APTIO^{TM} HASWELL CORE BIOS MANUAL

For Acromag® Products

using the

Haswell Processor

ACROMAG INCORPORATED
30765 South Wixom Road
Wixom, MI 48393-2417 U.S.A.
Tel: (248) 624-1541
Fax: (248) 624-9234

8501026D

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

1.7 Disclaimer

Changing BIOS setup parameters carries risks. It can lead to system instability and data loss or even cause the system to no longer boot. It is recommended that only advanced users change these settings.

Please proceed at your own risk. In no event shall Acromag be held liable for any loss, expenses, or damages of any kind, whether direct, indirect, incidental, or consequential, arising from the modification of BIOS settings or any other support materials provided in our products.

2.0 Aptio™ BIOS Setup

2.1 Main Menu

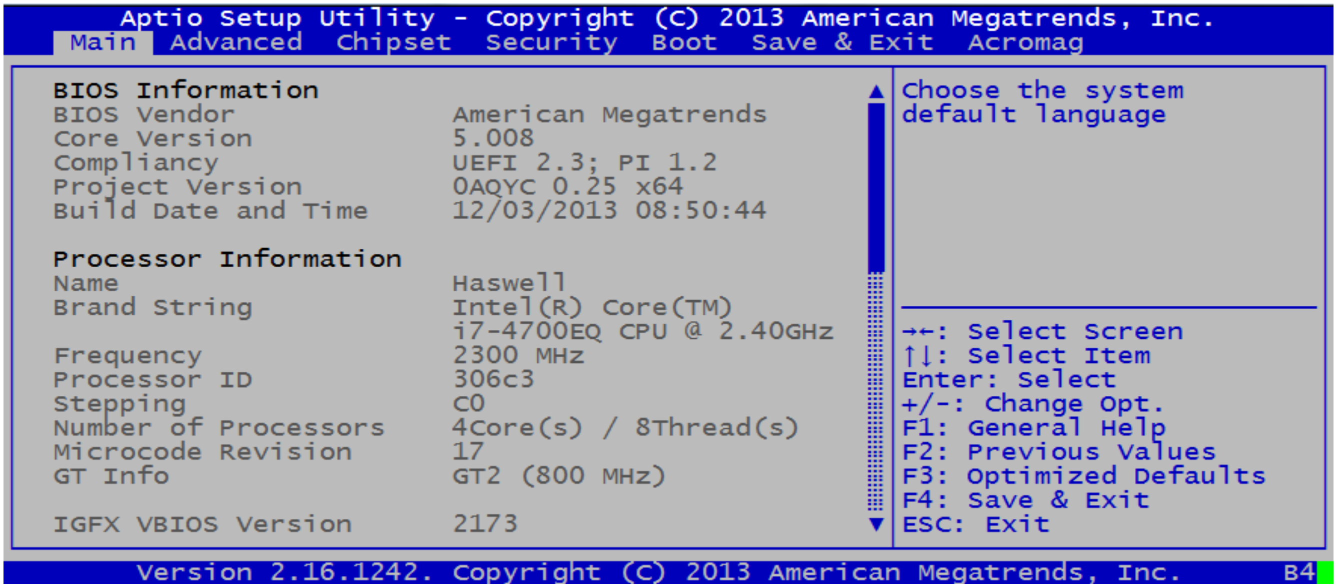
The Aptio™ TSE BIOS setup menu is the first screen that you can navigate. Each BIOS setup menu option is described in this user's manual.
To enter the Aptio™ TSE screens, follow the steps outlined below:

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.

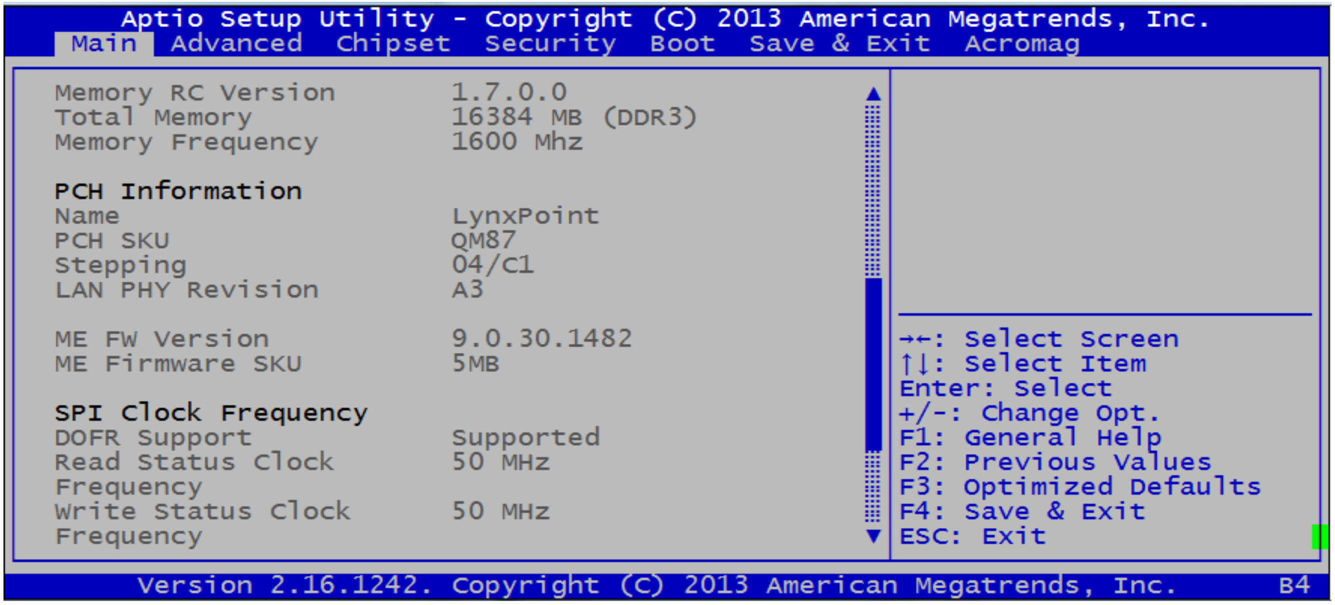
In most cases, the <Delete> key is used to invoke the Aptio™ TSE screen. There are a few cases where other keys are used, such as <F1>, <F2>, and so on. The user can press the <TAB> key during boot to switch from the boot splash screen (logo) to see the keystroke messages. The Aptio™ TSE BIOS setup menu (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)



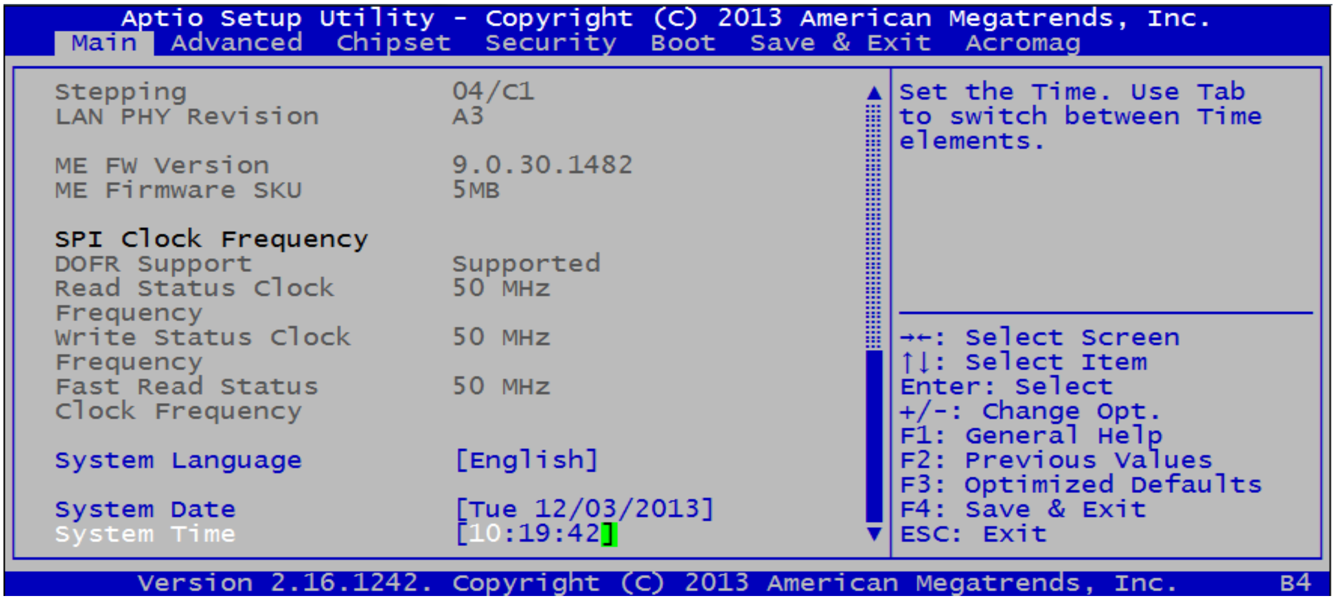
```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
     Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

  BIOS Information                                     Choose the system
  BIOS Vendor              American Megatrends         default language
  Core Version             5.008
  Compliancy               UEFI 2.3; PI 1.2
  Project Version          0AQYC 0.25 x64
  Build Date and Time      12/03/2013 08:50:44

  Processor Information
  Name                     Haswell
  Brand String             Intel(R) Core(TM)
                           i7-4700EQ CPU @ 2.40GHz     →←: Select Screen
  Frequency                2300 MHz                    ↑↓: Select Item
  Processor ID             306c3                       Enter: Select
  Stepping                 C0                          +/-: Change Opt.
  Number of Processors     4Core(s) / 8Thread(s)       F1: General Help
  Microcode Revision       17                          F2: Previous Values
  GT Info                  GT2 (800 MHz)               F3: Optimized Defaults
                                                       F4: Save & Exit
  IGFX VBIOS Version       2173                        ESC: Exit
        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.     B4
```

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



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

  Memory RC Version          1.7.0.0
  Total Memory               16384 MB (DDR3)
  Memory Frequency           1600 Mhz

  PCH Information
  Name                       LynxPoint
  PCH SKU                    QM87
  Stepping                   04/C1
  LAN PHY Revision           A3

  ME FW Version              9.0.30.1482            →←: Select Screen
  ME Firmware SKU            5MB                    ↑↓: Select Item
                                                    Enter: Select
  SPI Clock Frequency                               +/-: Change Opt.
  DOFR Support               Supported              F1: General Help
  Read Status Clock          50 MHz                 F2: Previous Values
  Frequency                                         F3: Optimized Defaults
  Write Status Clock         50 MHz                 F4: Save & Exit
  Frequency                                         ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.    B4
```

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



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

  Stepping                   04/C1                  Set the Time. Use Tab
  LAN PHY Revision           A3                     to switch between Time
                                                    elements.
  ME FW Version              9.0.30.1482
  ME Firmware SKU            5MB

  SPI Clock Frequency
  DOFR Support               Supported
  Read Status Clock          50 MHz
  Frequency
  Write Status Clock         50 MHz                 →←: Select Screen
  Frequency                                         ↑↓: Select Item
  Fast Read Status           50 MHz                 Enter: Select
  Clock Frequency                                   +/-: Change Opt.
                                                    F1: General Help
  System Language            [English]              F2: Previous Values
                                                    F3: Optimized Defaults
  System Date                [Tue 12/03/2013]       F4: Save & Exit
  System Time                [10:19:42]             ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.    B4
```

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.

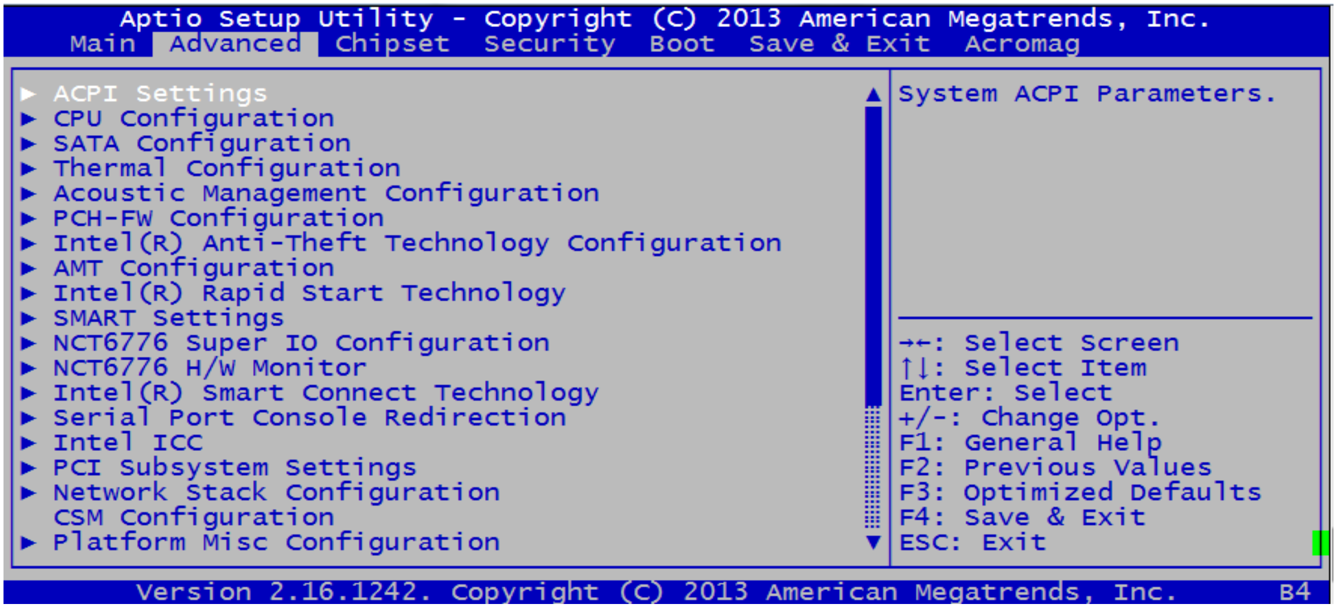
Fig. 2.1.1.a Keyboard-Based Navigation

Keystroke	Description
<Enter>	The *Enter* key allows the user to select an option to edit its value or access a sub menu.
<Left Arrow Key> and <Right Arrow Key>	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.
<Up Arrow Key> and <Down Arrow Key>	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* 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

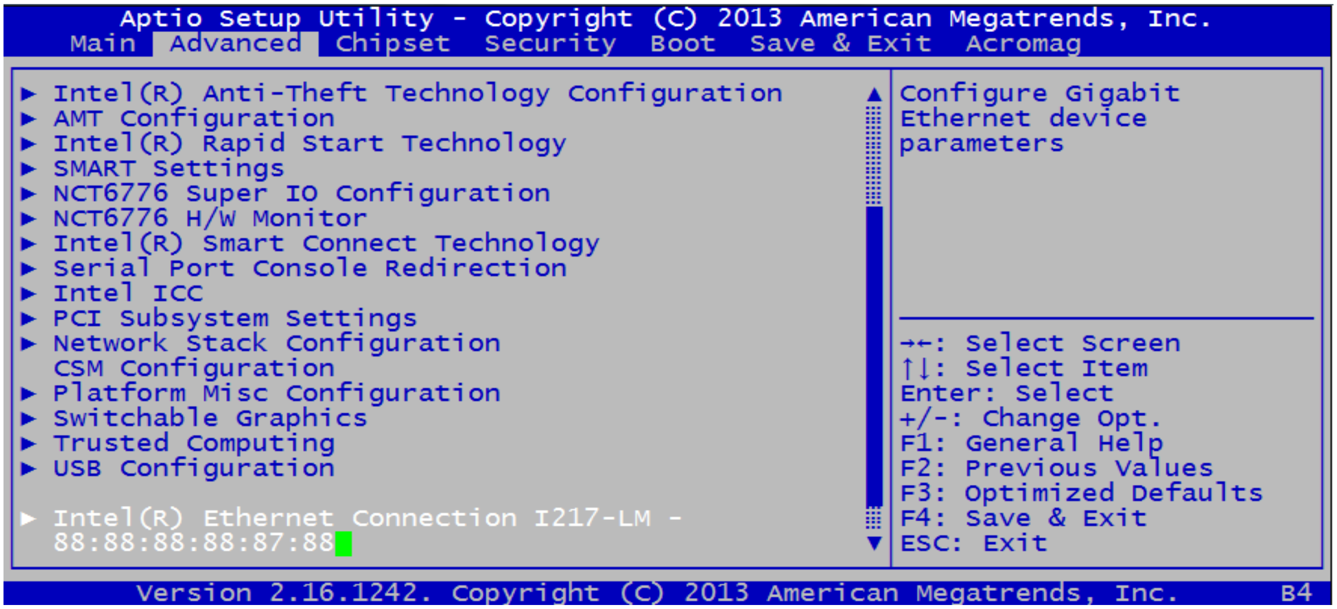
Select the *Advanced* menu item from the Aptio™ TSE screen to enter the Advanced BIOS Setup screen. You can select any of the items in the left frame of the screen.

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



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

 ▶ ACPI Settings                                     ▲ System ACPI Parameters.
 ▶ CPU Configuration
 ▶ SATA Configuration
 ▶ Thermal Configuration
 ▶ Acoustic Management Configuration
 ▶ PCH-FW Configuration
 ▶ Intel(R) Anti-Theft Technology Configuration
 ▶ AMT Configuration
 ▶ Intel(R) Rapid Start Technology
 ▶ SMART Settings
 ▶ NCT6776 Super IO Configuration                      →←: Select Screen
 ▶ NCT6776 H/W Monitor                                 ↑↓: Select Item
 ▶ Intel(R) Smart Connect Technology                   Enter: Select
 ▶ Serial Port Console Redirection                     +/-: Change Opt.
 ▶ Intel ICC                                           F1: General Help
 ▶ PCI Subsystem Settings                              F2: Previous Values
 ▶ Network Stack Configuration                         F3: Optimized Defaults
   CSM Configuration                                   F4: Save & Exit
 ▶ Platform Misc Configuration                       ▼ ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.      B4
```

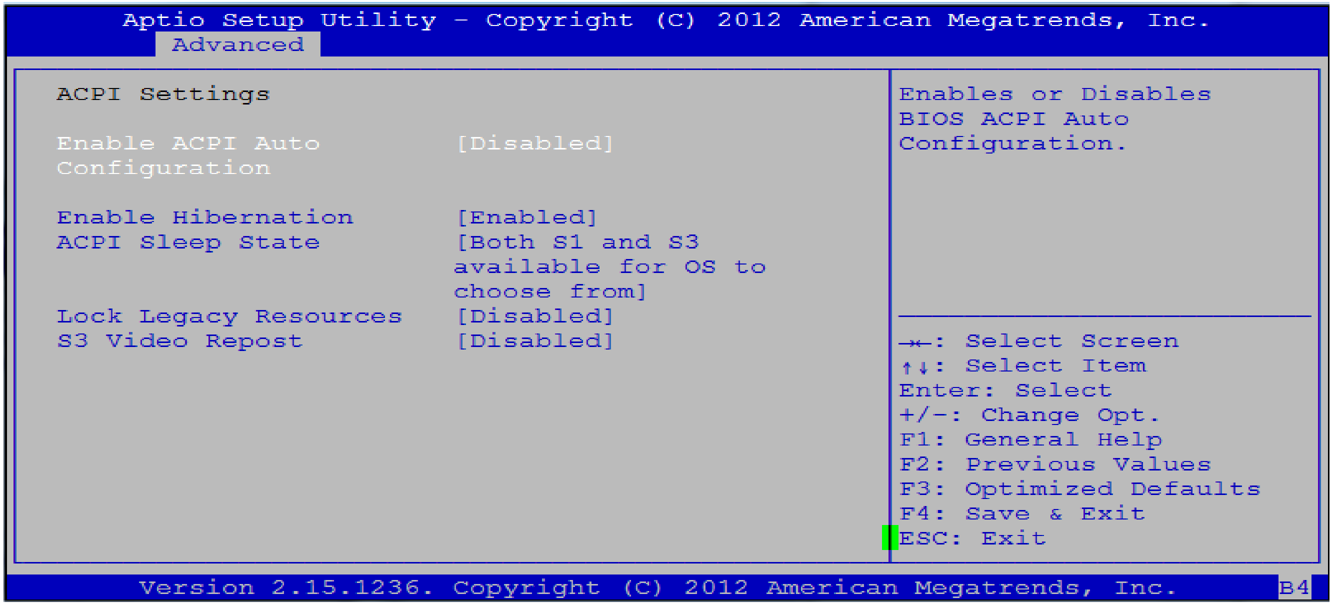
Fig. 2.2.b Advanced Menu (Screen 2 of 2)



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

 ▶ Intel(R) Anti-Theft Technology Configuration      ▲ Configure Gigabit
 ▶ AMT Configuration                                   Ethernet device
 ▶ Intel(R) Rapid Start Technology                     parameters
 ▶ SMART Settings
 ▶ NCT6776 Super IO Configuration
 ▶ NCT6776 H/W Monitor
 ▶ Intel(R) Smart Connect Technology
 ▶ Serial Port Console Redirection
 ▶ Intel ICC
 ▶ PCI Subsystem Settings
 ▶ Network Stack Configuration                         →←: Select Screen
   CSM Configuration                                   ↑↓: Select Item
 ▶ Platform Misc Configuration                         Enter: Select
 ▶ Switchable Graphics                                 +/-: Change Opt.
 ▶ Trusted Computing                                   F1: General Help
 ▶ USB Configuration                                   F2: Previous Values
                                                       F3: Optimized Defaults
 ▶ Intel(R) Ethernet Connection I217-LM -              F4: Save & Exit
   88:88:88:88:87:88                                 ▼ ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.      B4
```

2.2.1 ACPI Settings

Fig. 2.2.1.a ACPI Settings



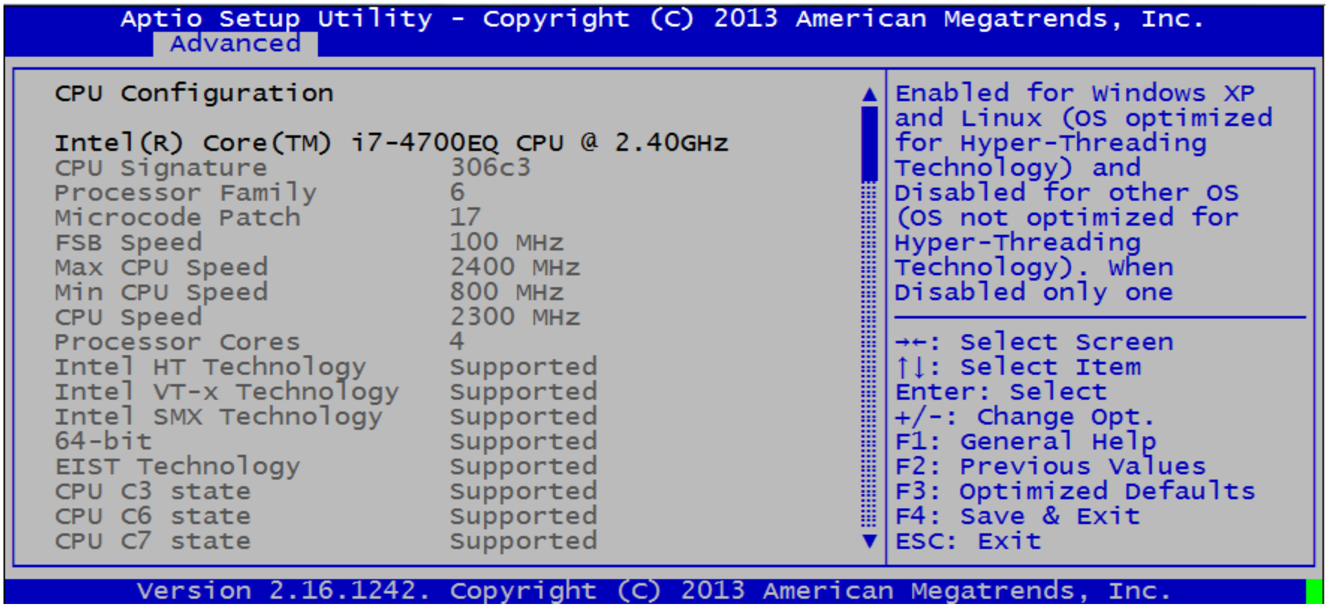
```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
         Advanced
  ACPI Settings                                  Enables or Disables
                                                 BIOS ACPI Auto
  Enable ACPI Auto         [Disabled]            Configuration.
  Configuration

  Enable Hibernation       [Enabled]
  ACPI Sleep State         [Both S1 and S3
                           available for OS to
                           choose from]
  Lock Legacy Resources    [Disabled]
  S3 Video Repost          [Disabled]            →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit
        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.      B4
```

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.
blah		
S3 Video Repost	*Enabled* *Disabled*	Enables or Disables S3 Video Repost.

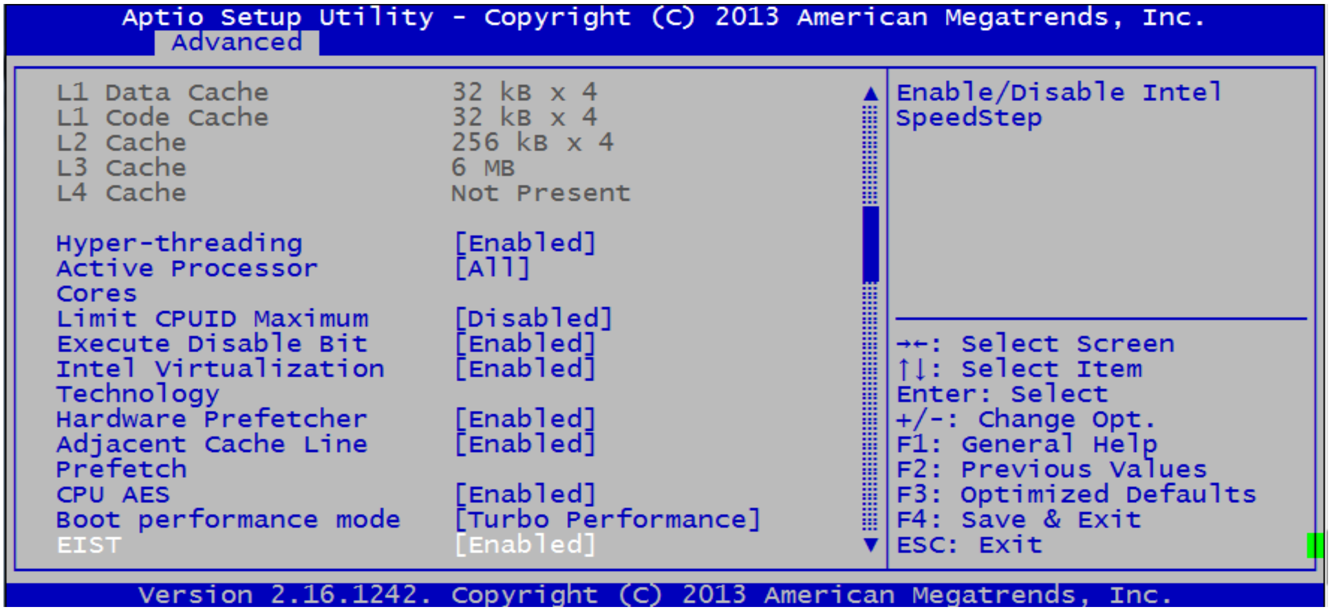
2.2.2 CPU Configuration

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



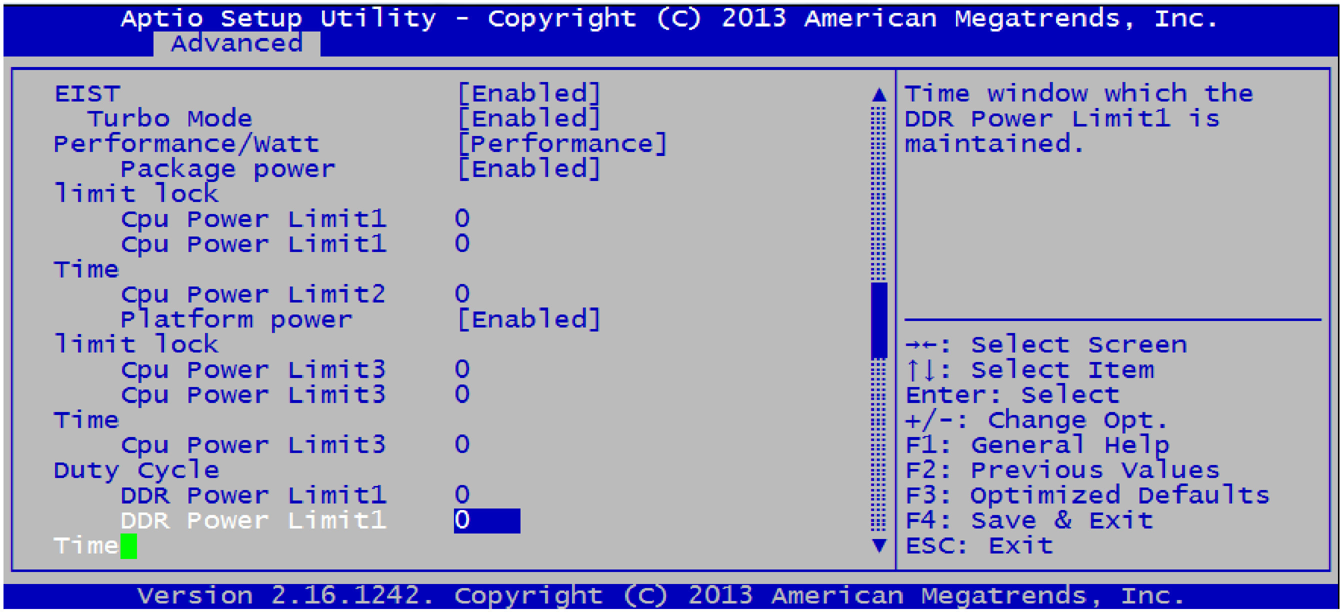
```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
           Advanced

  CPU Configuration                                ▲ Enabled for Windows XP
                                                     and Linux (OS optimized
  Intel(R) Core(TM) i7-4700EQ CPU @ 2.40GHz          for Hyper-Threading
  CPU Signature               306c3                  Technology) and
  Processor Family            6                      Disabled for other OS
  Microcode Patch             17                     (OS not optimized for
  FSB Speed                   100 MHz                Hyper-Threading
  Max CPU Speed               2400 MHz               Technology). When
  Min CPU Speed               800 MHz                Disabled only one
  CPU Speed                   2300 MHz
  Processor Cores             4                      →←: Select Screen
  Intel HT Technology         Supported              ↑↓: Select Item
  Intel VT-x Technology       Supported              Enter: Select
  Intel SMX Technology        Supported              +/-: Change Opt.
  64-bit                      Supported              F1: General Help
  EIST Technology             Supported              F2: Previous Values
  CPU C3 state                Supported              F3: Optimized Defaults
  CPU C6 state                Supported              F4: Save & Exit
  CPU C7 state                Supported        ▼     ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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



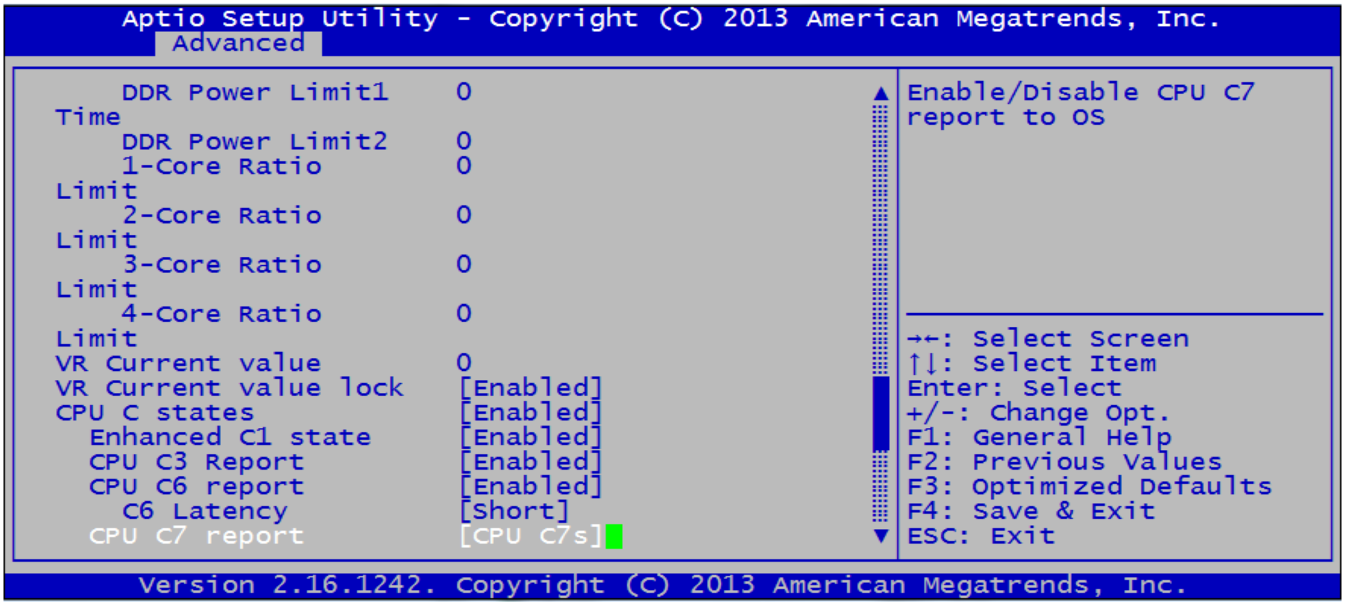
```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
           Advanced

  L1 Data Cache               32 kB x 4            ▲ Enable/Disable Intel
  L1 Code Cache               32 kB x 4              SpeedStep
  L2 Cache                    256 kB x 4
  L3 Cache                    6 MB
  L4 Cache                    Not Present

  Hyper-threading             [Enabled]
  Active Processor            [All]
  Cores
  Limit CPUID Maximum         [Disabled]
  Execute Disable Bit         [Enabled]              →←: Select Screen
  Intel Virtualization        [Enabled]              ↑↓: Select Item
  Technology                                         Enter: Select
  Hardware Prefetcher         [Enabled]              +/-: Change Opt.
  Adjacent Cache Line         [Enabled]              F1: General Help
  Prefetch                                           F2: Previous Values
  CPU AES                     [Enabled]              F3: Optimized Defaults
  Boot performance mode       [Turbo Performance]    F4: Save & Exit
  EIST                        [Enabled]        ▼     ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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



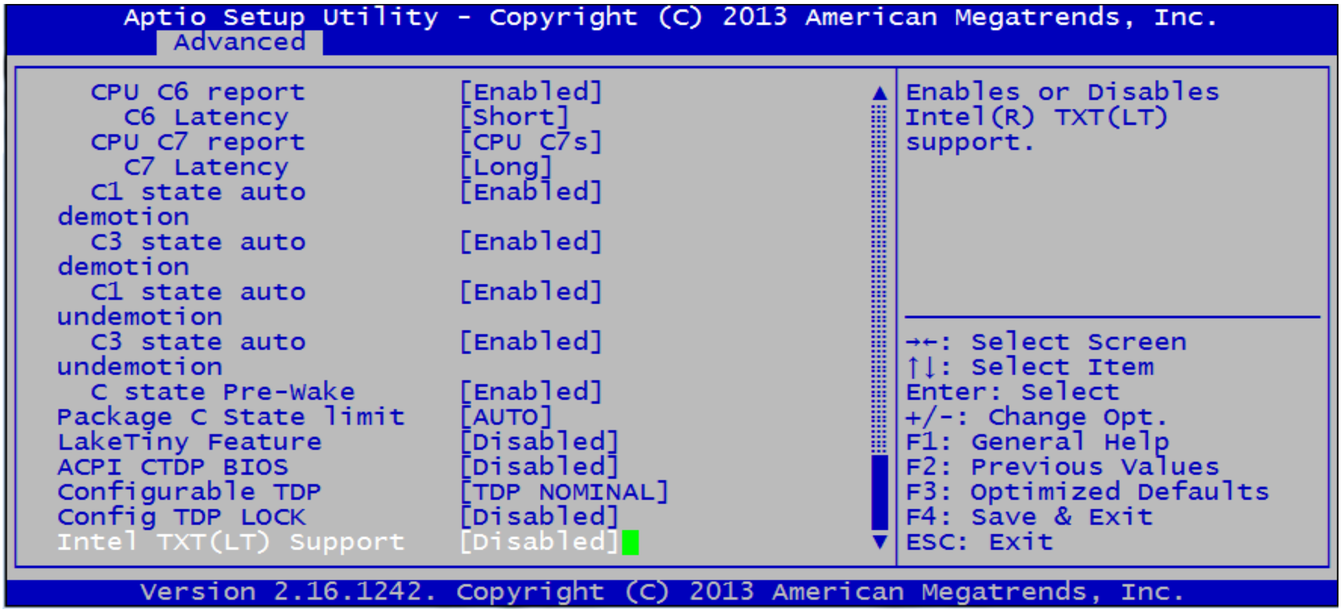
```
    Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
       Advanced

  EIST                         [Enabled]           ▲ Time window which the
    Turbo Mode                 [Enabled]             DDR Power Limit1 is
  Performance/Watt             [Performance]         maintained.
      Package power            [Enabled]
  limit lock
      Cpu Power Limit1         0
      Cpu Power Limit1         0
  Time
      Cpu Power Limit2         0
      Platform power           [Enabled]
  limit lock                                         →←: Select Screen
      Cpu Power Limit3         0                     ↑↓: Select Item
      Cpu Power Limit3         0                     Enter: Select
  Time                                               +/-: Change Opt.
      Cpu Power Limit3         0                     F1: General Help
  Duty Cycle                                         F2: Previous Values
      DDR Power Limit1         0                     F3: Optimized Defaults
      DDR Power Limit1         0                     F4: Save & Exit
  Time                                             ▼ ESC: Exit

     Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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



