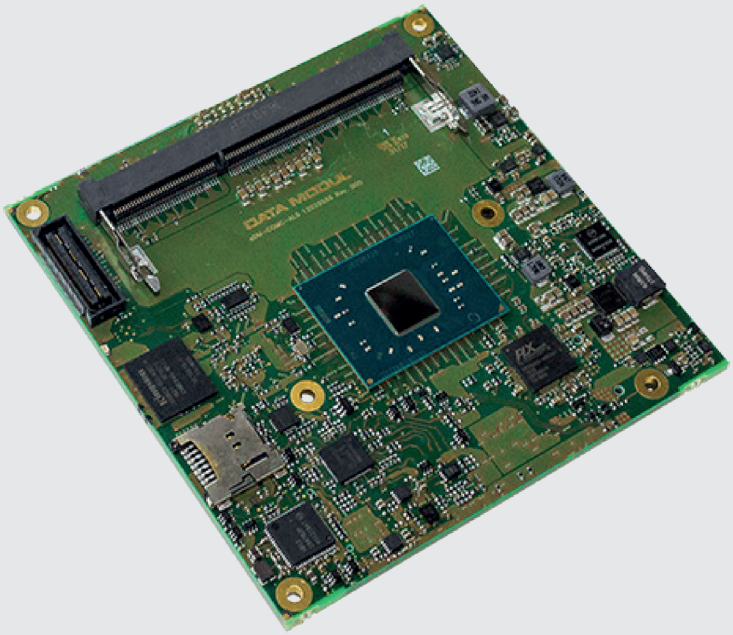
DATA MODUL

eDM-COMC-AL6



Revision History

Revision	Revision History	Date
00	First release	04/23/2019

Reference to this Specification
The purpose of all the figures and illustrations in this Specification is merely to provide a better explanation and can differ to the actual appearance of the board. They are to be understood as schematic representations.

[12038083 Rev. 00]

Contents

Preface

Using this Specification

- In this Specification, the eDM-COMC-AL6 is also referred to as „board“.
- Please read this Specification before using this board.
- This Specification contains information about the hardware, software and configuration of the board.
- Awareness of the safety instructions and instructions for use in this Specification will ensure the safe and correct use of the board.
- In addition to the information given here, you should comply with the local regulations for the prevention of accidents and generally applicable safety regulations.

Purpose of this Specification

The purpose of this document is the definition of the technical parameters, the electrical connections and the mechanical dimensions of the eDM-COMC-AL6.

Danger Symbols and Levels

In this Specification, symbols are used to highlight important safety instructions and any advice relating to the device. The instructions should be followed very carefully to avoid any risk of accident, personal injury or property damage.

Danger Symbols

	Dangerous Voltage, Electric shock
	Hazard point
	All DATA MODUL AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a DATA MODUL AG product except at an electrostatic-free workstation. Additionally, do not ship or store DATA MODUL AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the DATA MODUL AG Limited Warranty.

Danger Levels

DANGER	Indicates a hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a property damage message.

General Symbols

Notes that are marked with these symbols contain important or useful information for the operation respectively the handling of the device.

	Additional support or useful information.
	The crossed-out refuse bin indicates that the products must be properly recycled or disposed of appropriately in accordance with national legislation in the respective EU countries. If you wish to dispose of used electrical and electronic products outside the European Union, please contact your local authority so as to comply with the correct disposal method.

Technical Support

DATA MODUL's technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.data-modul.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@data-modul.com.

Abbreviations

Term	Description
COM	Computer On Module
DDC	Display Data Channel
EMI	Electrical Magnetic Interference
EN	European Norm
FFC	Flat Foil Cable
HDMI	High Definition Multimedia Interface
I²C	Inter-Integrated Circuit Bus
LCD	Liquid Crystal Display
LVDS	Low Voltage Differential Signal
NA	Not Available
NC	Not Connected
PCB	Printed Circuit Board
PWM	Pulse Width Modulation
SB	Standby
SSP	Synchronous Serial Protocol
TBD	To be defined
TCON	Timing Controller
TMDS	Transition Minimized Differential Signalling
TTL	Transistor Transistor Logic
UL	Underwriter Lab
USB	Universal Serial Bus

Specifications

Supported Operating Systems

- Microsoft® Windows® 10 (64 bit)
- Microsoft® Windows® 10 IoT Enterprise (64 bit)
- Linux (64 bit Yocto)

EFI / BIOS

- UEFI based Firmware using AMI Aptio V core
- Darkboot / Bootlogo support
- Legacy Free Operation
- Boot from external SPI as defined by COM Express specification
- Memory-initialization according to SPD, X.M.P. profiles supported
- LID and Sleep signals supported
- ACPI Wake Events (WOL S3-S5, USB S3-S4, LID S3, PwrBtn S3-S5)
- AC Power Loss configurable by setup
- Spread Spectrum configurable by setup, default ON
- ACPI 6.0
- DATA MODUL family feature: Embedded Controller specification

API

- eAPI as defined by COM Express
- Data Modul specific extension to eAPI

Tools

- BIOS update tool for EFI shell
- BIOS modification tool (for ROM file and running system to extract setup-settings)
- FPGA update tool for EFI shell
- API test tool

Standards & Certifications

Environmentalism

- 2011/65/EU (of 8. June 2011 directive of the European parliament and of the council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS))
- 2006/1907/EU (of 18. December 2006 of the European parliament and of the council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH))
- 2012/19/EC (of 04. July 2012 directive of the European parliament and of the council on waste electrical and electronic equipment (WEEE))
- The board is designed and manufactured to meet ISO 14001.
- The packing complies with directive 1994/62/EU.

EMC Standards

EMI/EMC: according to EN55022

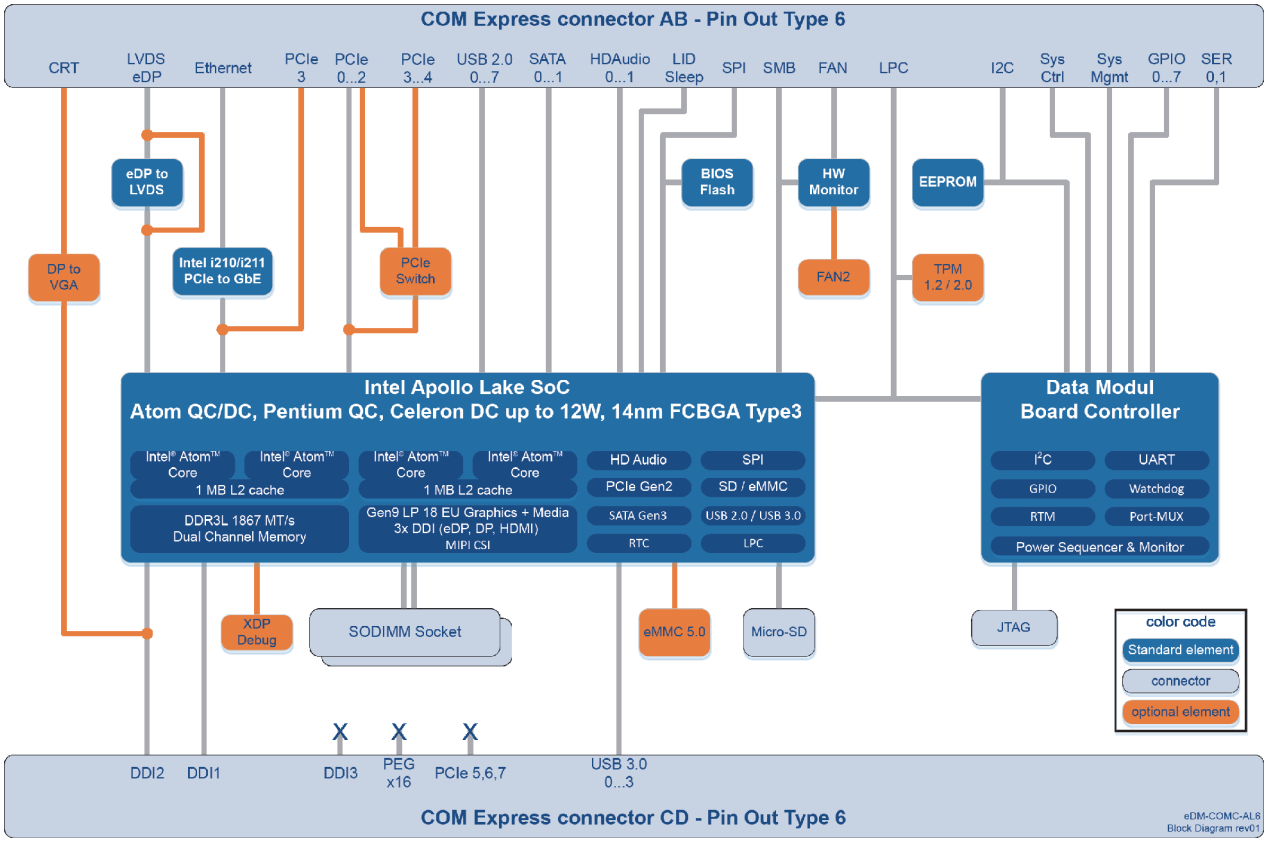
Electrical Safety

Designed to meet EN60950 and UL60950.

Shock & Vibration

Shock and Vibration according to IEC/EN60068-2-6 and IEC/EN60068-2-27.

Block Diagram



Ordering Information

Model Name	Part No.	Description
eDM-COMC-AL6-E3950	12024769	COM Express Type 6 Compact module with Intel® Atom® x5-E3950, -40°C to 85°C
eDM-COMC-AL6-E3940	12024770	COM Express Type 6 Compact module with Intel® Atom® x5-E3940, -40°C to 85°C
eDM-COMC-AL6-3930	12024771	COM Express Type 6 Compact module with Intel® Atom® x5-E3930, -40°C to 85°C
eDM-COMC-AL6-N3350	12024772	COM Express Type 6 Compact module with Intel® Celeron® N3350
eDM-COMC-AL6-N4200	12024773	COM Express Type 6 Compact module with Intel® Pentium® N4200
eDM-COMC-AL6-CH	12024774	Standard Cooling Heatspreader, for Pentium/Celeron SOC
eDM-COMC-AL6-CP	12024775	Standard Cooling Solution passive, for Pentium/Celeron SOC
eDM-COMC-AL6-eCP	12024776	Standard Cooling Solution passive, for lidded ATOM SOC
eDM-COMC-AL6-eCP	12024777	Standard Cooling Heatspreader, for lidded ATOM SOC

Platform Features

Platform

Intel® Apollo Lake Platform

CPU

The eDM-COMC-AL6 supports all available Apollo Lake SOCs in FCBGA Type3 package up to 12W TDP.

- Package: 14nm / 31x 24 mm Type3, FCBGA1296 pin count
- Supported Features:
  - C-States: CO-C6
  - 1 MB Cache per 2 cores
  - CPU Burst
  - Intel® 64 Architecture
  - Intel® SpeedStep® Technology
  - Intel® Virtualization Technology (VTx)

- Security Features:
  - Security Engine
  - Verified / Security Boot
  - Intel® Dynamic Application Loader (DAL)
  - Advanced Encryption Standard New Instructions (Intel® AES-NI)
- Real-time:
  - Prevention of cache collision
  - Virtual Channel functionality to CPU edge
  - Memory Arbiter QOS between CPU & VC
  - Precision Time Management support (Core Time Stamp Counter & PCIe clock synchronization)

Memory

- Two SO-DIMM sockets
- Memory type: DDR3L
- Speed: up to 1866 MT/s
- Size: up to 16 GB (2 x 8 GB)

Graphics & Media

- GFX type: Intel® HD Graphics Gen 9
- Class: up to 18 EUs
- Display Pipes: 3 independent
- Video Decode: 4k for HEVC, H.264, VP9
- Video Encode: 4k for HEVC, H.264, VP9
- Imaging: 4 Vector Unit Image Processing
- Hardware Acceleration: OpenGL 4.2, DirectX12, OpenCL 2.0

IO

- 4 x USB 3.0, 8 x USB 2.0
- 2 x SATA 6Gb/s
- 4 x SATA 3.0
- 1 x SDIO 3.0, 1 x SDXC for microSD socket
- 4 x PCIe
  (CPU Ports 0/1/2/3 PCIe Gen1/2 compliant Option PCIe Switch: Ports 2/3/4 PCIe Gen1 compliant, Gen2 compliant with restriction by PEX8605 (ClockJitter)), 1 x used for Gigabit LAN
- Optional PCIe Switch for total 6 x PCIe Gen2
- SPI for external boot flash
- LPC for Embedded Controller / TPM / external SIO
- 8 GPIOs with optional muxed functions:
  PWM, UART0 (or 1 if counting from 1) DTR/DSR/RTS/CTS, external WD-Kick, I2C
- Intel HD Audio supporting 2 external codecs
- 2 x UART

LAN

Intel®i210 (Industrial) / i211 (Commercial) Gigabit Ethernet Controller with SDP support.

Additional Interfaces & Functions

LVDS

The eDM-COMC-AL6 supports Dual channel LVDS 1/2x18/24bit up to 1920x1200 from an eDP2LVDS converter like NXP PTN3460. Optionally it shall be possible to bypass LVDS converter to redirect the eDP signals to the COM Express connector pins.

eMMC

optional onboard eMMC memory using JEDEC package BGA-153 or BGA169 (eMMC 5.0)

Micro-SD Card socket

According to SD-Card Specification.

TPM

The eDM-COMC-AL6 supports a Trusted Platform Module according to TPM standard 2.0 using the Infineon SLB9665 TPM controller in QFN32 package. Alternatively an Atmel-TPM 2.0 can be used at the same position.

Hardware Monitor

Hardware Monitoring supports on the eDM-COMC-AL6 design using the Nuvoton NCT7802Y.
Hardware Monitor providing following information:

- CPU DIE temperature measured through the on-DIE temperature diode of the CPU
- PCB temperature measured inside HW Monitor (place HWM at cool spot of PCB)
- Level of VCC input voltage
- Level of 5V_SBY input voltage
- Level of VCCRTC voltage follower OpAmp circuit.

The Hardware Monitor provides control signals to operate one Fan connected at the COM Express baseboard fan connector and on-board Connector.

Embedded Controller

An Embedded Controller providing the featureset defined in Data Modul Embedded Controller specification Rev 1.0 using a Altera MAX-10 FPGA supports by the eDM-COMC-AL6 design.

DATA MODUL Board Controller

The DATA MODUL Embedded Controller (DMEC) implements a set of typical embedded peripheral features in the Computer-On-Module (CoM) including devices like GPIO, I2C, Watchdog timers, UARTs etc. Depending on the DATA MODUL board type, the DMEC device is connected to the chipset either via LPC or eSPI.

The DMEC Controller on the eDM-COMC-AL6 module provides the following functionality:

- Connected to LPC on Intel Braswell SoC
- Two UARTs
  - Speed up to 115200Bd
  - I/O Address/IRQ configurable via BIOS setup.
  - UART1 optionally supports RTS/CTS/DSR/DTR signals through GPIOs, configurable via BIOS setup.
- I2C controller
  - Controls up to three I2C busses via multiplexer.
  - Supports Automatic Bus Clear to prevent bus hangs.
  - Supports Multiple masters on the bus. This feature is only supported if Automatic Bus Clear is off.
  - Supports FastMode+.
  - I2C speed configurable via BIOS setup.
  - Up to 400kHz in normal mode, up to 800kHz in FastMode+.
  - IRQ configurable via BIOS setup.
- Watchdog
  - Supports up to three stages.
  - Timeout per stage: 1ms- 65sec, with a granularity of 1ms or 128ms - ~140min, with a granularity of 128ms.
  - Supports Standard and Window Mode. Window mode is an advanced watchdog feature for safety critical applications. It only allows triggering the Watchdog within a specific time window. This covers the case where software hangs in a loop within the watchdog trigger routine.
  - Stage events include NMI, Reset and IRQ (if enabled in BIOS setup).
  - Supports Auto Reload (allows to use the Watchdog as an event ticker).
  - Supports register lock to prevent the Watchdog from being disabled or its configuration being changed in safety critical applications.
  - Fully configurable via BIOS setup.

- COM Express GPIOs:
  - Supports eight bi-directional GPIOs.
  - Initial state (In/Out, High/Low, set during early POST) can be configured via BIOS setup.
  - Capable to generate IRQ events (if IRQ enabled in BIOS setup). For details on how to enable IRQ generation please refer to the DMEC Functional Specification.
  - Additional GPIO function configurable via BIOS setup:
    - GPIO2: GPIO or UART1 DSR
    - GPIO4: GPIO or UART1 CTS or PWM0
    - GPIO5: GPIO or WD Kick Input or UART1 RTS or PWM1
    - GPIO6: GPIO or I2C2 CL or UART1 DTR
    - GPIO7: GPIO or I2C2 SDA.
- PWM controller
  - Supports either two independent 8Bit channels or one 16 Bit channel for higher resolution for example in DAC applications.
  - Left or center aligned PWM output
  - Programmable period and double buffered duty cycle registers
  - Configurable output polarity
  - Wide range PWM period configurable per channel via programmable pre-scaler".

Most common features are accessible through eApi function calls. eApi support and drivers for the DMEC device are available for Windows and Linux. For details on the DMEC register layout please refer to the DMEC Functional Specification which is available from DATA MODUL on request.

OnModule Memory

An 16 MByte SPI in SO-8 package flash to store EFI and setup configuration shall be used on the eDM-COMC-AL6 design.
One 32 kBit I2C EEPROM configured to address A0/A1 is connected to the fast I2C bus of the Embedded Controller and also to the I2C interface of the COM Express connector.

Environmental Specification

The eDM-COMC-AL6 is able to be operated and stored under the following environmental conditions:

- Temperature (operating): 0°C ... +60°C (commercial grade)
- Temperature (operating): -40°C ... +85°C (industrial grade)
- Temperature (storage): -40°C ... +85°C
- Relative humidity: ‹ 80%
- Tolerable air pressure: › 708 hPa (approx. altitude 2000m)

Power Supply

Input Voltage

- VCC: 12.0 V ± 5%
- 5V_SBY: 5.0 V ± 5%
- Modes: ATX Mode or VCC only without 5V_SBY

Specifications

- Voltage Ripple: max. 100mV peak to peak 0 ... 20 MHz
- Rise Time Specification: 0.1 ... 20ms from input voltage ‹ 10% nominal VCC
- Max. allowed Inrush Current 5V_SBY: 2A
  VCC: 5A

Power Features

- Reset Button Behavior
  Module resets immediately when reset button is pressed in S0 state.
  Module stays in reset condition when reset button is pressed and hold in any system state ‹ S0.

- Power Button Behavior
  A push of the power button power up the system to S0 if it is in S5/S3 state or shutdown to S5 if it is in S0 state. Operating system handle the power button event depending on the driver settings.
  Push and hold the power button >4s (power button override) shutdown the system into S5 independent of the other settings.

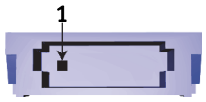
Interfaces / Connectors

COM Express connector, type 6 pin-out

- According COM Express specification Rev. 2.1.

Onboard Fan

- Supported by design but not assembled in series production.
- Connector type: JST part number SM04B-SURS-TF.
- Mating cable header type: JST part number 04SUR-32S.
- Pinout

Pin Arrangement	Pin	Description
	1	GND
	2	VCC
	3	SENSE
	4	PWM

BIOS Setup

The purpose of this chapter is to describe the settings in the UEFI BIOS Setup program on this Computer on Module and to explain the procedure for updating the UEFI BIOS.

Terms & Abbreviations

Term	Description
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
AFU	AMI Firmware Update
ASPM	Active State Power Management
BBS	BIOS Boot Specification
COM	Computer On Module
CRID	Compatible Revision ID
CSM	Compatibility Support Module
CTDP	Configurable TDP
DMI	Direct Memory Interface
DTS	Digital Thermal Sensor
DVMT	Dynamic Video Memory Technology
ECP	Enhanced Capabilities Port
EFP	External Flat Panel
EHCI	Enhanced Host Controller Interface
EIS	Enhanced Intel Speedstep
EPP	Enhanced Parallel Port
IGFX	Intel Graphics
IPv4/IPv6	Intel Protocol Version
KEK	Key Exchange Key
LBAR	Linear Base Address Register
LFP	Local Flat Panel
MRC	Memory Reference Code
NMI	Non-Maskable Interrupt
NVRAM	Non-Volatile Random-Access Memory
OPROM	Option ROM
OS	Operating System
PK	Platform Key
PME	Power Management Event
PVM	Pulse Width Modulation
PXE	Preboot Execution Environment
RAID	Redundant Array of Independent Disk
SCI	System Control Interrupt
SMI	System Management Interrupt
SO-DIMM	Small Outline Dual Inline Memory Module
SPP	Standard Parallel Port
TDP	Thermal Design Power
TOLUD	Top Of Lower Usable Memory
TXT	Trusted Execution Technology
VT-d	Virtualization Technology for Directed I/O
WDT	Watchdog Timeout
XHCI	eXtensible Host Controller Interface

BIOS Update Description

This COM is provided with an American Megatrends, Inc. Aptio V UEFI Firmware. Please use the AMI Firmware Update (AFU) utility suite for updating the BIOS. This is a scriptable command line tool, utilized for factory or field BIOS updates. It is available for DOS, Microsoft Windows®, Linux, and the UEFI shell.
Please contact your DATA MODUL support for accessing the tools.

For updating the complete 16MB firmware image with the UEFI version of AFU use following command:

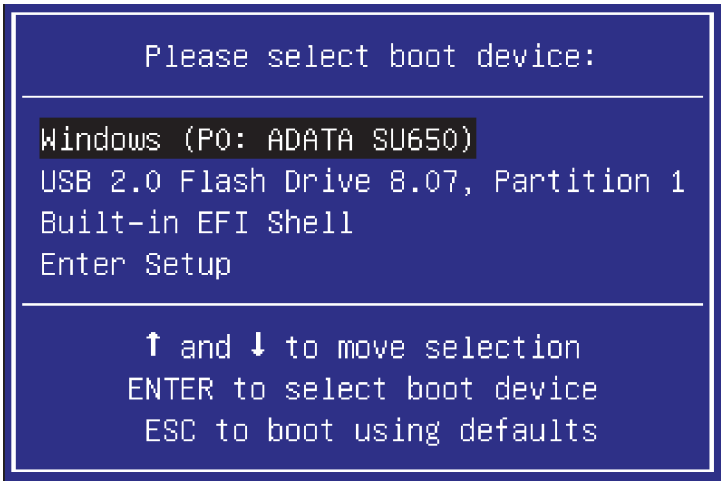
- afuefix64.efi newbiosfile.bin /P /N /FDR /DER.

For complete command reference, please check the appropriate readme files within the tools suites.

