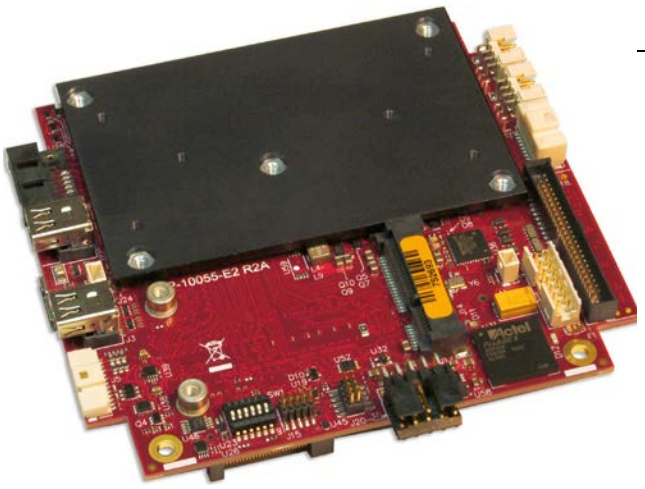
BIOS Reference Manual

REV. 7 August 2017



Bengal

(VL-EPMe-30)

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

VERSALOGIC CORPORATION

WWW.VERSALOGIC.COM

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

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.

† 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 Auto to Gen 1
Rev 3.00	1.04	Bengal_3.1.0.547.r1.104	
Rev 3.01	1.05	Bengal_3.1.0.547.r1.105	Updated Web Links Refer to the table below

Table 1: Changes from BIOS 334.r1.104 to BIOS 547.r1.105

Change	Ref.
Updated video BIOS and GOP driver to better support DP++ mode.	N/A
Added Intel PXE ROM for built-in I210 Ethernet	N/A
Added option to configure action on boot failure.	N/A
Fixed fan control issues.	N/A
Removed 9600 baud setting from console redirection options.	Page 16
Removed Load Optimized Defaults from Exit tab.	Page 132

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.

Contents

Overview 1

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.

```
                    Phoenix SecureCore Technology Setup
    Main     Advanced     Security     Boot     Exit
/-------------------------------------------------------------------------\
```

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

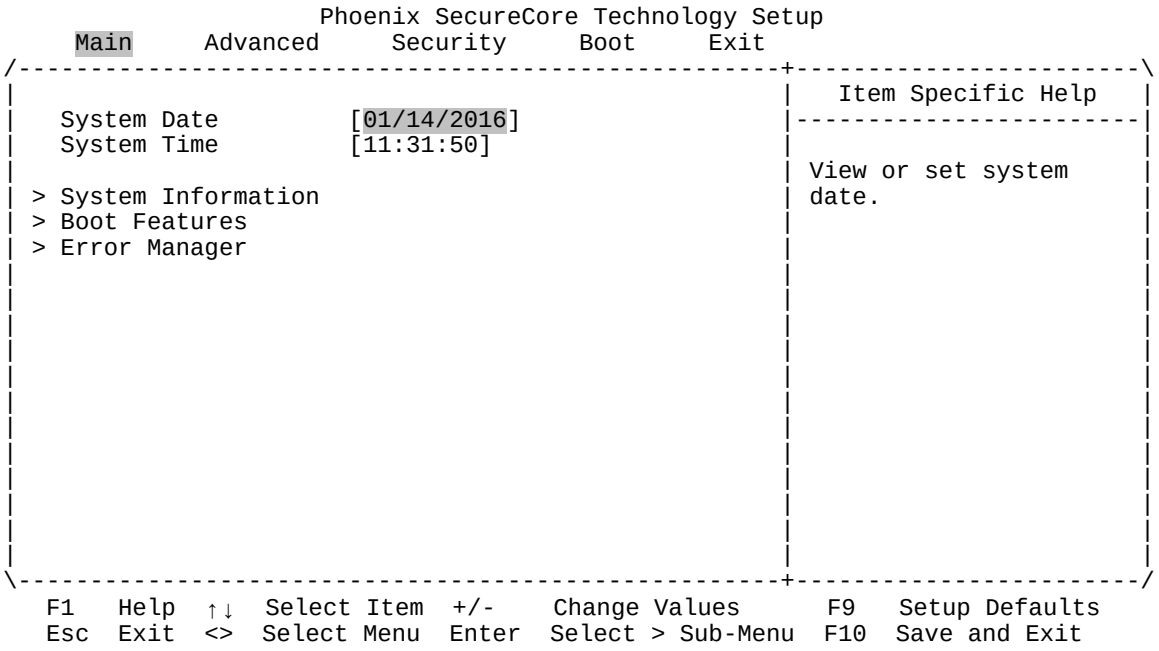
Menu	Function
F1	Help
↑ or ↓	Selects an item (Moves the cursor up or down)
+ or -	Changes values
F9	Loads setup default values
Esc	Exits the menu
← or →	Selects a different menu screen (Moves the cursor left or right)
Enter	Executes a command or selects a sub-menu
F10	Saves the current values and exits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

Main Menu 2

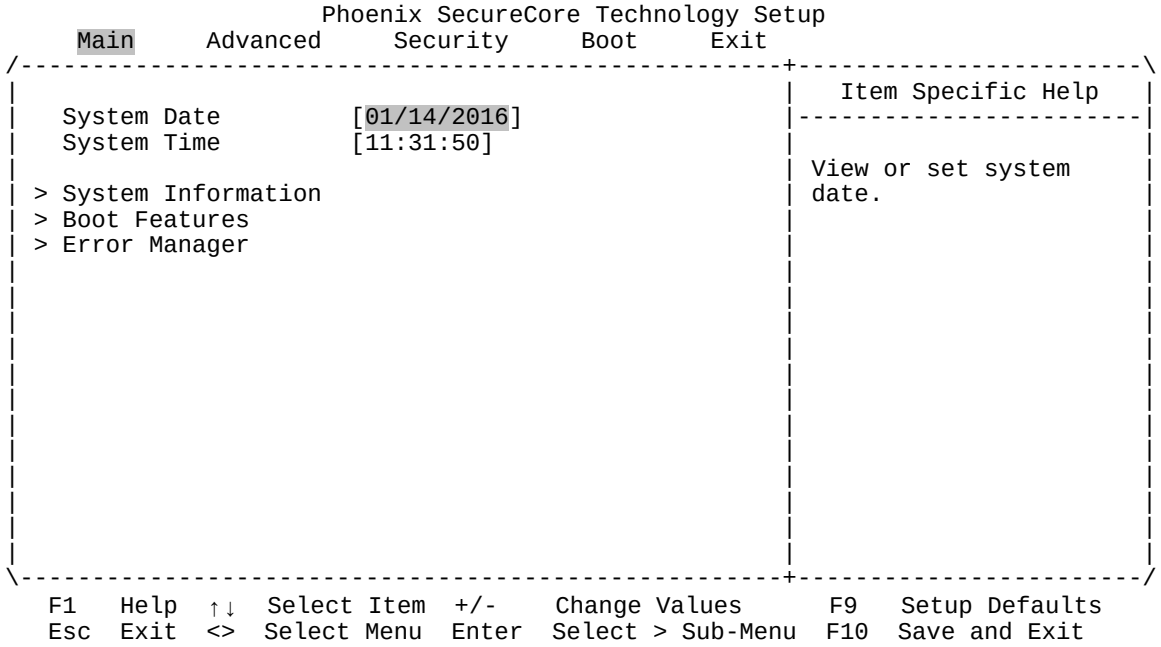
The Main menu enables you to:

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

Top level view of Main menu screen.



Main → System Date

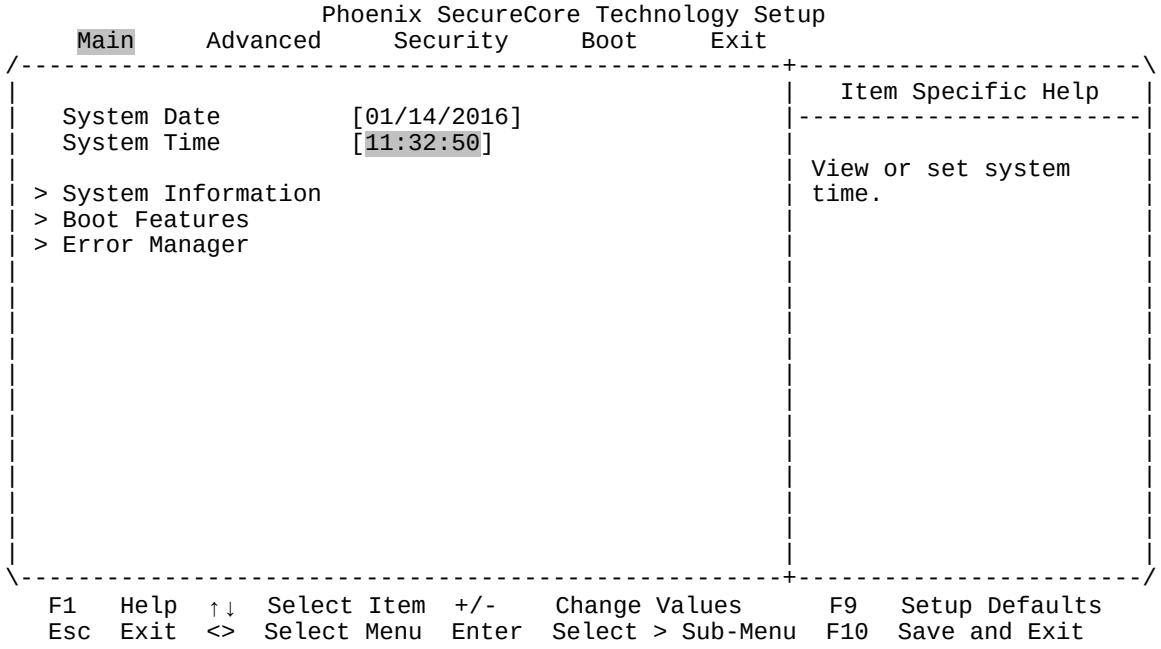


Use the ↑ and ↓ keys to switch between the System Date and System Time fields.

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

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

Main → System Time

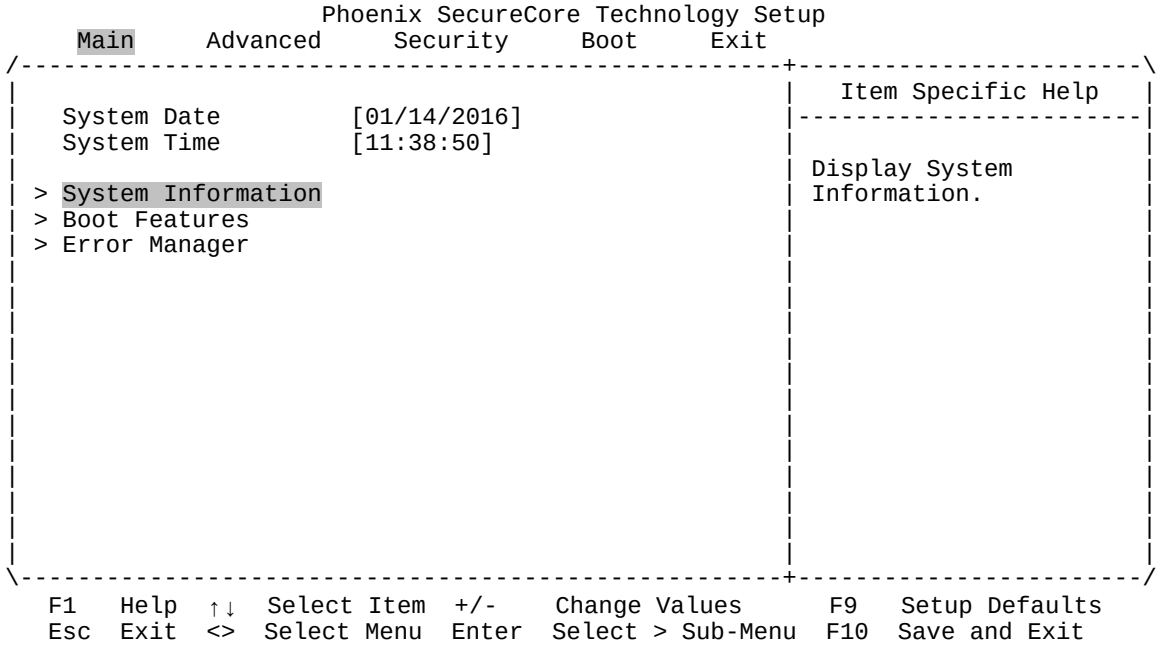


Use the ↑ and ↓ keys to switch between the System Date and System Time fields.

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

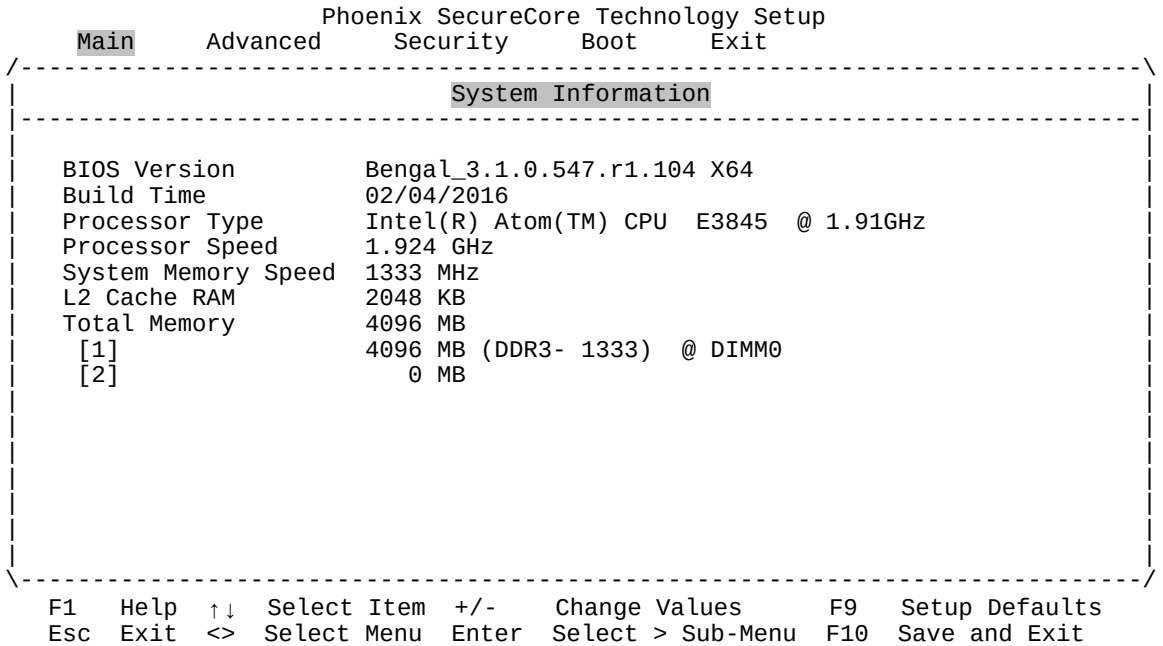
Use the Tab or Enter key to move from hours → minutes → seconds.

Main → System Information

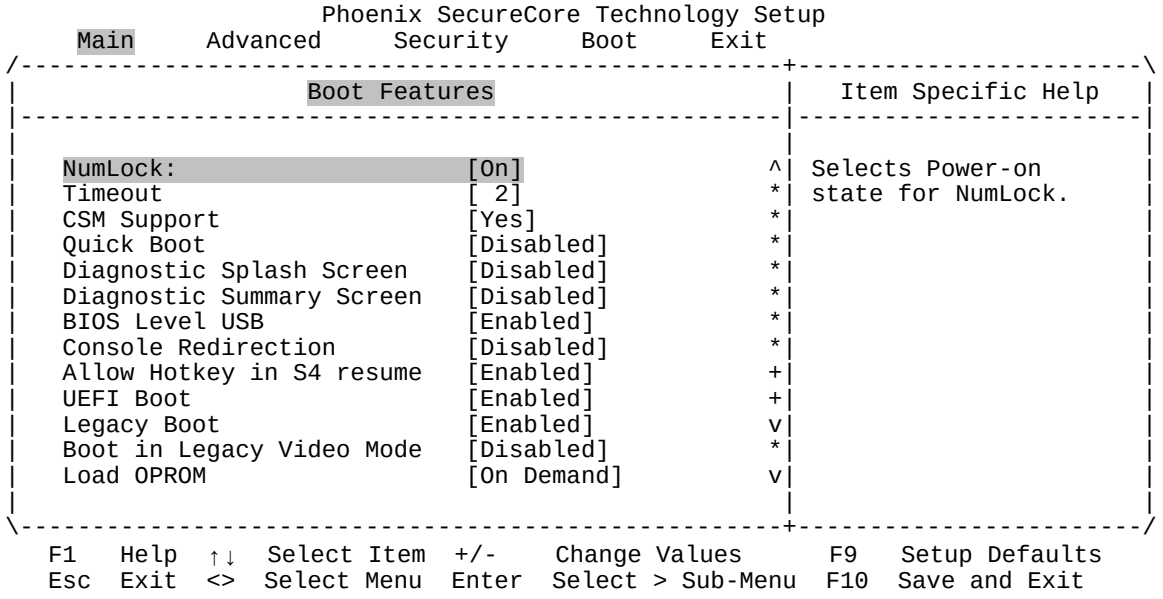


This screen is read-only; there are no user-configurable options.

