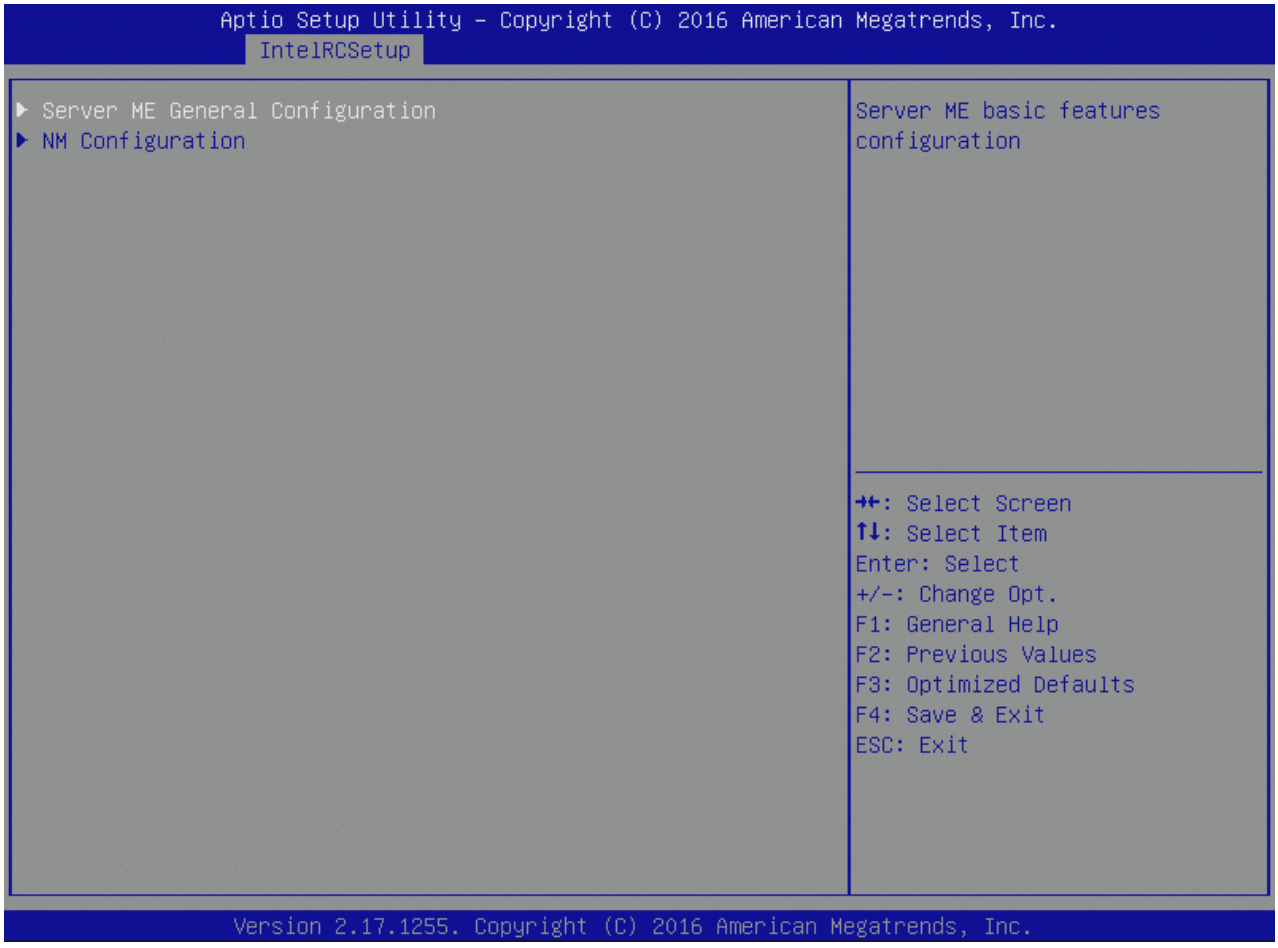
Table 114: Miscellaneous Configuration Features List

Feature	Options	Description
Fan PWM Offset	0	Specify fan speed offset
PCIe Max Read Request Size	128B 256B … **4096B**	Set Max Rest Request Size
PCIe LAtency Tolerance Reporting	Disable **Enable**	Enable or Disable or Auto the LTR support
PCI Minimum Secondary Bus Number	1	Specify the PCI minimum secondary bus number in system
PCIe Extended Tag Enable	Auto Disable **Enable**	Enable or Disable Extended Tag Enable Field Support
PCIe AtomicOp Request Support	**Disable** Enable	Enable or disable AtomicOp Request Support
Breakpoint Type	**None** After MRC After QPIRC …	Halt at specified points in BIOS

Feature	Options	Description
	Ready for IBIST	
Serial Debug Message Level	Disable **Minimum** Normal Maximum	Disable = no serial debug message, Minimum = high level debug messages, Normal = general debug messages
Trace Messages	**Disabled** Enabled Enabled for registry writes only.	Enables display of every IO access
Training Messages	**Disabled** Enabled	Enabled = set to disable the training results. Training results also get displayed if debug messages is set to Maximum.
RC Promote Warnings	Disabled **Enabled**	If enabled RC warnings are promoted to errors (except MRC warnings)
RC Promote MRC Warnings	Disabled **Enabled**	If enabled MRC warnings are promoted to errors
Active Video	Onboard Device **Offboard Device**	Select active Video type

6.5.3.55 Server ME Debug Configuration

Figure 97: Server ME Debug Configuration Menu Screen



6.5.3.56 Server ME General Configuration

Figure 98: Server ME General Configuration Menu Screen

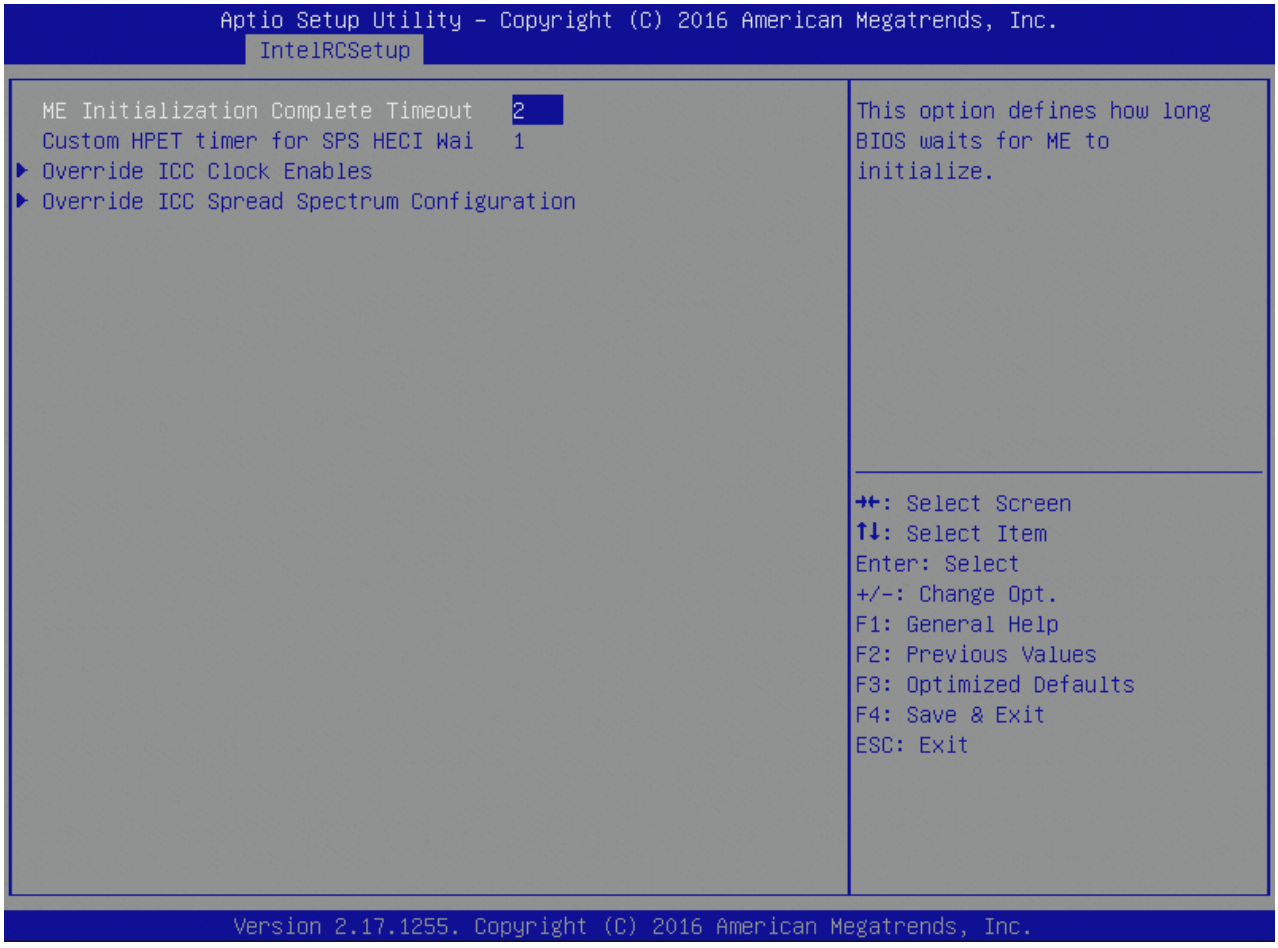


Table 115: Server ME General Configuration Features List

Feature	Options	Description
ME Initialization Complete Timeout	2	This option defines how long BIOS waits for ME to initialize.
Custom HPET timer for SPS HECI wai	1	Custom HPET timer for SPS HECI Waiting

6.5.3.57 Override ICC Clock Enables

Figure 99: Override ICC Clock Enables Menu Screen

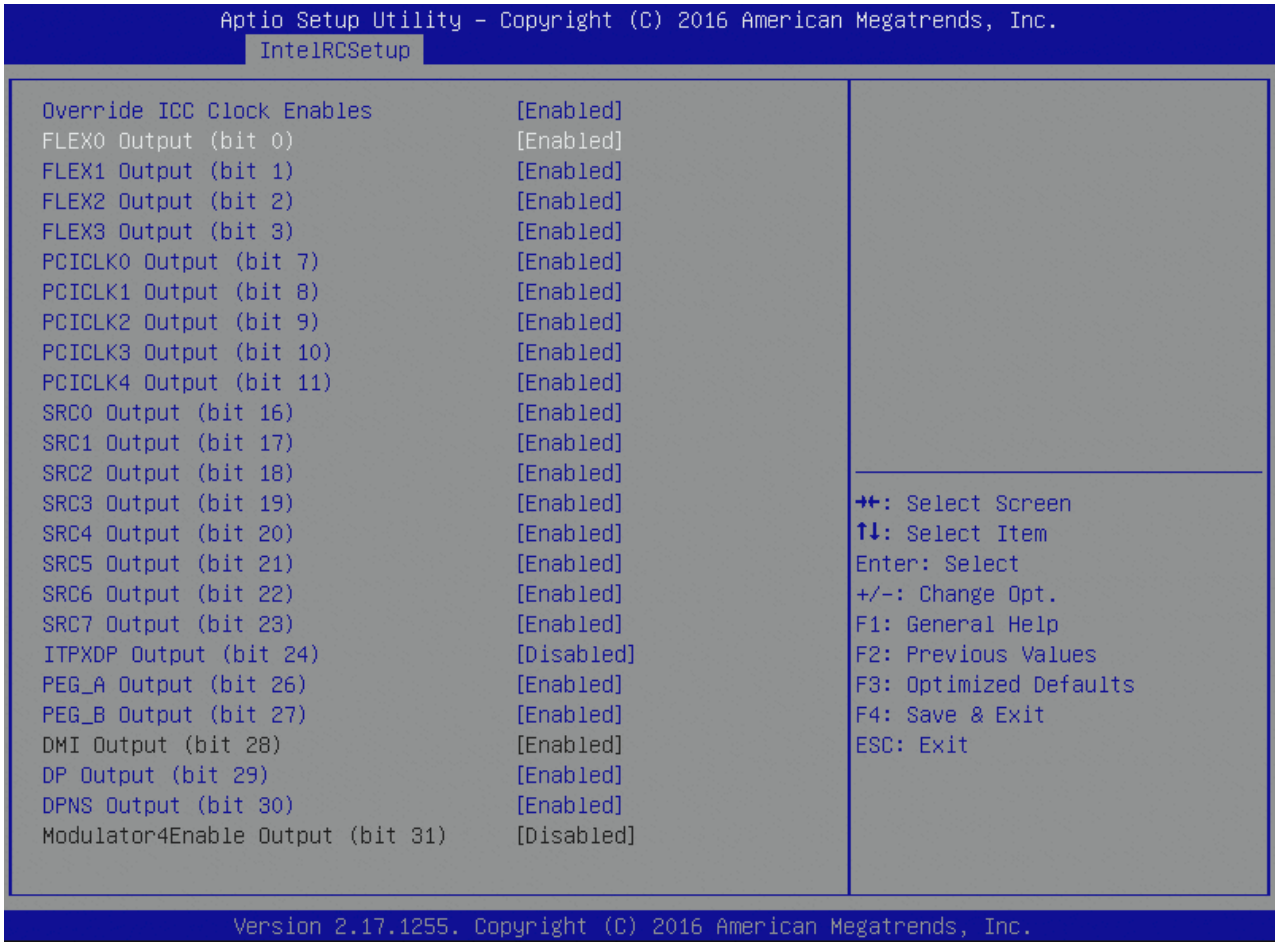


Table 116: Override ICC Clock Enables Features List

Feature	Options	Description
Override ICC Clock Enables	Disabled **Enabled**	This option allows customization of clock enables.
FLEX0 Output (bit 0)	Disabled **Enabled**	
FLEX0 Output (bit 1)	Disabled Enabled	
FLEX0 Output (bit 2)	Disabled Enabled	
FLEX0 Output (bit 3)	Disabled Enabled	
PCICL0 Output (bit 7)	Disabled Enabled	
PCICL1 Output (bit 8)	Disabled Enabled	

