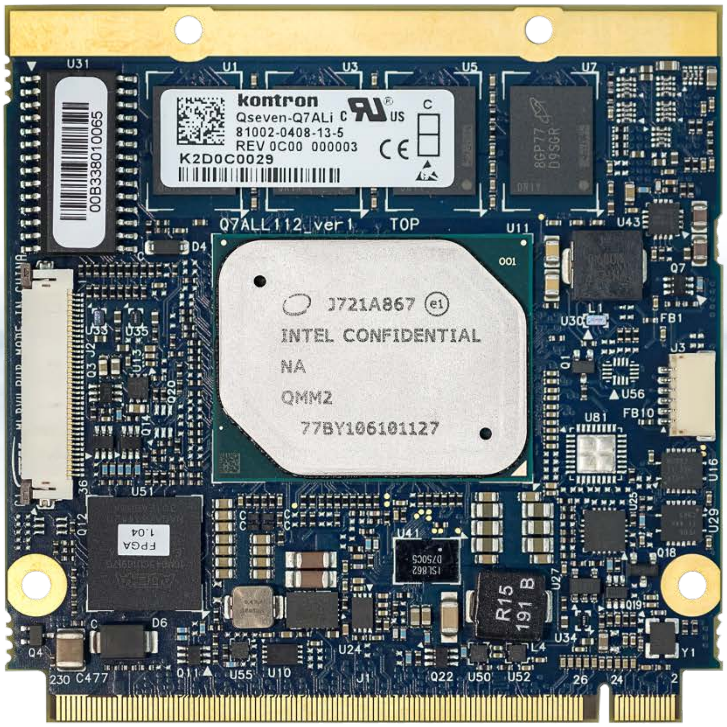
USER GUIDE



QSEVEN-Q7AL

Doc. Rev.1.0

Doc. ID: 1062-0408

This page has been intentionally left blank

QSEVEN-Q7AL - 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.

Kontron AG

Lise-Meitner-Str. 3-5
86156 Augsburg
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.

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
1.0	Initial version	2018-Sept-11	CW
0			

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: http://www.kontron.com/support.

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 http://www.kontron.com/support-and-services/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 user guide

⚠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.
▶ i	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 be 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

This user guide describes the QSEVEN form factor board - Qseven-Q7AL. The use of this user guide implies a basic knowledge of PC hardware and software. This user guide is focused on describing the special features and is not intended to be a standard PC textbook.

New users are recommended to study the short installation procedure stated in the following chapter before switching on the power.

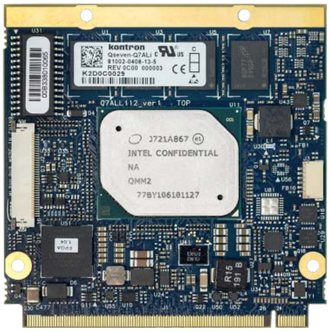
All configuration and setup of the module is either done automatically or manually by the user via the BIOS setup menus.

Latest revision of this user guide, datasheet, BIOS, drivers and BSPs (Board Support Packages) can be downloaded from Kontron Web Page.

2/ Product Description

The Qseven-Q7AL is a QSEVEN form factor module using a processor based on Intel x86 SoC. The Qseven-Q7AL is designed based on the QSEVEN specification Rev 2.1.

Figure 1: QSEVEN Form Factor Module



The main Qseven-Q7AL features are:

- Intel® processors with integrated chipset
- Small form factor QSEVEN® pinout, based on QSEVEN specification Rev 2.1
- Up to 8 GByte DDR3L memory down (non-ECC for commercial variants /ECC for Industrial variants)
- From 2 GB up to 64 GB eMMC 5.0 Flash (option)
- 2x SATA 6 Gb/s
- 4x PCIe x1 Gen 2
- 1x GbE LAN
- 2x USB 3.0 (QSEVEN port 0,1)
- 5x USB 2.0 Host (QSEVEN port 0,2,3,4,5)
- 1x USB 2.0 OTG (QSEVEN port 1)
- 1x Dual Channel LVDS / eDP bypass option / DDI bypass option
- 1x DP/ optional HDMI
- 1x SDIO
- 1x SPI external Boot (SPI0)
- 1x SPI for generic devices (SPI1)
- 1x HDA Audio / I2S Audio (muxed)
- 1x I2C interface
- 1x SMB interface
- 1x MIPI-CSI2
- 1x UART interfaces
- 8x GPIO's / LPC (muxed)
- 1x CAN BUS interface
- Onboard FPGA MAX10
- Support for both commercial and Industrial temperature grade environments

3/ Installation Procedure

3.1. Packing Check List

Check that your delivery is complete, and contains the items below (according to the ordered configuration). If you discover damaged or missing items, contact your dealer.

The delivered package includes the following:

- One Qseven-Q7AL Module Board

Note: The above packing list is for standard single box package only.

3.2. Requirements IEC62368-1

Users of the module must evaluate the end product to ensure the requirements of the IEC62368-1 safety standard are met:

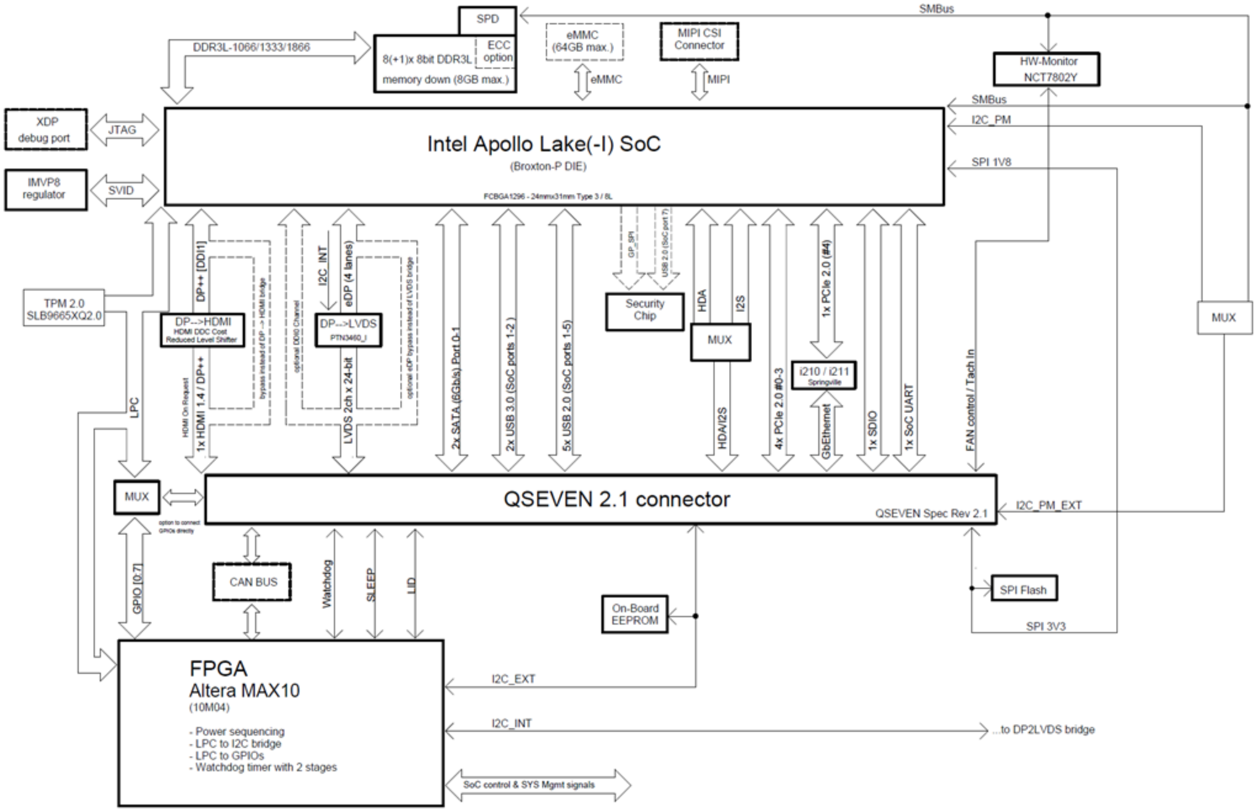
- The module must be installed in a suitable mechanical, electrical and fire enclosure.
- The system in its enclosure must be evaluated for temperature and air flow considerations.
- For interfaces having a power pin such as external power or fan, ensure that the connectors and wires are suitably rated.
- All connections from or to the product shall be with Safety Extra Low Voltage (SELV) circuits only.
- Wires have suitable rating to withstand the maximum available power.
- The enclosure of the peripheral device fulfills the fire protecting requirements of IEC62368-1.

4/ Product Specification

4.1. Block Diagram

The following figure displays the **Qseven-Q7AL** module's system block diagram..

Figure 2 : Block Diagram of Qseven-Q7AL



4.2. Component Main Data

The table below summarizes the module's features.

Table 1: Component Main Data

Qseven-Q7AL	
Form factor	QSEVEN module offer a standardized form factor of 70 mm x 70 mm.
Processor	The processor is Intel Atom SoC 14 nm, FCBGA1296 Type3 with 24 mm x 31 mm, Z-height 1,318mm x 2,318mm.
BIOS	Onboard 128 Mb SPI flash for BIOS storage
Embedded Controller	FPGA MAX10 for Embedded Feature set and logic control
Memory	1x LPDDR3L 1.35 V Memory up to 8 GB, (ECC optional), eight plus one soldered chips
Storage	2 GB up to 64 GB eMMC 5.0 Flash
Watchdog Timer	Dual Staged Watchdog timer will be supported by Watchdog time out (WDOUT) and watchdog trigger(WDTRIG#)
Wake On	Wake on LAN
H/W Status Monitor	The Qseven-Q7AL design shall incorporate a Nuvoton NCT7802Y hardware monitor. It delivers: ▶ SM Bus connection to the System on Chip (SoC) ▶ PWM and Tach interface to Qseven connector to satisfy Qseven specification ▶ Temperature measurement of the QSEVEN PCB (2x with external thermal diode) ▶ A/D measurements on V_RTC, V_3V3_S0 and V_IN_5V0_S3
Trusted Platform Module (TPM)	Incorporated
Complex Programmable Logic Devices (CPLD)	The Qseven-Q7AL design shall incorporate a Altera MAX10 CPLD controller which will handle the following. ▶ Power Sequencing ▶ Status and control signal level shifting mostly to allow signals routed to QSEVEN connector to comply with QSEVEN Specifications. ▶ Incorporated with a LPC to UART bridge to provide 4-wire UART. ▶ Incorporated with a LPC to I2C bridge to provide I2C interface. ▶ Incorporated with a LPC to GPIO bridge to provide eight GPIOs. ▶ Incorporated with a LPC to CAN bridge to provide CAN interface.
Power Management	C0, C1, C6, C7, C8, C9, C10
Expansion	The SOC provides 4 PCIe Gen 2 lanes that can be configured as 4 x1 (i.e. 4 PCIe links that are x1 wide) or as 1x4 (one link in an x4 configuration). The PCIe links and support signals are to be implemented as per the QSEVEN specification document.
Operating System Support	Windows® 10 Enterprise 64 bit, Windows 10 IoT 64 bit, Linux Yocto 64-bit
External I/O	
LAN, USB	One Gbit-Ethernet, two USB 3.0, five USB 2.0 and one USB 2.0 OTG
Audio	One High Definition Audio (HDA)or one Inter IC sound (I2S) (multiplexer)
Embedded Display Port	One embedded Display Port (eDP) interface. The Intel SoC eDP port is used to create the QSEVEN eDP0 interface which are sharing the same pins with the LVDS-A interface.

Display Port	One Digital Display Interface (DDI) channel 0 display port interface. The Intel SoC DDI port 0 is used to create the QSEVEN eDP1 interface that are sharing the same pins with the LVDS-B interface.
LVDS	The Intel SoC eDP is used to create the QSEVEN dual channel LVDS interface. The interface should be able to support 18 bit and 24 bit single and dual channel LVDS panels.
Internal I/O: QSEVEN I/O System Interconnection	
SATA	Two Gen3 SATA link
GbE LAN	One QSEVEN GBE port using Intel I210/I211 PCIe – GBE MAC/PHY controller
LVDS	One LVDS and one LVDS/eDP1.4/DDI0
PCIe	4 PCIe Gen 2 lanes that can be configured as 4 x1 (i.e. 4 PCIe links that are x1 wide) or as 1x4 (one link in an x4 configuration). The PCIe links and support signals are implemented as per the QSEVEN specification document.
Inter-IC Sound (I2S)	One I2S interface muxing with one HDA interface
Serial Port	One 4-wire UART interface (TX, RX, CTS, RTS) at 3.3V TTL derived from the MAX10 FPGA
Serial Peripheral Interface (SPI)	One fast SPI interface which is connected to the primary SPI chip and can also be used for external boot from the QSEVEN Carrier BIOS SPI chip. Another SPI interface shall be provided as a secondary SPI interface for generic SPI devices on the carrier.
I2C	Four I2C interfaces which are derived from the SoC
GPIO	8x general purpose inputs/outputs
Internal Header and Jumper	
MIPI Connector (option)	1x MIPI-CSI2 via onboard connector according to QSEVEN Specifications Rev 2.1 (36pin FCI connector)
Power	One 10-pin power connector: The Qseven-Q7ALi is supplied from a DUAL power supply supporting a Voltage supply of 5 V according to QSEVEN specification. The QSEVEN specification defines a maximum current per input voltage pin of 0.5A. Power is brought to the module through 12 pins. This leads to a maximum module-power of 12W when supplied with the minimum input voltage level.
Display	
Graphics Interface	The board supports onboard graphics through four Ports: ▶ LVDS: The Intel SoC eDP delivers the QSEVEN dual channel LVDS interface. The interface supports 18 bit and 24 bit single and dual channel LVDS panels via PTN3460. ▶ eDP: The Intel SoC eDP connects the display via the QSEVEN eDP0 interface, that shares the same pins with the LVDS-A interface. ▶ DDI0: The Intel SoC DDI0 connects the display via the QSEVEN eDP1 interface, that shares the same pins with the LVDS-B interface. ▶ Dual mode HDMI: Dual Mode (HDMI and DisplayPort on the same pins) implementations are realized through the Intel SoC DDI1 interface. ▶ DP++: The Intel SoC DDI1 shall be used to create the QSEVEN DP++ interface
Graphics Controller	Intel HD Gfx Gen9
Resolution	DP/LVDS 4096 x 2160 with 60 Hz
Ethernet	
Controller	Intel i210IT/i211AT
Interface	One GB Ethernet port via QSEVEN I/O
Security	

Kontron Security Solution Approtect	The board is equipped with the Kontron Security Solution Approtect, providing an embedded hardware security solution that enables applications to be secured, even in unsecure environments. The solution provides features such as: Copy protection, IP protection and licence module enforcement

⚠CAUTION Danger of explosion if the lithium battery is incorrectly replaced.