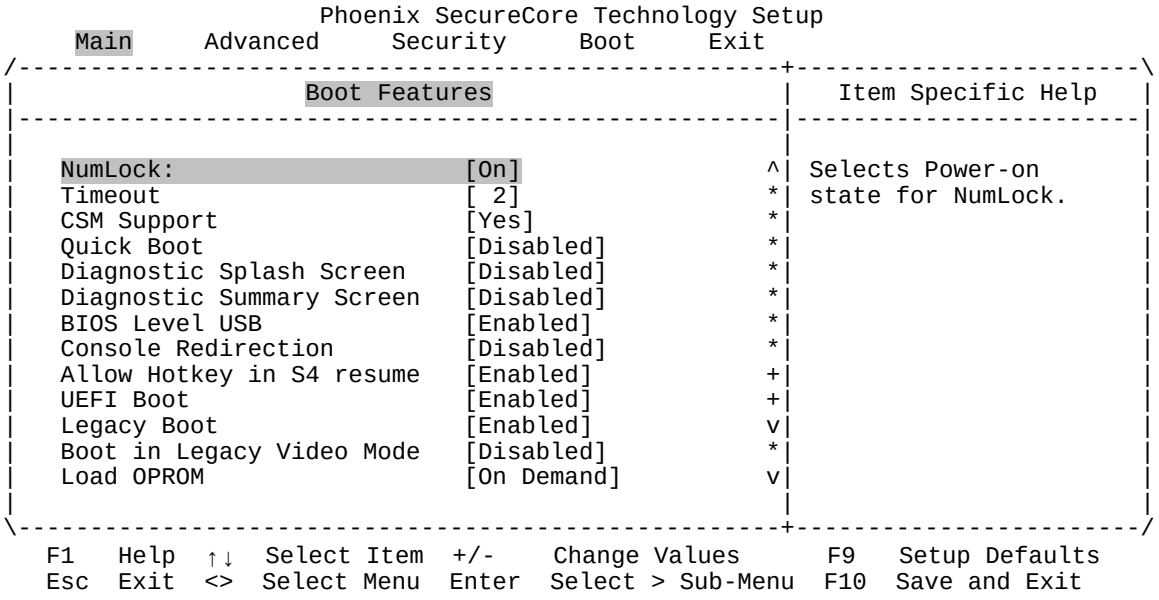
Example view of System Information screen:



Main → Boot Features

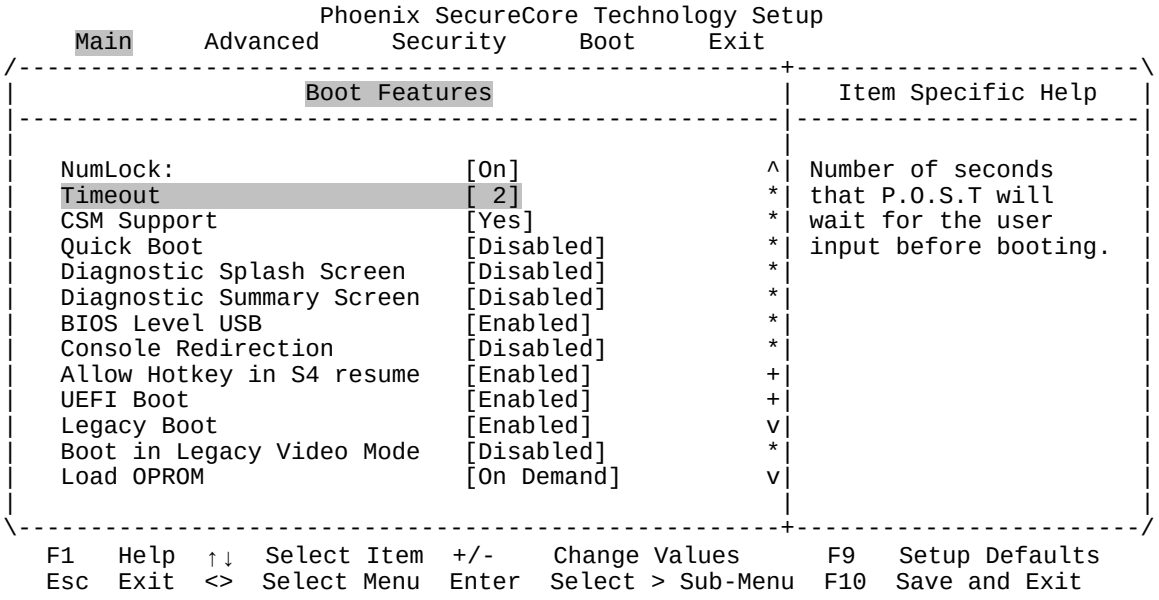


Main → Boot Features → NumLock



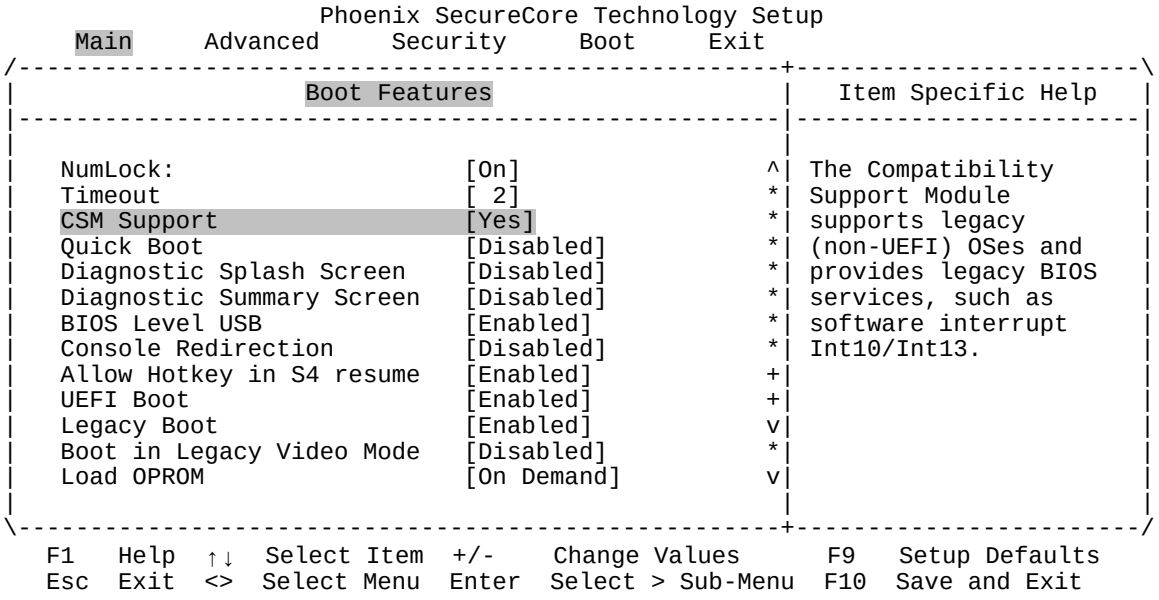
Options	**On (default)**	Enable keyboard NumLock function at power-on
	Off	Disable keyboard NumLock function at power-on

Main → Boot Features → Timeout



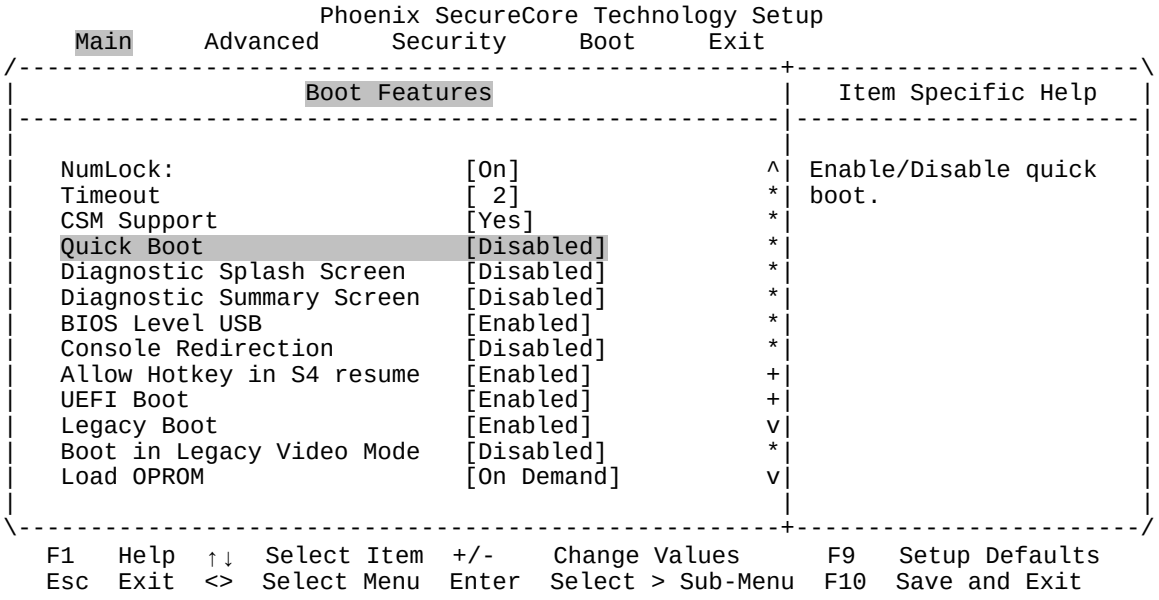
Options	**2 (default)**	Two-second delay
	0-99	Acceptable range

Main → Boot Features → CSM Support



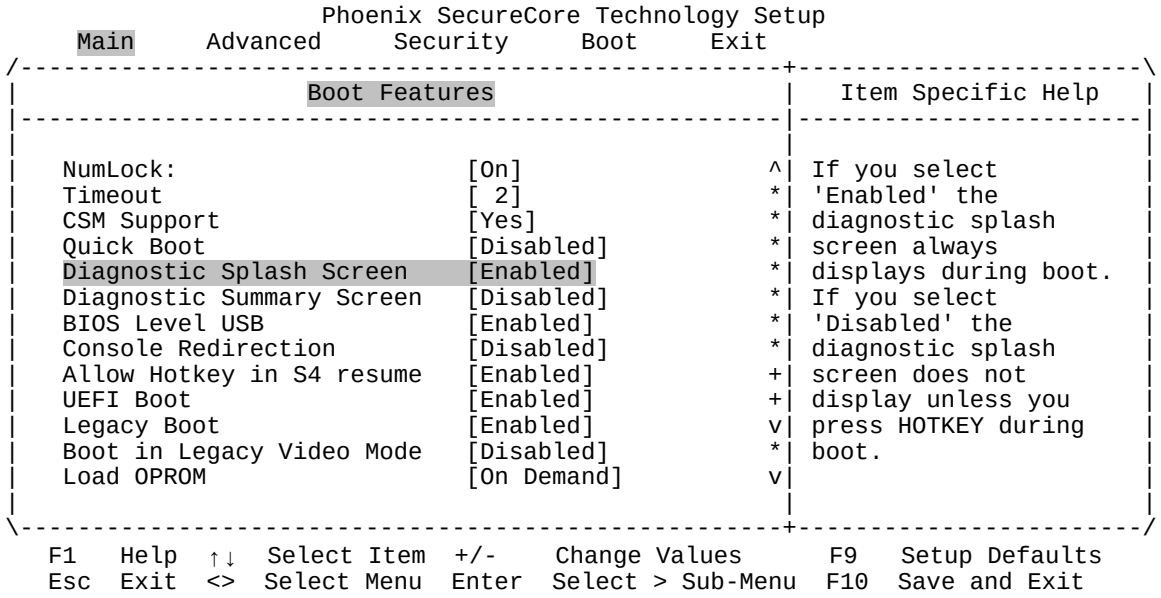
Options	No	Disable Compatibility Support Module (CSM)
	Yes (default)	Enable Compatibility Support Module (CSM)

Main → Boot Features → Quick Boot



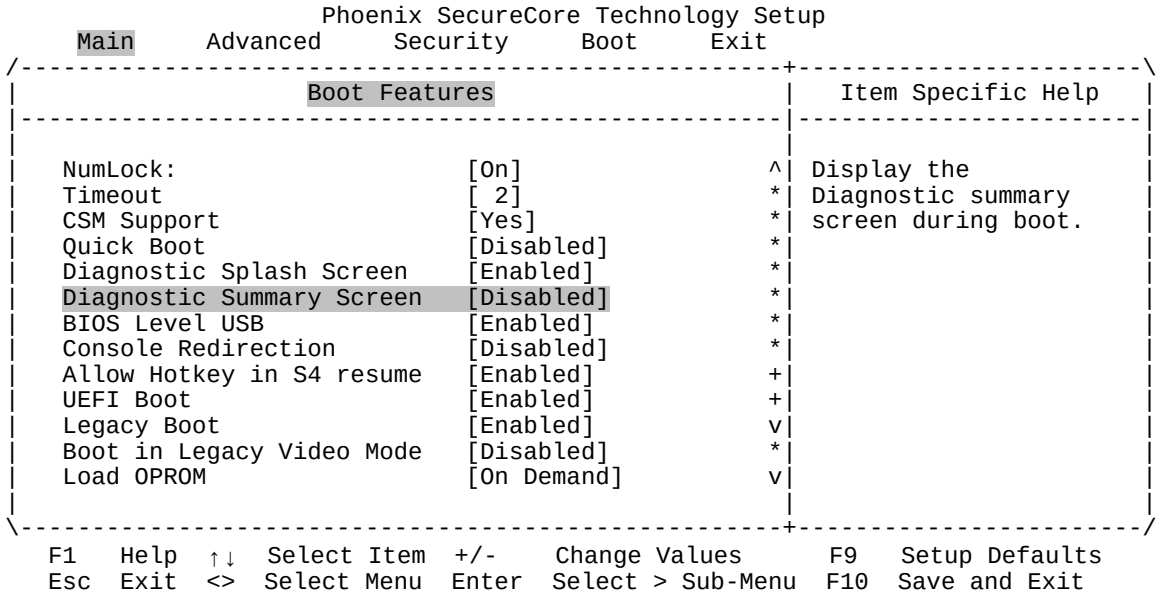
Options	**Disabled (default)**	Disable Quick Boot
	Enabled	Enable Quick Boot

Main → Boot Features → Diagnostic Splash Screen



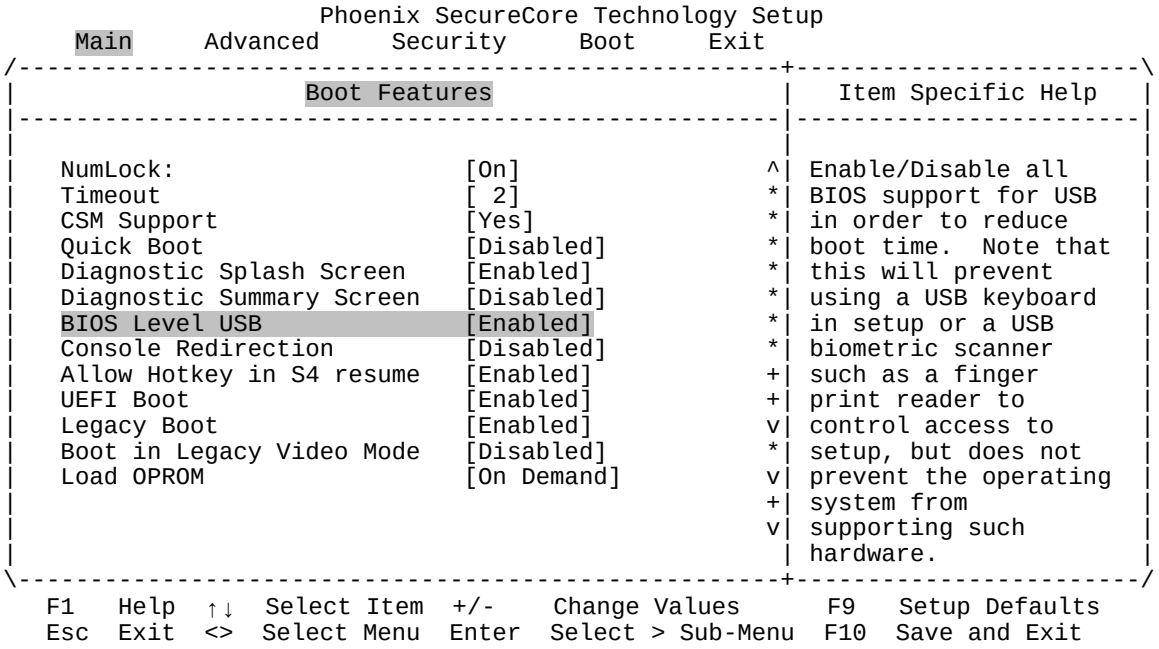
Options	**Disabled (default)**	Diagnostic splash screen does not display unless you press HOTKEY during boot
	Enabled	Diagnostic splash screen always displays during boot