Feature	Options	Description
PCICL2 Output (bit 9)	Disabled **Enabled**	
PCICL3 Output (bit 10)	Disabled **Enabled**	
PCICL4 Output (bit 11)	Disabled **Enabled**	
SRC0 Output (bit 16)	Disabled **Enabled**	
SRC1 Output (bit 17)	Disabled **Enabled**	
SRC2 Output (bit 18)	Disabled **Enabled**	
SRC3 Output (bit 19)	Disabled **Enabled**	
SRC4 Output (bit 20)	Disabled **Enabled**	
SRC5 Output (bit 21)	Disabled **Enabled**	
SRC6 Output (bit 22)	Disabled **Enabled**	
SRC7 Output (bit 23)	Disabled **Enabled**	
ITPXDP Output (bit 24)	Disabled Enabled	
PEG_A Output (bit 26)	Disabled **Enabled**	
PEG_B Output (bit 27)	Disabled **Enabled**	
DP Output (bit 29)	Disabled **Enabled**	
DPNS Output (bit 30)	Disabled **Enabled**	

6.5.3.58 Override ICC Spread Spectrum Configuration

Figure 100: Override ICC Spectrum Configuration Menu Screen

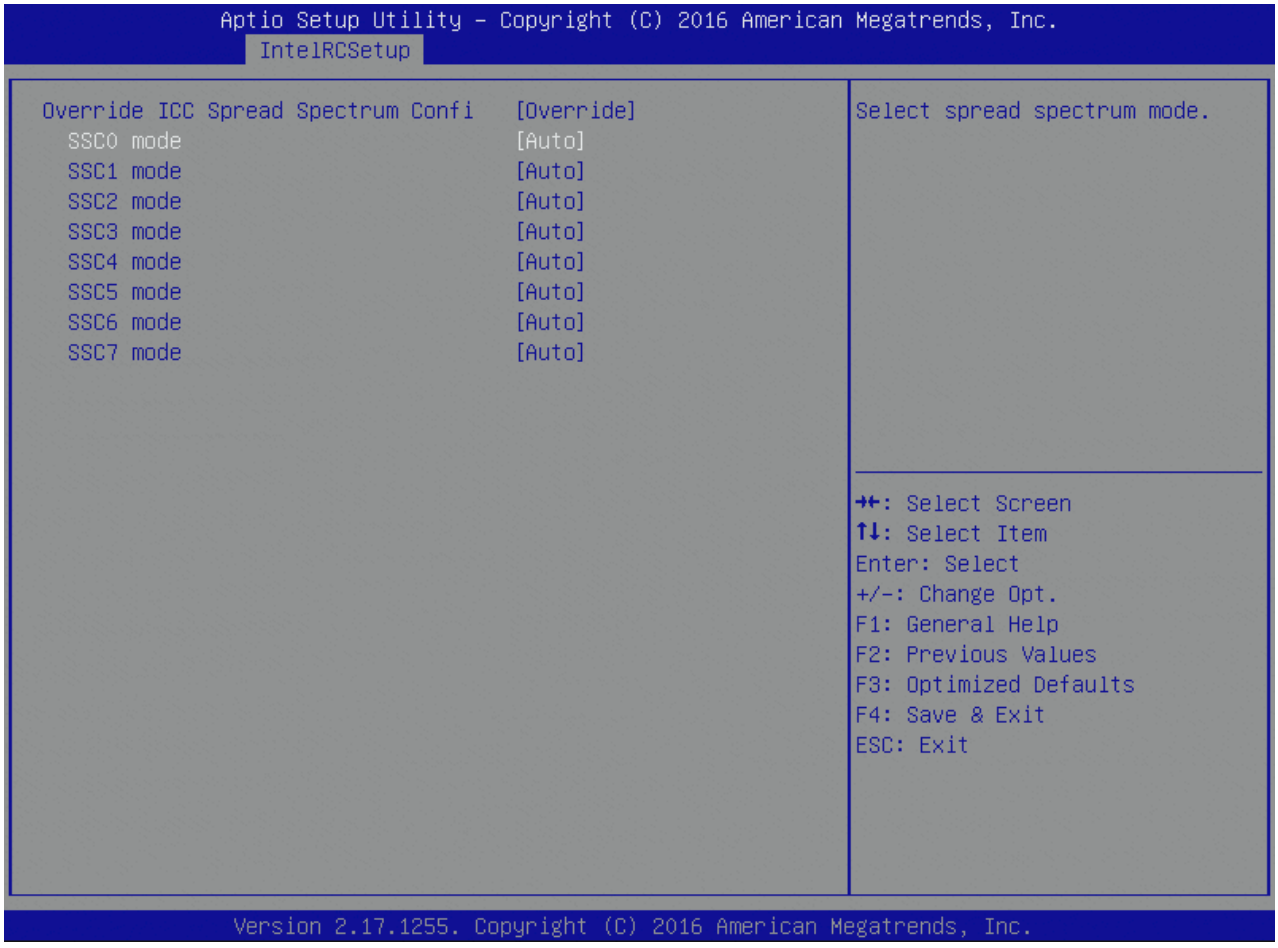


Table 117: Override ICC Spectrum Configuration Features List

Feature	Options	Description
Override ICC Spread Spectrum Confi	Override Auto	Set non-default ICC spread spectrum configuration.
SSC0 mode … SSC7 mode	Down Center Disable DoNotChange **Auto**	Select spread spectrum mode.

6.5.3.59 NM Configuration

Figure 101: NM Configuration Menu Screen

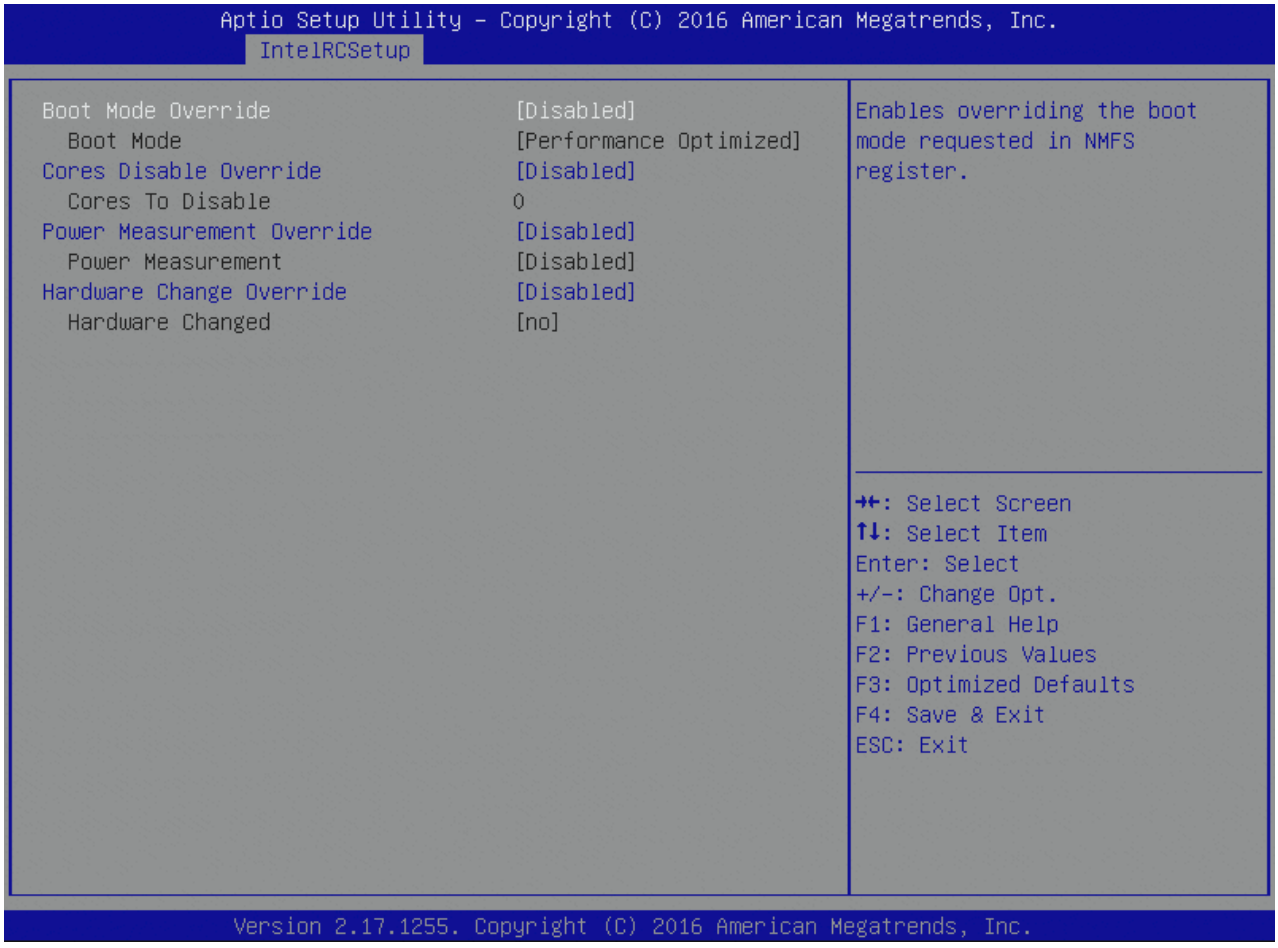


Table 118: NM Configuration Features List

Feature	Options	Description
Boot Mode Override	Disabled Enabled	Enables overriding the boot mode requested in NMFS register.
Boot Mode	Performance Optimized Power Optimized	The boot mode to use instead of the mode requested in NMFS register.
Cores Disable Override	Disabled Enabled	Enables overriding the value of the number of cores to disable requested in NMFS register.
Cores to Disable	0	The number of cores to disable instead of the number requested in NMFS register.
Power Measurement Override	Disabled Enabled	Override power measurement support status reported to ME
Power Measurement	Disabled Enabled	Override power measurement support status reported to ME
Hardware Change Override	Disabled Enabled	Override hardware change detection status reported to ME
Hardware Changed	no **yes**	Override hardware change detection status reported to ME