BIOS Setup Description

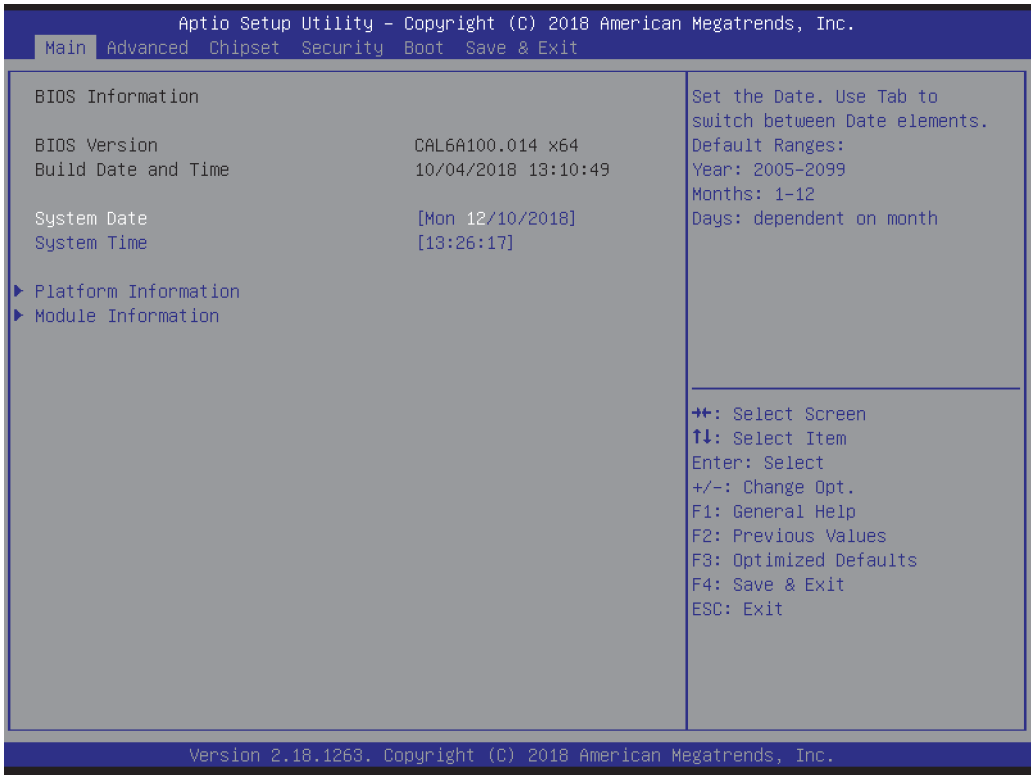
The UEFI Setup program allows users to modify the basic system configuration and save these settings to NVRAM.
To enter UEFI Setup, press DEL or ESC during POST.

To select a Boot Popup Menu, press F7 during POST. At End of Post a selection menu will show all available boot devices to choose from. UEFI Setup program can be entered from Boot Popup Menu as well.



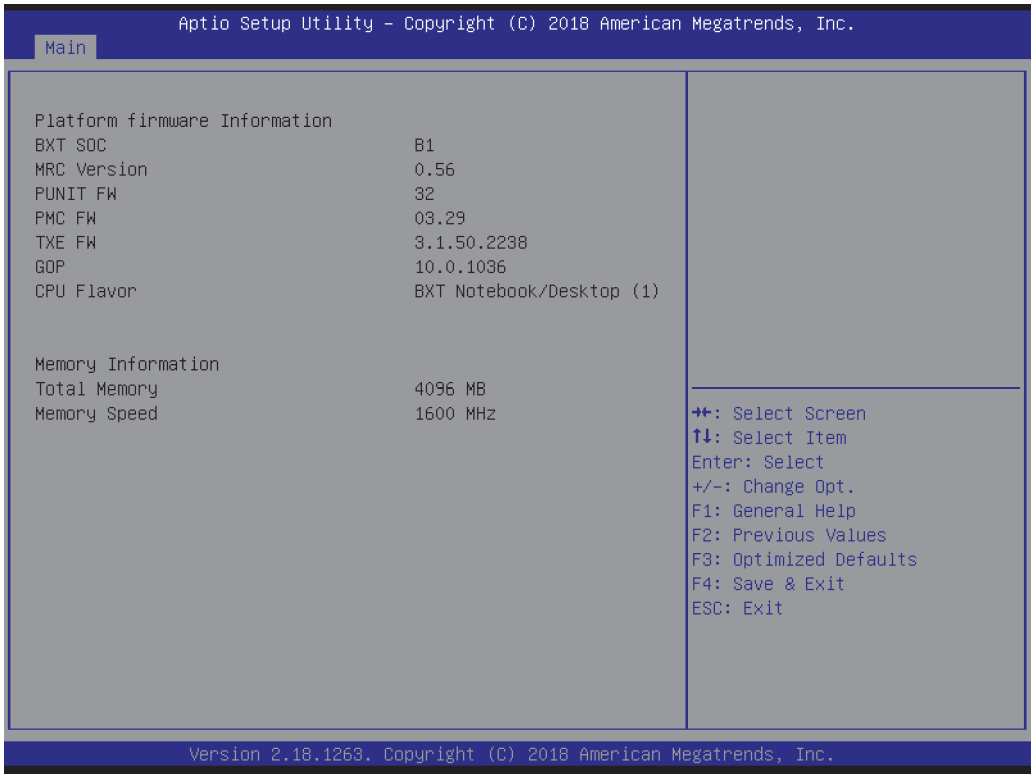
Following is a description of the UEFI Setup pages.

Main

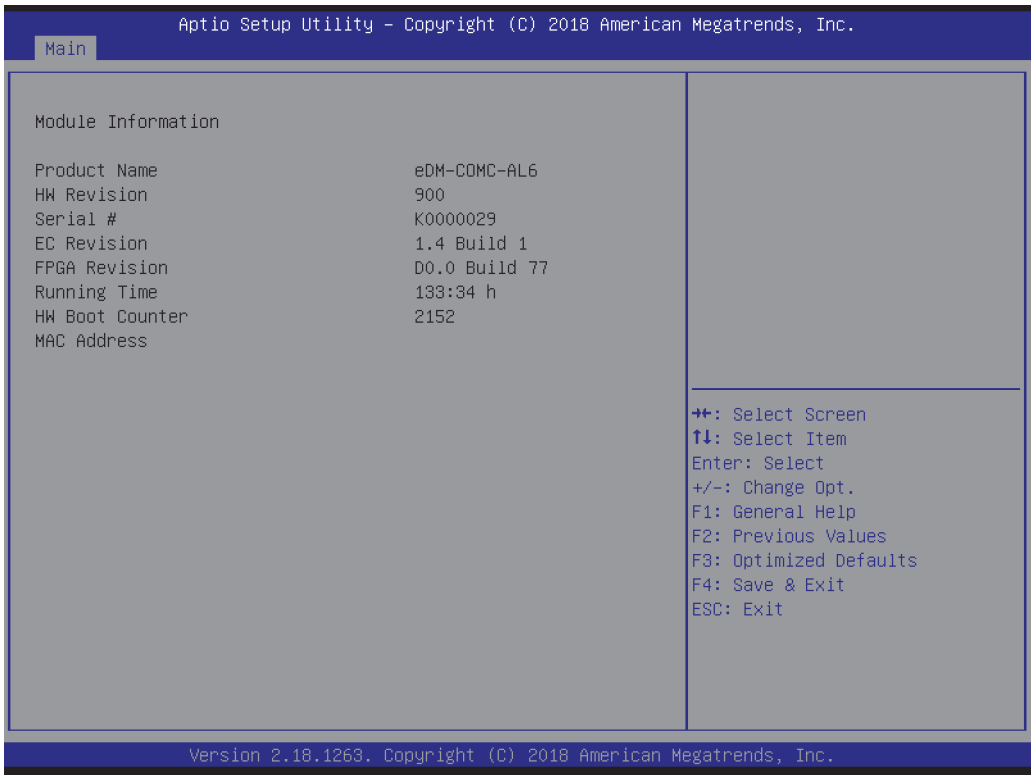


Parameter	Value	Comment
System Date	Day MM/DD/YYYY	Set the Date.
System Time	HH:MM:SS	Set the Time.
Platform Information	Submenu	Displays Platform Information.
Module Information	Submenu	Displays Module Information.

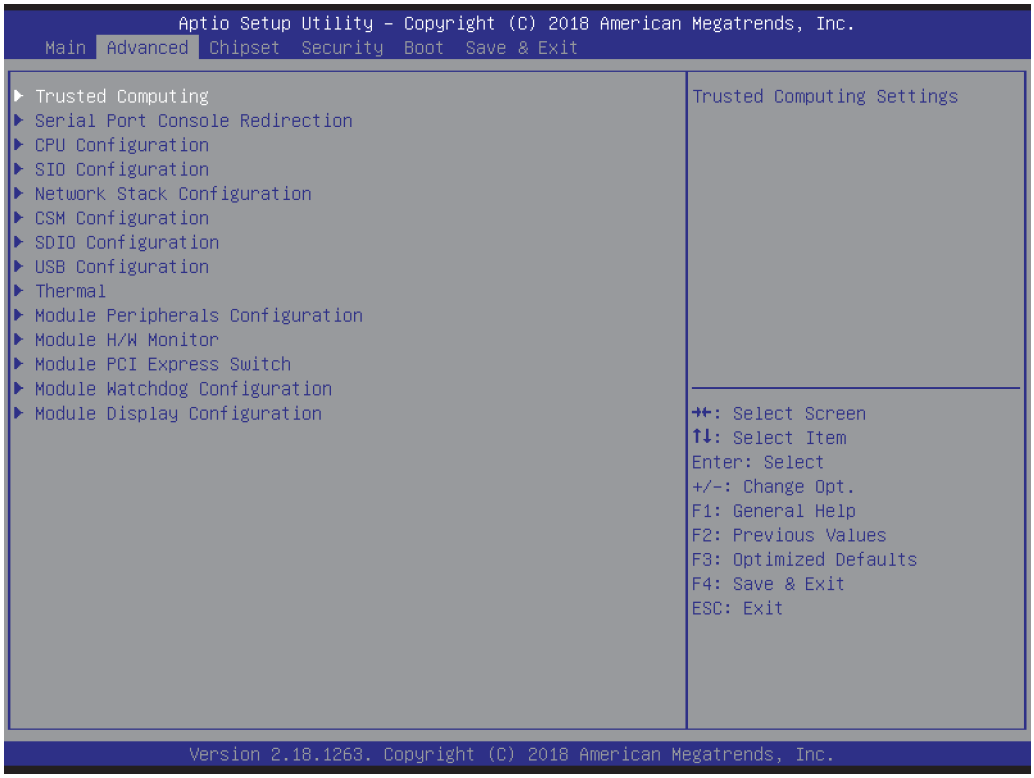
Platform Information



Module Information

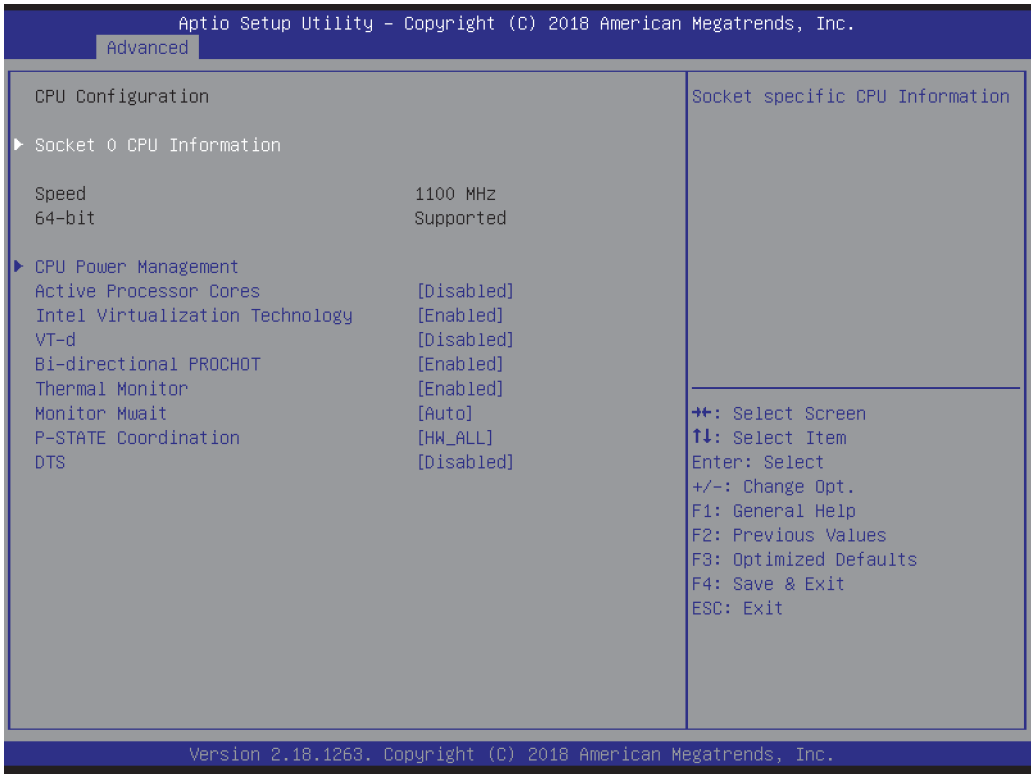


Advanced



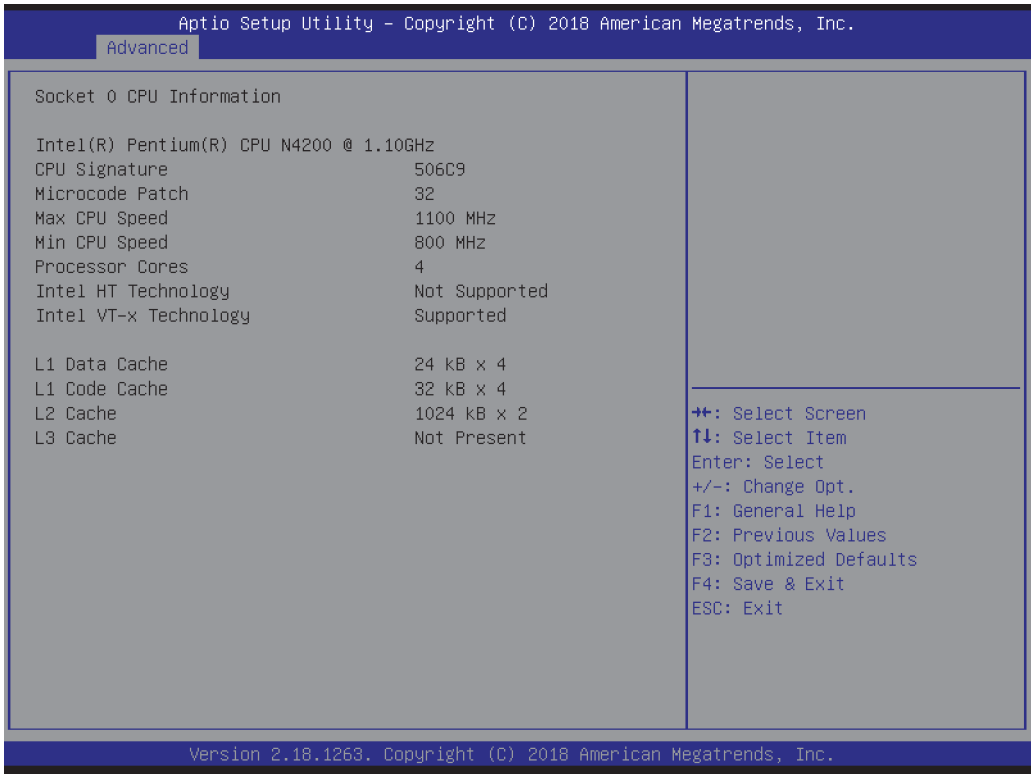
Parameter	Value	Comment
Trusted Computing	Submenu	Trusted Computing (TPM) Settings
Serial Port Console Redirection	Submenu	Serial Port Console Redirection Settings
CPU Configuration	Submenu	CPU Configuration Parameters
SIO Configuration	Submenu	SuperIO Settings
Network Stack Configuration	Submenu	Network Stack Settings
CSM Configuration	Submenu	Compatibility Support Module Settings
SDIO Configuration	Submenu	SDIO Configuration Parameters
USB Configuration	Submenu	USB Configuration Parameters
Thermal Configuration	Submenu	Thermal Configuration Parameters
Module Peripherals Configuration	Submenu	Configure Module Peripherals
Module H/W Monitor	Submenu	Monitor hardware status
Module PCI Express Switch	Submenu	Configure onboard PCI Express switch which spawns COMe PCIe ports 2/3/4.
Module Watchdog Configuration	Submenu	Configure Watchdog
Module Display Configuration	Submenu	Configure Module Display options

CPU Configuration

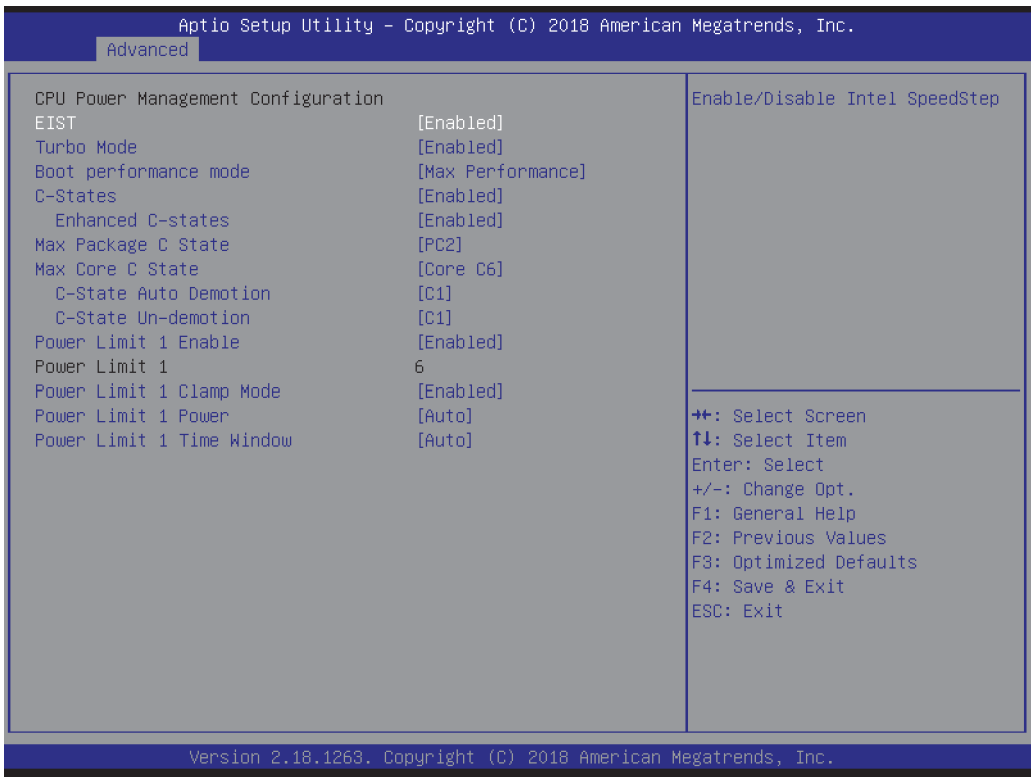


Parameter	Value	Comment
CPU Information	Submenu	CPU information and features.
CPU Power Management	Submenu	CPU power management options.
Active Processor Cores	Enabled **Disabled**	Number of cores to enable in each processor package.
Intel Virtualization Technology	**Enabled** Disabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
VT-d	Enabled **Disabled**	Enable/Disable CPU VT-d
Bi-directional PROCHOT	**Enabled** Disabled	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
Thermal Monitor	**Enabled** Disabled	Enable/Disable Thermal Monitor
Monitor Mwait	**Auto** Enabled Disabled	Enable/Disable Monitor Mwait
P-STATE Coordination	**HW_ALL** SW_ALL SW_ANY	Change P-STATE Coordination type.
DTS	Enabled **Disabled**	Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values. Disabled: DTS SMM and ACPI thermal management is disabled.

CPU Information

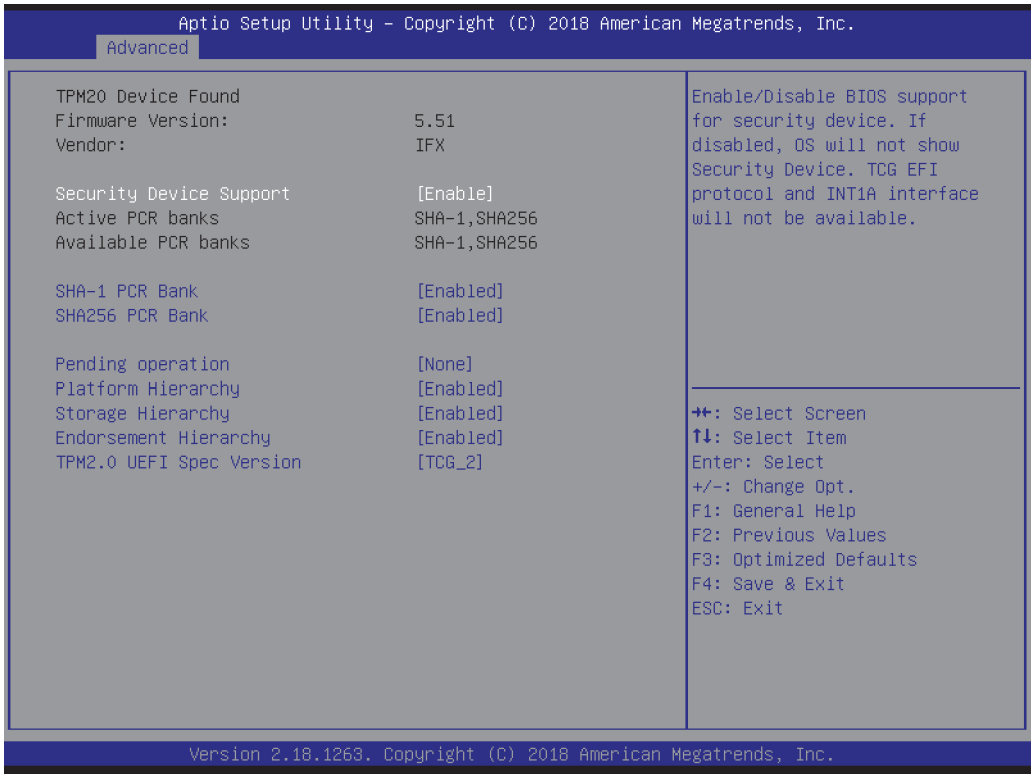


CPU - Power Management



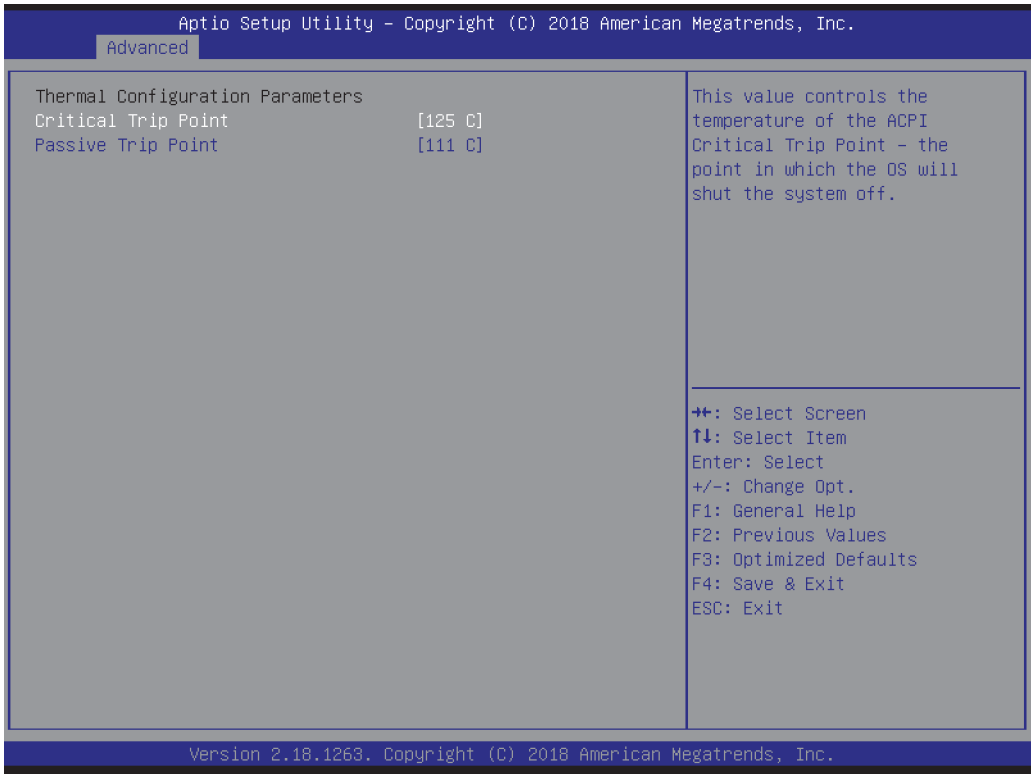
Parameter	Value	Comment
EIST	**Enabled** Disabled	Enable/Disable Intel SpeedStep.
Turbo Mode	**Enabled** Disabled	Enable/Disable Turbo Mode.
Boot performance mode	**Max Performance** Max Battery	Select the performance state that the BIOS will set before OS handoff.
C-States	**Enabled** Disabled	Enable/Disable C-States.
Enhanced C-states	**Enabled** Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
Max Package C State	**PC2** PC1 C0	Controls the Max Package C State that the processor will support.
Max Core C State	**Core C6** Core C1 Unlimited	This option controls the Max Core C State that cores will support.
C-State Auto Demotion	**C1** Disabled	Configure C-State Auto Demotion.
C-State Un-demotion	**C1** Disabled	Configure C-State Un-demotion.
Power Limit 1 Clamp Mode	**Enabled** Disabled	Enable/Disable Power Limit 1 Clamp Mode.
Power Limit 1 Power	**Auto** 6 - 25	Power Limit 1 in Watts. Auto will program Power Limit 1 based on silicon default support value.
Power Limit 1 Time Window	**Auto** 1 - 128	Power Limit 1 Time Window Value in Seconds. Auto will program Power Limit 1 Time Window based on silicon default support value.