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

4.3. Environmental Condition and Standards & Approvals

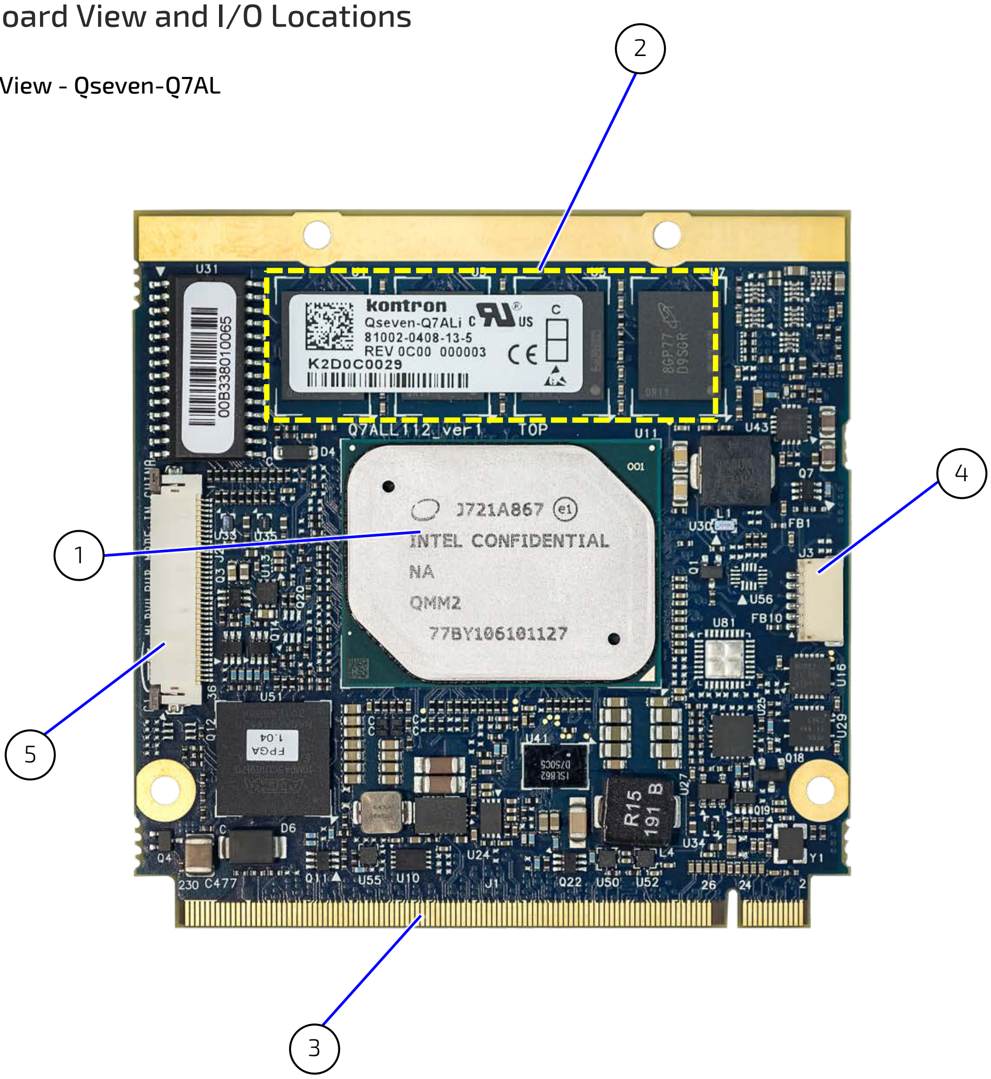
The Qseven-Q7AL module plans to comply with the Standards and Directives mentioned in Table 2.

Table 2: Environmental Condition and Standards & Approvals

Environmentals	
Operating	Commercial grade: 0°C to +60°C Extended (E1): -25°C to 75°C Industrial grade (E2): -40°C to +85°C Relative humidity: 93%, at +40°C, non-condensing (according to IEC 60068-2-78)
Storage	Commercial grade: -30°C to +85°C Extended (E1): -25°C to 75°C Industrial grade (E2): -40°C to +85°C Relative humidity: 93%, at +40°C, non-condensing (according to IEC 60068-2-78)
Standards & Approvals	
Electromagnetic Compatibility (EMC) and Interference (EMI)	Emissions: Conducted in standard available chassis. Compliant to the requirements of EN55032:2012/AC:2013 class B / FCC part 15 class B Electromagnetic compatible – Emission standard for information technology equipment (ITE). External test in certified test laboratory and declaration of conformity written by Kontron Technology only. Immunity: Conducted in standard available chassis with Q7 carrier board. Compliant to the requirements of IEC/EN 61000-6-1:2007 Electromagnetic compatible – Generic immunity standard Part1: Residential, commercial and light industrial environment. Internal test and declaration of conformity only.
Safety	Component Recognition to IEC62368-1
Vibration/ Shock	According to: IEC/EN60068-2-64 IEC/EN60068-2-27
Compliance/ Regulatory	▶ CE marked according to low voltage directive 2006/95/EC EN62368-1 ▶ Safety Component Recognition to IEC62368-1 ▶ EMC according to EN55032 ▶ Shock & Vibration according to IEC/EN60068-2-64 and IEC/EN60068-2-27
Theoretical MTBF	Not applicable
RoHS II Compliance	The product will comply to the European Council Restriction of Hazardous Substances (RoHS) II Directive on the approximation of the laws of the member states relating to Directive 20011/65/EU or the last status thereof.

4.4. Mainboard View and I/O Locations

Figure 3 : Top View - Qseven-Q7AL



1 CPU

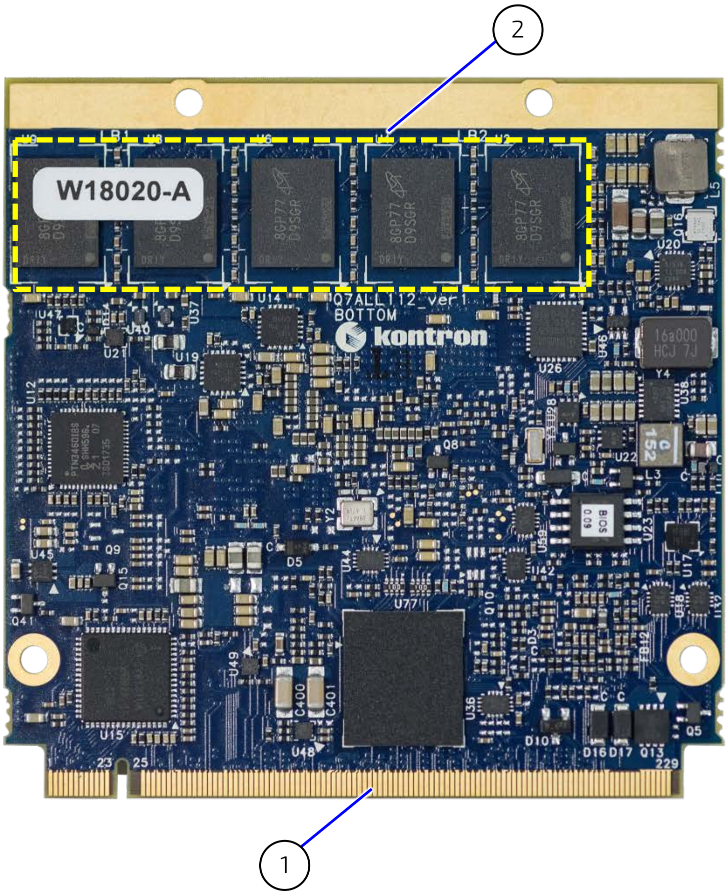
2 Memory down

3 Qseven connector

4 CPLD JTAG connector

5 MIPI-CSI2 Connector

Figure 4 : Rear View - Qseven-Q7AL



1	Qseven Connector	2	Memory down (rear side)

Figure 5: Front View - Qseven-Q7AL

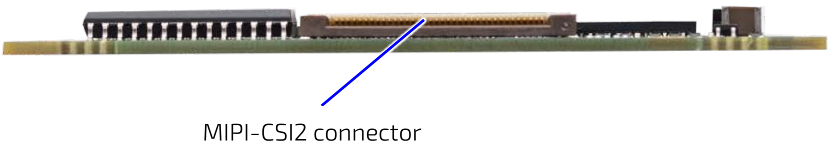
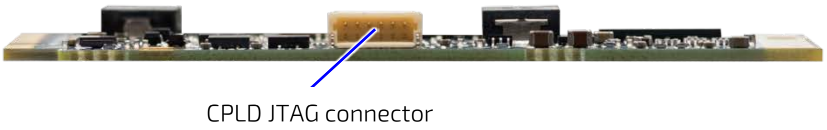


Figure 6: Back View - Qseven-Q7AL



4.5. Mechanical Specification

4.5.1. Qseven-Q7AL Mechanical Dimensions

Figure 7 : Module Top Placement (measurement in mm)

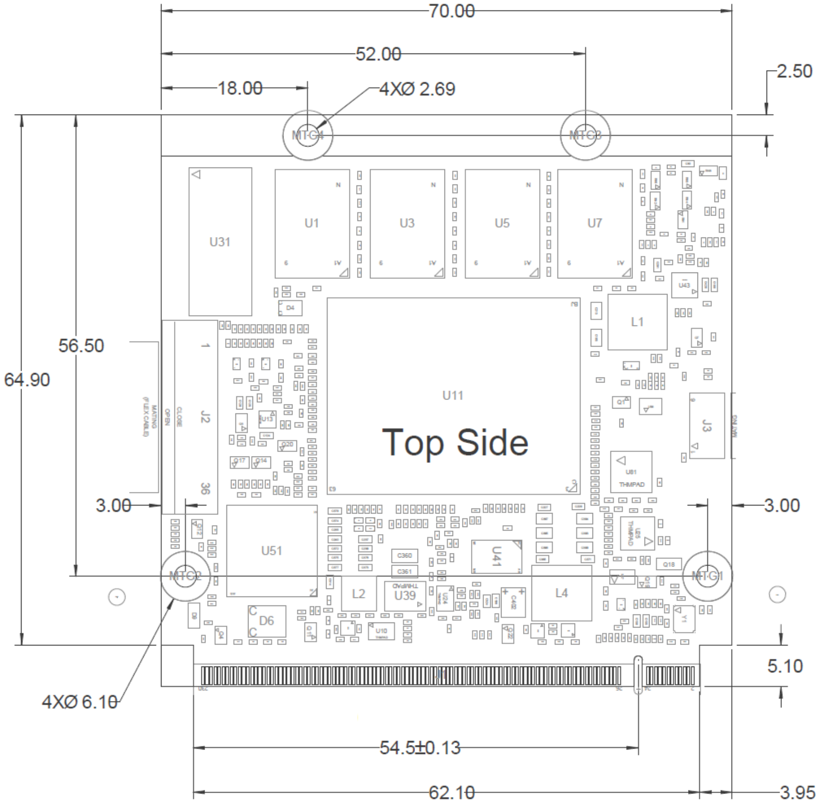
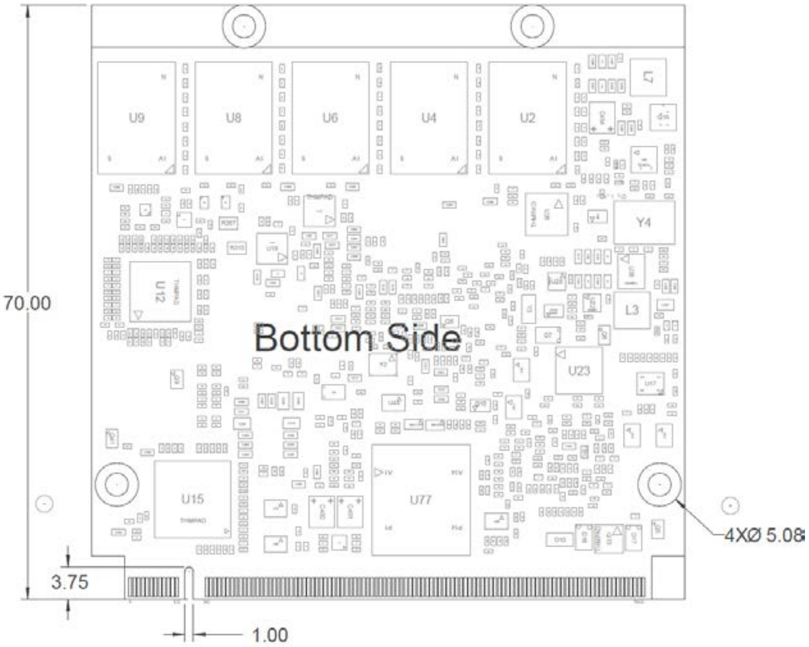


Figure 8: Module Bottom Placement(Mirrored) (measurement in mm)



4.5.2. Heat Spreader Mechanical Dimensions

Figure 9: Heat Spreader Part Number for Commercial Grade Processor 1061-8514

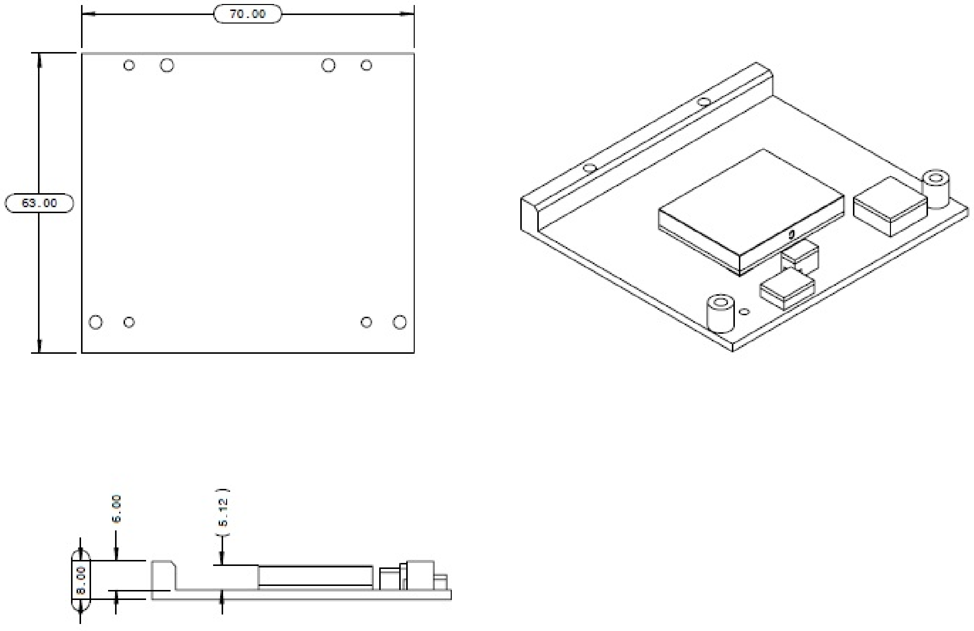
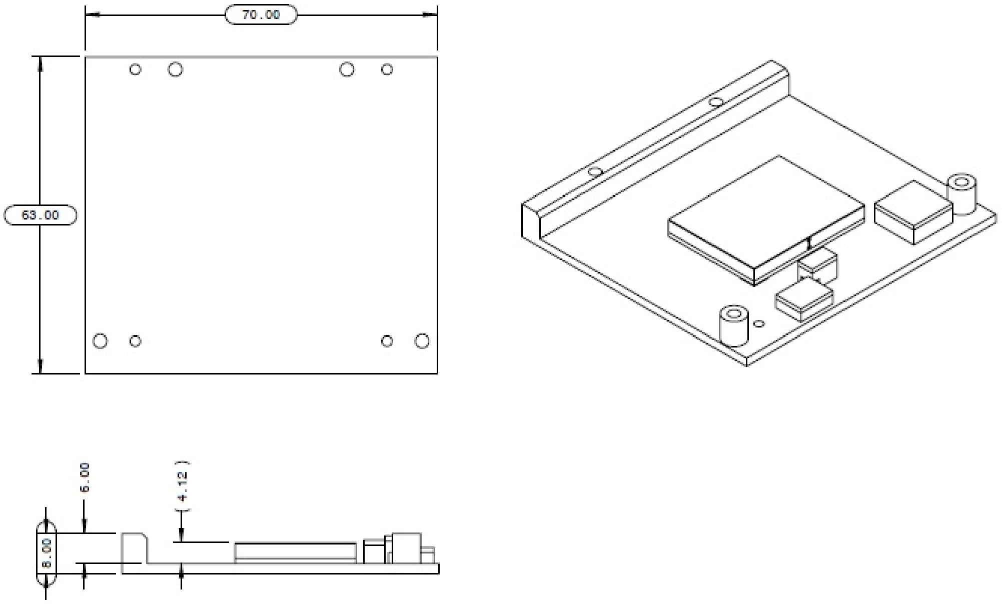


Figure 10: Heat Spreader Part Number for Industrial Grade Processor 1061-8515



4.6. Thermal Management

4.6.1. Heat Spreader and Cooling Solutions

A heatspreader plate assembly is available from Kontron for the Qseven-Q7AL. The heatspreader plate on top of this assembly is NOT a heat sink. It works as a QSEVEN-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 worstcase 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)

The aluminum slugs and thermal pads or the heat-pipe on the underside of the heatspreader assembly implement thermal interfaces between the heatspreader plate and the major heat-generating components. About 80 % of the power dissipated within the module is conducted to the heatspreader plate and can be removed by the cooling solution. For documentation and CAD drawings of heatspreader and cooling solutions refer to: http://emdcustomersection.kontron.com.