6.5.3.60 Server ME Configuration

Figure 102: Server ME Configuration Menu Screen

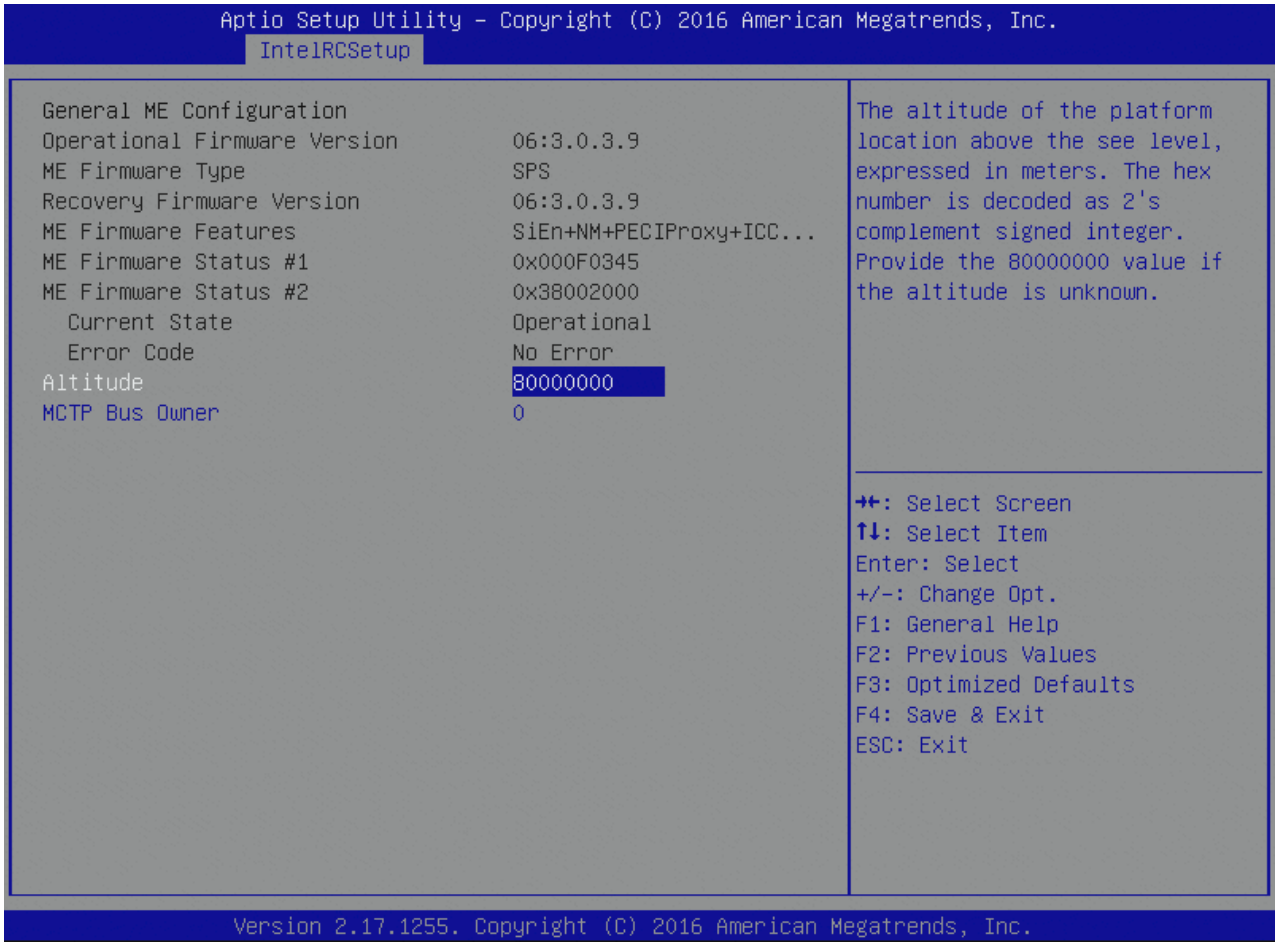


Table 119: Server ME Configuration Features List

Feature	Options	Description
Altitude	80000000	The altitude of the platform location above the see level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 80000000 value if the altitude is unknown.
MCTP Bus Owner	0	MTCP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.

6.5.3.61 Runtime Error Logging

Figure 103: Runtime Error Logging Menu Screen

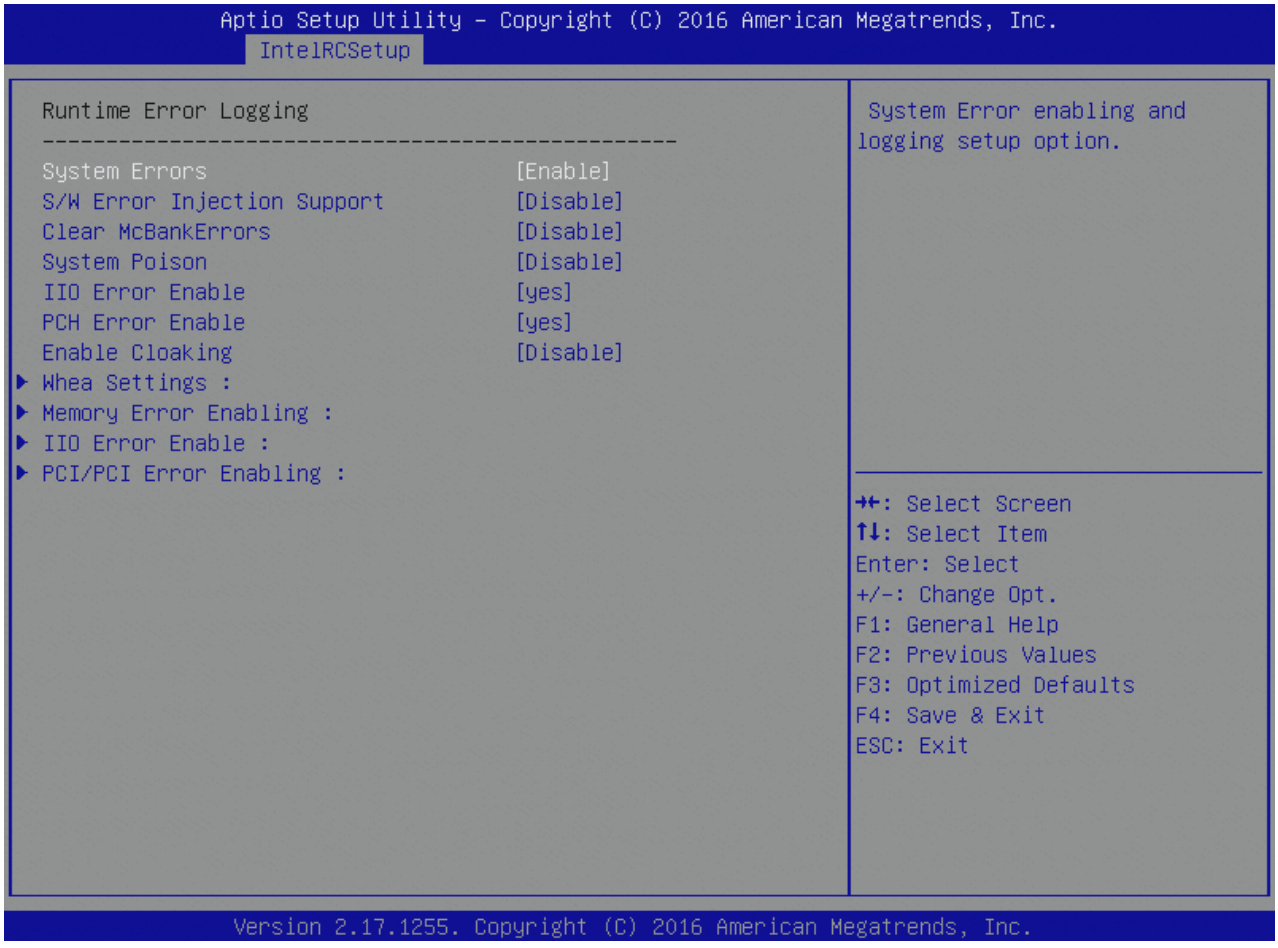


Table 120: Runtime Error Logging Features List

Feature	Options	Description
System Errors	Disable **Enable** Auto	System Error enabling and logging setup option.
S/W Error Injection Support	**Disable** Enable	When Enabled S/W Error Injection is supported by unlocking MSR 0x790
Clear McBankErrors	Disable Enable	Enables or Disables clearing MCBank erros on warm reset.
System Poison	Disable Enable	Enable/Disable Core, Uncore and IIO Poison
IIO Error Enable	no yes	
PCH Error Enable	no yes	
Enable Cloaking	Enable Disable	Enable / Disable Corrected Error Cloaking

6.5.3.62 Whea Settings

Figure 104: Whea Settings Menu Screen

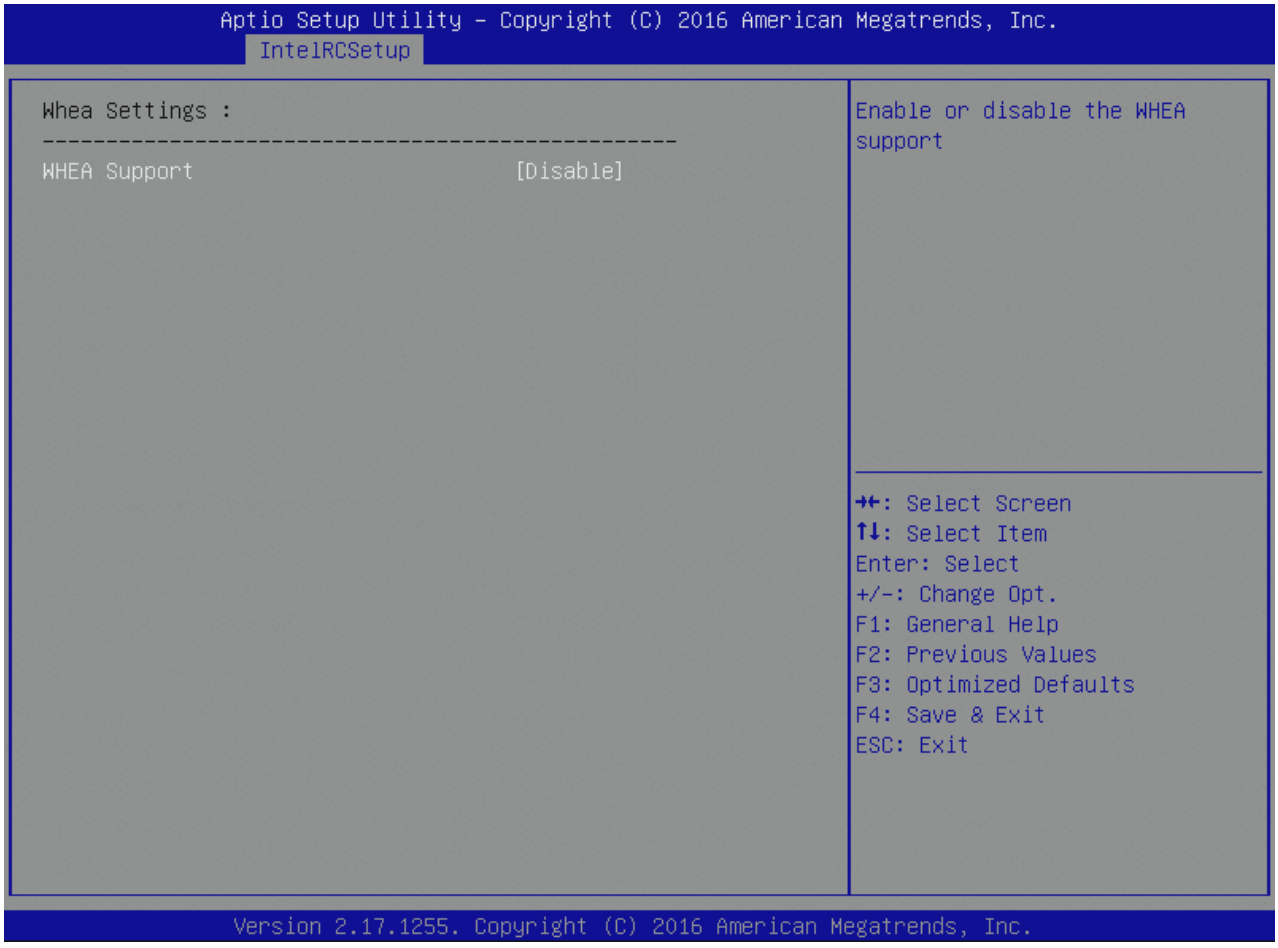


Table 121: Whea Settings Features List

Feature	Options	Description
Whea Support	**Disable** Enable	Enable or disable the WHEA support