Main → Boot Features → Diagnostic Summary Screen



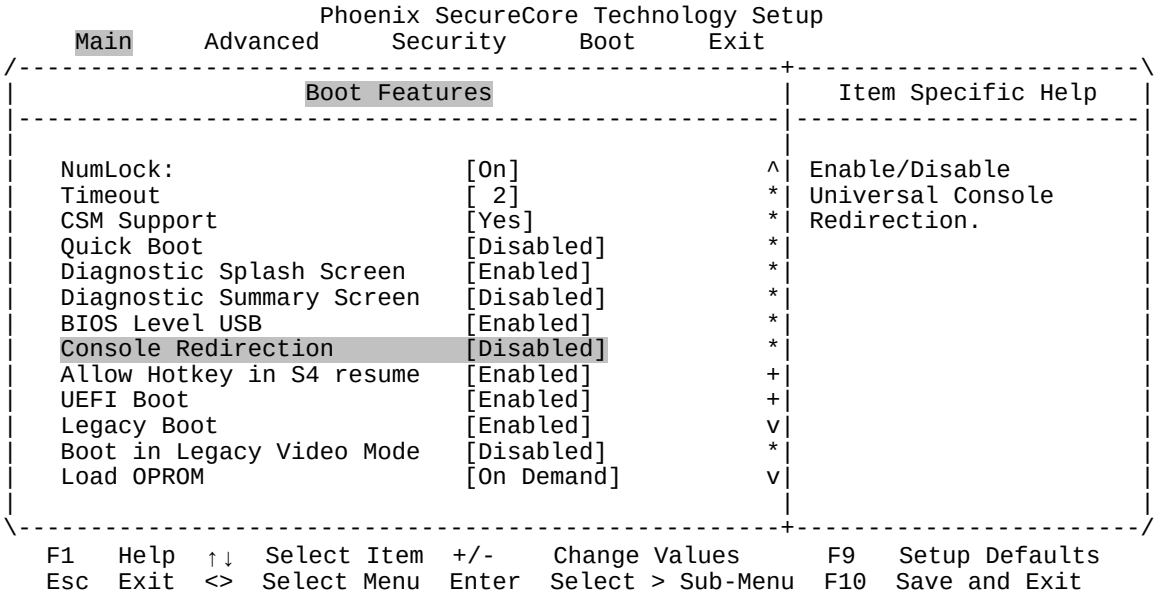
Options	**Disabled (default)**	Diagnostic summary screen does not display during boot
	Enabled	Diagnostic summary screen displays during boot

Main → Boot Features → BIOS Level USB



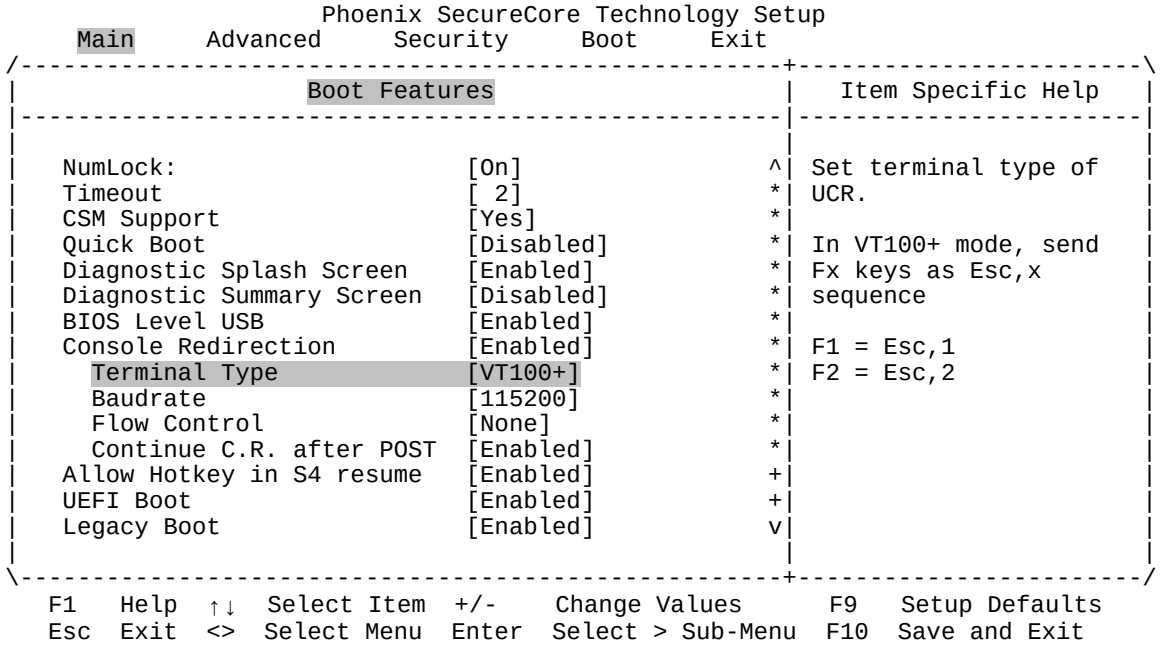
Options	Disabled	Disables USB support within BIOS
	Enabled (default)	Enables USB support within BIOS

Main → Boot Features → Console Redirection



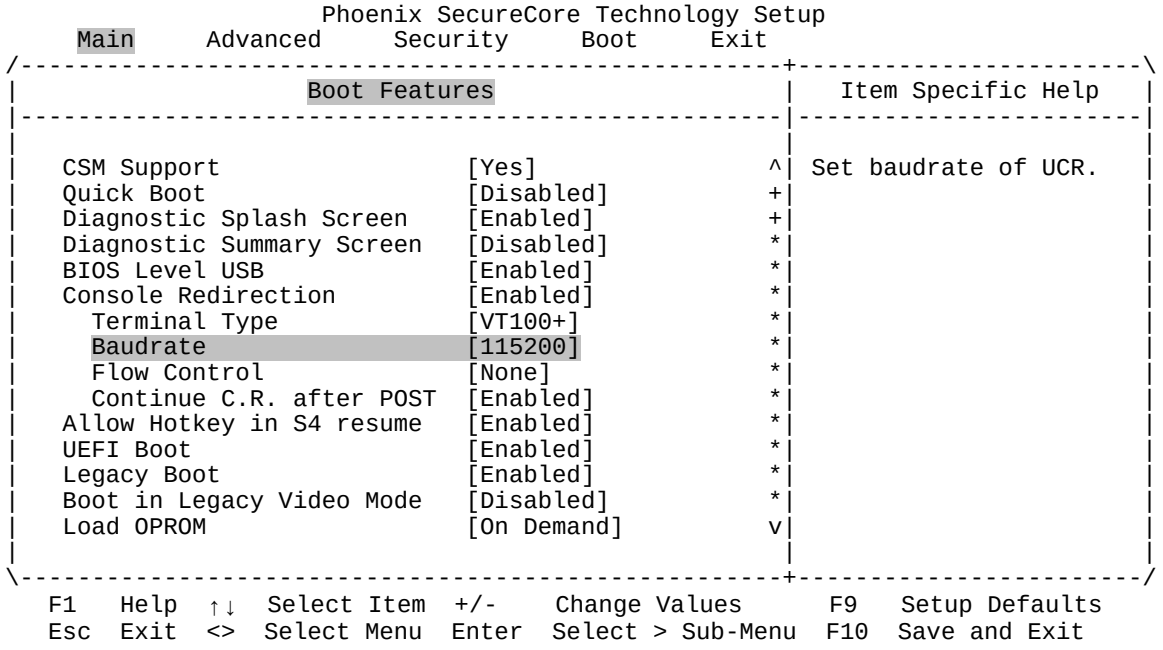
Options	**Disabled (default)**	Disables Universal Console Redirection (UCR)
	Enabled	Enables Universal Console Redirection (UCR). When enabled, four sub-menus appear for setting console redirection parameters.

Main → Boot Features → Console Redirection →Terminal Type



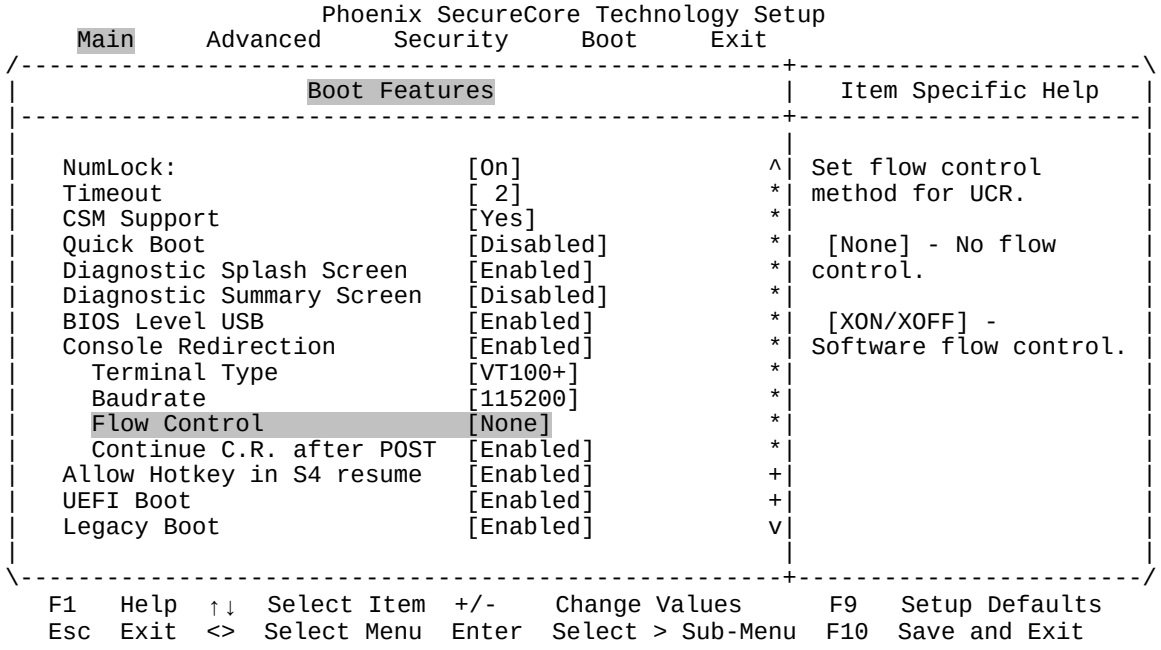
Options	ANSI	Sets terminal type to ANSI
	VT100	Sets terminal type to VT100
	VT100+ (default)	Sets terminal type to VT100+
	UTF8	Sets terminal type to UTF8

Main → Boot Features → Console Redirection →Baudrate



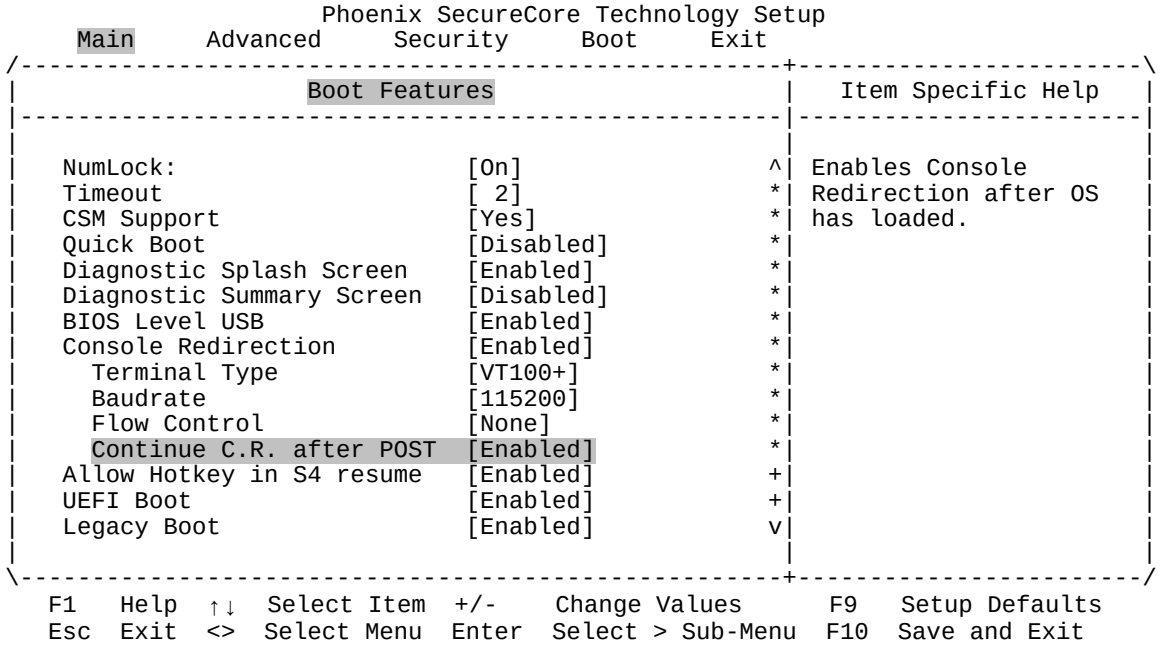
Options	19200	Sets baudrate to 19200
	38400	Sets baudrate to 38400
	57600	Sets baudrate to 57600
	115200 (default)	Sets baudrate to 115200

Main → Boot Features → Console Redirection →Flow Control



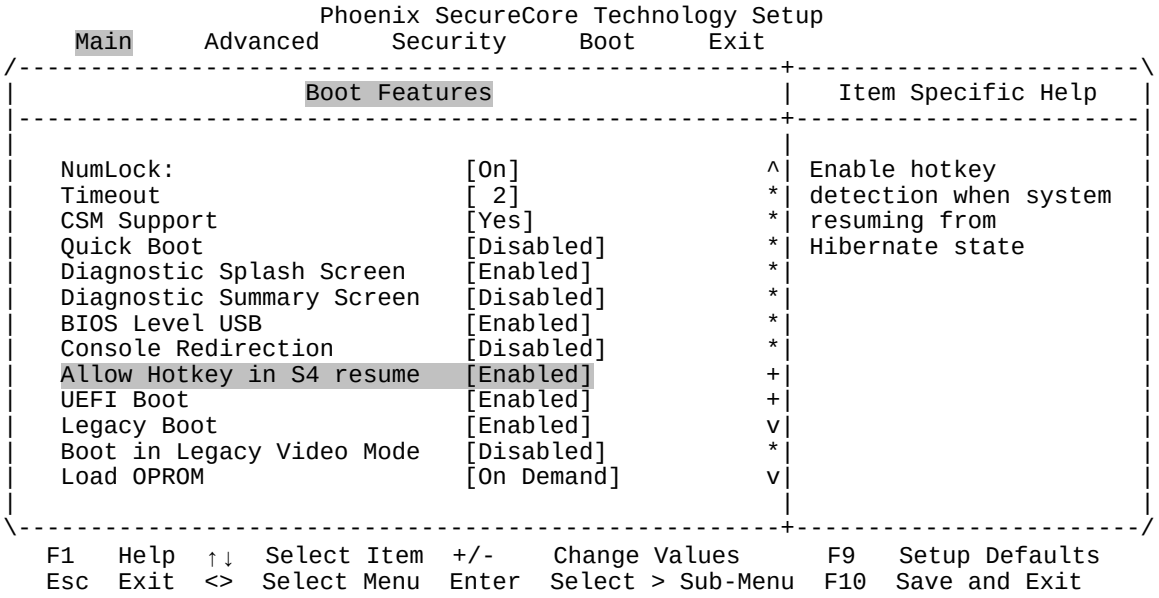
Options	**None (default)**	No flow control
	[XON/XOFF]	Software flow control

