USER GUIDE

COMe-bBD7 Module

User Guide Rev. 1.11

kontron

This page has been intentionally left blank

COME-BBD7 MODULE - USER GUIDE

Disclaimer

Kontron would like to point out that the information contained in this user guide 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 user guide or any product characteristics set out in the user guide. 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 user guide 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 user guide 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 user guide 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 user guide is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this user guide 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.

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	2018-March-28	hjs
1.1	BIOS design issues, block diagram changed, new layout,	2019-April-21	hjs
1.2	Table 30: I2C Bus Port Addresses modified	2019-September-24	hjs
1.3	modified SPI flash in Table 22: Supported SPI boot flash types for 8-SOIC package	2020-May-26	hjs
1.4	Word2016 issues, new PNs for HSP in Table 14, new memory in Table 15	2021-March-29	hjs
1.5	Port x8 in chapter 3.6.3 deleted, block diagram updated	2021-May-06	hjs
1.6	Wrong memory table in chapter 4/Accessories deleted	2021-November-04	hjs
1.7	Table 9: PCIe Gen 2 Ports updated	2022-May-24	hjs
1.8	Removed onboard SATA-option Removed WIBU-option Updated block diagram	2022-July-20	ih
1.9	New Kontron logo Added RTC description	2023-April-06	ih
1.10	Corrected wrong headlines for SODIMMs	2023-July-14	ih
1.11	Removed rapid shutdown function	2025-December 10	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.de/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.

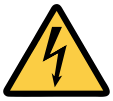
For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit https://www.kontron.de/support-and-services.

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

List of Tables

List of Figures

1/ Introduction

1.1. Product Description

Kontron's Computer-on-Module COMe-bBD7 is a COM Express® BASIC TYPE 7 with Intel® Xeon® PROCESSOR D-15xx family with support for Pin-out Type 7, 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 14 nm 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-bBD7 is also designed for industrial temperature environment.

- Intel® Xeon® Processor D-1500 System on Chip (SoC), member of the Intel® Xeon® Processor family
- DDR4 memory technology up to 32 GByte ECC, 2x SODIMMs
- high-speed connectivity 24x PCIE 3.0 + 8x PCIE2.0
- Dual 10 GbE interfaces (option)

1.2. Product Naming Clarification

COM Express® defines a Computer-on-Module, or COM, with all the components necessary for a bootable host computer, packaged as a super component. The product name for Kontron COM Express® Computer-On-Modules consists of:

Industry standard short form

- COMe-

Module form factor

- b=basic (125mm x 95mm)
- c=compact (95mm x 95mm)
- m=mini (84mm x 55mm)

Intel's processor code name

- BD = Broadwell

Pinout type

- Type 7

Available temperature variants

- Commercial
- Industrial (E2)

Processor Identifier

- Chipset identifier (if chipset assembled)

Memory size

- Memory module (#G) / eMMC SLC memory (#S)

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 of Type 7 and COMe-bBD7

Feature	Type 7 Standard	COMe-bBD7 Pinout
Gbit Ethernet	1x	1x
10GBaseKR Ethernet	4x	2x
NC-SI	1x	1x
PCI Express	32x	7x or 8x PCIe Gen2 24x PCIe Gen3
Serial ATA	2x	2x
USB	4x USB 3.0 4x USB 2.0	4x USB 3.0 4x USB 2.0
Serial Ports	2x	2x
LPC	1x	1x
External SPI	1x	1x
External SMB	1x	1x
External I2C	1x	1x
GPIO	8x	8x

NOTICE

Customized article with 8 PCIe Gen2 lanes can be defined on request. Please contact your local sales or support for further details.

1.4. COM Express® Documentation

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

1.5. COM Express® Benefits

COM Express® defines a Computer-On-Module, or COM, with all the components necessary for a bootable host computer, packaged as a highly integrated computer. All Kontron COM Express® modules are very compact and feature a standardized form factor and a standardized connector layout that 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 optimally designed to fit a system's packaging.

A single baseboard design can use a range of COM Express® modules with different sizes and pinouts. This flexibility differentiates products at various price and performance points and provides a built-in upgrade path when designing future-proof systems. 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-bBD7 (bBD7) follows pin-out Type 7 and is compatible to PICMG specification COM.0 Rev 3.0. The COMe-bBD7 is available in different variants to cover the different demands in performance, price and power.

2.2. 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	Description
68004-0000-08-2	COMe-bBD7 D-1508	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Pentium® Processor D1508, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-17-4	COMe-bBD7 D-1517	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Pentium® Processor D1517, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-27-4	COMe-bBD7 D-1527	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1527, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-28-6	COMe-bBD7 D-1528	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1528, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-37-8	COMe-bBD7 D-1537	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1537, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-48-8	COMe-bBD7 D-1548	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1548, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68004-0000-77-9	COMe-bBD7 D-1577	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1577, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM

2.3. Industrial Grade Modules

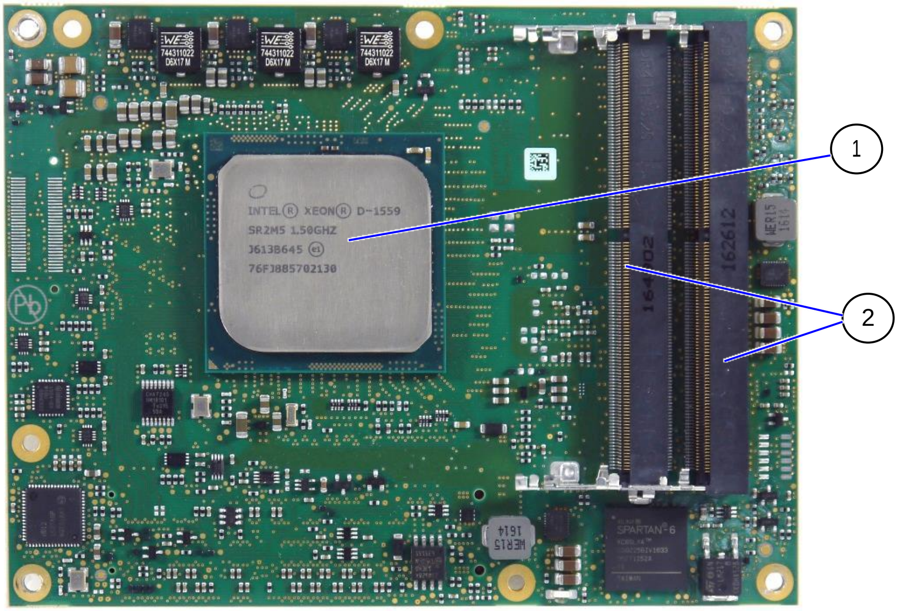
Industrial temperature grade modules are available based on their design. Please contact your local sales or support for further details.

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

Product Number	Product Name	Description
68005-0000-19-4	COMe-bBD7R E2 D-1519	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Pentium® Processor D1519, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68005-0000-39-8	COMe-bBD7R E2 D-1539	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1539, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM
68005-0000-59-9	COMe-bBD7R E2 D-1559	COM Express® basic pin-out type 7 Computer-on-Module with Intel® Xeon® Processor D-1559, dual 10GbE (KR), 1x GbE, 2x DDR4 non-ECC/ECC SO-DIMM

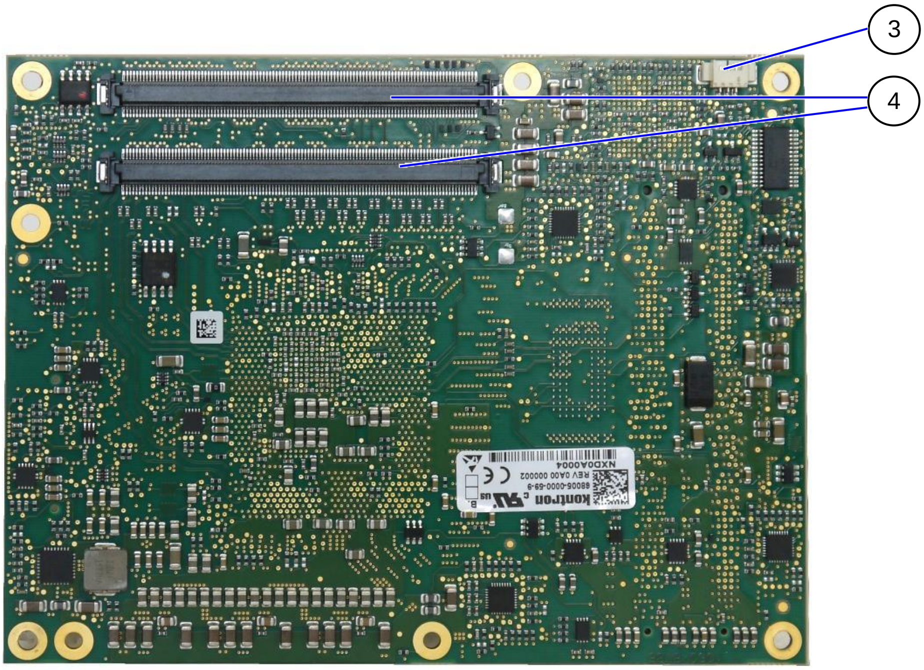
2.4. Product Views

Figure 1: Top View of COMe bBD7



1. Processor
2. 2x DDR4 memory

Figure 2: Bottom View of COMe bBD7



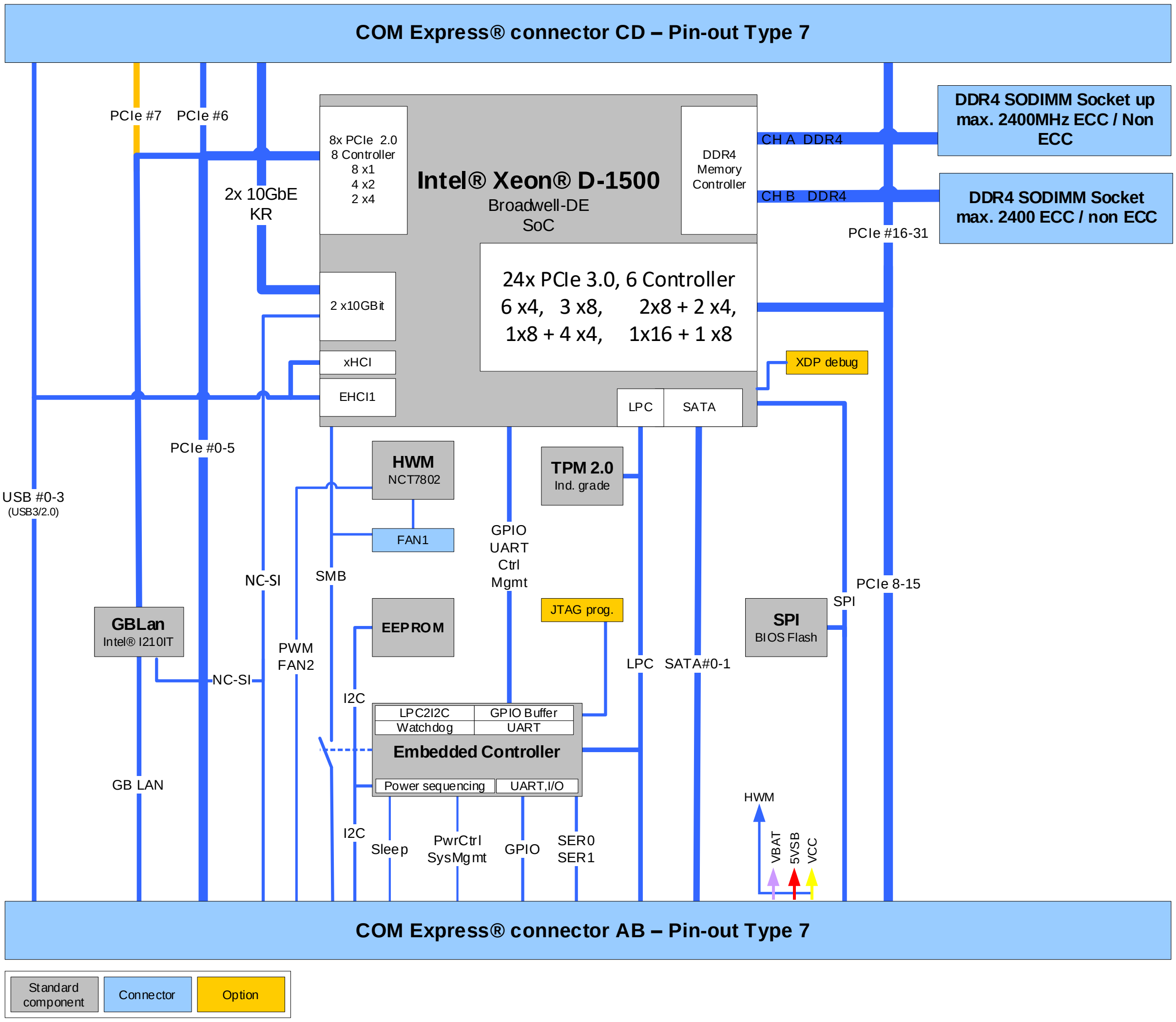
3. Fan Connector
4. 2x COMe interfaces

3/ Functional Specification

3.1. Block Diagram COMe-bBD7

Figure 3 displays the block diagram applicable to all COMe-bBD7 modules.

Figure 3: Block Diagram COMe-bBD7, basic pinout with Intel Xeon D-15XX Processor Family (Broadwell-DE SoC)



3.2. 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) (requires custom BIOS)
  - 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: Intel Xeon® Processor D-1500 Product Family Specifications

	Pentium			Xeon						
Intel Xeon® Processor	D1508	D1517	D1519	D1527	D1528	D1537	D1539	D1548	D1559	D1577
# of Cores	2	4	4	4	6	8	8	8	12	16
# of Threads	4	8	8	8	12	16	16	16	24	32
Base Freq.	2.2	2.2	1.5	2.2	1.9	1.7	1.6	2	1.5	1.3
Turbo Frequency (GHz)	2.6	2.6	2.1	2.7	2.4	2.3	2.2	2.6	2.1	2.1
Thermal Design Power (TDP) (W)	25	25	25	35	35	35	35	45	45	45
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 (MB)	3	6	6	6	9	12	12	12	18	24
Memory Type	DDR4-1866	DDR4-2133	DDR4-2133	DDR4-2133	DDR4-2133	DDR4-2133	DDR4-2133	DDR4-2400	DDR4-2133	DDR4-2133
Max Memory Size (GB) with SODIMM	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]	64 (4x 16)[1]
ECC Memory	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PCIe Express	32x	32x	32x	32x	32x	32x	32x	32x	32x	32x

[1] on the COMe-bBD7 two SODIMM sockets are supported for a max of 2x 32 GB memory

3.3. Memory

Table 5: Memory Features

Socket	2x DDR4 SO-DIMM
Memory Type	Dual Channel DDR4, up to 2400 MT/s, up to 32 GB per socket
Memory Module Size	4 GBytes, 8 GByte, 16 GByte and 32GByte

3.4. Platform Controller Hub (PCH)

The integrated Platform Controller Hub (PCH) supports:

Table 6: PCH Features

Feature	PCH
PCI Express	8x PCIe Gen 2 lanes,, Configurations x1, x4, x8
USB	3.0
VT-d	yes
Trusted Execution Technology (TXT)	yes (but not supported on COMe-bBD7)

3.5. USB

USB 3.0 ports are backwards compatible with the USB 2.0 specification. The COMe-bBD7 allows a maximum of four USB 3.0 (USB 2.0) ports.

Table 7: Supported USB Features

USB 3.0 Ports	4x USB 3.0
USB 2.0 Ports	4x USB 2.0
USB Over Current Signals	2x

3.6. 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.

3.6.1. Gen 3 PCI-Express x16 Port (COMe PCIE [16 to 31])

The Gen 3 PCI-Express x16 port is available on the COMe connector as COMe PCIE [16 to 31]. Four root ports are allowing the COMe-bBD7 to support the following port configurations:

- 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.

Table 8: 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				

3.6.2. Gen 3 PCI-Express x8 Port (COMe PCIE[8 to 15])

The Gen 3 PCI-Express x8 port is available on the COMe connector as COMe PCIE [8 to 15]. Two root ports are allowing the COMe-bBD7 to support the following port configurations:

- One port x8 (default)
- Two ports x4

3.6.3. Gen 2 PCI-Express x8 Port (COMe PCIE [0 to 7])

There are eight root ports which can be configured as an 8 x1 interface for connecting up to eight devices. By default 7 of the 8 lanes of this interface are available on the COMe connector COMe PCIe [0 to 6]. With default mounted I210 Ethernet controller PCIe Gen2 lane 7 is not available on the COMe connector. Customized articles with 8 PCIe Gen2 lanes can be defined on request. Please contact your local sales or support for further details. Following configurations are supported by different BIOS binary:

- One port x4 plus 4 ports x1 (default)
- Two ports x4
- Eight ports x1

Table 9: PCIe Gen 2 Ports

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

NOTICE

Configuration2 is by default. Configuration 3 does only work without Ethernet. All other configurations are provided in the BIOS download package available on EMD Customer Section.

3.7. SATA

The SATA high-speed storage interface supports two SATA Gen.3 ports with transfer rates of up to 6 Gb/s.

Table 10: COMe Connector Port and SoC Port Combinations for SATA

COMe Port	Comment
SATA_0	SATA Gen. 3, 6 Gb/s
SATA_1	SATA Gen. 3, 6 Gb/s

3.8. Ethernet

The COMe-bBD7 offers the following Ethernet Controllers:

- One Intel® Ethernet I210 Controller
- 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:

- 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

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.

NOTICE

Please download application note from EMD Customer Section.
Please contact your local sales or support for further details

3.9. COMe Features

The following table lists the supported COM Express® features.

Table 11: COMe Features

SPI	Boot from an external SPI
LPC	Supported
UART	2x UART (RX/TX)
Sleep Signals	Supported
SMBus	Speed configurable, default 100 k SMB

3.10. Kontron Features

The following table lists the supported Kontron specific product features.

Table 12: Kontron Features

External I2C Bus	Fast I2C, Multimaster capable
Embedded API	KeAPI 3.0 for all supported OS
Customer BIOS Settings / Flash Backup	Supported
Watchdog Support	Dual staged
External SIO	Supported on the base board
GPIO	Start-up level configurable, GPI interrupt capable

4/ Accessories

4.1. Product Specific Accessories

Table 13: Product Specific Accessories List

Product Number	Product	Description
68300-0000-00-0	COMe Eval Carrier T7	COM Express® Eval Carrier Type 7 with 4x 10G KR/DAC support
68301-0000-00-8	COMe Eval Carrier T7 G2-8	COM Express® Eval Carrier Type 7 Generation2 - COM.0 R3.0 - 8mm COMe connector
68301-0000-01-4	ADA-COMe-T7-G2 4x10G RJ45 - DEV-TOOL	Adaptercard for COMe Eval Carrier Gen2 4x RJ45: 10GBASE-KR-to-10GBASE-T via Intel PHY 2x X557-AT2
68301-0000-03-2	ADA-COMe-T7-G2 2x10G SFP+ - DEV-TOOL	Adaptercard for COMe Eval Carrier Gen2 2x SFP+: 10GBASE-KR-to-SFI via Inphi PHY CS4227
68301-0000-04-4	ADA-COMe-T7-G2 4X 10G DAC - DEV-TOOL	Adaptercard for COMe Eval Carrier Gen2 4x DAC: 10GBASE-KR signals directly routed from COMe connector to SFP+ cages
68004-0000-99-0	HSP COMe-bBD6/7 threaded mounting holes	Heatspreader for COMe-bBD6/bBD7, threaded mounting holes
68004-0000-99-1	HSP COMe-bBD6/7 through holes	Heatspreader for COMe-bBD6/bBD7, through holes
68002-0000-99-0C06	HSK COMe-bBD6 passive (w/o HSP)	Passive Cooler for COMe-bBD6/COMe-bBD7 to be mounted on HSP
68002-0000-99-0C05	HSK COMe-bBD6 active (w/o HSP)	Active Cooler for COMe-bBD6/bBD7 to be mounted on HSP

4.2. General Accessories

Table 14 provides a list of general accessories applicable to all COMe pin-out Type 7 products.

Table 14: General Accessories List

Product Number	Mounting	Description
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	Description
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)

Table 15: Memory Modules

Part Number	Memory (Non-ECC)	Description
97020-0424-COM7	DDR4-2400 SODIMM 4 GB_COM7	DDR4-2400, 4 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97020-0824-COM7	DDR4-2400 SODIMM 8 GB_COM7	DDR4-2400, 8 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97020-1624-COM7	DDR4-2400 SODIMM 16 GB_COM7	DDR4-2400, 16 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97020-3224-COM7	DDR4-2400 SODIMM 32 GB_COM7	DDR4-2400, 32 GB, 260P, 1200 MHz, PC4-2400 SODIMM
97021-0424-COM7	DDR4-2400 SODIMM 4 GB E2_COM7	DDR4-2400, 4 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97021-0824-COM7	DDR4-2400 SODIMM 8 GB E2_COM7	DDR4-2400, 8 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97021-1624-COM7	DDR4-2400 SODIMM 16 GB E2_COM7	DDR4-2400, 16 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97021-3224-COM7	DDR4-2400 SODIMM 32 GB E2_COM7	DDR4-2400, 32 GB, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
Part Number	Memory (ECC)	Description
97030-0424-COM7	DDR4-2400 SODIMM 4 GB ECC_COM7	DDR4-2400, 4 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97030-0824-COM7	DDR4-2400 SODIMM 8 GB ECC_COM7	DDR4-2400, 8GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97030-1624-COM7	DDR4-2400 SODIMM 16 GB ECC_COM7	DDR4-2400, 16 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97030-3224-COM7	DDR4-2400 SODIMM 32 GB ECC_COM7	DDR4-2400, 32 GB, ECC, 260P, 1200 MHz, PC4-2400 SODIMM
97031-0424-COM7	DDR4-2400 SODIMM 4 GB ECC E2_COM7	DDR4-2400, 4 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97031-0824-COM7	DDR4-2400 SODIMM 8 GB ECC E2_COM7	DDR4-2400, 8 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97031-1624-COM7	DDR4-2400 SODIMM 16 GB ECC E2_COM7	DDR4-2400, 16 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature
97031-3224-COM7	DDR4-2400 SODIMM 32 GB ECC E2_COM7	DDR4-2400, 32 GB, ECC, E2, 260P, 1200 MHz, PC4-2400 SODIMM, industrial temperature

5/ Electrical Specification

5.1. Supply Voltage

Table 16 provides information regarding the supply voltage specified at the COM Express® connector.