Trusted Computing



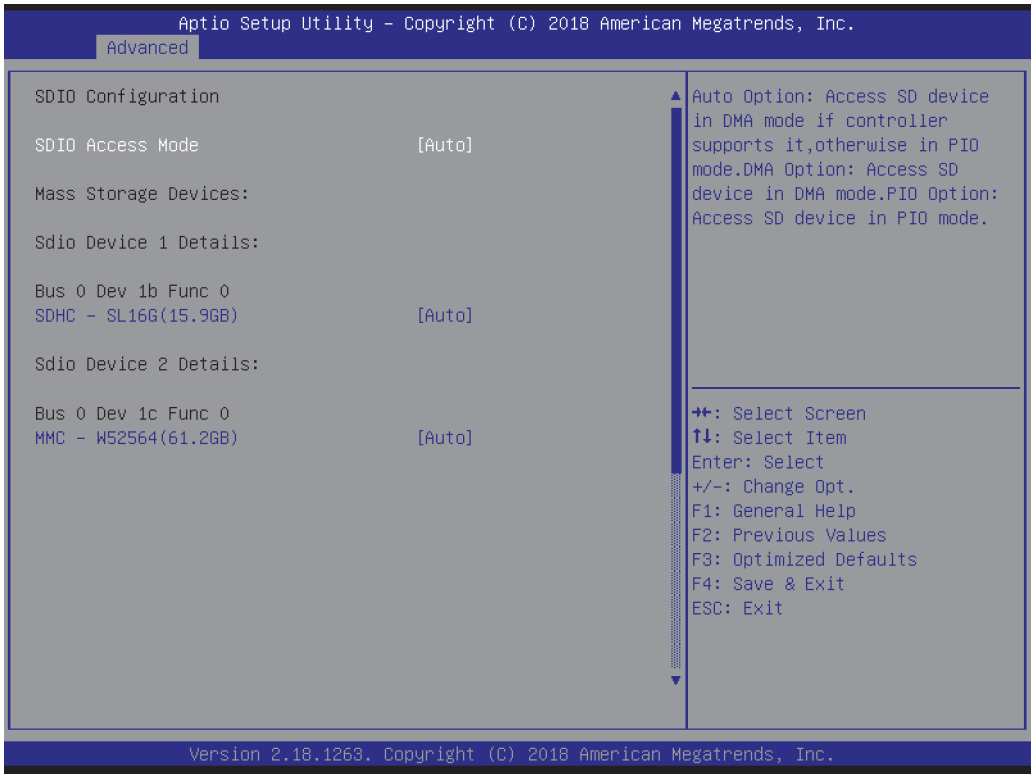
Parameter	Value	Comment
Security Device Support	Enabled **Disabled**	Enable/Disable BIOS support for security device. If disabled, OS will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank	**Enabled** Disabled	Enable or Disable SHA-1 PCR Bank.
SHA256 PCR Bank	Enabled **Disabled**	Enable or Disable SHA256 PCR Bank.
Pending operation	**None** TPM Clear	Clear TPM resets TPM to its default state. It removes the owner authorization value and any keys stored in the TPM.
Platform Hierarchy	**Enabled** Disabled	Enable or Disable Platform Hierarchy.
Storage Hierarchy	**Enabled** Disabled	Enable or Disable Storage Hierarchy.
Endorsement Hierarchy	**Enabled** Disabled	Enable or Disable Endorsement Hierarchy.
TPM2.0 UEFI Spec Version	TCG_1_2 **TCG_2**	Select the TCG2 Spec Version Support. TCG_1_2: the Compatible mode for Win8/Win10. TCG_2: Support new TCG2 protocol and event format for Win10 or later.

Thermal Configuration



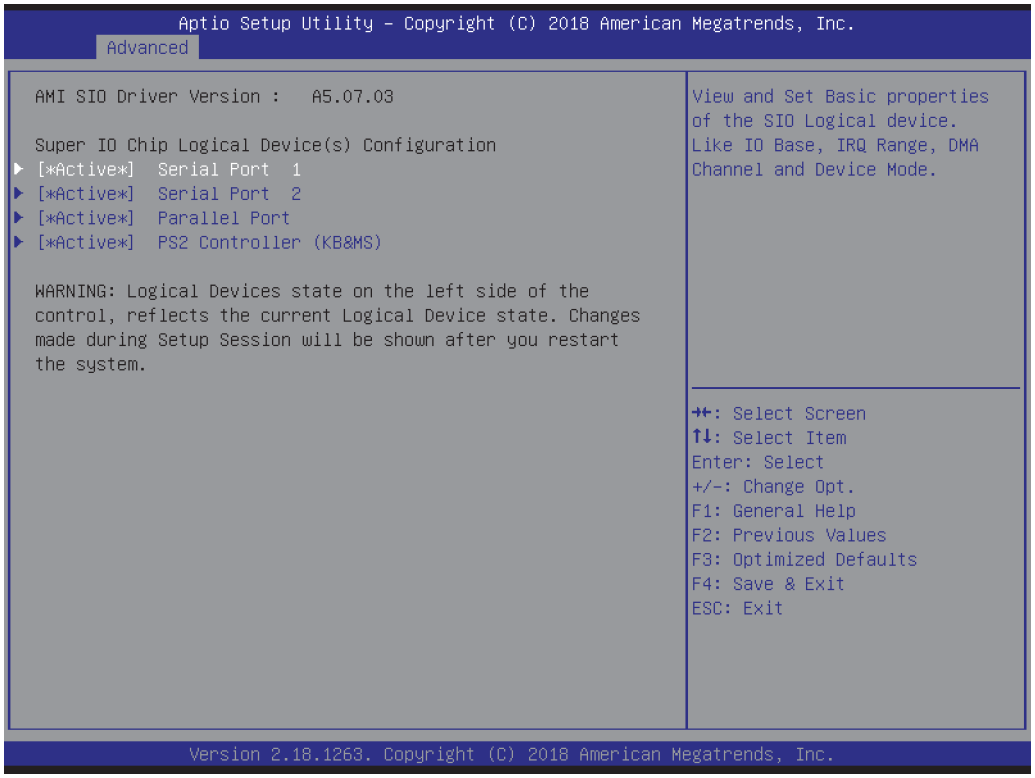
Parameter	Value	Comment
Critical Trip Point	15 ... 125 **125 (default)**	This value controls the temperature of the ACPI Critical Trip Point - the point at which the OS will shut the system off.
Passive Trip Point	15 ... 111 **111 (default)**	This value controls the temperature of the ACPI Passive Trip Point - the point at which the OS will begin throttling the processor.

SDIO Configuration



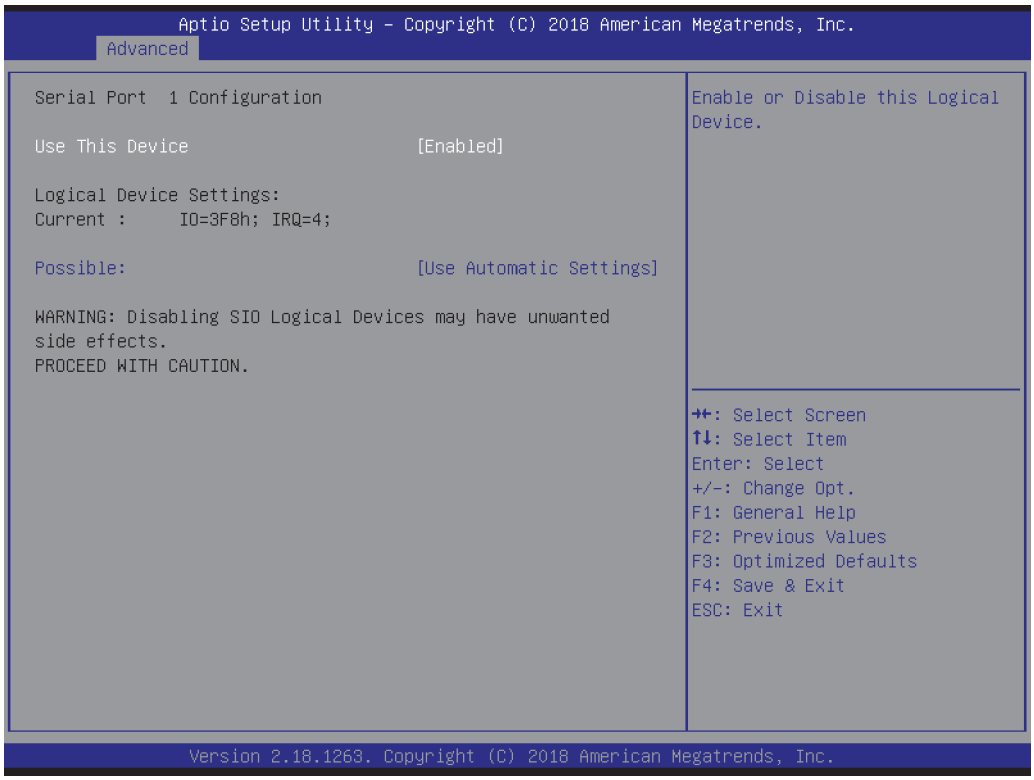
Parameter	Value	Comment
SDIO Access Mode	**Auto** ADMA SDMA PIO	Auto Option: Access SD device in DMA mode if controller supports it, otherwise in PIO mode. DMA Option: Access SD device in DMA mode. PIO Option: Access SD device in PIO mode.
Device Configuration	**Auto** Floppy Force FDD Hard Disk	Mass storage device emulation type. 'AUTO' enumerates devices less than 530MB as floppies. Forced FDD option can be used to force HDD formatted drive to boot as FDD.

SIO Configuration



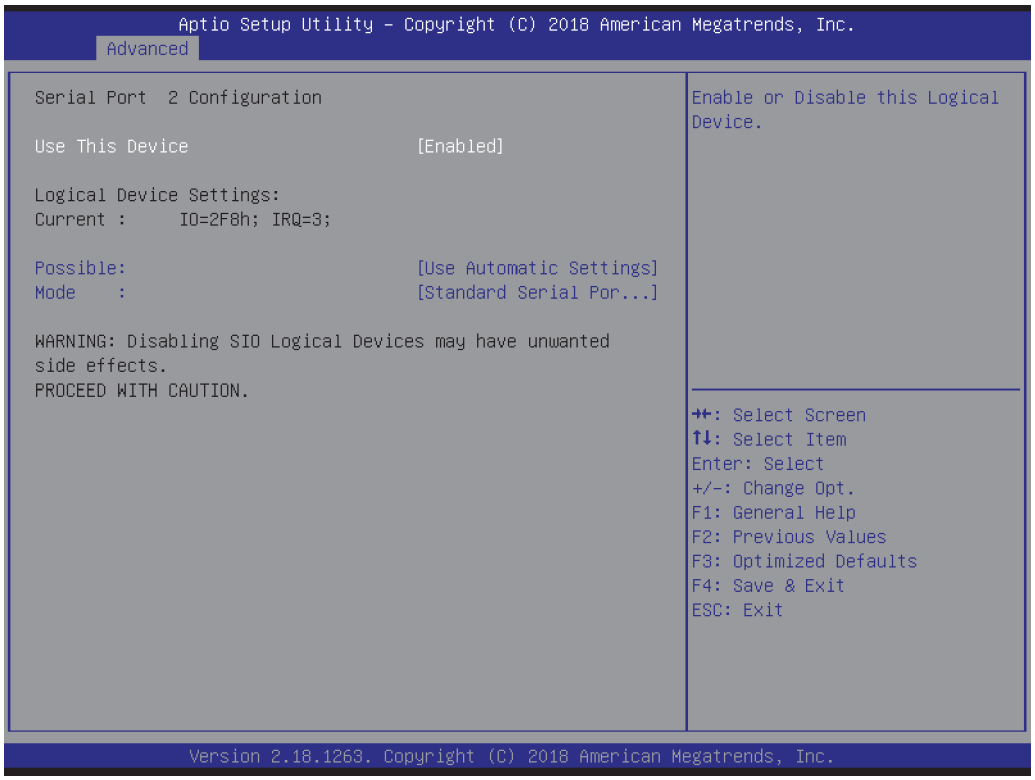
Parameter	Value	Comment
Serial Port 1	Submenu	View and set basic properties of the SIO logical device. Like IO base, IRQ range, DMA channel and device mode.
Serial Port 2	Submenu	
Parallel Port	Submenu	
PS2 Controller (KB&MS)	Submenu	

Serial Port 1 Configuration



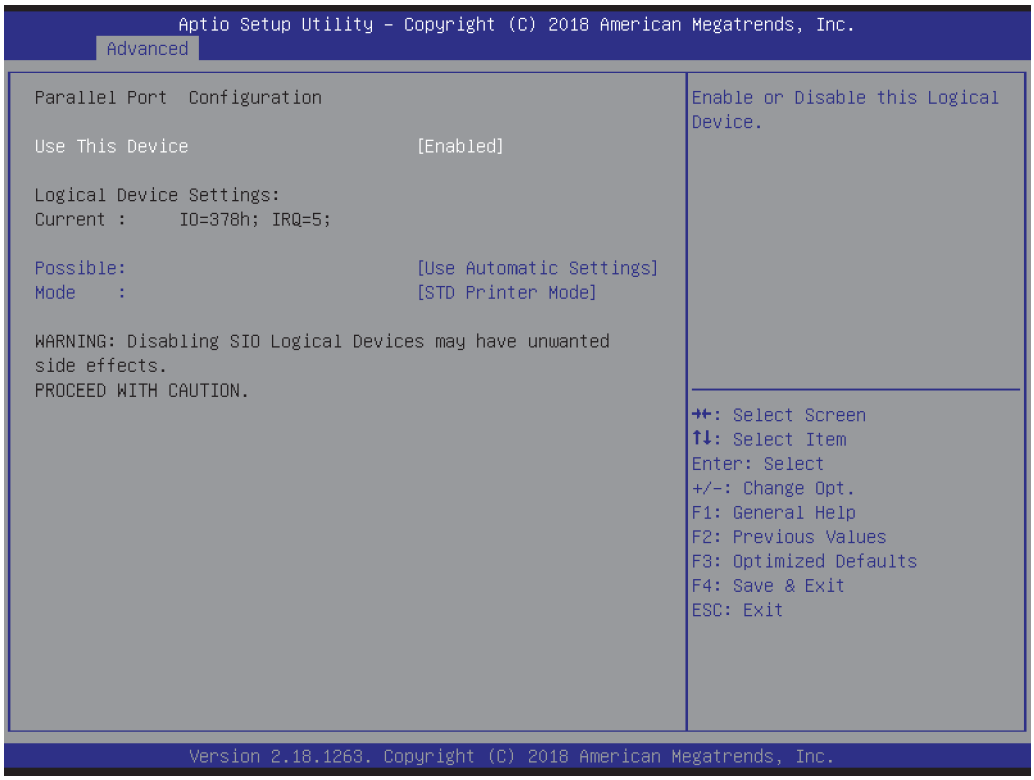
Parameter	Value	Comment
Use This Device	**Enabled** Disabled	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=3F8h; IRQ=4 IO=2F8h IO=3E8h IO=2E8h IRQ=3,4,5,7,9,10,11,12	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.

Serial Port 2 Configuration



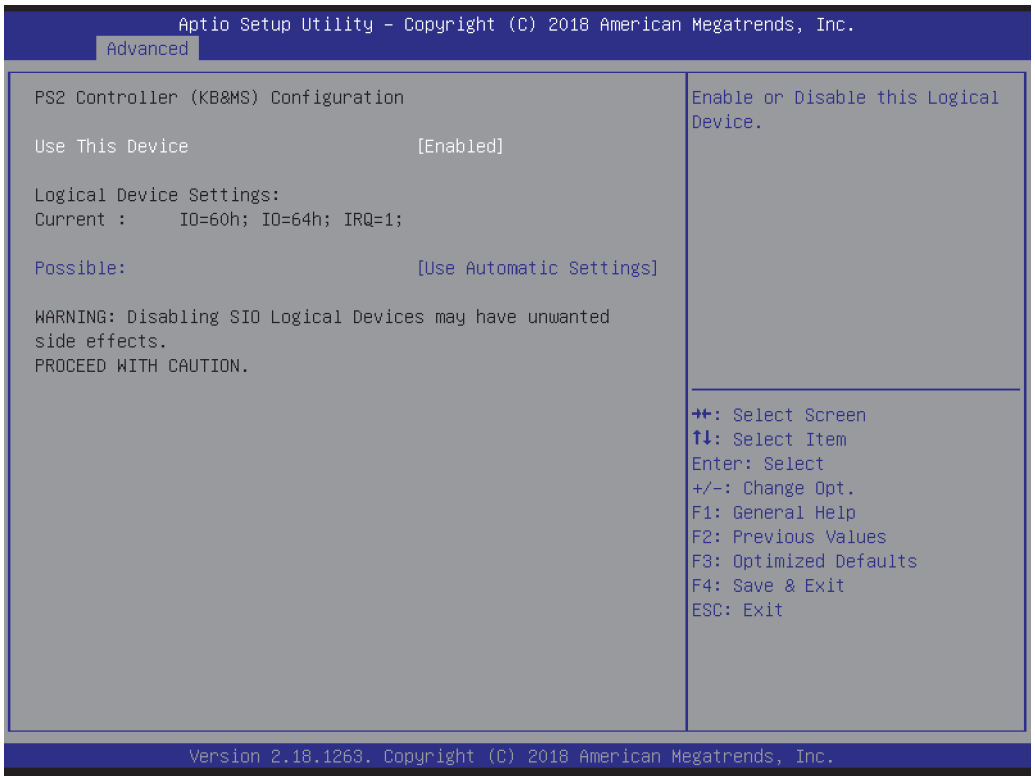
Parameter	Value	Comment
Use This Device	**Enabled** Disabled	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=3F8h; IRQ=4 IO=2F8h IO=3E8h IO=2E8h IRQ=3,4,5,7,9,10,11,12	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.
Mode	**Standard Serial Port Mode** IrDA Active pulse 1.6 µS IrDA Active pulse 3/16 bit time ASKIR Mode	Configure Standard or IrDA Mode of the Serial Port.

Parallel Port Configuration



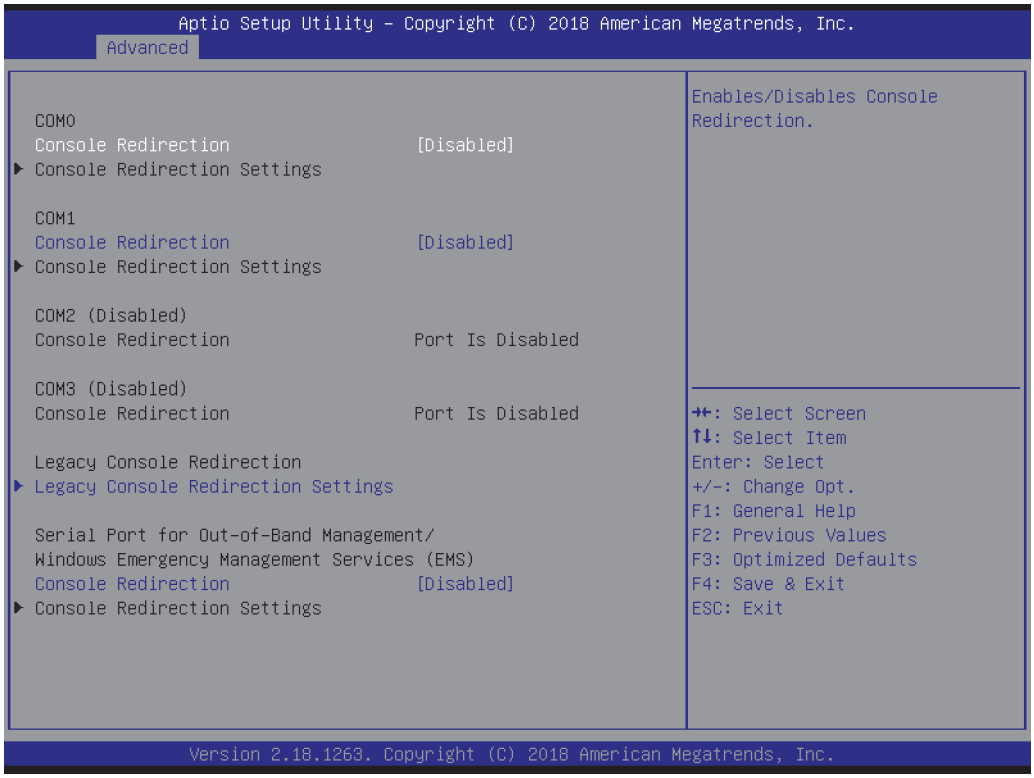
Parameter	Value	Comment
Use This Device	**Enabled** Disabled	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=378h; IRQ=5 IO=278h IO=3BCh IRQ=5,6,7,9,10,11,12	Configure Device's Resource settings. New settings will be reflected on This Setup Page after System restarts.
Mode	**STD Printer Mode** SPP Mode EPP-1.9 and SPP Mode EPP-1.7 and SPP Mode ECP Mode ECP and EPP 1.9 Mode ECP and EPP 1.7 Mode	Change Parallel Port mode. Some of the Modes required a DMA resource. After Mode changing, Reset the System to reflect actual device settings.

PS2 Controller (KB&MS) Configuration



Parameter	Value	Comment
Use This Device	**Enabled** Disabled	Enable or Disable this Logical Device.
Possible	**Use Automatic Settings** IO=60h; IO=64h; IRQ=1	Configure Device's Resource settings. New settings will be reflected on this Setup Page after System restarts.

Serial Port Console Redirection



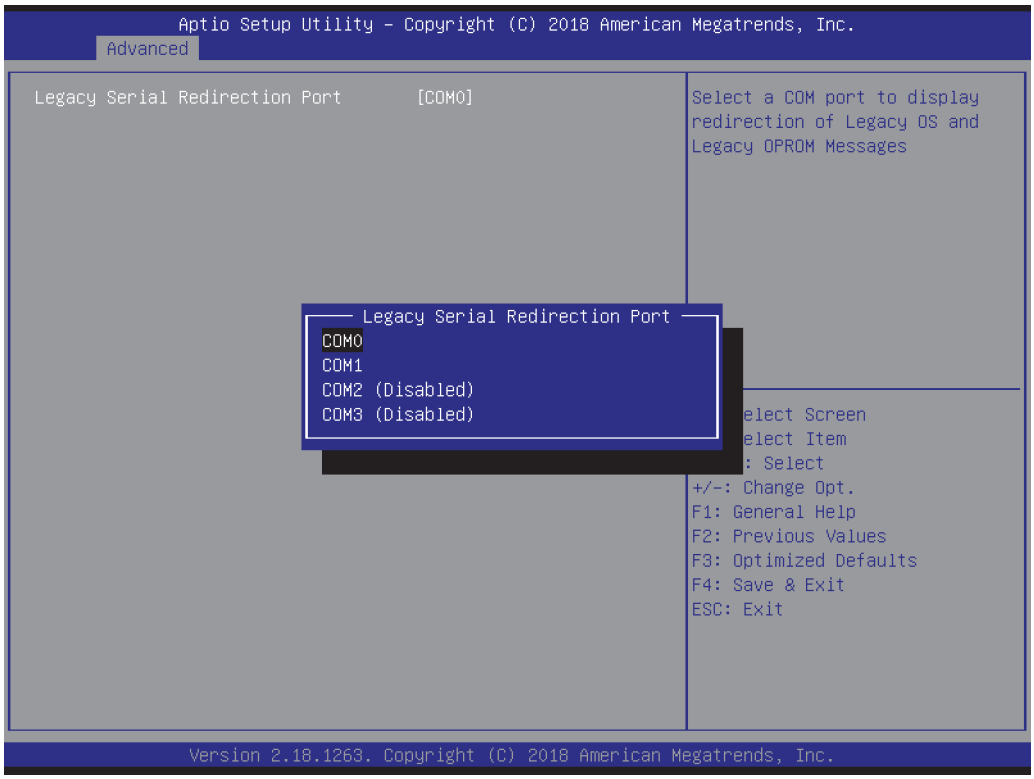
Parameter	Value	Comment
Console Redirection	Enabled **Disabled**	Enables/Disables Console Redirection.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
Legacy Console Redirection Settings	Submenu	Configure Port for Legacy Console Redirection.