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



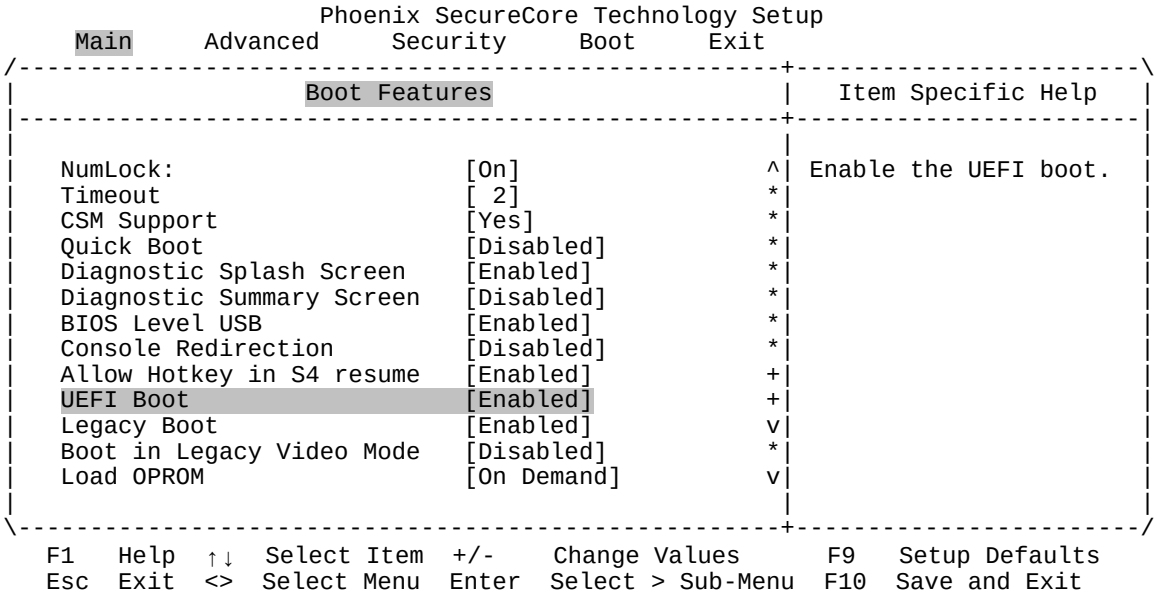
Options	Disabled	Disables console redirection after the operating system has loaded
	Enabled (default)	Enables console redirection after the operating system has loaded

Main → Boot Features → Allow Hotkey in S4 Resume



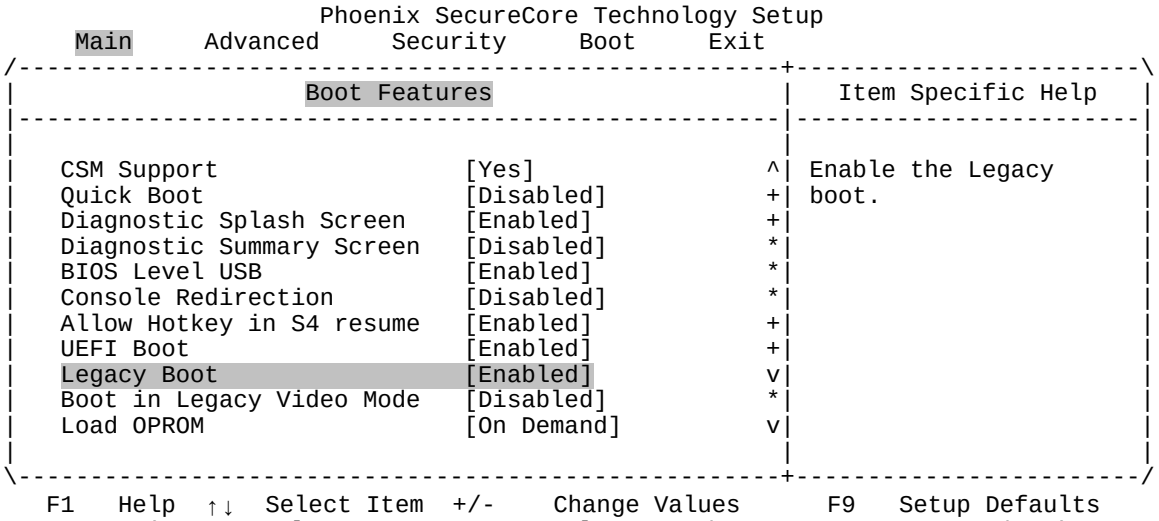
Options	Disabled	Disables Hotkey detection when system resumes from Hibernate state
	Enabled (default)	Enables Hotkey detection when system resumes from Hibernate state

Main → Boot Features → UEFI Boot



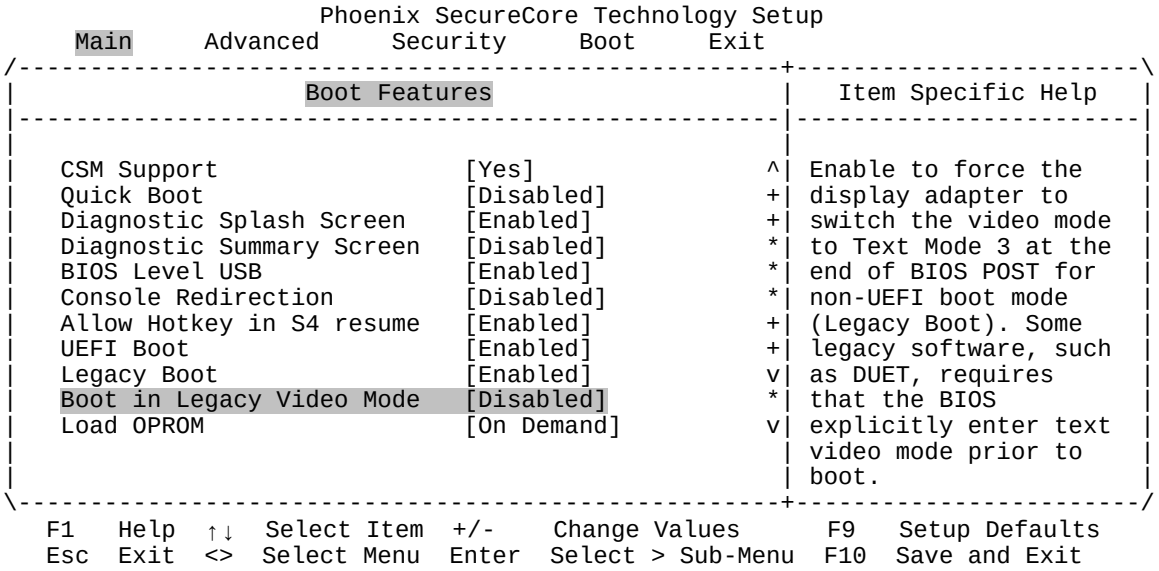
Options	Disabled	Disables Unified Extensible Firmware Interface (UEFI) boot
	Enabled (default)	Enables Unified Extensible Firmware Interface (UEFI) boot

Main → Boot Features → Legacy Boot



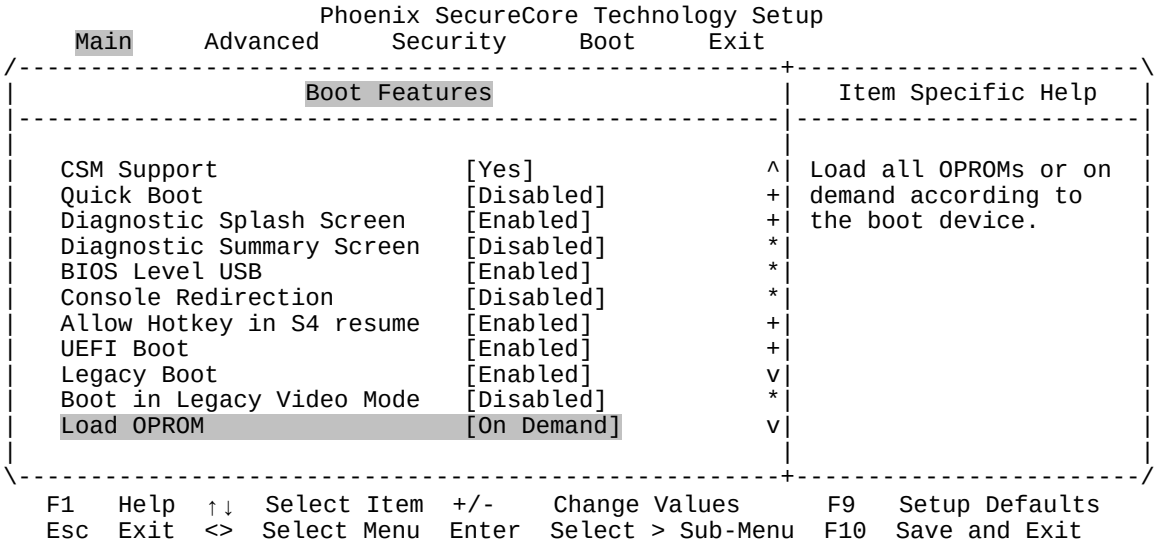
Options	Disabled	Disables Legacy boot
	Enabled (default)	Enables Legacy boot

Main → Boot Features → Boot In Legacy Video Mode



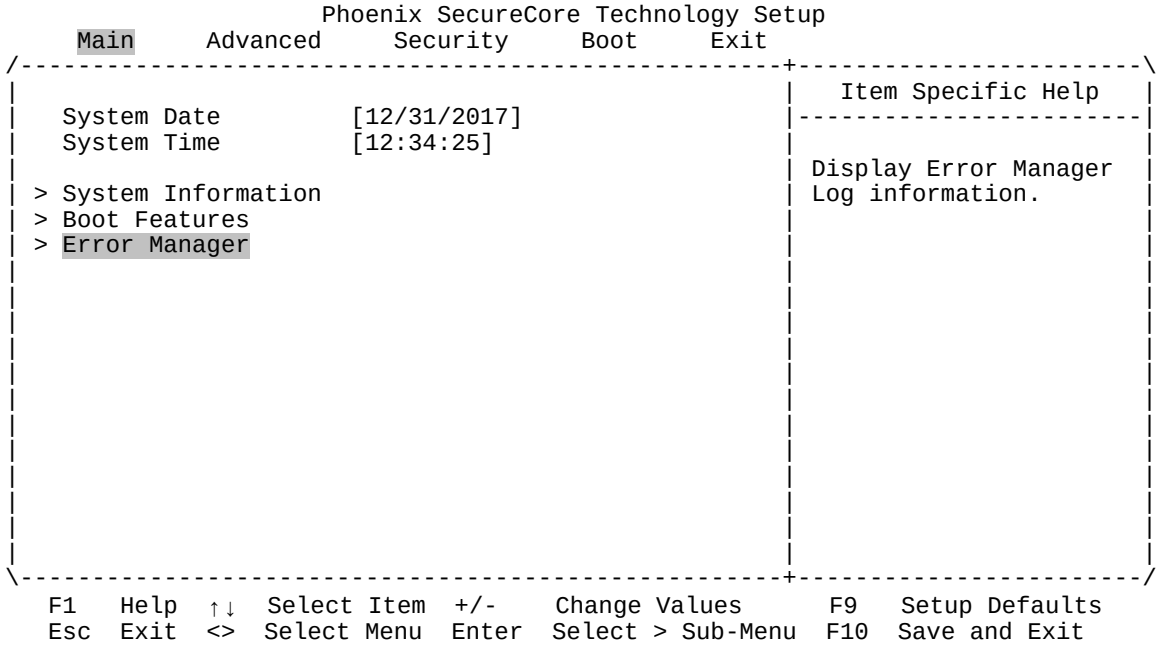
Options	**Disabled (default)**	Does not force a video mode switch to Text Mode 3.
	Enabled	Forces the display adapter to switch to Text Mode 3 at the end of BIOS POST for non-UEFI boot mode (that is, Legacy Boot).

Main → Boot Features → Load OPROM

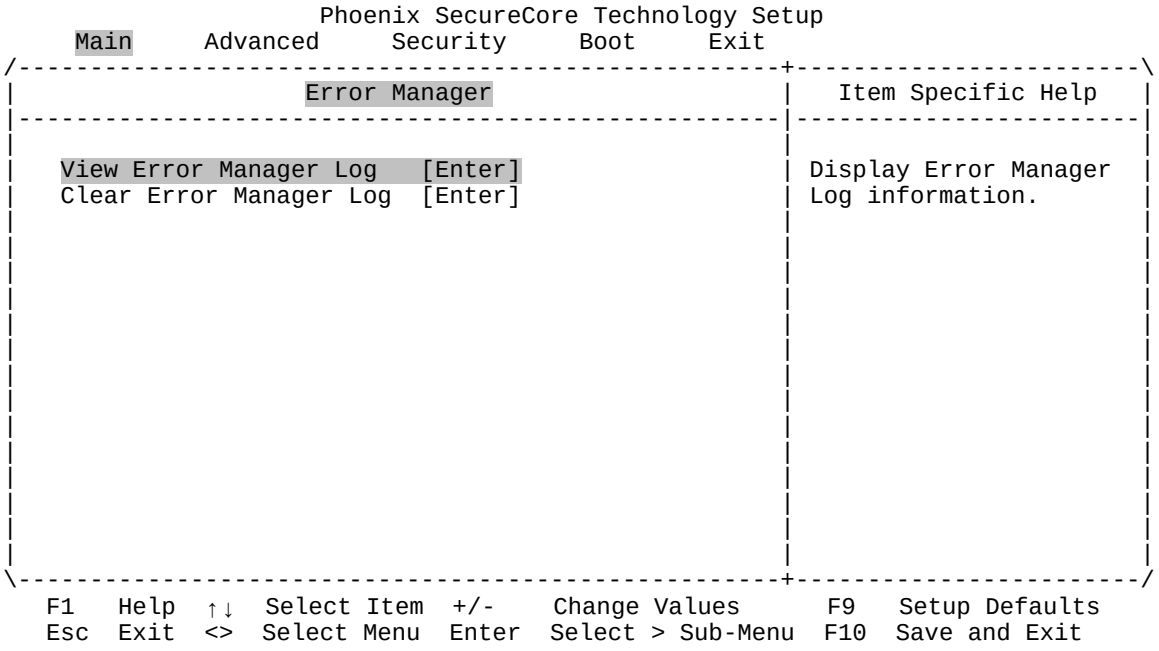


Options	All	Load all option ROMs.
	On Demand (default)	Load option ROMs (OPROMs) on demand according to the requirements of the boot device.

Main → Error Manager

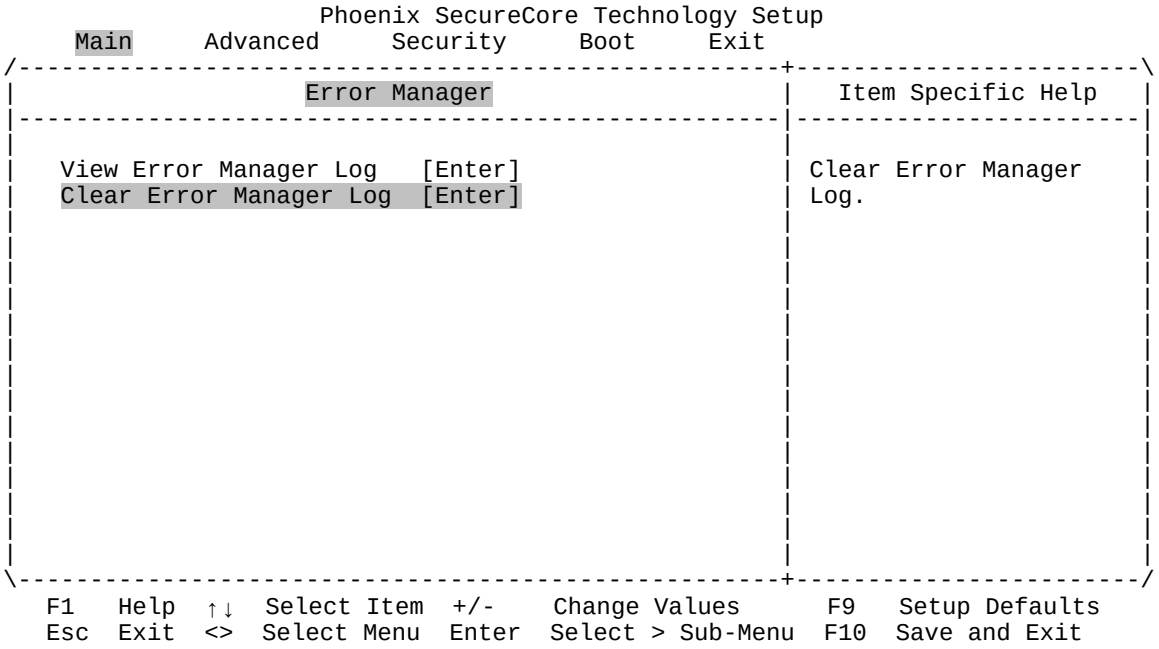


Main → Error Manager → View Error Manager Log



Press Enter to view the Error Manager Log information.