5/ Features and Interfaces

5.1. LPC

The Low Pin Count (LPC) Interface signals are connected to the LPC bus bridge located in the CPU or integrated chipset. The LPC low speed interface can be used for peripheral circuits such as an external Super I/O controller that typically combines legacy-device support into a single IC. The implementation of this subsystem complies with the QSEVEN® Specification.

The LPC bus does not support DMA (Direct Memory Access). When more than one device is used on LPC, a zero delay clock buffer is required that can lead to limitations for the ISA bus.

Table 3: Supported BIOS Features

Interface Signals	
PS/2	Not supported
UART	Supported as COM0 only (on CPLD *SoC optional)
LPT	Not supported
Floppy	Not supported
GPIO	Supported
CAN	Supported
I2C	Supported

Features marked as not supported do not exclude OS support (e.g. Hardware Monitor (HWM) is accessible via SMB). If any other LPC Super I/O additional BIOS implementations are necessary, contact Kontron Support.

5.2. Serial Peripheral Interface (SPI)

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

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

5.3. SPI boot

The Qseven-Q7AL supports boot from a 16 MB, 3.3 V serial external SPI Flash. Alternativly, the SPI Flash can be configured to boot from either on-module SPI Flash or the on-carrierboard Flash pin (Module_BIOS_DIS#).

Table 4: SPI Boot Pin Configuration

Configuration	MODULE_BIOS_DIS#	Function
1	Open	Boot on module BIOS
2	GND	Boot on carrierboard BIOS

The BIOS does not support being split between two chips. Booting takes place either from the module SPI or from the baseboard SPI.

The following table lists the supported SPI Boot Flash types for the 8-SOIC package.

Table 5: Supported SPI Boot Flash Types for 8-SOIC Package

Size	Manufacturer	Part Number	Device ID
16MB	Maxim	MX25L12835F	0x20
16MB	Winbond	W25Q128	0x90
16MB	Micron	N25Q128A	0xBA

5.4. Fast I2C

Fast I2C supports transfer between components on the same board. The Qseven-Q7AL features an embedded I2C controller connected to the LPC Bus.

The I2C controller supports:

- Multimaster transfers
- Clock stretching
- Collision detection
- Interruption on completion of an operation

5.5. UART

The UART implements a serial communication interface and supports to serial RX/TX port defined in the QSEVEN® specification on pin 171 (UART0_TX) and pin A 177 (UART0_RX) for UART0. The UART controller is fully 16550A compatible.

UART features are:

- On-Chip bit rate (baud rate) generator
- With handshake lines
- Interrupt function to the host
- FIFO buffer for incoming and outgoing data

5.6. Dual Staged Watchdog Timer (WTD)

A watchdog timer (WDT) or (computer operating properly (COP) timer) is a computer hardware or software timer. If there is a fault condition in the main program, the watchdog triggers a system reset or other corrective actions. The intention is to bring the system back from the non-responsive state to normal operation.

Possible fault conditions are a hang, or neglecting to service the watchdog regularly. Such as writing a "service pulse" to it, also referred to as "kicking the dog", "petting the dog", "feeding the watchdog" or "triggering the watchdog".

The Qseven-Q7AL offers a watchdog that works with two stages that can be programmed independently and used stage by stage.

Table 6: Dual Staged Watchdog Timer- Time-Out Events

0000b	No action	The stage is off and will be skipped.
0001b	Reset	A reset restarts the module and starts a new POST and operating system.
0101b	Delay -> No action*	Might be necessary when an operating system must be started and the time for the first trigger pulse must be extended. Only available in the first stage.
1000b	WDT Only	This setting triggers the WDT pin on the QSEVEN® connector (pin 72) only.
1001b	Reset + WDT	
1010b	NMI + WDT	
1011b	SMI + WDT	
1100b	SCI + WDT	
1101b	DELAY + WDT -> No action*	

5.6.1. Watchdog Timer Signal

Watchdog time-out event (pin 72) on the QSEVEN® connector offers a signal that can be asserted when a watchdog timer has not been triggered within a set time. The WDT signal is configurable to any of the two stages. After reset, the signal is automatically deasserted. If deassertion is necessary during runtime, contact Kontron Support for further help.

5.7. Real Time Clock (RTC)

The RTC keeps track of the current time accurately. The RTC's low power consumption means that the RTC can be powered from an alternative source of power, enabling the RTC to continue to keep time while the primary source of power is off or unavailable. The Qseven-Q7AL's RTC battery voltage range is 2.4 V - 3.3 V.

5.8. Trusted Platform Module (TPM 2.0)

A Trusted Platform Module (TPM) stores RSA encryption keys specific to the host system for hardware authentication. The term TPM refers to the set of specifications applicable to TPM chips. The LPC bus connects the TPM chip to the CPU.

Each TPM chip contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the TPM chip and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.

A second key, called an Attestation Identity Key (AIK) protects the device against unauthorized firmware and software modification by hashing critical sections of firmware and software before they are executed. When the system attempts to connect to the network, the hashes are sent to a server that verifies they match the expected values. If any of the hashed components have been modified since the last started, the match fails, and the system cannot gain entry to the network.

5.9. Kontron Security Solution

Kontron Security Solution is a combined hardware and software solution that includes an embedded hardware security module and a software framework to protect applications.

The Qseven-Q7AL includes an integrated security module connected to SoC port 7 that means that QSEVEN port 7 is not available. Features of the integrate security solution are:

- Copy protection
- IP protection
- License model enforcement

If required, customers can customize the solution to meet specific needs. For more information, contact Kontron Support.

5.10. SpeedStep™ Technology

SpeedStep™ technology enables the adaption of high performance computing in applications by switching automatically between maximum performance mode and battery-optimized mode, depending on the needs of the application. When battery powered or running in idle mode, the processor drops to lower frequencies (by changing the CPU ratios) and voltage, thus conserving battery life while maintaining a high level of performance. The frequency is automatically set back to the higher 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 Setup, manual control or modification of the CPU performance is possible. To achieve manual control setup the CPU Performance State in the BIOS Setup or use third party software to control the CPU Performance States.

6/ System Resources

6.1. Peripheral Component Interconnect (PCI) Devices

All devices follow the Peripheral Component Interconnect (PCI) 2.3 and PCI Express Base 1.0a specification. The BIOS and Operating System (OS) control the memory and I/O resources. For more information, refer to the PCI 2.3 specification.

6.2. I2C Bus

The following table specifies the devices connected the I2C bus including the I2C address.

Table 7: I2C Bus Port Address

8-bit I2C Address	Used For	Available	Comment
A0h	JIDA-EEPROM	Yes	Module EEPROM
C0h	LVDS PTN3460	Yes	LVDS EEPROM

6.3. System Management (SM) Bus

The 8-bit SMBus address uses the LSB (Bit 0) for the direction of the device.

Bit0 = 0 defines the write address
Bit0 = 1 defines the read address

The 8-bit address listed below shows the write address for all devices. The7-bit SMBus address shows the device address without bit0.

Table 8: SMBus Address

8-bit Address	7-bit Address	Device	Comment	SMBus
5Ch	2eh	HWM NCT7802Y	Do not use under any circumstances	SMB
A0h	50h	SPD DDR Channel 1 (SO-DIMM)		SMB
30h	18h	SO-DIMM Thermal Sensor	If available on the used memory-module	SMB

7/ Connectors

7.1. Hardware Configuration Setting

This chapter gives the definitions and shows the positions of headers and connectors.

7.1.1. Connectors

Table 9: Connectors of Qseven-Q7AL

Connector	Function	Remark
FCI (Option)	MIPI-CSI2 Connector	1x36-pin Connector
CPLD	CPLD Connector	1x6-pin Connector
QSEVEN	Central Interface	1x230-pin header

8/ Pin Definitions

The following sections provide pin definitions and detailed description of all on-board connectors.

The connector definitions follow the following notation:

Table 10: Supported BIOS Features

Column Name	Description
Pin	Shows the pin-numbers in the connector. The graphical layout of the connector definition tables is made similar to the physical connectors.
Signal	The mnemonic name of the signal at the current pin. The notation “XX#” states that the signal “XX” is active low.
Type	AI: Analog Input AO: Analog Output I: Input, TTL compatible if nothing else stated IO: Input / Output, TTL compatible if nothing else stated IOT: Bi-directional tristate IO pin. IS: Schmitt-trigger input, TTL compatible. IOC: Input / open-collector Output, TTL compatible IOD: Input / Output, CMOS level Schmitt-triggered (Open drain output) NC: Not Connected O: Output, TTL compatible OC: Output, open-collector or open-drain, TTL compatible OT: Output with tri-state capability, TTL compatible LVDS: Low Voltage Differential Signal PWR: Power supply or ground reference pins. Ioh: Typical current in mA flowing out of an output pin through a grounded load, while the output voltage is > 2.4 V DC (if nothing else stated). Iol: Typical current in mA flowing into an output pin from a VCC connected load, while the output voltage is < 0.4 V DC (if nothing else stated).
Pull U/D	On-board pull-up or pull-down resistors on input pins or open-collector output pins.
Note	Special remarks concerning the signal
Designation	Type and number of item described

8.1. Processor Support

Kontron has defined the board versions as listed in the following table, so far all based on Embedded CPUs.

Industrial Grade:

- Intel Atom x5 E3930 2C 1.8 GHz, 6,5W (Entry SKU @ -40°C to 85°C)
- Intel Atom x5 E3940 4C 1.8 GHz, 9,5W (Intermediate SKU @ -40°C to 85°C)
- Intel Atom x7 E3950 4C 2.0 GHz, 12W (High SKU @ -40°C to 85°C)

Commercial Grade

- Intel Mobile Celeron N3350 2C 2.3 GHz 6 W (Entry SKU @ 0°C to 60°C)
- Intel Mobile Celeron N4200 2C 2.5 GHz 6 W (High SKU @ 0°C to 60°C)

Table 11: Processor Support

Name	Product number	Speed	Embed.	Cache	Sspec	TDP / Tj
Atom x5 E3930 2C	1060-7110	1.8 GHz	Yes	2 MB		6.5 W/85ºC
Atom x5 E3940 4C	1060-7111	1.8 GHz	Yes	2 MB		9.5 W/85ºC
Atom x7 E3950 4C	1060-7114	2 GHz	Yes	2 MB		12 W/85°C
Mobile Celeron N3350 2C	1060-7116	2.4 GHz	Yes	2 MB	SR2YB	6 W/105°C
Mobile Celeron N4200 2C	1060-7115	2.5 GHz	Yes	2 MB	SR2Y9	6 W/105ºC

8.2. System Memory Support

The memory system has one LPDDR3L socket. The sockets support the following memory features:

- 1x Low Power DDR LPDDR3L with 1.35 V
- Max up to 8 GB (8 + 1 chip).
- DDR3-1867 (-1600) memory, ECC for Atom-versions

Kontron offers the following memory modules:

Table 12: Memory Support

Memory Module	Description
8 GByte LPDDR3L	

8.3. MIPI-CSI2 Connector

Figure 11 : MIPI-CSI2 Connector

Table 13: MIPI-CSI2 Connector

Pin	Signal	Pin	Signal
1	CAM_PWR 3.3V	19	CAM0_I2C_DAT
2	CAM_PWR 3.3V	20	CAM0_ENA#
3	CAM0_CSI_D0+	21	MCLK
4	CAM0_CSI_D0-	22	CAM1_ENA#
5	GND	23	CAM1_I2C_CLK
6	CAM0_CSI_D1+	24	CAM1_I2C_DAT
7	CAM0_CSI_D1-	25	GND
8	GND	26	CAM1_CSI_CLK+
9	CAM0_CSI_D2+	27	CAM1_CSI_CLK-
10	CAM0_CSI_D2-	28	GND
11	CAM0_RST#	29	CAM1_CSI_D0+
12	CAM0_CSI_D3+	30	CAM1_CSI_D0-
13	CAM0_CSI_D3-	31	CAM1_RST#
14	GND	32	CAM1_CSI_D1+
15	CAM0_CSI_CLK+	33	CAM1_CSI_D1-
16	CAM0_CSI_CLK-	34	GND

17	GND	35	CAM0_GPIO
18	CAM0_I2C_CLK	36	CAM1_GPIO

8.4. CPLD Programming Header

Figure 12 : 6-pin CPLD Connector

Table 14: 6-pin CPLD Connector

Pin	Signal
1	3.3V Supply
2	TDO
3	TDI
4	TCK
5	TMS
6	GND

8.5. QSEVEN Connector

The QSEVEN connector is MXM 230 pins connector; it has same pins on both sides:

- Top side: 103 pins are on the left side, 12 pins on the right side
- Bottom side(mirrored): 12 pins are on the left side, 103 pins on the right side

Table 15: QSEVEN Connector Pin Assignment

Pin	Signal (Bottom side row)	No	Signal (Top side row)
1	GND	2	GND
3	GBE_MDI3-	4	GBE_MDI2-
5	GBE_MDI3+	6	GBE_MDI2+
7	GBE_LINK100#	8	GBE_LINK1000#
9	GBE_MDI1-	10	GBE_MDI0-
11	GBE_MDI1+	12	GBE_MDI0+
13	GBE_LINK#	14	GBE_ACT#
15	GBE_CTREF	16	SUS_S5#

Pin	Signal (Bottom side row)	No	Signal (Top side row)
17	WAKE#	18	SUS_S3#
19	GPO0	20	PWRBTN#
21	SLP_BTN# / GPII1	22	LID_BTN# / GPII0
23	GND	24	GND
KEY		KEY	
25	GND	26	PWGIN
27	BATLOW# / GPII2	28	RSTBTN#
29	SATA0_TX+	30	SATA1_TX+
31	SATA0_TX-	32	SATA1_TX-
33	SATA_ACT#	34	GND
35	SATA0_RX+	36	SATA1_RX+
37	SATA0_RX-	38	SATA1_RX-
39	GND	40	GND
41	BIOS_DISABLE# / BOOT_ALT#	42	SDIO_CLK#
43	SDIO_CD#	44	reserved
45	SDIO_CMD	46	SDIO_WP
47	SDIO_PWR#	48	SDIO_DAT1
49	SDIO_DAT0	50	SDIO_DAT3
51	SDIO_DAT2	52	reserved
53	reserved	54	reserved
55	reserved	56	USB_OTG_PEN
57	GND	58	GND
59	HDA_SYNC / I2S_WS	60	SMB_CLK / GP1_I2C_CLK
61	HDA_RST# / I2S_RST#	62	SMB_DAT / GP1_I2C_DAT
63	HDA_BITCLK / I2S_CLK	64	SMB_ALERT#
65	HDA_SDI / I2S_SDI	66	GP0_I2C_CLK
67	HDA_SDO / I2S_SDO	68	GP0_I2C_DAT
69	THRM#	70	WDTRIG#
71	THRMTRIP#	72	WDOUT
73	GND	74	GND
75	USB_P7- / USB_SSTX0-	76	USB_P6- / USB_SSRX0-
77	USB_P7+ / USB_SSTX0+	78	USB_P6+ / USB_SSRX0+
79	USB_6_7_OC#	80	USB_4_5_OC#
81	USB_P5- / USB_SSTX2-	82	USB_P4- / USB_SSRX2-
85	USB_2_3_OC#	86	USB_0_1_OC#
87	USB_P3-	88	USB_P2-
89	USB_P3+	90	USB_P2+
91	USB_VBUS	92	USB_ID
93	USB_P1-	94	USB_P0-
95	USB_P1+	96	USB_P0+
97	GND	98	GND