```
    Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
       Advanced

      DDR Power Limit1         0                   ▲ Enable/Disable CPU C7
  Time                                               report to OS
      DDR Power Limit2         0
      1-Core Ratio             0
  Limit
      2-Core Ratio             0
  Limit
      3-Core Ratio             0
  Limit
      4-Core Ratio             0
  Limit                                              →←: Select Screen
  VR Current value             0                     ↑↓: Select Item
  VR Current value lock        [Enabled]             Enter: Select
  CPU C states                 [Enabled]             +/-: Change Opt.
    Enhanced C1 state          [Enabled]             F1: General Help
    CPU C3 Report              [Enabled]             F2: Previous Values
    CPU C6 report              [Enabled]             F3: Optimized Defaults
      C6 Latency               [Short]               F4: Save & Exit
    CPU C7 report              [CPU C7s]           ▼ ESC: Exit

     Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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



```
     Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
        Advanced

    CPU C6 report              [Enabled]        ▲ Enables or Disables
      C6 Latency               [Short]            Intel(R) TXT(LT)
    CPU C7 report              [CPU C7s]          support.
      C7 Latency               [Long]
    C1 state auto              [Enabled]
  demotion
    C3 state auto              [Enabled]
  demotion
    C1 state auto              [Enabled]
  undemotion
    C3 state auto              [Enabled]          →←: Select Screen
  undemotion                                      ↑↓: Select Item
    C state Pre-Wake           [Enabled]          Enter: Select
  Package C State limit        [AUTO]             +/-: Change Opt.
  LakeTiny Feature             [Disabled]         F1: General Help
  ACPI CTDP BIOS               [Disabled]         F2: Previous Values
  Configurable TDP             [TDP NOMINAL]      F3: Optimized Defaults
  Config TDP LOCK              [Disabled]         F4: Save & Exit
  Intel TXT(LT) Support        [Disabled]       ▼ ESC: Exit

      Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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 it is several different computers, in order to enable several operating systems to run at the same time on the same machine.
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

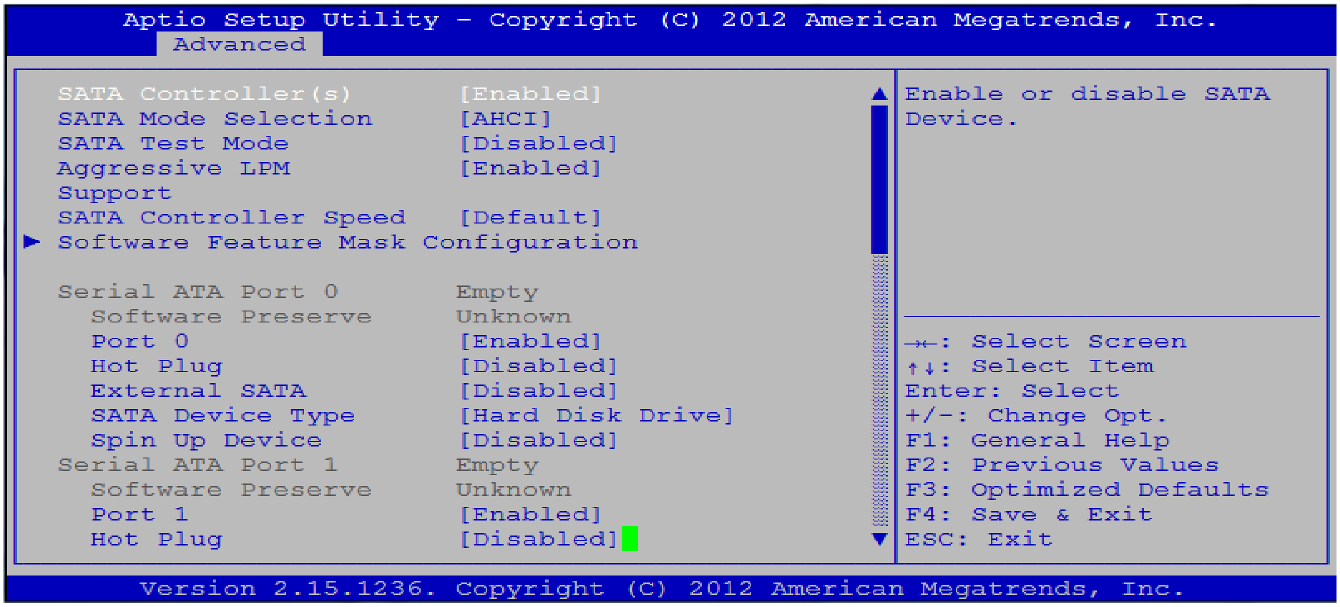
		energy efficiency. The default engages Turbo Boost immediately when possible.
Package power limit lock	*Enabled* *Disabled*	When Enabled, Package_Power_Limit MSR will not locked and a reset will be required to unlock the register.
Cpu Power Limit 1		CPU Power Limit1 value. Default is *0*.
Cpu Power Limit 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*	ACPI T States are a way of clock-gating the computer's cores as a way of cooling the machine when all other methods fail. Intel asserts that T States are no longer

		relevant, and offers a more detailed explanation of T States on their website.
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



```
    Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
           Advanced

   SATA Controller(s)          [Enabled]             Enable or disable SATA
   SATA Mode Selection         [AHCI]                Device.
   SATA Test Mode              [Disabled]
   Aggressive LPM              [Enabled]
   Support
   SATA Controller Speed       [Default]
 ► Software Feature Mask Configuration

   Serial ATA Port 0           Empty
     Software Preserve         Unknown
     Port 0                    [Enabled]             →←: Select Screen
     Hot Plug                  [Disabled]            ↑↓: Select Item
     External SATA             [Disabled]            Enter: Select
     SATA Device Type          [Hard Disk Drive]     +/-: Change Opt.
     Spin Up Device            [Disabled]            F1: General Help
   Serial ATA Port 1           Empty                 F2: Previous Values
     Software Preserve         Unknown               F3: Optimized Defaults
     Port 1                    [Enabled]             F4: Save & Exit
     Hot Plug                  [Disabled]            ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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

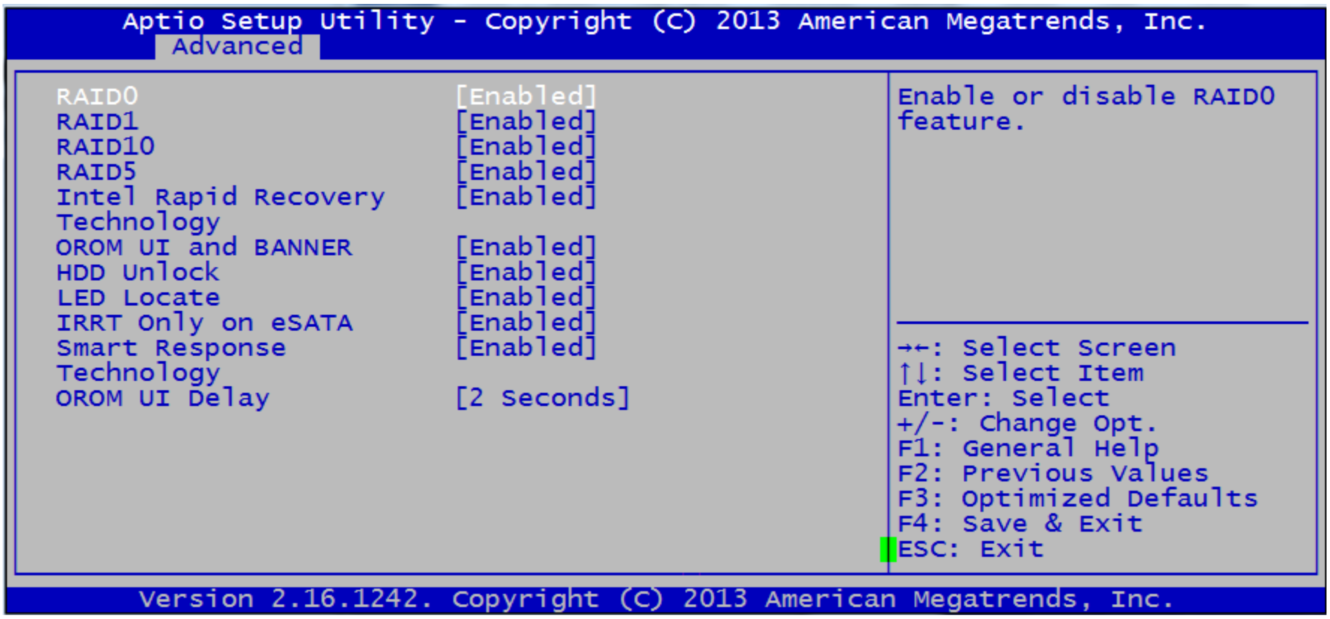
Feature	Options	Description
SATA Controllers(s)	*Enabled* *Disabled*	Enable or Disable the onboard SATA controller.
SATA Mode Selection	*IDE* *AHCI* *RAID*	Determines how SATA controller(s) operate. Please note that modifying this option after installation may require you to reinstall Windows.
SATA Test 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



```
     Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
        Advanced
   RAID0                      [Enabled]        Enable or disable RAID0
   RAID1                      [Enabled]        feature.
   RAID10                     [Enabled]
   RAID5                      [Enabled]
   Intel Rapid Recovery       [Enabled]
   Technology
   OROM UI and BANNER         [Enabled]
   HDD Unlock                 [Enabled]
   LED Locate                 [Enabled]
   IRRT Only on eSATA         [Enabled]
   Smart Response             [Enabled]        →←: Select Screen
   Technology                                  ↑↓: Select Item
   OROM UI Delay              [2 Seconds]      Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit
       Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

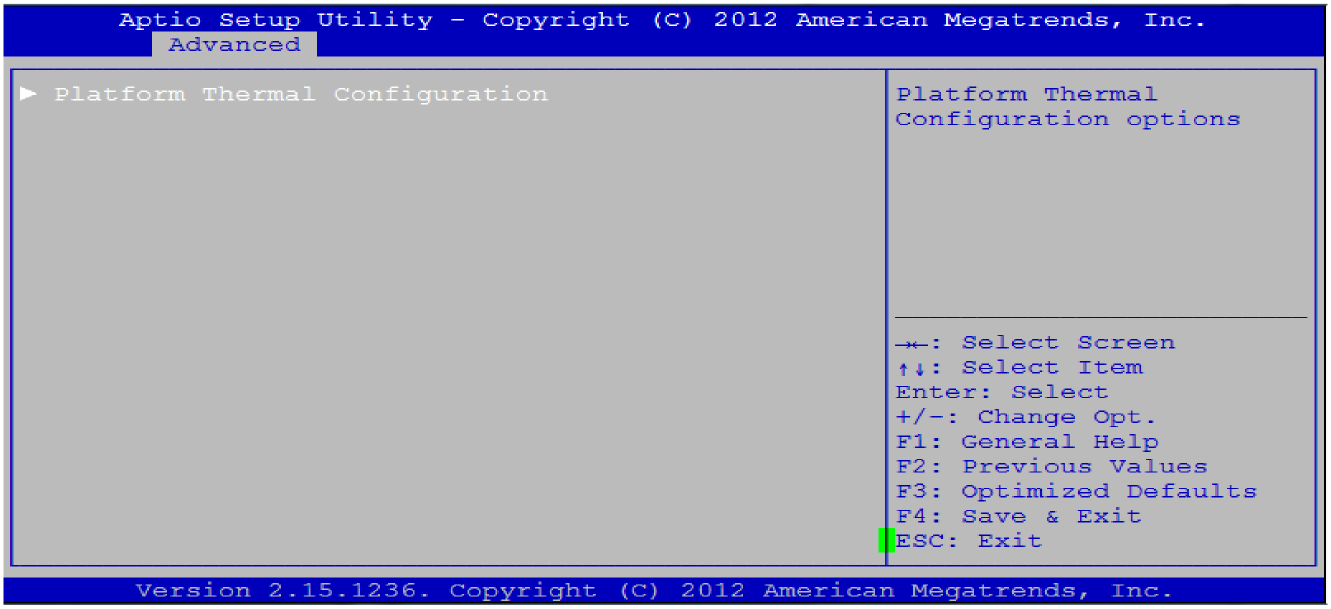
This option allows the user to view and configure the SATA Software Feature Mask Configuration options.

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. .

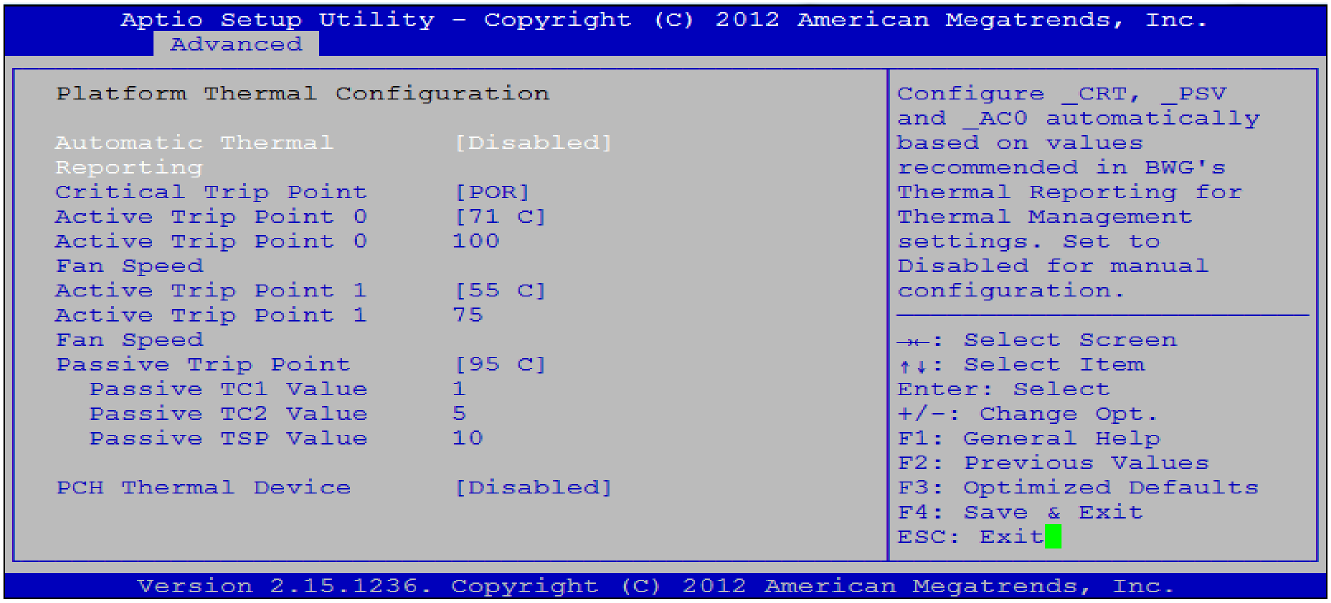
2.2.4 Thermal Configuration

Fig. 2.2.4.a Thermal Configuration



```
        Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
            Advanced
 ► Platform Thermal Configuration                    Platform Thermal
                                                     Configuration options

                                                     →←: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit
         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Fig. 2.2.4.b Platform Thermal Configuration



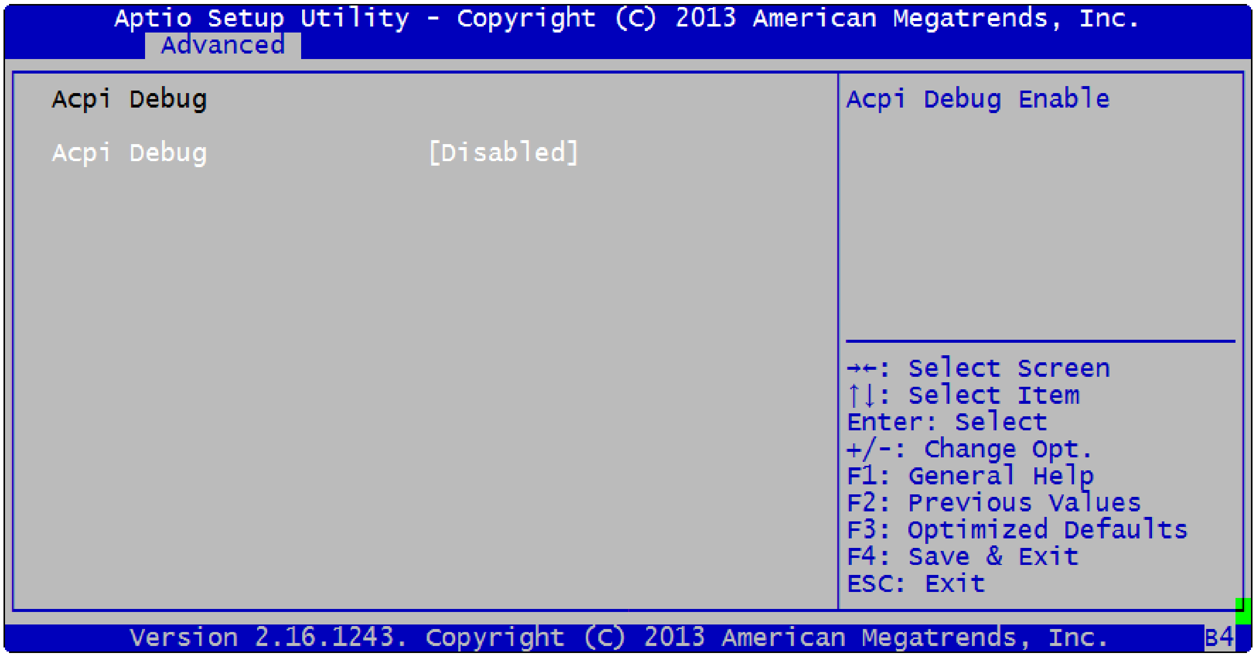
```
        Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
            Advanced
  Platform Thermal Configuration                     Configure _CRT, _PSV
                                                     and _AC0 automatically
  Automatic Thermal           [Disabled]             based on values
  Reporting                                          recommended in BWG's
  Critical Trip Point         [POR]                  Thermal Reporting for
  Active Trip Point 0         [71 C]                 Thermal Management
  Active Trip Point 0         100                    settings. Set to
  Fan Speed                                          Disabled for manual
  Active Trip Point 1         [55 C]                 configuration.
  Active Trip Point 1         75
  Fan Speed                                          →←: Select Screen
  Passive Trip Point          [95 C]                 ↑↓: Select Item
    Passive TC1 Value         1                      Enter: Select
    Passive TC2 Value         5                      +/-: Change Opt.
    Passive TSP Value         10                     F1: General Help
                                                     F2: Previous Values
  PCH Thermal Device          [Disabled]             F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit
         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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

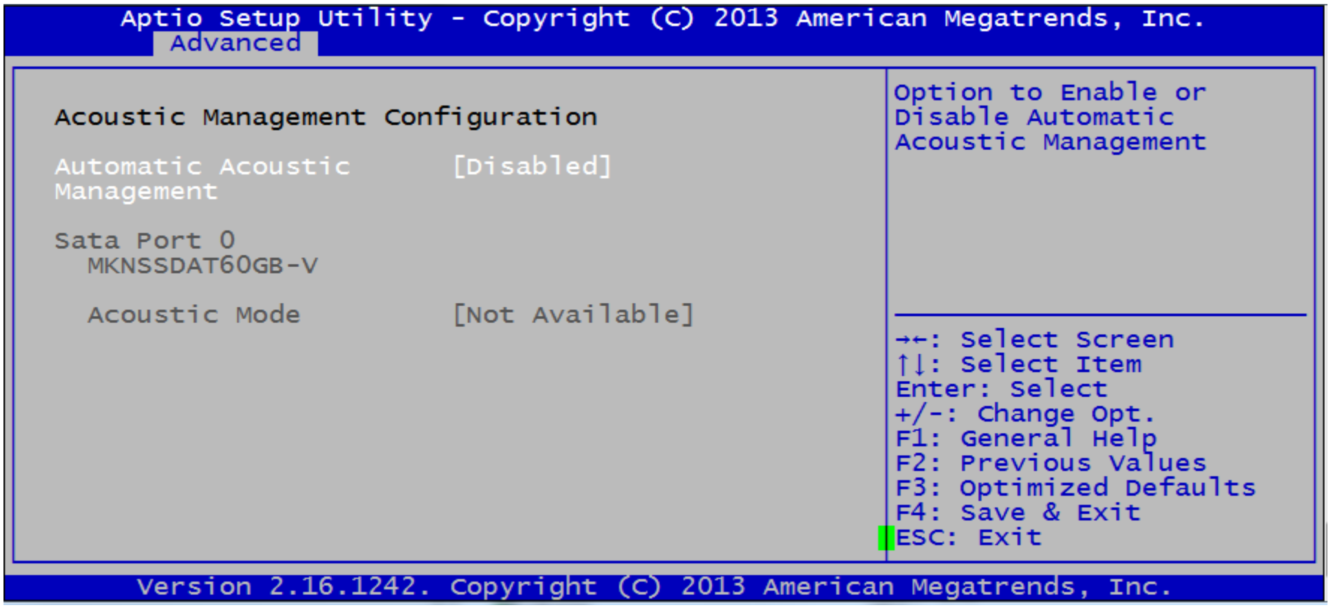
Fig. 2.2.5.a ACPI Debug Configuration



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
  Advanced

Acpi Debug                                  Acpi Debug Enable

Acpi Debug             [Disabled]

                                            →←: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/-: Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F3: Optimized Defaults
                                            F4: Save & Exit
                                            ESC: Exit
     Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.    B4
```

2.2.6 Acoustic Management Technology Configuration

Fig. 2.2.6.a Acoustic Management Technology Configuration

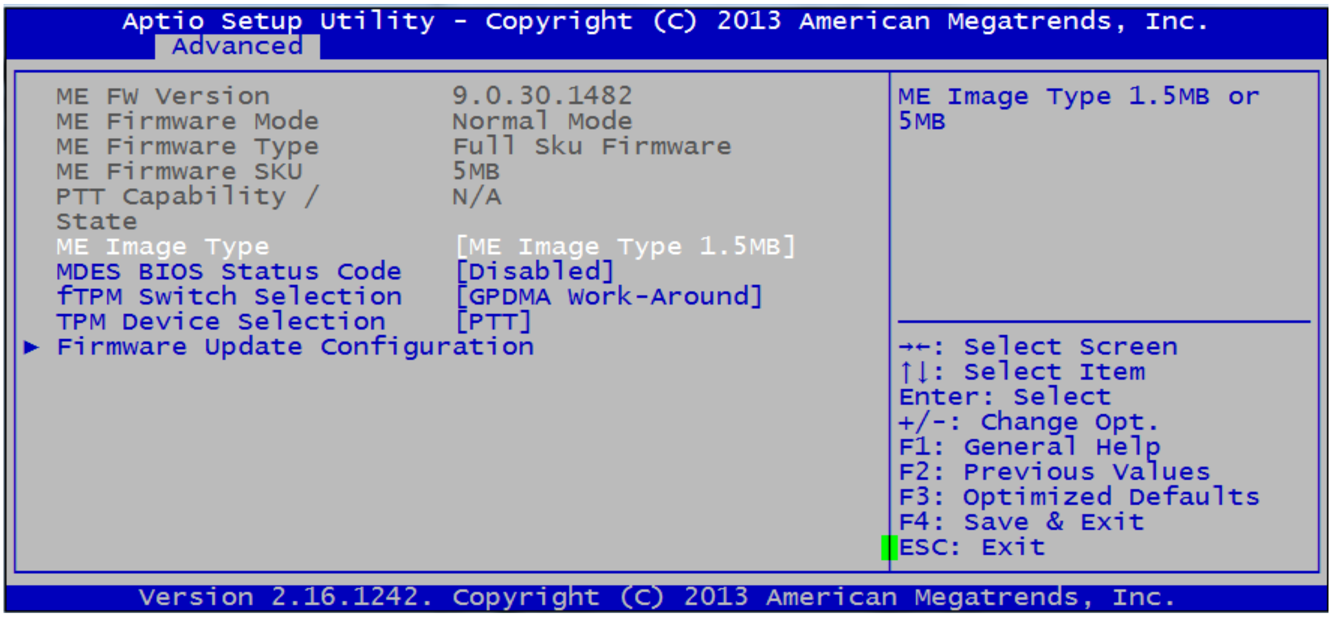


```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
  Advanced

                                            Option to Enable or
Acoustic Management Configuration           Disable Automatic
                                            Acoustic Management
Automatic Acoustic     [Disabled]
Management

Sata Port 0
  MKNSSDAT60GB-V

  Acoustic Mode        [Not Available]
                                            →←: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/-: Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F3: Optimized Defaults
                                            F4: Save & Exit
                                            ESC: Exit
     Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Acoustic management is a form of hard-drive power management that allows for the adjustment of noise, performance, temperature, power requirements, and life expectancy.

2.2.7 PCH-FW Configuration

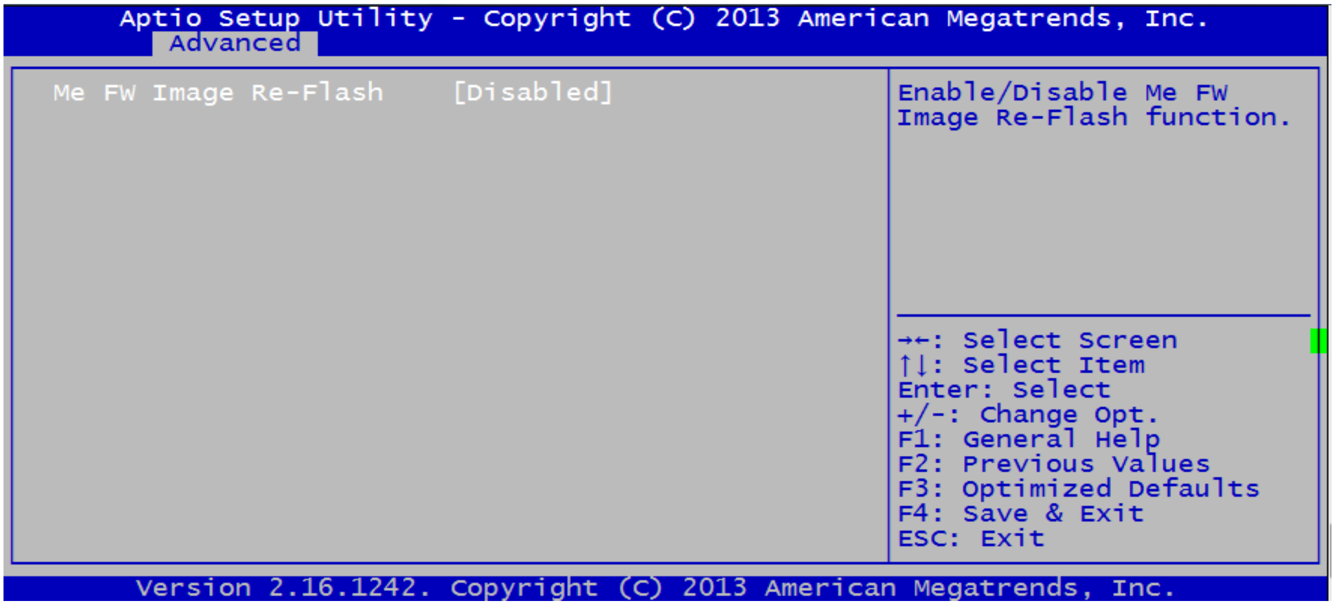
Fig. 2.2.7.a PCH-FW Configuration



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
              Advanced
 ME FW Version              9.0.30.1482               ME Image Type 1.5MB or
 ME Firmware Mode           Normal Mode               5MB
 ME Firmware Type           Full Sku Firmware
 ME Firmware SKU            5MB
 PTT Capability /           N/A
 State
 ME Image Type              [ME Image Type 1.5MB]
 MDES BIOS Status Code      [Disabled]
 fTPM Switch Selection      [GPDMA Work-Around]
 TPM Device Selection       [PTT]
► Firmware Update Configuration
                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
          Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Feature	Options	Description
fTPM Switch Selection		Firmware-based Trusted Platform Module (fTPM). It is a firmware implementation of a TPM chip, which is a microcontroller that stores keys, passwords, and digital certificates for the machine.
TPM Device Selection	PTT dTPM	This option allows the user to select the preferred TPM device: PTT or discrete TPM (dTPM). PTT is the firmware implementation of TPM, and dTPM is the hardware implementation on a chip that is separate from other system elements, which communicates with the system on a dedicated hardware bus.

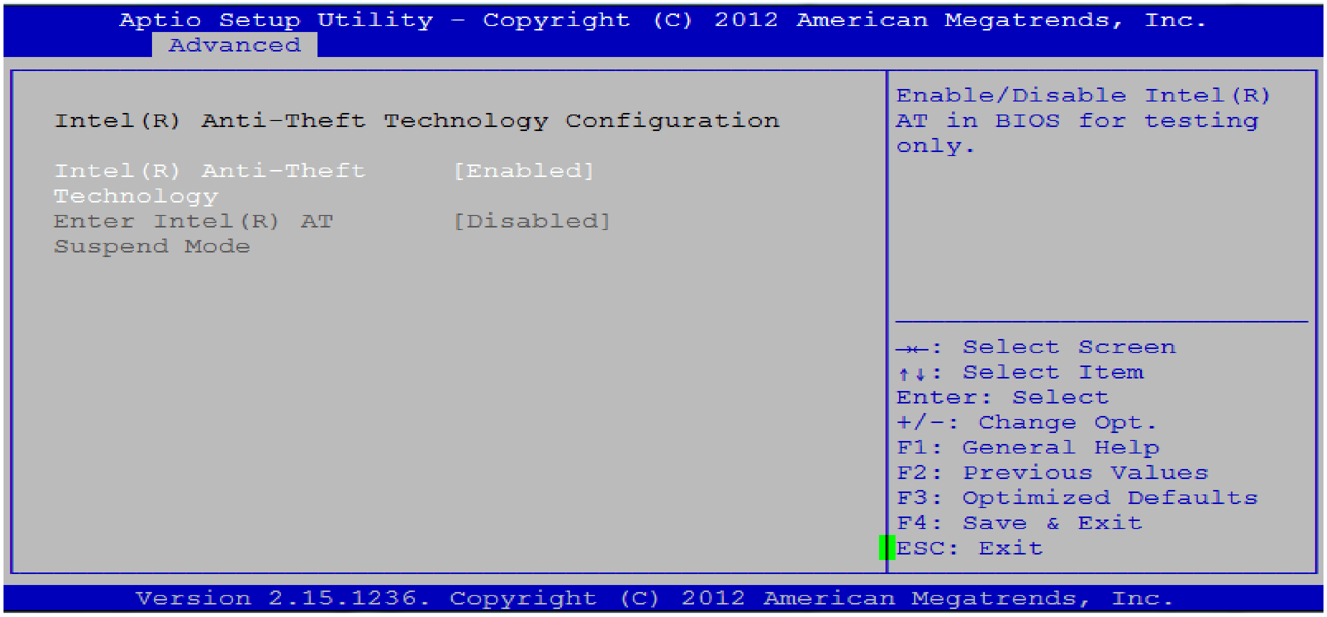
Fig. 2.2.7.b Firmware Update



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
    Advanced

  Me FW Image Re-Flash     [Disabled]          Enable/Disable Me FW
                                               Image Re-Flash function.

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

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

2.2.8 Intel® Anti-Theft Technology Configuration

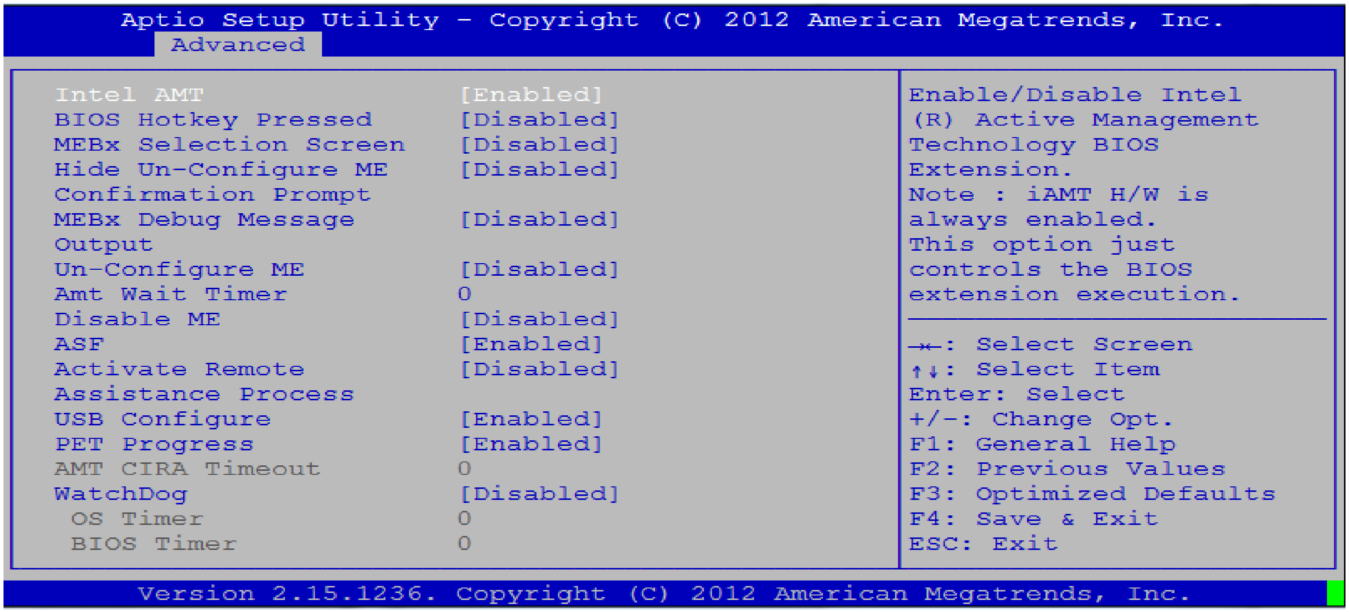
Fig. 2.2.8.a Intel® Anti-Theft Technology Configuration



```
Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
Advanced

Intel(R) Anti-Theft Technology Configuration

Intel(R) Anti-Theft         [Enabled]
Technology
Enter Intel(R) AT           [Disabled]
Suspend Mode

Enable/Disable Intel(R)
AT in BIOS for testing
only.