Main → Error Manager → Clear Error Manager Log



Press Enter to clear the Error Manager Log information.

Advanced Menu

3

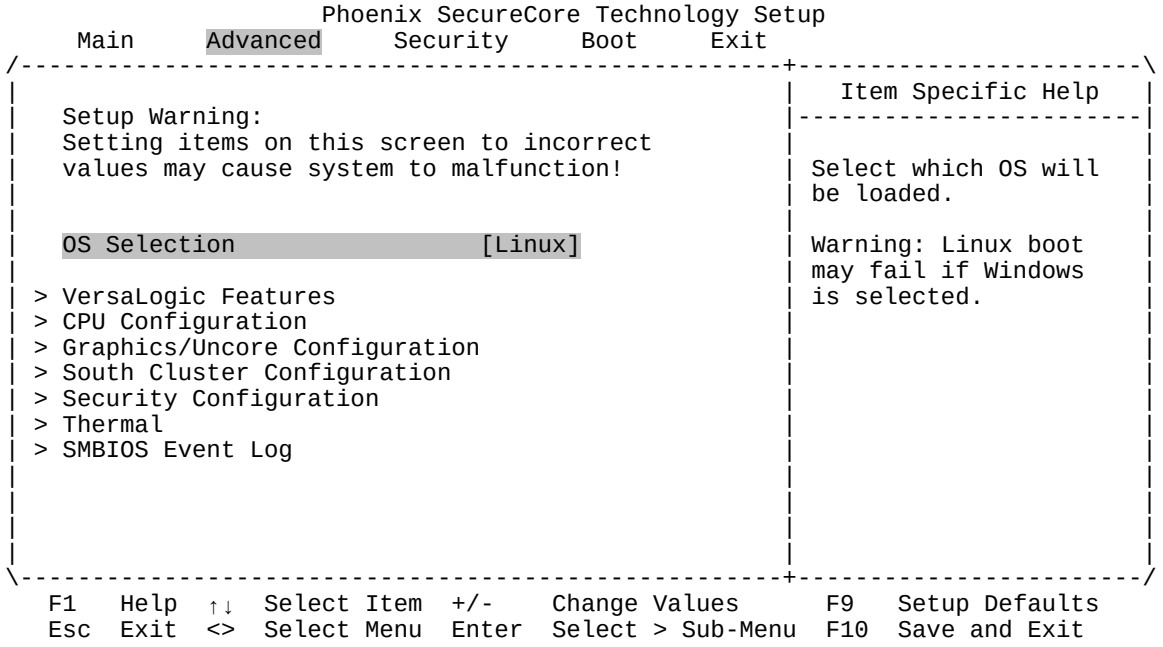
The Advanced menu enables you to:

- 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:

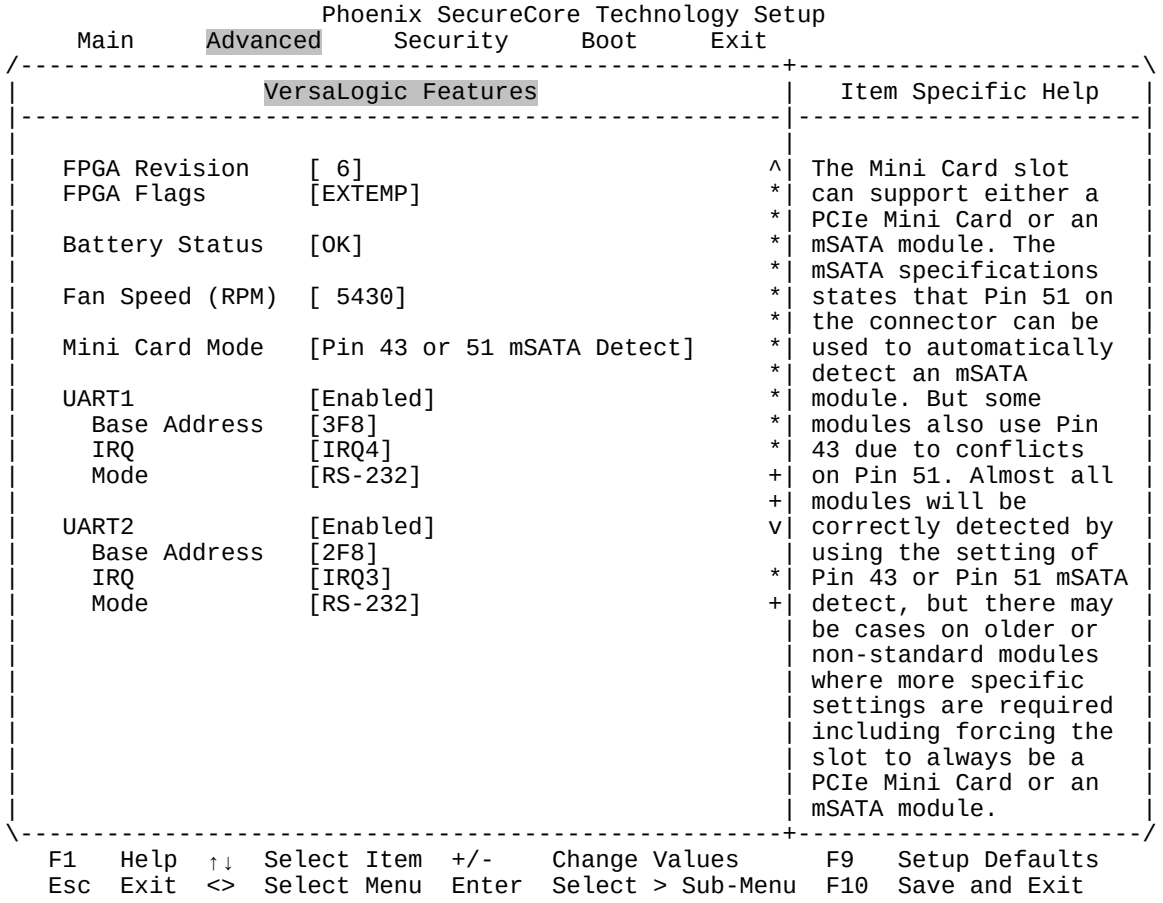
```
                    Phoenix SecureCore Technology Setup
     Main     Advanced     Security     Boot     Exit
/-------------------------------------------------------+-------------------------\
|                                                       |   Item Specific Help    |
|   Setup Warning:                                      |-------------------------|
|   Setting items on this screen to incorrect           |                         |
|   values may cause system to malfunction!             | Select which OS will    |
|                                                       | be loaded.              |
|                                                       |                         |
|   OS Selection                   [Linux]              | Warning: Linux boot     |
|                                                       | may fail if Windows     |
| > VersaLogic Features                                 | is selected.            |
| > CPU Configuration                                   |                         |
| > Graphics/Uncore Configuration                       |                         |
| > South Cluster Configuration                         |                         |
| > Security Configuration                              |                         |
| > Thermal                                             |                         |
| > SMBIOS Event Log                                    |                         |
|                                                       |                         |
|                                                       |                         |
|                                                       |                         |
|                                                       |                         |
\-------------------------------------------------------+-------------------------/
   F1   Help  ↑↓  Select Item  +/-    Change Values      F9   Setup Defaults
   Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit
```

Advanced → OS Selection



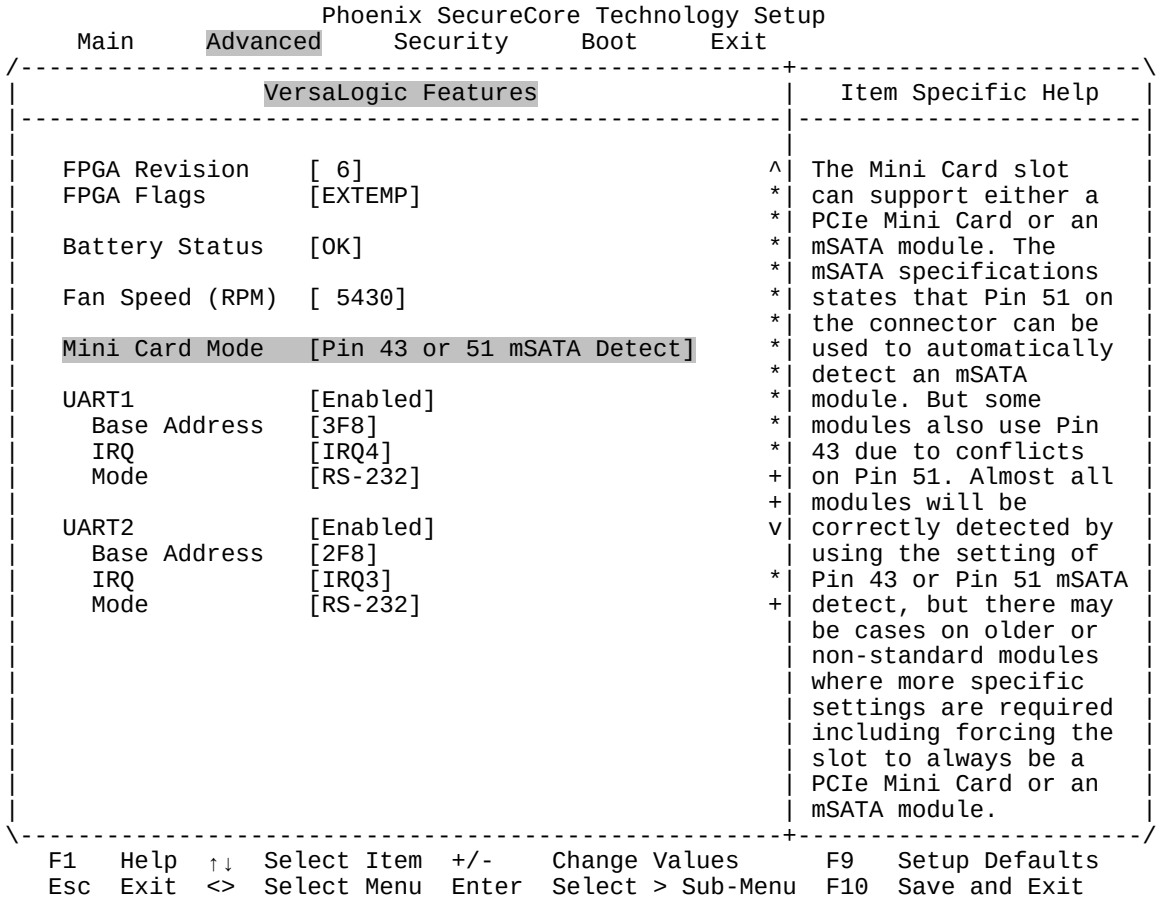
Options	Windows	Selects Microsoft Windows as the boot operating system [Assumes boot device contains a Microsoft Windows operating system.]
	Linux (default)	Selects Linux as the boot operating system [Assumes boot device contains a Linux operating system.]

Advanced → VersaLogic Features



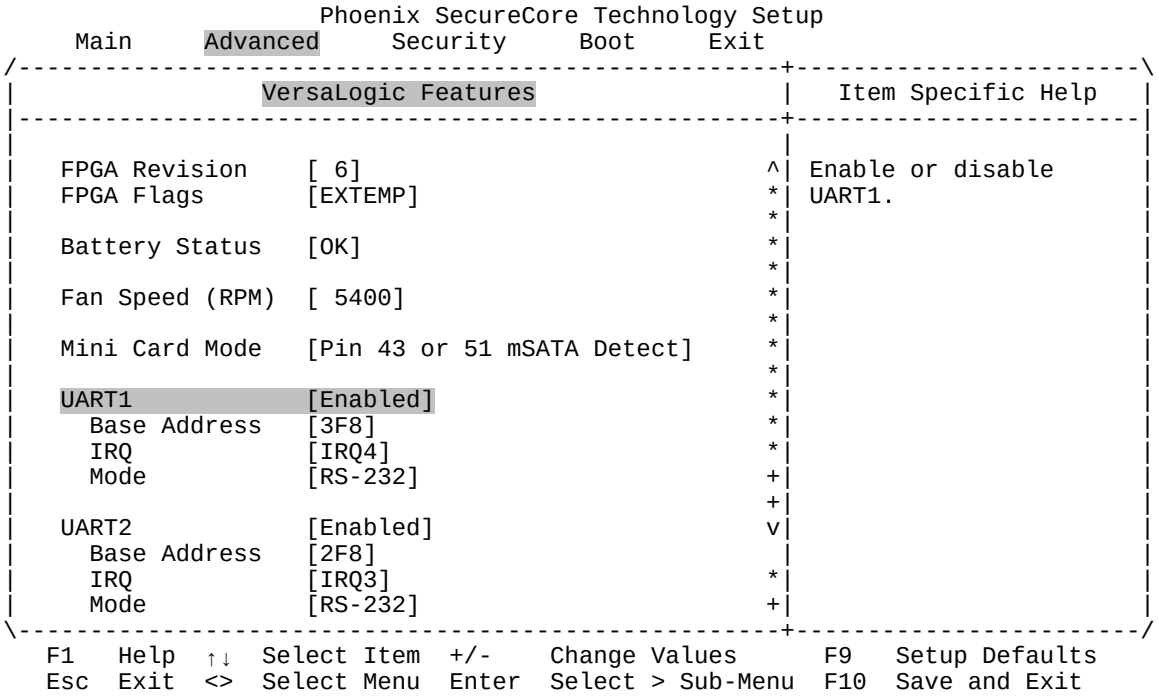
This screen provides information on the FPGA, battery status, and fan speed.

Advanced → VersaLogic Features → Mini Card Mode



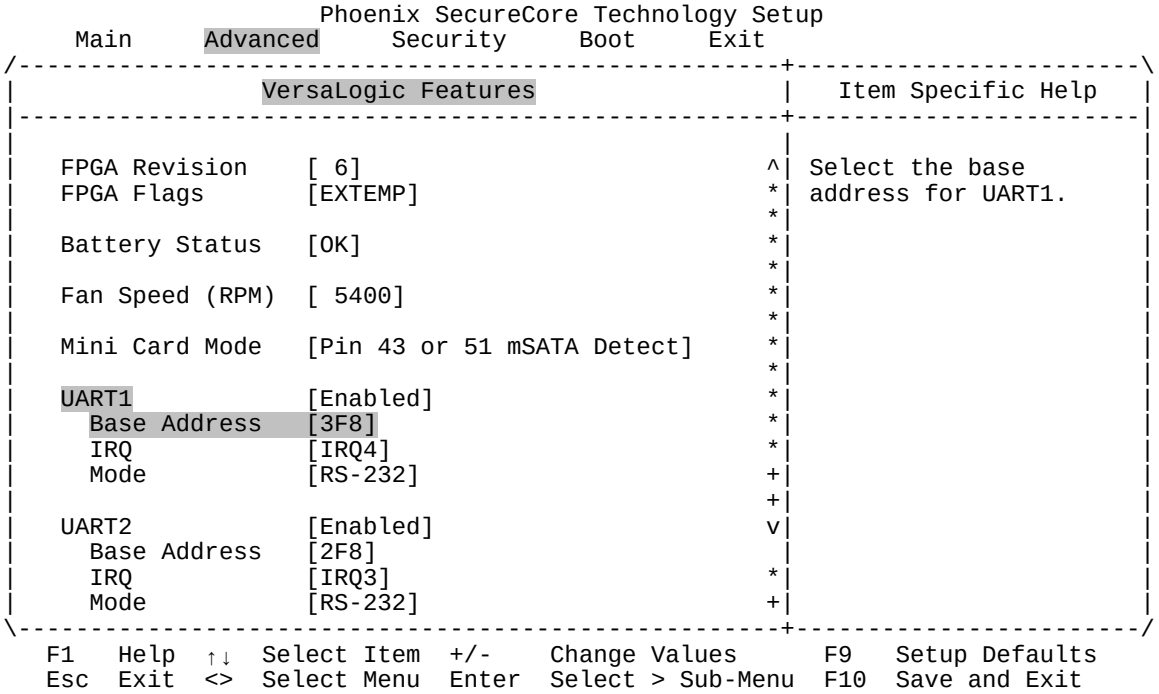
Options	**Pin 43 or 51 mSATA Detect (default)**
	Pin 43 mSATA Detect
	Pin 51 mSATA Detect
	Force PCIe Mini Card Mode
	Force mSATA SSD Mode