Pin	Signal (Bottom side row)	No	Signal (Top side row)
99	eDP0_TX0+ / LVDS_A0+	100	eDP1_TX0+ / LVDS_B0+
101	eDP0_TX0- / LVDS_A0-	102	eDP1_TX0- / LVDS_B0-
103	eDP0_TX1+ / LVDS_A1+	104	eDP1_TX1+ / LVDS_B1+
105	eDP0_TX1- / LVDS_A1-	106	eDP1_TX1- / LVDS_B1-
107	eDP0_TX2+ / LVDS_A2+	108	eDP1_TX2+ / LVDS_B2+
109	eDP0_TX2- / LVDS_A2-	110	eDP1_TX2- / LVDS_B2-
111	LVDS_PPEN	112	LVDS_BLEN
113	eDP0_TX3+ / LVDS_A3+	114	eDP1_TX3+ / LVDS_B3+
115	eDP0_TX3- / LVDS_A3-	116	eDP1_TX3- / LVDS_B3-
117	GND	118	GND
119	eDP0_AUX+ / LVDS_A_CLK+	120	eDP1_AUX+ / LVDS_B_CLK+
121	eDP0_AUX- / LVDS_A_CLK-	122	eDP1_AUX- / LVDS_B_CLK-
123	LVDS_BLT_CTRL / GP_PWM_OUT0	124	GP_1-Wire_Bus / HDMI_CEC
125	GP2_I2C_DAT / LVDS_DID_DAT	126	eDP0_HPD# / LVDS_BLC_DAT
127	GP2_I2C_CLK / LVDS_DID_CLK	128	eDP1_HPD# / LVDS_BLC_CLK
129	CAN0_TX	130	CAN0_RX
131	DP_LANE3+ / TMDS_CLK+	132	USB_SSTX1-
133	DP_LANE3-/TMDS_CLK	134	USB_SSTX1+
135	GND	136	GND
137	DP_LANE1+ / TMDS_LANE1+	138	DP_AUX+
139	DP_LANE1- / TMDS_LANE1-	140	DP_AUX-
141	GND	142	GND
143	DP_LANE2+ / TMDS_LANE0+	144	USB_SSRX1-
145	DP_LANE2- / TMDS_LANE0-	146	USB_SSRX1+
147	GND	148	GND
149	DP_LANE0+ / TMDS_LANE2+	150	HDMI_CTRL_DAT
151	DP_LANE0- / TMDS_LANE2-	152	HDMI_CTRL_CLK
153	HDMI_HPD#	154	DP_HPD#
155	PCIE_CLK_REF+	156	PCIE_WAKE#
157	PCIE_CLK_REF-	158	PCIE_RST#
159	GND	160	GND
161	PCIE3_TX+	162	PCIE3_RX+
163	PCIE3_TX-	164	PCIE3_RX-
165	GND	166	GND
167	PCIE2_TX+	168	PCIE2_RX+
169	PCIE2_TX-	170	PCIE2_RX-
171	UART0_TX	172	UART0_RTS#
173	PCIE1_TX+	174	PCIE1_RX+
175	PCIE1_TX-	176	PCIE1_RX-
177	UART0_RX	178	UART0_CTS#
179	PCIE0_TX+	180	PCIE0_RX+

Pin	Signal (Bottom side row)	No	Signal (Top side row)
181	PCIE0_TX-	182	PCIE0_RX-
183	GND	184	GND
185	LPC_AD0 / GPIO0	186	LPC_AD1 / GPIO1
187	LPC_AD2 / GPIO2	188	LPC_AD3 / GPIO3
189	LPC_CLK / GPIO4	190	LPC_FRAME# / GPIO5
191	SERIRQ / GPIO6	192	LPC_LDRQ# / GPIO7
193	VCC_RTC	194	SPKR / GP_PWM_OUT2
195	FAN_TACHOIN / GP_TIMER_IN	196	FAN_PWMOUT / GP_PWM_OUT1
197	GND	198	GND
199	SPI_MOSI	200	SPI_CS0#
201	SPI_MISO	202	SPI_CS1#
203	SPI_SCK	204	MFG_NC4
205	VCC_5V_SB	206	VCC_5V_SB
207	MFG_NC0	208	MFG_NC2
209	MFG_NC1	210	MFG_NC3
211	NC	212	NC
213	NC	214	NC
215	NC	216	NC
217	NC	218	NC
219	VCC	220	VCC
221	VCC	222	VCC
223	VCC	224	VCC
225	VCC	226	VCC
227	VCC	228	VCC
229	VCC	230	VCC

9/ uEFI BIOS

9.1. Staring the uEFI BIOS

The Qseven-Q7AL uses a Kontron-customized, pre-installed and configured version of Aptio ® V uEFI BIOS 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 Qseven-Q7AL.

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.

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

The uEFI BIOS QSEVENs 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.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <DEL> key.
4. If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Chapter 9.2.4 Security Setup Menu), press <RETURN>, and proceed with step 5.
5. A Setup menu appears.

The Qseven-Q7AL 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 16: 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

9.2. Setup Menus

The Setup utility features menus listed in the selection bar at the top of the screen are:

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

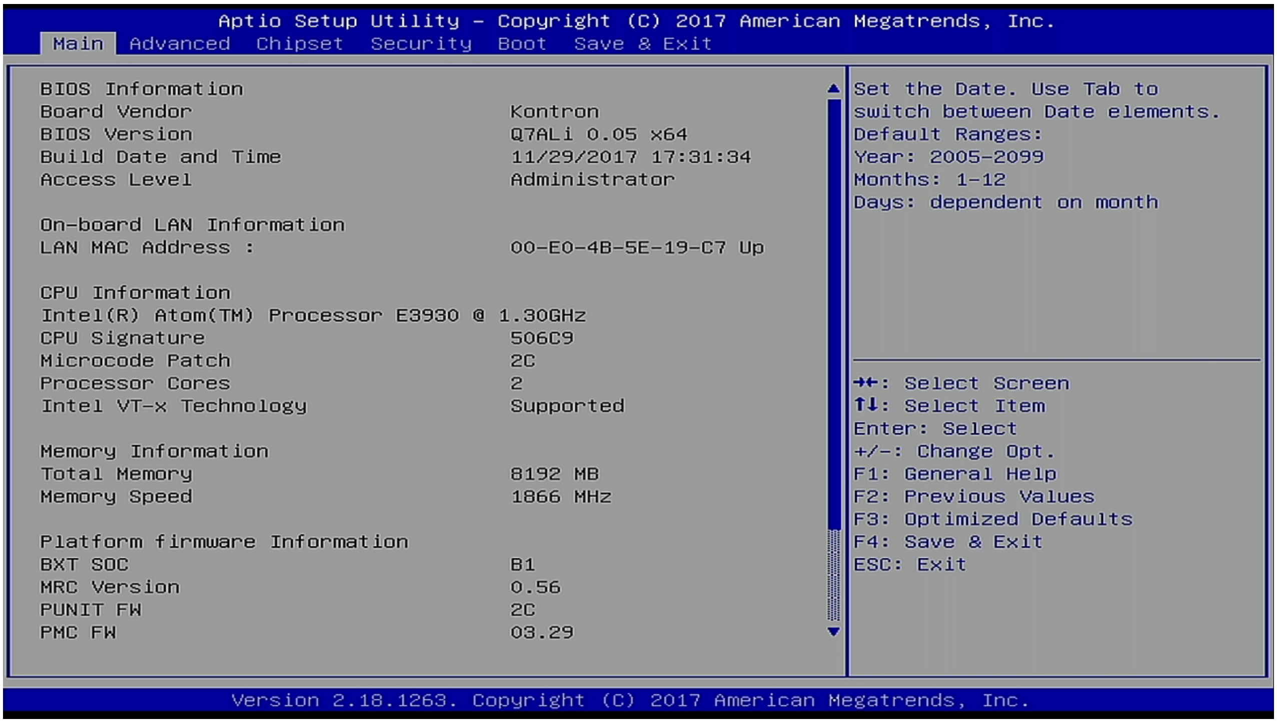
The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white. Use the left and right arrow keys to select the Setup menus.

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.

9.2.1. Main Setup Menu

On entering the uEFI BIOS, the setup program displays the Main Setup menu. This screen lists the Main Setup menu sub-screens and provides basic system information as well as functions for setting the system language, time and date.

Figure 13: Main Setup Menu Initial Screen

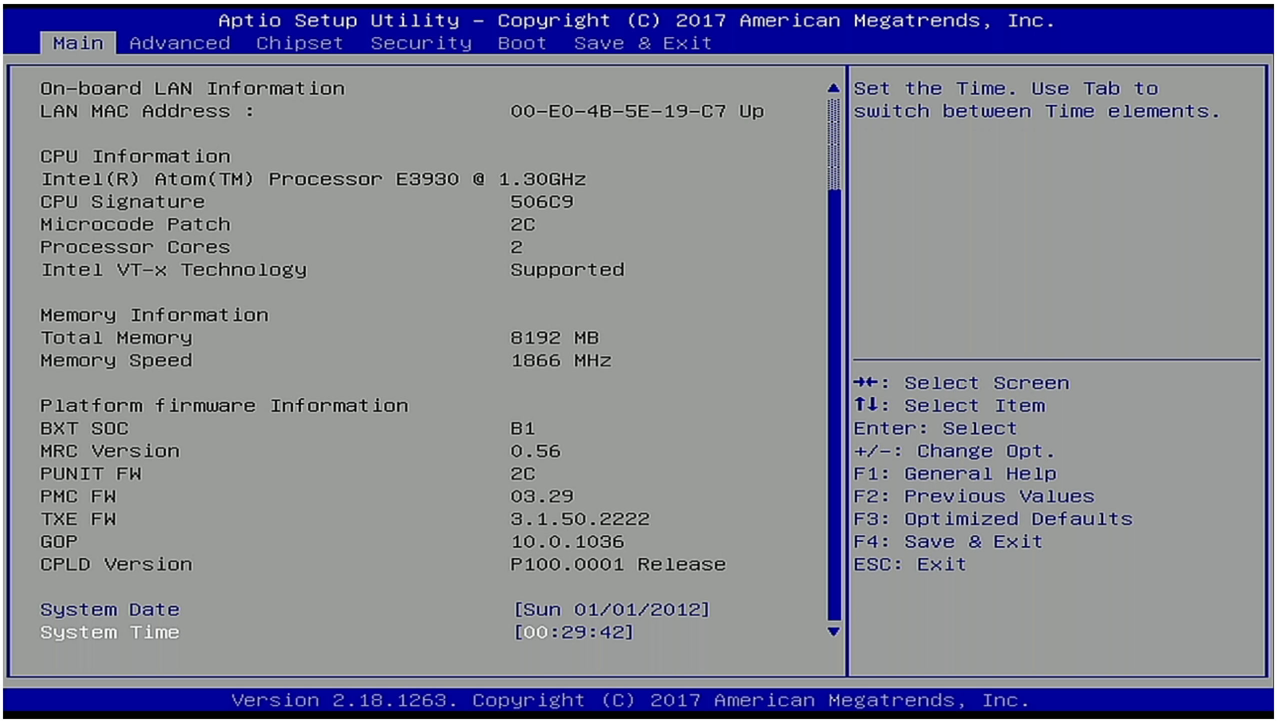


```
          Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

  BIOS Information                                        Set the Date. Use Tab to
  Board Vendor                    Kontron                 switch between Date elements.
  BIOS Version                    Q7ALi 0.05 x64          Default Ranges:
  Build Date and Time             11/29/2017 17:31:34     Year: 2005-2099
  Access Level                    Administrator           Months: 1-12
                                                          Days: dependent on month
  On-board LAN Information
  LAN MAC Address :               00-E0-4B-5E-19-C7 Up

  CPU Information
  Intel(R) Atom(TM) Processor E3930 @ 1.30GHz
  CPU Signature                   506C9
  Microcode Patch                 2C
  Processor Cores                 2                       →←: Select Screen
  Intel VT-x Technology           Supported               ↑↓: Select Item
                                                          Enter: Select
  Memory Information                                      +/-: Change Opt.
  Total Memory                    8192 MB                 F1: General Help
  Memory Speed                    1866 MHz                F2: Previous Values
                                                          F3: Optimized Defaults
  Platform firmware Information                           F4: Save & Exit
  BXT SOC                         B1                      ESC: Exit
  MRC Version                     0.56
  PUNIT FW                        2C
  PMC FW                          03.29

          Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```



```
           Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
  Main  Advanced  Chipset  Security  Boot  Save & Exit

  On-board LAN Information                              Set the Time. Use Tab to
  LAN MAC Address :                00-E0-4B-5E-19-C7 Up  switch between Time elements.

  CPU Information
  Intel(R) Atom(TM) Processor E3930 @ 1.30GHz
  CPU Signature                    506C9
  Microcode Patch                  2C
  Processor Cores                  2
  Intel VT-x Technology            Supported

  Memory Information
  Total Memory                     8192 MB
  Memory Speed                     1866 MHz
                                                        →←: Select Screen
  Platform firmware Information                         ↑↓: Select Item
  BXT SOC                          B1                   Enter: Select
  MRC Version                      0.56                 +/-: Change Opt.
  PUNIT FW                         2C                   F1: General Help
  PMC FW                           03.29                F2: Previous Values
  TXE FW                           3.1.50.2222          F3: Optimized Defaults
  GOP                              10.0.1036            F4: Save & Exit
  CPLD Version                     P100.0001 Release    ESC: Exit

  System Date                      [Sun 01/01/2012]
  System Time                      [00:29:42]

           Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Main Menu sub-screens and functions and describes the content.

Table 17: Main Setup Menu Sub-screens and Functions

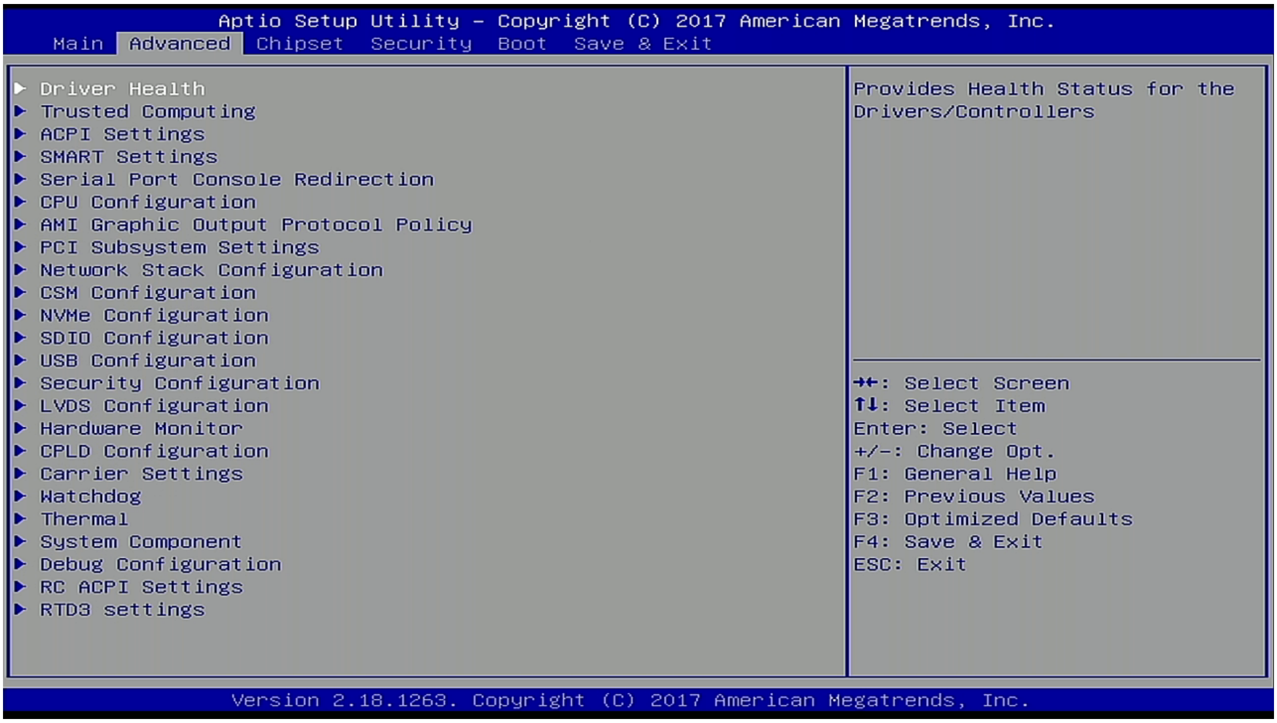
Sub-Screen	Description
BIOS Information>	Read only field BIOS vendor, Core version, Compliancy, Project version, Build date and time, and Access level
Onboard LAN Information>	Read only field LAN MAC Address **Additional information for MAC Address** The MAC address entry is the value used by the Ethernet 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).
CPU Information>	Read only field Processor Type, CPU signature, Microcode patch, CPU Speed, processor Core, intel VT-x technology
Memory Information>	Read only field Total memory and Memory speed
Platform Firmware Information>	Read only field *Module Information* BXT SOC, MRC Version, PUNIT FW, PMC FW, TXE FW, GOP, and CPLD rev
System Date>	Displays the system date [Week day mm/dd/yyyy]
System Time>	Displays the system time [hh:mm:ss]

9.2.2. Advanced Setup Menu

The Advanced Setup menu displays sub-screens and second level sub-screens with functions, for advanced configurations.