Console Redirection Settings

Parameter	Value	Comment
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Configures the number of data bits. 8 is recommended to easily use the link for file transfer and non-English text transfer.
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	**Enabled** Disabled	Enable: VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	Enabled **Disabled**	With this mode enabled, only text will be sent. This is to capture Terminal data.
Resolution 100x31	**Enabled** Disabled	Enables/Disables extended terminal resolution.

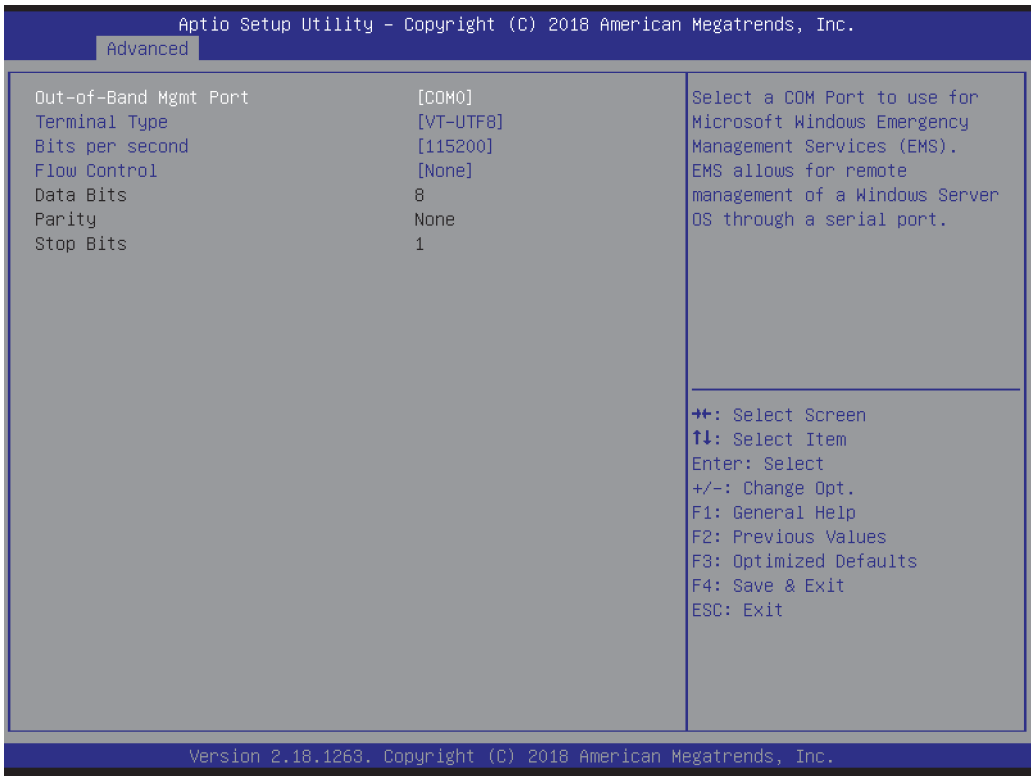
Parameter	Value	Comment
Legacy OS Redirection Resolution	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported by redirection.
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	**Enabled** Disabled	Enabled: Console Redirection is available for Legacy OS. Disabled: Legacy console redirection is disabled before booting to Legacy OS.

Legacy Console Redirection Settings



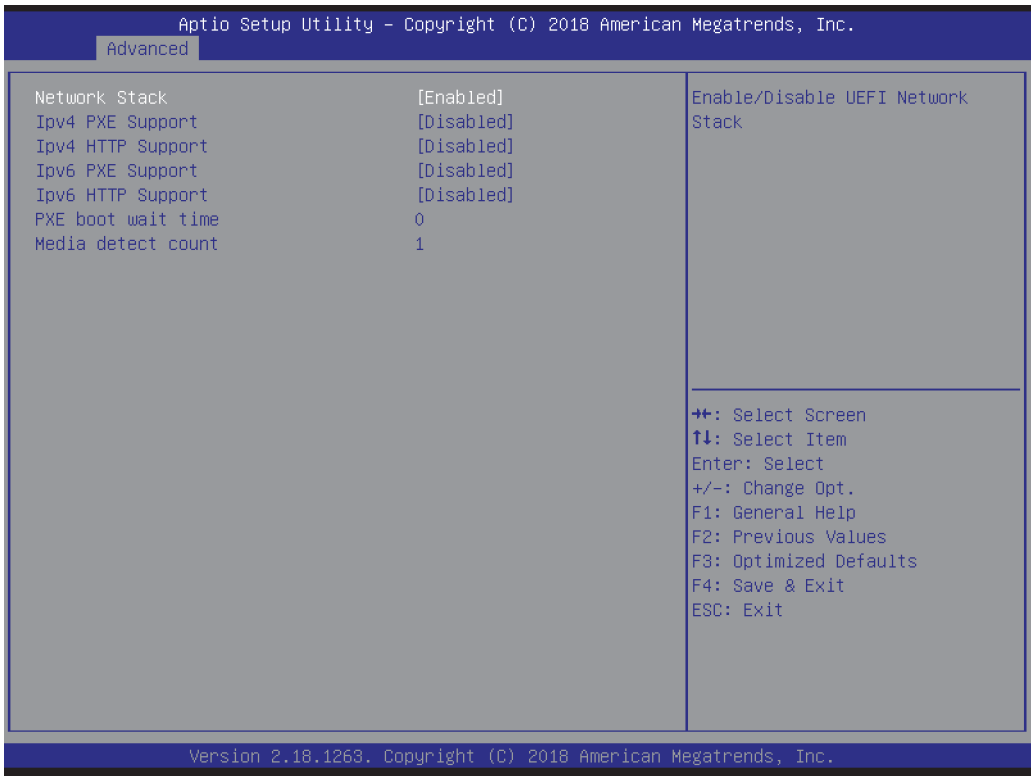
Parameter	Value	Comment
Legacy Redirection COM Port	**COM0** COM1 COM2 COM3	Select a COM Port to use for Legacy OS and Legacy OPROM Console Redirection.

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)



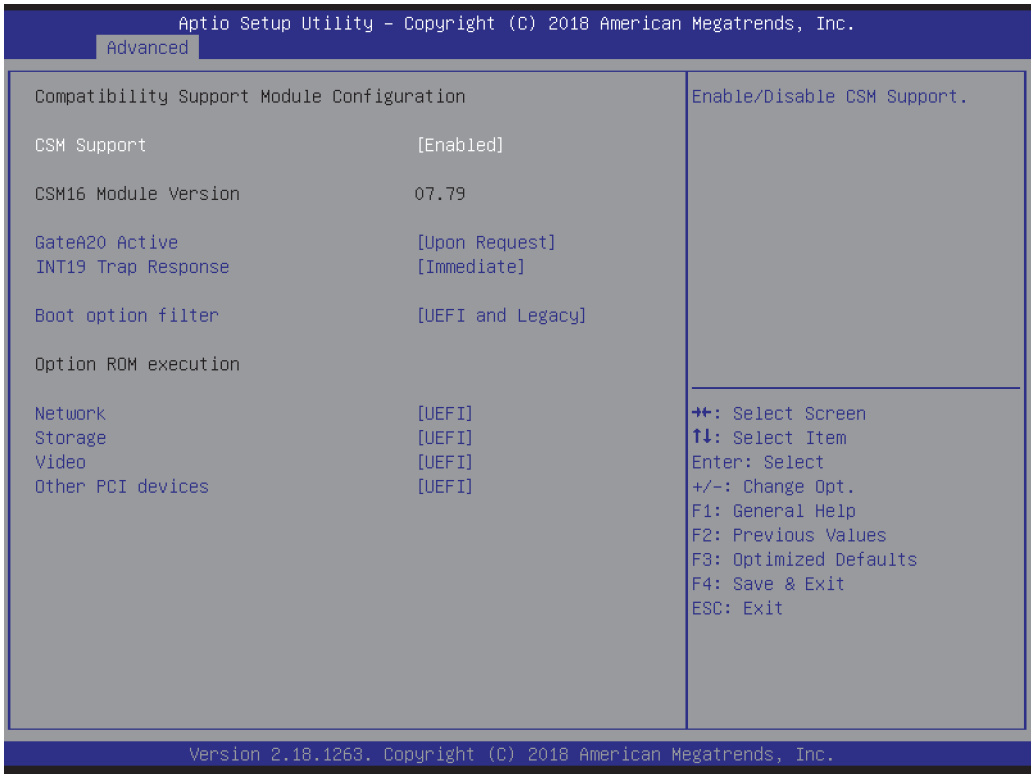
Parameter	Value	Comment
Out-of-Band Mgmt Port	**COM0** COM1 COM2 COM3	Select a COM Port to use for Microsoft Windows Emergency Management Services (EMS). EMS allows for remote management of a Windows Server OS through a serial port.
Terminal Type	VT100 VT100+ **VT-UTF8** ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per seconds	9600 19200 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	**None** Hardware RTS/CTS Software Xon/Xoff	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

Network Stack Configuration



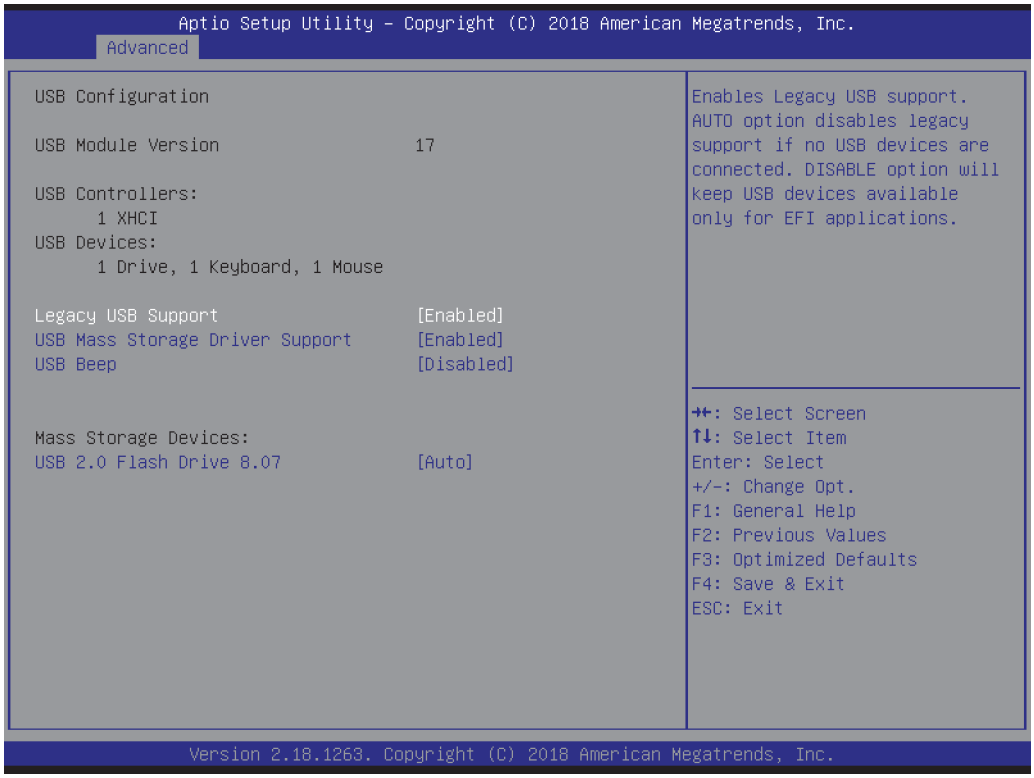
Parameter	Value	Comment
Network Stack	Enabled **Disabled**	Enable/Disable UEFI Network Stack.
Ipv4 PXE Support	Enabled **Disabled**	Enable Ipv4 PXE Boot Support. If disabled IPV4 PXE boot option will not be created.
Ipv4 HTTP Support	Enabled **Disabled**	Enable Ipv4 HTTP Boot Support. If disabled IPV4 HTTP boot option will not be created.
Ipv6 PXE Support	Enabled **Disabled**	Enable Ipv6 PXE Boot Support. If disabled IPV6 PXE boot option will not be created.
Ipv6 HTTP Support	Enabled **Disabled**	Enable Ipv6 HTTP Boot Support. If disabled IPV6 HTTP boot option will not be created.
PXE boot wait time	0 ... 5 (**0** default)	Wait time to press ESC key to abort the PXE boot.
Media detect count	1 ... 50 (**1** default)	Number of times presence of media will be checked.

Compatibility Support Module (CSM) Configuration



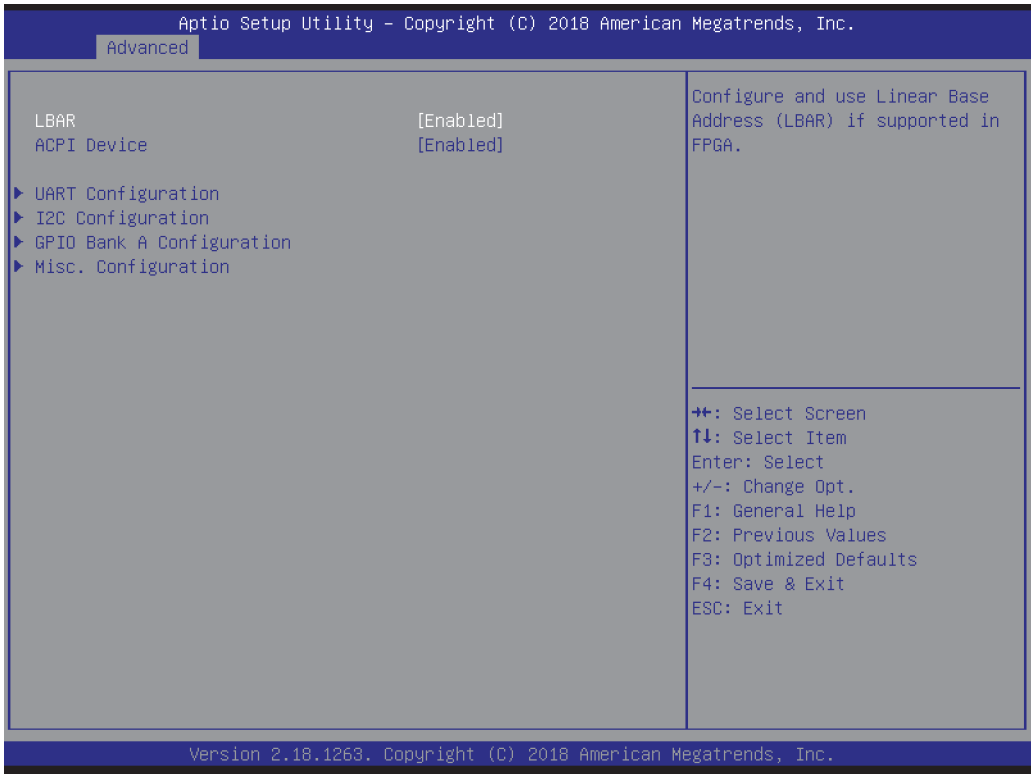
Parameter	Value	Comment
CSM Support	Enabled **Disabled**	Enable/Disable CSM Support.
GateA20 Active	**Upon Request** Always	UPON REQUEST – GA20 can be disabled using BIOS services. ALWAYS – do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	**Force BIOS** Keep Current	Force BIOS: Change display to text mode and show OpROM messages. Keep Current: Don't change display mode and suppress legacy OpROM messages.
INT19 TRAP Response	**Immediate** Postponed	BIOS reaction on INT19 trapping by Option ROM: IMMEDIATE – execute the trap right away; POSTPONED – execute the trap during legacy boot.
Boot Option Filter	**UEFI and Legacy** Legacy only UEFI only	Configure available boot options.
Network	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy PXE OpROM.
Storage	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy Storage OpROM.
Video	Do not launch **UEFI** Legacy	Controls the execution of UEFI and Legacy Video OpROM.
Other PCI Devices	Do not launch **UEFI** Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video.

USB Configuration



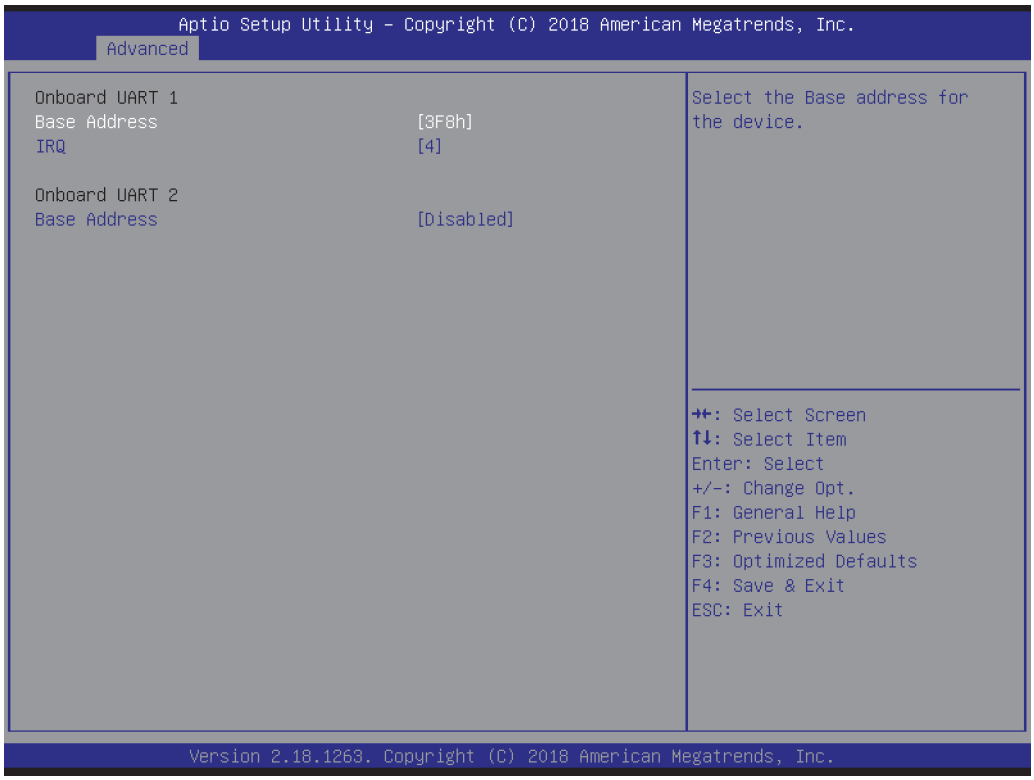
Parameter	Value	Comment
Legacy USB Support	**Enabled** Disabled Auto	Enables Legacy USB support. Auto: Disables legacy support if no USB devices are connected. Disabled: Keep USB devices available only for EFI applications.
USB Mass Storage Driver Support	**Enabled** Disabled	Enable/Disable USB Mass Storage Driver Support.
USB Beep	Enabled **Disabled**	Enable/Disable Beep on USB events.
Mass Storage Devices	**Auto** Floppy Forced FDD Hard Disk CD-ROM	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CD-ROM', drives with no media information will be emulated according to a drive type.

Module Peripherals Configuration



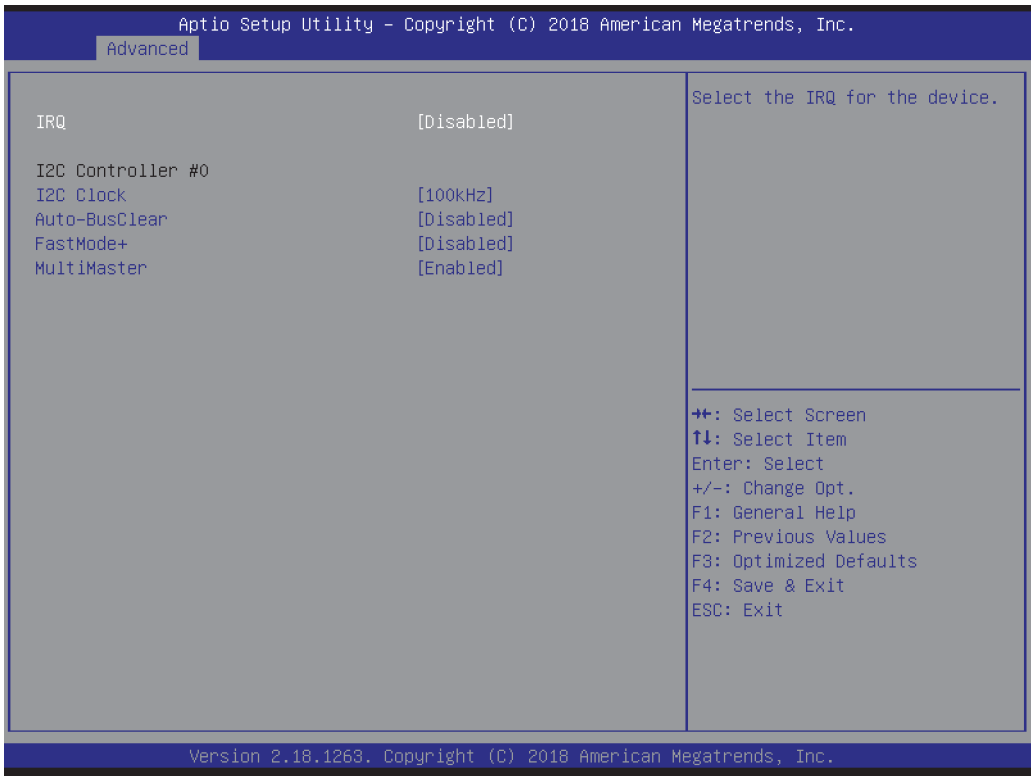
Parameter	Value	Comment
LBAR	**Enabled** Disabled	Configure and use Linear Base Address (LBAR) if supported in FPGA.
ACPI Devices	**Enabled** Disabled	Select how resources are reported to the OS via ACPI. Enabled: Separate device, may require Driver. Disabled: Motherboard Resource.
UART Configuration	Submenu	Configure integrated UARTs.
I2C Configuration	Submenu	Configure integrated I2C controllers.
GPIO Bank A Configuration	Submenu	Configure GPIO Bank A pins.
Misc. Configuration	Submenu	Miscellaneous Configuration

UART Configuration



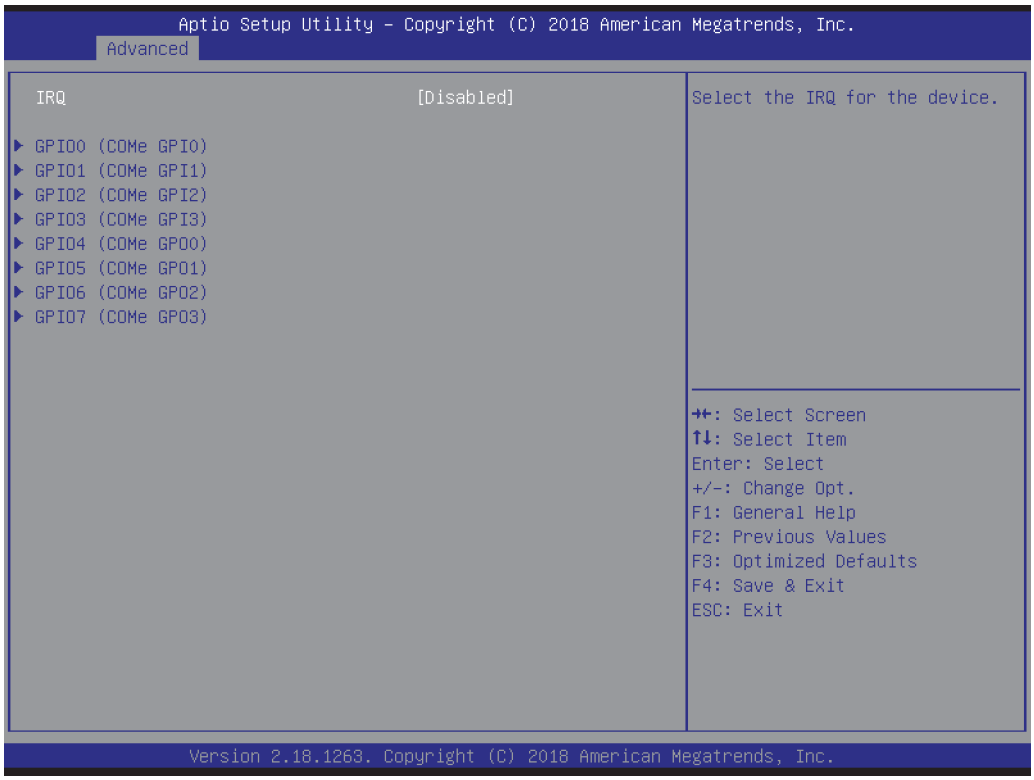
Parameter	Value	Comment
Base Address	**Disabled** 3F8h 2F8h 3E8h 2E8h	Select the Base address for the device.
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.

I2C Configuration



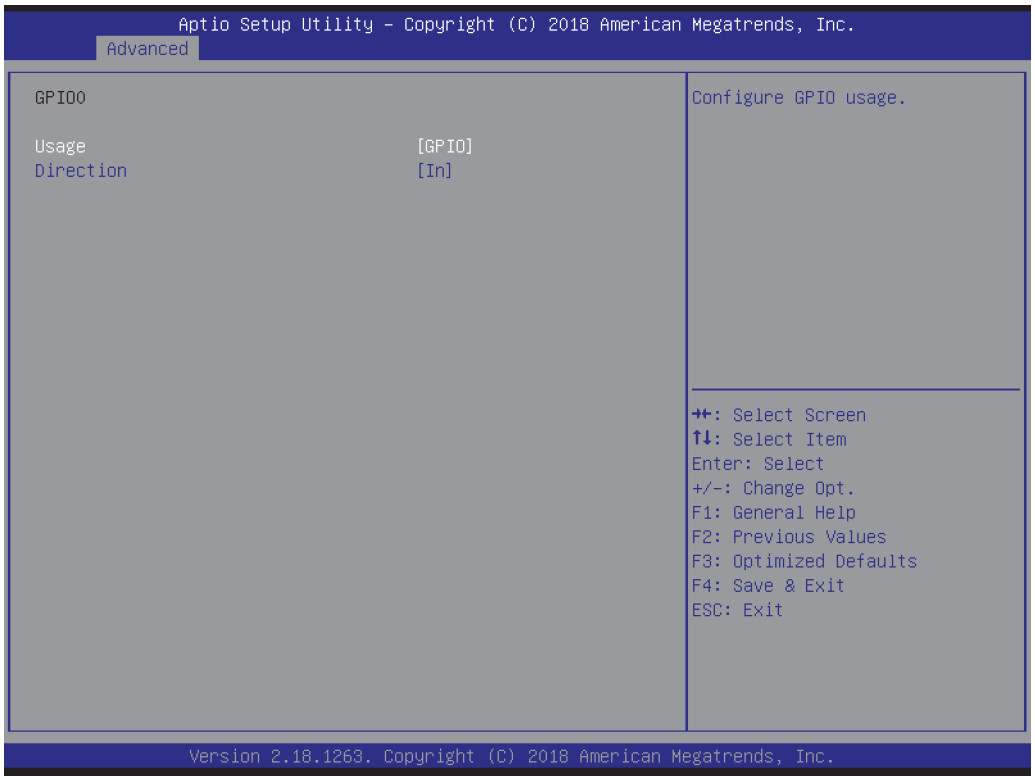
Parameter	Value	Comment
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.
I2C Clock	1kHz 10kHz 50kHz **100kHz** 200kHz 400kHz 625kHz 800kHz	Select I2C Speed (OS driver may use different speed). Note: Depending on I2C controller, actual speed may be slightly below selected values.
Auto-BusClear	**Disabled** Automatic	If enabled, the I2C controller monitors the SDA line for conditions where the slave device blocks it and tries to recover the bus by pulsing the SCL line. Note: If enabled, the multi-master capability is no longer guaranteed!
FastMode+	Enabled **Disabled**	If enabled, the SCL line is switched from open drain to push-pull to allow for higher speeds. Note: If enabled, multi-master capability and Clock stretching functionality is no longer guaranteed!
MultiMaster	**Enabled** Disabled	If disabled, the I2C master will omit bus arbitration.

GPIO Configuration



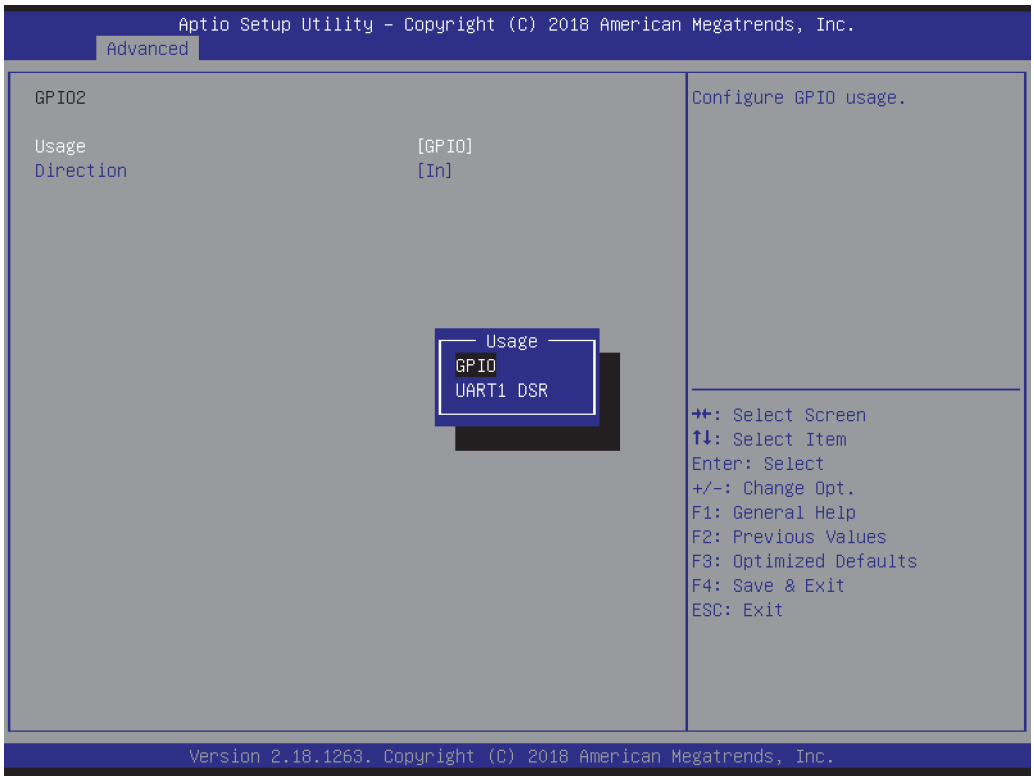
Parameter	Value	Comment
IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the device.
GPIO0 (COMe GPI0)	Submenu	Configure GPIO Bank A pins.
GPIO1 (COMe GPI1)	Submenu	
GPIO2 (COMe GPI2)	Submenu	
GPIO3 (COMe GPI3)	Submenu	
GPIO4 (COMe GPO0)	Submenu	
GPIO5 (COMe GPO1)	Submenu	
GPIO6 (COMe GPO2)	Submenu	
GPIO7 (COMe GPO3)	Submenu	

GPIO0, GPIO1, GPIO3



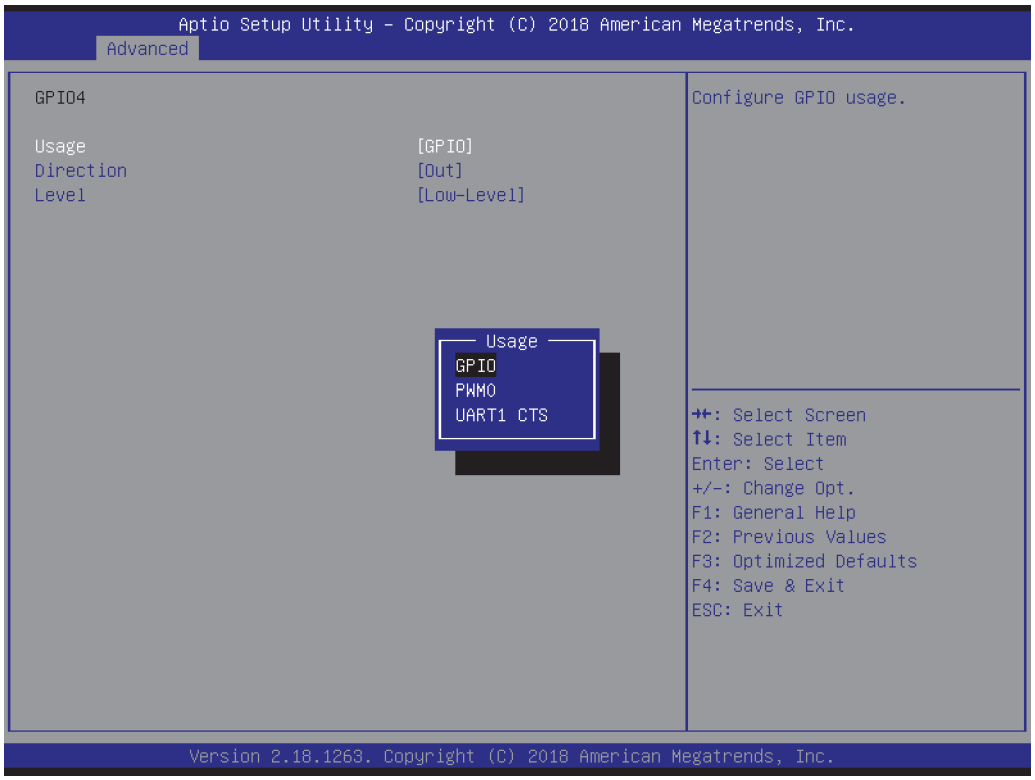
Parameter	Value	Comment
Usage	**GPIO**	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO2



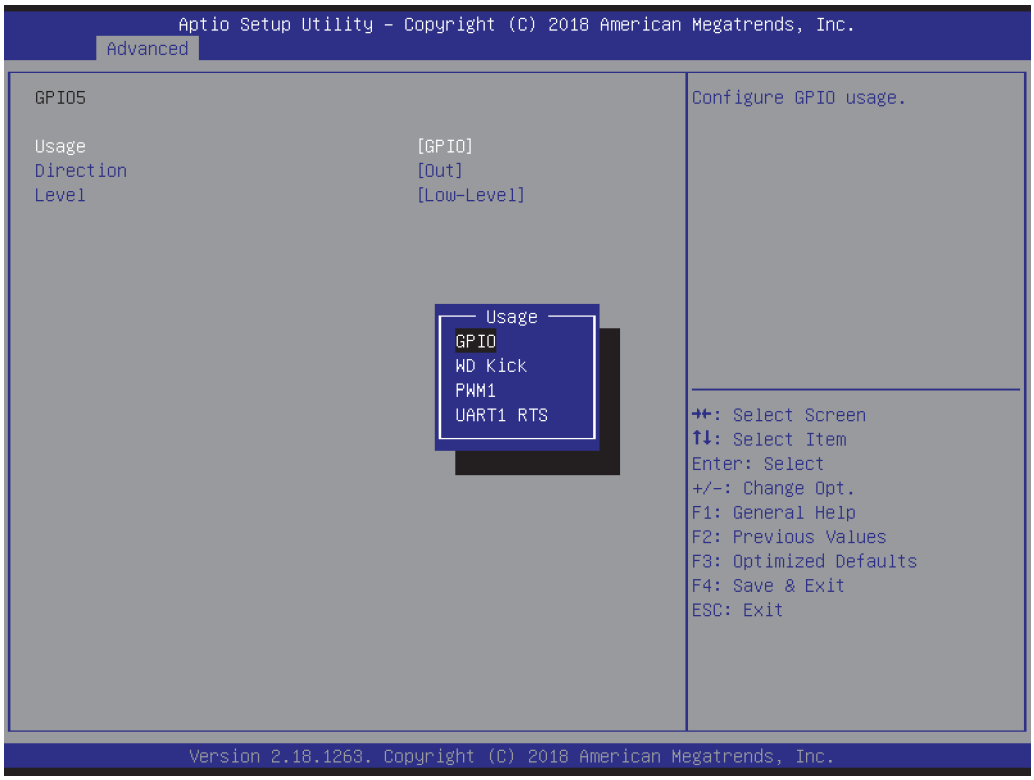
Parameter	Value	Comment
Usage	**GPIO** UART1 DSR	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO4



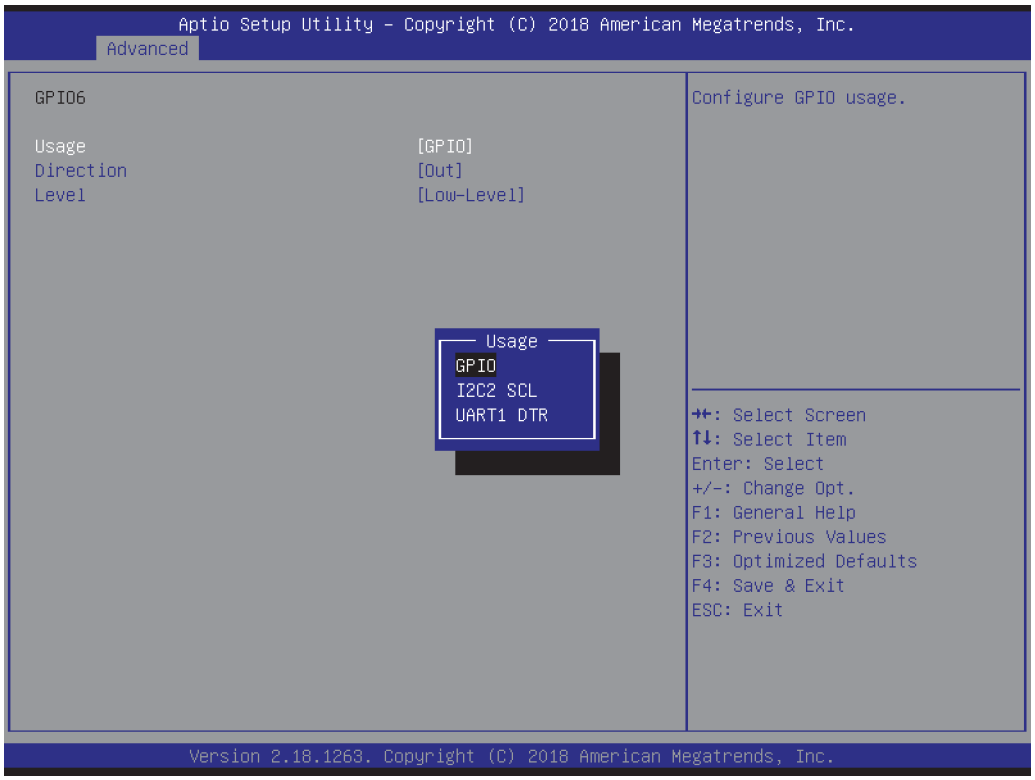
Parameter	Value	Comment
Usage	**GPIO** PWM0 UART1 CTS	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO5



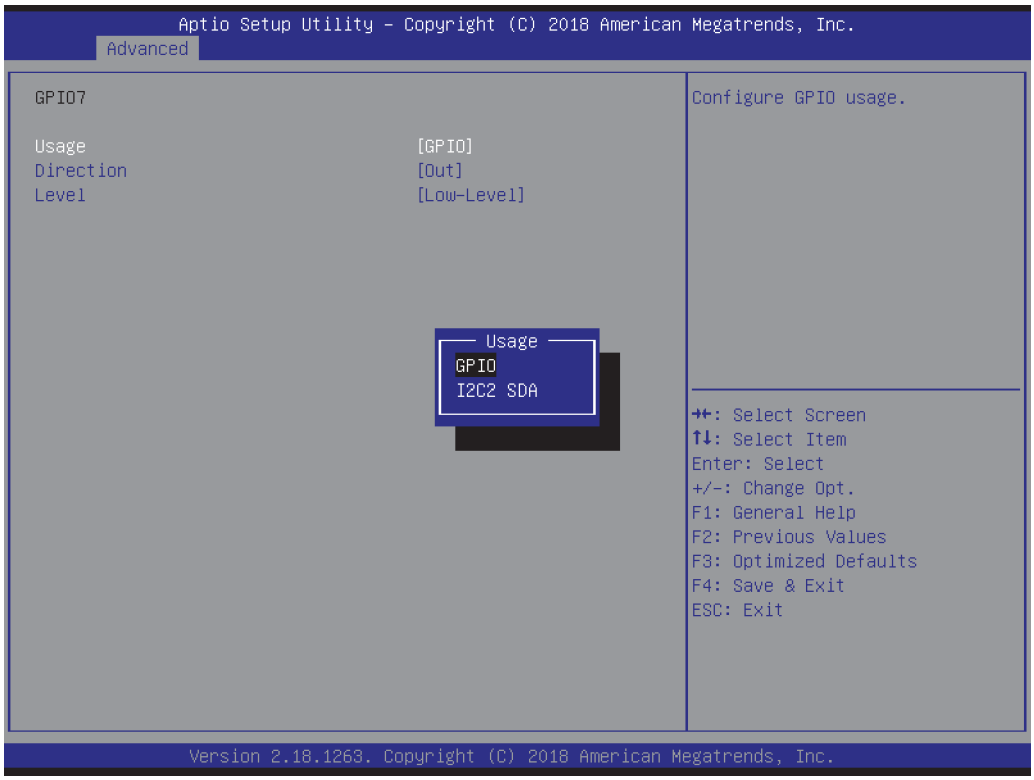
Parameter	Value	Comment
Usage	**GPIO** WD Kick **PWM1** UART1 RTS	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO6



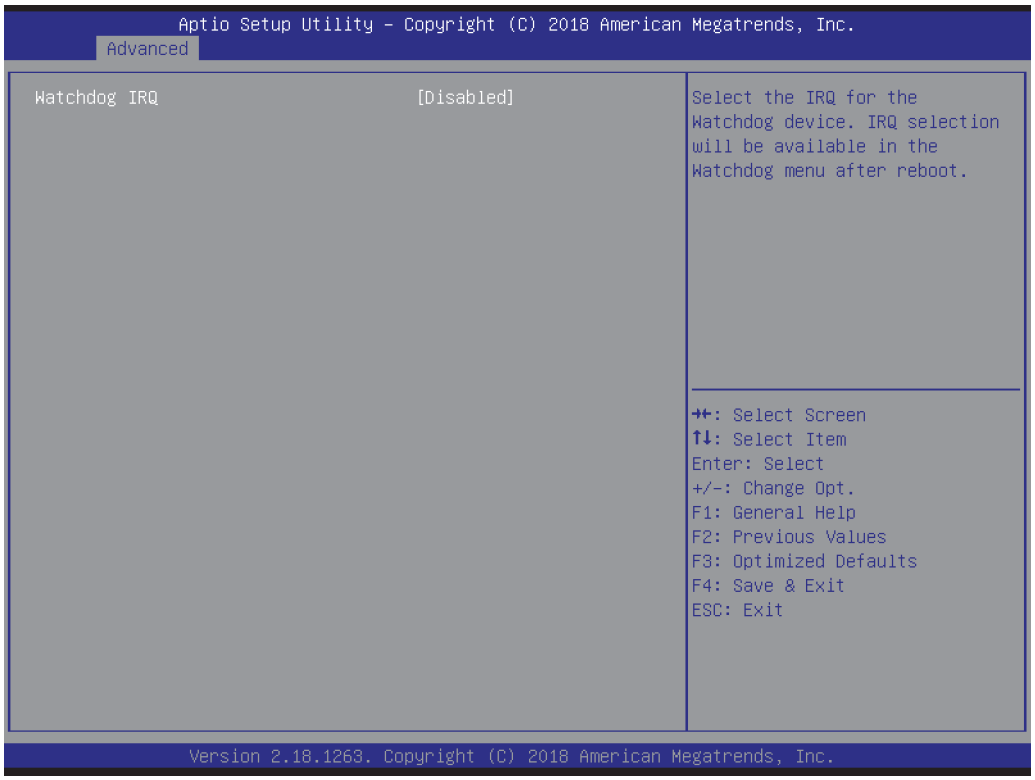
Parameter	Value	Comment
Usage	**GPIO** I2C2 SCL UART1 DTR	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

GPIO7



Parameter	Value	Comment
Usage	**GPIO** I2C2 SDA	Configure GPIO usage.
Direction	In **(default for GPIO0-3)** Out **(default for GPIO5-7)**	Configure GPIO direction.
Level	**Low-Level** High-Level	Configure GPIO initial level.

Misc. Configuration



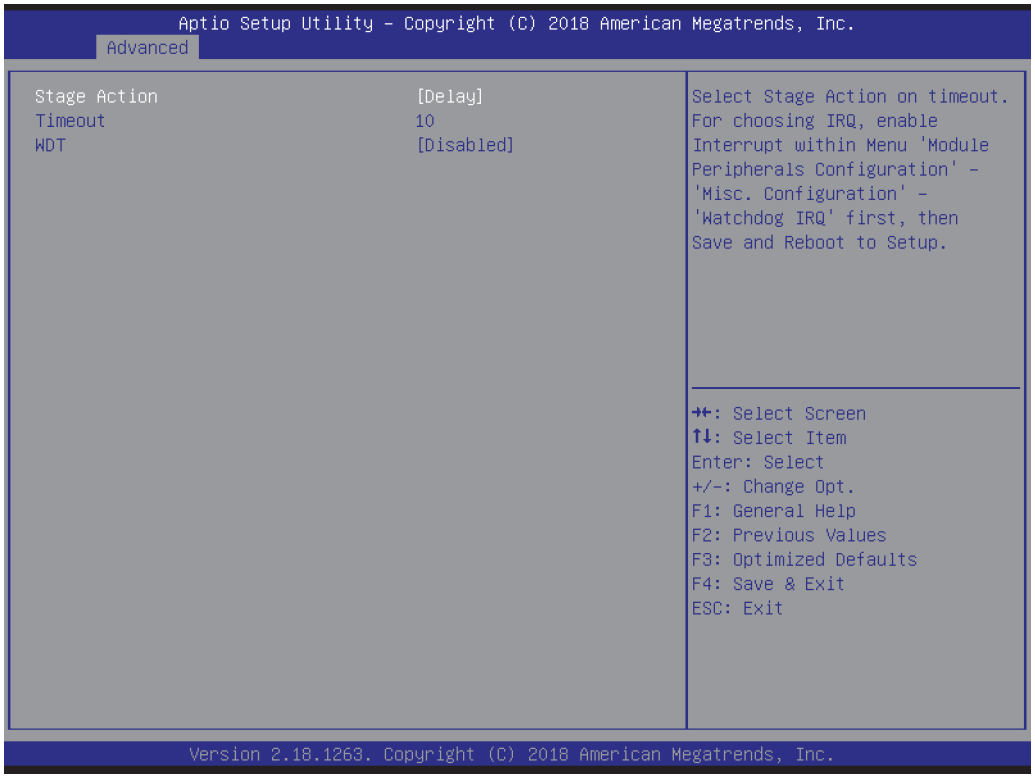
Parameter	Value	Comment
Watchdog IRQ	**Disabled** 3, 4, 5, 6, 7, 10, 11, 12, 14, 15	Select the IRQ for the Watchdog device. IRQ selection will be available in the Watchdog menu after reboot.

Module Watchdog Configuration

Standard Mode

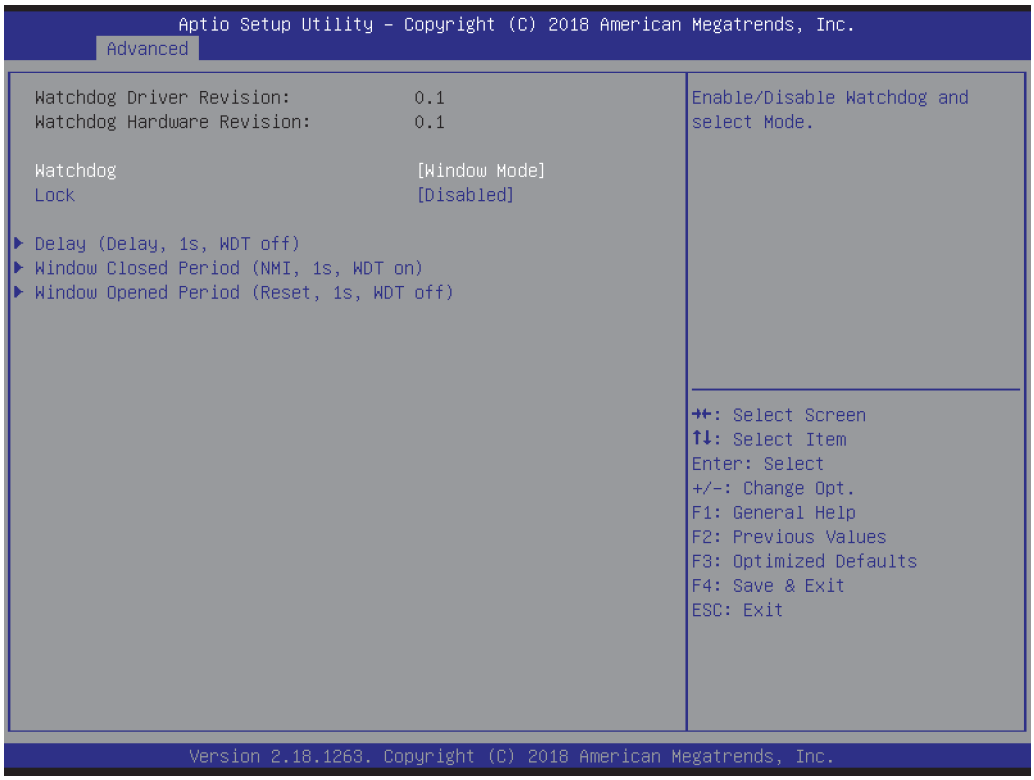
Parameter	Value	Comment
Watchdog	**Disabled** Standard Mode Window Mode	Enable/Disable Watchdog and select Mode.
Auto Reload	Enabled **Disabled**	Enable Auto Reload. If enabled, Timeout registers will be reloaded automatically after expiration.
Lock	Enabled **Disabled**	If enabled, the Watchdog registers will be locked and become read only after initialization.
Stage	Submenu	Configure Watchdog Stage.

Stage Configuration



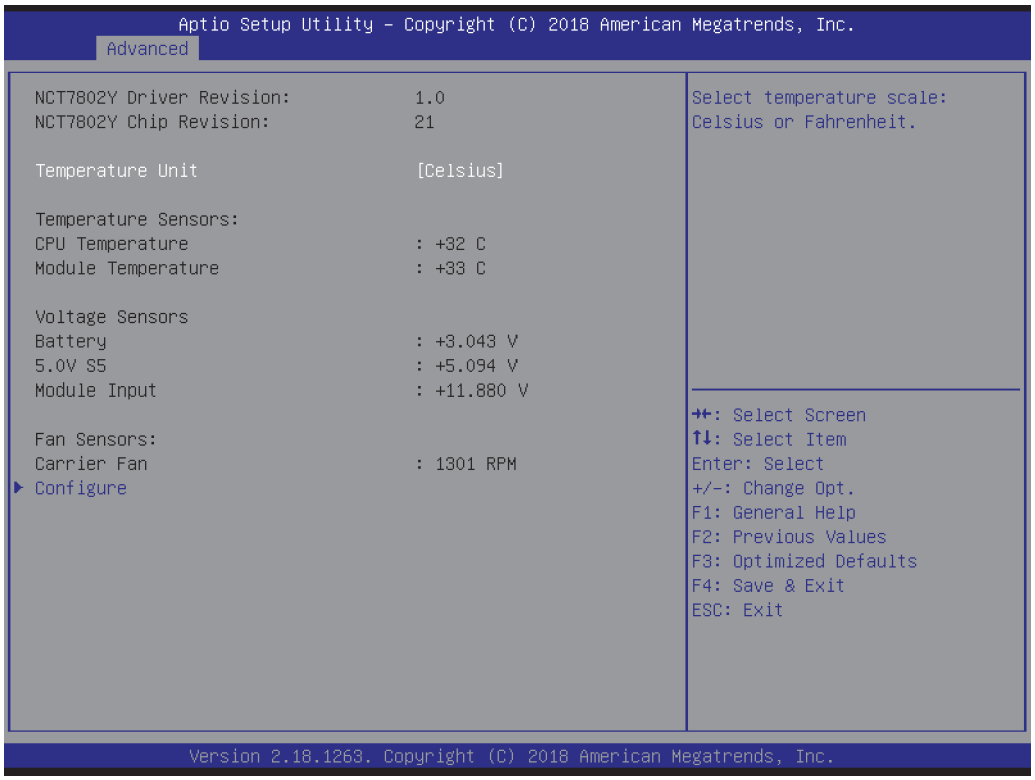
Parameter	Value	Comment
Stage Action	**Disabled** Delay Reset NMI IRQ	Select Stage Action on timeout. For choosing IRQ, enable Interrupt within Menu 'Module Peripherals Configuration' – 'Misc. Configuration' – Watchdog IRQ' first, then Save and Reboot to Setup.
Timeout	1 ... 65535 (**1** default)	Select the timeout value for the stage.
WDT#	Enabled **Disabled**	Assert WDT# signal to Baseboard.

Window Mode



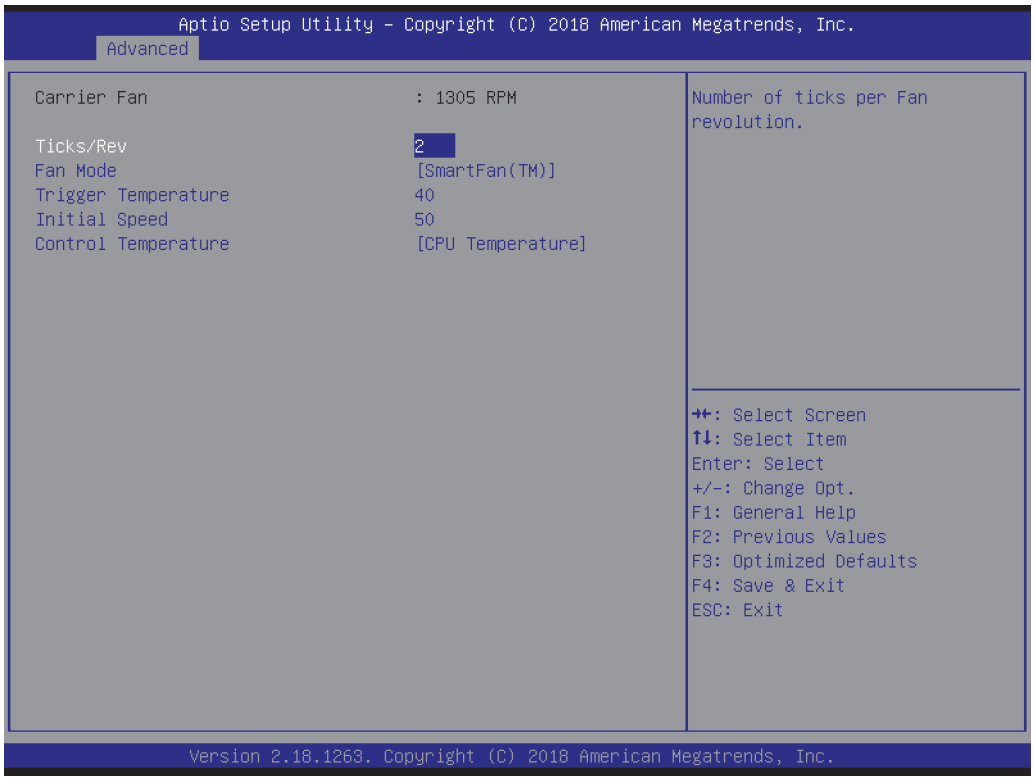
Parameter	Value	Comment
Watchdog	**Disabled** Standard Mode Window Mode	Enable/Disable Watchdog and select Mode.
Lock	Enabled **Disabled**	If enabled, the Watchdog registers will be locked and become read only after initialization.
Delay	Submenu	Enable/Disable Watchdog and select Mode.
Window Closed Period	Submenu	Trigger events during this period will be treated as error and cause the time-out event selected in the Window Open Stage.
Window Opened Period	Submenu	Trigger events during this period will reload the watchdog timer and transition the internal state machine to the Window Closed Stage.

Module H/W Monitor



Parameter	Value	Comment
Temperature Unit	**Celsius** Fahrenheit	Select temperature scale Celsius or Fahrenheit.
Configure Fan Sensors	Submenu	Configure Fan parameters.

Fan Configuration



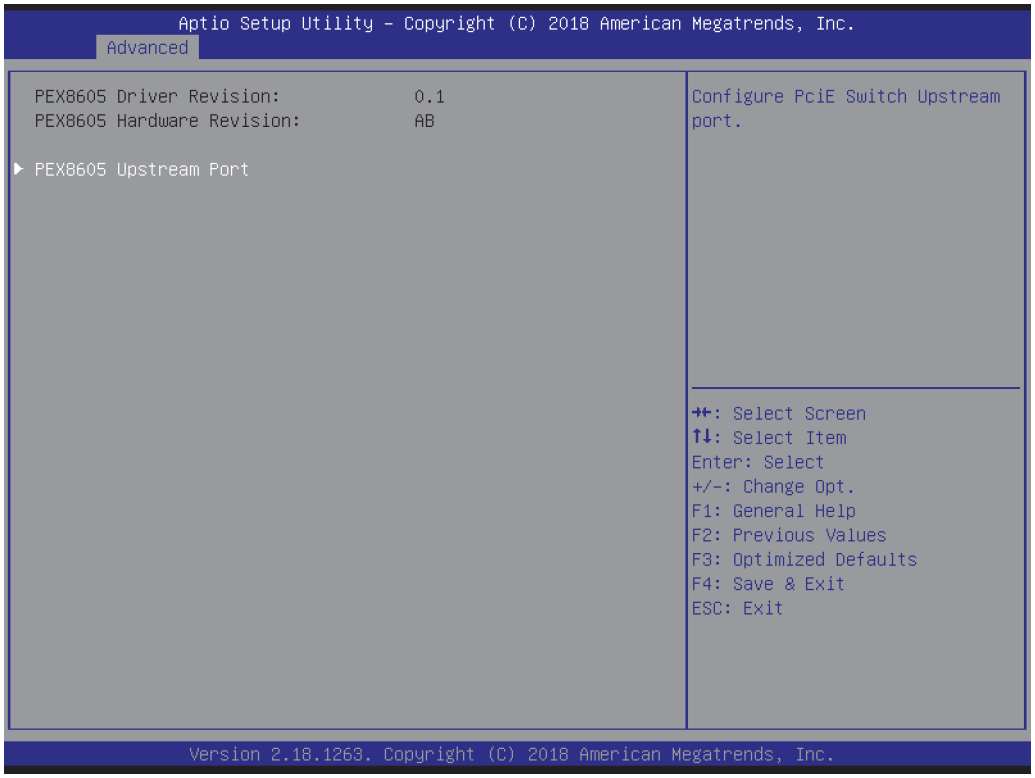
Parameter	Value	Comment
Ticks/Rev	1 ... 16 (**2** default)	Number of ticks per Fan revolution.
Fan Mode	Off Manual **SmartFan(TM)**	Select Fan mode of operation.
Fan Speed	10 ... 100 (**40** default)	Select fixed Fan Speed in %.
Trigger Temperature	Celsius: 20 ... 80 (**40** default) **Fahrenheit:** 68 ... 176 (**104** default)	Select the temperature at which the Fan starts spinning.
Initial Speed	10 ... 80 (**50** default)	Initial Fan Speed in %.
Control Temperature	**CPU Temperature** PCH Temperature Module Temperature	Temperature to use.

Module Display Configuration

Parameter	Value	Comment
Primary IGFX Boot Display	**Auto** LFP EFP1 EFP2	Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display.
Secondary IGFX Boot Display	**Disabled** LFP EFP1 EFP2	Select Secondary Display Device.
LFP Panel Type	**Auto** LVDS EEPROM Carrier EEPROM Module EERPOM 640x480 800x600 ...	Select LFP timings used by Internal Graphics Device. LVDS, Carrier and Module EEPROM timings are available if appropriate data is found.
LFP Fallback Type	**Disabled** 640x480 800x600 ...	Enable LFP with selected timings if auto detection fails.
Panel Color Depth	**18 Bit** 24 Bit VESA 24 Bit oLDI	Panel Color Depth for EDID 1.3 detection.
Panel Channel Count	**Single Channel** Dual Channel	Panel Channel Count for EDID detection.
Backlight Type	None **PWM** PWM Inverted I2C I2C inverted	Select Backlight Inverter Type and Polarity.
Backlight Value	0 ... 100 (**50** default)	Set Backlight Value in Percentage.
PWM Frequency	200 ... 40000 Hz (**200 Hz** default)	Set PWM Frequency in Hz.

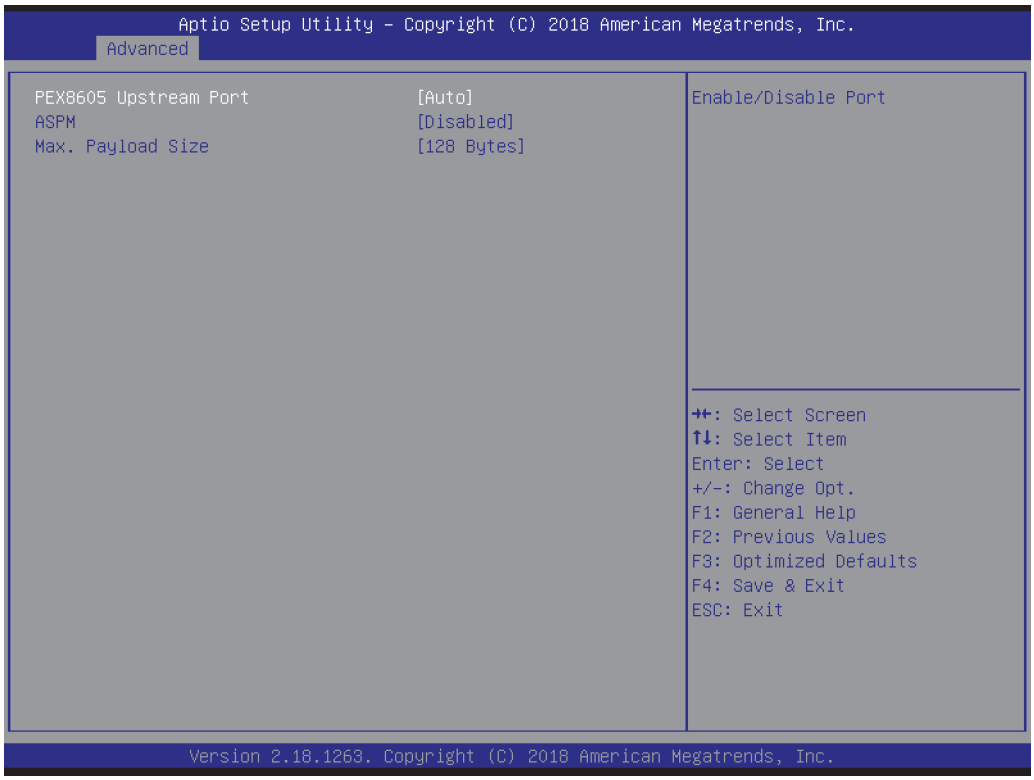
Parameter	Value	Comment
Backlight On	**Enabled** At the End of Post	Configure if LVDS Backlight should be set when panel is powered, or inhibit until End Of Post.
Backlight OS Controlled	**Enabled** Disabled	Configure if PWM values can be overridden by OS Power Options.
LVDS Spread Spectrum	**Disabled** 0.5 % 1.0 % 1.5 % 2.0 % 2.5 %	Set LVDS Center Spreading.
EFP Type	HDMI/DVI **DP w. HDMI/DVI Comp.** DP only	Select the type of the EFP.

Module PCI Express Switch



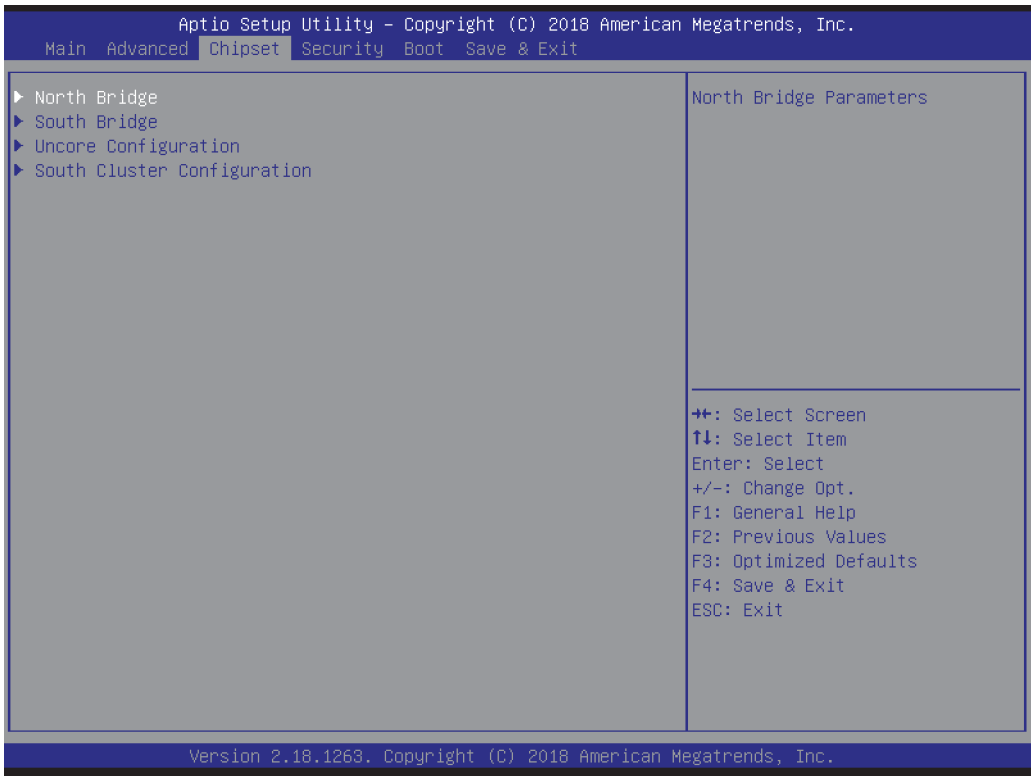
Parameter	Value	Comment
PEX8605 Upstream Port	Submenu	Configure PCIe Switch Upstream port.

PEX8605 Upstream Port



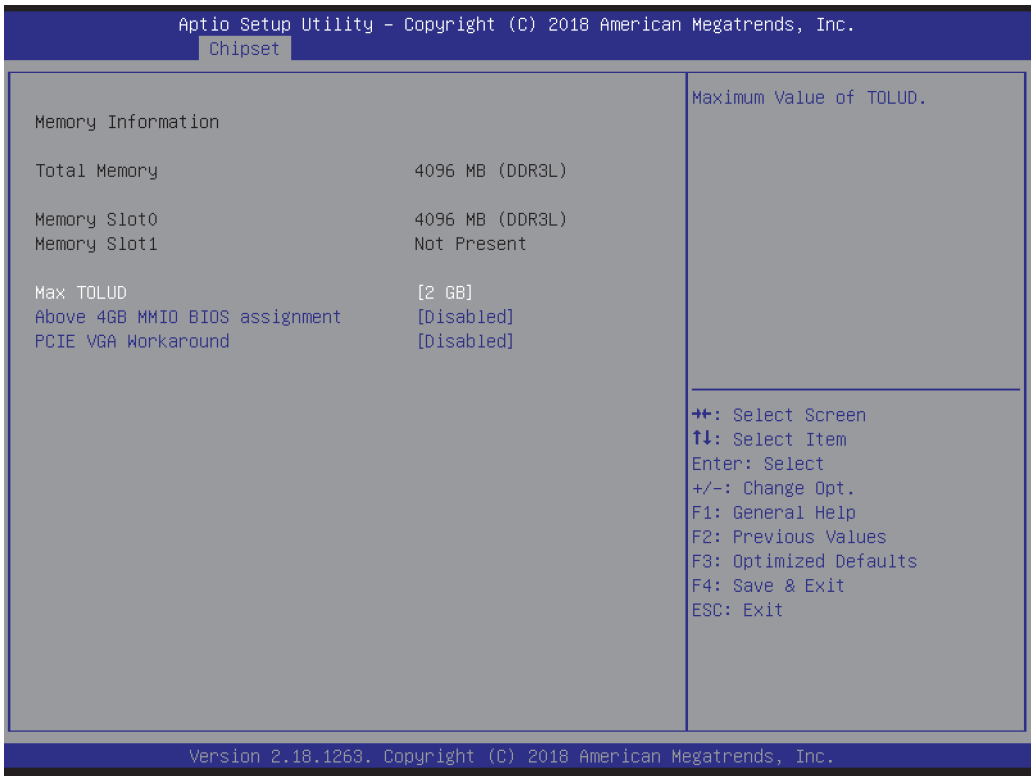
Parameter	Value	Comment
PEX8605 Upstream Port	**Auto** Enabled Disabled	Enable/ Disable Port.
ASPM	**Disabled** L0s L1 L0sL1 Auto	PCI Express Active State Power Management settings.
Max. Payload Size	**128 Bytes** 256 Bytes	Select maximum payload size.