Advanced → VersaLogic Features → UART1



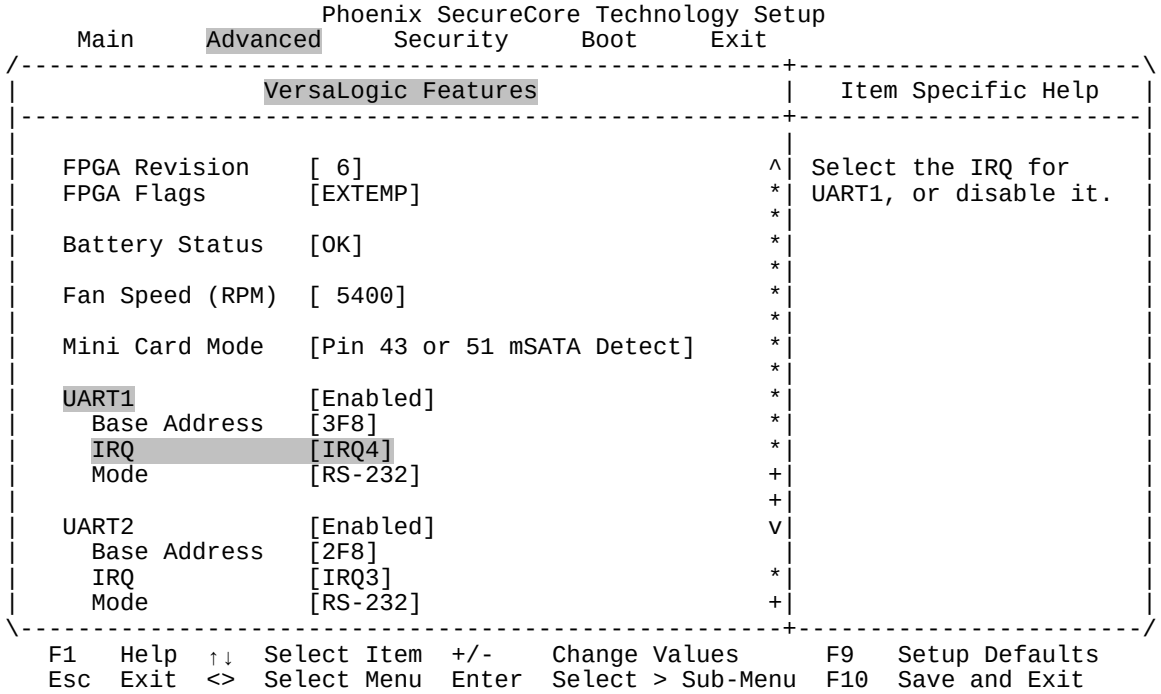
Options	Disabled	Disables UART1
	Enabled (default)	Enables UART1

Advanced → VersaLogic Features → UART1 → Base Address



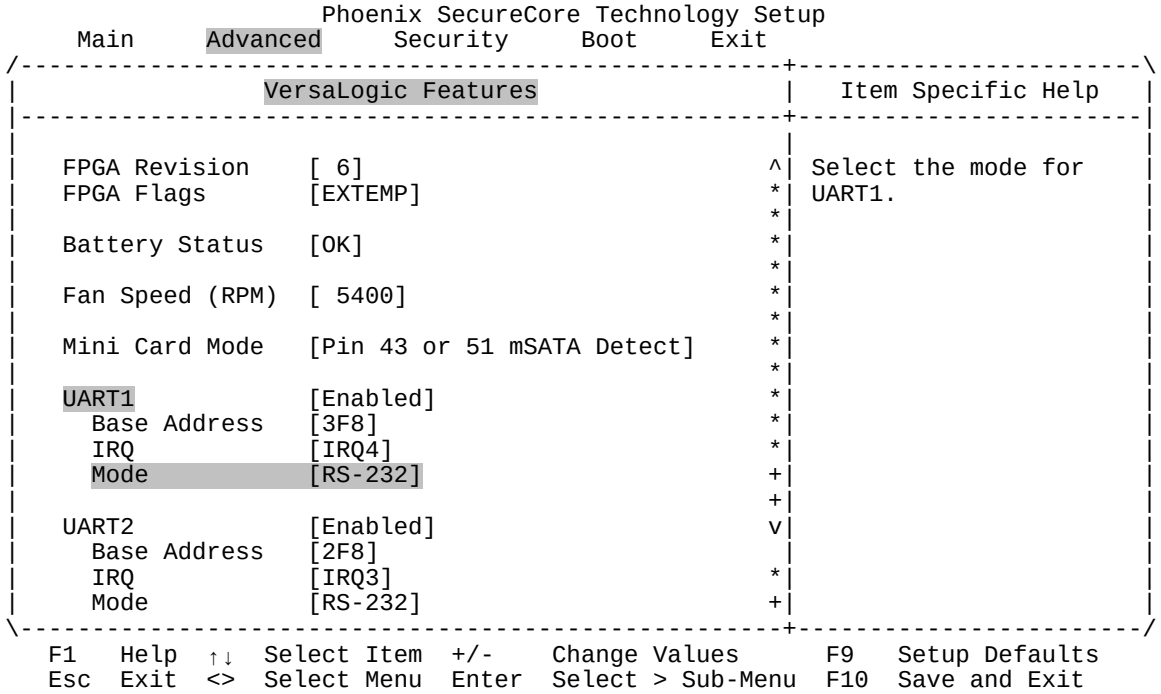
Options
3F8 (default)
2F8
3E8
2E8
200
208
220
228
238
338

Advanced → VersaLogic Features → UART1 → IRQ



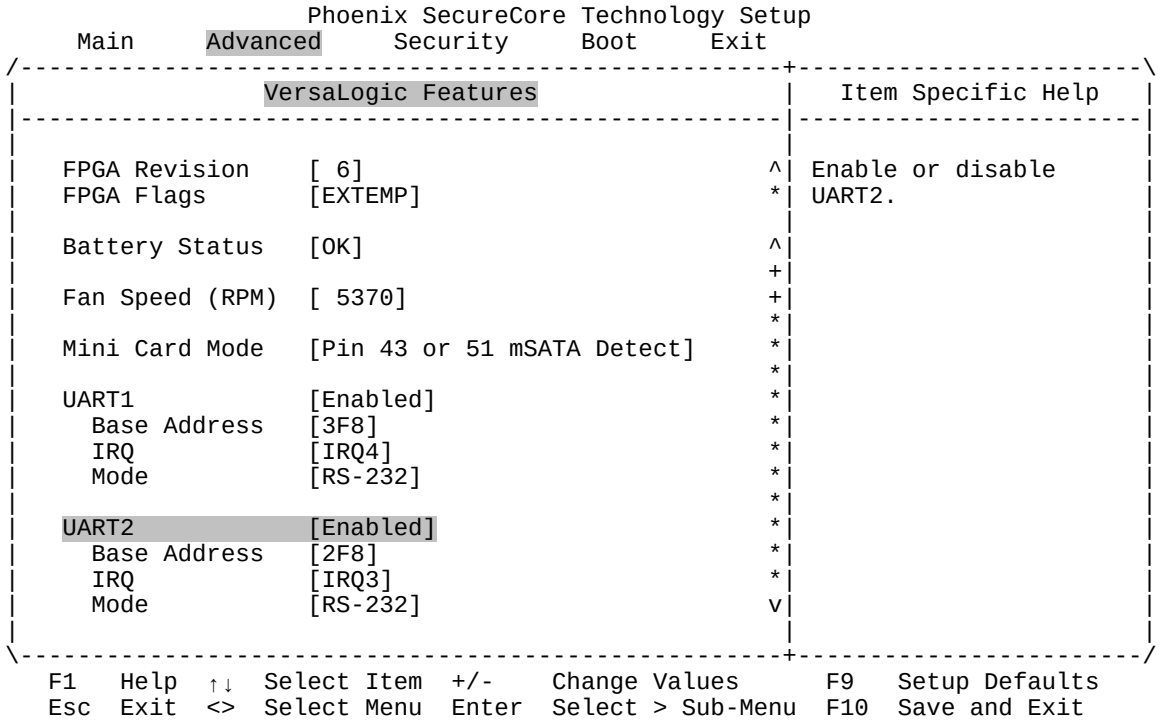
Options
Disabled
IRQ3
IRQ4 (default)
IRQ5
IRQ10
IRQ6
IRQ7
IRQ9
IRQ11

Advanced → VersaLogic Features → UART1 → Mode



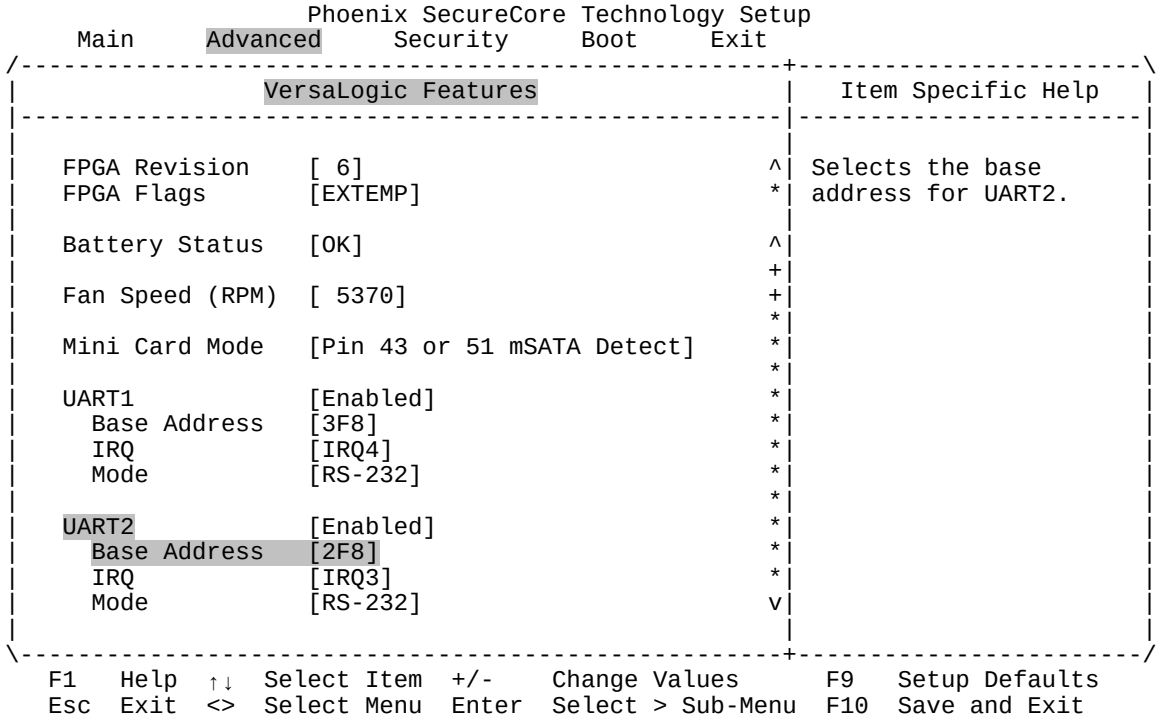
Options	**RS-232 (default)**
	RS-422
	RS-485 (Manual Direction Control)
	RS-485 (Automatic Direction Control)

Advanced → VersaLogic Features → UART2



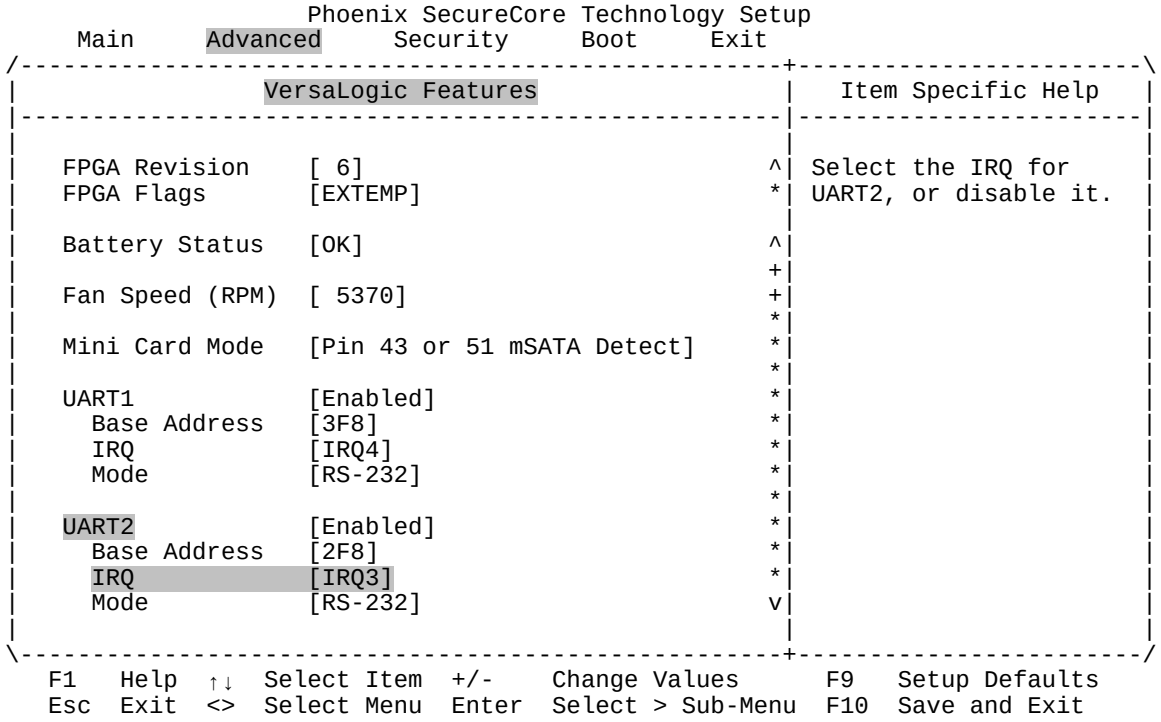
Options	Disabled	Disables UART2
	Enabled (default)	Enables UART2

Advanced → VersaLogic Features → UART2 → Base Address



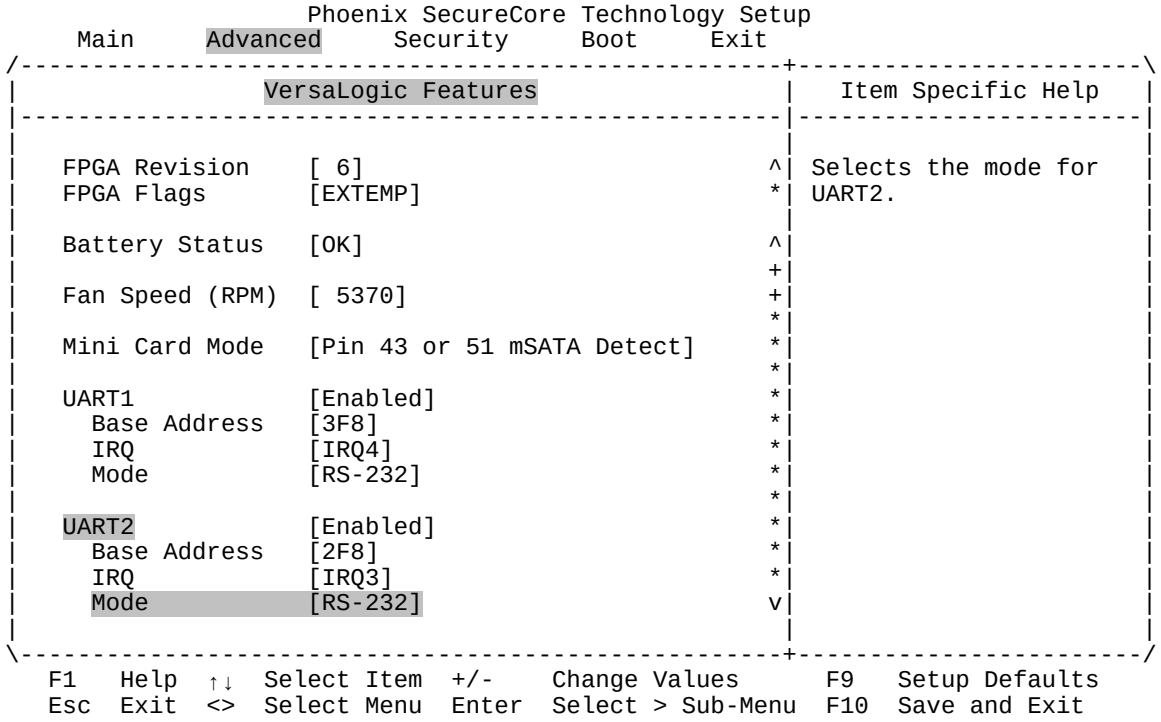
Options
3F8
2F8 (default)
3E8
2E8
200
208
220
228
238
338