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

Figure 14: Advanced Setup Menu Initial Screen



```
        Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

 ▶ Driver Health                                  Provides Health Status for the
 ▶ Trusted Computing                              Drivers/Controllers
 ▶ ACPI Settings
 ▶ SMART Settings
 ▶ Serial Port Console Redirection
 ▶ CPU Configuration
 ▶ AMI Graphic Output Protocol Policy
 ▶ PCI Subsystem Settings
 ▶ Network Stack Configuration
 ▶ CSM Configuration
 ▶ NVMe Configuration
 ▶ SDIO Configuration
 ▶ USB Configuration
 ▶ Security Configuration                         →←: Select Screen
 ▶ LVDS Configuration                             ↑↓: Select Item
 ▶ Hardware Monitor                               Enter: Select
 ▶ CPLD Configuration                             +/-: Change Opt.
 ▶ Carrier Settings                               F1: General Help
 ▶ Watchdog                                       F2: Previous Values
 ▶ Thermal                                        F3: Optimized Defaults
 ▶ System Component                               F4: Save & Exit
 ▶ Debug Configuration                            ESC: Exit
 ▶ RC ACPI Settings
 ▶ RTD3 settings

            Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the Advanced sub-screens and functions and describes the content. Default settings are in **bold** and for some functions, additional information is included.

Table 18: Advanced Setup menu Sub-screens and Functions

Sub-Screen	Function	Second level Sub-Screen / Description
Driver Health>	Read only Information Provides Health Status for the Drivers/Controllers	
Trusted Computing>	Read only Information TPM20 device Found, Vendor and Firmware version	
	Security Device Support>	Enables or disables BIOS support for security device Operating System will not show security device, and TCG EFI protocol and INT1A interface are not available. [**Enabled**, Disabled]
	Active PCR Banks>	Read only field Displays active PCR Banks
	Available PCR Banks>	Read only field Displays available PCR Banks
	SHA-1 PCR Bank>	SHA-1 PCR Bank [**Enabled**, Disabled]

Sub-Screen	Function	Second level Sub-Screen / Description
Trusted Computing> (continued)	SHA256 PCR Bank>	SHA256 PCR Bank [**Enabled**, Disabled]
	Pending Operation>	Schedules an operation for security device Note: Computer reboots on restart 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: is compatible mode for Win8/Win10 and TCG_2: supports TCG2 protocol and event format Win 10 or later. [TCG_1_2, **TCG_2**]
	Physical Presence Spec Version>	Select to inform 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
	Device Select>	Selects BIOS support for security devices. Auto: supports both TPM 1.2 and TPM 2.0 TPM 1.2: restricts support to TPM 1.2 devices TPM 2.0: restricts support to TPM 2.0 devices [TPM 1.2, TPM 2.0, **Auto**]
ACPI Settings>	Enable ACPI Auto Configuration>	Enables or disables BIOS 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]
	ACPI Sleep State>	Selects highest ACPI sleep state the system enters when the SUSPEND button is pressed [Suspend Disabled, **S3 Suspend to Ram**]
	Lock Legacy Resources>	Lock of legacy resources [Enabled, **Disabled**]
SMART Settings>	SMART Self Test>	Run SMART Self Test on all HDDs during POST [Enabled, **Disabled**]
Serial Port Console Redirection>	COM0 Console Redirection>	Console redirection via QSEVEN module's COM1 [Enabled, **Disabled**]
	COM1 Console Redirection>	Console redirection via QSEVEN module's COM2 [Enabled, **Disabled**]
	COM2 Console Redirection>	Console redirection via QSEVEN module's COM3 [Enabled, **Disabled**]
	COM3 Console Redirection>	Console redirection via QSEVEN module's COM4 [Enabled, **Disabled**]

Sub-Screen	Function	Second level Sub-Screen / Description	
Serial Port Console Redirection> (continued)	**Additional Information COM # Console** If redirection is enabled then the port settings such as Terminal type, Bits per second, Data bits, Parity etc. can be adjusted here. On-module COM ports do not support flow control. If the Port is disabled, the COM# port is displayed as a read only field.		
	Legacy Console Redirection settings>	Legacy Serial Redirection Port>	Selects a COM port to display redirection of legacy OS and legacy OPROM messages [**COM0**, COM1, COM2, COM3]
	Serial Port for Out-of-Band Management / Windows EMS Console Redir.>	Console redirection [Enabled, **Disabled**]	
CPU Configuration>	Turbo Mode>	Enables or disables processor turbo mode Note: EMTTM must also be enabled. Auto means enabled unless the max. turbo ratio is bigger than 16-SKL A0 W/A. [**Enabled**, Disabled]	
	Intel (VME) Virtual Technology>	Enables VMM to utilize additional hardware capabilities provided by Vanderpool Technology [**Enabled**, Disabled]	
	VT-d>	CPU VT-d [Enabled, **Disabled**]	
	Monitor Mwait>	Monitor Mwait [Enabled, **Disabled**, Auto]	
AMI Graphic Output Protocol Policy>	Read only field AMI Graphic driver version		
	Output Select>		
PCI Subsystem Settings>	Read only field AMI PCI driver version		
	Above 4G Decoding>	64 bit capable devices to be decoded in above 4G address space [Enabled, **Disabled**]	
	Hot-Plug Support>	Hot-Plug support for the entire system [**Enabled**, Disabled]	
Network Stack Configuration>	Network Stack>	UEFI Network Stack [Enabled, **Disabled**]	
Compatibility Support Module (CSM) Configuration	CSM Support>	CSM Support [Enabled, **Disabled**]	
NVMe Configuration>	Read only field NVMe controller and driver version		
SDIO Configuration>	SDIO Access Mode>	Auto Option: Access SD device in DMA mode if controller supports it, otherwise in PIO mode. DMA option: Access SD device in DMA mode. PIO Option: Access SD device in PIO mode. [**Auto**, ADMA, SDMA, PIO]	
	Mass storage devices>	Mass storage device emulation type. [**Auto**, Floppy, Forced FDD, Hard Disk]	

Sub-Screen	Function	Second level Sub-Screen / Description
USB Configuration>	Read only fields USB Configuration, UBS module Version, USB controllers, and USB devices	
	Legacy USB Support>	Enable- supports legacy USB Auto– disables legacy support, if no USB devices are connected Disable-keeps USB devices available for EFI applications only [**Enabled**, Disabled, Auto]
	XHCI Hand-off>	XHCI ownership change 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 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>	Displays maximum time taken for the device to report itself to the host properly. Auto uses the default :root port 100 ms /hub port delay is taken from hub port descriptor. [**Auto**, Manual]
	Mass Storage Devices>	Mass storage device emulation type [**Auto**, Floppy, Forced FDD, Hard Disk, CD-ROM]
Security Configuration>	TXE HMRFPO>	TXE HMRFPO [Enabled, **Disabled]**
	TXE EOP Message>	Send EOP Message before enter OS [**Enabled,** Disabled]
LVDS Configuration>	LVDS Flat Panel Display Support>	Enables or disables the LVDS Flat Panel Display Support [Enabled, **Disabled]**
Hardware Monitor>	CPU Temperature>	Read only field CPU temperature (°C)
	PCB Temperature>	Read only field PCB temperature (°C)
	Module Temperature>	Read only field Module temperature (°C)
	Module Voltage>	Read only field Module voltage (V)
	RTC Voltage>	Read only field RTC Voltage (V)
	DDR Voltage>	Read only field DDR Voltage (V)
	Input Voltage>	Read only field Input Voltage (V)
	System Fan – Fan Pulse>	Displays number of pulses the fan produces during one revolution. (Range: 1-4)
	System Fan - Control Mode>	Sets System Fan Control mode [Manual, SMART FAN IV]

Sub-Screen	Function	Second level Sub-Screen / Description
Hardware Monitor> (continued)	System Fan – Fan Trip Point>	Displays temperature at which the fan accelerates. (Range: 20°C – 80°C)
	System Fan – Trip Point Speed>	Displays Fan speed at trip point in %. Minimum value is 30 %. Fan always runs at 100 % at (TJmax.-10°C).
CPLD Configuration>	Serial Port 0>	Enables or disables the LVDS Flat Panel Display Support [**Enabled**, Disabled]
	Base Address>	Configure Serial Port Base Address [3F8, 2F8, **3E8**, 2E8]
	IRQ>	Configure Serial Port IRQ [7, 9, **10**, 11, 12, 13, 15]
	GPIO IRQ>	Configure IRQ for GPIO pins [Disabled, 9, 10, 11, 12, 13, 15]
	I2C IRQ>	Configure IRQ for I2C Controller [Disabled, 9, 10, 11, 12, 13, 15]
	Audio Codec Mux Select>	Mux select for Audio Codec type on Carrier Board [Mux to I2S Codec, Mux to HDA Codec]
	GPIO-LPC Mux Select>	MUX select for pin as GPIO or LPC Bus to pass through to carrier board [Mux to LPC, Mux to GPIO]
	GPO0 Mux Select>	MUX select for the pin as GPIO or SUS_STAT [Mux to GPIO, Mux to SUS_STAT#]
Carrier Settings>	Carrier I2C0/SMBUS>	Switch to select which controller own the I2C_PM_CK & I2C_PM_DAT pins on Qseven connector [Use I2C0 Controller, Use SMBUS Controller]
	Lid Switch Mode>	Shows or hides Lid switch inside ACPI OS [**Enabled**, Disabled]
	Sleep Button Mode>	Shows or hides Sleep button inside ACPI OS [**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 the module is reset. [Enabled, **Disabled**]
	Stage 1 Mode>	Selects action for Watchdog stage 1 [**Disable**, Reset, NIM, SCI, Delay, WDT Signal only]
Thermal>	Automatic Thermal Reporting>	Configure _CRT, _PSV and _AC0 automatically based on values recommended in BWG's Thermal Reporting [Enabled, **Disabled**]
	Critical Trip Point>	Configure temperature value of the ACPI Critical Trip Point – point which OS will shut the system off. [15°C, 23°C, 31°C, 39°C, 47°C, 55°C, 63°C, 71°C, 79°C, 87°C, 95°C, 100°C, 103°C, 110°C, 119°C, **125°C**]
	Passive Trip Point>	Configure temperature value of the ACPI Passive Trip Point – point which OS will begin throttling the processor. [Disable, 15°C, 23°C, 31°C, 39°C, 47°C, 55°C, 63°C, 71°C, 79°C, 87°C, **95°C**, 103°C, 111°C]
	Passive TC1 Value>	Sets the TC1 value for the ACPI Passive Cooling Formula. (Range: 1 – 6)

Sub-Screen	Function	Second level Sub-Screen / Description
Thermal> (continued)	Passive TC2 Value>	Sets TC2 value for the ACPI Passive Cooling Formula.(Range: 1 – 16)
	Passive TSP Value>	Sets TSP value for the ACPI Passive Cooling Formula.(Range: 2 – 32)
System Component>	OS Reset Selet>	Select the reset type in FACP table [Warm Reset, **Cold Reset**]
	Spread Spectrum Clocking Configuration (SSC)	
	DDR SSC>	Enable DDR SSC [**Enable**, Disable]
	DDR SSC Selection Table>	Select the item in SSC selection table for DDR spread spectrum [0% (No SSC), -0.1%, -0.2%, -0.3%, -0.4%, **-0.5%**,]
	DDR Clock Bending Selection Table>	Select Clock Bending [1.3%, 0.6%, **0% (No Clock Bending)**, -0.9%]
	HighSpeed SerialIO SSC>	Enable HighSpeed SerialIO SSC configuration [**Enable**, Disable]
	HighSpeed SerialIO SSC Selection T>	Select the item in SSC selection table for HighSpeed SerialIO spread spectrum [0% (No SSC), -0.1%, -0.2%, -0.3%, -0.4%, **-0.5%**,]
Debug Configuration>	Kernel Debugger Enable>	Enable or disable support for a kernel debugger [Enable, **Disable**]
	APEI BERT>	Enable or disable APEI BERT [**Enable**, Disable]
	ACPI Memory Debug>	Enable or disable ACPI Memory Debug [Enable, **Disable**]
	End Of Post (TXE Debug)>	Disable to stop BIOS from sending End of Post Message [**Enabled**, Disabled]
	Lock Directory (TXE Debug)>	Enable BIOS to lock SETUP variable after end of post [Enabled, **Disabled**]
	Suppress PTT Commands>	Bypass TPM2 commands submitting to PTT FW [Enabled, **Disabled**]
	TDO GPIO Pin>	If select Auto, TDO will be disabled for A0 silicon only. For other steppings, TDO will be enabled. [Enable, Disable, Auto]
	Max Memory 2G>	Set Maximum Memory Size to 2 GB [Enable, **Disable**]
	Persistent RAM size>	Specify the amount of main memory to be reserved for Pram. [4MB, 16MB, 64MB, **Disable**]
	OS DnX focus entry>	Enable OS Dnx [Enable, **Disable**]
	Processor Trace Memory Allocation>	Disable or Select Processor trace memory region size : from 4 KB to 128 MB [**Disabled**, 4KB, 8KB, 16KB, 32KB, 64KB, 128KB, 256KB, 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB, 128MB]
	CSE Data Clear>	Data Clear is for reset/clearing of the CSE data region
RC ACPI Setting>	Native PCIE Enable>	Enable or disable PCI Express Native Control in Windows [**Enable**, Disable]

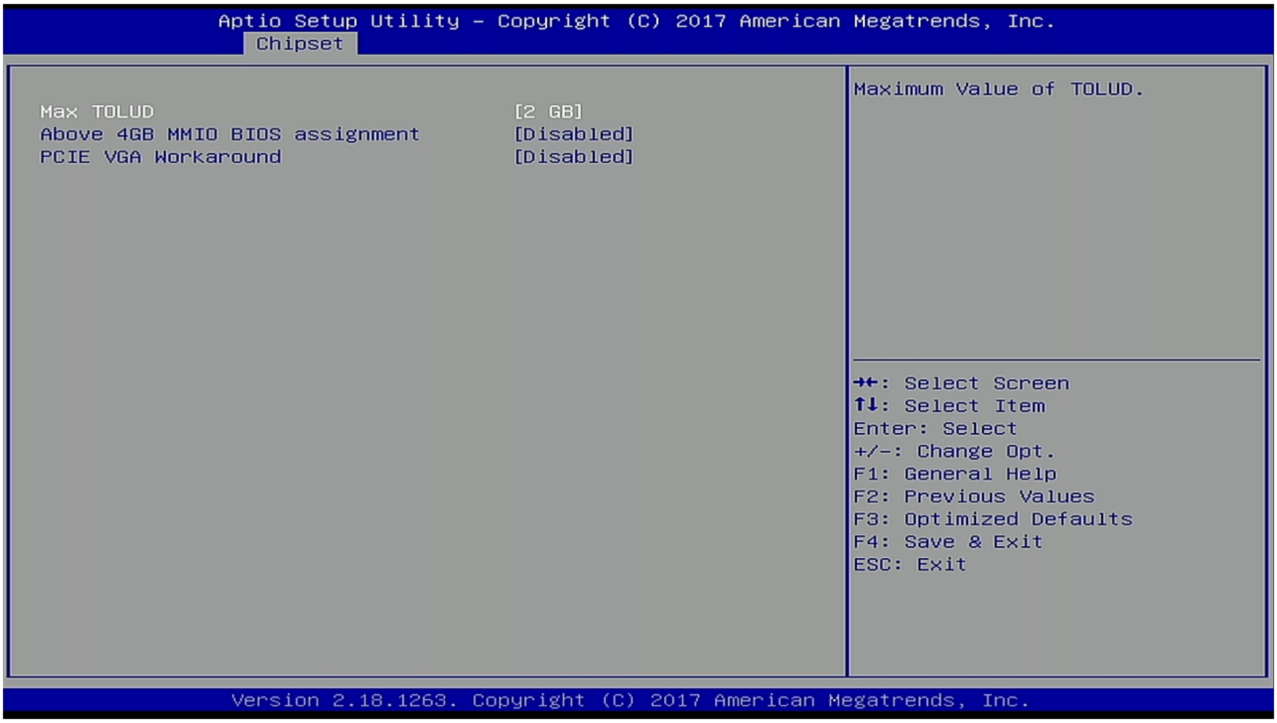
Sub-Screen	Function	Second level Sub-Screen / Description
RC ACPI Setting> (continued)	Native ASPM>	On enable, windows will control the ASPM support for the device. If disabled, the BIOS will [**Enable**, Disable]
RTD3 Settings>	RTD3 Support>	Enable or disable Runtime D3 support [Enabled, **Disabled**]

9.2.3. Chipset Setup Menu

On entering the Chipset Setup menu, the screen lists four sub-screen options North bridge, South bridge, Uncore Configuration and South Cluster Configuration.

9.2.3.1. Chipset> North Bridge

Figure 15: Chipset > North Bridge Menu Initial Screen



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Chipset

Max TOLUD                                [2 GB]          Maximum Value of TOLUD.
Above 4GB MMIO BIOS assignment           [Disabled]
PCIE VGA Workaround                      [Disabled]

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

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

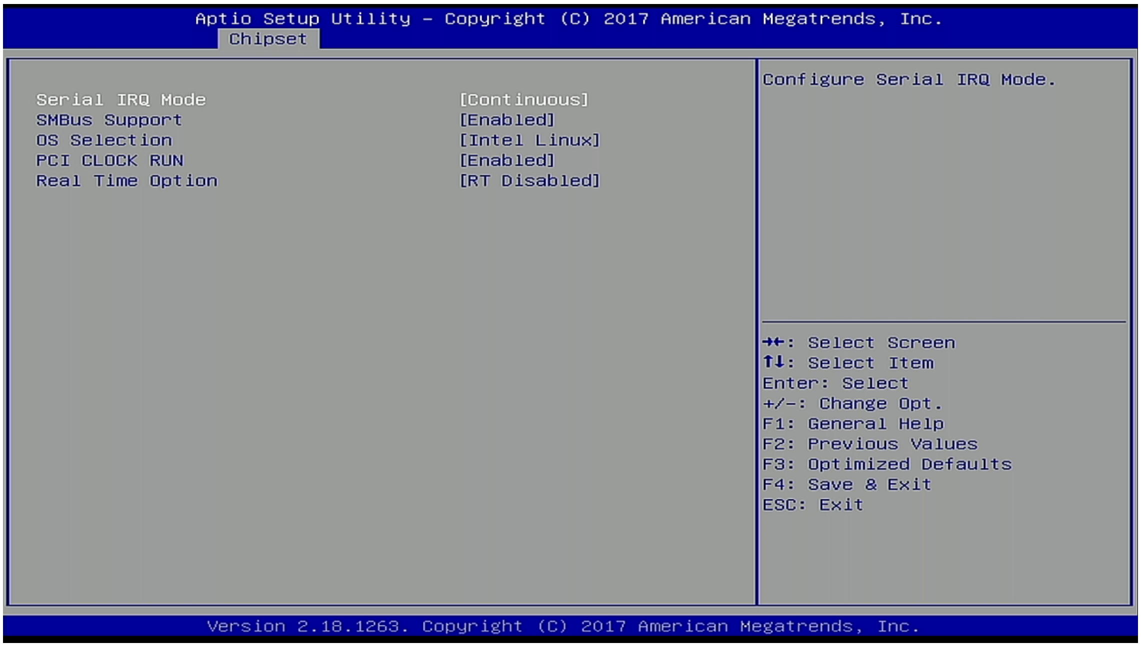
The following table shows the North bridge sub-screens and functions and describes the content. Default settings are in **bold**.

Table 19: Chipset Set > North Bridge Sub-screens and Function

Function	Second level Sub-Screen / Description	
Memory Configuration>	Max TOLUD>	Sets the maximum TOLUD value. Dynamic assignment adjusts TOLUD automatically, based on largest MMIO length of the installed graphic controller. [**2 GB**, 2.25 GB, 2.5 GB, 2,75 GB, 3 GB]
	Above 4GB MMIO BIOS Assignment>	Enables or disables above 4 GB memorymappedIO BIOS assignment. This is disabled automatically when aperture size is set to 2048 MB. [Enabled, **Disabled**]
	PCIE VGA Workaround>	Enable If PCIe card cannot boot in DOS. For test purposes only. [Enabled, **Disabled**]

9.2.3.2. Chipset > South Bridge

Figure 16: Chipset>South Bridge Menu Initial Screen



