APTIO™ CORE BIOS MANUAL

For Acromag® Products

ACROMAG INCORPORATED
30765 South Wixom Road
Wixom, MI 48393-7037 U.S.A.
Tel: (248) 624-1541
Fax: (248) 624-9234

8501026B

Table of Contents

1.0 GENERAL INFORMATION

1.1 Intended Audience

This users' manual was written for technically qualified personnel who will need working information for the system BIOS used with Acromag® I/O devices that are based upon the Intel® Haswell 4th Generation core processor. It is not intended for a general, non-technical audience that is unfamiliar with the Haswell core processor or the devices that use this core processor..

1.2 About Aptio™

Aptio™ is AMI's next-generation BIOS firmware based on the UEFI Specifications and the Intel® Platform Innovation Framework for EFI. Aptio™ is specifically designed to address firmware portability and extensibility to future platforms. Along with silicon enabling components, Aptio™ can be expanded using a variety of drivers, development tools, support utilities and pre-boot application solutions. (*Aptio™ TSE User Manual, pg. 6).*

1.3 About Aptio™ Text Setup Environment (TSE)

Aptio™ Text Setup Environment (TSE) is a text-based basic input and output system. The purpose of Aptio™ TSE is to empower the user with complete system control at boot. AMI Text Setup Environment (TSE) provides advance UEFI functionality with a familiar BIOS interface. AMI TSE is an AMI firmware user interface designed to work in conjunction with Aptio™. It is made up of a series of drivers, applications and images, which can be customized according to an OEM's requirements, or can use AMI's default interface.
In Aptio™, as in any firmware project, lack of flash space is always one of the biggest obstacles. One of the goals of Aptio™ is to offer a complete solution in 512 KB of flash ROM. In order to satisfy customers who require small ROM footprint without sacrificing the ability to use setup to configure the system, AMI offers space-optimized setup environment components called AMI Text Setup Environment (TSE).
This document explains the basic navigation of Aptio™ TSE. (*Ibid, pg. 6).*

1.4 Preface

The information contained in this manual is subject to change without notice, and Acromag, Inc. (Acromag) does not guarantee its accuracy. Acromag makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Further, Acromag assumes no responsibility for any errors that may appear in this manual and makes no commitment to update, or keep current, the information contained in this manual. No part of this manual may be copied or reproduced in any form, without the prior written consent of Acromag,

1.5 Trademark, Trade Name and Copyright Information

Acromag Incorporated
30765 South Wixom Road
P.O. BOX 437
Wixom, MI 48393-7037 U.S.A.

The text information used in this manual in support of the specifications, screen, implementation, and use of the Aptio BIOS has been reprinted by permission from the public document Aptio™ *Text Setup Environment (TSE) User Manual*, Document Revision 1.00, Copyright © 2010 by American Megatrends, Inc (AMI). In addition, the figures, tables and all other visuals that appear in this manual are also taken from, or are based upon, content from the Aptio™ *Text Setup Environment (TSE) User Manual*, again with the permission of AMI. Because of the extent of the use of the AMI-supplied material in this material, that use is referenced in this paragraph in lieu of using individual in-text citations.
The images (figures, tables and screen shots) shown in this manual that are not from the *TSE User Manual* were also provided by AMI for the expressed purpose of inclusion in this Acromag-provided Core BIOS user manual.

1.6 Related Material

The following manuals and part specifications provide the necessary information for in-depth understanding of the XCOM-6400 module.

- *Aptio™ Text Setup Environment (TSE) User Manual*, Document Revision 1.00, Copyright © 2010 by American Megatrends, Inc.

- Intel® document No. 328901, "Mobile 4th Generation Intel® Core™ Processor Family Datasheet – Volume 1 of 2", Rev: 002; September, 2013.

http://www.intel.com/content/www/us/en/processors/core/CoreTechnicalResources.html

2.0 Aptio™ BIOS Setup

2.1 Main Menu

The Aptio™ TSE BIOS setup menu is the first screen that you can navigate. Each BIOS setup menu option is described in this user's manual.
To enter the Aptio™ TSE screens, follow the steps outlined below:

Table 2.1.a Entering the Aptio™ TSE Screens

Step	Description
1	Power on the motherboard
2	Press the <Delete> key on your keyboard when you see the following text prompt: "Press DEL or F2 to enter Setup"
3	After selecting <Delete> key, the Aptio™ TSE main BIOS setup menu is displayed. You can access the other setup screens from the main BIOS setup menu, such as the Chipset and Power menus.

In most cases, the <Delete> key is used to invoke the Aptio™ TSE screen. There are a few cases where other keys are used, such as <F1>, <F2>, and so on. The user can press the <TAB> key during boot to switch from the boot splash screen (logo) to see the keystroke messages. The Aptio™ TSE BIOS setup menu (see Figs. 2.1.b-d below) is the first screen that you can navigate. Each BIOS setup menu option is described in this user's manual. The Main Setup menu is shown in Figs. 2.1.b through 2.1.d below.

Fig. 2.1.b Main Menu (Screen 1 of 3)

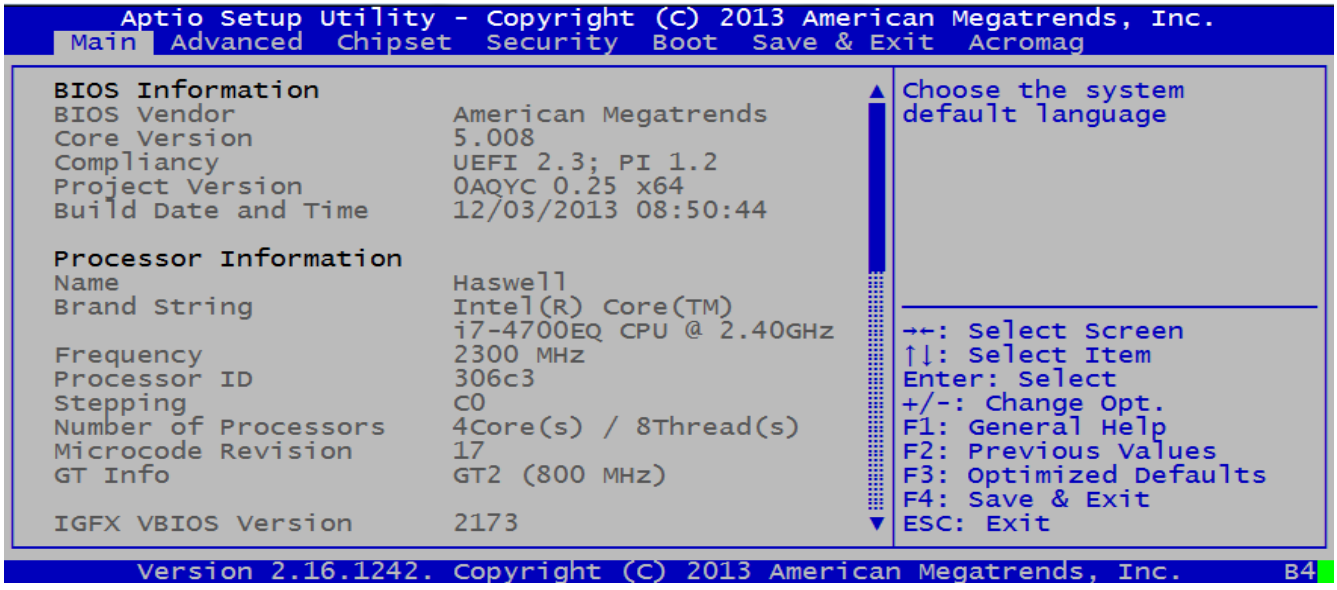


Fig. 2.1.c Main Menu (Screen 2 of 3)

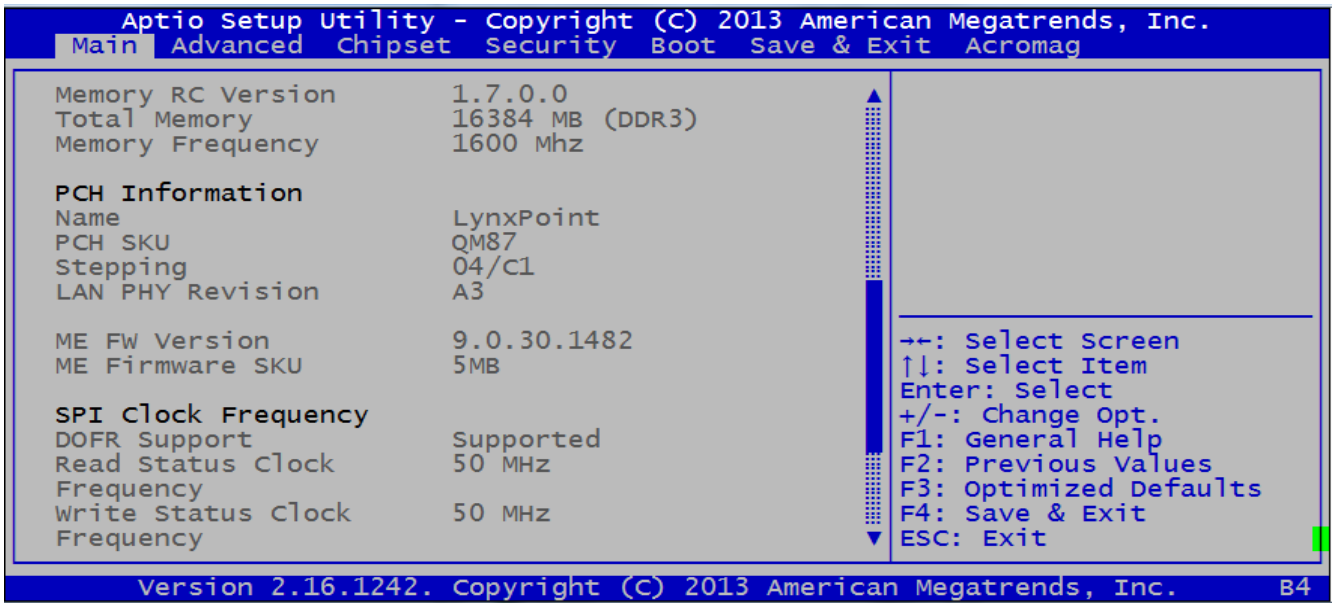
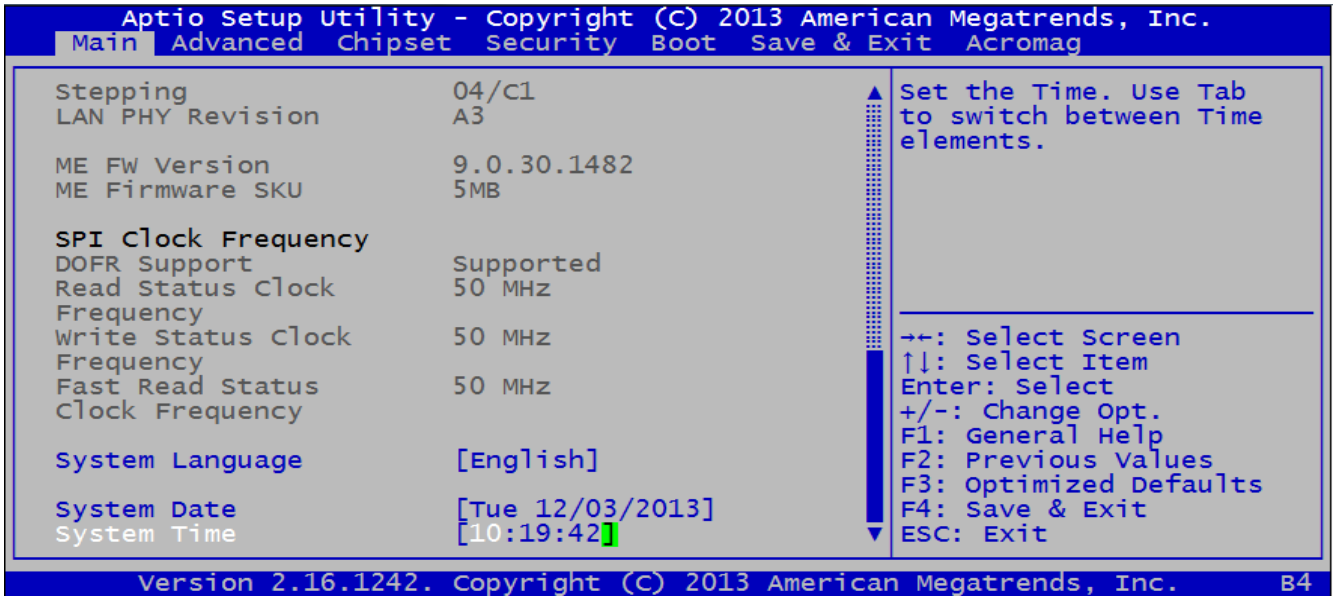


Fig. 2.1.d Main Menu (Screen 3 of 3)



The “System Date” option allows the user to set the date on the system real-time clock RTC. Simply navigate to the month, day, or year and type in the correct numeric value.

The “System Time” option allows the user to set the time on the RTC. Simply navigate to the hour, minute, or second and type in the correct numeric value. Note that he time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.

2.1.1 Keyboard-Based Navigation of the TSE BIOS Screens

The Aptio™ TSE keyboard-based navigation can be accomplished using a combination of the keyboard keys (<FUNCTION> keys, <ENTER>, <ESC>, <ARROW> keys, etc.). See figure 2.1.1.a below.

Fig. 2.1.1.a Keyboard-Based Navigation

Keystroke	Description
<Enter>	The *Enter* key allows the user to select an option to edit its value or access a sub menu.
" " and " " (left and right arrow keys)	The *Left and Right* <Arrow> keys allow you to select an Aptio™ TSE screen. For example: Main screen, Advanced screen, Chipset screen, and so on.
" " and " " (up and down arrow keys)	The *Up and Down* <Arrow> keys allow you to select an Aptio™ TSE item or sub-screen.
"+" and "-" (plus and minus keys)	The *Plus and Minus* <Arrow> keys allow you to change the field value of a particular setup item. For example: Date and Time.
<Tab>	The <Tab> key allows you to select Aptio™ TSE fields.
<F1>	This key displays the general help window for the user.
<F2>	This key enables users to load pervious values in TSE.
<F3>	This key enables users to load optimized default values in TSE.
<F4>	This key enables users to save the current configuration and exit TSE.
<ESC>	The <Esc> key allows you to discard any changes you have made and exit the Aptio™ TSE. Press the <Esc> key to exit the Aptio™ TSE without saving your changes. The following screen will appear: Press the <Enter> key to discard changes and exit. You can also use the <Arrow> key to select *Cancel* and then press the <Enter> key to abort this function and return to the previous screen.
Function Keys	When other function keys are available, they are displayed in the help screen along with their intended function.

2.2 Advanced Menu

Select the *Advanced* menu item from the Aptio™ TSE screen to enter the Advanced BIOS Setup screen. You can select any of the items in the left frame of the screen.

Fig. 2.2.a Advanced Menu (Screen 1 of 2)

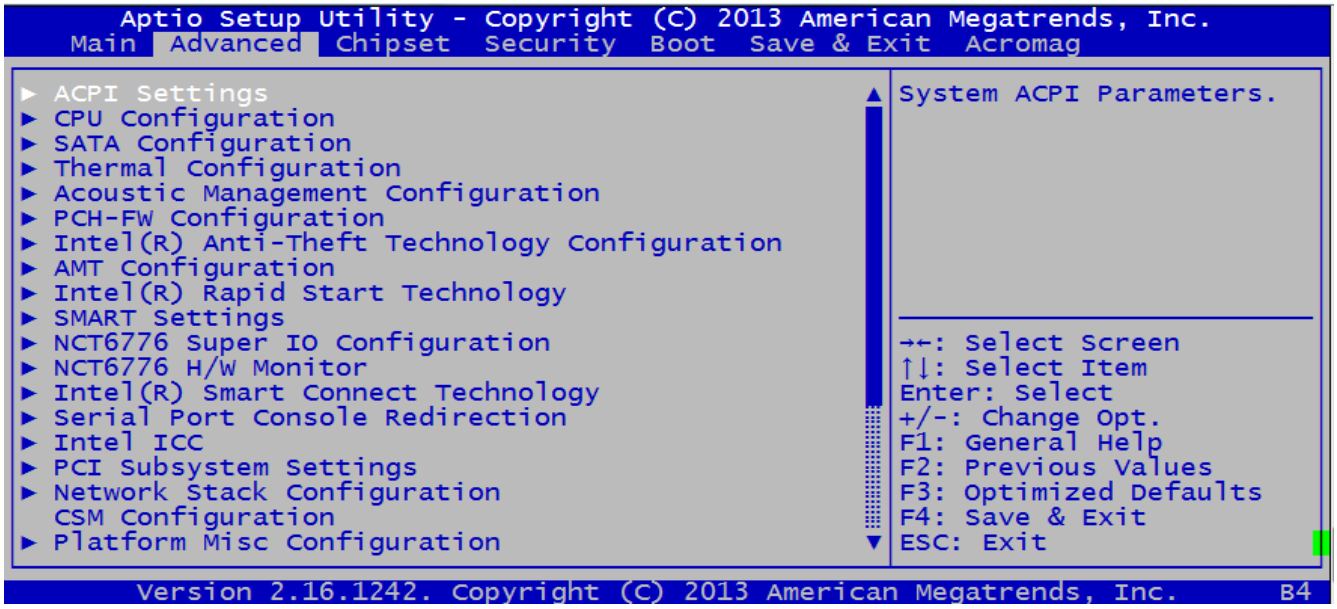
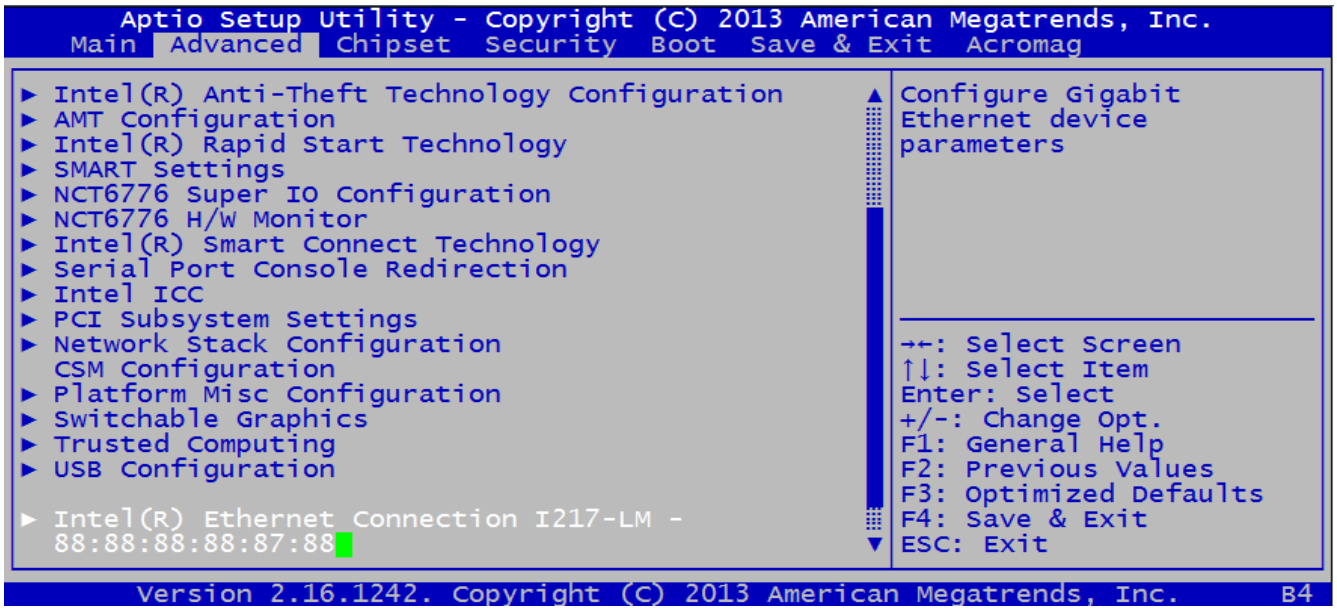
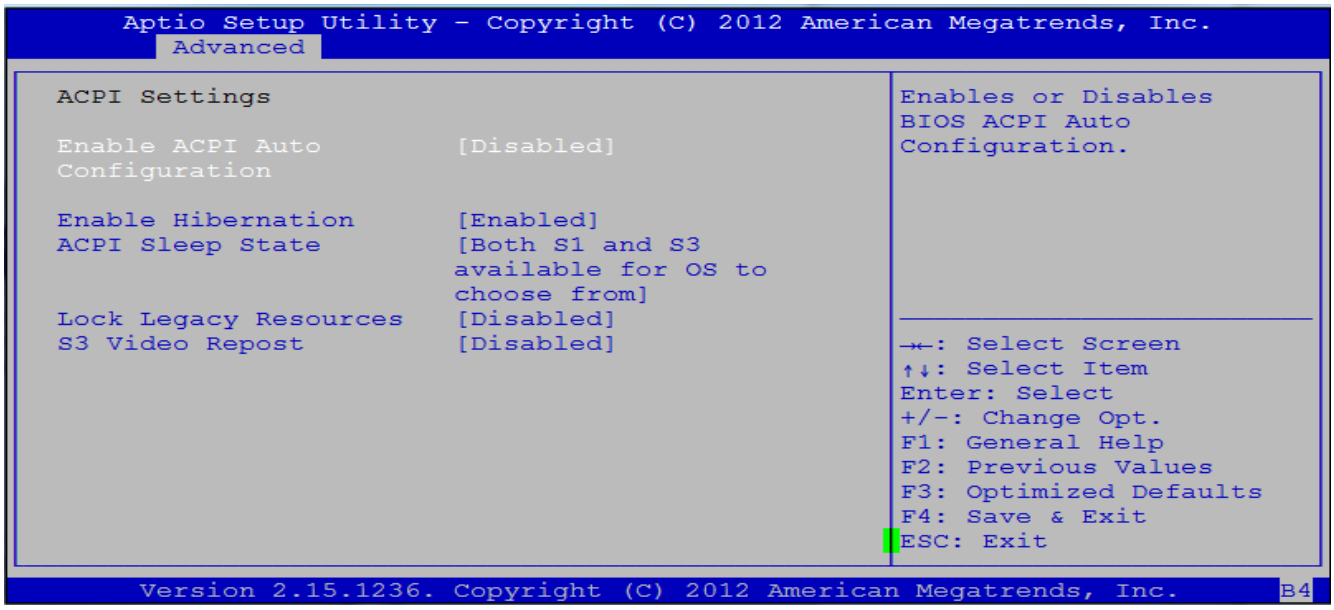


Fig. 2.2.b Advanced Menu (Screen 2 of 2)



2.2.1 ACPI Settings

Fig. 2.2.1.a ACPI Settings



This option allows the user to view and configure the system Advanced Configuration and Power Interface (ACPI) parameters.

Feature	Options	Description
Enable ACPI Auto Configuration	*Enabled* *Disabled*	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	*Enabled* *Disabled*	Enables or disables system ability to Hibernate (OS/S4 Sleep State).
ACPI Sleep State	*Suspend Disabled* *S1 (CPU Stop Clock)* *S3 (Suspend to RAM)* *Both S1 and S3 available for OS to choose from*	Select the highest ACPI sleep state the system will enter when the SUSPEND button is Selected.
Lock Legacy Resource	*Enabled* *Disabled*	Enables or Disables Lock of Legacy Resources.
S3 Video Repost	*Enabled* *Disabled*	Enables or Disables S3 Video Repost.

2.2.2 CPU Configuration

Fig. 2.2.2.a CPU Configuration (Screen 1 of 5)

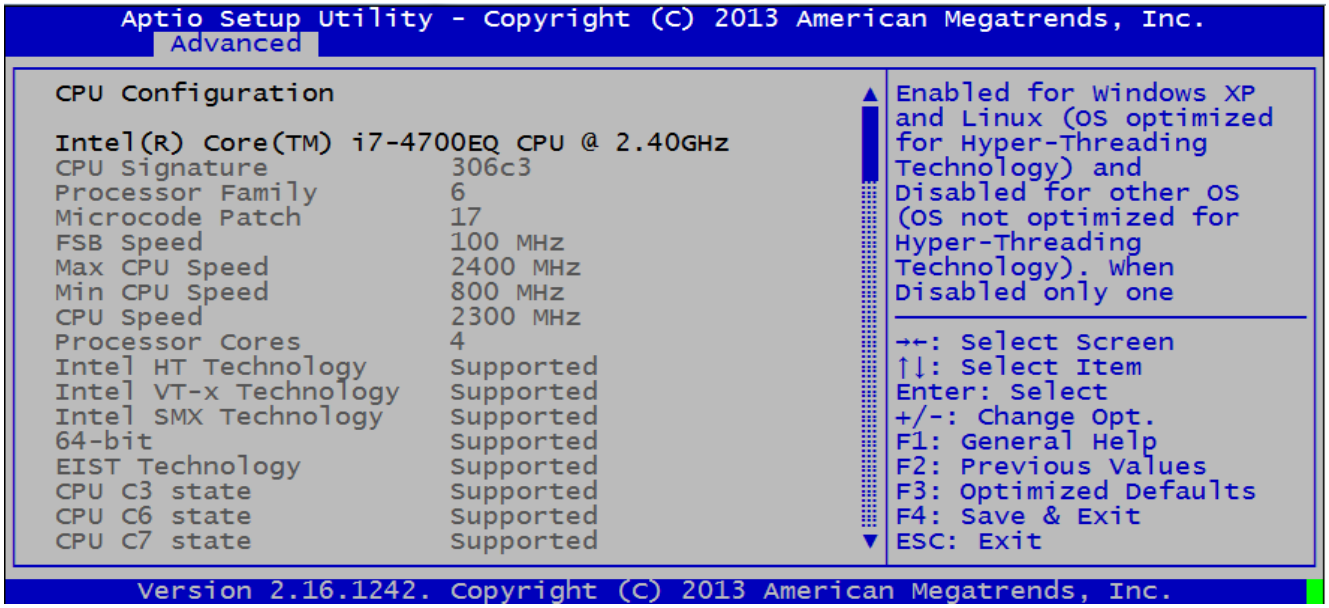


Fig. 2.2.2.b CPU Configuration (Screen 2 of 5)

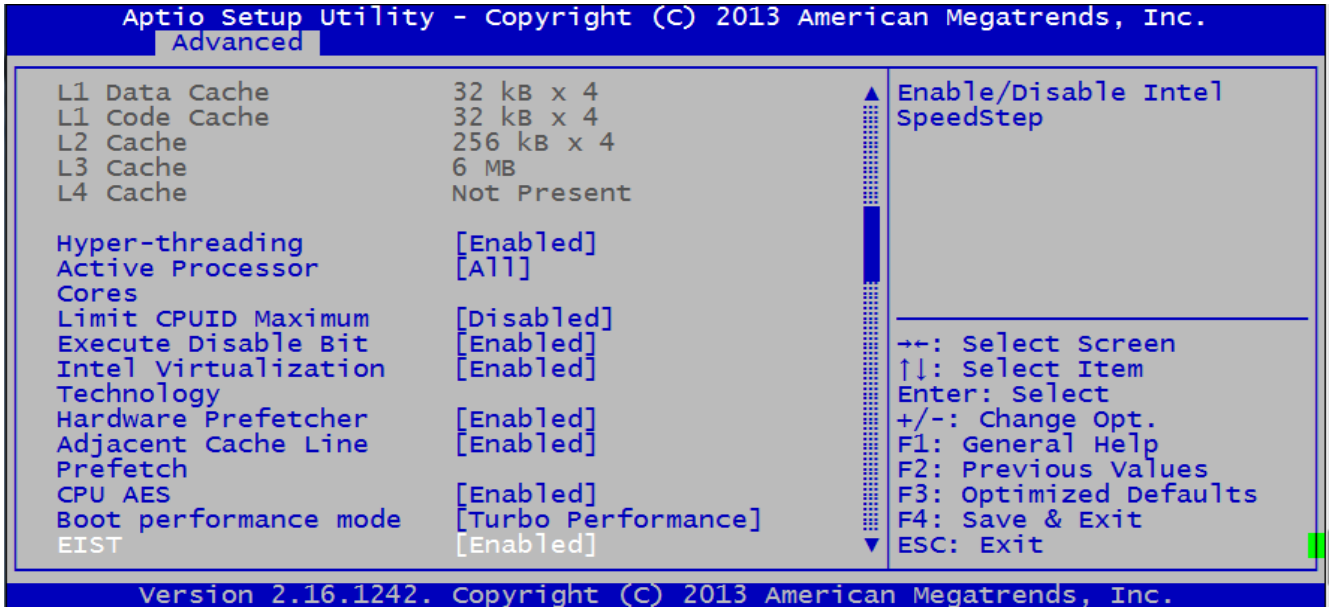


Fig. 2.2.2.c CPU Configuration (Screen 3 of 5

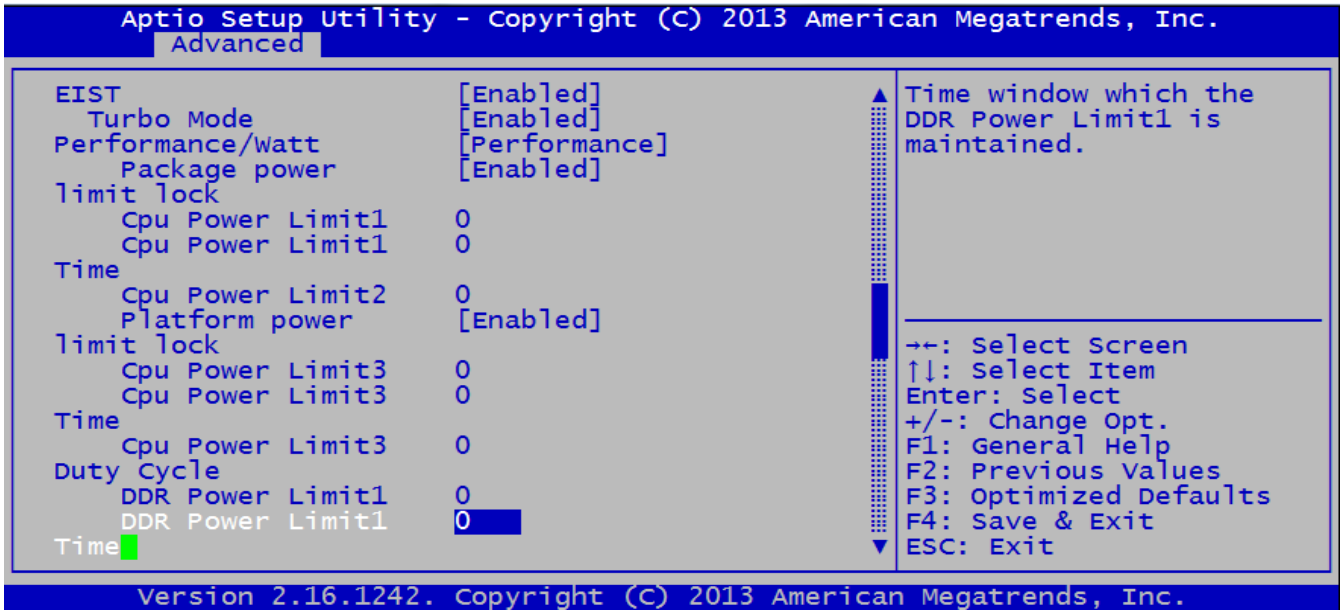


Fig. 2.2.2.d CPU Configuration (Screen 4 of 5)

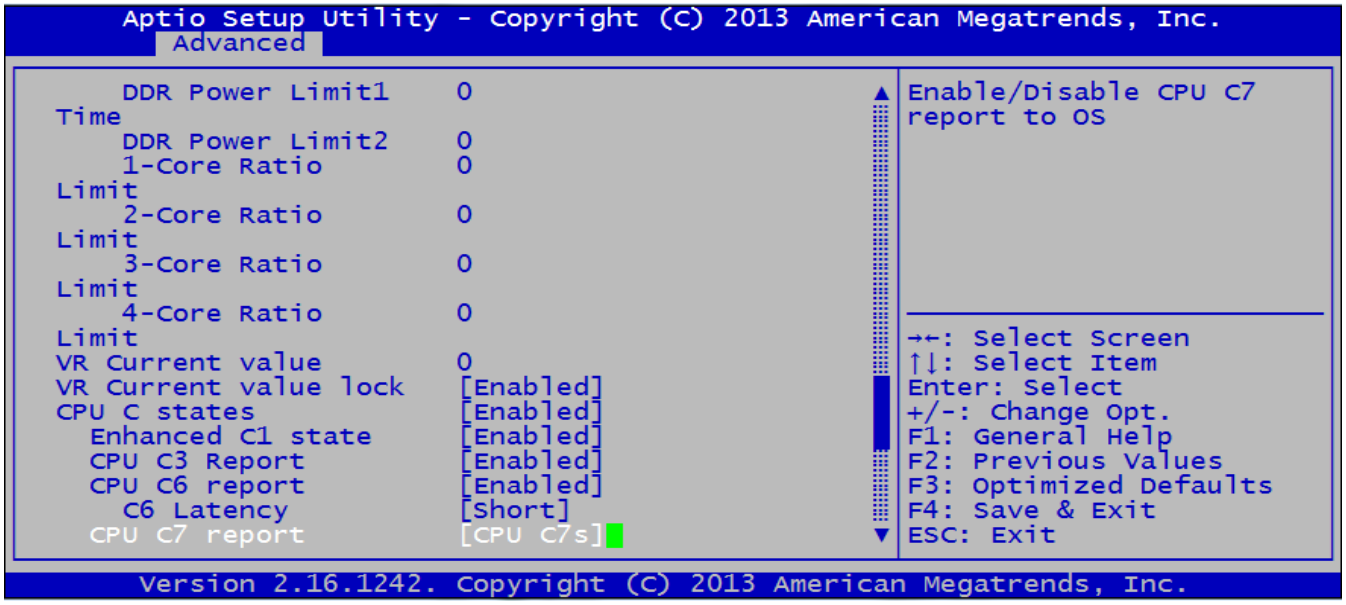
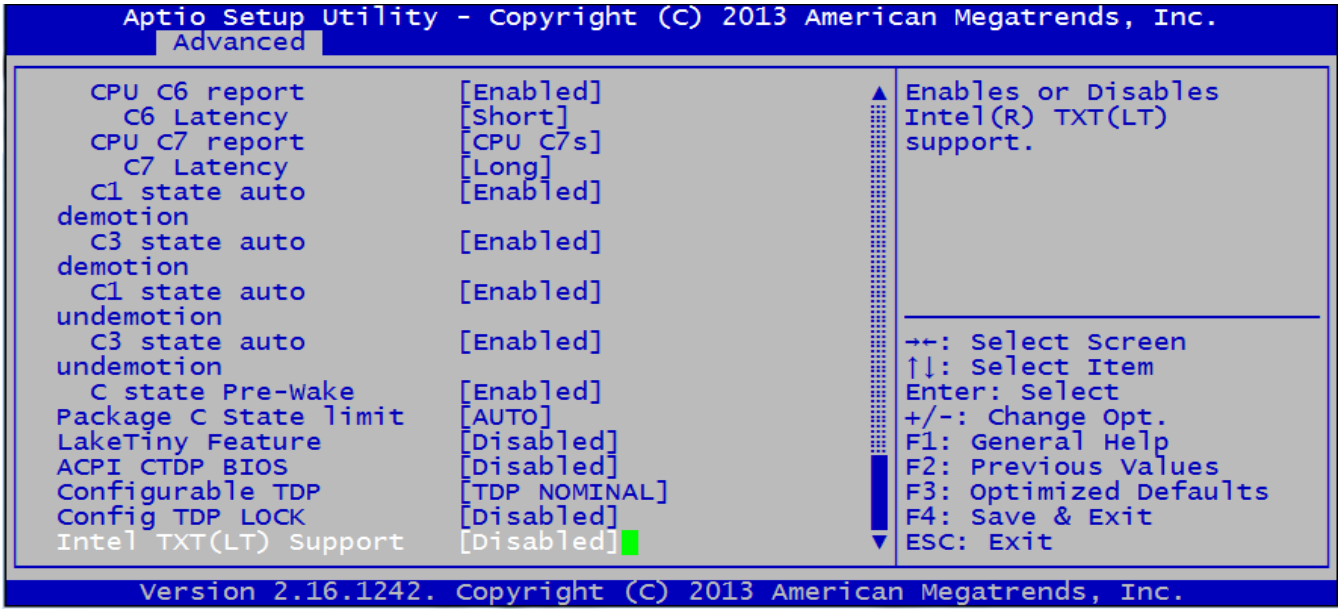


Fig. 2.2.2.e CPU Configuration (Screen 5 of 5



This option allows the user to view and configure the settings of the CPU installed on the computer system.