6.5.3.63 Memory Error Enabling

Figure 105: Memory Error Enabling Menu Screen

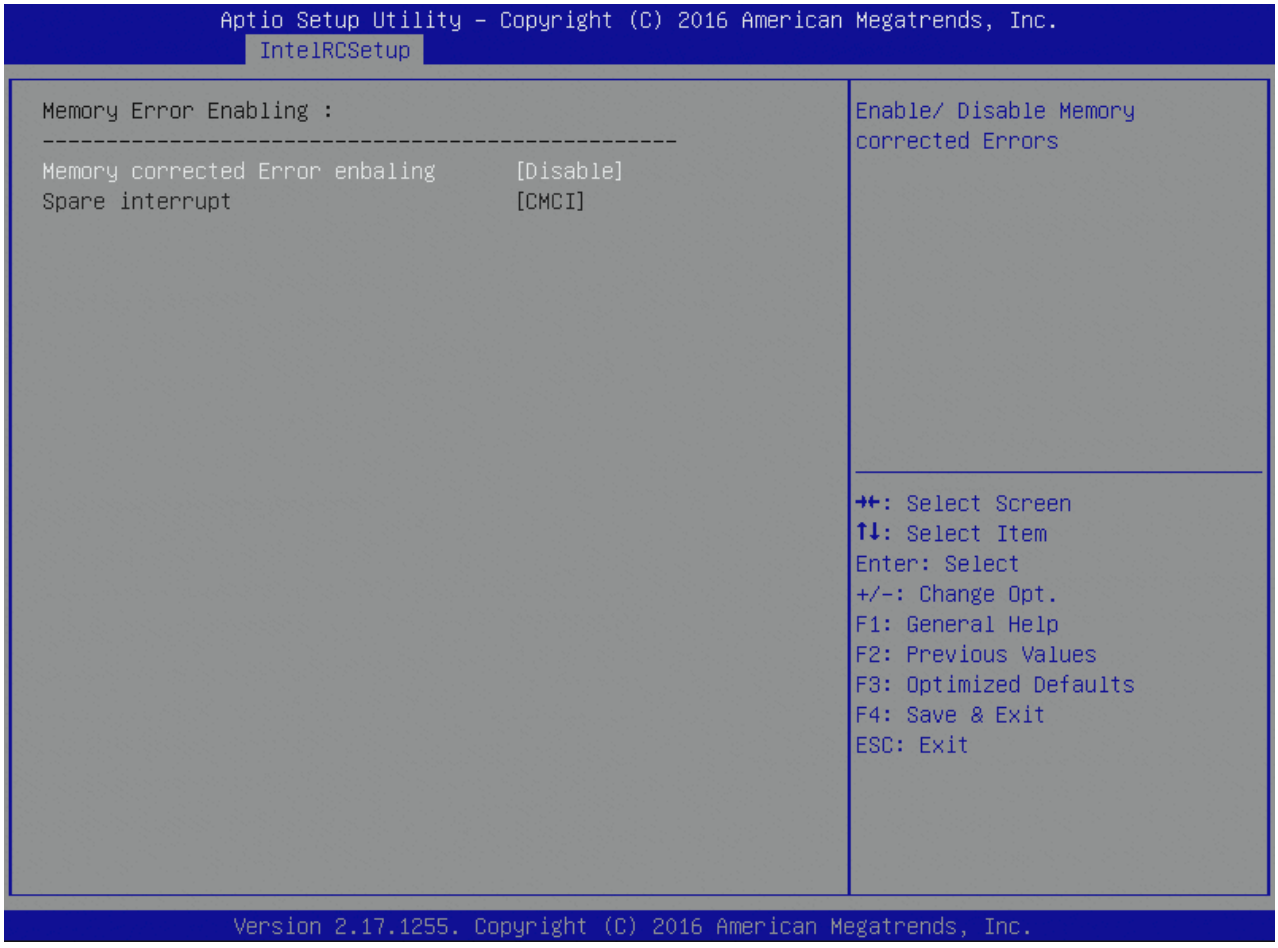


Table 122: Memory Error Enabling Features List

Feature	Options	Description
Memory corrected Error enbaling	**Disable** Enable	Enable/ Disable Memory corrected Errors
Spare interrupt	SMI **CMCI** Error Pin	Select SMI/CMCI/ErrPin for spare interrupt

6.5.3.64 IIO Error Enable

Figure 106: IIO Error Enable Menu Screen

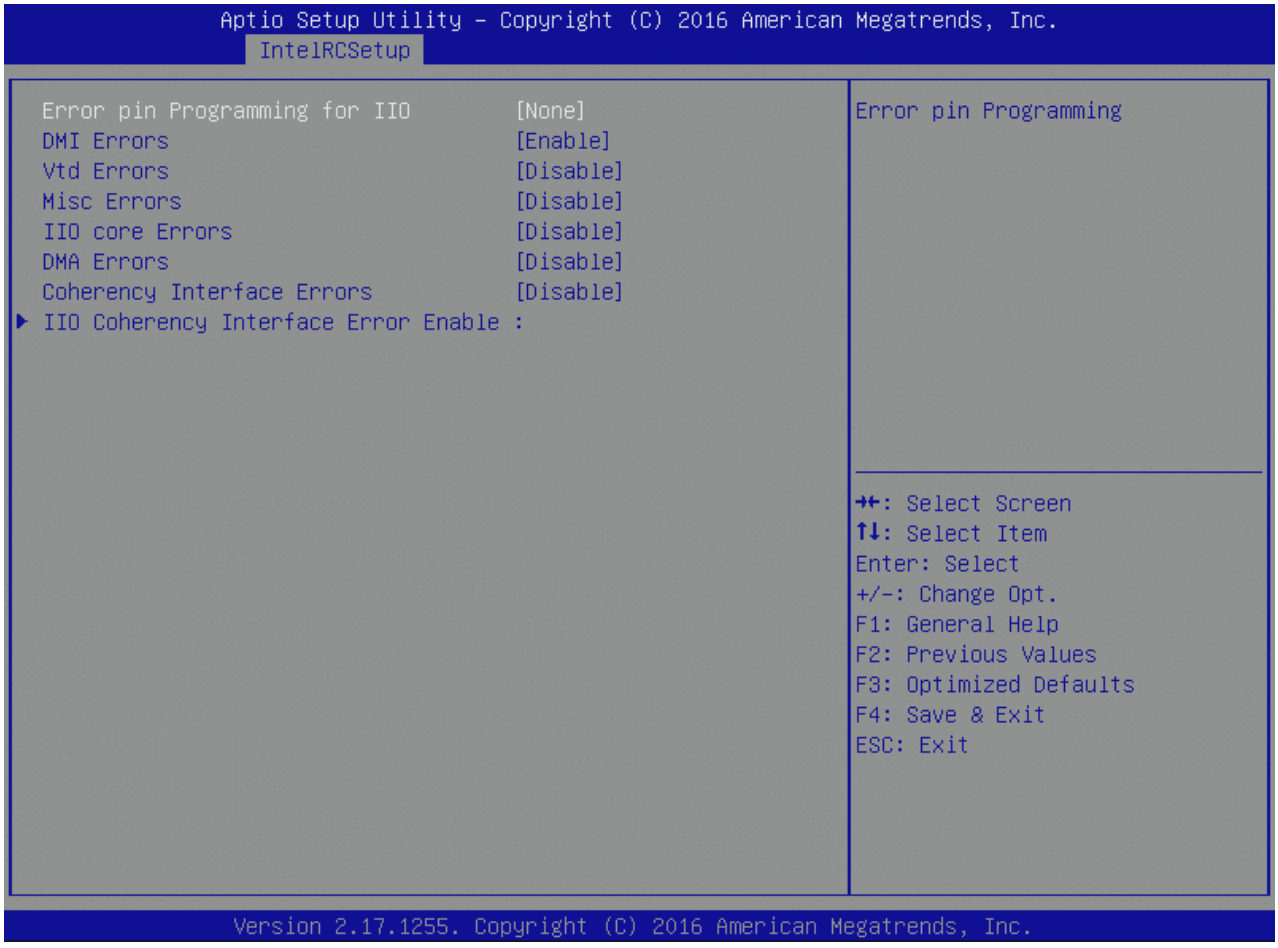


Table 123: IIO Error Enable Features List

Feature	Options	Description
Error pin Programming for IIO	**None** SMI	Error pin Programming
DMI Errors	Disable Enable	Enable/Disable DMI errors
Vtd Errors	Disable Enable	Enable/Disable Vtd errors
Misc Errors	Disable Enable	Enable/Disable Miscellaneous errors
IIO core Errors	Disable Enable	Enable/Disable IIO core errors
DMA Errors	Disable Enable	Enable/Disable DMA errors
Coherency Interface Errors	Disable Enable	Enable/Disable Coherency Interface errors

6.5.3.65 IIO Coherency Interface Error Enable

Figure 107: IIO Coherency Interface Error Enable Menu Screen

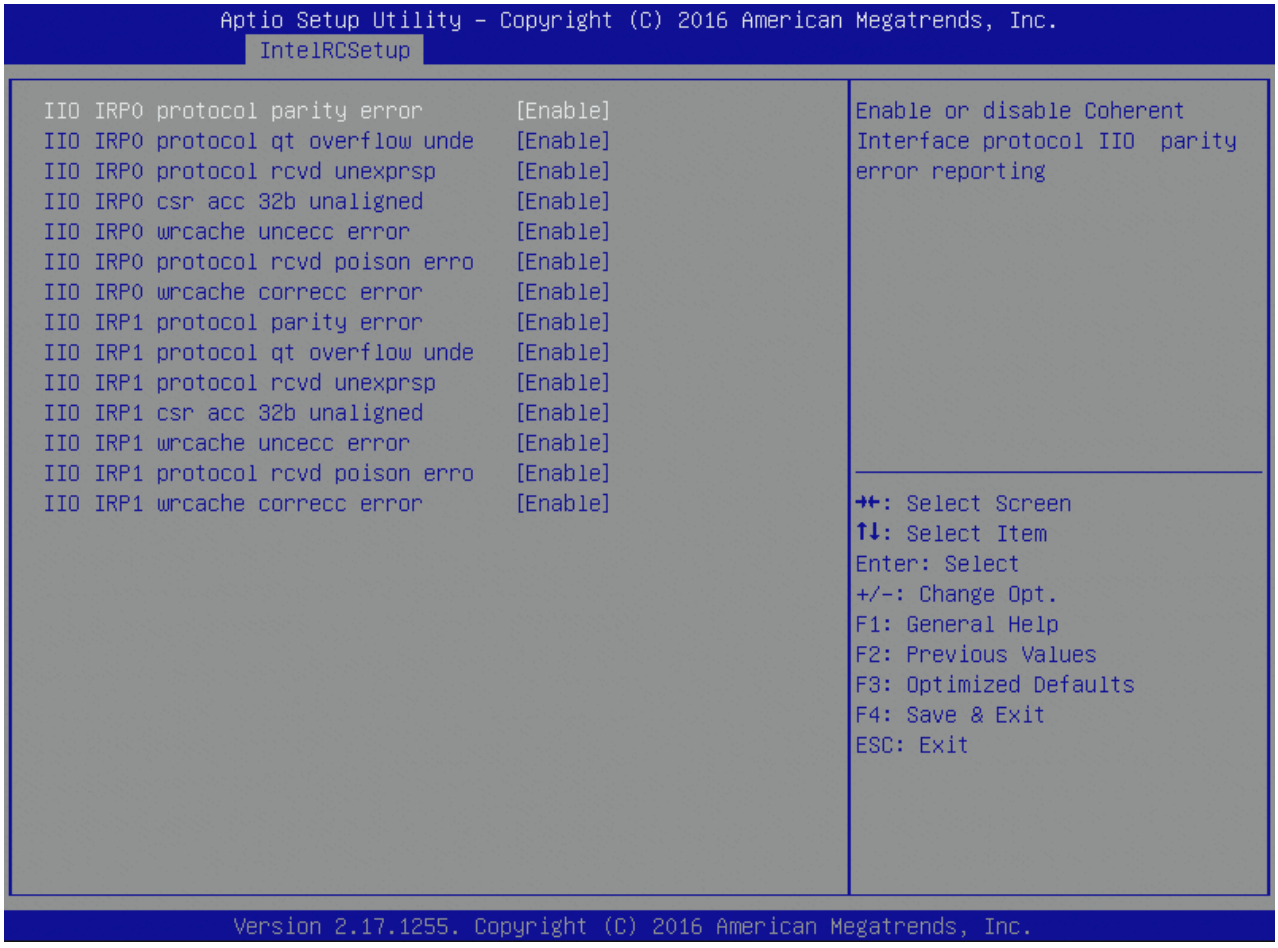


Table 124: IIO Coherency Interface Error Enable Features List

Feature	Options	Description
IIO IRP0 protocol parity error	Disable Enable	Enable or disable Coherent Interface protocol IIO parity error reporting
IIO IRP0 protocol qt overflow unde	Disable **Enable**	Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting
IIO IRP0 protocol rcvd unexprsp	Disable Enable	Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting
IIO IRP0 csr acc 32b unaligned	Disable Enable	Enable or disable IIO Coherent Interface CSR access Crossing 32-bit Boundary error reporting
IIO IRP0 wrcache uncecc error	Disable Enable	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting
IIO IRP0 protocol rcvd poison erro	Disable Enable	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting
IO IRP0 wrcache correcc error	Disable **Enable**	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting

6.5.3.66 PCI/PCI Error Enabling

Figure 108: PCI/PCI Error Enabling Menu Screen

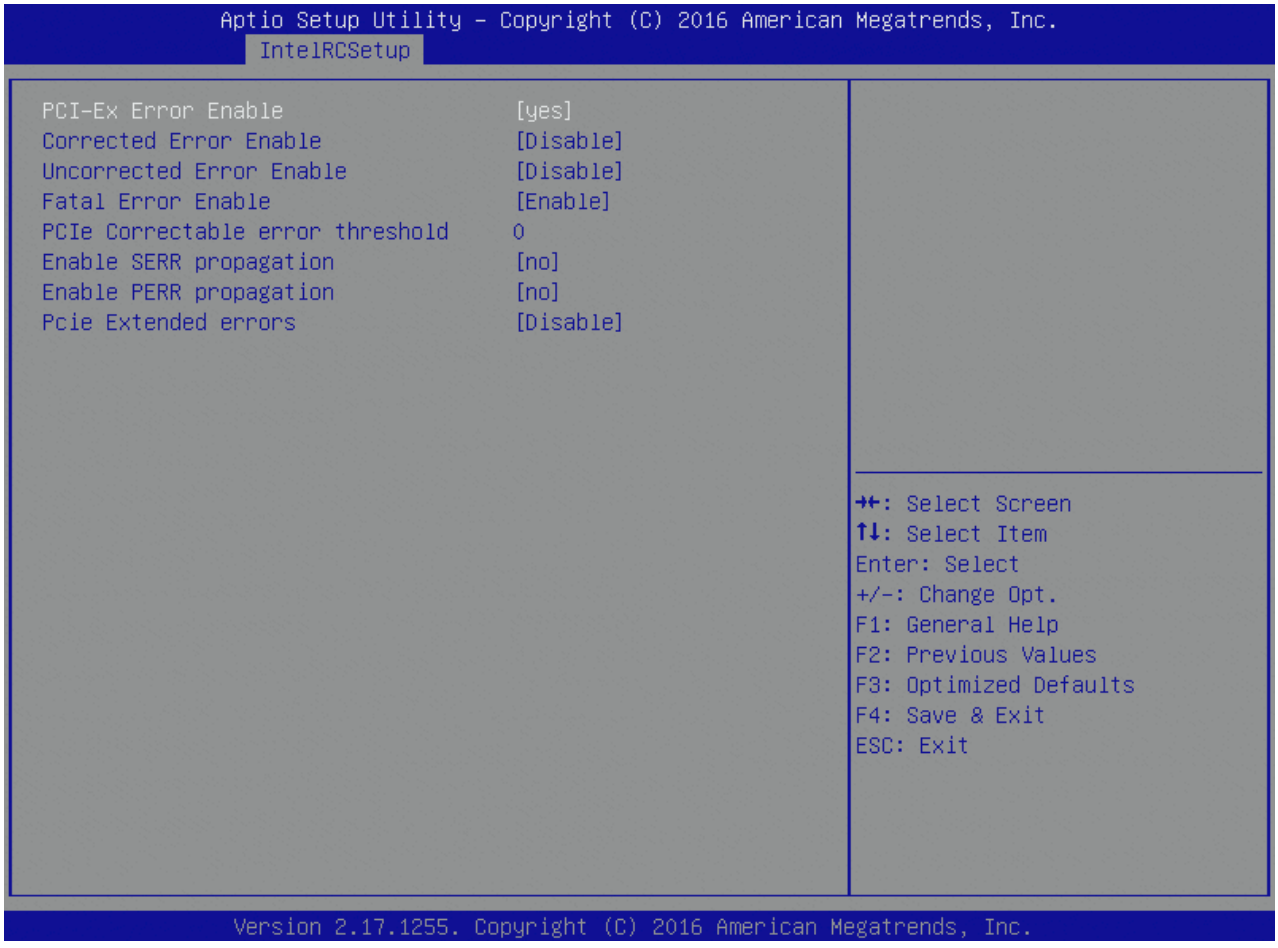


Table 125: PCI/PCI Error Enabling Features List

Feature	Options	Description
PCI-Ex Error Enable	no **yes**	
Corrected Error Enable	Disabled Enabled	Enable/Disable PCIe Correctable errors.
Uncorrected Error Enable	Disabled **Enabled**	Enable/Disable PCIe Uncorrectable errors.
Fatal Error Enable	Disabled **Enabled**	Enable/Disable PCIe Fatal errors.
PCIe Correctable error threshold	0	PCIe CE threshold(1-255), 0-No threshold.
Enable SERR propagation	**no** yes	
Enable PERR propagation	**no** yes	
Pcie Extended errors	Disabled Enabled	Enable/Disable –IIO Pcie Rootport errors

6.5.3.67 Reserved Memory

Figure 109: Reserved Memory Menu Screen

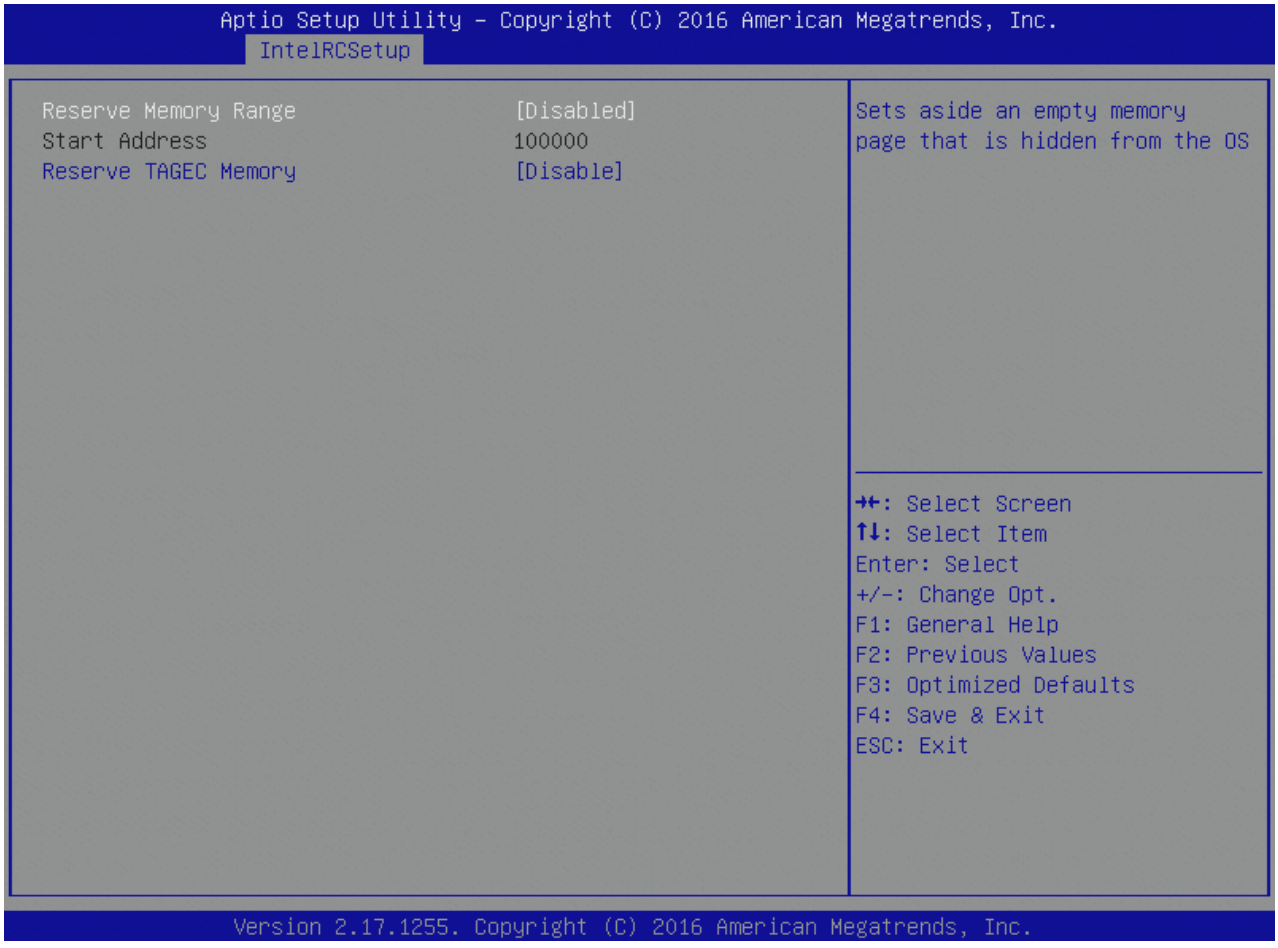


Table 126: Reserved Memory Features List

Feature	Options	Description
Reserve Memory Range	**Disabled** Enabled	Sets aside an empty memory page that is hidden from the OS
Start Address	100000	Address that reserved memory page starts at
Reserve TAGEC Memory	**Disable** Enable	Reserve 16M for TAGEC

6.5.4 Security

Figure 110: Security Menu Screen

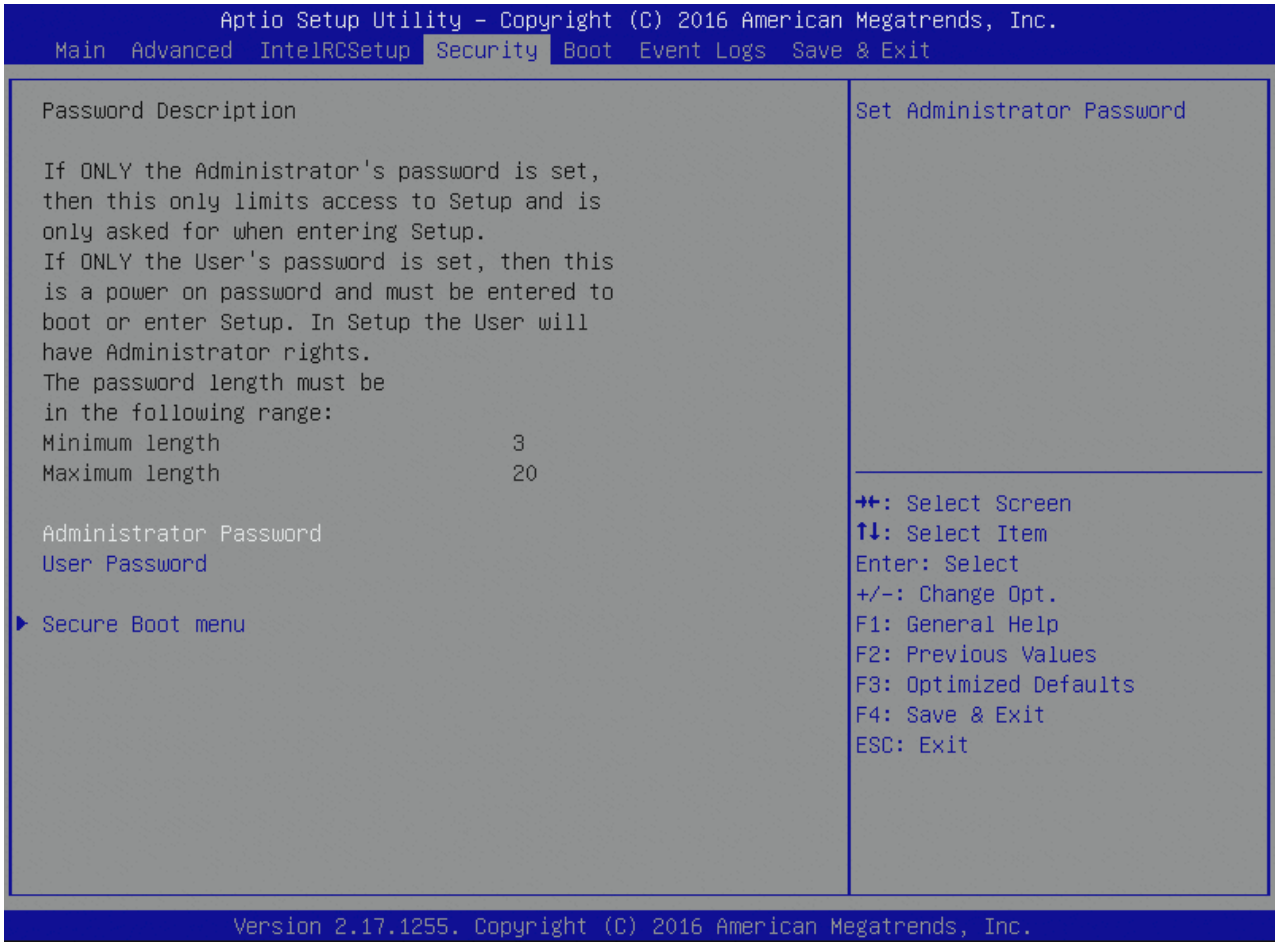


Table 127: Security Features List

Feature	Options	Description
Administrator Password		Set administrator Password
User Password		Set user Password