```
Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Chipset

Serial IRQ Mode                         [Continuous]      Configure Serial IRQ Mode.
SMBus Support                           [Enabled]
OS Selection                            [Intel Linux]
PCI CLOCK RUN                           [Enabled]
Real Time Option                        [RT Disabled]

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

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

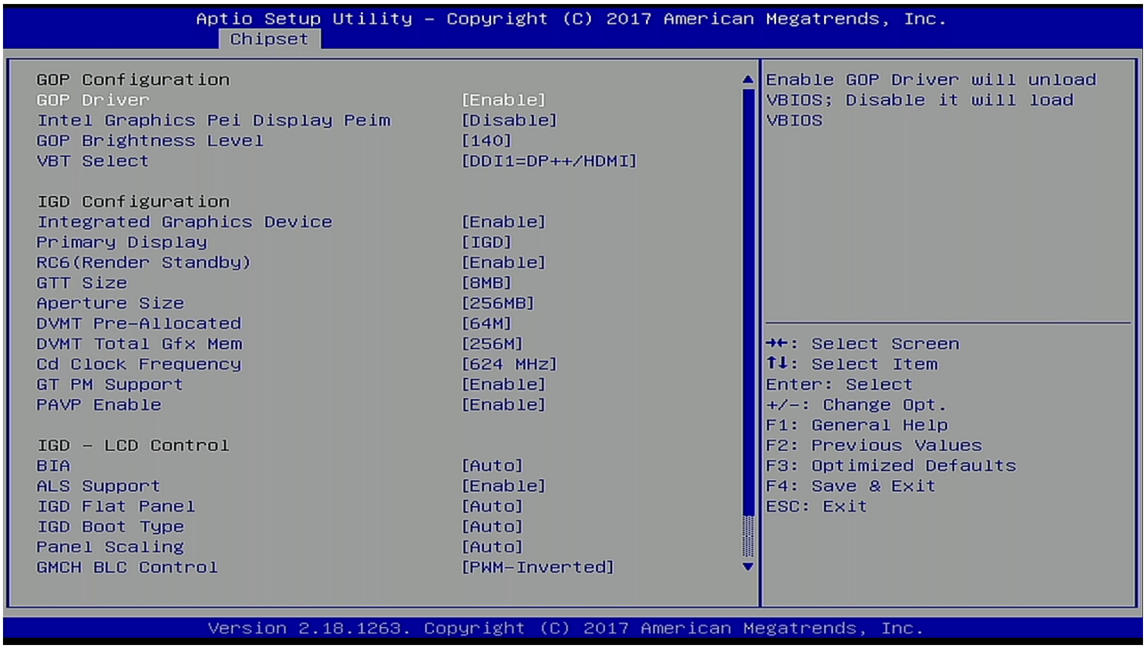
The following table shows the South Bridge sub-screens and functions, and describes the content. Default settings are in **bold**.

Table 20: Chipset Set> South Bridge Sub-screens and Functions

Function	Second level Sub-Screen / Description
Serial IRQ Mode>	Configure Serial IRQ Mode [Quiet, **Continuous**]
SMBus Support>	Enable or disable SMBus Support [**Enabled**, Disabled]
OS Selection>	Selects target OS. [Windows 10 (Ver>=1607), **Intel Linux**]
PCI Clock Run>	Enables CLKRUN# logic to stop PCI clocks [**Enabled**, Disabled]
Real Time Option>	Select Read-Time Enable and IDI Agent Real-Time Traffic Mask Bits [**RT Disabled**, RT Enabled (Agent IDI1), RT Enabled (Agent Disabled)]

9.2.3.3. Chipset> Uncore Configuration

Figure 17: Chipset>Uncore Configuration Menu Initial Screens

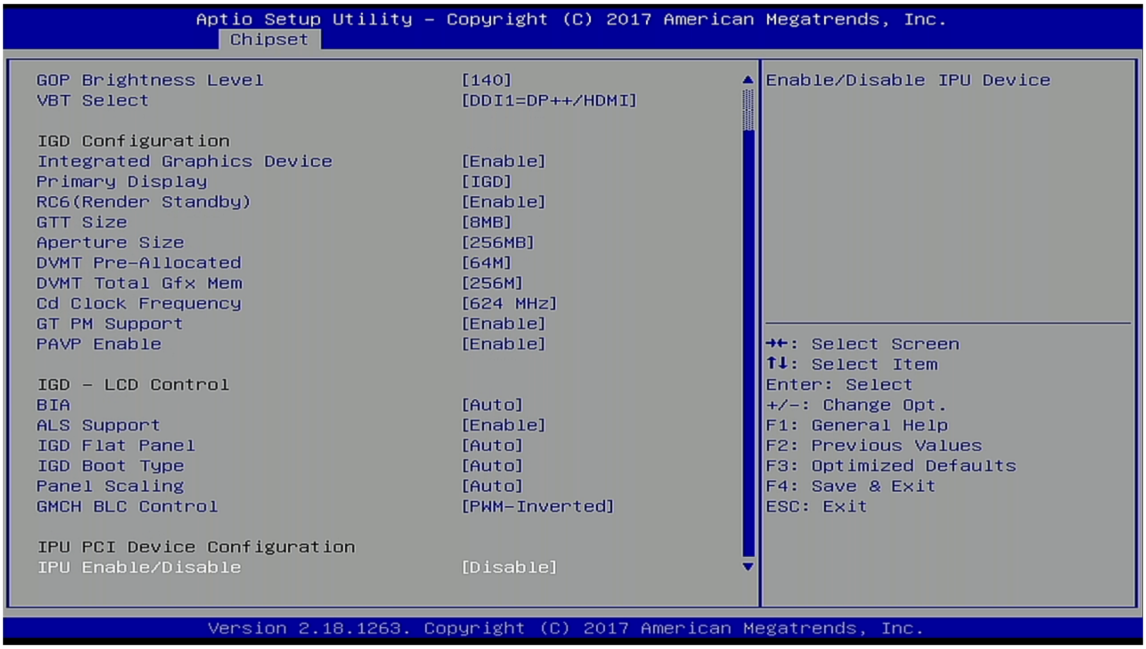


```
            Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
              Chipset

  GOP Configuration                                      Enable GOP Driver will unload
  GOP Driver                      [Enable]               VBIOS; Disable it will load
  Intel Graphics Pei Display Peim [Disable]              VBIOS
  GOP Brightness Level            [140]
  VBT Select                      [DDI1=DP++/HDMI]

  IGD Configuration
  Integrated Graphics Device      [Enable]
  Primary Display                 [IGD]
  RC6(Render Standby)             [Enable]
  GTT Size                        [8MB]
  Aperture Size                   [256MB]
  DVMT Pre-Allocated              [64M]
  DVMT Total Gfx Mem              [256M]                 →←: Select Screen
  Cd Clock Frequency              [624 MHz]              ↑↓: Select Item
  GT PM Support                   [Enable]               Enter: Select
  PAVP Enable                     [Enable]               +/-: Change Opt.
                                                         F1: General Help
  IGD - LCD Control                                      F2: Previous Values
  BIA                             [Auto]                 F3: Optimized Defaults
  ALS Support                     [Enable]               F4: Save & Exit
  IGD Flat Panel                  [Auto]                 ESC: Exit
  IGD Boot Type                   [Auto]
  Panel Scaling                   [Auto]
  GMCH BLC Control                [PWM-Inverted]

            Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```



```
            Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
              Chipset

  GOP Brightness Level            [140]                  Enable/Disable IPU Device
  VBT Select                      [DDI1=DP++/HDMI]

  IGD Configuration
  Integrated Graphics Device      [Enable]
  Primary Display                 [IGD]
  RC6(Render Standby)             [Enable]
  GTT Size                        [8MB]
  Aperture Size                   [256MB]
  DVMT Pre-Allocated              [64M]
  DVMT Total Gfx Mem              [256M]
  Cd Clock Frequency              [624 MHz]
  GT PM Support                   [Enable]
  PAVP Enable                     [Enable]               →←: Select Screen
                                                         ↑↓: Select Item
  IGD - LCD Control                                      Enter: Select
  BIA                             [Auto]                 +/-: Change Opt.
  ALS Support                     [Enable]               F1: General Help
  IGD Flat Panel                  [Auto]                 F2: Previous Values
  IGD Boot Type                   [Auto]                 F3: Optimized Defaults
  Panel Scaling                   [Auto]                 F4: Save & Exit
  GMCH BLC Control                [PWM-Inverted]         ESC: Exit

  IPU PCI Device Configuration
  IPU Enable/Disable              [Disable]

            Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

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

Table 21: Chipset Set> Uncore Configuration Sub-screens and Functions

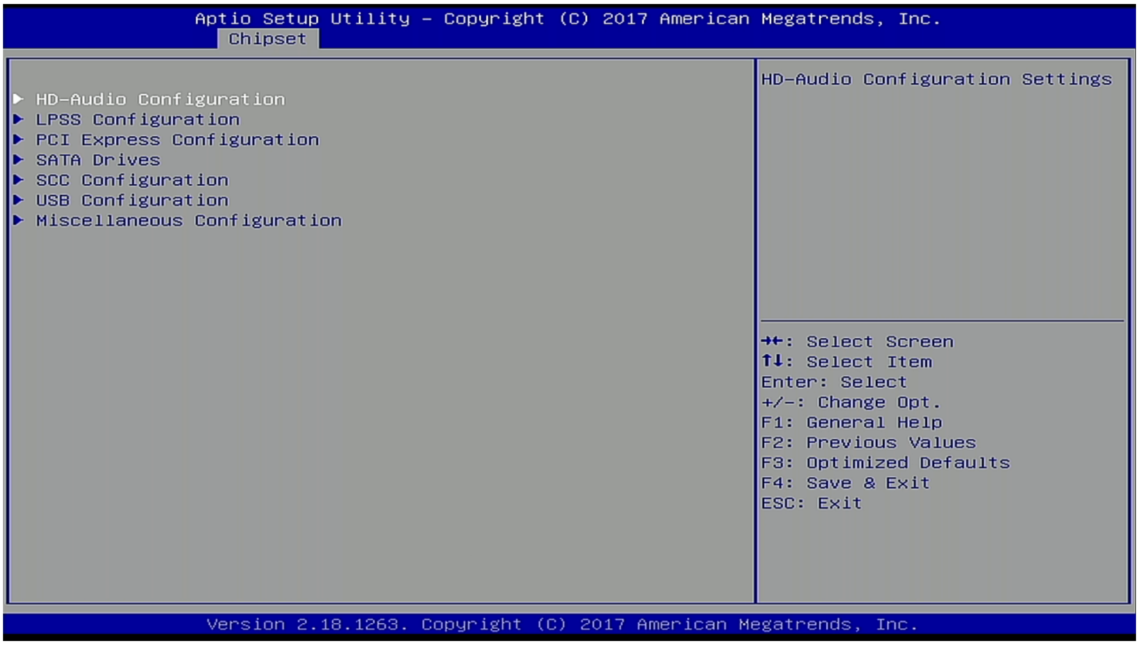
Function	Second level Sub-Screen / Description
GOP Driver>	Enable GOP Driver will unload VBIOS; Disable it will load VBIOS [**Enabled**, Disabled]