Feature	Options	Description
		The initial information is for view only purpose, this includes Processor Type, CPU Speed, L1, L2, and L3 Cache RAM
Hyper-threading	*Enabled* *Disabled*	Enabled for Linux, most Windows versions (OS Optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology). When disabled only one thread per enabled core is enabled. Note: This setting should be disabled in Windows 2000.
Active Processor Cores	*All* *1* *2* *3* *4*	Number of cores to enable in each processor package.
Limit CPUID Maximum	*Disabled* *Enabled*	When CPUID instruction is executed, the CPU may return a value greater than 3 which causes certain problem with specific operating systems. Enabling "CPUID Maximum Value Limit" in the CPU configuration of BIOS setup menu will limit the returned value to 3 and less to get rid of the problem. The problem is not seen with newer Windows series operating systems such as XP and higher so the default is set to *Disabled*.
Execute Disable Bit	*Enabled* *Disabled*	Execute Disable Bit (XD) is an Intel hardware-based security feature that can help reduce system exposure to viruses and malicious code. XD allows the processor to

		classify areas in memory where application code can or cannot execute. When a malicious worm attempts to insert code in the buffer, the processor disables code execution, preventing damage and worm propagation. To use Execute Disable Bit you must have a supporting OS.
Intel Virtualization Technology	*Enabled* *Disabled*	Formerly known as Vanderpool, this technology enables a CPU to act as if you have several independent computers in order to enable several operating systems to run at once.
Hardware Prefetcher	*Enabled* *Disabled*	This option operates transparently, without programmer intervention, to fetch streams of data and instruction from memory into the unified second-level cache. The prefetcher is capable of handling multiple streams in either the forward or backward direction. It is triggered when successive cache misses occur in the last-level cache and a stride in the access pattern is detected, such as in the case of loop iterations that access array elements. The prefetching occurs up to a page boundary.
Adjacent Cache Line Prefetch	*Enabled* *Disabled*	The Adjacent Cache-Line Prefetch mechanism, like automatic hardware prefetch, operates without programmer intervention. When enabled through the BIOS, two 64-byte cache lines are fetched into a 128-byte sector, regardless of whether the additional cache line(L2) has been requested or not. In applications with relatively poor spatial locality, the cache miss ratio is higher.
CPU AES	*Enabled* *Disabled*	Enables or Disables CPU Advanced Encryption Standards.
Boot performance mode	*Max Non-Turbo* *Max Battery* *Turbo Performance*	Selects the performance state that the BIOS will set before OS handoff.
EIST	*Enabled* *Disabled*	Enable or Disable Enhanced Intel SpeedStep Technology. Enhanced Intel SpeedStep Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production.
Turbo Mode	*Enabled* *Disabled*	Also known as Intel Turbo Boost Technology, this option automatically allows the processor cores to run faster that the rated operating frequency if they're operating below power, current, and temperature specification limits. This option is not available unless EIST is enabled.
Performance/Watt	*Performance* *Balanced Performance* *Balanced Energy* *Energy Efficient*	Depending on the setting, this BIOS option parameterizes the internal "Power Control Unit (PCU)" of the processors and optimizes the power management functions of the processors between performance and

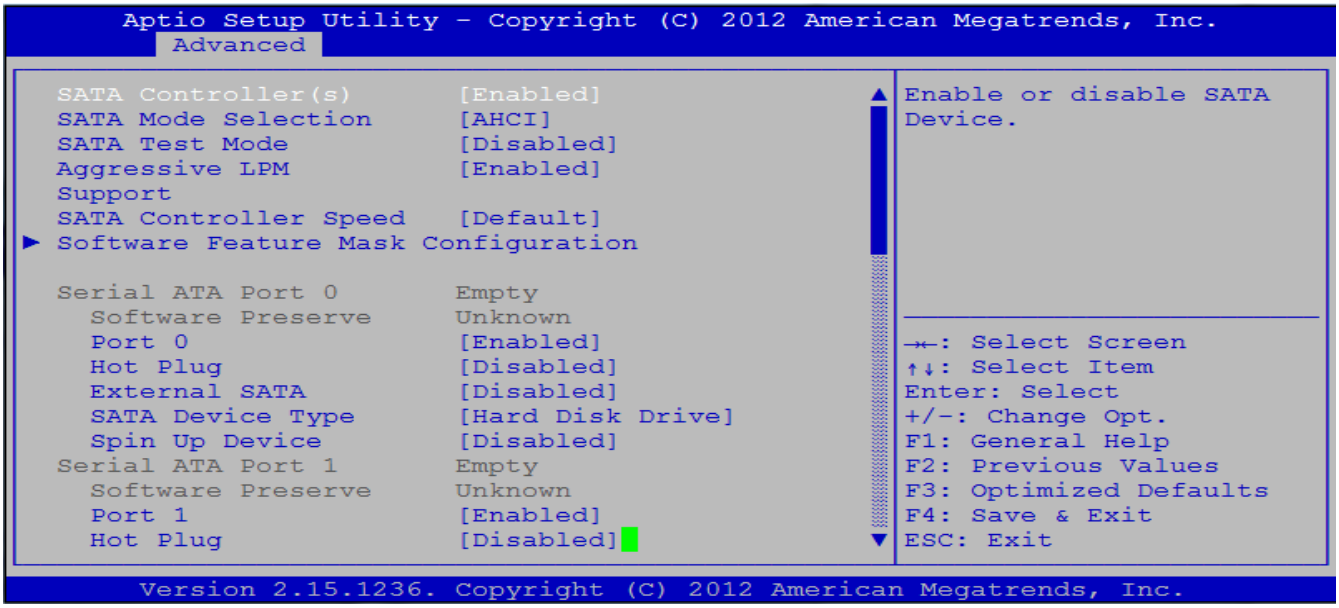
		energy efficiency. The default engages Turbo Boost immediately when possible.
Package power limit lock	*Enabled* *Disabled*	When Enabled, Package_Power_Limit MSR will not locked and a reset will be required to unlock the register.
Cpu Power Limit 1		CPU Power Limit1 value. Default is *0*.
Cpu Power Limit 1 Time		Time window which the Power Limit1 is maintained. Default is *0*.
Cpu Power Limit 2		CPU Power Limit2 value. Default is *0*.
Platform power Limit lock	*Enabled* *Disabled*	When enabled, PLAT_FORM_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
Cpu Power Limit 3		CPU Power Limit3 value. Default is *0*.
Cpu Power Limit 3 Time		Time window which the Power Limit3 is maintained. Default is *0*.
Cpu Power Limit 3 Duty Cycle		Specify the duty cycle in percentage that the CPU is required to maintain over the configured Power Limit3 time windows. Default is *0*.
DDR Power Limit 1		DDR Power Limit1 Value. Default is *0*.
DDR Power Limit 1 Time		Time window which the DDR Power Limit1 is maintained. Default is *0*.
DDR Power Limit 2		DDR Power Limit2 Value. Default is *0*.
1-Core Ratio Limit		This limit is for 1 core active. 0 means using the factory-configured value. Default is *0*.
2-Core Ratio Limit		This limit is for 2 cores active. 0 means using the factory-configured value. Default is *0*.
3-Core Ratio Limit		This limit is for 3 cores active. 0 means using the factory-configured value. Default is *0*.
4-Core Ratio Limit		This limit is for 4 cores active. 0 means using the factory-configured value. Default is *0*.
VR Current value		Voltage Regulator Current Limit. 0 means AUTO. Default is *0*.
VR Current value lock	*Enabled* *Disabled*	Locks VR Current Value from further writes until reset.
CPU C states	*Enabled* *Disabled*	Enable or disable CPU C states.
Enhanced C1 state	*Enabled* *Disabled*	Enhanced C1 state.
CPU C3 Report	*Enabled* *Disabled*	Enable/Disable CPU C3 Report to OS.
CPU C6 Report	*Enabled* *Disabled*	Enable/Disable CPU C6 Report to OS.
C6 Latency	*Short* *Long*	Configure Short/Long latency for C6.
CPU C7 Report	*Disabled*	Enable/Disable CPU C7 Report to OS.

	CPU C7 *CPU C7s*	
C7 Latency	*Short* *Long*	Configure Short/Long latency for C7.
C1 state auto demotion	*Enabled* *Disabled*	Processor will conditionally demote C3/C6/C7 requests to C1 based on uncore autodemote information. Default is *Enabled*.
C3 state auto demotion	*Enabled* *Disabled*	Processor will conditionally demote C6/C7 requests to C3 based on uncore autodemote information. Default is *Enabled*.
C1 state auto undemotion	*Enabled* *Disabled*	Un-demotion from Demoted C1.
C3 state auto undemotion	*Enabled* *Disabled*	Un-demotion from Demoted C3.
C state Pre-Wake	*Enabled* *Disabled*	Enable or Disable C State Pre-Wake feature.
Package C State Limit	*C0* *C2* *C3* *C6* *C7* *C7s* *AUTO*	Select Auto for the AMI BIOS to automatically set the limit on the C-State package register..
LakeTiny Feature	*Disabled* *Enabled*	Select Enabled for LakeTiny feature support for C-State configuration. Default is *Disabled*.
ACPI CTDP BIOS	*Disabled* *Enabled*	Enable/Disable Advanced Configuration and Power Interface (ACPI) Configurable Thermal Design Power (cTDP) support. Default is *Disabled*.
Configurable TDP	*TDP NOMINAL* *TDP DOWN* *TDP UP* *Disabled*	Allows re-configuration of the Configurable Thermal Design Power (TDP) levels based on current power and thermal delivery capabilities of the system. When the processor runs at its rated frequency and TDP. When a cooler or quieter mode of operation is desired, this mode specifies a lower TDP and lower guaranteed frequency versus the nominal mode. TDP UP is not currently supported. This option disabled TDP.
Config TDP Lock	*Disabled* *Enabled*	This feature allows the lock the Configurable Thermal Design Power Control Register.
Intel TXT(LT) Support	*Disabled* *Enabled*	Enables or Disables Intel's Trusted Execution Technology (TXT). This technology was formerly known as LaGrande Technology (LT). This feature provides dynamic root of trust for measurement (DRTM), data protection in case of improper shutdown, and measurement and verification of launched environment.
ACPI T State	*Disabled* *Enabled*	Select Enabled to support Advanced Configuration and Power Interface (ACPI) Throttling States (T State), which will lower the power consumption level for the

		system as to the power consumption level set for CPU Performance State 1 to achieve power efficiency.
CPU DTS	*Disabled* *Enabled*	When Disabled, ACPI thermal management uses EC reported temperature values. When Enabled, ACPI Thermal management uses Digital Thermal Sensors (DTS) to obtain CPU Temperature values.
Debug Interface	*Disabled* *Enabled*	Enable or Disable CPU debug feature.
Debug Interface Lock	*Enabled* *Disabled*	Lock CPU Debug feature setting.

2.2.3 SATA Configuration

Fig. 2.2.3.a SATA Configuration



The general SATA options allow the user to view and configure the SATA settings of the system.

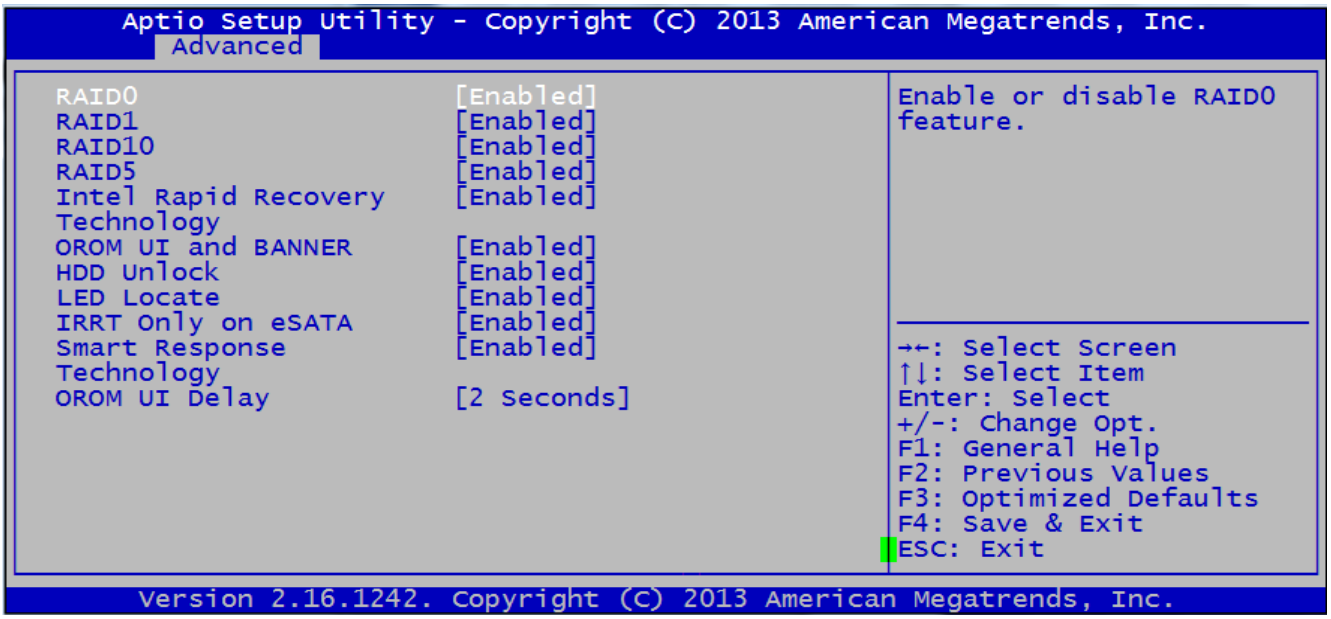
Feature	Options	Description
SATA Controllers(s)	*Enabled* *Disabled*	Enable or Disable the onboard SATA controller.
SATA Mode Selection	*IDE* *AHCI* *RAID*	Determines how SATA controller(s) operate. Please note that modifying this option after installation may require you to reinstall Windows.
SATA Test Mode	*Enabled* *Disabled*	Enable or Disable Test Mode.
Aggressive LPM Support	*Enabled* *Disabled*	Enable PCH to aggressively enter link power state. *Aggressive Link Power Management* (ALPM) is a power-saving technique that helps the disk save power by setting a SATA link to the disk to a low-power setting during idle time (that is when there is no I/O). ALPM automatically sets the SATA link back to an active power state once I/O requests are queued to that link. Power savings introduced by ALPM come at the expense of disk latency. As such, you should only use ALPM if you expect the system to experience long periods of idle I/O time.
SATA Controller Speed	*Default* *Gen1* *Gen2* *Gen3*	Indicates the maximum speed the SATA controller can support. Please select based on your SATA device.

The SATA port setting options allow the user to view and configure individual SATA devices on each of the SATA ports from 0 to 5.

Feature	Options	Description
Serial ATA Port X		This option is view only and identifies the SATA drive and size of the SATA device connected to this port. i.e. *MKNSSDAT120GB (120.0GB)*
Software Preserve		This is a view only option that specified whether the SATA device supports Software Preserve.
Port X	*Enabled* *Disabled*	Enable or Disable SATA Port. Please consult your specific board's user manual for what SATA Pots are available.
Hot Plug	*Enabled* *Disabled*	Designates whether this port is hot pluggable.
Mechanical Presence Switch	*Enabled* *Disabled*	Controls reporting if this port has an optional Mechanical Presence switch. This option is currently not supported.
External SATA	*Enabled* *Disabled*	Identifies if the drive needs External SATA (eSATA) Support.
SATA Device Type	*Hard Disk Drive* *Solid State Drive*	Identify if the SATA port is connected to a Solid State Drive (SSD) or a mechanical Hard Disk Drive.
Spin Up Device	*Enabled* *Disabled*	When enabled, on an edge detect from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.

2.2.3.1 SATA Software Feature Mask Configuration

Fig. 2.2.3.1.a SATA Software Feature Mask Configuration



This option allows the user to view and configure the SATA Software Feature Mask Configuration options.

Feature	Options	Description
RAID0	*Enabled* *Disabled*	Enable or disable RAID0 feature.
RAID1	*Enabled* *Disabled*	Enable or disable RAID1 feature.
RAID10	*Enabled* *Disabled*	Enable or disable RAID10 feature.
RAID5	*Enabled* *Disabled*	Enable or disable RAID5 feature.
Intel Rapid Recovery Technology	*Enabled* *Disabled*	Enable or disable Intel Rapid Recovery Technology.
OROM UI and BANNER	*Enabled* *Disabled*	If enabled, then the Option ROM (OROM) User Interface (UI) is shown. Otherwise, no OROM banner or information will be displayed if all disks and RAID volumes are Normal.
HDD Unlock	*Enabled* *Disabled*	If enabled, indicates that the Hard Disk Drive (HDD) password unlock in the OS is enabled.
LED Locate	*Enabled* *Disabled*	If enabled, it indicates that the LED/SGPIO hardware is attached and the *ping to locate* feature is enabled on the OS.
IRRT only on eSATA	*Enabled* *Disabled*	If enabled, then only IRRT volumes can span internal and eSATA drives. If disabled, then any RAID volume can span internal and eSATA drives.
Smart Response Technology	*Enabled* *Disabled*	Enable or Disable Smart Response Technology.

OROM UI Delay	*2 Seconds* *4 Seconds* *6 Seconds* *8 Seconds*	If enabled, indicates the delay of the Option ROM (OROM) User Interface (UI)Splash Screen in a normal status. .

2.2.4 Thermal Configuration

Fig. 2.2.4.a Thermal Configuration

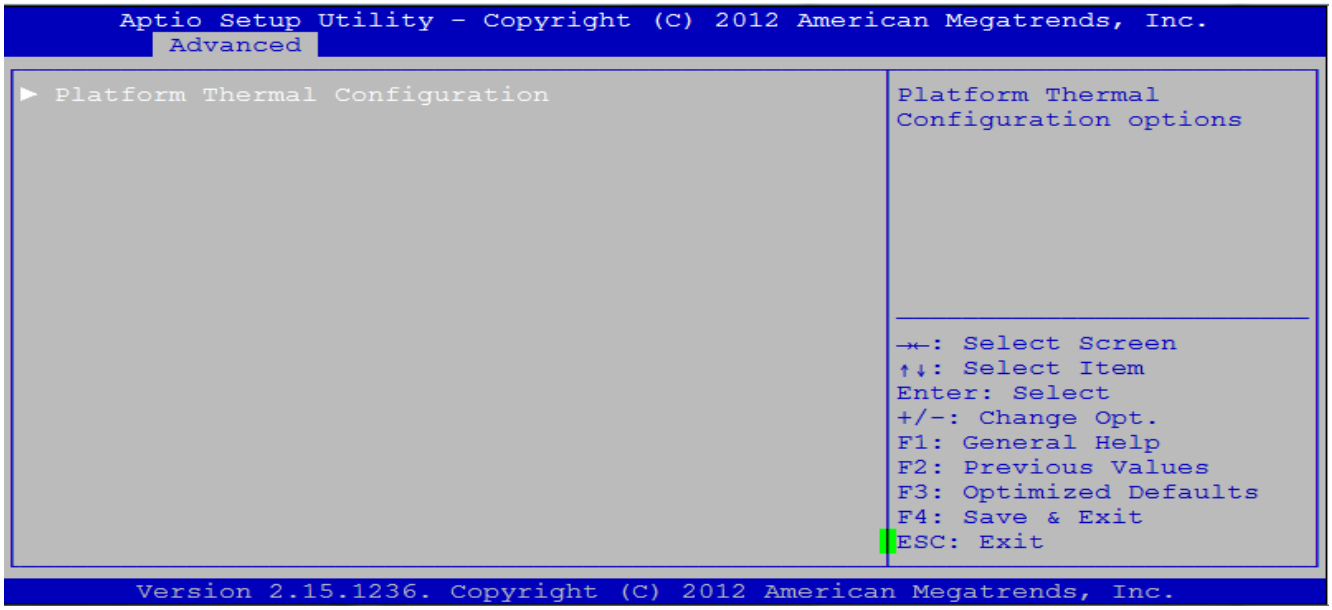
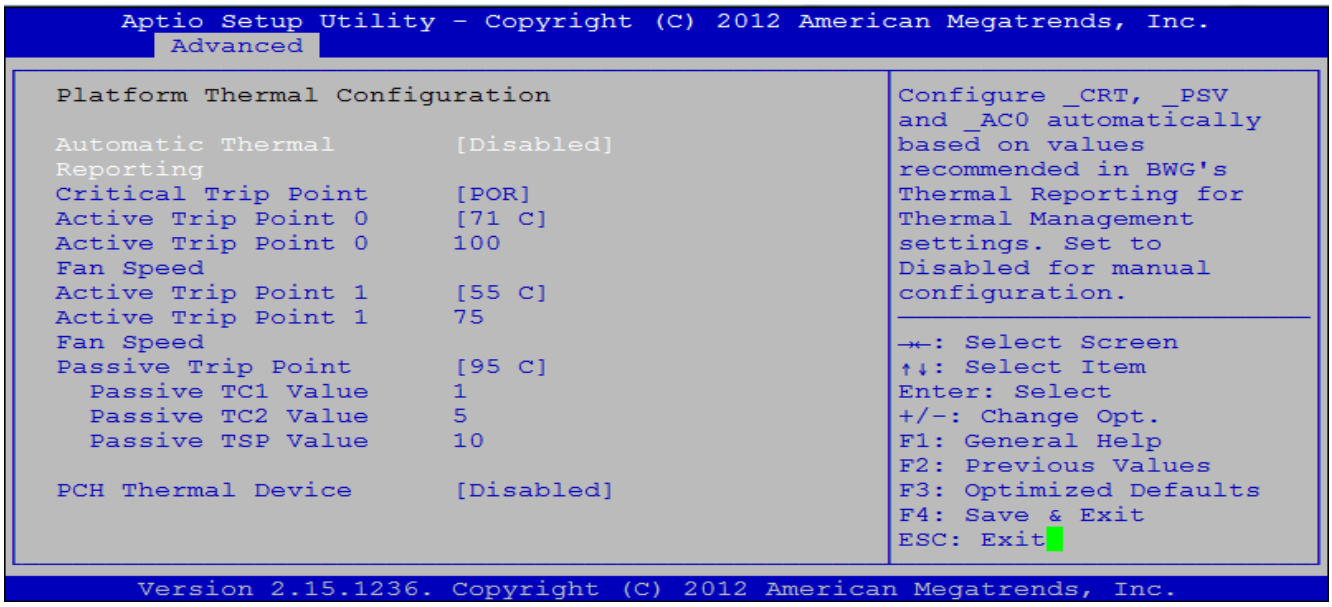


Fig. 2.2.4.b Platform Thermal Configuration

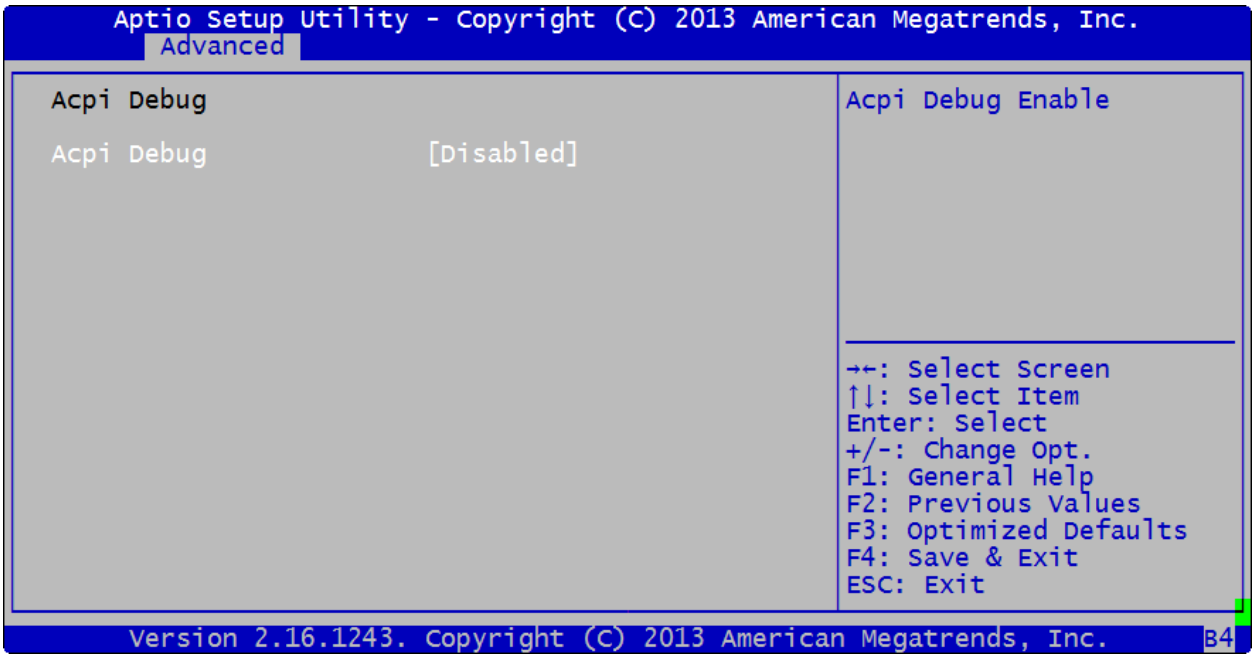


This option allows the user to view and configure the Platform Thermal Configuration options.

Feature	Options	Description
Automatic Thermal Reporting	*Enabled* *Disabled*	Configure _CRT, _PSV, and _ACO automatically based on values recommended in BWG's Thermal Reporting for Thermal Management settings. Set to Disabled for manual configuration.
Critical Trip Point	*POR* *15°C* *23 °C* ... *127°C*	This value controls the temperature of the ACPI Critical Trip Point – the point in which the OS will shut the system off. The temperature range is from 15°C to 127°C. Please note that this feature is only available when Automatic Thermal Reporting is Disabled. NOTE: 100°C is the Plan of Record (POR) for all Intel mobile processors. Default value is *POR.*
Active Trip Point 0	*Disabled* *15°C* *23 °C* ... *71°C* *119°C*	This value controls the temperature of the ACPI Active Trip Point 0 – the point in which the OS will turn the processor fan on Active Trip Point 0 Fan Speed. Please note that this feature is only available when Automatic Thermal Reporting is Disabled.
Active Trip Point 0 Fan Speed	*0%* … *100%*	Active Trip Point 0 Fan speed in percentage. Value must be between 0 (Fan off) – 100 (Max fan speed). This is the speed at which fan will run when Active Trip Point 0 is crossed.
Active Trip Point 1	*Disabled* *15°C* *23 °C* ... *55°C* *119°C*	This value controls the temperature of the ACPI Active Trip Point 1 – the point in which the OS will turn the processor fan on Active Trip Point 1 Fan Speed.
Active Trip Point 1 Fan Speed	*0%* ... *75%* *100%*	Active Trip Point 1 Fan speed in percentage. Value must be between 0 (Fan off) – 100 (Max fan speed). This value must be less than Active Trip Point 0 Fan Speed. This is the speed at which fan will run when Active Trip Point 1 is crossed.
Passive Trip Point	*Disabled* *15°C* *23 °C* ... *95°C* *119°C*	This value controls the temperature of the ACPI Passive Tip Point – the point in which the OS will begin throttling the processor down. Please note that this feature is only available when Automatic Thermal Reporting is Disabled.
Passive TC1 Value		This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 – 16. Default is *1.*
Passive TC2 Value		This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 – 16. Default is *5.*
Passive TSP Value		This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 – 32. Default is *10.*
PCH Thermal Device	*Enabled* *Disabled*	Enable or Disable the PCH Thermal Device (D31:F6). Default is *Disabled.*