6.5.4.1 Secure Boot menu

Figure 111: Secure Boot menu Menu Screen

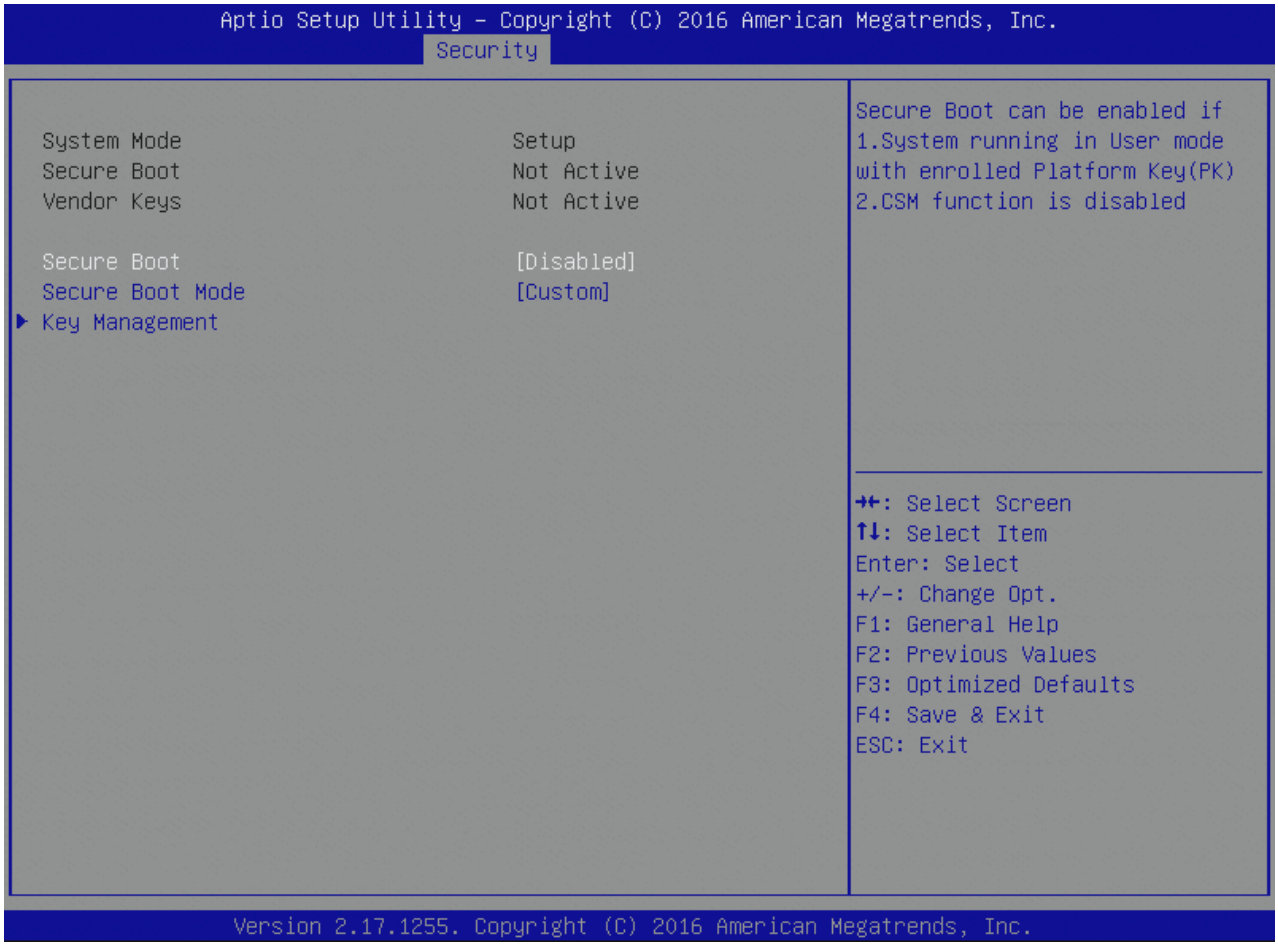


Table 128: Secure Boot menu Features List

Feature	Options	Description
Secure Boot	Disabled Enabled	Secure Boot can be enabled if 1.System running in User mode with enrolled Platform Key(PK) 2.CSM function is disabled
Secure Boot Mode	Standard **Custom**	Secure Boot mode selector. 'Custom' Mode enables users to change Image Execution policy and manage Secure Boot Keys

6.5.4.2 Key Management

Figure 112: Key Management Menu Screen

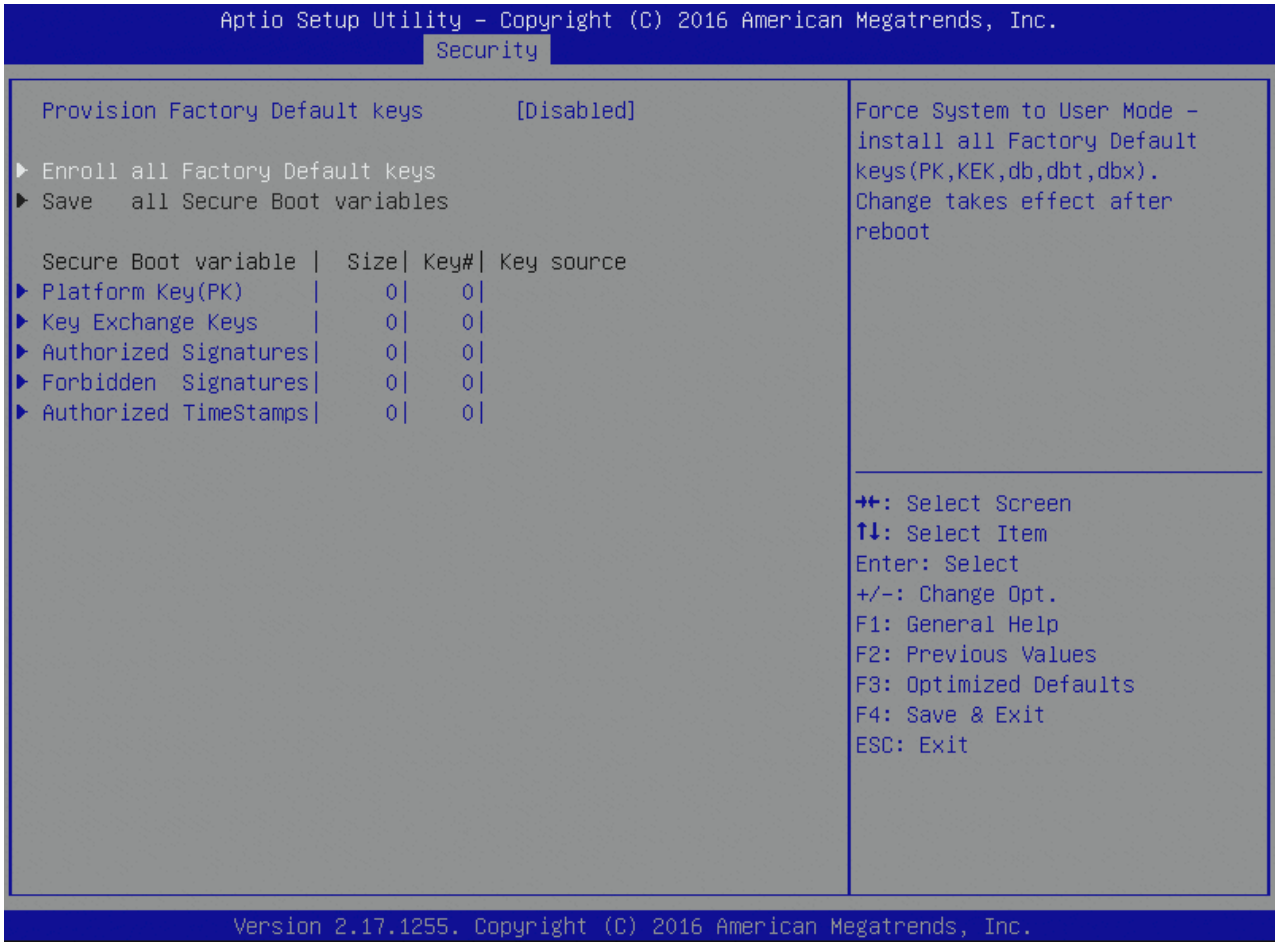


Table 129: Key Management Features List

Feature	Options	Description
Provision Factory Default keys	**Disable** Enable	Install factory default Secure Boot keys when System is in Setup Mode
Enroll all Factory Default Keys		Force System to User Mode – install all Factory Default keys(PK,KEK,db,dbt,dbx). Change takes effect after reboot
Platform Key(PK)		Enroll Factory Defaults or load the keys from a file with: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key source:Default,Custom,Mixed (*) modified from Setup menu
Key Exchange keys		
Authorized Signatures		
Forbidden Signatures		
Authorized TimeStamps		