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

Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.2.9 AMT Configuration

Fig. 2.2.9.a AMT Configuration



```
       Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
          Advanced

  Intel AMT                 [Enabled]          Enable/Disable Intel
  BIOS Hotkey Pressed       [Disabled]         (R) Active Management
  MEBx Selection Screen     [Disabled]         Technology BIOS
  Hide Un-Configure ME      [Disabled]         Extension.
  Confirmation Prompt                          Note : iAMT H/W is
  MEBx Debug Message        [Disabled]         always enabled.
  Output                                       This option just
  Un-Configure ME           [Disabled]         controls the BIOS
  Amt Wait Timer            0                  extension execution.
  Disable ME                [Disabled]
  ASF                       [Enabled]          →←: Select Screen
  Activate Remote           [Disabled]         ↑↓: Select Item
  Assistance Process                           Enter: Select
  USB Configure             [Enabled]          +/-: Change Opt.
  PET Progress              [Enabled]          F1: General Help
  AMT CIRA Timeout          0                  F2: Previous Values
  WatchDog                  [Disabled]         F3: Optimized Defaults
   OS Timer                 0                  F4: Save & Exit
   BIOS Timer               0                  ESC: Exit

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

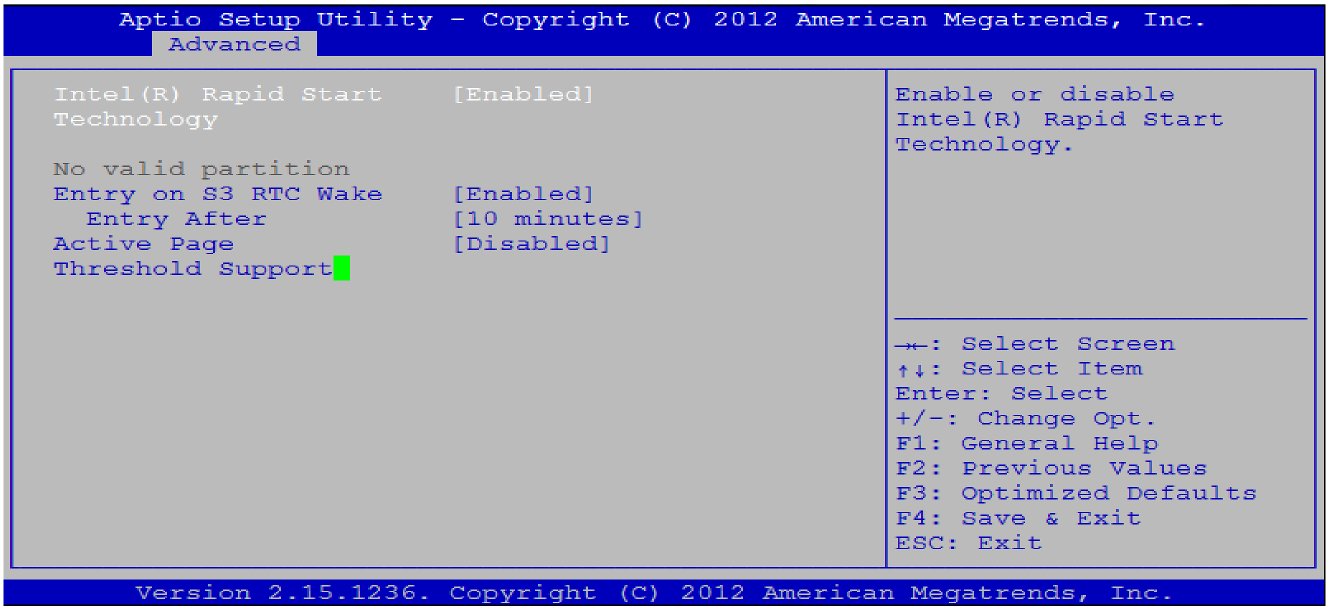
This option allows the user to view and configure the Intel Activate Management Technology (AMT) parameters.

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

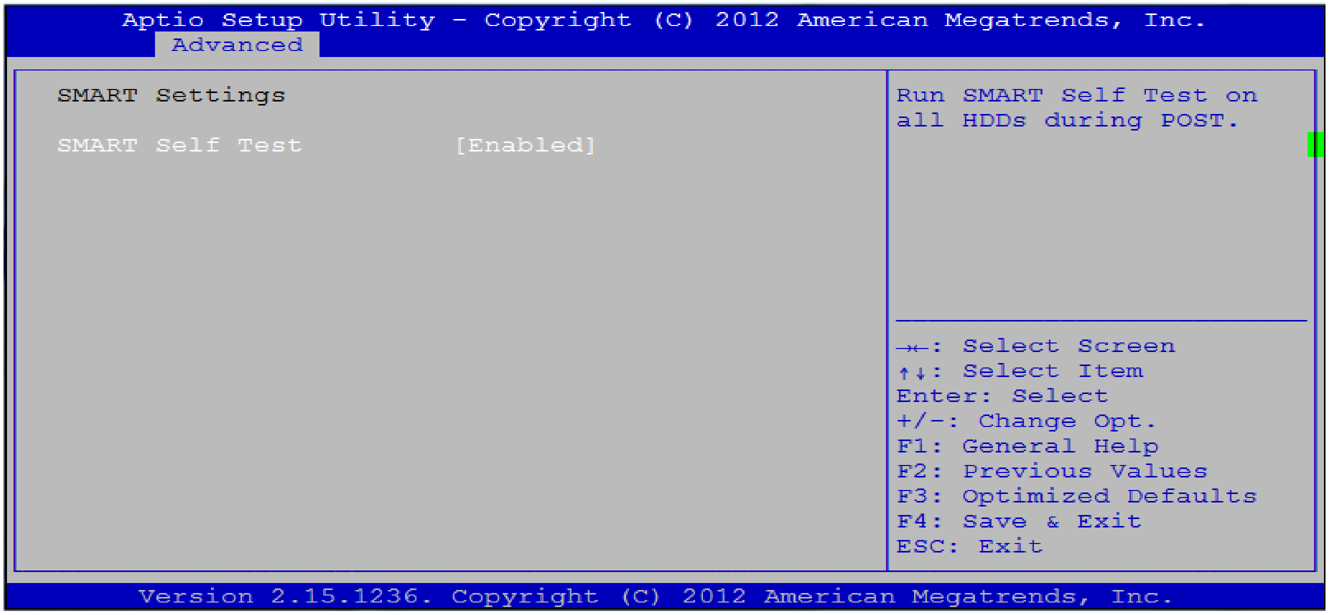
Fig. 2.2.10.a Intel® Rapid Start Technology



```
          Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
           Advanced
  Intel(R) Rapid Start        [Enabled]                 Enable or disable
  Technology                                            Intel(R) Rapid Start
                                                        Technology.
  No valid partition
  Entry on S3 RTC Wake        [Enabled]
    Entry After               [10 minutes]
  Active Page                 [Disabled]
  Threshold Support

                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/-: Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F3: Optimized Defaults
                                                        F4: Save & Exit
                                                        ESC: Exit
           Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.2.11 Smart Settings

Fig. 2.2.11.a Smart Settings

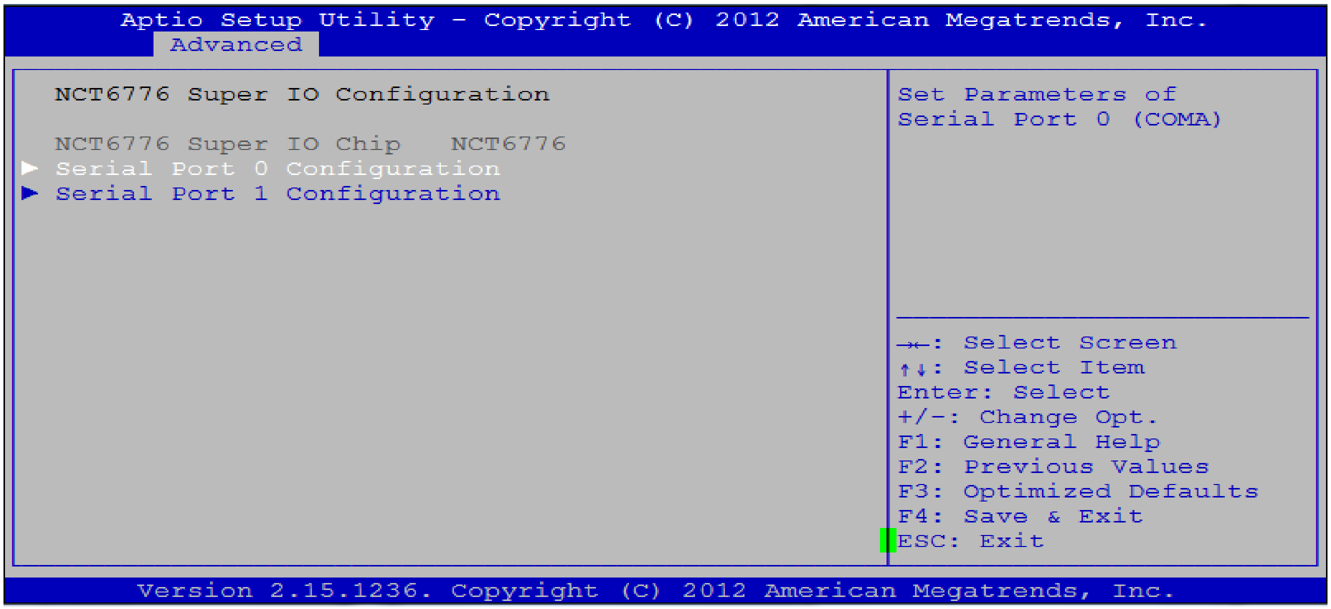


```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
    Advanced

  SMART Settings                          Run SMART Self Test on
                                          all HDDs during POST.
  SMART Self Test          [Enabled]

                                          →←: Select Screen
                                          ↑↓: Select Item
                                          Enter: Select
                                          +/-: Change Opt.
                                          F1: General Help
                                          F2: Previous Values
                                          F3: Optimized Defaults
                                          F4: Save & Exit
                                          ESC: Exit
   Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

SMART stands for Self-Monitoring, Analysis and Reporting Technology. SMART keeps track of hard-drive stats in an attempt to anticipate hard drive hardware failure. The SMART Self-Test checks up on the recorded data levels, and provides an on-demand overview of the drive's health.

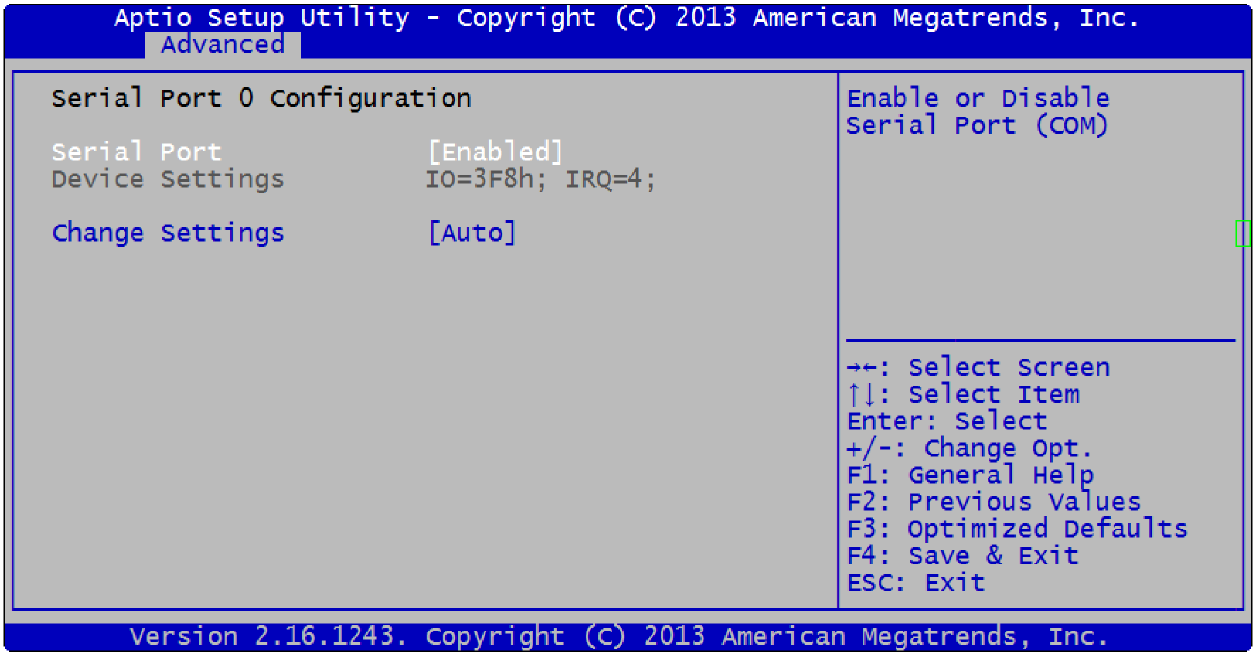
2.2.12 NCT6776 Super IO Configuration

Fig. 2.2.12.a NCT6776 Super IO Configuration



```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
    Advanced

  NCT6776 Super IO Configuration          Set Parameters of
                                          Serial Port 0 (COMA)
  NCT6776 Super IO Chip   NCT6776
► Serial Port 0 Configuration
► Serial Port 1 Configuration

                                          →←: Select Screen
                                          ↑↓: Select Item
                                          Enter: Select
                                          +/-: Change Opt.
                                          F1: General Help
                                          F2: Previous Values
                                          F3: Optimized Defaults
                                          F4: Save & Exit
                                          ESC: Exit
   Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Fig. 2.2.12.b Serial Port 0 Configuration

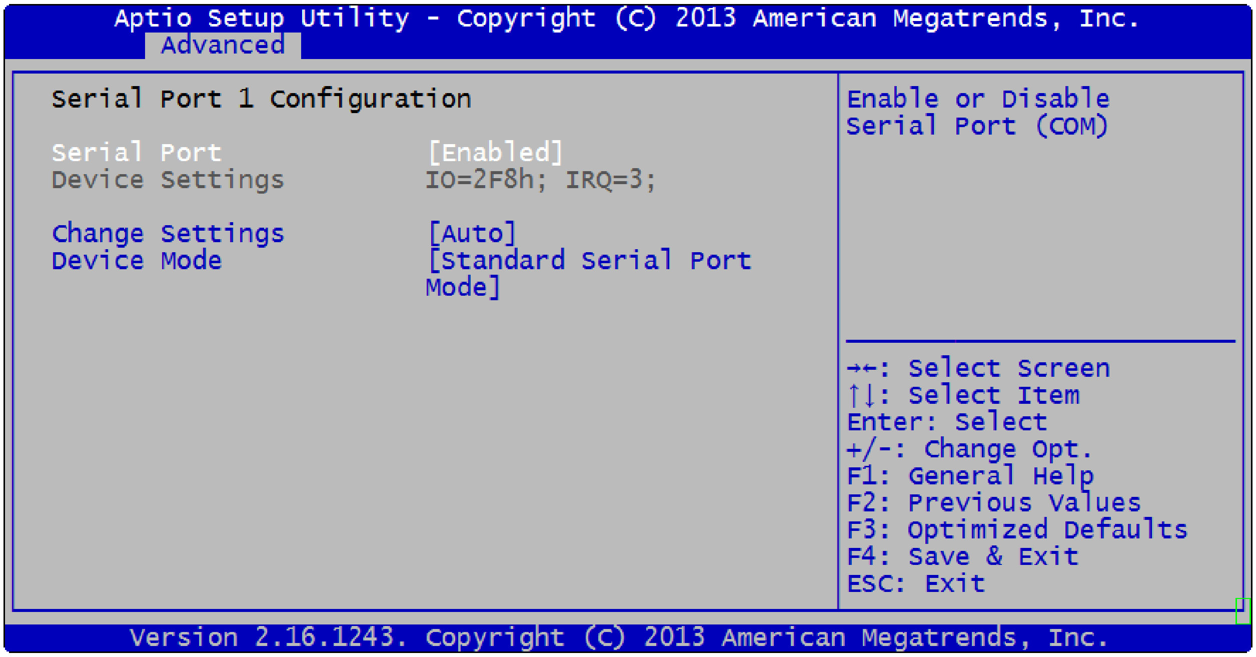


```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
              Advanced
  Serial Port 0 Configuration                          Enable or Disable
                                                       Serial Port (COM)
  Serial Port                 [Enabled]
  Device Settings             IO=3F8h; IRQ=4;

  Change Settings             [Auto]



                                                       →←: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit
        Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

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



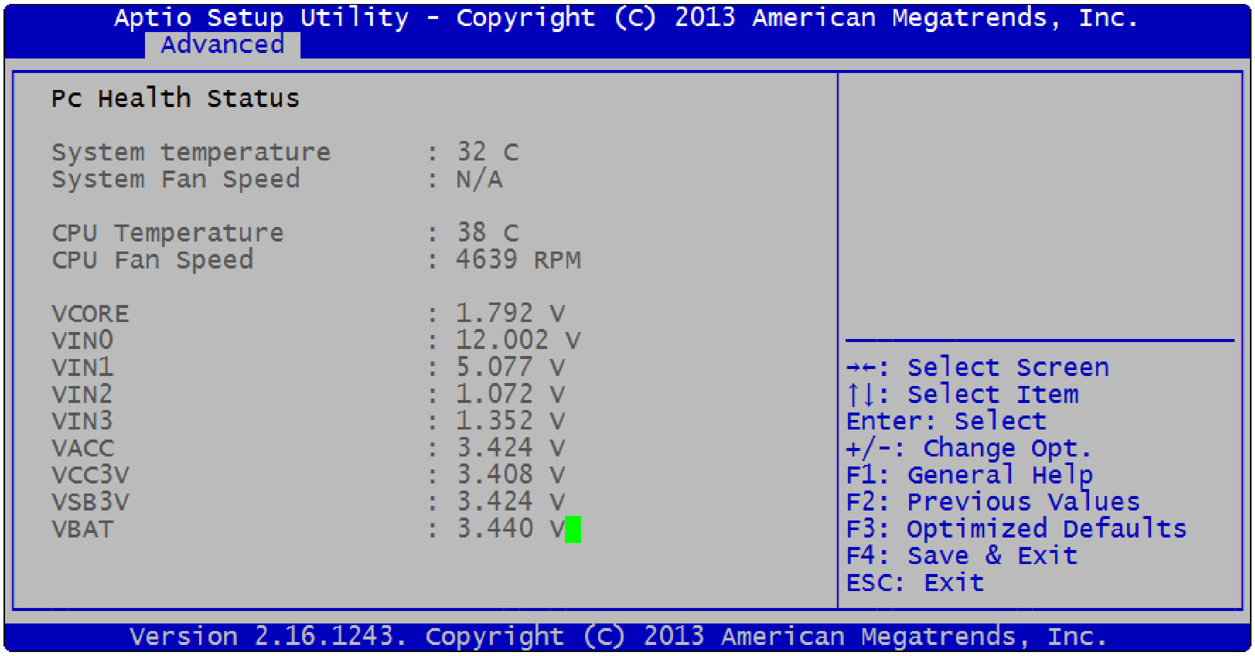
```
         Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                Advanced
  Serial Port 1 Configuration                          Enable or Disable
                                                       Serial Port (COM)
  Serial Port                  [Enabled]
  Device Settings              IO=2F8h; IRQ=3;

  Change Settings              [Auto]
  Device Mode                  [Standard Serial Port
                               Mode]
                                                       →←: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit
      Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

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



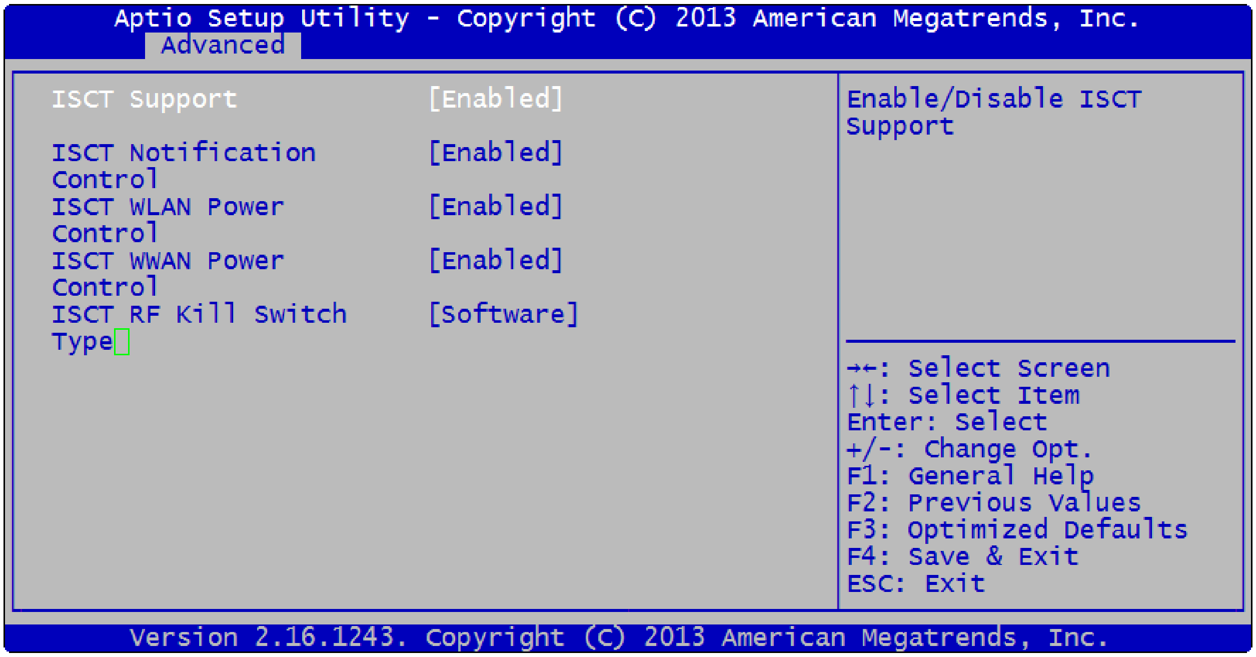
```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
           Advanced
  Pc Health Status

  System temperature        : 32 C
  System Fan Speed          : N/A

  CPU Temperature           : 38 C
  CPU Fan Speed             : 4639 RPM

  VCORE                     : 1.792 V
  VIN0                      : 12.002 V
  VIN1                      : 5.077 V          →←: Select Screen
  VIN2                      : 1.072 V          ↑↓: Select Item
  VIN3                      : 1.352 V          Enter: Select
  VACC                      : 3.424 V          +/-: Change Opt.
  VCC3V                     : 3.408 V          F1: General Help
  VSB3V                     : 3.424 V          F2: Previous Values
  VBAT                      : 3.440 V          F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit
         Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

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

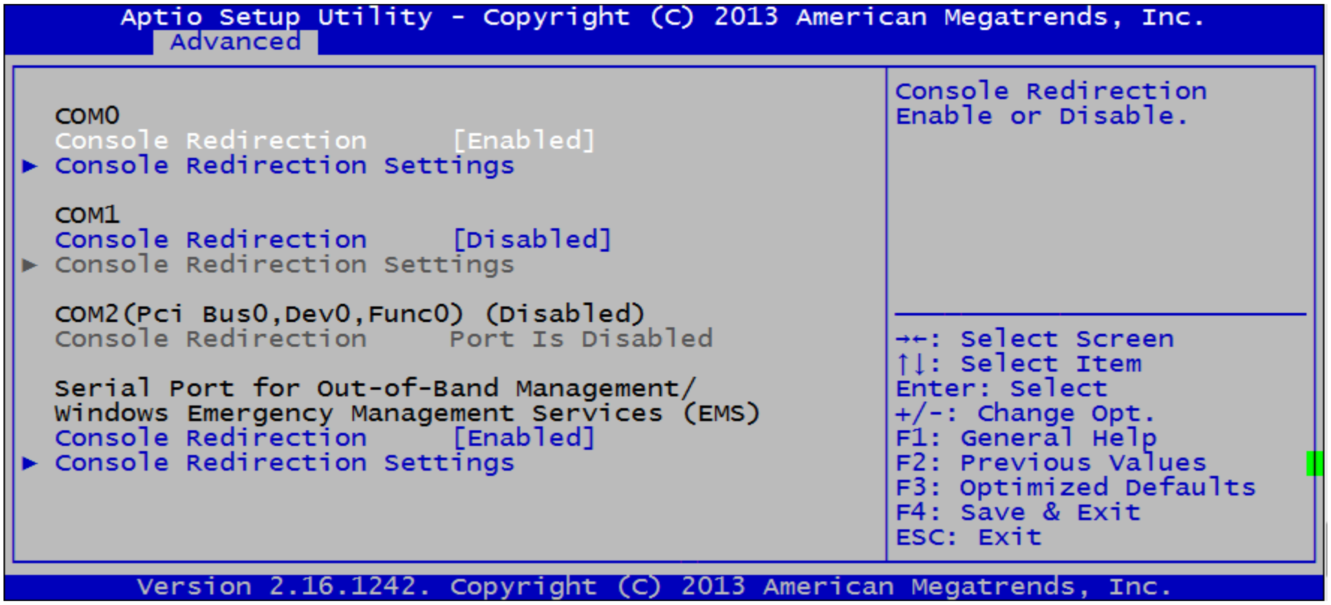


```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
         Advanced

  ISCT Support                [Enabled]          Enable/Disable ISCT
                                                 Support
  ISCT Notification           [Enabled]
  Control
  ISCT WLAN Power             [Enabled]
  Control
  ISCT WWAN Power             [Enabled]
  Control
  ISCT RF Kill Switch         [Software]
  Type
                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

        Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

Intel Smart Connect Technology (ISCT) is a feature designed to periodically wake the computer from sleep or standby mode so that certain programs and features can update themselves automatically.

2.2.15 Serial Port Console Redirection

Fig. 2.2.15.a Serial Port Console Redirection

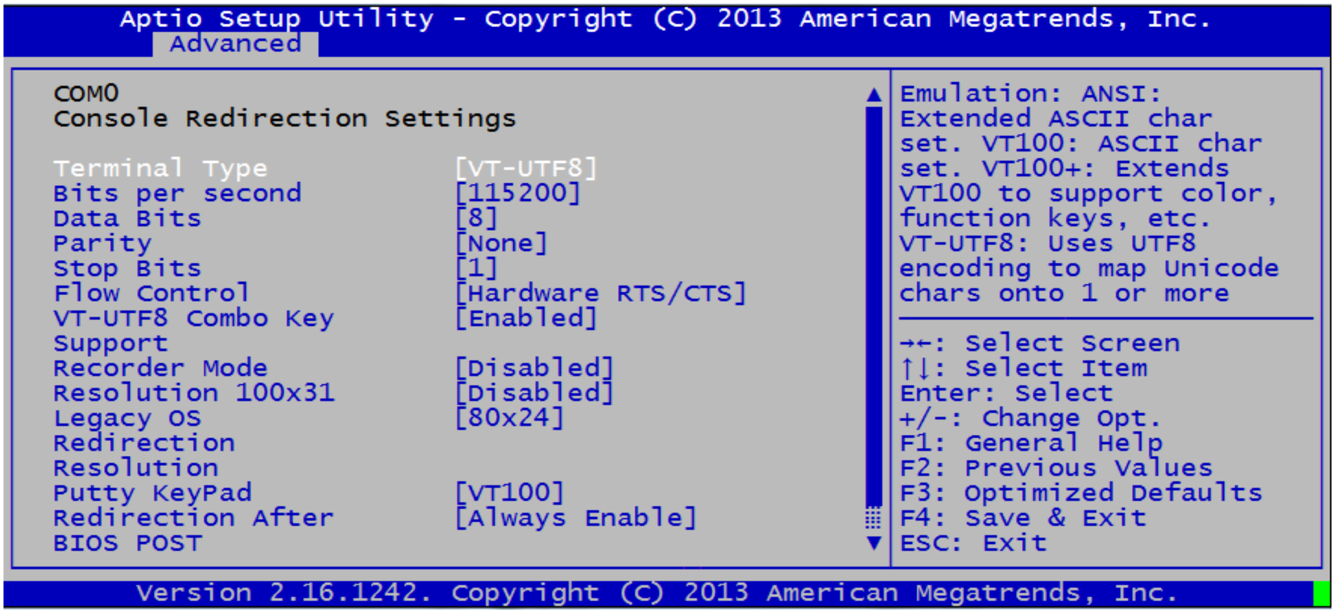


```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
         Advanced

                                                   Console Redirection
   COM0                                            Enable or Disable.
   Console Redirection       [Enabled]
 ► Console Redirection Settings

   COM1
   Console Redirection       [Disabled]
 ► Console Redirection Settings

   COM2(Pci Bus0,Dev0,Func0) (Disabled)
   Console Redirection       Port Is Disabled      →←: Select Screen
                                                   ↑↓: Select Item
   Serial Port for Out-of-Band Management/         Enter: Select
   Windows Emergency Management Services (EMS)     +/-: Change Opt.
   Console Redirection       [Enabled]             F1: General Help
 ► Console Redirection Settings                    F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Serial Port Console Redirection allows a user to remotely control the computer's keyboard and mouse through the computer's serial port.

2.2.15.1 Console Redirection Settings

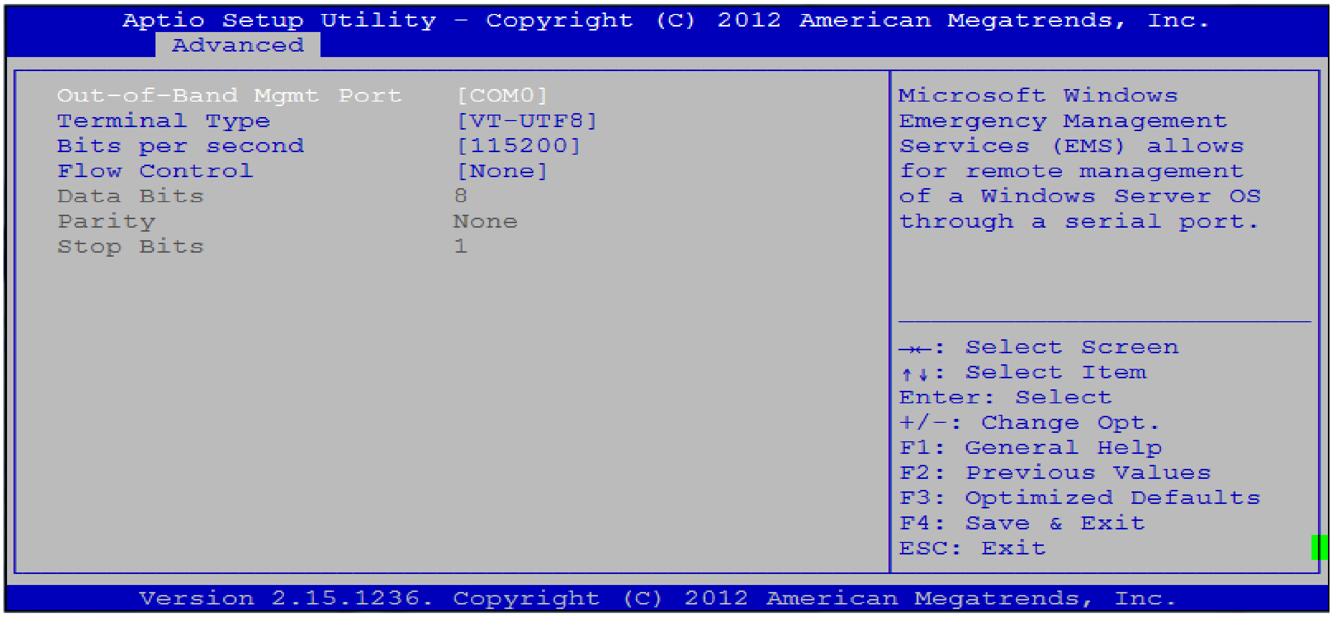
Fig. 2.2.15.1.a Console Redirection Settings (Screen 1 of 2)



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
          Advanced

  COM0                                             Emulation: ANSI:
  Console Redirection Settings                     Extended ASCII char
                                                   set. VT100: ASCII char
  Terminal Type               [VT-UTF8]            set. VT100+: Extends
  Bits per second             [115200]             VT100 to support color,
  Data Bits                   [8]                  function keys, etc.
  Parity                      [None]               VT-UTF8: Uses UTF8
  Stop Bits                   [1]                  encoding to map Unicode
  Flow Control                [Hardware RTS/CTS]   chars onto 1 or more
  VT-UTF8 Combo Key           [Enabled]
  Support                                          →←: Select Screen
  Recorder Mode               [Disabled]           ↑↓: Select Item
  Resolution 100x31           [Disabled]           Enter: Select
  Legacy OS                   [80x24]              +/-: Change Opt.
  Redirection                                      F1: General Help
  Resolution                                       F2: Previous Values
  Putty KeyPad                [VT100]              F3: Optimized Defaults
  Redirection After           [Always Enable]      F4: Save & Exit
  BIOS POST                                        ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The options include Enable/Disable for each COM port.

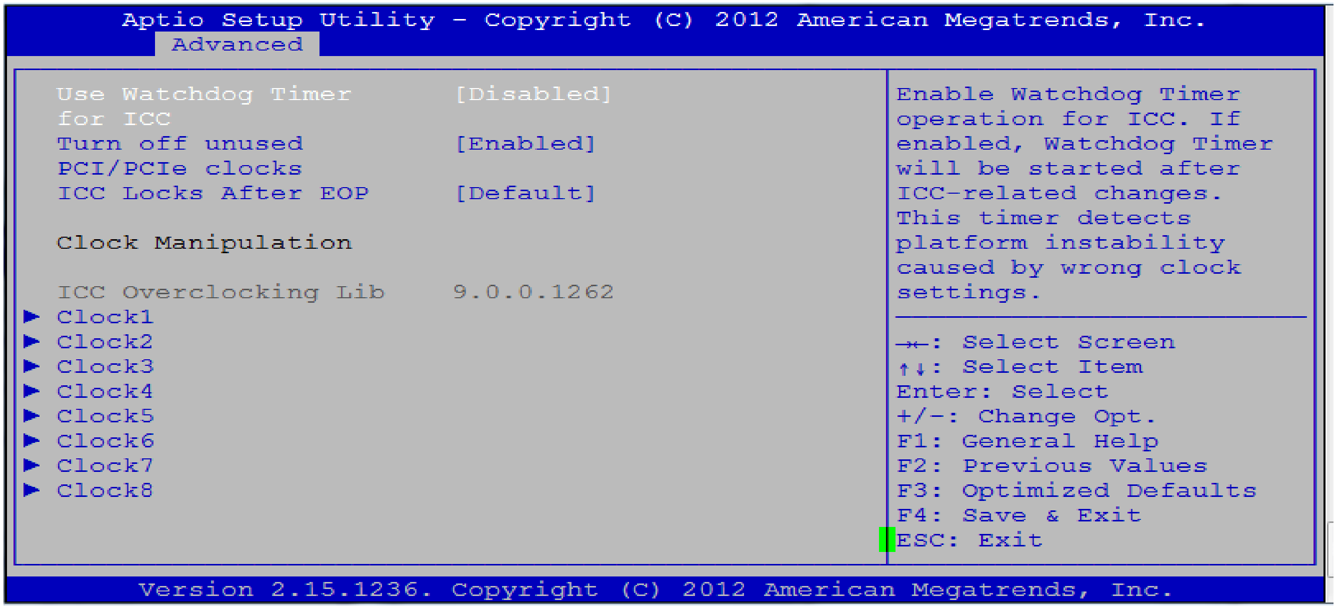
Fig. 2.2.15.1.b Console Redirection Settings (Screen 2 of 2)



```
        Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
          Advanced

  Out-of-Band Mgmt Port       [COM0]               Microsoft Windows
  Terminal Type               [VT-UTF8]            Emergency Management
  Bits per second             [115200]             Services (EMS) allows
  Flow Control                [None]               for remote management
  Data Bits                   8                    of a Windows Server OS
  Parity                      None                 through a serial port.
  Stop Bits                   1


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

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.2.16 Intel® ICC (Watchdog Timer)