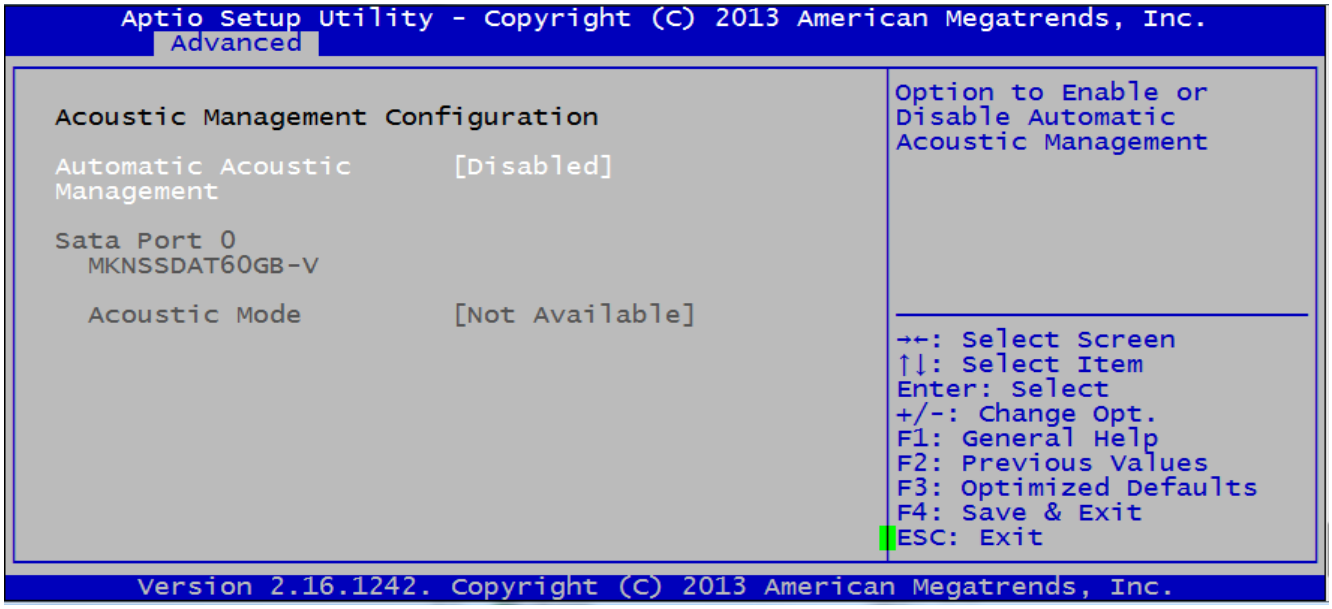
2.2.5 Acpi Debug Configuration

Fig. 2.2.5.a ACPI Debug Configuration



2.2.6 Acoustic Management Technology Configuration

Fig. 2.2.6.a Acoustic Management Technology Configuration



2.2.7 PCH-FW Configuration

Fig. 2.2.7.a PCH-FW Configuration

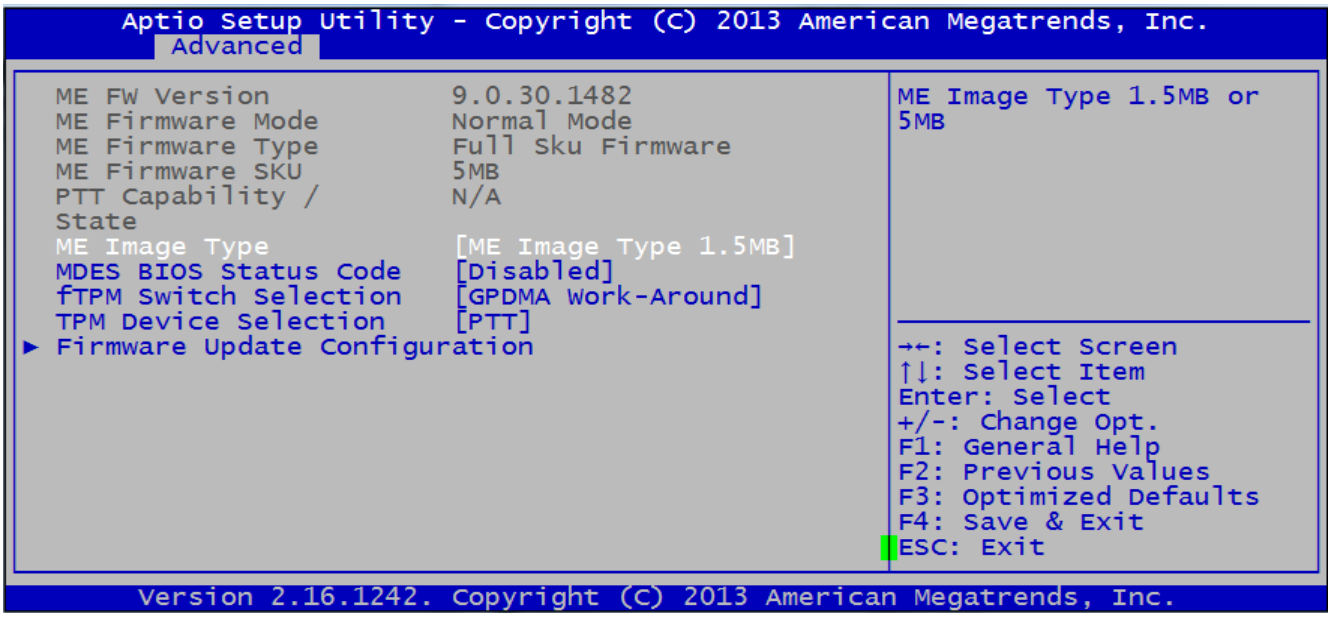
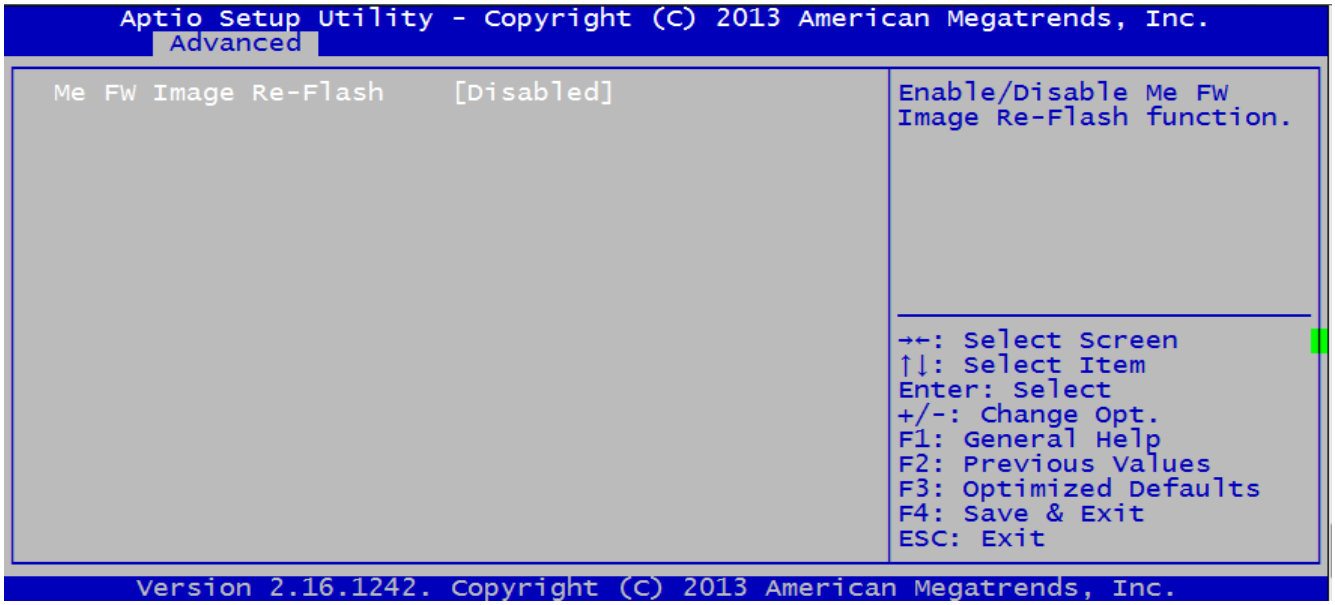
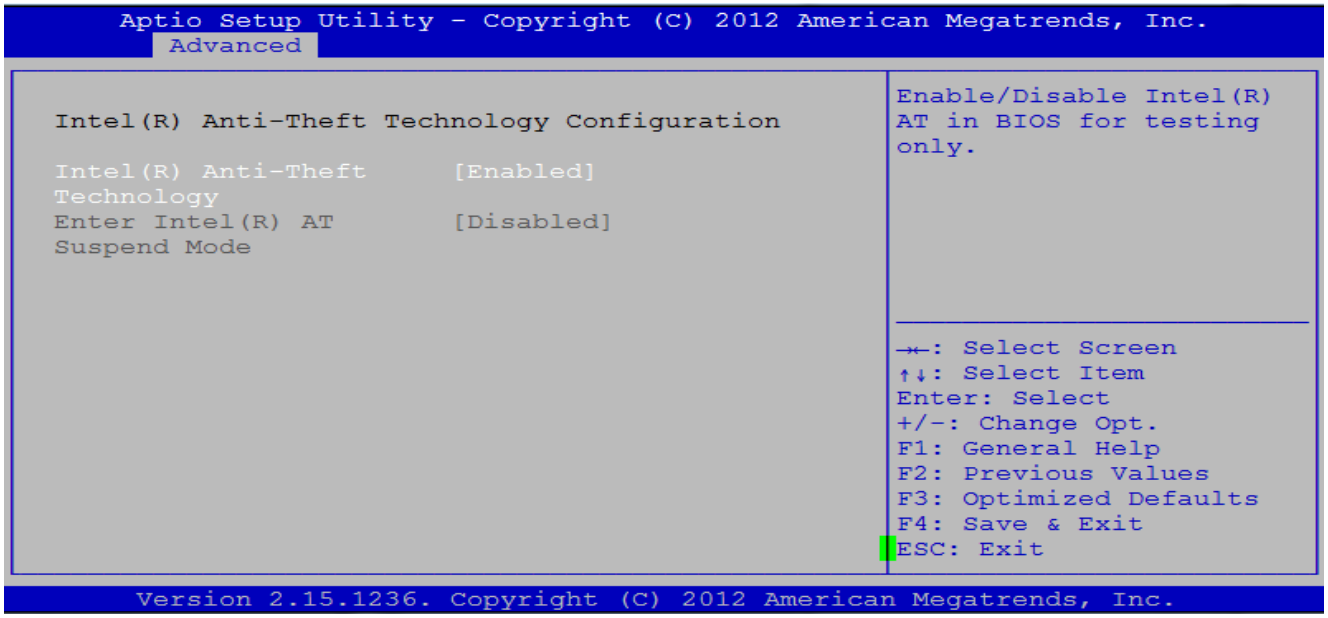


Fig. 2.2.7.b Firmware Update



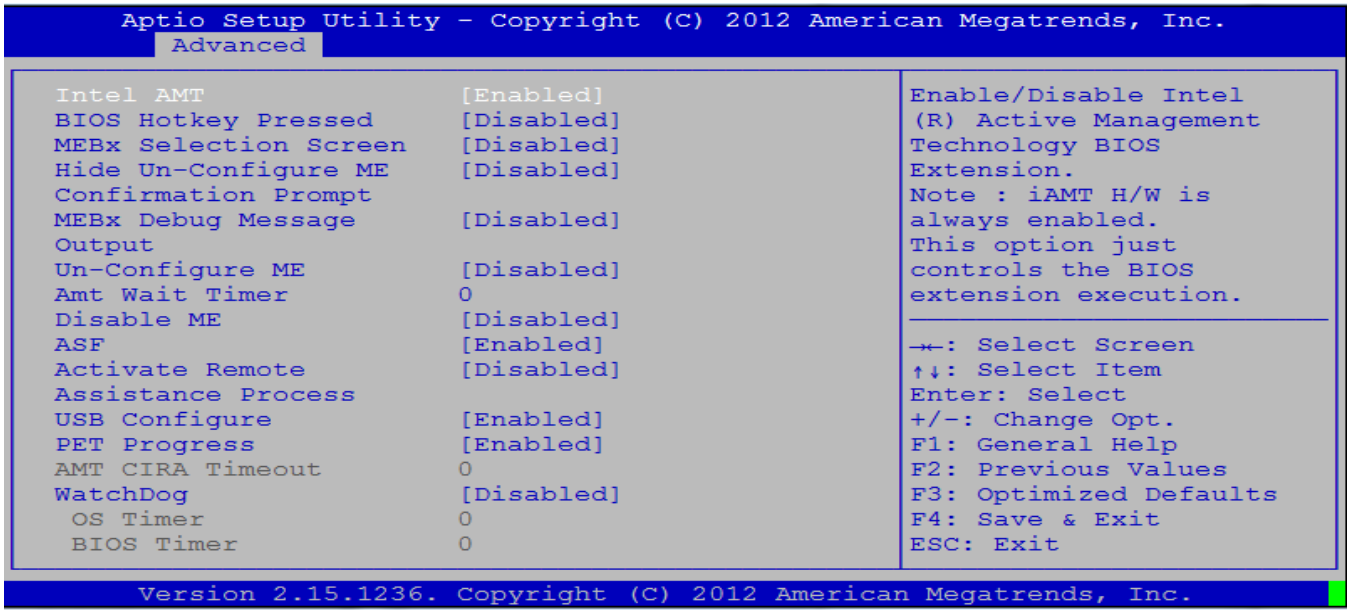
2.2.8 Intel® Anti-Theft Technology Configuration

Fig. 2.2.8.a Intel® Anti-Theft Technology Configuration



2.2.9 AMT Configuration

Fig. 2.2.9.a AMT Configuration



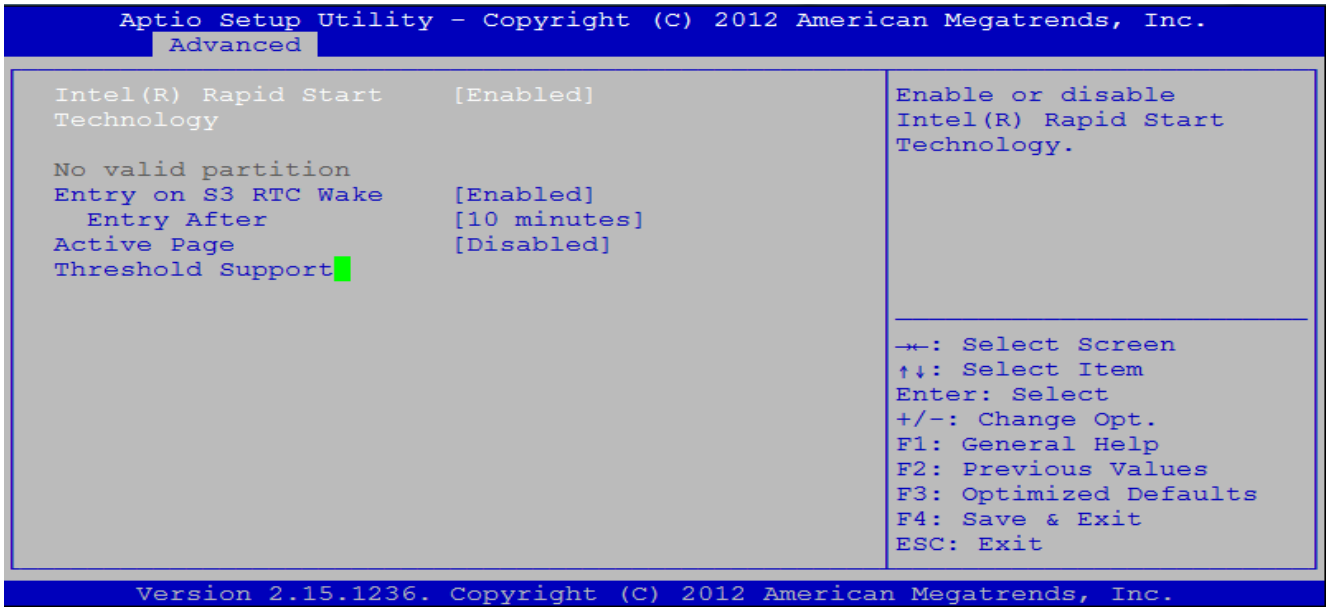
This option allows the user to view and configure the Intel Activate Management Technology (AMT) parameters.

Feature	Options	Description
Intel AMT	*Enabled* *Disabled*	Use this item to enable or disable the Intel Active Management Technology (iAMT) BIOS Extension. Note: iAMT Hardware is always enabled. This option just controls the BIOS extension execution. If enabled, this requires additional firmware in the SPI device.
BIOS Hotkey Pressed	*Enabled* *Disabled*	Use this item to enable/disable BIOS hotkey press. (OEMFlag Bit 1)
MEBx Selection Screen	*Enabled* *Disabled*	Use this item to enable/disable the Management Engine BIOS Extension (MEBx) selection screen. (OEMFlag Bit 2)
Hide Un-Configure ME Confirmation Prompt	*Enabled* *Disabled*	Use this item to enable/disable hide un-configure Management Engine (ME) without password confirmation prompt. (OEMFlag Bit 6)
MEBx Debug Message Output	*Enabled* *Disabled*	Use this item to enable/disable the Management Engine Bios Extension (MEBx) debug message output. (OEMFlag Bit 14)
Un-Configure ME	*Enabled* *Disabled*	Use this item to enable/disable un-configure Management Engine (ME) without password. (OEMFlag Bit 15)
AMT Wait Timer		Set the Active Management Technology (AMT) timer to wait before sending ASF_GET_BOOT_OPTIONS. Default is *0*.
Disable ME	*Enabled* *Disabled*	Use this item to enable/disable set Management Engine (ME) to Soft Temporary Disabled.
ASF	*Enabled* *Disabled*	Use this item to enable/disable Alert Specification Format (ASF).

Activate Remote Assistance Process	*Enabled* *Disabled*	Use this item to enable/disable trigger Client Initiated Remote Access (CIRA) boot.
USB Configure	*Enabled* *Disabled*	Use this item to enable/disable USB configure function.
PET Progress	*Enabled* *Disabled*	When Enabled, the Intel(R) AMT firmware receives all progress Platform Event Trap (PET) events.
AMT CIRA Timeout		This option is only available when Activate Remote Assistance Process is Enabled. This is the amount of time to wait to establish a Client Initiated Remote Access (CIRA) connection. Default is *0*. 0 – Use the default timeout value of 60 seconds 255 – MEBX waits until the connection succeeds.
WatchDog	*Enabled* *Disabled*	Use this item to enable or disable the WatchDog Timer.
OS Timer	*0*	Sets the Operating System (OS) Watchdog Timer.
BIOS Timer	*0*	Sets the BIOS Watchdog Timer.

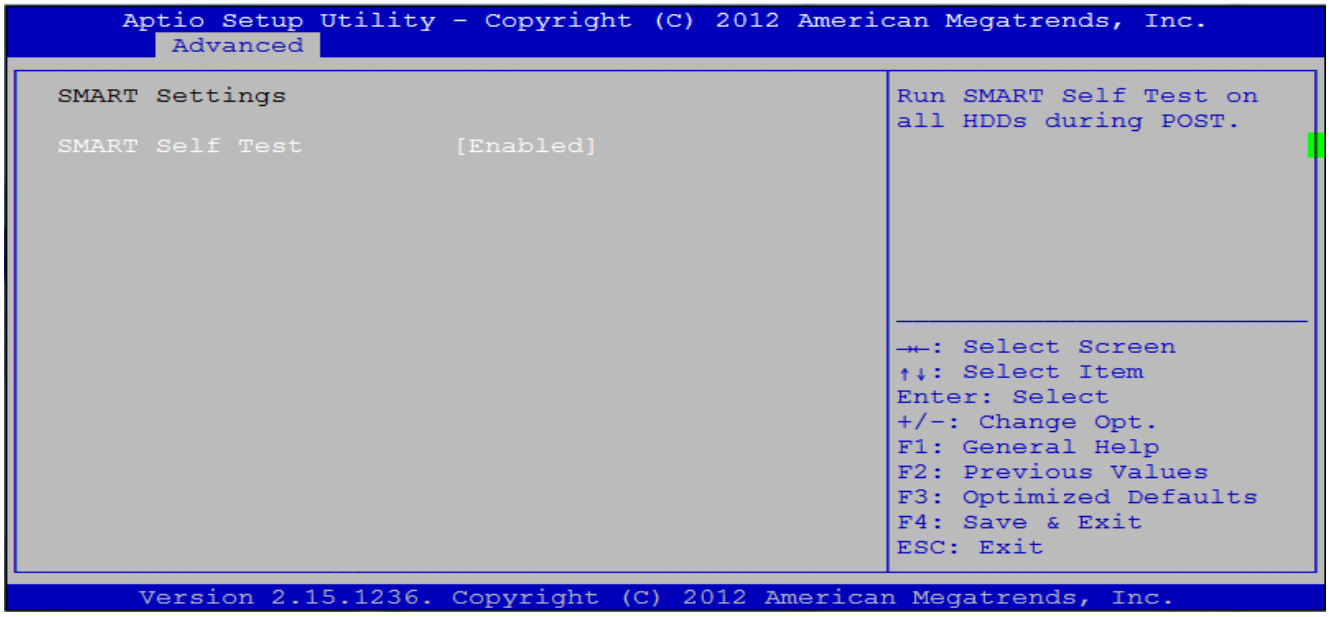
2.2.10 Intel® Rapid Start Technology

Fig. 2.2.10.a Intel® Rapid Start Technology



2.2.11 Smart Settings

Fig. 2.2.11.a Smart Settings



2.2.12 NCT6776 Super IO Configuration

Fig. 2.2.12.a NCT6776 Super IO Configuration

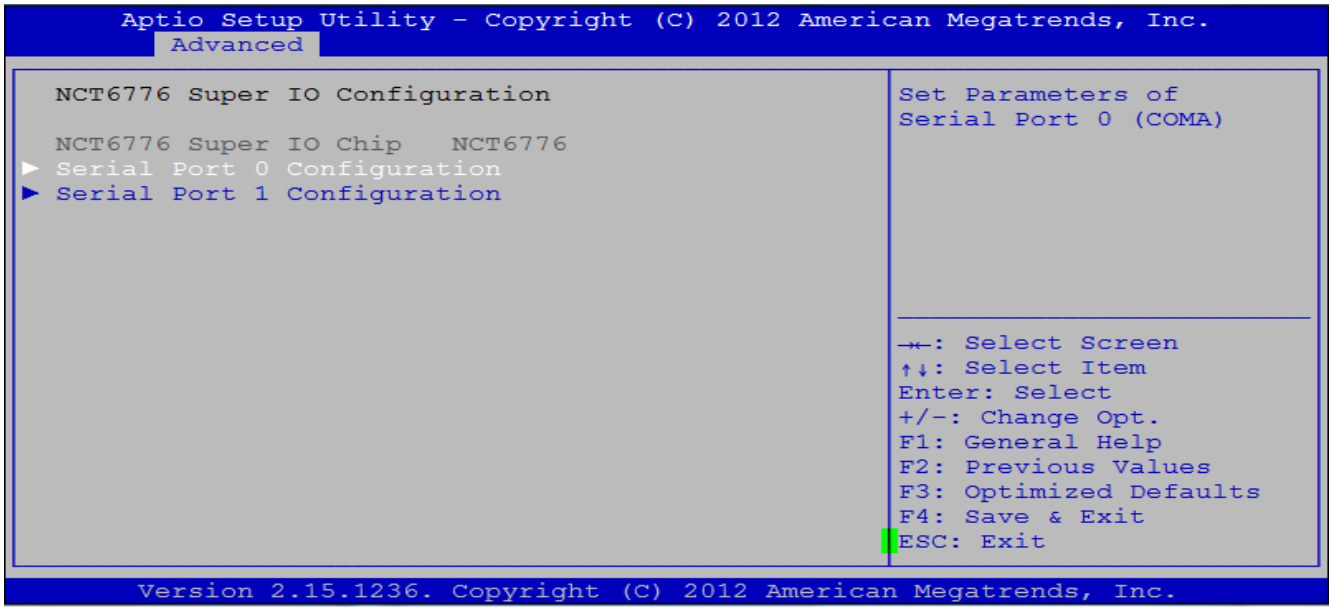
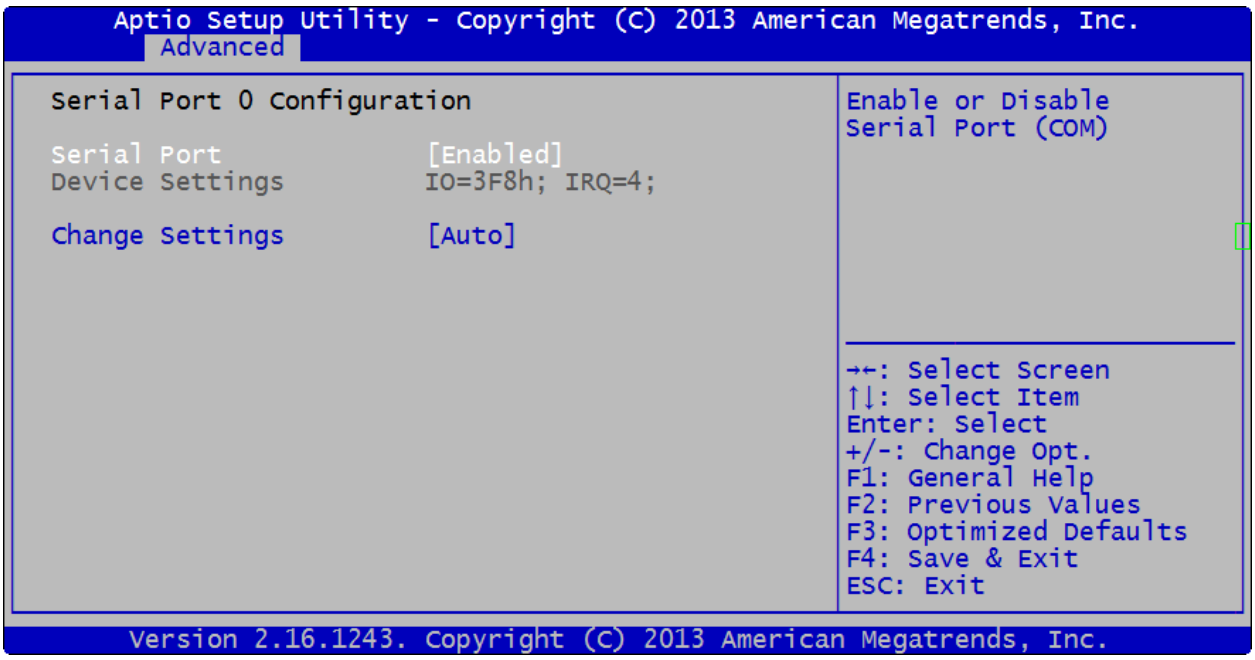


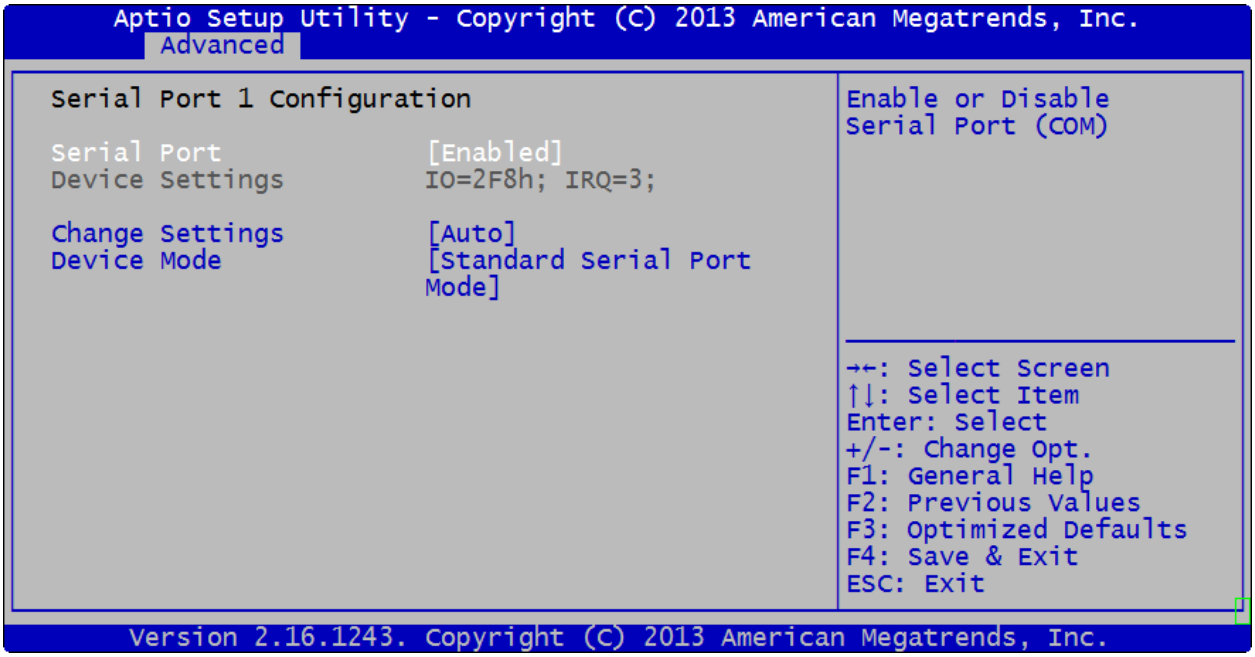
Fig. 2.2.12.b Serial Port 0 Configuration



This option allows the user to view and configure Serial Port 0.

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

Fig. 2.2.12.c NCT6776 Super IO Serial Port 1 Configuration

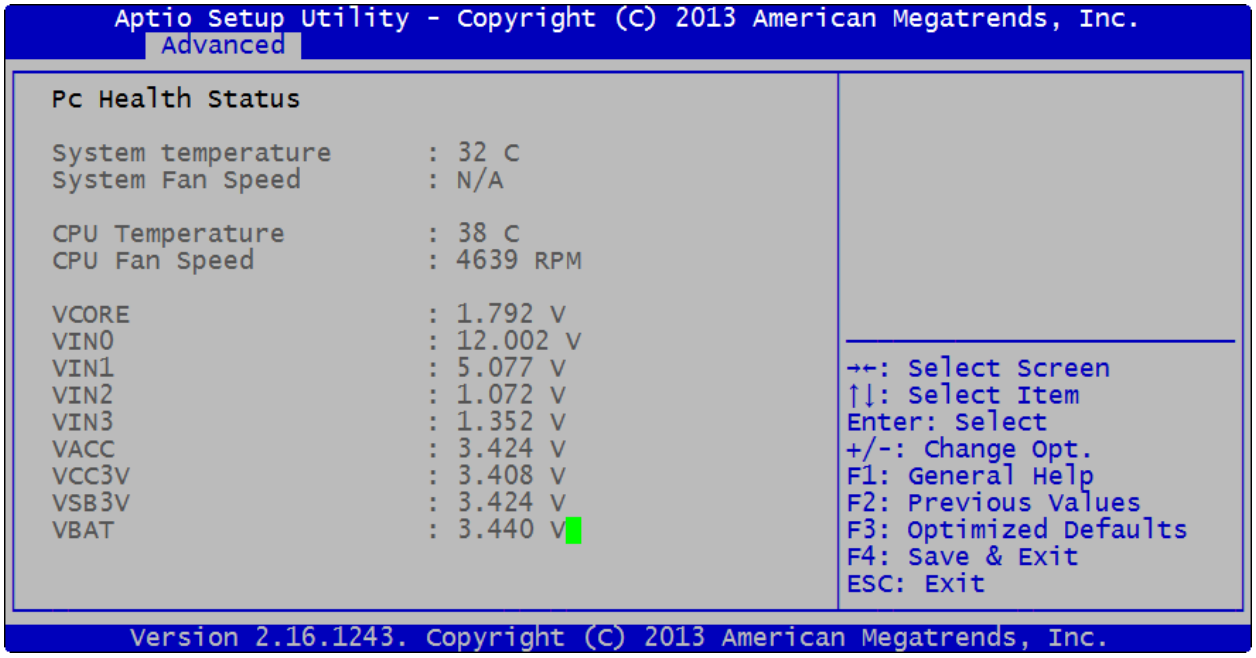


This option allows the user to view and configure Serial Port 1.

Feature	Options	Description
Serial Port	*Enabled* *Disabled*	Enable or Disable Serial Port (COM)
Change Settings	*Auto* *IO=2F8h; IRQ=3;* *IO=3F8h; IRQ=3,4,5,6,7…;* *IO=2F8h; IRQ=3,4,5,6,7…;* *IO=3E8h; IRQ=3,4,5,6,7…;* *IO=2E8h; IRQ=3,4,5,6,7…;*	Select an optimal setting for Serial IO Device
Device Mode	*Standard Serial Port Mode* *IrDA 1.0 (HP SIR) Mode* *ASKIR Mode*	Change the Serial Port mode. Please note that our current hardware only supports Standard Serial Port Mode.

2.2.13 NCT6776 HW Monitor Configuration

Fig. 2.2.13.a NCT6776 HW Monitor Configuration

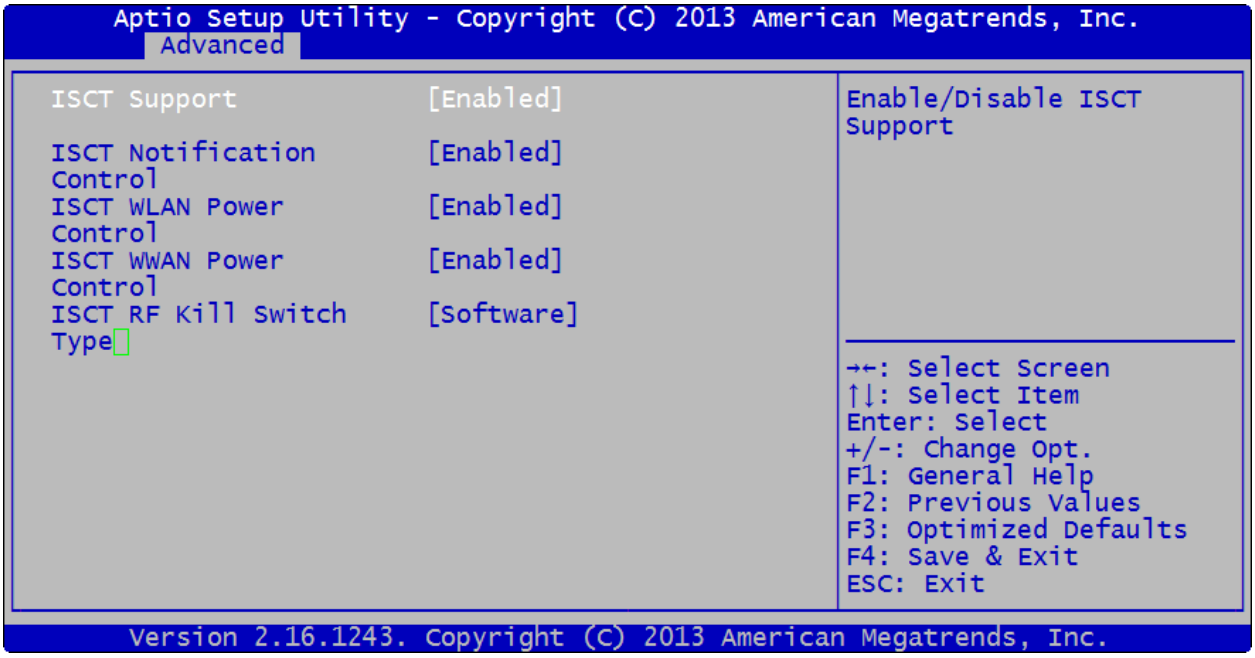


This option allows the user to view system and CPU temperatures, voltages, and the FAN speed.

Option	Description
System Temperature	This reports the 'ambient' temperature of the PCB in Celsius.
System Fan Speed	This option is not available since the system fan is not connected.
CPU Temperature	This reports the CPU temperature in Celsius.
CPU Fan Speed	This value reports the CPU Fan Speed.
VCORE	This value reports the Core CPU voltage.
VIN0	This value reports the 12V Input voltage.
VIN1	This value reports the 5V_standby voltage.
VIN2	This value reports the 1.05V PCH supply voltage.
VIN3	This value reports the supply voltage to the SODIMMs.
VACC VCC3V VSB3V VBAT	All of these values report the 3.3V supply voltage.