6.5.5 Boot

Figure 113: Boot Menu Screen



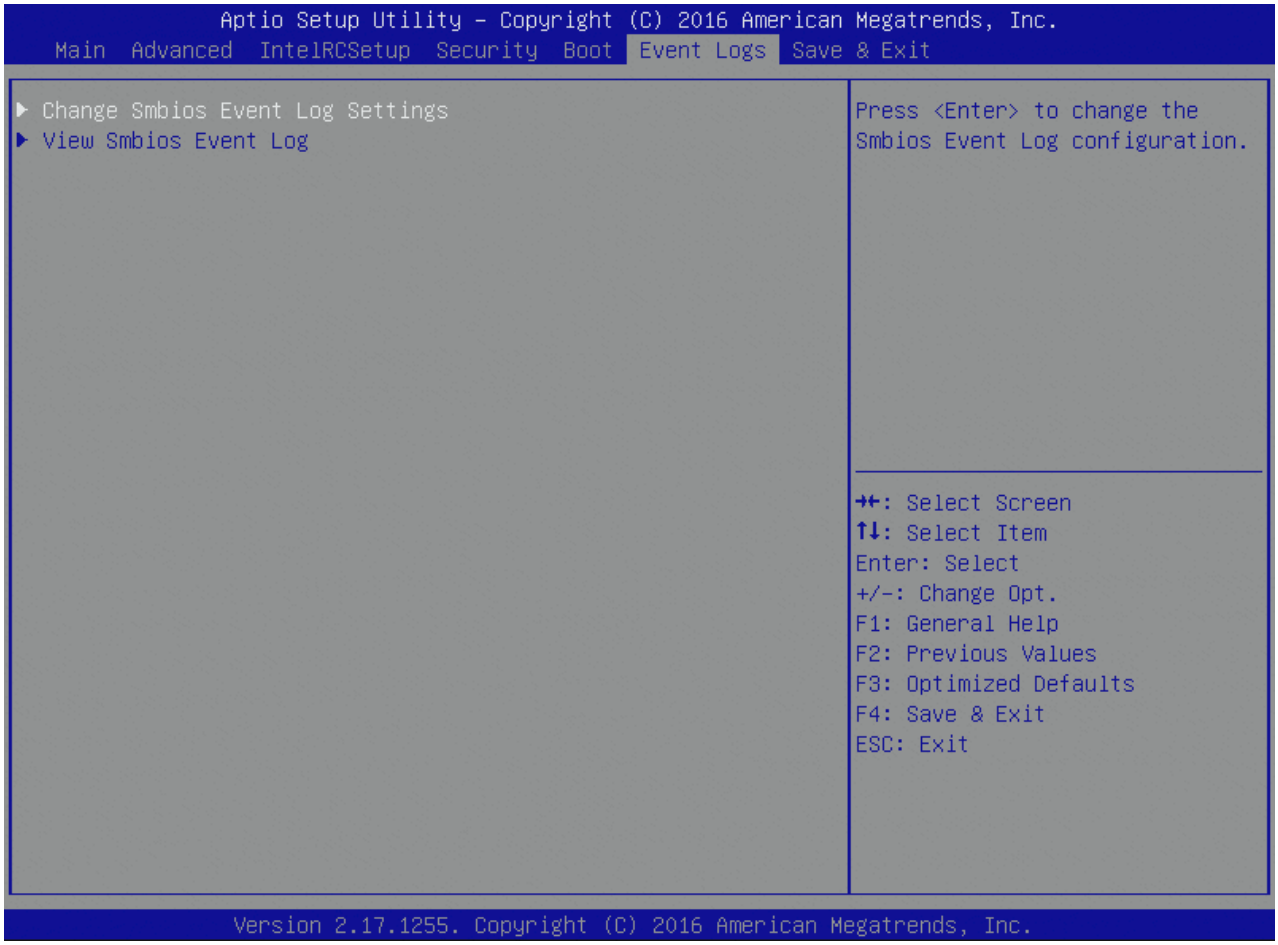
Table 130: Boot Features List

Feature	Options	Description
Setup Prompt Timeout	1	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard NumLock state
Quiet Boot	Disabled Enabled	Enables or disables Quiet Boot option
Boot Option #1	IBA GE Slot 0200 v1570 IBA XE Slot 0400 v2353 IBA XE Slot 0401 v2353 **UEFI: Built-in EFI Shell** Disabled	Sets the system boot order
Boot Option #2	**IBA GE Slot 0200 v1570** IBA XE Slot 0400 v2353 IBA XE Slot 0401 v2353 UEFI: Built-in EFI Shell Disabled	Sets the system boot order

Feature	Options	Description
Boot Option #3	IBA GE Slot 0200 v1570 IBA XE Slot 0400 v2353 IBA XE Slot 0401 v2353 UEFI: Built-in EFI Shell **Disabled**	Sets the system boot order
Boot Option #4	IBA GE Slot 0200 v1570 IBA XE Slot 0400 v2353 IBA XE Slot 0401 v2353 UEFI: Built-in EFI Shell **Disabled**	Sets the system boot order

6.5.6 Event Logs

Figure 114: Event Logs Menu Screen



6.5.6.1 Change Smbios Event Log Settings

Figure 115: Change Smbios Event Log Settings Menu Screen

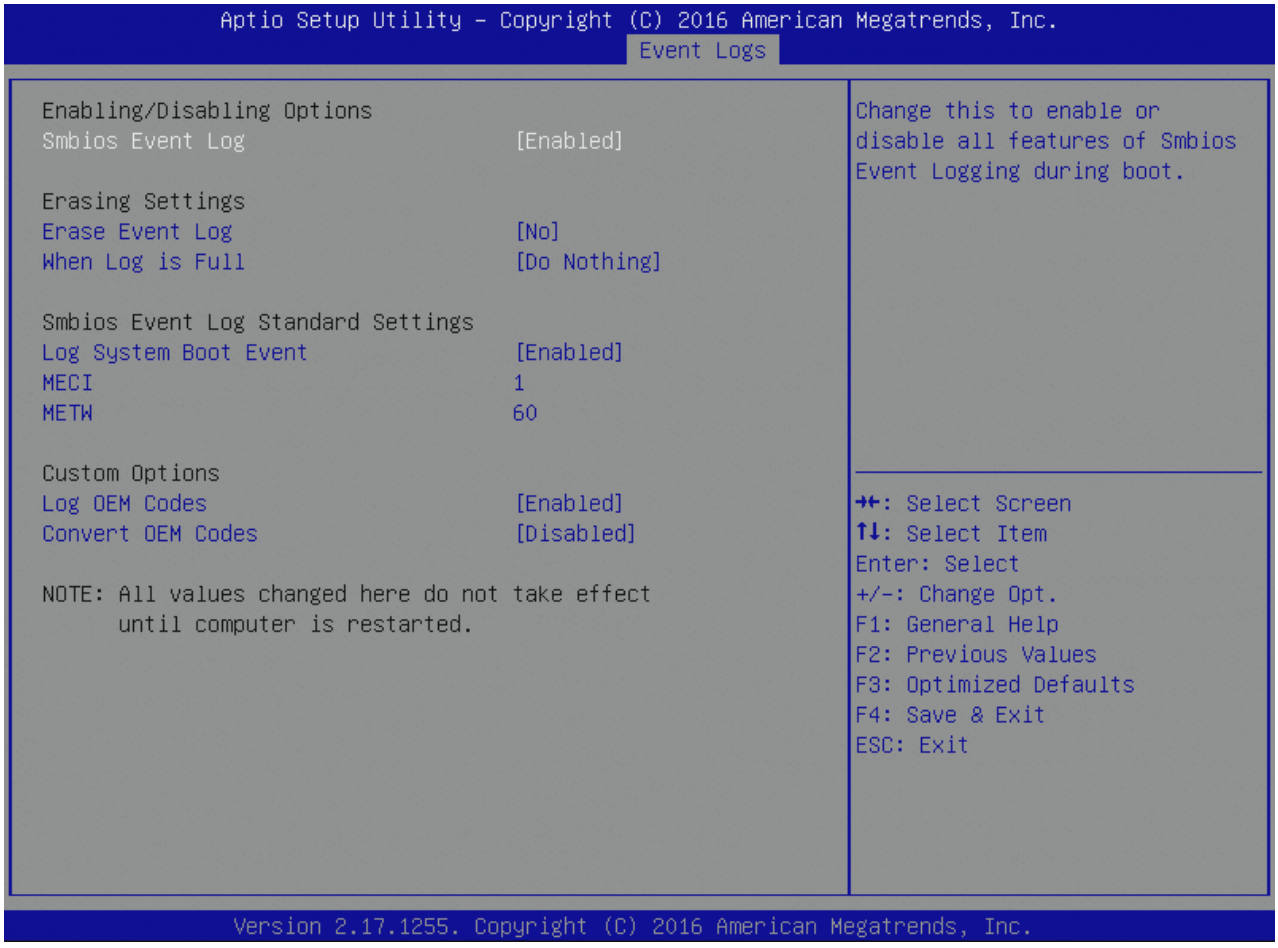


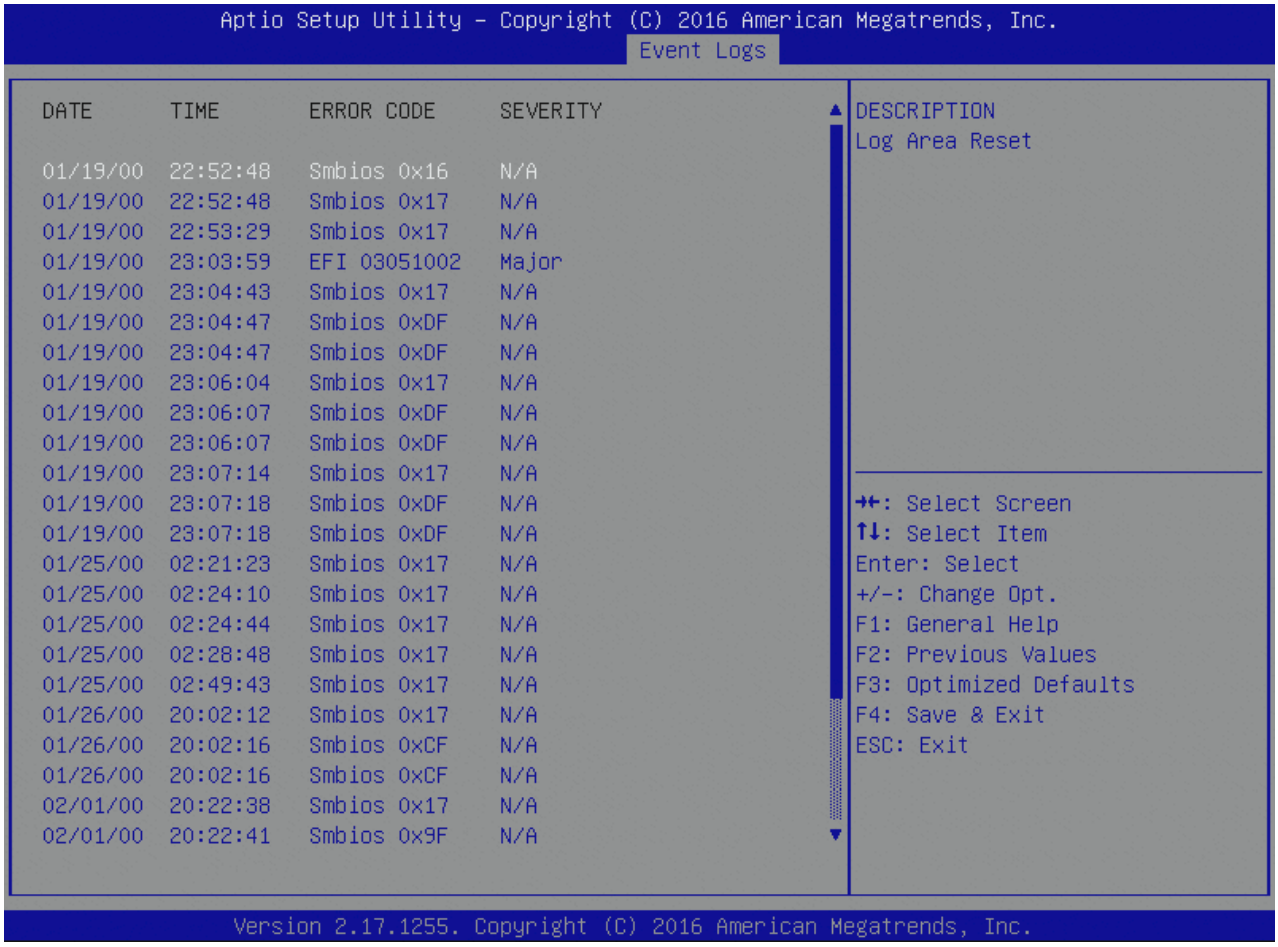
Table 131: Change Smbios Event Log Settings Features List

Feature	Options	Description
Smbios Event Log	Enabled	Change this to enable or disable all features of Smbios Event Logging during boot.
Erase Event Log	**No** Yes, Next reset Yes, Every reset	Choose options for erasing Smbios Event Log. Erasing is done prior to any logging activation during reset.
When Log is Full	**Do Nothing** Erase Immediately	Choose options for reactions to a full Smbios Event Log.
Log System Boot Event	**Enable** Disable	Choose option to enable/disable logging of System boot event
MECI	1	Multiple Event Count Increment: The number of occurrences of a duplicate event that must pass before the multiple-event counter of log entry is updated. The value ranges from 1 to 255.
METW	60	Multiple Event Time Window: The number of minutes which must pass between duplicate log entries which utilize a multiple-event counter. The value ranges from 0 to 99 minutes.
Log OEM Codes	**Enable** Disable	Enable or disable the logging of EFI Status Codes as OEM Codes (if not already converted to legacy).

Convert OEM Codes	**Enable** Disable	Enable or disable the converting of EFI Status Codes to Standard Smbios Types (Not all may be translated).