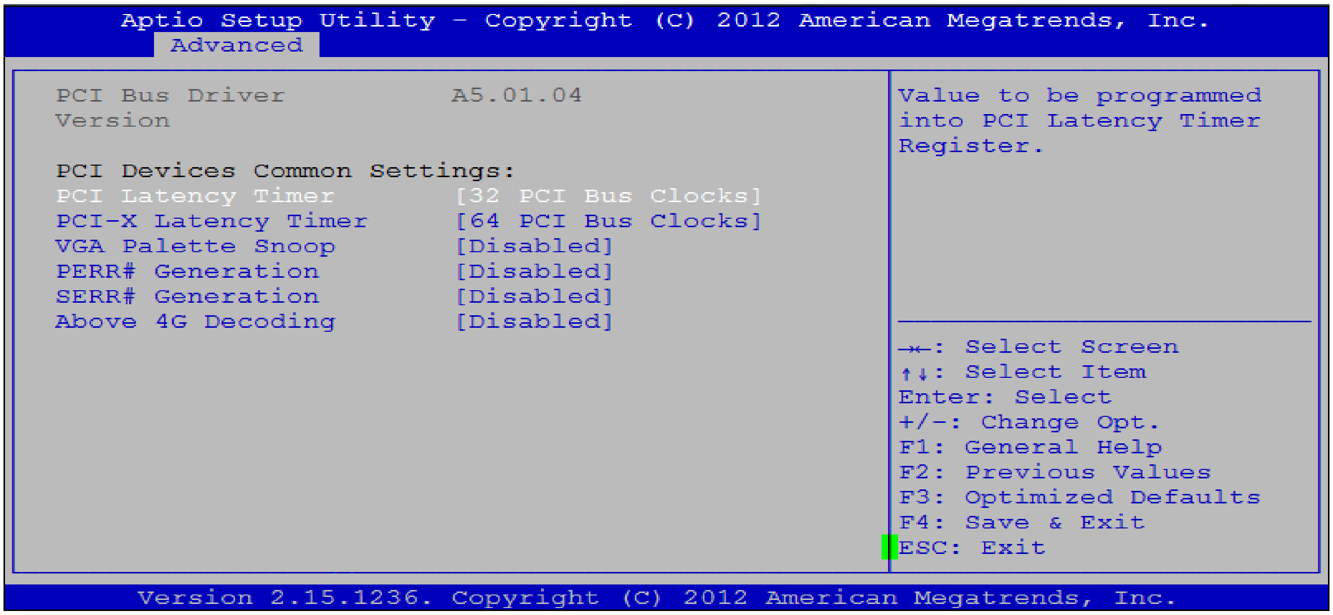
Fig. 2.2.16.a Intel® ICC (Watchdog Timer)



```
    Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
        Advanced
  Use Watchdog Timer          [Disabled]      Enable Watchdog Timer
  for ICC                                     operation for ICC. If
  Turn off unused             [Enabled]       enabled, Watchdog Timer
  PCI/PCIe clocks                             will be started after
  ICC Locks After EOP         [Default]       ICC-related changes.
                                              This timer detects
  Clock Manipulation                          platform instability
                                              caused by wrong clock
  ICC Overclocking Lib        9.0.0.1262      settings.
▶ Clock1                                      -------------------------
▶ Clock2                                      →←: Select Screen
▶ Clock3                                      ↑↓: Select Item
▶ Clock4                                      Enter: Select
▶ Clock5                                      +/-: Change Opt.
▶ Clock6                                      F1: General Help
▶ Clock7                                      F2: Previous Values
▶ Clock8                                      F3: Optimized Defaults
                                              F4: Save & Exit
                                              ESC: Exit
    Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.2.17 PCI Subsystem Settings

Fig. 2.2.17.a PCI Subsystem Settings



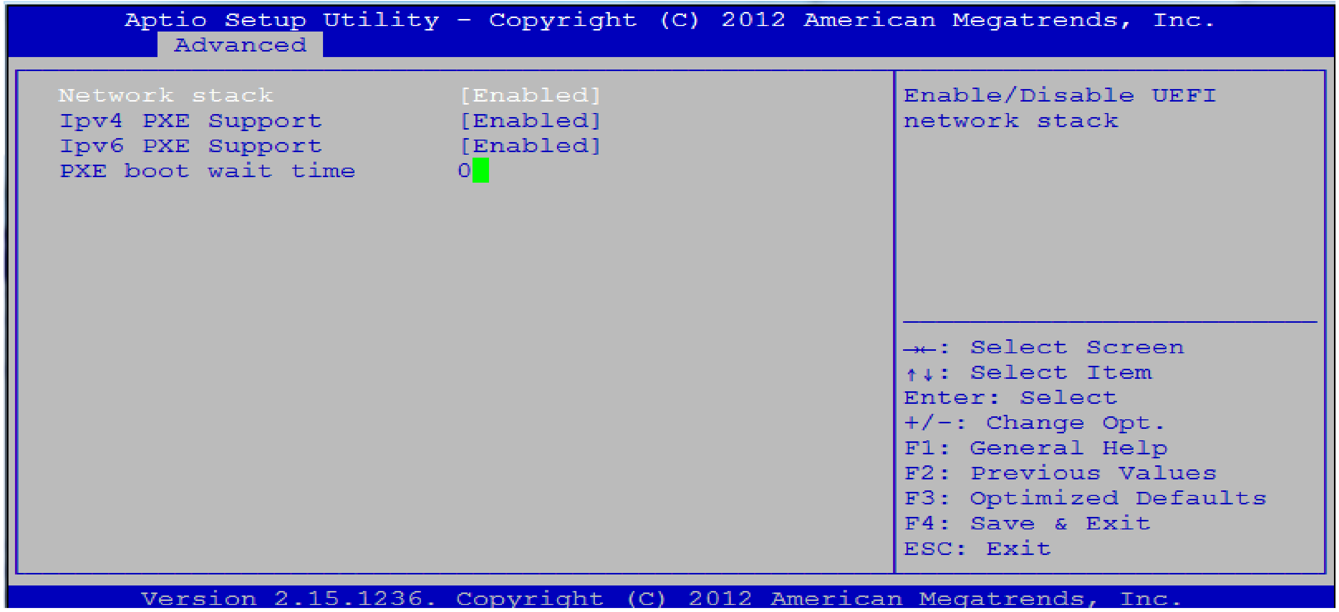
```
    Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
        Advanced
  PCI Bus Driver              A5.01.04            Value to be programmed
  Version                                         into PCI Latency Timer
                                                  Register.
  PCI Devices Common Settings:
  PCI Latency Timer           [32 PCI Bus Clocks]
  PCI-X Latency Timer         [64 PCI Bus Clocks]
  VGA Palette Snoop           [Disabled]
  PERR# Generation            [Disabled]
  SERR# Generation            [Disabled]
  Above 4G Decoding           [Disabled]
                                                  -------------------------
                                                  →←: Select Screen
                                                  ↑↓: Select Item
                                                  Enter: Select
                                                  +/-: Change Opt.
                                                  F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit
    Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.2.18 AMI Graphic Output Protocol Policy

Feature	Options	Description
AMI Graphic Output Protocol Policy		When outputting graphics, and there are multiple graphics devices, secify a device order, a brightness setting, and enable or disable the Built-In Self Test (BIST)

2.2.19 Network Stack

Fig. 2.2.18.a Network Stack



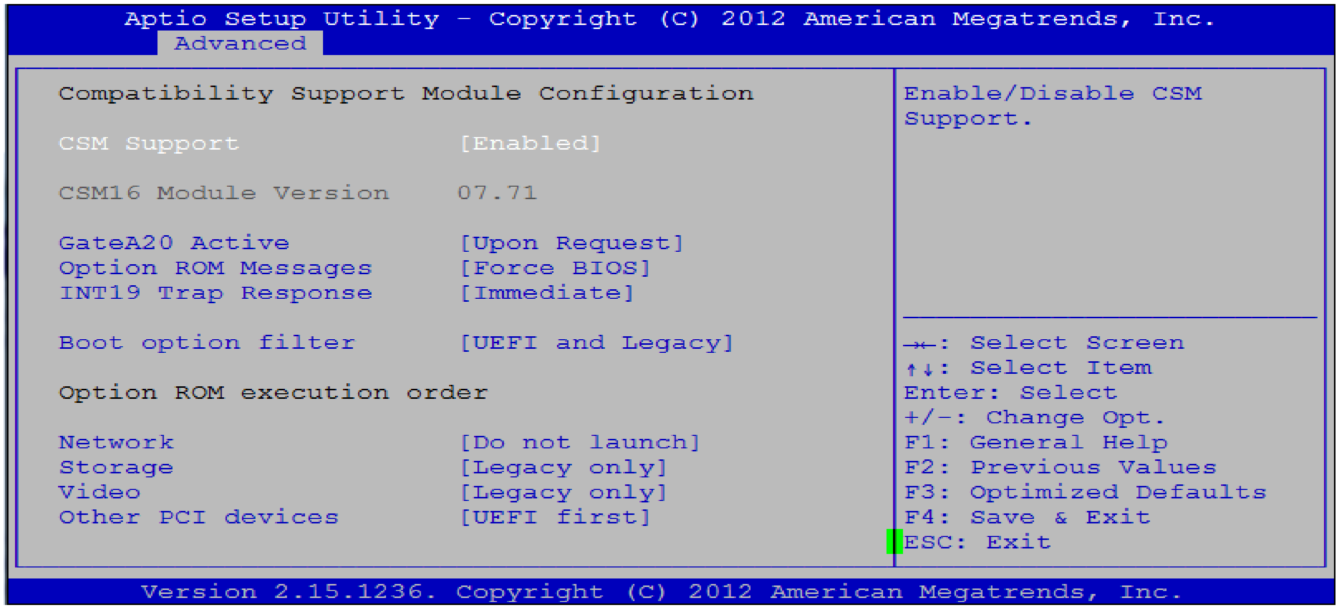
```
        Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
           Advanced

   Network stack              [Enabled]            Enable/Disable UEFI
   Ipv4 PXE Support           [Enabled]            network stack
   Ipv6 PXE Support           [Enabled]
   PXE boot wait time         0




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

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

PXE stands for Preboot Execution Environment. PXE allows networked computers to be configured and booted remotely via Ethernet before their Operating System is booted.

Feature	Options	Description
IPv4 PXE Support	*Enabled* *Disabled*	This option, when enabled, allows for PXE booting via IPv4.
IPv6 PXE Support	*Enabled* *Disabled*	This option, when enabled, allows for PXE booting via IPv6.
PXE Boot Wait Time		This specifies how long this remote (client) computer will delay before accepting PXE boot requests from the server.

2.2.20 Compatibility Support Mode (CSM) Configuration

Fig. 2.2.20.a CSM Configuration



```
         Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
               Advanced

   Compatibility Support Module Configuration               Enable/Disable CSM
                                                            Support.
   CSM Support                 [Enabled]

   CSM16 Module Version        07.71

   GateA20 Active              [Upon Request]
   Option ROM Messages         [Force BIOS]
   INT19 Trap Response         [Immediate]

   Boot option filter          [UEFI and Legacy]            →←: Select Screen
                                                            ↑↓: Select Item
   Option ROM execution order                               Enter: Select
                                                            +/-: Change Opt.
   Network                     [Do not launch]              F1: General Help
   Storage                     [Legacy only]                F2: Previous Values
   Video                       [Legacy only]                F3: Optimized Defaults
   Other PCI devices           [UEFI first]                 F4: Save & Exit
                                                            ESC: Exit

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

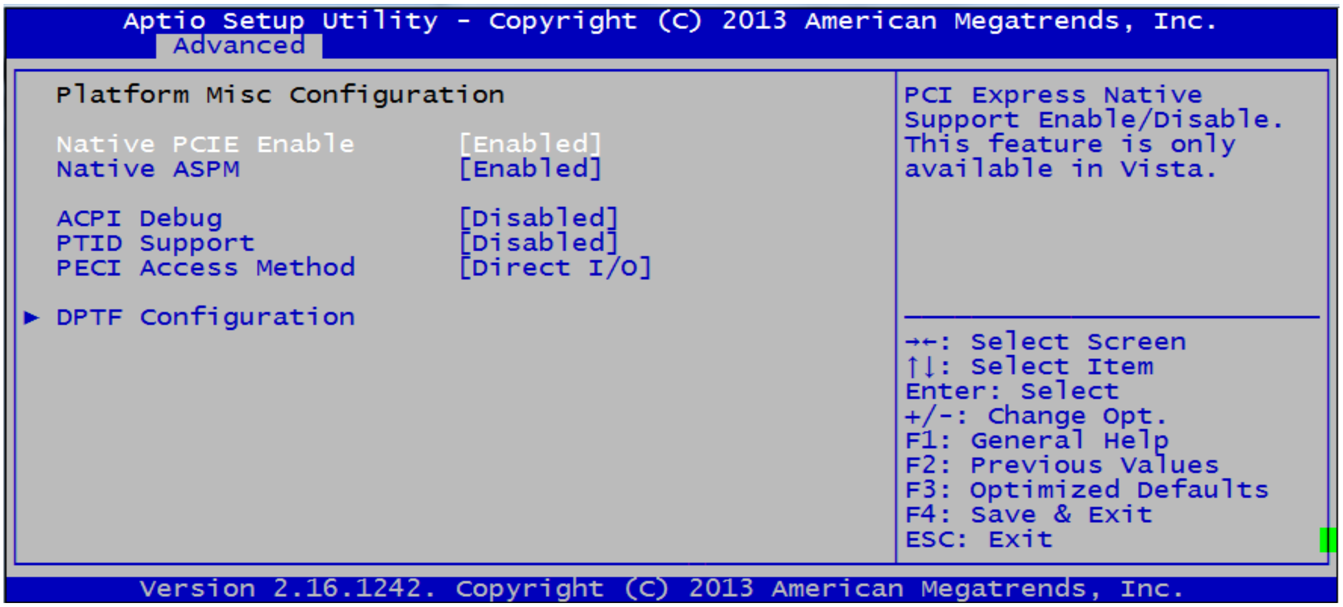
This option allows the user to view and configure the Compatibility Support Mode (CSM) Configuration.

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.

2.2.21 Platform Miscellaneous Configuration

Fig. 2.2.21.a Platform Miscellaneous Configuration



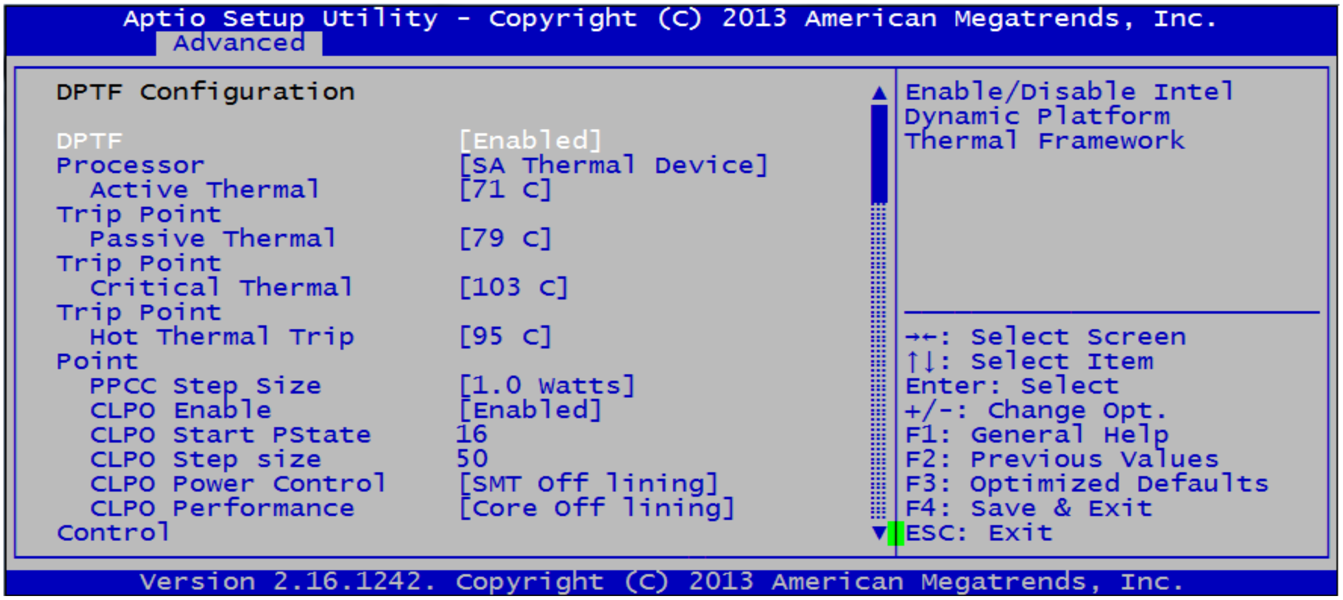
```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
         Advanced
   Platform Misc Configuration                        PCI Express Native
                                                      Support Enable/Disable.
   Native PCIE Enable          [Enabled]              This feature is only
   Native ASPM                 [Enabled]              available in Vista.

   ACPI Debug                  [Disabled]
   PTID Support                [Disabled]
   PECI Access Method          [Direct I/O]

 ► DPTF Configuration
                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The options in this menu allow users to configure the platform-related features.

Feature	Options	Description
Native PCIe Enable		Enabling this provides native support for PCIe. This feature is only available in Windows Vista.
Native ASPM		When enabled, Windows Vista will control the Active State Power Management (ASPM), when disabled, BIOS controls it.
ACPI Debug		This option opens a memory buffer for storing debug strings, and uses the Advanced Configuration and Power Interface (ACPI) debug method to write strings to the buffer.
PTID Support		Enable/Disable the Power and Temperature Instrumentation Details SSDT table in ACPI.

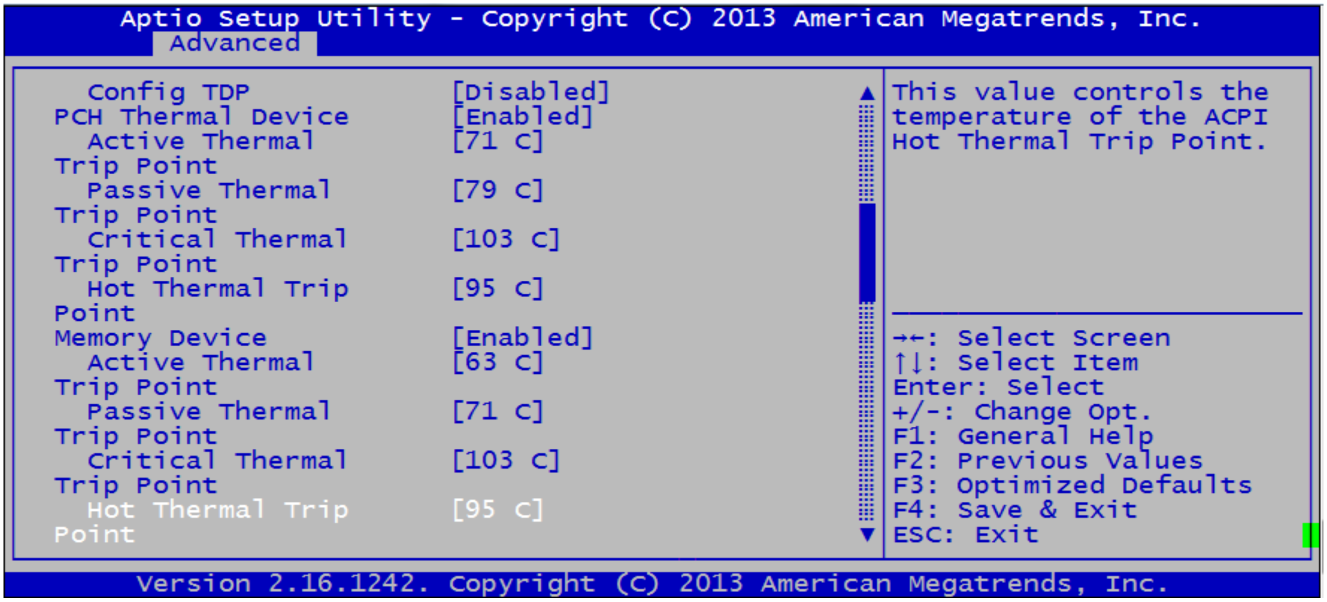
2.2.21.1 DPTF Configuration

Fig. 2.2.21.1.a DPTF Configuration (Screen 1 of 5)



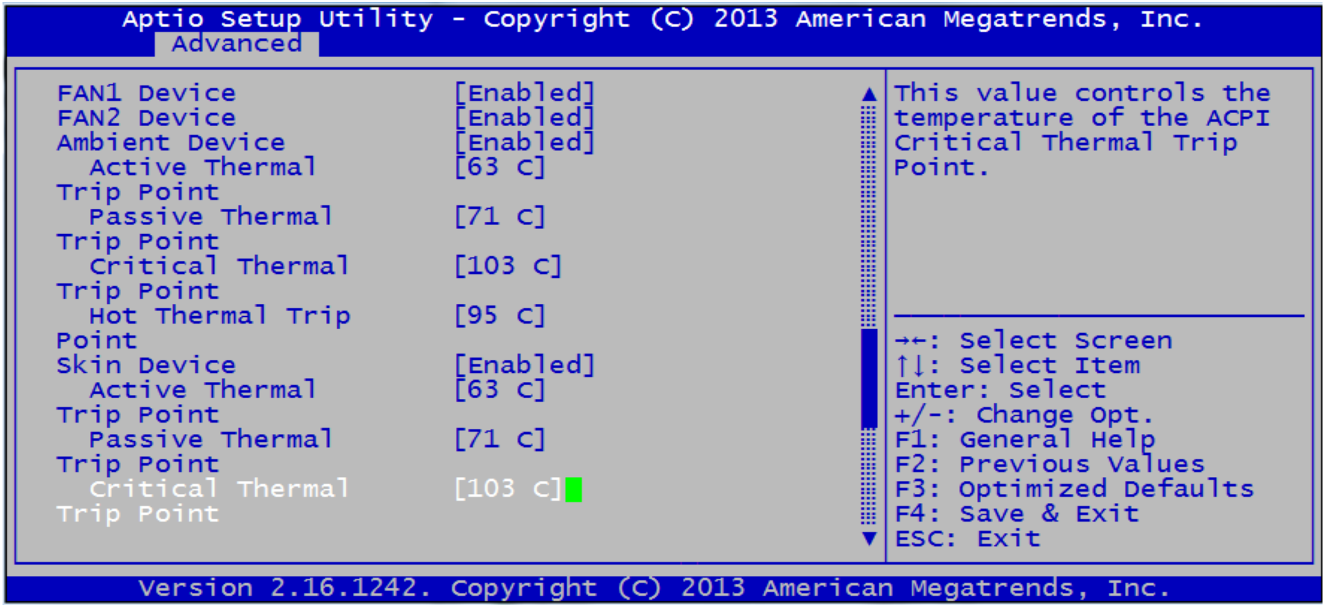
```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
          Advanced

  DPTF Configuration                                 Enable/Disable Intel
                                                     Dynamic Platform
  DPTF                    [Enabled]                  Thermal Framework
  Processor               [SA Thermal Device]
     Active Thermal       [71 C]
  Trip Point
     Passive Thermal      [79 C]
  Trip Point
     Critical Thermal     [103 C]
  Trip Point
     Hot Thermal Trip     [95 C]                     →←: Select Screen
  Point                                              ↑↓: Select Item
     PPCC Step Size       [1.0 Watts]                Enter: Select
     CLPO Enable          [Enabled]                  +/-: Change Opt.
     CLPO Start PState    16                         F1: General Help
     CLPO Step size       50                         F2: Previous Values
     CLPO Power Control   [SMT Off lining]           F3: Optimized Defaults
     CLPO Performance     [Core Off lining]          F4: Save & Exit
  Control                                            ESC: Exit

       Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Fig. 2.2.21.1.b DPTF Configuration (Screen 2 of 5)



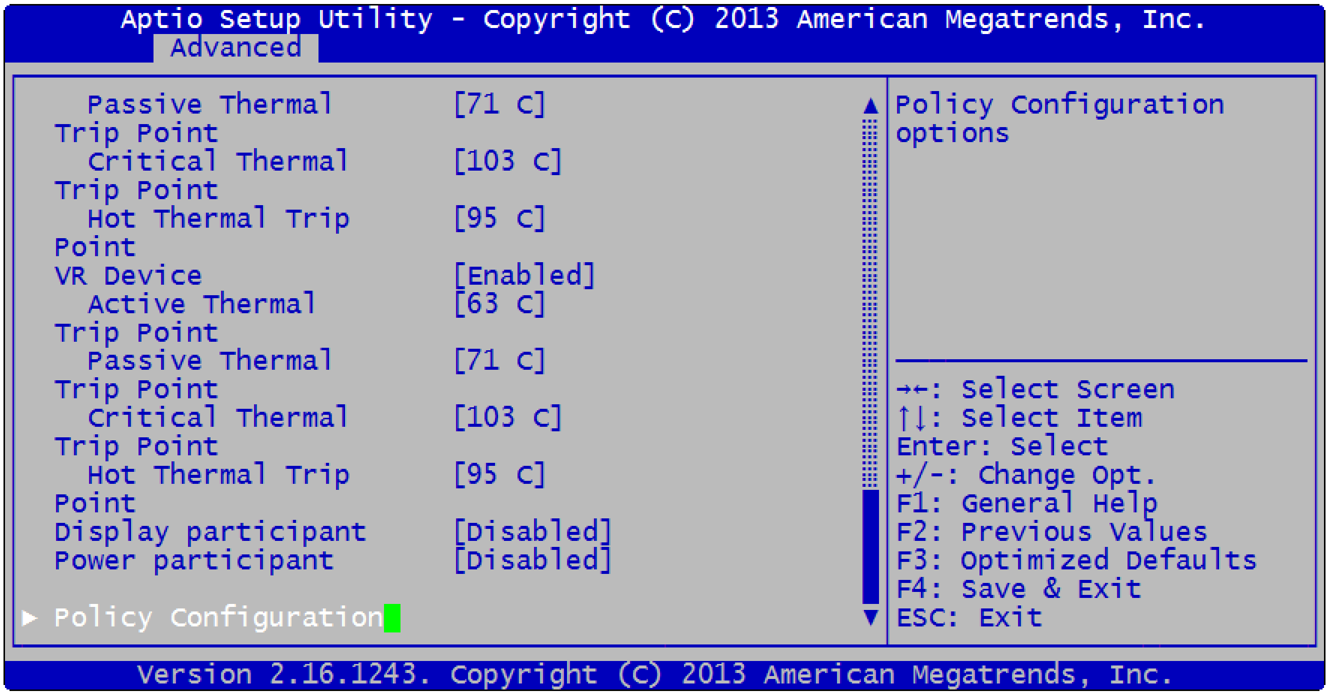
```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
          Advanced

     Config TDP           [Disabled]                 This value controls the
  PCH Thermal Device      [Enabled]                  temperature of the ACPI
     Active Thermal       [71 C]                     Hot Thermal Trip Point.
  Trip Point
     Passive Thermal      [79 C]
  Trip Point
     Critical Thermal     [103 C]
  Trip Point
     Hot Thermal Trip     [95 C]
  Point
  Memory Device           [Enabled]                  →←: Select Screen
     Active Thermal       [63 C]                     ↑↓: Select Item
  Trip Point                                         Enter: Select
     Passive Thermal      [71 C]                     +/-: Change Opt.
  Trip Point                                         F1: General Help
     Critical Thermal     [103 C]                    F2: Previous Values
  Trip Point                                         F3: Optimized Defaults
     Hot Thermal Trip     [95 C]                     F4: Save & Exit
  Point                                              ESC: Exit

       Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Fig. 2.2.21.1.c DPTF Configuration (Screen 3 of 5)



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
          Advanced

  FAN1 Device                [Enabled]         This value controls the
  FAN2 Device                [Enabled]         temperature of the ACPI
  Ambient Device             [Enabled]         Critical Thermal Trip
    Active Thermal           [63 C]            Point.
  Trip Point
    Passive Thermal          [71 C]
  Trip Point
    Critical Thermal         [103 C]
  Trip Point
    Hot Thermal Trip         [95 C]          ----------------------------
  Point                                        →←: Select Screen
  Skin Device                [Enabled]         ↑↓: Select Item
    Active Thermal           [63 C]            Enter: Select
  Trip Point                                   +/-: Change Opt.
    Passive Thermal          [71 C]            F1: General Help
  Trip Point                                   F2: Previous Values
    Critical Thermal         [103 C]           F3: Optimized Defaults
  Trip Point                                   F4: Save & Exit
                                               ESC: Exit
       Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Fig. 2.2.21.1.d DPTF Configuration (Screen 4 of 5)



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
          Advanced

    Passive Thermal          [71 C]            Policy Configuration
  Trip Point                                   options
    Critical Thermal         [103 C]
  Trip Point
    Hot Thermal Trip         [95 C]
  Point
  VR Device                  [Enabled]
    Active Thermal           [63 C]
  Trip Point
    Passive Thermal          [71 C]          ----------------------------
  Trip Point                                   →←: Select Screen
    Critical Thermal         [103 C]           ↑↓: Select Item
  Trip Point                                   Enter: Select
    Hot Thermal Trip         [95 C]            +/-: Change Opt.
  Point                                        F1: General Help
  Display participant        [Disabled]        F2: Previous Values
  Power participant          [Disabled]        F3: Optimized Defaults
                                               F4: Save & Exit
► Policy Configuration                         ESC: Exit
       Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

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

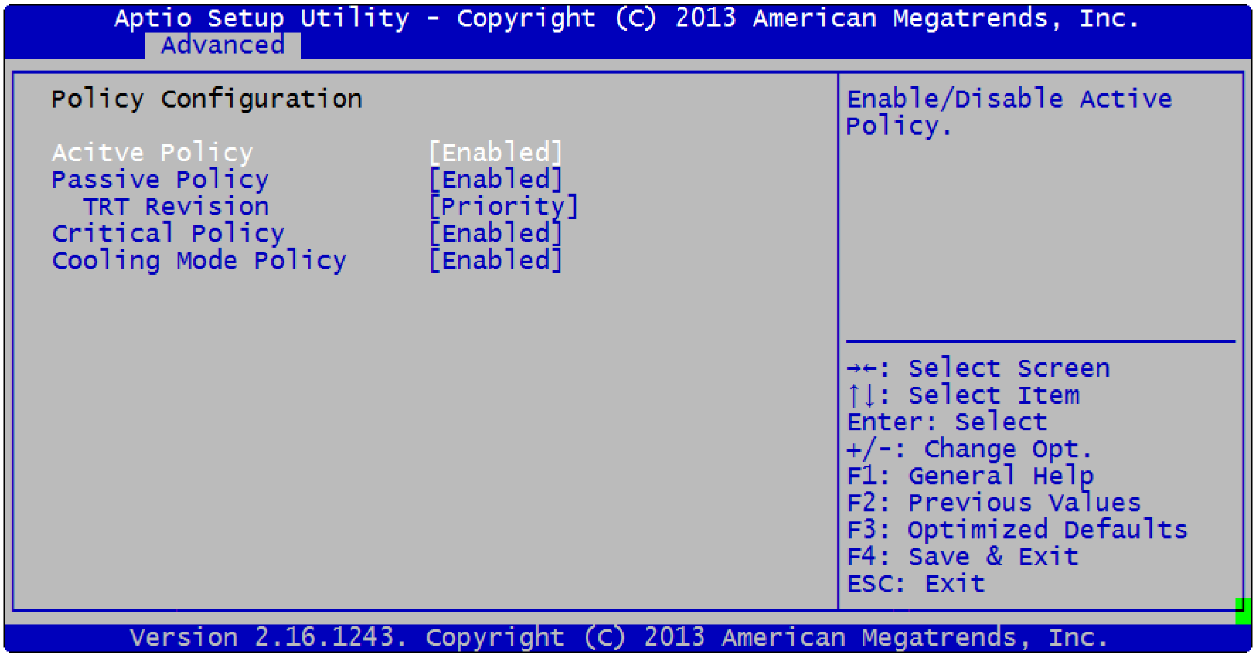
		to be used in P1 or when performance control is applied.
Config TDP	*Disabled* *Enabled*	Enable or Disable Configurable Thermal Design Power (TDP).
PCH Thermal Device	*Enabled* *Disabled*	Enable or Disable Platform Control Hub (PCH) Thermal Device.
Active Thermal Trip Point	*Disabled* *15°C* *23 °C* *…* *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. 2.2.21.1.e Policy Configuration (Screen 5 of 5)



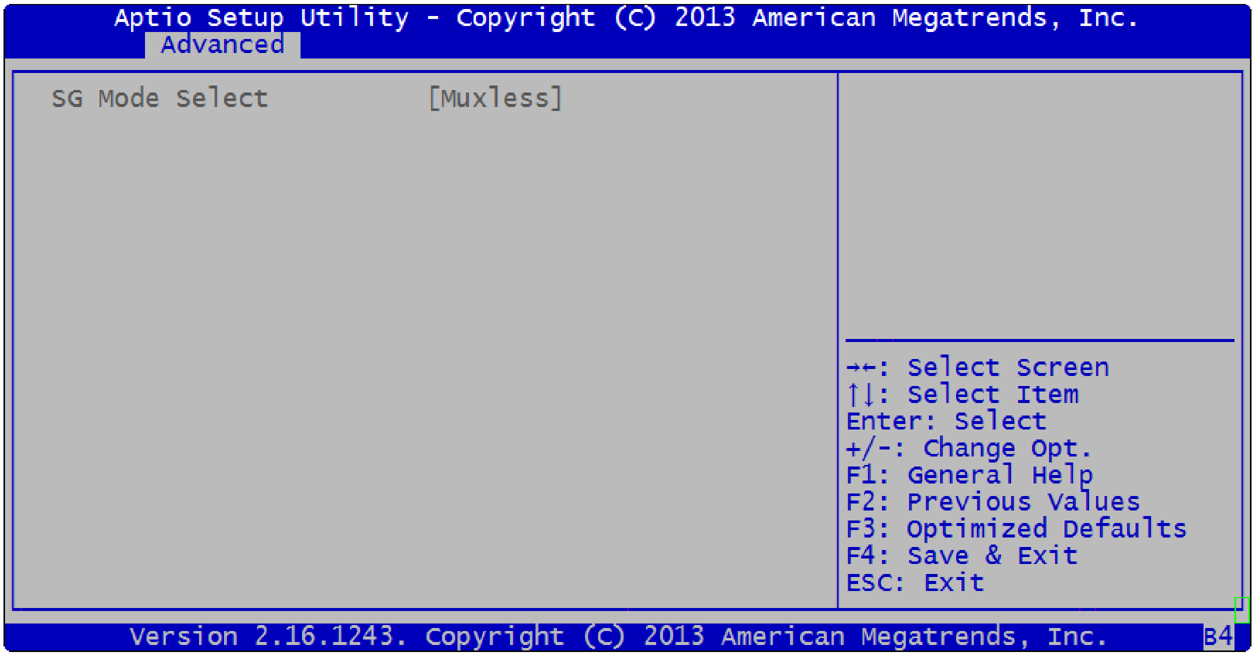
```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
  Advanced

Policy Configuration                                 Enable/Disable Active
                                                     Policy.
Acitve Policy                [Enabled]
Passive Policy               [Enabled]
  TRT Revision               [Priority]
Critical Policy              [Enabled]
Cooling Mode Policy          [Enabled]

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

Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.
```

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.

2.2.22 Switchable Graphics

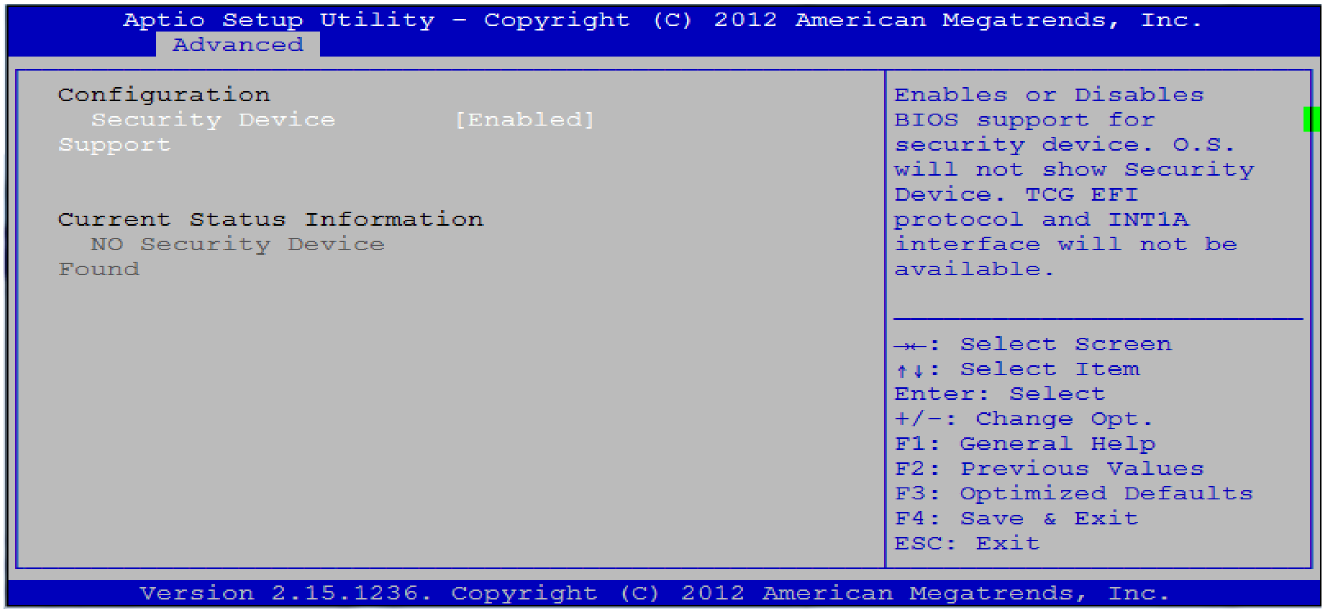
Fig. 2.2.22.a Switchable Graphics



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
Advanced

SG Mode Select          [Muxless]

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

Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.   B4
```

2.2.23 Trusted Computing

Fig. 2.2.23.a Trusted Computing

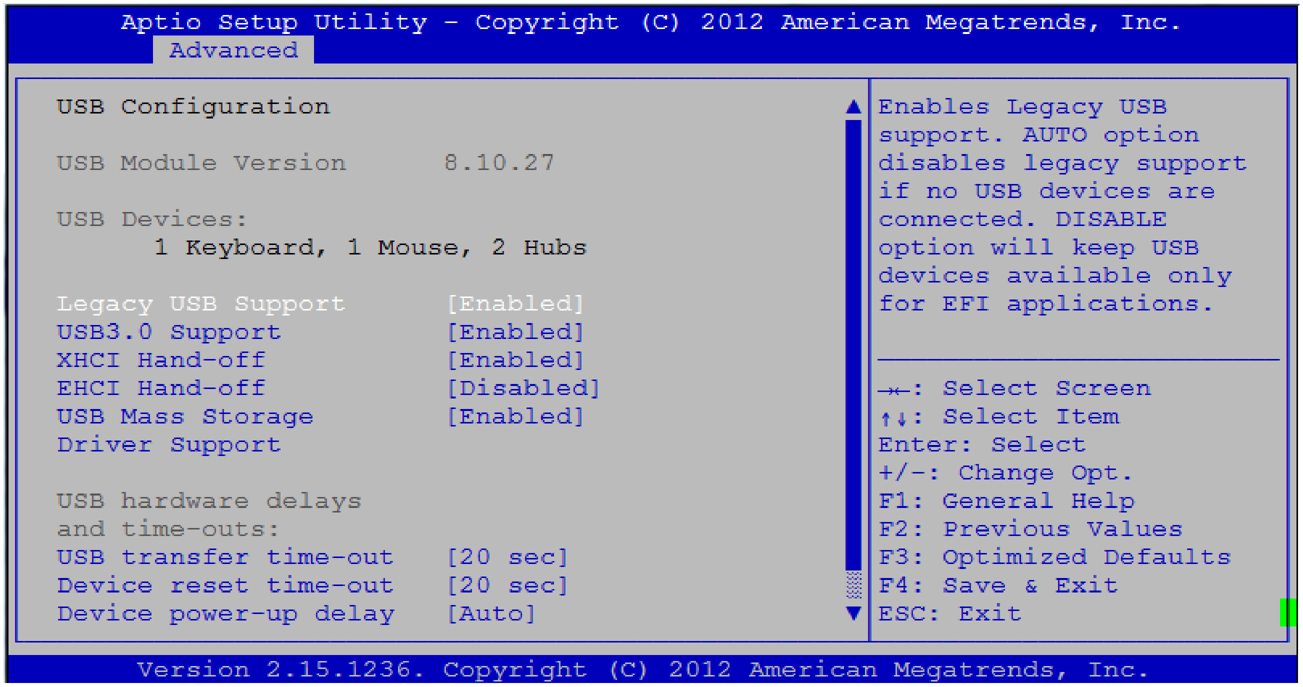


```
          Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
              Advanced

   Configuration                                       Enables or Disables
     Security Device          [Enabled]                BIOS support for
   Support                                             security device. O.S.
                                                       will not show Security
                                                       Device. TCG EFI
   Current Status Information                          protocol and INT1A
     NO Security Device                                interface will not be
   Found                                               available.

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

           Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
Security Device Support		Enables or Disables BIOS support for security device (ie TPM). Affects visibility of security device in OS, and whether TCG EFI protocol and INT1A interface will be available.

2.2.24 USB Configuration

Fig. 2.2.24.a USB Configuration



```
       Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
         Advanced

  USB Configuration                                  ▲ Enables Legacy USB
                                                       support. AUTO option
  USB Module Version       8.10.27                     disables legacy support
                                                       if no USB devices are
  USB Devices:                                         connected. DISABLE
        1 Keyboard, 1 Mouse, 2 Hubs                    option will keep USB
                                                       devices available only
  Legacy USB Support       [Enabled]                   for EFI applications.
  USB3.0 Support           [Enabled]
  XHCI Hand-off            [Enabled]                   ─────────────────────────
  EHCI Hand-off            [Disabled]                  →←: Select Screen
  USB Mass Storage         [Enabled]                   ↑↓: Select Item
  Driver Support                                       Enter: Select
                                                       +/-: Change Opt.
  USB hardware delays                                  F1: General Help
  and time-outs:                                       F2: Previous Values
  USB transfer time-out    [20 sec]                    F3: Optimized Defaults
  Device reset time-out    [20 sec]                    F4: Save & Exit
  Device power-up delay    [Auto]                    ▼ ESC: Exit

       Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

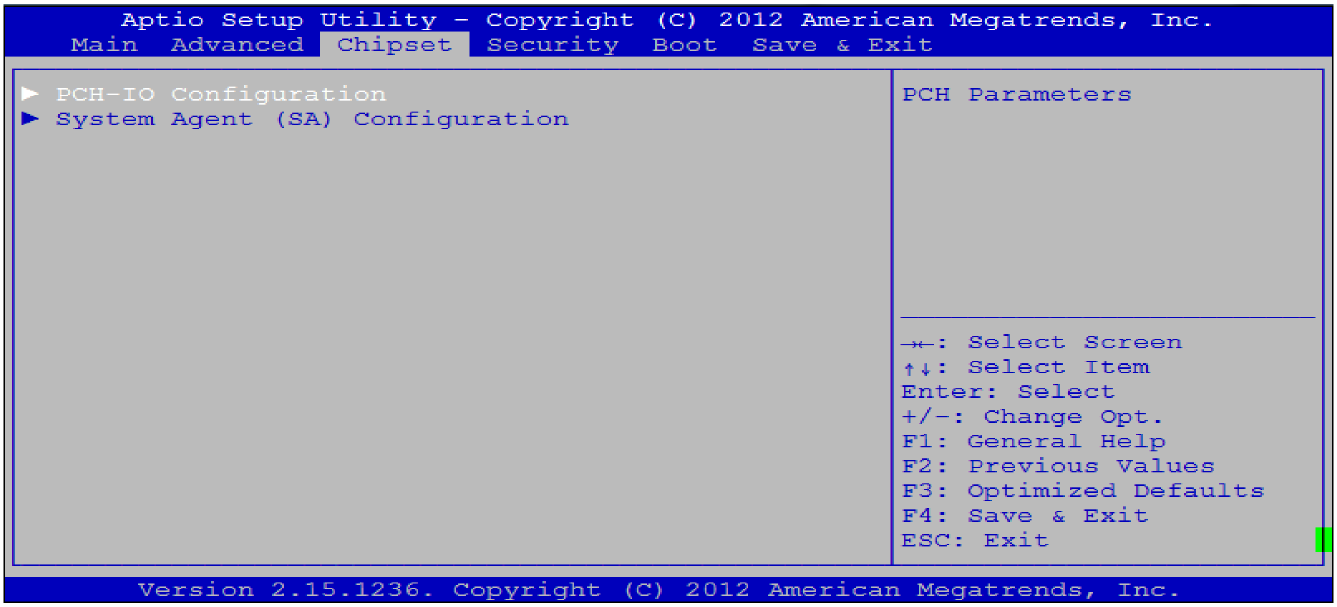
This option allows the user to view and change the USB Configuration.

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

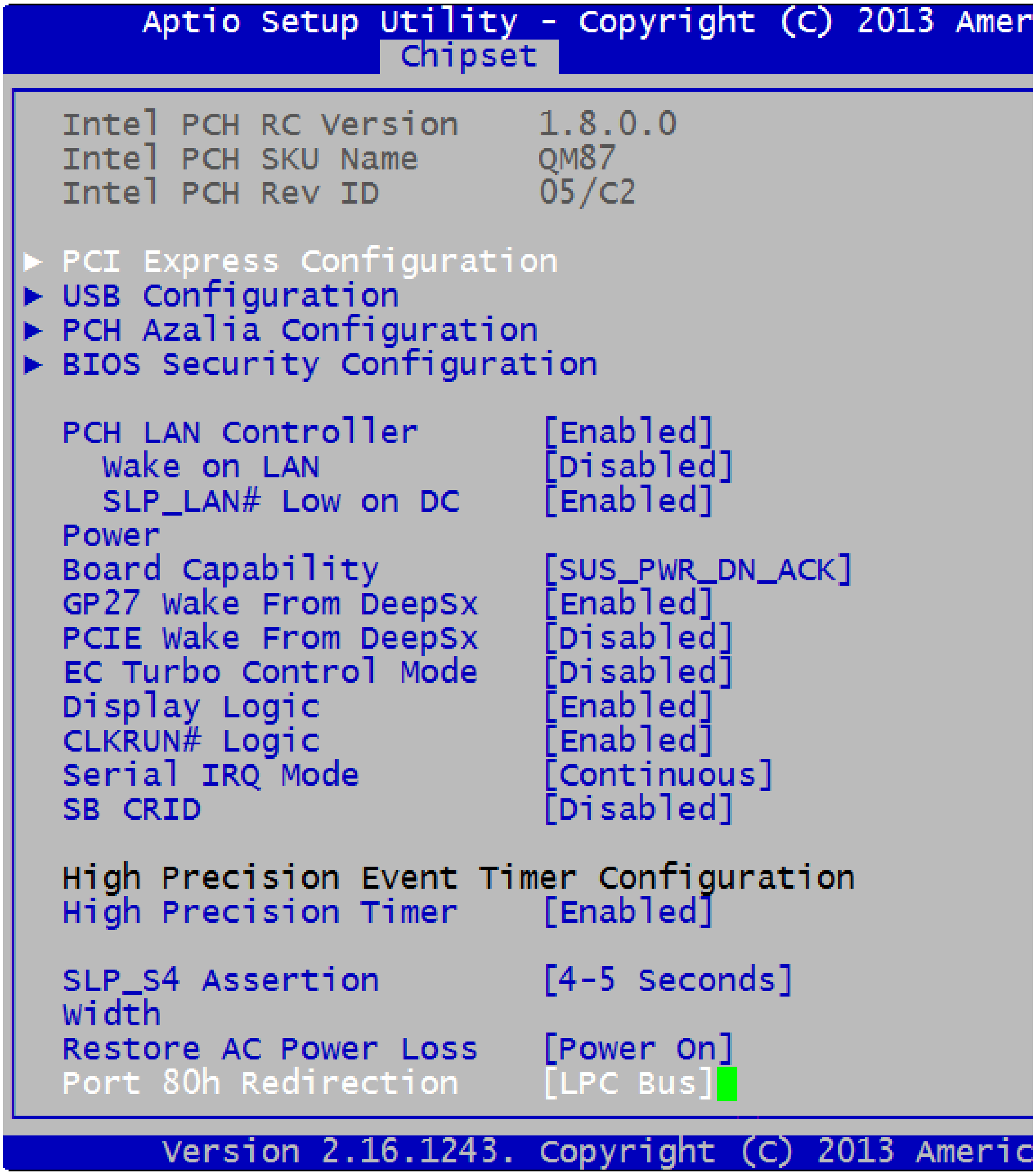
Fig. 2.3.a Chipset Menu



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

 ► PCH-IO Configuration                                   PCH Parameters
 ► System Agent (SA) Configuration

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

          Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.3.1 PCH I/O Configuration

Fig. 2.3.1.a PCH I/O Configuration



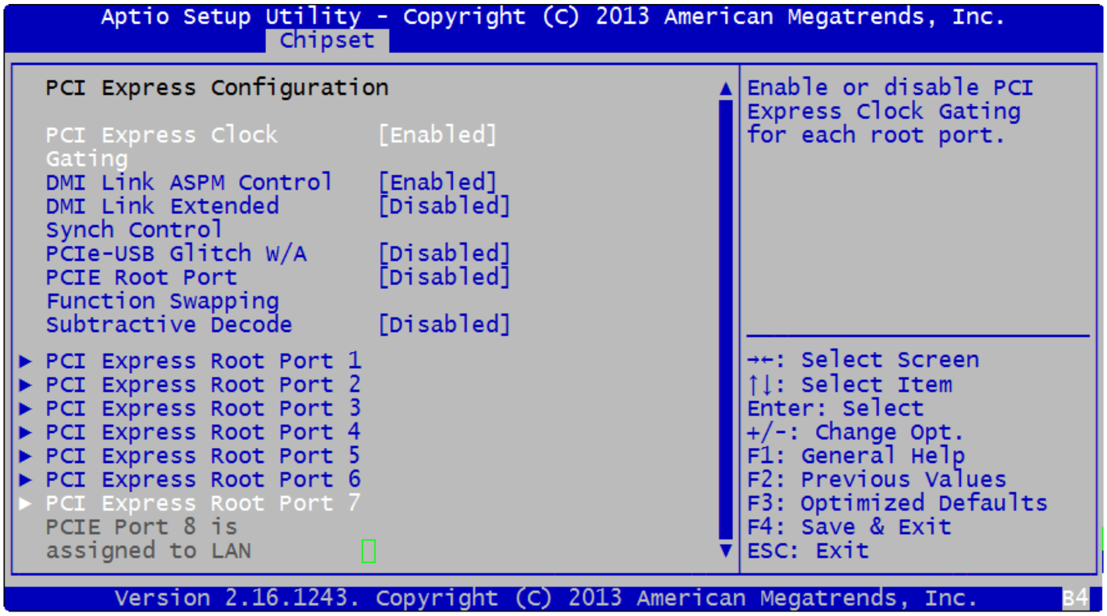
```
       Aptio Setup Utility - Copyright (C) 2013 Amer
                         Chipset

   Intel PCH RC Version    1.8.0.0
   Intel PCH SKU Name      QM87
   Intel PCH Rev ID        05/C2

 ▶ PCI Express Configuration
 ▶ USB Configuration
 ▶ PCH Azalia Configuration
 ▶ BIOS Security Configuration

   PCH LAN Controller      [Enabled]
     Wake on LAN           [Disabled]
     SLP_LAN# Low on DC    [Enabled]
   Power
   Board Capability        [SUS_PWR_DN_ACK]
   GP27 Wake From DeepSx   [Enabled]
   PCIE Wake From DeepSx   [Disabled]
   EC Turbo Control Mode   [Disabled]
   Display Logic           [Enabled]
   CLKRUN# Logic           [Enabled]
   Serial IRQ Mode         [Continuous]
   SB CRID                 [Disabled]

   High Precision Event Timer Configuration
   High Precision Timer    [Enabled]

   SLP_S4 Assertion        [4-5 Seconds]
   Width
   Restore AC Power Loss   [Power On]
   Port 80h Redirection    [LPC Bus]

        Version 2.16.1243. Copyright (C) 2013 Americ
```

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	*DisabledEnabled*	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

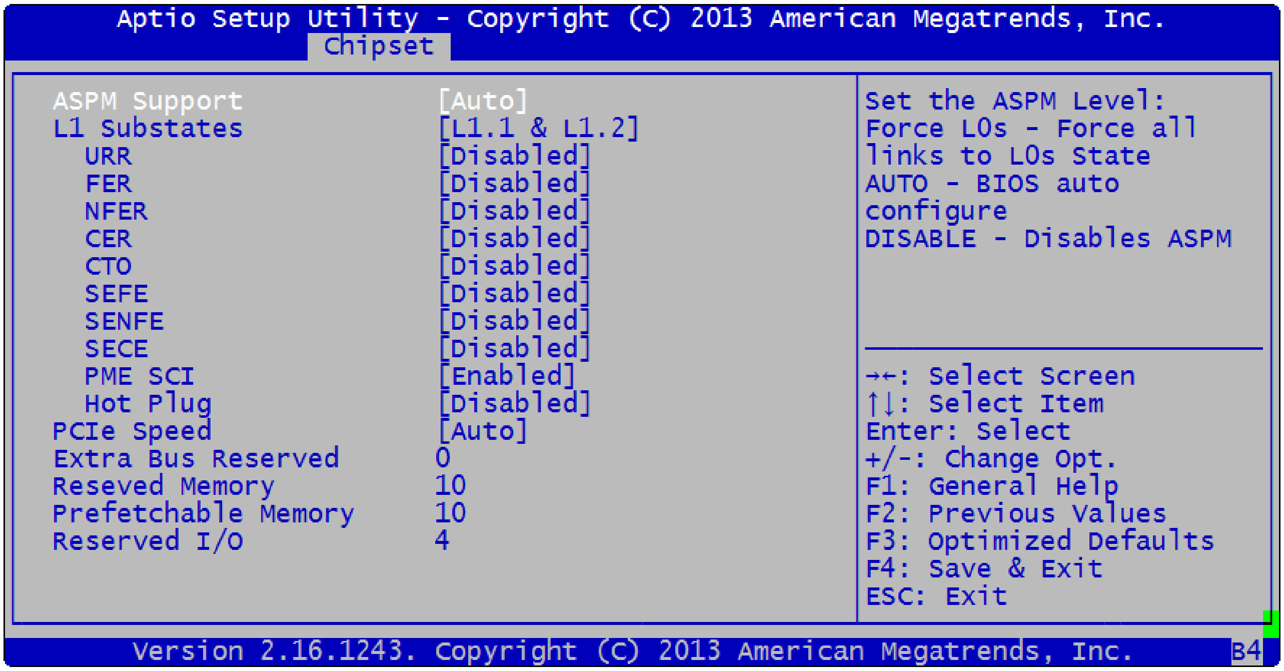
Fig. 2.3.1.1.a PCI Express Configuration



```
         Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                        Chipset
  PCI Express Configuration                       Enable or disable PCI
                                                  Express Clock Gating
  PCI Express Clock        [Enabled]              for each root port.
  Gating
  DMI Link ASPM Control    [Enabled]
  DMI Link Extended        [Disabled]
  Synch Control
  PCIe-USB Glitch W/A      [Disabled]
  PCIE Root Port           [Disabled]
  Function Swapping
  Subtractive Decode       [Disabled]
                                                  ----------------------------
▶ PCI Express Root Port 1                         →←: Select Screen
▶ PCI Express Root Port 2                         ↑↓: Select Item
▶ PCI Express Root Port 3                         Enter: Select
▶ PCI Express Root Port 4                         +/-: Change Opt.
▶ PCI Express Root Port 5                         F1: General Help
▶ PCI Express Root Port 6                         F2: Previous Values
▶ PCI Express Root Port 7                         F3: Optimized Defaults
  PCIE Port 8 is                                  F4: Save & Exit
  assigned to LAN                                 ESC: Exit
        Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.       B4
```

Feature	Options	Description
PCI Express Clock Gating		Controls Power Gating: reducing PCI Express power consumption to mobile levels.
PCI Express Root Port 1-7 All	Enabled Disabled	Master enable/disable of the individual PCI Express root port controllers within the chipset.

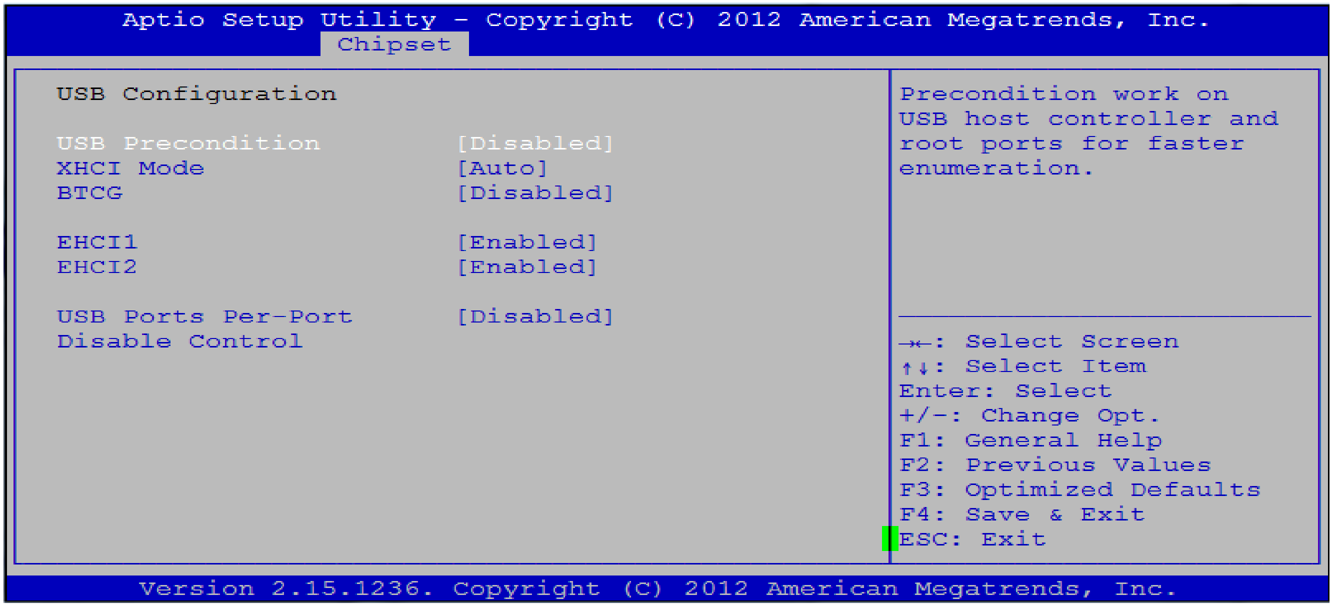
Fig. 2.3.1.1.b PCI Express Root Port (1 to 7)



```
         Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                        Chipset
  ASPM Support               [Auto]               Set the ASPM Level:
  L1 Substates               [L1.1 & L1.2]        Force L0s - Force all
    URR                      [Disabled]           links to L0s State
    FER                      [Disabled]           AUTO - BIOS auto
    NFER                     [Disabled]           configure
    CER                      [Disabled]           DISABLE - Disables ASPM
    CTO                      [Disabled]
    SEFE                     [Disabled]
    SENFE                    [Disabled]
    SECE                     [Disabled]           ----------------------------
    PME SCI                  [Enabled]            →←: Select Screen
    Hot Plug                 [Disabled]           ↑↓: Select Item
  PCIe Speed                 [Auto]               Enter: Select
  Extra Bus Reserved         0                    +/-: Change Opt.
  Reseved Memory             10                   F1: General Help
  Prefetchable Memory        10                   F2: Previous Values
  Reserved I/O               4                    F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit
        Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.       B4
```

2.3.1.2 USB Configuration

Fig. 2.3.1.2.a USB Configuration



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                          Chipset
  USB Configuration                                   Precondition work on
                                                      USB host controller and
  USB Precondition           [Disabled]               root ports for faster
  XHCI Mode                  [Auto]                   enumeration.
  BTCG                       [Disabled]

  EHCI1                      [Enabled]
  EHCI2                      [Enabled]

  USB Ports Per-Port         [Disabled]
  Disable Control                                     →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit
         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

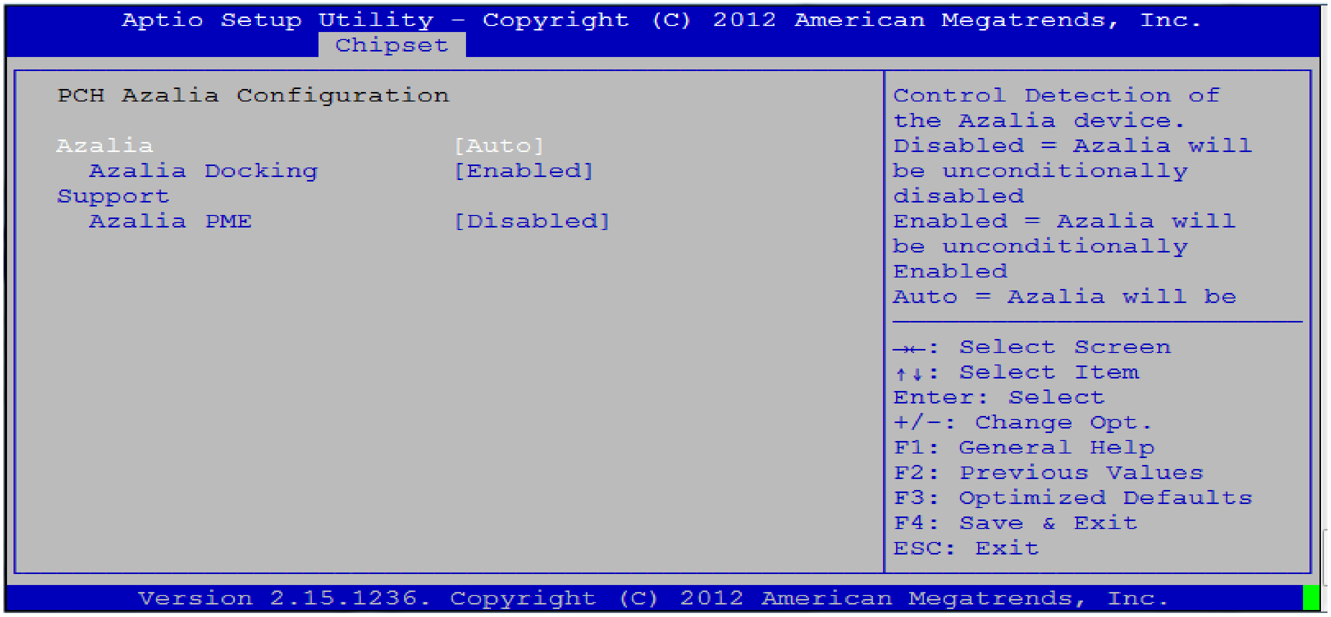
This option allows the user to view and change the USB Configuration.

Feature	Options	Description
USB Precondition	*Enabled* *Disabled*	Precondition work on USB host controller and root ports for faster enumeration.
XHCI Mode	 *Auto* *Smart Auto* *Enabled*	The Extensible Host Controller Interface (xHCI) is the USB 3.0 controller. The different modes of operation are: 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. 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. 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



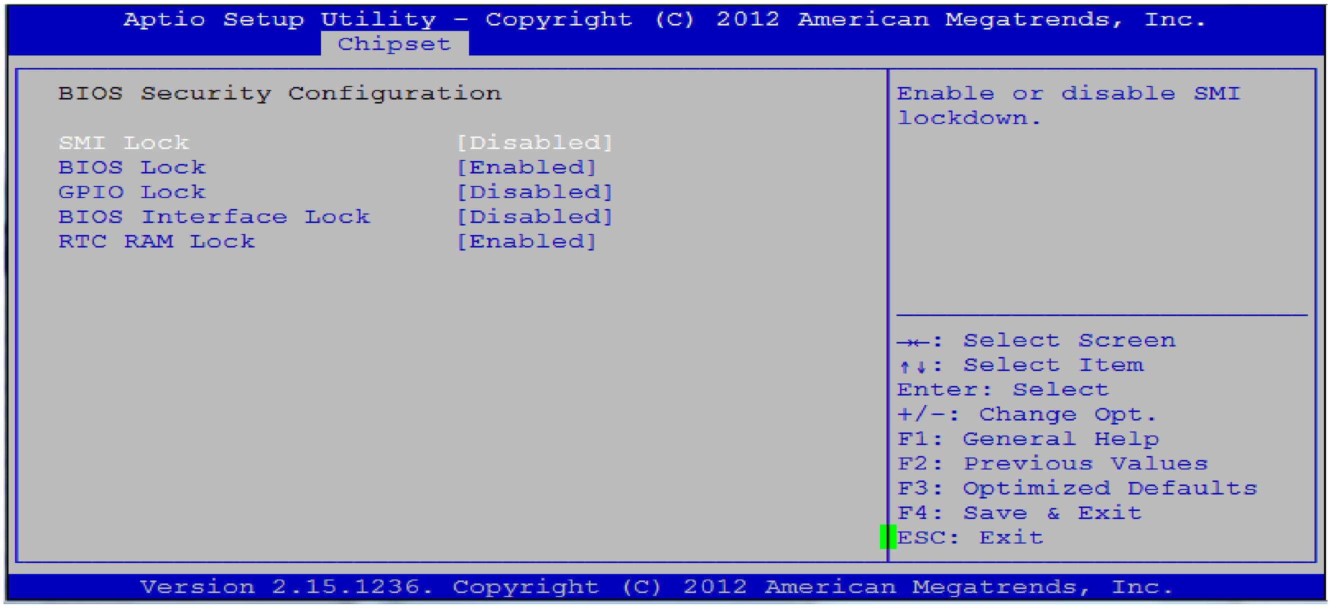
```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                        Chipset

  PCH Azalia Configuration                            Control Detection of
                                                      the Azalia device.
  Azalia                       [Auto]                 Disabled = Azalia will
    Azalia Docking             [Enabled]              be unconditionally
  Support                                             disabled
    Azalia PME                 [Disabled]             Enabled = Azalia will
                                                      be unconditionally
                                                      Enabled
                                                      Auto = Azalia will be

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

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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



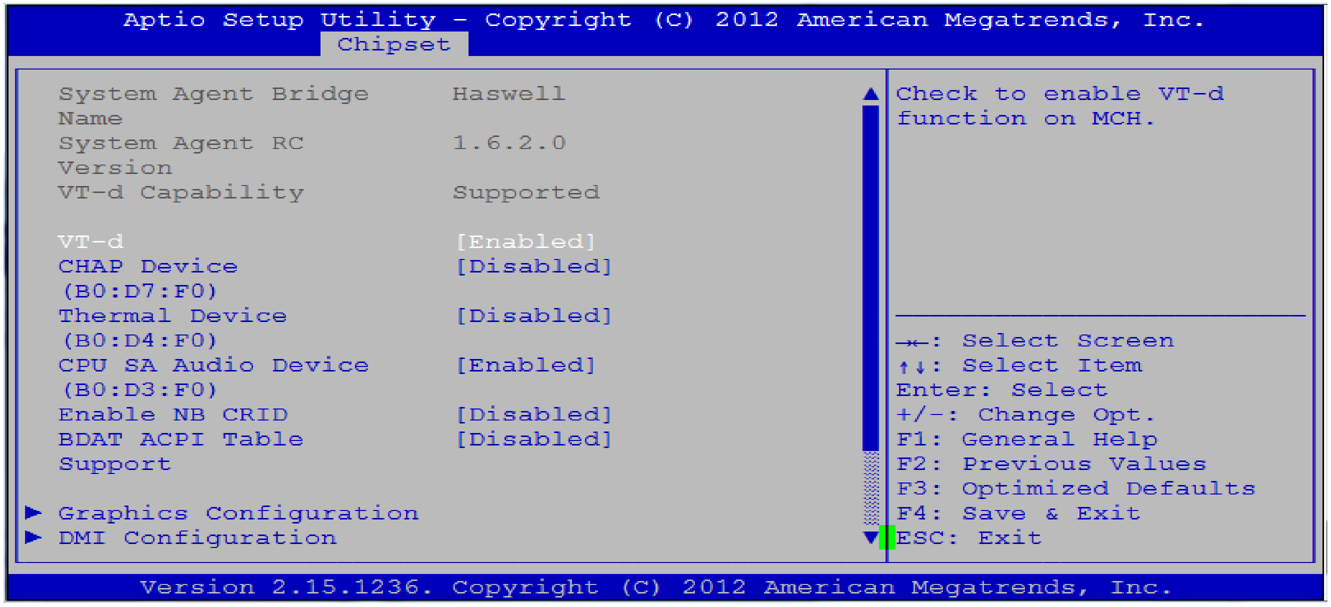
```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                          Chipset

  BIOS Security Configuration                      Enable or disable SMI
                                                   lockdown.
  SMI Lock                    [Disabled]
  BIOS Lock                   [Enabled]
  GPIO Lock                   [Disabled]
  BIOS Interface Lock         [Disabled]
  RTC RAM Lock                [Enabled]

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

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

The BIOS Security Configuration are the controls related to the security of the BIOS, including lockdown of SMI operation, GPIO settings, BIOS chip write access, and others.

Feature	Options	Description
SMI Lock	*Enabled* *Disabled*	Intel strongly recommends that SMI_LOCK be enabled in BIOS. This setting, when enabled, prevents writes to the Global SMI Enable bit. Enabling this bit mitigates malicious software attempts to gain system management mode privileges.
BIOS Lock	*Enabled* *Disabled*	When enabled, causes the chipset to block all access to the BIOS flash part unless they come through an SMI handler.
GPIO Lock	*Enabled* *Disabled*	When enabled, causes chipset to block attempts to change GPIO-related registers unless they come through an SMI handler.
BIOS Interface Lock	*Enabled* *Disabled*	When enabled, this bit mitigates malicious software attempts to replace the system BIOS option ROM with its own code.
RTC RAM Lock	*Enabled* *Disabled*	When enabled, this feature blocks writes to upper and lower CMOS RAM ranges, up until the next system reset.

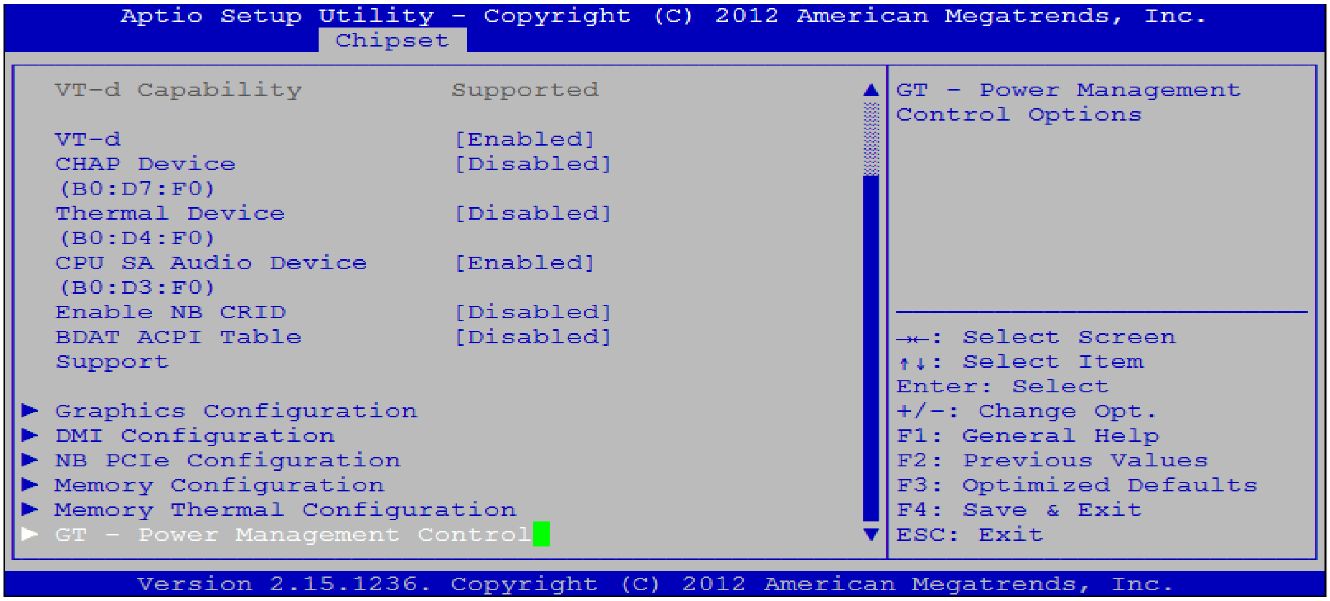
2.3.2 System Agent Configuration

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



```
       Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                         Chipset
  System Agent Bridge       Haswell                  Check to enable VT-d
  Name                                               function on MCH.
  System Agent RC           1.6.2.0
  Version
  VT-d Capability           Supported

  VT-d                      [Enabled]
  CHAP Device               [Disabled]
  (B0:D7:F0)
  Thermal Device            [Disabled]
  (B0:D4:F0)                                         →←: Select Screen
  CPU SA Audio Device       [Enabled]                ↑↓: Select Item
  (B0:D3:F0)                                         Enter: Select
  Enable NB CRID            [Disabled]               +/-: Change Opt.
  BDAT ACPI Table           [Disabled]               F1: General Help
  Support                                            F2: Previous Values
                                                     F3: Optimized Defaults
► Graphics Configuration                             F4: Save & Exit
► DMI Configuration                                  ESC: Exit
        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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



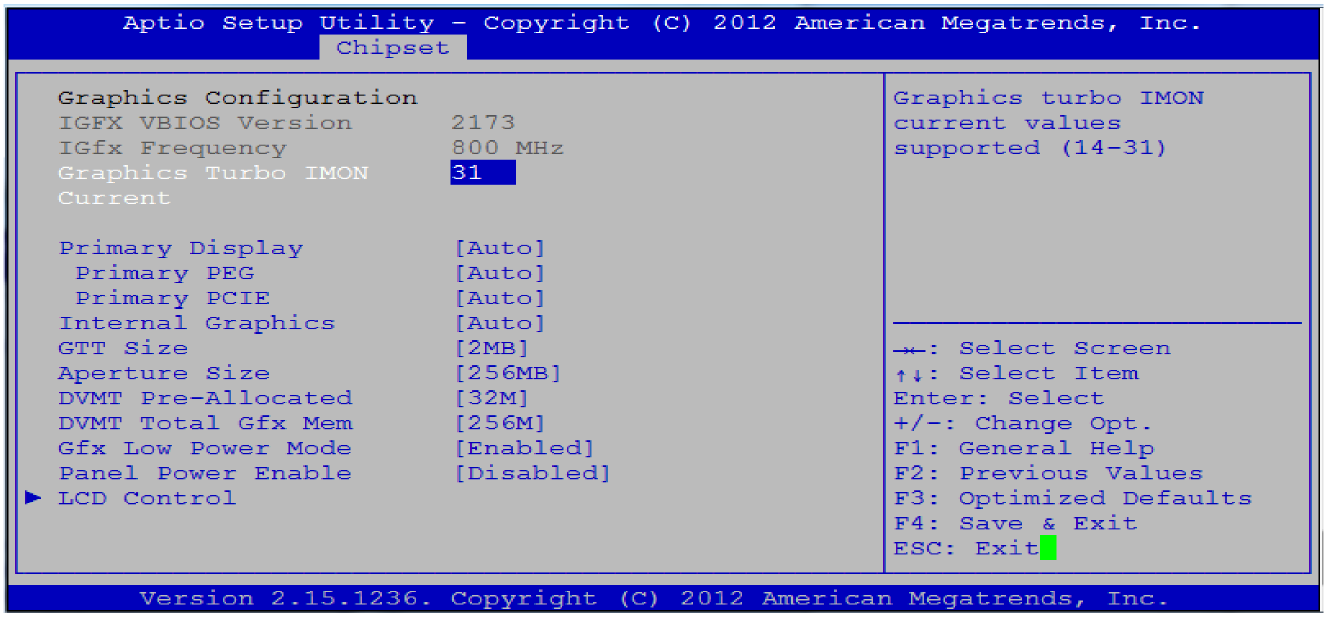
```
       Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                         Chipset
  VT-d Capability           Supported                GT - Power Management
                                                     Control Options
  VT-d                      [Enabled]
  CHAP Device               [Disabled]
  (B0:D7:F0)
  Thermal Device            [Disabled]
  (B0:D4:F0)
  CPU SA Audio Device       [Enabled]
  (B0:D3:F0)
  Enable NB CRID            [Disabled]
  BDAT ACPI Table           [Disabled]               →←: Select Screen
  Support                                            ↑↓: Select Item
                                                     Enter: Select
► Graphics Configuration                             +/-: Change Opt.
► DMI Configuration                                  F1: General Help
► NB PCIe Configuration                              F2: Previous Values
► Memory Configuration                               F3: Optimized Defaults
► Memory Thermal Configuration                       F4: Save & Exit
► GT - Power Management Control                      ESC: Exit
        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
VT-d		Virtualization Technology for Directed I/O. Using this specific type of VT, users and/or administrators can: a) easily assign I/O devices to VMs, b) easily translate addresses in device DMA data transfers, and c) isolate the different VM's device interrupts from each other, and d) facilitate better I/O, DMA, and interrupt error reporting when using VT.

CHAP Device		Challenge Handshake Authentication Protocol. A CHAP device uses the CHAP protocol to validate the identity of servers and/or remote clients. Enabling this feature enables this device to authenticate or be authenticated using the CHAP protocol.
Thermal Device		Controls the chipset System Agent Thermal Device (Device 4).
CPU SA Audio Device		Enable or disable the System Agent audio device.
Enable NB CRID		Northbridge Compatible Revision ID (NB CRID), when enabled, makes it easy for the BIOS to load OS drivers that are optimized for a previous revision of the silicon instead of the current revision. This is enabled in order to minimize driver updates to the OS image for minor silicon optimizations.
BDAT ACPI Table Support		Disabled by default. This is a bios data table defined by Intel. Usually used for diagnostic purposes along with RMT support.

2.3.2.1 Graphics Configuration

Fig. 2.3.2.1.a Graphics Configuration



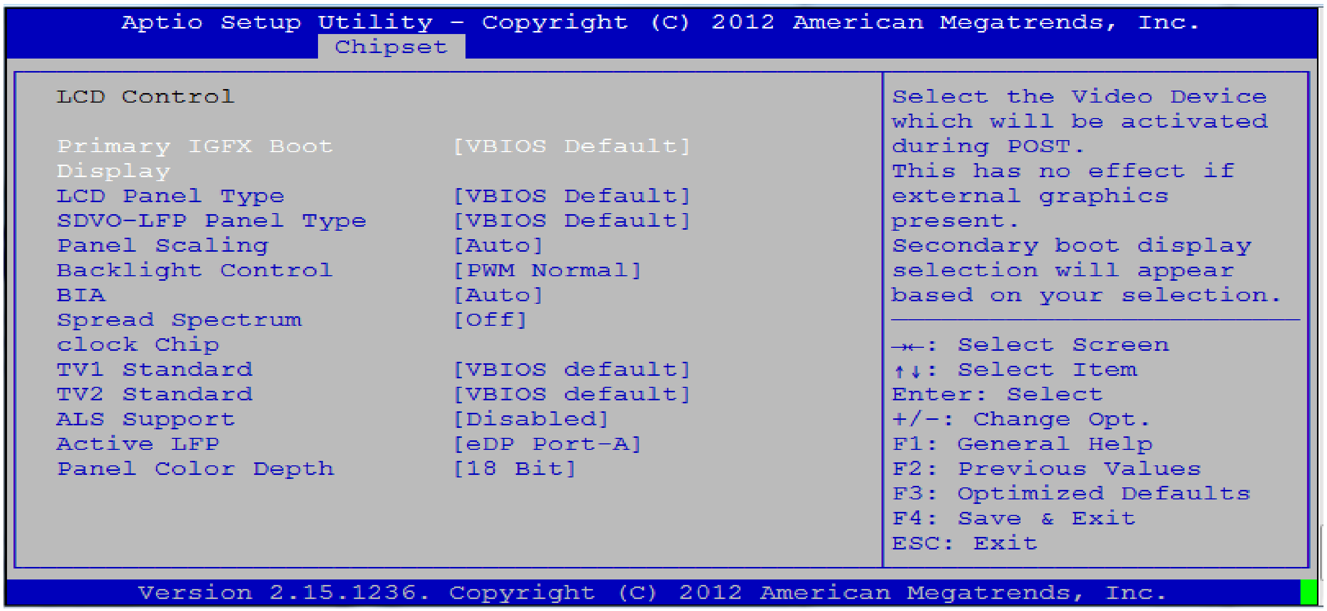
```
       Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                            Chipset

   Graphics Configuration                         Graphics turbo IMON
   IGFX VBIOS Version          2173               current values
   IGfx Frequency              800 MHz            supported (14-31)
   Graphics Turbo IMON         31
   Current

   Primary Display             [Auto]
    Primary PEG                [Auto]
    Primary PCIE               [Auto]
   Internal Graphics           [Auto]
   GTT Size                    [2MB]              →←: Select Screen
   Aperture Size               [256MB]            ↑↓: Select Item
   DVMT Pre-Allocated          [32M]              Enter: Select
   DVMT Total Gfx Mem          [256M]             +/-: Change Opt.
   Gfx Low Power Mode          [Enabled]          F1: General Help
   Panel Power Enable          [Disabled]         F2: Previous Values
 ► LCD Control                                    F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit

        Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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



```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                       Chipset

  LCD Control                                   Select the Video Device
                                                which will be activated
  Primary IGFX Boot        [VBIOS Default]      during POST.
  Display                                       This has no effect if
  LCD Panel Type           [VBIOS Default]      external graphics
  SDVO-LFP Panel Type      [VBIOS Default]      present.
  Panel Scaling            [Auto]               Secondary boot display
  Backlight Control        [PWM Normal]         selection will appear
  BIA                      [Auto]               based on your selection.
  Spread Spectrum          [Off]
  clock Chip                                    →←: Select Screen
  TV1 Standard             [VBIOS default]      ↑↓: Select Item
  TV2 Standard             [VBIOS default]      Enter: Select
  ALS Support              [Disabled]           +/-: Change Opt.
  Active LFP               [eDP Port-A]         F1: General Help
  Panel Color Depth        [18 Bit]             F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

       Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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.

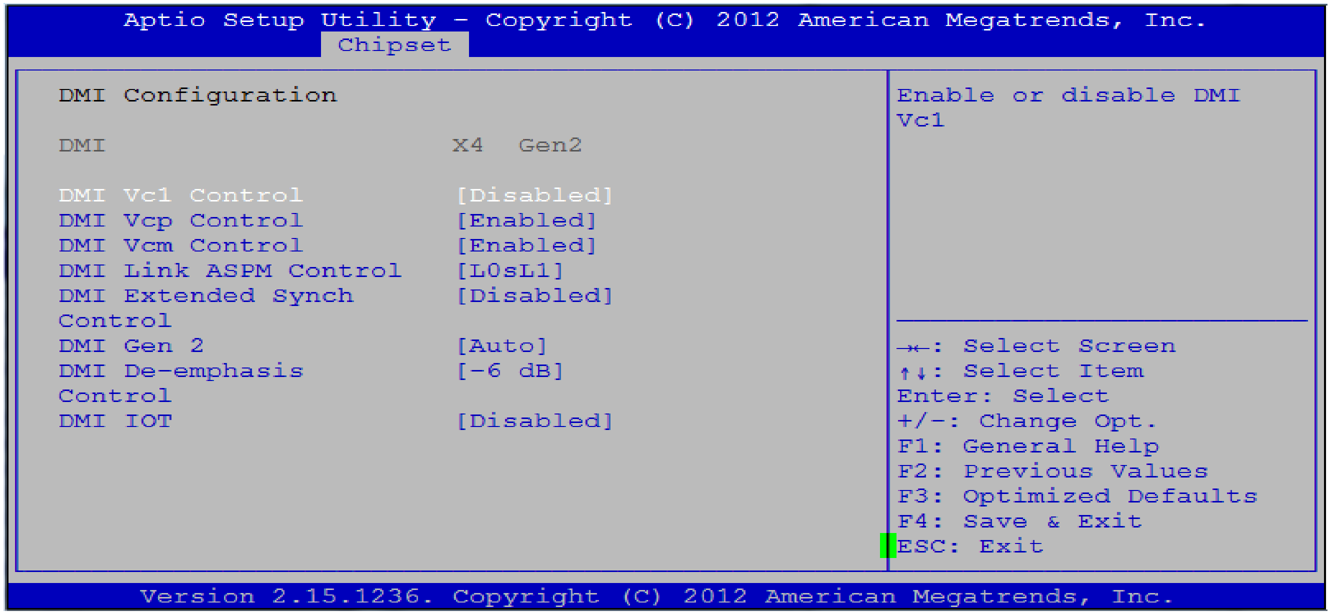
BIA	*Auto* *Disabled* *Level 1 to 5*	The Graphics and Memory Control Hub (GMCH) uses VBT Default. Disable Enable with Selected Aggressiveness Level.
Spread Spectrum Clock Chip	*Off* *Hardware* *Software*	Spread is disabled. Spread is controlled by chip. Spread is controlled by BIOS.
TV1 Standard	*VBIOS 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

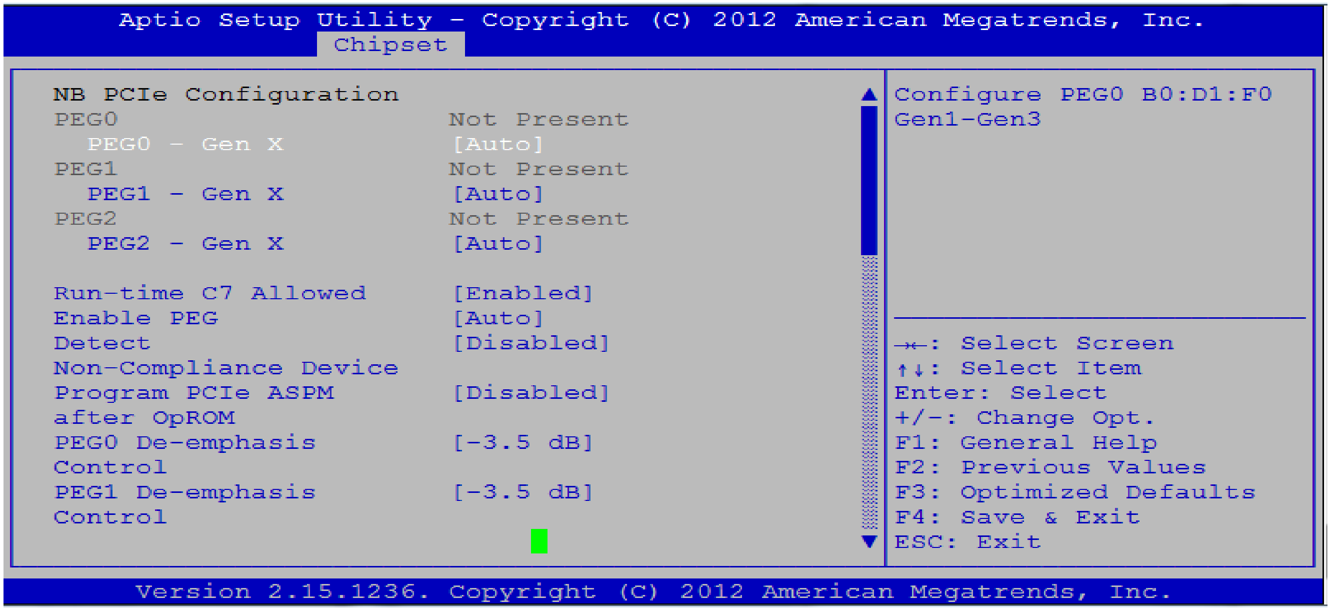


```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                           Chipset

  DMI Configuration                              Enable or disable DMI
                                                 Vc1
  DMI                     X4  Gen2

  DMI Vc1 Control          [Disabled]
  DMI Vcp Control          [Enabled]
  DMI Vcm Control          [Enabled]
  DMI Link ASPM Control    [L0sL1]
  DMI Extended Synch       [Disabled]
  Control                                        ─────────────────────────
  DMI Gen 2                [Auto]                →←: Select Screen
  DMI De-emphasis          [-6 dB]               ↑↓: Select Item
  Control                                        Enter: Select
  DMI IOT                  [Disabled]            +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

     Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
DMI Vc1 Control		Enables or disables DMI Virtual Channel 1. Controls the resources associated with PCI Express Virtual Channel 1 on PCH.
DMI Vcp Control		Virtual Channel (Private). This feature assigns a private ID to a given VC, and once assigned to a VC it cannot be altered.
DMI Vcm Control		Enables or disables DMI Virtual Channel Memory (the bus technology between the CPU and RAM).
DMI Link ASPM Control		DMI Active State Power Management (ASPM), when enabled, allows the DMI connection to the PCH chipset to enter a low-power state in order to reduce power consumption.
DMI Extended Sync Control		Disabled by default. DMI Extended sync is only to be used in a debug or testing environment and can cause lockups when Enabled with L0s.
DMI Gen 2		Auto by default, so actual default is a function of hardware. Serves as a chip to chip interface between the CPU and the PCH. The setting determines whether the interface is allowed to operate at faster Gen 2 speeds.
DMI De-emphasis Control		6DB by default. Allows user to alter the de-emphasis setting of the chipset for the DMI electrical interface.
DMI IOT		Disabled by default. Appears to alter chipset in some way beneficial to IoT usage. Check with Intel for details.

2.3.2.3 NB PCIe Configuration

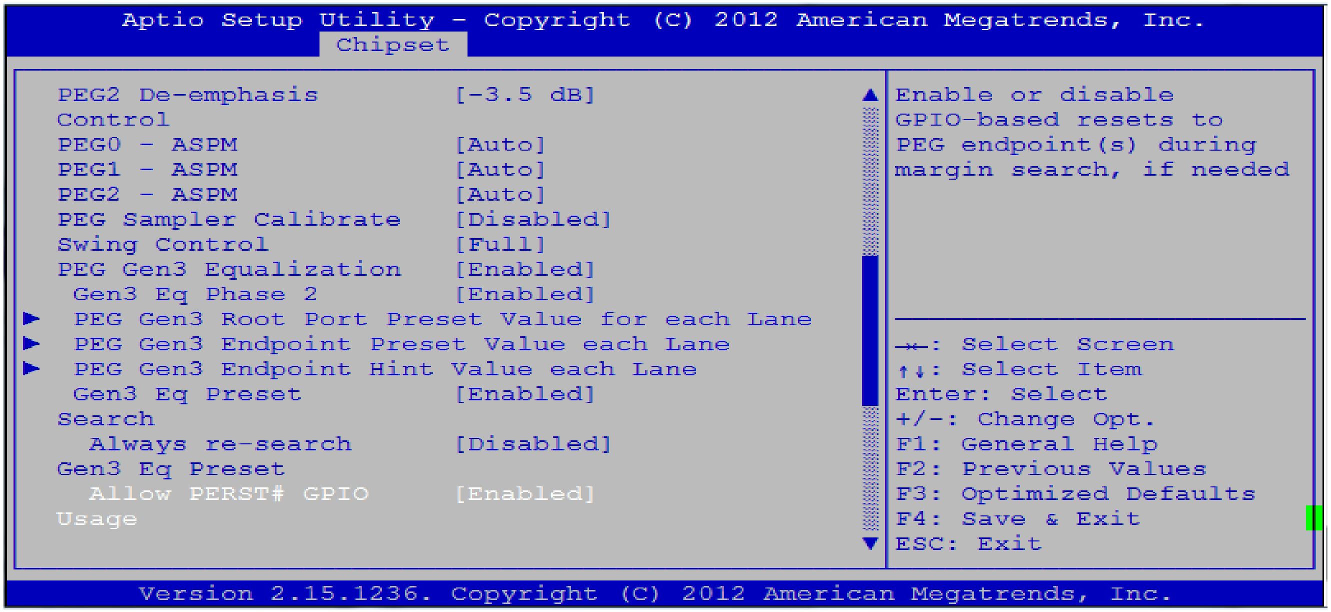
Fig. 2.3.2.3.a NB PCIe Configuration (Screen 1 of 3)



```
  Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                     Chipset
 NB PCIe Configuration                                  Configure PEG0 B0:D1:F0
 PEG0                       Not Present                 Gen1-Gen3
   PEG0 - Gen X             [Auto]
 PEG1                       Not Present
   PEG1 - Gen X             [Auto]
 PEG2                       Not Present
   PEG2 - Gen X             [Auto]

 Run-time C7 Allowed        [Enabled]
 Enable PEG                 [Auto]
 Detect                     [Disabled]                  →←: Select Screen
 Non-Compliance Device                                  ↑↓: Select Item
 Program PCIe ASPM          [Disabled]                  Enter: Select
 after OpROM                                            +/-: Change Opt.
 PEG0 De-emphasis           [-3.5 dB]                   F1: General Help
 Control                                                F2: Previous Values
 PEG1 De-emphasis           [-3.5 dB]                   F3: Optimized Defaults
 Control                                                F4: Save & Exit
                                                        ESC: Exit
  Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
PEG0 thru PEG2 – Gen X		Auto for default, meaning actual default driven by hardware capabilities. This option determines the PCIe Generation speed that the slot should operate at.
Runtime C7 Allowed		Enabled by default. Determines whether information needed for the OS to be aware of and use the C7 state is made visible to the OS.
Enable PEG		Auto by default. Determines whether the PEG slot is active or not.
Detect Non-Compliance Device		Disabled by default. Detects whether the device installed in the slot is compliant or not.
Program PCIe ASPM after OpROM		Disabled by default. User control to allow selecting whether ASPM would be enabled before or after the OpRoms have been executed.
PEG De-emphasis Control		Chipset feature to allow user to control the electrical characteristics of the PEG port.

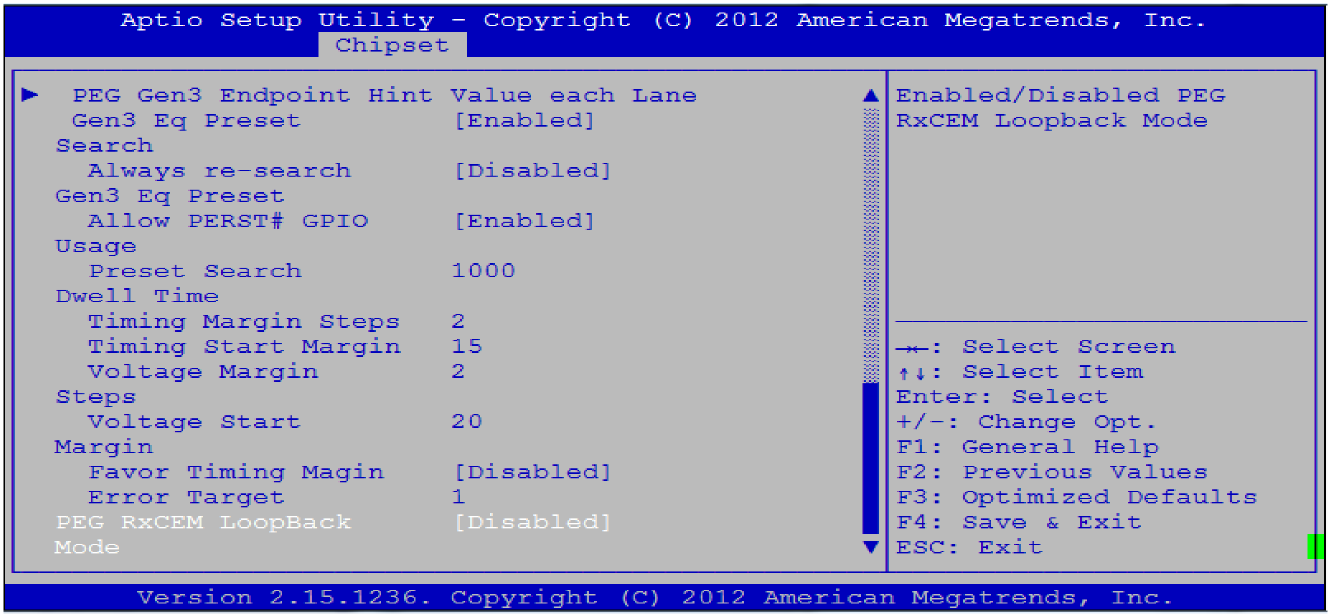
Fig. 2.3.2.3.b NB PCIe Configuration (Screen 2 of 3)



```
      Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                     Chipset

  PEG2 De-emphasis          [-3.5 dB]            ▲ Enable or disable
  Control                                          GPIO-based resets to
  PEG0 - ASPM               [Auto]                 PEG endpoint(s) during
  PEG1 - ASPM               [Auto]                 margin search, if needed
  PEG2 - ASPM               [Auto]
  PEG Sampler Calibrate     [Disabled]
  Swing Control             [Full]
  PEG Gen3 Equalization     [Enabled]
   Gen3 Eq Phase 2          [Enabled]
▶  PEG Gen3 Root Port Preset Value for each Lane
▶  PEG Gen3 Endpoint Preset Value each Lane        →←: Select Screen
▶  PEG Gen3 Endpoint Hint Value each Lane          ↑↓: Select Item
   Gen3 Eq Preset           [Enabled]              Enter: Select
  Search                                           +/-: Change Opt.
    Always re-search        [Disabled]             F1: General Help
  Gen3 Eq Preset                                   F2: Previous Values
    Allow PERST# GPIO       [Enabled]              F3: Optimized Defaults
  Usage                                            F4: Save & Exit
                                                 ▼ ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
PEG ASPM		Active State Power Management control for user to disable if needed.
PEG Sampler Calibrate		Default is disabled. Additional calibration action for the PEG slot PCIe lanes.
Swing Control		Default is full. Control allows user to setup the MCH for either half or full swing control.
PEG Gen3 Equalization		Default is enabled. Control over the equalization process to ensure PCIe Gen3 links are working at the optimal speed.

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

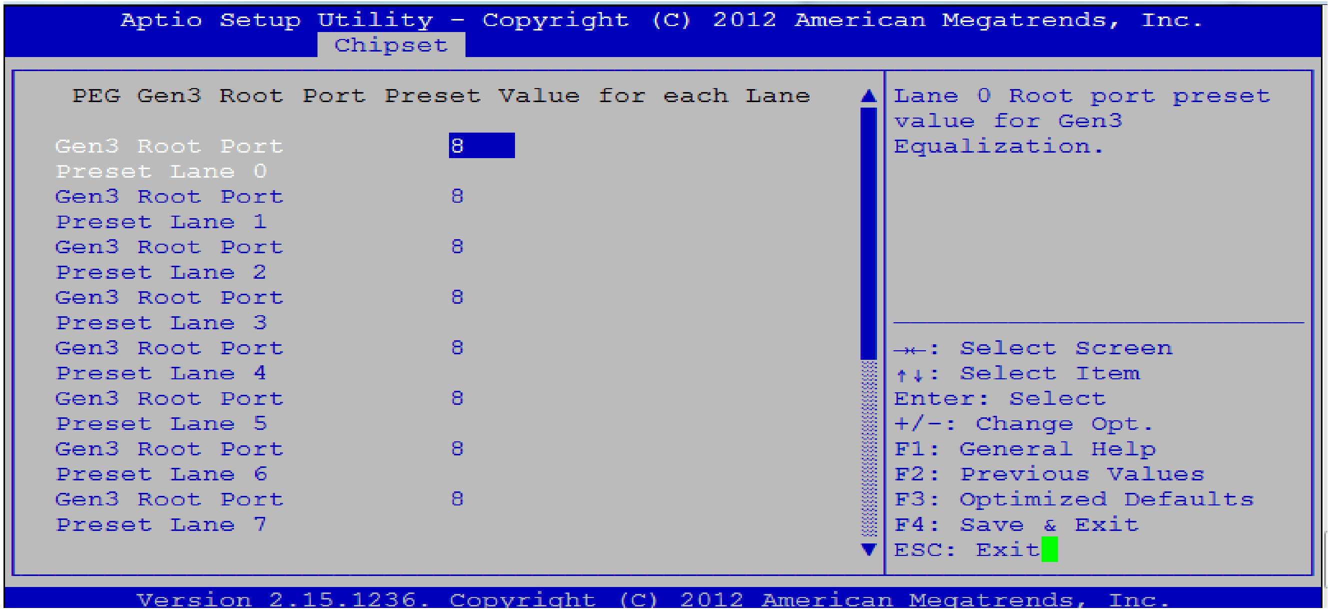


```
      Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                     Chipset

▶  PEG Gen3 Endpoint Hint Value each Lane        ▲ Enabled/Disabled PEG
   Gen3 Eq Preset           [Enabled]              RxCEM Loopback Mode
  Search
    Always re-search        [Disabled]
  Gen3 Eq Preset
    Allow PERST# GPIO       [Enabled]
  Usage
    Preset Search           1000
  Dwell Time
    Timing Margin Steps     2
    Timing Start Margin     15                     →←: Select Screen
    Voltage Margin          2                      ↑↓: Select Item
  Steps                                            Enter: Select
    Voltage Start           20                     +/-: Change Opt.
  Margin                                           F1: General Help
    Favor Timing Magin      [Disabled]             F2: Previous Values
    Error Target            1                      F3: Optimized Defaults
  PEG RxCEM LoopBack        [Disabled]             F4: Save & Exit
  Mode                                           ▼ ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
PEG RxCEM LoopBack Mode		Disabled by default. Check with Intel about hardware implications.

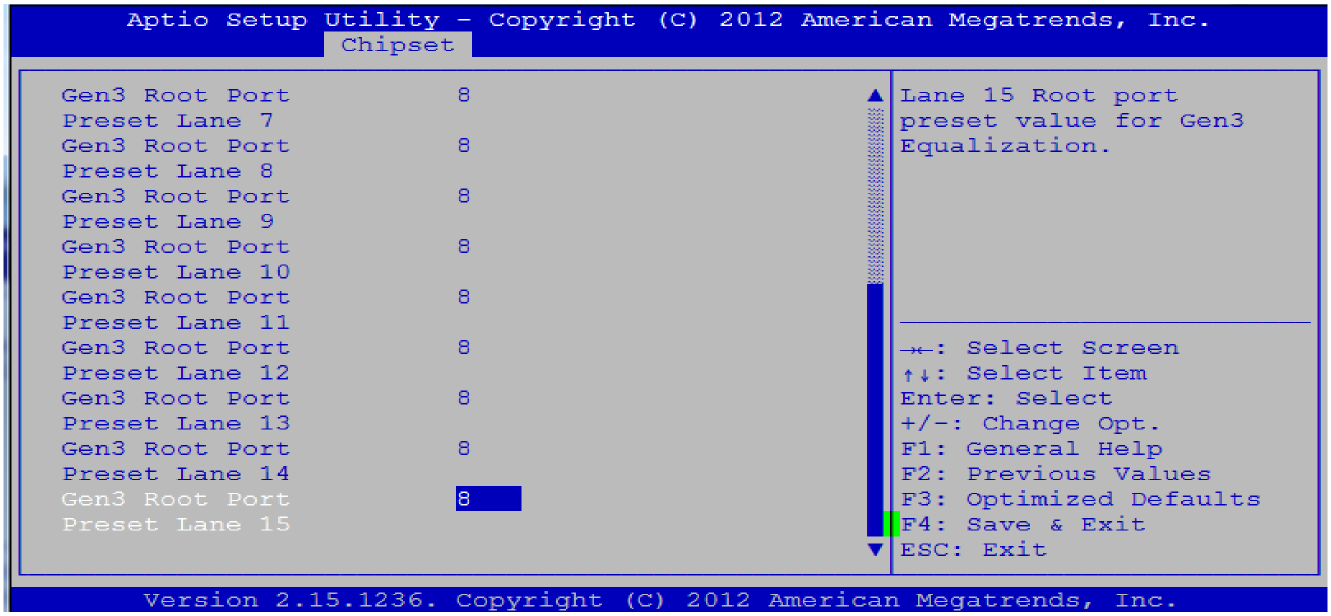
2.3.2.3.1 PEG Gen3 Root Port Preset Value

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



```
   Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                       Chipset

  PEG Gen3 Root Port Preset Value for each Lane        Lane 0 Root port preset
                                                        value for Gen3
 Gen3 Root Port           8                             Equalization.
 Preset Lane 0
 Gen3 Root Port           8
 Preset Lane 1
 Gen3 Root Port           8
 Preset Lane 2
 Gen3 Root Port           8
 Preset Lane 3
 Gen3 Root Port           8                             →←: Select Screen
 Preset Lane 4                                          ↑↓: Select Item
 Gen3 Root Port           8                             Enter: Select
 Preset Lane 5                                          +/-: Change Opt.
 Gen3 Root Port           8                             F1: General Help
 Preset Lane 6                                          F2: Previous Values
 Gen3 Root Port           8                             F3: Optimized Defaults
 Preset Lane 7                                          F4: Save & Exit
                                                        ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

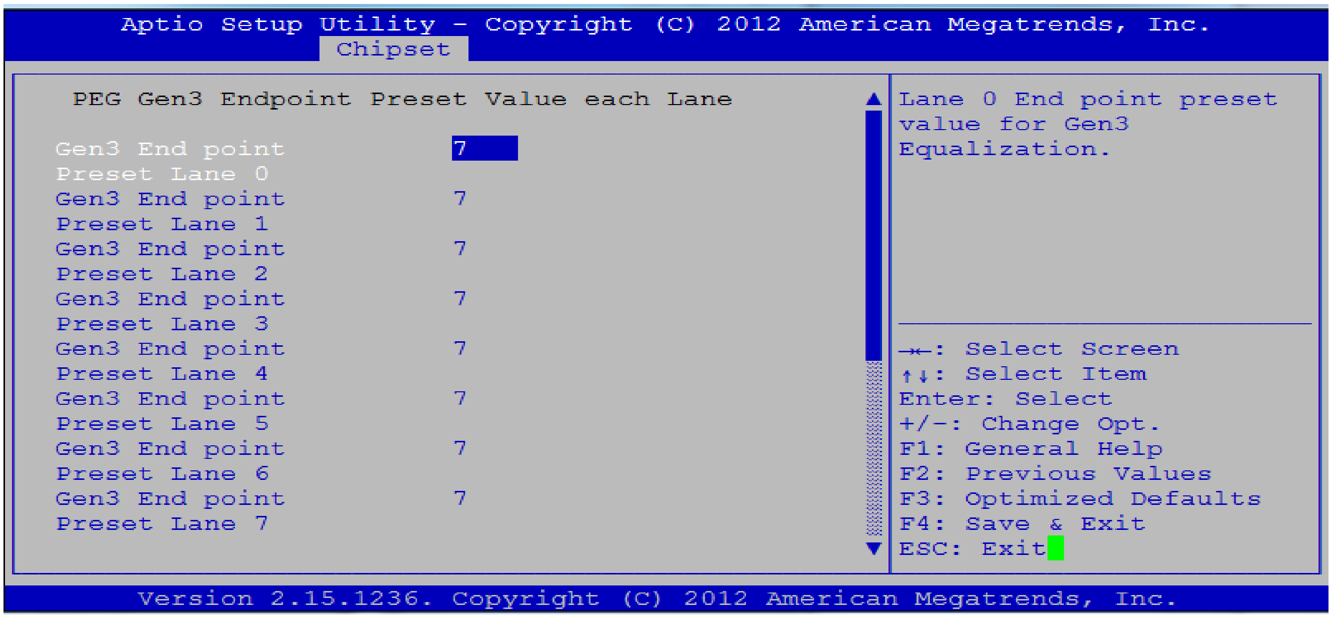
Fig. 2.3.2.3.1.b PEG Gen3 Root Port Preset Value (Screen 2 of 2)



```
   Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                       Chipset

 Gen3 Root Port           8                             Lane 15 Root port
 Preset Lane 7                                          preset value for Gen3
 Gen3 Root Port           8                             Equalization.
 Preset Lane 8
 Gen3 Root Port           8
 Preset Lane 9
 Gen3 Root Port           8
 Preset Lane 10
 Gen3 Root Port           8
 Preset Lane 11
 Gen3 Root Port           8                             →←: Select Screen
 Preset Lane 12                                         ↑↓: Select Item
 Gen3 Root Port           8                             Enter: Select
 Preset Lane 13                                         +/-: Change Opt.
 Gen3 Root Port           8                             F1: General Help
 Preset Lane 14                                         F2: Previous Values
 Gen3 Root Port           8                             F3: Optimized Defaults
 Preset Lane 15                                         F4: Save & Exit
                                                        ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.3.2.3.2 PEG Gen3 Endpoint Preset Value

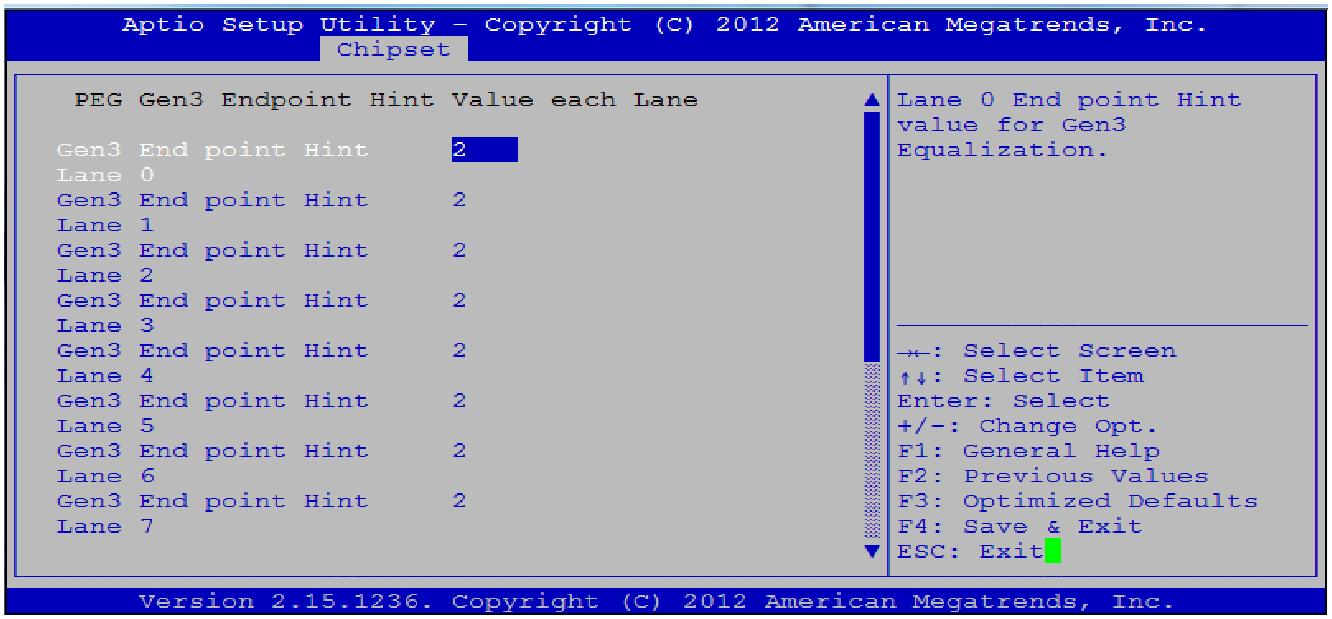
Fig. 2.3.2.3.2.a PEG Gen3 Endpoint Preset Value



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                          Chipset

   PEG Gen3 Endpoint Preset Value each Lane          ▲ Lane 0 End point preset
                                                       value for Gen3
  Gen3 End point            7                          Equalization.
  Preset Lane 0
  Gen3 End point            7
  Preset Lane 1
  Gen3 End point            7
  Preset Lane 2
  Gen3 End point            7
  Preset Lane 3
  Gen3 End point            7                          →←: Select Screen
  Preset Lane 4                                        ↑↓: Select Item
  Gen3 End point            7                          Enter: Select
  Preset Lane 5                                        +/-: Change Opt.
  Gen3 End point            7                          F1: General Help
  Preset Lane 6                                        F2: Previous Values
  Gen3 End point            7                          F3: Optimized Defaults
  Preset Lane 7                                        F4: Save & Exit
                                                     ▼ ESC: Exit

         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.3.2.3.3 PEG Gen3 Endpoint Hint Value

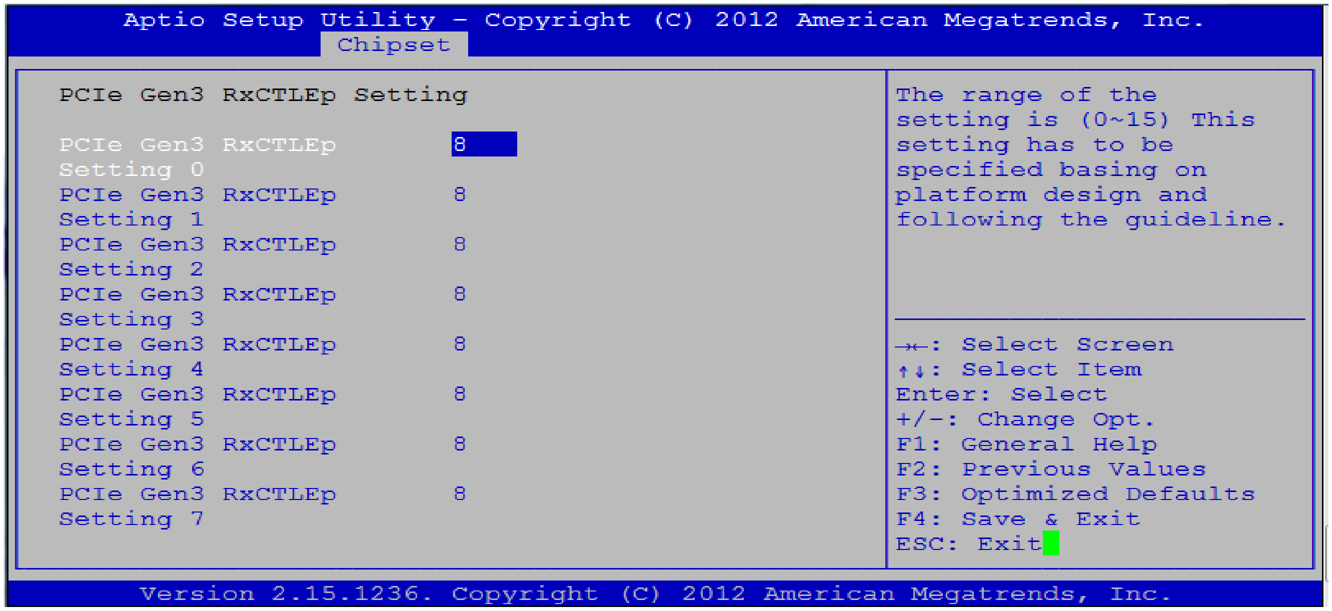
Fig. 2.3.2.3.3.a PEG Gen3 Endpoint Hint Value



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                          Chipset

   PEG Gen3 Endpoint Hint Value each Lane            ▲ Lane 0 End point Hint
                                                       value for Gen3
  Gen3 End point Hint       2                          Equalization.
  Lane 0
  Gen3 End point Hint       2
  Lane 1
  Gen3 End point Hint       2
  Lane 2
  Gen3 End point Hint       2
  Lane 3
  Gen3 End point Hint       2                          →←: Select Screen
  Lane 4                                               ↑↓: Select Item
  Gen3 End point Hint       2                          Enter: Select
  Lane 5                                               +/-: Change Opt.
  Gen3 End point Hint       2                          F1: General Help
  Lane 6                                               F2: Previous Values
  Gen3 End point Hint       2                          F3: Optimized Defaults
  Lane 7                                               F4: Save & Exit
                                                     ▼ ESC: Exit

         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.3.2.3.4 PCIe Gen3 RxCTLEp Setting

Fig. 2.3.2.3.4.a PCIe Gen3 RxCTLEp Setting

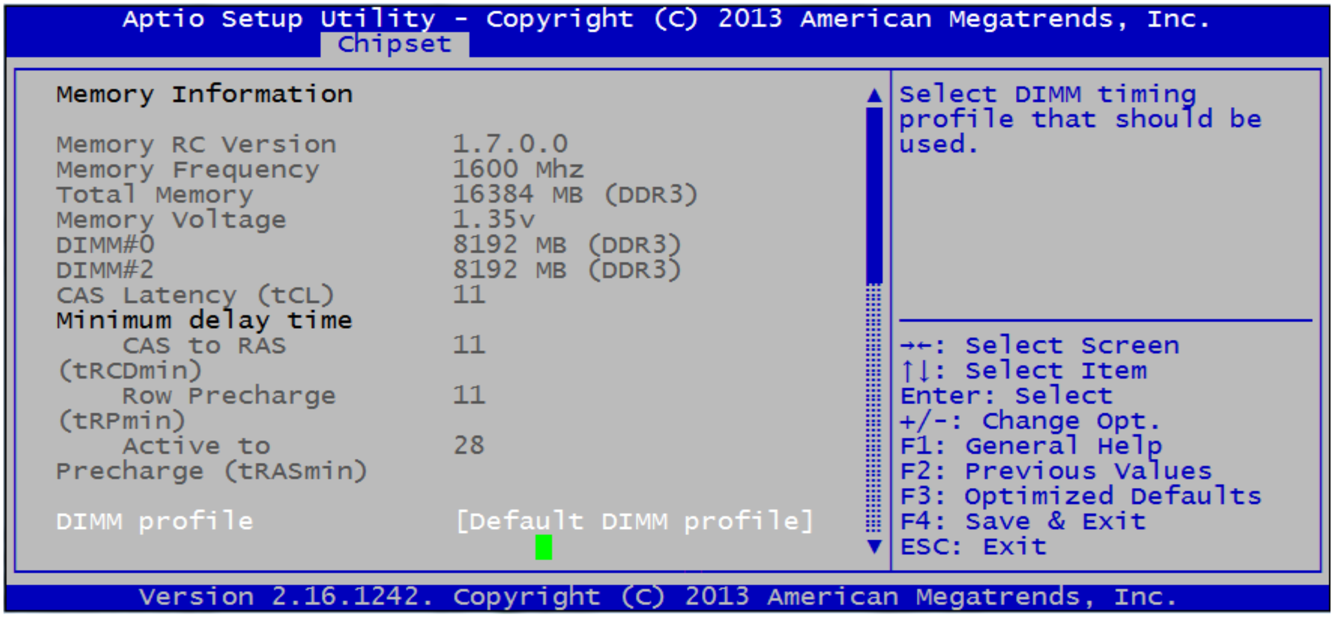


```
     Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                     Chipset

  PCIe Gen3 RxCTLEp Setting                  The range of the
                                             setting is (0~15) This
  PCIe Gen3 RxCTLEp        8                 setting has to be
  Setting 0                                  specified basing on
  PCIe Gen3 RxCTLEp        8                 platform design and
  Setting 1                                  following the guideline.
  PCIe Gen3 RxCTLEp        8
  Setting 2
  PCIe Gen3 RxCTLEp        8
  Setting 3                                  ─────────────────────────
  PCIe Gen3 RxCTLEp        8                 →←: Select Screen
  Setting 4                                  ↑↓: Select Item
  PCIe Gen3 RxCTLEp        8                 Enter: Select
  Setting 5                                  +/-: Change Opt.
  PCIe Gen3 RxCTLEp        8                 F1: General Help
  Setting 6                                  F2: Previous Values
  PCIe Gen3 RxCTLEp        8                 F3: Optimized Defaults
  Setting 7                                  F4: Save & Exit
                                             ESC: Exit

      Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Feature	Options	Description
PCIe Gen3 RxCTLEp Setting		Default is CRB value. This is a tuning parameter related to trace lengths of the particular board. Should be set based on board design and Intel guidelines.

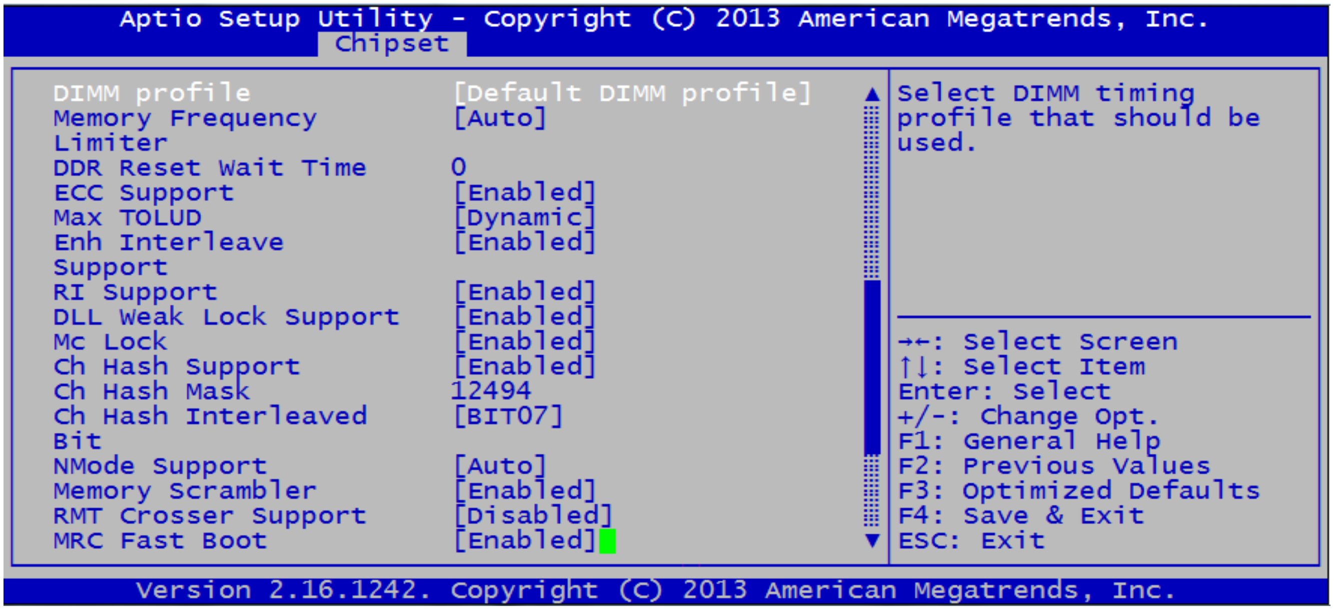
2.3.2.4 Memory Configuration

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



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                     Chipset
  Memory Information                                   Select DIMM timing
                                                       profile that should be
  Memory RC Version          1.7.0.0                   used.
  Memory Frequency           1600 Mhz
  Total Memory               16384 MB (DDR3)
  Memory Voltage             1.35v
  DIMM#0                     8192 MB (DDR3)
  DIMM#2                     8192 MB (DDR3)
  CAS Latency (tCL)          11
  Minimum delay time
      CAS to RAS             11                        →←: Select Screen
  (tRCDmin)                                            ↑↓: Select Item
      Row Precharge          11                        Enter: Select
  (tRPmin)                                             +/-: Change Opt.
      Active to              28                        F1: General Help
  Precharge (tRASmin)                                  F2: Previous Values
                                                       F3: Optimized Defaults
  DIMM profile               [Default DIMM profile]    F4: Save & Exit
                                                       ESC: Exit
        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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

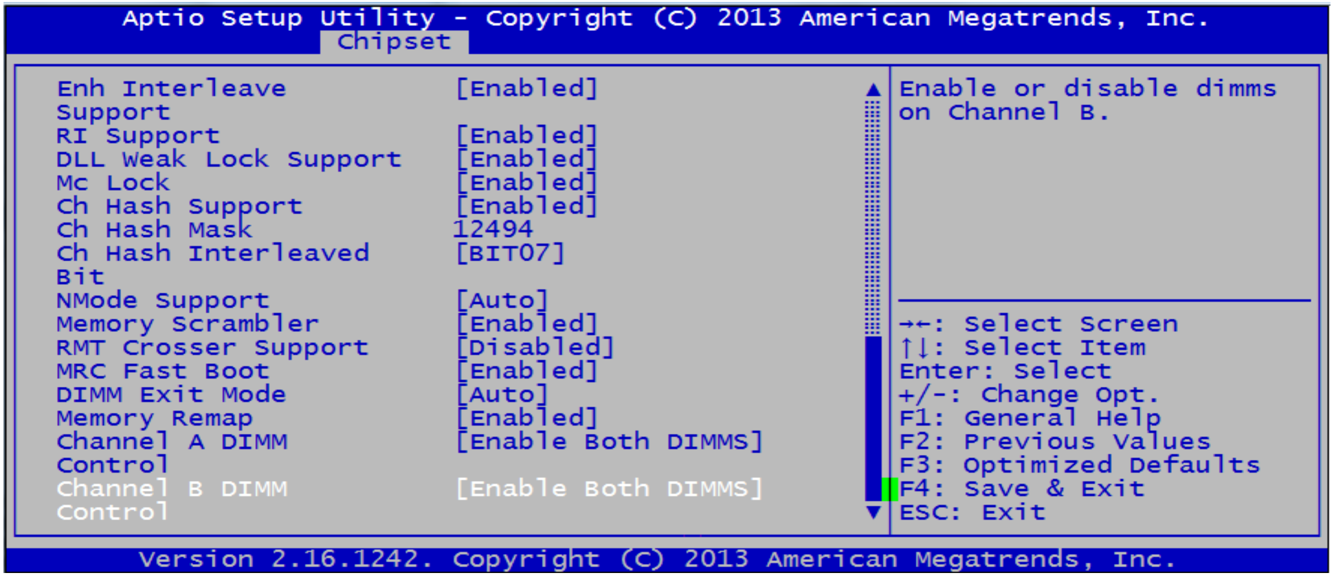


```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                     Chipset
  DIMM profile               [Default DIMM profile]    Select DIMM timing
  Memory Frequency           [Auto]                    profile that should be
  Limiter                                              used.
  DDR Reset Wait Time        0
  ECC Support                [Enabled]
  Max TOLUD                  [Dynamic]
  Enh Interleave             [Enabled]
  Support
  RI Support                 [Enabled]
  DLL Weak Lock Support      [Enabled]
  Mc Lock                    [Enabled]                 →←: Select Screen
  Ch Hash Support            [Enabled]                 ↑↓: Select Item
  Ch Hash Mask               12494                     Enter: Select
  Ch Hash Interleaved        [BIT07]                   +/-: Change Opt.
  Bit                                                  F1: General Help
  NMode Support              [Auto]                    F2: Previous Values
  Memory Scrambler           [Enabled]                 F3: Optimized Defaults
  RMT Crosser Support        [Disabled]                F4: Save & Exit
  MRC Fast Boot              [Enabled]                 ESC: Exit
        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Feature	Options	Description
DIMM Profile		Default is the DIMM SPD profile. A mechanism to allow the user to change the memory timing parameter profiles to XMP (if supported by DIMM) or even a custom profile.
Memory Frequency Limiter		Auto is default. A control to allow the user to limit the frequency memory runs at. Auto should result in published memory frequency – if the MRC supports that frequency on that DIMM.

DDR Reset Wait Time		Default is 2,000,000 nS. A wait time for DDR voltage changes after a reset.
ECC Support		Enabled by default. Allows user to disable ECC operation when ECC DRAMs are installed if desired.
Max TOLUD		Set for Dynamic by default. Feature to specify the Top Of Low User Dram. This is the point where DRAM ends and PCI MMIO begins below 4GB in the memory map. Dynamic means the bios figures out what PCI resources are needed in the current configuration then sets the top of DRAM accordingly. If re-mapping is enabled the DRAM between this point and 4GB will be moved to available space above 4GB in the address map.
Enh Interleave Support		Enabled by default. Control for the Enhanced Interleaving feature of the memory controller.
RI Support		Enabled by default. Control for the Rank Interleaving feature of the memory controller.
DLL Weak Lock Support		Enabled by default. Control over delay locked loop feature of the memory signal timings.
Mc Lock		Default is enabled. Enables chipset feature to lock registers related to memory configuration so that they cannot be changed at runtime.
Ch Hash Support		Enabled by default . Checksum and data validity/integrity checks.
Ch Hash Mask		Set to 0x30CE by default. Checksum and data validity/integrity checks.
Ch Hash Interleaved Bit		Set to Bit7 by default. Checksum and data validity/integrity checks.
NMode Support		Auto by default. Can be 1N, 2N or Auto. Check with Intel about hardware implications.
Memory Scrambler		Enabled by default. Chipset feature to randomize memory usage somewhat to avoid potentially inducing unintended bit changes in adjacent cells. See also Row Hammer.
RMT Crosser Support		Disabled by default. Control of the Rank Margining Tool that can be used by hardware folks to ensure the memory trainings are optimum during development.
MRC Fast Boot		Enabled by default. Allows MRC to use ‘remembered’ training data to speed up MRC execution if nothing has changed related to memory.

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

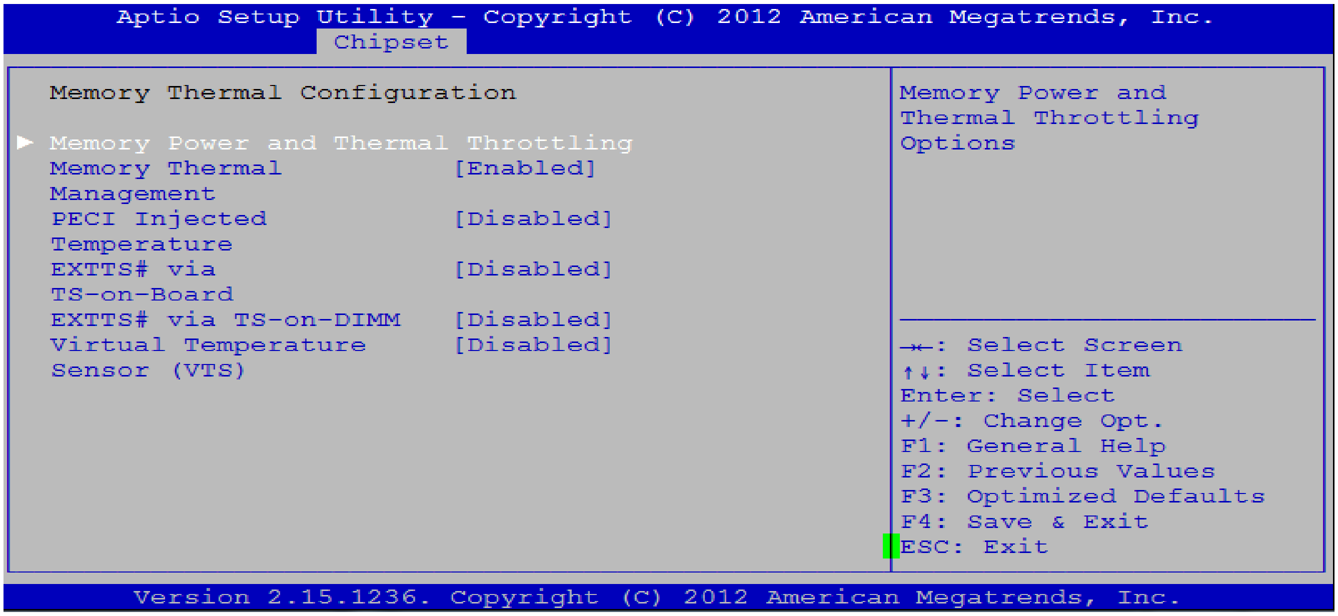


```
     Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                   Chipset
   Enh Interleave           [Enabled]            ▲ Enable or disable dimms
   Support                                         on Channel B.
   RI Support               [Enabled]
   DLL Weak Lock Support    [Enabled]
   Mc Lock                  [Enabled]
   Ch Hash Support          [Enabled]
   Ch Hash Mask             12494
   Ch Hash Interleaved      [BIT07]
   Bit
   NMode Support            [Auto]
   Memory Scrambler         [Enabled]              →←: Select Screen
   RMT Crosser Support      [Disabled]             ↑↓: Select Item
   MRC Fast Boot            [Enabled]              Enter: Select
   DIMM Exit Mode           [Auto]                 +/-: Change Opt.
   Memory Remap             [Enabled]              F1: General Help
   Channel A DIMM           [Enable Both DIMMS]    F2: Previous Values
   Control                                         F3: Optimized Defaults
   Channel B DIMM           [Enable Both DIMMS]    F4: Save & Exit
   Control                                       ▼ ESC: Exit
      Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Feature	Options	Description
DIMM Exit Mode		Auto by default. Slow exit mode saves more power than fast exit mode.
Memory Remap		Enabled by default. Control to determine whether DRAM memory displaced by the PCI/PCIe/MMIO region below 4GB in the address map should be remapped to appear above 4GB (e.g. a 1GB region for 32-bit PCI devices in a system with 8GB installed DRAM would result in the loss of 1GB of DRAM unless remapped to appear between 8GB and 9GB in the address map.
Channel A DIMM Control		Both DIMMs enabled by default. Allows either or both DIMMs on Channel A to be disabled.
Channel B DIMM Control		Both DIMMs enabled by default. Allows either or both DIMMs on Channel B to be disabled.
GDXC Support		Control for chipset feature Generic Debug eXternal Connection which allows for monitoring of traffic between IA cores and other signals with appropriate equipment.

2.3.2.5 Memory Thermal Configuration

Fig. 2.3.2.5.a Memory Thermal Configuration

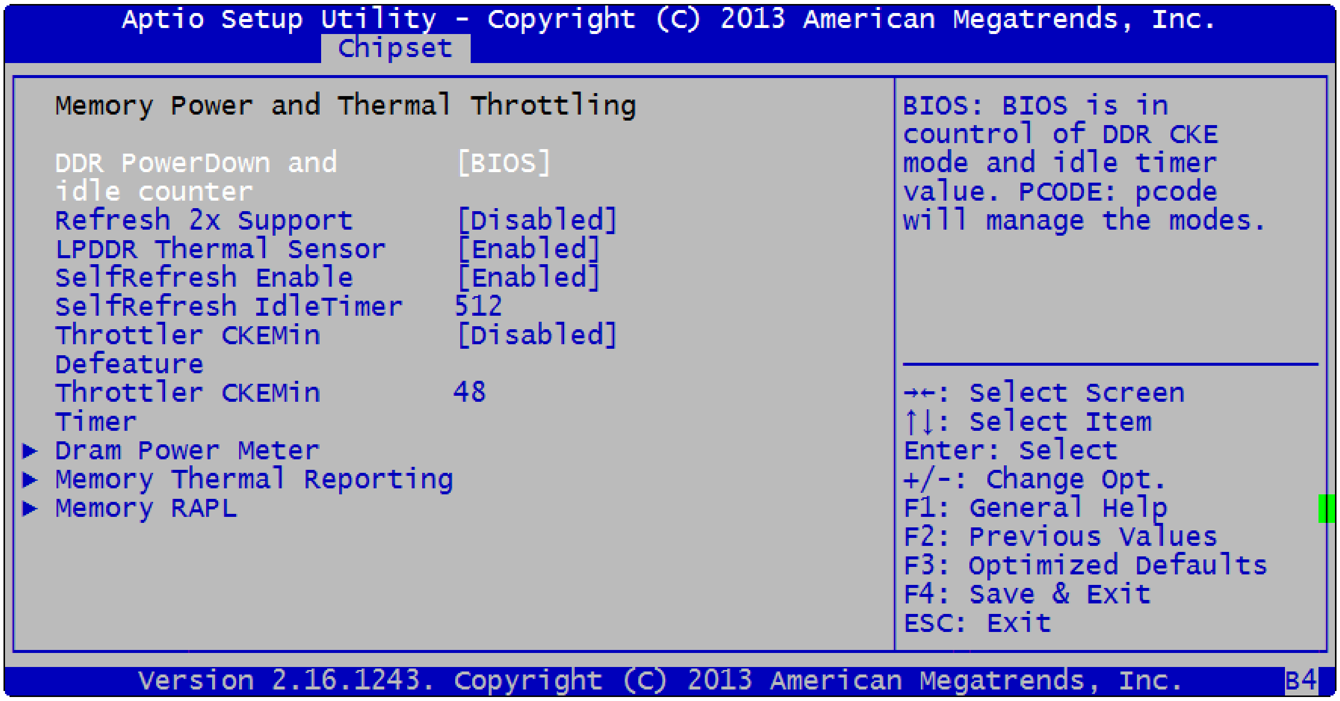


```
      Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                         Chipset

  Memory Thermal Configuration                         Memory Power and
                                                       Thermal Throttling
► Memory Power and Thermal Throttling                  Options
  Memory Thermal              [Enabled]
  Management
  PECI Injected               [Disabled]
  Temperature
  EXTTS# via                  [Disabled]
  TS-on-Board
  EXTTS# via TS-on-DIMM       [Disabled]
  Virtual Temperature         [Disabled]               →←: Select Screen
  Sensor (VTS)                                         ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit

       Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

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

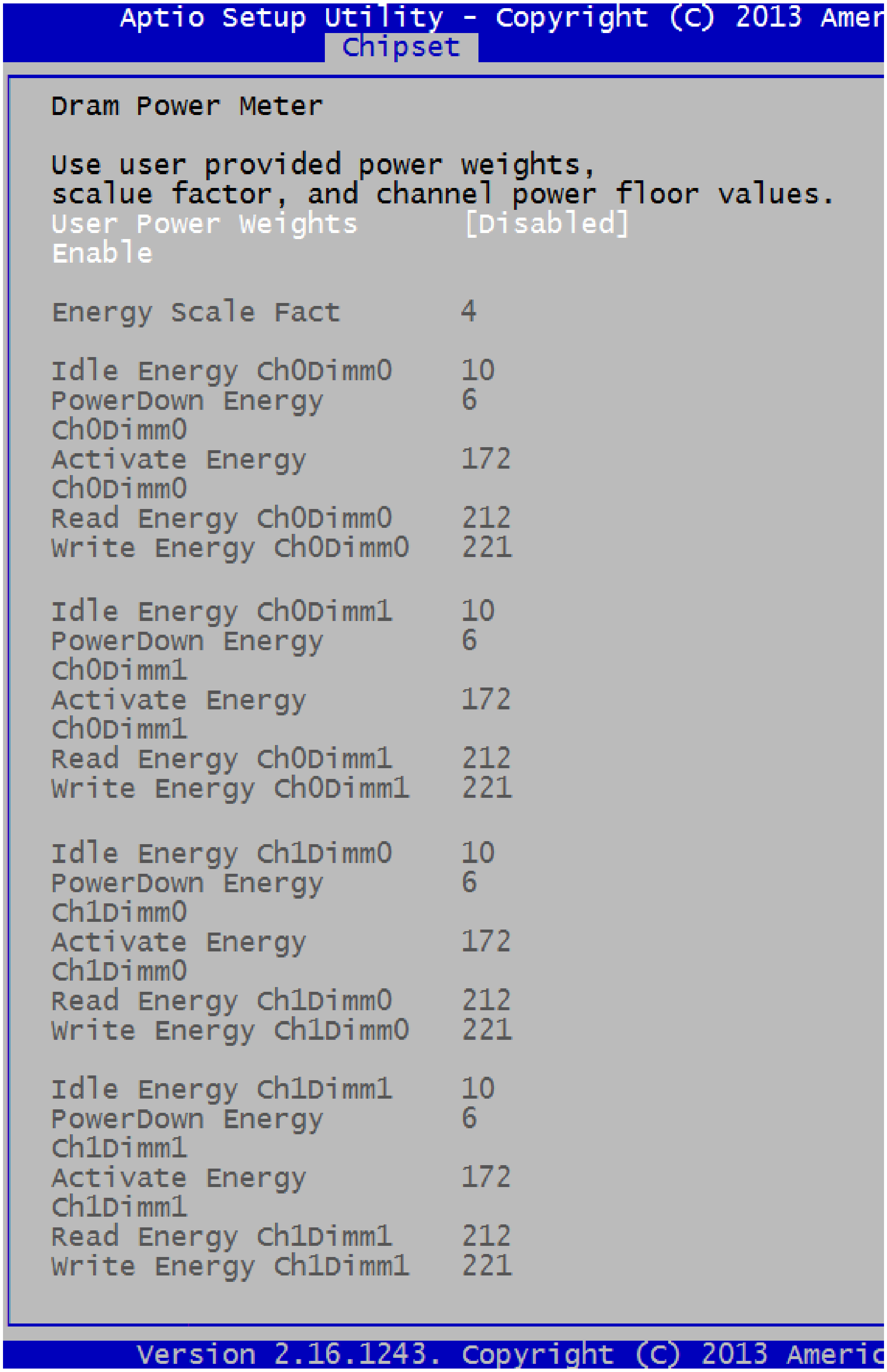


```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                  Chipset
  Memory Power and Thermal Throttling             BIOS: BIOS is in
                                                  control of DDR CKE
  DDR PowerDown and            [BIOS]             mode and idle timer
  idle counter                                    value. PCODE: pcode
  Refresh 2x Support           [Disabled]         will manage the modes.
  LPDDR Thermal Sensor         [Enabled]
  SelfRefresh Enable           [Enabled]
  SelfRefresh IdleTimer        512
  Throttler CKEMin             [Disabled]
  Defeature
  Throttler CKEMin             48                 →←: Select Screen
  Timer                                           ↑↓: Select Item
▶ Dram Power Meter                                Enter: Select
▶ Memory Thermal Reporting                        +/-: Change Opt.
▶ Memory RAPL                                     F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit
      Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.     B4
```

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

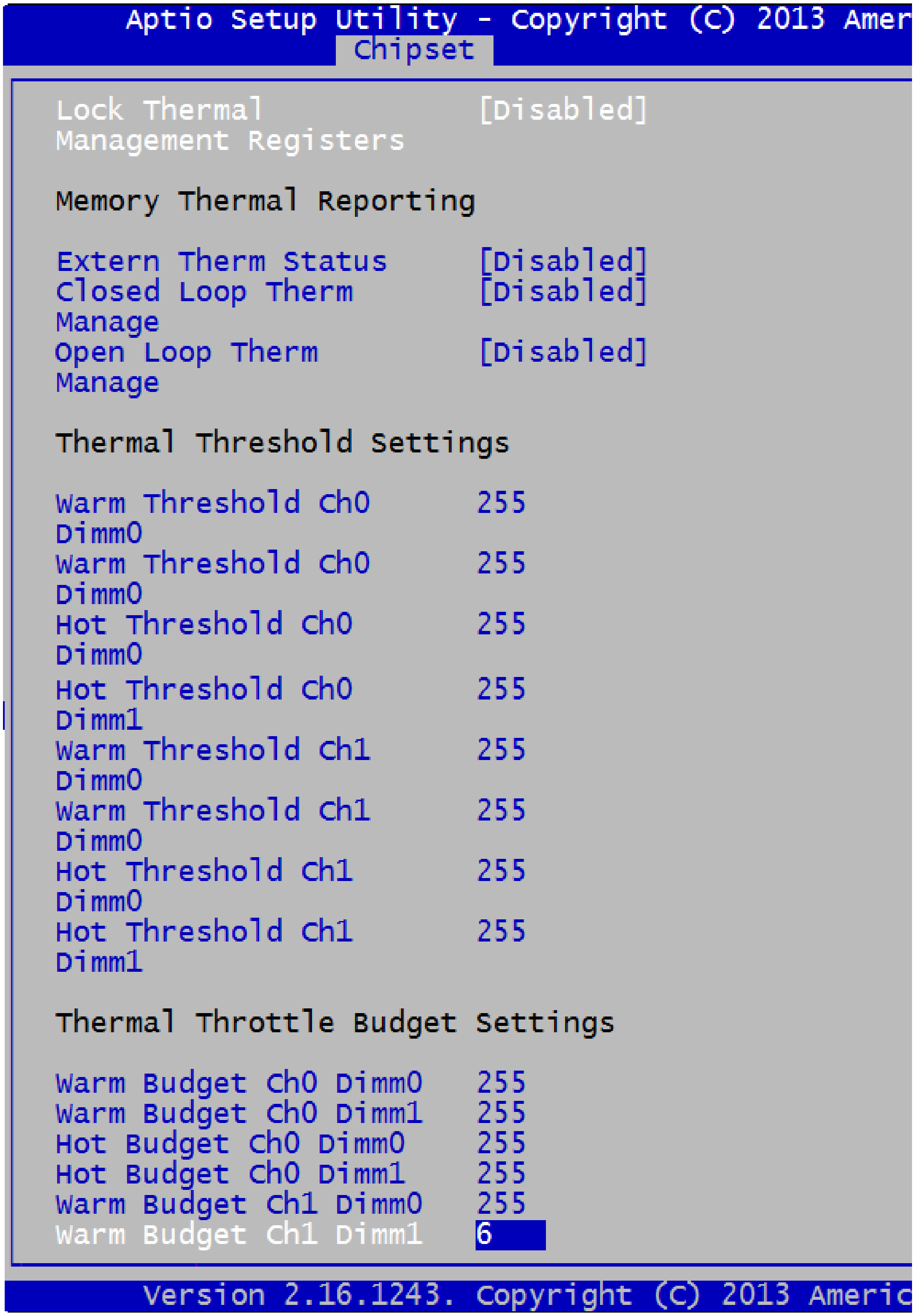


```
      Aptio Setup Utility - Copyright (C) 2013 Amer
                          Chipset

  Dram Power Meter

  Use user provided power weights,
  scalue factor, and channel power floor values.
  User Power Weights       [Disabled]
  Enable

  Energy Scale Fact        4

  Idle Energy Ch0Dimm0     10
  PowerDown Energy         6
  Ch0Dimm0
  Activate Energy          172
  Ch0Dimm0
  Read Energy Ch0Dimm0     212
  Write Energy Ch0Dimm0    221

  Idle Energy Ch0Dimm1     10
  PowerDown Energy         6
  Ch0Dimm1
  Activate Energy          172
  Ch0Dimm1
  Read Energy Ch0Dimm1     212
  Write Energy Ch0Dimm1    221

  Idle Energy Ch1Dimm0     10
  PowerDown Energy         6
  Ch1Dimm0
  Activate Energy          172
  Ch1Dimm0
  Read Energy Ch1Dimm0     212
  Write Energy Ch1Dimm0    221

  Idle Energy Ch1Dimm1     10
  PowerDown Energy         6
  Ch1Dimm1
  Activate Energy          172
  Ch1Dimm1
  Read Energy Ch1Dimm1     212
  Write Energy Ch1Dimm1    221

        Version 2.16.1243. Copyright (C) 2013 Americ
```