Function	Second level Sub-Screen / Description
Intel Graphics Pei Display Peim>	Enable or disable Pei (Early) Display [Enabled, **Disabled**]
GOP Brightness Level>	Set GOP Brightness Level; (Range: 0 – 255) [20, 40, 60, 80, 100, 120, **140**, 160, 180, 200, 220, 240, 255]
VBT Select>	Select VBT for GOP Driver [DDI1=DP++/HDMI, DDI1=HDMI]
Integrated Graphics Device (IGD)>	Enable: Enable IGD when selected as the Primary Video Adaptor; Disable: Always disable IGD [**Enabled**, Disabled]
Primary Display>	Select which of IGD/PCI Graphics device should be Primary Display [**IGD**, PCIe, HG]
RC6 (render Standby)>	Check to enable render standby support. IF S0ix is enabled, RC6 should be enabled. This function is read only if S0ix is enabled. [**Enabled**, Disabled]
GTT Size>	Selects the GTT size [2 MB, 4 MB, **8 MB**]
Aperature Size>	Selects the aperture size [128 MB, **256 MB**, 512 MB]
DVMT Pre-Allocated>	Selects DVMT 5.0 pre-allocated (fixed) graphics memory size used by Internal graphics [**64 M**, 96 M, 128 M, 160 M, 192 M, 224 M, 256 M, 288 M, 320 M, 352 M 384 M, 416 M, 448 M, 480M, 512 M]
DVMT Total Gfx Mem>	Selects DVMT 5.0 total graphics memory size used by internal graphics device [128 M, **256 M**, MAX]
Cd Clock Frequency>	Selects the highest Cd clock frequency supported by the platform [144 MHz, 288 MHz, 384 MHz, 576 MHz, **624 MHz**]
GT PM Support>	GT PM Support [**Enabled**, Disabled]
PAVP Enable>	PAVP [**Enabled**, Disabled]
BIA>	Auto: GMCH uses VBIOS default Level n: is enabled with selected aggressiveness level [**Auto**, Disabled, Level 1, Level 2, Level 3, Level 4, Level5]
ALS Support>	Valid only for ACPI [**Enable**, Disable]
IGD Flat Panel>	[**Auto**, 640x480, 800x600, 1024x768, 1280x1024, 1366x768, 1680x1050, 1920x1200, 1280x800]
IGD Boot Type>	Select preference for IGD display interface used when system boots. [**Auto**, VGA port, HDMI, DP Port B, Dp Port C, eDP, DSI Prt A, DSI Port C]
Panel Scaling>	Sets Panel scaling [**Auto**, Centering, Stretching]
GMCH BLC Control>	Backlight control settings [**PWM-Inverted**, GMBus-Inverted, PWM-Normal, GMBus-Normal]

Function	Second level Sub-Screen / Description
IPU Enable/Disable>	IPU Device [Enable, **Disable**]

9.2.3.4. Chipset> South Cluster Configuration

Figure 18: Chipset>South Cluster Configuration Menu Initial Screen



```
              Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
                      Chipset

▶ HD-Audio Configuration                                       HD-Audio Configuration Settings
▶ LPSS Configuration
▶ PCI Express Configuration
▶ SATA Drives
▶ SCC Configuration
▶ USB Configuration
▶ Miscellaneous Configuration

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

               Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

The following table shows the South Cluster Configuration sub-screens and functions and describes the content. Default settings are in **bold** and for some functions, additional information is included.

Table 22: Chipset>South Cluster Configuration Sub-screens and Functions

Function	Second level Sub-Screen / Description	
HD Audio Configuration>	HD-Audio Support>	HD-Audio support [**Enable**, Disable]
	HD-Audio DSP>	HD-Audio DSP [**Enable**, Disable]
	Audio DSP Feature Support:	
	Audio DSP Compliance Mode>	Sets DSP enabled system complaice: 1: Non_UAA (IntelSST driver support only – CC_040100) 2: UAA (HD Audio Inbox or IntelSST driver support – CC_040380) Note: NHLT (DMIC/BT/I2S configuration) is published for non-UAA only. [Non_UAA (IntelSST), **UAA (HD Inbox/IntelSST)**]
	WoV (Wake on Vocie)>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Bluetooth	DSP Feature.

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)	Sideband>	Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled]
	SRAM Reclaim>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled]
	BT Intel HFP>	DSP Feature./ Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [**Enabled**, Disabled] [**Enabled**, Disabled]
	BT Intel A2DP>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Context Aware>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)		[Enabled, **Disabled**]
	NHLT Endpoints Configuration:	
	DMIC>	Selects DMIC to expose in NHLT ACPI table [2 Mic Array, 4 Mic Array, **Disabled**]
	Bluetooth>	Enables/Disables Bluetooth Endpoint in NHLT ACPI table [Enabled, **Disabled**]
	I2S SKP>	Read only, **Enabled**
	I2S HP>	Read only, **Enabled**
	Codex based VAD>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	DSP based Speech Pre-Processing>	DSP Feature. Bitmask structure: [BIT0] – WoV [BIT1] – BT Sideband [BIT2] – Codec based VAD [BIT3] – SRAM Reclaim [BIT5] – BT Intel HFP [BIT6] – BT Intel A2DP [BIT9] – Context Aware [Enabled, **Disabled**]
	Voice Activity Detection>	Read only, **Intel Wake On Voice**
	Post-Processing Module Support:	
	Waves>	Enables/Disables 3rd Party Processing Module Support (identlfied by GUID). WoV must be enabled as a feature first to selecr relevent WoV IP. [Enabled, **Disabled**]
	DTS>	
	Spatial>	
	Dolby>	
	Samsung SoundAlive>	
	Samsung SoundBooster>	
	Samsung EQ/DRC>	
	ForteMedia SAMSoft>	

Function	Second level Sub-Screen / Description	
HD Audio Configuration> (continued)	Intel WoV>	Read only, **Disabled**
	Sensory WoV>	Read only, **Disabled**
	Conexant Pre-Process>	Enables/Disables 3rd Party Processing Module Support (identlfied by GUID). WoV must be enabled as a feature first to selecr relevent WoV IP. [Enabled, **Disabled**]
	Context Aware Pre-Process>	
	Custom Module 'Alpha'>	
	Custom Module 'Beta'>	
	Custom Module 'Gamma'>	
	HD-Audio CSME Memory Transfers>	Sets HD-Audio CSME memory transfers to VC0/VC2 [**VC0**, VC2]
	HD-Audio Host Memory Transfers>	Sets HD-Audio Host memory transfers to VC0/VC2 [**VC0**, VC2]
	HD-Audio I/O Buffer Ownership Select>	Sets HD-Audio I/O buffer ownership [**HD-Audio link owns all the I/O buffers**, I2S port owns all the I/O buffers]
	HD-Audio Clock Gating>	HD-Audio Clock gating [**Enabled**, Disabled]
	HD-Audio Power Gating>	HD-Audio Power gating [**Enabled**, Disabled]
	HD-Audio PME>	HD-Audio PME [**Enabled**, Disabled]
	HD-Audio Link Frequency>	Selects HD-Audio link frequency Applicable only if HDA codec supports selected frequency. [6 MHz, 12 MHz, **24 MHz**]
	iDisplay Link Frequency>	Selects iDisplay Link frequency Applicable only if iDisp codec supports selected frequency. [48 MHz, **96 MHz**]
LPSS Configuration>	LPSS I2C1 Support (D22:F1)>	LPSS I2C1 Support (I2C_CAM0) [**Enable**, Disable]
	LPSS I2C2 Support (D22:F2)>	LPSS I2C2 Support (I2C_CAM1) [**Enable**, Disable]
	LPSS I2C3 Support (D22:F3)>	LPSS I2C3 Support (I2C_GP) [**Enable**, Disable]
	LPSS I2C4 Support (D22:F0)>	LPSS I2C4 Support (I2C_LCD) [**Enable**, Disable]
	LPSS HSUART1 Support (D24:F1)>	LPSS HSUART1 Support [**Enable**, Disable]
	LPSS HSUART2	LPSS HSUART2 Support

Function	Second level Sub-Screen / Description		
LPSS Configuration> (continued)	Support (D24:F2)>	[**Enable**, Disable]	
	LPSS SPI0 Support (D25:F0)>	LPSS SPI0 Support [**Enable**, Disable]	
	LPSS IOSF PMCTL S0ix Enable>	LPSS IOSF Bridge PMCTL Register S0ix Bits [**Enable**, Disable]	
PCI Express Configuration>	PCI Express Clock Gating>	PCI Express clock gating for each root port [**Enabled**, Disabled]	
	Port8xh Decode>	PCI express port 8xh decode [Enabled, **Disabled**]	
	Peer Memory Write Enable>	Peer memory write [Enabled, **Disabled**]	
	Compliance Test Mode>	Enable when using compliance load board [Enabled, **Disabled**]	
	PCI Root Port 4 (GbE)> or PCI Root Port 5 (NC) or PCI Root Port 0 (QSEVEN PCIe#0)> or PCI Root Port 1 (QSEVEN PCIe#1)> or PCI Root Port 2 (QSEVEN PCIe#2)> or PCI Root Port 3 (QSEVEN PCIe#3)>	PCI Express Root Port[#]>	Controls the PCI Express port Auto automatically disables the unused root port for optimum power saving. [**Auto**,Enabled, Disabled]
		ASPM>	Active State Power Management (ASPM) level settings [**Disabled**, Auto, L0s, L1, L0sL1]
		L1 Substates>	PCI Express L1 substrates settings [Disabled, L1.1, L1.2, **L1.1 & L1.2**]
		ACS>	Access Control Service Extended Capability [**Enabled**, Disabled]
		URR>	PCI Express unsupported request reporting [Enabled, **Disabled**]
		FER>	PCI Express device fatal error reporting [Enabled, **Disabled**]
		NFER>	PCI Express device non-fatal error reporting [Enabled, **Disabled**]
		CER>	PCI Express device correctable error reporting [Enabled, **Disabled**]
		CTO>	PCI Express completion timer (T0) [**Default Setting**, 16-55 ms, 65-210 ms, 260-900 ms, 1-3.5 s, Disabled]
		SEFE>	Root PCI Express System Error on Fatal Error [Enabled, **Disabled**]
		SENFE>	Root PCI Express System Error on non-Fatal Error [Enabled, **Disabled**]
		SECE>	Root PCI Express System Error on correctable error

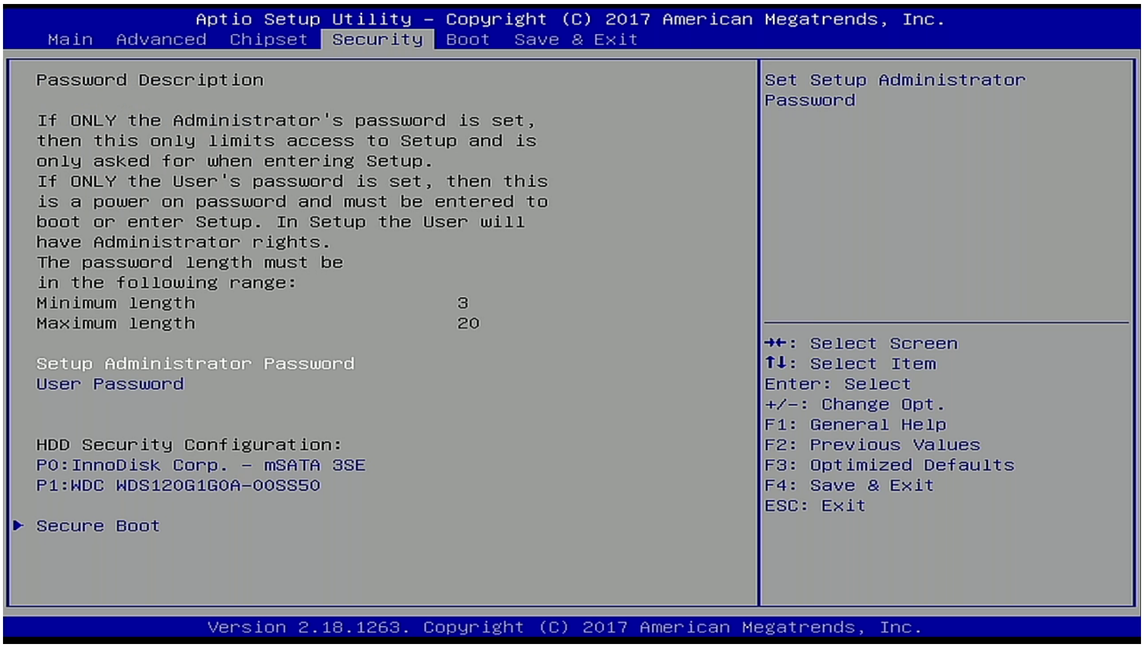
Function	Second level Sub-Screen / Description		
PCI Express Configuration> (contined)	PCI Root Port 4 (GbE)> or PCI Root Port 5 (NC) or PCI Root Port 0 (QSEVEN PCIe#0)> or PCI Root Port 1 (QSEVEN PCIe#1)> or PCI Root Port 2 (QSEVEN PCIe#2)> or PCI Root Port 3 (QSEVEN PCIe#3)> (continued)		[Enabled, **Disabled**]
		PME SCI>	PCI Express PME SCI [**Enabled**, Disabled]
		Hot Plug>	PCI Express hot plug [Enabled, **Disabled**]
		PCIe Speed>	Configures PCIe speed [**Auto**, Gen 1, Gen2]
		Transmitter Half Swing>	Transmitter half swing [Enabled, **Disabled**]
		Extra Bus Reserved>	Extra bus reserved for bridges behind this root bridge. (0-7)
		Reserved Memory>	Reserved memory and prefetchable memory for this root bridge Range: (1 MB-20 MB)
		Reserved I/O>	Reserved I/O for this root bridge Range: (**4** k, 8 k, 12 k, 16 k, 20 k)
		PCH PCIE LTR>	PCH PCIE latency reporting [**Enabled**, Disabled]
		Snoop Latency Override>	Snoop latency override or Non Snoop override for PCH PCIE. Disabled: disables override Manual: manually enters override values Auto: maintains default BIOS flow. [Disabled, Manual, **Auto**]
		Non Snoop Latency Override>	
		PCIE1 LTR Lock>	PCIE LTR configuration lock [Enabled, **Disabled**]
		PCIE Selectable De-emphasis>	Selects level of de-emphasis for an upstream component, if the Link operates at 5.0 GT/s speed. 1b – 3.5 dB 0b – 6 dB [**Enabled,** Disabled]
SATA Drivers>	SATA Test Mode>	Test mode [Enabled, **Disabled**]	
	SATA Port 0> or SATA Port 1>	SATA Port #>	Read only field SATA port installed/Not Installed and software preserve
		Port #>	SATA port # [**Enabled,** Disabled]
		SATA Port # Hot Plug Capability>	Reports SATA port as being Hot Plug capable [Enabled, **Disabled]**

Function	Second level Sub-Screen / Description	
SCC Configuration>	SCC SD Card Support (D27:F0)>	SCC card support [**Enabled**, Disabled]
	SCC eMMC Support (D28:F0)>	SCC eMMC Support [**Enabled**, Disabled]
	eMMC Max Speed>	Selects the eMMC max. speed allowed [HS400, **HS200**, DDR50]
USB Configuration>	USB Port Disable Override>	Selectively enables or disables the corresponding USB port from reporting a device connection to the controller. [Enable, **Disable**]
	xDCI Support>	XDCI [Enable, **Disable**]
	xHCI Disable Compliance Mode>	xHCI Disable Compliance Mode [FALSE, TRUE]
	USB HW Mode AFE Comparators>	USB HW mode AFE comparators [Enabled, **Disabled**]
Miscellaneous Configuration>	State After G3>	Specifies the state to go to if power is reapplied after power failure (G3 state) S0 state: system boots directly as soon as power is applied. S5 state: system remains in power-off states until the power button is pressed. [**S0 State**, S5 State]
	Power Button Debounce Mode>	Enable interrupt when PWRBTN# is asserted [**Enable**, Disable]
	Wake On LAN>	Wake on LAN [Enable, **Disable**]
	BIOS Lock>	Enable/Disable the SC BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash [Enabled, **Disabled**]
	RTC Lock>	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM [**Enabled**, Disabled]
	TCO Lock>	Enable TCO and Lock Down TCO [Enabled, **Disabled**]
	DCI Enable (HDCIEN)>	If enabled the user is considered to have consented to enable DCI and allows debug over the USB 3 interface. If disabled, the host controller does not enable the DCI feature. [Enabled, **Disabled**]
	DCI Auto Detect Enable>	If set, DCI Auto detects if DCI is connected during BIOS post time and enables DCI. If not set, DCI is disabled. [**Enabled**, Disabled]
	GPIO Lock>	Enable to set GPIO Pad Configuration Lock for security [Enabled, **Disabled**]

9.2.4. Security Setup Menu

The Security Setup menu provides information about the passwords and functions for specifying the security settings such as Hard Disk user and master passwords.

Figure 19: Security Setup Menu Initial Screen



```
            Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

  Password Description                              Set Setup 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:
  Minimum length                        3
  Maximum length                        20
                                                    →←: Select Screen
  Setup Administrator Password                      ↑↓: Select Item
  User Password                                     Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
  HDD Security Configuration:                       F2: Previous Values
  P0:InnoDisk Corp. - mSATA 3SE                     F3: Optimized Defaults
  P1:WDC WDS120G1G0A-00SS50                         F4: Save & Exit
                                                    ESC: Exit
▶ Secure Boot

            Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Table 23: Security Setup Menu Sub-screens and Functions

Function	Description		
Setup Administrator Password>	Sets administrator password		
User Password>	Sets user password		
HDD Security Configuration>	Read Only Information Allows access to set, modify and clear Hard Disk user and master passwords. User Passwords need to be installed for Enabling Security. Master Password can be modified only when successfully unlocked with the Master Password in Post. If the 'Set HDD Password' is grayed out, then power cycle to enable the option again. HDD Password Configuration Security supported : Yes Security Enabled : No Security Locked : No Security Frozen : No HDD User Pwd Status : Not Installed HDD Master Pwd Status : Installed		
	Set User Password> Set User Password> (continued)	Sets HDD password. Note: It is advisable to power cycle the system after setting Hard Disk passwords. The 'Discarding or Saving Changes' in the setup does not have an impact on HDD when the password is set or removed. If the setup HDD user Password is grayed out, do power cycle enable the option again.	
Secure Boot>	System Mode>	Read only information.	
	Secure Boot>		
	Vendor Keys>		
	Attempt Secure Boot>	Secure Boot activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled [Enabled, **Disabled**]	
	Secure Boot Mode>	Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode [Standard, **Customized**]	
	Key Management>	Enables expert users to modify Secure Boot Policy variables without full authentication	
		Provision Factory Default keys>	Allow to provision factory default Secure Boot keys when System is in Setup Mode [Enabled, **Disabled**]
		Install Factory Default keys>	Force System to User Mode – install all Factory Default keys
		Enroll Efi Image>	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash Certificate of the Image into Authorized

Function	Description		
Secure Boot> (continued)			Signature Database (db)
		Platfrom Key (PK)>	Enroll Factory Defaults or load certificates from a file: Public Key Certicate in: EFI_SIGNATURE_LIST EFI_CERT_X509 (DER encoded) EFI_CERT_RSA2048 (bin) EFI_CERT_SHA256,385,512 Authenticated UEFI Variable EFI PE/COFF Image (SHA256) Key Source : Default, External, Mixed, test
		Key Exchange Keys>	
		Authorized Signatures>	
		Forbidden Signatures>	
		Authorized TimeStamps>	
		OsRecovery Signatures>	

If only the administrator's password is set, then only access to setup is limited. The password is only entered 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. Within the setup menu the user has administrator rights.

Password length requirements are maximum length 20 and minimum length 3.

9.2.4.1. Remember the Password

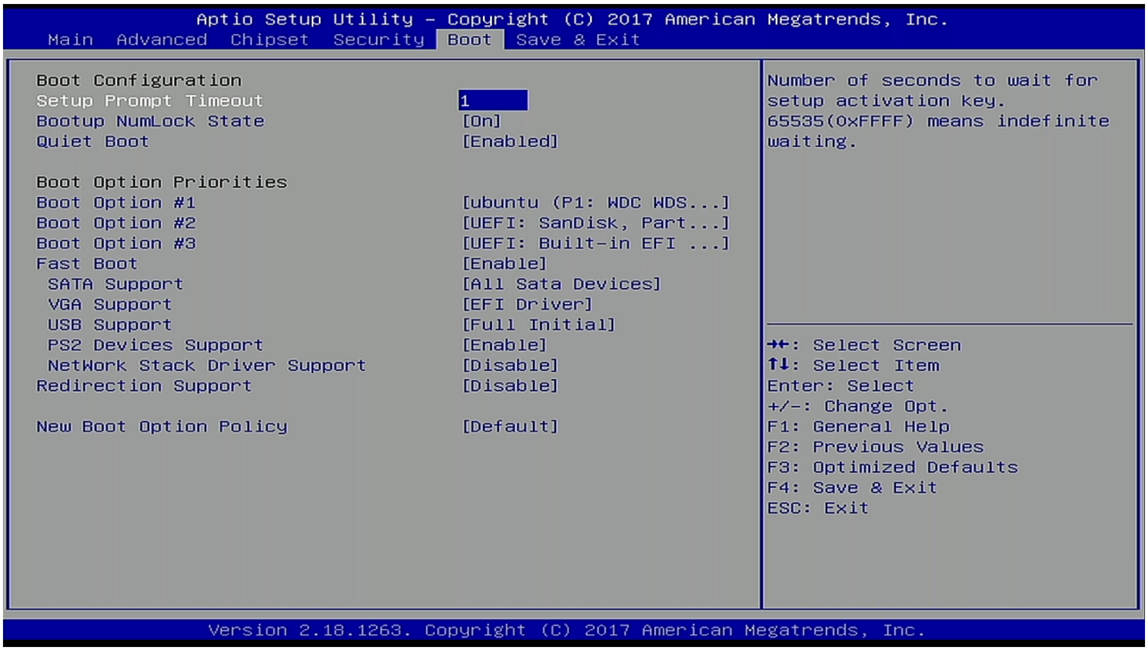
It is recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system. If the system cannot be booted because the User Password or the Supervisor Password are not known, clear the uEFI BIOS settings, or contact Kontron Support for further assistance.

HDD security passwords cannot be cleared using the above method.

9.2.5. Boot Setup Menu

The Boot Setup menu lists the dynamically generated boot-device priority order.

Figure 20: Boot Setup Menu Initial Screen



```
            Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

  Boot Configuration                                    Number of seconds to wait for
  Setup Prompt Timeout                 1                setup activation key.
  Bootup NumLock State                 [On]             65535(0xFFFF) means indefinite
  Quiet Boot                           [Enabled]        waiting.

  Boot Option Priorities
  Boot Option #1                       [ubuntu (P1: WDC WDS...]
  Boot Option #2                       [UEFI: SanDisk, Part...]
  Boot Option #3                       [UEFI: Built-in EFI ...]
  Fast Boot                            [Enable]
   SATA Support                        [All Sata Devices]
   VGA Support                         [EFI Driver]
   USB Support                         [Full Initial]
   PS2 Devices Support                 [Enable]         →←: Select Screen
   Network Stack Driver Support        [Disable]        ↑↓: Select Item
  Redirection Support                  [Disable]        Enter: Select
                                                        +/-: Change Opt.
  New Boot Option Policy               [Default]        F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit

           Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

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

Table 24: Boot Setup Menu Sub-screens and Functions

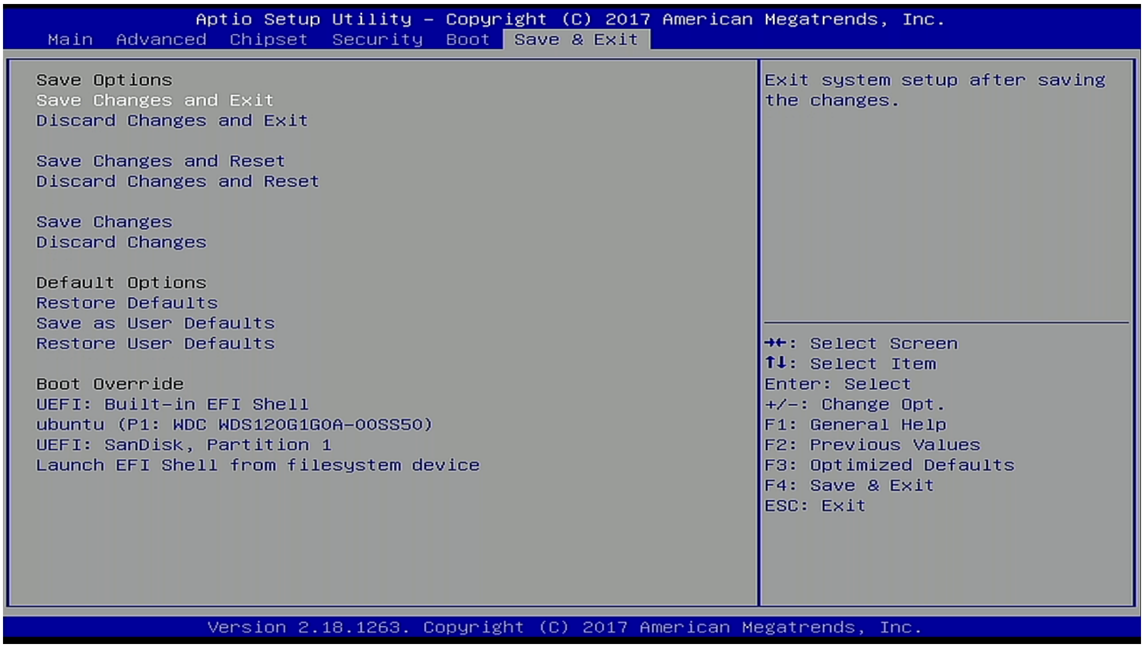
Function	Description
Setup Prompt Timeout>	Displays number of seconds that the firmware waits for setup activation key The value 65535(0xFFFF) means an indefinite wait.
Bootup NumLock State>	Selects keyboard NumLock state [**ON**, OFF]
Quiet Boot>	Quiet Boot [Enabled, **Disabled**]
Boot Option #>	Sets the system boot order
Fast Boot>	Enables or disables FastBoot features Note: Most probes are skipped to reduce time and cost during boot. [Enabled, **Disabled**]
SATA Support>	SATA Support [Last Boot HDD only, **All Sata Devices**]
VGA Support>	If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. Efi driver will still be installed with EFI OS. [Auto, **EFI Driver**]
USB Support>	If disabled, all USB devices will NOT be available untill after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Full Initial, all USB devices will be available in OS and Post. [**Full Initial**, Partial Initial, Disable]

Function	Description
PS2 Support>	PS2 Support [**Enabled**, Disabled]
Netwrok Stack Driver Support>	Netwrok Stack Driver Support [Enabled, **Disabled**]
Redirection Support>	Redirection Support [Enabled, **Disabled**]
New Boot Option Policy>	Controls the placement of newly detected UEFI boot options [**Default**, Place First, Place Last]

9.2.6. Save and Exit Setup Menu

The Save and Exit Setup menu provides functions for handling changes made to the settings and exiting the program.

Figure 21: Save and Exit Setup Menu Initial Screen


Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Main
Advanced
Chipset
Security
Boot
Save & Exit

```
Save Options
Save Changes and Exit
Discard Changes and Exit

Save Changes and Reset
Discard Changes and Reset

Save Changes
Discard Changes

Default Options
Restore Defaults
Save as User Defaults
Restore User Defaults

Boot Override
UEFI: Built-in EFI Shell
ubuntu (P1: WDC WDS120G1G0A-00SS50)
UEFI: SanDisk, Partition 1
Launch EFI Shell from filesystem device
```

```
Exit system setup after saving
the changes.

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

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.

The following table shows the Save and Exit sub-screens and functions and describes the content.

Table 25: Save and Exit Setup Menu Sub-screens and Functions

Function	Description
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
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
UEFI: Built in EFI Shell>	Attempts to launch the boot option #1
Ubuntu (P1: WDC WDS120G1G0A-00SS50)>	Attempts to launch the boot option #2
UEFI: SanDisk, Partition 1>	Attempts to launch the boot option #3
Launch EFI Shell from File System Device>	Attempts to launch EFI Shell application (Shell.efi) from one of the available filesystem devices

9.3. 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.

9.3.1. 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.

9.3.1.1. 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)
```

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

4. The output produced by the device-mapping table can vary depending on the board's configuration.
5. If the <ESC> key is pressed before the 5 second timeout elapses, the shell prompt is shown:

```
Shell>
```

9.3.1.2. 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.

9.4. uEFI Shell Scripting

9.4.1. 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.

9.4.2. 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.

9.4.3. Example of Startup Scripts

9.4.3.1. 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
```

9.5. 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.

9.5.1. Updating Procedure

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

1. Copy these files to an USB stick.

- flash.nsh (if available)
- fpt.efi
- fparts.txt
- Q7ALi<xxx>.bin (where xxx stands for the version #)
- Start the system into setup.

2. Change the following setup items:

Chipset > South Cluster Configuration> Miscellaneous Configuration > BIOS Lock > Disabled

3. Save and Exit the BIOS setup.

4. On the next start, boot into shell.
5. Change to the drive representing the USB stick.

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

Change to the directory where you copied the flash tool.

```
cd <your_directory>
```

6. Start flash.nsh (if available) OR enter

```
fpt  –F Q7ALi<xxx>.bin
```

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

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

i **Changes made in step 3 above are only effective during the first boot after applying the changes. If you fail to flash during the next boot, then you might have to repeat steps 3.**

Appendix A: List of Acronyms

Table 26: List of Acronyms

BIOS	Basic Input Output System
BSP	Board Support Package
CAN	Controller-area network
Carrier Board	Application specific circuit board that accepts a COM Express ® module
COM	Computer-on-Module
DDC	Display Data Control
DDI	Digital Display Interface –
DDIO	Digital Display Input/Output
DIMM	Dual In-line Memory Module
DP	DisplayPort (digital display interface standard)
DMA	Direct Memory Access
DRAM	Dynamic Random Access Memory
DVI	Digital Visual Interface
ECC	Error Checking and Correction
EEPROM	Electrically Erasable Programmable Read-Only Memory
eDP	Embedded Display Port
EMC	Electromagnetic Compatibility (EMC)
ESD	Electro Sensitive Device
FAT	File Allocation Table
FIFO	First In First Out
Gb	Gigabit
GBE	Gigabit Ethernet
GPI	General Purpose Input
GPIO	General Purpose Input Output
GPO	General Purpose Output
GPU	Graphics Processing Unit
HBR2	High Bitrate 2
HDA	High Definition Audio (HD Audio)
HD/HDD	Hard Disk /Drive
HDMI	High Definition Multimedia Interface
HWM	Hardware Monitor
I2C	Inter integrated Circuit Communications
IOT	Internet of Things
ISA	Industry Standard Architecture
LAN	Local Area Network
LPC	Low Pin-Count Interface:
LPT	Line Printing Terminal
LSB	Least Significant Bit
LVDS	Low Voltage Differential Signaling –
M.A.R.S.	Mobile Application for Rechargeable Systems
MIPI	Mobile Industry processor Industry
MTBF	Mean Time Before Failure
NA	Not Available
NC	Not Connected
NCSI2	Network Communications Services Interface
NTC	Negative Temperature Coefficient resistor
PCI	Peripheral Component Interface
PCIe	PCI-Express
PEG	PCI Express Graphics
SGET®	PCI Industrial Computer Manufacturers Group
PHY	Ethernet controller physical layer device
Pin-out Type	QSEVEN® definitions for signals on QSEVEN® Module connector pins.
PSU	Power Supply Unit
RoHS	Restriction of the use of certain Hazardous Substances
RTC	Real Time Clock
SATA	Serial AT Attachment:
SCSI2	Small Computer System Interface
SEL	System Event Log
SoC	System on a Chip
SOL	Serial Over LAN
SPI	Serial Peripheral Inteface
SSH	Secure Shell
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VGA	Video Graphics Adapter
WDT	WatchDog Timer
WDOUT	WatchDog Time Out
WDTRIG	WatchDog TRigger
WEEE	Waste Electrical and Electronic Equipement (directive)

About Kontron

Kontron is a global leader in embedded computing technology (ECT). As a part of technology group S&T, Kontron offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall. For more information, please visit: www.kontron.com

▼

Global Headquarters

Kontron S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com