Advanced → VersaLogic Features → UART2 → IRQ



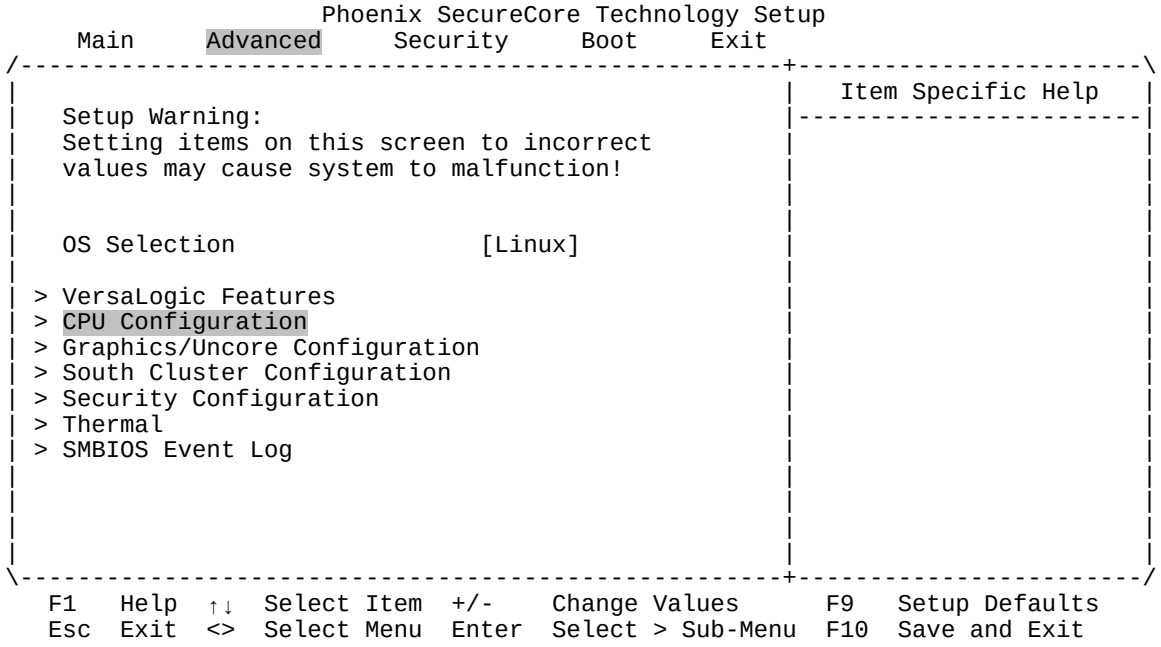
Options	Disabled
	IRQ3 (default)
	IRQ4
	IRQ5
	IRQ10
	IRQ6
	IRQ7
	IRQ9
	IRQ11

Advanced → VersaLogic Features → UART2 → Mode



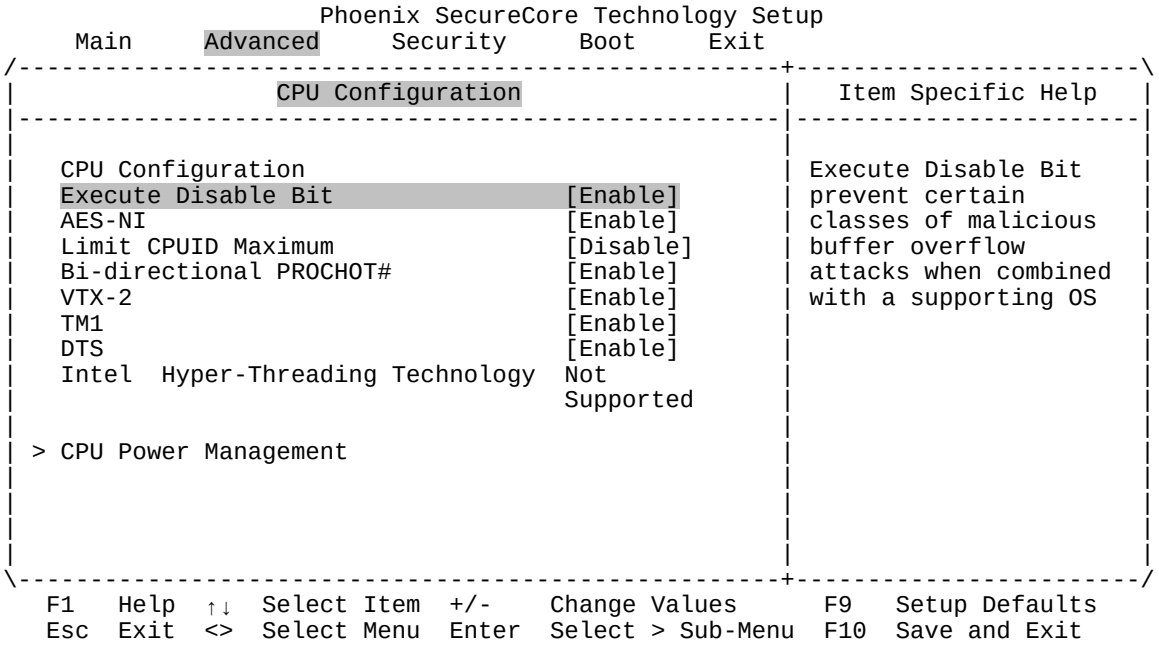
Options	**RS-232 (default)**
	RS-422
	RS-485 (Manual Direction Control)
	RS-485 (Automatic Direction Control)

Advanced → CPU Configuration



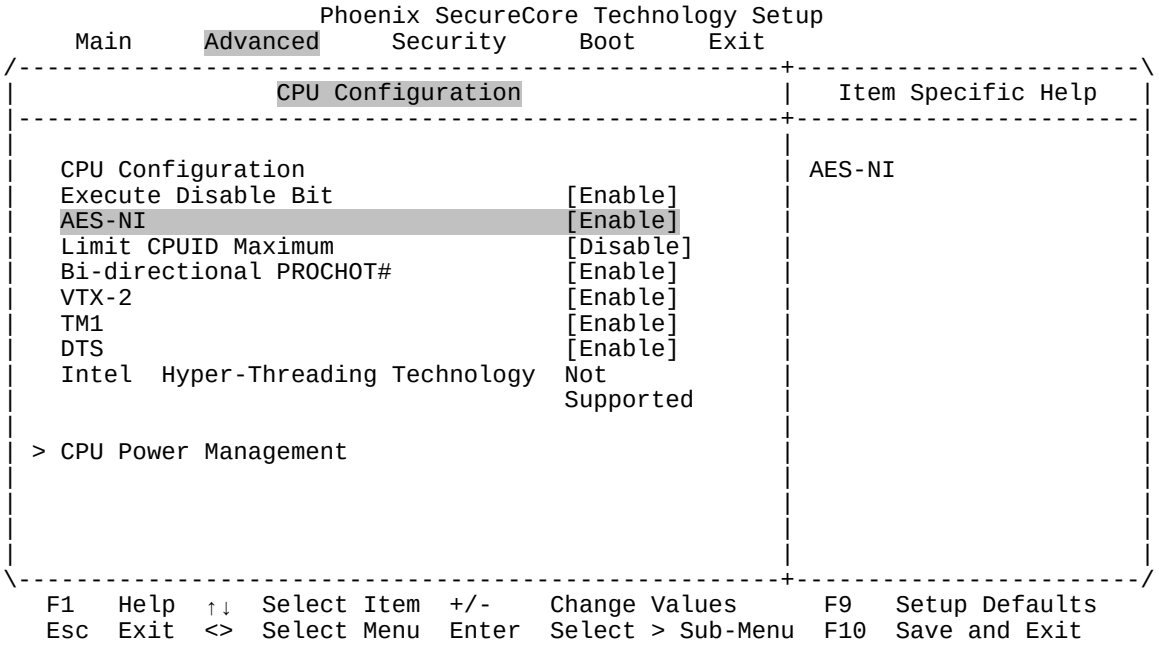
This is the top-level screen for the CPU Configuration menu.

Advanced → CPU Configuration → Execute Disable Bit



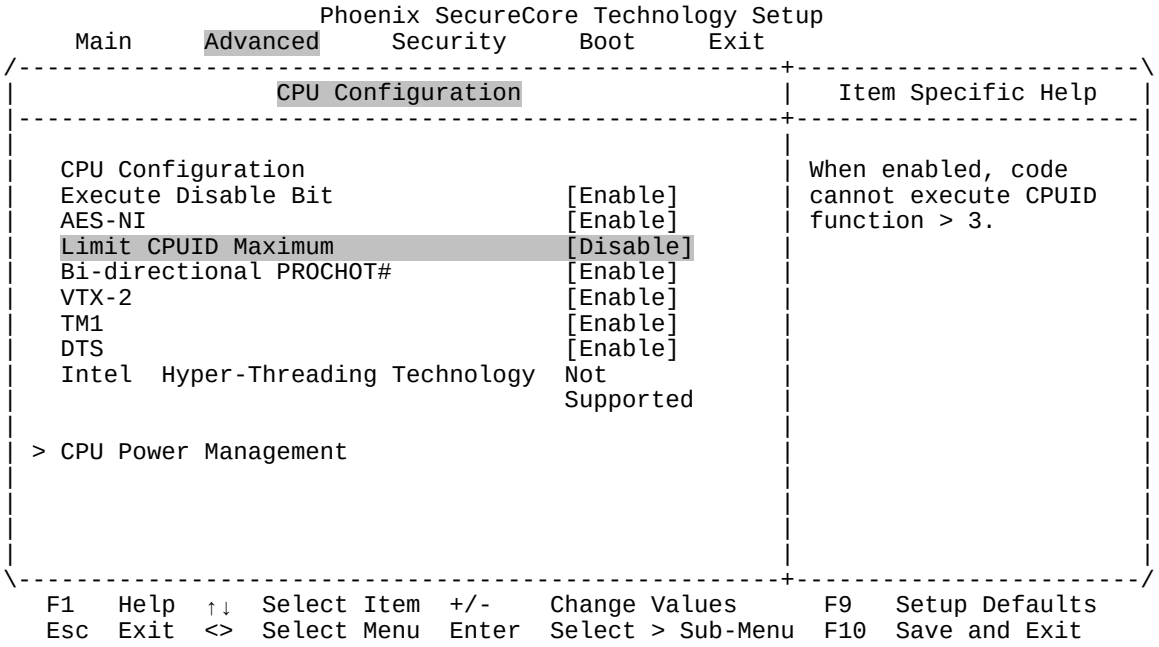
Options	Disable
	Enable (default)

Advanced → CPU Configuration → AES-NI



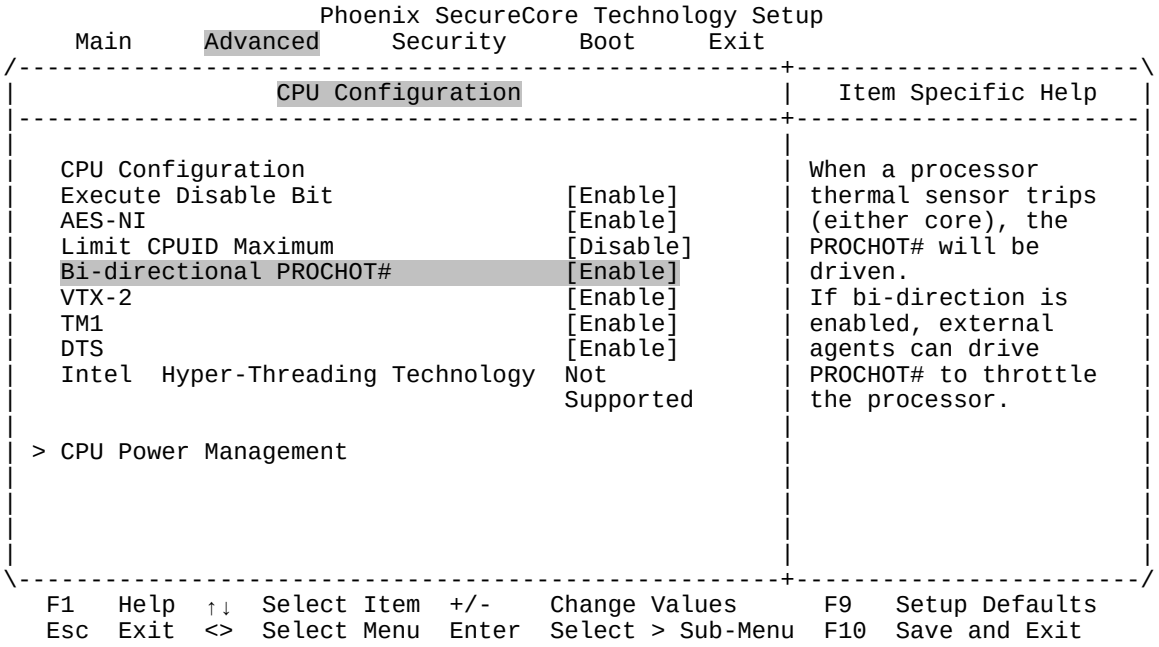
Options	Disable	Disables Advanced Encryption Standard New Instructions **(**AES-NI)
	Enable (default)	Enables Advanced Encryption Standard New Instructions **(**AES-NI)

Advanced → CPU Configuration → Limit CPUID Maximum



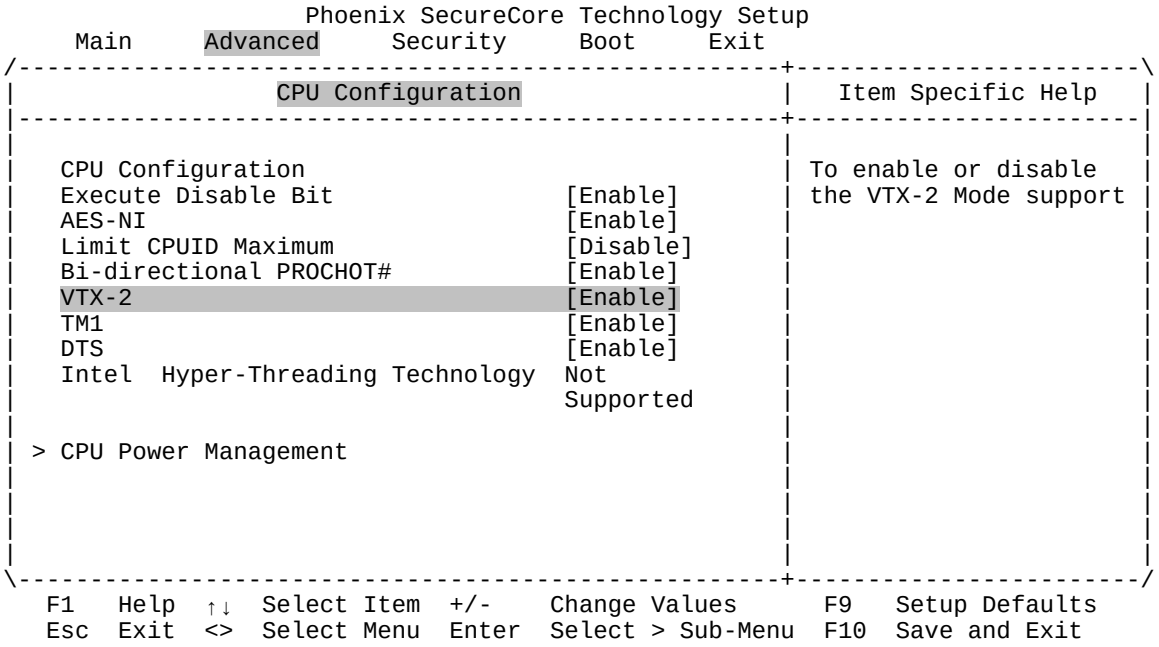
Options	**Disable (default)**
	Enable

Advanced → CPU Configuration → Bi-directional PROCHOT#



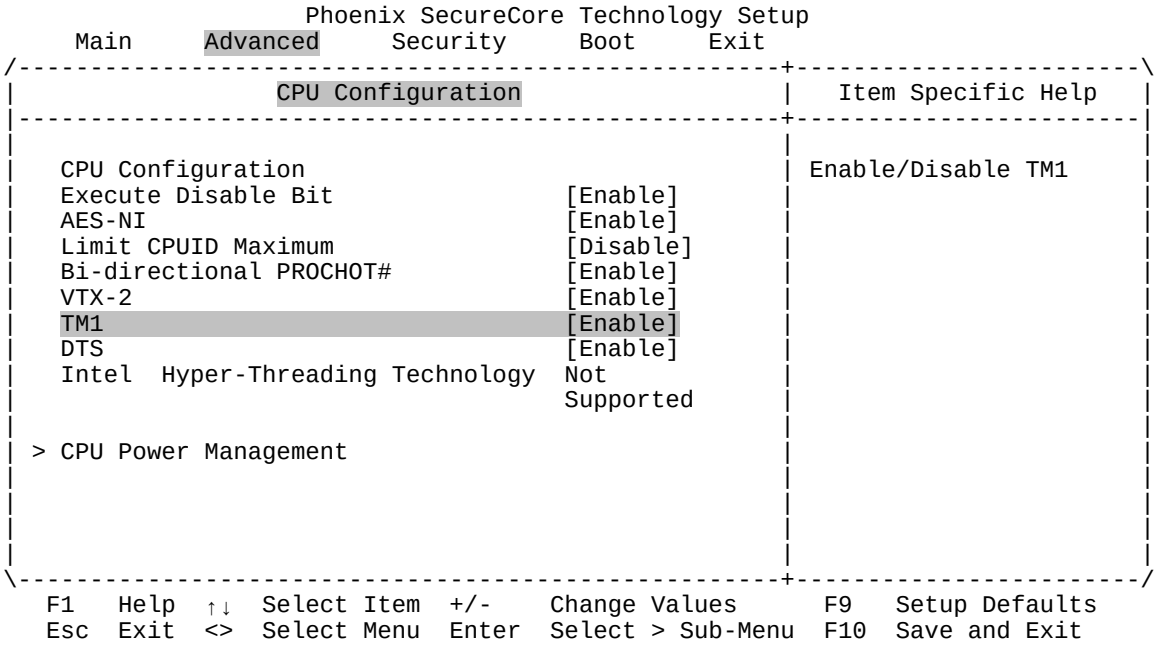
Options	Disable
	Enable (default)