6.5.6.2 View Smbios Event Log

Figure 116: View Smbios Event Log Menu Screen



6.5.7 Save & Exit

Figure 117: Save & Exit Menu Screen

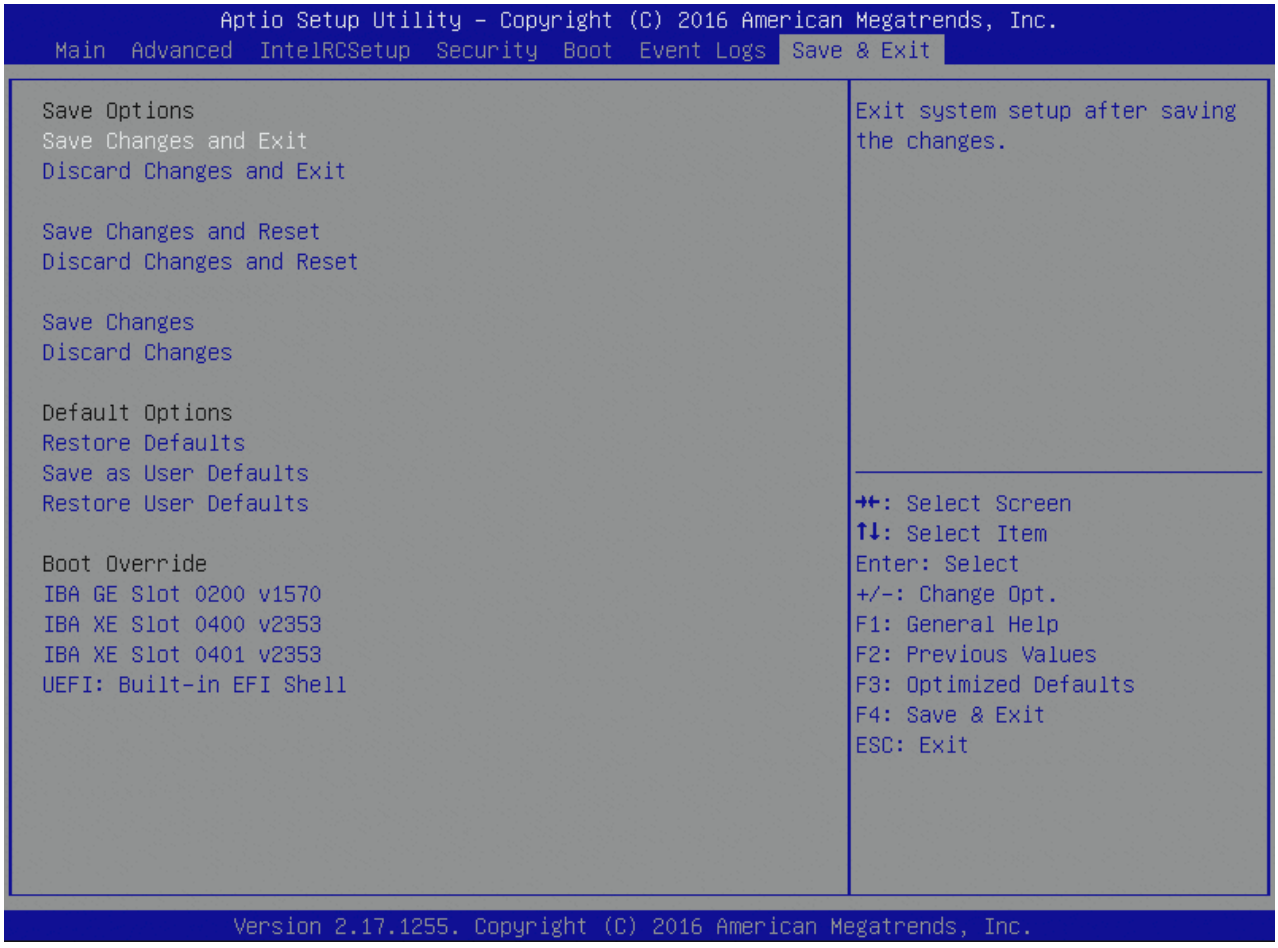


Table 132: Save & Exit Features List

Feature	Options	Description
Save Changes and Exit	-	Exit system setup after saving the changes.
Discard Changes and Exit	-	Exit system setup without saving any changes.
Save Changes and Reset	-	Reset system after saving the changes.
Discard Changes and Reset	-	Reset system without saving any changes.
Save Changes	-	Save Changes done so far to any of the setup options.
Discard Changes	-	Discard Changes done so far to any of the setup options.
Restore Defaults	-	Restore/Load Default values for all the setup options.
Save as User Defaults	-	Save the changes done so far as User Defaults.
Restore User Defaults	-	Restore the User Defaults to all the setup options.
Boot Override	List of all boot options	Boot directly from selected device

Appendix A: PICMG COME.0 Signal Terminology

Table 133: PICMG COME.0 Signal Terminology

Term	Definition
AC '97	Audio CODEC (Coder-Decoder)
ACPI	Advanced Configuration Power Interface – standard to implement power saving modes in PCAT systems
Basic Module	COM Express® 125mm x 95mm Module form factor.
BIOS	Basic Input Output System – firmware in PC-AT system that is used to initialize system components before handing control over to the operating system.
CAN	Controller-area network (CAN or CAN-bus) is a vehicle bus standard designed to allow microcontrollers to communicate with each other within a vehicle without a host computer.
Carrier Board	An application specific circuit board that accepts a COM Express® Module.
CCTV	Closed Circuit Television
CVBS	Composite Video Baseband Signal
Compact Module	COM Express® 95x95 Module form factor
DDC	Display Data Control – VESA (Video Electronics Standards Association) standard to allow identification of the capabilities of a VGA monitor
DDI	Digital Display Interface – containing DisplayPort, HDMI/DVI and SDVO
DIMM	Dual In-line Memory Module
DisplayPort	DisplayPort is a digital display interface standard put forth by the Video Electronics Standards Association (VESA). It defines a new license free, royalty free, digital audio/video interconnect, intended to be used primarily between a computer and its display monitor.
DRAM	Dynamic Random Access Memory
DVI	Digital Visual Interface - a Digital Display Working Group (DDWG) standard that defines a standard video interface supporting both digital and analog video signals. The digital signals use TMDS.
EAPI	Embedded Application Programming Interface Software interface for COM Express® specific industrial functions ▶ System information ▶ Watchdog timer ▶ I2C Bus ▶ Flat Panel brightness control ▶ User storage area ▶ GPIO
EEPROM	Electrically Erasable Programmable Read-Only Memory
Embedded DisplayPort	Embedded Display Port (eDP) is a digital display interface standard produced by the Video Electronics Standards Association (VESA) for digital interconnect of Audio and Video.
Extended Module	COM Express® 155mm x 110mm Module form factor.

Term	Definition
FR4	A type of fiber-glass laminate commonly used for printed circuit boards.
Gb	Gigabit
GBE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
HDA	Intel High Definition Audio (HD Audio) refers to the specification released by Intel in 2004 for delivering high definition audio that is capable of playing back more channels at higher quality than AC97.
HDMI	High Definition Multimedia Interface
I2C	Inter Integrated Circuit – 2 wire (clock and data) signaling scheme allowing communication between integrated circuits, primarily used to read and load register values.
IDE	Integrated Device Electronics – parallel interface for hard disk drives – also known as PATA
Legacy Device	Relics from the PC-AT computer that are not in use in contemporary PC systems: primarily the ISA bus, UART-based serial ports, parallel printer ports, PS-2 keyboards, and mice. Definitions vary as to what constitutes a legacy device. Some definitions include IDE as a legacy device.
LAN	Local Area Network
LPC	Low Pin-Count Interface: a low speed interface used for peripheral circuits such as Super I/O controllers, which typically combine legacy-device support into a single IC.
LS	Least Significant
LVDS	Low Voltage Differential Signaling – widely used as a physical interface for TFT flat panels. LVDS can be used for many high-speed signaling applications. In this document, it refers only to TFT flat-panel applications.
ME	Management Engine
Mini Module	COM Express® 84x55mm Module form factor
MS	Most Significant
NA	Not Available
NC	No Connect
NTSC	National Television Standards Committee – video broadcast standard used in North America
OEM	Original Equipment Manufacturer
PAL	Phase Alternating Line – video broadcast standard used in many European countries.
PATA	Parallel AT Attachment – parallel interface standard for hard-disk drives – also known as IDE, AT Attachment, and as ATA
PC-AT	"Personal Computer – Advanced Technology" – an IBM trademark term used to refer to Intel x86 based personal computers in the 1990s
PCB	Printed Circuit Board
PCI	Peripheral Component Interface
PCI Express PCIE	Peripheral Component Interface Express – next-generation high speed Serialized I/O bus
PEG	PCI Express Graphics

Term	Definition
PHY	Ethernet controller physical layer device
Pin-out Type	A reference to one of seven COM Express® definitions for the signals that appear on the COM Express® Module connector pins.
PS2 PS2 Keyboard PS2 Mouse	"Personal System 2" - an IBM trademark term used to refer to Intel x86 based personal computers in the 1990s. The term survives as a reference to the style of mouse and keyboard interface that were introduced with the PS2 system.
Ra	Roughness Average – a measure of surface roughness, expressed in units of length.
ROM	Read Only Memory – a legacy term – often the device referred to as a ROM can actually be written to, in a special mode. Such writable ROMs are sometimes called Flash ROMs. BIOS is stored in ROM or Flash ROM.
RTC	Real Time Clock – battery backed circuit in PC-AT systems that keeps system time and date as well as certain system setup parameters
SAS	Serial Attached SCSI – high speed serial version of SCSI
SCSI	Small Computer System Interface – an interface standard for high end disk drives and other computer peripherals
SPD	Serial Presence Detect – refers to serial EEPROM on DRAMs that has DRAM Module configuration information
SPI	Serial Peripheral Interface
SO-DIMM	Small Outline Dual In-line Memory Module
S0, S1, S2, S3, S4, S5	System states describing the power and activity level S0 Full power, all devices powered S1 S2 S3 Suspend to RAM System context stored in RAM; RAM is in standby S4 Suspend to Disk System context stored on disk S5 Soft Off Main power rail off, only standby power rail present
SATA	Serial AT Attachment: serial-interface standard for hard disks
SDVO	Serialized Digital Video Output – Intel defined format for digital video output that can be used with Carrier Board conversion ICs to create parallel, TMDS, and LVDS flat-panel formats as well as NTSC and PAL TV outputs
SM Bus	System Management Bus
Super I/O	An integrated circuit, typically interfaced via the LPC bus that provides legacy PC I/O functions including PS2 keyboard and mouse ports, serial and parallel port(s) and a floppy interface.
TFT	Thin Film Transistor – refers to technology used in active matrix flat-panel displays, in which there is one thin film transistor per display pixel.
TMDS	Transition Minimized Differential Signaling - a digital signaling protocol between the graphics subsystem and display. TMDS is used for the DVI digital signals.
TPM	Trusted Platform Module, chip to enhance the security features of a computer system.
USB	Universal Serial Bus
VGA	Video Graphics Adapter – PC-AT graphics adapter standard defined by IBM.
WDT	Watch Dog Timer.
XAUI	10 Gigabit / sec Attachment Unit Interface.

7 / Technical Support

For technical support contact our Support department:

E-mail: support@kontron.com
Phone: +49-821-4086-888

Make sure you have the following information available when you call:

Product ID Number (PN),
Serial Number (SN)
Module's revision
Operating System and Kernel/Build version
Software modifications
Addition connected hardware/full description of hardware set up
Be ready to explain the nature of your problem to the service technician.



The serial number can be found on the Type Label, located on the product's rear side.

7.1 Warranty

Due to their limited service life, parts that by their nature are subject to a particularly high degree of wear (wearing parts) are excluded from the warranty beyond that provided by law. This applies to the CMOS battery, for example.



If there is a protection label on your product, then the warranty is lost if the product is opened.

7.2 Returning Defective Merchandise

All equipment returned to Kontron must have a Return of Material Authorization (RMA) number assigned exclusively by Kontron. Kontron cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The buyer accepts responsibility for all freight charges for the return of goods to Kontron's designated facility. Kontron will pay the return freight charges back to the buyer's location in the event that the equipment is repaired or replaced within the stipulated warranty period. Follow these steps before returning any product to Kontron.

1. Visit the RMA Information website:
http://www.kontron.com/support-and-services/support/rma-information

   Download the RMA Request sheet for Kontron Europe GmbH and fill out the form. Take care to include a short detailed description of the observed problem or failure and to include the product identification Information (Name of product, Product number and Serial number). If a delivery includes more than one product, fill out the above information in the RMA Request form for each product.

2. Send the completed RMA-Request form to the fax or email address given below at Kontron Europe GmbH. Kontron will provide an RMA-Number.

   Kontron Europe GmbH
   RMA Support
   Phone: +49 (0) 821 4086-0
   Fax: +49 (0) 821 4086 111
   Email: service@kontron.com

3. The goods for repair must be packed properly for shipping, considering shock and ESD protection.



Goods returned to Kontron Europe GmbH in non-proper packaging will be considered as customer caused faults and cannot be accepted as warranty repairs.

4. Include the RMA-Number with the shipping paperwork and send the product to the delivery address provided in the RMA form or received from Kontron RMA Support.

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). Kontron offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

For more information, please visit: www.kontron.com



GLOBAL HEADQUARTERS

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP