

# BIOS Reference Manual

DOC. REV. 14 MAR 2016

## Bengal (VL-EPMe-3o)

Intel® Atom™-based SBC with Dual Ethernet, Video, USB, SATA, Serial I/O, Digital I/O, Trusted Platform Module Security, Counter/Timers, Mini PCIe, mSATA, SPX, and PCIe/104 OneBank™ Interface





[WWW.VERSALOGIC.COM](http://WWW.VERSALOGIC.COM)

12100 SW Tualatin Road  
Tualatin, OR 97062-7341  
(503) 747-2261  
Fax (971) 224-4708

Copyright © 2016 VersaLogic Corp. All rights reserved.

**Notice:**

Although every effort has been made to ensure this document is error-free, VersaLogic makes no representations or warranties with respect to this product and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

VersaLogic reserves the right to revise this product and associated documentation at any time without obligation to notify anyone of such changes.

<sup>†</sup> Other names and brands may be claimed as the property of others.

## Product Release Notes

This document reflects the content of the BIOS Setup program for the EPMe-30 Bengal Board.

Board Revision	BIOS Version	BIOS ID String	Comments
Rev 2.00	1.01	Bengal_3.1.0.334.r1.101	First release of document
Rev 2.02A	1.02	Bengal_3.1.0.334.r1.102	Changed default setting of PCIe 1 speed from <u>Auto</u> to <u>Gen 1</u>
Rev 3.00	1.04	Bengal_3.1.0.547.r1.104	Refer to the table below

**Table 1: Changes from BIOS 334.r1.102 to BIOS 547.r1.104**

Screen/Menu	Change	Ref.
Main→ System Information	New BIOS ID string	Page 5
Boot Features →Console Redirection→ Terminal Type	Default changed from <u>ANSI</u> to <u>VT100+</u>	Page 15
Main→ Boot Features →Load OPROM	<u>Disabled</u> option replaced with <u>All</u>	Page 23
Advanced→ OS Selection	Default changed from <u>Windows</u> to <u>Linux</u>	Page 28
Advanced→ CPU Power Management→ Max C State	Option <u>C4</u> removed (default setting <u>C7</u> not changed)	Page 54
Advanced→ Graphics/Uncore Configuration	Added <u>Graphics/</u> to submenu title	Page 55
Advanced→ Graphics/Uncore Configuration→ DVMT Total Gfx Mem	New screen/option added to this BIOS	Page 64
Advanced→ Graphics/Uncore Configuration→ IGD Boot Type	Option <u>eDP</u> was removed	Page 68
Advanced→ Graphics/Uncore Configuration→ GMCH BLC Control	New screen/option added to this BIOS	Page 70
Advanced→ USB Configuration→ USB Port #3	New screen/option added to this BIOS	Page 86
Advanced→ Audio Configuration→ Audio Controller	Default setting changed to <u>Disable</u>	Page 87
Advanced→ LPSS & SCC Configuration→ MPI HSI Support	Removed from this BIOS	N/A
Advanced→ LPSS & SCC Configuration→ LPSS DMA #2 Support	Default changed to <u>Enable</u>	Page 94
Advanced→ LPSS & SCC Configuration→ LPSS I2C #1 Support	Default changed to <u>Enable</u>	Page 95
Advanced→ LPSS & SCC Configuration→ LPSS HSUART #1	Removed from this BIOS	N/A
Advanced→ LPSS & SCC Configuration→ LPSS HSUART #2	Removed from this BIOS	N/A

## Support Page

The [Bengal Support Page](#) contains additional information and resources for this product including:

- Operating system information and software drivers
- Data sheets and manufacturers' links for chips used in this product
- BIOS information and upgrades

## VersaTech KnowledgeBase

The [VersaTech KnowledgeBase](#) contains useful technical information about VersaLogic products, along with product advisories.

## Customer Support

If you are unable to solve a problem after reading this manual, visiting the product support page, or searching the KnowledgeBase, contact VersaLogic Technical Support at (503) 747-2261. VersaLogic support engineers are also available via e-mail at [Support@VersaLogic.com](mailto:Support@VersaLogic.com).

# Contents

---

<b>Overview .....</b>	<b>1</b>
<b>Main Menu.....</b>	<b>2</b>
Main → System Date.....	3
Main → System Time.....	4
Main → System Information .....	5
Main → Boot Features.....	6
Main → Boot Features → NumLock.....	7
Main → Boot Features → Timeout .....	8
Main → Boot Features → CSM Support .....	9
Main → Boot Features → Quick Boot .....	10
Main → Boot Features → Diagnostic Splash Screen.....	11
Main → Boot Features → Diagnostic Summary Screen.....	12
Main → Boot Features → BIOS Level USB.....	13
Main → Boot Features → Console Redirection.....	14
Main → Boot Features → Allow Hotkey in S4 Resume.....	19
Main → Boot Features → UEFI Boot .....	20
Main → Boot Features → Legacy Boot .....	21
Main → Boot Features → Boot In Legacy Video Mode.....	22
Main → Boot Features → Load OPPROM .....	23
Main → Error Manager .....	24
Main → Error Manager → View Error Manager Log.....	25
Main → Error Manager → Clear Error Manager Log.....	26
<b>Advanced Menu .....</b>	<b>27</b>
Advanced → OS Selection .....	28
Advanced → VersaLogic Features.....	29
Advanced → VersaLogic Features → Mini Card Mode .....	30
Advanced → VersaLogic Features → UART1 .....	31
Advanced → VersaLogic Features → UART2 .....	35
Advanced → CPU Configuration .....	39
Advanced → CPU Configuration → Execute Disable Bit .....	40
Advanced → CPU Configuration → AES-NI .....	41
Advanced → CPU Configuration → Limit CPUID Maximum.....	42
Advanced → CPU Configuration → Bi-directional PROCHOT# .....	43
Advanced → CPU Configuration → VTX-2.....	44
Advanced → CPU Configuration → TM1 .....	45
Advanced → CPU Configuration → DTS.....	46
Advanced → CPU Configuration → Intel Hyper-Threading Technology .....	47
Advanced → CPU Power Management .....	48
Advanced → CPU Power Management → Intel SpeedStep .....	49
Advanced → CPU Power Management → Intel Turbo Boost Technology .....	51
Advanced → CPU Power Management → C-States .....	52
Advanced → CPU Power Management → Max C State .....	54

Advanced → Graphics/Uncore Configuration .....	55
Advanced → Graphics/Uncore Configuration → GOP Driver .....	56
Advanced → Graphics/Uncore Configuration → Integrated Graphics Device ..	57
Advanced → Graphics/Uncore Configuration → Primary Display .....	58
Advanced → Graphics/Uncore Configuration → RC6 (Render Standby).....	59
Advanced → Graphics/Uncore Configuration → PAVC.....	60
Advanced → Graphics/Uncore Configuration → GTT Size.....	61
Advanced → Graphics/Uncore Configuration → Aperture Size .....	62
Advanced → Graphics/Uncore Configuration → DVMT Pre-Allocated .....	63
Advanced → Graphics/Uncore Configuration → DVMT Total Gfx Mem .....	64
Advanced → Graphics/Uncore Configuration → IGD Turbo.....	65
Advanced → Graphics/Uncore Configuration → BIA.....	66
Advanced → Graphics/Uncore Configuration → LCD Panel Type .....	67
Advanced → Graphics/Uncore Configuration → IGD Boot Type .....	68
Advanced → Graphics/Uncore Configuration → Panel Scaling.....	69
Advanced → Graphics/Uncore Configuration → GMCH BLC Control .....	70
Advanced → South Cluster Configuration.....	71
Advanced → PCI Express Configuration → PCIe 0 Speed .....	72
Advanced → PCI Express Configuration → PCIe 1 Speed .....	73
Advanced → PCI Express Configuration → PCIe 2 Speed .....	74
Advanced → PCI Express Configuration → PCIe 3 Speed .....	75
Advanced → PCI Express Configuration → PCI Express Root Port 1 .....	76
Advanced → PCI Express Configuration → PCI Express Root Port 2.....	77
Advanced → PCI Express Configuration → PCI Express Root Port 3.....	78
Advanced → PCI Express Configuration → PCI Express Root Port 4.....	79
Advanced → USB Configuration → XHCI Link Power Management.....	80
Advanced → USB Configuration → EHCI Controller .....	81
Advanced → USB Configuration → USB Per-Port Control.....	82
Advanced → USB Configuration → USB Port #0.....	83
Advanced → USB Configuration → USB Port #1.....	84
Advanced → USB Configuration → USB Port #2.....	85
Advanced → USB Configuration → USB Port #3.....	86
Advanced → Audio Configuration → Audio Controller .....	87
Advanced → Audio Configuration → Azalia VCi Enable.....	88
Advanced → Audio Configuration → Azalia HDMI CODEC .....	89
Advanced → SATA Drives → Chipset SATA.....	90
Advanced → SATA Drives → Chipset SATA Mode .....	91
Advanced → LPSS & SCC Configuration → LPSS Devices Mode .....	92
Advanced → LPSS & SCC Configuration → LPSS DMA #1 Support .....	93
Advanced → LPSS & SCC Configuration → LPSS DMA #2 Support .....	94
Advanced → LPSS & SCC Configuration → LPSS I2C #1 Support .....	95
Advanced → LPSS & SCC Configuration → LPSS PWM #1 Support .....	96
Advanced → LPSS & SCC Configuration → LPSS PWM #2 Support.....	97
Advanced → Miscellaneous Configuration → High Precision Timer .....	98
Advanced → Miscellaneous Configuration → Boot Time with HPET Timer ...	99
Advanced → Miscellaneous Configuration → State After G3 .....	100
Advanced → Miscellaneous Configuration → SoC Debug UART .....	101
Advanced → Miscellaneous Configuration → SMM Lock .....	102

Advanced → Miscellaneous Configuration → PCI MMIO Size .....	103
Advanced → Security .....	104
Advanced → Security Configuration → TXE.....	105
Advanced → Security Configuration → TXE HMRFPO .....	106
Advanced → Security Configuration → TXE Firmware Update.....	107
Advanced → Security Configuration → TXE EOP Message .....	108
Advanced → Security Configuration → TXE Unconfiguration Perform .....	109
Advanced → Thermal.....	110
Advanced → Thermal → Critical Trip Point .....	111
Advanced → Thermal → Passive Trip Point .....	112
Advanced → Thermal → Active Trip Point.....	113
Advanced → Thermal → Start Fan With Cold CPU.....	114
Advanced → SMBIOS Event Log.....	115
Advanced → SMBIOS Event Log → Event Log .....	116
Advanced → SMBIOS Event Log → Mark SMBIOS Events As Read.....	117
Advanced → SMBIOS Event Log → Clear SMBIOS Events .....	118
<b>Security Menu.....</b>	<b>119</b>
Security → Set Supervisor Password .....	120
Security → Supervisor Hint String.....	121
Security → Set User Password .....	122
Security → User Hint String.....	123
Security → Min. Password Length.....	124
Security → TPM Support .....	125
Security → TPM Configuration .....	126
Security → TPM Configuration → Current TPM State.....	127
Security → TPM Configuration → TPM Action .....	128
Security → TPM Configuration → Omit Boot Measurements .....	129
<b>Boot Menu.....</b>	<b>130</b>
<b>Exit Menu .....</b>	<b>132</b>

## Overview

The BIOS Setup utility is stored in the Serial Peripheral Interface (SPI) Flash device. The initial production BIOS ID string is Bengal\_3.1.0.547.r1.104.

The BIOS Setup utility can be used to view and change the BIOS settings for the Bengal board.

To access the BIOS Setup utility, press **F2** during the early boot cycle.

The top-level menu bar is shown below.

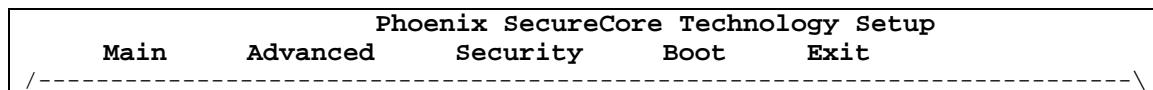


Table 2 lists the BIOS Setup utility top-level menu bar features.

**Table 2: Top-level Menu Bar Features**

Menu	Function
Main	Displays processor and memory configuration
Advanced	Configures advanced features available through the chipset
Security	Sets passwords and security features
Boot	Selects boot device options
Exit	Saves or discards changes to Setup utility options

Table 3 lists the function keys available for menu screens.

**Table 3. BIOS Setup Utility Function Keys**

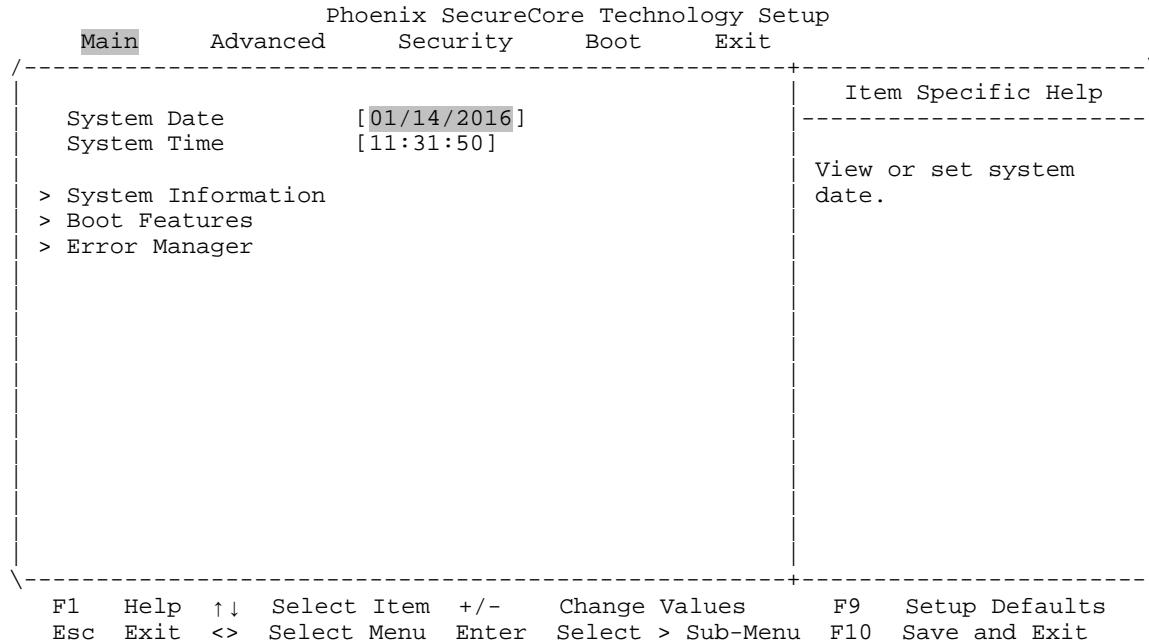
Menu	Function
<b>F1</b>	Help
<b>↑</b> or <b>↓</b>	Selects an item (Moves the cursor up or down)
<b>+</b> or <b>-</b>	Changes values
<b>F9</b>	Loads setup default values
<b>Esc</b>	Exits the menu
<b>←</b> or <b>→</b>	Selects a different menu screen (Moves the cursor left or right)
<b>Enter</b>	Executes a command or selects a sub-menu
<b>F10</b>	Saves the current values and exits the BIOS Setup utility

## Main Menu

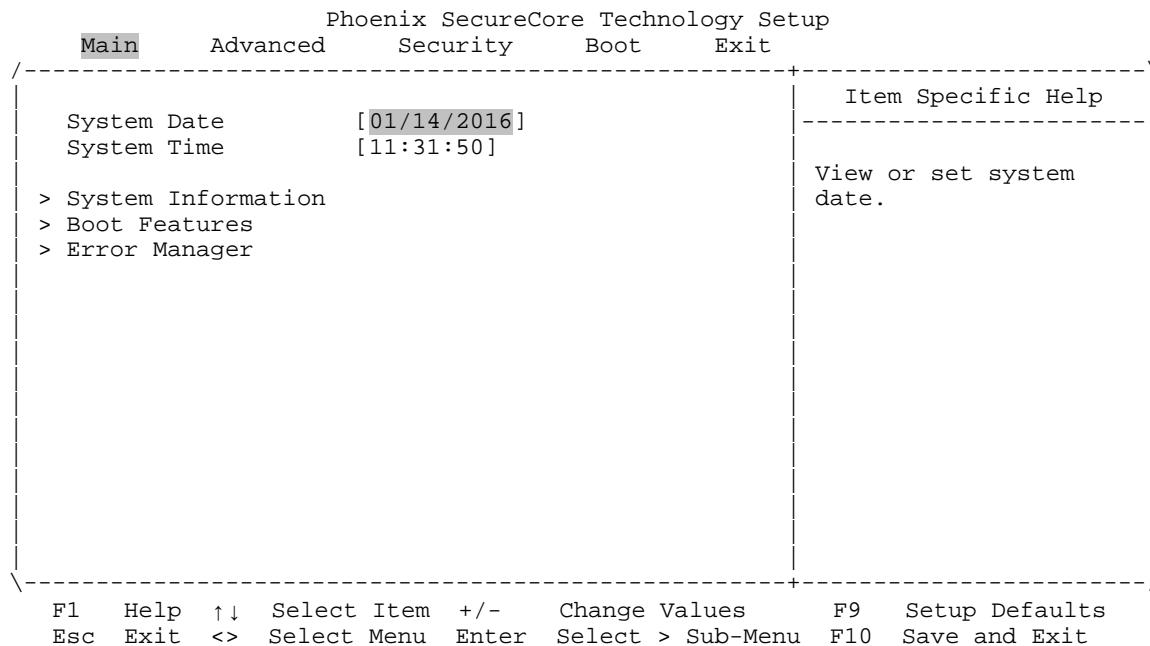
The Main menu enables you to:

- Set system date and time
- Set boot features
- View and clear the error log

Top level view of Main menu screen.



## Main → System Date

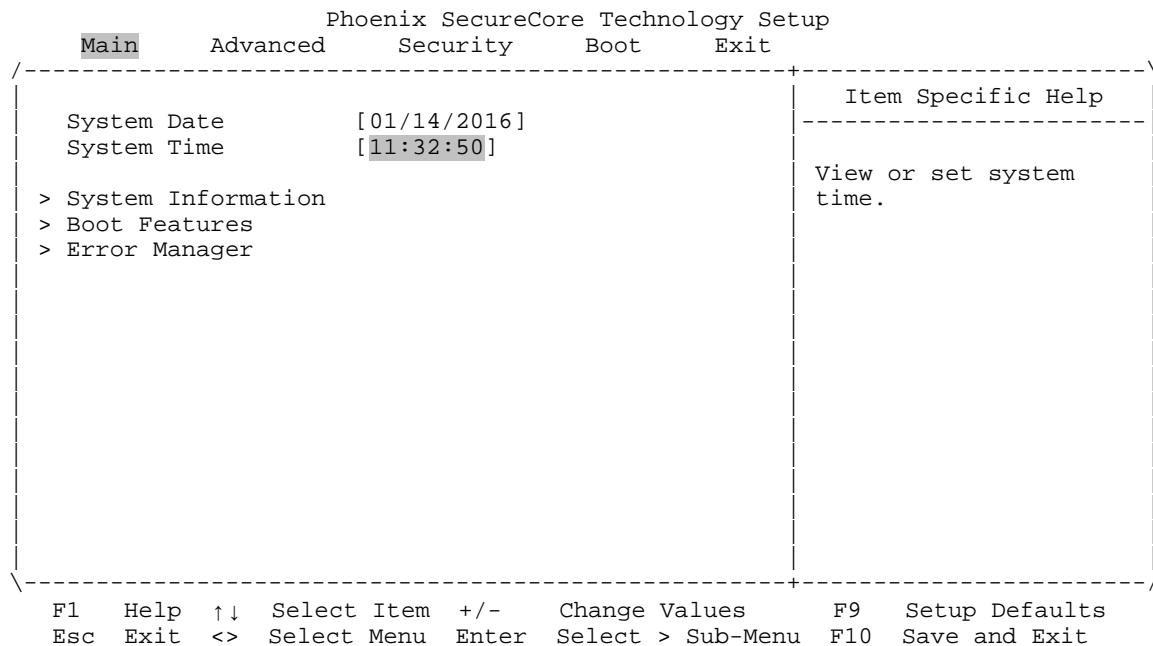


Use the and keys to switch between the System Date and System Time fields.

Use the and keys to set the month, day, and year.

Use the or key to move from month → day → year.

## Main → System Time

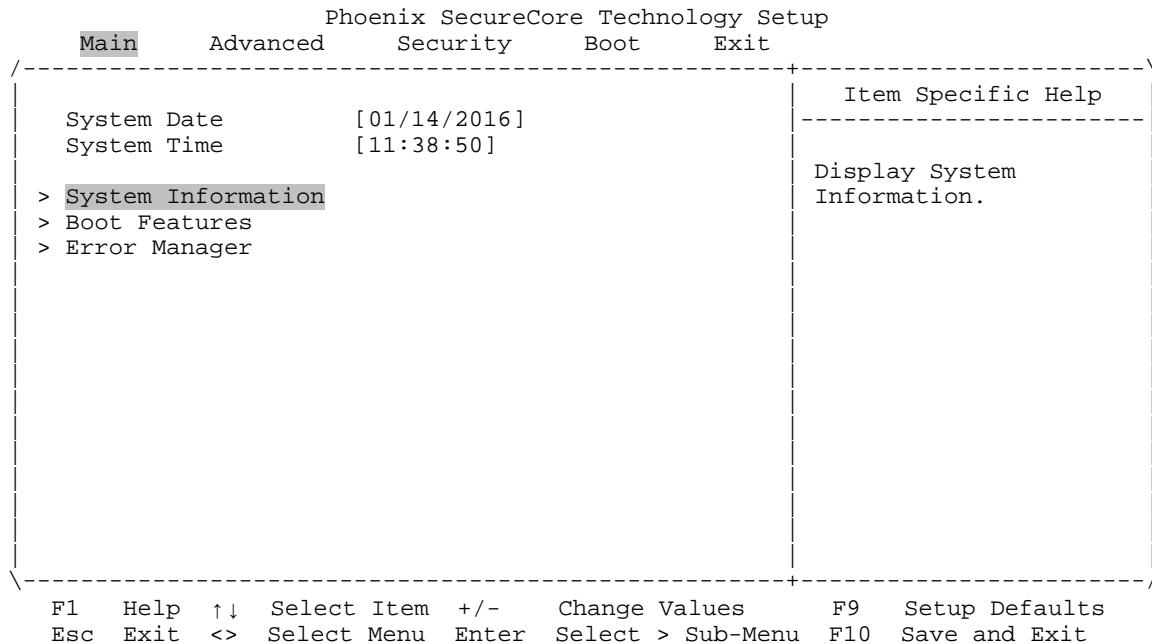


Use the and keys to switch between the System Date and System Time fields.

Use the and keys to set the hours, minutes, and seconds.

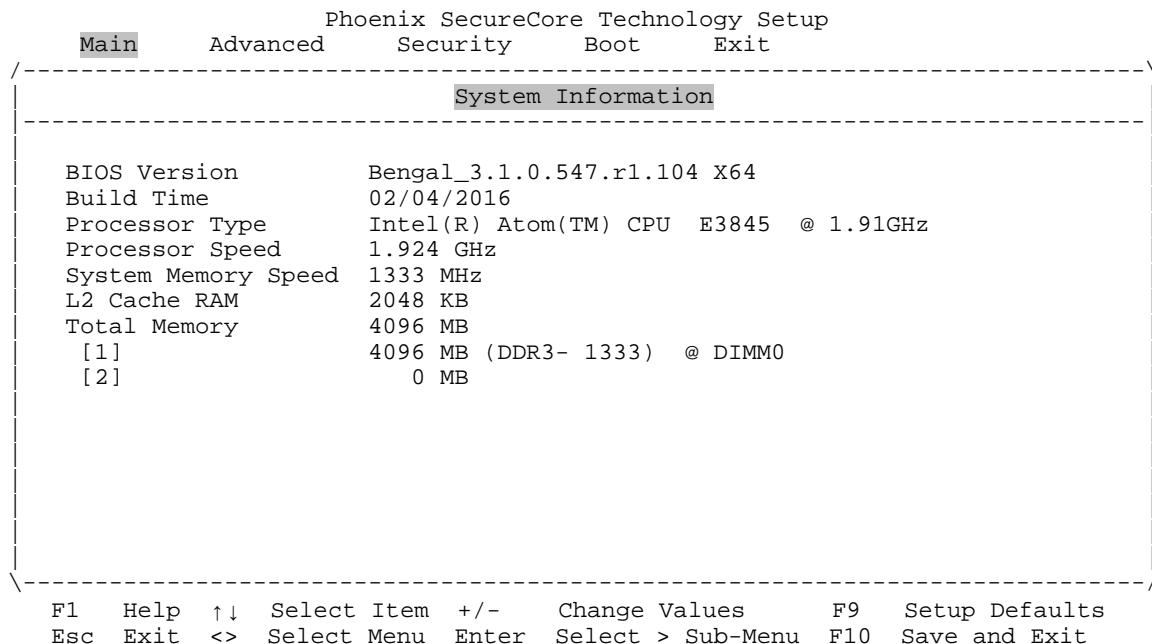
Use the or key to move from hours → minutes → seconds.

## Main → System Information



This screen is read-only; there are no user-configurable options.

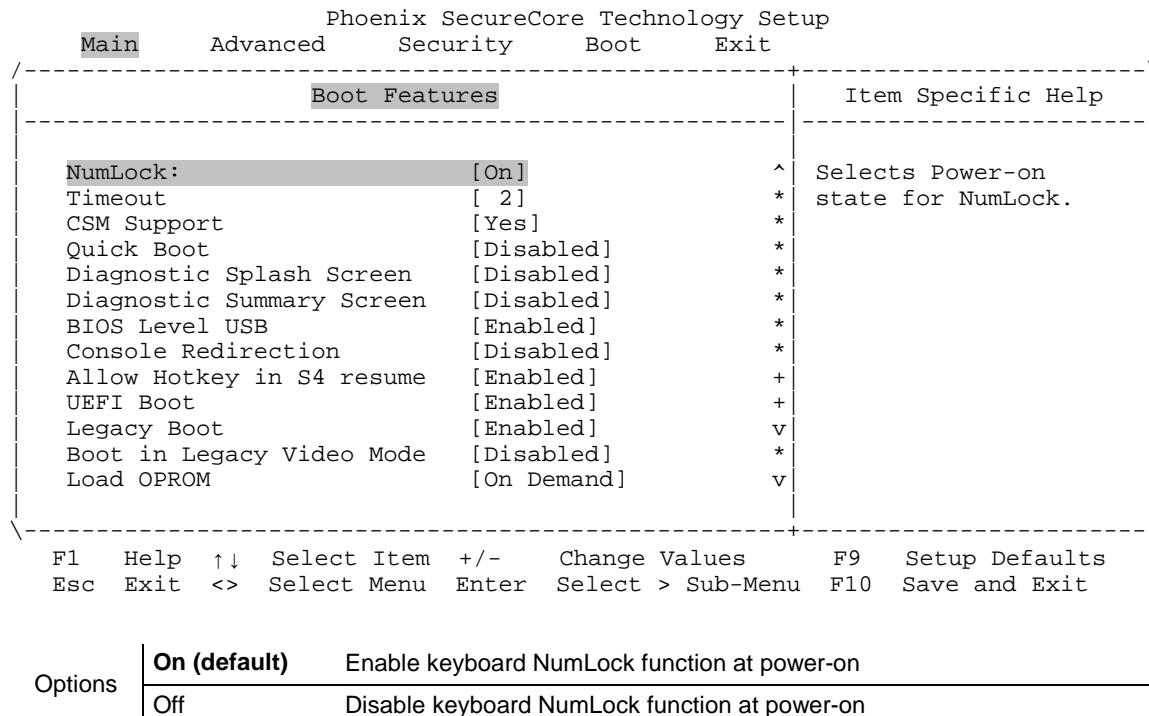
Example view of System Information screen:



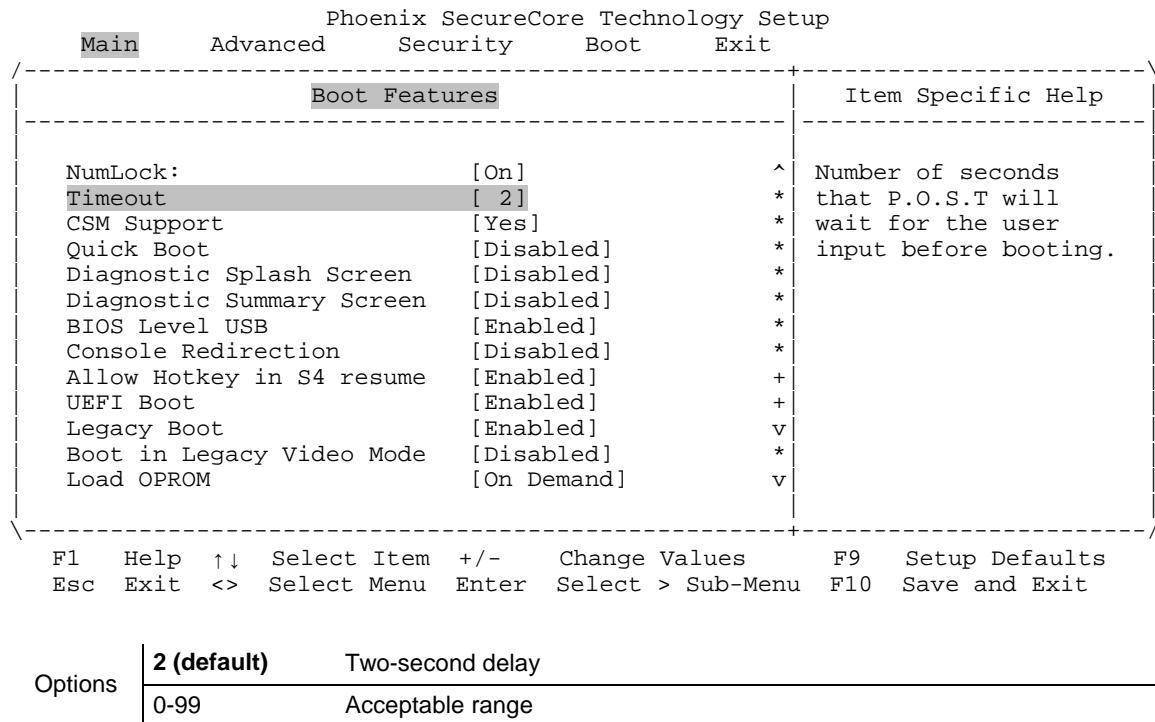
## Main → Boot Features

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
/-----\			
<b>Boot Features</b>			Item Specific Help
/-----\			
NumLock:	[On]		^ Selects Power-on state for NumLock.
Timeout	[2]	*	
CSM Support	[Yes]	*	
Quick Boot	[Disabled]	*	
Diagnostic Splash Screen	[Disabled]	*	
Diagnostic Summary Screen	[Disabled]	*	
BIOS Level USB	[Enabled]	*	
Console Redirection	[Disabled]	*	
Allow Hotkey in S4 resume	[Enabled]	+	
UEFI Boot	[Enabled]	+	
Legacy Boot	[Enabled]	v	
Boot in Legacy Video Mode	[Disabled]	*	
Load OPROM	[On Demand]	v	
\-----/			
F1	Help	↑↓	Select Item
Esc	Exit	<>	Select Menu
		Enter	Change Values
			Select > Sub-Menu
F9	Setup Defaults		
F10	Save and Exit		

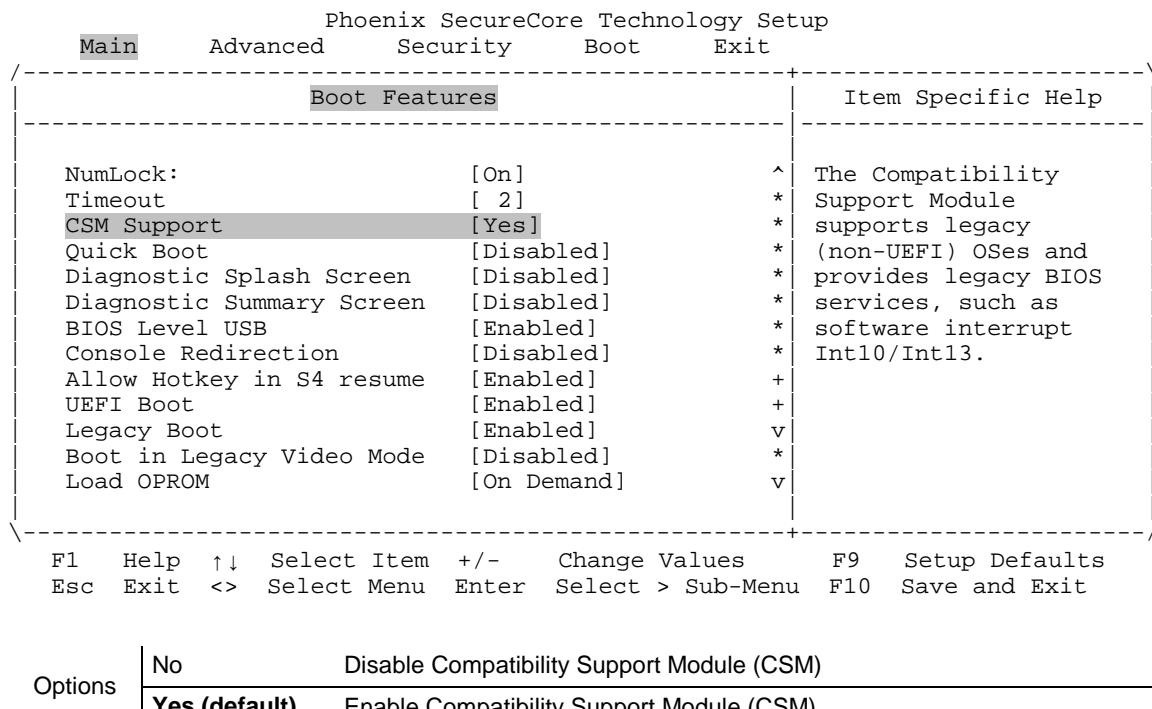
## Main → Boot Features → NumLock



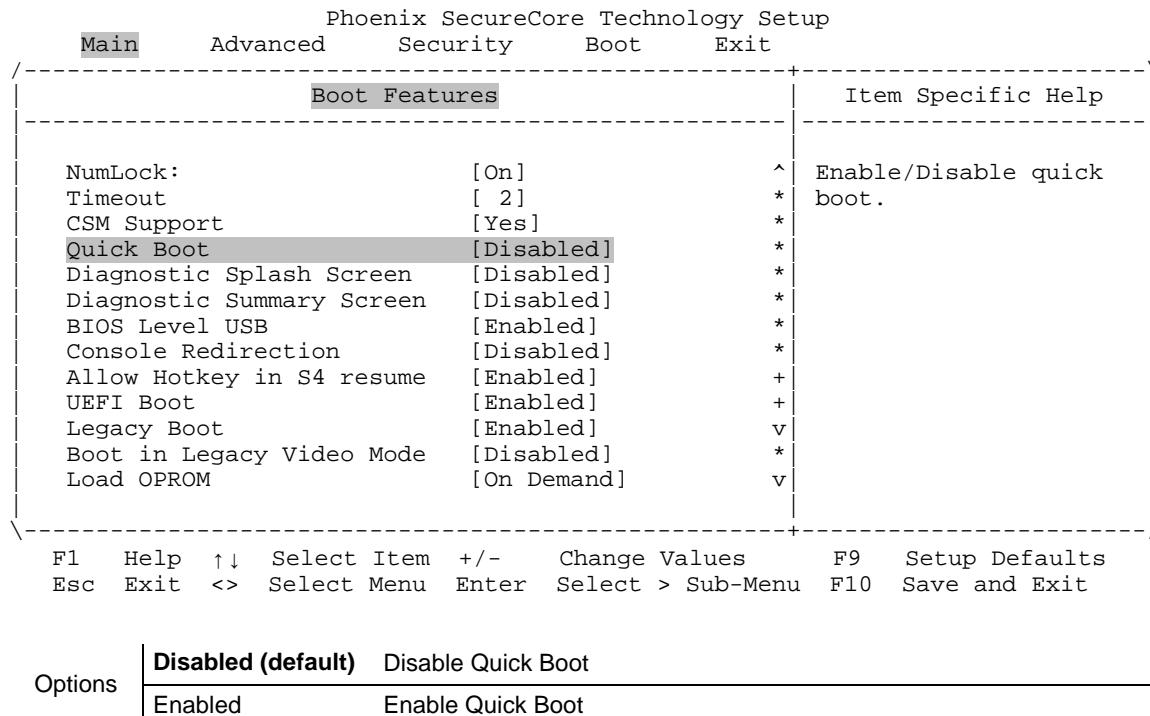
## Main → Boot Features → Timeout



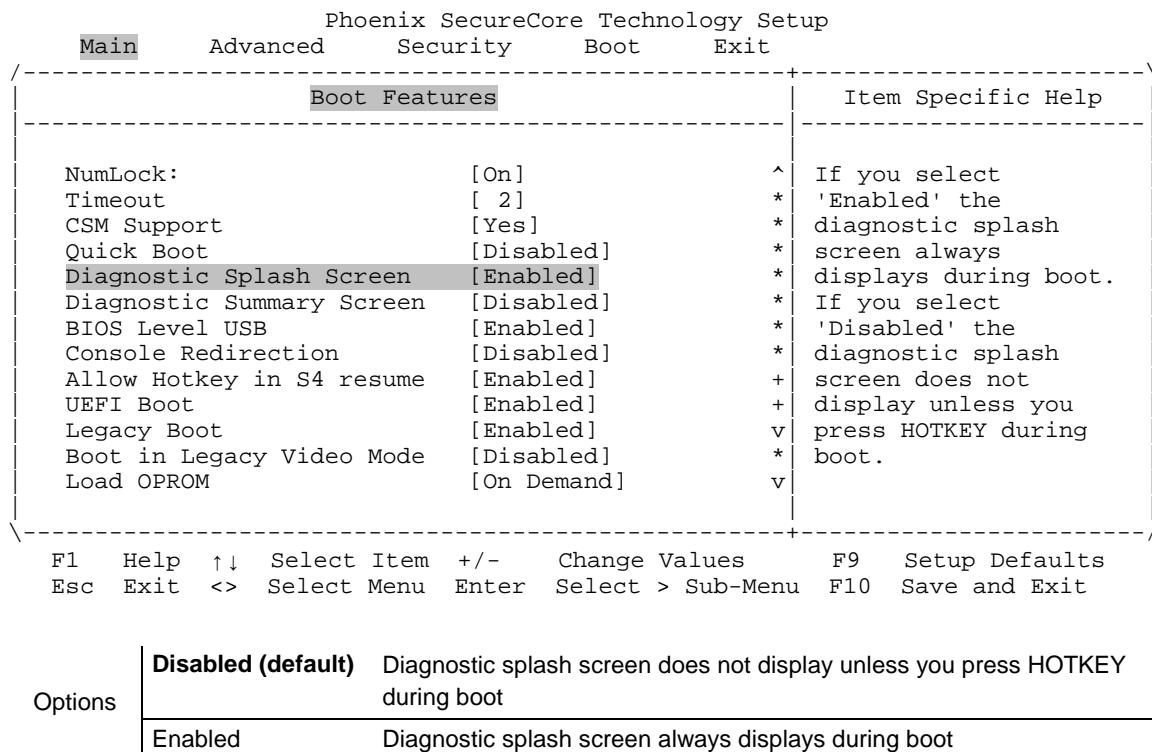
## Main → Boot Features → CSM Support



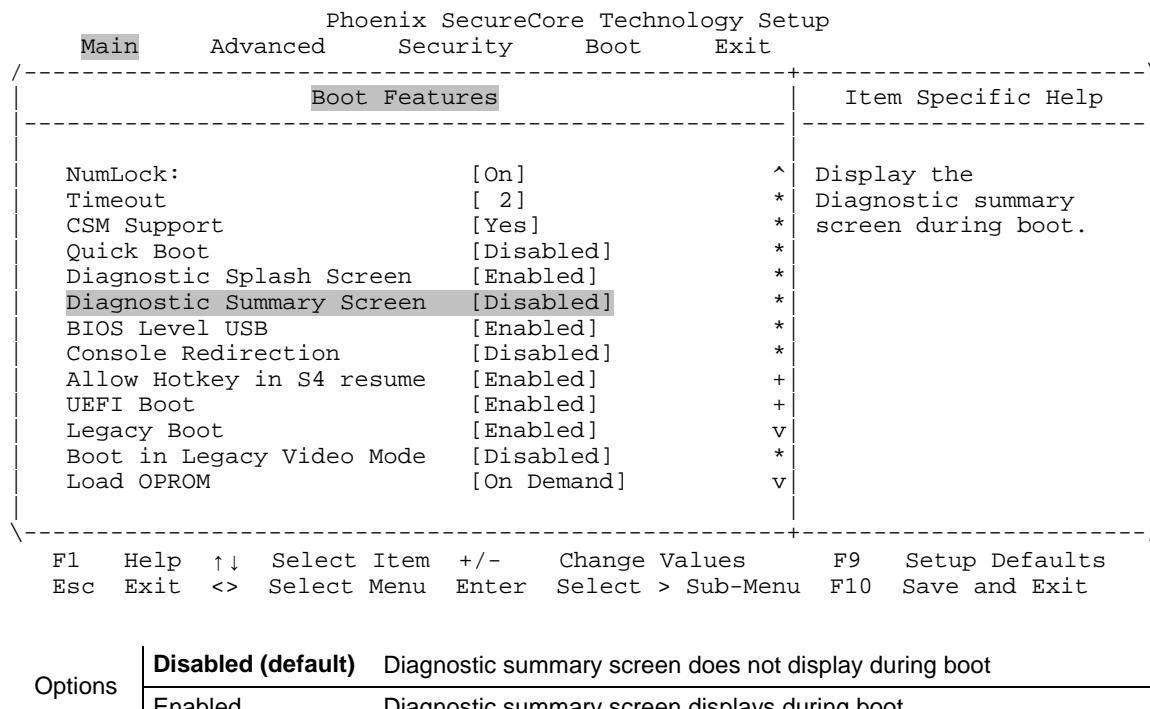
## Main → Boot Features → Quick Boot



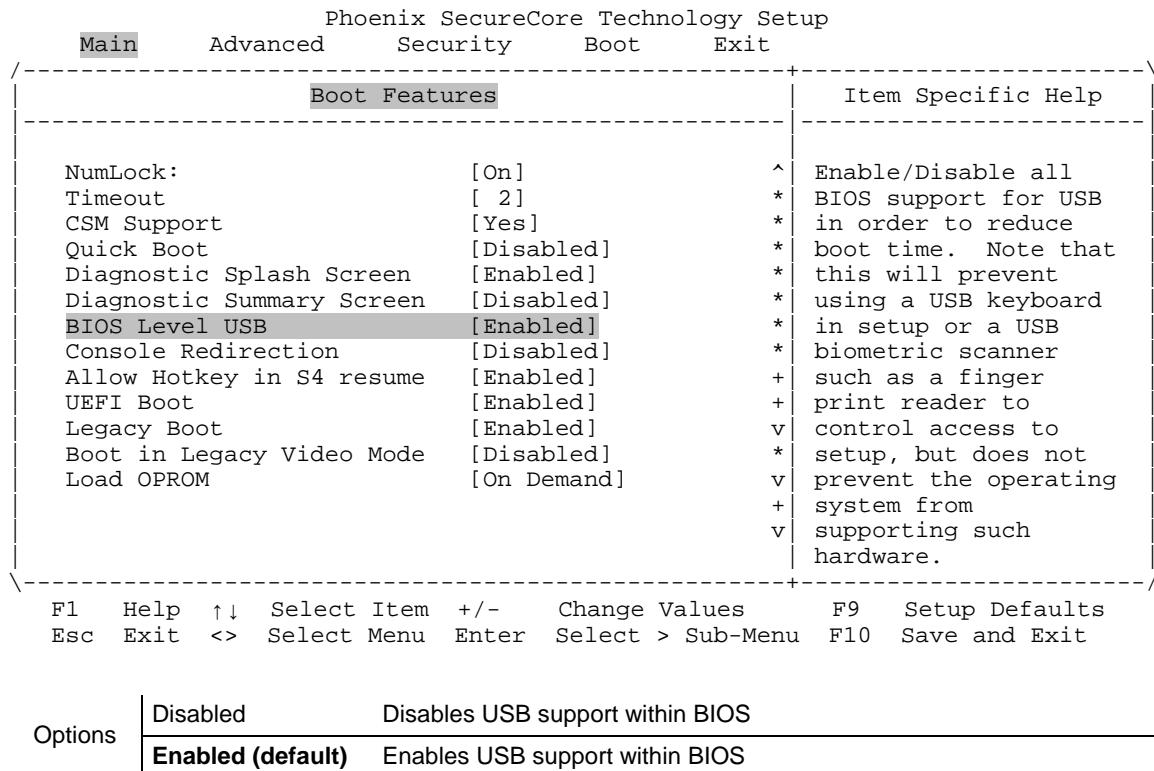
## Main → Boot Features → Diagnostic Splash Screen



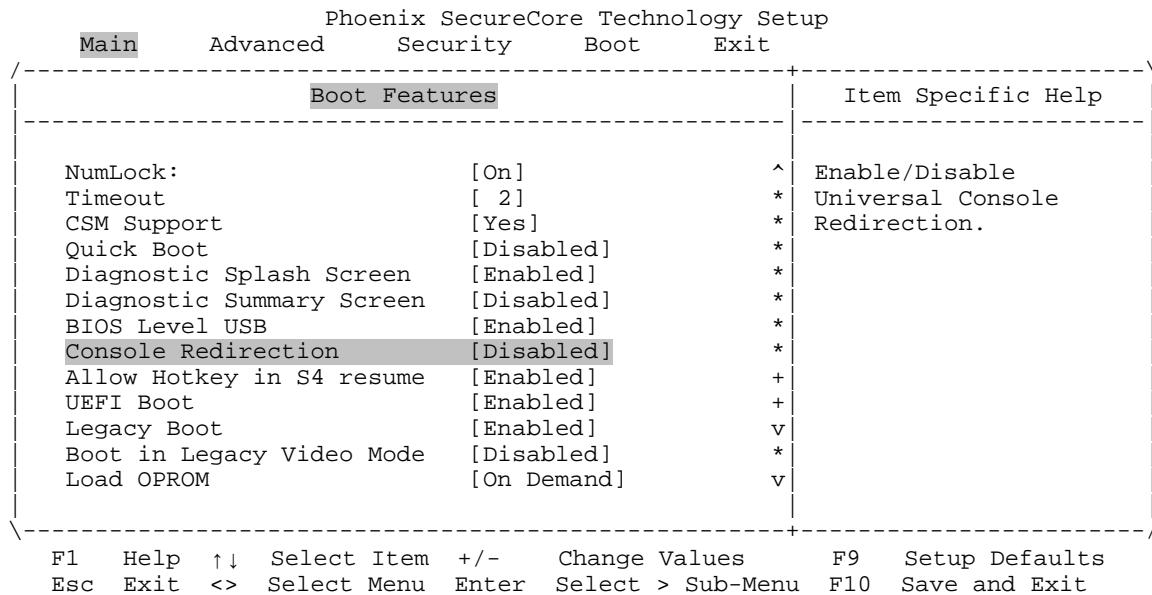
## Main → Boot Features → Diagnostic Summary Screen



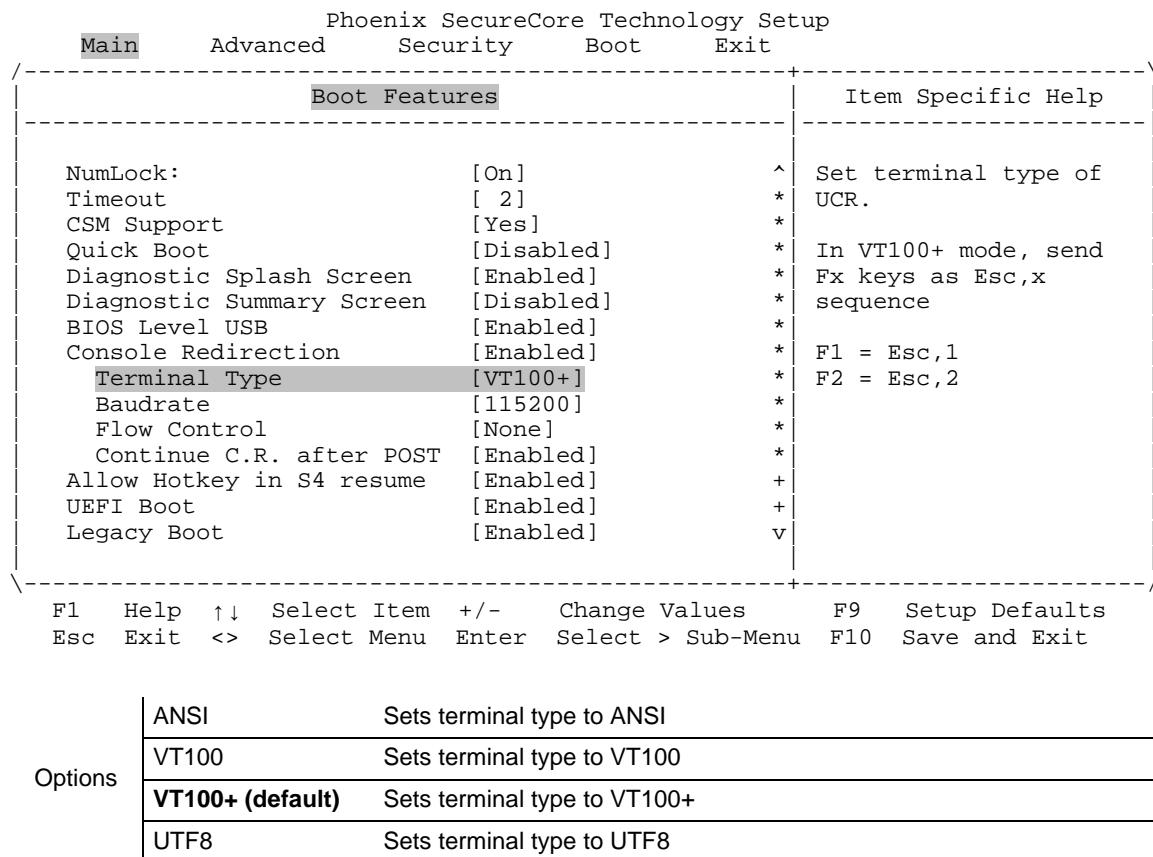
## Main → Boot Features → BIOS Level USB



## Main → Boot Features → Console Redirection



Options	<b>Disabled (default)</b> Disables Universal Console Redirection (UCR)
	Enabled      Enables Universal Console Redirection (UCR). When enabled, four sub-menus appear for setting console redirection parameters.

**Main → Boot Features → Console Redirection → Terminal Type**

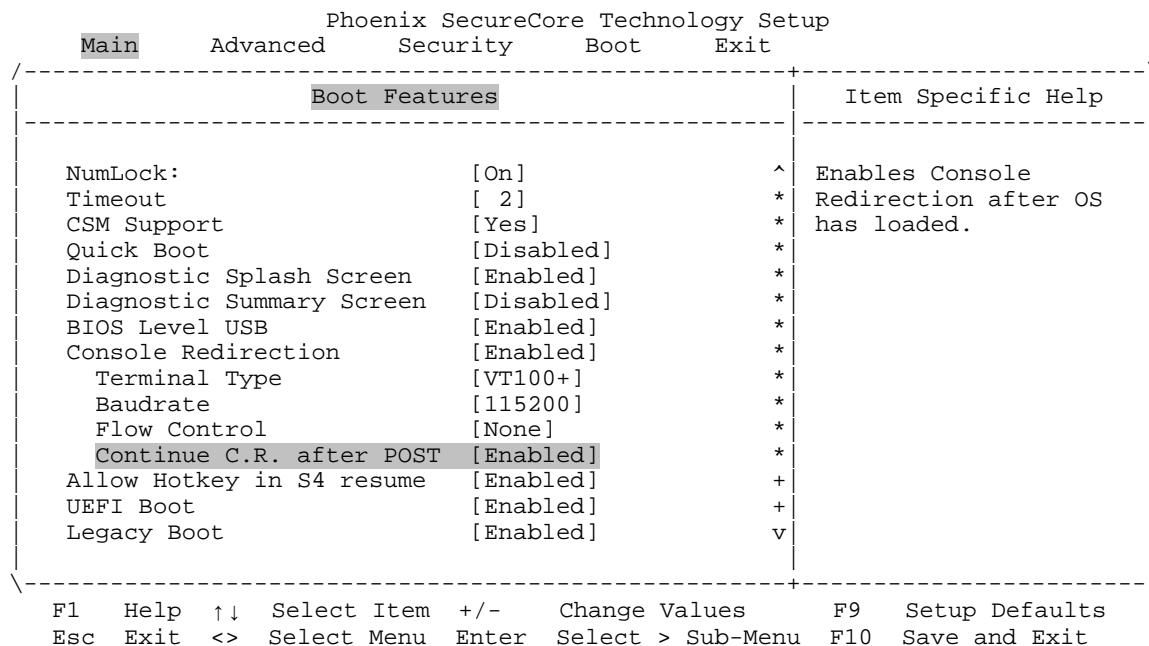
## Main → Boot Features → Console Redirection → Baudrate

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
			Boot Features
			Item Specific Help
CSM Support	[Yes]		^ Set baudrate of UCR.
Quick Boot	[Disabled]	+	
Diagnostic Splash Screen	[Enabled]	+	
Diagnostic Summary Screen	[Disabled]	*	
BIOS Level USB	[Enabled]	*	
Console Redirection	[Enabled]	*	
Terminal Type	[VT100+]	*	
Baudrate	[115200]	*	
Flow Control	[None]	*	
Continue C.R. after POST	[Enabled]	*	
Allow Hotkey in S4 resume	[Enabled]	*	
UEFI Boot	[Enabled]	*	
Legacy Boot	[Enabled]	*	
Boot in Legacy Video Mode	[Disabled]	*	
Load OPROM	[On Demand]	v	

Options	9600	Sets baudrate to 9600
	19200	Sets baudrate to 19200
	38400	Sets baudrate to 38400
	57600	Sets baudrate to 57600
	<b>115200 (default)</b>	Sets baudrate to 115200

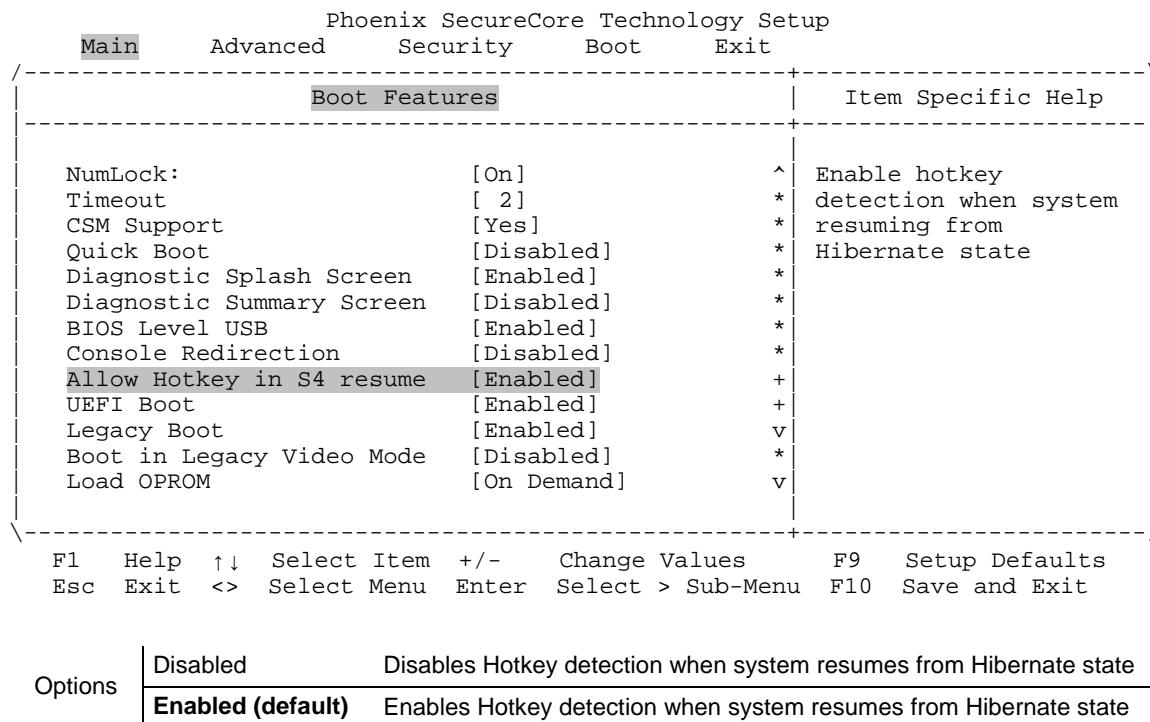
**Main → Boot Features → Console Redirection → Flow Control**

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
<b>Boot Features</b>				Item Specific Help
NumLock:	[On]			^ Set flow control
Timeout	[ 2 ]			* method for UCR.
CSM Support	[Yes]			*
Quick Boot	[Disabled]			* [None] - No flow
Diagnostic Splash Screen	[Enabled]			* control.
Diagnostic Summary Screen	[Disabled]			*
BIOS Level USB	[Enabled]			* [XON/XOFF] -
Console Redirection	[Enabled]			* Software flow control.
Terminal Type	[VT100+]			*
Baudrate	[115200]			*
<b>Flow Control</b>	<b>[None]</b>			*
Continue C.R. after POST	[Enabled]			*
Allow Hotkey in S4 resume	[Enabled]			+
UEFI Boot	[Enabled]			+
Legacy Boot	[Enabled]			v
F1 Help ↑↓ Select Item +/− Change Values F9 Setup Defaults				
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				
Options	None (default)      No flow control			
	[XON/XOFF]      Software flow control			

**Main → Boot Features → Console Redirection →Continue C.R. after POST**

Options	<b>Disabled</b> Disables console redirection after the operating system has loaded
	<b>Enabled (default)</b> Enables console redirection after the operating system has loaded

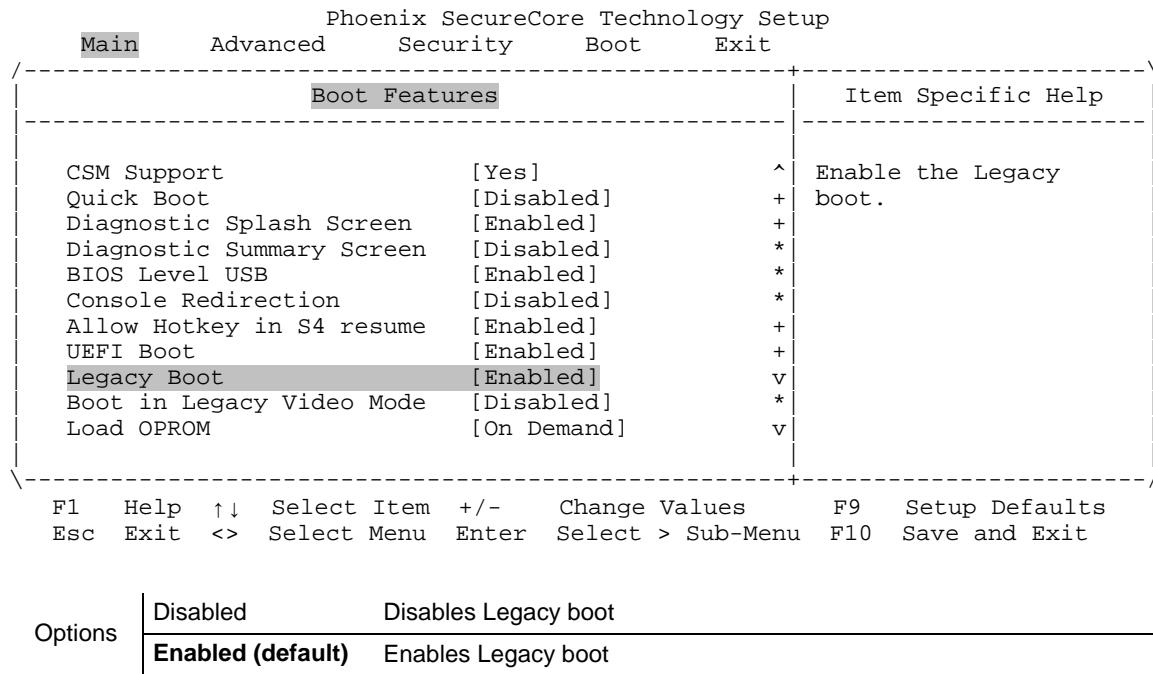
## Main → Boot Features → Allow Hotkey in S4 Resume



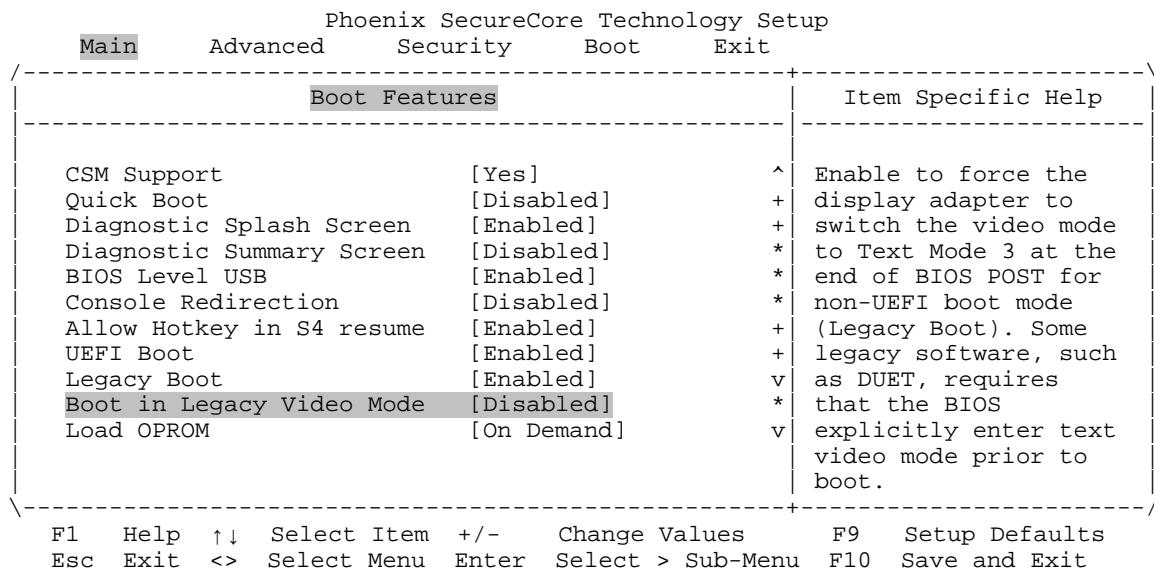
## Main → Boot Features → UEFI Boot

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
Boot Features			Item Specific Help
			^ Enable the UEFI boot.
NumLock:	[On]	*	
Timeout	[ 2 ]	*	
CSM Support	[Yes]	*	
Quick Boot	[Disabled]	*	
Diagnostic Splash Screen	[Enabled]	*	
Diagnostic Summary Screen	[Disabled]	*	
BIOS Level USB	[Enabled]	*	
Console Redirection	[Disabled]	*	
Allow Hotkey in S4 resume	[Enabled]	+	
<b>UEFI Boot</b>	<b>[Enabled]</b>	<b>+</b>	
Legacy Boot	[Enabled]	v	
Boot in Legacy Video Mode	[Disabled]	*	
Load OPROM	[On Demand]	v	
F1 Help $\uparrow\downarrow$ Select Item    +/ - Change Values    F9 Setup Defaults Esc Exit    <> Select Menu    Enter Select > Sub-Menu    F10 Save and Exit			
Options	Disabled	Disables Unified Extensible Firmware Interface (UEFI) boot	
	<b>Enabled (default)</b>	Enables Unified Extensible Firmware Interface (UEFI) boot	

## Main → Boot Features → Legacy Boot



## Main → Boot Features → Boot In Legacy Video Mode



Options	<b>Disabled (default)</b> Does not force a video mode switch to Text Mode 3.
	<b>Enabled</b> Forces the display adapter to switch to Text Mode 3 at the end of BIOS POST for non-UEFI boot mode (that is, Legacy Boot).

## Main → Boot Features → Load OPROM

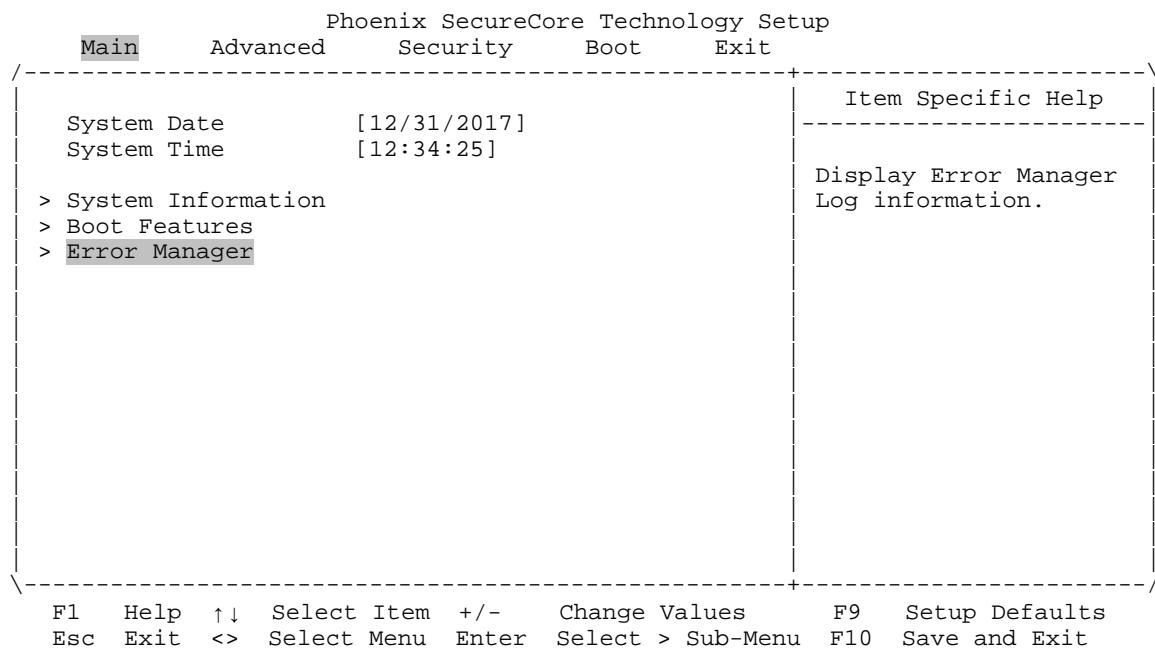
Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
Boot Features			Item Specific Help
			^ Load all OPROMs or on demand according to the boot device.
CSM Support	[Yes]		+
Quick Boot	[Disabled]		+
Diagnostic Splash Screen	[Enabled]		+
Diagnostic Summary Screen	[Disabled]		*
BIOS Level USB	[Enabled]		*
Console Redirection	[Disabled]		*
Allow Hotkey in S4 resume	[Enabled]		+
UEFI Boot	[Enabled]		+
Legacy Boot	[Enabled]		v
Boot in Legacy Video Mode	[Disabled]		*
<b>Load OPROM</b>	<b>[On Demand]</b>		<b>v</b>

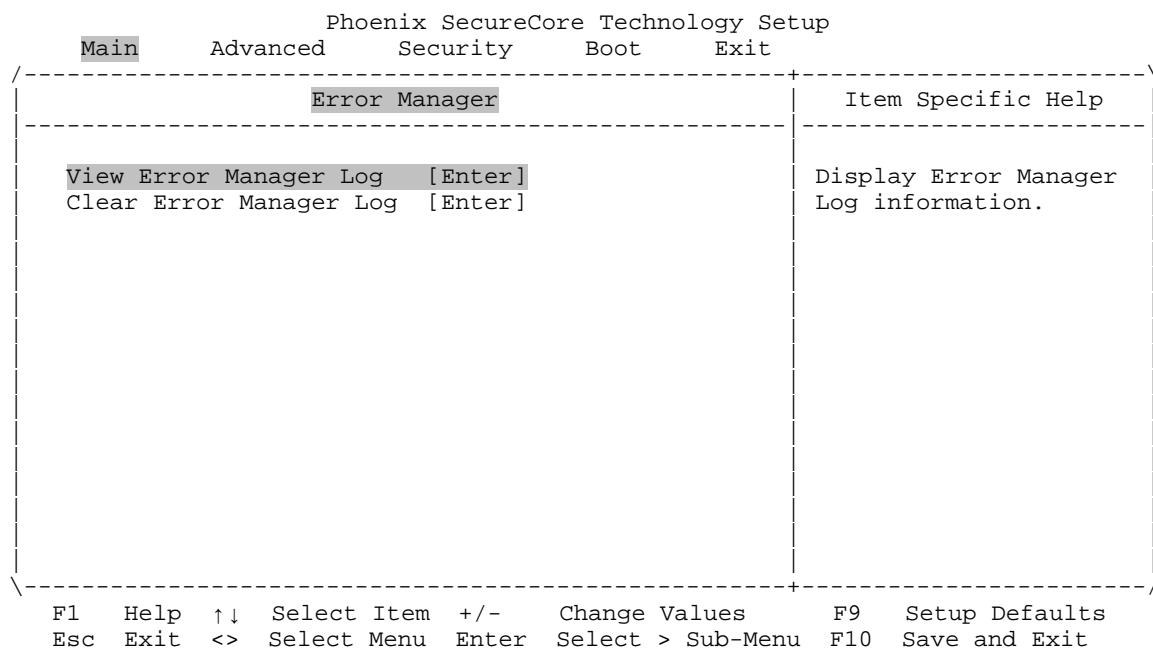
F1 Help    F9 Setup Defaults  
 Esc Exit    F10 Save and Exit

---

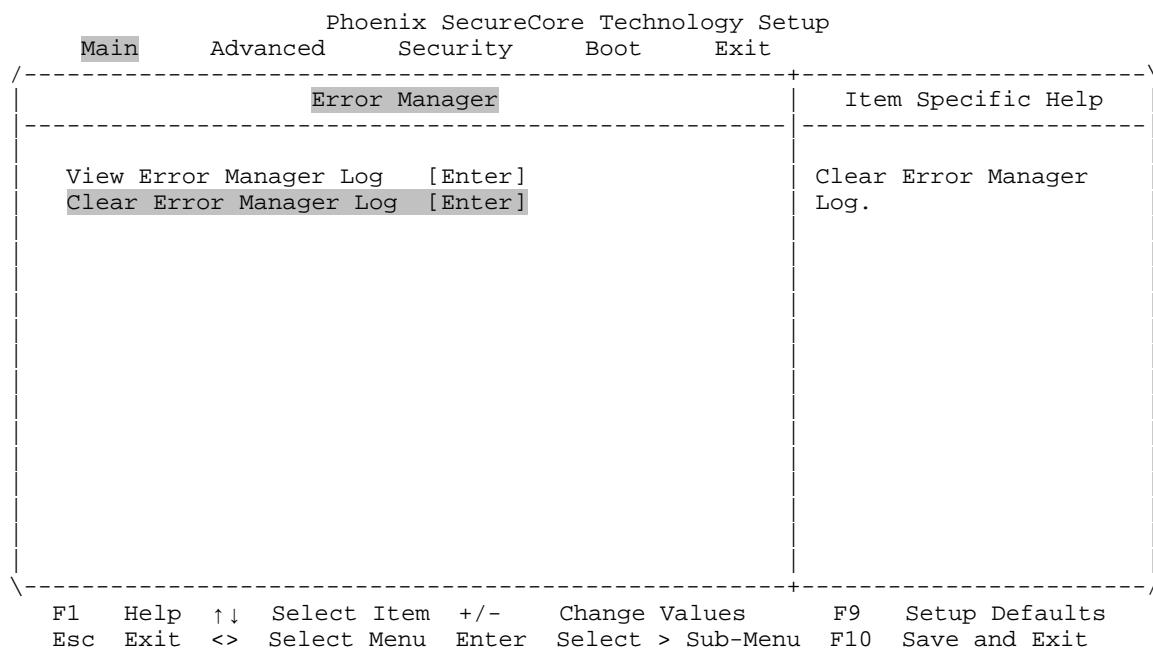
Options	All	Load all option ROMs.
	<b>On Demand (default)</b>	Load option ROMs (OPROMs) on demand according to the requirements of the boot device.

## Main → Error Manager



**Main → Error Manager → View Error Manager Log**

Press to view the Error Manager Log information.

**Main → Error Manager → Clear Error Manager Log**

Press  to clear the Error Manager Log information.

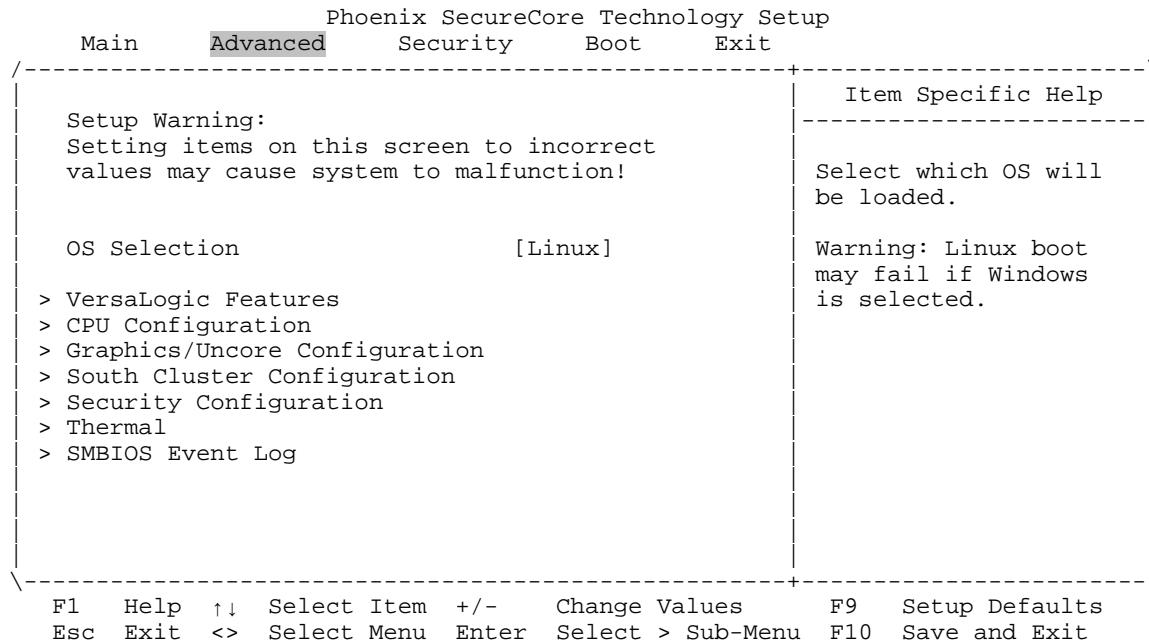
## Advanced Menu

3

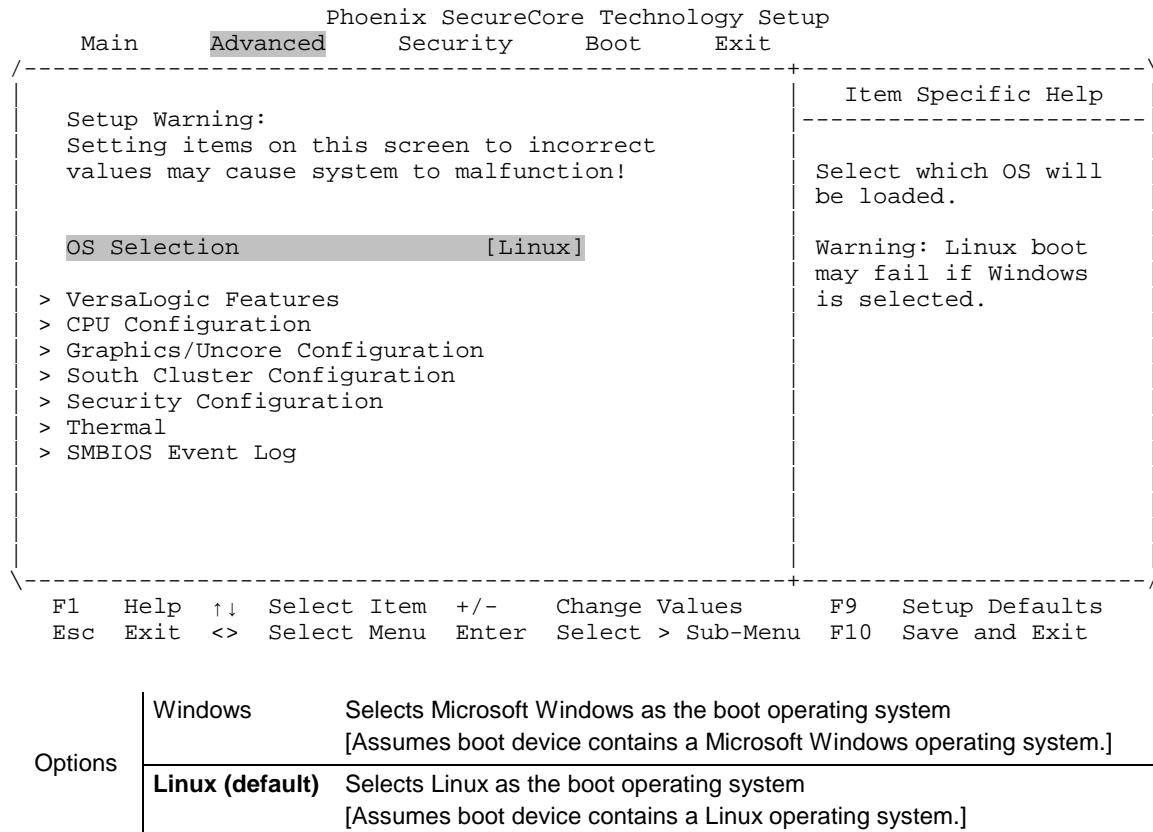
The Advanced menu enables you to:

- Select the operating system
- Configure VersaLogic product-specific features
- Configure CPU parameters
- Configure graphics and non-core related parameters
- Configure chipset parameters
- Configure certain security/TXE (Trusted Execution Environment) parameters
- Configure thermal monitor parameters
- Examine SMBIOS event log items

Top-level view of Advanced menu screen:



## Advanced → OS Selection

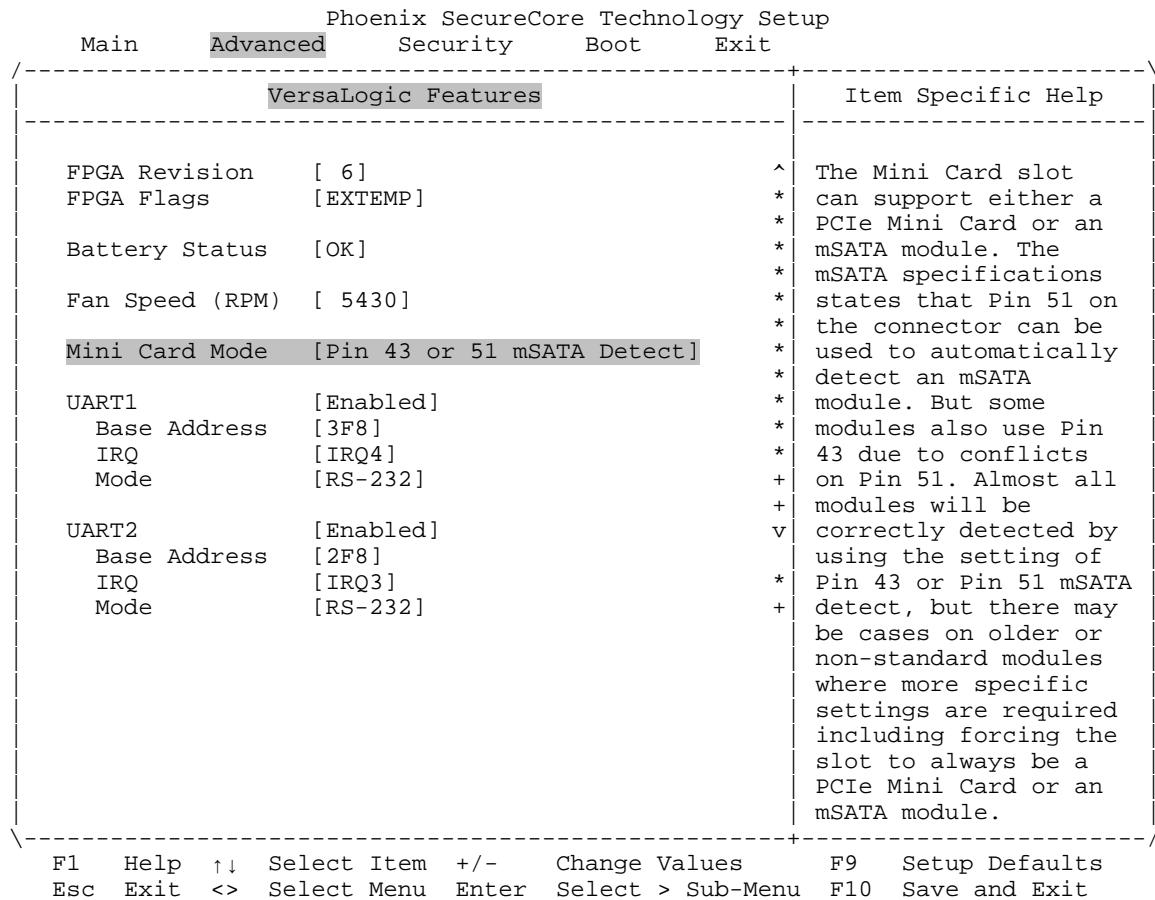


## Advanced → VersaLogic Features

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
<b>VersaLogic Features</b>			
FPGA Revision [ 6 ]			^ The Mini Card slot
FPGA Flags [ EXTEMP ]			* can support either a
Battery Status [ OK ]			* PCIe Mini Card or an
Fan Speed (RPM) [ 5430 ]			* mSATA module. The
Mini Card Mode [Pin 43 or 51 mSATA Detect]			* mSATA specifications
UART1 [Enabled]			* states that Pin 51 on
Base Address [3F8]			* the connector can be
IRQ [IRQ4]			* used to automatically
Mode [RS-232]			* detect an mSATA
UART2 [Enabled]			* module. But some
Base Address [2F8]			* modules also use Pin
IRQ [IRQ3]			* 43 due to conflicts
Mode [RS-232]			+ on Pin 51. Almost all
			+ modules will be
			v correctly detected by
			* using the setting of
			* Pin 43 or Pin 51 mSATA
			+ detect, but there may
			+ be cases on older or
			non-standard modules
			where more specific
			settings are required
			including forcing the
			slot to always be a
			PCIe Mini Card or an
			mSATA module.
F1 Help ↑↓ Select Item +/− Change Values F9 Setup Defaults	Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit		

This screen provides information on the FPGA, battery status, and fan speed.

## Advanced → VersaLogic Features → Mini Card Mode

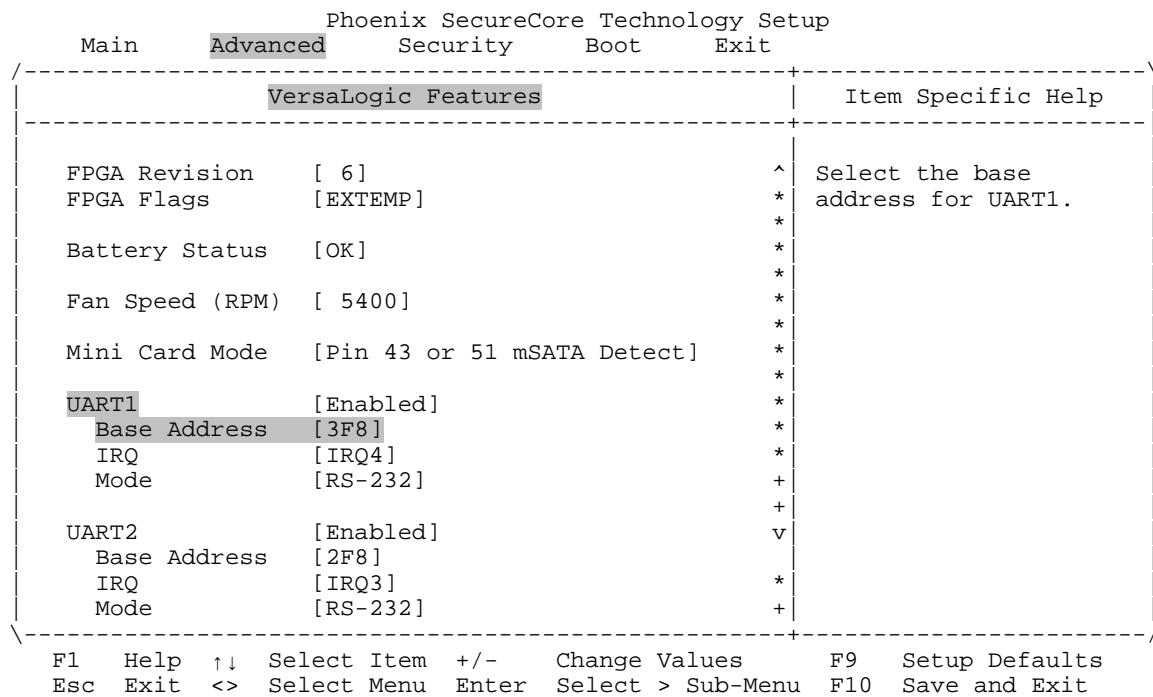


Options

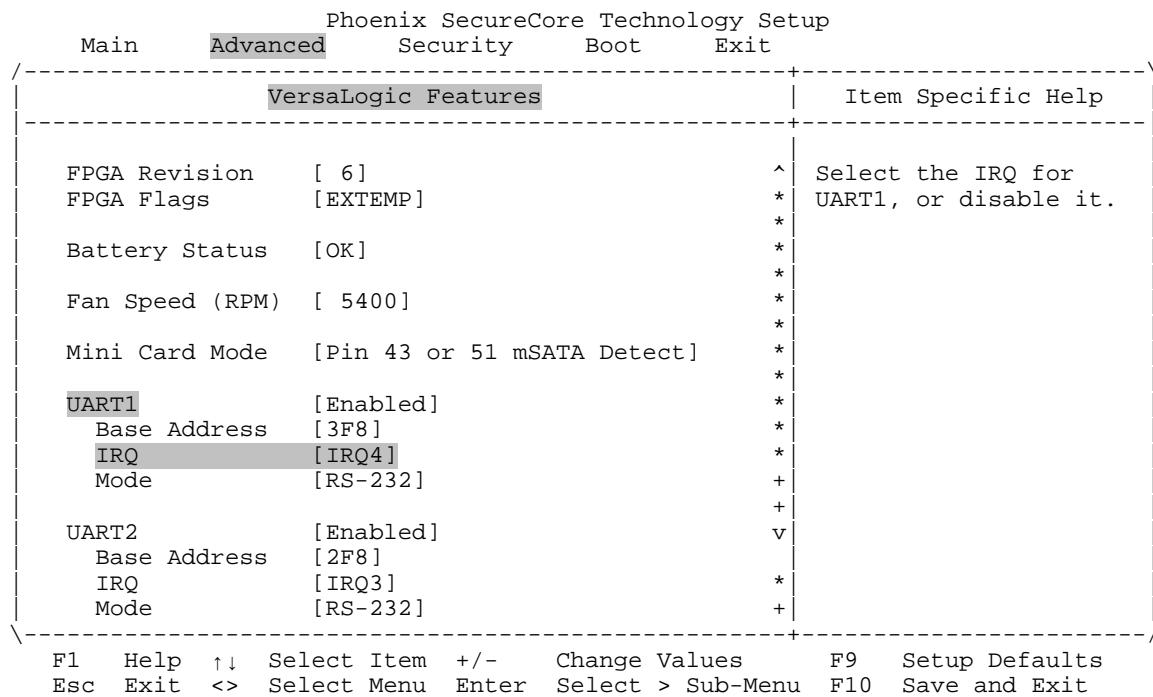
## Advanced → VersaLogic Features → UART1

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot
<b>VersaLogic Features</b>			Item Specific Help
FPGA Revision	[ 6 ]		^ Enable or disable
FPGA Flags	[ EXTEMP ]	*	UART1.
Battery Status	[OK]	*	
Fan Speed (RPM)	[ 5400 ]	*	
Mini Card Mode	[Pin 43 or 51 mSATA Detect]	*	
<b>UART1</b>	[Enabled]	*	
Base Address	[3F8]	*	
IRQ	[IRQ4]	*	
Mode	[RS-232]	+	
<b>UART2</b>	[Enabled]	v	
Base Address	[2F8]	*	
IRQ	[IRQ3]	+	
Mode	[RS-232]	+	
F1 Help	Select Item	+/-	Change Values
Esc Exit	<> Select Menu	Enter	Select > Sub-Menu
			F9 Setup Defaults
			F10 Save and Exit

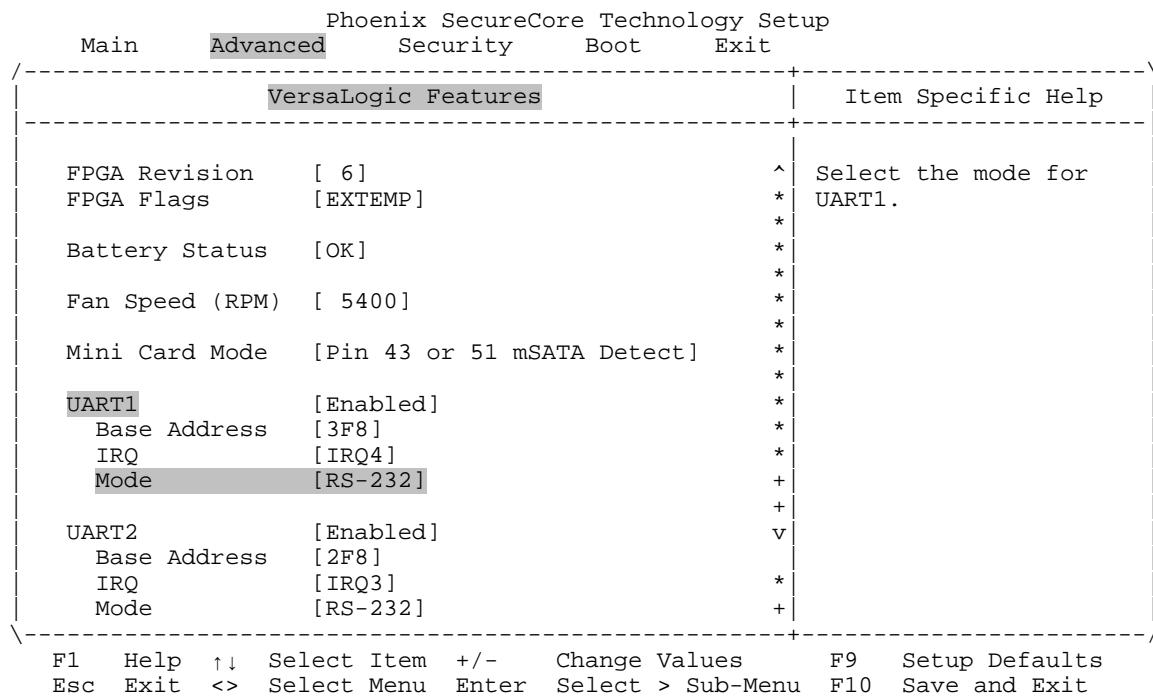
Options | **Disabled**      Disables UART1  
**Enabled (default)**      Enables UART1

**Advanced → VersaLogic Features → UART1 → Base Address**

Options		3F8 (default)
		2F8
		3E8
		2E8
		200
		208
		220
		228
		238
		338

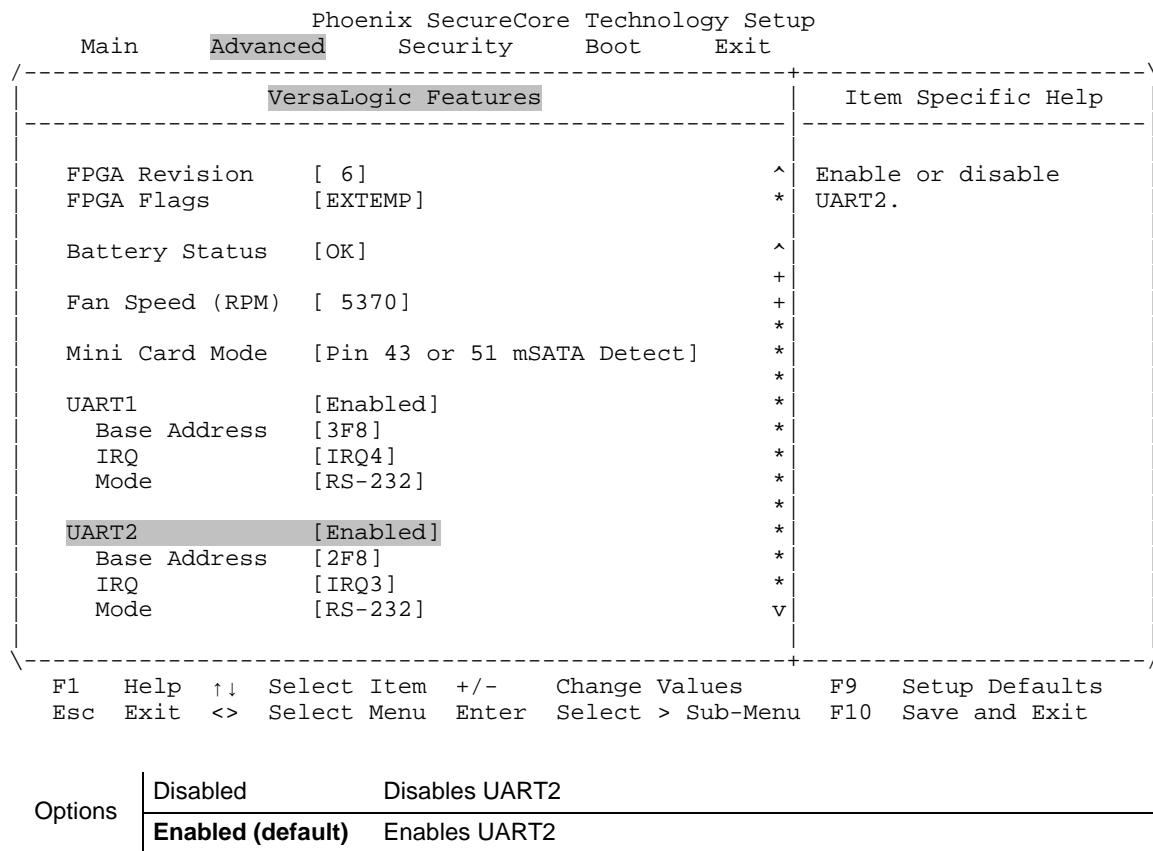
**Advanced → VersaLogic Features → UART1 → IRQ**

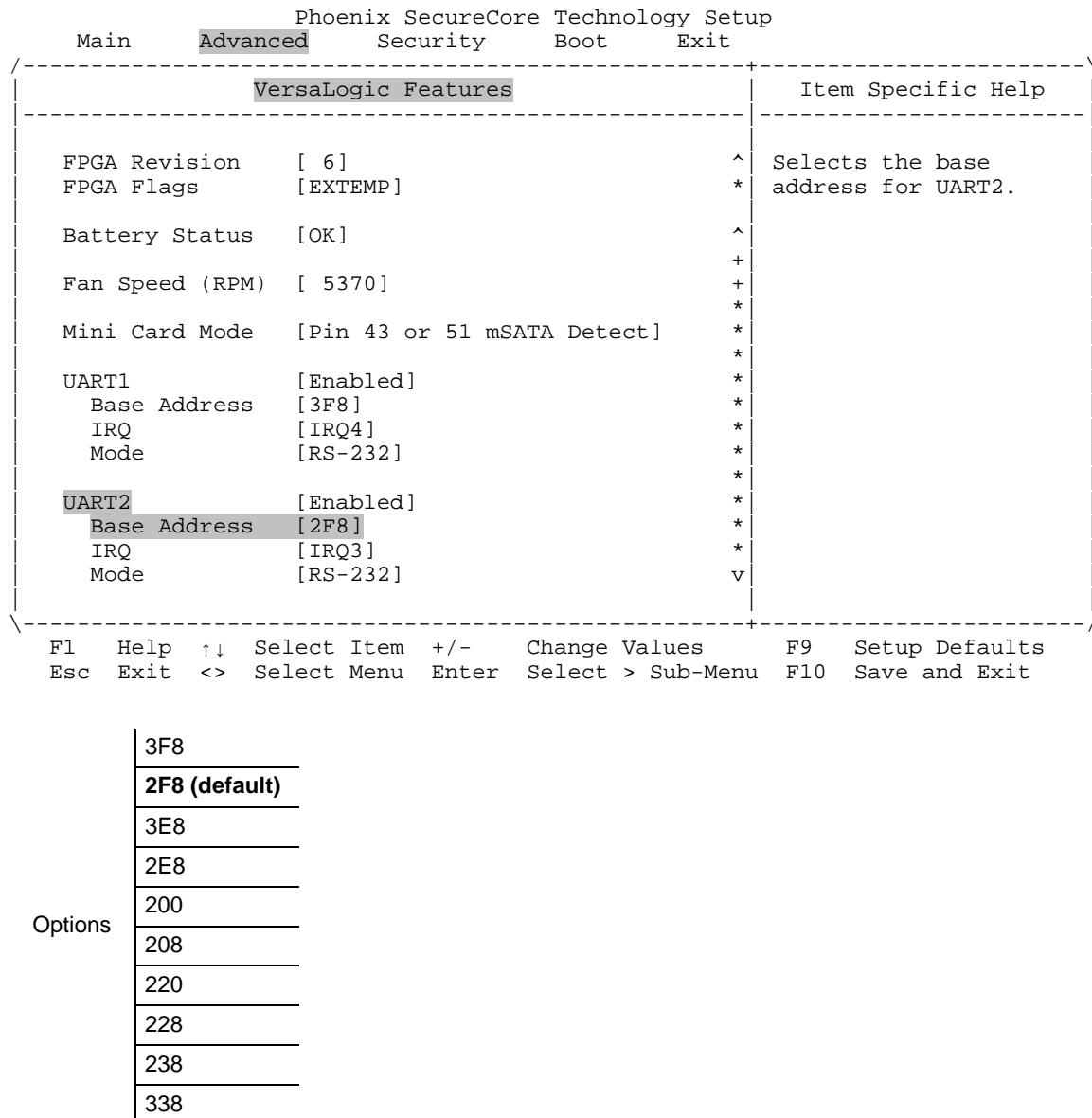
Options	Disabled
	IRQ3
	<b>IRQ4 (default)</b>
	IRQ5
	IRQ10
	IRQ6
	IRQ7
	IRQ9
	IRQ11

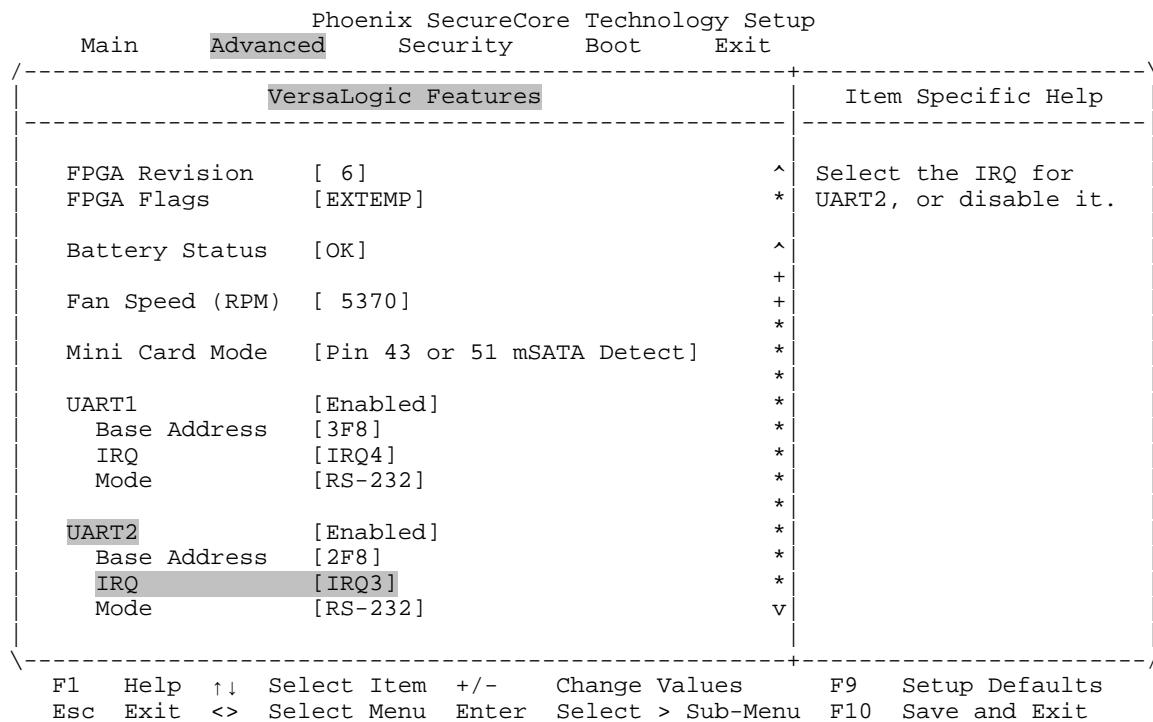
**Advanced → VersaLogic Features → UART1 → Mode**

Options	<b>RS-232 (default)</b>
	RS-422
	RS-485 (Manual Direction Control)
	RS-485 (Automatic Direction Control)

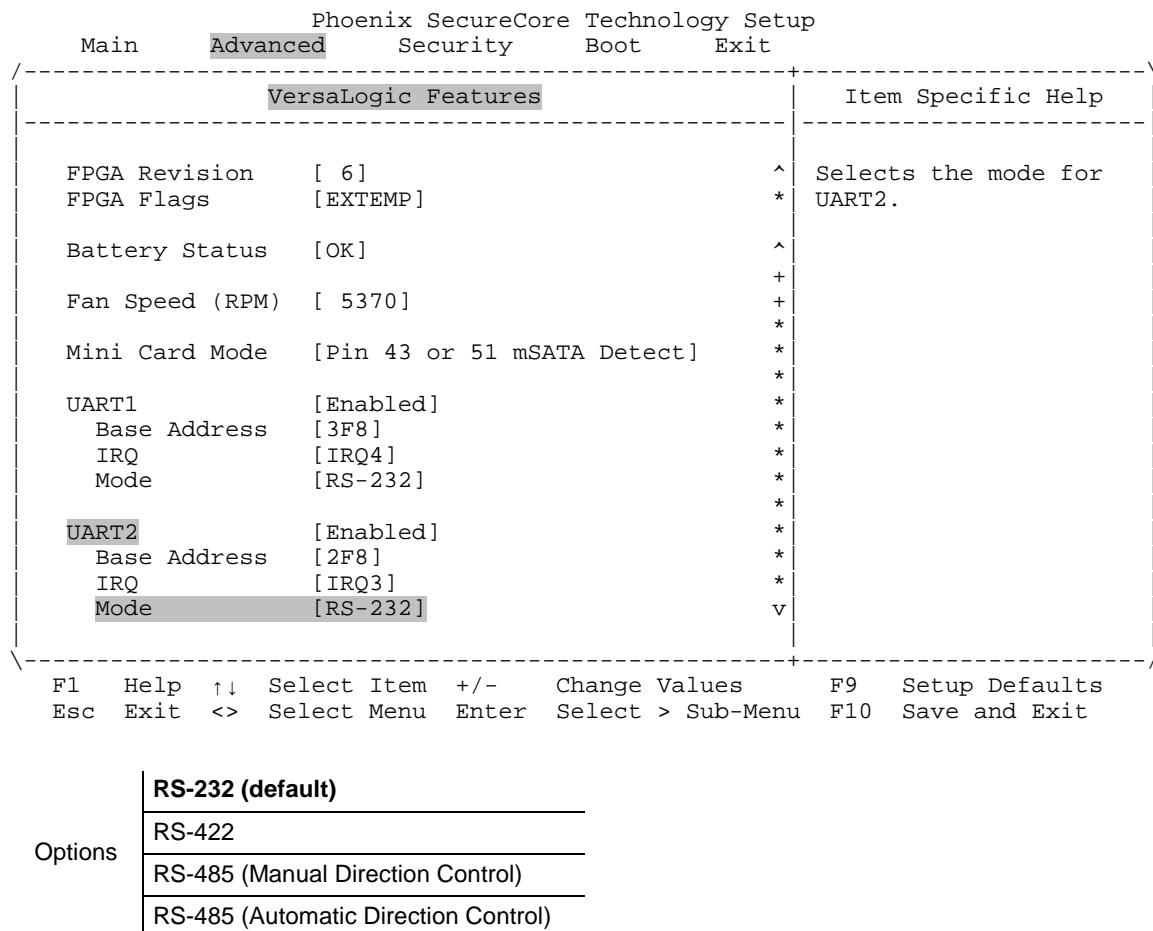
## Advanced → VersaLogic Features → UART2



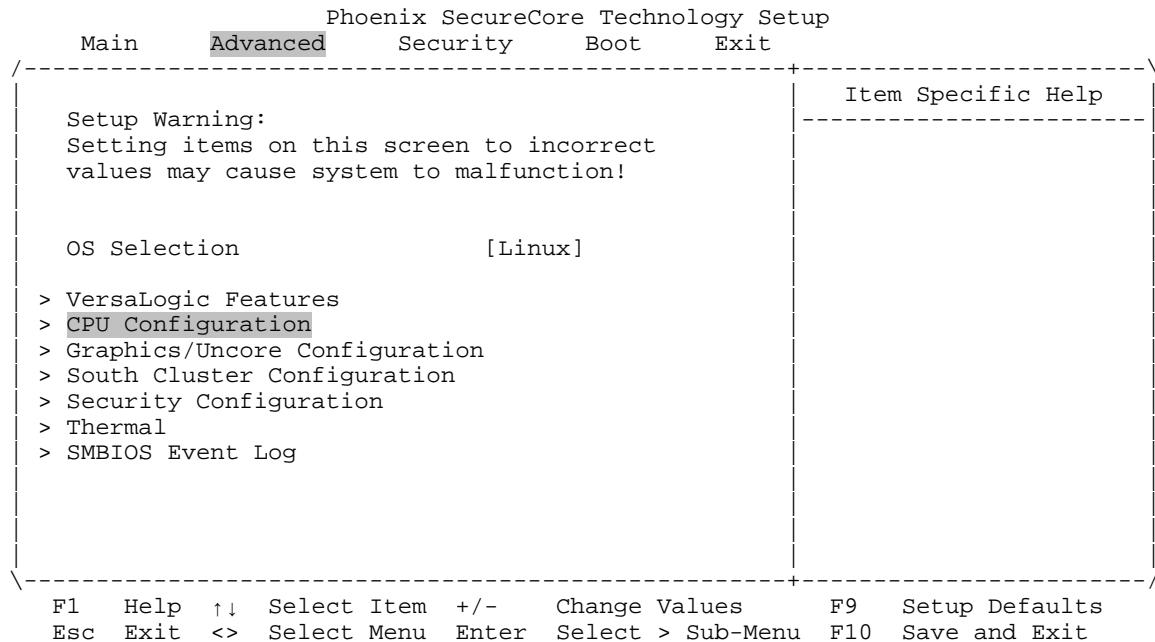
**Advanced → VersaLogic Features → UART2 → Base Address**

**Advanced → VersaLogic Features → UART2 → IRQ**

Options	Disabled
	<b>IRQ3 (default)</b>
	IRQ4
	IRQ5
	IRQ10
	IRQ6
	IRQ7
	IRQ9
	IRQ11

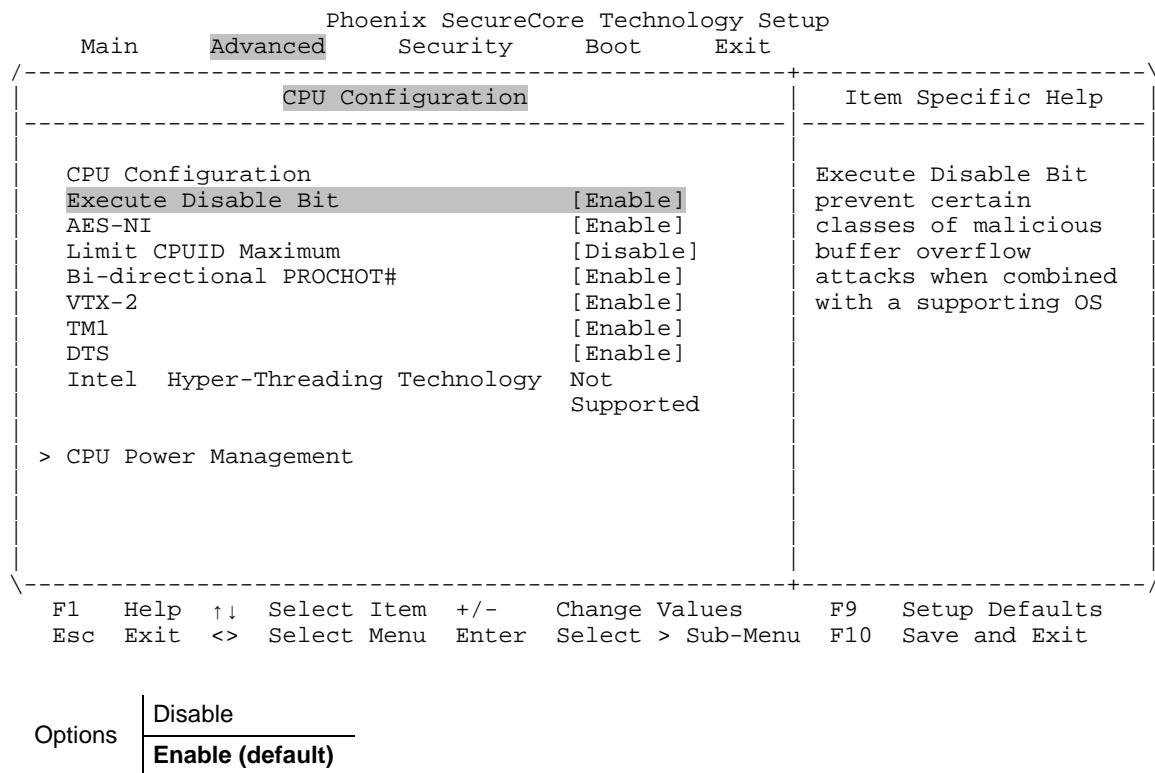
**Advanced → VersaLogic Features → UART2 → Mode**

## Advanced → CPU Configuration

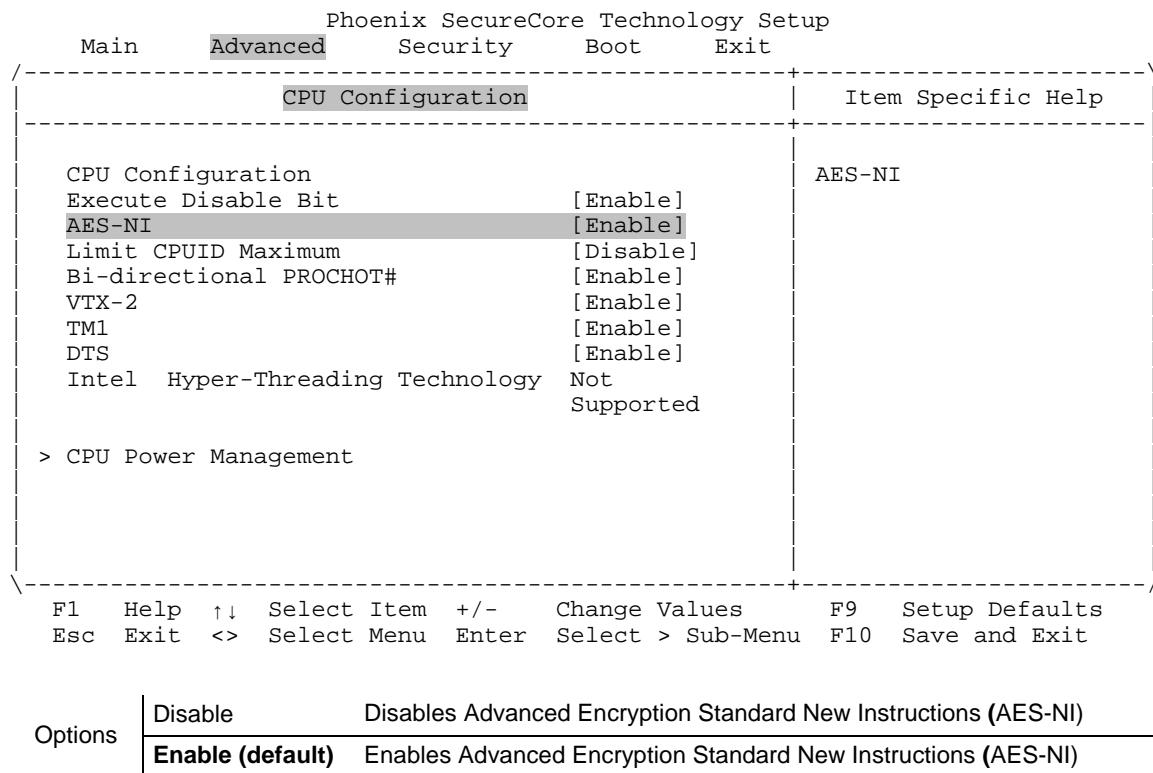


This is the top-level screen for the CPU Configuration menu.

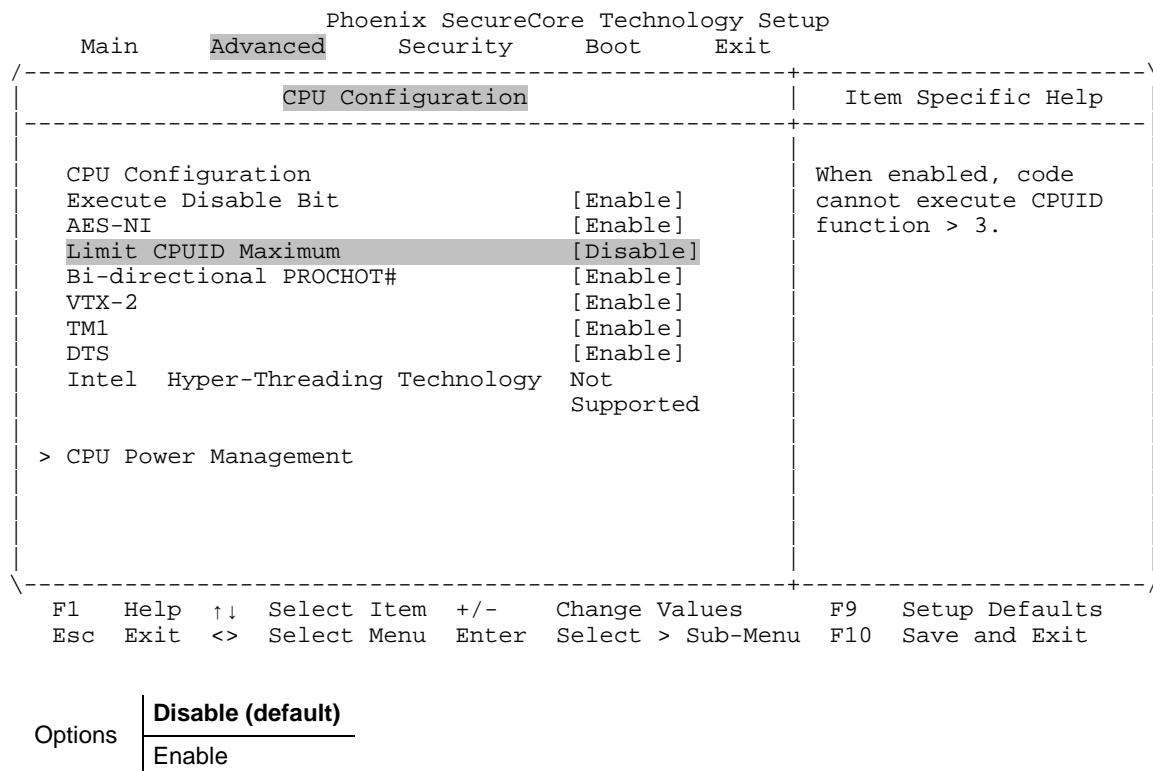
## Advanced → CPU Configuration → Execute Disable Bit



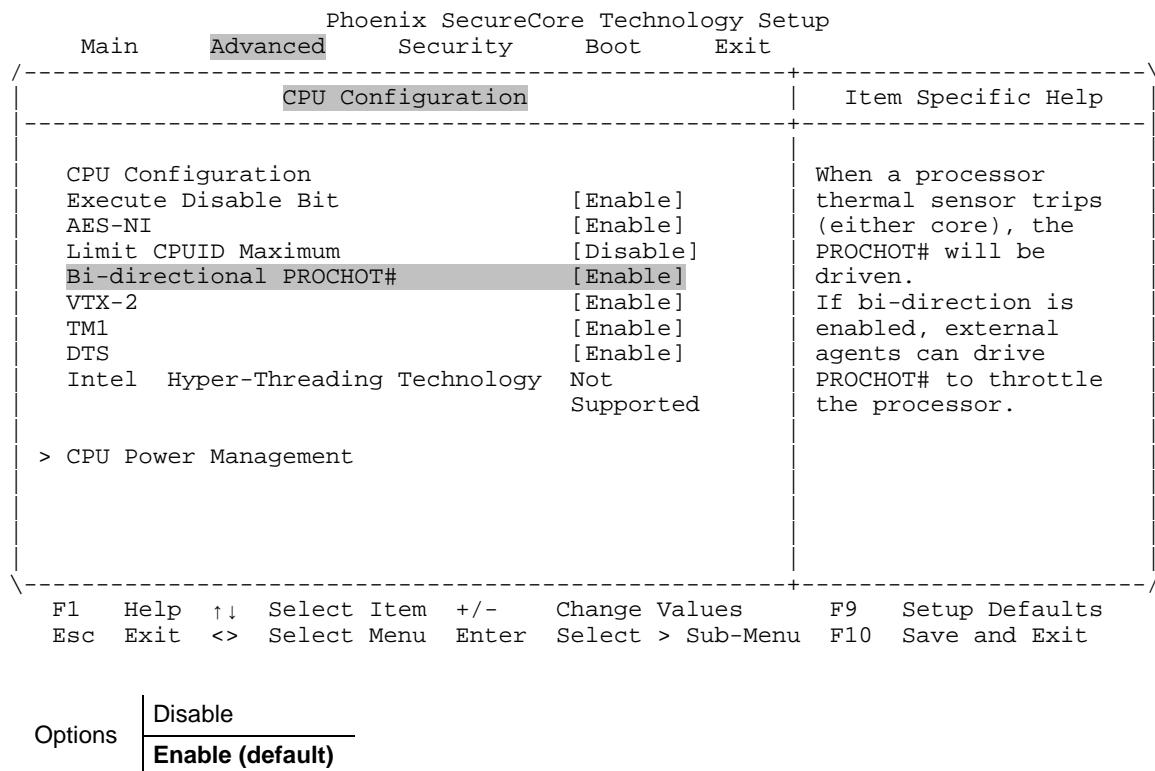
## Advanced → CPU Configuration → AES-NI



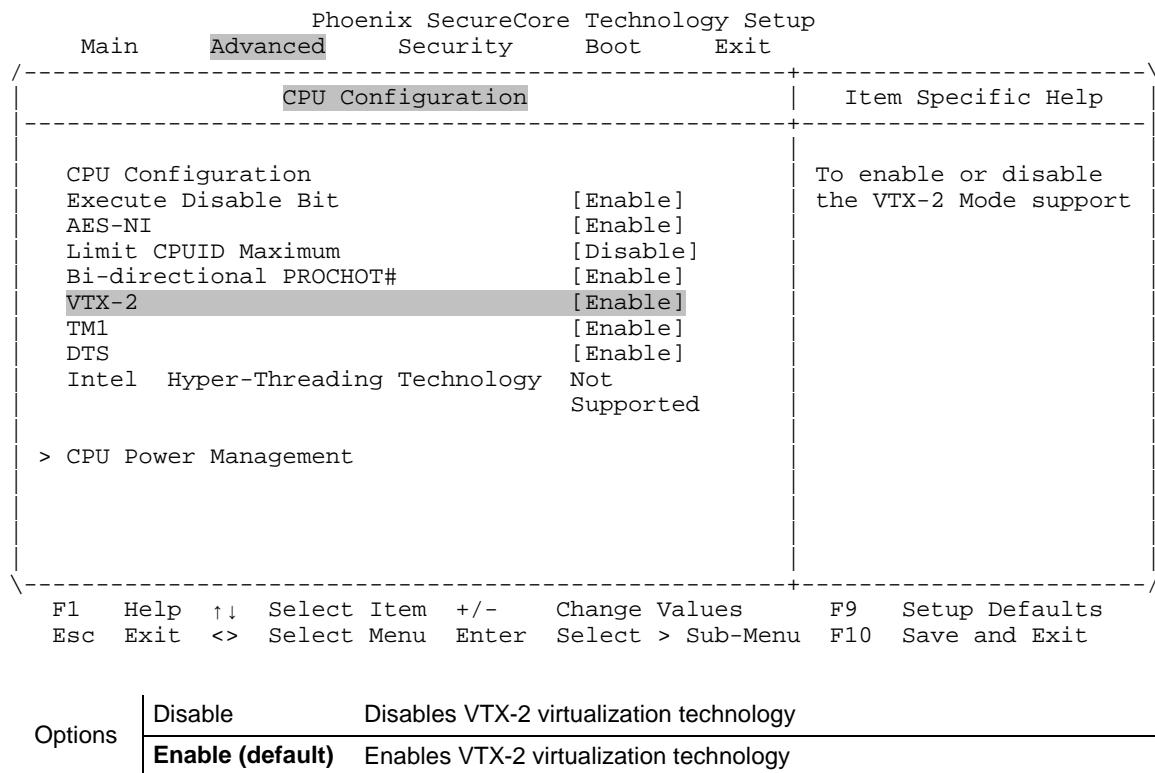
## Advanced → CPU Configuration → Limit CPUID Maximum



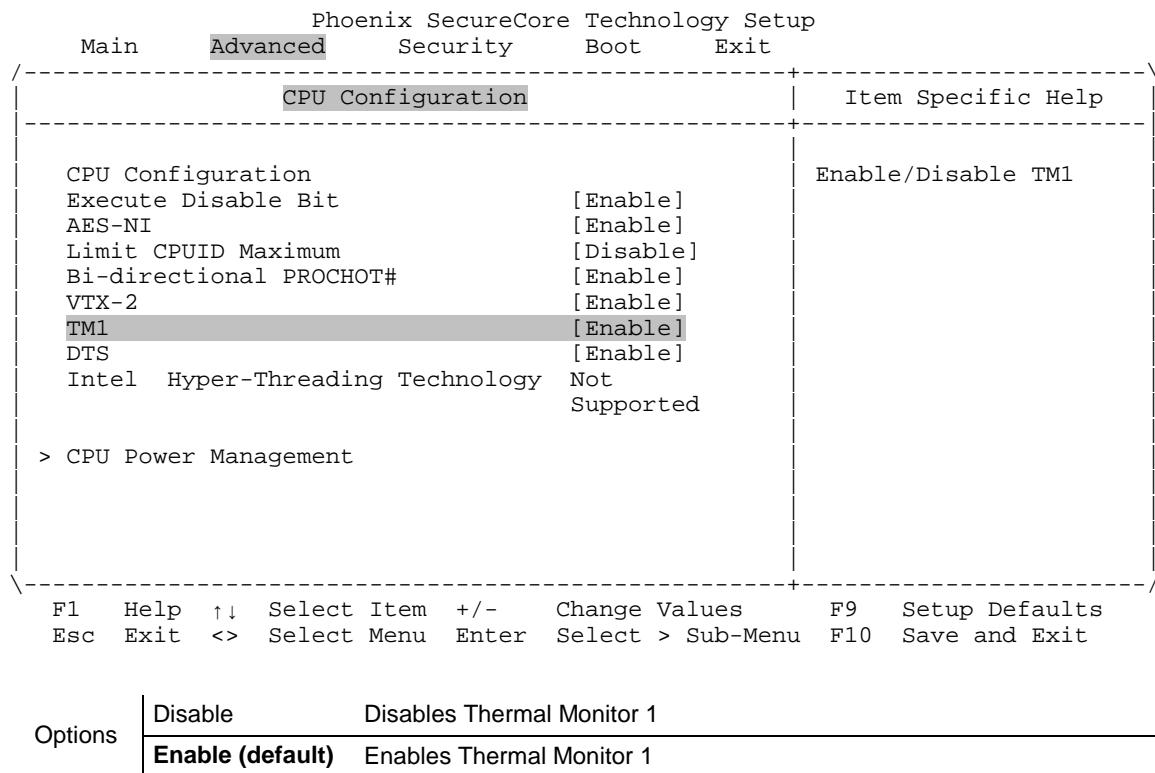
## Advanced → CPU Configuration → Bi-directional PROCHOT#



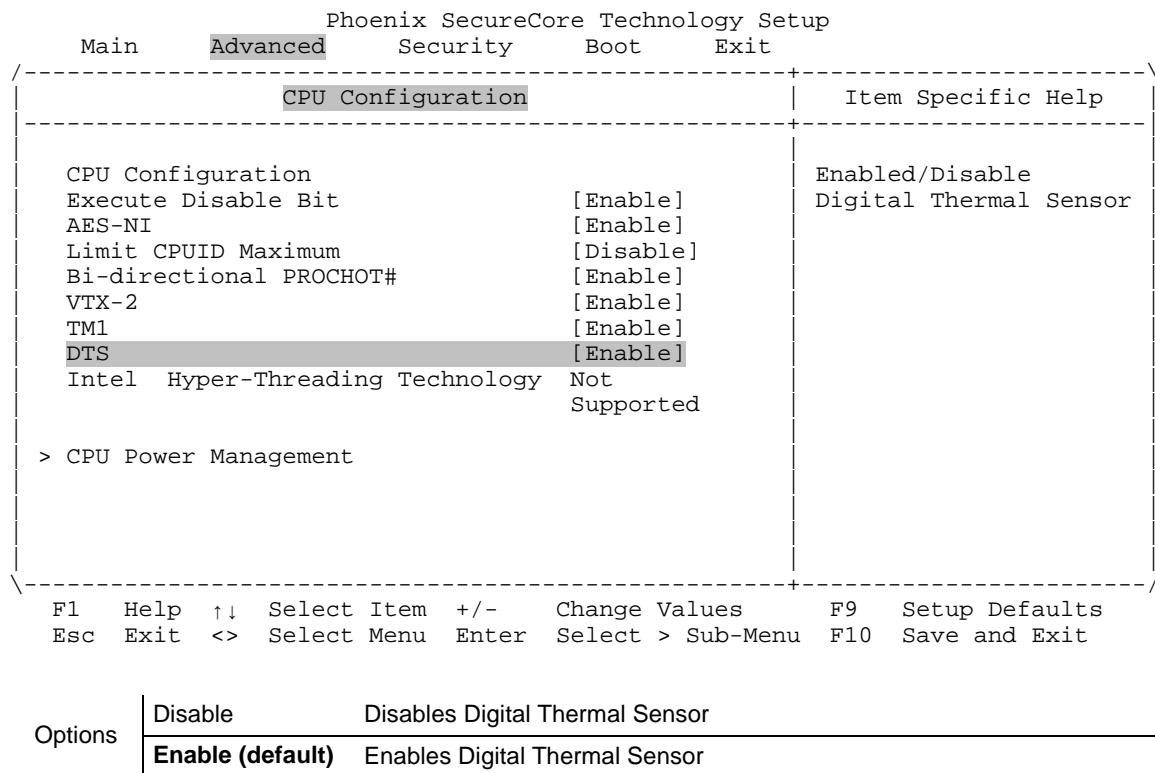
## Advanced → CPU Configuration → VTX-2

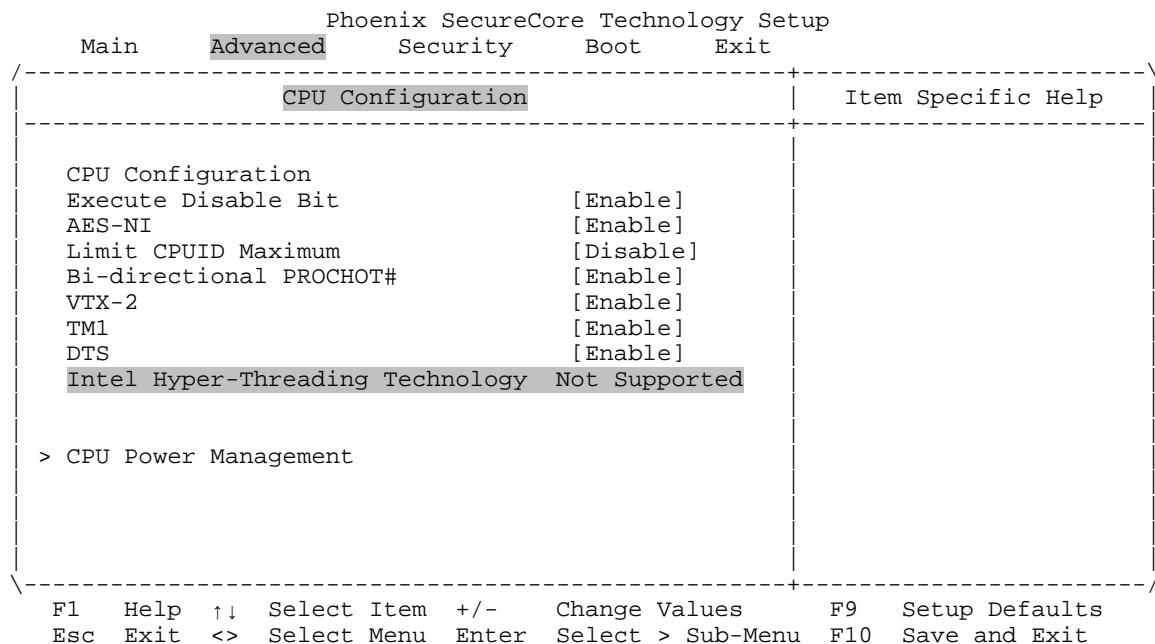


## Advanced → CPU Configuration → TM1



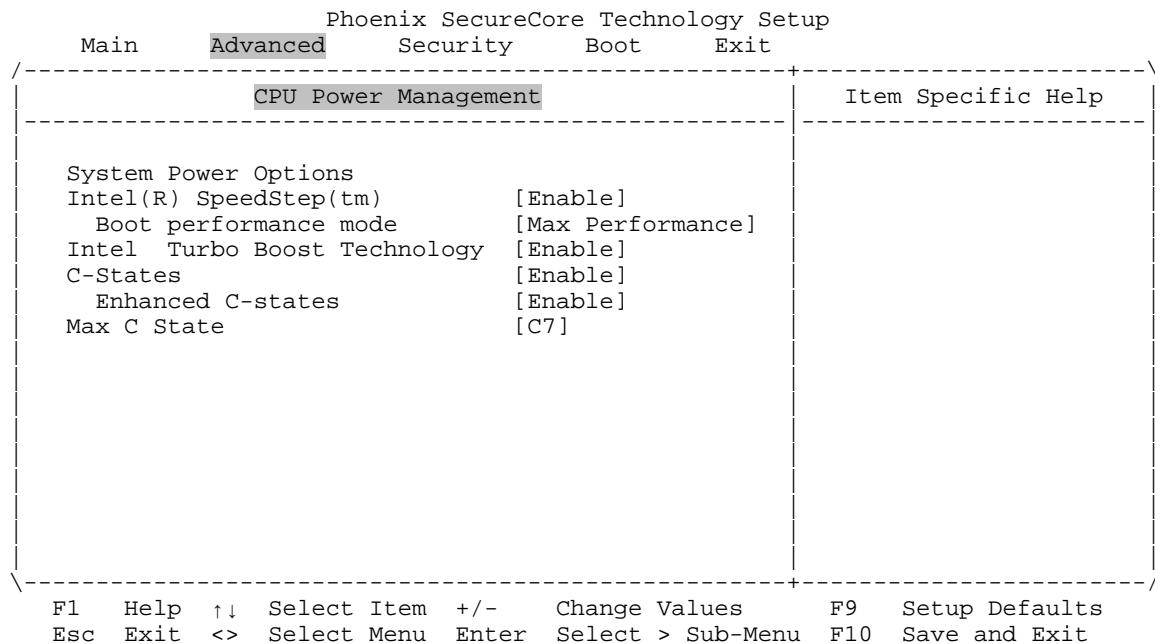
## Advanced → CPU Configuration → DTS



**Advanced → CPU Configuration → Intel Hyper-Threading Technology**

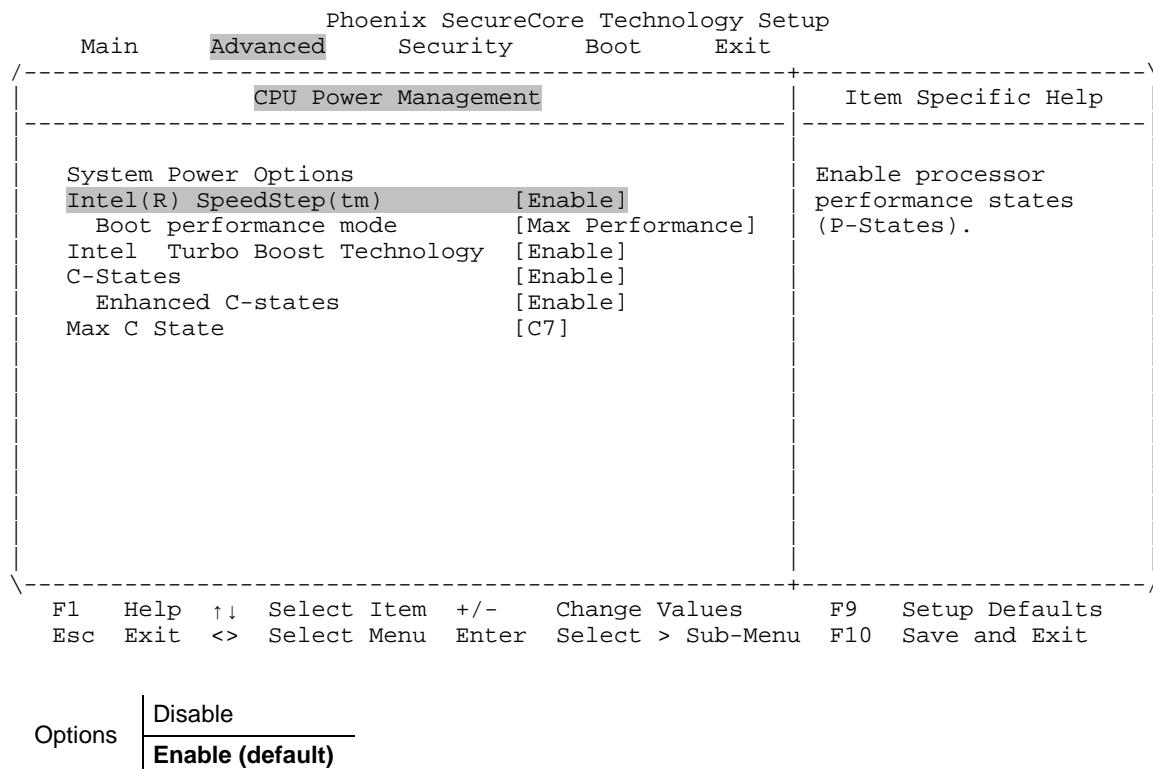
**Note:** This feature is not supported at this time.

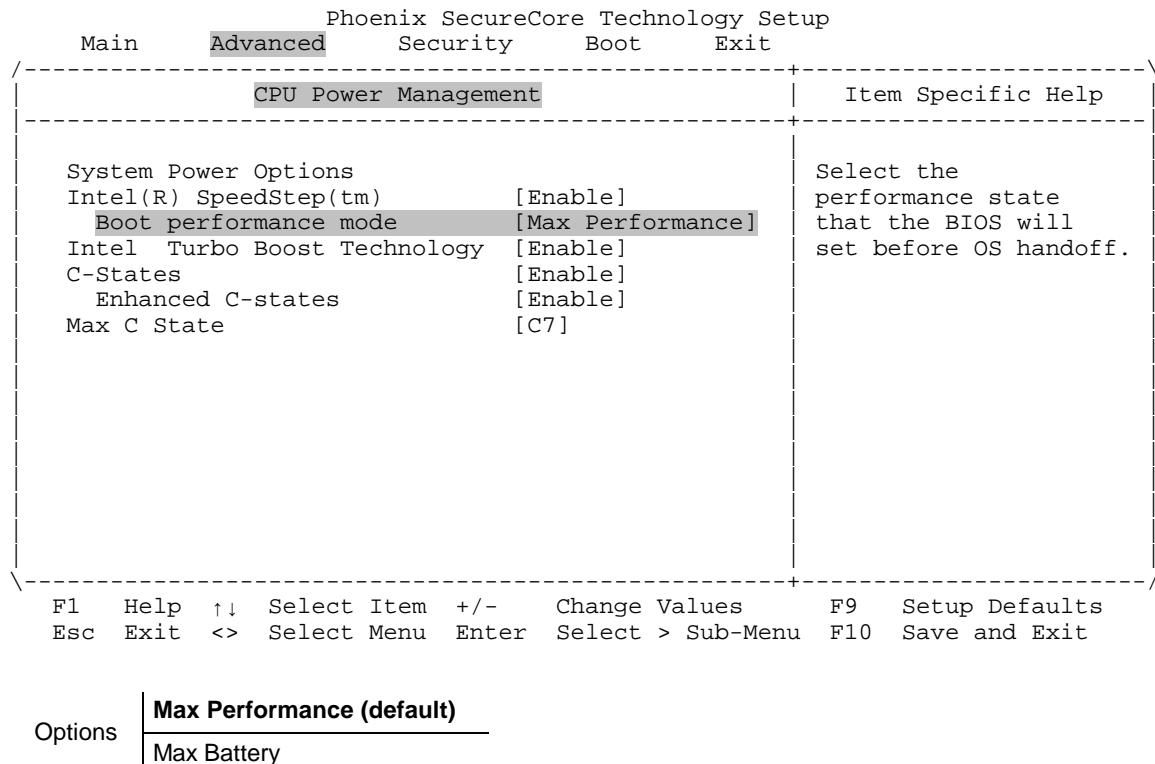
## Advanced → CPU Power Management



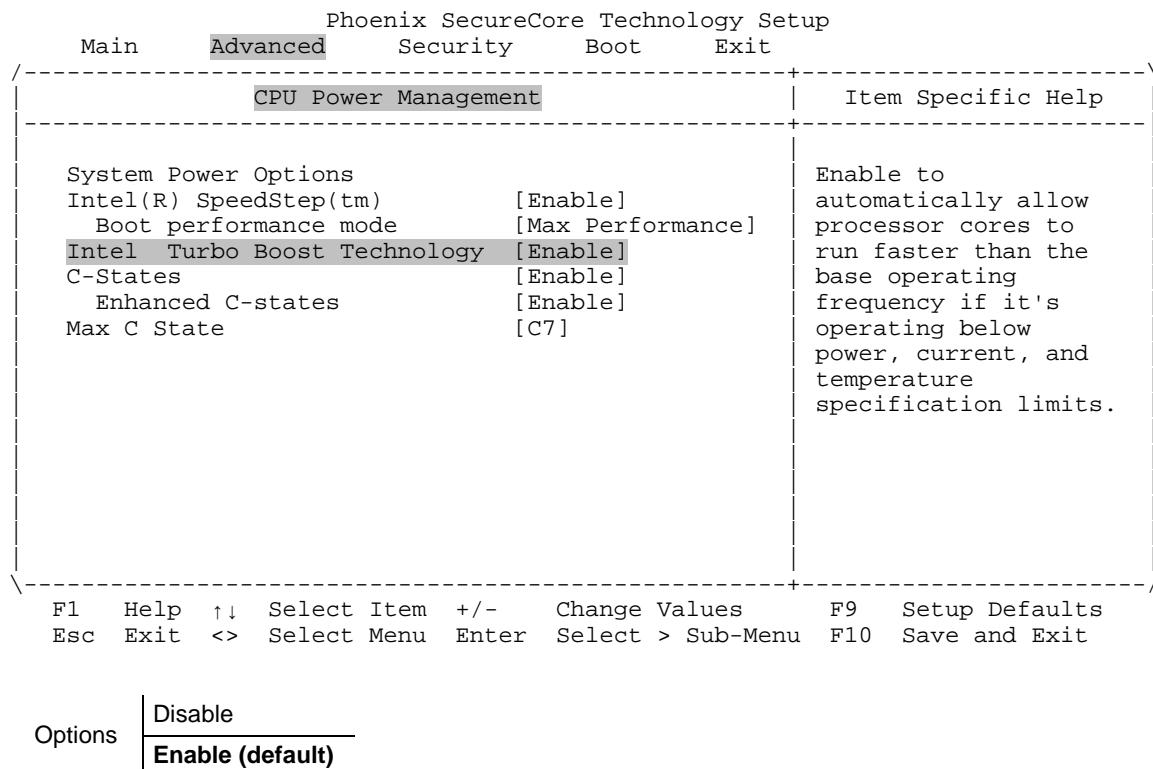
This is the top-level screen of the CPU Power Management menu.

## Advanced → CPU Power Management → Intel SpeedStep

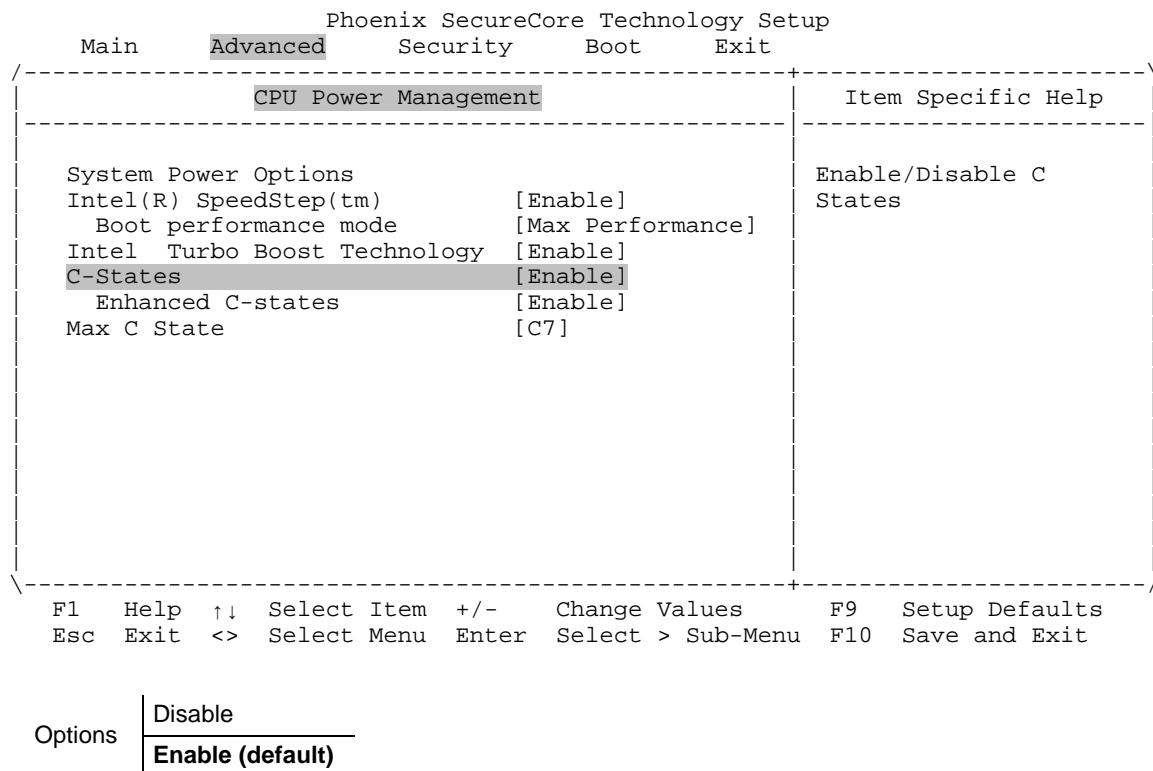


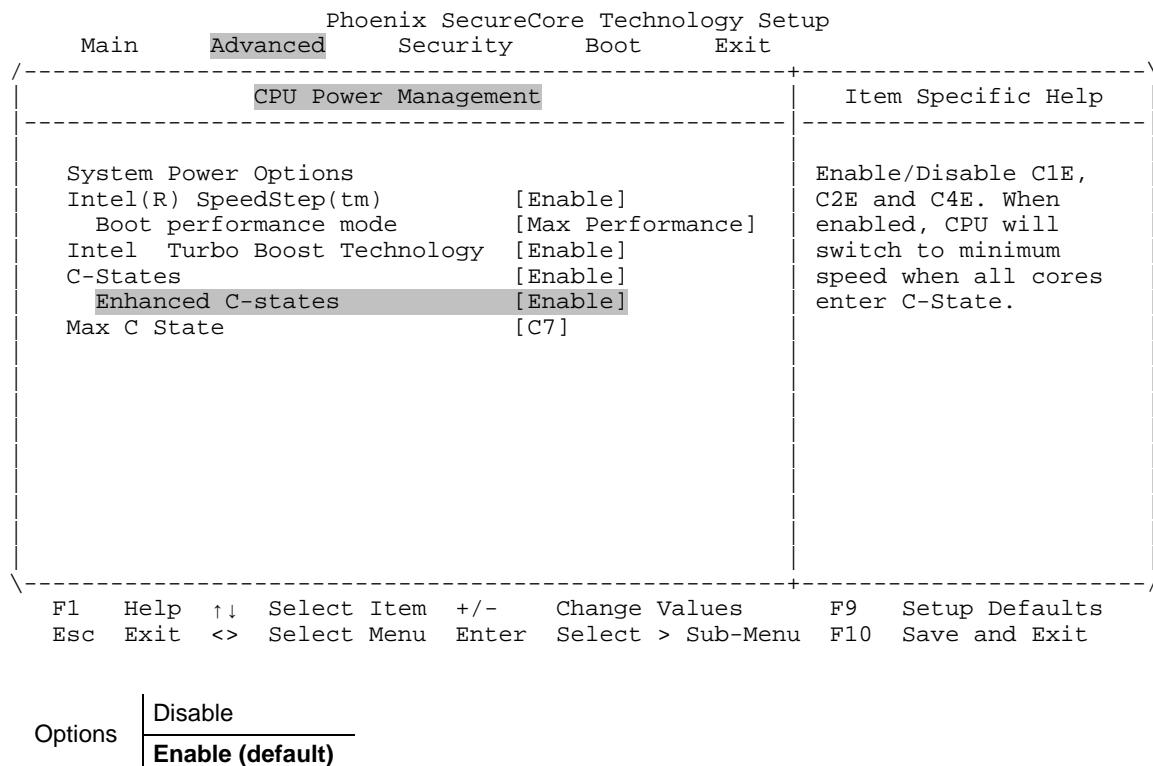
**Advanced → CPU Power Management → Intel SpeedStep → Boot Performance Mode**

## Advanced → CPU Power Management → Intel Turbo Boost Technology

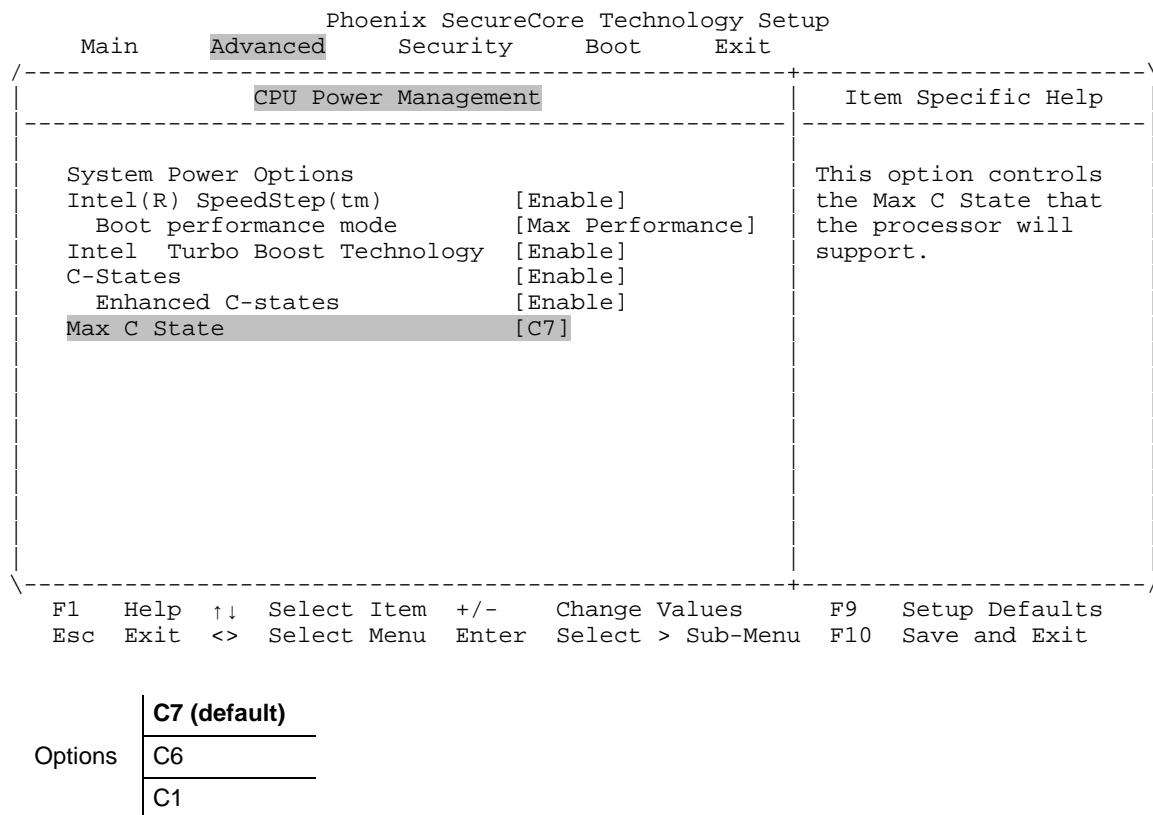


## Advanced → CPU Power Management → C-States

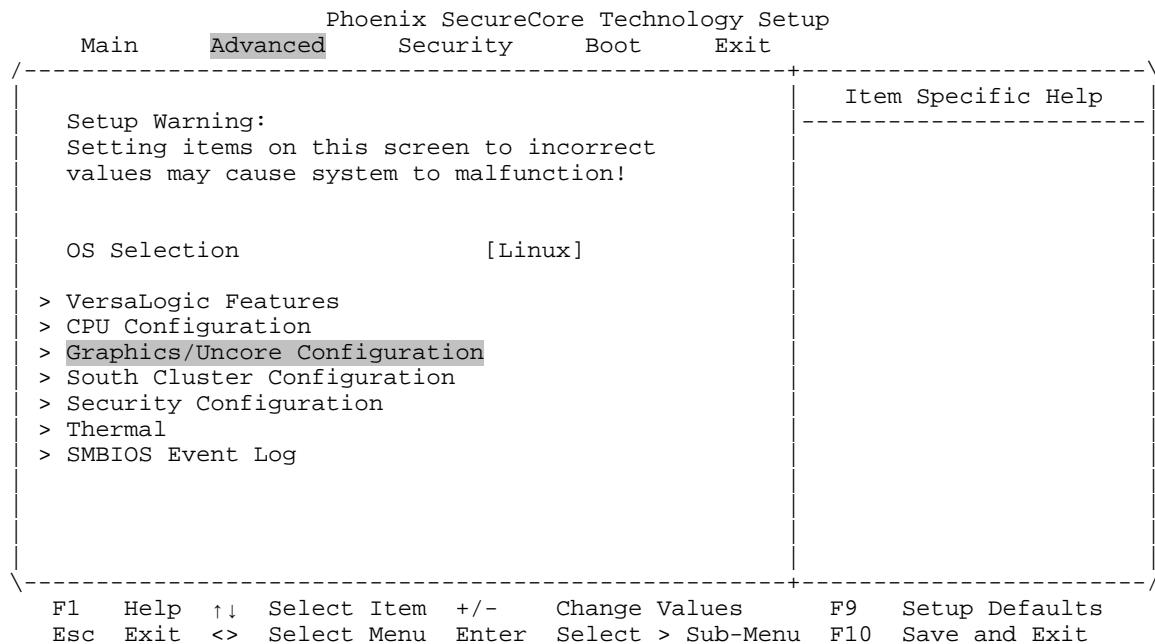


**Advanced → CPU Power Management → C-States → Enhanced C-States**

## Advanced → CPU Power Management → Max C State

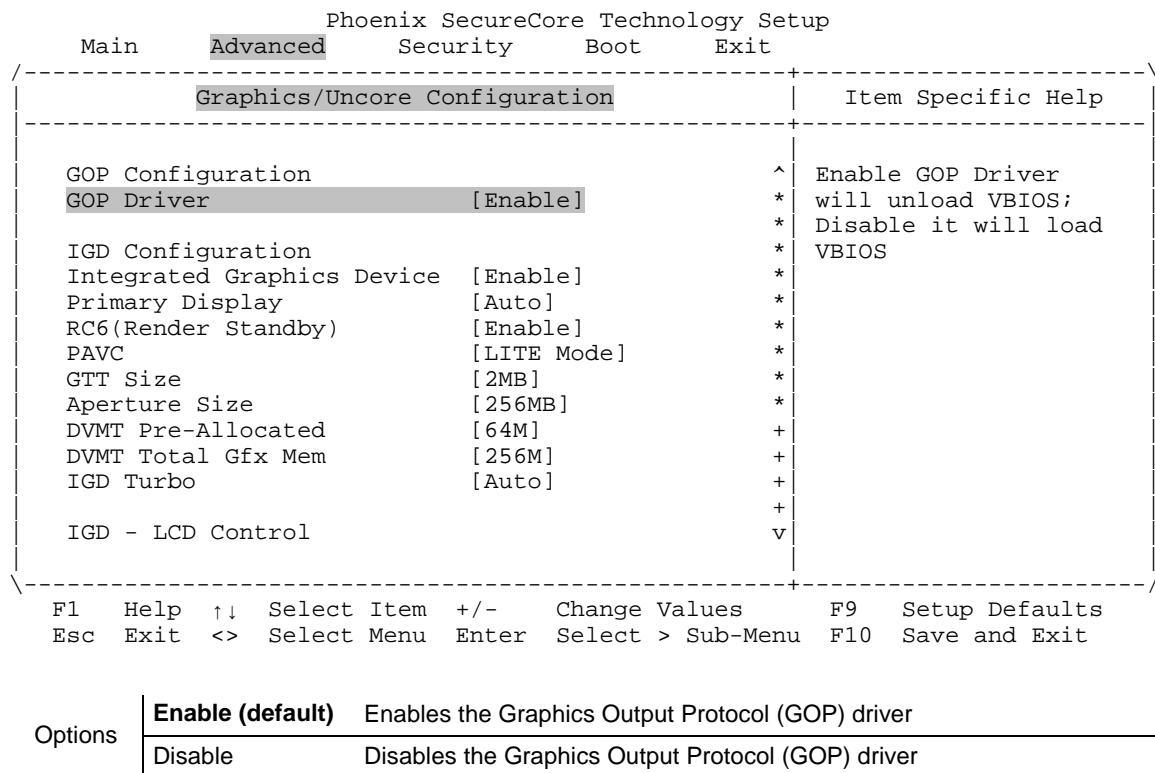


## Advanced → Graphics/Uncore Configuration

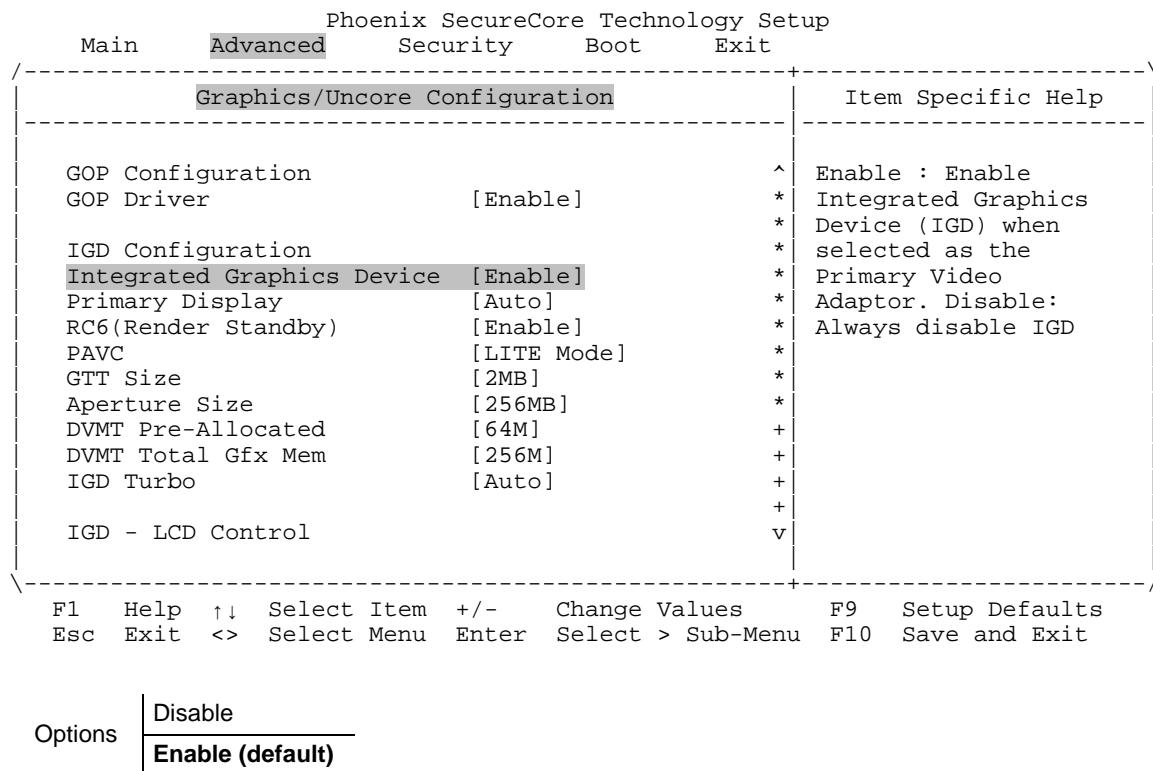


This menu enables you to configure graphics and “uncore” (that is, outside of the SoC’s core) functions.

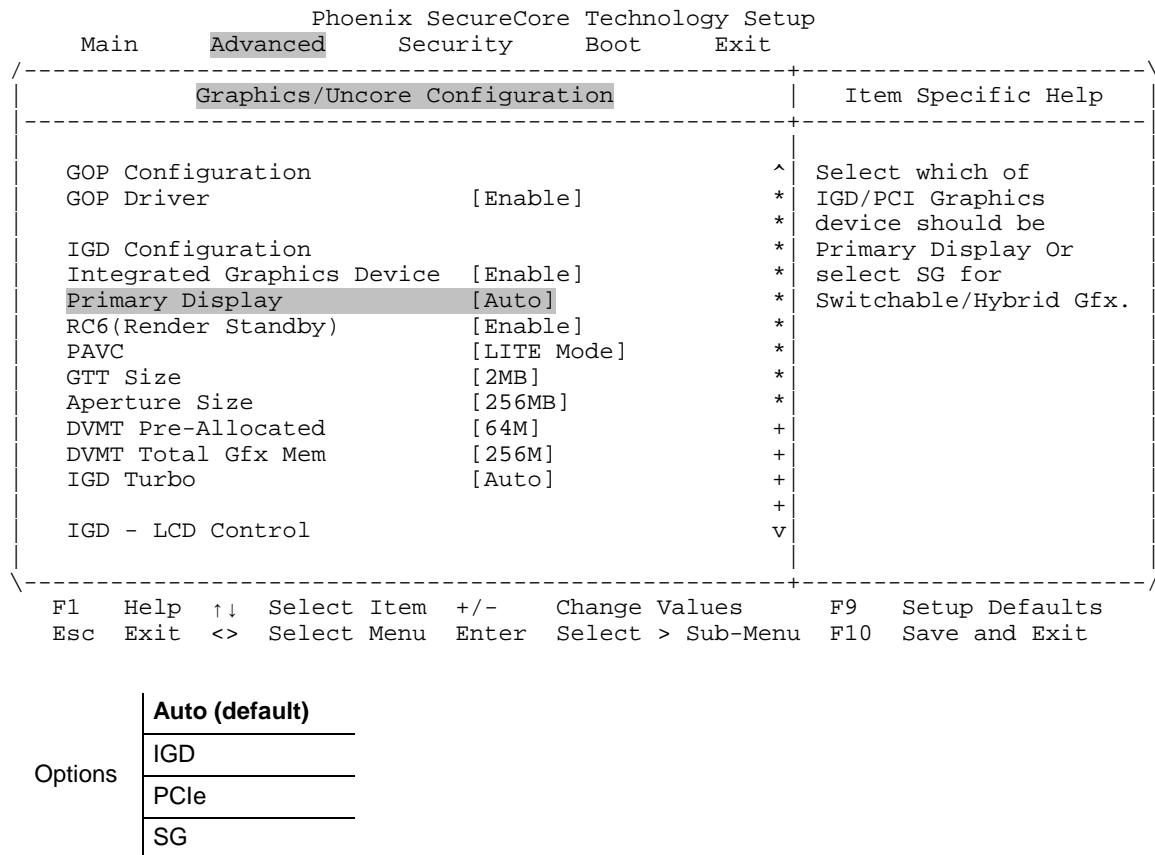
## Advanced → Graphics/Uncore Configuration → GOP Driver



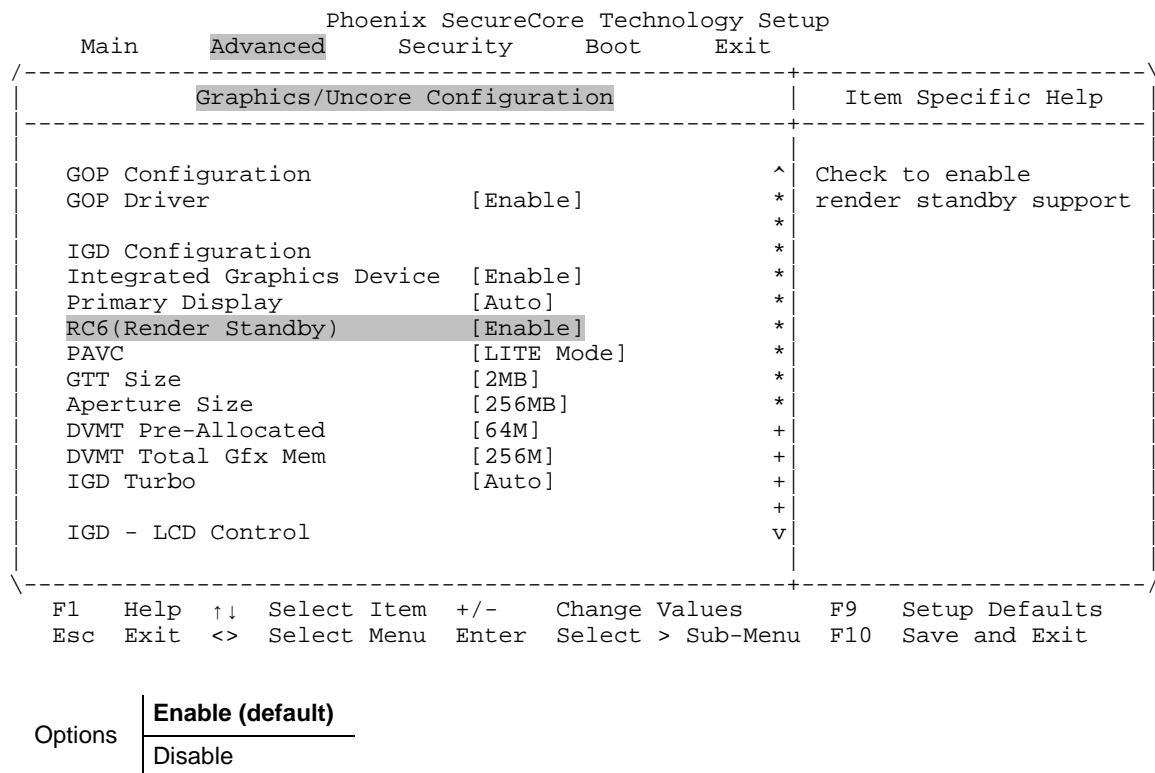
## Advanced → Graphics/Uncore Configuration → Integrated Graphics Device



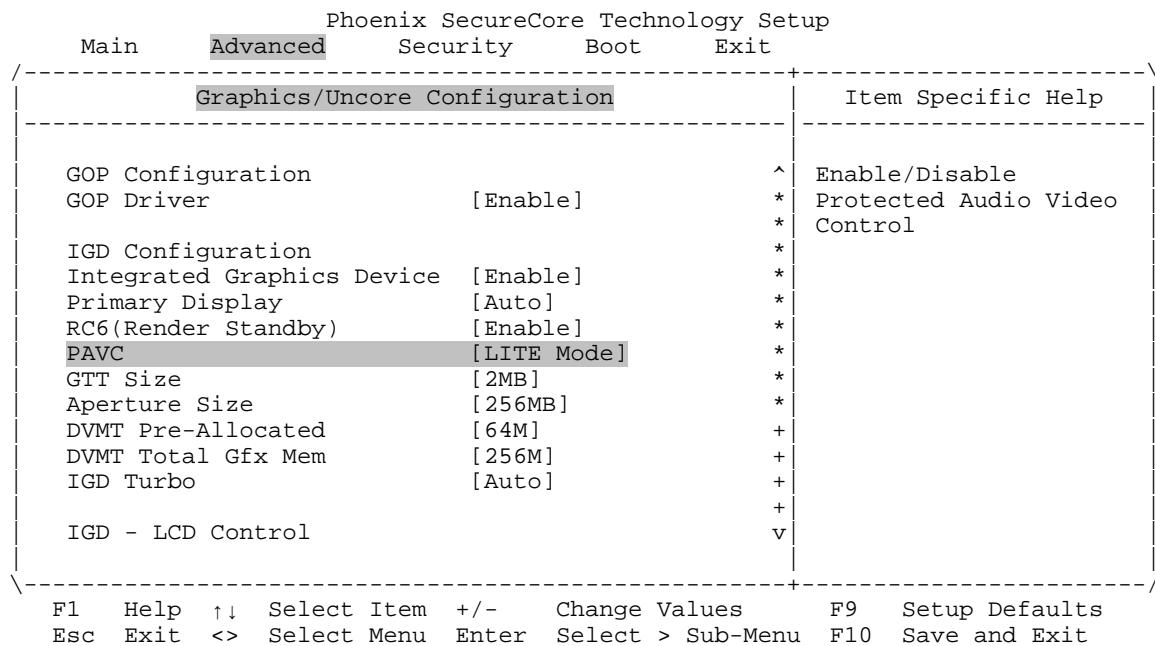
## Advanced → Graphics/Uncore Configuration → Primary Display



## Advanced → Graphics/Uncore Configuration → RC6 (Render Standby)

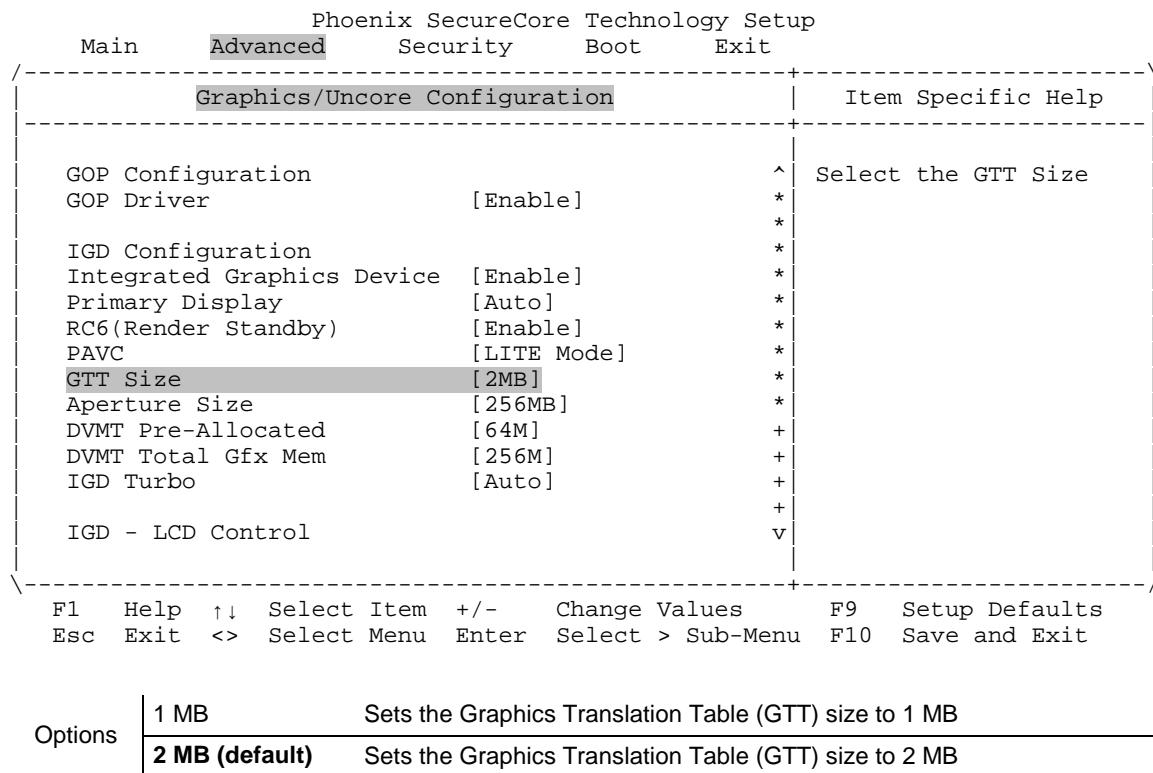


## Advanced → Graphics/Uncore Configuration → PAVC

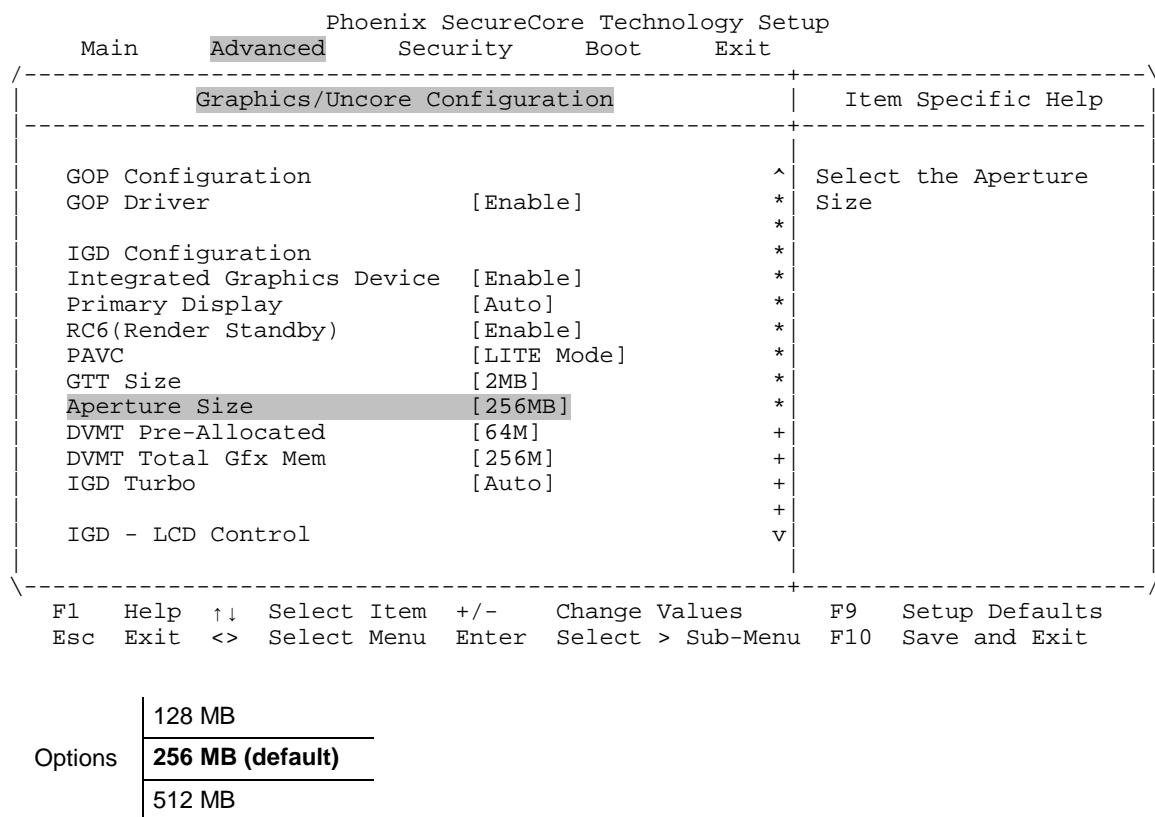


Options	Disable	Disables Protected Audio Video Control (PAVC) support
	<b>LITE Mode (default)</b>	Allows PAVC-protected Blu-ray disks to play.
	SERPENT Mode	Disables the Windows Aero interface and uses ~96 MB of RAM for encrypted data that the operating system cannot see.

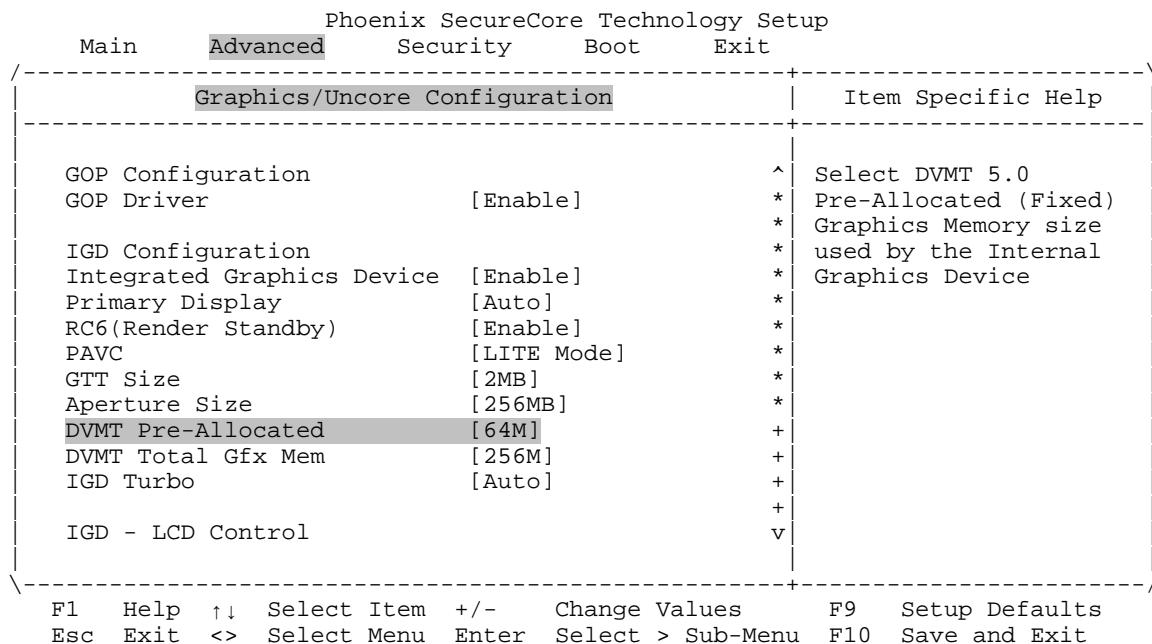
## Advanced → Graphics/Uncore Configuration → GTT Size



## Advanced → Graphics/Uncore Configuration → Aperture Size

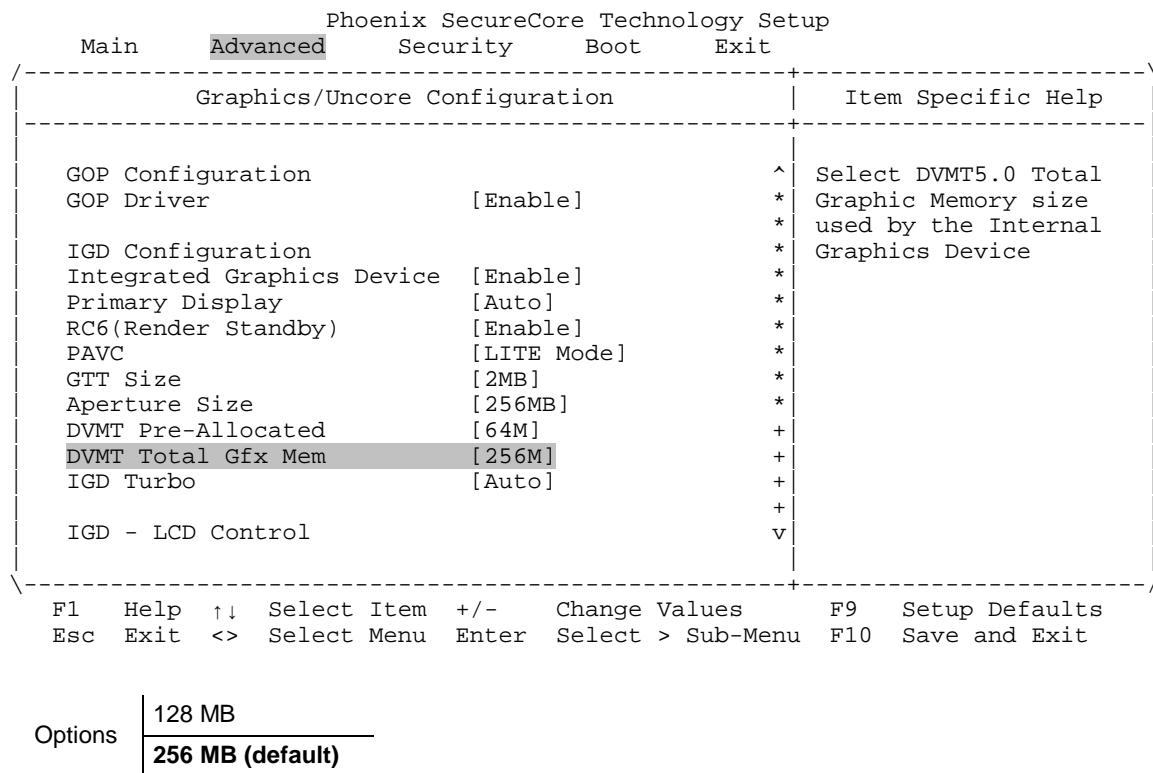


## Advanced → Graphics/Uncore Configuration → DVMT Pre-Allocated

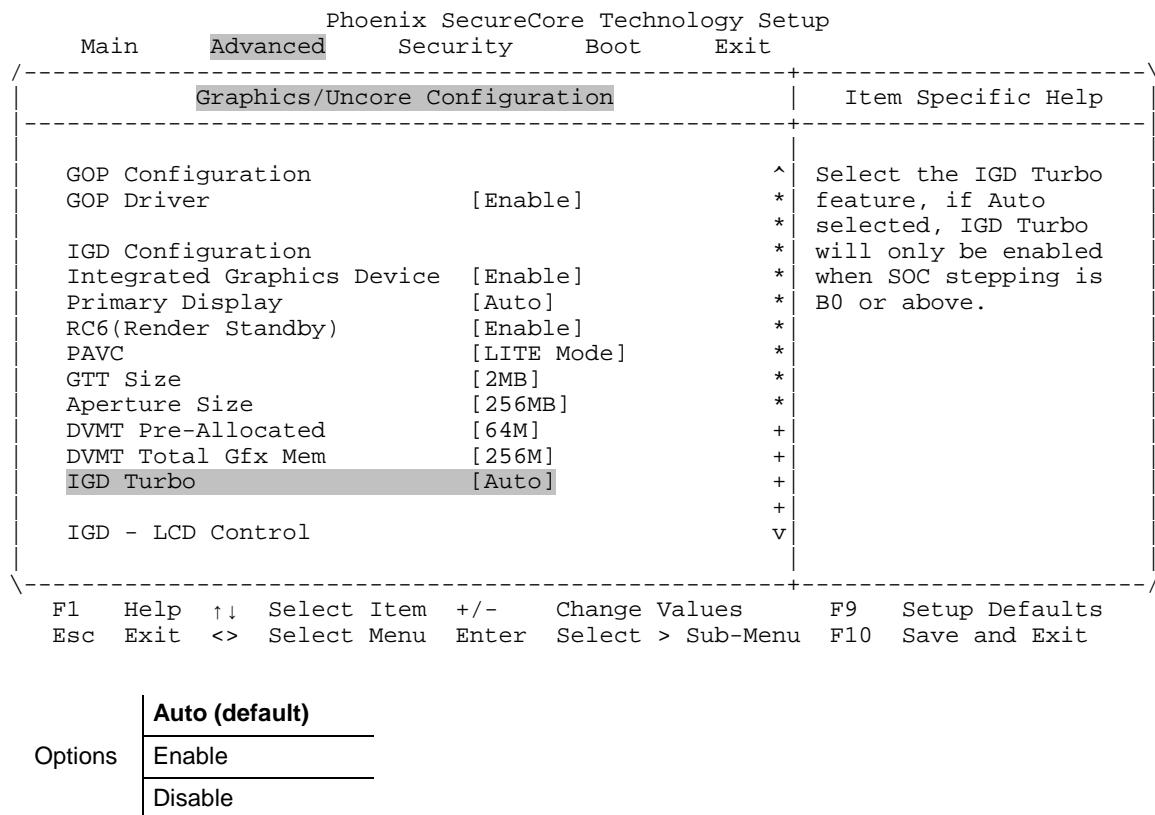


Options	<b>64M (default)</b>	Sets the Dynamic Video Memory Technology (DVMT) size to 64 MB
	96M	Sets the Dynamic Video Memory Technology (DVMT) size to 96 MB
	128M	Sets the Dynamic Video Memory Technology (DVMT) size to 128 MB
	160M	Sets the Dynamic Video Memory Technology (DVMT) size to 160 MB
	192M	Sets the Dynamic Video Memory Technology (DVMT) size to 192 MB
	224M	Sets the Dynamic Video Memory Technology (DVMT) size to 224MB
	256M	Sets the Dynamic Video Memory Technology (DVMT) size to 256 MB
	288M	Sets the Dynamic Video Memory Technology (DVMT) size to 288 MB
	320M	Sets the Dynamic Video Memory Technology (DVMT) size to 320 MB
	352M	Sets the Dynamic Video Memory Technology (DVMT) size to 352 MB
	384M	Sets the Dynamic Video Memory Technology (DVMT) size to 384 MB
	416M	Sets the Dynamic Video Memory Technology (DVMT) size to 416 MB
	448M	Sets the Dynamic Video Memory Technology (DVMT) size to 448 MB
	480M	Sets the Dynamic Video Memory Technology (DVMT) size to 480 MB
	512M	Sets the Dynamic Video Memory Technology (DVMT) size to 512 MB

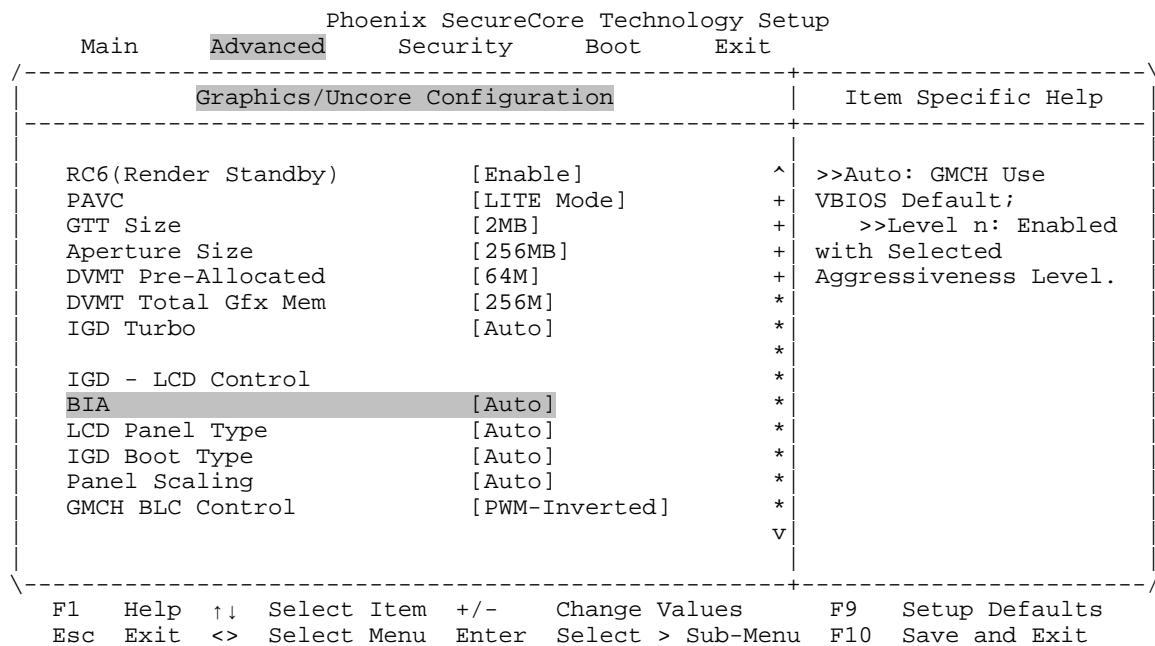
## Advanced → Graphics/Uncore Configuration → DVMT Total Gfx Mem



## Advanced → Graphics/Uncore Configuration → IGD Turbo

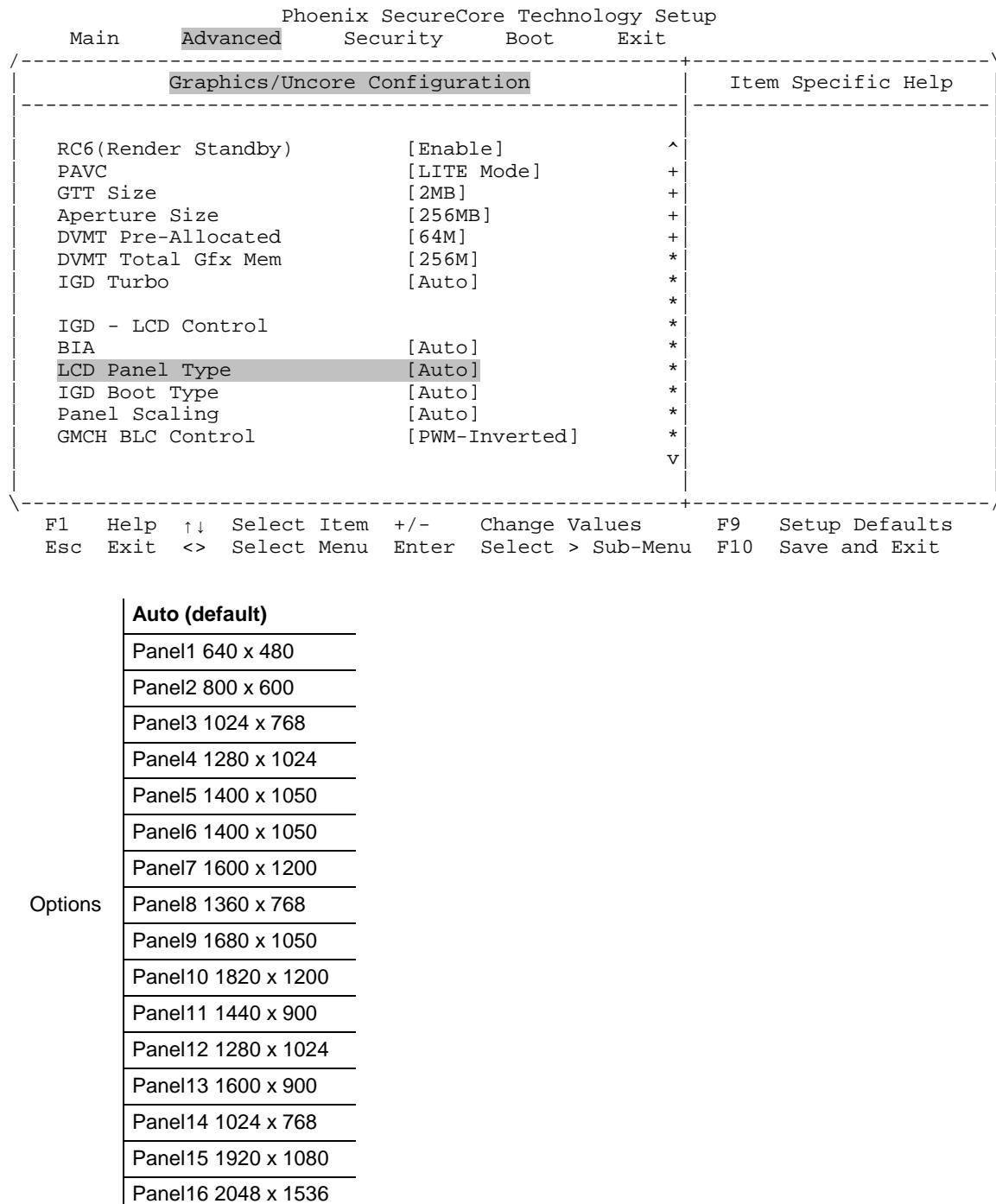


## Advanced → Graphics/Uncore Configuration → BIA

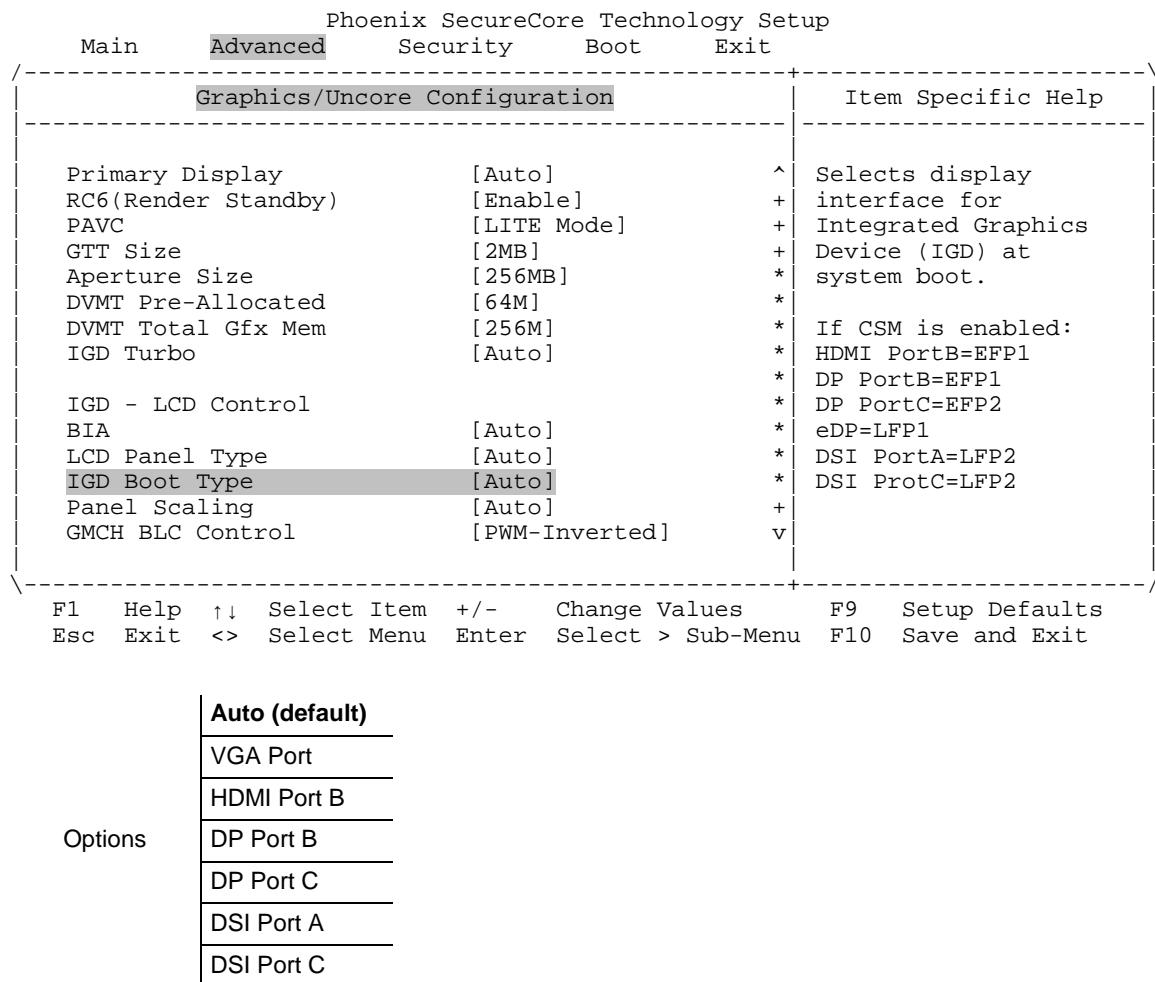


<b>Auto (default)</b> Auto-configures Backlight Image Adaptation (BIA)	
Options	Disabled
	Level 1
	Level 2
	Level 3
	Level 4
	Level 5

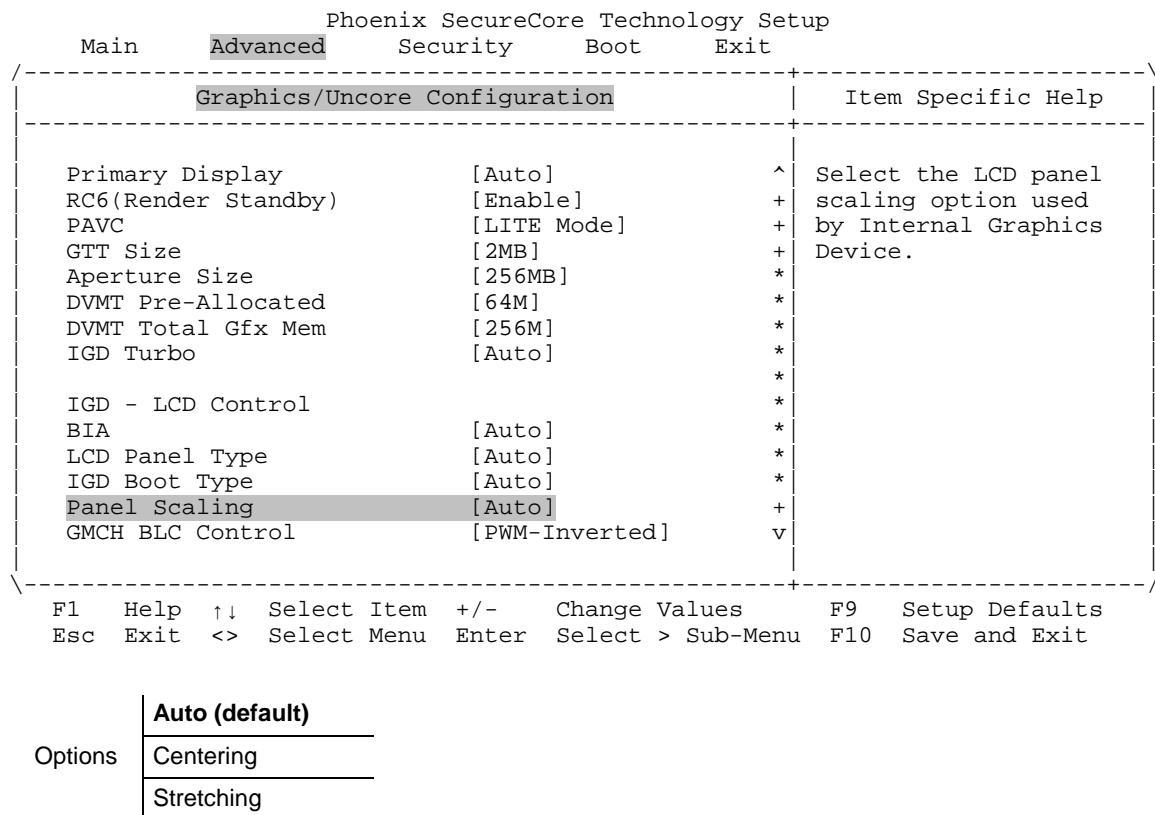
## Advanced → Graphics/Uncore Configuration → LCD Panel Type



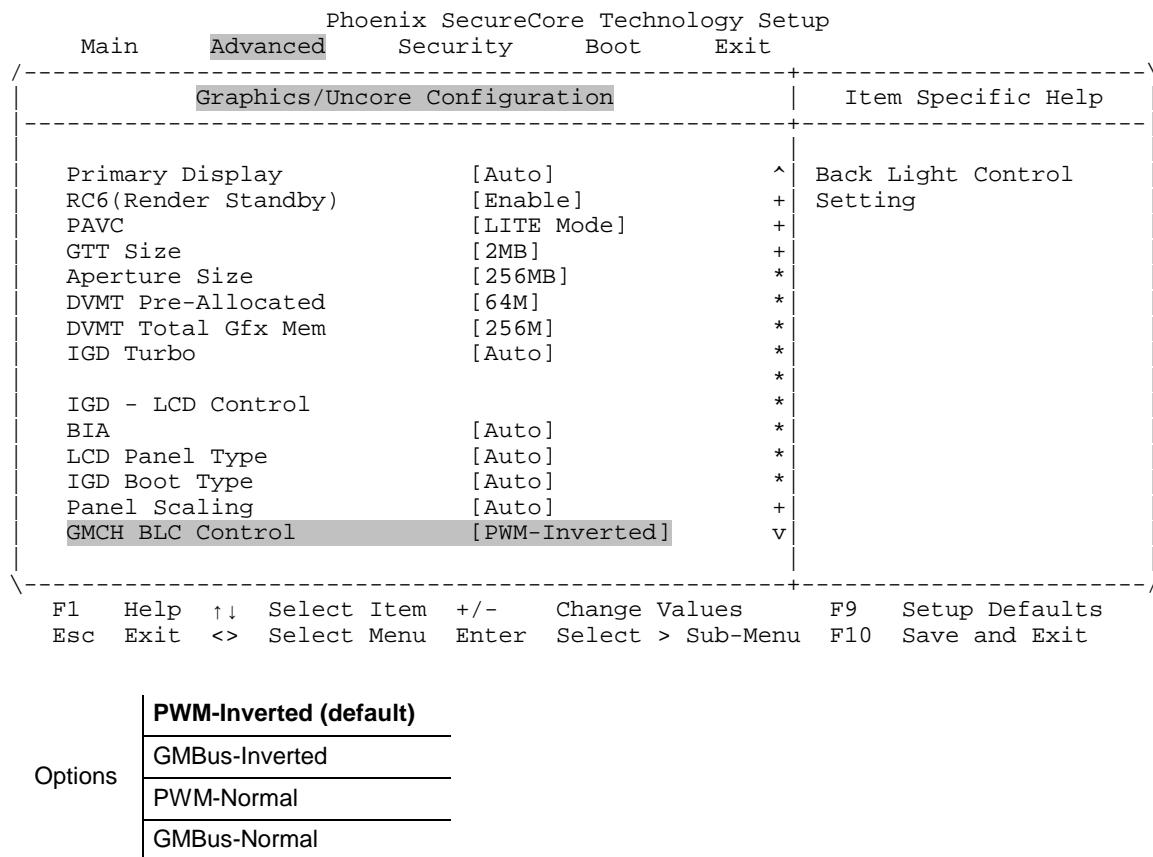
## Advanced → Graphics/Uncore Configuration → IGD Boot Type



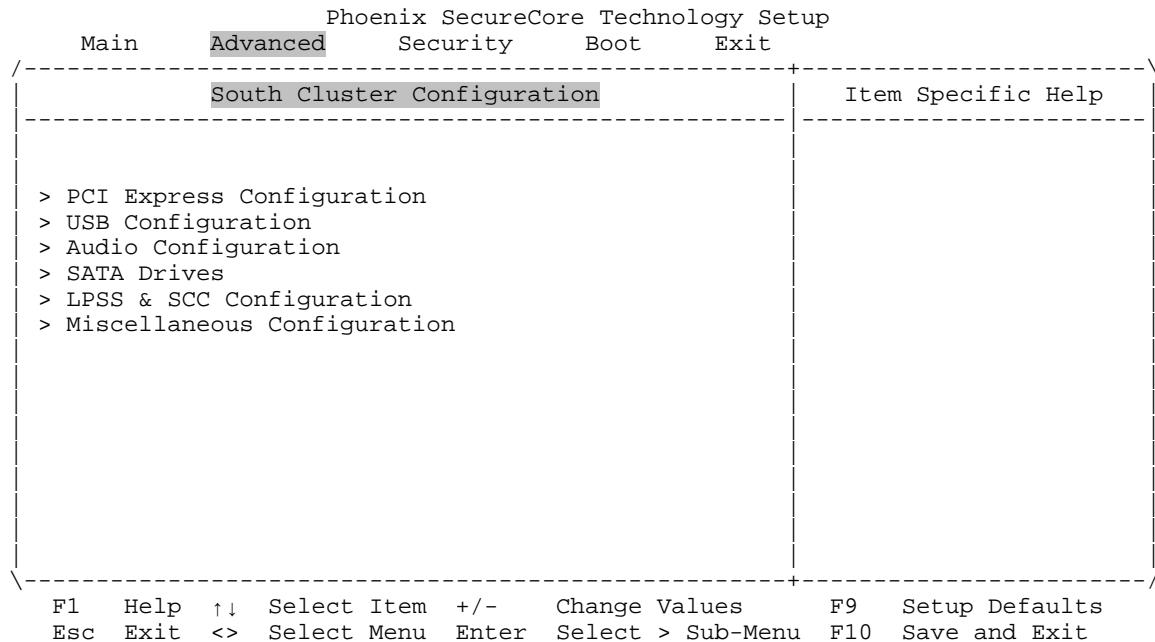
## Advanced → Graphics/Uncore Configuration → Panel Scaling



## Advanced → Graphics/Uncore Configuration → GMCH BLC Control

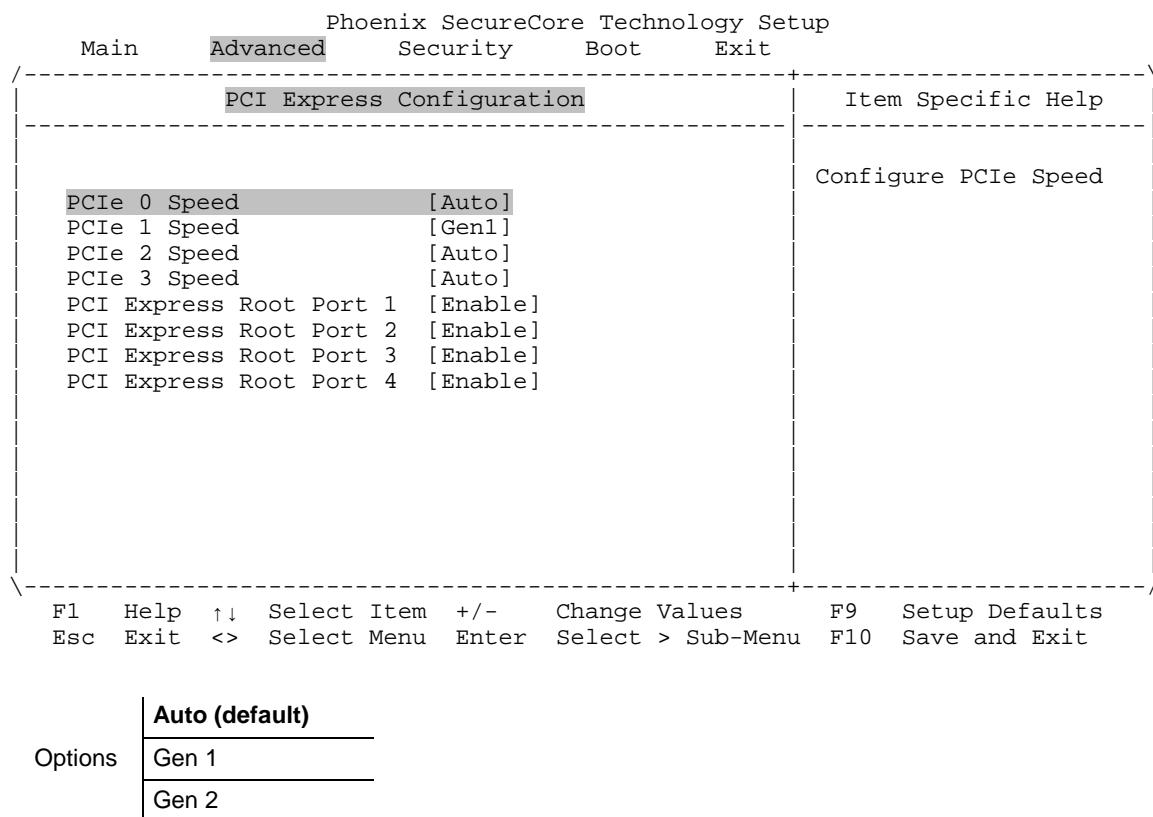


## Advanced → South Cluster Configuration

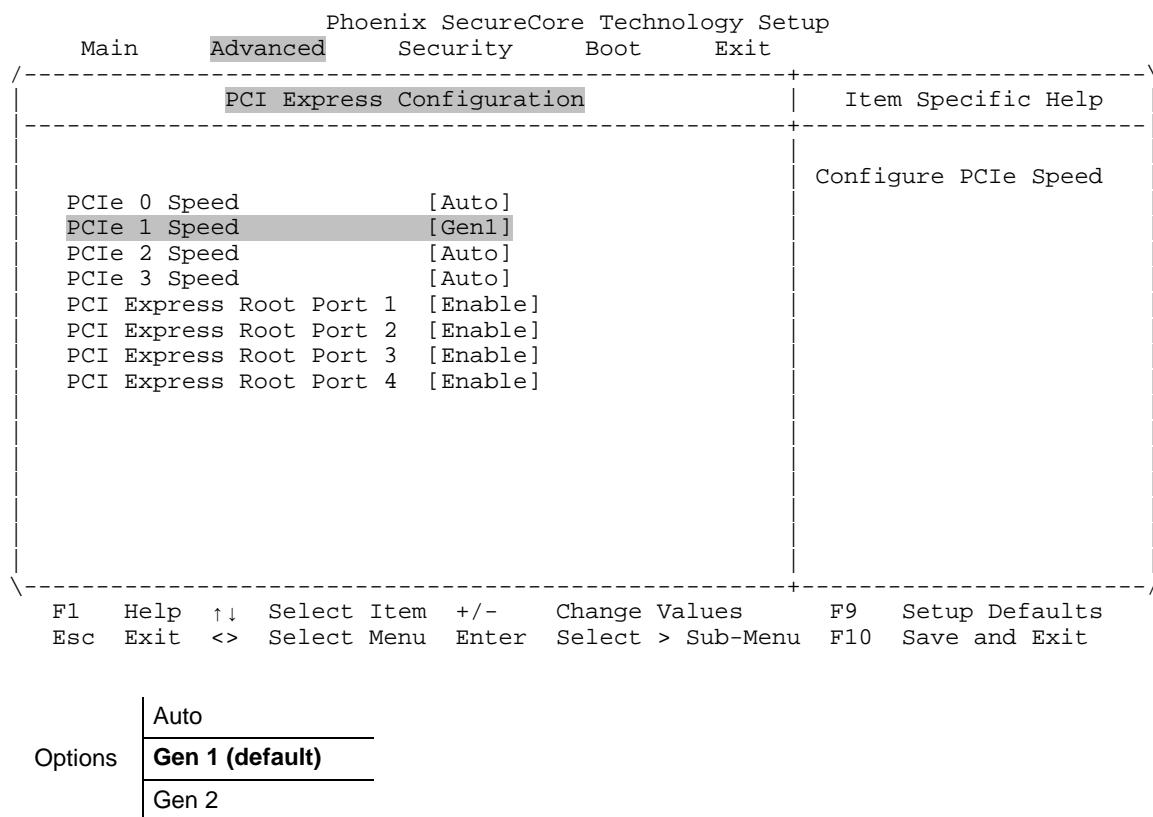


This is the top-level screen for the South Cluster Configuration sub-menu.

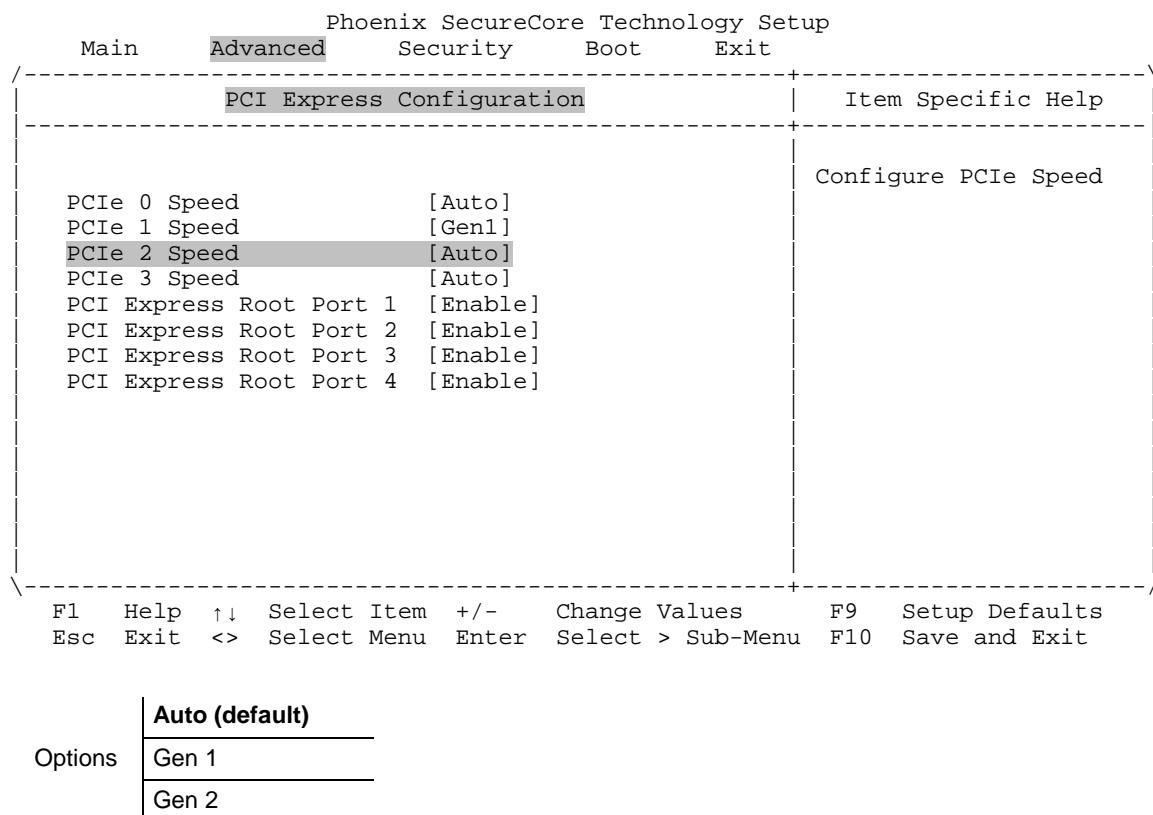
## Advanced → PCI Express Configuration → PCIe o Speed



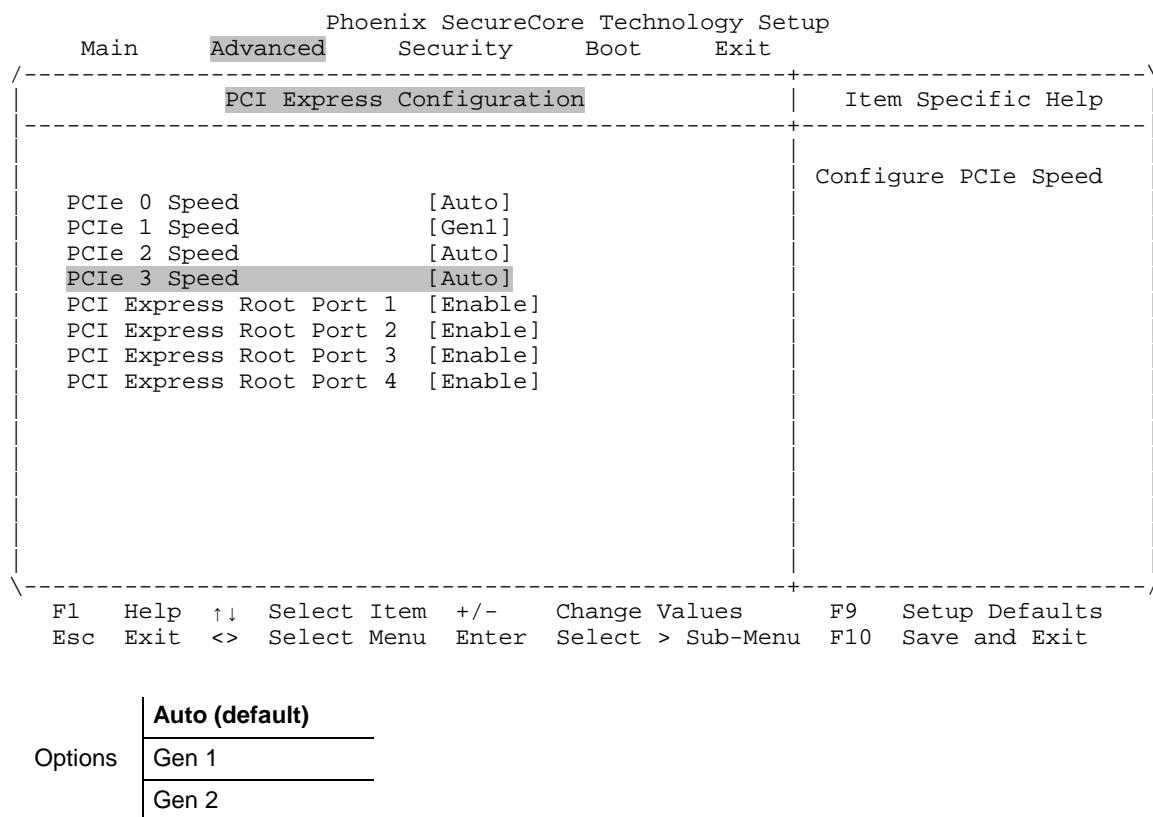
## Advanced → PCI Express Configuration → PCIe 1 Speed



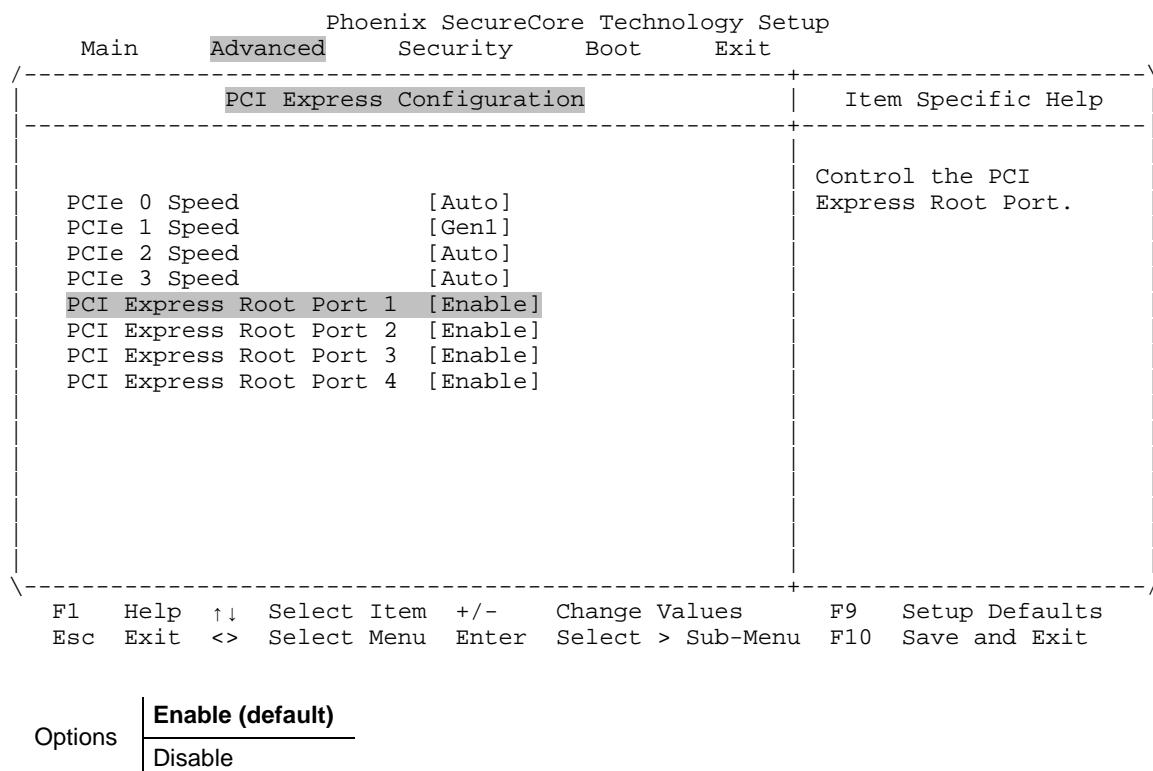
## Advanced → PCI Express Configuration → PCIe 2 Speed



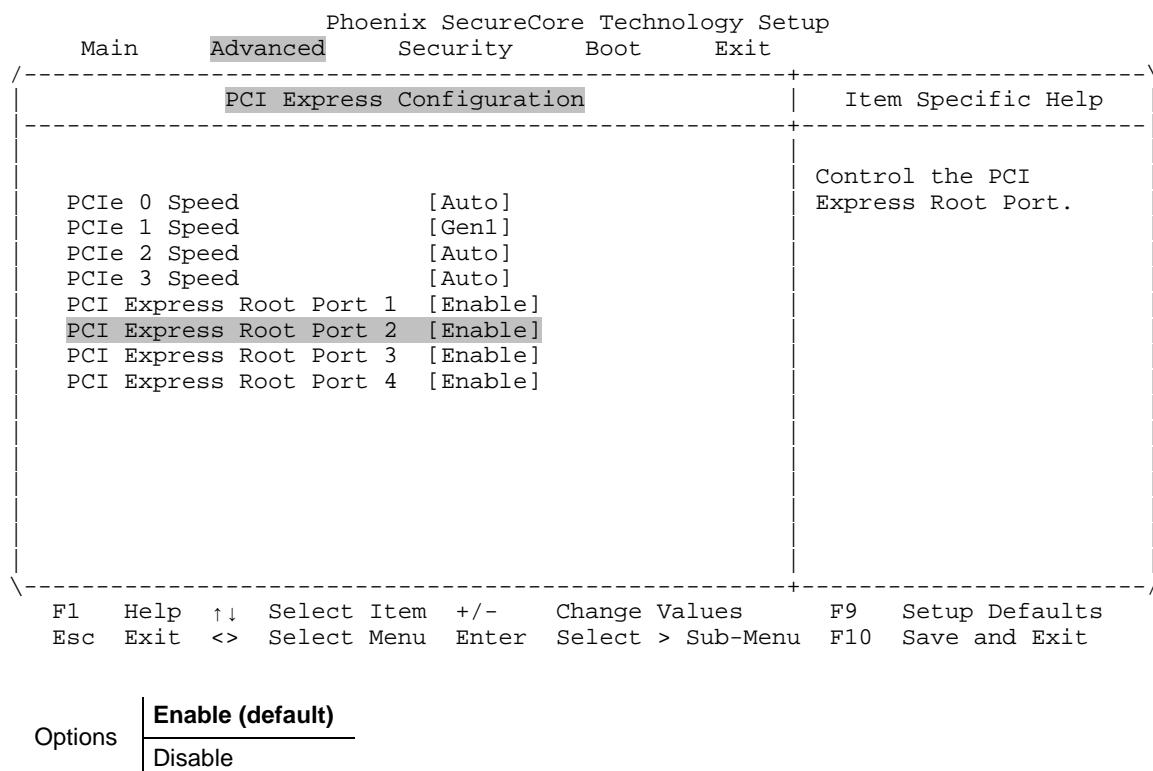
## Advanced → PCI Express Configuration → PCIe 3 Speed

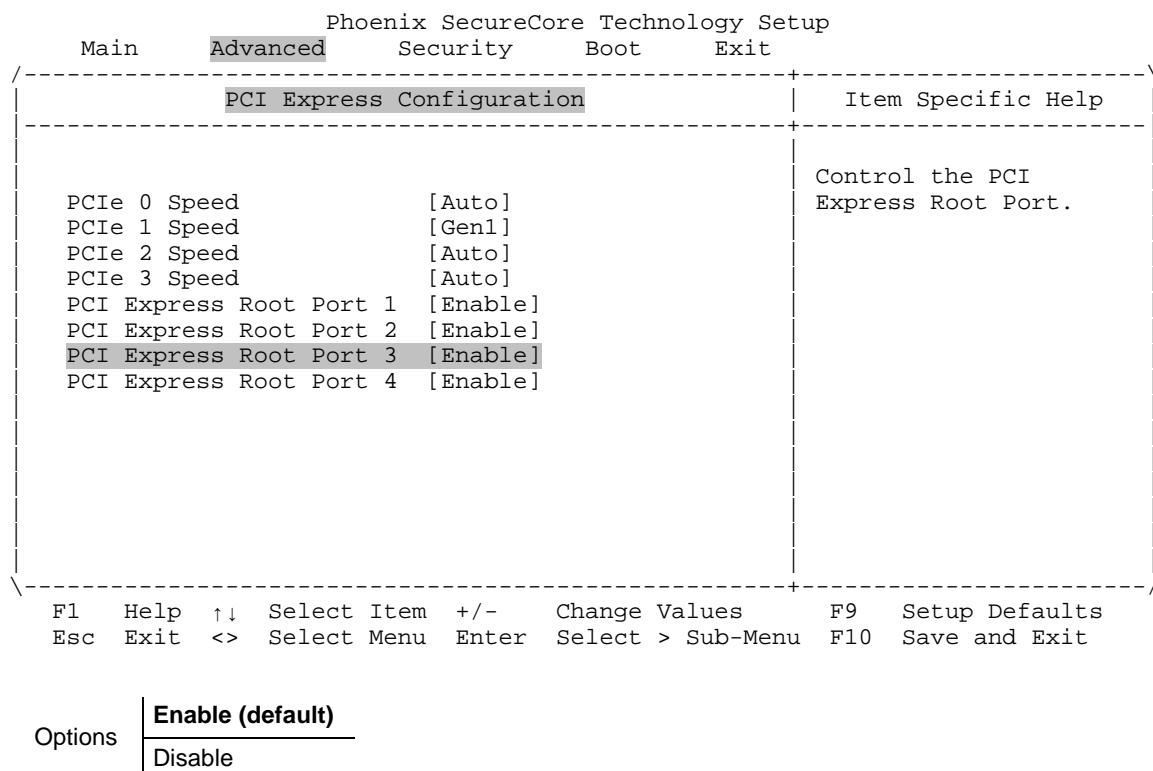


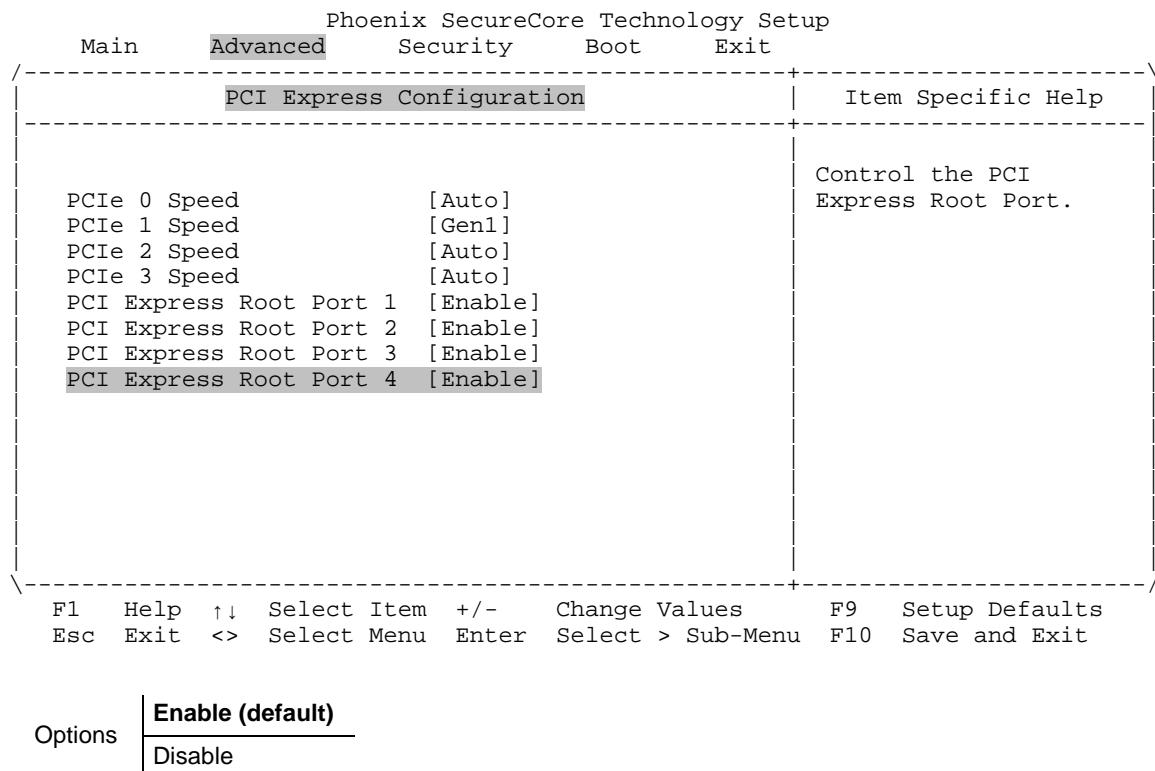
## Advanced → PCI Express Configuration → PCI Express Root Port 1



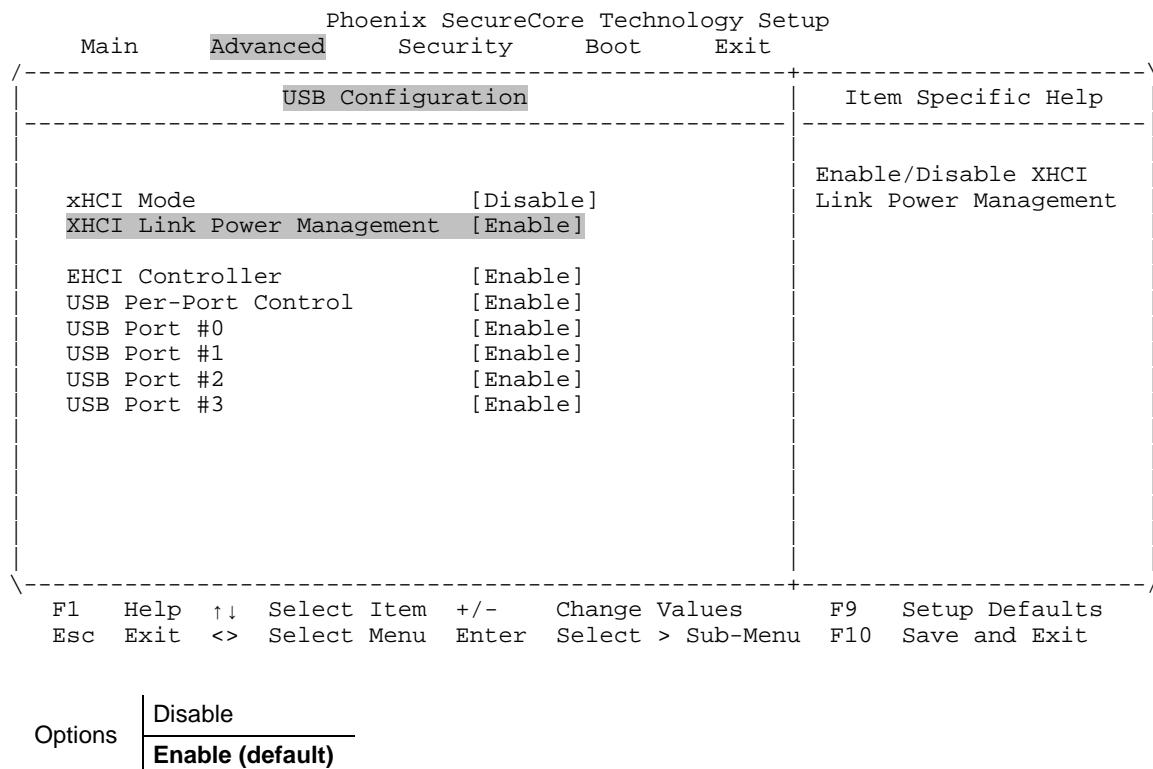
## Advanced → PCI Express Configuration → PCI Express Root Port 2



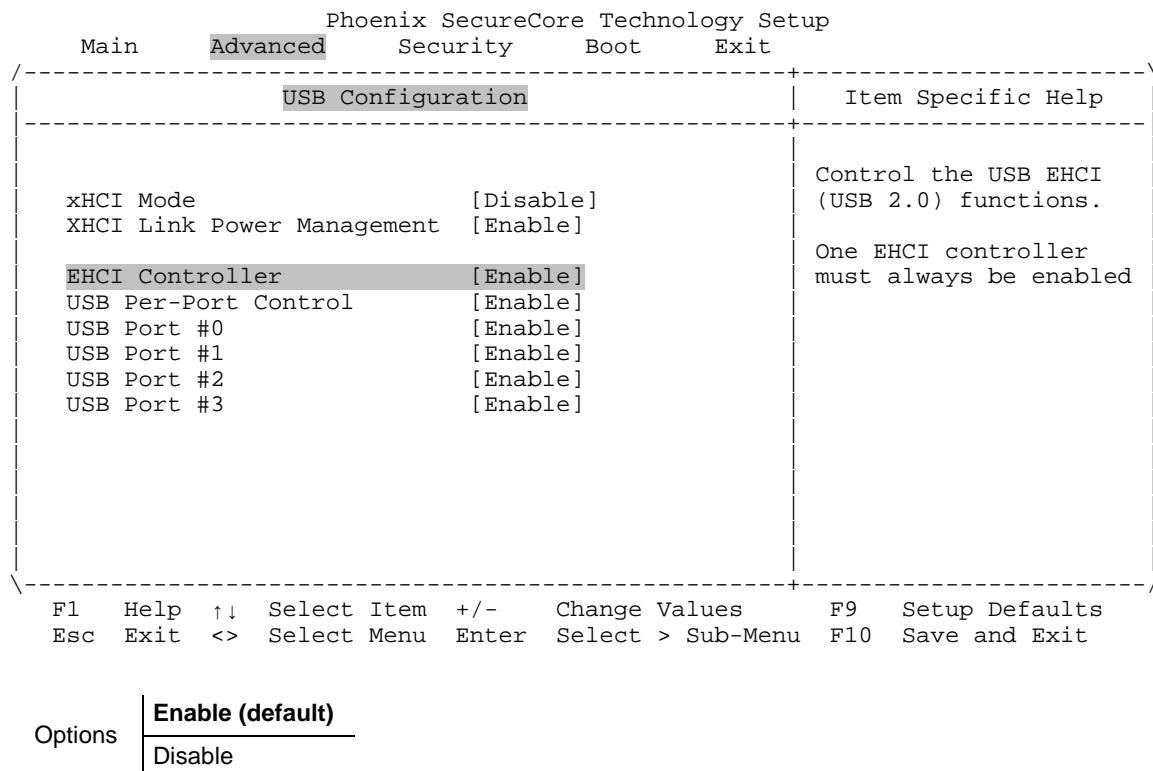
**Advanced → PCI Express Configuration → PCI Express Root Port 3**

**Advanced → PCI Express Configuration → PCI Express Root Port 4**

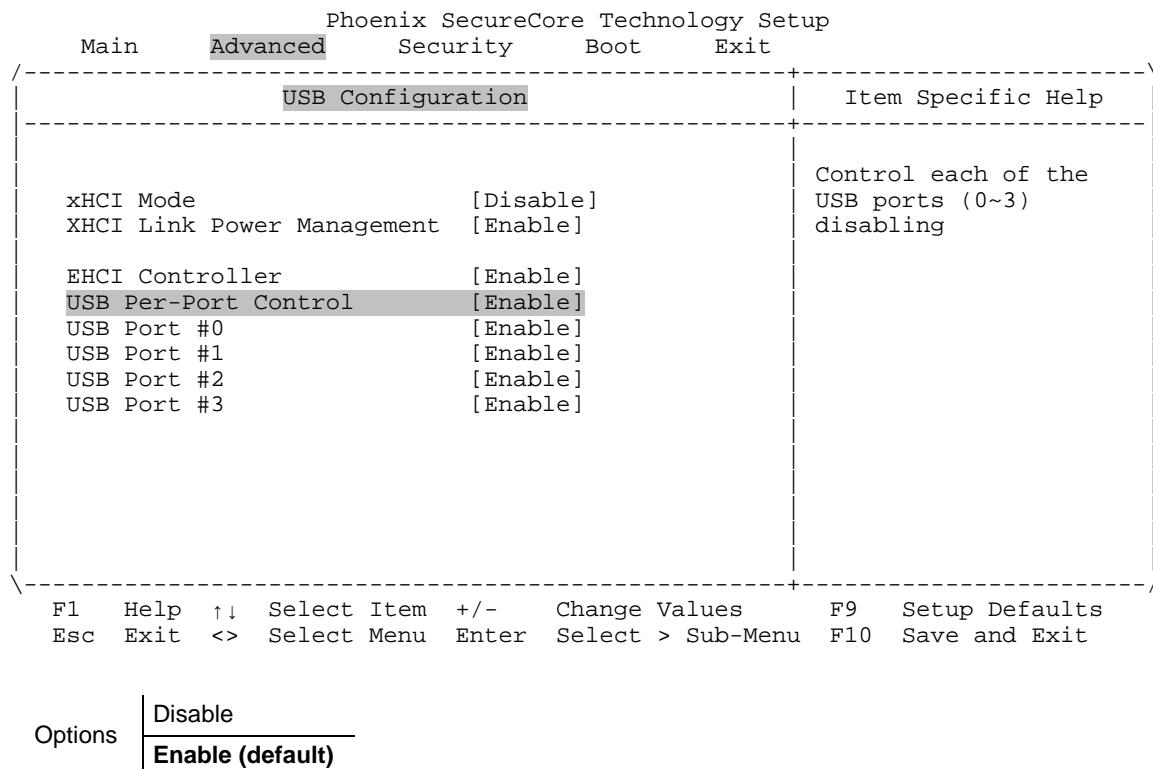
## Advanced → USB Configuration → XHCI Link Power Management



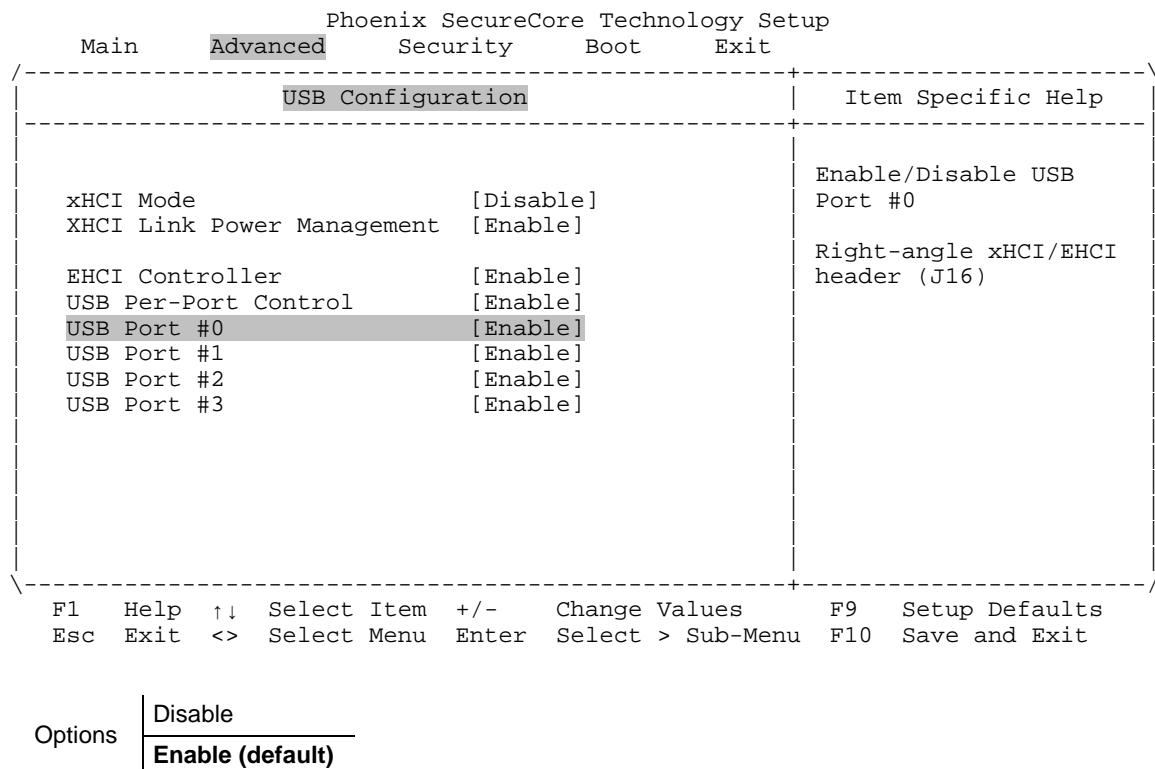
## Advanced → USB Configuration → EHCI Controller



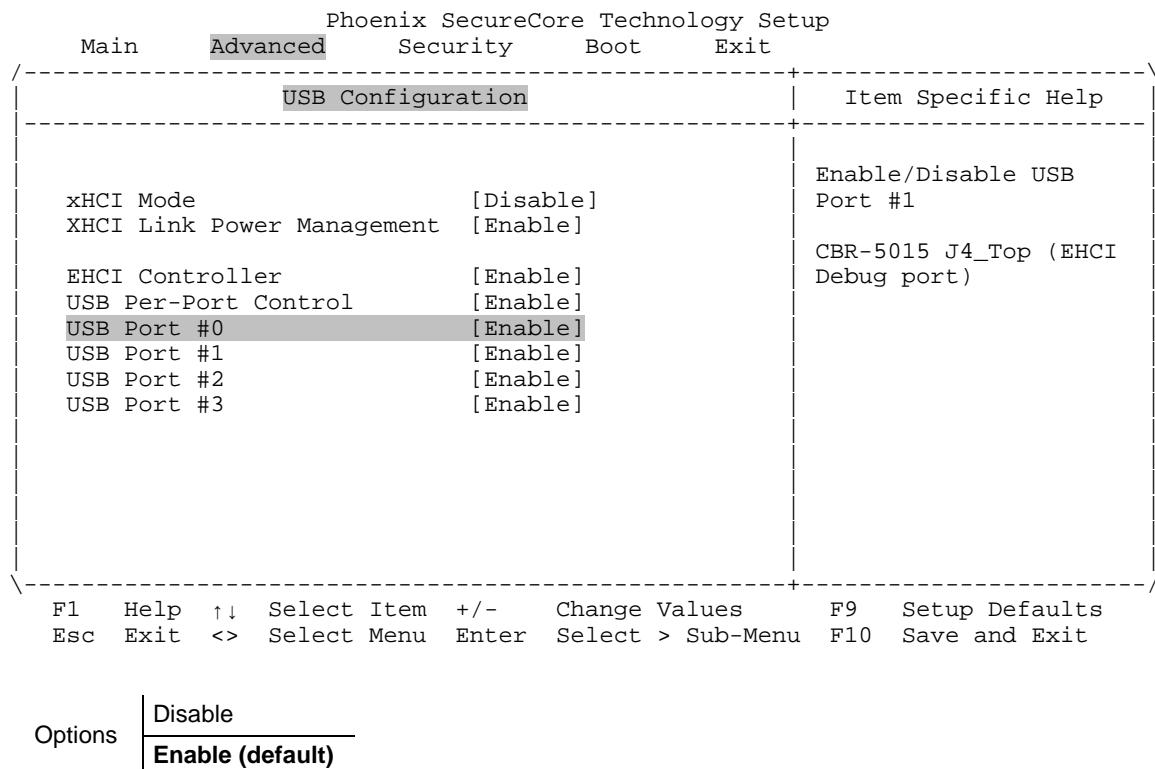
## Advanced → USB Configuration → USB Per-Port Control



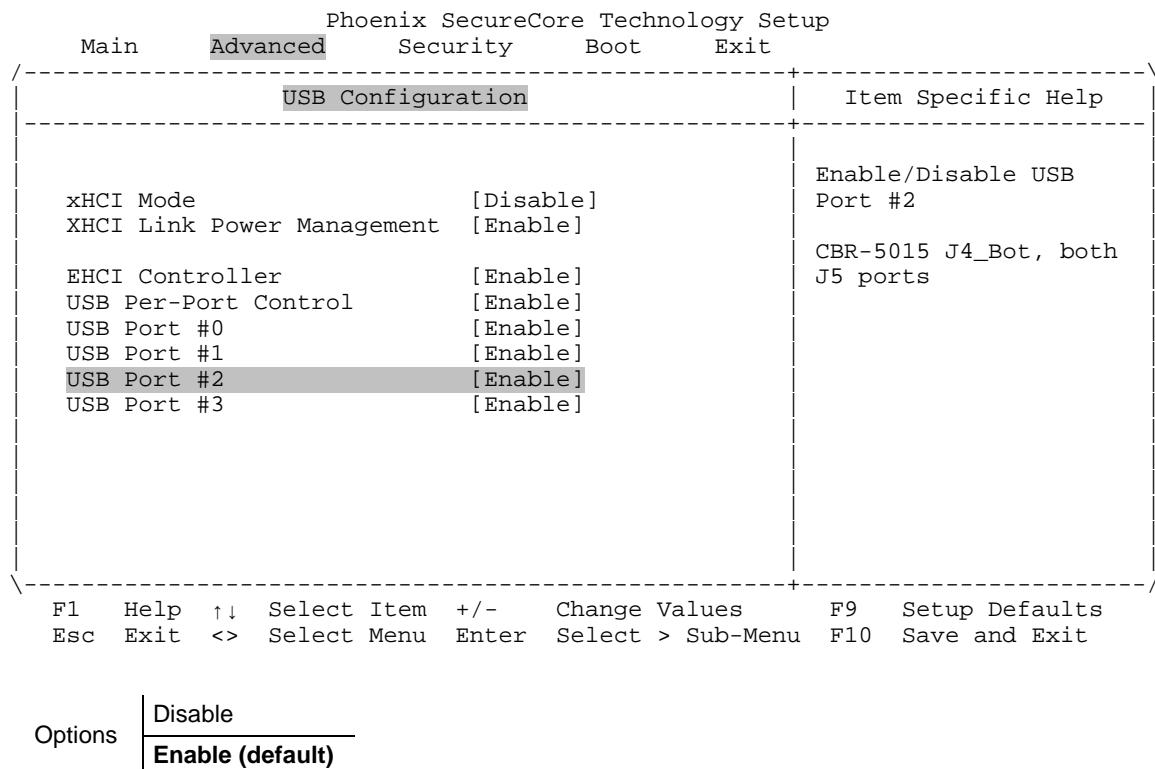
## Advanced → USB Configuration → USB Port #0



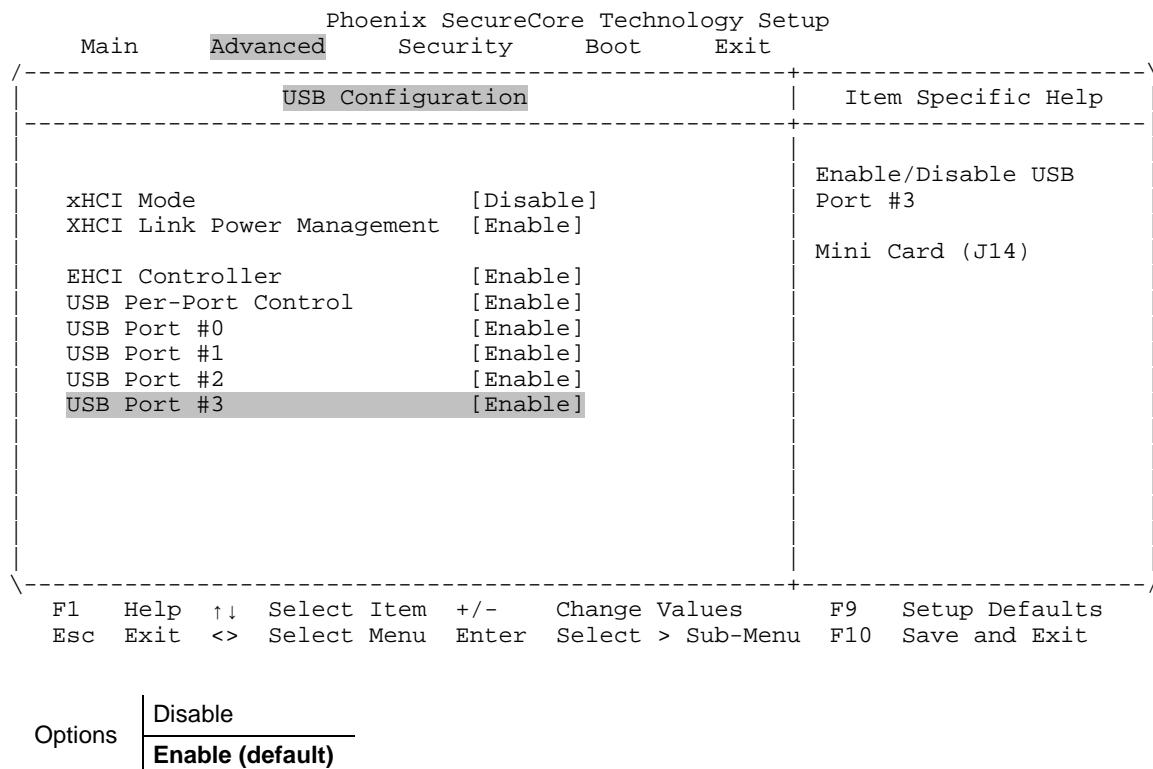
## Advanced → USB Configuration → USB Port #1



## Advanced → USB Configuration → USB Port #2



## Advanced → USB Configuration → USB Port #3



## Advanced → Audio Configuration → Audio Controller

Phoenix SecureCore Technology Setup

Main	Advanced	Security	Boot	Exit
------	----------	----------	------	------

---

<p style="text-align: center;"><b>Audio Configuration</b></p>	Item Specific Help
---	--------------------

---

<p><b>Audio Controller</b> [Disable]</p>	<p>Enable or disable the Azalia (HD Audio) device.</p> <p>Disabled = Azalia will be disabled</p> <p>Enabled = Azalia will be enabled</p>
--	--

---

F1    Help $\uparrow\downarrow$ Select Item    +/-	Change Values	F9    Setup Defaults
Esc    Exit    <>    Select Menu    Enter	Select Menu    Enter    Select > Sub-Menu	F10    Save and Exit

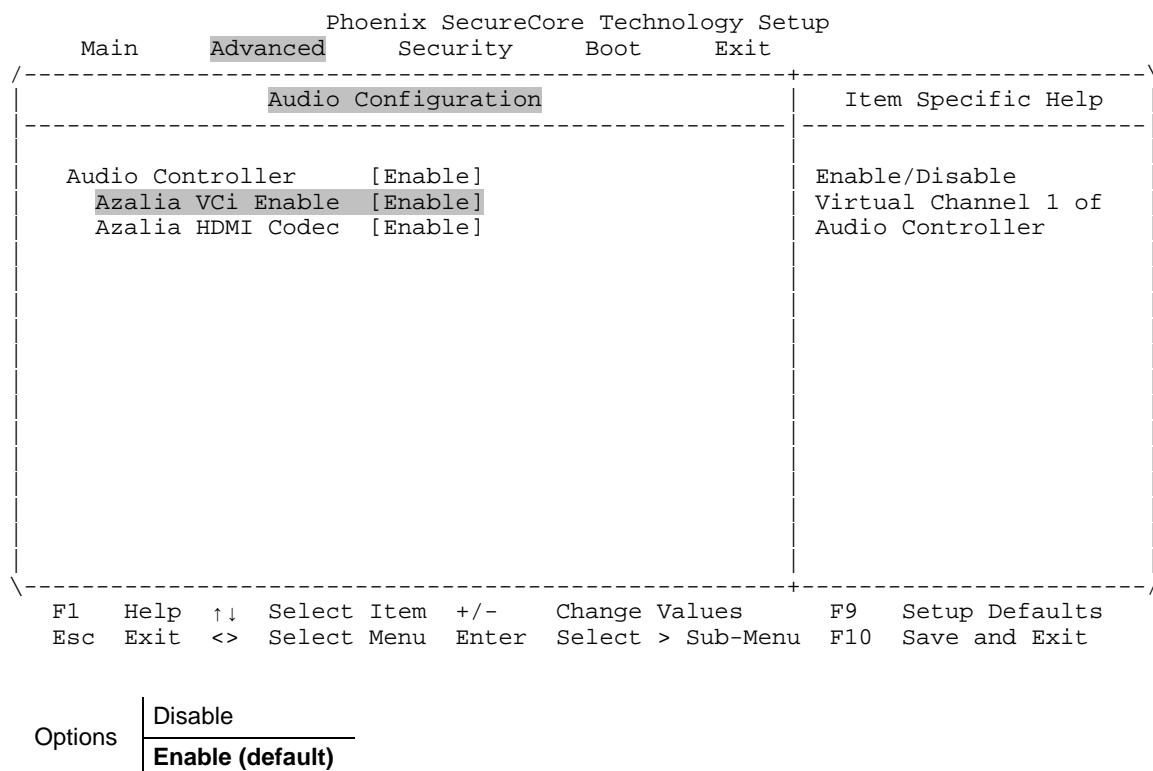
  

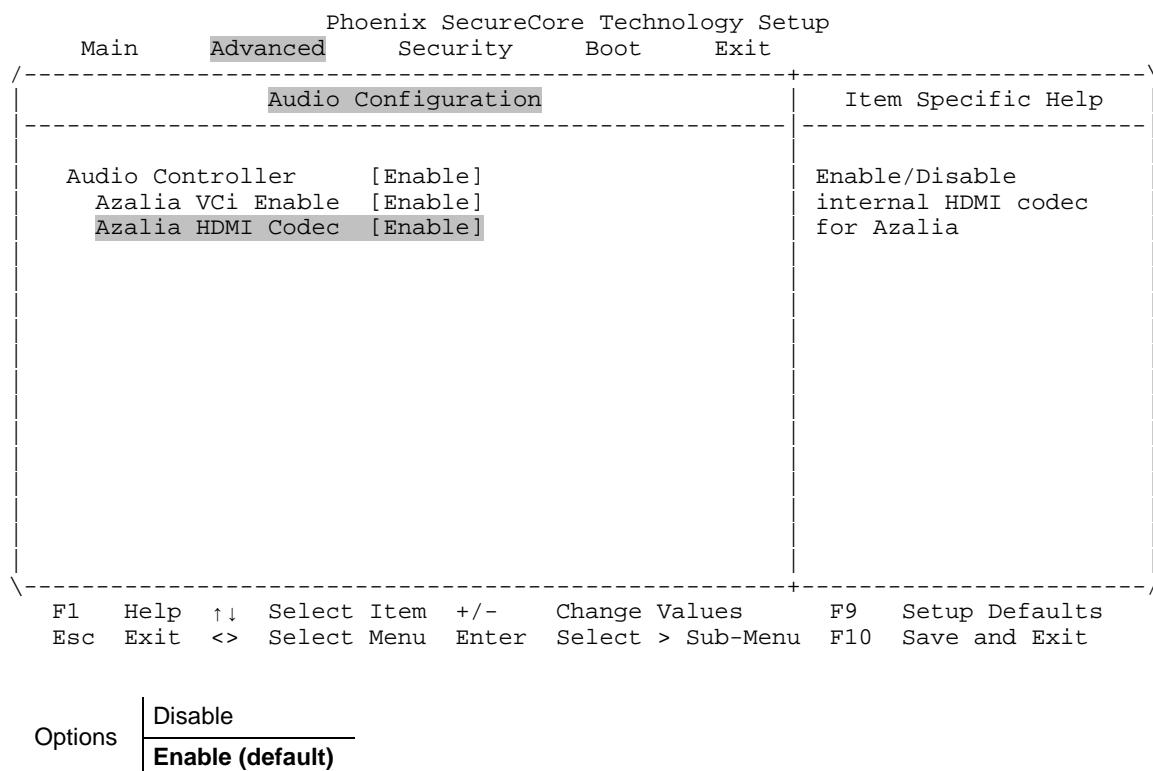
Options	<b>Disable (default)</b> Disable “Azalia” (high-definition) audio
	<input type="button" value="Enable"/> Enable “Azalia” (high-definition) audio



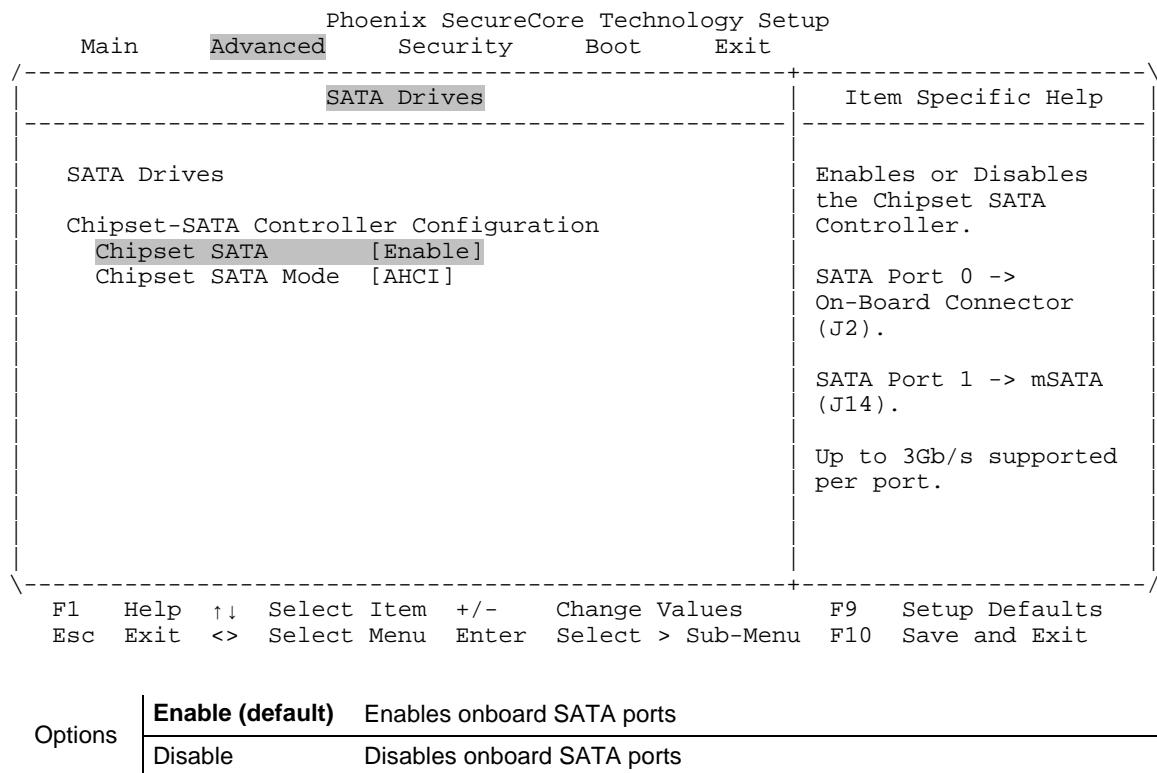
**Note:** The default setting for this menu item is Disable. When the audio controller is enabled, two additional options will be available:

- Azalia VCI Enable (see page 88)
- Azalia HDMI Codec (see page 89)

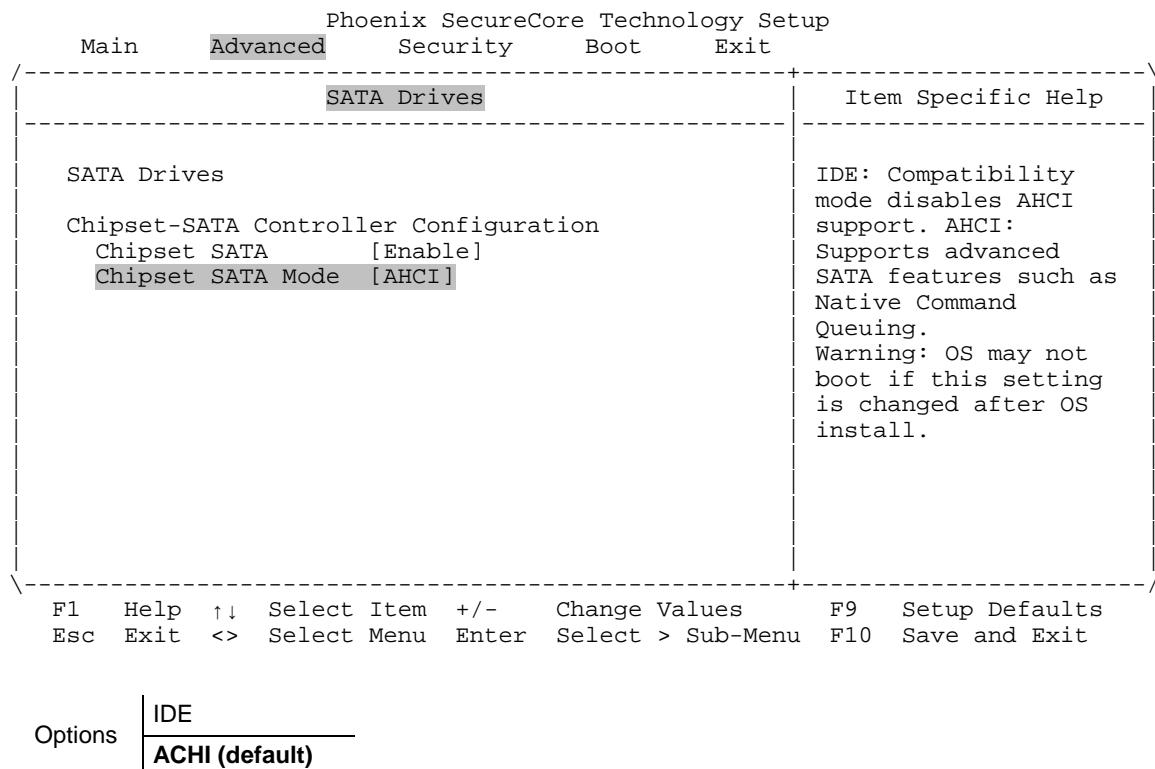
**Advanced → Audio Configuration → Azalia VCi Enable**

**Advanced → Audio Configuration → Azalia HDMI CODEC**

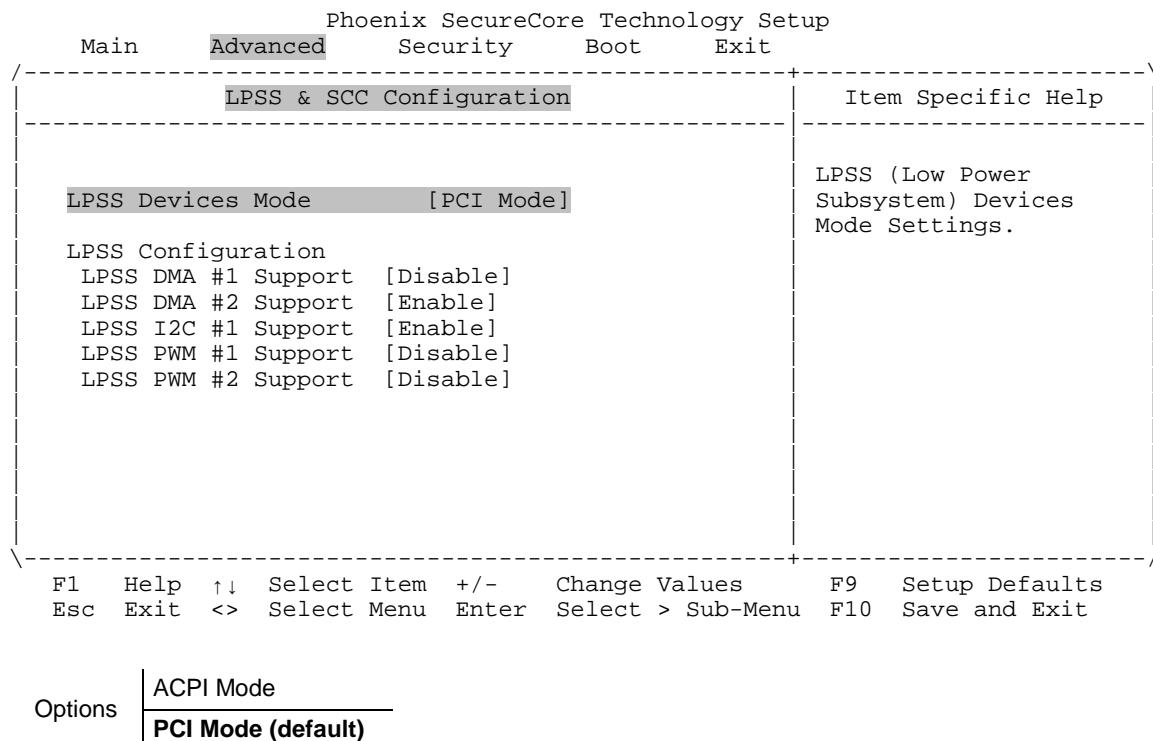
## Advanced → SATA Drives → Chipset SATA



## Advanced → SATA Drives → Chipset SATA Mode



## Advanced → LPSS & SCC Configuration → LPSS Devices Mode



## Advanced → LPSS & SCC Configuration → LPSS DMA #1 Support

Phoenix SecureCore Technology Setup

Main	<b>Advanced</b>	Security	Boot	Exit
------	-----------------	----------	------	------

---

LPSS & SCC Configuration	Item Specific Help
--------------------------	--------------------

---

LPSS Devices Mode [PCI Mode]	LPSS DMA #1 Support Enable\Disable
------------------------------	---------------------------------------

---

LPSS Configuration	
--------------------	--

LPSS DMA #1 Support [Disable]	
-------------------------------	--

LPSS DMA #2 Support [Enable]	
------------------------------	--

LPSS I2C #1 Support [Enable]	
------------------------------	--

LPSS PWM #1 Support [Disable]	
-------------------------------	--

LPSS PWM #2 Support [Disable]	
-------------------------------	--

---

F1 Help ↑↓ Select Item +/− Change Values F9 Setup Defaults	F10 Save and Exit
--	-------------------

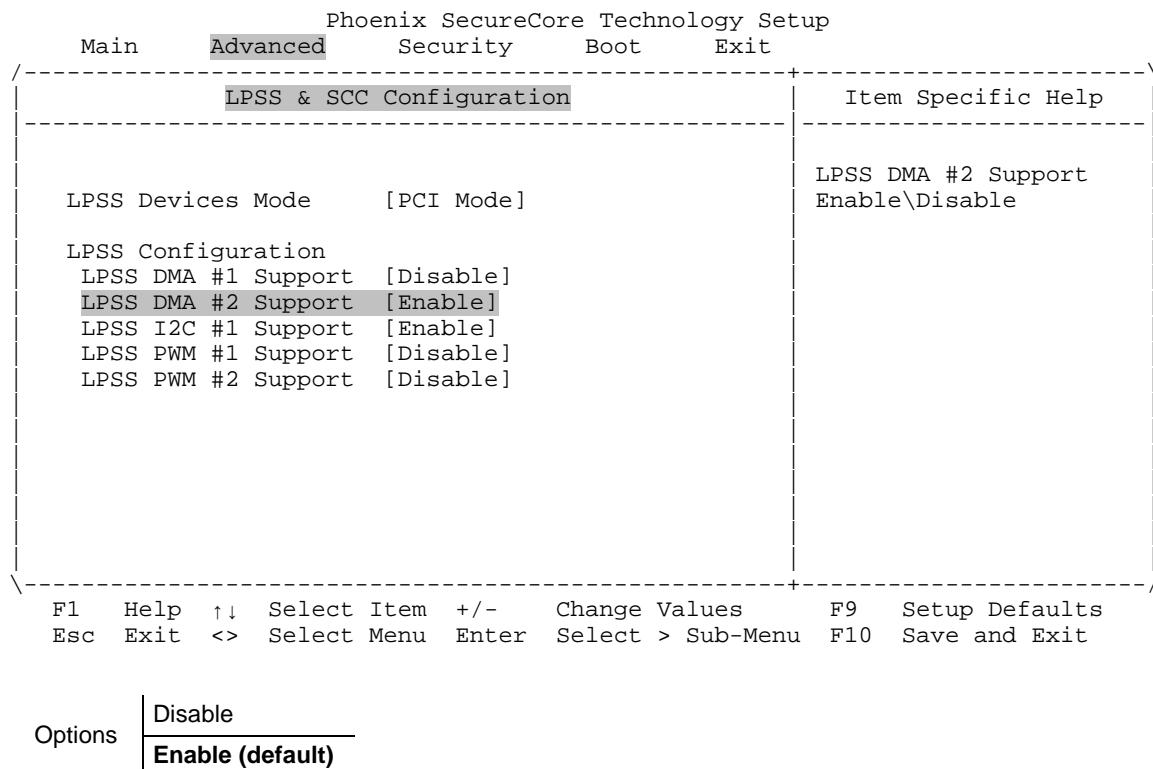
Esc Exit <> Select Menu Enter Select > Sub-Menu	
---	--

Options	<div style="border-bottom: 1px solid black; padding-bottom: 5px; margin-bottom: 5px;">Disable (default)</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px; margin-bottom: 5px;">Enable</div>
---------	--

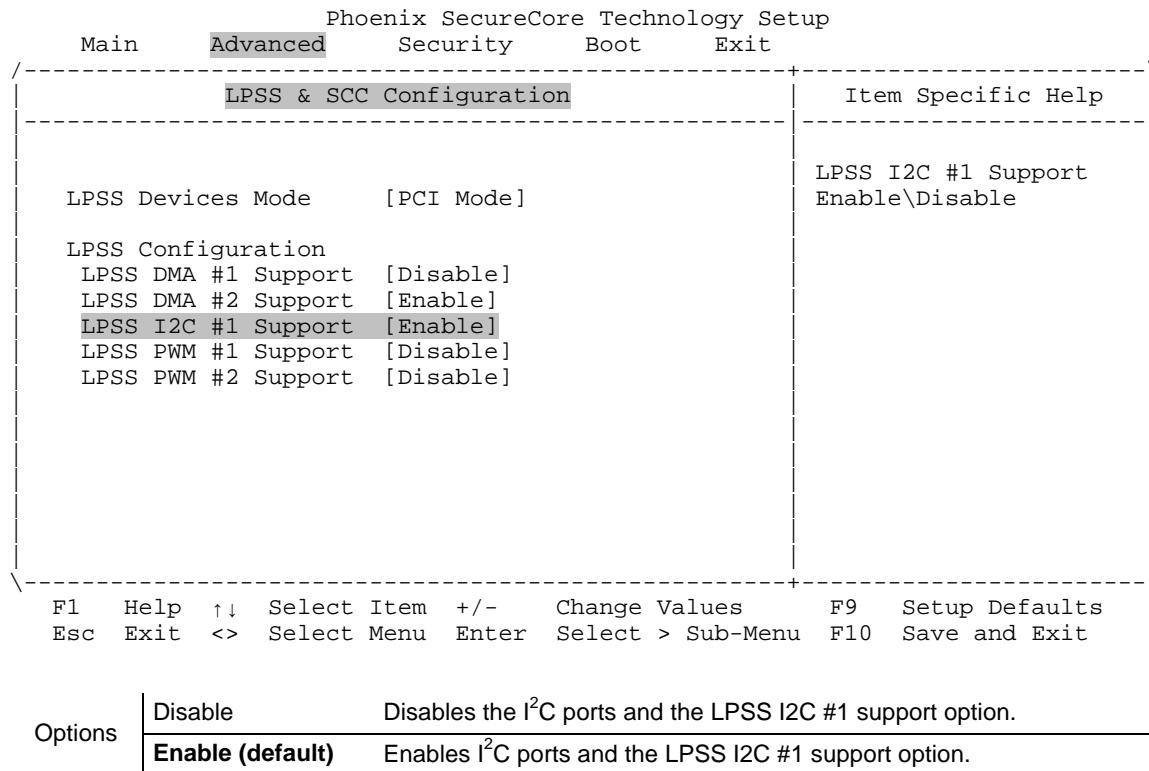


**Note:** The default setting for this menu item is Disable. In this mode, the following menu items are not accessible:

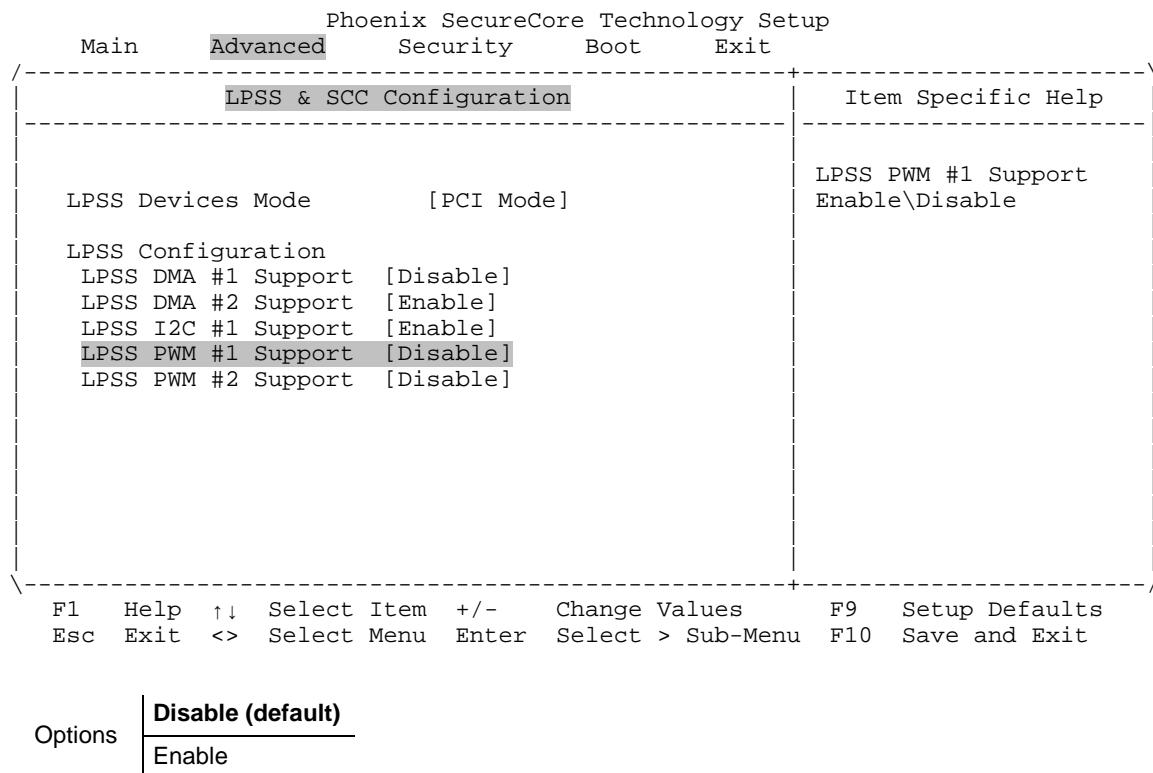
- LPSS PWM #1 Support
- LPSS PWM #2 Support

**Advanced → LPSS & SCC Configuration → LPSS DMA #2 Support**

## Advanced → LPSS & SCC Configuration → LPSS I<sup>2</sup>C #1 Support

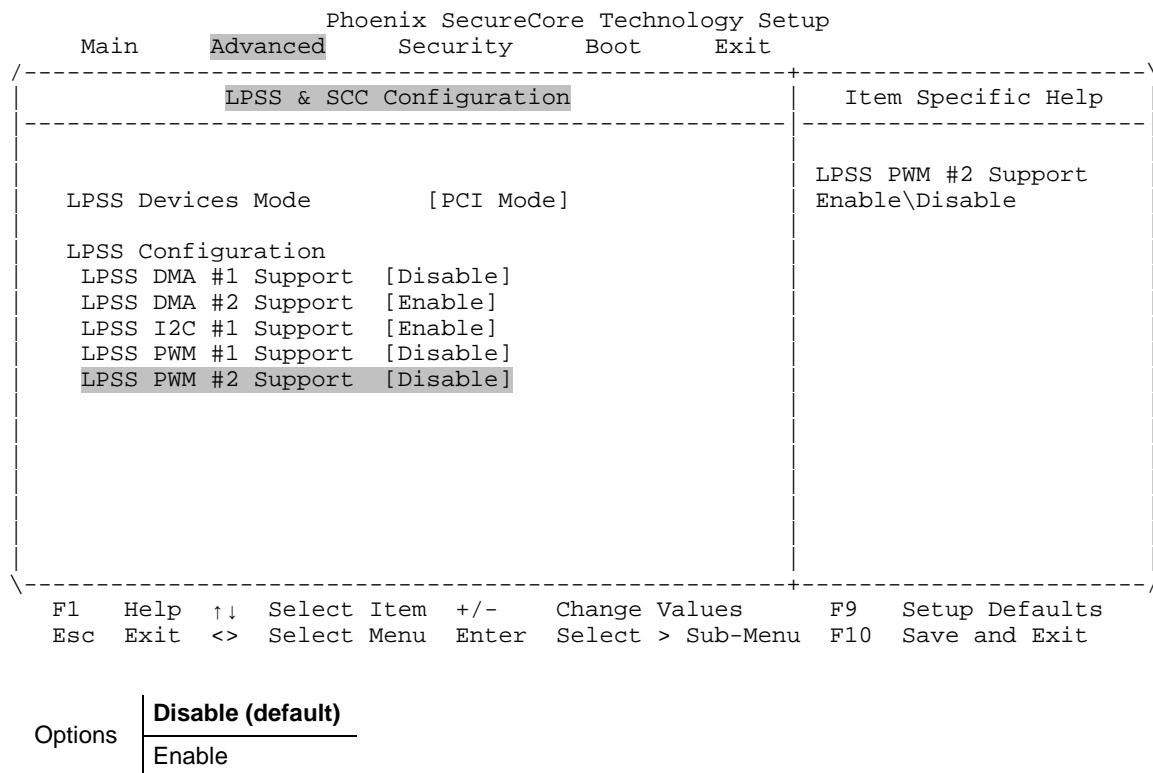


## Advanced → LPSS & SCC Configuration → LPSS PWM #1 Support

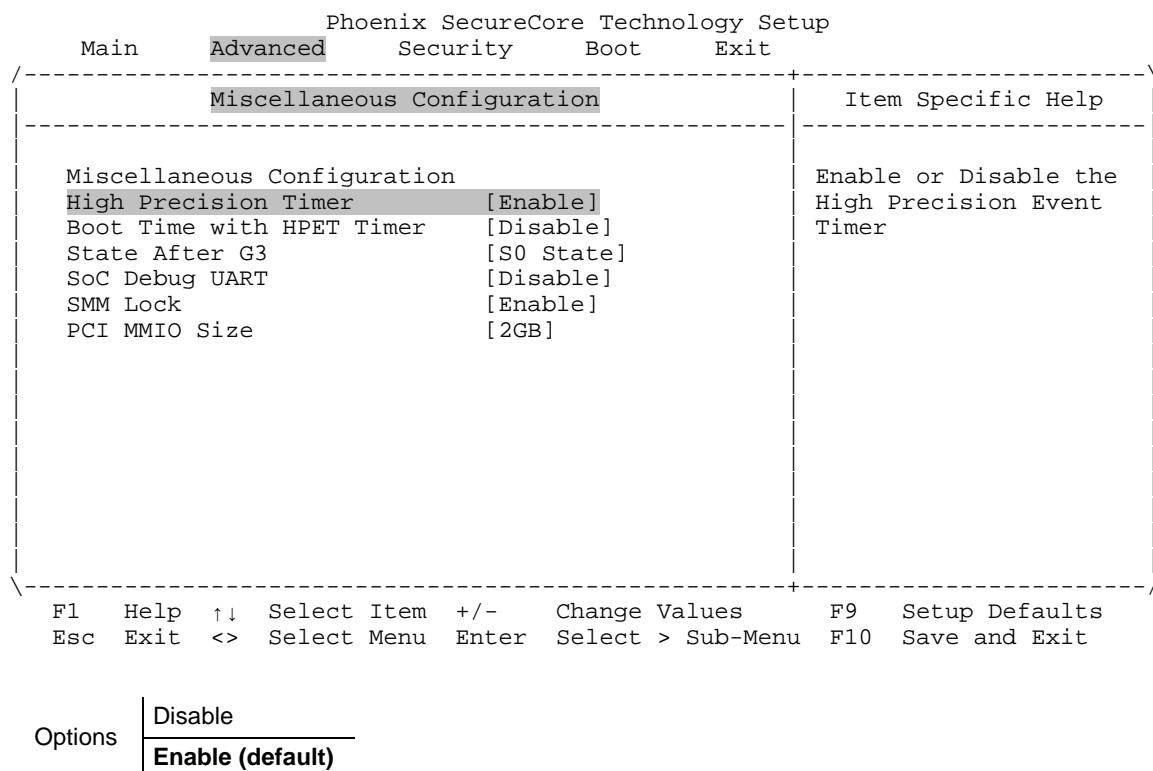


**Note:** This option is accessible only when LPSS DMA #1 is enabled. (See page 93.)

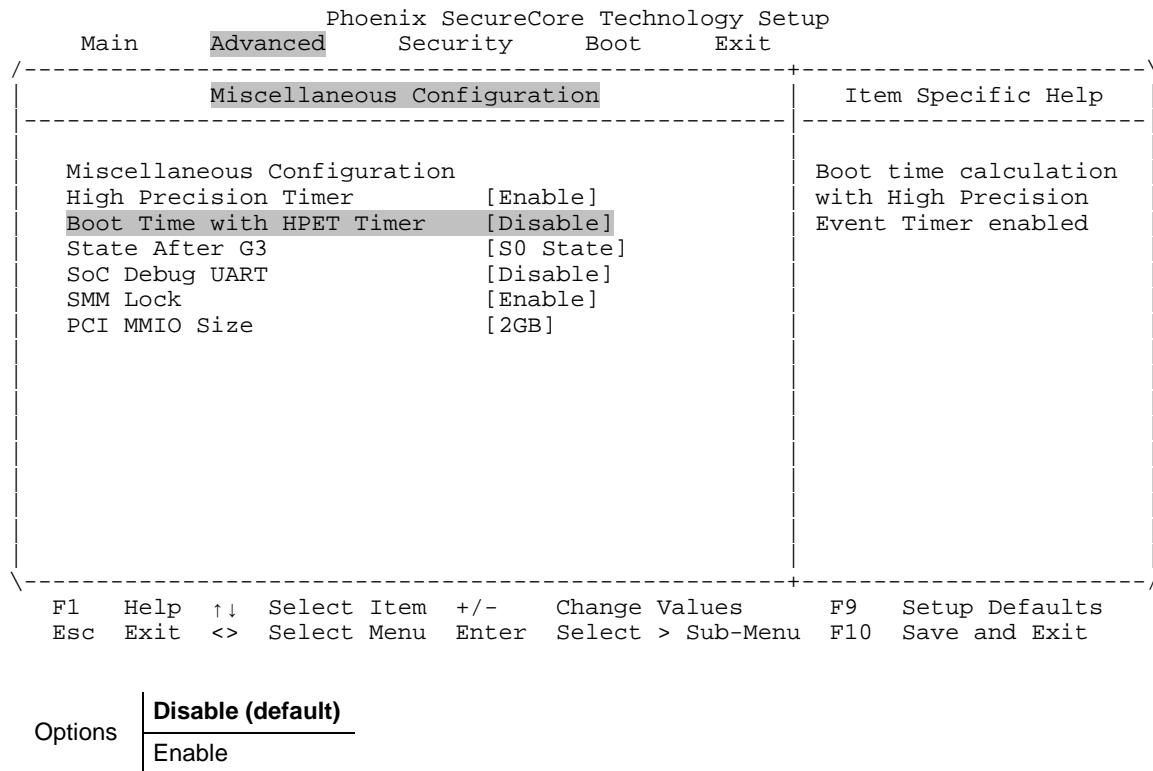
## Advanced → LPSS & SCC Configuration → LPSS PWM #2 Support



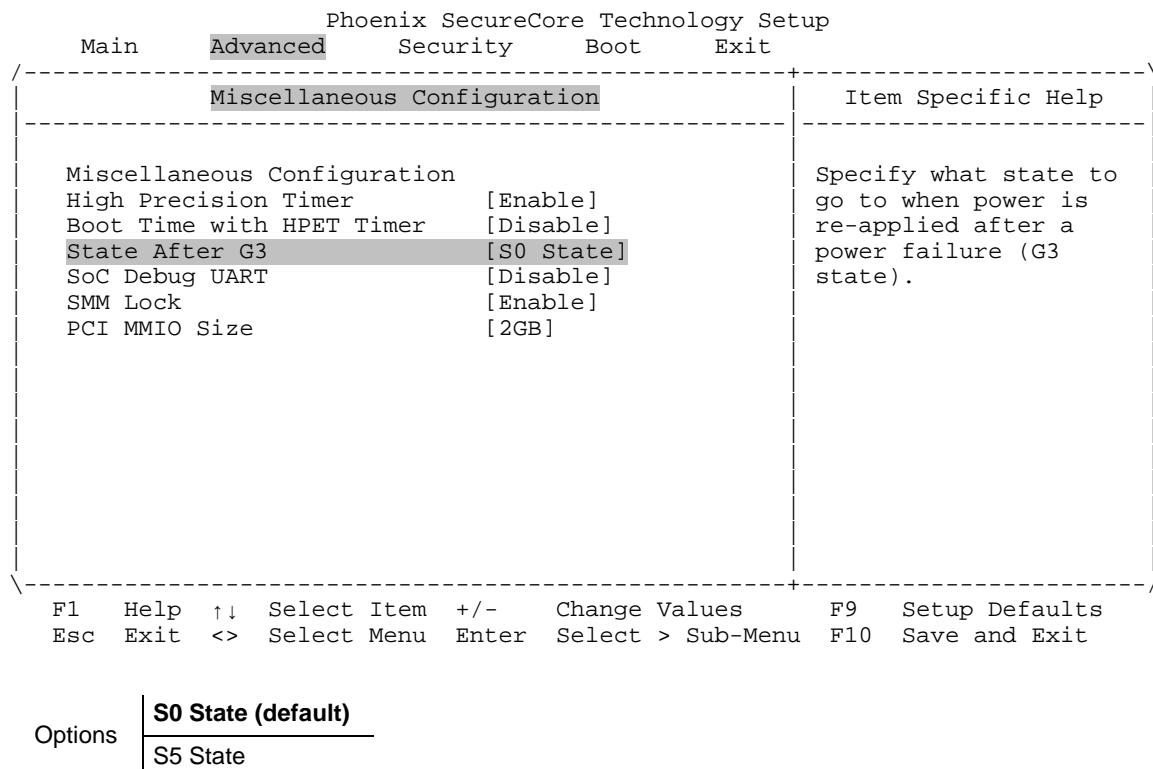
**Note:** This option is accessible only when LPSS DMA #1 is enabled. (See page 93.)

**Advanced → Miscellaneous Configuration → High Precision Timer**

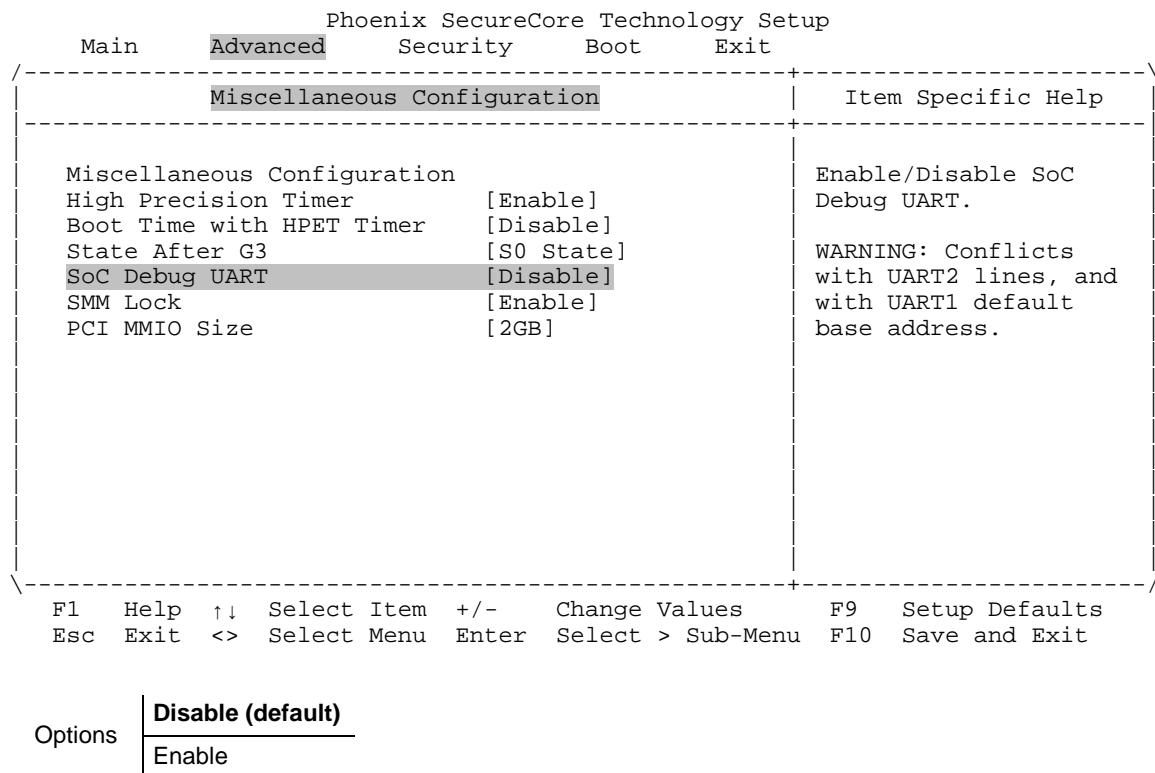
## Advanced → Miscellaneous Configuration → Boot Time with HPET Timer



## Advanced → Miscellaneous Configuration → State After G3



## Advanced → Miscellaneous Configuration → SoC Debug UART



## Advanced → Miscellaneous Configuration → SMM Lock

Phoenix SecureCore Technology Setup

Main	Advanced	Security	Boot	Exit
------	----------	----------	------	------

---

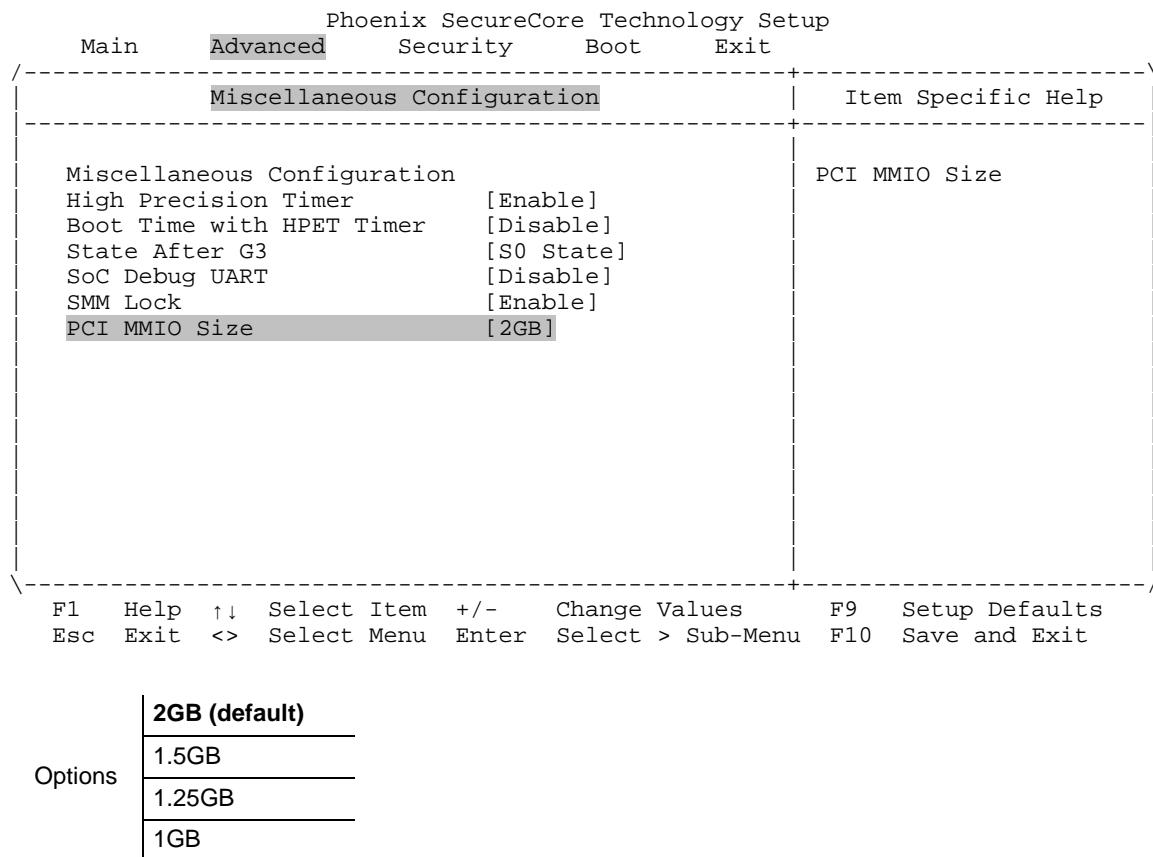
<b>Miscellaneous Configuration</b> <ul style="list-style-type: none"> <li>High Precision Timer [Enable]</li> <li>Boot Time with HPET Timer [Disable]</li> <li>State After G3 [S0 State]</li> <li>SoC Debug UART [Disable]</li> <li><b>SMM Lock</b> [Enable] <span style="float: right;">(Selected)</span></li> <li>PCI MMIO Size [2GB]</li> </ul>	Item Specific Help
---	--------------------

---

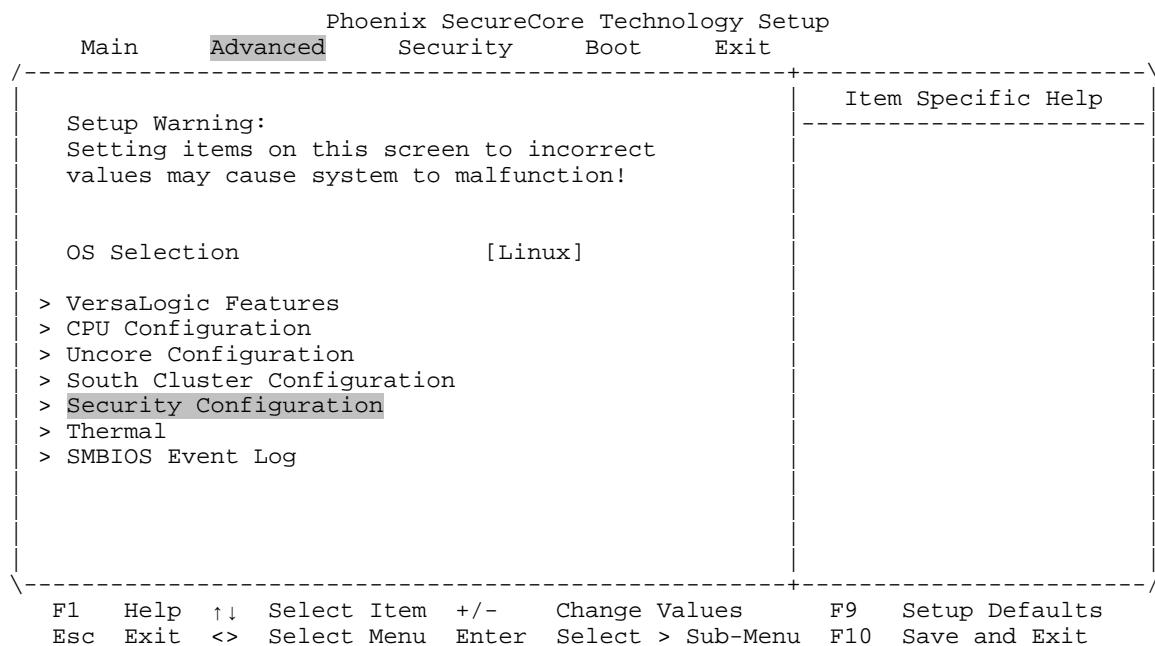
F1    Help $\uparrow\downarrow$ Select Item    +/-	Change Values	F9    Setup Defaults
Esc    Exit    <>	Select Menu    Enter    Select > Sub-Menu	F10    Save and Exit

Options	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Disable</td> <td>Allows additional SMM (System Management Mode) drivers to be loaded</td> </tr> <tr> <td><b>Enable (default)</b></td> <td>Prevents additional SMM (System Management Mode) drivers from being loaded</td> </tr> </table>	Disable	Allows additional SMM (System Management Mode) drivers to be loaded	<b>Enable (default)</b>	Prevents additional SMM (System Management Mode) drivers from being loaded
Disable	Allows additional SMM (System Management Mode) drivers to be loaded				
<b>Enable (default)</b>	Prevents additional SMM (System Management Mode) drivers from being loaded				

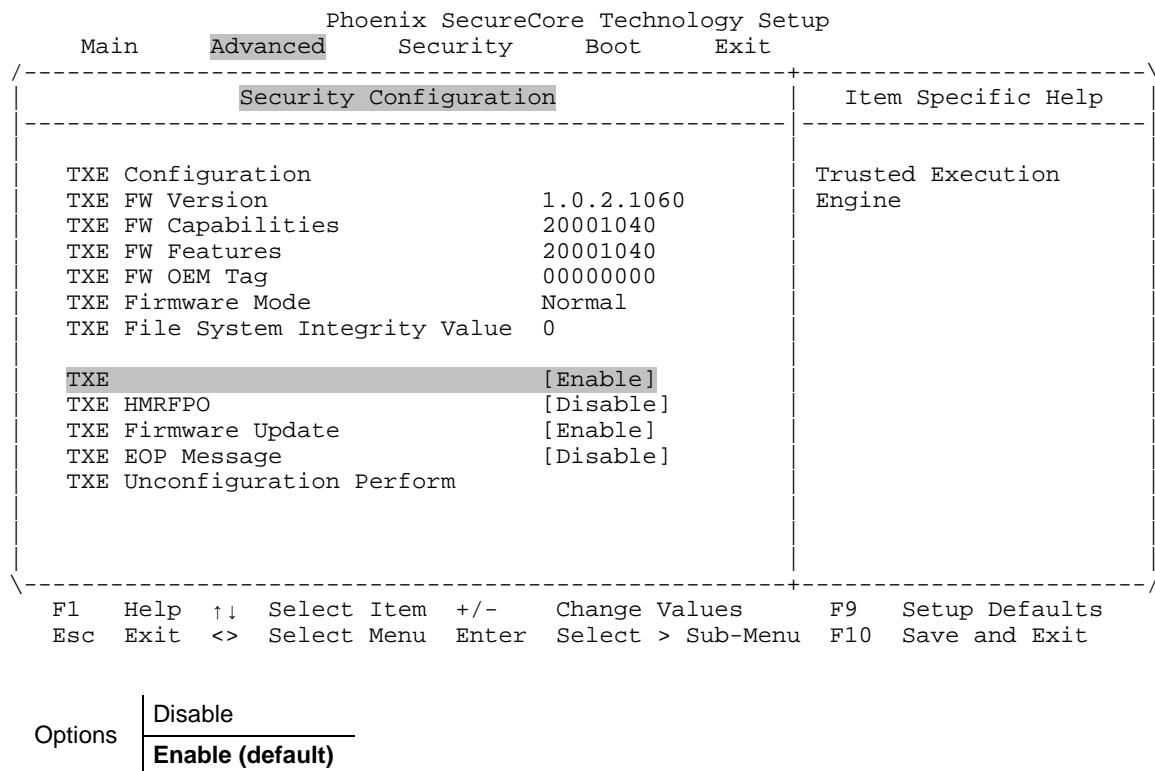
**Advanced → Miscellaneous Configuration → PCI MMIO Size**

## Advanced → Security



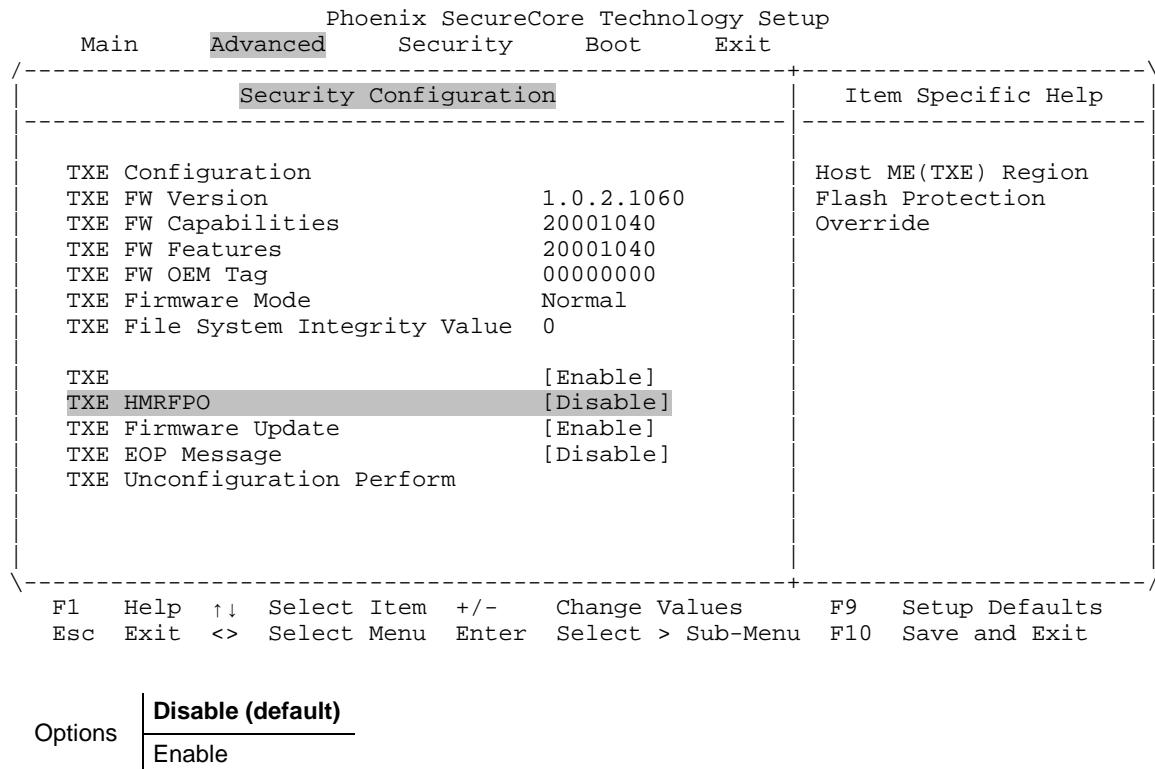
This is the top-level screen for the Security sub-menu.

## Advanced → Security Configuration → TXE



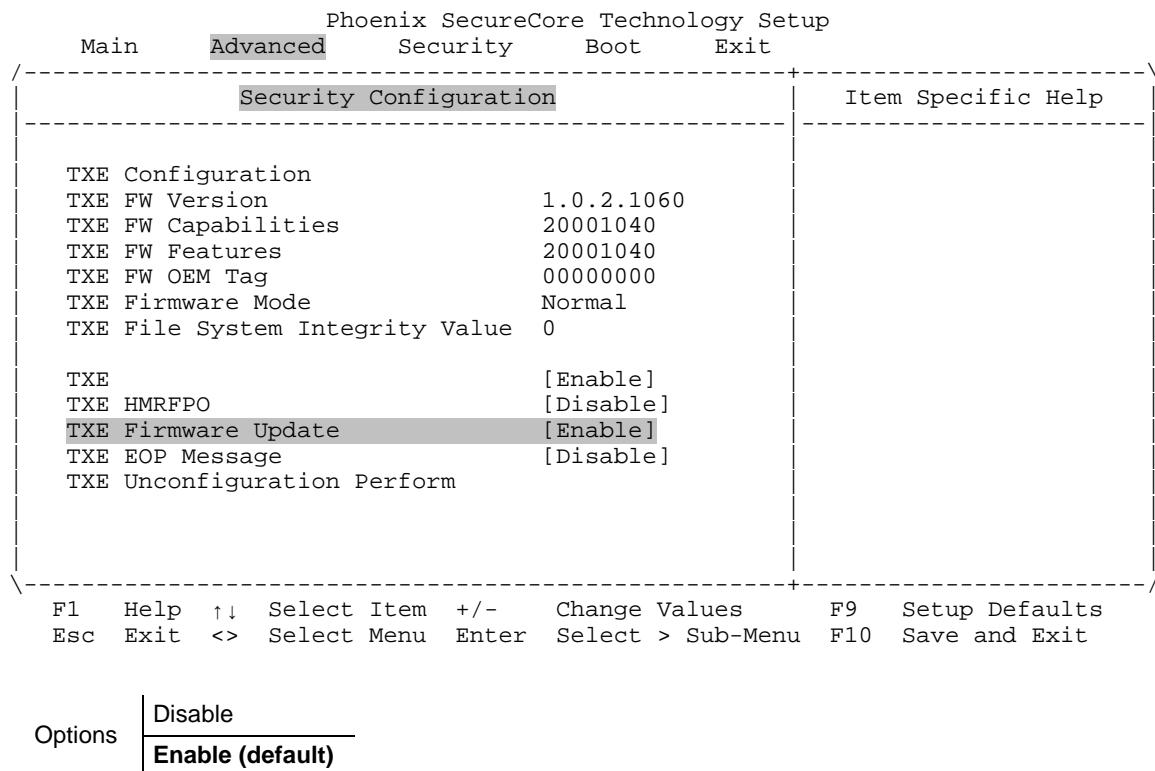
This screen also provides status on the Trusted Execution Engine (TXE).

## Advanced → Security Configuration → TXE HMRFPO



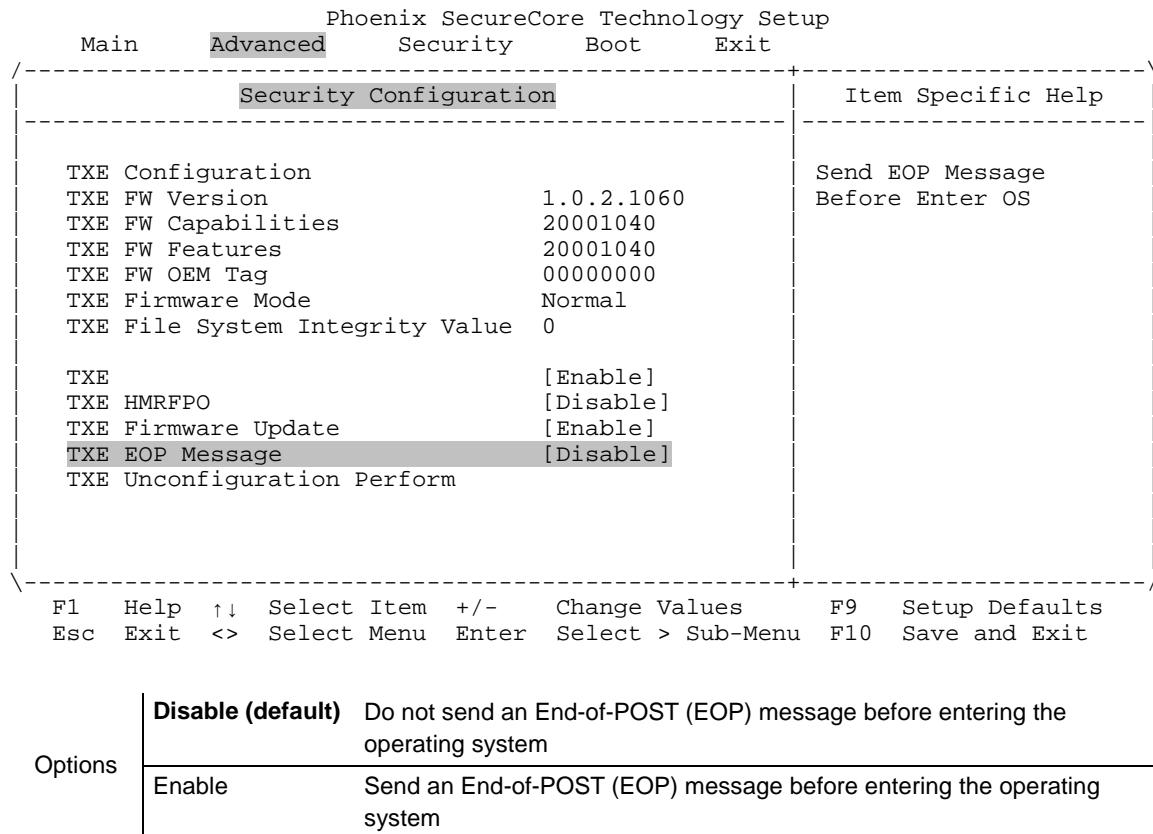
This screen also provides status on the Trusted Execution Engine (TXE).

## Advanced → Security Configuration → TXE Firmware Update



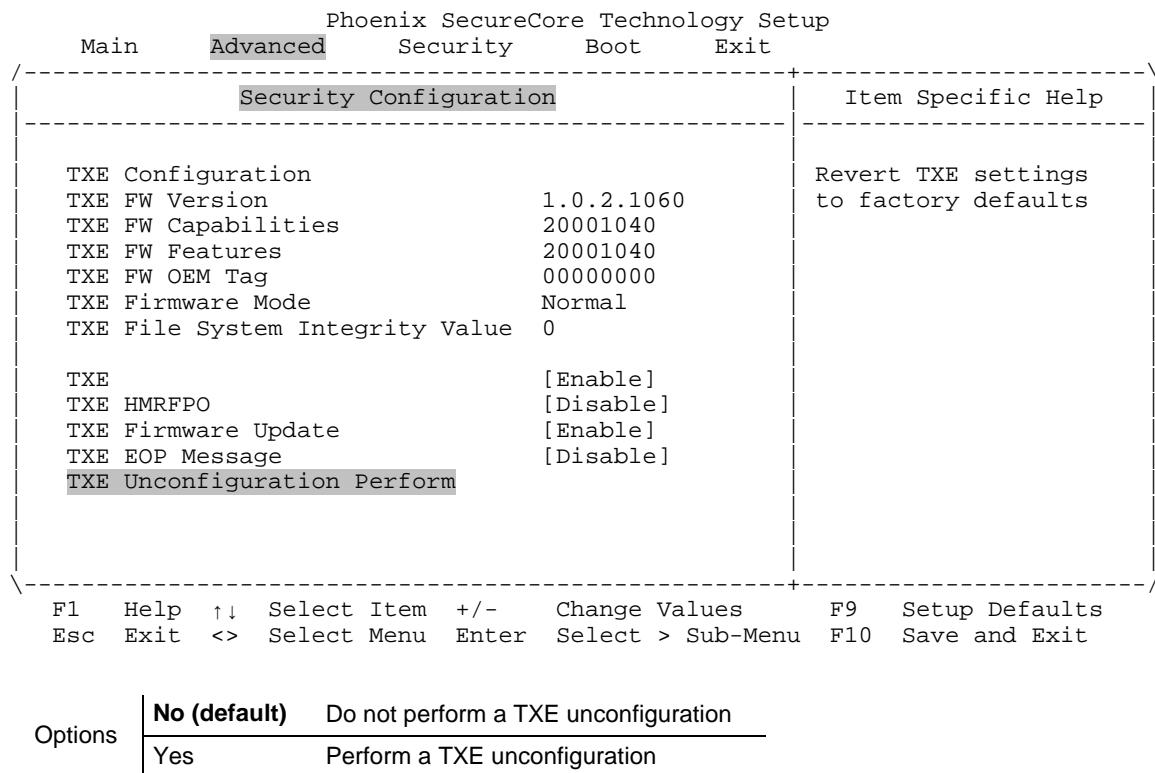
This screen also provides status on the Trusted Execution Engine (TXE).

## Advanced → Security Configuration → TXE EOP Message

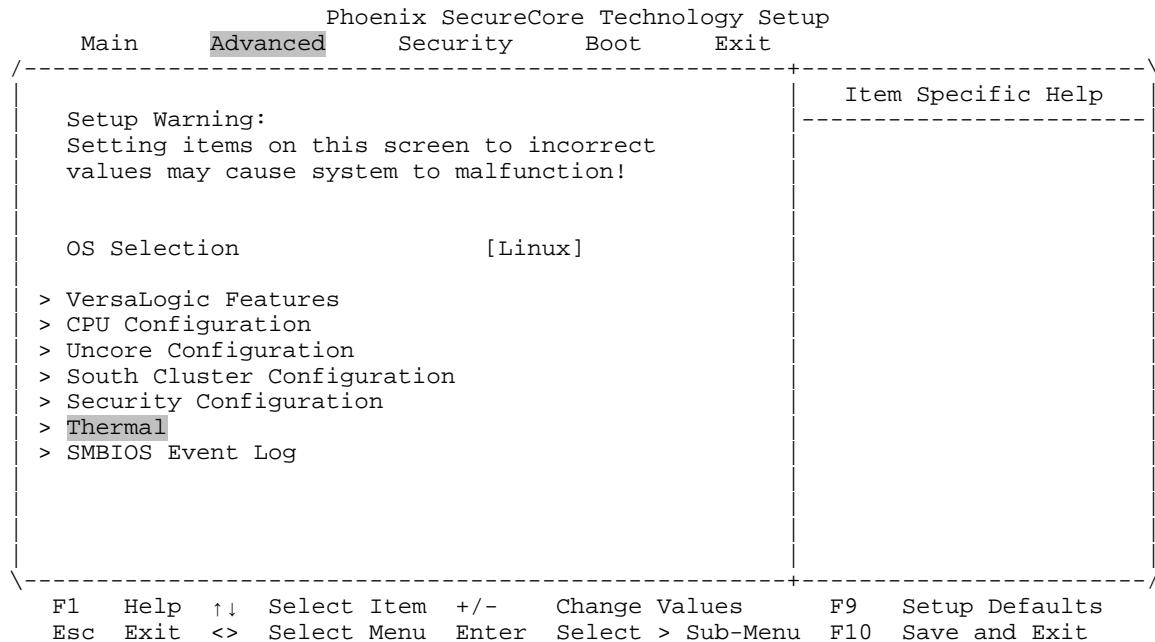


This screen also provides status on the Trusted Execution Engine (TXE).

## Advanced → Security Configuration → TXE Unconfiguration Perform

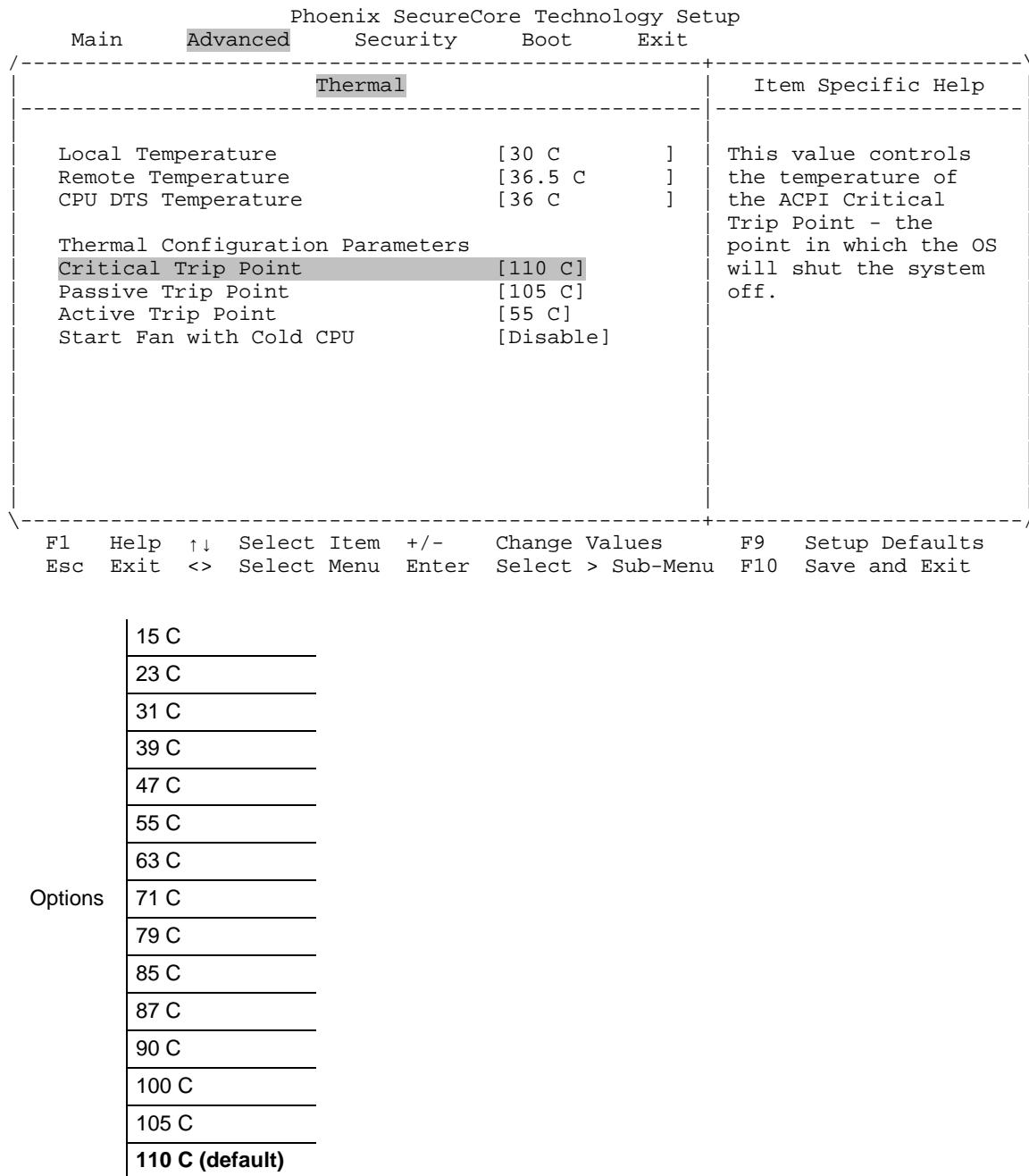


## Advanced → Thermal



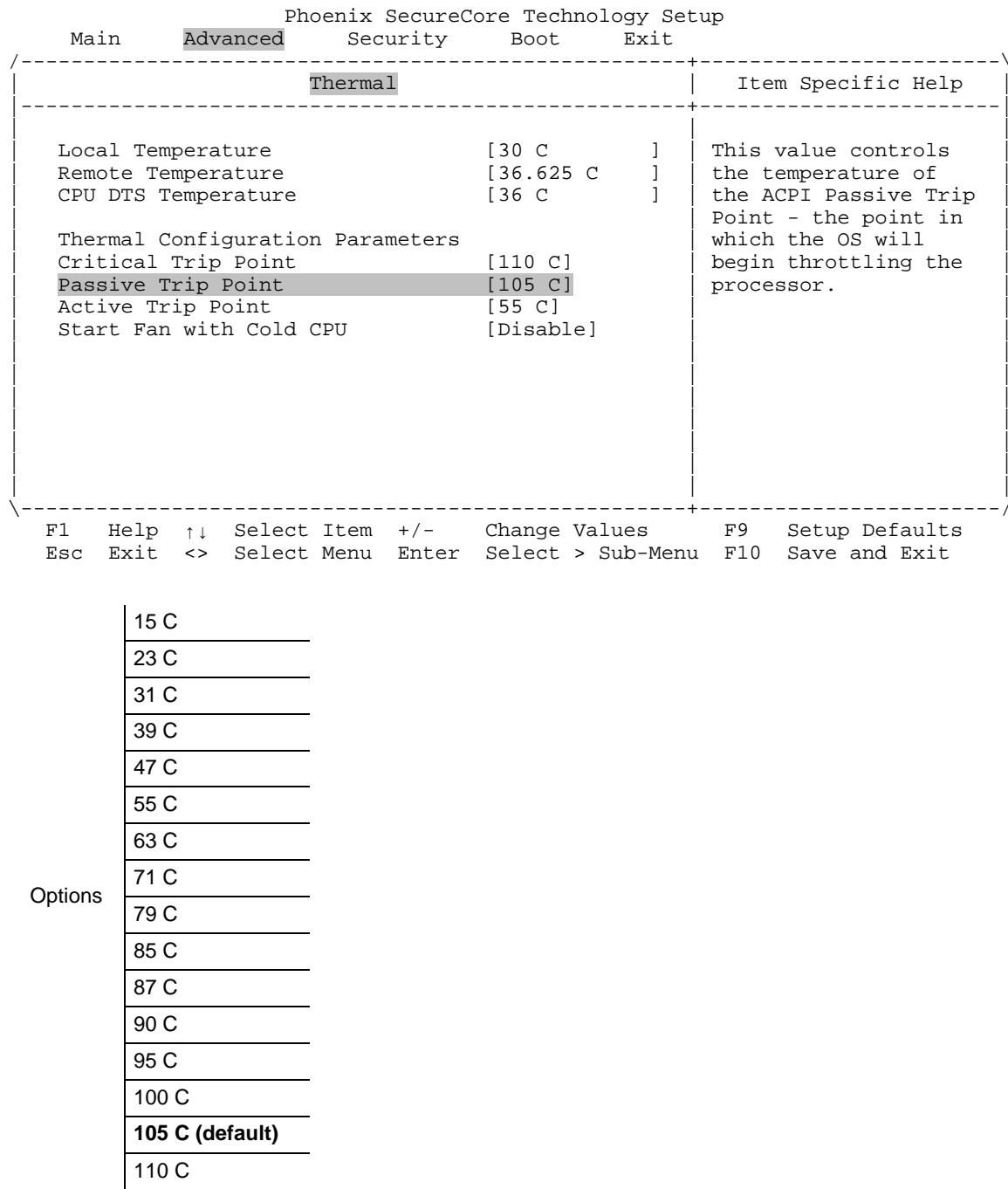
This is the top level screen for the Thermal sub-menu.

## Advanced → Thermal → Critical Trip Point



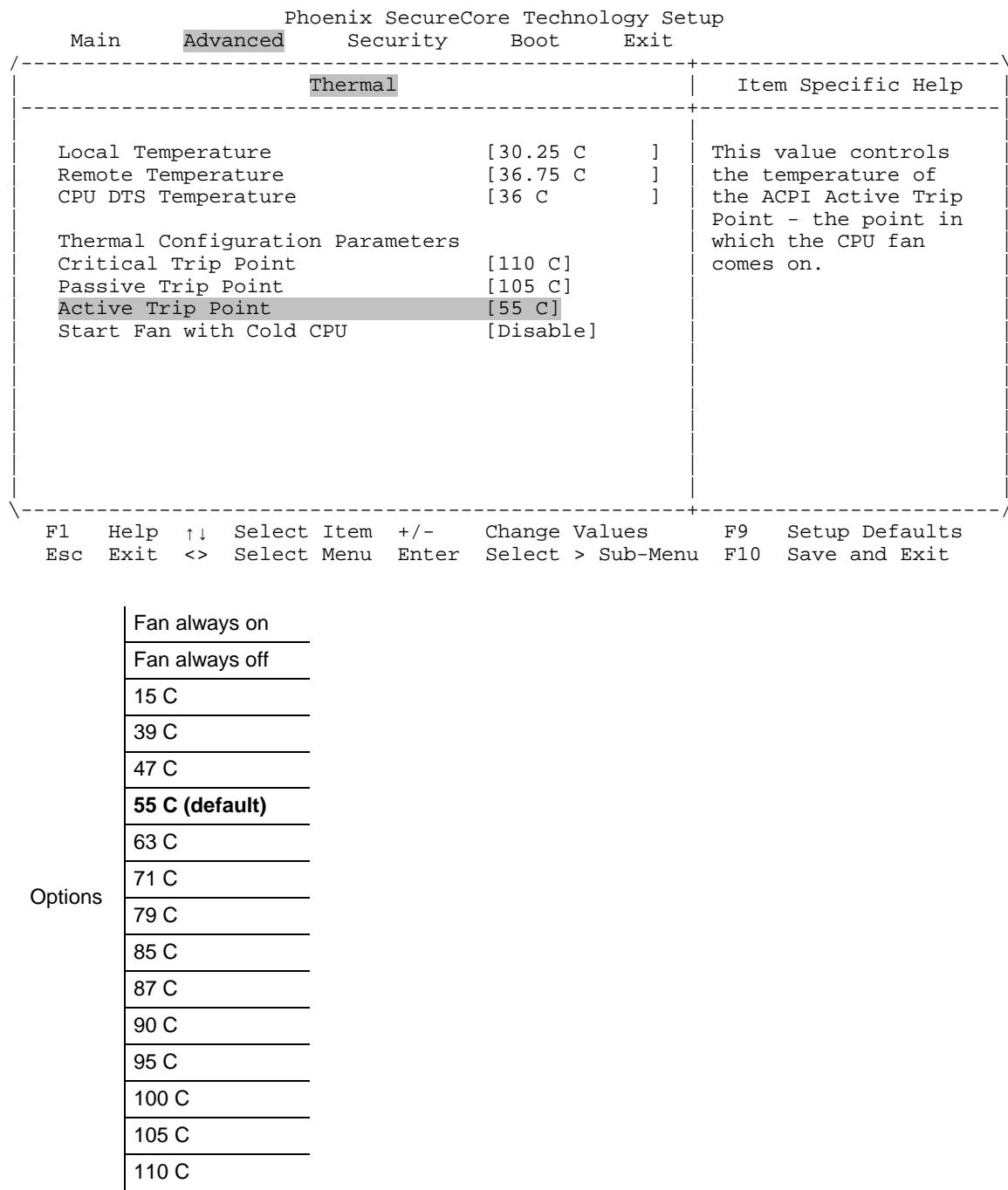
This screen also provides temperature information (local, remote, and CPU digital thermal sensor).

## Advanced → Thermal → Passive Trip Point



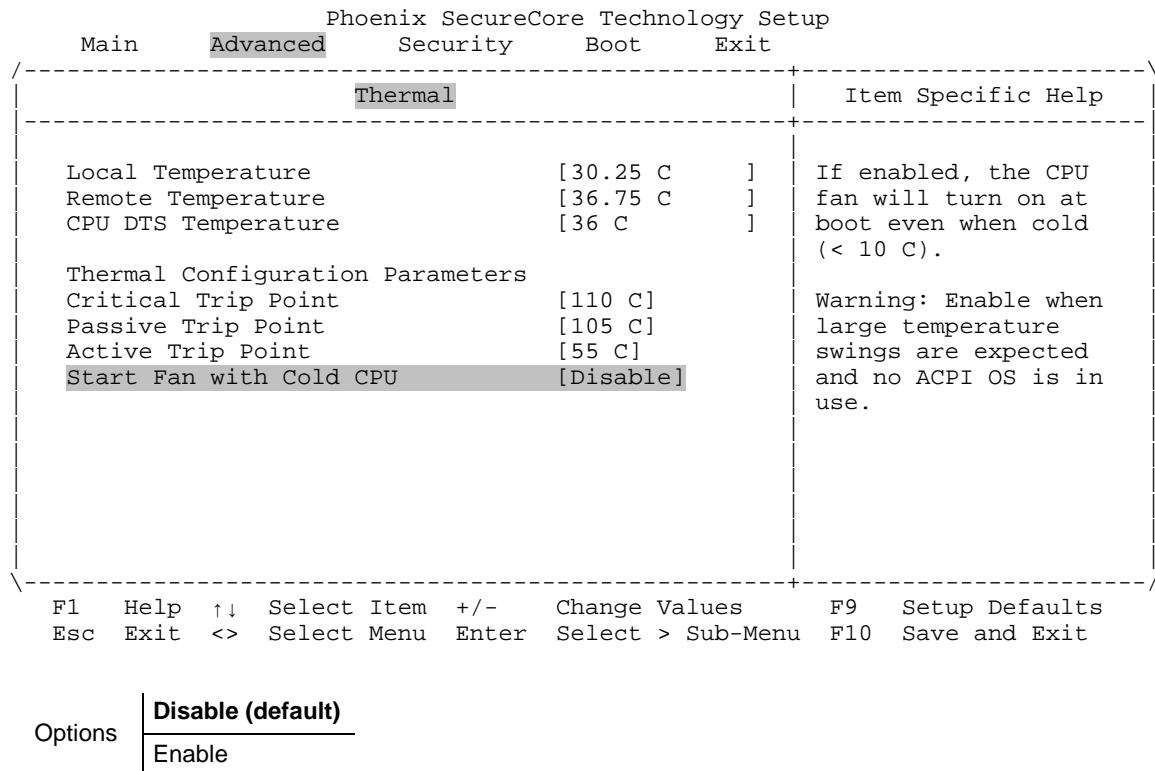
This screen also provides temperature information (local, remote, and CPU digital thermal sensor).

## Advanced → Thermal → Active Trip Point



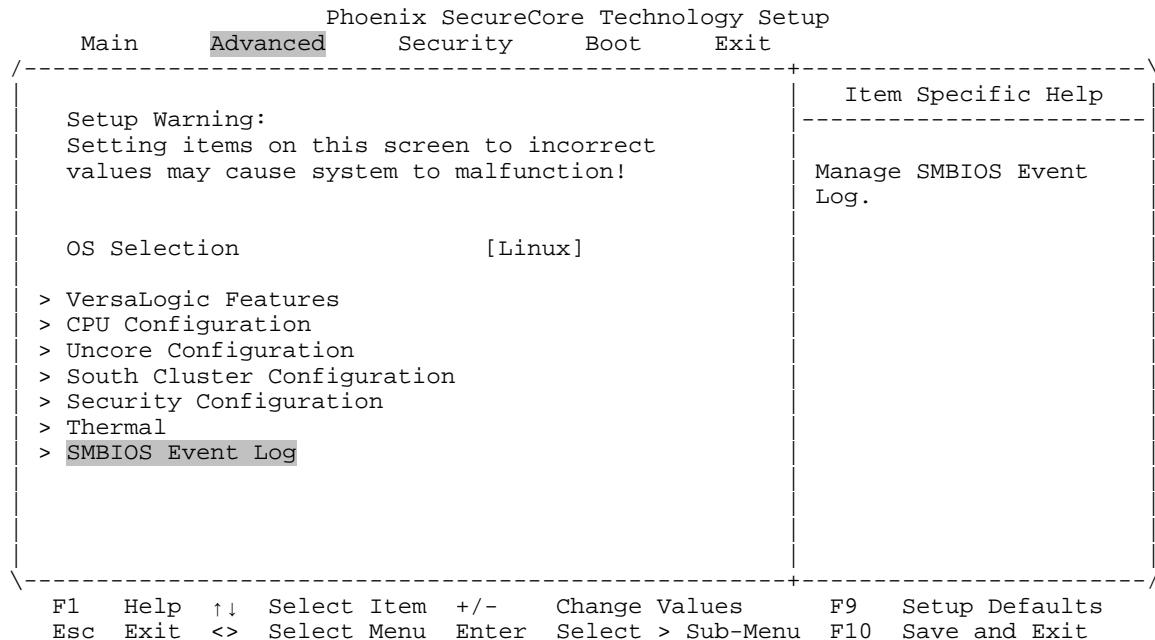
This screen also provides temperature information (local, remote, and CPU digital thermal sensor).

## Advanced → Thermal → Start Fan With Cold CPU

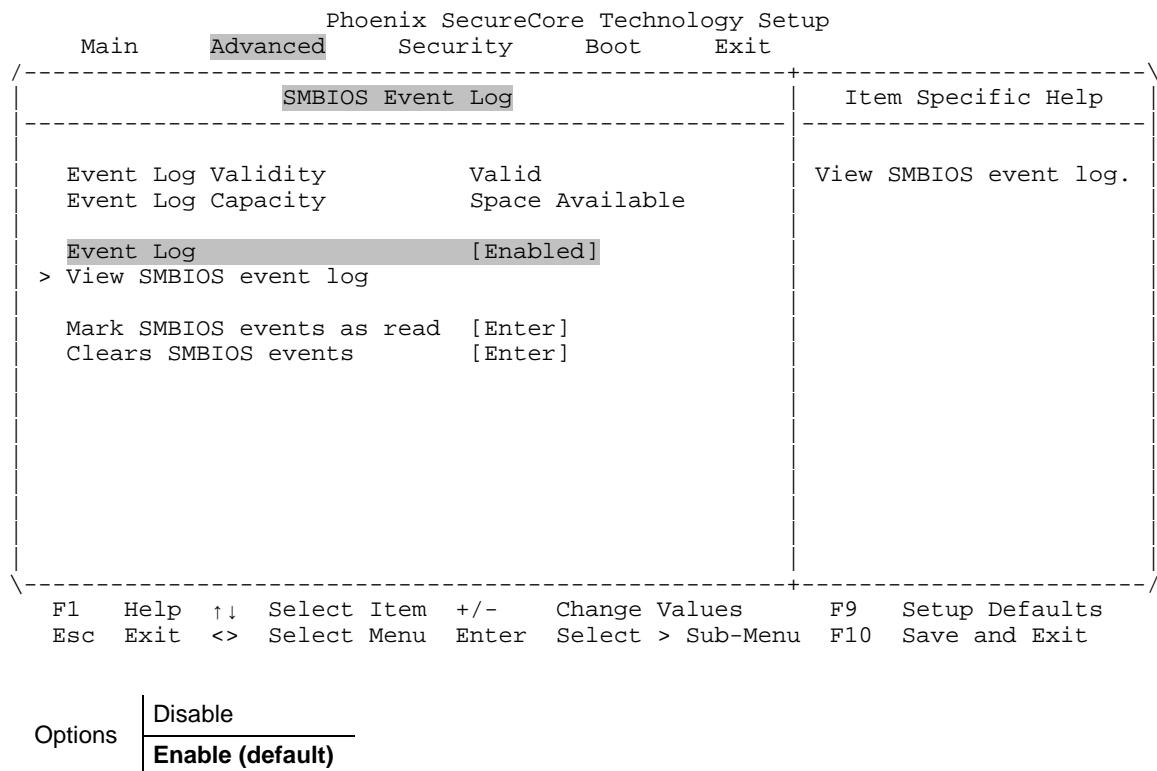


This screen also provides temperature information (local, remote, and CPU digital thermal sensor).

## Advanced → SMBIOS Event Log

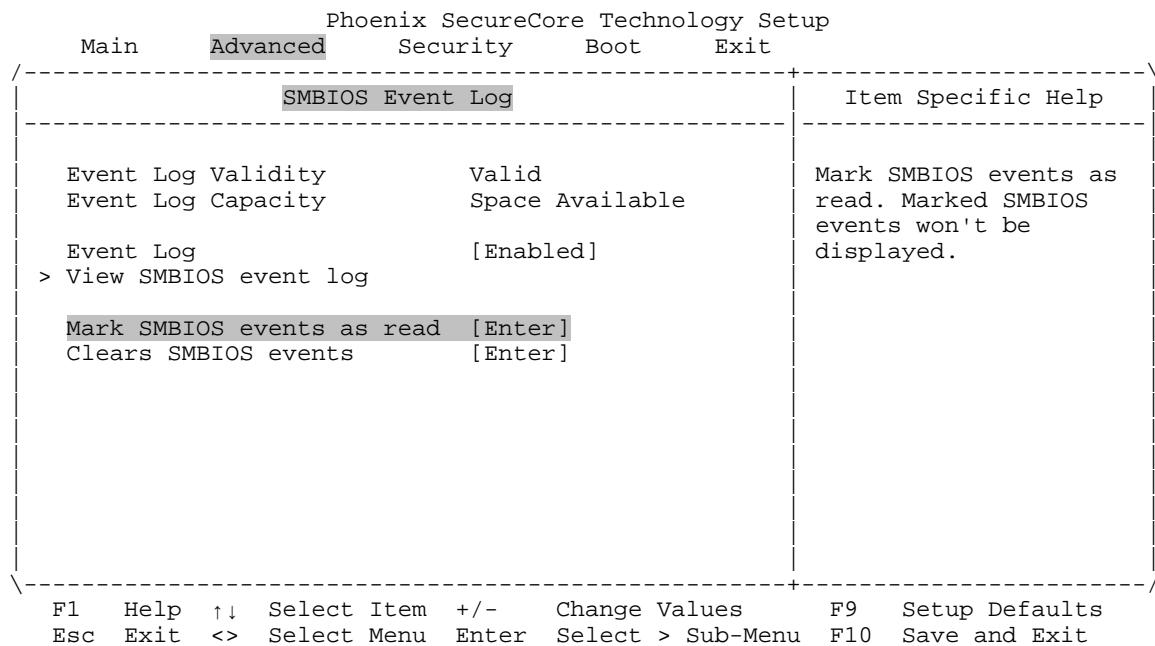


This is the top level screen for the SMBIOS Event Log sub-menu.

**Advanced → SMBIOS Event Log → Event Log**

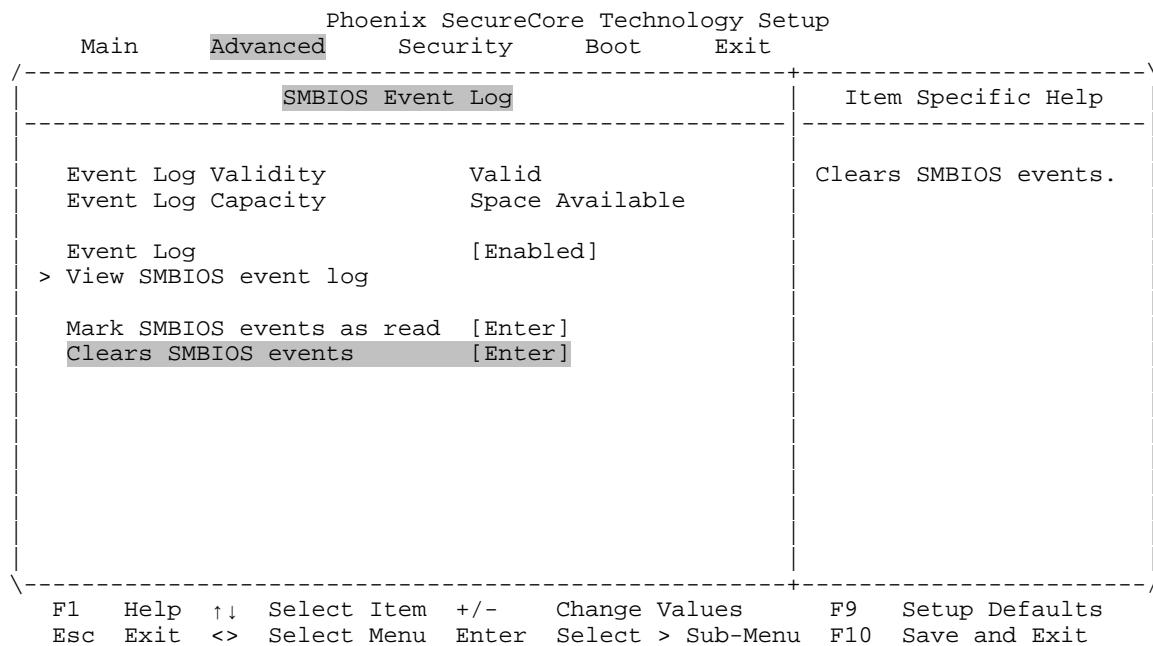
This screen also provides information about the event log's validity and capacity.

## Advanced → SMBIOS Event Log → Mark SMBIOS Events As Read



Press to mark SMBIOS events as read.

This screen also provides information about the event log's validity and capacity.

**Advanced → SMBIOS Event Log → Clear SMBIOS Events**

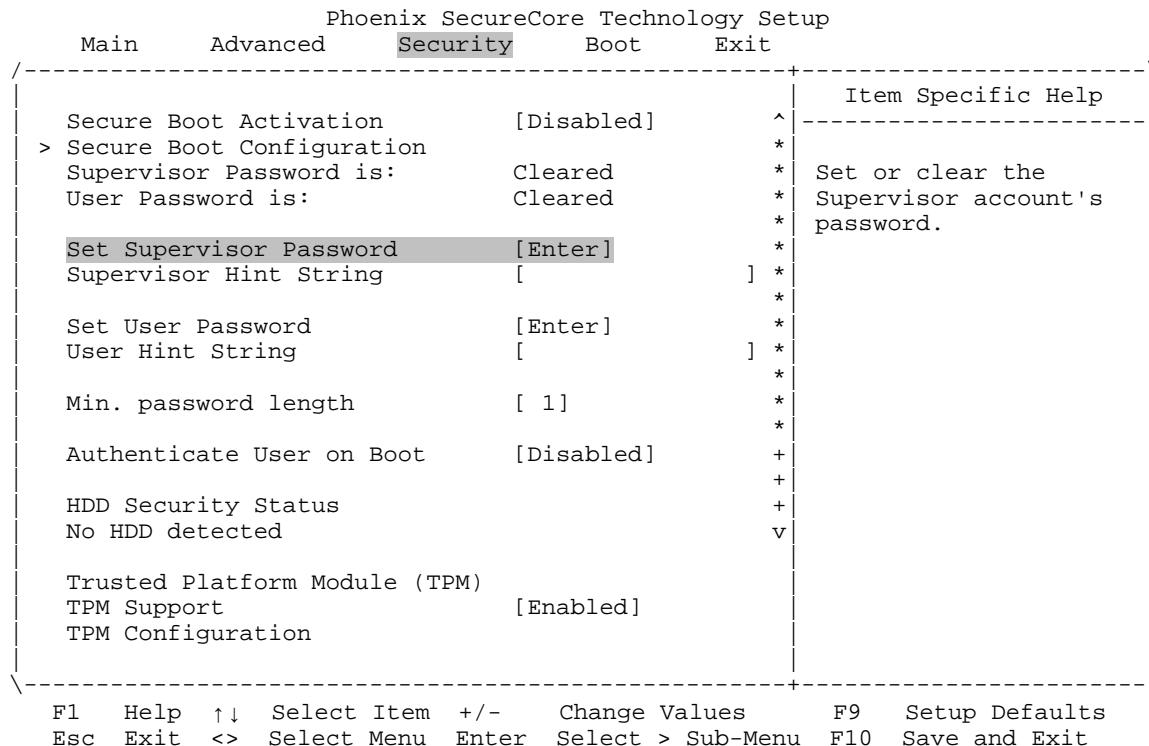
Press to clear SMBIOS events.

This screen also provides information about the event log's validity and capacity.

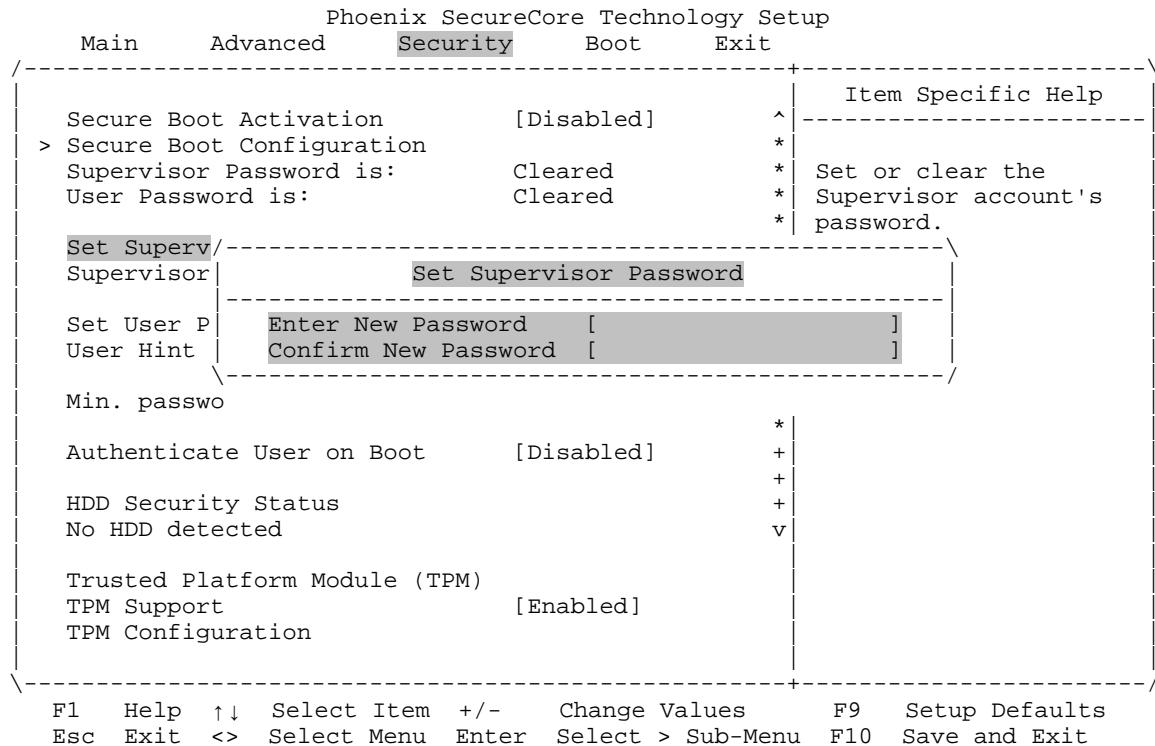
The Security menu enables you to:

- Activate Secure Boot options
- Set and clear supervisor passwords
- Set and clear user passwords
- Configure the Trusted Platform Module (TPM)

Top-level view of Security menu screen:

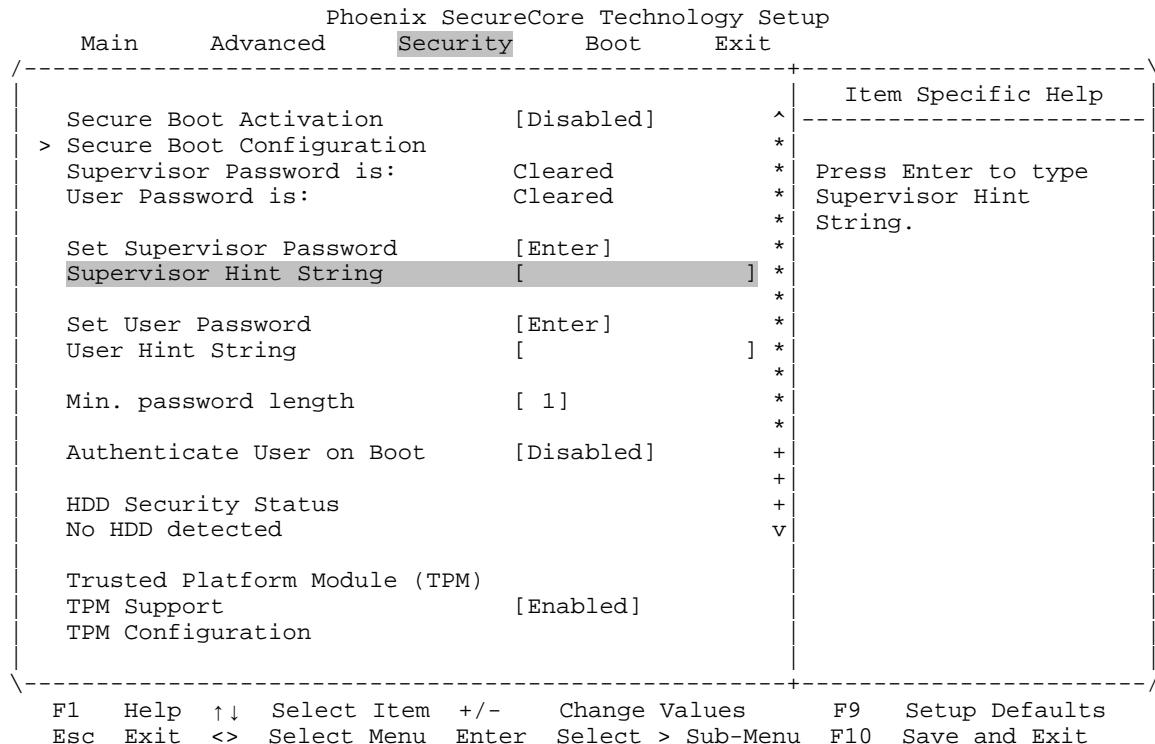


## Security → Set Supervisor Password



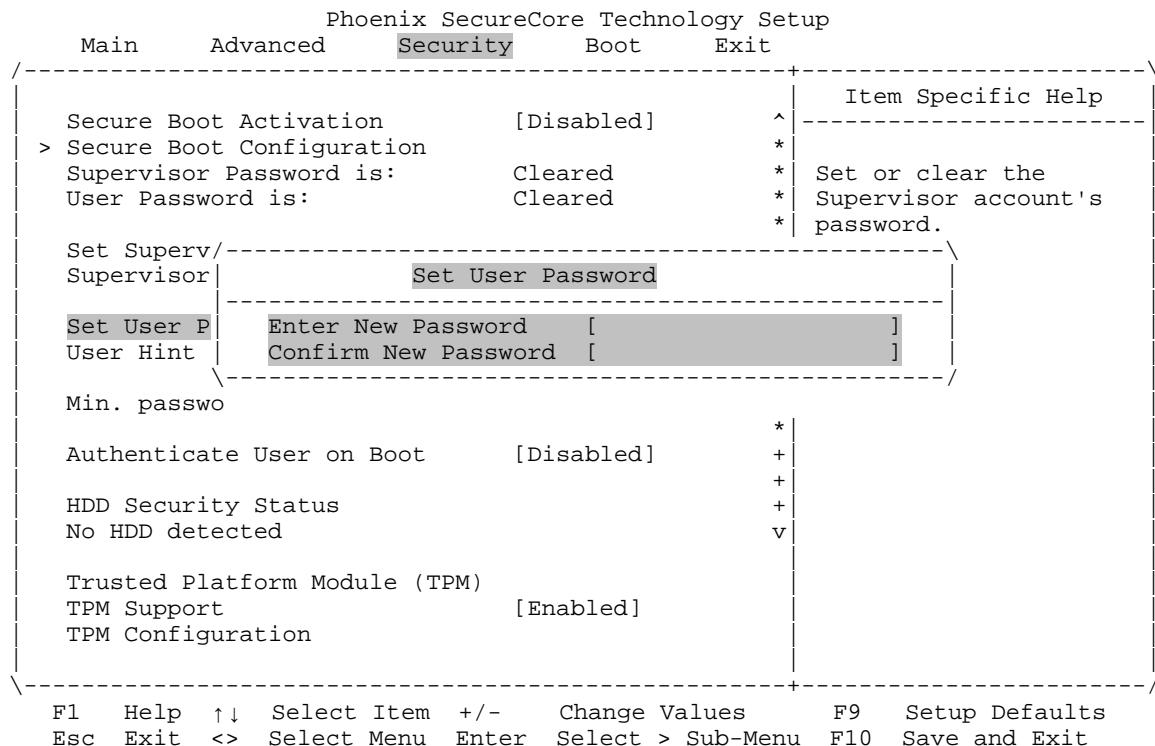
1. Type the supervisor password
2. Confirm the supervisor password

## Security → Supervisor Hint String



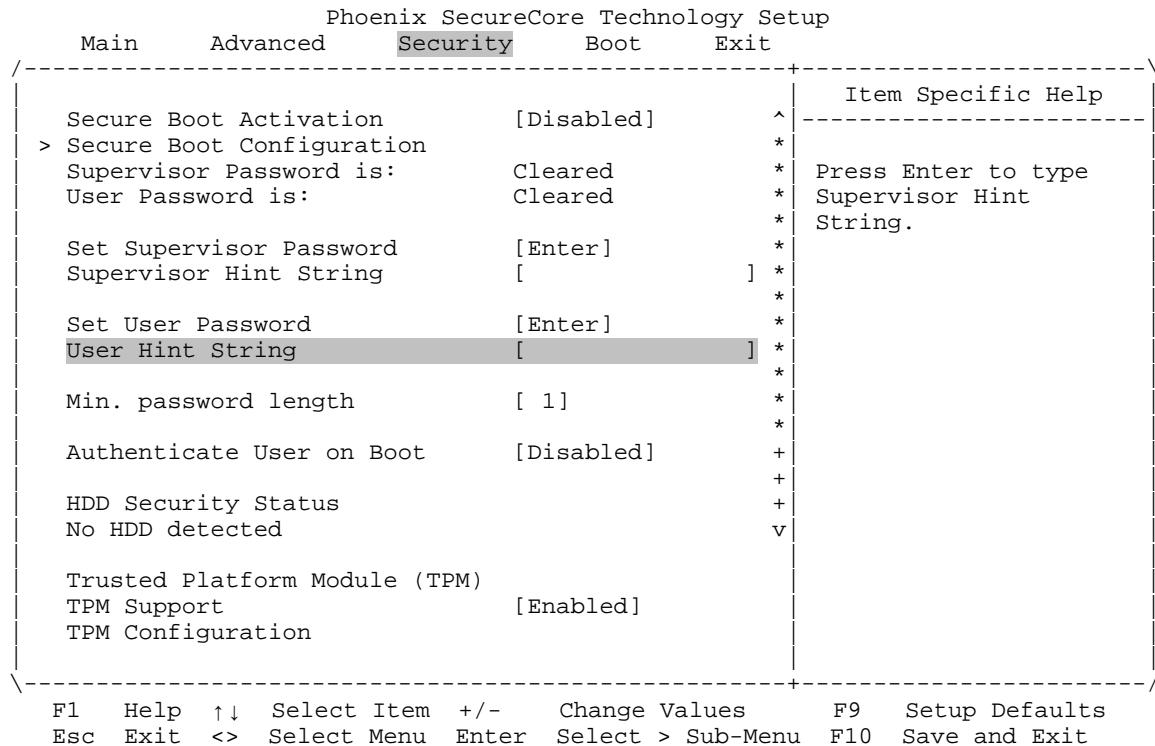
Press to type the supervisor password hint string.

## Security → Set User Password



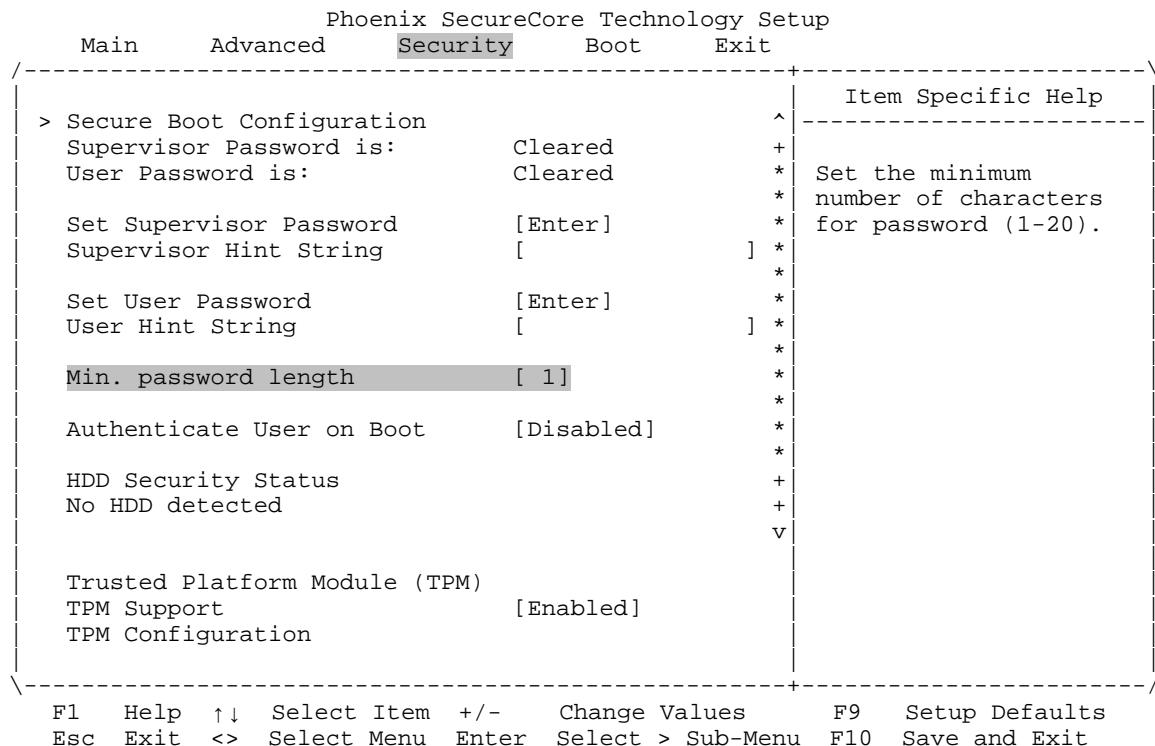
1. Type the user password
2. Confirm the user password

## Security → User Hint String



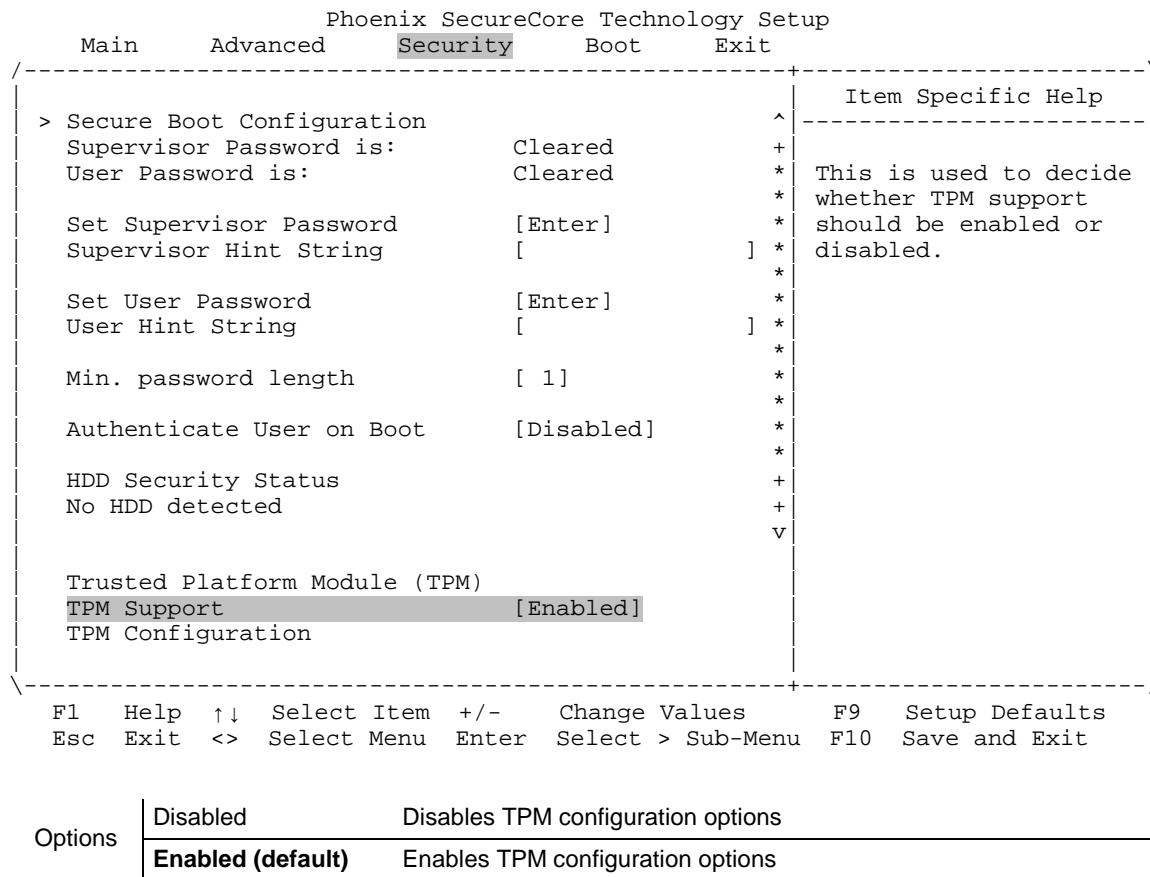
Press  to type the user password hint string.

## Security → Min. Password Length

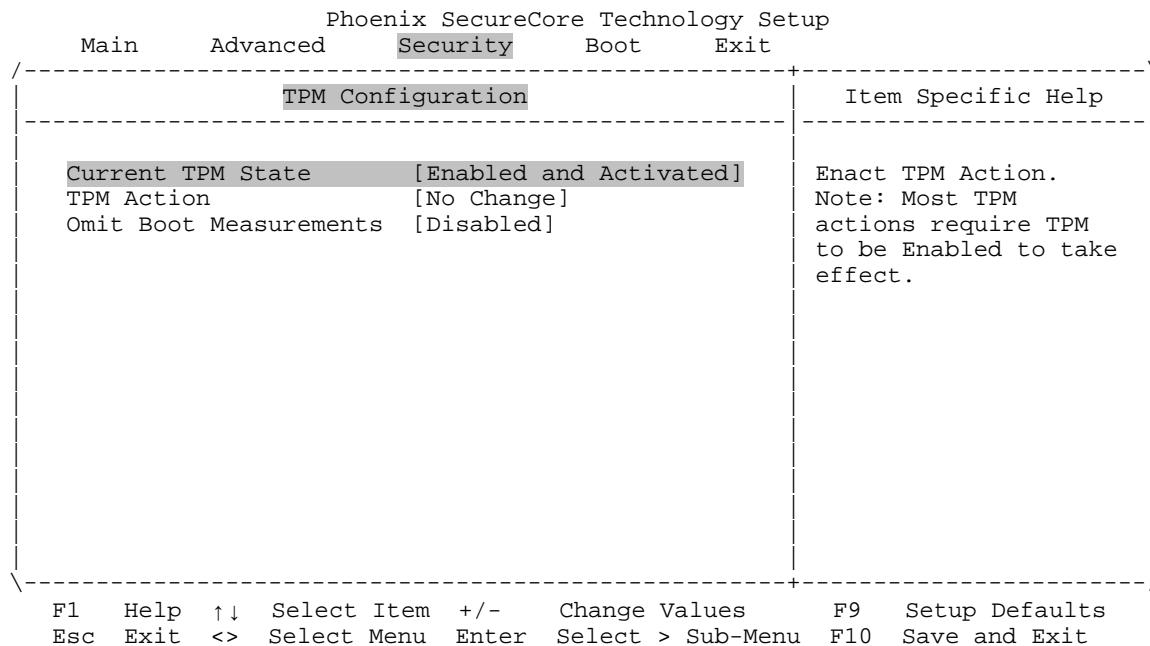


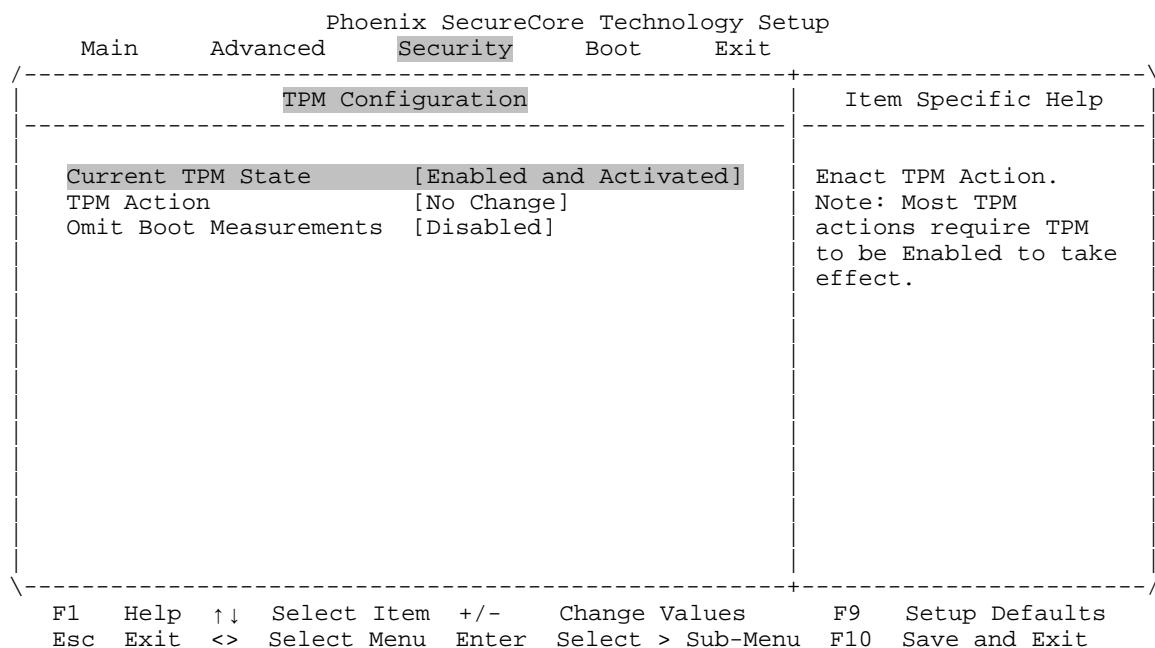
Enter the minimum number of characters for passwords. Range is 1 to 20.

## Security → TPM Support



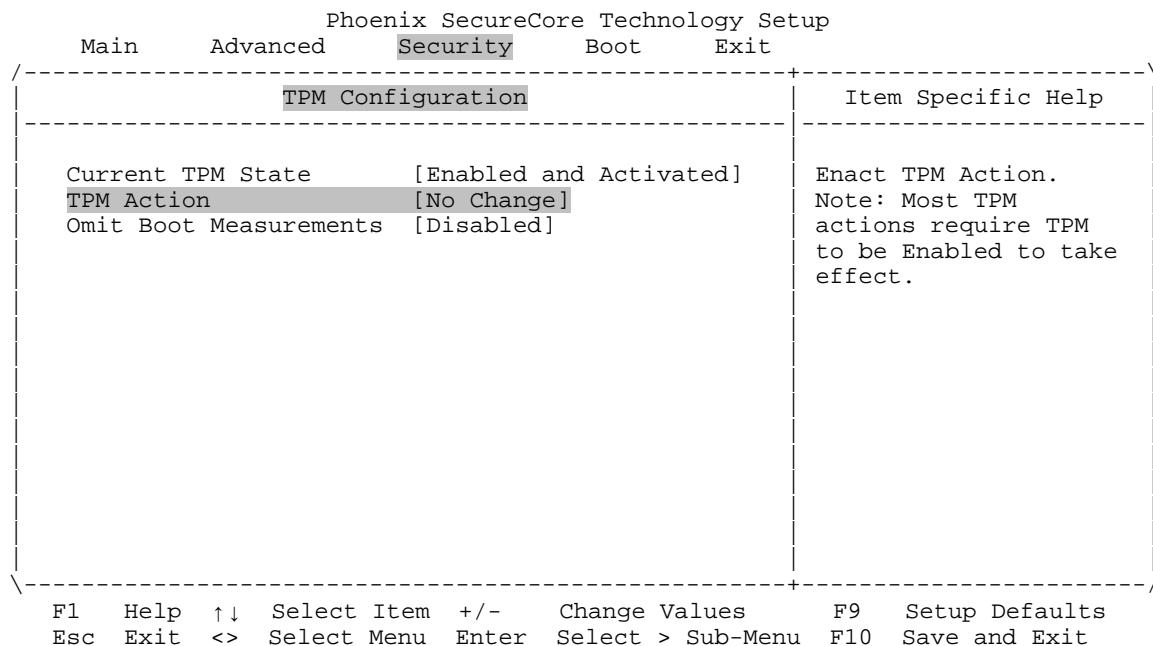
## Security → TPM Configuration



**Security → TPM Configuration → Current TPM State**

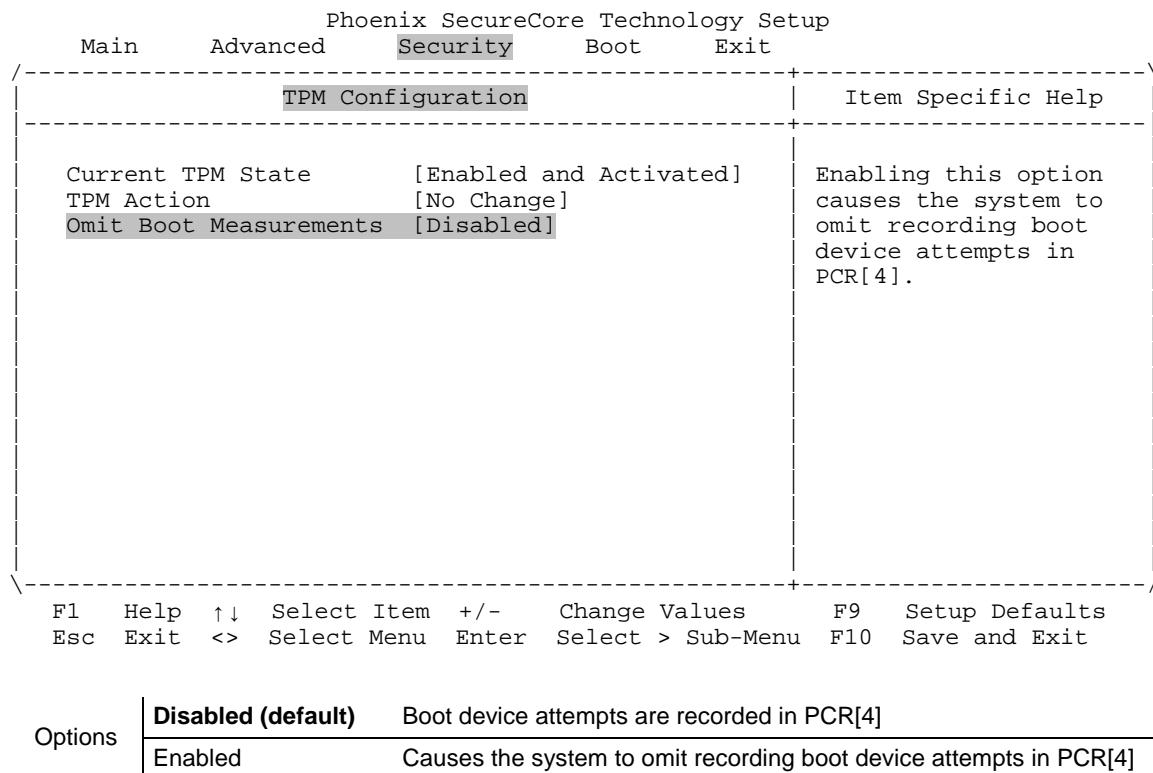
This screen displays the current state of the TPM.

## Security → TPM Configuration → TPM Action



<b>No change (default)</b>	
Options	Enable
	Disable
	Activate
	Deactivate
	Clear
	Enable and Activate
	Disable and Deactivate
	Set Owner Install, with state=True
	Set Owner Install, with state=False
	Enable, Activate, and Set Owner Install with state=True
	Disable, Deactivate, and Set Owner Install with state=False
	Clear, Enable, and Activate
	Require PP for provisioning
	Do not require PP for provisioning
	Require PP for clear
	Do not require PP for clear
	Enable, Activate, and Clear
	Enable, Activate, Clear, Enable, and Activate

## Security → TPM Configuration → Omit Boot Measurements



## Boot Menu

The Boot menu enables you to set the priority of boot devices.

Phoenix SecureCore Technology Setup

Main	Advanced	Security	<b>Boot</b>	Exit
------	----------	----------	-------------	------

---

<b>Boot Priority Order</b> 1. USB CD: 2. ATAPI CD: 3. USB HDD: 4. ATA HDD0: 5. ATA HDD1: 6. USB FDD: 7. Internal Shell 8. PCI LAN:	<b>Item Specific Help</b>  Keys used to view or configure devices: ^ and v arrows Select a device. '+' and '-' move the device up or down. 'Shift + 1' enables or disables a device. 'Del' deletes an unprotected device.
--	---

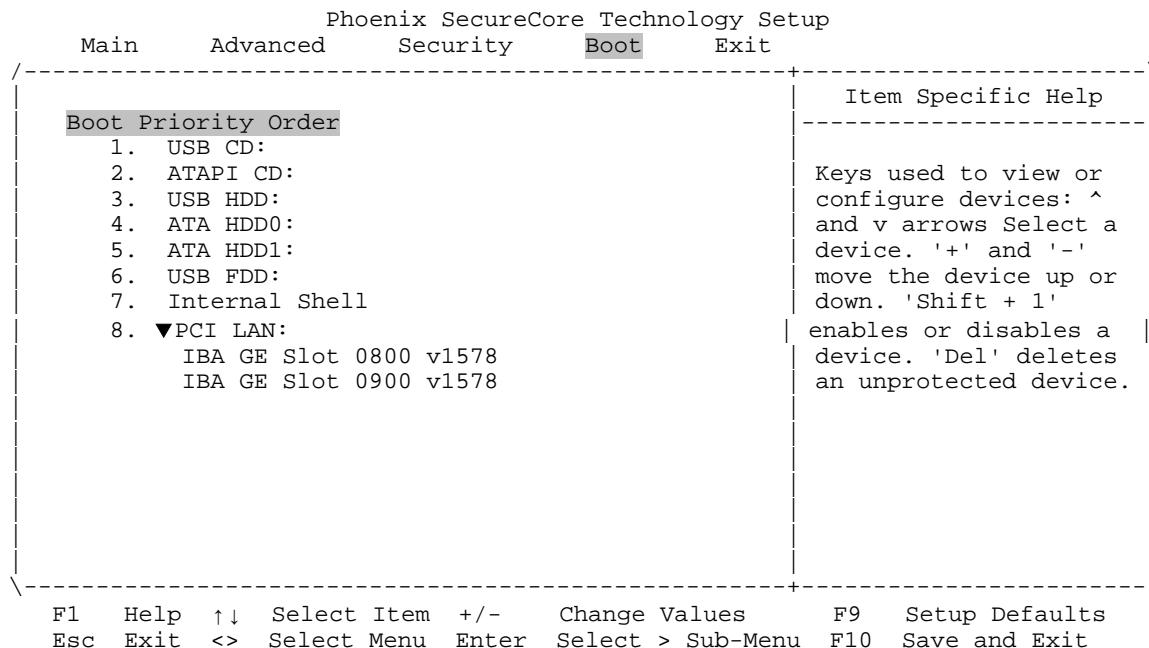
---

F1 Help     $\uparrow\downarrow$  Select Item    +/- Change Values    F9 Setup Defaults  
 Esc Exit    <> Select Menu    Enter Select > Sub-Menu    F10 Save and Exit

Options

 or 	Selects a device from the list
 or 	Moves a selected device up or down the list
 	Enables or disables a device
	Deletes an unprotected device

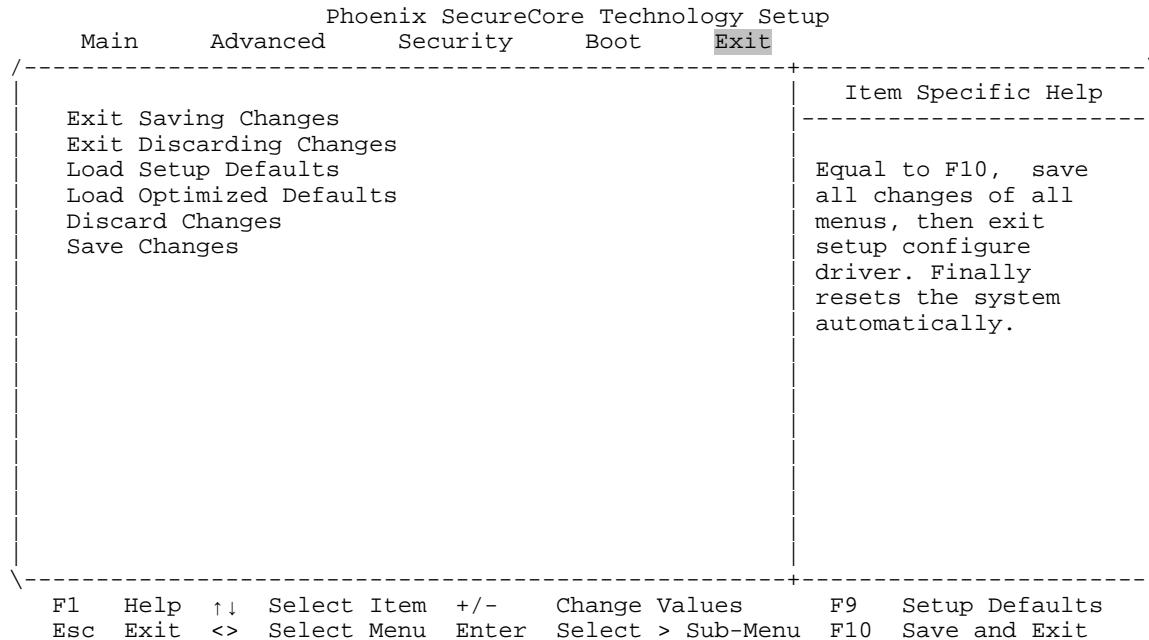
If you have updated the firmware in the board's I210 Ethernet controllers, the PCI LAN entry will include options for network boot, as shown below. The example below shows both LAN ports (NIC1/Ethernet Port 0 and NIC2/Ethernet Port 1, respectively) enabled for network boot.



## Exit Menu

The Exit menu provides options for the following:

- Exiting the BIOS Setup utility without saving changes
- Loading or re-loading default values
- Saving or discarding changes



<b>Exit Saving Changes</b>	Save all changes in all menus, exit setup, and perform a reset; same as <b>F10</b> .
<b>Exit Discarding Changes</b>	Exit Setup without saving changes; same as <b>Esc</b> .
<b>Load Setup Defaults</b>	Load standard default values; same as <b>F9</b> .
<b>Load Optimized Defaults</b>	Load settings for optimized boot time and system performance
<b>Discard Changes</b>	Load original values of this boot time (not the default values).
<b>Save Changes</b>	Save all changes in all menus, but do not reset system.

\*\*\* End of document \*\*\*