Table 16: COM Express® Connector Electrical Specifications

	Commercial Grade	Industrial Grade
VCC	8.5 V – 20 V	12 V
Standby	5V DC +/- 5% (5 VSB is not mandatory for operation)	5 V DC +/- 5%
RTC	2.8 V - 3.47 V	2.8 V - 3.47 V

5 V Standby voltage is not mandatory for operation.

5.2. Power Supply Rise Time

- The input voltages should rise from ≤10% of nominal to within the regulation ranges within 0.1 ms to 20 ms.
- 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.

5.3. Supply Voltage Ripple

Maximum 100 mV peak to peak 0 – 20 MHz.

5.4. Power Consumption

The maximum Power Consumption of the different COMe-bBD7 variants is 35 W to 70 W (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 at EMD Customer Section.

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 17: ATX Mode

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

5.6. Single Supply Mode

In single supply mode, without 5V standby the module will start automatically when VCC power is connected and Power Good input is open or at high level (internal PU to 3.3V). 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 18: 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	reconnect VCC

All ground pins have to be tied to the ground plane of the carrier board.

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.

6/ Power Control

6.1. Power Supply

The COMe-bBD7 supports a power input from 8.5 V to 20 V in the commercial grade version, but 12 V in the industrial version. 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.

i Suspend-to-RAM (S3) is not supported by the Xeon D-1500 product family.

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 50ms (50 ms ≤ t < 4 s, typical 400 ms) at low level (Power Button Event).

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

6.3. Power Good (PWR_OK)

The COMe-bBD7 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 3.3 V and must be high level to power on the module. This is typically driven by the ATX power supply PWR_OK signal. The carrier needs to release the signal when ready.

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*.

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

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".

7/ Environmental Specification

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-bBD7.

Table 19: General Temperature Specification

Temperature Specification	Operating	Non-operating
Commercial grade	0°C to +60°C	-30°C to +85°C
Extended Temperature (E1)	-25°C to +75°C	-30°C to +85°C
Industrial grade by Screening (E2S)	-40°C to +85°C	-40°C to +85°C
Industrial grade by Design (E2)	-40°C to +85°C	-40°C to +85°C

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 20: 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 (E2S)	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

7.3. Operating without Kontron heatspreader plate assembly

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

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

7.4. Standards and Certifications

- RoHS II: The COMe-bBD7 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 4: RoHS

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.

CE

CE according to

- EN62368-1:2014 + AC:2015
- EN610000-6-3:2005 + Cor:2005
- CISPR 22: Edition 6.0 2008-09
- CISPR 32: 2015
- EN55022:2010+AC:2011
- EN55024:2010

UL Listings:

- NWGQ2.E304278
- NWGQ8.E304278

Figure 5: Component Recognition UL

WEEE Directive

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

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.

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, 10 Hz to 2000 Hz, +/-0.15 mm, 2 g)
- IEC/EN 60068-2-27 (Non operating Shock Test, half-sinusoidal, 11 ms, 15 g)

EMC

Validated in Kontron reference housing for EMC the COMe-bBD7 follows the requirements for electromagnetic compatibility standards:

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

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. or 62 years

Figure 6 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) = 548 007 h @ 40°C or 62 years

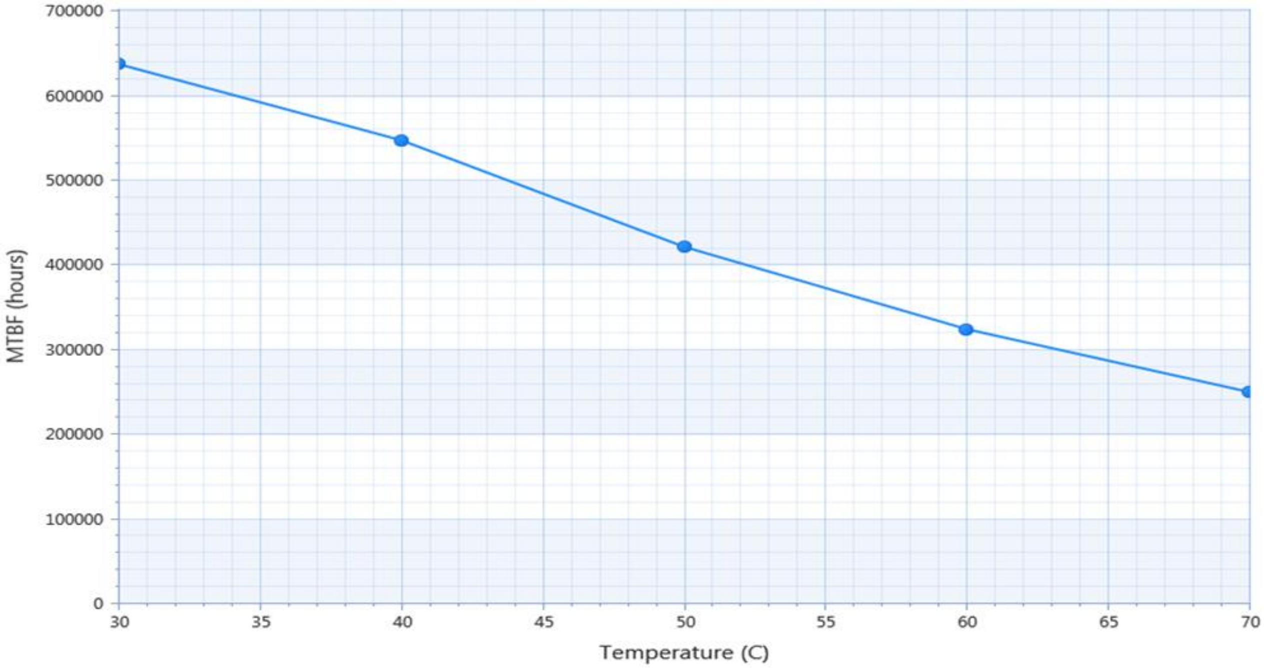


Figure 6: MTBF Temperature De-rating for Product 68005-0000-59-9 COMe-bBD7R E2 with D-1559 Processor

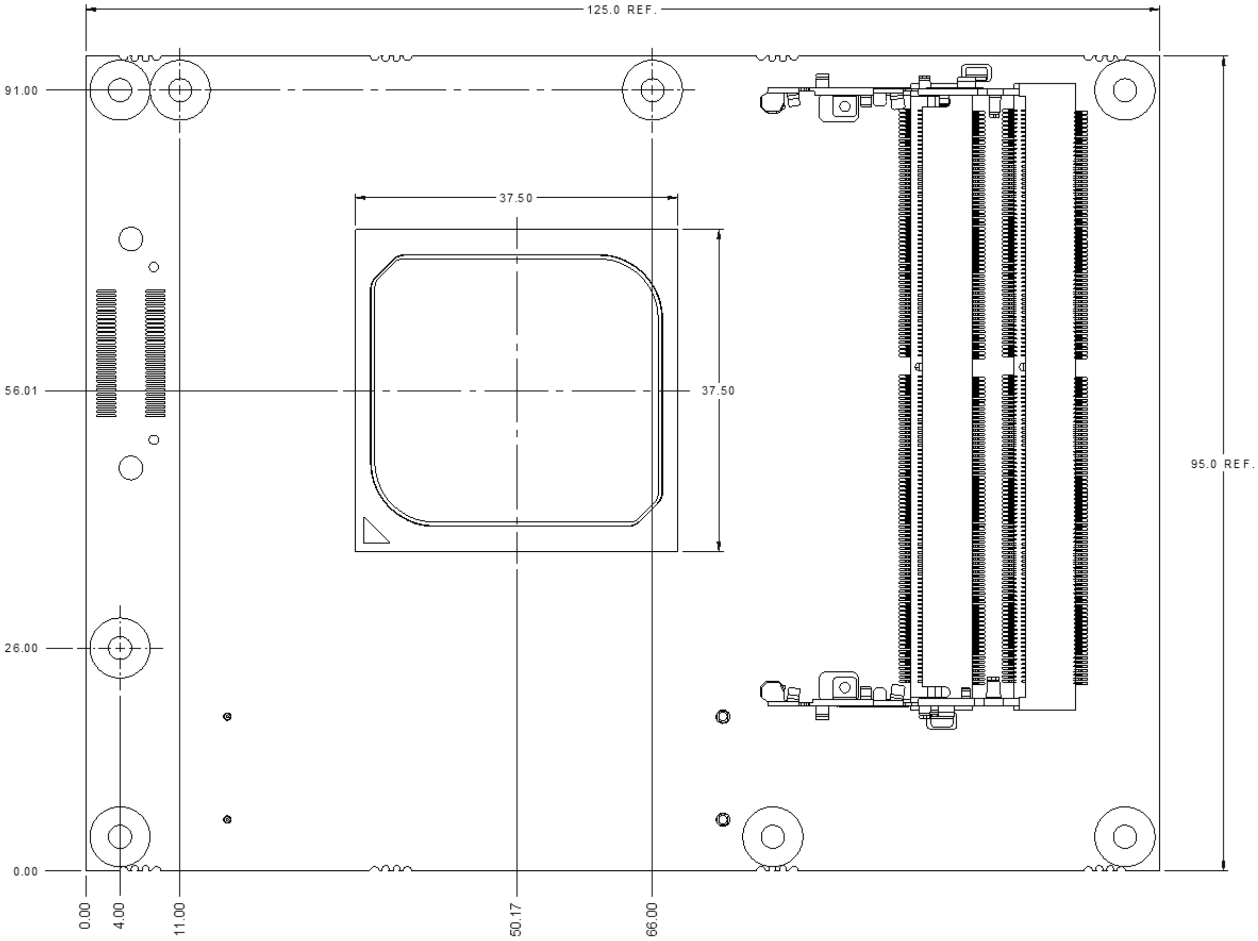
The above estimates assume no fan, but a passive heat sinking arrangement. Estimated RTC battery life (as opposed to battery failures) is not accounted for in the above figure and needs to be considered for separately. Battery life depends on both temperature and operating conditions. When the Kontron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

8/ Mechanical Specification

8.1. Dimensions

The dimensions of the module are 95.0 mm x 125.0 mm.

Figure 7: Module Dimensions



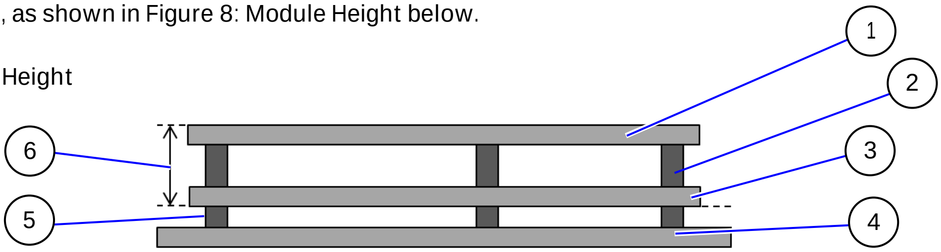
CAD drawings are available at EMD Customer Section.

8.1.1. Height

The height of the module depends on the height of the implemented cooling solution. The height of the cooling solution is not specified in the COM Express® specification.

The COM Express® specification defines a module height of approximately 13 mm from module PCB bottom to heatspreader top, as shown in Figure 8: Module Height below.

Figure 8: Module Height



1. Heatspreader
2. Heatspreaader standoff(s)
3. Module PCB
4. Carrier Board PCB
5. Connector standoff(s) 5 mm or 8 mm
6. 13 mm +/- 0.65 mm

8.2. Thermal Management, Heatspreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron for the COMe-bBD7. 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/XT)

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

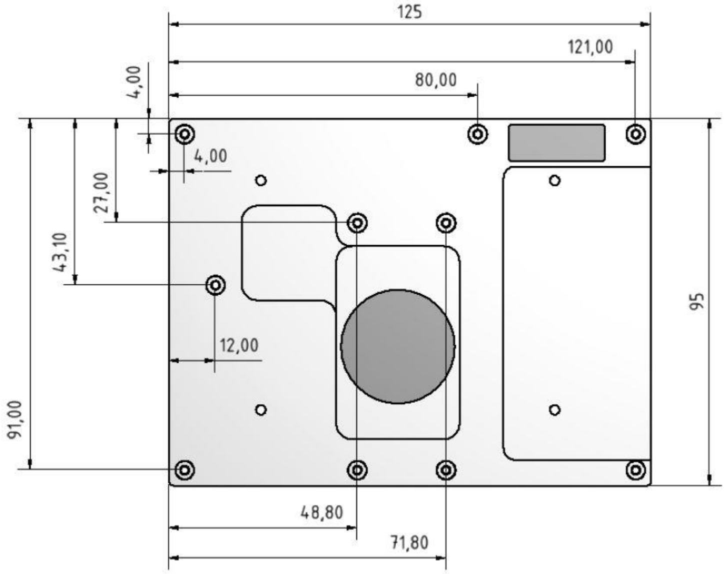
The optimum cooling solution varies, depending on the COM Express® application and environmental conditions. Active or passive cooling solutions provided from Kontron for the COMe-bBD7 are usually designed to cover the power and thermal dissipation for a commercial grade temperature range used in a housing with proper air flow.

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

8.2.1. Heatspreader Dimensions

The following figure shows the heatspreader's dimensions and location on the module.

Figure 9: Heatspreader Location and Dimensions



*All dimensions shown in mm.

9/ Features and Interfaces

9.1. Rapid Shutdown

The rapid shutdown function is no longer supported.

Please refer to the PCN BBD7V270.

9.2. 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.

9.3. SPI boot

The COMe-bBD7 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 21: SPI Boot Pin Configuration

Configuration	BIOS_DIS0#	BIOS_DIS1#	Function
1	open	open	Boot on module BIOS
2	GND	open	Not supported
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 22: Supported SPI boot flash types for 8-SOIC package

Size	Manufacturer	Part Number	Device ID
128 Mbit	Macronix	MX25L12805D	0xC22018
128 Mbit	Micron	N25Q128	0x20BA18
128 Mbit	Winbond	W25Q128JVSIG	0xEF7018

9.4. Using an external SPI flash

There are two possible flash utility to use. First one is internal Kflash utility (included in BIOS) or external AfuEfix64.efi utility. The Kflash utility has limited support of flash devices. In case the Kflash not support the flash chip you are using, you can try to use the external AfuEfix64.efi utility.

The Kflash "v" verify parameter 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.

Preparation to flash the carrier or module flash chip (common for Kflash and AfuEfix64):

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 pin 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.

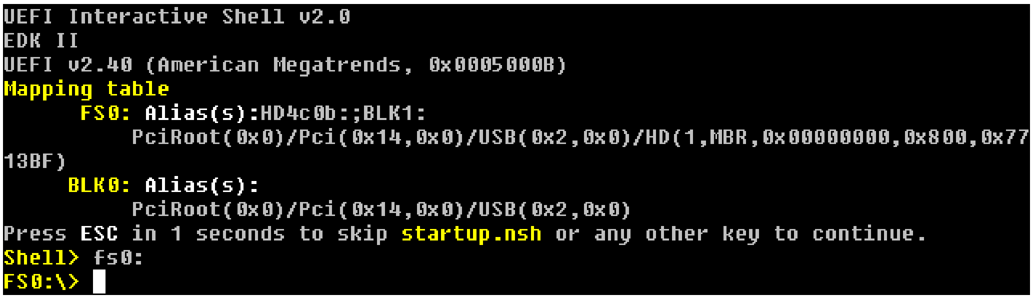
4. The BIOS Lock must be set to Disabled to be able to program flash. Default setting of BIOS Lock is Enabled. To change the BIOS Lock setting go to BIOS Setup and select IntelRCSetup | PCH Configuration | Security Configuration | BIOS Lock and press F4 (Save & Exit).

5. Connect pin B88 (BIOS_DIS1#) to ground to enable the external SPI flash.

6. From the EFI shell, enter the name of the partition of your USB Key in this example:

   FS0: , then **Enter**.

Figure 10: Entering USB Key Partition Name



```
UEFI Interactive Shell v2.0
EDK II
UEFI v2.40 (American Megatrends, 0x0005000B)
Mapping table
      FS0: Alias(s):HD4c0b:;BLK1:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x2,0x0)/HD(1,MBR,0x00000000,0x800,0x77
13BF)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x2,0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> 
```

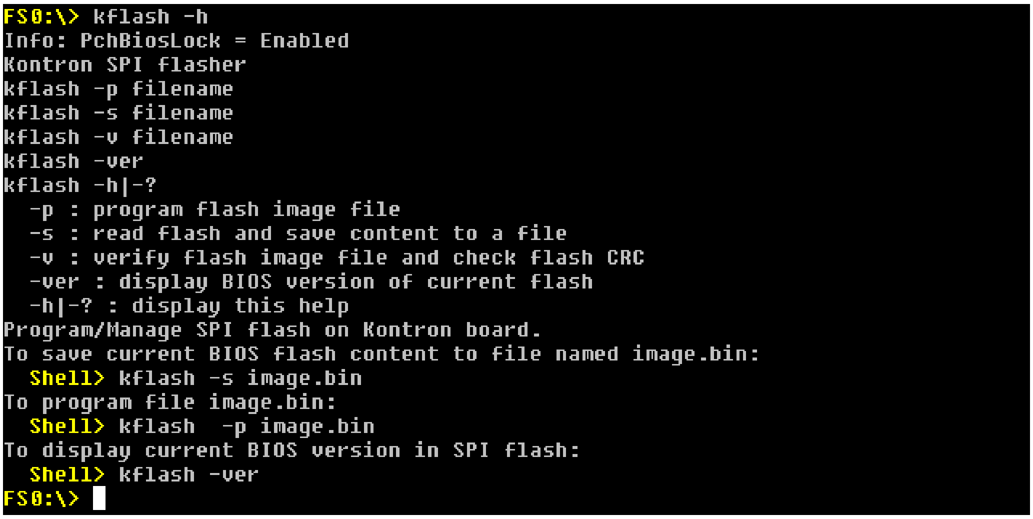
Use of internal Kflash utility:

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

   - **kflash -h**

   The kflash utility shows status of BIOS Lock (Info: PchBiosLock = Enabled/Disabled).

Figure 11: Using kflash help option



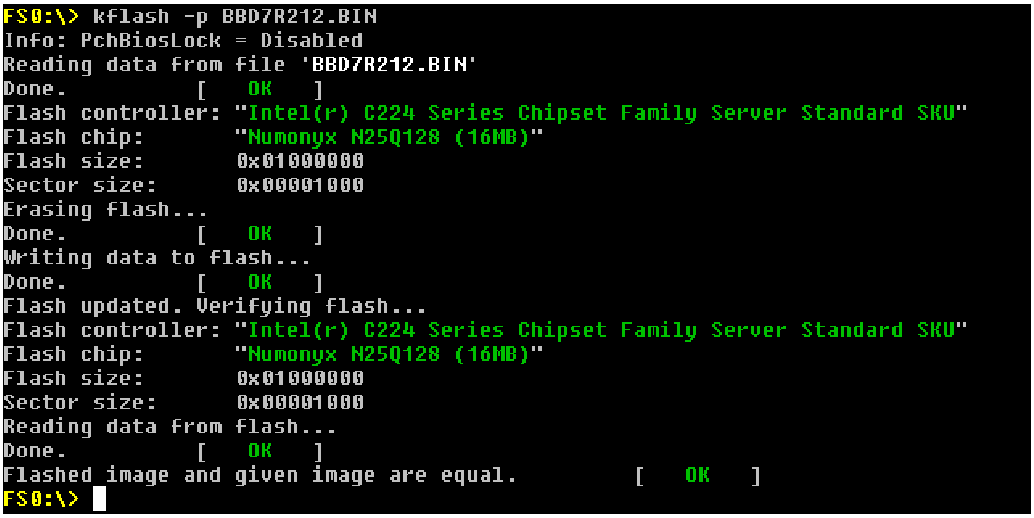
```
FS0:\> kflash -h
Info: PchBiosLock = Enabled
Kontron SPI flasher
kflash -p filename
kflash -s filename
kflash -v filename
kflash -ver
kflash -h|-?
  -p : program flash image file
  -s : read flash and save content to a file
  -v : verify flash image file and check flash CRC
  -ver : display BIOS 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
FS0:\> 
```

2. On your terminal, enter the following command:

   ▶ kflash -p “binary_name.bin”

   The following is displayed (see Figure 12)

Figure 12: Programming the Flash Image using Kflash



```
FS0:\> kflash -p BBD7R212.BIN
Info: PchBiosLock = Disabled
Reading data from file 'BBD7R212.BIN'
Done.          [   OK   ]
Flash controller: "Intel(r) C224 Series Chipset Family Server Standard SKU"
Flash chip:       "Numonyx N25Q128 (16MB)"
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:       "Numonyx N25Q128 (16MB)"
Flash size:       0x01000000
Sector size:      0x00001000
Reading data from flash...
Done.          [   OK   ]
Flashed image and given image are equal.         [   OK   ]
FS0:\>
```

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

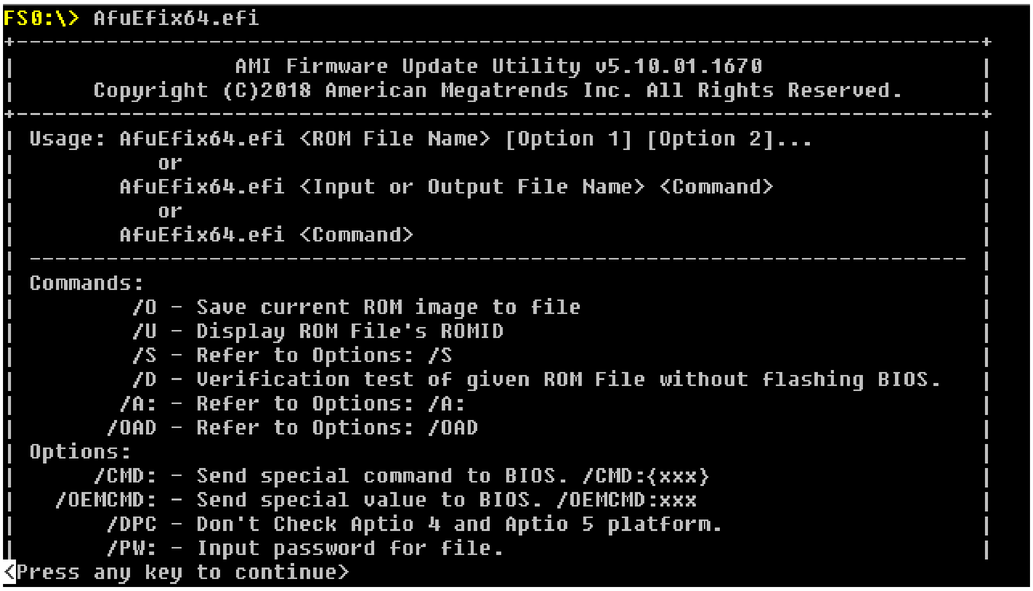
4. Your system has now been updated.

Use of external AfuEfix64.efi utility:

1. If you want to see a help guide regarding “AfuEfix64.efi” usage, enter following command:

   ▶ AfuEfix64.efi

Figure 13: Using AfuEfix64.efi help option



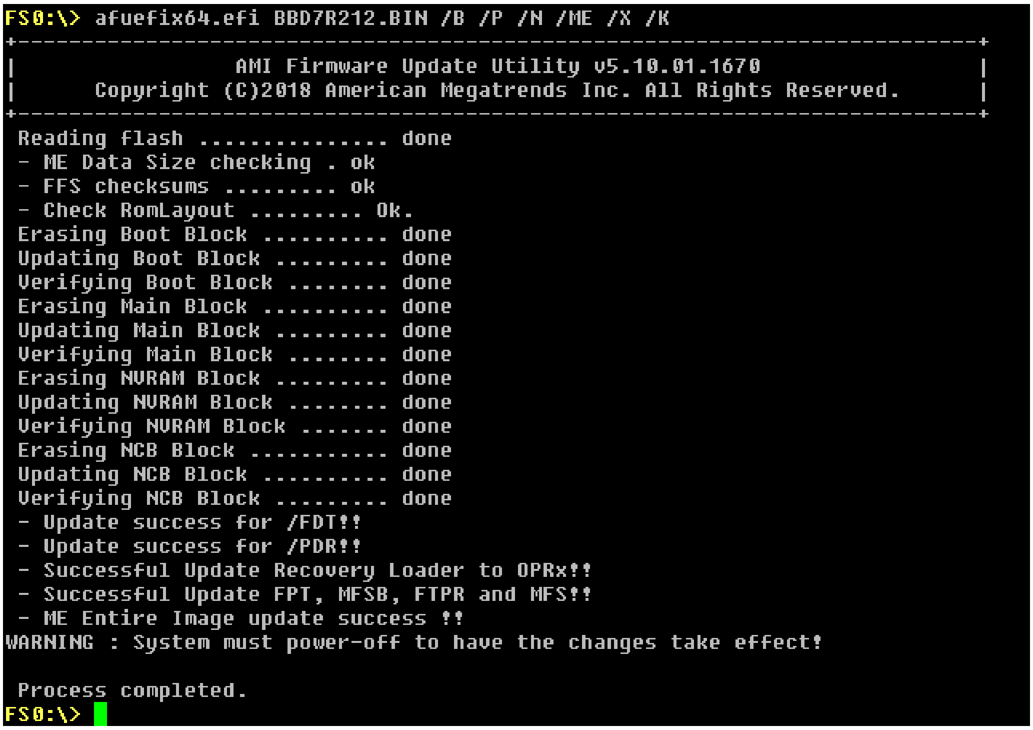
```
FS0:\> AfuEfix64.efi
+---------------------------------------------------------------------------+
|                 AMI Firmware Update Utility v5.10.01.1670                 |
|      Copyright (C)2018 American Megatrends Inc. All Rights Reserved.      |
+---------------------------------------------------------------------------+
| Usage: AfuEfix64.efi <ROM File Name> [Option 1] [Option 2]...             |
|          or                                                               |
|        AfuEfix64.efi <Input or Output File Name> <Command>                |
|          or                                                               |
|        AfuEfix64.efi <Command>                                            |
| ------------------------------------------------------------------------- |
| Commands:                                                                 |
|         /O - Save current ROM image to file                               |
|         /U - Display ROM File's ROMID                                     |
|         /S - Refer to Options: /S                                         |
|         /D - Verification test of given ROM File without flashing BIOS.   |
|        /A: - Refer to Options: /A:                                        |
|       /OAD - Refer to Options: /OAD                                      |
| Options:                                                                  |
|      /CMD: - Send special command to BIOS. /CMD:{xxx}                     |
|   /OEMCMD: - Send special value to BIOS. /OEMCMD:xxx                      |
|       /DPC - Don't Check Aptio 4 and Aptio 5 platform.                    |
|       /PW: - Input password for file.                                     |
<Press any key to continue>
```

2. On your terminal, enter the following command:

   - **AfuEfix64.efi** “binary_name.bin” /B /P /N /ME /X /K

   The following is displayed

Figure 14: Programming the Flash Image using AfuEfix64.efi



```
FS0:\> afuefix64.efi BBD7R212.BIN /B /P /N /ME /X /K
+---------------------------------------------------------------------------+
|                 AMI Firmware Update Utility v5.10.01.1670                 |
|      Copyright (C)2018 American Megatrends Inc. All Rights Reserved.      |
+---------------------------------------------------------------------------+
 Reading flash ............... done
 - ME Data Size checking . ok
 - FFS checksums ......... ok
 - Check RomLayout ......... Ok.
 Erasing Boot Block .......... done
 Updating Boot Block ......... done
 Verifying Boot Block ........ done
 Erasing Main Block .......... done
 Updating Main Block ......... done
 Verifying Main Block ........ done
 Erasing NVRAM Block ......... done
 Updating NVRAM Block ........ done
 Verifying NVRAM Block ....... done
 Erasing NCB Block ........... done
 Updating NCB Block .......... done
 Verifying NCB Block ......... done
 - Update success for /FDT!!
 - Update success for /PDR!!
 - Successful Update Recovery Loader to OPRx!!
 - Successful Update FPT, MFSB, FTPR and MFS!!
 - ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!

 Process completed.
FS0:\>
```

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

4. Your system has now been updated.

For more information, visit the EMD Customer Section.

9.5. 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 flashed device.

To avoid this issue 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.

9.6. Triple Staged Watchdog Timer

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-bBD7 offers a watchdog which works with three stages that can be programmed independently and used one by one.

Table 23: 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.

9.7. 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. Reassertion of the signal is done automatically after reset. If deassertion during runtime is necessary, please ask your Kontron technical support for further help.

9.8. 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.

9.9. 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 24: Following C-States are defined

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 may 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.

9.10. Hyper-Threading

Hyper-Threading (officially termed Hyper Threading Technology or HTT) is an Intel®-proprietary technology used to improve parallelization of computations performed on PCs. 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 always depends on the Operating System.

9.11. ACPI Suspend Modes and Resume Events

The COMe-bBD7 supports the S-states S0, S4, and S5.

The following events resume the system from S4:

- Power Button
- WakeOnLan

The following events resume the system from S5:

- Power Button
- WakeOnLan

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

9.12. Fan Connector (J7)

Figure 15: 3-pin Fan Connector

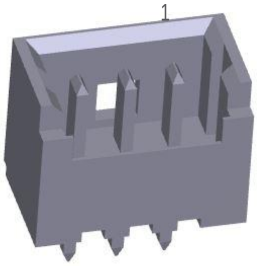


Table 25: 3-pin Fan Connector

Pin	Signal	Description	Type
1	TACHO	Rotation speed	I
2	PWM	PWM output	O-5 V
3	GND	Ground	PWR

Table 26: Signal Description

Signal	Description
GND	Power Supply GND signal
TACHO	Tacho input signal from the fan, for rotation speed supervision RPM (Rotations Per Minute).
PWM	Output signal for FAN speed control.

10 / System Resources

10.1. Interrupt Request (IRQ) Lines

Table 27: List of Interrupt Requests

IRQ/Data frame	Signal Sampled	# of clocks past start	Employed by
1	IRQ0	2	Reserved
2	IRQ1	5	Keyboard
3	SMI#	8	H/W Monitor & SMI
4	IRQ3	11	UART B
5	IRQ4	14	UART A
6	IRQ5	17	-
7	IRQ6	20	FDC
8	IRQ7	23	LPT
9	IRQ8	26	-
10	IRQ9	29	-
11	IRQ10	32	-
12	IRQ11	35	-
13	IRQ12	38	Mouse
14	IRQ13	41	Reserved
15	IRQ14	44	-
16	IRQ15	47	-
17	IOCHCK#	50	-
18	INTA#	53	-
19	INTB#	56	-
20	INTC#	59	-
21	INTD#	62	-
32:22	Unassigned	95	-

10.2. 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 28: 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	-

10.3. I/O Address Map

The I/O-port addresses of the bBD7 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 29: 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

I/O Address	Used for	Available	Comment
0000-001F	DMA 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.

10.4. I2C Bus

Table 30: I2C Bus Port Addresses

8-bit Address	7-bit Address	Device	I2C Bus
		Embedded Controller FPGA	I2C_EXT
A0	50	COMe Module EEPROM	I2C_EXT
58	2C	5ECO Circuit	I2C_EXT
var.	var.	COMexpress connector	I2C_EXT
(AE)	(57)	(carrier EEPROM)	I2C_EXT

10.5. 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.

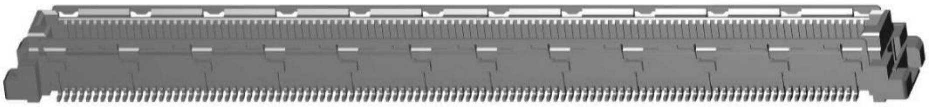
Table 31: Designated I/O Port Addresses

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.

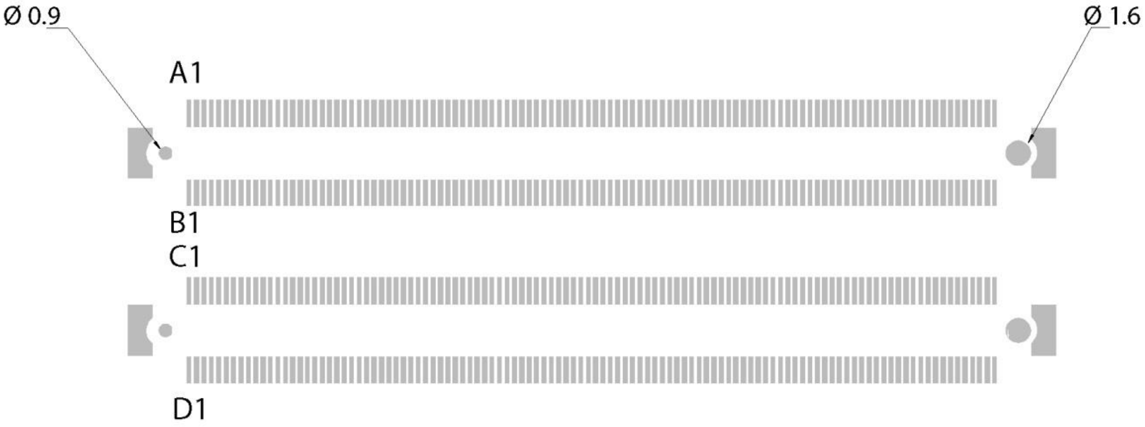
11/ COMe Connector Pin-out List

Figure 16: COMe Connector with 220 pins



This table lists the pins and signals according to the PICMG specification COM.0 Rev 3.0 Type 7 standard.

Figure 17: COMe Connector Pinout



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.

Table 32: Pin-out List

Pin	Row A	Row B	Row C	Row D
1	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
2	GBE0_MDI3-	GBE0_ACT#	GND	GND
3	GBE0_MDI3+	LPC_FRAME#/ESPI_CS0#	USB_SSRX0-	USB_SSTX0-
4	GBE0_LINK100#	LPC_AD0/ESPI_IO_0	USB_SSRX0+	USB_SSTX0+
5	GBE0_LINK1000#	LPC_AD1/ESPI_IO_1	GND	GND
6	GBE0_MDI2-	LPC_AD2/ESPI_IO_2	USB_SSRX1-	USB_SSTX1-

Pin	Row A	Row B	Row C	Row D
7	GBE0_MDI2+	LPC_AD3/ESPI_IO_3	USB_SSRX1+	USB_SSTX1+
8	GBE0_LINK#	LPC_DRQ0#/ESPI_ALERT0#	GND	GND
9	GBE0_MDI1-	LPC_DRQ1#/ESPI_ALERT1#	USB_SSRX2-	USB_SSTX2-
10	GBE0_MDI1+	LPC_CLK/ESPI_CK	USB_SSRX2+	USB_SSTX2+
11	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
12	GBE0_MDI0-	PWRBTN#	USB_SSRX3-	USB_SSTX3-
13	GBE0_MDI0+	SMB_CK	USB_SSRX3+	USB_SSTX3+
14	GBE0_CTREF	SMB_DAT	GND	GND
15	SUS_S3#	SMB_ALERT#	10G_PHY_MDC_SCL3	10G_PHY_MDIO_SDA3
16	SATA0_TX+	SATA1_TX+	10G_PHY_MDC_SCL2	10G_PHY_MDIO_SDA2
17	SATA0_TX-	SATA1_TX-	10G_SDP2	10G_SDP3
18	SUS_S4#	SUS_STAT#/ESPI_RESET#	GND	GND
19	SATA0_RX+	SATA1_RX+	PCIE_RX6+	PCIE_TX6+
20	SATA0_RX-	SATA1_RX-	PCIE_RX6-	PCIE_TX6-
21	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
22	PCIE_TX15+	PCIE_RX15+	PCIE_RX7+	PCIE_TX7+
23	PCIE_TX15-	PCIE_RX15-	PCIE_RX7-	PCIE_TX7-
24	SUS_S5#	PWR_OK	10G_INT2	10G_INT3
25	PCIE_TX14+	PCIE_RX14+	GND	GND
26	PCIE_TX14-	PCIE_RX14-	10G_KR_RX3+	10G_KR_TX3+
27	BATLOW#	WDT	10G_KR_RX3-	10G_KR_TX3-
28	(S)ATA_ACT#	RSVD	GND	GND
29	RSVD	RSVD	10G_KR_RX2+	10G_KR_TX2+
30	RSVD	RSVD	10G_KR_RX2-	10G_KR_TX2-
31	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
32	RSVD	SPKR	10G_SFP_SDA3	10G_SFP_SCL3

Pin	Row A	Row B	Row C	Row D
33	RSVD	I2C_CK	10G_SFP_SDA2	10G_SFP_SCL2
34	BIOS_DIS0#/ESPI_SAFS	I2C_DAT	10G_PHY_RST_23	10G_PHY_CAP_23
35	THRMTRIP#	THRM#	10G_PHY_RST_01	10G_PHY_CAP_01
36	PCIE_TX13+	PCIE_RX13+	10G_LED_SDA	RSVD
37	PCIE_TX13-	PCIE_RX13-	10G_LED_SCL	RSVD
38	GND	GND	10G_SFP_SDA1	10G_SFP_SCL1
39	PCIE_TX12+	PCIE_RX12+	10G_SFP_SDA0	10G_SFP_SCL0
40	PCIE_TX12-	PCIE_RX12-	10G_SDP0	10G_SDP1
41	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
42	USB2-	USB3-	10G_KR_RX1+	10G_KR_TX1+
43	USB2+	USB3+	10G_KR_RX1-	10G_KR_TX1-
44	USB_2_3_OC#	USB_0_1_OC#	GND	GND
45	USB0-	USB1-	10G_PHY_MDC_SCL1	10G_PHY_MDIO_SDA1
46	USB0+	USB1+	10G_PHY_MDC_SCL0	10G_PHY_MDIO_SDA0
47	VCC_RTC	ESPI_EN#	10G_INT0	10G_INT1
48	RSVD	USB0_HOST_PRSNT	GND	GND
49	GBE0_SDP	SYS_RESET#	10G_KR_RX0+	10G_KR_TX0+
50	LPC_SERIRQ/ESPI_CS1#	CB_RESET#	10G_KR_RX0-	10G_KR_TX0-
51	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
52	PCIE_TX5+	PCIE_RX5+	PCIE_RX16+	PCIE_TX16+
53	PCIE_TX5-	PCIE_RX5-	PCIE_RX16-	PCIE_TX16-
54	GPI0	GPO1	TYPE0#	RSVD
55	PCIE_TX4+	PCIE_RX4+	PCIE_RX17+	PCIE_TX17+
56	PCIE_TX4-	PCIE_RX4-	PCIE_RX17-	PCIE_TX17-
57	GND	GPO2	TYPE1#	TYPE2#
58	PCIE_TX3+	PCIE_RX3+	PCIE_RX18+	PCIE_TX18+

Pin	Row A	Row B	Row C	Row D
59	PCIE_TX3-	PCIE_RX3-	PCIE_RX18-	PCIE_TX18-
60	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
61	PCIE_TX2+	PCIE_RX2+	PCIE_RX19+	PCIE_TX19+
62	PCIE_TX2-	PCIE_RX2-	PCIE_RX19-	PCIE_TX19-
63	GPI1	GPO3	RSVD	RSVD
64	PCIE_TX1+	PCIE_RX1+	RSVD	RSVD
65	PCIE_TX1-	PCIE_RX1-	PCIE_RX20+	PCIE_TX20+
66	GND	WAKE0#	PCIE_RX20-	PCIE_TX20-
67	GPI2	WAKE1#	RAPID_SHUTDOWN	GND
68	PCIE_TX0+	PCIE_RX0+	PCIE_RX21+	PCIE_TX21+
69	PCIE_TX0-	PCIE_RX0-	PCIE_RX21-	PCIE_TX21-
70	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
71	PCIE_TX8+	PCIE_RX8+	PCIE_RX22+	PCIE_TX22+
72	PCIE_TX8-	PCIE_RX8-	PCIE_RX22-	PCIE_TX22-
73	GND	GND	GND	GND
74	PCIE_TX9+	PCIE_RX9+	PCIE_RX23+	PCIE_TX23+
75	PCIE_TX9-	PCIE_RX9-	PCIE_RX23-	PCIE_TX23-
76	GND	GND	GND	GND
77	PCIE_TX10+	PCIE_RX10+	RSVD	RSVD
78	PCIE_TX10-	PCIE_RX10-	PCIE_RX24+	PCIE_TX24+
79	GND	GND	PCIE_RX24-	PCIE_TX24-
80	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
81	PCIE_TX11+	PCIE_RX11+	PCIE_RX25+	PCIE_TX25+
82	PCIE_TX11-	PCIE_RX11-	PCIE_RX25-	PCIE_TX25-
83	GND	GND	RSVD	RSVD
84	NCSI_TX_EN	VCC_5V_SBY	GND	GND
85	GPI3	VCC_5V_SBY	PCIE_RX26+	PCIE_TX26+
86	RSVD	VCC_5V_SBY	PCIE_RX26-	PCIE_TX26-

Pin	Row A	Row B	Row C	Row D
87	RSVD	VCC_5V_SBY	GND	GND
88	PCIE_CK_REF+	BIOS_DIS1#	PCIE_RX27+	PCIE_TX27+
89	PCIE_CK_REF-	NCSI_RX_ER	PCIE_RX27-	PCIE_TX27-
90	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
91	SPI_POWER	NCSI_CLK_IN	PCIE_RX28+	PCIE_TX28+
92	SPI_MISO	NCSI_RXD1	PCIE_RX28-	PCIE_TX28-
93	GPO0	NCSI_RXD0	GND	GND
94	SPI_CLK	NCSI_CRS_DV	PCIE_RX29+	PCIE_TX29+
95	SPI_MOSI	NCSI_TXD1	PCIE_RX29-	PCIE_TX29-
96	TPM_PP	NCSI_TXD0	GND	GND
97	TYPE10#	SPI_CS#	RSVD	RSVD
98	SER0_TX	NCSI_ARB_IN	PCIE_RX30+	PCIE_TX30+
99	SER0_RX	NCSI_ARB_OUT	PCIE_RX30-	PCIE_TX30-
100	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)
101	SER1_TX	FAN_PWMOUT	PCIE_RX31+	PCIE_TX31+
102	SER1_RX	FAN_TACHIN	PCIE_RX31-	PCIE_TX31-
103	LID#	SLEEP#	GND	GND
104	VCC_12V	VCC_12V	VCC_12V	VCC_12V
105	VCC_12V	VCC_12V	VCC_12V	VCC_12V
106	VCC_12V	VCC_12V	VCC_12V	VCC_12V
107	VCC_12V	VCC_12V	VCC_12V	VCC_12V
108	VCC_12V	VCC_12V	VCC_12V	VCC_12V
109	VCC_12V	VCC_12V	VCC_12V	VCC_12V
110	GND(FIXED)	GND(FIXED)	GND(FIXED)	GND(FIXED)

12/ uEFI BIOS

12.1. Starting the uEFI BIOS

The COMe-bBD7 uses a Kontron-customized, pre-installed and configured version AMI EFI BIOS Aptio ® V based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI. This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the COMe-bDV7.

i 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.

i Register for the EMD Customer Section to access BIOS downloads and the Product Change Notification (PCN) service.

The uEFI BIOS comes with a Setup program that provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration. The Setup program allows for access to various menus that provide functions or access to sub-menus with further specific functions of their own.

To start the uEFI BIOS Setup program, follow the steps below:

1. Power on the board.

Wait until the first characters appear on the screen (POST messages or splash screen).

Press the <DEL> key.

If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Security Setup Menu), press <RETURN>, and proceed with step 5.

A Setup menu appears.

The COMe-bBD7 uEFI BIOS Setup program uses a hot key navigation system. The hot key legend bar is located at the bottom of the Setup screens. The following table provides a list of navigation hot keys available in the legend bar.

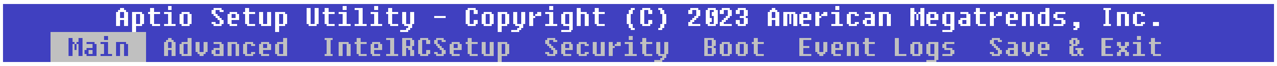
Table 33: Navigation Hot Keys Available in the Legend Bar

Sub-screen	Description
<F1>	<F1> key invokes the General Help window
<->	<Minus> key selects the next lower value within a field
<+>	<Plus> key selects the next higher value within a field
<F2>	<F2> key loads previous values
<F3>	<F3> key loads optimized defaults
<F4>	<F4> key Saves and Exits
<→> or <←>	<Left/Right> arrows selects major Setup menus on menu bar, for example, Main or Advanced
<↑> or <↓>	<Up/Down> arrows select fields in the current menu, for example, Setup function or sub-screen
<ESC>	<ESC> key exits a major Setup menu and enters the Exit Setup menu Pressing the <ESC> key in a sub-menu displays the next higher menu level
<RETURN>	<RETURN> key executes a command or selects a submenu

12.2. Setup Menus

The Setup utility features a selection bar at the top of the screen that lists the menus.

Figure 18: Setup Menu Selection Bar



```
       Aptio Setup Utility – Copyright (C) 2023 American Megatrends, Inc.
   Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit
```

The Setup menus available for the COMe-bBD7 are:

- Main
- Advanced
- IntelRCSetup
- Security
- Boot
- Event Logs
- Save & Exit

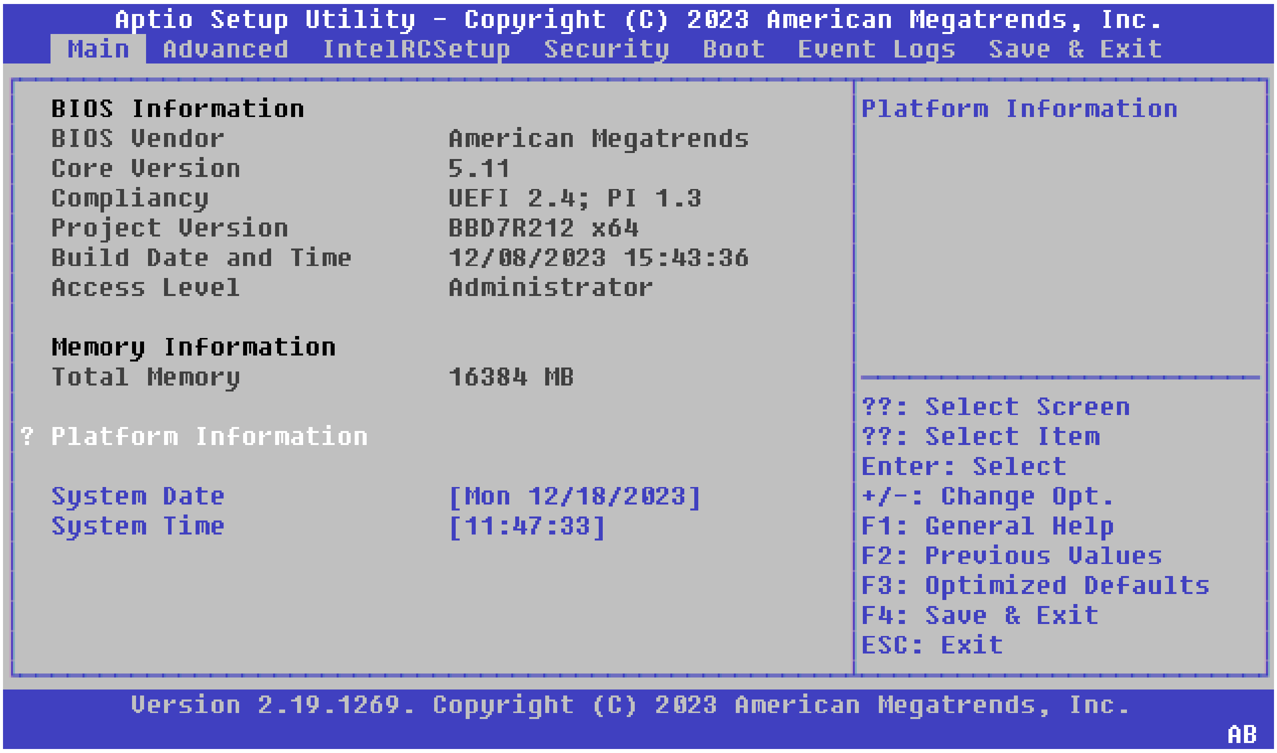
The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white. Use the left and right arrow keys to select the Setup menus.

Each Setup menu provides two main frames. The left frame displays all available functions. Configurable functions are displayed in blue. Functions displayed in grey provide information about the status or the operational configuration. The right frame displays a Help window providing an explanation of the respective function.

12.3. Main Menu

On entering the uEFI BIOS, the Setup program displays the Main Setup menu that lists basic system information.

Figure 19: Main Setup Menu



```
       Aptio Setup Utility – Copyright (C) 2023 American Megatrends, Inc.
   Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

   BIOS Information                                     Platform Information
   BIOS Vendor               American Megatrends
   Core Version              5.11
   Compliancy                UEFI 2.4; PI 1.3
   Project Version           BBD7R212 x64
   Build Date and Time       12/08/2023 15:43:36
   Access Level              Administrator

   Memory Information
   Total Memory              16384 MB
                                                        ??: Select Screen
 ? Platform Information                                 ??: Select Item
                                                        Enter: Select
   System Date               [Mon 12/18/2023]           +/-: Change Opt.
   System Time               [11:47:33]                 F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit

         Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                        AB
```

The following table shows Main sub-screens and functions, and describes the content. Default settings are in **bold**. Some function contain additional information

Table 34: Main Setup Menu Sub-screens

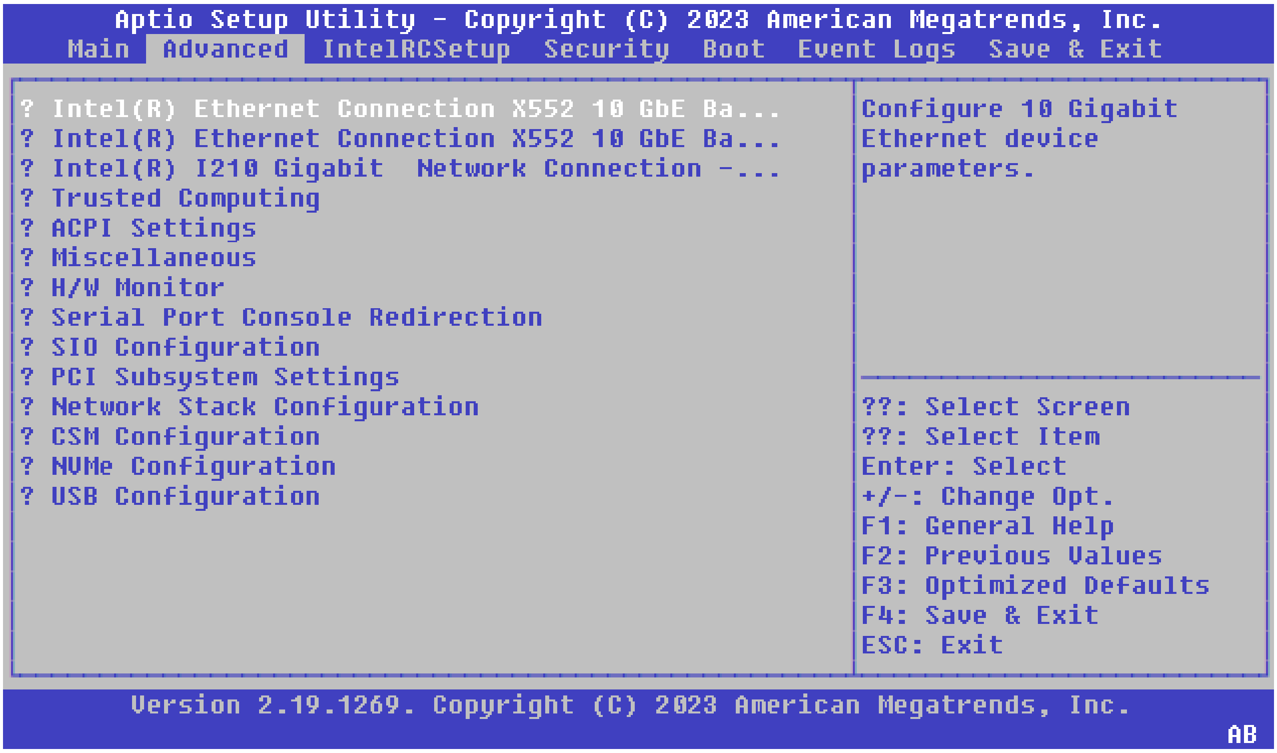
Sub-Screen	Description
BIOS Information>	Read only field BIOS Vendor, Cor Version, Compliancy, project Version, Build Date and Time, Access Level
Memory Information>	Read only field Total memory
System Language>	Selects system default language [**English**]
Platform Information>	Read only field Product Name, revision, Serial #, MAC Address, Boot Counter, FPD Rev
	Additional information for MAC Address The MAC address entry is the value used by the Ethernet controller and may contain the entry' Inactive' - Ethernet chip is inactive. To activate the Ethernet chip set the following: Advanced > Network Stack Configuration > Network Stack > Enable 88:88:88:88:87:88 is a special pattern that will be filled in by the Ethernet firmware if there is no valid entry in the firmware block of the BIOS SPI (i.e. the MAC address has been overwritten during the last attempt to flash the system). For more information, see Chapter 12.10 Firmware Update.
System Date>	Displays the system date [Week Day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

12.4. Advanced Setup Menu

The Advanced Setup menu provides sub-screens and second level sub-screens with functions, for advanced configuration and Kontron specific configurations.

NOTICE Setting items on this screen to incorrect values may cause system malfunctions.

Figure 20: Advanced Setup Menu



```
      Aptio Setup Utility – Copyright (C) 2023 American Megatrends, Inc.
   Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

? Intel(R) Ethernet Connection X552 10 GbE Ba...   Configure 10 Gigabit
? Intel(R) Ethernet Connection X552 10 GbE Ba...   Ethernet device
? Intel(R) I210 Gigabit  Network Connection -...   parameters.
? Trusted Computing
? ACPI Settings
? Miscellaneous
? H/W Monitor
? Serial Port Console Redirection
? SIO Configuration
? PCI Subsystem Settings
? Network Stack Configuration                      ??: Select Screen
? CSM Configuration                                ??: Select Item
? NVMe Configuration                               Enter: Select
? USB Configuration                                +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

        Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                        AB
```

The following table provides an over view of the Advanced menu sub-screens and functions listed below and describes the content. Default settings are in **bold**. Some function contain additional information

Table 35: Advanced Setup menu Sub-screens and Functions

Sub-Screen	Second Level Sub-screen	Further Sub-Screens/Description	
Intel® Ethernet Connection	NIC Configuration>	Configure the Network device port	
		Link Speed>	Auto Negotiated
		Wake On LAN>	[**Enabled**, Disabled]
	Blink LED	Identify the physical Network port by blinking the associated LED	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		

Intel® Ethernet Connection	NIC Configuration>	Configure the Network device port	
		Link Speed>	Auto Negotiated
		Wake On LAN>	[**Enabled**, Disabled]
	Blink LED	Identify the physical Network port by blinking the associated LED	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		
Intel® I210 Gigabit Network Connection	NIC Configuration>	Configure the Network device port	
		Link Speed>	Auto Negotiated
		Wake On LAN>	[**Enabled**, Disabled]
	Blink LED>	Identify the physical Network port by blinking the associated LED	
	Read only field UEFI Driver, Adapter PBA, Device Name, Chip Type, PCI Device ID, PCI Address, Link status, MAC Address, Virtual MAC Address		
Trusted Computing>	Security device Sup>	Enables or disables BIOS support for security device. Operating System will not show security device. The TCG EFI protocol and INT1A interface are not available. [**Enabled**, Disabled]	
	Active PCR Banks>	Read only field [**SHA-1**]	
	Available PCR Banks>	Read only field [**SHA-1, SHA256**]	
	SHA-1 PCR Bank>	SHA-1 PCR Bank [**Enable**/Disable]	
	SHA256 PCR Bank>	SHA256 PCR Bank [Enable/**Disable**]	
	Pending Operation>	Schedules an operation for Security Device Note: Computer reboots on restart in order to change the state of the security device. [**None**, TPM Clear]	
	Platform Hierarchy>	Platform Hierarchy [**Enabled**, Disabled]	
	Storage Hierarchy>	Storage Hierarchy [**Enabled**, Disabled]	
	Endorsement Hierarchy>	Endorsement Hierarchy [**Enabled**, Disabled]	
	TPM2.0 UEFI Spec Version>	Selects TCG2 Spec Version support: TCG_1_2 -compatible mode for Win8/Win10 and TCG_2: supports TCG2 protocol and event format for Win10 or later. [TCG_1_2, **TCG_2**]	
	Physical Presence Spec Version>	Select to tell OS to support either PPI Spec 1.2 or 1.3 Note: Some HCK tests might not support 1.3. [**1.2**, 1.3]	
	TPM 20 InterfaceType>	Read only field [**TIS**]	

Trusted Computing> (continued)	Device Select>		BIOS support for security devices. Auto supports both TPM 1.2 and TPM 2.0. TPM 1.2 supports TPM 1.2 devices only and TPM 2.0 supports TPM 2.0. devices only. [TPM 1.2, TPM 2.0, **Auto**]
ACPI Settings>	Enable ACPI Auto Configuration>		Enables or disables ACPI auto configuration. If enabled, the system uses generic ACPI settings that may not fit the system best. [Enabled, **Disabled**]
	Enable Hibernation>		Enables or disables systems ability to hibernate (OS/S4 Sleep State) This option may not be effective with some operating systems. [**Enabled**, Disabled]
	Lock Legacy Resources>		Enables or disable lock of legacy resources [Enabled, **Disabled**]
Miscellaneous>	Generic LPC Decode Ranges>	Generic LPC Decode Ranges>	Enables or disables the generic LPC decode range [Enabled, **Disabled**]
	Watchdog>	Auto Reload>	Enables automatic reload of watchdog timers on timeout [Enabled, **Disabled**]
		Global Lock>	Enable sets all Watchdog registers (except for WD_KICK) to read only, until board is reset. [Enabled, **Disabled**]
		Stage 1 Mode>	Selects action for this Watchdog stage [**Disabled**, Reset, NMI, SCI, Delay, WDT Signal only]
	I2C Speed>		Selects internal I2C bus speed between (1 kHz and 400 kHz) For a default system 200KHz is appropriate.
	GPIO I2C MUX Enable>		Enable or Disable GPIO I2C MUX on GPIO 6,7 [**Disabled**, Enabled]
	Reset Button Behavior>		Selects reset button behavior [**Chipset Reset**, Power Cycle]
	Skip S5 Eco config.>		Skip S5 Eco configuration (in case Enabled, then no access to S5 Eco I2C register) [Disabled, **Enabled**]
	S5 Eco>		S5 Eco> Item is shown only in case the Skip S5 Eco congig. is set to Disabled. Reduces Supply current in softoff(S%) to less than 1 mA. If enabled, power button is the only wakeup source and 'save changes and reset' will power-down the system insread of PCH full. [Enabled, **Disabled**]
	LID Switch Mode>		Read only field Shows or hides Lid Switch Inside ACPI OS. [**Disabled**]
	Sleep Button Mode>		Shows or hides Sleep Button inside ACPI OS. Default setting is disabled. [**Enabled**, Disabled]

Miscellaneous> (continued)	Manufacturing Mode>	Read only field [**Disabled**]
	TPM Enable>	Enables or disables the Trusted Platform Module (TPM) [**Enabled**, Disabled]
	PCI ExpressCard 0>	Controls PCIe port for ExpressCard support If not used, keep in the disabled state. [Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, **Disabled**]
	PCI ExpressCard 1>	Controls PCIe port for ExpressCard support If not used, keep in the disabled state. [Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, **Disabled**]
H/W Monitor>	Read only field Hardware Monitor name	
	CPU Temperature>	Read only field Displays CPU temperature in °C
	PCH Temperature>	Read only field Displays PCH temperature in °C
	Module Temperature>	Read only field Displays module temperature in °C
	CPU Fan – Fan Control>	Set fan control mode. 'Disable' will totally stop the fan. a. Disable - stops fan. b. Manual – manually sets the fan. c. Auto – Hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disable, Manual, **Auto**]
	CPU Fan – Fan Pulse>	Displays number of pulses fan produces during 1 revolution. (Range: 1-4) [**2**]
	CPU Fan – Fan Trip Point>	Displays temperature at which the fan accelerates. (Range: 20°C – 80°) [**50**]
	CPU Fan – Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30 %. Fan always runs at 100 % at TJmax (-10°C). [**50**]
	CPU Fan – Ref. Temperature>	Determines temperature source used for automatic fan control [PCH Temperature, Module Temperature, **CPU Temperature**]
	External Fan- Fan Control>	Set fan control mode. 'Disable' will totally stop the fan. a. Disable - stops fan. b. Manual – manually sets the fan. c. Auto – Hardware monitor controls cooling, similar to ACPI based 'Active Cooling', without producing a software load to the system. [Disable, Manual, **Auto**]

H/W Monitor> (continued)	External Fan– Fan Pulse>	Displays number of pulse fan produces during 1 revolution (Range: 1-4) [**2**]	
	External Fan- Fan Trip point>	Displays temperature at which fan accelerates. (Range: 20°C to 80°C) [**50**]	
	External Fan- Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30% Fan always runs at 100% at TJmax (-10°C) [**50**]	
	External Fan Reference Temperature>	Determines temperature source used for automatic fan control [PCH Temperature, Module Temperature, **CPU Temperature**]	
	Additional information External Fan An external fan can be connected to baseboard. The external fan control lines are routed via the COMe pins.		
	5.0 V Standby>	Read only field Displays standby voltage	
	Batt Volt. at COMe Pin>	Read only field Displays battery voltage at COMe pin	
	Widerange Vcc>	Read only field Displays wide range VCC	
Serial Port Console Redirection>	COM1 Console Redirection Settings>	Console redirection via COMe module's COM1. If redirection is enabled then the port settings such as Terminal type, Bits per second, Data bits, Parity etc. can be adjusted here. Note: On-module COM ports do not support flow control. [**Enabled**, Disabled]	
		The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	
		Terminal Type>	Emulation: ANSI: Extended ASCII character set VT100: ASCII character set VT100+: Extend VT100 to support color, function keys etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes. [VT100, VT100+, VT-UTF8, **ANSI**]
		Bits per Second>	Selects the serial port transmission speed. The sped must be matched on the other side. Long or noisy lines may require lower speeds. [9600, 19200, 38400, 57600, **115200**]
		Data Bits>	Data Bits [7, **8**]
		Parity> Parity> (cont.)	A parity bit can be sent with the data bits to detect 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 the num of 1's in the data bits is odd.

Serial Port Console Redirection> (continued)	COM1 Console Redirection settings> (continued)		Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow error detection. [**None** , Even, Odd, Mark, Space]
		Stop Bits>	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. [**1**, 2]
		Flow Control>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. [**None**, hardware RTS/CTS]
		VT-UTF8 Combo Key Support	Enables VT-UTF8 combination key support for ANSI/VT100 terminals [**Enabled**, Disabled]
		Recorder Mode>	If enabled, only text will be sent. This is to capture terminal data. [Enabled, **Disabled**]
		Resolution 100x31>	Enables or disables extended terminal resolution. [Enabled, **Disabled**]
		Legacy OS Redirection Resolution>	On legacy OS, the number of row and columns supported redirection [**80x24**, 80x25]
		Putty Keypad>	Select function key and key pad on putty. [**VT100**, LINUX, XTERMR6, SCO, ESCN, VT400]
		Redirection After BIOS POST>	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. [**Always Enable**, Bootloader]
	COM2 Console Redirection>	Console redirection via COMe module's COM2. If redirection is enabled then the port settings such as Terminal type, Bits per second, Data bits, Parity etc. can be adjusted here. Note: On-module COM ports do not support flow control. [Enabled, **Disabled**]	
		The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	
		Terminal Type>	Emulation:

Serial Port Console Redirection> (continued)	COM2 Console Redirection settings> (continued)		ANSI: Extended ASCII character set VT100: ASCII character set VT100+: Extend VT100 to support color, function keys etc. VT-UTF8: uses UTF8 encoding to map Unicode chars onto 1 or more bytes. [VT100, VT100+, VT-UTF8, ANSI]
		Bits per Second>	Selects the serial port transmission speed. The sped must be matched on the other side. Long or noisy lines may require lower speeds. [9600, 19200, 38400, 57600, 115200]
		Data Bits>	Data Bits [7, 8]
		Parity>	A parity bit can be sent with the data bits to detect 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 the 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 error detection. [None , Even, Odd, Mark, Space]
		Stop Bits>	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. [1, 2]
		Flow Control>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. [None, hardware RTS/CTS]
		VT-UTF8 Combo Key Sup>	Enables VT-UTF8 combination key support for ANSI/VT100 terminals

Serial Port Console Redirection> (continued)			[Enabled, Disabled]
		Recorder Mode>	If enabled, only text will be sent. This is to capture terminal data. [Enabled, Disabled]
		Resolution 100x31>	Enables or disables extended terminal resolution. [Enabled, Disabled]
		Legacy OS Redirecton Resolution>	On legacy OS, the number of row and columns supported redirection [80x24, 80x25]
		Putty Keypad>	Select function key and key pad on putty. [VT100, LINUX, XTERMR6, SCO, ESCN, VT400]
		Redirection After BIOS POST>	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. [Always Enable, Bootloader]
	Legacy Console Redirection Settings>	Legacy Serial Redirection Port>	Selects a COM port to display redirection of legacy OS and legacy OPROM messages [**COM1**, COM2]
	Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS) - Console Redirection>	Console redirection [Enabled, **Disabled**]	
	Console Redirection Settings>	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.	
		Out-of-Band Mgmt Port>	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. [COM1, COM2]
		Terminal Type>	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. [VT100, VT100+, VT-UTF8, ANSI]
		Bits per second>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

Serial Port Console Redirection> (continued)			[9600, 19200, 57600, 115200]
		Flow Control>	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals. [None, Hardware RTS/CTS, Software Xon/Xoff]
SIO Configuration>	Read only field AMI SIO Driver Version		
	Serial Port 0>	Use This Device>	Enables the user to change the device's resource settings. New setting will be reflected on this setup page after system restart. [**Enabled**, Disabled]
SIO Configuration> (continued)	Serial Port 0> (continued)	Logical Device Settings Current>	Read only field IO=3F8h; IRQ=4

		Logical Device Settings: Possible>	Allows the user to change the device's resource settings. New settings are reflected on the Setup page after system restarts.
			[**Use Automatic Settings**,
			IO=3F8h; IRQ=4,
			IO=3F8h; IRQ=3,4,5,7,9,10,11,12,
			IO=2F8h; IRQ=3,4,5,7,9,10,11,12,
			IO=3E8h; IRQ=3,4,5,7,9,10,11,12,
			IO=2E8h; IRQ=3,4,5,7,9,10,11,12]

	Read Only field WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.		
	Serial Port 1>	Use This Device>	Enables the user to change the device's resource settings. New setting will be reflected on this setup page after system restart. [**Enabled**, Disabled]
		Logical Device Settings Current>	Read only field IO=2F8h; IRQ=3

		Logical Device Settings: Possible>	Allows the user to change the device's resource settings. New settings are reflected on the Setup page after system restarts.
			[**Use Automatic Settings**,
			IO=2F8h; IRQ=3,
			IO=3F8h; IRQ=3,4,5,7,9,10,11,1,
			IO=2F8h; IRQ=3,4,5,7,9,10,11,12,
			IO=3E8h; IRQ=3,4,5,7,9,10,11,12,
			IO=2E8h; IRQ=3,4,5,7,9,10,11,12]