Chipset



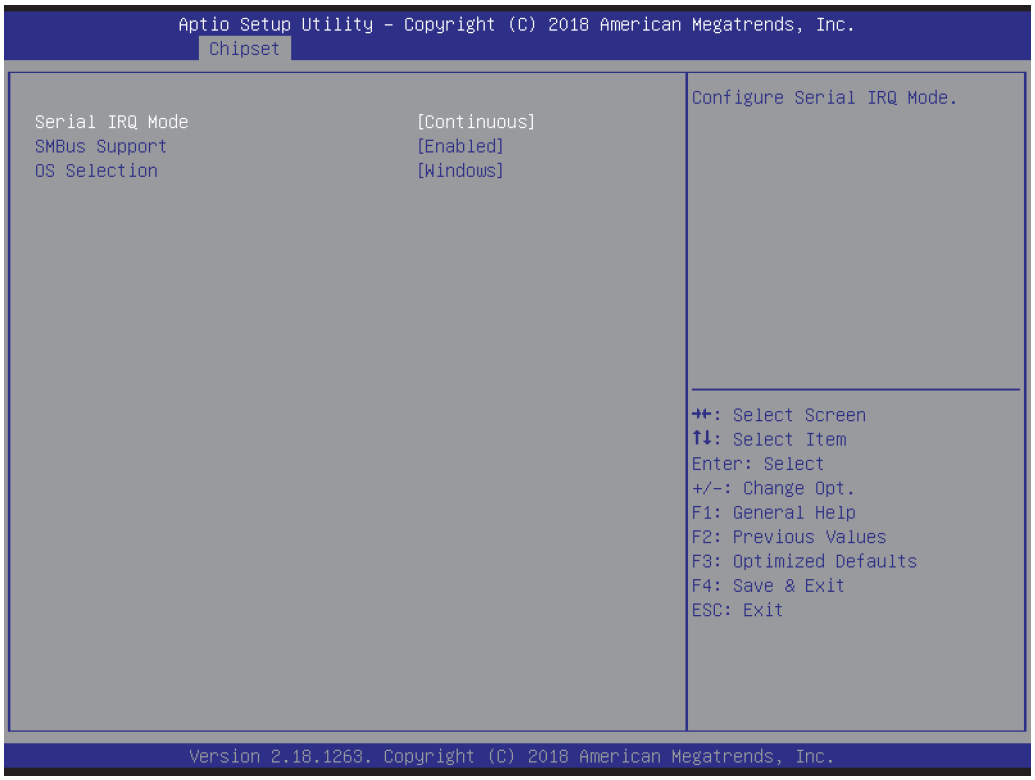
Parameter	Value	Comment
North Bridge	Submenu	North Bridge Parameters
South Bridge	Submenu	South Bridge Parameters
Uncore Configuration	Submenu	Uncore Configuration
South Cluster Configuration	Submenu	South Cluster Configuration

North Bridge



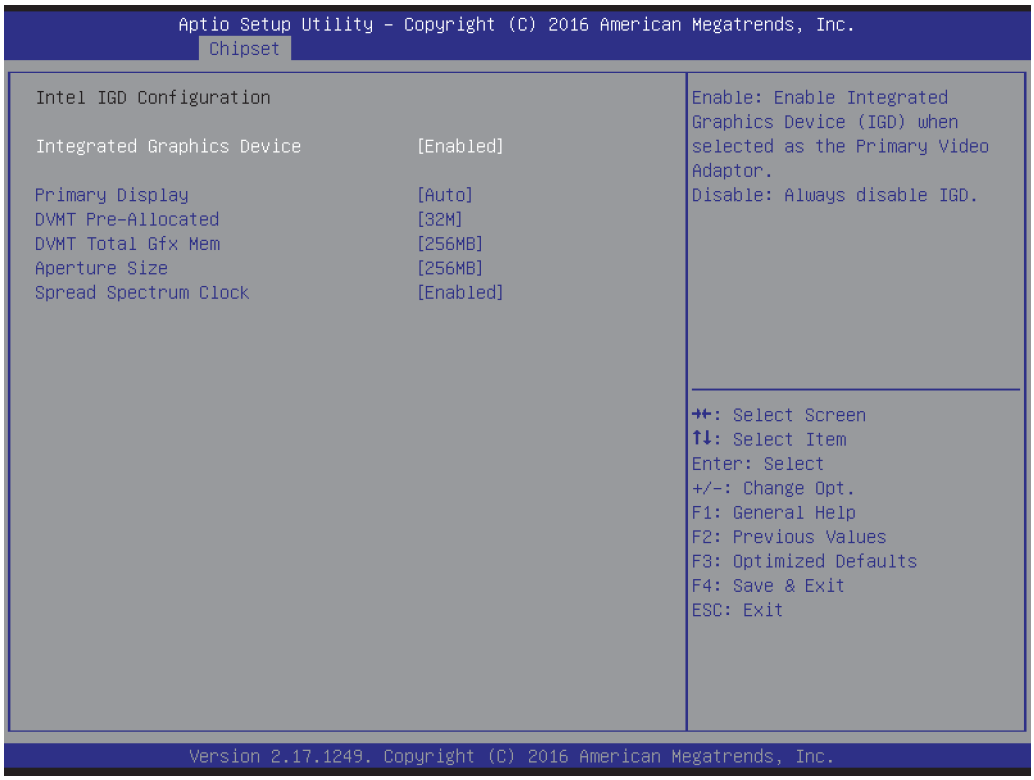
Parameter	Value	Comment
Max TOLUD	**2 GB** 2.25 GB 2.5 GB 2.75 GB 3 GB	Maximum Value of TOLUD. (Top of Low Usable DRAM).
Above 4GB MMIO BIOS assignment	Enabled **Disabled**	Enable/Disable above 4GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.
PCIE VGA Workaround	Enabled **Disabled**	Enable it if your PCIe card cannot boot to DOS.

South Bridge



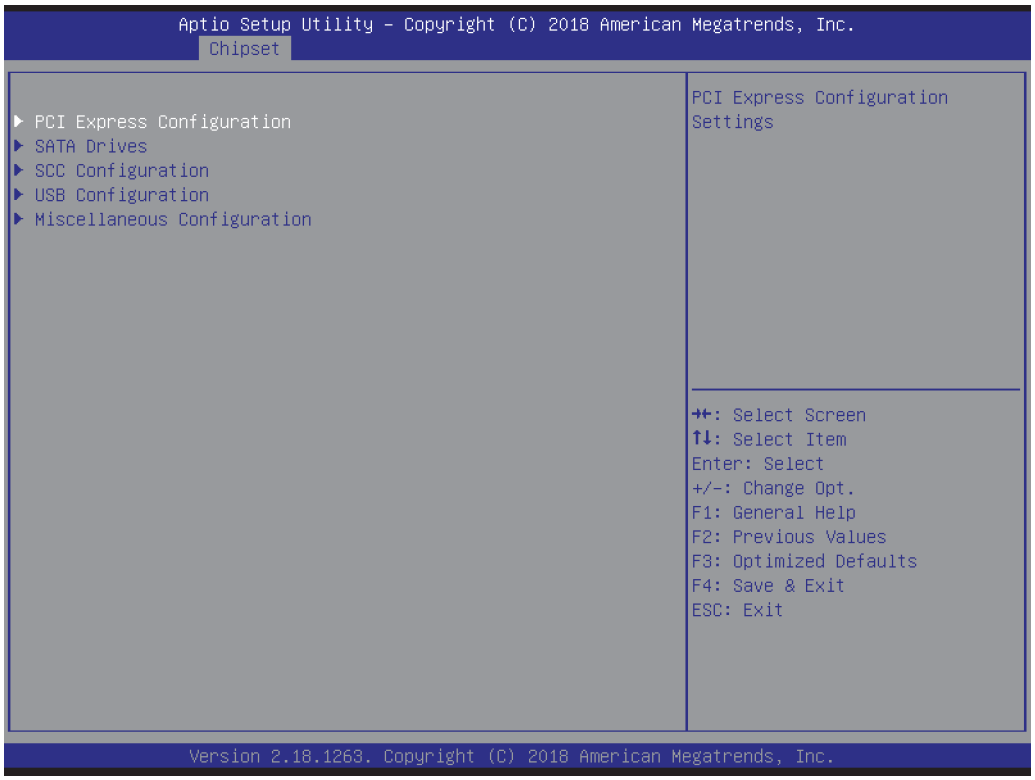
Parameter	Value	Comment
Serial IRQ Mode	Quiet **Continuous**	Configure Serial IRQ Mode.
SMBus Support	**Enabled** Disabled	Enable/Disable SMBus Support.
OS Selection	**Windows** Android Win7 Intel Linux	Select the target OS.

Uncore Configuration



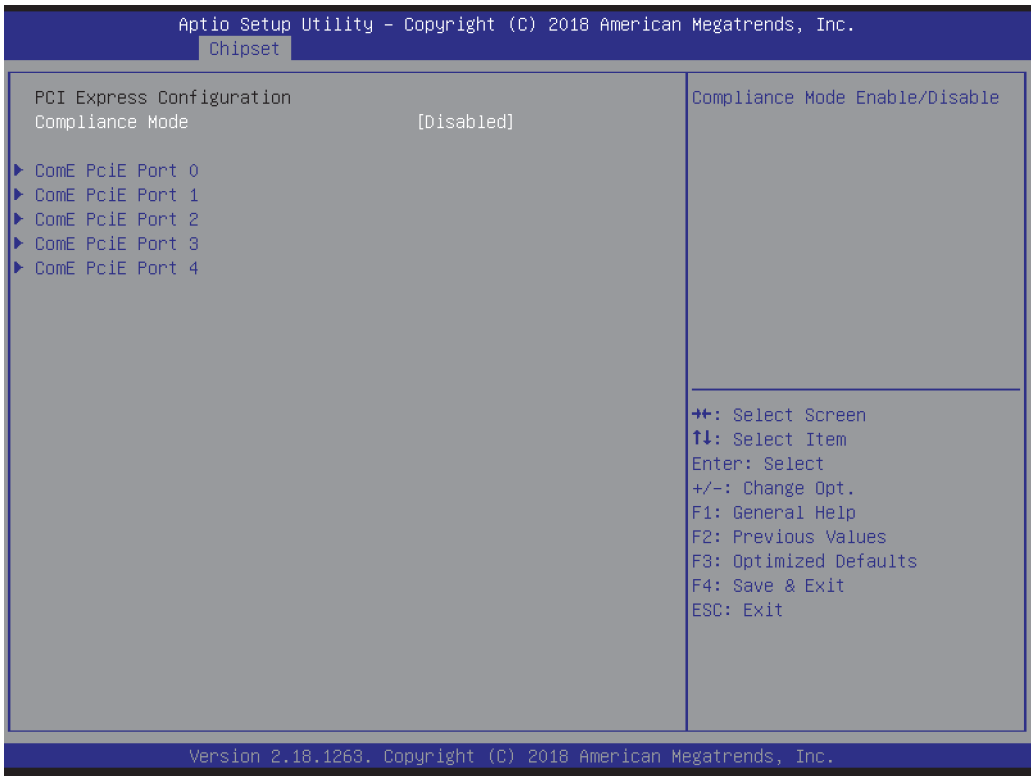
Parameter	Value	Comment
Integrated Graphics Device	**Enabled** Disabled	Enable: Enable Integrated Graphics Device (IGD) when selected as the Primary Video Adaptor. Disable: Always disable IGD.
Primary Display	**IGD** PCIe HG	Select which of IGD/PCIe Graphics device should be Primary Display.
RC6 (Render Standby)	**Enabled** Disabled	Enable/Disable render standby support.
Aperture Size	128MB **256MB** 512MB	Select the Aperture Size.
DVMT Pre-Allocated	64MB … 512MB **64MB** (default)	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128MB **256MB** MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

South Cluster Configuration



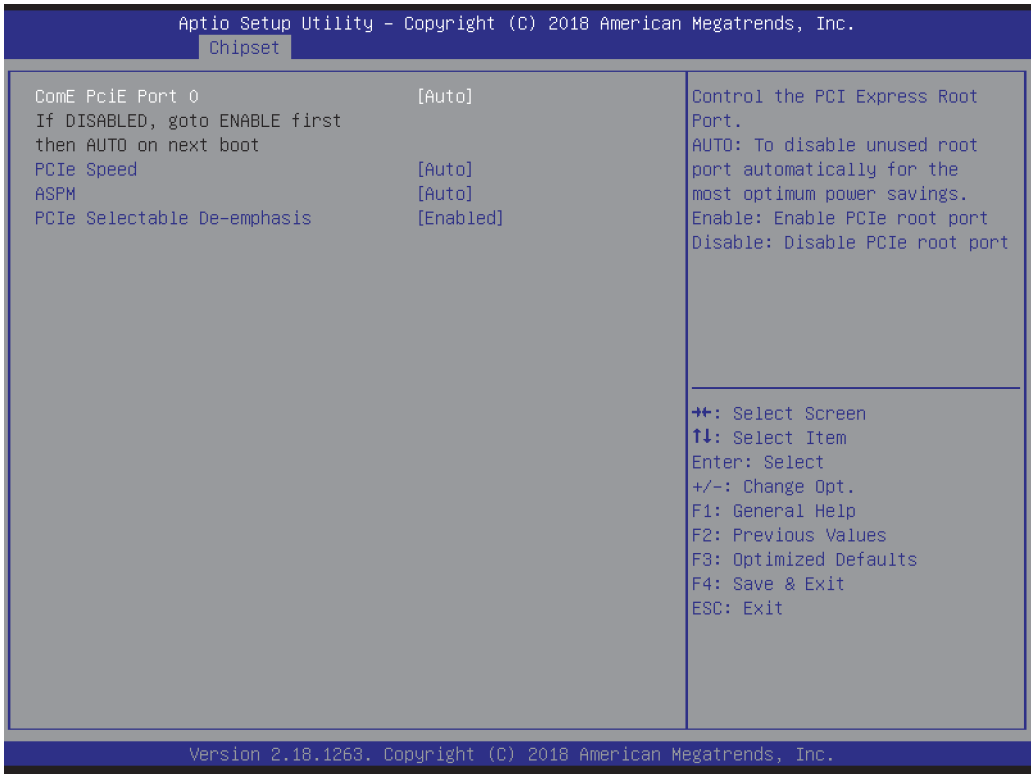
Parameter	Value	Comment
PCI Express Configuration	Submenu	PCI Express Configuration settings
SATA Drives	Submenu	SATA Device Configuration
SCC Configuration	Submenu	SCC Configuration settings
USB Configuration	Submenu	USB Configuration settings
Miscellaneous Configuration	Submenu	Enable/Disable Misc. Features

PCI Express Configuration



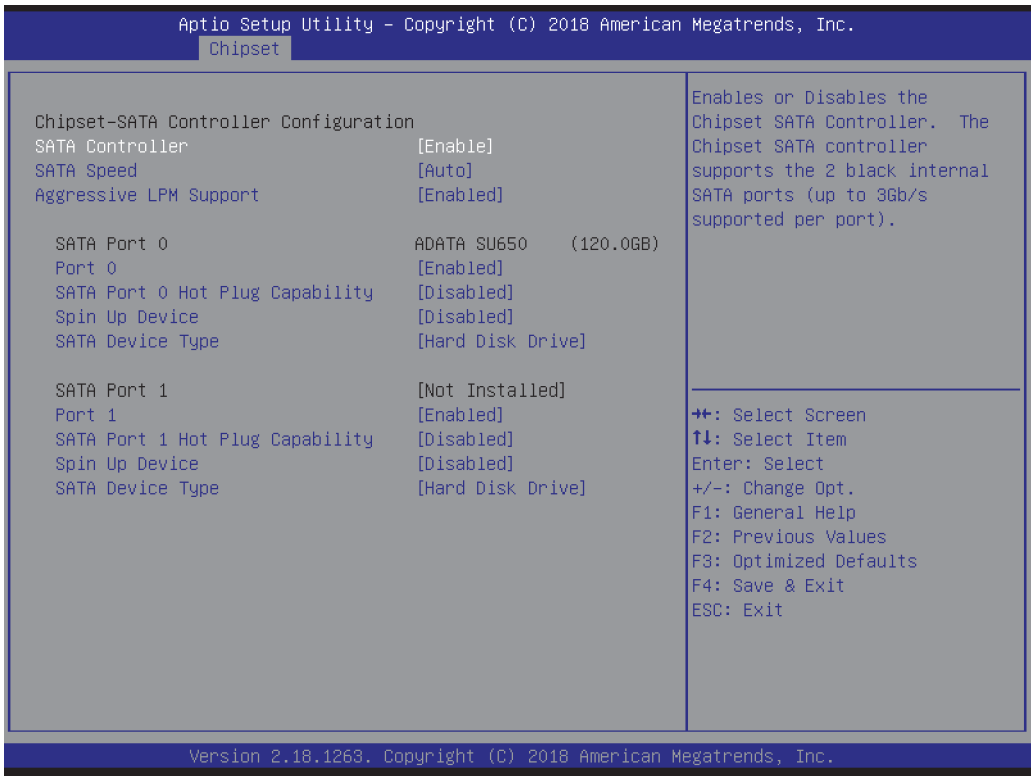
Parameter	Value	Comment
Compliance Mode	Enabled **Disabled**	Enable/Disable Compliance Mode.
COMe PCIe Port	Submenu	PCI Express Root Port Settings.

COMe PCIe Port



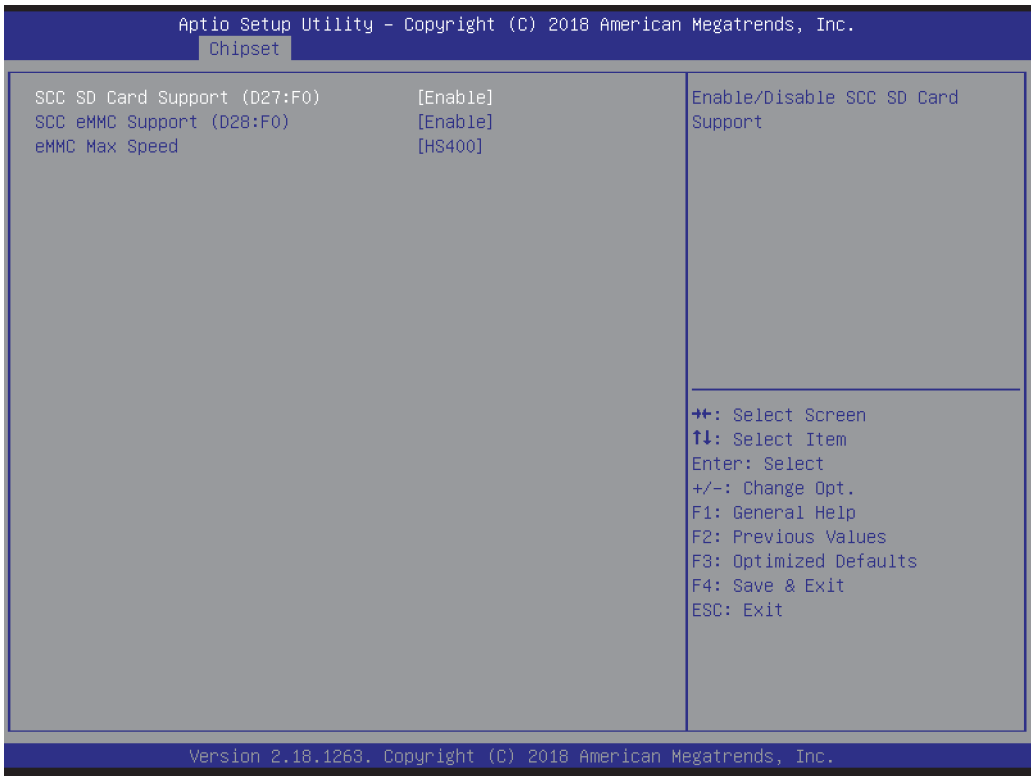
Parameter	Value	Comment
COMe PCIe Port	Enabled Disabled **Auto**	Control the PCI Express Root Port.
PCIe Speed	**Auto** Gen1 Gen2	Select PCI Express Port speed.
ASPM	**Auto** Disabled L0s L1 L0sL1	Set the Active State Power Management Level: Force all links to appropriate ASPM state, or Auto negotiate ASPM configuration or Disable ASPM.
PCIe Selectable De-emphasis	**Enabled** Disabled	When the Link is operating at 5.0 GT/s speed, this bit selects the level of de-emphasis for an Upstream component. Enabled: -3.5 dB Disabled: -6 dB

SATA Configuration



Parameter	Value	Comment
SATA Controller	**Enabled** Disabled	Enable/Disable the Chipset SATA Controller.
SATA Speed	**Auto** Gen1 Gen2 Gen3	Auto configures controller speed to max supported speed of connected devices. Other values limit speed to according value.
Aggressive LPM Support	**Enabled** Disabled	Enable PCH to aggressively enter link power state.
Port	**Enabled** Disabled	Enable/Disable SATA Port.
SATA Port Hot Plug Capability	Enabled **Disabled**	If enabled, SATA port will be reported as Hot Plug capable.
Spin Up Device	Enabled **Disabled**	If enabled for any of ports Staggered Spin Up will be performed and only the drives which hav this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

SCC Configuration

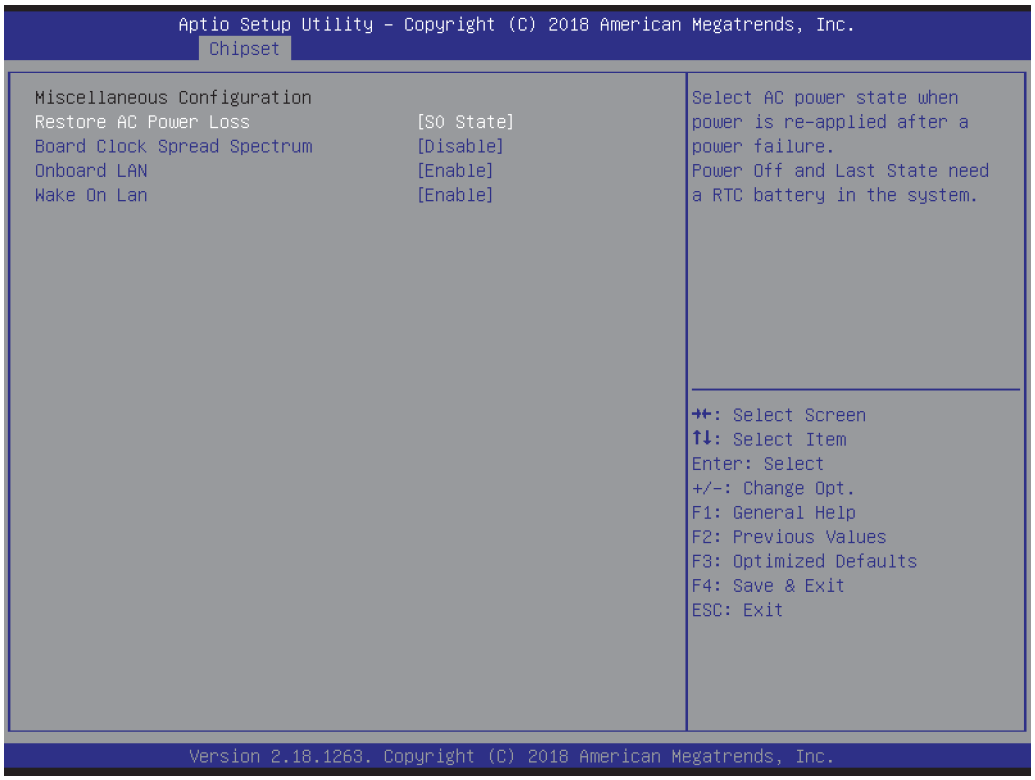


Parameter	Value	Comment
SCC SD Card Support	**Enabled** Disabled	Enabled/Disable SCC SD Card Support.
SCC eMMC Support	**Enabled** Disabled	Enabled/Disable eMMC Support.
EMMC Max Speed	**HS400** HS200 DDR50	Select the eMMC max Speed allowed.