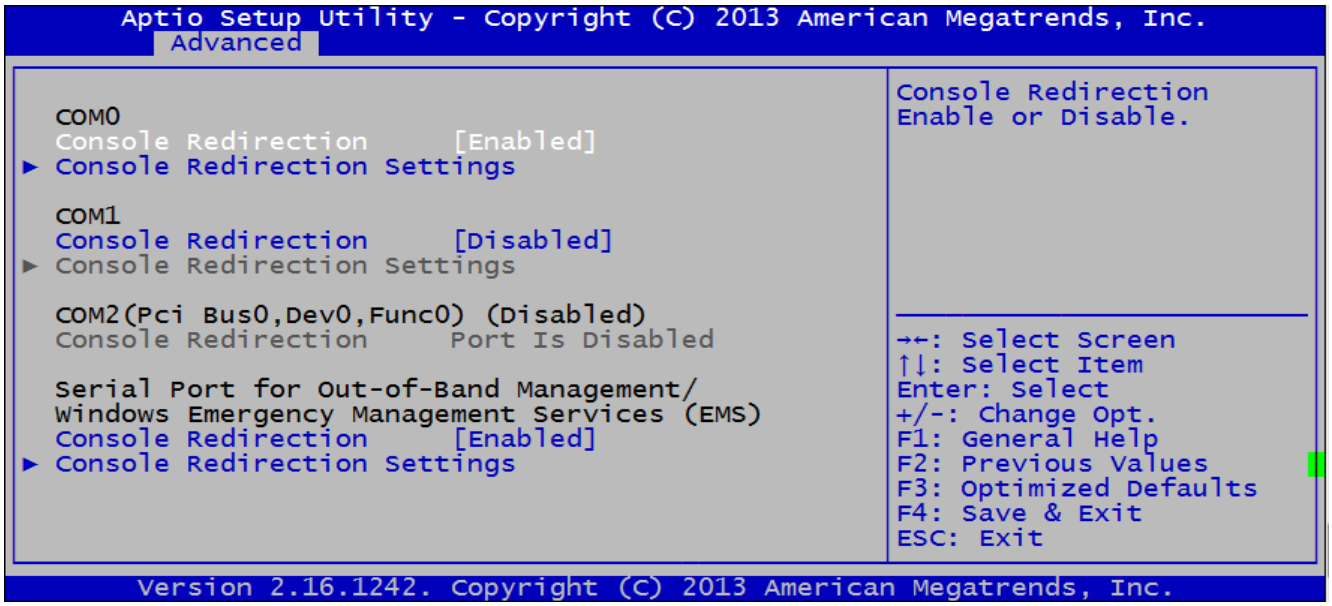
2.2.14 Intel Smart Connect Technology

Fig. 2.2.14.a Intel Smart Connect Technology



2.2.15 Serial Port Console Redirection

Fig. 2.2.15.a Serial Port Console Redirection



2.2.15.1 Console Redirection Settings

Fig. 2.2.15.1.a Console Redirection Settings (Screen 1 of 2)

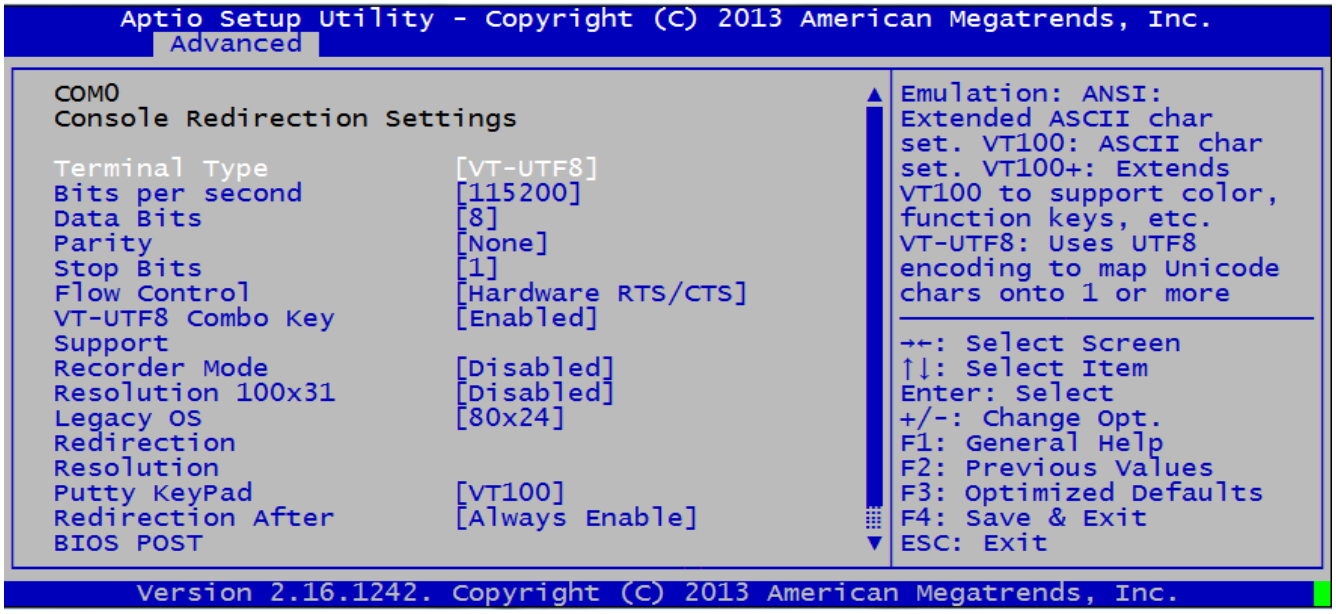
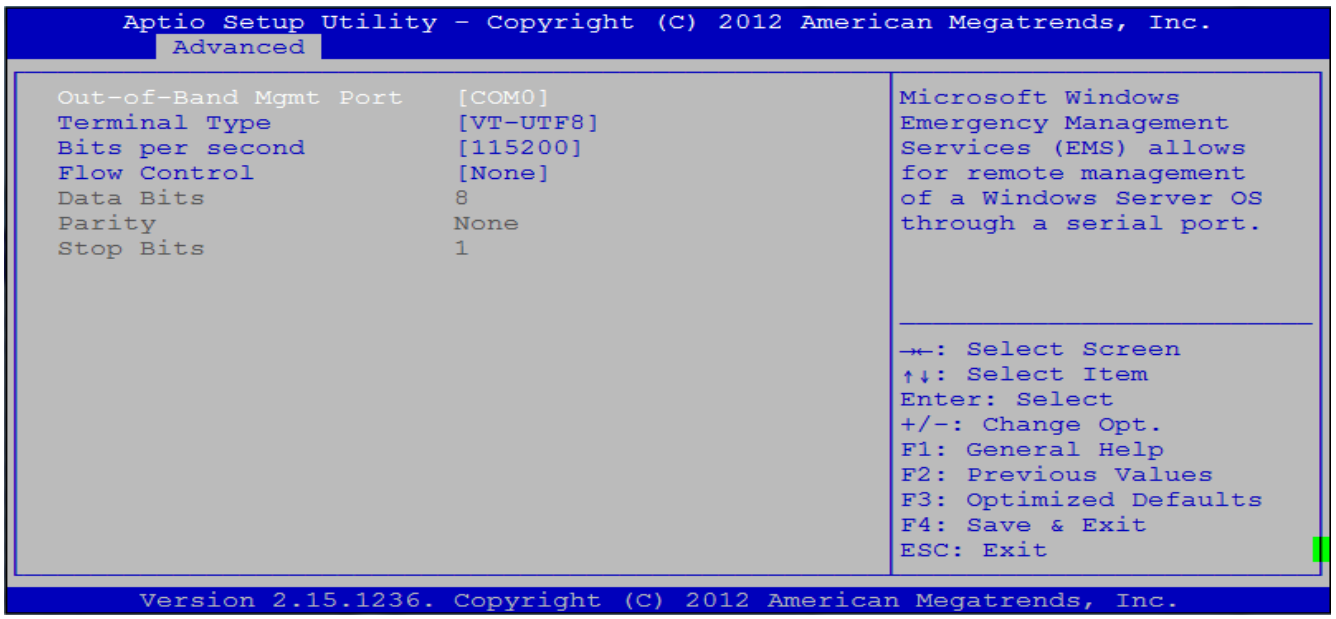
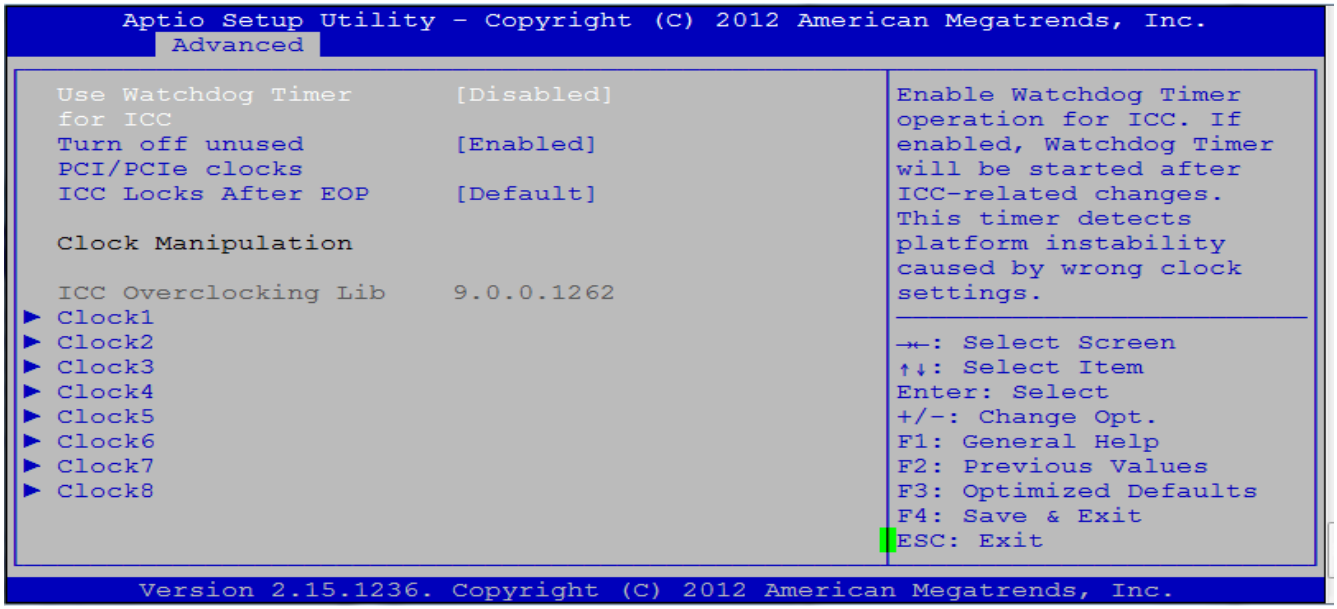


Fig. 2.2.15.1.b Console Redirection Settings (Screen 2 of 2)



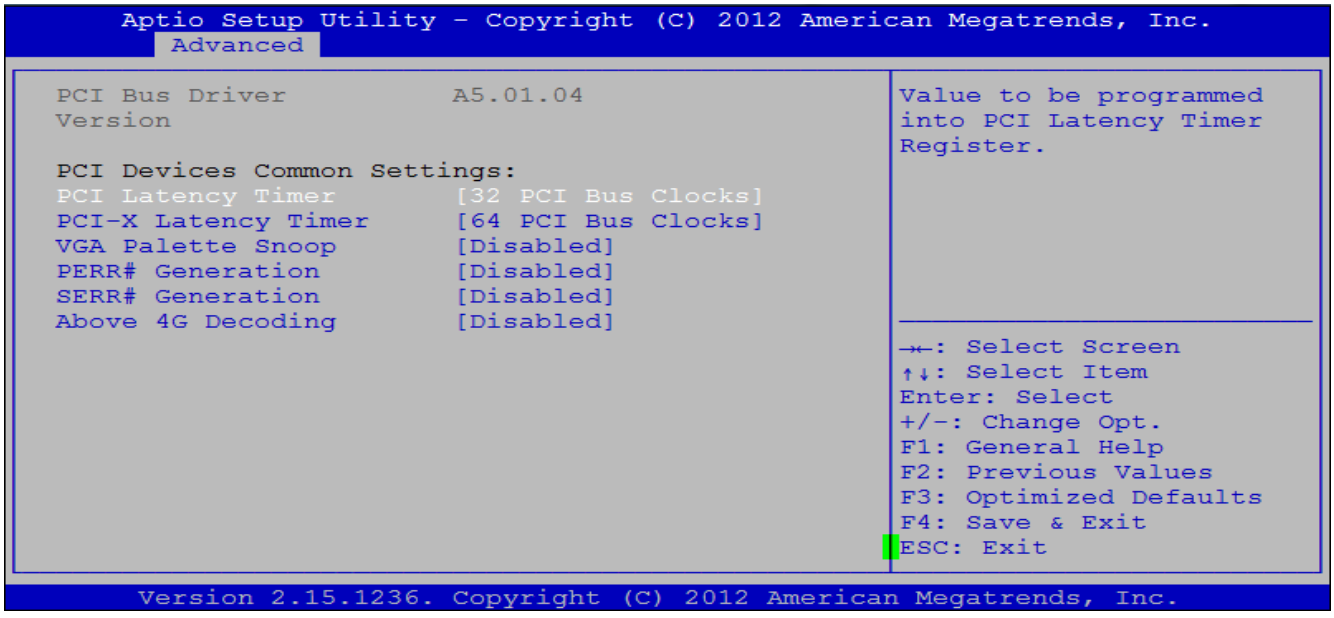
2.2.16 Intel® ICC (Watchdog Timer)

Fig. 2.2.16.a Intel® ICC (Watchdog Timer)



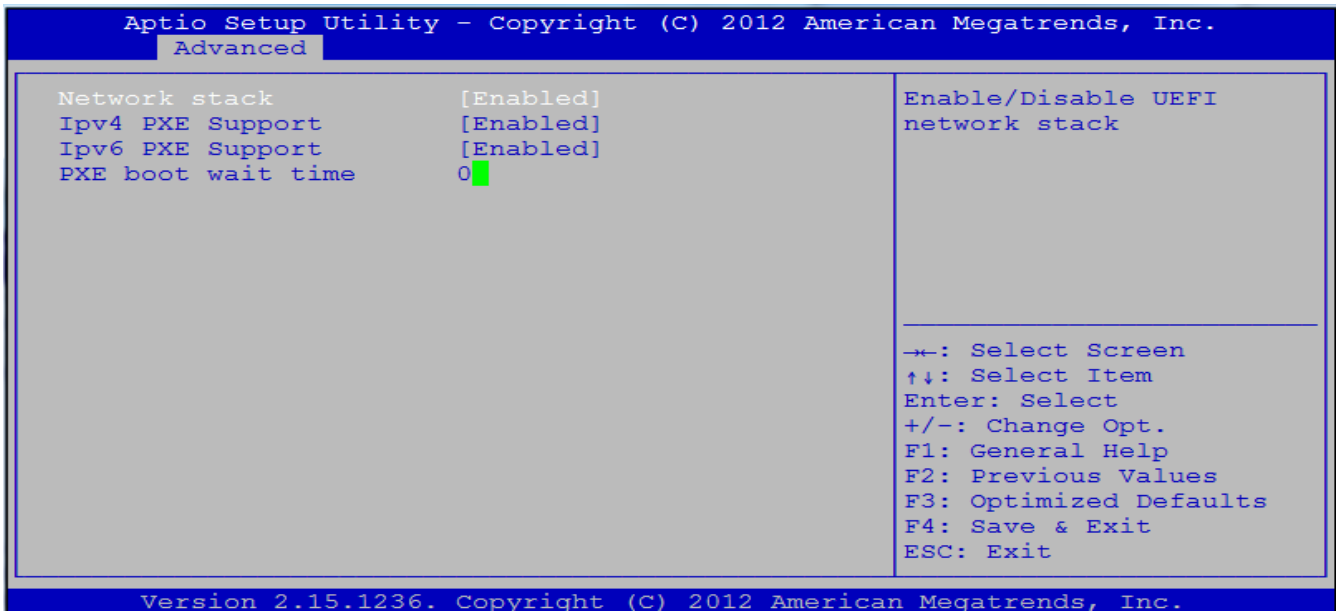
2.2.17 PCI Subsystem Settings

Fig. 2.2.17.a PCI Subsystem Settings



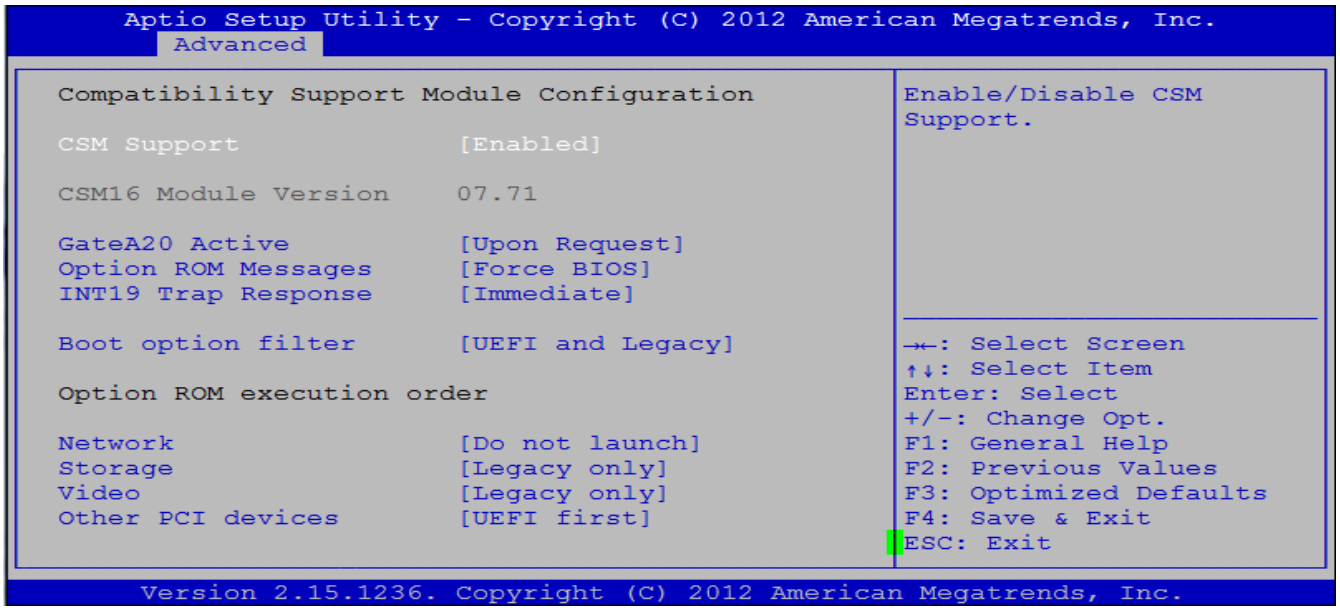
2.2.18 Network Stack

Fig. 2.2.18.a Network Stack



2.2.19 Compatibility Support Mode (CSM) Configuration

Fig. 2.2.19.a CSM Configuration



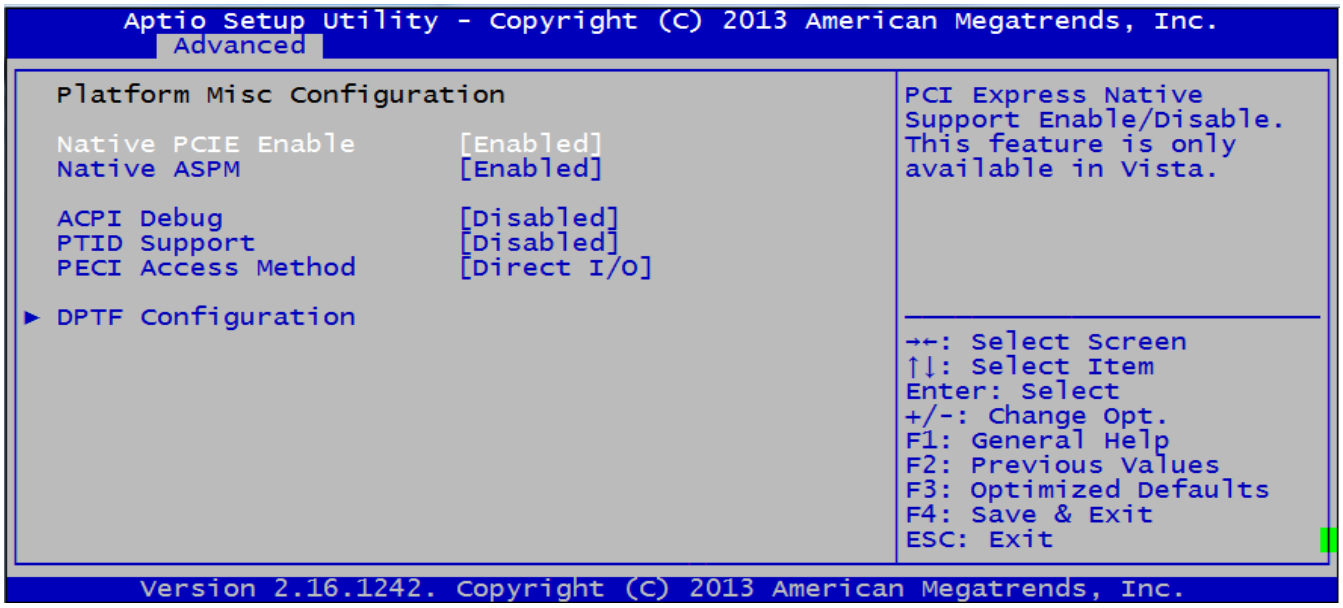
This option allows the user to view and configure the Compatibility Support Mode (CSM) Configuration.

Feature	Options	Description
CSM Support	*Enabled* *Disabled*	Enable or Disable Compatibility Support Mode (CSM) Support.
CSM16 Module Version		Displays CSM Module Version
GateA20 Active	*Upon Request* *Always*	GateA20 (GA20) can be disabled using BIOS Services. Do not allow disabling GA20; This option is useful when any RT code is executed above 1MB.
Option ROM Messages	*Force BIOS* *Keep Current*	Set display mode for Option ROM.
INT19 Trap Response	*Immediate* *Postponed*	BIOS reaction on INT19 trapping by Option ROM. Execute the trap right away. Execute the trap during legacy boot.
Boot Option filter	*UEFI and Legacy* *Legacy only* *UEFI only*	This option filters which ROM type(s) will be available during boot
Network	*Do not launch* *UEFI* *Legacy*	Controls the execution of UEFI and Legacy PXE Option Rom.

Storage	*Do not launch* *UEFI* *Legacy*	Controls the execution of UEFI and Legacy Storage Option Rom (OpROM).
Video	*Do not launch* *UEFI* *Legacy*	Controls the execution of UEFI and Legacy PXE Option Rom (OpROM).
Other PCI devices	*UEFI* *Legacy*	Determines Option ROM (OpROM) execution policy for devices other than Network, Storage, or Video.

2.2.20 Platform Miscellaneous Configuration

Fig. 2.2.18.a Platform Miscellaneous Configuration



2.2.20.1 DPTF Configuration

Fig. 2.2.20.1.a DPTF Configuration (Screen 1 of 5)

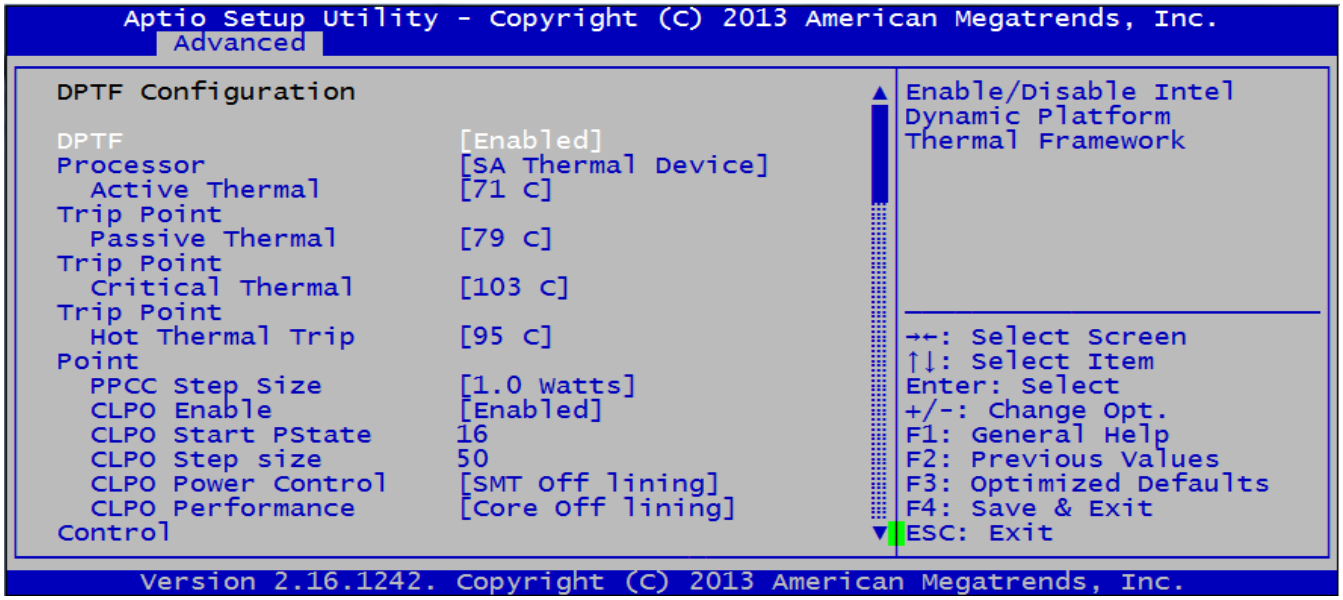


Fig. 2.2.20.1.b DPTF Configuration (Screen 2 of 5)

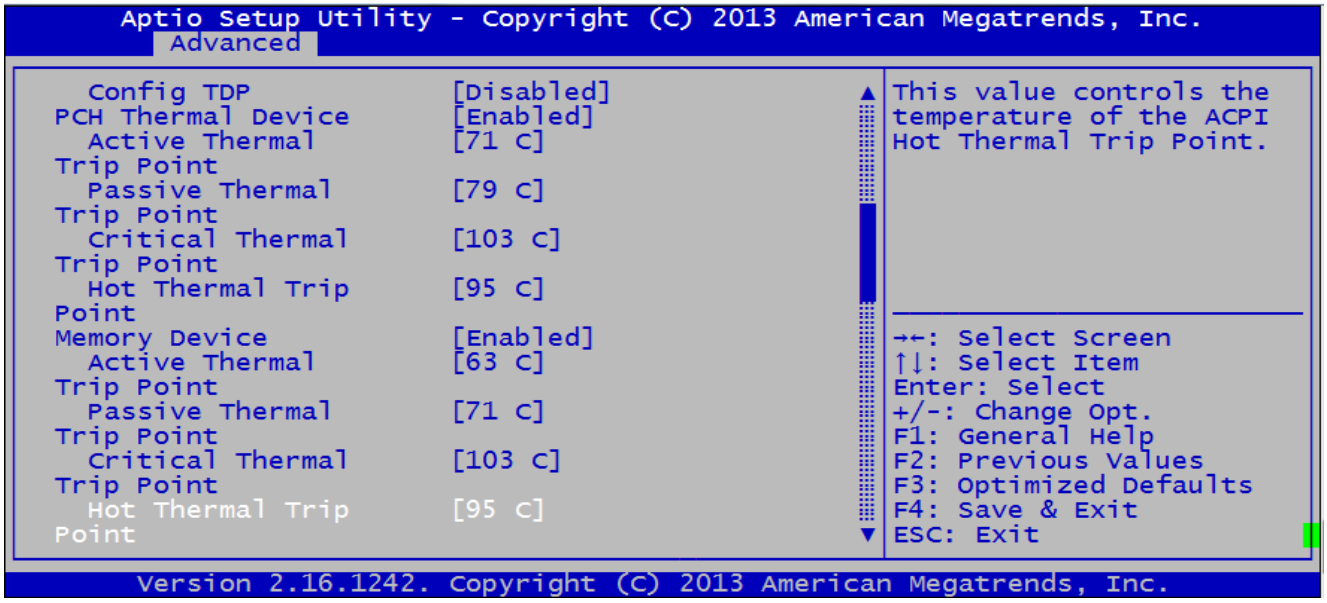


Fig. 2.2.20.1.c DPTF Configuration (Screen 3 of 5)

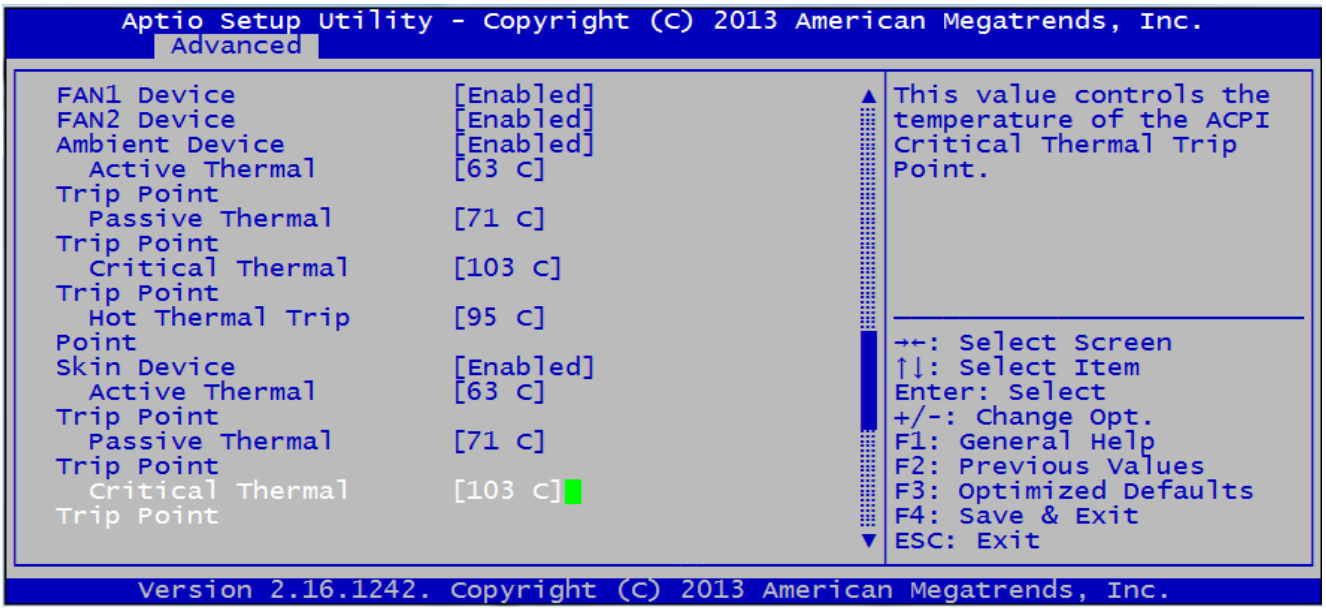
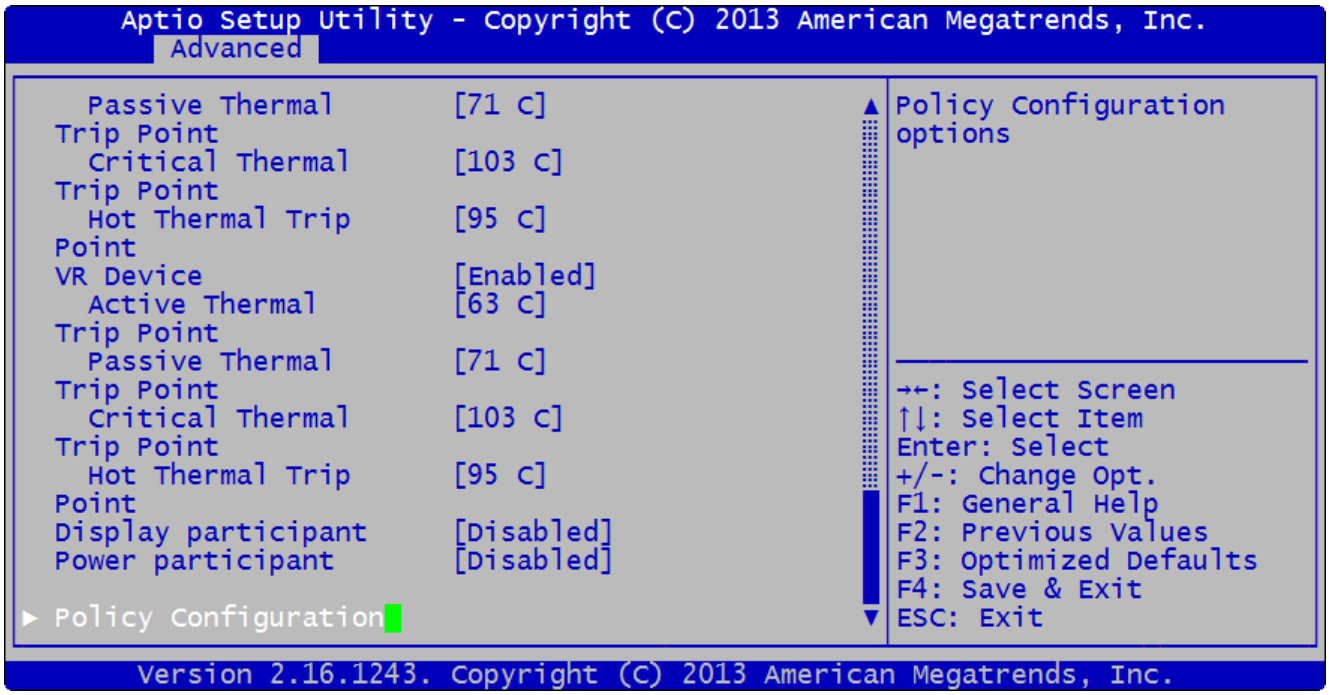


Fig. 2.2.20.1.d DPTF Configuration (Screen 4 of 5)



This option allows the user to view and configure the Dynamic Platform Thermal Framework (DPTF) Configuration.

Feature	Options	Description
DPTF	*Enabled* *Disabled*	Enable or Disable Compatibility Support Mode (CSM) Support.
Processor	*Disabled* *SA Thermal Device* *CPU Thermal Device*	Enable or Disable Processor Thermal Device
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
PPCC Step Size	*0.5 Watts* *1.0 Watts* *1.5 Watts* *2.0 Watts*	Step size for Turbo power Limit (RAPL) control.
CLP0 Enable	*Enabled* *Disabled*	Instructs the policy to use Active Cores if they are available.
CLP0 Start PState	*16*	Instructs the policy when to initiate Active Core control if enabled. Note: 16=LFM
CLP0 Step size	*50*	Instructs the policy to take away logical processors in the specified percentage steps.
CLP0 Power Control	*Disabled* *SMT Off lining* *Core Off lining*	Instructs the policy whether to use Core off lining or SMT off lining if Active core control is enabled to be used in P0 or when power control is applied.
CLP0 Performance Control	*Disabled* *SMT Off lining* *Core Off lining*	Instructs the policy whether to use Core off lining or SMT off lining if Active core control is enabled

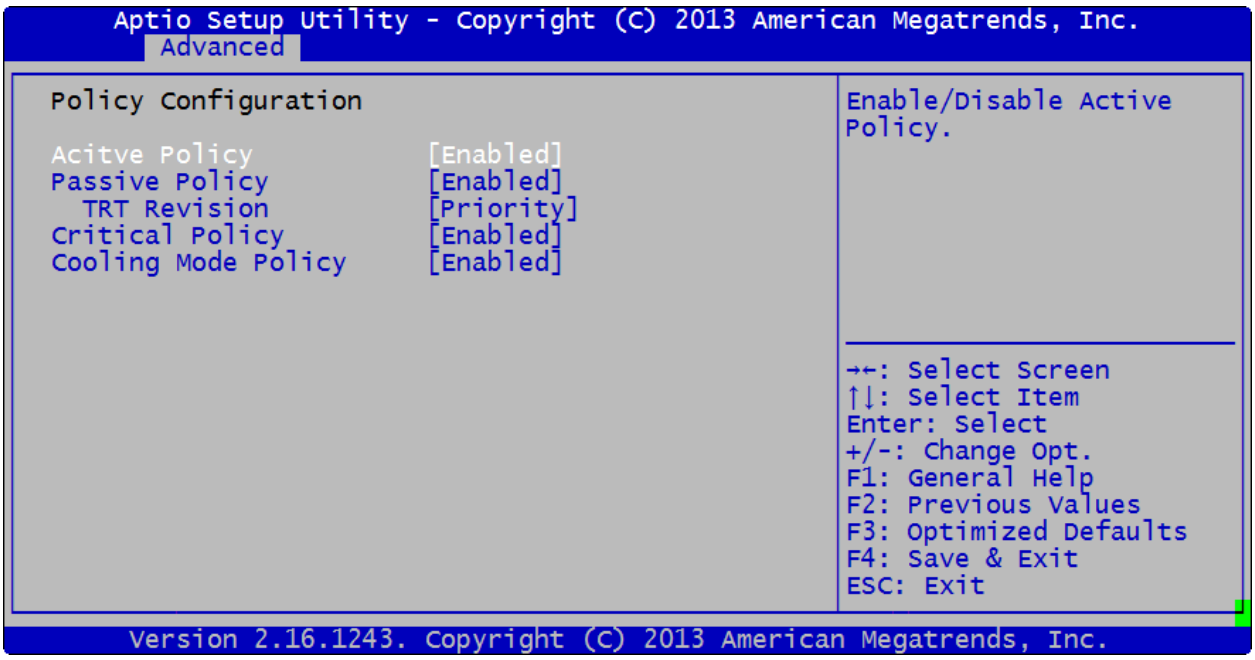
		to be used in P1 or when performance control is applied.
Config TDP	*Disabled* *Enabled*	Enable or Disable Configurable Thermal Design Power (TDP).
PCH Thermal Device	*Enabled* *Disabled*	Enable or Disable Platform Control Hub (PCH) Thermal Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
Memory Device	*Enabled* *Disabled*	Enable or Disable Memory Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ...	This value controls the temperature of the ACPI Critical Thermal Trip Point.