	Read only field		

	WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.		
PCI Subsystem Settings>	Read only field PCI Bus Driver version		
	PCI Latency Timer>	Displays value to be programmed into the PCI latency timer register [**32**, 64, 96, 128, 160, 192, 224, 248]	
	PCI-X Latency Timer>	Displays value to be programmed into the PCI latency timer register [32, **64**, 96, 128, 160, 192, 224, 248]	
	VGA Palette Snoop>	Enables or disables VGA palette register snooping [Enabled, **Disabled]**	
	PERR# Generation>	Enables or disables PCI device to generate PERR# [Enabled, **Disabled**]	
	SERR# Generation>	Enables or disables PCI device to generate SERR# [Enabled, **Disabled**]	
	Above 4G Decoding>	Enables or disables decoding in Address Space above '4G' for 64 bit capable devices. Note: Only if system supports 64 bit PCI decoding. [Enabled, **Disabled**]	
	SR-IOV Support>	Enables or disables single root IO virtualization support If the system has SR-IOV capable PCIe devices. [**Enabled**, Disabled]	
	Don't Reset VC-TC Map>	If the system has virtual channels, software can reset traffic class mapping through virtual channels, to its default state. Enabling this option will not modify VC. [**Enabled**, Disabled]	
	PCI Express Settings>	Relaxed ordering>	Enables or disables PCI express device relaxed ordering [Enabled, **Disabled**]
		Extended Tag>	If enabled the device is allowed to use 8-bit tag field as a requester. [Enabled, **Disabled**]
		No Snoop>	Enables or disables PCI express device No Snoop option. [Enabled, Disabled]
		Maximum Payload>	Sets maximum payload of PCI Express device or allows System BIOS to select the value automatically. [**Auto**, 128 Bytes, 256 Bytes, 512 bytes, 1024 bytes, 2048 Bytes, 4096 Bytes]
		Warning Enabling ASPM may cause some PCI-E devices to fail.	
		Extended Synch>	Allows Extended synchronization patterns. [Enabled, **Disabled**]

PCI Subsystem Settings> (continued)	PCI Express Settings> (continued)	Link Training Retry>	Defines te number of retry attempts taken by Software to retain the link if a previous training attempt was unsuccessful [Disables, 2, 3, **5**]
		Link Training Timeout>	Defines number of mssec the software waits before polling link training bit in Link status register. Range is from (10 µsec. to 10000 µsec). [**1000**]
		Unpopulated Links>	Setting disable link disables unpopulated PCI express links to save power [**Keep Link On**, Disable Link]
		Restore PCIE Register>	On non-PCI Express aware OS'S (pre Windows Vista) some devices may not be correctly initialized after S3. Enabling this restores the PCI express device configurations on S3 [Enabled, **Disabled**]
	PCI Express GEN 2 Settings>	Completion Timeout>	Allows System software to modify the completion timeout value. Default range 50 µs to 50 ms. Available for device function that support Completion timeout programmability. [**Default**, Shorter, Longer, Disabled]
		ARI Forwarding>	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 [Enabled, **Disabled**]
		Atomic Op Requester Enable>	If enabled and the function is supported by the hardware, AtomicOp requests are initiated only if bus master enable bit is set in the command register. [Enabled, **Disabled**]
		AtomicOP Egress Block>	If enabled and the function is supported by the hardware, outbound AtomicOp requests via Egress ports are blocked. [Enabled, **Disabled**]
		IDO request Enable>	If enabled and the function is supported by the hardware, the number of ID-based ordering (IDO) bit (attribute [2]) requests to be initiation is allowed to be set. [Enabled, **Disabled**]
	PCI Express GEN 2 Settings>	IDO Completion Enable>	If enabled and the function is supported by the hardware, the number of ID-based ordering (IDO) bit (attribute [2]) requests to be initiation is allowed to be set.

PCI Subsystem Settings> (continued)	(continued)		[Enabled, **Disabled**]
		LTR mechanism Enable>	If enabled and the function is supported by the hardware, the latency tolerance reporting (LTR) mechanism is enabled. [Enabled, **Disabled**]
		End-End TLP prefix B1>	If enabled and the function is supported by the hardware, the forwarding of TLP containing End-End TLP prefixes is blocked. [Enabled, **Disabled**]
		Target Link Speed>	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. [**Auto**, Force to 2.5 GT/s, Force to 5.0 GT/s]
		Clock Power management>	If enabled and the function is supported by the hardware, the device is permitted to use the CLTREQ' signals for power management of the link clock in accordance to the protocol. [Enabled, **Disabled**]
		Compliance SOS>	If enabled and the function is supported by the hardware, LTSSM is forced to send SKP ordered sets between sequences when sending compliance pattern or modified compliance. [Enabled, **Disabled**]

PCI Subsystem Settings> (continued)	PCI Express GEN 2 Settings> (continued)	Hardware Autonomous Width>	If disabled and the function is supported by the hardware, the ability to change link width (except width size reduction for correction purposes) is disabled. [**Enabled**, Disabled]
		Hardware Autonomous Speed>	If disabled and the function is supported by the hardware, the ability to change link speed (except speed rate reduction for correction purposes) is disabled. [**Enabled**, Disabled]
	PCI Hot-Plug Settings>	BIOS Hot Plug Support>	Enable – allows BIOS built in hot-plug support Note: Use if OS does not support PCIe and SHPC hot-plug natively. [**Enabled**, Disabled]
		PCI Buses Padding>	Padd PCI Buses behind the bridge for hot-plug [Disabled, **1,** 2, 3, 4, 5]
		I/O Resources Padding>	Padd PCI I/O resources behind the bridge for hot-plug [Disabled, **4 k,** 8 k, 16 k, 32 k]
		MMIO 32 bit Resources Padding>	Padd PCI MMIO 32-bit resources behind the bridge for hot-plug. [Disabled, 1 M, 2 M, 4 M, 8 M, **16, M**, 32 M, 64 M, 128 M]
		PFMMIO 32 bit Resources Padding>	Padd PCI MMIO 32-bit prefetchable resources behind the bridge for hot-plug. [Disabled, 1 M, 2 M, 4 M, 8 M, **16, M**, 32 M, 64 M, 128 M]
Network Stack Configuration>	Network Stack>	Enables or disables the UEFI network stack. [Enabled, **Disabled**]	
	Ipv4 PXE Support>	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created. [Enabled, Disabled]	
	Ipv6 PXE Support>	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created. [Enabled, Disabled]	
	PXE boot wait time>	Wait time to press ESC key to abort the PXE boot. Default: 0 [0 .. 5]	
	Media detect count>	Number of times presence of media will be checked. Default: 1 [1 .. 50]	
	CSM Support>	Enables or disables CSM Support	

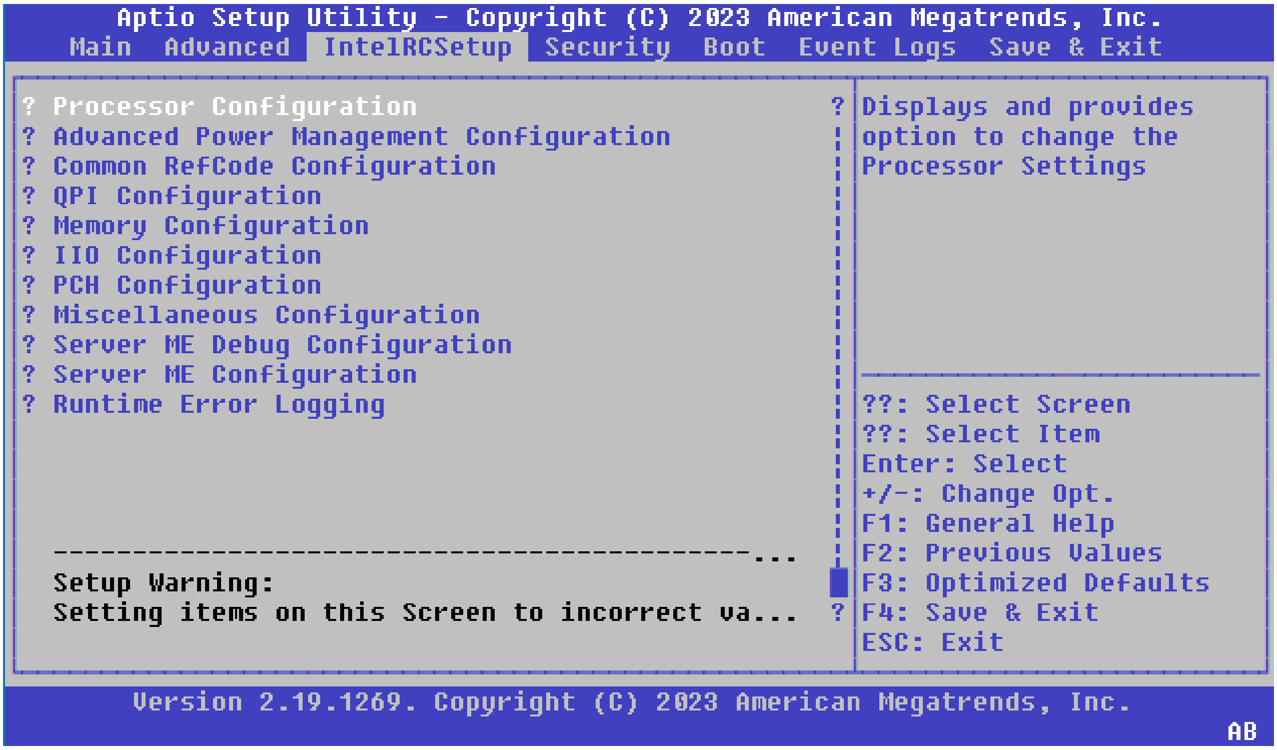
CSM Configuration>		[**Enabled**, Disabled]
	Read Only field CSM module version	
CSM Configuration> (continued)	Gate A20 Active>	To allow for gateA20 to be disabled. UPON REQUEST: GA20 can be disabled using BIOS services ALWAYS: Does not allow disabling GA20 This option is useful when any RT code is executed above 1 MB. [**Upon Request**, Always]
	Option ROM Messages>	Sets display mode for option ROM [**Keep Current**, Force BIOS]
	INT19 Trap response>	BIOS reaction on INT19 traping by Option ROM: IMMEDIATE: executed the trap right away POSTPONED: executed the trap during legacy boot [**Immediate**, Postponed]
	Boot Option Filter>	Controls the legacy/UEFI Roms priority [**UEFI and Legacy**, Legacy only, UEFI only]
	Network>	Controls the execution of UEFI and legacy PXE OpROM [Do not launch, **UEFI**, Legacy]
	On-board Interfaces>	Enables or disables the OpROMs for the on-board network interfaces [**Enable**, Disable]
	Extern Interfaces>	Enables or disables the OpROMs for the extern network interfaces [**Enable**, Disable]
	Storage>	Controls the execution of UEFI and legacy OpROM [Do not launch, **UEFI,** Legacy]
	Video>	Controls the execution of UEFI and legacy video OpROM [Do not launch, UEFI, **Legacy**]
	Other PCI devices>	Determins OpROM execution policy for devices other than network storage or video. [Do not launch, **UEFI**, Legacy]
NVMe Configuration>	Read only field Acts as a message showing NVMe (Non-Volatile memory PCIe) devices connected to the system. [**NO NVME Device Found**]	
USB Configuration>	Read only fields USB Configuration, UBS Module Version, USB Controllers, and USB devices	
	Legacy USB Support>	Enables legacy USB support. Enable- Supports legacy USB Auto– disables legacy support, if no USB devices are connected Disable-keeps USB devices available only for EFI applications [**Enabled**, Disabled, Auto]
	XHCI Hand-off>	XHCI ownership change should be claimed by XHCI driver. Note: this is a work around for OS(s) without XHCI hand-off support. [**Enabled**, Disabled]
	USB Mass Storage Driver Support>	Enables or disables USB mass storage driver support [**Enabled**, Disabled]

USB Configuration> (continued)	Port 60/64 Emulation>	Enables I/O port 60h/64h emulation support Note: Enable for USB keyboard legacy support for non-USB aware OS(s). [Enabled, **Disabled**]
	USB Transfer Time-out>	Displays timeout value for control, bulk and interrupt transfers [1 sec, 5 sec, 10 sec, **20 sec**]
	Device Reset Time-out>	Displays USB mass storage device start unit command time-out [10 sec, **20 sec**, 30 sec, 40 sec]
	Device Power-up Delay>	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor. [**Auto**, Manual]
	Device power-up delay in seconds>	Delay range is 1..40 seconds, in one second increments. Default: 5 seconds

12.4.1. InterlRCSetup

The IntelRCsetupSetup menu provides sub-screens and second level sub-screens for processor related functions.

Figure 21: IntelRCSetup Menu



```
        Aptio Setup Utility – Copyright (C) 2023 American Megatrends, Inc.
     Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

 ? Processor Configuration                           ? Displays and provides
 ? Advanced Power Management Configuration           ¦ option to change the
 ? Common RefCode Configuration                      ¦ Processor Settings
 ? QPI Configuration                                 ¦
 ? Memory Configuration                              ¦
 ? IIO Configuration                                 ¦
 ? PCH Configuration                                 ¦
 ? Miscellaneous Configuration                       ¦
 ? Server ME Debug Configuration                     ¦
 ? Server ME Configuration                           ¦
 ? Runtime Error Logging                             ¦ ??: Select Screen
                                                     ¦ ??: Select Item
                                                     ¦ Enter: Select
                                                     ¦ +/-: Change Opt.
                                                     ¦ F1: General Help
   --------------------------------------------...  ¦ F2: Previous Values
   Setup Warning:                                    ¦ F3: Optimized Defaults
   Setting items on this Screen to incorrect va...  ? F4: Save & Exit
                                                       ESC: Exit

        Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                        AB
```

The following table provides an over view of the Advanced menu sub-screens and functions listed below and describes the content. Default settings are in **bold**. Some function contain additional information.

Table 36: InterlRCSetup Sub-screens and Functions

Function	Second level Sub-Screen / Description	
Processor Configuration>	Read only field Processor socket, Processor ID, processor Frequency; processor max. ratio, processor min. ratio, Microcode revision, L1 Cache RAM, L2 Cache RAM, L3 Cache RAM, processor 0 Version	
	Hyper-Threaading [ALL]>	Enables or disables Hyper threading, the software method of enabling or disabling processor threads. [**Enable**, Disable]
	Monitor/ MWait>	Enables or disables MonitorMWait [**Enable**, Disable]
	Execute Disable Bit>	If disabled, the XD flag always returns 0 [**Enable**, Disable]
	Enable Intel TXT Supp>	Enables or disable the Intel® Trust Execution technology configuration. If TXT is enabled, the Ev DFX feature must be disabled. [Enable, **Disable**]
Processor Configuration> (continued)	VMX>	Enables or disables vanderpool Technology. This takes effect after reboot. [**Enable**, Disable]
	Enable SMX>	Enables or disables Safer Mode Extensions,

Function	Second level Sub-Screen / Description	
Processor Configuration> (continued)		[Enable, **Disable**]
	Lock Chipset>	Lock and unlock chipset [**Enable**, Disable]
	MSR Lock Control>	If enabled –MSR 3Ah, MSR OE2h and CSR 80h are locked. A Power Good rset is reqired to remove the lock bits. [**Enable**, Disable]
	PPIN Control>	Unlocks and enables or disables the PPIN control [**Unlock/Enable**, Unlock/Disable]
	DEBUG INTERFACE>	Setting MSR 0C80h bit [0] enables the debug feature [Enable, **Disable**]
	Hardware Prefetcher>	MLC Streamer prefetcher (MSR 1A4h Bit [0]) [**Enabled**, Disabled]
	Adjacent cache prefer>	MLC Spatial prefetcher (MSR 1A4h Bit [1]) [**Enable**, Disable]
	DCU Streamer Prefetch>	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2] [**Enable**, Disable]
	DCU IP Prefetch>	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3] [**Enable**, Disable]
	DCU Mode>	MSR 31h Bit[0]- A write of 1 selects [**32KB 8 Way without ECC**, 16KB 4Way with ECC]
	Direct Cache Access>	Enables or disables direct cache access [**Auto**, Enable, Disable]
	DCA Prefertch Delay>	DCA prefetch delay [Disable, 8, 16, 24, **32**, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112]
	X2APIC>	Enables or disables extended APIC support [Enable, **Disable**]
	AES-NI>	Enables or disables the AES-NI support [**Enable**, Disable]
	Down Stream PECI>	Enables or disables PCIe down stream PECI write [Enable, **Disable**]
	IIO LLC WAYS [19:0]>	Displays MSR CBO_SLICE0_CR_IIO_LLC_WAYS bitmask
	QLRU Config [63:32]>	Displays VIRTUAL_MSR_CR_QLRU_CONFIG bitmask
	QLRU Config [31:0]>	Displays VIRTUAL_MSR_CR_QLRU_CONFIG bitmask
	SMM Save State>	Enables or disables the SM Save State feature [Enable, **Disable**]
	Target Smi>	Enables or disables the Target Smi feature [Enable, **Disable**]

Function	Second level Sub-Screen / Description		
Advanced Power Management Configuration>	Displays and provides options to change the power management settings		
	LOT26 Enable>	For HEDT only! Selects whether VR power is turned off to empty DIMM channels. [**Enable**, Disable]	
	UFS>	Setting in PCU_MISC_CONFIG Bit[28] [**Enable**, Disable]	
	CPU PM Tuning>	If selected as AUTO, all bits in MSR 1FCh keep the PO value. [**Auto**, Manual]	
	EIST (P-states)>	If enabled, OS sets CPU frequency according to load and if disabled, CPU frequency is set at max. non-turbo [**Enable**, Disable]	
	Config. TDP>	Enables or disables Config TDP [Enable, **Disable**]	
	IOTG Setting>	Enables or disables IOTG setting via sticky scratch pad register [Enable, **Disable**]	
	Uncore CLR Freq OVRD<	Overrides Uncore max CLR Freq ratio programming to MSR 0x620 bits[6:0] [**Auto,** Manual]	
	CPU P State Control>	P State Domain>	Per Logical: indicates the P-state domain for each logical processor in the system. Per Package: all processors indicate the same domain in the same package. [**All**, One]
		P-State Coordination>	HW_ALL (hardware) coordination is recommended over SW_ALL and SW_ANY (software coordination). [**HW_ALL**, SW_ALL, SW_ANY]
		Single_PCTL>	MSR_CR_MISC_PWR_MGMT 0x1AA Bit[0]: SINGLE_PCTL_EN [**No**, Yes]
		SPD>	PCU_MISC_CONFIG Bit[30]: SPD [Enable**, Disable**]
		PL2_Safety_ Net_Enable>	PCU_MISC_CONFIG Bit[1]: PL2_SAFETY_NET_ENABLE [**Enable**, Disable]
		Energy Efficient P-State>	Enables or disable Energy efficient P-state feature. [**Enable**, Disable]
		Boot Performance Mode>	Selects the performance state that the BIOS sets before OS handoff. [**Max. Performance**, Max. Efficiency]
Advanced Power Management Configuration>	CPU P State Control> (continued)	Turbo Mode>	Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceeding CPU defined limits. [**Enable**, Disable]

Function	Second level Sub-Screen / Description			
(continued)		XE Ratio Limit>	Overclocking Lock>	Enables or disables overclocking [**Enabled**, Disabled]
	CPU HWPM State Control>	Enable CPU HWPM>	Enables CPU HWPM for CPU for better Energy performance [**Disable**, HWPM NATIVE MODE, HWPM OOB MODE]	
		Enable CPU Autonomous>	Enables CPU Autonomous Cstate in which CPU converts HALT instruction to MWAIT [Enable**, Disable**]	
	CPU C State Control>	C2C3TT>	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].	
		CPU C State>	Enables the Enhanced Cx state of the CPU that takes effect after reboot [**Enable**, Disable]	
		Package C State Limit>	Package C State limit [C0/C1 state, C2 state, C6(non-Retention) state, **C6(Retention) state**, No Limit]	
		CPU C3 Report>	Enables or disables CPU C3(ACPI C2) report to OS. Recommended to be disabled [Enable**, Disable**]	
		CPU C6 Report>	Enable or disable CPU C6(ACPI C2) report to OS. Recommended to be enabled [**Enable**, Disable]	
		Enhanced Halt State (C1E)>	Enables the Enhanced C1E state of the CPU that takes effect after reboot [**Enable**, Disable]	
		OS ACPI Cx>	Report CC3/CC6 to OS ACPI C2 or ACPI C3 [**ACPI C2**, ACPI C3]	
	CPU T State Control>	ACPI T-States>	Enables or disable CPU throttling by OS. Throttling reduces power consumption. [Enable**, Disable**]	
	CPU Thermal Management>	Bi-directional PROCHOT#>	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. [Output-only, Disable, Bidirectional (normal input response), **Input-only**]	
	CPU Thermal Management> (continued)	Thermal Monitor>	Enable/Disable Thermal Monitor [**Enable**, Disable]	
		PROCHOT RESPONSE> PROCHOT RESPONSE> (continued)	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). [**Pn clamping**, Pm clamping]	

Function	Second level Sub-Screen / Description			
Advanced Power Management Configuration> (continued)		Use PCH_HOT>	Pcode is allowed to use PCH_HOT pin information for thermal management. [**Enable**, Disable]	
		Use PCH Temp From ME>	Pcode is allowed to use PCH Temperature provided by ME. [**Enable**, Disable]	
		CPU to PCH Throttle>	Enable Pcode to throttle PCH [**Enable**, Disable]	
	CPU Advanced PM Turning>	Energy perf Bias>	Energy Performance Tuning>	Selects whether BIOS or OS chooses energy performance bias tuning. [**Enable**, Disable]
			Energy Performance Bias Setting>	Read only field [**Balance Performance**]
			Power / Performance Switch>	MSR 1FCh Bit[24] = PWR_PERF_TUNING_ENABLE_DYN_ SWITCHING [**Enable**, Disable]
			Workload Configuration>	Optimization for the workload characterization. Balanced is recommended. [**UMA**, NUMA]
			Averaging Time Window>	Displays the value used to control the effective window of the average for C0 and P0 time. [**23**]
			P0 Total_Time_ Threshold Low>	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than the threshold displayed. [**35**]
			P0 Total_Time_ Threshold High>	The HW switching mechanism ENABLES the performance setting (0) when the total P0 time is greater than the threshold displayed. [**58**]
		Program PowerCTL_ MSR>	PKG C-state Lat. Neg.>	MSR 1FCh Bit[30] = PCH_NEG_DISABLE [**Enable**, Disable]
		Program PowerCTL_ MSR> (continued)	LTR Software Input>	MSR 1FCh Bit[28] = LTR_SW_DISABLE. Disable = Ignore SW LTR input. [Take SW LT input.**Ignore SW LTR input**]
	CPU Advanced PM Turning> (continued)		SAPM Control>	MSR 1FCh Bit[22] = PWR_PERF_TUNING_DISABLE_SAPM _CTRL [**Enable**, Disable]
			PHOLD_SR>	MSR 1FCh Bit[17] = PHOLD_SR_Disable [**Enable**, Disable]