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

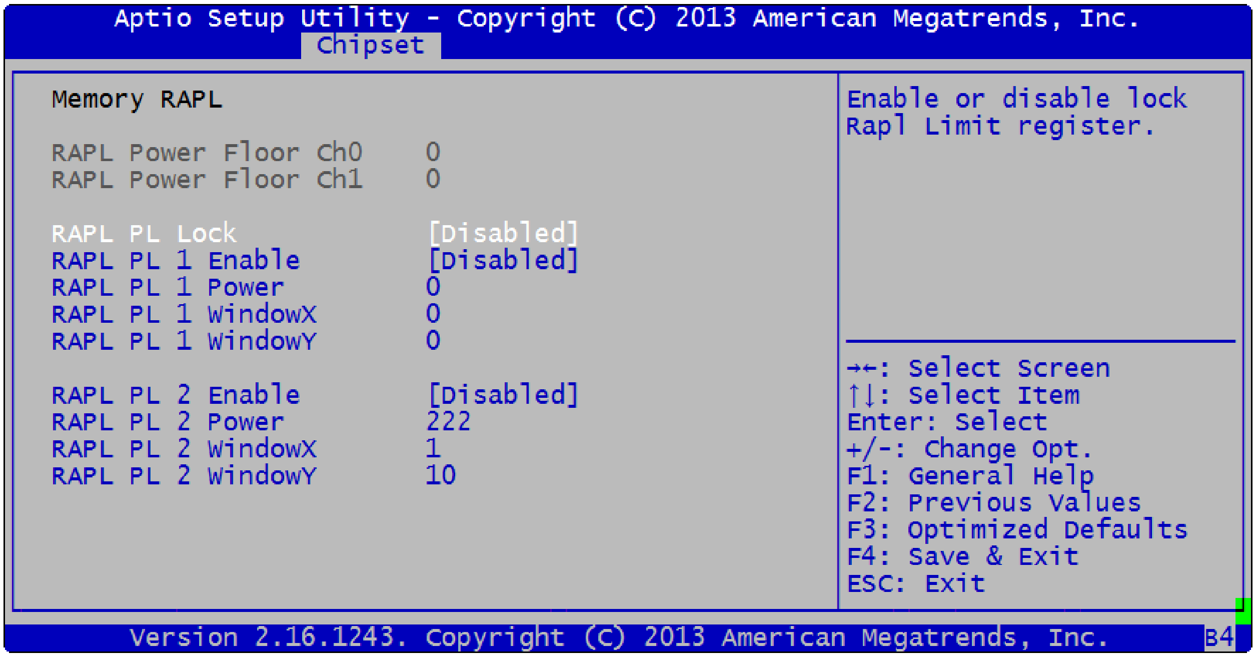


```
     Aptio Setup Utility - Copyright (C) 2013 Amer
                        Chipset

  Lock Thermal                 [Disabled]
  Management Registers

  Memory Thermal Reporting

  Extern Therm Status          [Disabled]
  Closed Loop Therm            [Disabled]
  Manage
  Open Loop Therm              [Disabled]
  Manage

  Thermal Threshold Settings

  Warm Threshold Ch0           255
  Dimm0
  Warm Threshold Ch0           255
  Dimm0
  Hot Threshold Ch0            255
  Dimm0
  Hot Threshold Ch0            255
  Dimm1
  Warm Threshold Ch1           255
  Dimm0
  Warm Threshold Ch1           255
  Dimm0
  Hot Threshold Ch1            255
  Dimm0
  Hot Threshold Ch1            255
  Dimm1

  Thermal Throttle Budget Settings

  Warm Budget Ch0 Dimm0        255
  Warm Budget Ch0 Dimm1        255
  Hot Budget Ch0 Dimm0         255
  Hot Budget Ch0 Dimm1         255
  Warm Budget Ch1 Dimm0        255
  Warm Budget Ch1 Dimm1        6

        Version 2.16.1243. Copyright (C) 2013 Americ
```

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



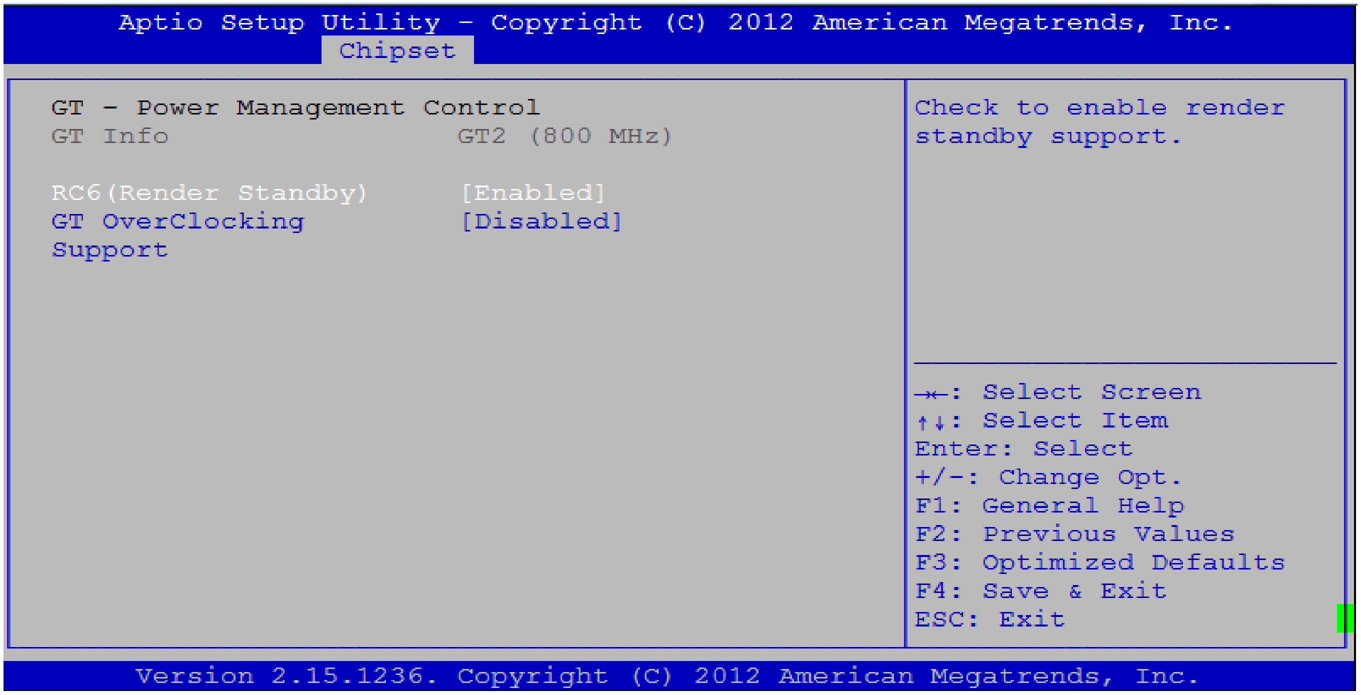
```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
                      Chipset
 Memory RAPL                                       Enable or disable lock
                                                   Rapl Limit register.
 RAPL Power Floor Ch0     0
 RAPL Power Floor Ch1     0

 RAPL PL Lock             [Disabled]
 RAPL PL 1 Enable         [Disabled]
 RAPL PL 1 Power          0
 RAPL PL 1 WindowX        0
 RAPL PL 1 WindowY        0
                                                   →←: Select Screen
 RAPL PL 2 Enable         [Disabled]               ↑↓: Select Item
 RAPL PL 2 Power          222                      Enter: Select
 RAPL PL 2 WindowX        1                        +/-: Change Opt.
 RAPL PL 2 WindowY        10                       F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit
      Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc.        B4
```

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



```
        Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
                             Chipset

  GT - Power Management Control                   Check to enable render
  GT Info                    GT2 (800 MHz)        standby support.

  RC6(Render Standby)        [Enabled]
  GT OverClocking            [Disabled]
  Support

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

         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

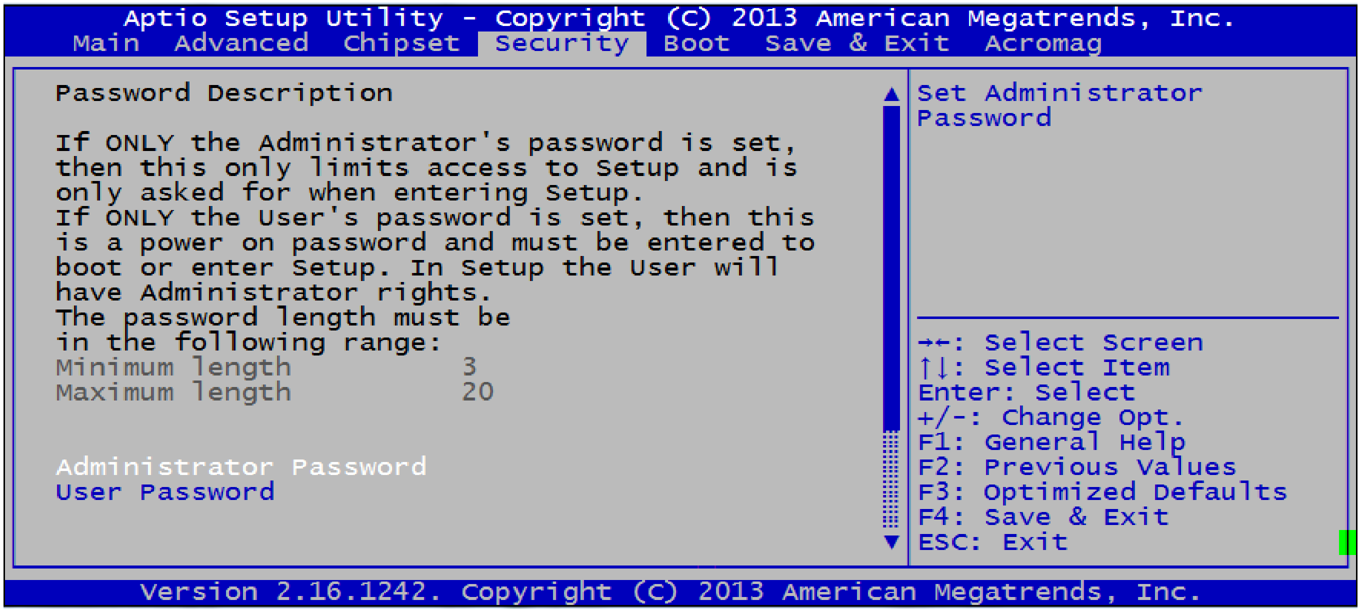
Feature	Options	Description
RC6 (Render Standby)		Enabled by default. Control of Intel graphics controller feature to reduce power consumption when asleep.
GT OverClocking Support		Disabled by default. Gateway control to graphics related frequency and voltage settings used for overclocking purposes.

2.4 Security, Boot, and Save and Exit

2.4.1 Security Screens

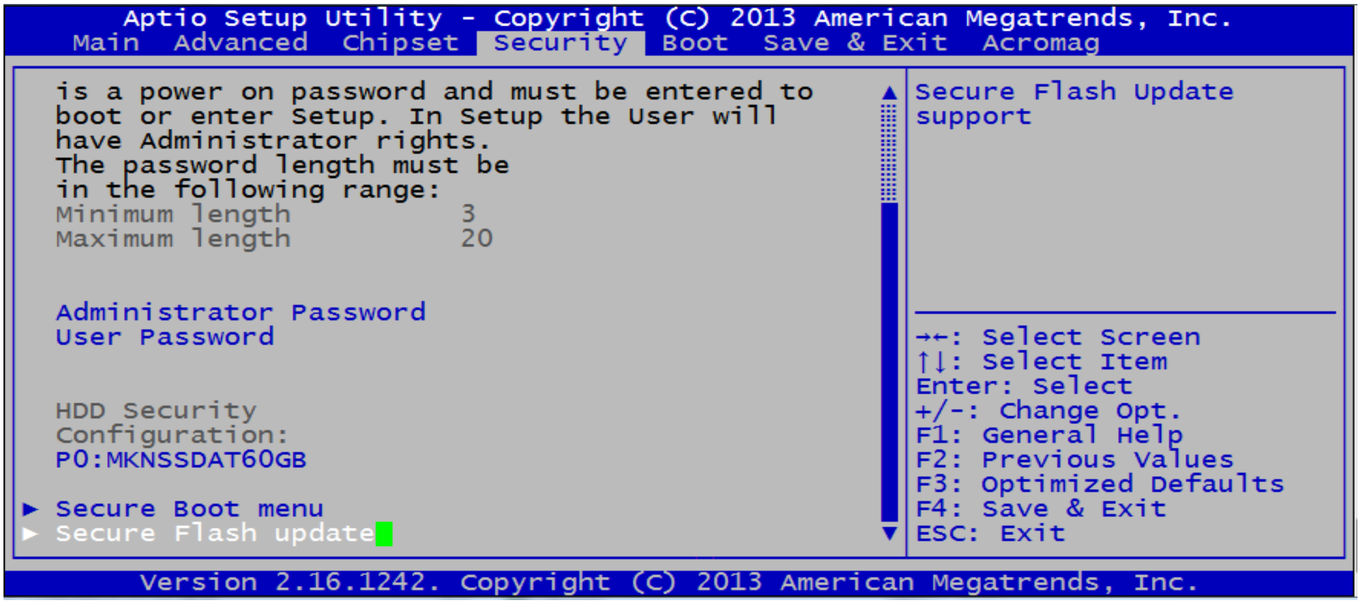
2.4.1.1 Passwords

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



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

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

          Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

   is a power on password and must be entered to  ▲ Secure Flash Update
   boot or enter Setup. In Setup the User will      support
   have Administrator rights.
   The password length must be
   in the following range:
   Minimum length             3
   Maximum length             20

   Administrator Password
   User Password                                    →←: Select Screen
                                                    ↑↓: Select Item
                                                    Enter: Select
   HDD Security                                     +/-: Change Opt.
   Configuration:                                   F1: General Help
   P0:MKNSSDAT60GB                                  F2: Previous Values
                                                    F3: Optimized Defaults
 ▶ Secure Boot menu                                 F4: Save & Exit
 ▶ Secure Flash update                            ▼ ESC: Exit

          Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

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.

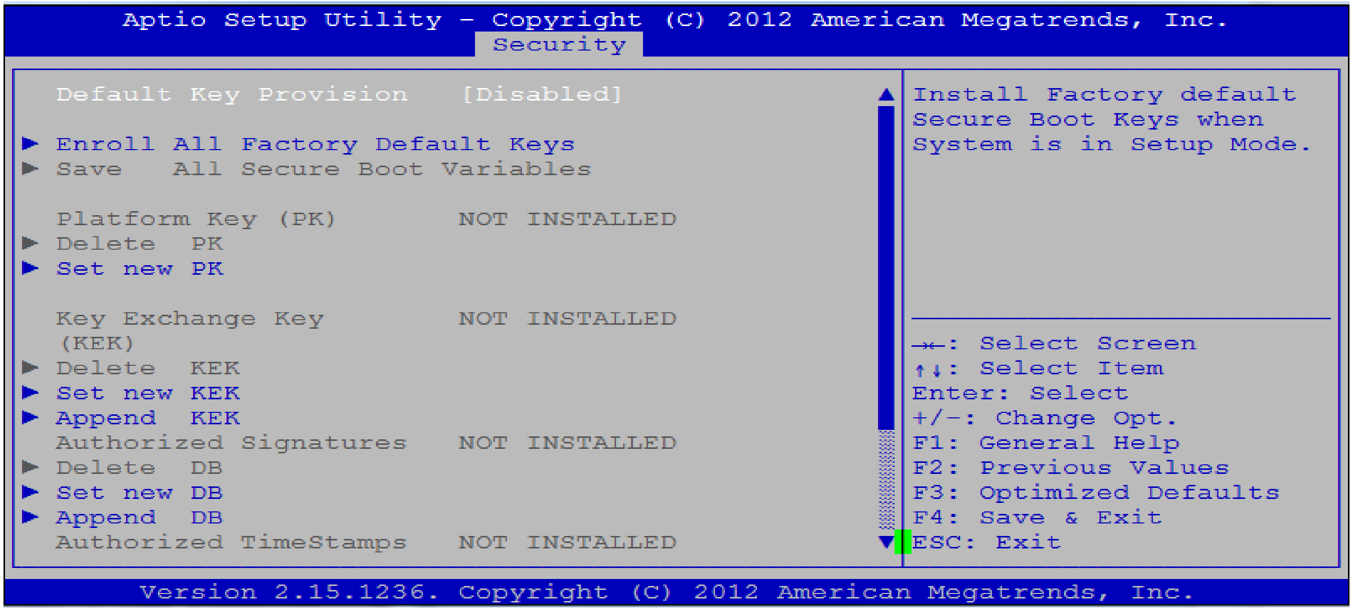
Feature	Description
User Password	This option allows the user to set a user level password for the BIOS. There is no Default password. If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.
Administrator 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.

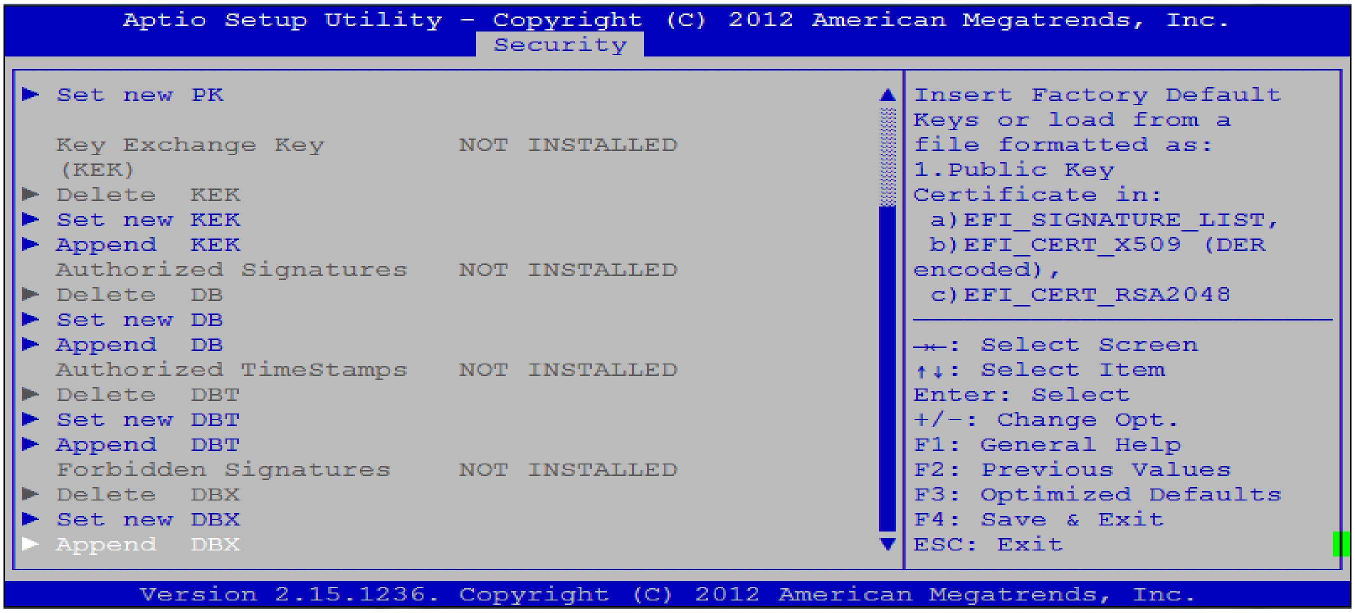
2.4.1.2 Key Management

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



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                              Security

   Default Key Provision       [Disabled]            Install Factory default
                                                     Secure Boot Keys when
▶  Enroll All Factory Default Keys                   System is in Setup Mode.
▶  Save   All Secure Boot Variables

   Platform Key (PK)          NOT INSTALLED
▶  Delete  PK
▶  Set new PK

   Key Exchange Key           NOT INSTALLED          ──────────────────────────
   (KEK)                                             →←: Select Screen
▶  Delete  KEK                                       ↑↓: Select Item
▶  Set new KEK                                       Enter: Select
▶  Append  KEK                                       +/-: Change Opt.
   Authorized Signatures      NOT INSTALLED          F1: General Help
▶  Delete  DB                                        F2: Previous Values
▶  Set new DB                                        F3: Optimized Defaults
▶  Append  DB                                        F4: Save & Exit
   Authorized TimeStamps      NOT INSTALLED          ESC: Exit

         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

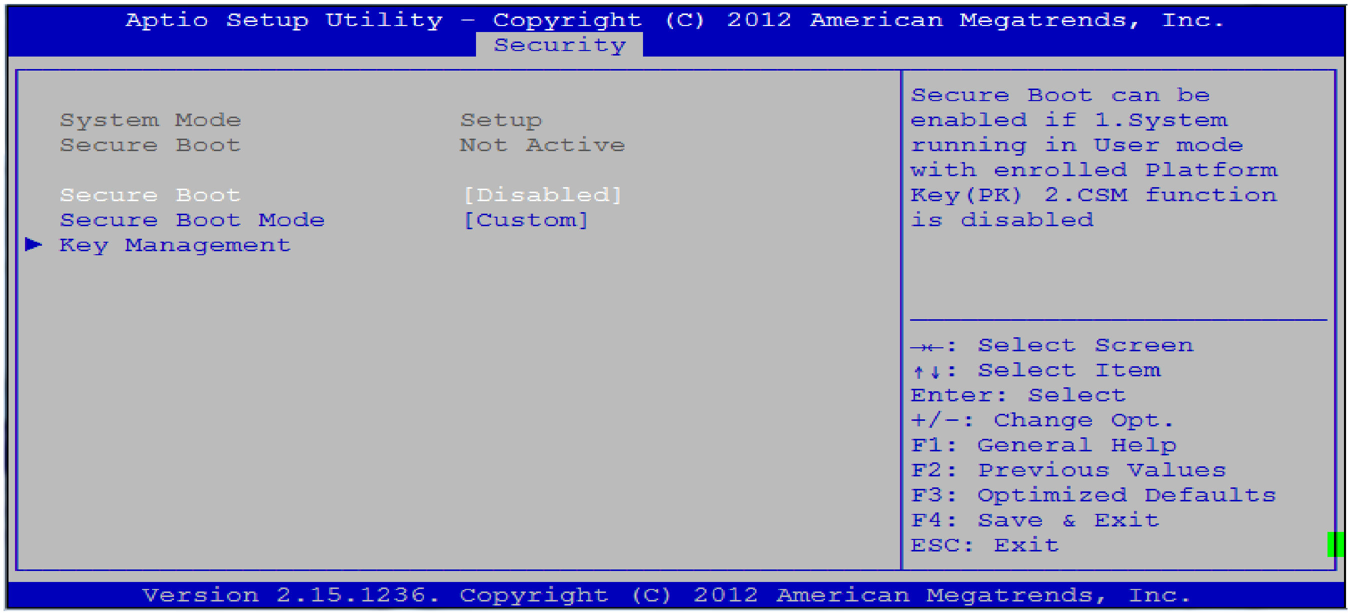
Fig. 2.4.1.2.b Key Management (Screen 2 of 2)



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                              Security

▶  Set new PK                                        Insert Factory Default
                                                     Keys or load from a
   Key Exchange Key           NOT INSTALLED          file formatted as:
   (KEK)                                             1.Public Key
▶  Delete  KEK                                       Certificate in:
▶  Set new KEK                                        a)EFI_SIGNATURE_LIST,
▶  Append  KEK                                        b)EFI_CERT_X509 (DER
   Authorized Signatures      NOT INSTALLED          encoded),
▶  Delete  DB                                         c)EFI_CERT_RSA2048
▶  Set new DB                                        ──────────────────────────
▶  Append  DB                                        →←: Select Screen
   Authorized TimeStamps      NOT INSTALLED          ↑↓: Select Item
▶  Delete  DBT                                       Enter: Select
▶  Set new DBT                                       +/-: Change Opt.
▶  Append  DBT                                       F1: General Help
   Forbidden Signatures       NOT INSTALLED          F2: Previous Values
▶  Delete  DBX                                       F3: Optimized Defaults
▶  Set new DBX                                       F4: Save & Exit
▶  Append  DBX                                       ESC: Exit

         Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.4.1.3 Secure Boot Menu

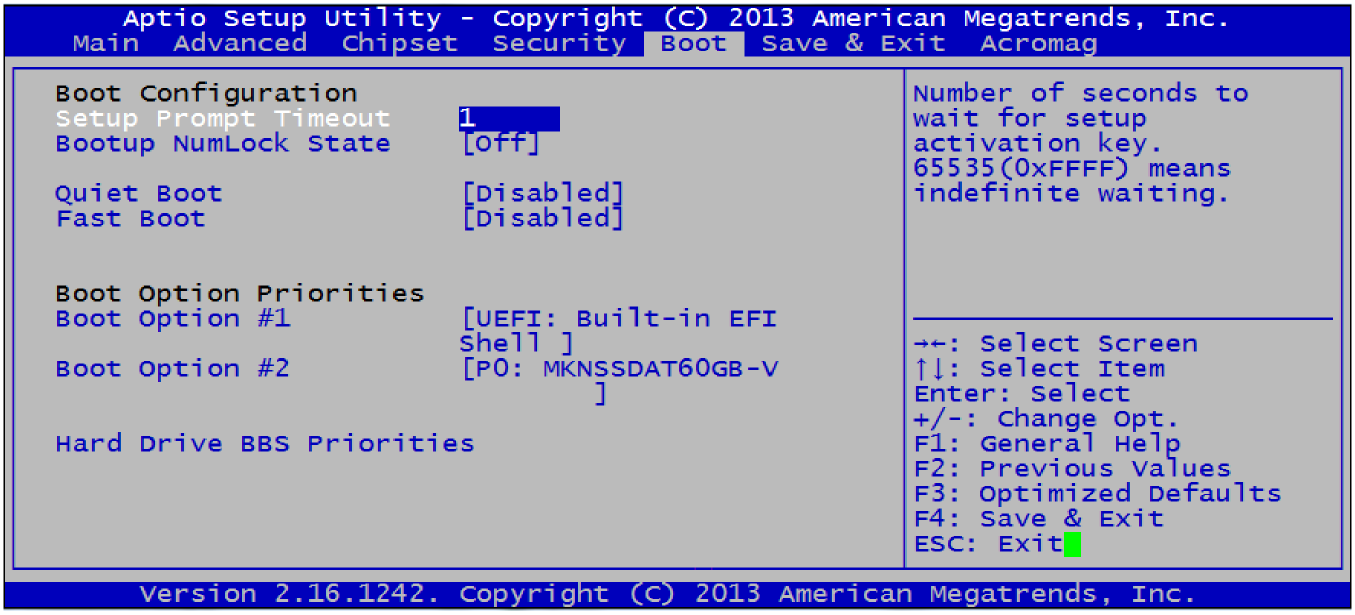
Fig. 2.4.1.3.a Secure Boot Menu



```
        Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
                                 Security

   System Mode                 Setup                  Secure Boot can be
   Secure Boot                 Not Active             enabled if 1.System
                                                      running in User mode
   Secure Boot                 [Disabled]             with enrolled Platform
   Secure Boot Mode            [Custom]               Key(PK) 2.CSM function
 ► Key Management                                     is disabled

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

          Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

2.4.2 Boot Menu

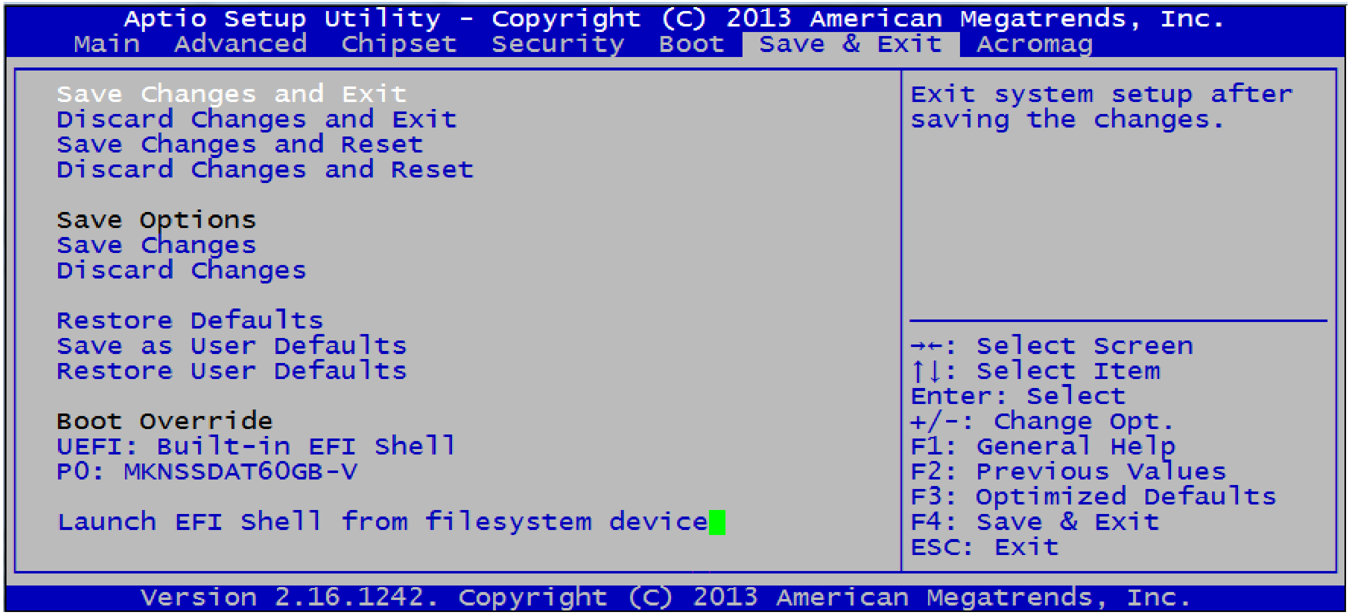
Fig. 2.4.2.a Boot Menu



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
     Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

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


   Boot Option Priorities
   Boot Option #1              [UEFI: Built-in EFI
                               Shell ]                 ______________________
   Boot Option #2              [P0: MKNSSDAT60GB-V     →←: Select Screen
                                      ]                ↑↓: Select Item
                                                       Enter: Select
   Hard Drive BBS Priorities                           +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit

          Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

2.4.3 Save and Exit

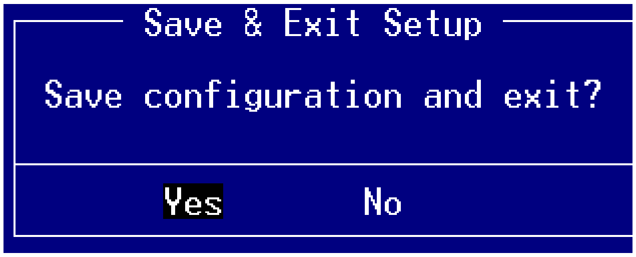
Fig. 2.4.3.a Save and Exit



```
   Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
 Main  Advanced  Chipset  Security  Boot  Save & Exit  Acromag

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

  Save Options
  Save Changes
  Discard Changes

  Restore Defaults
  Save as User Defaults                      →←: Select Screen
  Restore User Defaults                      ↑↓: Select Item
                                             Enter: Select
  Boot Override                              +/-: Change Opt.
  UEFI: Built-in EFI Shell                   F1: General Help
  P0: MKNSSDAT60GB-V                         F2: Previous Values
                                             F3: Optimized Defaults
  Launch EFI Shell from filesystem device    F4: Save & Exit
                                             ESC: Exit
    Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Save Changes and Exit

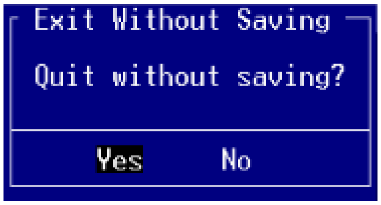
When you have completed the system configuration changes, select this option to save the changes and Exit from BIOS Setup, so the new system configuration parameters can take effect. The following window will appear after selecting the 'Save Changes and Exit' option selected. Select *YES* to Save Changes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



```
Save & Exit Setup

Save configuration and exit?

      Yes        No
```

Discard Changes and Exit

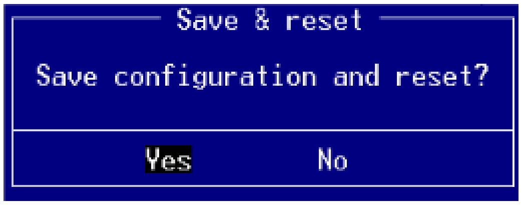
Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after selecting the 'Discard Changes and Exit' option selected. Select *YES* to Discard changes and Exit Setup.



```
Exit Without Saving

Quit without saving?

    Yes     No
```

Save Changes and Reset

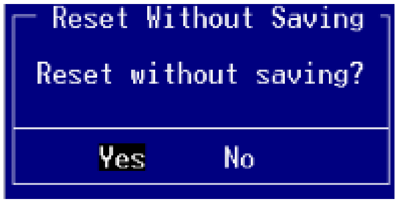
When you have completed the system configuration changes, select this option to save the changes and reboot the system, so the new system configuration parameters can take effect. The following window will appear after selecting the ‘Save Changes and Reset’ option selected. Select *YES* to Save Changes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


Save & reset

Save configuration 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.


Reset Without Saving

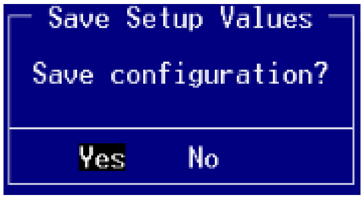
Reset without saving?

Save Options

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

Save Changes

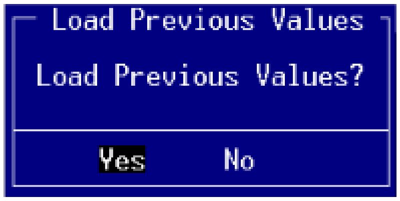
When you have completed the system configuration changes, select this option to save your system configuration and continue. For some of the options it required to reset the system to take effect. Select *YES* to Save Changes and continue.


Save Setup Values

Save configuration?

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

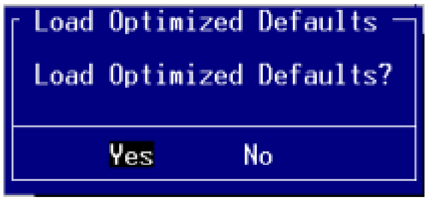


Load Previous Values

Load Previous Values?

Restore Defaults

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

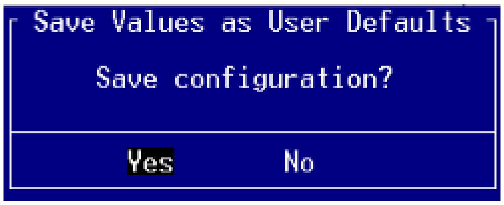


Load Optimized Defaults

Load Optimized Defaults?

Save as User Defaults

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

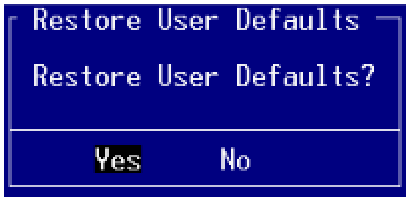


Save Values as User Defaults

Save configuration?

Restore User Defaults

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



Restore User Defaults

Restore User Defaults?

3.0 Revision History

The following table shows the revision history for this document:

Release Date	Version	EGR/DOC	Description of Revision
16 DEC 2013	A	BLD/TG	Preliminary release
18 DEC 2013	A1	BLD	Edits
08 JUL 2014	B	BLD	Add details for menu items that are referenced in the XCOM-6400 User’s Manual
21 DEC 2016	C	BLD/ARP	Change the Manual title to: “APTIO HASWELL CORE BIOS MANUAL For Acromag Products using the Haswell Processor”.
26 Nov 2018	D	JBO/RRP/ARP	Updated to include more BIOS menu items.