	103 °C *119 °C*	
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
Fan1 Device	*Disabled* *Enabled*	Enable the Fan1 device. There is no Fan1 or System Fan connected to this system.
Fan2 Device	*Enabled* *Disabled*	Enable the Fan2 or CPU Fan device.
Ambient Device	*Enabled* *Disabled*	Enable or Disable the Ambient Thermal Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
Skin Device	*Enabled* *Disabled*	Enable or Disable the Skin Thermal Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.

	23 °C ... *79 °C* *119 °C*	
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
Exhaust Fan Device	*Enabled* *Disabled*	Enable or Disable the Exhaust Fan Thermal Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *71 °C* *119 °C*	This value controls the temperature of the ACPI Active Thermal Trip Point.
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
VR Device	*Enabled* *Disabled*	Enable or Disable the VR Thermal Device.
Active Thermal Trip Point	*Disabled* *15 °C* *23 °C* ...	This value controls the temperature of the ACPI Active Thermal Trip Point.

	71 °C *119 °C*	
Passive Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *79 °C* *119 °C*	This value controls the temperature of the ACPI Passive Thermal Trip Point.
Critical Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *103 °C* *119 °C*	This value controls the temperature of the ACPI Critical Thermal Trip Point.
Hot Thermal Trip Point	*Disabled* *15 °C* *23 °C* ... *95 °C* *119 °C*	This value controls the temperature of the ACPI Hot Thermal Trip Point.
Display participant	*Disabled* *Enabled*	Enable or Disable the Display participant.
Power Participant	*Disabled* *Enabled*	Enable or Disable the Power participant.
▶Policy Configuration		Policy Configuration Options Menu

Fig. 2.2.20.1.e Policy Configuration (Screen 5 of 5)

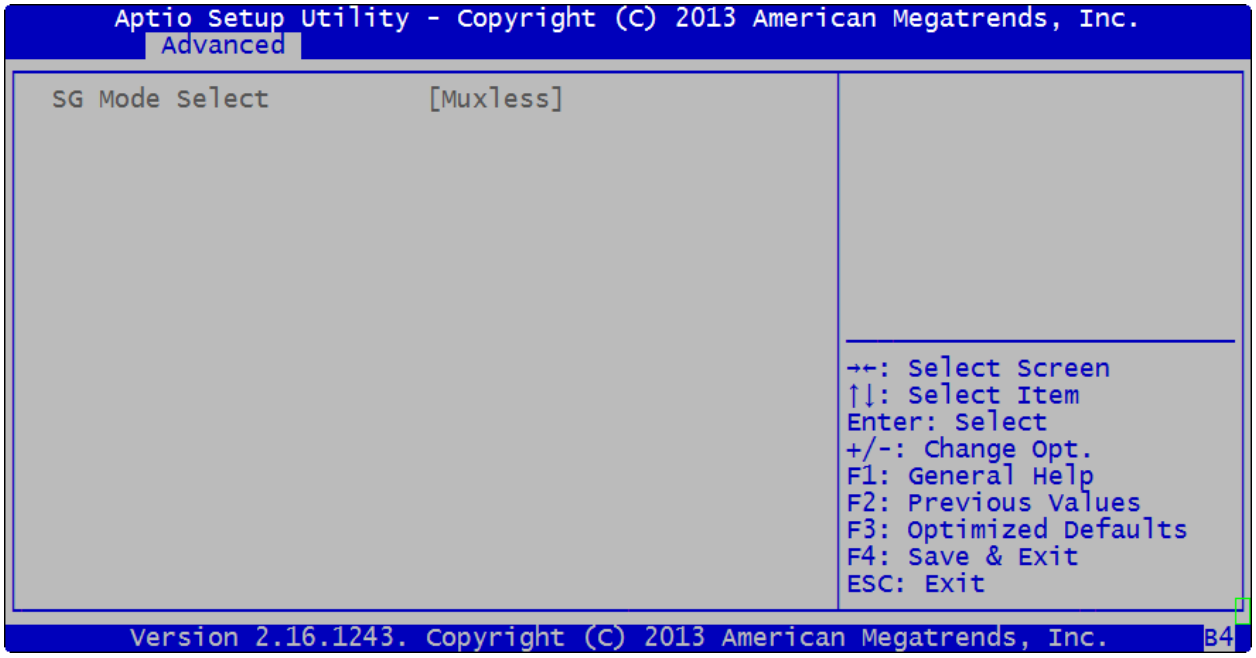


This option allows the user to view and configure Serial Port 1.

Feature	Options	Description
Active Policy	*Enabled* *Disabled*	Enable or Disable Active Policy.
Passive Policy	*Enabled* *Disabled*	Enable or Disable Passive Policy.
TRT Revision	*Traditional* *Priority*	Select the TRT influence.
Critical Policy	*Enabled* *Disabled*	Enable or Disable Critical Policy.
Cooling Mode Policy	*Enabled* *Disabled*	Enable or Disable Cooling Mode Policy.

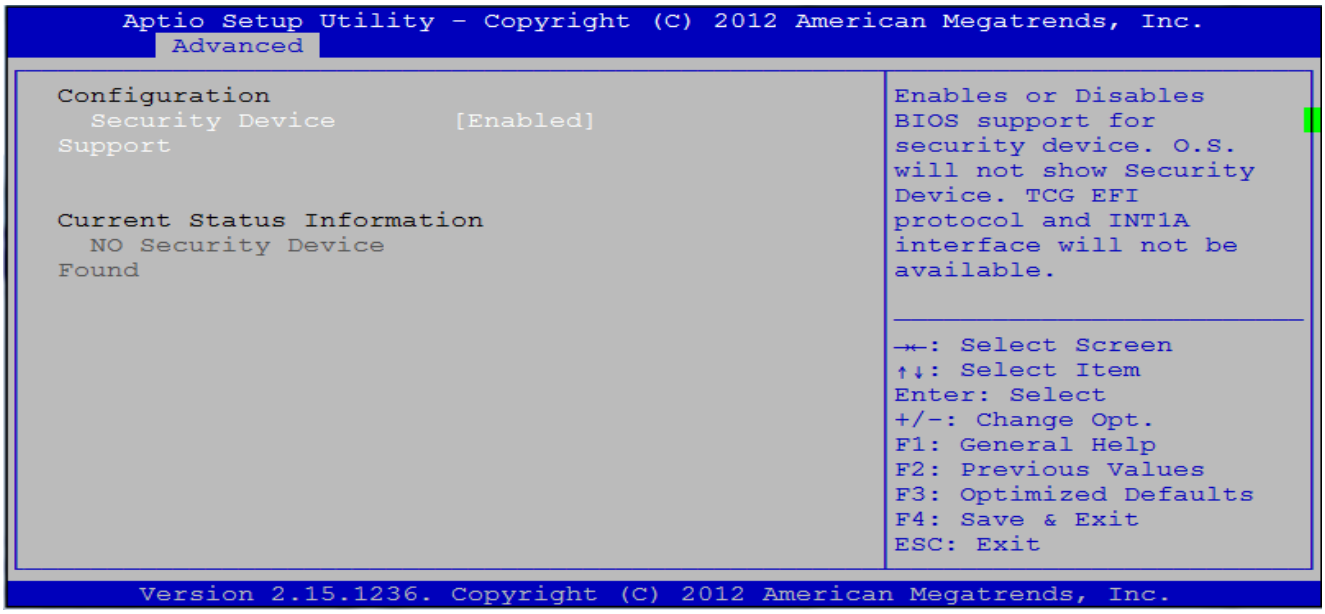
2.2.21 Switchable Graphics

Fig. 2.2.21.a Switchable Graphics



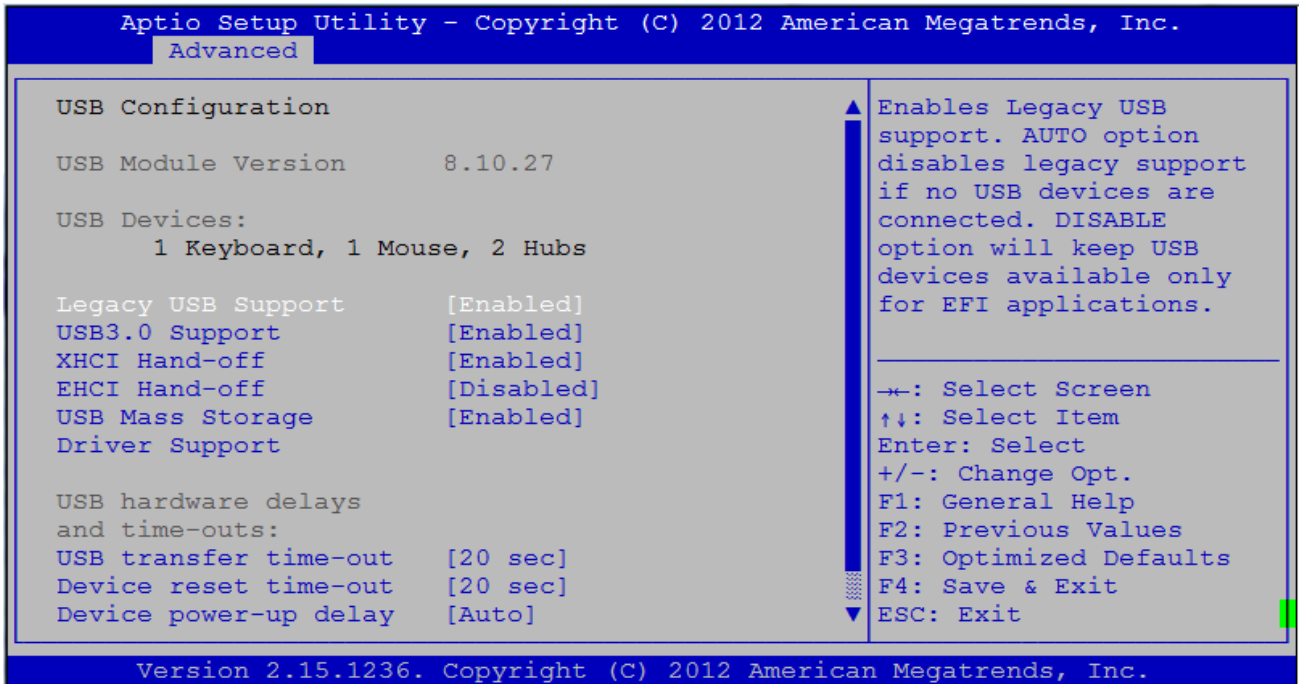
2.2.22 Trusted Computing

Fig. 2.2.22.a Trusted Computing



2.2.23 USB Configuration

Fig. 2.2.23.a USB Configuration



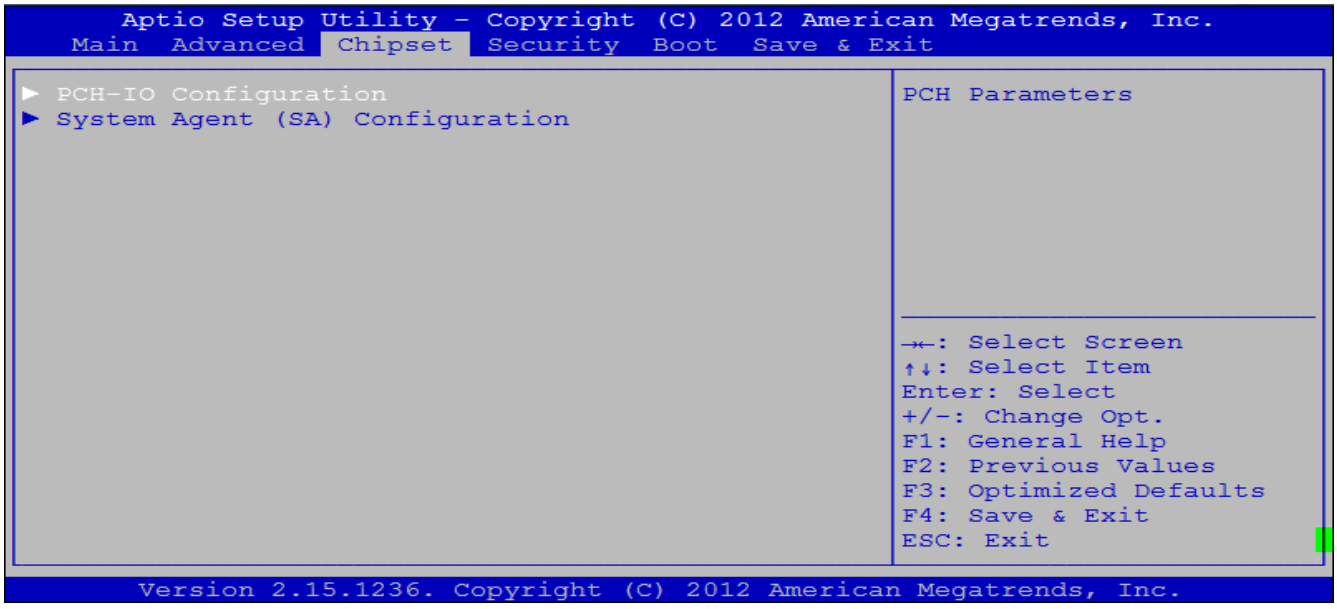
This option allows the user to view and change the USB Configuration.

Feature	Options	Description
Legacy USB Support	*Enabled* *Disabled* *Auto*	Allows selection of legacy support for USB devices. Enables Legacy USB support. Keep USB devices available only for EFI application. Disables legacy support if no USB devices are connected.
USB 3.0 Support	*Enabled* *Disabled*	Enables USB3,0 Extensible Host Controller Interface (xHCI) controller support.
XHCI Hand-off	*Enabled* *Disabled*	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
EHCI Hand-off	*Enabled* *Disabled*	This is a workaround for OSes without EHCI hand-off support. The XHCI ownership change should be claimed by EHCI driver.
USB Mass Storage Driver Support	*Enabled* *Disabled*	Enables or Disables USB Mass storage Driver Support.
USB transfer time-out	*1 sec* *5 sec* *10 sec* *20 sec*	The time-out value for control, bulk, and interrupt transfers.
Device reset time-out	*10 sec* *20 sec* *30 sec* *40 sec*	Sets USB mass storage devices start unit command time-out.
Device power-up delay	*Auto* *Manual*	Maximum time the device will take before it reports itself to the Host controller. 'Auto' uses default values; for a Root port it is 100ms, for a Hub port the delay is taken from Hub descriptor.

2.3 Chipset Menu, Configuration, and Settings

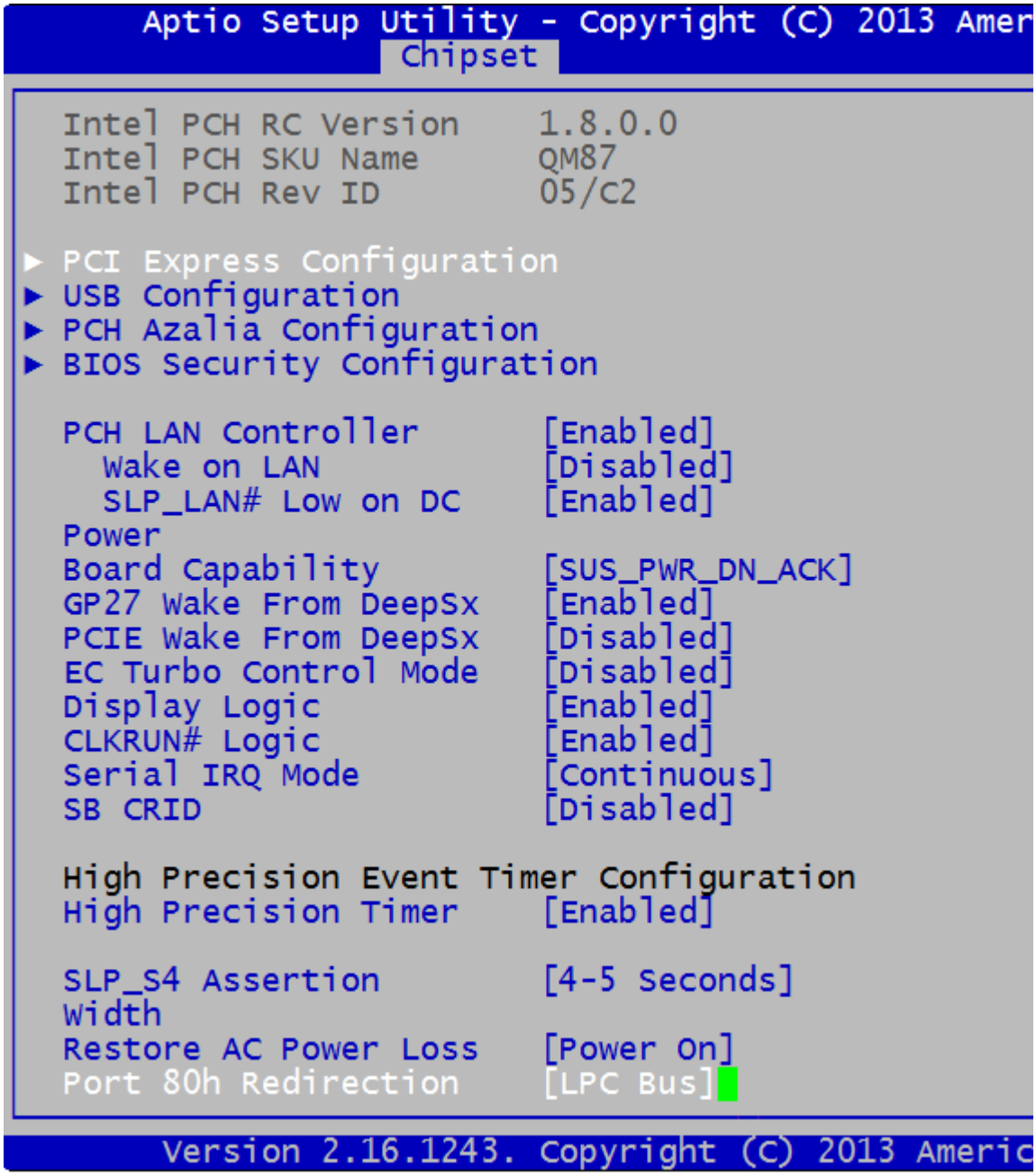
2.3 Chipset Menu

Fig. 2.3.a Chipset Menu



2.3.1 PCH I/O Configuration

Fig. 2.3.1,a PCH I/O Configuration



This option allows the user to view or edit the PCH I/O Configuration.

Feature	Options	Description
▶PCI Express Configuration		PCI Express Configuration Menu Settings
▶USB Configuration		USB Configuration Menu Settings
▶PCH Azalia Configuration		PCH Azalia Configuration Menu Settings
▶Bios Security Configuration		Bios Security Configuration Menu Settings
PCH Lan Controller	*Enabled* *Disabled*	Enables or Disables onboard NIC
Wake on LAN	*Disabled**Enabled*	Enables or Disables integrated LAN to wake the system. The Wake on LAN cannot be disabled if ME is on at Sx state.
SLP_LAN# Low on DC Power	*Enabled* *Disabled*	Enables or Disables SLP_LAN# Low on DC Power.
Board Capability	*SUS_PWR_DN_ACK* *DeepSx*	Send Disabled to PCH Show DeepSx Policies Note: Our Boards currently do not support DeepSx.
GP27 Wake from DeepSx	*Enabled* *Disabled*	Enables or Disables Wake from DeepSx by the assertion of GP27 pin. Note: Our Boards currently do not support DeepSx.
PCIE Wake from DeepSx	*Disabled* *Enabled*	Enables or Disables Wake from DeepSx by the assertion of PCIE. Note: Our Boards currently do not support DeepSx.
EC Turbo Control Mode	*Disabled* *Enabled*	Enables or Disables Embedded Controller (EC) Turbo Control Mode.
Display Logic	*Enabled* *Disabled*	Enables or Disables the Platform Controller Hub (PCH) Display Logic.
CLKRUN# Logic	*Enabled* *Disabled*	Enables or Disables the CLKRUN# lgic to stop the PCI clocks
Serial IRQ Mode	*Quiet* *Continuous*	Configure Serial IRQ Mode
SB CRID	*Disabled* *Enabled*	When disabled, the Revision ID (RID) register reports Stepping Revision ID (SRID). When enabled, the RID register reports the Compatible Revision ID.
High Precision Event Timer Configuration		
High Precision Timer	*Enabled* *Disabled*	Enables or Disables the High Precision Event Timer.
SLP_S4 Assertion Width	*Disabled* *1-2 Seconds* *2-3 Seconds* *3-4 Seconds* *4-5 Seconds*	Select a minimum assertion width of the SLP_S4# signal.
Restore AC Power Loss	*Power Off* *Power On* *Last State*	Selects AC power state when power is re-applied after a power failure.
Port 80h Redirection	*LPC Bus* *PCIE Bus*	Controls where the Port 80h Cycles are sent.

2.3.1.1 PCI Express Configuration

Fig. 2.3.1.1.a PCI Express Configuration

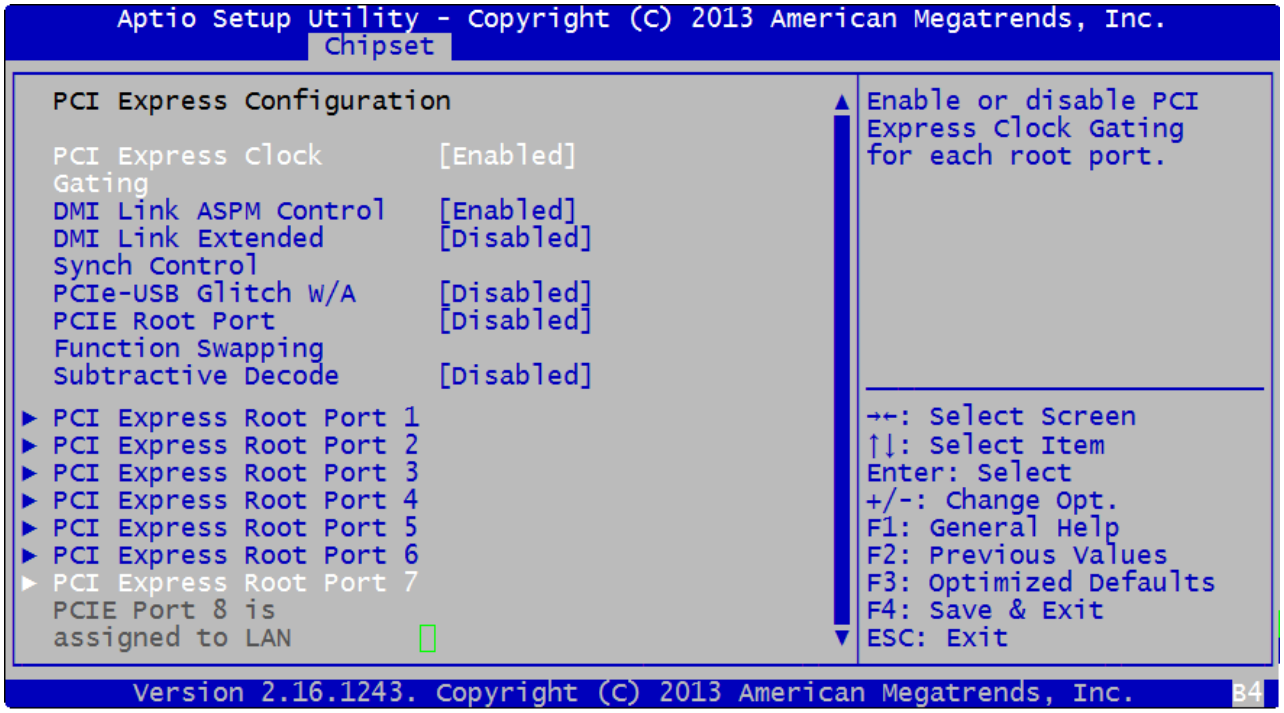
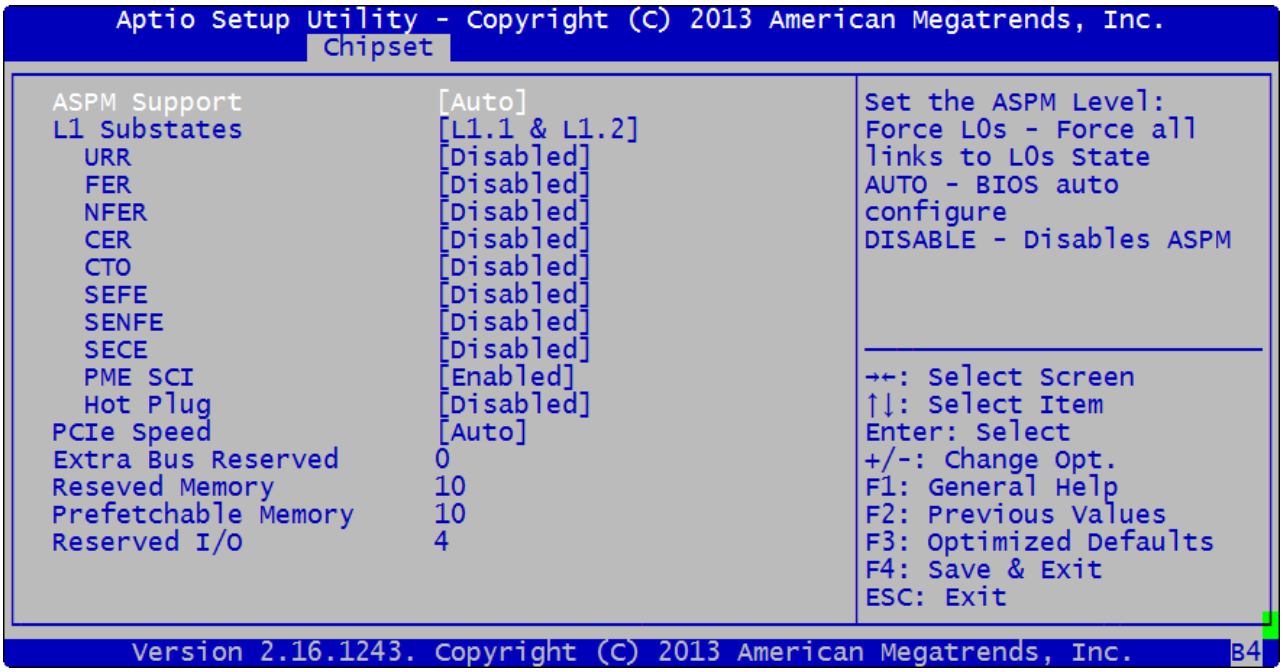
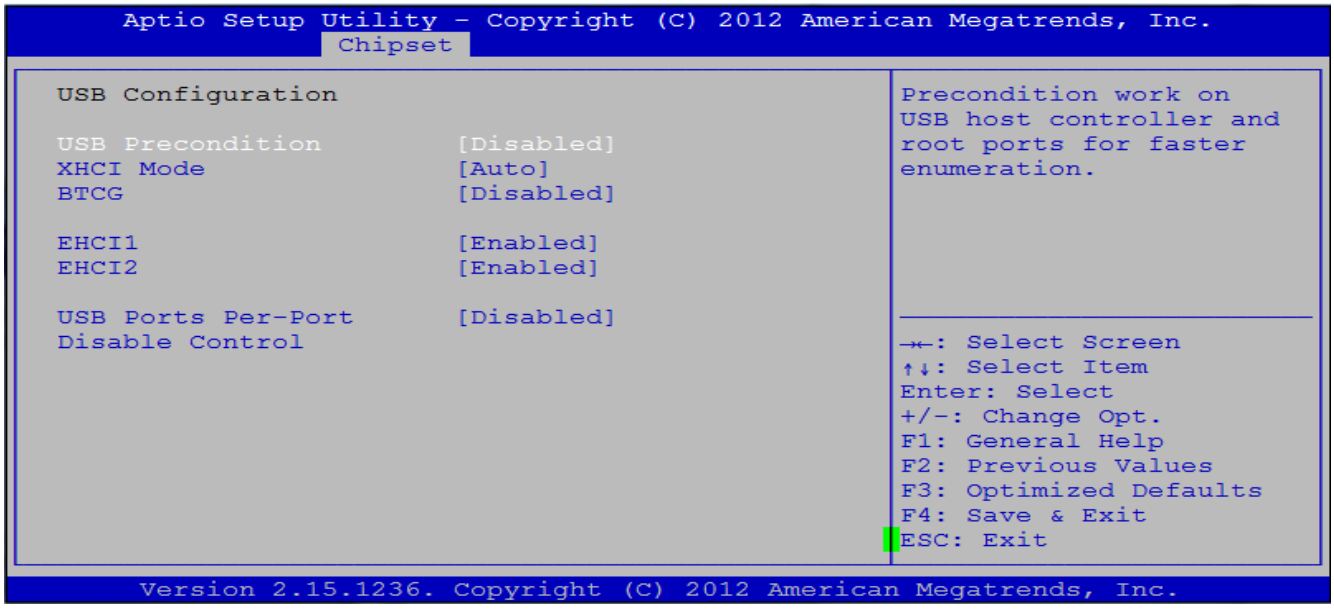


Fig. 2.3.1.1.b PCI Express Root Port (1 to 7)



2.3.1.2 USB Configuration

Fig. 2.3.1.2.a USB Configuration



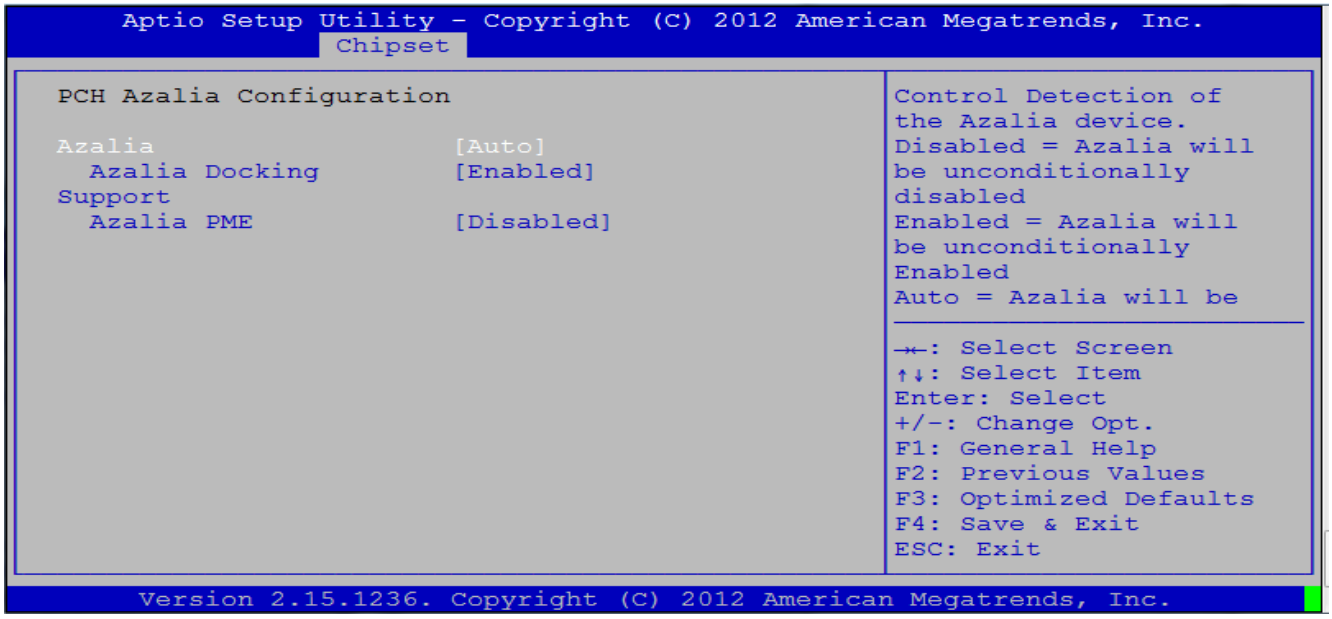
This option allows the user to view and change the USB Configuration.

Feature	Options	Description
USB Precondition	*Enabled* *Disabled*	Precondition work on USB host controller and root ports for faster enumeration.
XHCI Mode		The Extensible Host Controller Interface (xHCI) is the USB 3.0 controller. The different modes of operation are:
	Auto	BIOS routes the sharable ports to EHCI controller. Then it uses ACPI protocols to provide an option to enable the xHCI controller and reroute the sharable ports. Note: This is the recommended mode when BIOS does NOT have xHCI pre-boot support.
	Smart Auto	This mode is available only when the BIOS supports the xHCI controller in the pre-boot environment. This mode is similar to Auto, but it adds the capability to route the ports to xHCI or EHCI according to setting used in previous boots (for non-G3 boot) in the pre-boot environment. This allows the use of USB 3.0 devices prior to OS boot. xHCI controller enabling and rerouting should follow the steps in Auto, when previous boot routs ports to EHCI. Note: This is the recommended mode when BIOS has xHCI pre-boot support.
	Enabled	All shared ports are eventually routed to the xHCI controller during the BIOS boot process. If BIOS does not have pre-boot support for the xHCI controller, it should initially route the sharable ports to the EHCI controller and then prior to OS boot it should route the ports to xHCI controller. Note: OS has to provide support for the xHCI controller in this mode. If the OS does not provide support, all sharable ports won't work.