Function	Second level Sub-Screen / Description				
Advanced Power Management Configuration> (continued)			PHOLD_CST_PREVENTION_INIT>	MSR 1FCh Bit[16] = PHOLD_CST_PREVENTION_INIT [**Enable**, Disable]	
			FAST_Brk_Int_En>	MSR 1FCh Bit[4] = FAST_Brk_Int_En. Disable = Use 'fast' VID swing rate. [Enable, **Disable**]	
			FAST_Brk_Snp_En>	MSR 1FCh Bit[3] = FAST_Brk_Snp_En. Disable = Use 'fast' VID swing rate. [Enable, **Disable**]	
			Energy Efficient Turbo>	Energy Efficient Turbo Disable, MSR 0x1FC [19] [**Enable**, Disable]	
		Program PRO_CURT_CFG_CTRL_ MSR>	PPO Current_Cfg_Ctl Ovrd>	Allows manual overrides for Primary_Plane_Current_Config_Control [Auto, **Manual**]	
			Current Config>	0 – Deafult, do nothing; 1 – Manual, override Current limitation in 1/8 A increments. [Enable, **Disable**]	
			PCI Config.>	PSI3 threshold value [**1**]	
				PSI3 threshold value [**5**]	
				PSI3 threshold value [**20**]	
				Lock Indication>	This bit Locks the CURRENT_LIMIT settings in this register and also locks this setting. [Enable, **Disable**]
		Program CSR_Entry_Criteria>	PKG_CST_Entry_Criteria O>	Allows manual overrides for PKG_CST_ENTRY_CRITERIA_MASK [**Auto**, Manual]	
			Read only field CPU0 Advanced PM Turning CPU1 Advanced PM Turning CPU2 Advanced PM Turning CPU3 Advanced PM Turning		
	CPU Advanced PM Turning> (continued)	PROGRAM CSR_SWLTROVRD>	Snoop Latency Valid>	When this bit is set to 0b, PCODE ignores the Snoop Latency override value [Enable, **Disable**]	
			Snoop Latency Override>	Forces PCODe to always use values provided in SW_LTR_OVRD	

Function	Second level Sub-Screen / Description			
Advanced Power Management Configuration> (continued)				[Enable, **Disable**]
			Snoop Latency Multiplier>	Value is multipled by to yield a time value
			Snoop Latency Value>	Latency requirement for Snoop requests
			Non-Snoop Latency Value>	When this bit is set to 0b, PCODE ignores the Non-Snoop Latency override value [Enable, **Disable**]
			Non-Snoop Latency Override>	Forces PCODe to always use values provided in SW_LTR_OVRD [Enable, **Disable**]
			NonSnoop LatencyMultiplier>	Value is multipled by to yield a time value
			Non-Snoop Latency Value>	Latency requirement for Non-Snoop requests
	DRAM RAPL Configuration>	DRAM RAPL Baseline>	DRAM RAPL Baseline enabled and baseline mode [Disable, DRAM RAPL Mode 0, **DRAM RAPL Mode 1]**	
		Override BW_LIMIT_ TF>	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled [1]	
		DRAM RAPL Extended Range>	Select DRAM RAPL Extended Range [**Enable**, Disable]	
	Socket RAPL Config.>	Fast_RAPL_NSTRIKE_PL2>	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value. (Range between 25 (10%) – 64 (25%)) [**64**]	
		Turbo Pwr Limit Lock>	Enables or disables locking of turbo settings. If enabled, TURBO_POWER_LIMIT MSR is locked and a reset is required to unlock the register. [Enable, **Disable**]	
		Long Pwr Limit Ovrd>	Enables or disable Long Term Power Limit override. If this option is disabled, BIOS programs the default values for Long Term Power Limit and Long Term Power Limit Time Window. [**Enable**, Disable]	
		Long Dur Pwr Limit>	Displays the Turbo Mode Long Duration Power Limit (aka Power Limit 1) in Watts. (Range 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. [**0**]	
		Long Dur Time Window>	Displays Long Duration Time Window (also known as Power Limit 1 Time) value in seconds. (Range 0 to 56). Indicates the time window over which TDP value	

Function	Second level Sub-Screen / Description		
Advanced Power Management Configuration> (continued)			should be maintained. If the value is 0, the fused value will be programmed. [**1**]
		Pkg Clmp Lim1>	Pkg Clamping limit 1 allows going below P1. 0: PBBM limited between P1 and P0 1: PBM can go below P1 [Between P1/P0, **Below P1]**
		Short Dur Pwr Limit Enable>	Enables or disables Short Duration Power Limit (also known as Power Limit 2) [**Enabled**, Disabled]
		Short Dur Pwr Limit>	Displays the Short Duration Power Limit value (also known as Power Limit 2) in Watts. (Range 0 to 32767). If the value is 0, BIOS programs this value as 125%TDP. Processor applies control policies to ensure that the package power does not exceed this limit.[**0**]
		Pkg Clmp Lim2>	Pkg Clamping limit 2, Allow going below P1. 0: PBBM limited between P1 and P0, 1: PBM can go below P1 [Bewtee P1/P0**, Below P1]**
Common RefCode Configuration>	MMCFG Base>	Selects MMCFG Base [**2G**, 1G, 3G]	
	MMIOBase>	Sets the MMIOH Base [63:32]; must be between 4032 – 4078 [**56T**, 48T, 24T, 16T, 12T, 4T, 2T, 1T]	
Common RefCode Configuration> (continued)	MMIO High Size>	Selects MMIOH High Size [**256G**, 128G, 512G, 1024G]	
	Isoc Mode>	Disables or enables Isoc [**Disable**]	
	MeSeg Mode>	Selects the MeSeg mode [Enable, **Disable**, Auto]	
	Numa>	Enables or disables Non Uniform Memory Access (NUMA). [**Enable**, Disable]	
QPI Configuration>	QPI General Configuration>	QPI Status	
		Degrade 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. [**Topology Precedence** Feature Precedence]
		Link Speed Mode>	Select the QPI link speed as either the POR speed (Fast) or default speed (Slow) [Slow, **Fast]**
		Link Frequency Select>	Allows for selecting the QPI Link Frequency [6.4GB/s, 8.0GB/s, 9.6GB/s**, Auto**, Auto Limited]

Function	Second level Sub-Screen / Description			
QPI Configuration> (continued)	QPI General Configuration> (continued)	Link L0p Enable>	Link L0p Enable [Disable, **Enable]**	
		Link L1 Enable>	Link L1 Enable [Disable, **Enable]**	
		Legacy VGA Socket>	Displays the VGA range for Socket that claims the legacy VGA range. Valid values are 0-7; 0 is default. [**0**]	
		MMIO P2P Disable>	Disables MMIOL P2P traffic across sockets. Default is NO, to not disable. [**No**, Yes]	
		E2E Parity Enable>	Enable/Disable E2E Parity [**Disable**, Enable].	
		COD Enable>	Enable/disable Cluster on Die. [Disable, Enable, **Auto**]	
		Early Snoop>	[Disable, Enable, **Auto**]	
		Home Dir Snoop with IVT-Style OSB>	Enables or disables Home Dir Snoop with IVT- Style OSB [Disable, Enable, **Auto**]	
		QPI Debug Print Level>	QPI Debug Print Level Enable-Disable. [Fatal, Warning, Summary, Detail, **All]**	
	QPI Per Socket Configuration>	CPU 0> or CPU>1 or CPU 2> or CPU3>	Bus Resources Allocation Ration>	Bus resources allocation ratio, Range 0 to 8 [1]
			IO Resources Allocation Ration>	IO resources allocation ratio, range 0 to 8 [1]
			MMIOL:Resources Allocation Ratio>	MMIOL resources allocation ratio, range 0 to 8 [1]
			IIO Disable>	Disable Ports and Clock Gate IIO [**no** Disable Ports and IIO without memory hotplug Disable Ports Only with memory hotplug]
Memory Configuration>	Enforce POR>	Enable to enforce POR restrictions for DDR4 frequency and voltage programming [**Auto**, Enforce POR, Disabled, Enforce Stretch Goals]		
	PPR type>	Selects the PPR type [Hard PPR, Soft PPR, **PPR Disabled**]		

Function	Second level Sub-Screen / Description	
Memory Configuration> (continued)	PPR Error Injection Test>	Enables or disables support for c-script error injection test [**Disabled**, Enabled]
	Memory Frequency>	Maximum memory frequency selections in MHz. Note: Do not select Reserved [**Auto**, 1333 …3200, Reserved]
	MRC Promote Warnings>	Determines if MRC warnings are promoted to system level [**Enabled**, Disabled]
	Promote Warnings>	Determines if warnings are promoted to system level [**Enable**, Disable]
	Halt on Mem Training Error>	Enables or disables halt on memory training error [**Enabled**, Disabled]
	Multi-Threaded MRC>	Enable to execute the Memory Reference Code multi-threaded [**Auto**, Disabled, Enabled]
	ECC Support>	Enables or disables DDR ECC Support [**Auto**, Disable, Enable]
	Enforce Timeout>	Enables or disables forcing cold reset after 3 months [**Auto**, Disable, Enable]
	Enhanced Log Parsing>	Enables additional output in debug log for easier machine parsing [**Disabled**, Enabled]
	Backside RMT>	Enables Backside RMT [**Auto**, Disable, Enable]
	Rank Multiplication>	Force the Rank Multiplication factor for LRDIMM [**Auto**, Enabled]
	LRDIMM Module Delay>	Selects the LRDIMM Module Delay Disabled-MRC will not use SPD bytes 90-95 for LRDIMM Module Delay. Auto- MRC will boundary check the values and use default values, if SPD is 0 or out of range [**Auto**, Disabled]
	MemTest>	Enables or disables memory test during normal boot [**Auto**, Disable, Enable]
	MemTestLoops>	Number of memory test loops during normal boot, set to 0 to run memtest infinitely [**1**]
	DRAM Maintenance Test>	DRAM maintenance test during normal boot [**Auto**, Disabled, Enabled]
	Memory Type>	Selects the memory type supported by this platform [RDIMMs only UDIMMs only **UDIMMs and RDIMMs**]

Function	Second level Sub-Screen / Description	
Memory Configuration> (continued)	CECC WA CH Mask>	Displays the CH bitmask to apply CECC WA. 1 bit per CH. Value 2 applies WA on CH1, 3 on CH0 and 1 [**10**]
	Rank Margin Tool>	Enables the rank margin tool to run after DDR4 memory training [**Auto**, Disabled, Enabled]
	RMT Pattern Length>	Sets the pattern length for the Rank Margin Tool [**32767**]
	CMD Pattern Length>	Sets the pattern length for the Rank Margin Tool [**32767**]
	Per Bit Margin>	Enables the logging from the serial port of DDR Per Bit Margin Data [**Auto**, Disable, Enable]
	Training Result Offset Config>	Option to offset the final memory training results [**Auto**, Disabled, Enabled]
	Attempt Fast Boot>	If enabled, portions of memory reference code will be skipped when possible to increase boot speed. [**Auto**, Disabled, Enabled]
	Attempt Fast Cold Boot>	IF enabled, portions of memory reference code will be skipped when possible to increase boot speed [**Auto**, Disable, Enable]
	MemTest On Fast Boot>	Enables or disables memory test during fast boot [**Auto**, Disabled, Enabled]
	RMT on Cold Fast Boot>	Enables or disable Rank Margin Tool on Cold Fast Boot [**Auto**, Disabled, Enabled]
	BDAT>	Enables or disables BDAT [**Disabled**, Enabled]
	Data Scrambling>	Enables data scrambling [**Auto**, Disabled, Enabled]
	Allow SBE During Training>	Allow SBE during training knob enable/disable [**Auto**, Disabled, Enabled]
	Platform Type Input for SPD page selection>	Controls the SPD page selection feature. Default is disabled. [**Auto**, Disabled, Enabled]
	CECC WA Control>	Controls the CECC WA. Disabled by default on L0 and later processors. [**Auto**, Disabled, Enabled]
	CAP ERR LOW feature>	Controls the CAP ERR FLOW feature. Disabled by Default. [**Auto**, Disabled, Enabled]
	Scrambling Seed Low>	Displays low 32-bits of the scrambling seed [**41003**]

Function	Second level Sub-Screen / Description			
Memory Configuration> (continued)	Scrambling Seed High>	Displays high 32-bits of the scrambling seed [**54165**]		
	Enable ADR>	Enables the detecting and enabling of ADR [**Disabled,** Hardware Triggered ADR, Software Triggered ADR]		
	MC BGF Threshold>	The HA to MC BGF threshold is used for scheduling MC request in bypass condition.[**0**]		
	DLL Reset Test>	Sets 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 execute RMT for the same number of loops with DLL resets. [**0**]		
	MC ODT Mode>	Select MC ODT Mode [**Auto**, 100 Ohms, 50 Ohms]		
	Opp Read During WMM>	Enables or disables issuing read commands opportunistically during WMM [**Auto**, Disabled, Enabled]		
	Normal Operation Duration>	Sets normal operation duration interval (Range : 0 – 65535) **[1024]**		
	Number of Sparing Transaction>	Sets number of sparing transactions interval (range: 0 – 65535) [**4**]		
	PSMI Support>	Enables or disables PSMI Support [Enabled, **Disabled**]		
	C/A Parity Enable>	Enables or disables DDR4 Command Address Parity [**Auto**, Disabled, Enabled]		
	SMB Clock Frequency>	Sets DDR4 SMB Clock Frequencys For SPD ACCESS [**400 kHz**, 1 MHz]		
	Memory Topology>	Read only field Contains information about the content of the memory sockets. Socket 0.Ch1.DIMM0: 2133 MT/S unknown SRx8 8GB SODIMM		
	Memory Thermal>	Set Throttling Mode>	Configure Thermal Throttling Mode. Select OLTT or CLTT mode. [Disabled, OLTT, **CLTT]**	
		Phase Shedding>	DDR4 VR Static Phase Shedding Support. PS0: full-phase, PS1: single-phase, typically <18A load, PS2: fixed loss, typically <5A load [Enabled, Disabled, **Auto**]	
		Memory Power Savings Mode>	Configures CKE and related Memory Power Savings Features [**Auto**, Disabled, Slow, Fast, APD on, User Defined]	
		Memory Power Saving Advanced Options>	CK in SR>	Configures CK behavior during self-refresh [**Auto**, Driven, Tri-state, Pull low, Pulled high]

Function	Second level Sub-Screen / Description		
Memory Configuration> (continued)		MDLL Off>	Enable to shut down MDLL during SR [Enabled, Disabled, **Auto**]
		MEMHOT Throttling Mode>	Configure MEMHOT Input and Output Mode: Mem Hot Sense Therm Throt or Mem Hot Output Therm Throt. [Disabled, Output-only, **Input-only]**
		Mem Electrical Throttling>	Configure memory electrical throttling [Enabled, **Disabled**, Auto]
	Memory Timings & Voltage Override>	DIMM Profile>	Selects the XMP profile to use [**Disabled**, Manual]
		Memory Frequency>	Maximum memory frequency selections in MHz. Do not select Reserved [**Auto**, 800, ….. 3000]
	Memory Map>	Socket Interleave Below 4GB>	Splits the 0-4GB address space between two sockets, so that both sockets get a chunk of local memory below 4GB [Enable, **Disable**]
		Channel Interleaving>	Selects Channel Interleaving setting [**Auto,** 1-way Interleave, 2-way Interleave, 3-way Interleave, 4-way Interleave]
		Rank Interleaving>	Selects Rank Interleaving setting [**Auto,** 1-way Interleave, 2-way Interleave, 3-way Interleave, 4-way Interleave]
		IOT Memory Buffer Reservation>	Enables or disable Select IOT Memory Buffer Reservation [**0**]
		A7 Mode>	Enables or disables A7 Mode [**Enable**, Disable]
	Memory RAS Configuration>	Correctable Error Threshold>	Displays the Correctable Error Threshold (1 – 32767) used for sparing, tagging, and leaky bucket [**32767**]
		Leaky Bucket Low Bit>	Displays the Leaky bucket low bit" (1 – 63) [**40**]
		Leaky Bucket High Bit>	Displays the Leaky bucket high bit" (1 – 63) [**41**]
		DRAM Maintenance>	Selects the DRAM Maintenance settings Manual customizes DRAM Maintenance settings [**Auto**, Manual, Disabled]
		Patrol Scrub>	Enabled or disable Patrol Scrub [**Enable**, Disable]
		Patrol Scrub Interval>	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto! [**24**]

Function	Second level Sub-Screen / Description			
		Demand Scrub>	Enables or disable Demand Scrub [**Enable**, Disable]	
		Device Tagging>	Enables or disable Device Tagging [Enable, **Disable**]	
		Memory Power Management>	Enable memory power management for this platform [Enable, **Disable**]	
	DIMM Rank Enable Mask>	Selects rank to enable or disable per DIMM [Enabled, **Disabled**]		
IIO Configuration>	IIO PCIe Link on phase>	Link training can be done either before memory chipset init or post chipset init [Before memory chipset init**, Post chipset init]**		
	PCIe Train by BIOS>	Assume IIO is strapped for Wait-for-BIOS because straps are unreliable in A-O Silicon [no, **yes]**		
	PCIe Hot Plug>	Enables or disables PCIe Hot Plug globally [**Disable**, Enable, Auto, MANUAL]		
	PCIe ACPI Hot Plug>	Enables or disables PCIe ACPI Hot Plug globally, or allow per-port control. Disabled – generates MSI on HP event Enabled – generates HPGPE message [**Disable**, Enable, Per-Port]		
	EV DFX Features>	Set this option to allow DFX Lock Bits to remain clear [Enable, **Disable**]		
	IIO0 Configuration>	IOU2 (IIO PCIe Port 1)>	Selects PCIe port Bifurcation for selected slots(s) [x4x4, x8, Auto]	
		IOU1 (IIO PCIe Port 3)>	Selects PCIe port Bifurcation for selected slots(s) [x4x4x4x4, x4x4x8 x8x4x4 x8x8 **x16** Auto]	
		No PCIe port active ECOPCIe ACPI Hot Plug>	Workaround settings when no PCIe port active [PCU Squelsh exit ignore option, Reset the SQ FLOP by CSR option9	
		Sockets 0 PCIeD00F0-Port 0 /DMI>	Link Speed>	**[Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s)]
			Override Max Link Width>	Override the max link width that was set by bifurcation [**Auto** , x1, x2, x4, x8, x16]

Function	Second level Sub-Screen / Description			
IIO Configuration> (continued)	IIO0 Configuration> (continued)	Sockets 0 PCIeD00F0-Port 0 /DMI> (continued)	PCI-E Port DeEmphasis >	De-Emphasis control (LNKCON2[6]) for this PCIe port. [**-6.0 dB**, -3.5 dB]
			PCI-E Port Link Status>	Read only field Linked as x4
			PCI-E Port Link Max.>	Read only field Max width x4
			PCI-E Port Link Speed>	Read only field Gen 2 (5.0 GT/s)
			PCI-E Port L0s Exit Latency>	The length of time this port requires to complete transition from L0s to L0 [**4uS – 8uS**]
			PCI-E Port L1 Exit Latency>	The length of time this port requires to complete transition from L1 to L0 [1uS, 1uS-2Us, 2uS-4uS, 4uS-8uS, **8uS – 16uS**, 16uS-32us, 32uS-64uS, >64uS]
			Fatal Err Over>	Enables forcing fatal error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			Non-Fatal Err Over>	Enable forcing non-fatal error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			Corr Err Over>	Enables forcing correctable error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			L0s Support>	When disabled, IIO never puts its transmitter in L0s state [**Disabled**]
		Sockets 0 PCIeD0XFX-Port X>	PCI-E Port>	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. [**Auto**, Enabled, Disabled]
			Hot Plug Capable>	This option specifies if the link is considered Hot Plug capable. [Enabled, **Disabled**]
			PCI-E Port Link>	This option disables the link so that the no training occurs but the CFG space is still active. [**Enabled,** Disabled]

Function	Second level Sub-Screen / Description			
IIO Configuration> (continued)	IIO0 Configuration> (continued)	Sockets 0 PCIeD0**X**F**X**-Port **X**> (continued)	Link Speed>	Selects the link speed [**Auto,** Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s)]
			Override Max Link Width>	Overrides the max link width that was set by bifurcation [**auto** , x1, x2, x4, x8, x16]
			PCI-E Port DeEmphasis >	De-Emphasis control (LNKCON2[6]) for this PCIe port. [**-6.0 dB**, -3.5 dB]
			PCI-E Port Link Status>	Read only field Link did not train
			PCI-E Port Link max>	Read only field Max width x8
			PCI-E Port Link Speed>	Read only field Link did not train
			PCI-E Port L0s Exit Latency>	The length of time this port requires to complete transition from L0s to L0 [**4uS – 8uS**]
			PCI-E Port L1 Exit Latency>	The length of time this port requires to complete transition from L1 to L0 [1uS, 1uS-2Us, 2uS-4uS, 4uS-8uS, **8uS – 16uS**, 16uS-32us, 32uS-64uS, >64uS]
			Fatal Err Over>	Enables forcing fatal error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			Non-Fatal Err Over>	Enable forcing non-fatal error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			Corr Err Over>	Enables forcing correctable error propogation to the IIO core error logic for this port [Enabled, **Disabled**]
			L0s Support>	When disabled, IIO never puts its transmitter in L0s state [**Disabled**]
			PM ACPI Mode>	When disabled, MSI is generated on PM event. Ehen enabled, _HPGPE message is generated. [Enabled, **Disabled**]
			Gen3 Eq Mode>	Selects the PCIe Gen3 adaptive equilization mode [Auto, enable pahse 0,1,2,3