USB Configuration

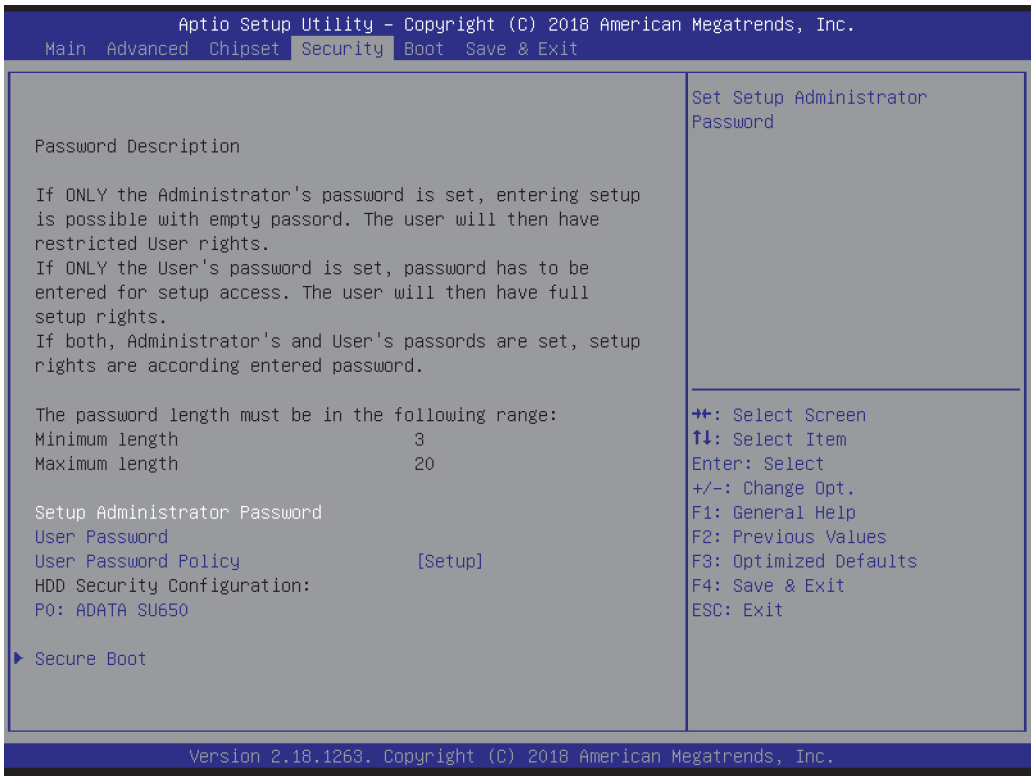
Parameter	Value	Comment
XHCI Pre-Boot Driver	Enabled **Disabled**	Enabled/Disable XHCI Pre-Boot Driver support.
USB Port Disable Override	Enabled **Disabled**	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB Port #	**Enabled** Disabled	Enabled/Disable USB Port.

Miscellaneous Configuration



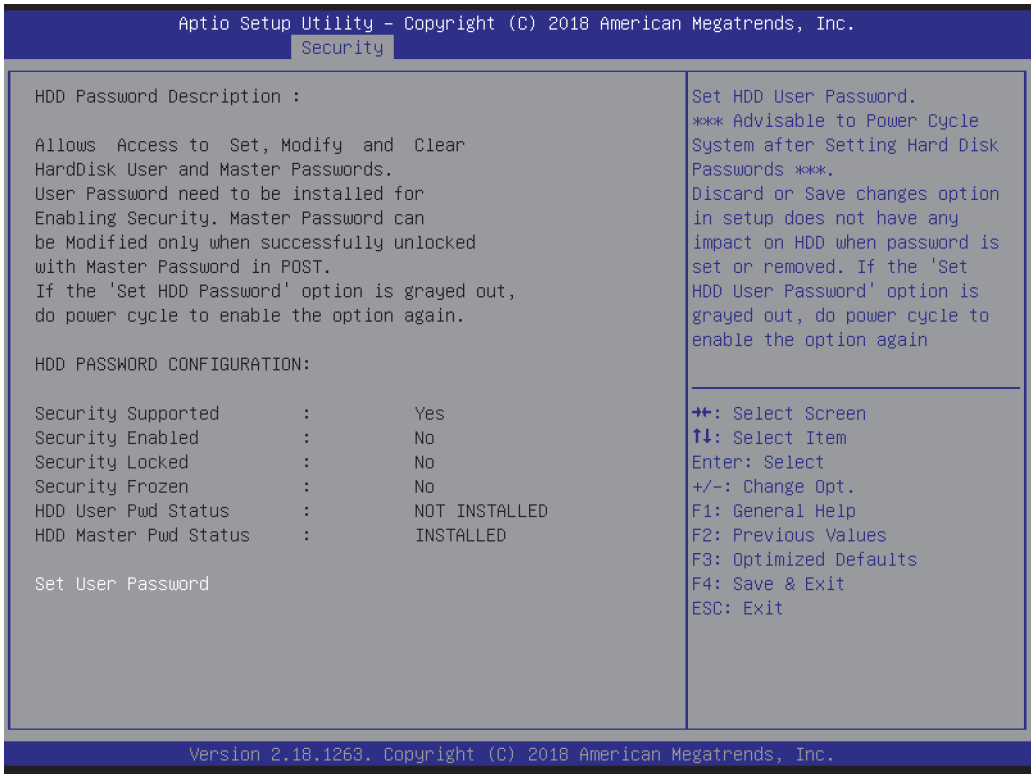
Parameter	Value	Comment
Restore AC Power Loss	**S0 State** S5 State Last State	Select AC power state when power is re-applied after a power failure. Power Off and Last State need a RTC battery in the system.
Board Clock Spread Spectrum	Enabled **Disabled**	Enable Clock Chip's Spread Spectrum feature.
Onboard LAN	Enabled **Disabled**	Enable/Disable onboard GBe LAN Controller.
Wake On Lan	**Enabled** Disabled	Enable/Disable the Wake On Lan.

Security



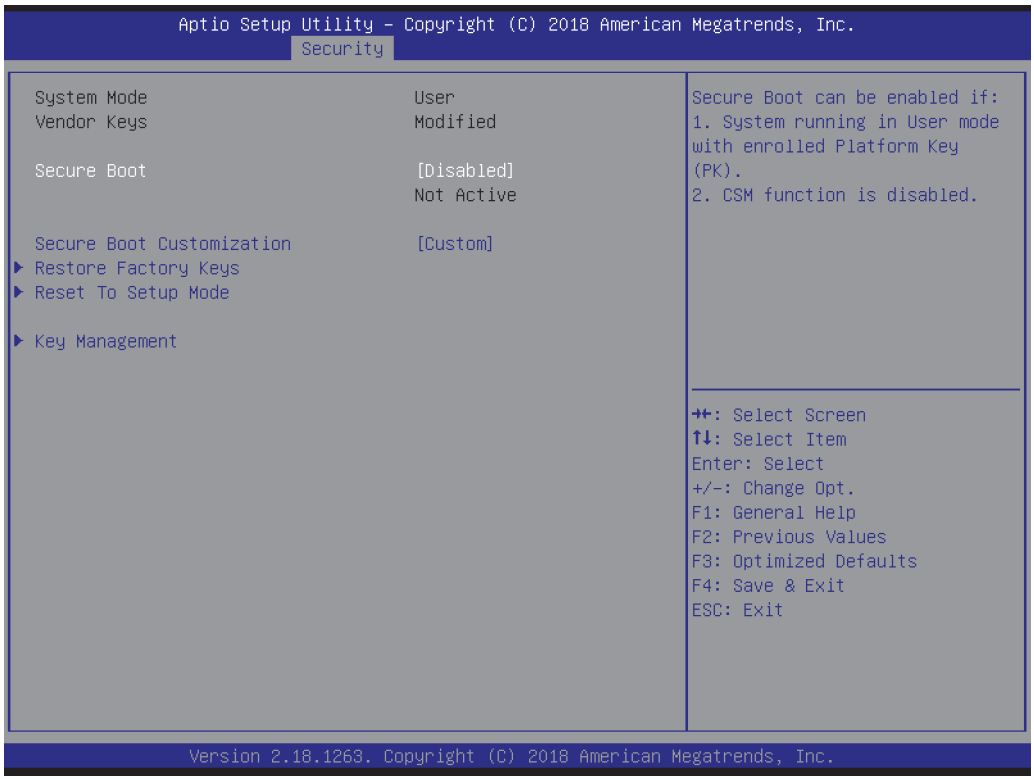
Parameter	Value	Comment
Administrator Password		Set Administrator Password.
User Password		Set User Password.
User Password Policy	**Setup** Boot Boot + Setup	Setup: Password is necessary to enter Setup. Boot: Password is needed for starting system. If Administrator Password is also active, Setup can only be entered with Administrator Password. Boot+Setup: Password needed during POST, enter setup with User Password possible.
HDD Security Configuration	Submenu	HDD Security Configuration for selected drive.
Secure Boot	Submenu	Customizable Secure Boot settings

HDD Security Configuration



Parameter	Value	Comment
Set User Password		Set HDD User Password. *** Advisable to Power Cycle System after Setting Hard Disk Passwords ***. Discard or Save changes option in setup does not have any impact on HDD when password is set or removed. If the 'Set HDD User Password' option is grayed out, do power cycle to enable the option again.

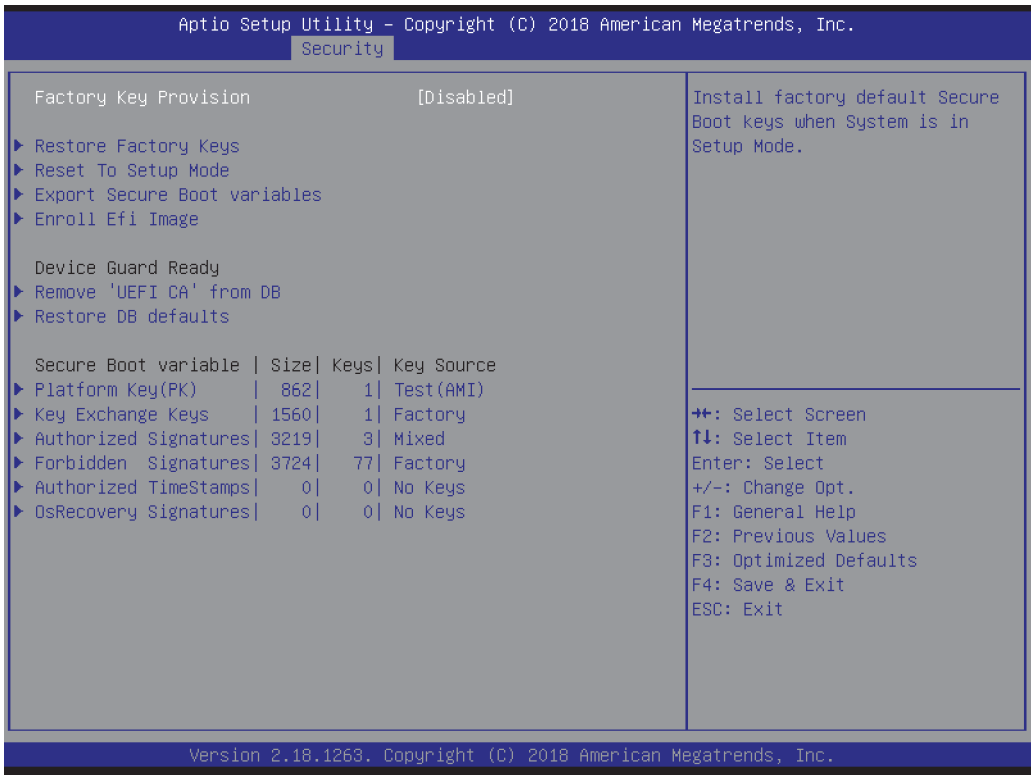
Secure Boot Configuration



Parameter	Value	Comment
Secure Boot	Enabled **Disabled**	Secure Boot can be enabled if: 1. System running in User mode with enrolled Platform Key(PK). 2. CSM function is disabled.
Secure Boot Mode	Standard **Custom**	Secure Boot mode selector: In Custom mode Secure Boot Variables can be configured without authentication.
Restore Factory Keys	Function Key	Force System to User Mode. Install factory default Secure Boot key databases.
Reset To Setup Mode	Function Key	Delete all Secure Boot key databases from NVRAM.
Key Management	Submenu	Enables expert users to modify Secure Boot Policy variables without full authentication.

Key Management

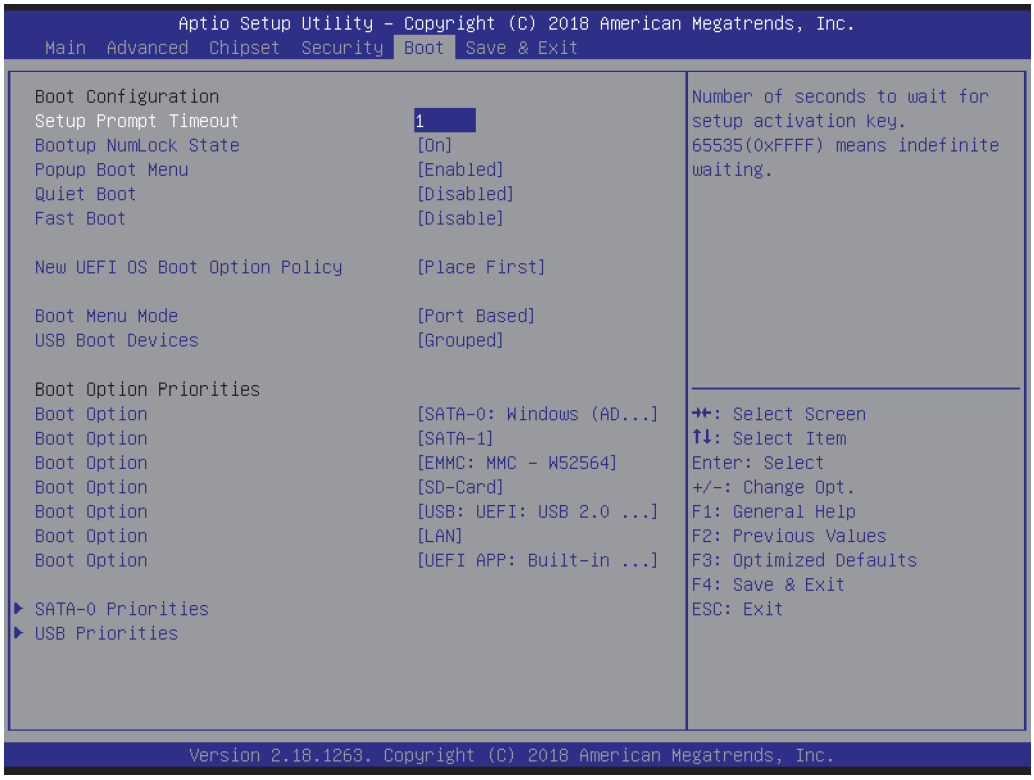
Note: Default Secure Variables PK, KEK, db, dbt and dbx should be updated and signed by OEM PK/KEK Keys.



Parameter	Value	Comment
Factory Key Provision	Enabled **Disabled**	Install factory default Secure Boot keys when System is in Setup Mode.
Restore Factory Keys	Function Key	Force System to User Mode. Install factory default Secure Boot key databases.
Reset to Setup Mode	Function Key	Delete all Secure Boot key databases from NVRAM.
Export Secure Boot variables	Function Key	Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.
Enroll Efi Image	Function Key	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).
Remove 'UEFI CA' from DB	Function Key	Device Guard ready system must not list ‘Microsoft UEFI CA’ Certificate in Authorized Signature databes (db).
Restore DB defaults	Function Key	Restore DB variable to factory defaults.
Platform Key (PK)	Function Key	Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate in: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER encoded) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key source: Default, External, Mixed, Test
Key Exchange Keys	Function Key	
Authorized Signatures	Function Key	
Forbidden Signatures	Function Key	
Authorized TimeStamps	Function Key	
OsRecovery Signatures	Function Key	

Boot

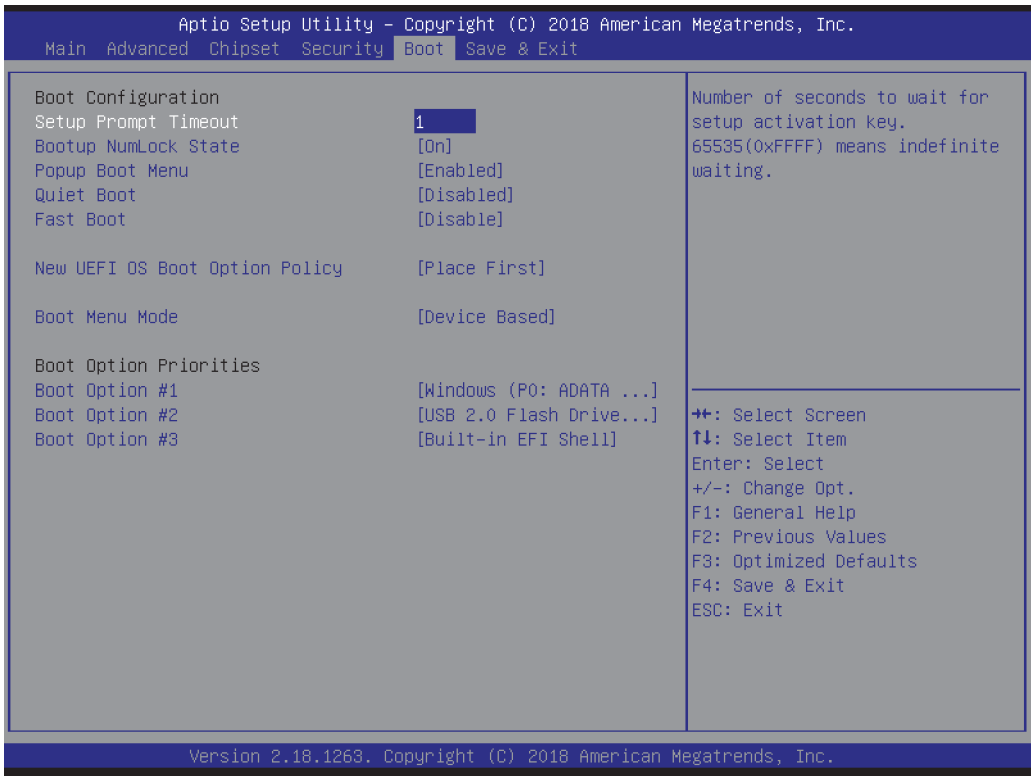
Port Based



Parameter	Value	Comment
Setup Prompt Timeout	1 … 65535 (**1** default)	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard NumLock state.
Popup Boot Menu	**Enabled** Disabled	Enable/Disable Popup Boot Menu.
Quiet Boot	Enabled **Disabled**	Enables or Disables Quiet Boot option.
Fast Boot	Enabled **Disabled**	Enables/Disables boot with initialization of a minimal set of devices required to launch active boot option.
SATA Support	**Last Boot HDD Only** All Sata Devices	Select if only last HDD booted or all SATA HDD should be initialized.
VGA Support	Auto **EFI Driver**	If Auto, only install Legacy OpROM with Legacy OS. Logo would NOT be shown during post. Efi driver will still be installed with EFI OS.
USB Support	Disabled **Full Initial** Partial Initial	If Disabled, all USB devices will NOT be available until OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Device Support	Enabled **Disabled**	If Disabled, PS2 devices will be skipped.
Network Stack Driver Support	Enabled **Disabled**	If Disabled, Network Stack Driver will be skipped.
Redirection Support	Enabled **Disabled**	If Disabled, Redirection function will be disabled.
New Boot Option Policy	Default **Place First** Place Last	Controls the placement of newly detected UEFI boot options.
Boot Menu Mode	Device Based **Port Based**	Device: Choose Boot Option by Device, Port: Choose Boot Option by Type. Need to reset and enter setup again for changes.

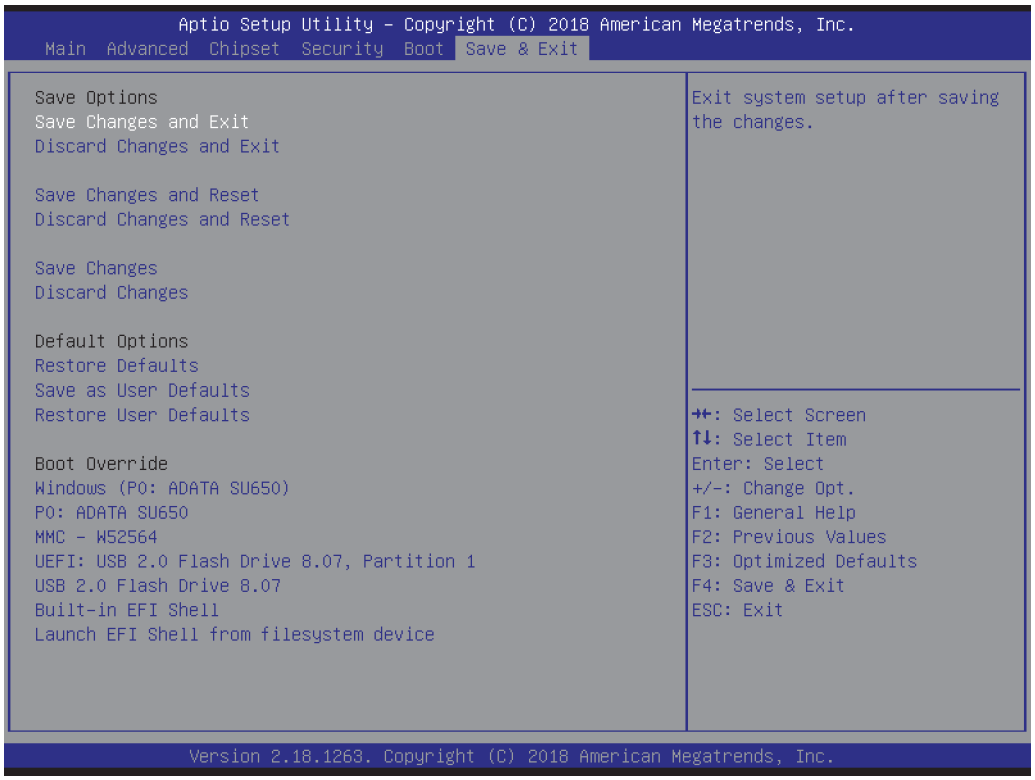
Parameter	Value	Comment
USB Boot Devices	**Grouped** By Port	Show all USB Boot Devices in one group or show all USB Ports.
Boot Option Priorities	Depends on recognized device	Sets the boot order. Priority of devices from same type can be selected in BBS priority menus.
SATA Priorities	Submenu	Set the order of the devices in this group. Appears if more than 1 device of this group is connected.
USB Priorities	Submenu	Set the order of the devices in this group. Appears if more than 1 device of this group is connected.

Device Based



Parameter	Value	Comment
Boot Option Priorities	Depends on recognized device	Sets the boot order. Priority of devices from same type can be selected in Priority Submenus.
Hard Drive BBS Priorities	Submenu	Set the order of the legacy devices in this group. Appears if more than 1 legacy device of this group is connected.
USB Device BBS Priorities	Submenu	Set the order of the legacy devices in this group. Appears if more than 1 legacy device of this group is connected.

Save & Exit



Parameter	Value	Comment
Save Changes and Exit	Function Key	Exit system setup after saving the changes.
Discard Changes and Exit	Function Key	Exit system setup without saving any changes.
Save Changes and Reset	Function Key	Reset the system after saving the changes.
Discard Changes and Reset	Function Key	Reset system setup without saving any changes.
Save Changes	Function Key	Save Changes done so far to any of the setup options.
Discard Changes	Function Key	Discard Changes done so far to any of the setup options.
Restore Defaults	Function Key	Restore/Load Default values for all the setup options.
Save as User Defaults	Function Key	Save the changes done so far as User Defaults.
Restore User Defaults	Function Key	Restore the User Defaults to all the setup options.
Boot Override	Depends on recognized device	Boots to selected device.
Launch EFI Shell from filesystem device	Function Key	Attempts to Launch EFI Shell application (shell.efi) from one of the available filesystem devices.

This page intentionally left blank.

This page intentionally left blank.

DATA MODUL

Headquarters:

DATA MODUL AG
Landsberger Str. 322
DE-80687 Munich - Germany
Phone: +49-89-56017-0
Fax: +49-89-56017-119
www.data-modul.com

Logistics, Production & Services:

DATA MODUL Weikersheim GmbH
Lindenstrasse 8
DE-97990 Weikersheim - Germany
Phone: +49-7934-101-0
Fax: +49-7934-101-101

Subsidiaries & Sales Offices:

Germany – Hamburg
Germany – Duesseldorf
Denmark
Dubai
Finland/Baltic
France
Italy
Singapore
Spain
Switzerland
UK
USA

DATA MODUL's worldwide offices
can be found on our website:
www.data-modul.com/eu/sm/contact-us/offices.html

10.2013

DIN-EN-ISO 9001/14001 | www.data-modul.com