	Disabled *Manual*	The USB 3.0 ports are routed to the EHCI controller and the xHCI controller is turned off. All USB 3.0 devices function as High Speed devices regardless of xHCI software support or availability. Allows you to determine whether to rout the USB 3.0 ports to the xHCI or EHCI controller before booting to OS, and also provides you with options to manually rout each USB 3.0/2.0 port to xHCI or EHCI.
BTCG	*Enabled* *Disabled*	Allows you to enable or disable USB related trunk clock gating (BTCG).
EHCI1	*Enabled* *Disabled*	The USB Enhanced Controller Interface (EHCI) is the USB2.0 Controller. EHCI #1 controls Port 0 to 7.
EHC2	*Enabled* *Disabled*	The USB Enhanced Controller Interface (EHCI) is the USB2.0 Controller. EHCI #1 controls Port 8 to 13.
USB Ports Per-Port Disable Control	*Enabled* *Disabled*	This option allows enabling and disabling of the individual USB ports 0 to 14. Consult your specific hardware on what USB ports are available for your system.

2.3.1.3 PCH Azalia Configuration

Fig. 2.3.1.3.a PCH Azalia Configuration

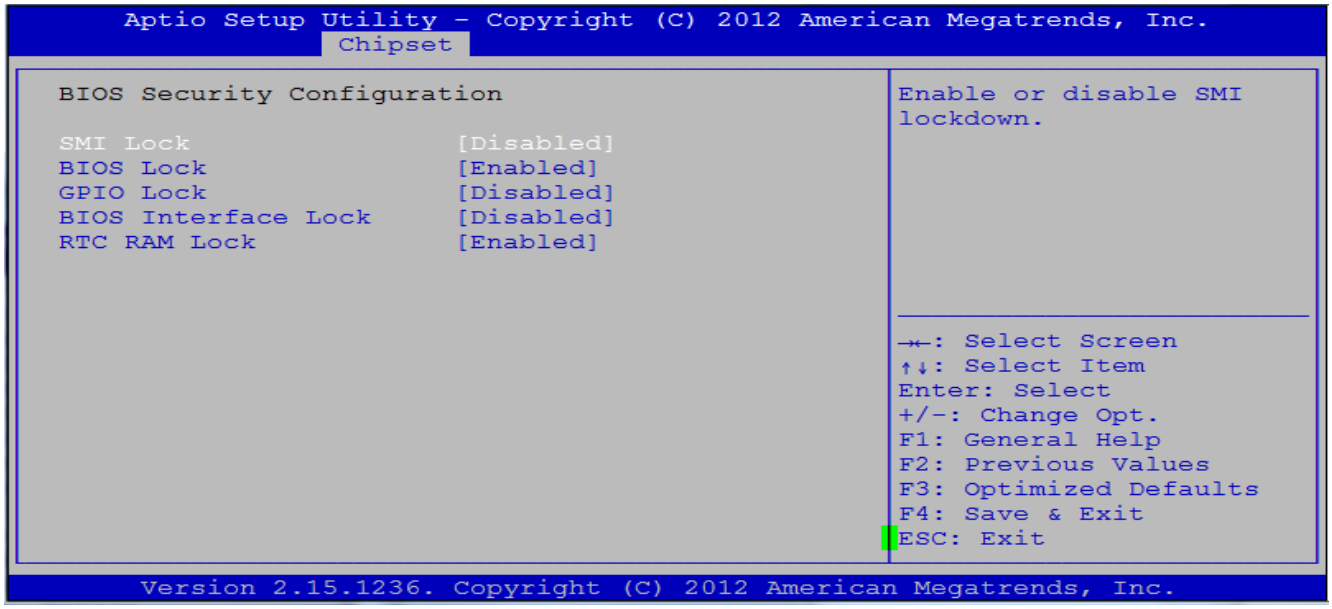


This option allows the user to view and change the Azalia Configuration. Azalia is the on-board audio controller.

Feature	Options	Description
Azalia	*Disabled* *Enabled* *Auto*	This item controls detection of the Azalia device. Azalia will be unconditionally disabled. Azalia will be unconditionally Enabled. Azalia will be enabled if present, disabled otherwise.
Azalia Docking Support	*Enabled* *Disabled*	Enable or disable Azalia Docking Support of Audio Controller.
Azalia PME	*Disabled* *Enabled*	Enable or disable Power Management Capability of Audio Controller.

2.3.1.4 BIOS Security Configuration

Fig. 2.3.1.4.a BIOS Security Configuration



2.3.2 System Agent Configuration

Fig. 2.3.2.a System Agent Configuration (Screen 1 of 2)

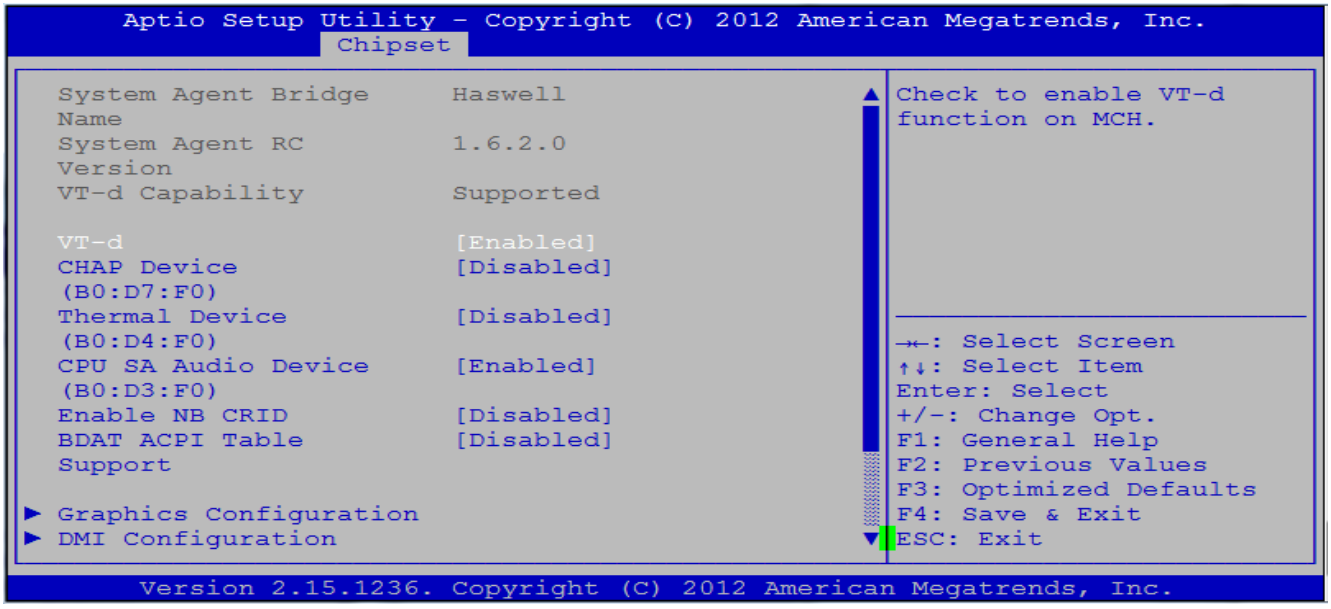
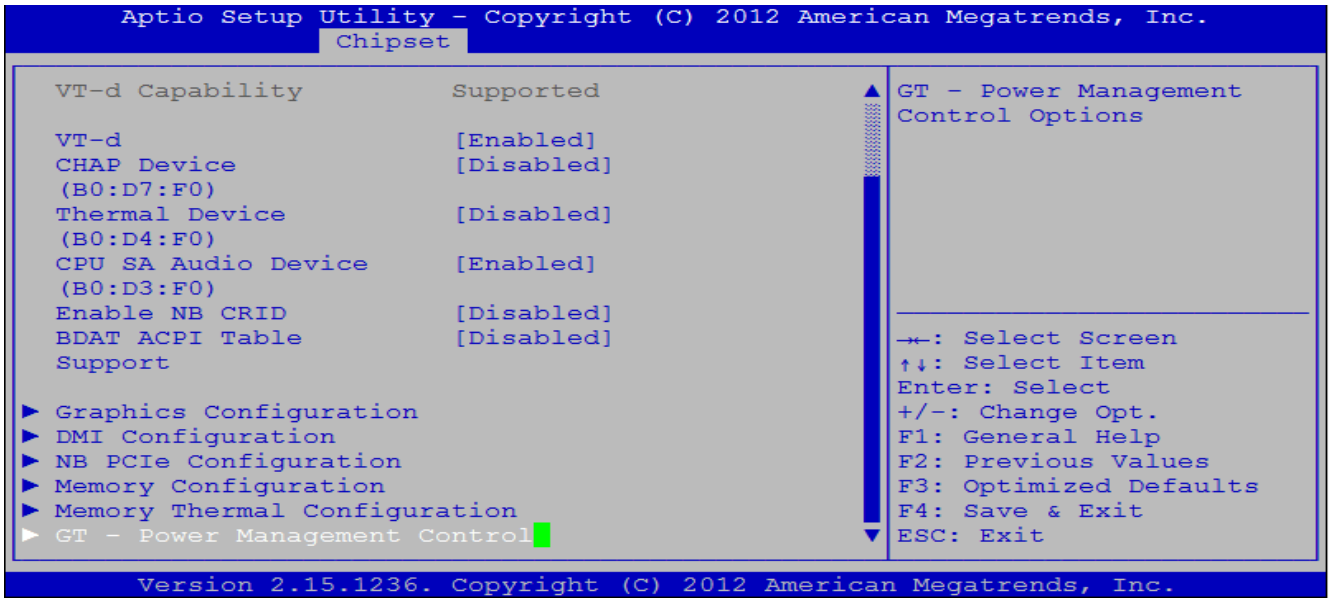
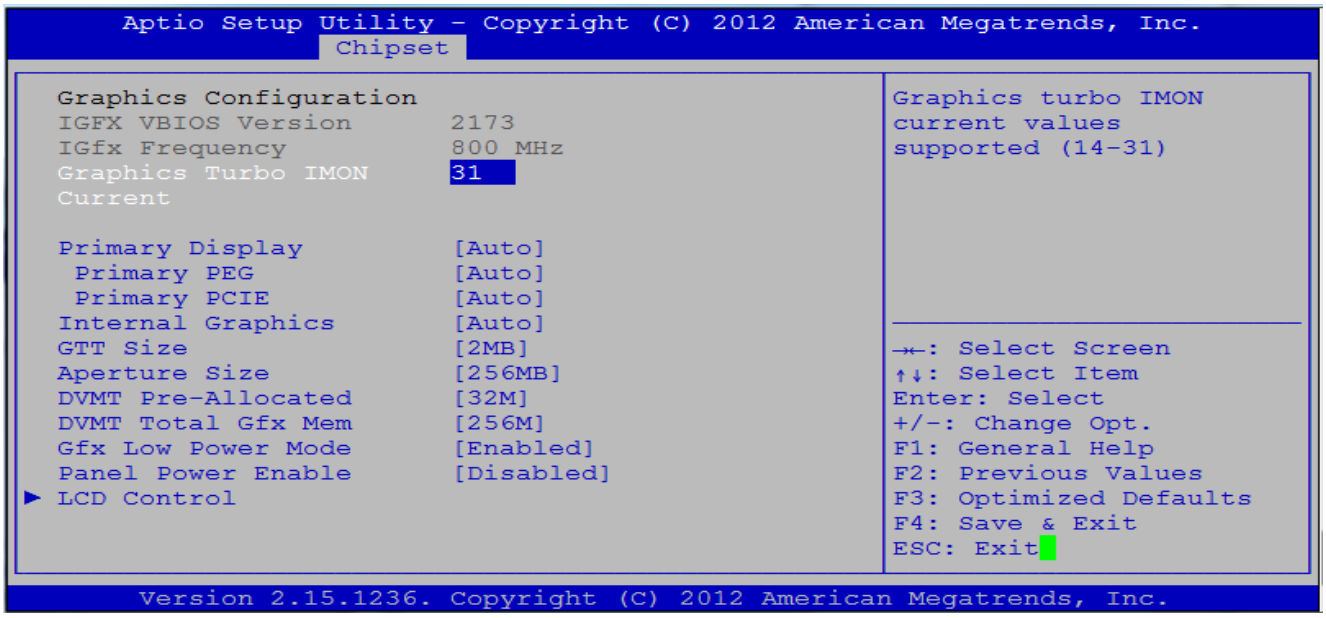


Fig. 2.3.2.b System Agent Configuration (Screen 2 of 2)



2.3.2.1 Graphics Configuration

Fig. 2.3.2.1.a Graphics Configuration

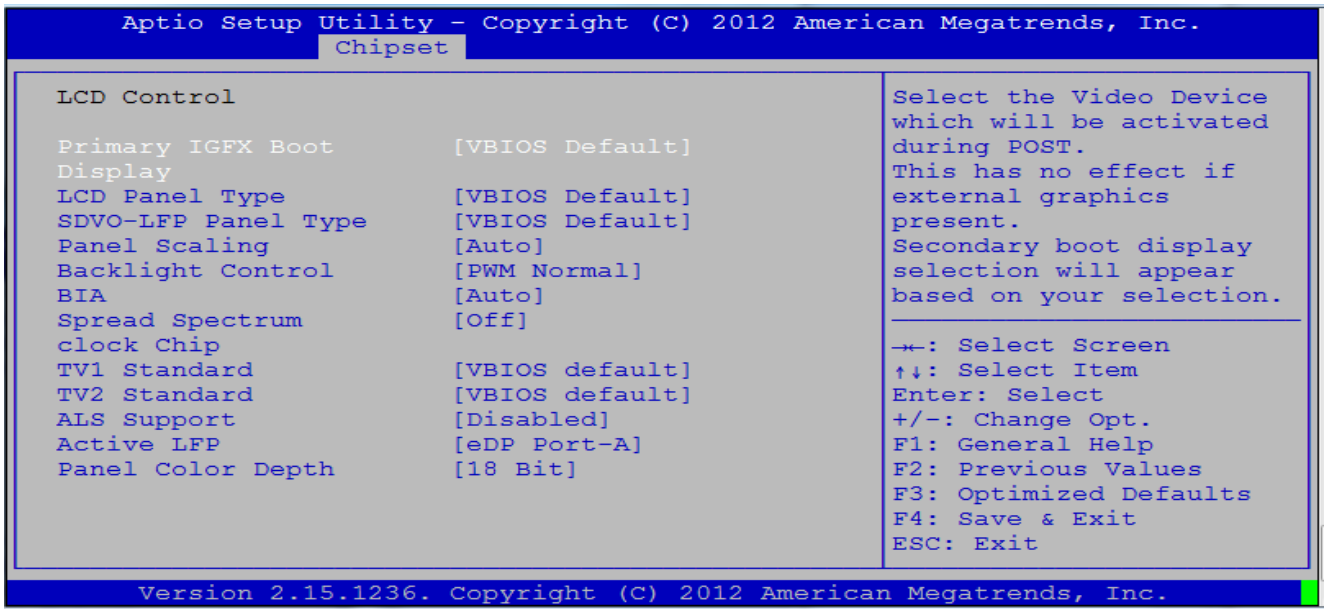


This option allows the user to view and configure the Graphics Configuration parameters

Feature	Options	Description
IGFX VBIOS Version		Displays the Intel Internal Graphics (IGFx) Video BIOS Version.
IGFX Frequency	*Enabled* *Disabled*	Displays the Internal Graphics (IGFx) card frequency in MHz.
Graphics Turbo IMON Current	*14-31*	Graphics turbo IMON current values supported (14-31)
Primary Display	*Auto* *IGFX* *PEG* *PCI* *SG*	Select which Graphics device should be the Primary Display. Auto Selection Internal Graphics Card PEG Port Graphics Card PCI Graphics Card Switchable Graphics (Gfx)
Primary PEG	*Auto* *PEG11* *PEG12*	Select which PEG Graphics should be the Primary graphics card.
Primary PCIE	*Auto* *PCIE1-7*	Select which PCIe Graphics should be the Primary graphics card.
Internal Graphics	*Auto* *Disabled* *Enabled*	Keep the Internal Graphics Display (IGD) enabled based on the setup options.
GTT Size	*1 MB* *2 MB*	Select the GTT Size. Options are 1MB or 2MB.
Aperture Size	*128 MB* *256 MB* *512 MB*	Select the Aperture Size.
DVMT Pre-Allocated	*0M* *32M* *64M* *…* *512M*	Select Dynamic Video Memory Technology (DVMT) 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	*128M* *256M* *MAX*	Select Dynamic Video Memory Technology (DVMT) 5.0 Total Graphic Memory size used by the Internal Graphics Device.
Gfx Low Power Mode	*Enabled* *Disabled*	This option is applicable for SFF only.
Panel Power Enable	*Enabled* *Disabled*	This option allows enabling or disabling the forcing of the Panel Power in the BIOS.

2.3.2.1.1 LCD Control Configuration

Fig. 2.3.2.1.1.a LCD Control Configuration



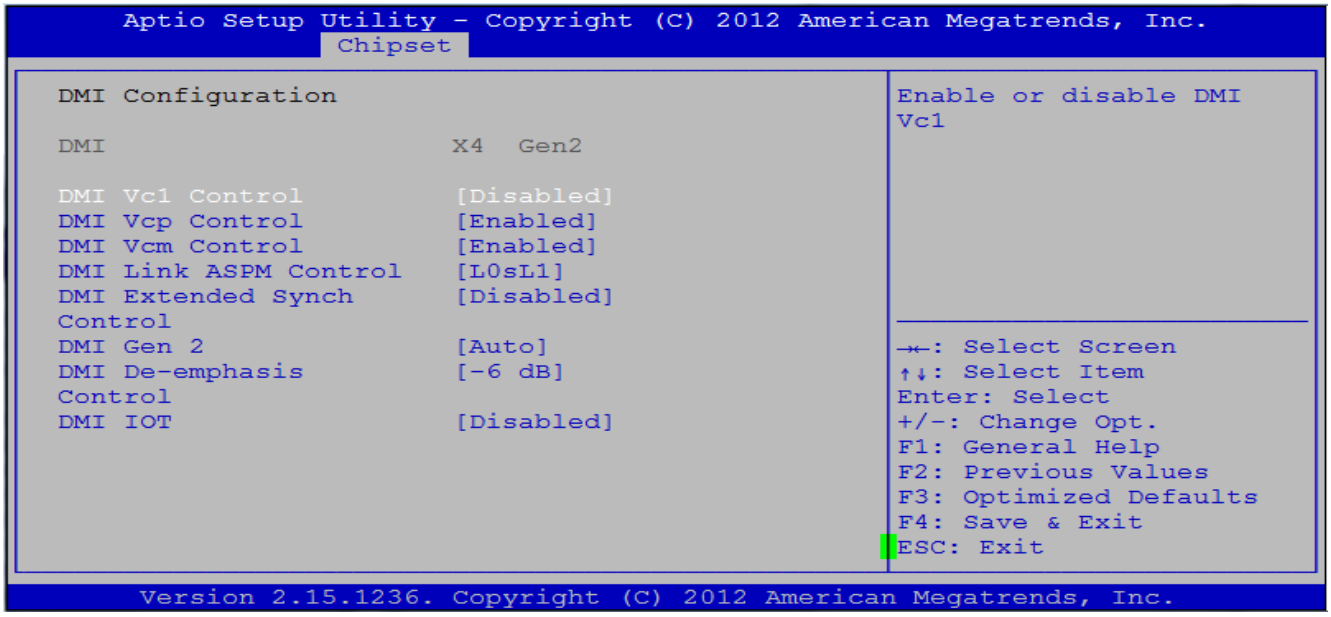
This option allows the user to view and configure the LCD Control parameters.

Features	Options	Description
Primacy IGFX Boot Display	*VBIOS Default* *CRT* *EFP* *LFP* *EFP3* *EFP2* *LFP2*	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.
LCD Panel Type	*VBIOS Default* *640x480* … *2048x1536*	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.
SDVO-LFP Panel Type	*VBIOS Default* *1024x768* *1280x1024* *1400x1050* *1600x1200*	Select the Serial Digital Video Out (SDVO) panel used by Internal Graphics Device by selecting the appropriate setup item.
Panel Scaling	*Auto* *Off* *Force Scaling*	Select the LCD panel scaling option used by the Internal Graphics Device.
Backlight Control	*PWM Inverted* *PWM Normal* *GMBus Inverted* *GMBus Normal*	Back Light Control Setting.

BIA	*Auto* *Disabled* *Level 1 to 5*	The Graphics and Memory Control Hub (GMCH) uses VBT Default. Disable Enable with Selected Aggressiveness Level.
Spread Spectrum Clock Chip	*Off* *Hardware* *Software*	Spread is disabled. Spread is controlled by chip. Spread is controlled by BIOS.
TV1 Standard	*VBIOS default* NTSC_ … PAL_ … SECAM_ … HDTV_ …	Select the ability to configure a TV Format.
TV2 Standard	*VBIOS default* NTSC_ … PAL_ … SECAM_ … HDTV_ …	Select the ability to configure a TV Minor Format.
ALS Support	*Enabled* *Disabled*	Ambient Light Sensor (ALS) Support is valid only for ACPI. Legacy = ALS Support through the IGD INT10 function, ACPI = ALS support through an ACPI ALS driver.
Active LFP	 No LVDS Int-LVDS SDVO LVD *eDP Port-A* eDP Port-D	Select the Active LFP Configuration. VBIOS does not enable LVDS. VBIOS enables LVDS driver by Integrated encoder. VBIOS enables LVDS driver by SDVO encoder. LFP Driven by Int-DisplayPort encoder from Port-A. LFP Driven by Int-DisplayPort encoder from Port-D.
Panel Color Depth	*18 Bit* *24 Bit*	Select the LFP Panel Color Depth.

2.3.2.2 DMI Configuration

Fig. 2.3.2.2.a DMI Configuration



2.3.2.3 NB PCIe Configuration

Fig. 2.3.2.3.a NB PCIe Configuration (Screen 1 of 3)

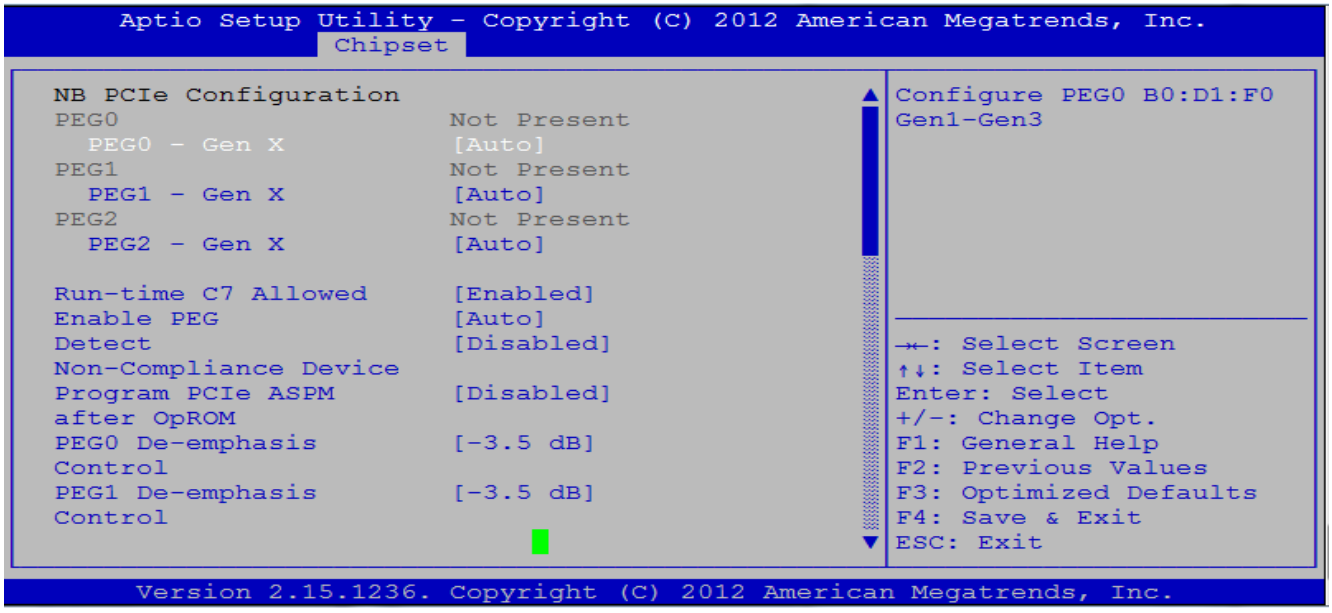


Fig. 2.3.2.3.b NB PCIe Configuration (Screen 2 of 3)

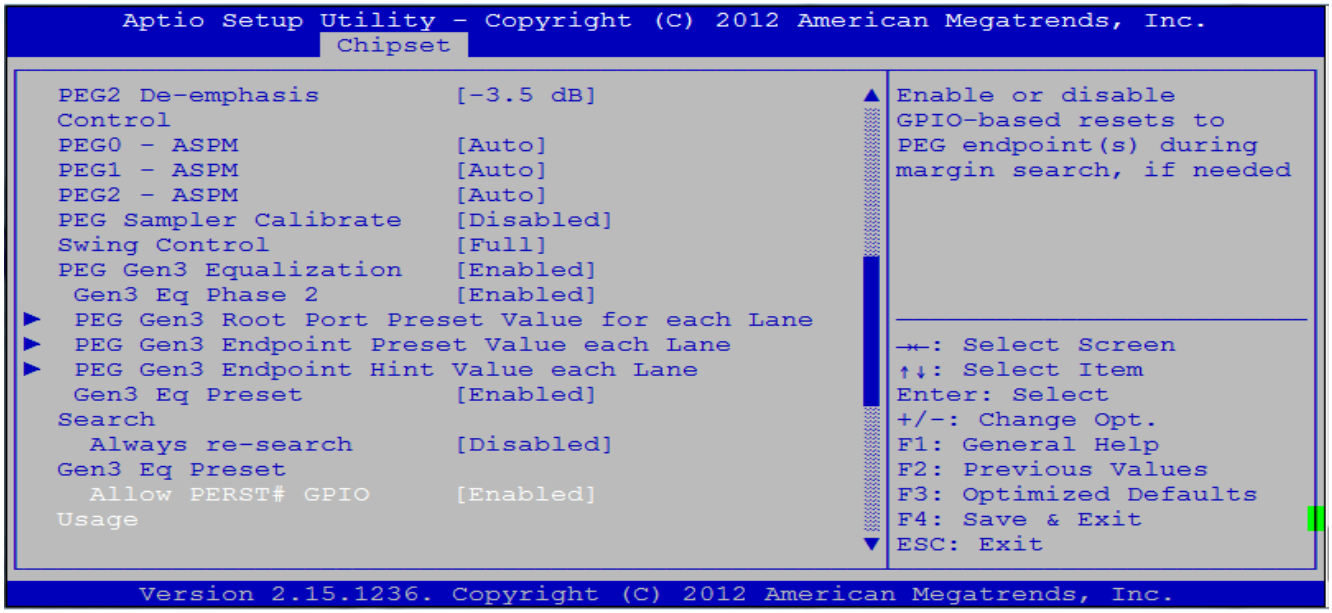
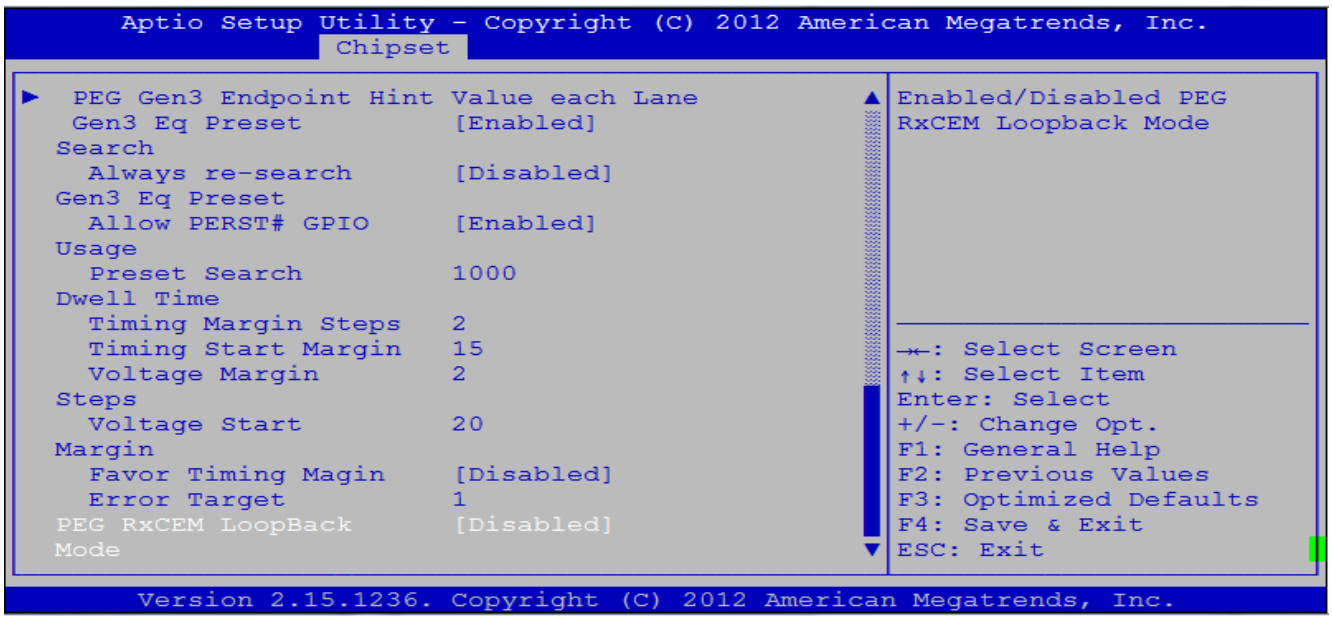


Fig. 2.3.2.3.c NB PCIe Configuration (Screen 3 of 3)



2.3.2.3.1 PEG Gen3 Root Port Preset Value

Fig. 2.3.2.3.1.a PEG Gen3 Root Port Preset Value (Screen 1 of 2)

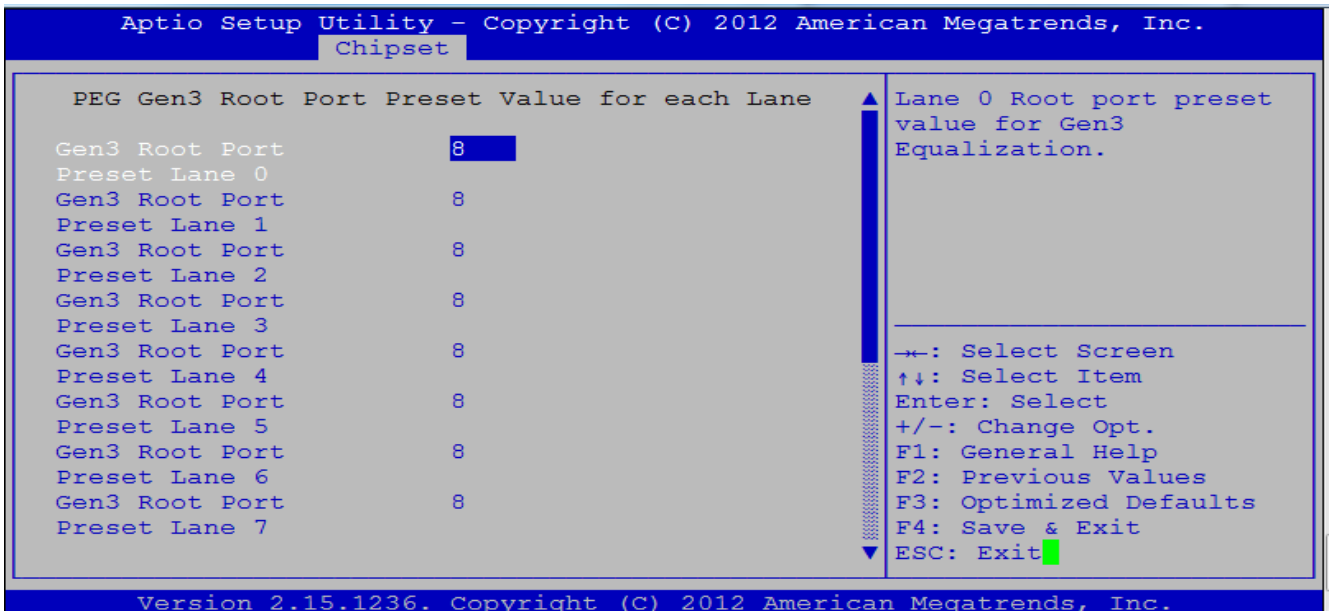
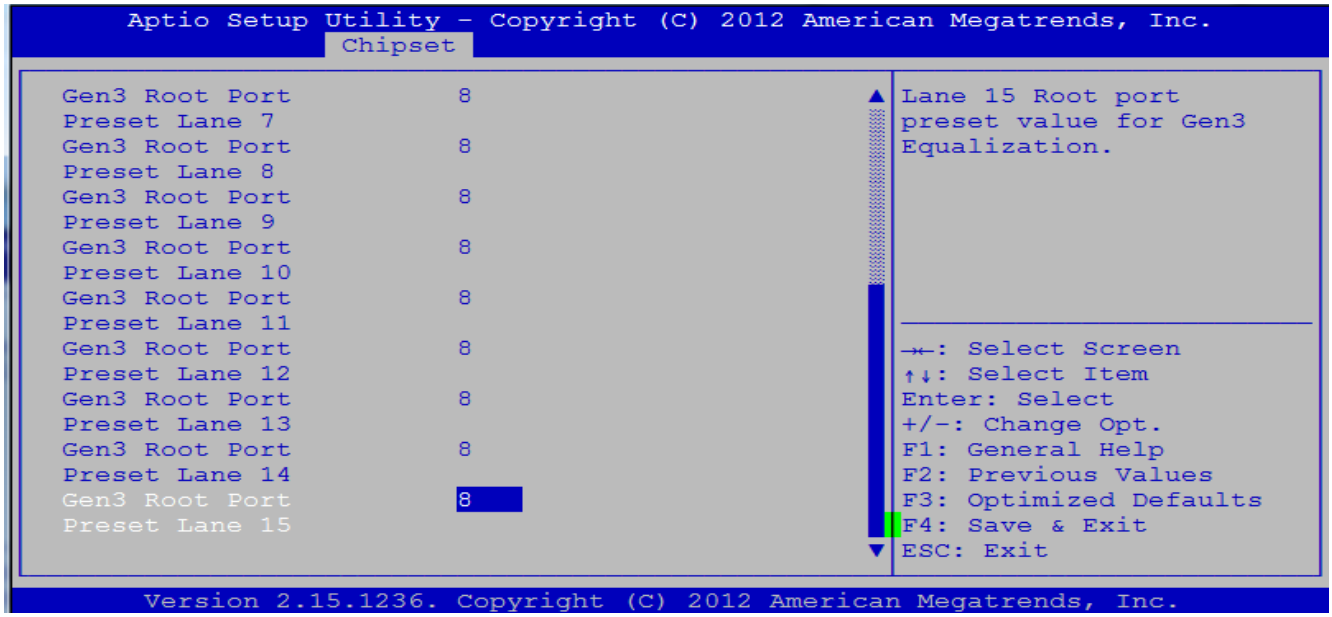
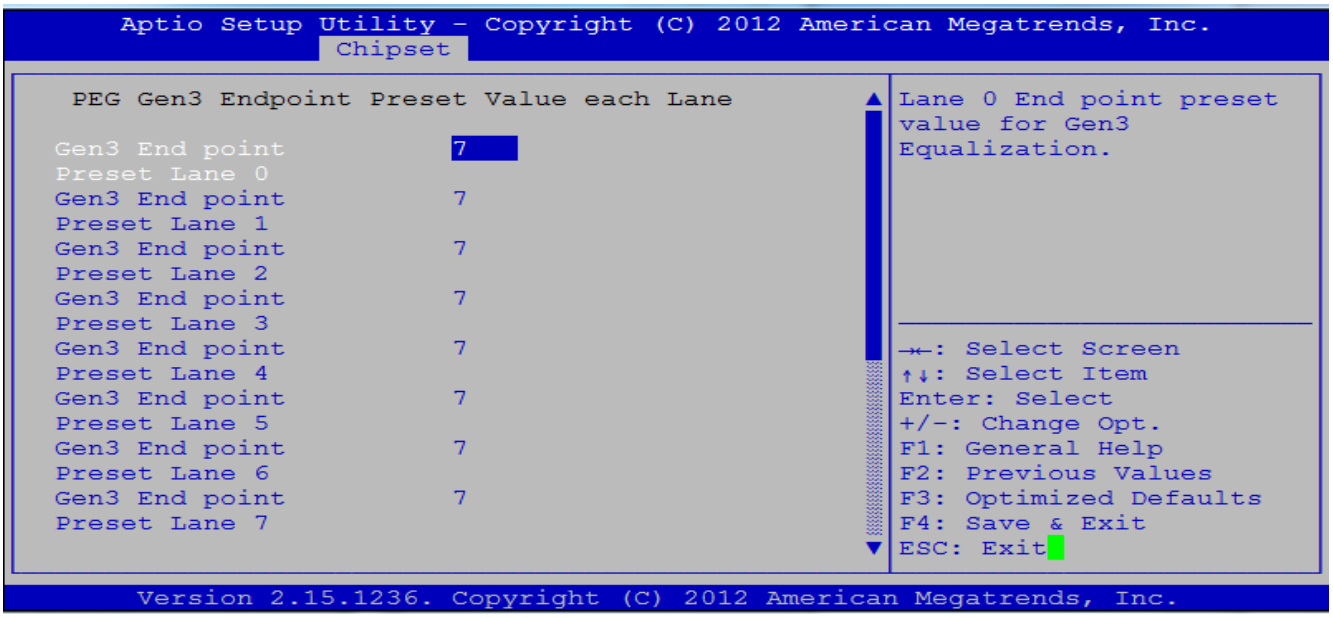