Function	Second level Sub-Screen / Description			
IIO Configuration> (continued)	IIO0 Configuration> (continued)	Sockets 0 PCIeD0**X**F**X**-Port **X**> (continued)		Disable phase 0,1,2,3 Enable phase 1 only Enable phase 0,1 only Advanced Enable MMM offset West Alt short channel
			Gen3 Spec Mode>	Selects the PCIe Gen3 Spec Mode [**Auto,** 0.70 July, 0.70 Sept, 0.71 Sept]
			Gen3 Phase2 Mode>	Selects the PCI Gen 3 phase 2 mode [**Hardware Adaptive** Manual]
			Gen3 DN Tx Preset>	Selects the PCIe Gen3 downstream Tx preset [Auto, PO (-6.0/0.0 db) ... P9 (0.0/ 3.5 db)]
			Gen3 DN Rx Preset>	Selects the PCIe Gen3 downstream Rx preset hint [Auto, P0 (-6.0 dB), P6 (-12.0 dB)]
			Gen3 UP Tx Preset>	Selects the PCIe Gen3 Upstream Tx Preset [Auto, PO (-6.0/0.0 db) ... P9 (0.0/ 3.5 db)]
			Hide Port?>	Forces hide for this root port from OS [**No**, Yes]
			Pcie Ecrc>	Enables or disables PCIE Ercr Support for this port. [Enabled, Disabled, **Auto**]
		IOU0 Non-Posted Prefetch>	Enables or disables IOU0 Non-Posted Prefetch [Enable, **Disable**]	
		IOU1 Non-Posted Prefetch>	Enables or disables IOU1 Non-Posted Prefetch [Enable, **Disable**]	
		IOU2 Non-Posted Prefetch>	Enables or disables IOU2 Non-Posted Prefetch [Enable, **Disable**]	
	IOAT Configuration>	Enable IOAT>	Enables or disables IOAT devices [Enable, **Disable**]	
		No Snoop>	Enables or disables No Snoop for each CB device [Enable, **Disable**]	
	IOAT Configuration> (continued)	Disable TPH>	TLP processing Hint disable [**Enable**, Disable]	

Function	Second level Sub-Screen / Description		
IIO Configuration> (continued)	IIO General Configuration>	TXT DPR memory Setting>	Allows selection of the TXT DPR size in system [1M DPR, **3M DPR**, 64M DPR, 128M DPR, 255M DPR]
		IIO 0>	Read only field
		IIO IOAPIC>	Enables or disables the IIO IOAPIC [**Enable,** Disable]
	Intel VT for Directed I/O (VT-d)>	VTd Azalea VCp Optimizations>	Enables or disables Azalea VCp Optimizations [Enable, **Disable**]
		Intel VT for Directed I/O (VT-d)>	Enables or disables Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables. [**Enable**, Disable]
		ACS Control>	Controls Programming or ACS to PCIE Enable: Programs ACS only to Chipset PCIE Root Ports Bridges; Disable: Programs ACS to all PCIE bridges
		Interrupt Remapping>	Enables or disables VT_D Interrupt Remapping Support [**Enable**, Disable]
		Coherency Support (Non-Isoch)>	Enables or disables Non-Isoch VT_D Engine Coherency support [**Enable**, Disable]
		Coherency Support (Isoch)>	Enables or disables Isoch VT_D Engine Coherency support [**Enable**, Disable]
	IIO south Complex configuration>	Disable SC GbE>	Disables South Complex GbE completely [**Enable**, Disable]
		SC GbE PF0>	Enables or disables SC GbE physical function 0 [**Auto**, Enable, Disable]
		SC GbE PF1>	Enable or disables SC GbE physical function 1 [**Auto**, Enable, Disable]
		Disable SC CB3 DMA>	Disables South Complex CB3 DMA completely [**Enable**, Disable]
	TX EQ WA>	Use special table for TX_EQ and vendor specific cards [Enable, **Disable**]	
	WA 4167453>	Disable IIO VCP, Disable PHC VC1, Set IIO VC1 & PCH VCP to TC2, clear irp_misc_dfx0.force_no_snp_on_vc1_vcm [Enable, **Disable**]	
	DMI Vc1 Control>	Enables or disables DMI Vc1 [Enable, **Disable**]	

Function	Second level Sub-Screen / Description		
IIO Configuration> (continued)	DMI Vcp Control>	Enables or disables DMI Vcp [Enable, **Disable**]	
	DMI Vcm Control>	Enables or disables DMI Vcm [Enable, **Disable**]	
	VC0 No-Snoop Configuration>	Enables No-Snoop on reads and writes for Vc0 traffic. [Enable, **Disable**]	
	Gen3 Phase3 Loop Count>	[1, 4, **16,** 256]	
	Skip Halt On DMI Degradation>	Enable this option to avoid that the system is halted on DMI width/link degradation [Enable, **Disable**]	
	Power Down Unused Ports>	Power down unused ports [no, **yes]**	
	SLD WA Revision>	[**Auto**]	
	Rx Clock WA>	Rx Clock WA [Enable, **Disable**]	
	PCI-E ASPM Support (Global)>	Enables or disables the ASPM support for all downstream devices. [L1 Only, **Disable**]	
	PCIE Stop & Scream Support>	Enables or disables PCIE Stop & Scream Support [Enable, **Disable**]	
	Snoop Response Hold Off>	Sets Snoop Response Hold Off value, 256 cycles as Default [**6**]	
PCH Configuration>	PCH devices>	Board Capacity>	Selects Board Capability SUS_PWR_DN_ACK -> Send Disabled to PCH, DeepSx -> Show DeepSx Policies [SUS_PWR_ON_ACK, **DeepSx]**
		DeepSx Power Policies>	Configures the DeepSx Mode configuration. **[Disabled,** Enabled in S5, Enabled in S4-S5 Enabled in S3-S4-S5]
		GP27 Wake From DeepSx>	Selects Wake from DeepSx by the assertion of GP27 pin [Enabled, **Disabled**]
PCH Configuration> (continued)	PCH devices> (continued)	SMBUS Device>	Enable or disable SMBUS Device. **[Enabled**, Disabled]
		PCH Server Error Reporting Mode (SERM)>	If enabled MCH is the final target of all errors otherwise SPCH is the final target to all errors [Enabled, **Disabled**]
		PCH Display>	Enables or disables PCH Display **[Enabled**, Disabled]

Function	Second level Sub-Screen / Description			
PCH Configuration> (continued)		Serial IRQ Mode>	Read only Field [Continuous}	
		High Precision Timer>	Enables or disables the High Precision Event Timer. [Enabled, **Disabled**]	
		Boot Time with HPET Timer>	Enables or disables Boot time calculation with High Precision Event Timer [Enabled, **Disabled**]	
		External SSC Enable – CK420>	Enable Spread Spectrum – only affects external clock generator [Enabled, **Disabled**]	
		PCH state after G3>	Selects the ACPI state after a G3 [**S0**, S5, last state]	
		PCH CRID>	Enables or disables PCH's CRID [Enabled, **Disabled**]	
	PCI Express Configuration> PCI Express Configuration> (continued)	PCI-E ASPM Support (Global)>	Enables or disables the ASPM support for all downstream devices. [**Disable**, L1 Only]	
		PCI-E Clock Gating>	Enables or disables PCIE Clock Gating for all PCH PCIE ports. [**Enabled**, Disabled]	
		DMI Link Extended Synch Control>	Controls Extended Synch on SB slide of the DMI Link [Enabled, **Disabled**].	
		Stop and Scream>	When Enabled DS packets on DMI with the EP bit set, will have their UT bit set.	
		LAN PCIE Port Use>	Read only field [None]	
		Substractive Decode>	Read only field [Disabled]	
		PCIe-USB Glitch W/A>	PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port. [Enabled, **Disabled**]	
		PCIe Root Port Function Swapping>	Enable PCIe root port function swapping feature to dynamically assign function 0 to enabled root port. [Enabled, **Disabled**].	
		PCI Express Root Port 1 -8>	PCI Express Root Port>	Control the PCI Express Root Port

Function	Second level Sub-Screen / Description			
PCH Configuration> (continued)	PCI Express Configuration> (continued)	PCI Express Root Port 1 -8> (continued)	L1 Substates>	PCI Express L1 Substates settings
			URR>	PCI Express Unsupported Request Reporting [Enable,Disable]
			FER>	PCI Express Device Fatal Error Reporting [Enable,Disable]
			NFER>	PCI Express Device Non-Fatal Error Reporting [Enable,Disable]
			CER>	PCI Express Device Correctable Error Reporting [Enable,Disable]
			CTO>	PCI Express Completion Timer T0 [Enable,Disable]
			SEFE>	Root PCI Express System Error on Fatal Error [Enable,Disable]
			SENFE>	Root PCI Express System Error on Non-Fatal Error [Enable,Disable]
			SECE>	Root PCI Express System Error on Correctable Error [Enable,Disable]
			PME SCI>	PCI Express PME SCI [Enable,Disable]
			Hot Plug>	PCI Express Hot Plug [Enable,Disable]
			PCIe Speed>	Configure PCIe Speed
			PME Interrupt>	PCI Express PME Interrupt [Enable,Disable]
			MSI>	PCIE MSI [Enable,Disable]
			Extra Bus Reserved>	Extra Bus Reserved (0-7) for bridges behind this root Bridge.
			Reseved Memory>	Reserved Memory and Prefetchable Memory (1-20MB) Range for this Root Bridge.
			Reserved I/O>	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.
	PCH SATA Configuration>	SATA Controller>	Enables or disables SATA Controller [Disabled, **Enabled**]	

Function	Second level Sub-Screen / Description			
PCH Configuration> (continued)		Configure SATA as>	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive [IDE, **AHCI**]	
		SATA test mode>	Enables or Disables SATA test mode [**Disabled**, Enabled]	
		SATA Mode Options>	SATA HDD Unlock>	If enabled, HDD password unlock is enabled in the OS. [Disabled, **Enabled**]
			SATA LED locate>	If enabled, LED/SGPIO hardware is attached. [Disabled, **Enabled**]
		SATA AHCI LPM>	Enables or disables Link Power Management [Disabled, **Enabled**]	
		Support Aggressive Link Power Management>	Enables or disables SALP [Disabled, **Enabled**]	
		For each SATA port [0-1].		
		Port [0-1].>	Enables or disables the SATA Port [Disabled, **Enabled**]	
		Hot Plug>	Designates this port as Hot Pluggable. [**Disabled**, Enabled]	
		Configure as eSATA>	Configures port as External SATA (eSATA) [**Disabled**, Enabled]	
		Spin Up Device>	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. [**Disabled**, Enabled]	
		SATA Device Type>	Identifies if the SATA port is connected to Solid State Drive or Hard Disk Drive [**Hard Disk Drive**, Solid State Drive]	
	USB Configuration>	USB Precondition>	Precondition work on USB host controller and root ports for faster enumeration. [Enabled, **Disabled**]	
		xHCI Mode>	Mode of operation of xHCI controller [Smart Auto, Auto, **Enabled**, Disabled, Manual].	
		USB Ports per-Port Disable Control>	Control each of the USB ports (0~13) disabling. [Enabled, **Disabled**]	

Function	Second level Sub-Screen / Description		
		XHCI Idle L1>	Enabled XHCI Idle L1. Disabled to workaround USB3 hot plug will fail after 1 hot plug removal. Note: For new settings to take effect, put system to G3. [**Enabled**, Disabled]
	Security Configuration>	GPIO Lockdown>	Enables or disables the PCH GPIO Lockdown feature. [Enabled, **Disabled**]
		RTC Lock>	Enable locks bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM [**Enabled**, Disabled]
		BIOS Lock>	Enables or disables the PCH BIOS Lock Enable feature. [**Enabled**, Disabled]
		Host Flash Lock-Down>	Enabled or disables Host Flash Lock-Down [Enabled, **Disabled**]
		Gbe Flash Lock-Down>	Enables or disables Gbe Flash Lock-Down [Enabled, **Disabled**]
	Platform thermal Configuration>	PCH Thermal Device>	Enable or disables PCH Thermal Device (D31:F6) [Enabled, **Disabled,** Auto]
		Alert Enable Lock>	Enables or disables lock all alert enable settings [Enabled, **Disabled**]
		Enable Thermal Lock-Down>	Enable executes thermal programming, use disable as WA for PCHHOT [**Enabled**, Disabled]
Miscellaneous Configuration>	Fan PWM Offset>	Specify fan speed offset [**0**]	
	PCIe Max Read Request Size>	Sets Max Rest Request Size [Auto leaves HW default values, 128B, 256B, 512B, 1024B, 2048B, **4096B**]	
Miscellaneous Configuration> (contined)	PCIe Latency Tolerance Reporting>	Enables or disables the LTR support [**Enable**, Disable]	
	PCI Minimum Secondary Bus Number>	Specify the PCI minimum secondary bus number in system [1]	
	PCIe Extended Tag Enable>	Enables or disables extended tag enable field support [**Enable**, Disable, Auto]	
	PCIe AtomicOp Request Support>	Enables or disables AtomicOp request support [Enable, **Disable**]	
	Breakpoint Type>	Halts at specified points in BIOS [**None**, After MRC, After QPIRC, After Resource Allocation, After Post, After FullSpeed Setup, Ready for IBIST]	

Function	Second level Sub-Screen / Description			
	BIOS Guard>	Read only field [Disabled]		
	Serial Debug Message Level>	Selects the level of the debug messages Disable - no serial debug message, Minimum - high level debug messages, Normal =- general debug messages [**Disable**, Minimum, Normal, Maximum]		
	Trace Messages>	Enables display of every IO access [Enabled, **Disabled**, Enabled for registry writes only]		
	Training Messages>	Enabled = set to disable the training results. Training results also get displayed if debug messages is set to maximum. [Enabled, **Disabled**]		
	RC Promote Warnings>	If enabled RC warnings are promoted to errors (except MRC warnings) [**Enabled**, Disabled]		
	RC Promote MRC Warnings>	If enabled MRC warnings are promoted to errors [**Enabled**, Disabled]		
	Active Video>	Selects active video type [Onboard Device **Offboard Device]**		
	TargetVGA>	Read only field VGA from CPU 0		
Server ME debug Configuration>	Server ME General Configuration>	ME Initialization Complete Timeout>	Defines how long BIOS waits for ME to initialize. [**2**]	
		Custom HPET timer for SPS HECI Waiting>	Custom HPET timer for SPS HECI Waiting. [1]	
Server ME debug Configuration> (continued)	Server ME General Configuration> (continued)	Override ICC Clock Enables>	Override ICC Clock Enables>	Allows for customization of the clock enables [Enabled, **Disabled**]
			The following options are read only fields	
			FLEX0 Output (bit 0)	[**Enabled**]
			FLEX1 Output (bit 1)	[**Enabled**]
			FLEX2 Output (bit 2)	[**Enabled**]
			FLEX3 Output (bit 3)	[**Enabled**]
			PCICLK0 Output (bit 7)	[**Enabled**]
			PCICLK1 Output (bit 8)	[**Enabled**]
			PCICLK2 Output (bit 9)	[**Enabled**]
			PCICLK3 Output (bit 10)	[**Enabled**]

Function	Second level Sub-Screen / Description			
Server ME debug Configuration> (continued)	Server ME General Configuration> (continued	Override ICC Clock Enables> (continued)	PCICL4 Output (bit 11)	[**Enabled**]
			SRC0 Output (bit 16)	[**Enabled**]
			SRC1 Output (bit 17)	[**Enabled**]
			SRC2 Output (bit 18)	[**Enabled**]
			SRC3 Output (bit 19)	[**Enabled**]
			SRC4 Output (bit 20)	[**Enabled**]
			SRC5 Output (bit 21)	[**Enabled**]
			SRC6 Output (bit 22)	[**Enabled**]
			SRC7 Output (bit 23)	[**Enabled**]
			ITPXDP Output (bit 24)	[**Disabled**]
			PEG_A Output (bit 26)	[**Enabled**]
			PEG_B Output (bit 27)	[**Enabled**]
			DMI Output (bit 28)	[**Enabled**]
			DP Output (bit 29)	[**Enabled**]
			DPNS Output (bit 30)	[**Enabled**]
			Modulator4Enable Output (bit 31)>	[**Disabled**
		Override ICC Spread Spectrum Configuration>	Override ICC Spread Spectrum Configuration>	Sets non-default ICC spread spectrum configuration. [Override, **Auto**]
			The following options are read only fields	
			SSC0 Mode 0 … SSC7 Mode>	[**Auto**]
	NM Configuration>	Cores Disable Override>	Enables overriding the value of the number of cores to disable requested in NMFS register. [Enabled, **Disabled**]	

Function	Second level Sub-Screen / Description		
		Cores to Disable>	Read only field The number of cores to disable instead of the number requested in NMFS register. [**0**]
		Power Measurement Override>	Override power measurement support status reported to ME [Enabled, **Disabled**]
		Power Measurement >	Read only field [**Disabled,** Enabled]
		Hardware Change Override>	Overrides hardware change detection status reported to ME [Enabled, **Disabled**]
		Hardware Changed>	Read only field [**no, yes**]
Server ME Configuration>	Read only field Operational Firmware, ME firmware Type, recovery Firmware Version, ME Firmware features, ME Firmware Status #1, ME Firmware Status #2, Current status, error code		
	Altitude>	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 80000000 value if the altitude is unknown. **[80000000]**	
	MCTP Bus Owner>	MTCP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros, sending bus owner is disabled. [**0**]	
Runtime Error Logging>	System Errors>	System error enabling and logging setup option [**Enable**, Disable, Auto]	
	S/W Error Injection Support>	If enabled S/W error injection supported by unlocking MSR 0x790 [Enable**, Disable**]	
	Clear McBankErrors>	Enables or disables clearing MCBank errors on warm reset [Enable, **Disable**]	
	System Poison>	Enables or disables Core, Uncore and IIO Poison [Enabled, **Disabled**]	
	IIO Error Enable>	[No, **Yes**]	
	PCH Error Enable>	[No, **Yes**]	
	Enable Cloaking>	Enables or disables corrected error cloaking [Enable, **Disable**]	
	Whea Settings>	Whea Support>	Enables or disables the WHEA support, to view or change the WHEA configuration. [Enable, **Disable]**

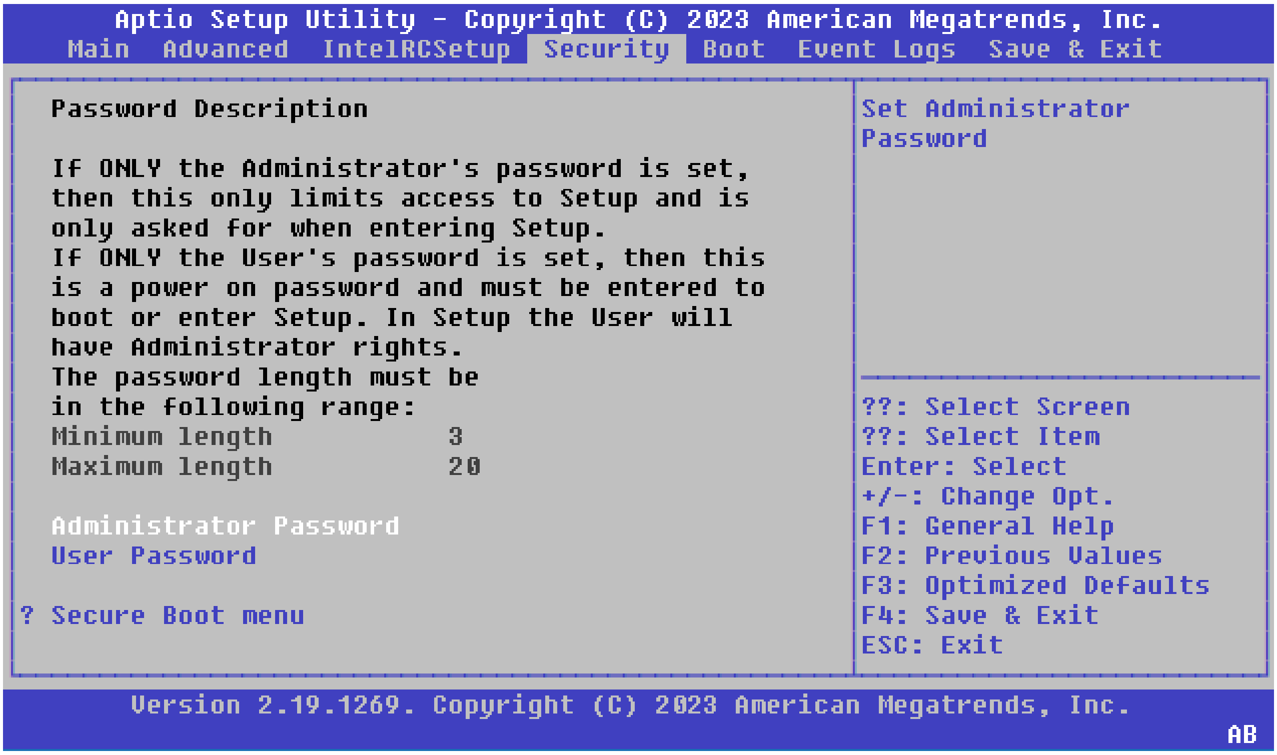
Function	Second level Sub-Screen / Description			
Runtime Error Logging> (continued)	Memory Error Enabling>	Memory Corrected Error Enabling>	Enables or disables Memory corrected Errors support, to view or change the memory errors enabling options [Enable, **Disable**]	
		Spare Interrupt>	Read only field Displays the implemented spare interrupt from SMI, CMCI or ErrPin for spare interrupt [**CMCI**]	
	IIO Error Enabling> IIO Error Enabling> (continued)	Error Pin Programming for IIO>	Error pin Programming [**None**, SMI]	
		DMI Errors>	Enables or disables DMI errors [**Enable**, Disable]	
		Vtd Errors>	Enables or disables Vtd errors [Enable, **Disable**]	
		Misc Errors>	Enables or disables Miscellaneous errors [Enable, **Disable**]	
		IIO Core Errors>	Enables or disables IIO core errors [Enable, **Disable**]	
		DMA Errors>	Enables or disables DMA errors [Enable, **Disable**]	
		Coherency Interface Errors>	Enables or disables Coherency Interface errors [Enable, **Disable**]	
		IIO Coherency Interface Error Enable>	For IRP0 and IRP1	
			IIO <IRP0 and IRP1> protocol parity error>	Enables or disables Coherent Interface protocol IIO parity error reporting [**Enable**, Disable]
			IIO <IRP0 and IRP1 protocol qt overflow underflow>	Enables or disables IIO Coherent Interface protocol queue table overflow or underflow error reporting [**Enable**, Disable]
			IIO <IRP0 and IRP1> protocol rcvd Unexprsp>	Enables or disables IIO Coherent Interface protocol layer received unexpected response or completion error reporting [**Enable**, Disable]
			IIO <IRP0 and IRP1> csr acc 32b unaligned>	Enables or disables IIO Coherent Interface CSR access crossing 32-bit Boundary error reporting [**Enable**, Disable]

Function	Second level Sub-Screen / Description			
Runtime Error Logging> (continued)			IIO <IRP0 and IRP1> wrcache uncecc error>	Enables or disables IIO Coherent Interface Write Cache Un-correctable ECC error reporting [**Enable**, Disable]
			IIO <IRP0 and IRP1> protocol rcvd poison error>	Enables or disables IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting [**Enable**, Disable]
			IO <IRP0 and IRP1> wrcache correcc error>	Enables or disables IIO Coherent Interface Write Cache Correctable ECC error reporting [**Enable**, Disable]
	PCI/PCI Error enabling> PCI/PCI Error enabling> (continued)	PCI-Ex Error Enable>	[No, **Yes**]	
		Corrected Error Enable>	Enables or disables PCIe Correctable errors [Enable, **Disable**]	
		Uncorrected Error Enable>	Enables or disables PCIe Uncorrectable errors. [Enable, **Disable**]	
		Fatal Error Enable>	Enables or disables PCIe Fatal errors. [**Enable**, Disable]	
		PCIe Correctable Error Threshold>	Shows the PCIe CE threshold. Range (1-255), where 0 means no threshold. [**0**]	
		Enable SERR Propagation>	[**No**, Yes]	
		Enable PERR Propagation>	[**No**, Yes]	
		PCIE Extended Errors>	Enables or disables IIO PCIE root port errors [Enable, **Disable**]	

12.4.2. Security Setup Menu

The Security Setup menu provides information about the passwords and functions for specifying the security settings.