Fig. 2.3.2.3.1.b PEG Gen3 Root Port Preset Value (Screen 2 of 2)



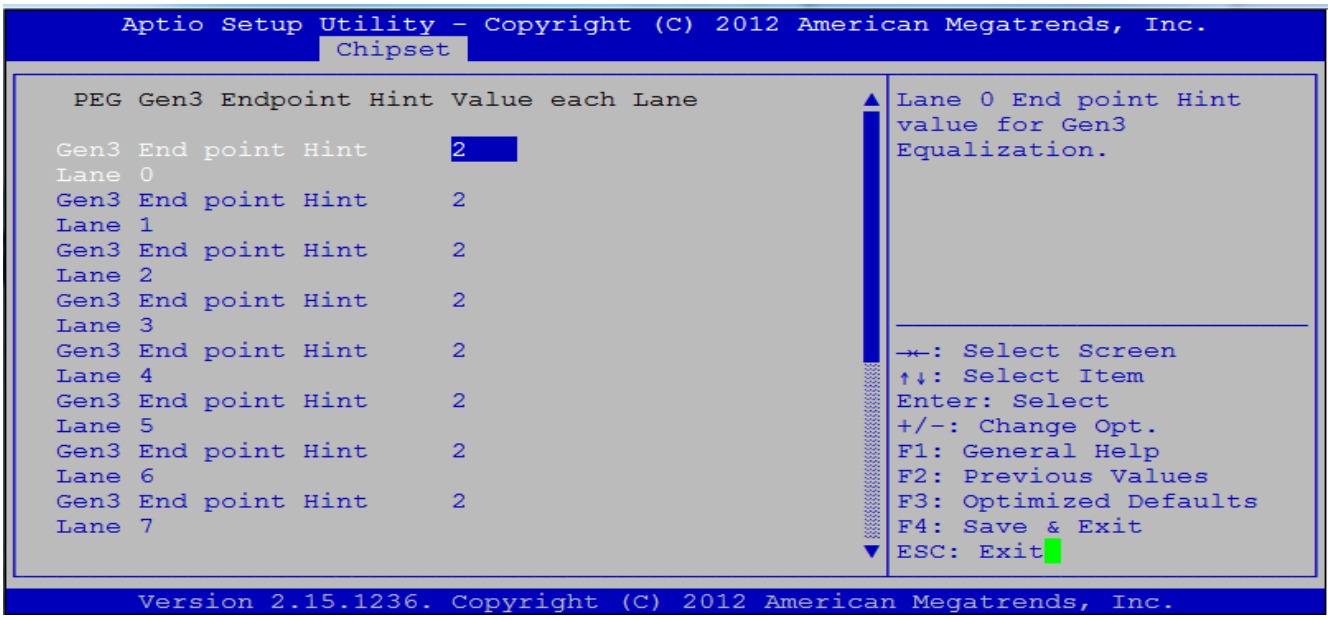
2.3.2.3.2 PEG Gen3 Endpoint Preset Value

Fig. 2.3.2.3.2.a PEG Gen3 Endpoint Preset Value



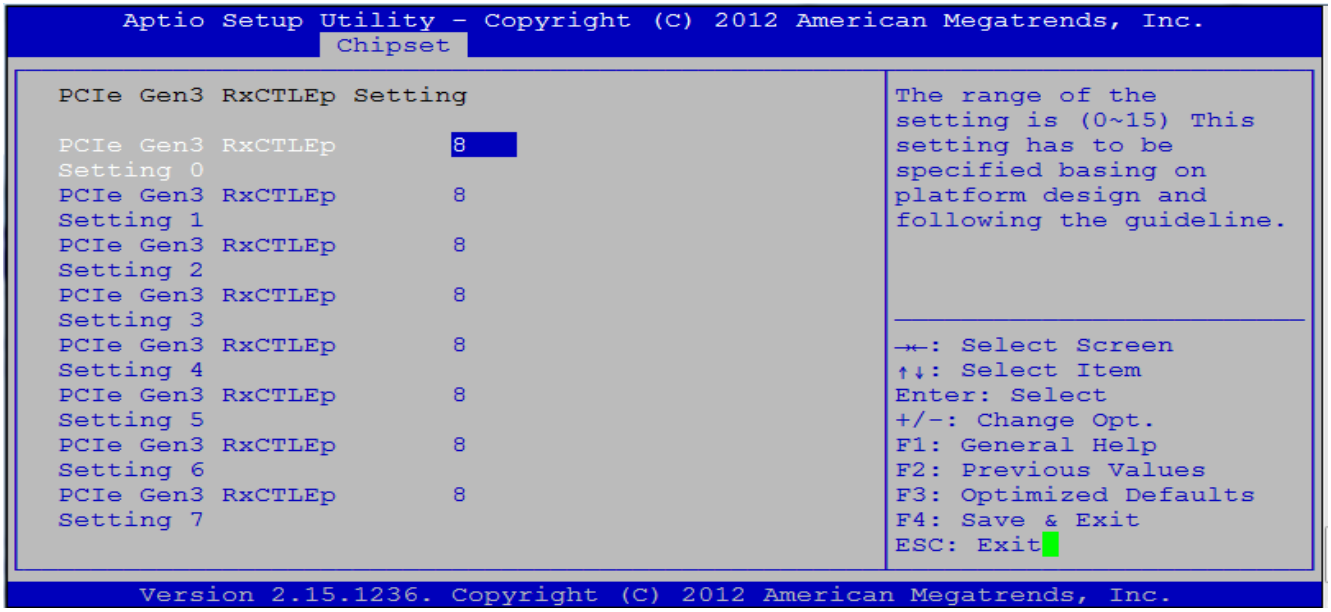
2.3.2.3.3 PEG Gen3 Endpoint Hint Value

Fig. 2.3.2.3.3.a PEG Gen3 Endpoint Hint Value



2.3.2.3.4 PCIe Gen3 RxCTLEp Setting

Fig. 2.3.2.3.4.a PCIe Gen3 RxCTLEp Setting



2.3.2.4 Memory Configuration

Fig. 2.3.2.4.a Memory Configuration (Screen 1 of 3)

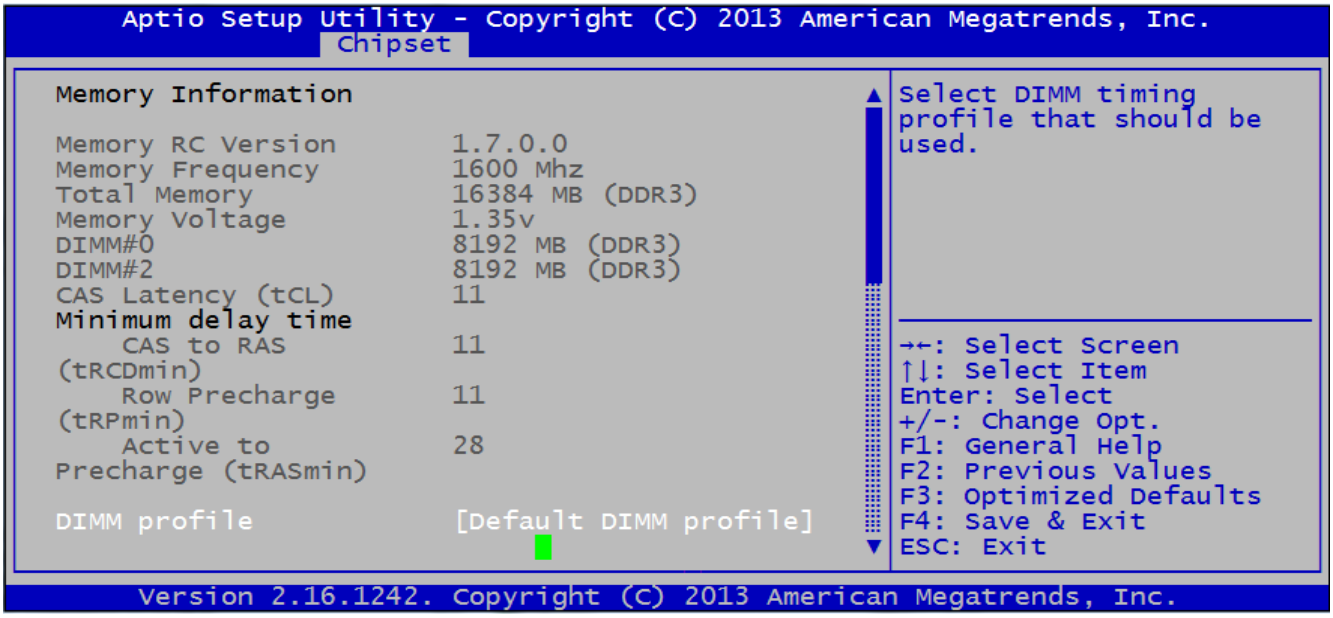


Fig. 2.3.2.4.b Memory Configuration (Screen 2 of 3)

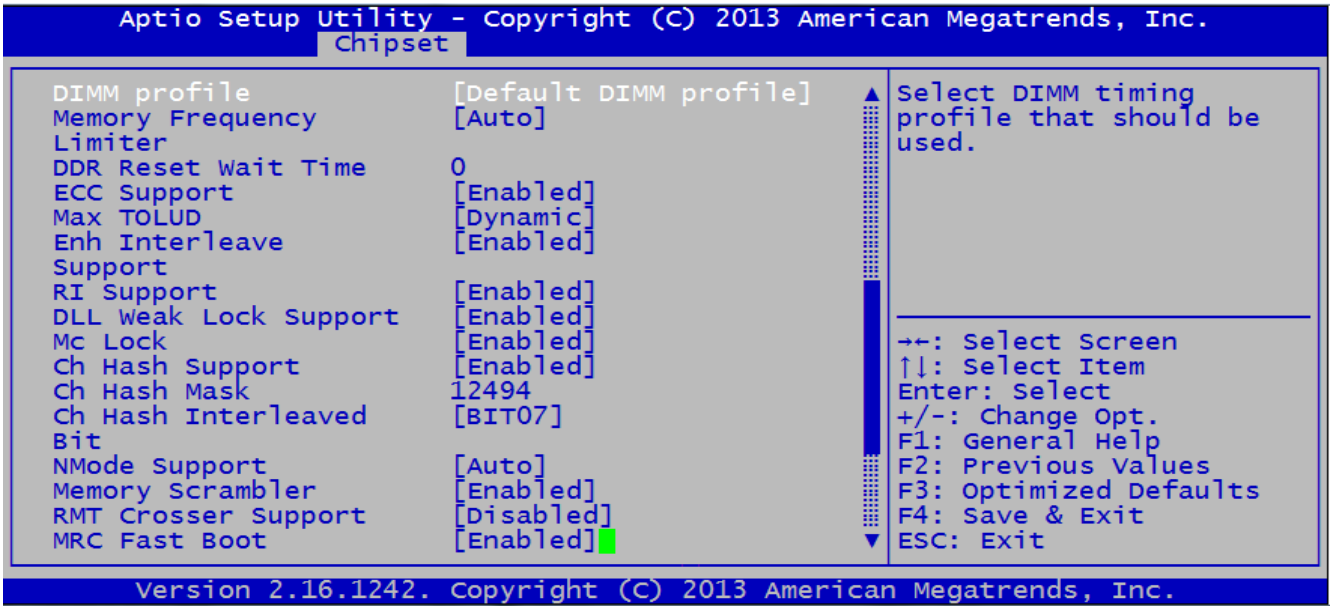
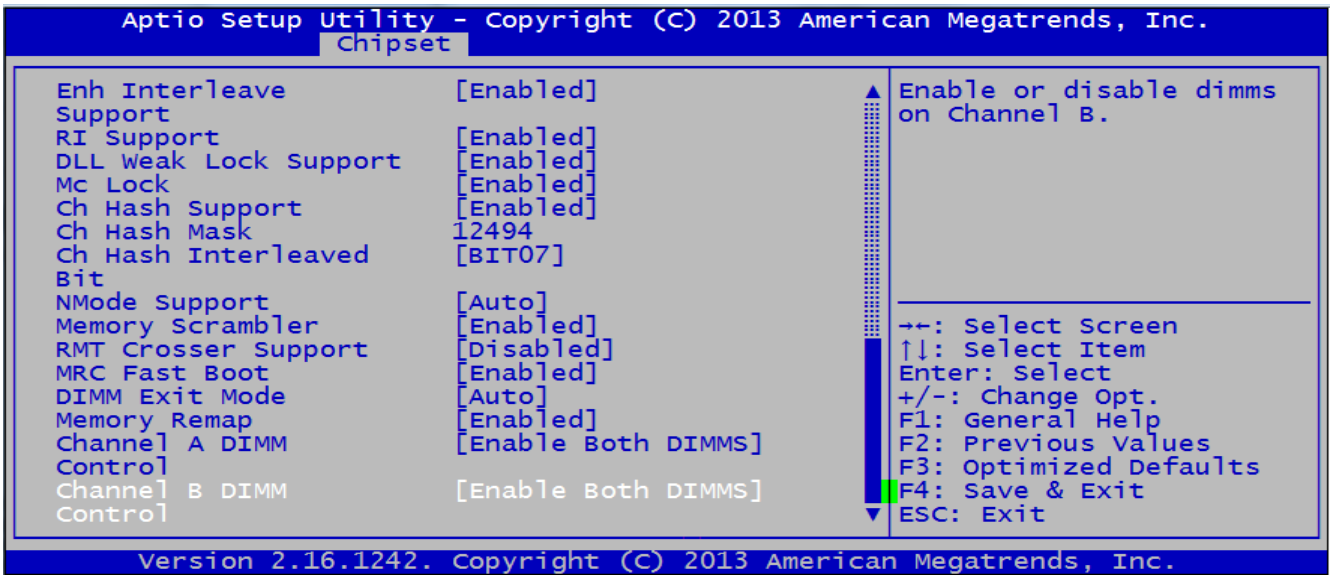
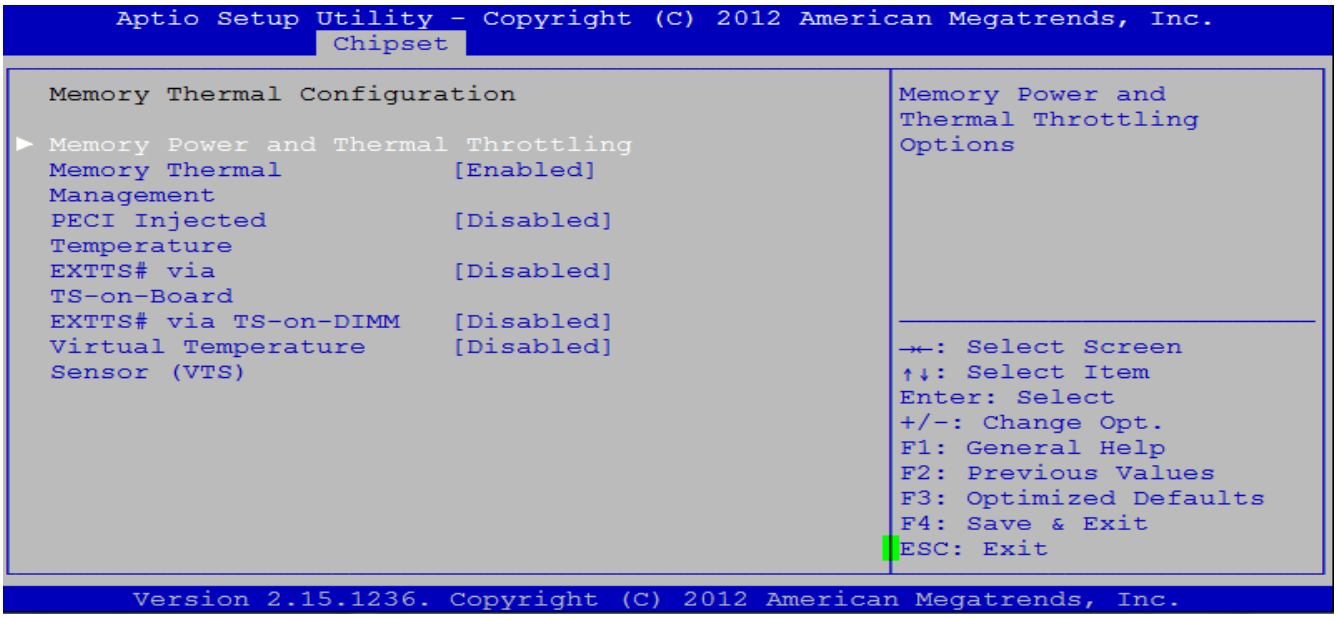


Fig. 2.3.2.4.c Memory Configuration (Screen 3 of 3)



2.3.2.5 Memory Thermal Configuration

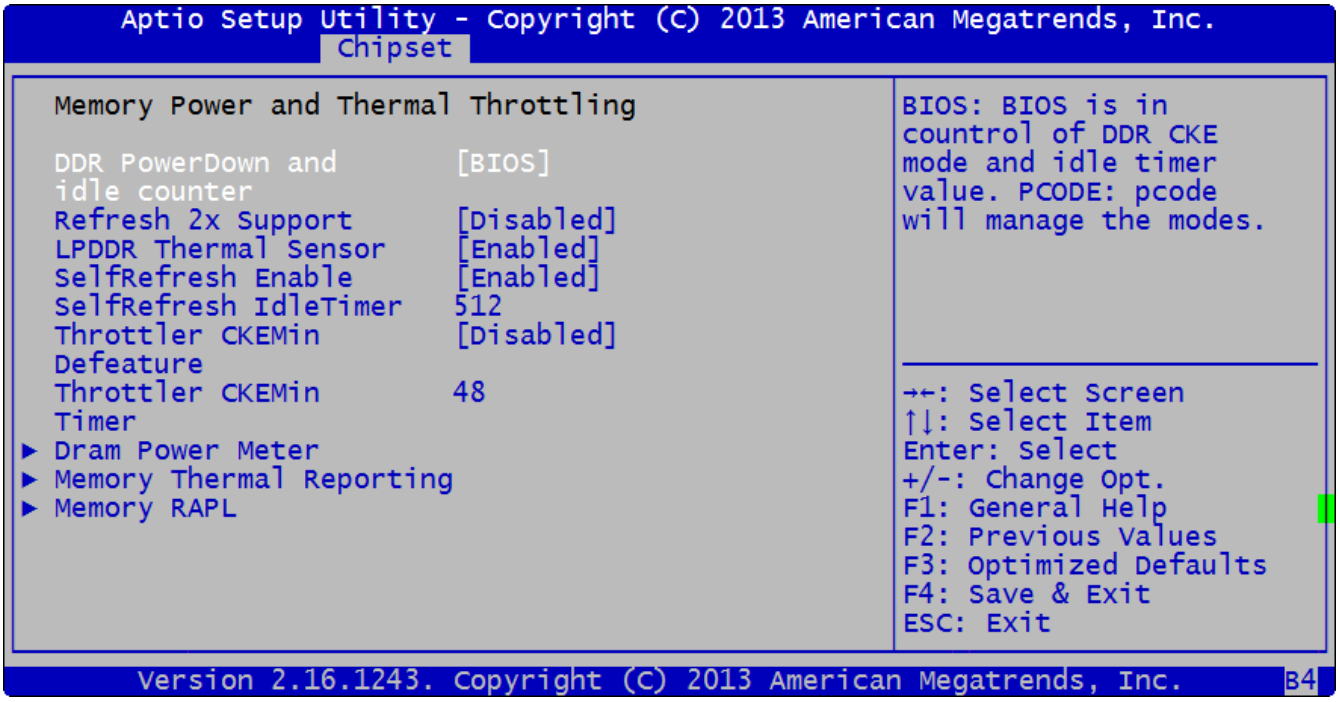
Fig. 2.3.2.5.a Memory Thermal Configuration



This option allows the user to view and change the Memory Thermal Configuration.

Feature	Options	Description
►Memory Power and Thermal Throttling		Memory Power and Thermal Throttling Options Menu
Memory Thermal	*Enabled* *Disabled*	Enable or disable Memory Thermal Management.
PECI Injected Temperature	*Disabled* *Enabled*	Enable or disable memory temperatures to be injected to the processor via the Platform Environment Control Interface (PECI).
EXTTS# via TS-on-Board	*Disabled* *Enabled*	Enable or disable routing Thermal Sensor-on-Board's ALERT# and THERM# to External Thermal Sensor (EXTTS#) pins on the Platform Control Hub (PCH).
EXTTS# via TS-on-DIMM	*Disabled* *Enabled*	Enable or disable routing Thermal Sensor-on-DIMM's ALERT# to External Thermal Sensor (EXTTS#) pins on the Platform Control Hub (PCH).
Virtual Temperature Sensor (VTS)	*Disabled* *Enabled*	Enable or disable Virtual Thermal Sensor (VTS).

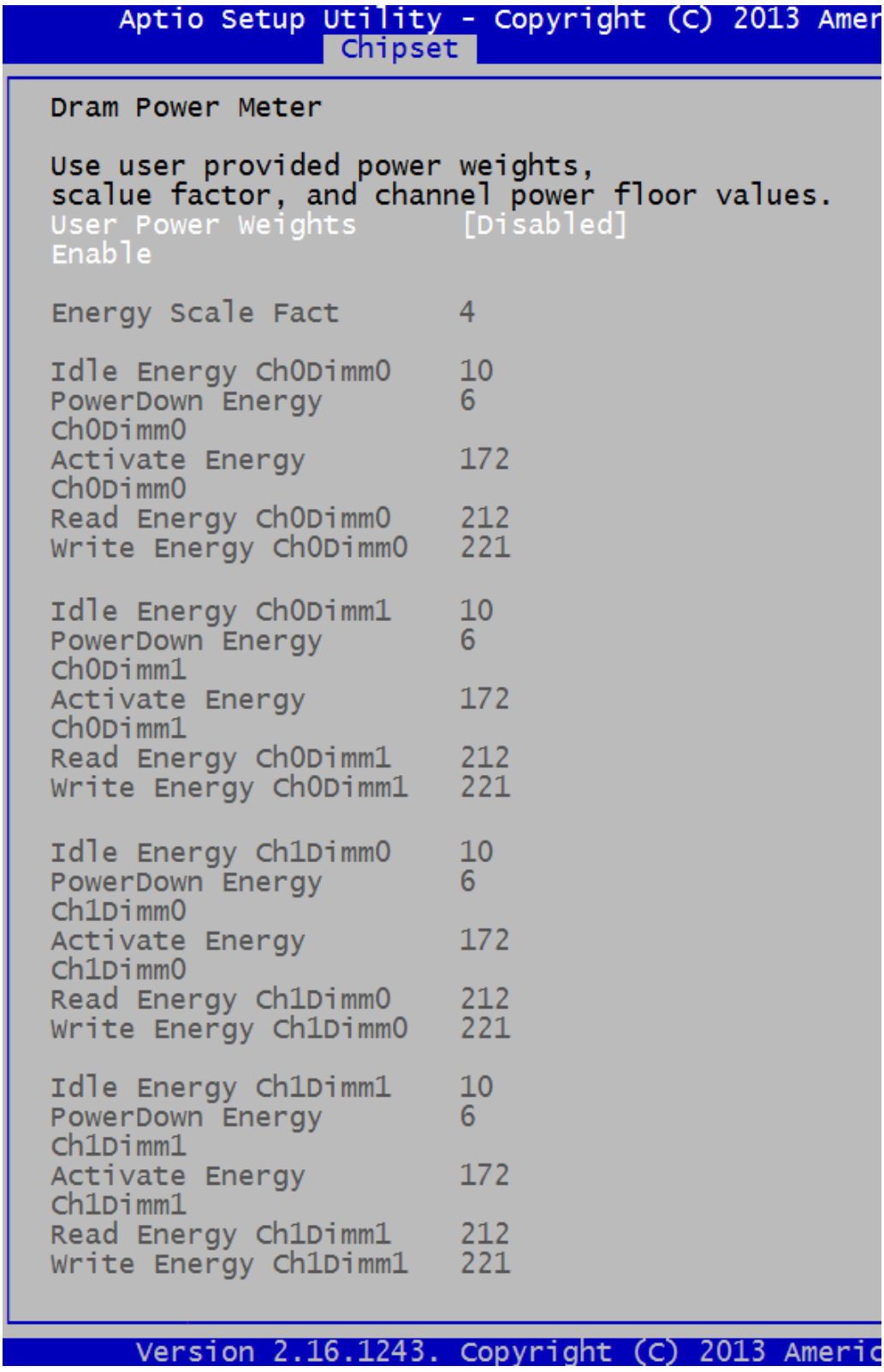
Fig. 2.3.2.5.1.a Memory Power and Thermal Throttling



This option allows the user to view and change the Memory Power and Thermal Throttling.

Feature	Options	Description
DDR PowerDown and Idle counter	*BIOS* *PCODE*	· BIOS is in control of Double Data Rate (DDR) Clock Enable (CKE) mode and idle timer value. · PCODE will manage the modes.
Refresh 2x Support	*Disabled* *Enabled*	Enable or disable Refresh 2x support.
LPDDR Thermal Sensor	*Enabled* *Disabled*	When enabled, MC uses MR4 to read LPDDR (Low Power Double Data Rate) thermal sensors.
SelfRefresh Enable	*Enabled* *Disabled*	Enable or disable SelfRefresh.
SelfRefresh IdleTimer	*512*	Range [64K-1;512] in DLCK800s.
Throttler CKEmin Defeature	*Disabled* *Enabled*	Enable or disable Throttler CKEmin Defeature.
Throttler CKEmin Timer	*512*	Range [64K-1;512] in DLCK800s.
▶Dram Power Meter		Dram Power Meter Options Menu
▶Memory Thermal Reporting		Memory Thermal Reporting Options Menu
▶Memory RAPL		Memory RAPL Options Menu

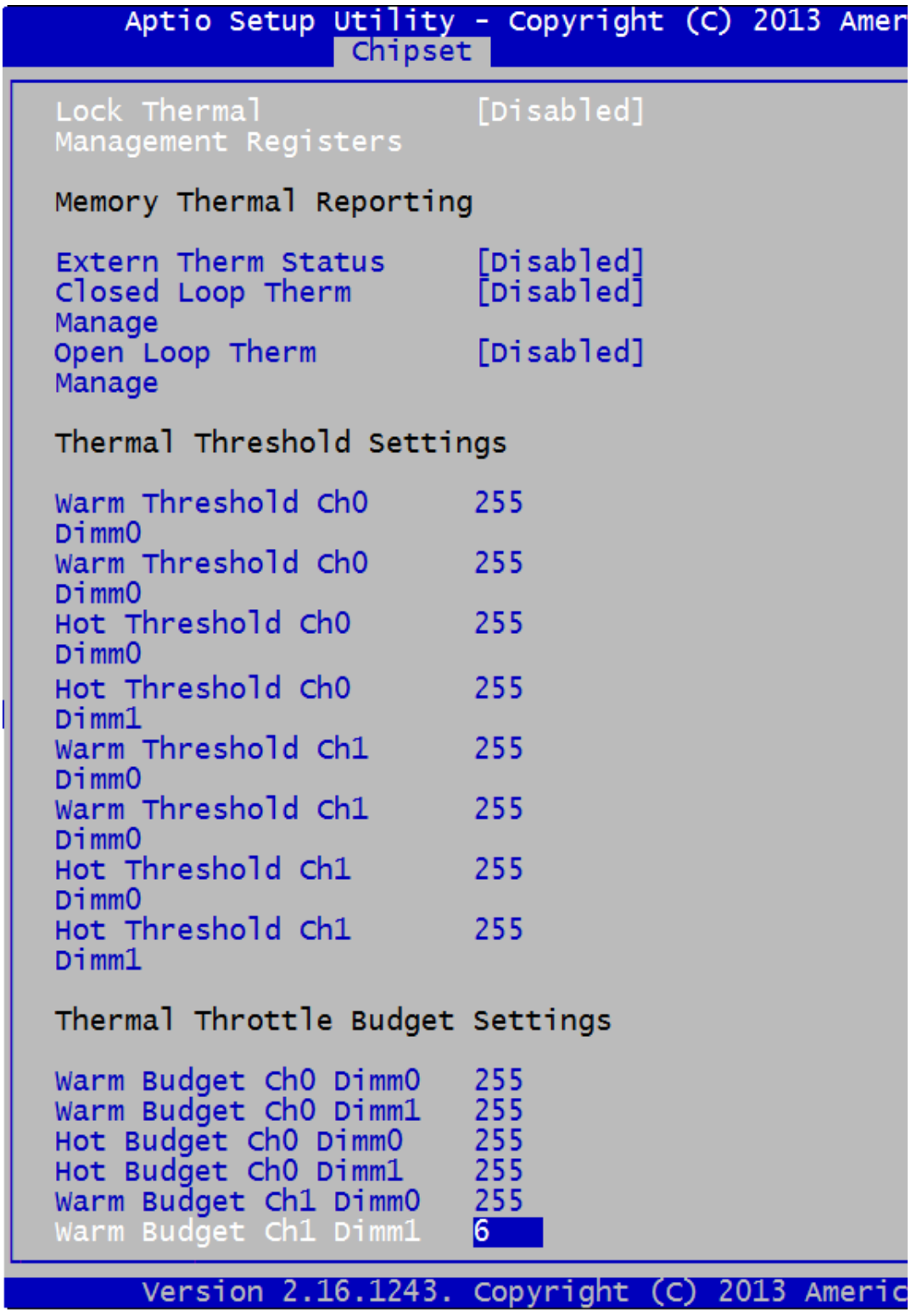
Fig. 2.3.2.5.1.1.a Dram Power Meter



This option allows the user to view and change the Dram Power Meter Configuration.