Figure 22: Security Setup Menu



```
       Aptio Setup Utility - Copyright (C) 2023 American Megatrends, Inc.
    Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

    Password Description                                  Set Administrator
                                                          Password
    If ONLY the Administrator's password is set,
    then this only limits access to Setup and is
    only asked for when entering Setup.
    If ONLY the User's password is set, then this
    is a power on password and must be entered to
    boot or enter Setup. In Setup the User will
    have Administrator rights.
    The password length must be
    in the following range:                               ??: Select Screen
    Minimum length            3                           ??: Select Item
    Maximum length            20                          Enter: Select
                                                          +/-: Change Opt.
    Administrator Password                                F1: General Help
    User Password                                         F2: Previous Values
                                                          F3: Optimized Defaults
  ? Secure Boot menu                                      F4: Save & Exit
                                                          ESC: Exit

        Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                          AB
```

The following table shows Security sub-screens and functions. Default settings are in **bold**

Table 37: Security Setup Menu Functions

Function	Description		
Administrator Password>	Set administrator password		
User Password>	Set user password		
Secure Boot Menu>	Read only field Shows the status of System mode, Secure boot and Vendor keys.		
	Secure Boot>	Secure boot can be enabled if 1. System runs in user mode with enrolled Platform Key(PK) 2. CSM function is disabled. [Enabled, **Disabled**]	
	Secure Boot Mode>	Selects the secure boot mode. Customer mode enables users to change image execution policy and manage the secure boot keys. [Standard, **Custom**]	
	Key Management>	Provisional Factory Default Keys>	Install factory default secure boot keys when system is in setup mode [Enabled, **Disabled**]

Function	Description		
Secure Boot Menu> (continued)	Key Management> (continued)	Enroll all Factor Default Keys>	Forces system to user mode – install all factory default keys (PK, KEK, db, dbt, dbx. The change takes effect after reboot. [Yes, No]
		Save all secure Boot variables>	Read on field
		Platform Key>	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>	

If only the administrator's password is set, access to the setup is limited and is requested when entering the setup.

If only the user's password is set, then the password is a power on password and must be entered to boot or enter setup. In the setup the user has administrator rights.

The required password length in characters is max. 20 and min. 3 and the passwords are case-sensitive.

12.4.3. Remember the Password

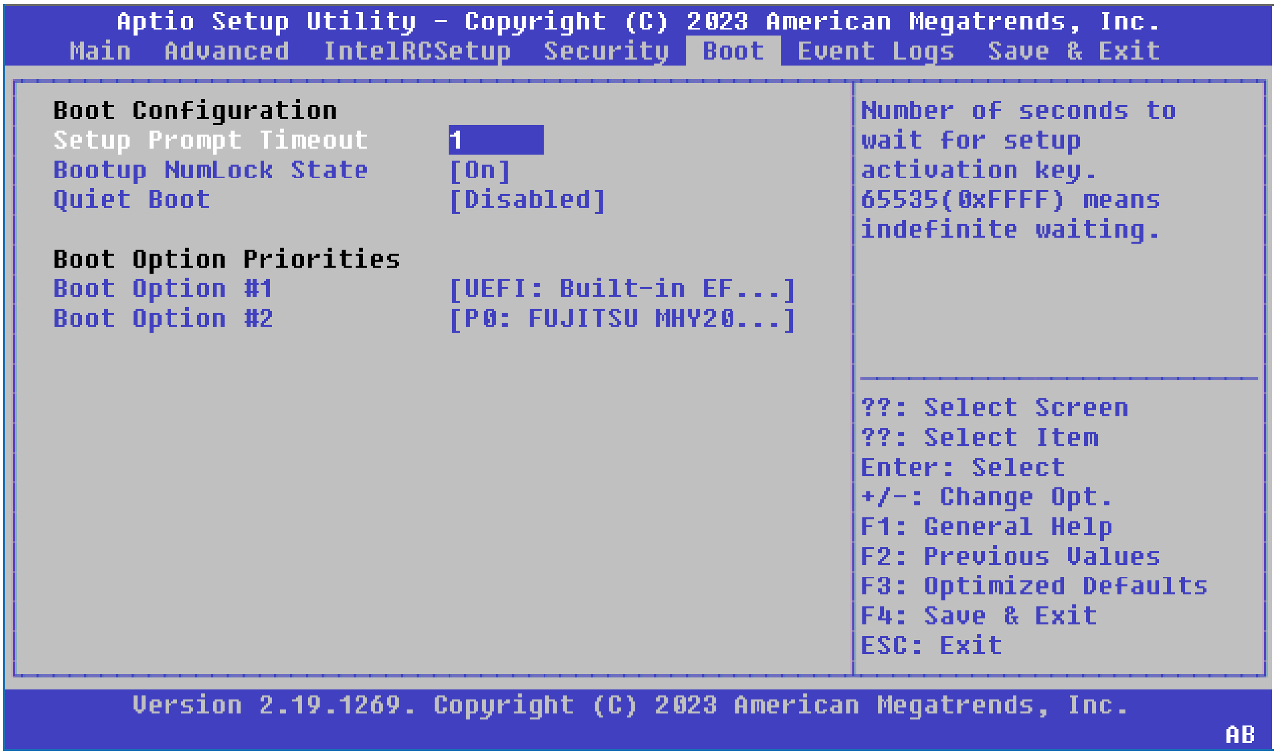
It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system.

If the system cannot be booted because the User Password or the Supervisor Password are not known, clear the uEFI BIOS settings, or contact Kontron Support for further assistance.

12.4.4. Boot Setup Menu

The Boot Setup menu lists the dynamically generated boot device priority order and the boot options. The shown options depends e.g. on CSM Configuration, Network Stack Configuration and others boot devices related settings.

Figure 23: Boot Setup Menu



```
        Aptio Setup Utility – Copyright (C) 2023 American Megatrends, Inc.
     Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

    Boot Configuration                              Number of seconds to
    Setup Prompt Timeout        1                   wait for setup
    Bootup NumLock State        [On]                activation key.
    Quiet Boot                  [Disabled]          65535(0xFFFF) means
                                                    indefinite waiting.
    Boot Option Priorities
    Boot Option #1              [UEFI: Built-in EF...]
    Boot Option #2              [P0: FUJITSU MHY20...]

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

         Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                        AB
```

The following table shows Boot sub-screens and functions, and describes the content. Default settings are in **bold**.

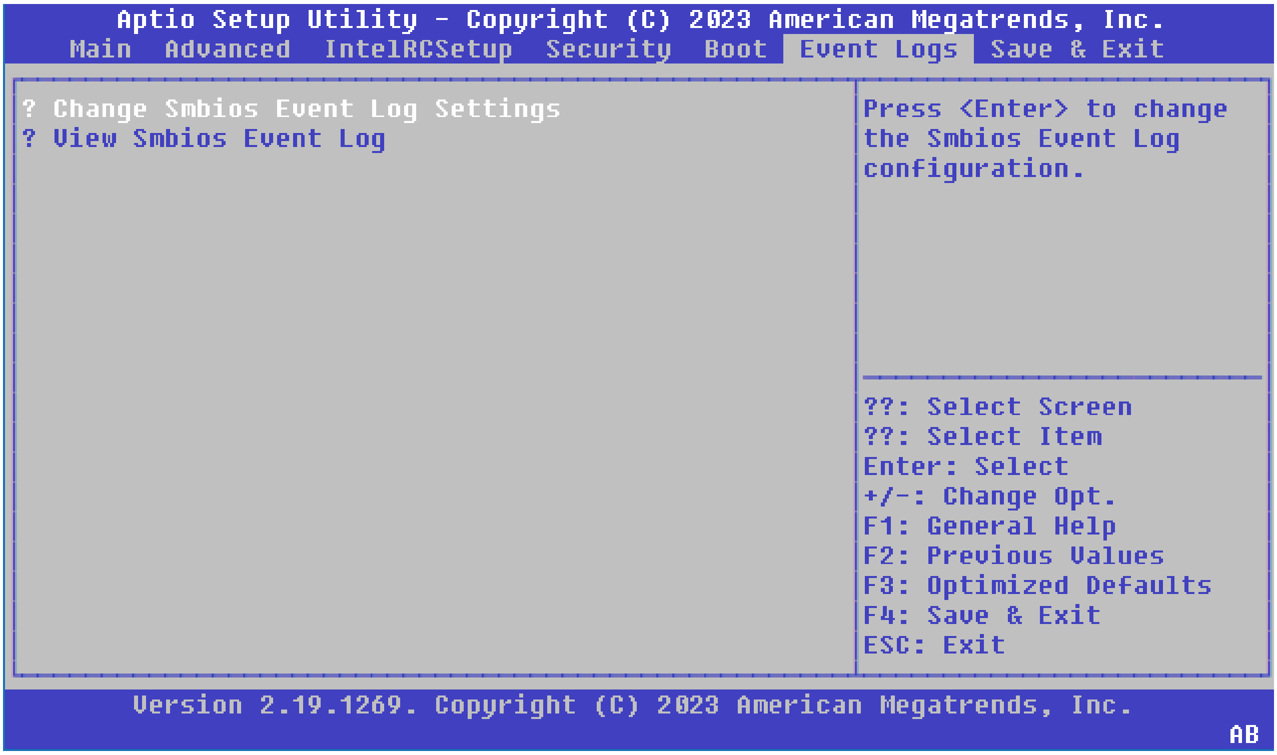
Table 38: Boot Setup Menu Functions

Function	Description
Setup Prompt Timeout>	Displays number of seconds to wait for the setup activation key. 65535(OXFFF) means indefinite waiting [1]
Bootup NumLock State>	Selects keyboard NumLock state [**On**, Off]
Quiet Boot>	Enables or disables Quiet Boot [Enabled, **Disabled**]
Boot Option #1>	Sets the system boot order (option 1) [**UEFI Built-in EFI shell**, PO: FUJITSU MHY2040BH ESW, Disabled]
Boot Option #2>	Sets the system boot order (option 2) [UEFI Built-in EFI shell, **PO: FUJITSU MHY2040BH ESW**, Disabled]

12.5. Event Logs

The Event Logs Setup menu lists the event log settings and options.

Figure 24: Event Log Setup Menu



```
        Aptio Setup Utility - Copyright (C) 2023 American Megatrends, Inc.
     Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

 ? Change Smbios Event Log Settings                      Press <Enter> to change
 ? View Smbios Event Log                                 the Smbios Event Log
                                                         configuration.

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

          Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                              AB
```

The following table shows Event Logs sub-screens and functions, and describes the content. Default settings are in bold and some functions include additional information

Table 39: Event Logs Setup Menu Functions

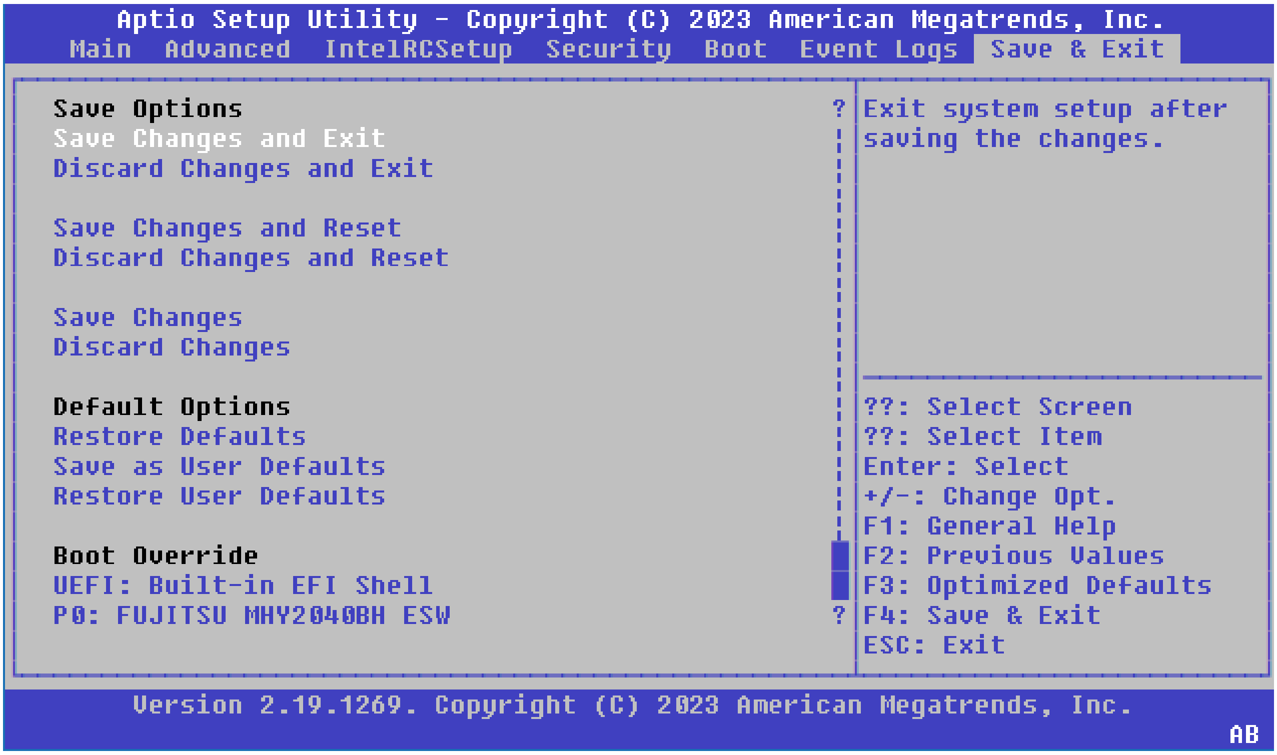
Function	Sub FunctionsDescription	
Change Smbios Event Log Settings>	Enabling and disabling options	
	Smbios Event Log>	Enables or disables all the Smbios event logging features during boot. [**Enabled**, Disabled]
	Erasing settings	
	Erase Event Log>	Choose option for erasing SmBIOS Event Log. Erasing is performed prior to any logging activation during reset. [**No**, Yes next reset , Yes every reset]
	When Log is Full>	Choose option for the reaction to a full Smbios Event log [**Do nothing**, Erase immediately]
	Smbios Event Log Standard	
	Log System Boot Event>	Enables or disables logging of the System boot event [**Enabled**, Disabled]
	MECI>	Displays Multiple Event Count Increment value. The number of duplicate event occurrences that must pass before log entriy multiple event counter is updated. [1]

Function	Sub FunctionsDescription	
Change Smbios Event Log Settings> (continued)	METW>	Displays the Multiple Event Time Window value. The number of minutes that must pass between duplication log entries that utilize a multiple-event counter. (Range from 0-99 minutes) [**60**]
	Custom Options	
	Log OEM Codes>	Enables or disables the logging of EFI staues codes as OEM codes if they have not already been converted to legacy. [**Enabled**, Disabled]
	Convert OEM Codes>	Enables or disables the converting of EFI status codes to standard Smbios types. Note: Not all may be translated. [Enabled, **Disabled**]
	Additional Information: All values changed here take effect only after the computer is restarted	
View Smbios Event log>	List the Event Information: Date: Time. Error Code. Severity.	Error code descriptions: a. Smbios 0x16 - Log area reset b. Smbios 0x17 - System boot c. Smbios x0C3 - Unspecified Processor unrecognised

12.6. Save and Exit

The Save and Exit Setup menu lists the save, default and override options.

Figure 25: Save and Exit Setup Menu



```
    Aptio Setup Utility - Copyright (C) 2023 American Megatrends, Inc.
    Main  Advanced  IntelRCSetup  Security  Boot  Event Logs  Save & Exit

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

    Save Changes and Reset
    Discard Changes and Reset

    Save Changes
    Discard Changes

    Default Options                             ??: Select Screen
    Restore Defaults                            ??: Select Item
    Save as User Defaults                       Enter: Select
    Restore User Defaults                       +/-: Change Opt.
                                                F1: General Help
    Boot Override                               F2: Previous Values
    UEFI: Built-in EFI Shell                    F3: Optimized Defaults
    P0: FUJITSU MHY2040BH ESW                 ? F4: Save & Exit
                                                ESC: Exit

      Version 2.19.1269. Copyright (C) 2023 American Megatrends, Inc.
                                                                    AB
```

The following table shows Boot sub-screens and functions, and describes the content. Default settings are in bold.

Table 40: Save and Exit Menu Functions

Function	Description
Save Options	
Save Changes and Exit>	Exits system after saving changes
Discard Changes and Exit>	Exits system setup without saving changes
Save Changes and Reset>	Resets system after saving changes
Discard Changes and Reset>	Resets system setup without saving changes
Save Changes>	Saves changes made so far for any setup options
Discard Changes>	Discards changes made so far for any setup options
Default Options	
Restore Defaults>	Restores/loads standard default values for all setup options
Save as User Defaults>	Saves changes made so far as User Defaults
Restore User Defaults>	Restores User Defaults to all setup options
Boot Override Options	
UEFI Built-in EFI shell>	Attempts to launch the built in EFI Shell
PO: FUJITSU MHY2040BH ESW>	Attempts to launch PO: FUJITSU MHY2040BH ESW from one of the available file system devices

12.7. The uEFI Shell

The Kontron uEFI BIOS features a built-in and enhanced version of the uEFI Shell. For a detailed description of the available standard shell scripting, refer to the EFI Shell User Guide. For a detailed description of the available standard shell commands, refer to the EFI Shell Command Manual. Both documents can be downloaded from the EFI and Framework Open Source Community homepage (http://sourceforge.net/projects/efi-shell/files/documents/).

AMI APTIO update utilities for DOS, EFI Shell and Windows are available at AMI.com: http://www.ami.com/support/downloads/amiflash.zip.

Kontron uEFI BIOS does not provide all shell commands described in the EFI Shell Command Manual.

12.7.1. Basic Operation of the uEFI Shell

The uEFI Shell forms an entry into the uEFI boot order and is the first boot option by default.

12.7.1.1. Entering the uEFI Shell

To enter the uEFI Shell, follow the steps below:

1. Power on the board.
2. Press the <F7> key (instead of <DEL>) to display a choice of boot devices.
3. Choose 'UEFI: Built-in EFI shell'.

```
EFI Shell version 2.40 [5.11]
Current running mode 1.1.2
Device mapping table
Fs0      :HardDisk - Alias hd33b0b0b fs0
   Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
```

4. Press the <ESC> key within 5 seconds to skip startup.nsh, and any other key to continue.

The output produced by the device mapping table can vary depending on the board's configuration.

If the <ESC> key is pressed before the 5 second timeout elapses, the shell prompt is shown:

```
Shell>
```

12.7.1.2. Exiting the uEFI Shell

To exit the uEFI Shell, follow one of the steps below:

1. Use the exit uEFI Shell command to select the boot device, in the Boot menu, that the OS boots from.
2. Reset the board using the reset uEFI Shell command.

12.8. uEFI Shell Scripting

12.8.1. Startup Scripting

If the <ESC> key is not pressed and the timeout has run out then the uEFI Shell automatically tries to execute some startup scripts. It searches for scripts and executes them in the following order:

1. Initially searches for Kontron flash-stored startup script.
2. If there is no Kontron flash-stored startup script present, then the uEFI-specified startup.nsh script is used. This script must be located on the root of any of the attached FAT formatted disk drive.
3. If none of the startup scripts are present or the startup script terminates then the default boot order is continued.

12.8.2. Create a Startup Script

Startup scripts can be created using the uEFI Shell built-in editor edit or under any OS with a plain text editor of your choice. To create a startup shell script, simply save the script on the root of any FAT-formatted drive attached to the system. To copy the startup script to the flash, use the kBootScript uEFI Shell command.

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the SPI boot flash using the kRamdisk uEFI Shell command.

12.9. Example of Startup Scripts

12.9.1. Execute Shell Script on other Harddrive

This example (startup.nsh) executes the shell script named bootme.nsh located in the root of the first detected disc drive (fs0).

```
        fs0:
        bootme.nsh
```

12.10. Firmware Update

Firmware updates are typically delivered as a ZIP archive containing only the firmware images. The content of the archive with the directory structure must be copied onto a data storage device with FAT partition.

12.10.1. Updating Procedure

BIOS can be updated with the Intel tool fpt.efi using the procedure below:

Copy these files to an USB stick.

flash.nsh (if available)

fpt.efi

fparts.txt

cAL6r<xxx>.bin (where xxx stands for the version #)

Start the system into setup (see Chapter 12.1: Starting the uEFI BIOS).

Check that the following setup entry is set to disabled:

IntelRCSetup > PCH Configuration > Security Configuration > BIOS Lock > Disabled

Save and Exit the BIOS setup.

On the next start, boot into shell (see Chapter 12.7.1.1).

Change to the drive representing the USB stick

```
        fsx:   (x = 0,1,2,etc. represents the USB stick)
```

and then change to the directory where you copied the flash tool.

```
        cd <your_directory>
```

Start flash.nsh (if available) OR enter

```
        fpt  -F bBD7r<xxx>.bin
```

Wait until flashing is successful and then power cycle the board.

Do not switch off the power during the flash process! Doing so leaves your module unrecoverable.

13/ 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

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

Be ready to explain the nature of your problem to the service technician.

13.1. 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.

13.2. 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.

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.

Appendix: 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.

Term	Definition
Extended Module	COM Express® 155mm x 110mm Module form factor.
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
IIO	Integrated Input Output
Legacy Device	Relicts 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

Term	Definition
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
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

Term	Definition
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.

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