Feature	Options	Description
User Power Weights Enable	*Enabled* *Disabled*	· User provides power weights, scale factor, and channel power floor values are used. · BIOS sets power weights, scale factor, and channel power floor values based on DIMMs present in system.
Energy Scale Fact	*4*	Range [7;0] = [7.3;931.3] in pJ.
Idle Energy Ch0Dimm0	*10*	Idle Energy Consumed for 1 clk w/ dim idle/cke on, range[63;0].
PowerDown Energy Ch0Dimm0	*6*	PowerDown Energy Consumed for 1 clk w/ dim idle/cke off, range[63;0].
Activate Energy Ch0Dimm0	*172*	Activate Energy Contribution, range [255;0].
Read Energy Ch0Dimm0	*212*	Read Energy Contribution, range [255;0].
Write Energy Ch0Dimm0	*221*	Write Energy Contribution, range [255;0].
Idle Energy Ch0Dimm1	*10*	Idle Energy Consumed for 1 clk w/ dim idle/cke on, range[63;0].
PowerDown Energy Ch0Dimm1	*6*	PowerDown Energy Consumed for 1 clk w/ dim idle/cke off, range[63;0].
Activate Energy Ch0Dimm1	*172*	Activate Energy Contribution, range [255;0].
Read Energy Ch0Dimm1	*212*	Read Energy Contribution, range [255;0].
Write Energy Ch0Dimm1	*221*	Write Energy Contribution, range [255;0].
Idle Energy Ch1Dimm0	*10*	Idle Energy Consumed for 1 clk w/ dim idle/cke on, range[63;0].
PowerDown Energy Ch1Dimm0	*6*	PowerDown Energy Consumed for 1 clk w/ dim idle/cke off, range[63;0].
Activate Energy Ch1Dimm0	*172*	Activate Energy Contribution, range [255;0].
Read Energy Ch1Dimm0	*212*	Read Energy Contribution, range [255;0].
Write Energy Ch1Dimm0	*221*	Write Energy Contribution, range [255;0].
Idle Energy Ch1Dimm1	*10*	Idle Energy Consumed for 1 clk w/ dim idle/cke on, range[63;0].
PowerDown Energy Ch1Dimm1	*6*	PowerDown Energy Consumed for 1 clk w/ dim idle/cke off, range[63;0].
Activate Energy Ch1Dimm1	*172*	Activate Energy Contribution, range [255;0].
Read Energy Ch1Dimm1	*212*	Read Energy Contribution, range [255;0].
Write Energy Ch1Dimm1	*221*	Write Energy Contribution, range [255;0].

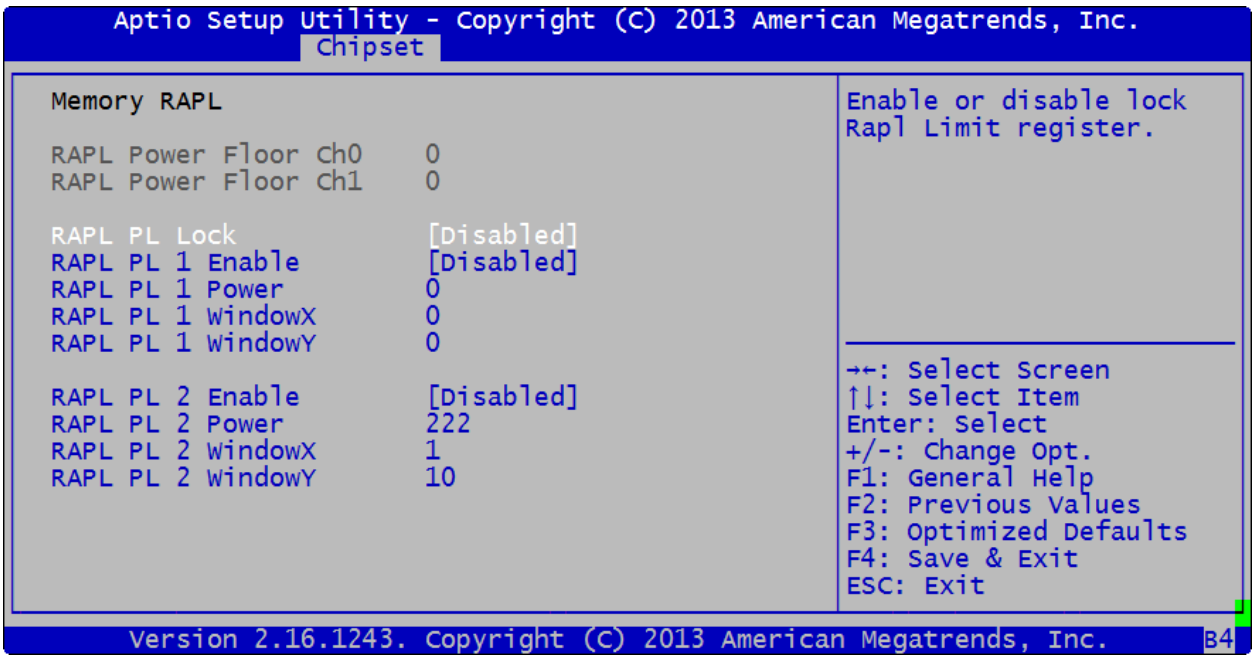
Fig. 2.3.2.5.1.2.a Memory Thermal Reporting



This option allows the user to view and change the Memory Thermal Reporting Configuration.

Feature	Options	Description
Lock Thermal Management Registers	*Enabled* *Disabled*	Enable or disable Lock several PCU registers related to DDR power Thermal Management.
Memory Thermal Reporting		
Extern Therm Status	*Enabled* *Disabled*	· The value from External thermal Sensors (EXTTS) are used. · Pcode ignores the EXTTS.
Closed Loop Therm Manage	*Enabled* *Disabled*	· CLTM pcode algorithm will be used. · CLTM pcode algorithm will be disabled. Note: CLTM will precede OLTM.
Open Loop Therm Manage	*Enabled* *Disabled*	· OLTM pcode algorithm will be used. · OLTM pcode algorithm will be disabled. Note: CLTM will precede OLTM.
Thermal Threshold Settings		
Warm Threshold Ch0 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch0 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch0 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch0 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch1 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch1 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch1 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Threshold Ch1 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Thermal Throttle Budget Settings		
Warm Budget Ch0 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Budget Ch0 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Hot Budget Ch0 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Hot Budget Ch0 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Budget Ch1 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Warm Budget Ch1 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Hot Budget Ch1 Dimm0	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)
Hot Budget Ch1 Dimm1	*255*	Range [255;0] = [0;31.875] in W, (255= 31.875W=Def)

Fig. 2.3.2.5.1.3.a Memory RAPL

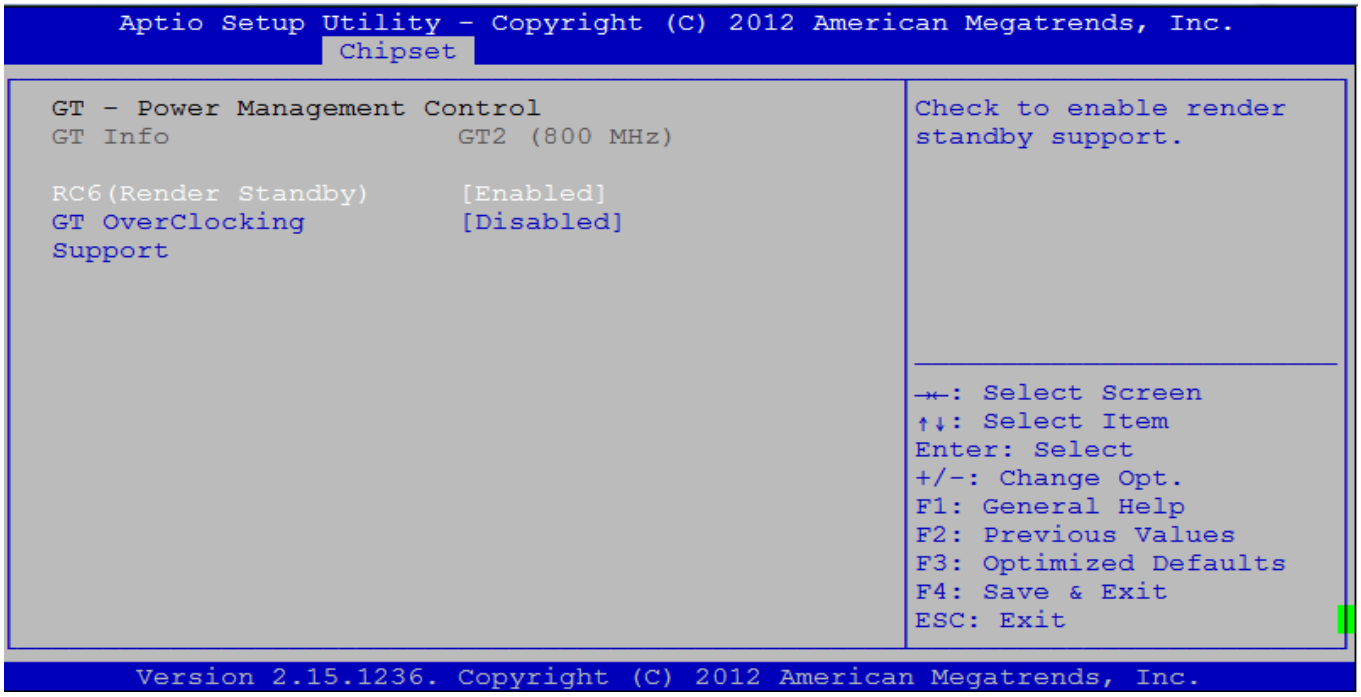


This option allows the user to view and change the Memory Running Average Power Limit (RAPL) Configuration.

Feature	Options	Description
RAPL Power Floor Ch0	*0*	
RAPL Power Floor Ch1	*0*	
RAPL PL Lock	*Disabled* *Enabled*	Enable or disable lock RAPL Limit register.
RAPL PL 1 Enable	*Disabled* *Enabled*	Enable or disable RAPL PL 1.
RAPL PL 1 Power	*0*	Range [0;2^14-1]=[2047.875;0] in W.
RAPL PL 1 WindowsX	*0*	Power PL 1 time window, X value, (1/1024)*(1+(x/4))*(2^y)
RAPL PL 1 WindowsY	*0*	Power PL 1 time window, Y value, (1/1024)*(1+(x/4))*(2^y)
RAPL PL 2 Enable	*Disabled* *Enabled*	Enable or disable RAPL PL 2.
RAPL PL 2 Power	*0*	Range [0;2^14-1]=[2047.875;0] in W.
RAPL PL 2 WindowsX	*0*	Power PL 2 time window, X value, (1/1024)*(1+(x/4))*(2^y)
RAPL PL 2 WindowsY	*0*	Power PL 2 time window, Y value, (1/1024)*(1+(x/4))*(2^y)

2.3.2.6 GT Power Management Control

Fig. 2.3.2.6.a GT Power Management Control



2.4 Security, Boot, and Save and Exit

2.4.1 Security Screens

2.4.1.1 Passwords

Fig. 2.4.1.1.a Passwords (Screen 1 of 2)

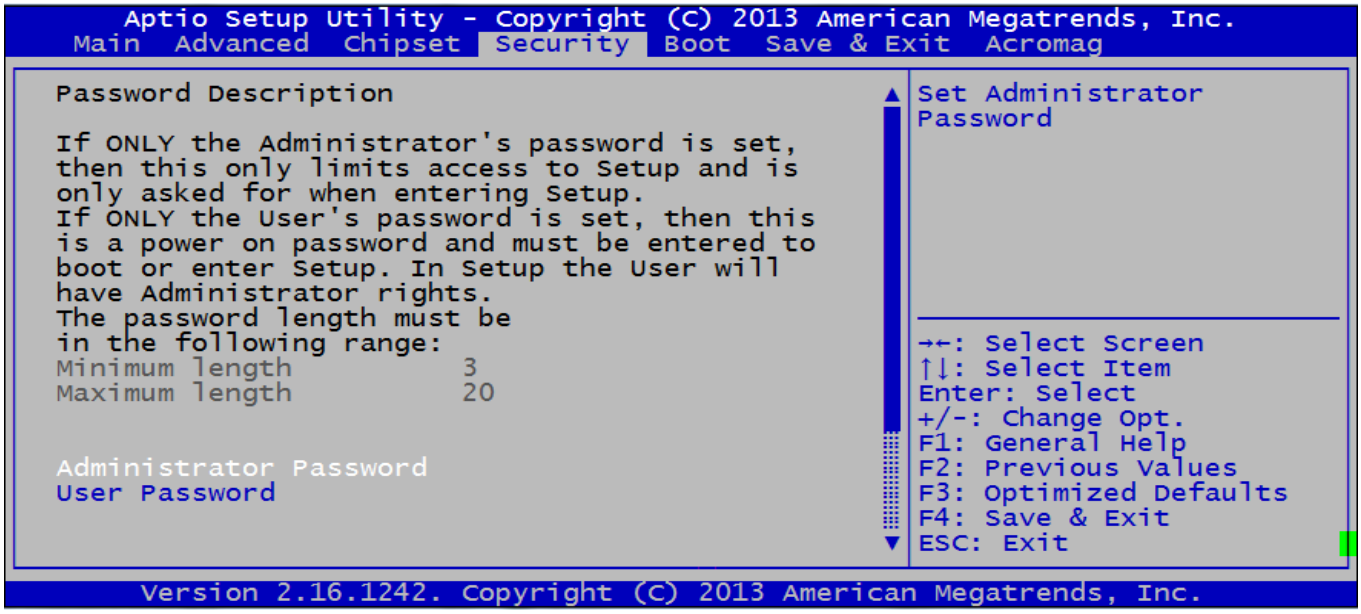
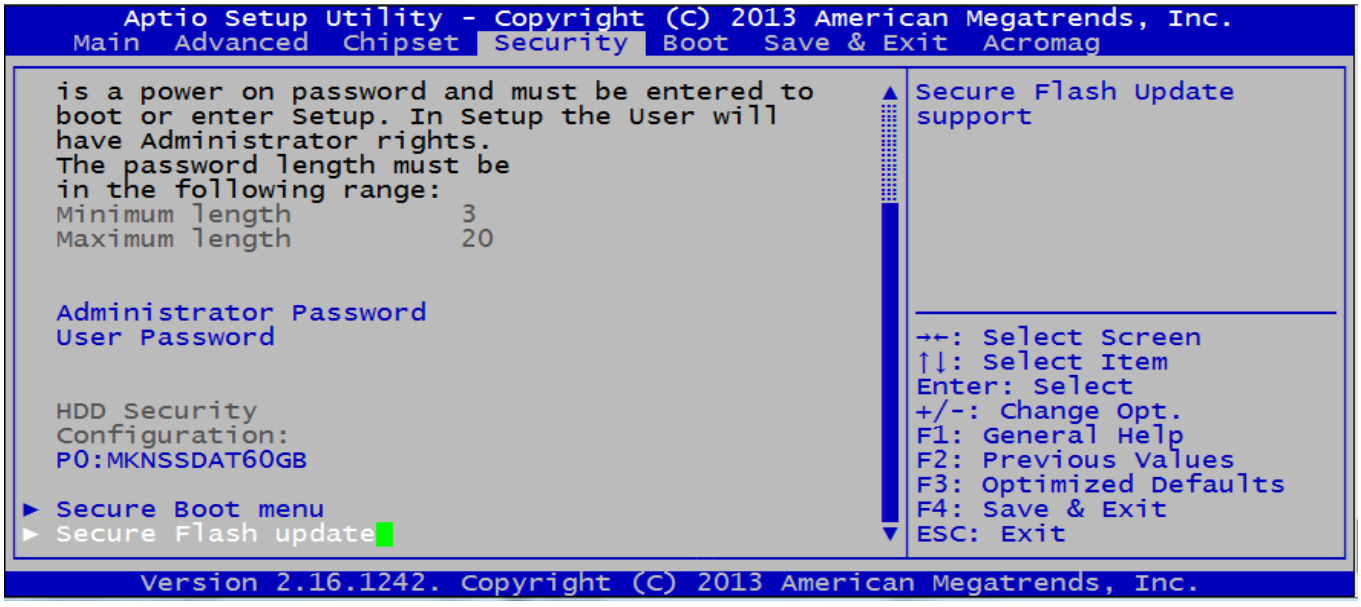


Fig. 2.4.1.1.b Passwords (Screen 2 of 2)



Two Levels of Password Protection

Security Setup provides both Administrator and User password. If you use both passwords, the Administrator password must be set first.

The system can be configured so that all users must enter a password every time the system boots or when Setup is executed, using either the Administrator password or User password.

The Administrator and User passwords activate two different levels of password security as described in the table below.

If you select password support, you are prompted for a three to twenty character password. Type the password on the keyboard. The password does not appear on the screen when typed. Make sure you write it down. If you forget it, you must drain NVRAM and reconfigure.

This option allows the user to view and configure the Security setup parameters.

Feature	Description
User Password	This option allows the user to set a user level password for the BIOS. There is no Default password. 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.
Administrator Password	This option allows the user to set an administrative level password for the BIOS. There is no Default password. If ONLY the Administrator's password is set, this this only limits access to Setup and is only asked for when entering Setup.

Remember the Password

Keep a record of the new password when the password is changed. If you forget the password, you must erase the system configuration information in NVRAM.

2.4.1.2 Key Management

Fig. 2.4.1.2.a Key Management (Screen 1 of 2

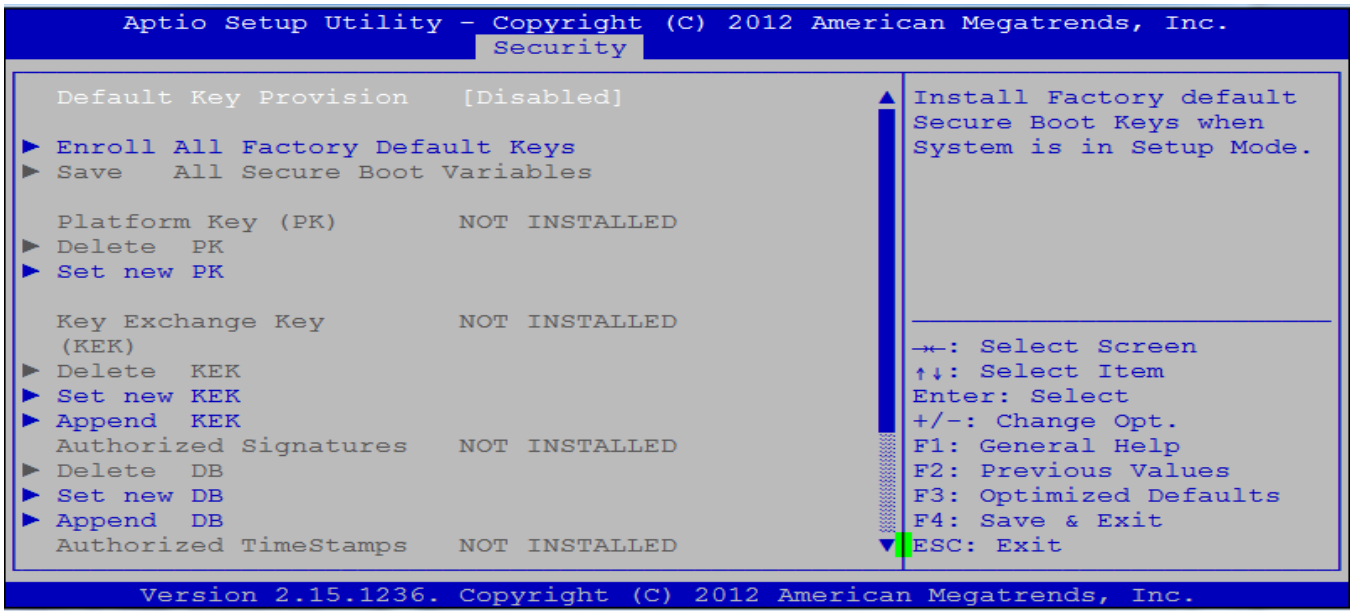
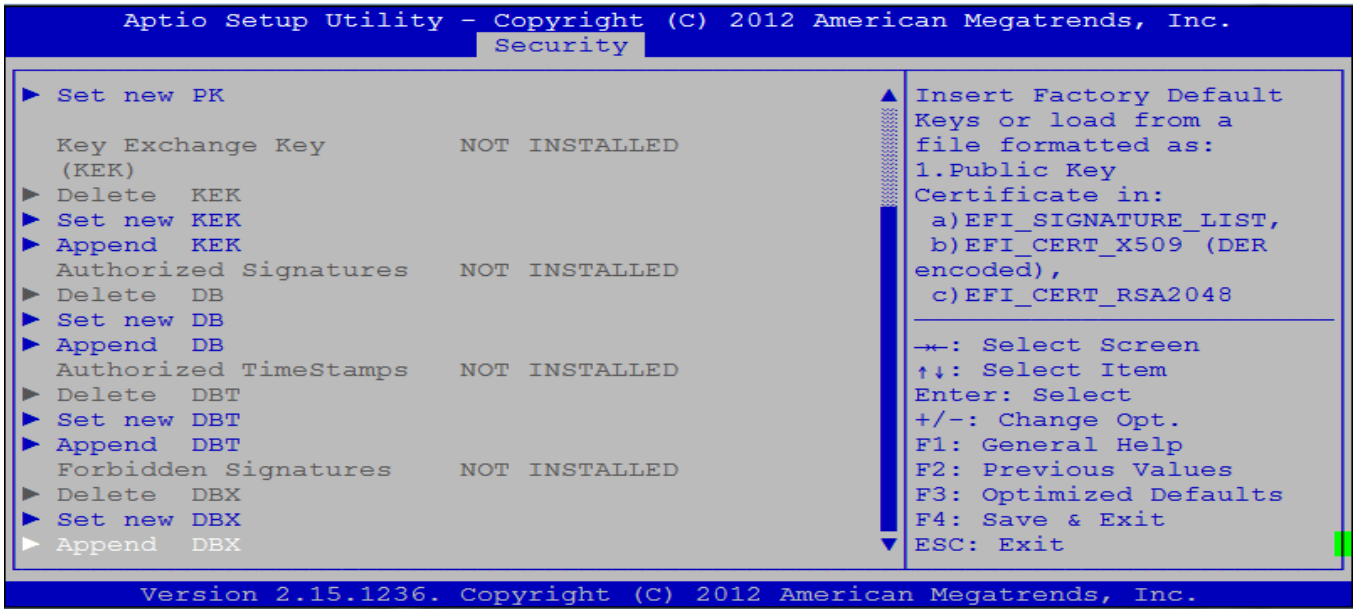
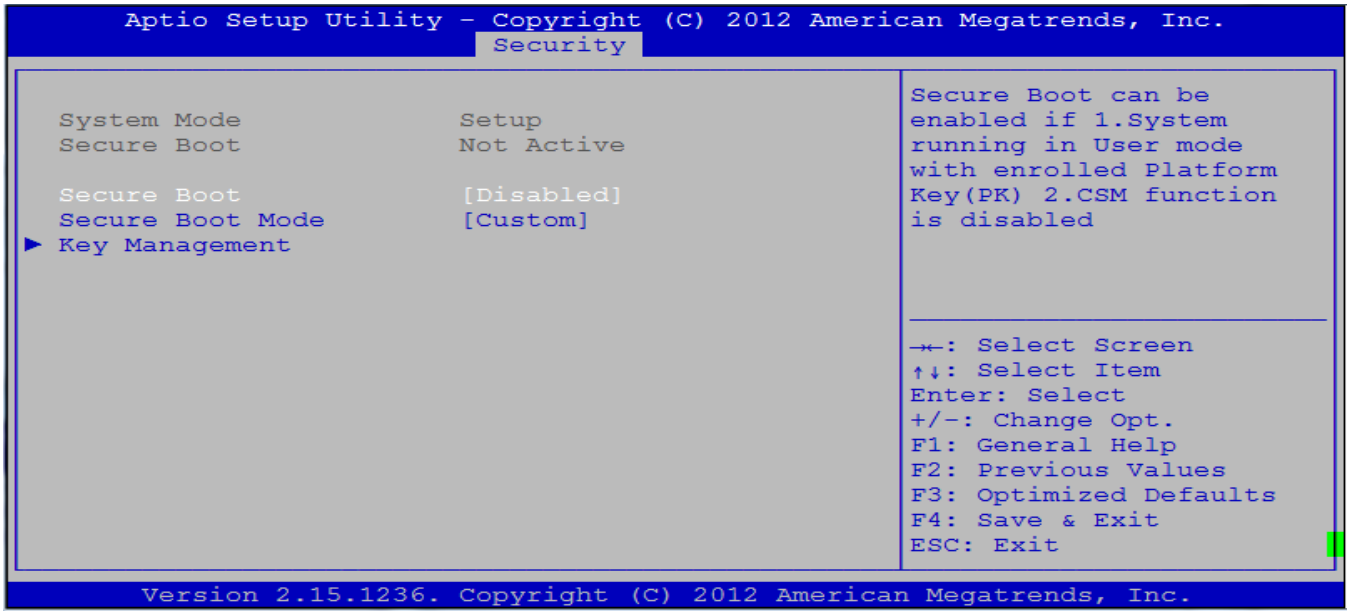


Fig. 2.4.1.2.b Key Management (Screen 2 of 2)



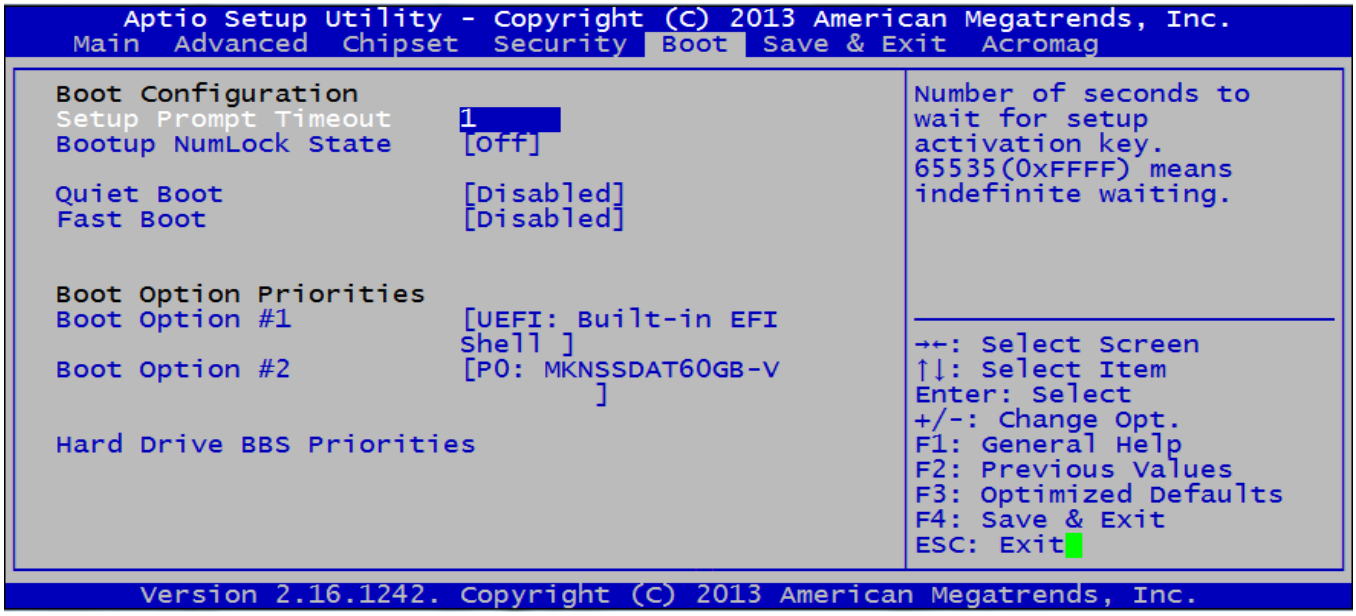
2.4.1.3 Secure Boot Menu

Fig. 2.4.1.3.a Secure Boot Menu



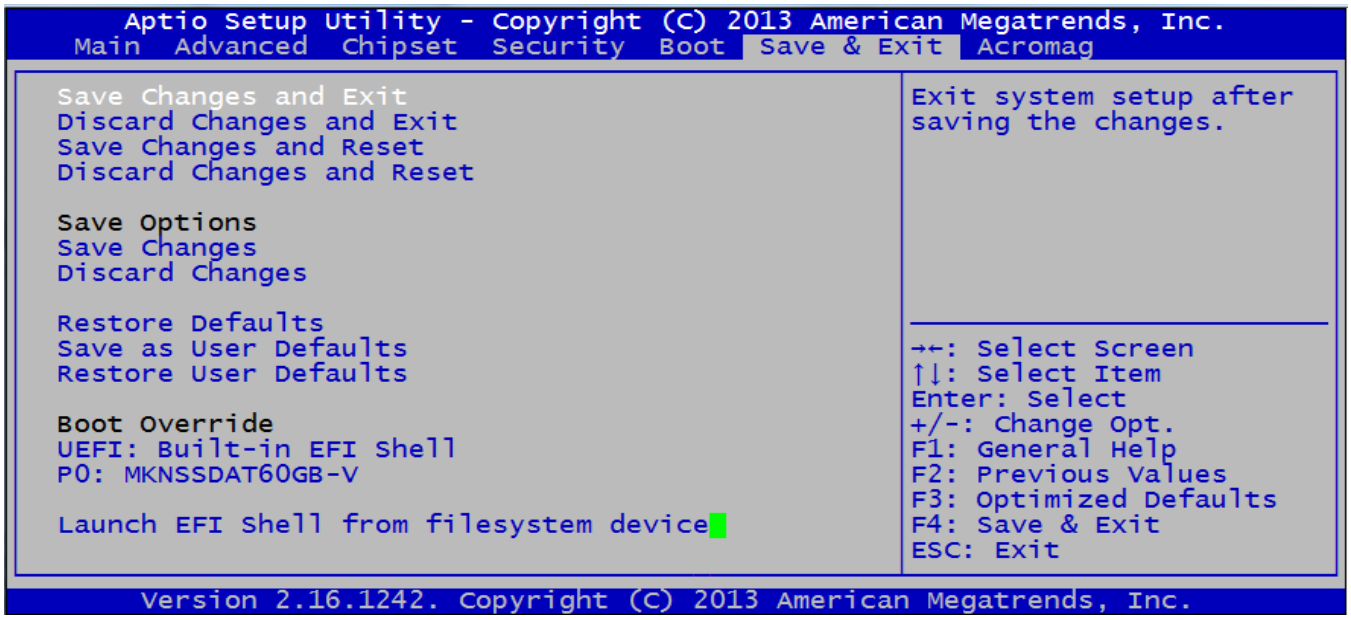
2.4.2 Boot Menu

Fig. 2.4.2.a Boot Menu



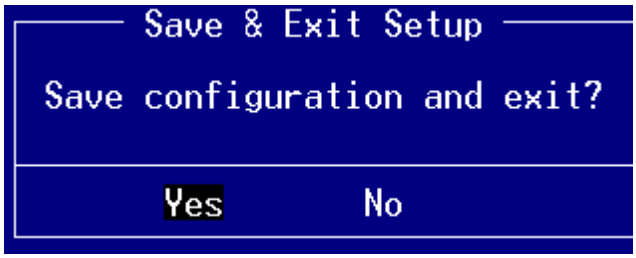
2.4.3 Save and Exit

Fig. 2.4.3.a Save and Exit



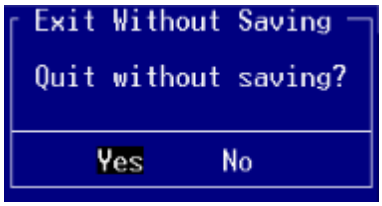
Save Changes and Exit

When you have completed the system configuration changes, select this option to save the changes and Exit from BIOS Setup, so the new system configuration parameters can take effect. The following window will appear after selecting the 'Save Changes and Exit' option selected. Select *YES* to Save Changes and Exit Setup.



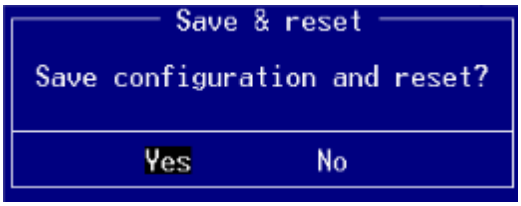
Discard Changes and Exit

Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after selecting the 'Discard Changes and Exit' option selected. Select *YES* to Discard changes and Exit Setup.



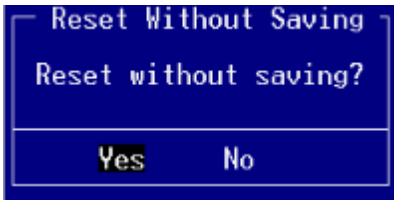
Save Changes and Reset

When you have completed the system configuration changes, select this option to save the changes and reboot the system, so the new system configuration parameters can take effect. The following window will appear after selecting the 'Save Changes and Reset' option selected. Select *YES* to Save Changes and Reset.



Discard Changes and Reset

Select this option to reboot the system without saving the changes done in the setup configuration. The following window will appear after selecting the 'Discard Changes and Reset' option selected. Select *YES* to Reset without saving.

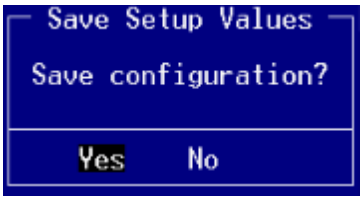


Save Options

Save Changes done so far to any of the setup options.

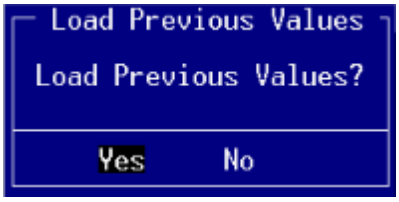
Save Changes

When you have completed the system configuration changes, select this option to save your system configuration and continue. For some of the options it required to reset the system to take effect. Select *YES* to Save Changes and continue.



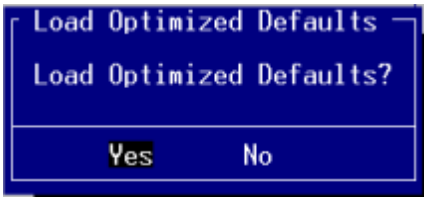
Discard Changes

When you have completed the system configuration changes, select this option to undo the previous changes Select *YES* to load previous value and continue



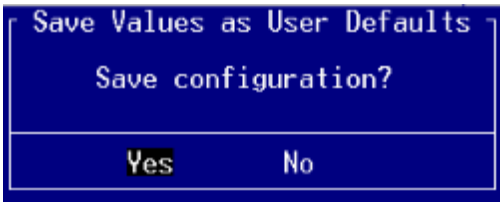
Restore Defaults

Restore default values for all setup options. Select *YES* to load Optimized defaults.



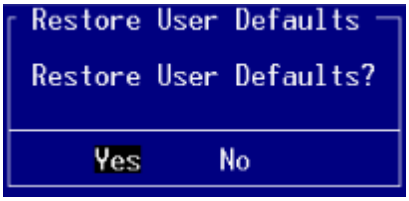
Save as User Defaults

Save changes done so far as User defaults. Select *YES* to save changes and continue.



Restore User Defaults

Restore the User defaults to all the setup options Select *YES* to restore changes to user defaults and continue.



3.0 Revision History

The following table shows the revision history for this document:

Release Date	Version	EGR/DOC	Description of Revision
12/16/2013	A	BD/TG	Preliminary release
12/18/2013	A1	BD	Edits
7/8/2014	B	BD	Add details for menu items that are referenced in the XCOM-6400 User's Manual