Advanced → CPU Configuration → VTX-2



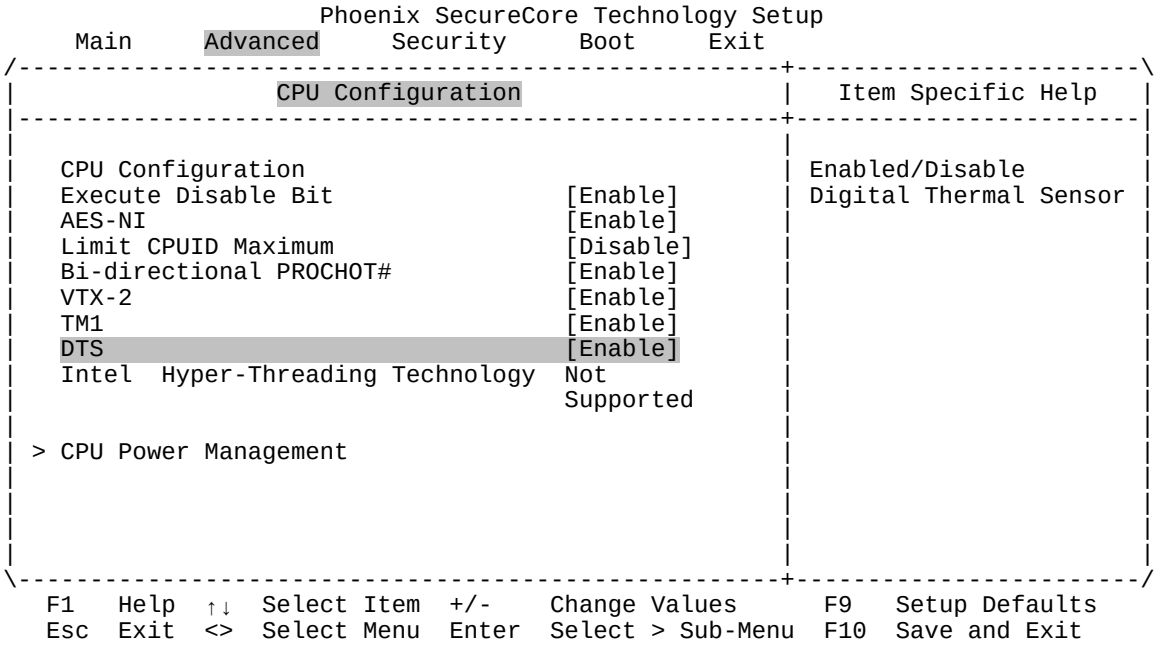
Options	Disable	Disables VTX-2 virtualization technology
	Enable (default)	Enables VTX-2 virtualization technology

Advanced → CPU Configuration → TM1



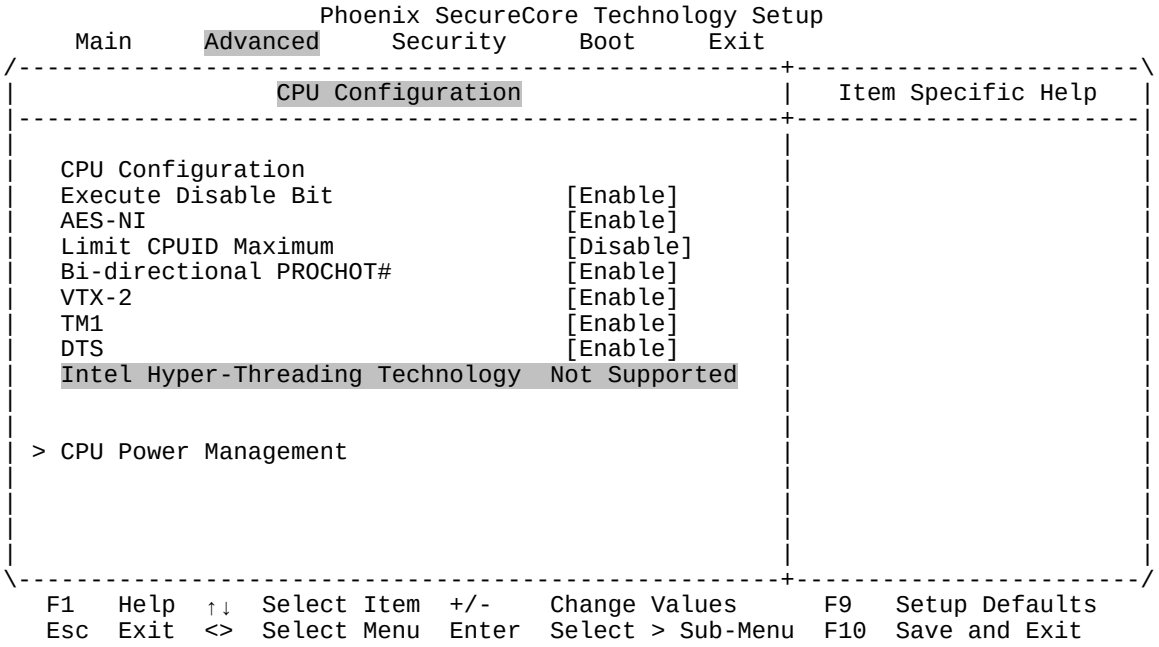
Options	Disable	Disables Thermal Monitor 1
	Enable (default)	Enables Thermal Monitor 1

Advanced → CPU Configuration → DTS



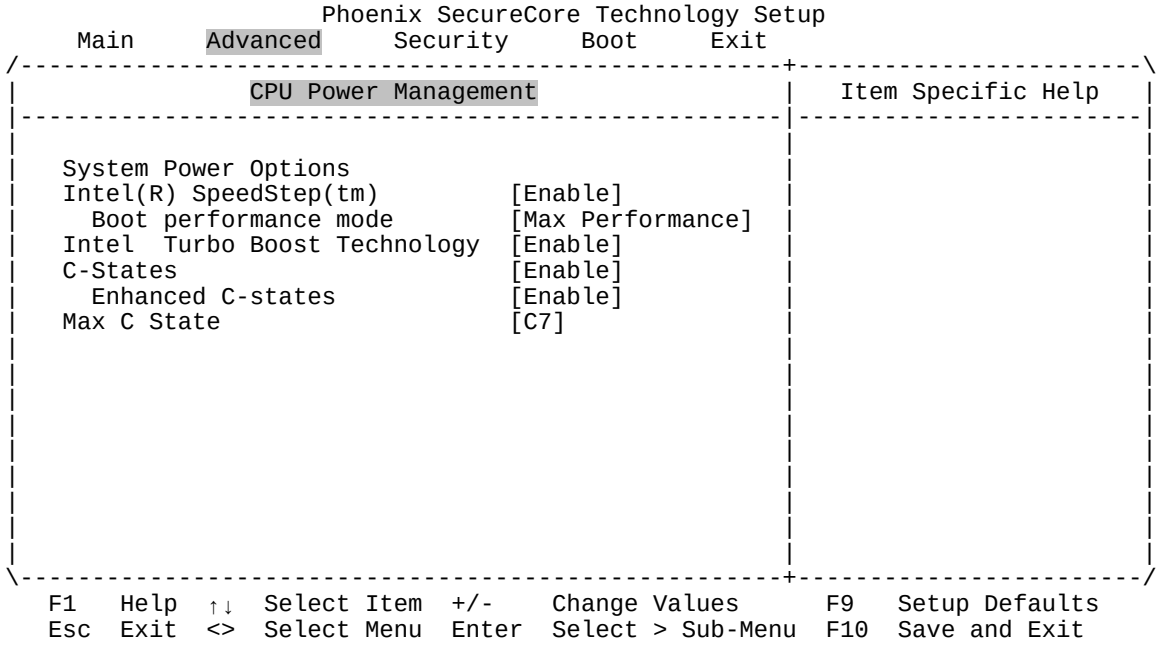
Options	Disable	Disables Digital Thermal Sensor
	Enable (default)	Enables Digital Thermal Sensor

Advanced → CPU Configuration → Intel Hyper-Threading Technology



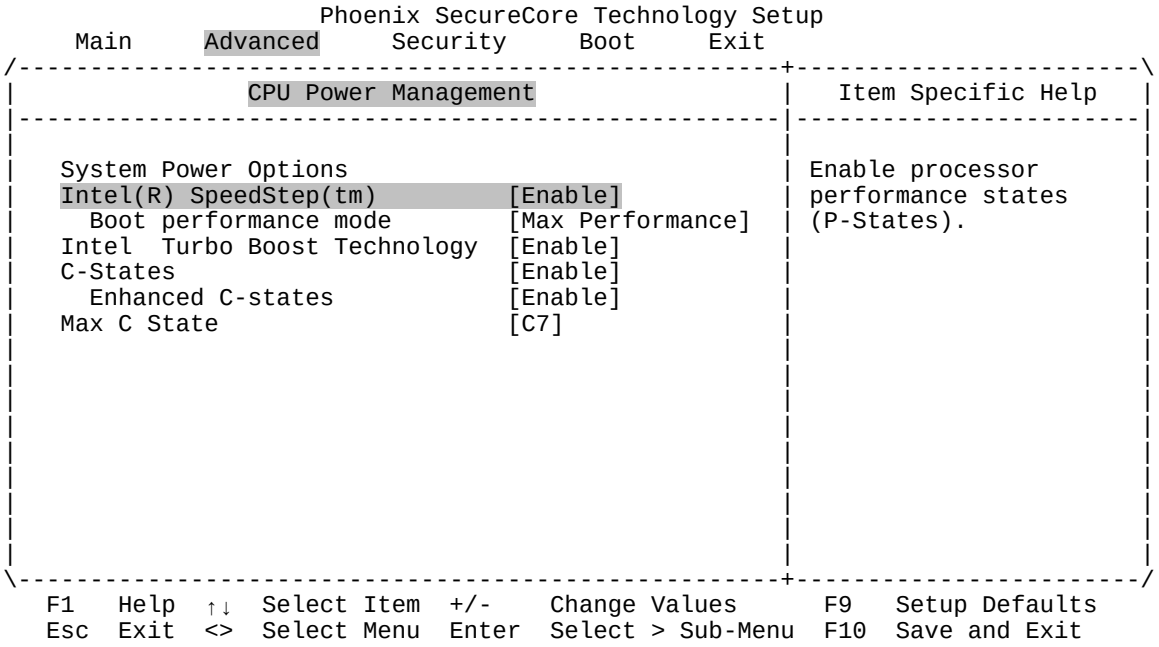
Note: This feature is not supported at this time.

Advanced → CPU Power Management



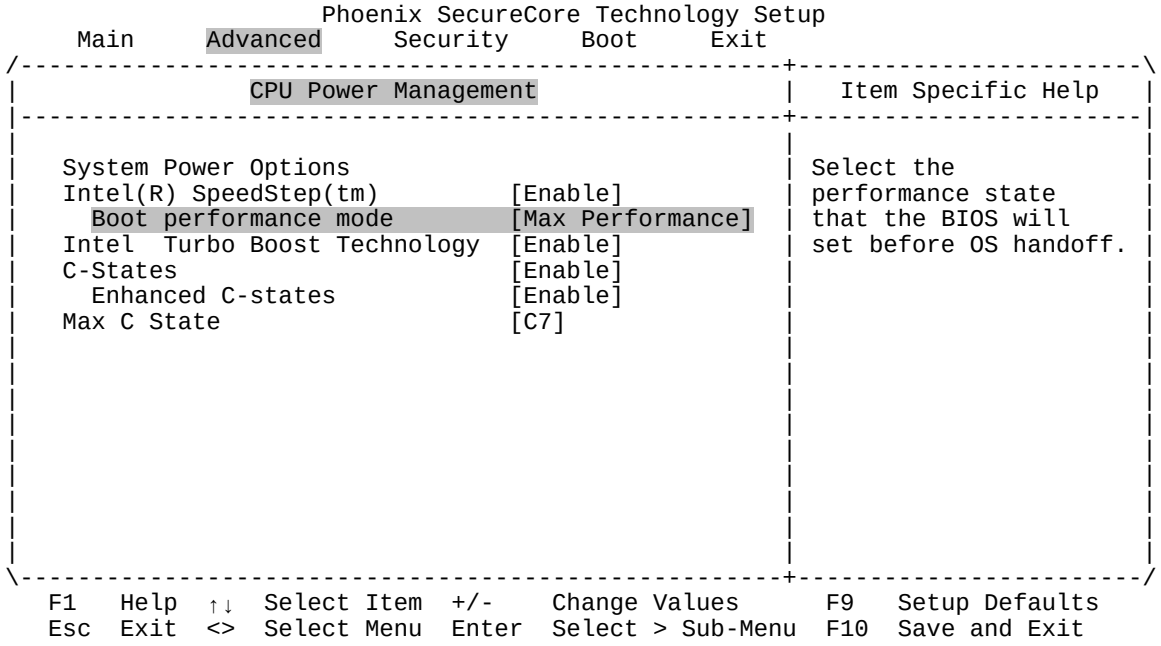
This is the top-level screen of the CPU Power Management menu.

Advanced → CPU Power Management → Intel SpeedStep



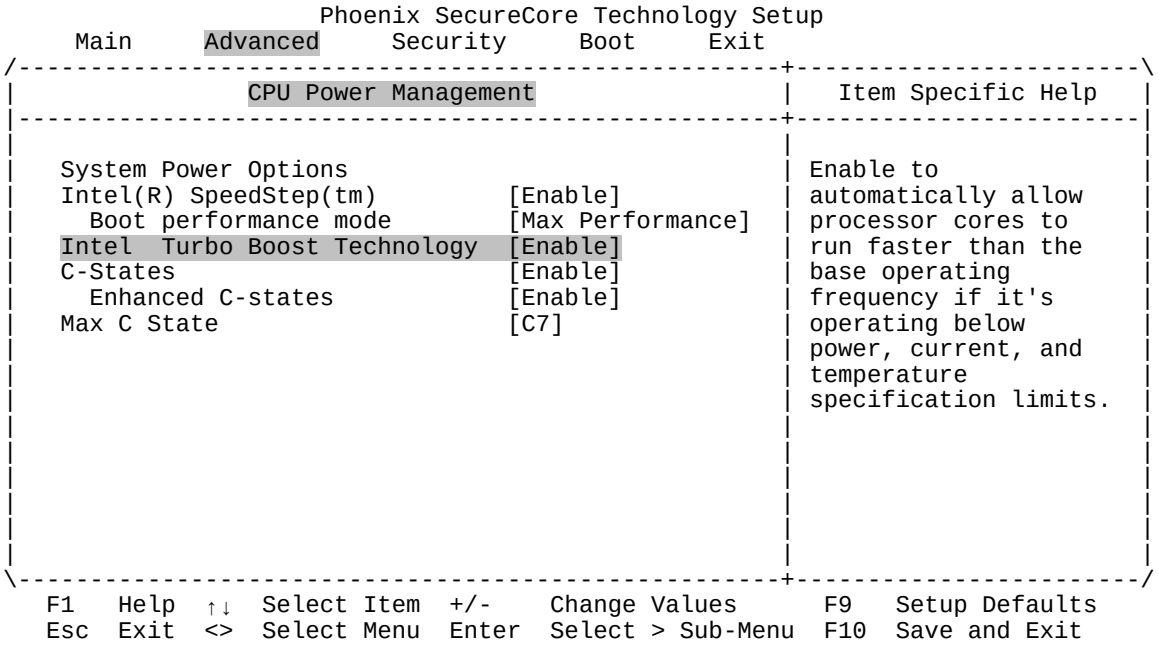
Options	Disable
	Enable (default)

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



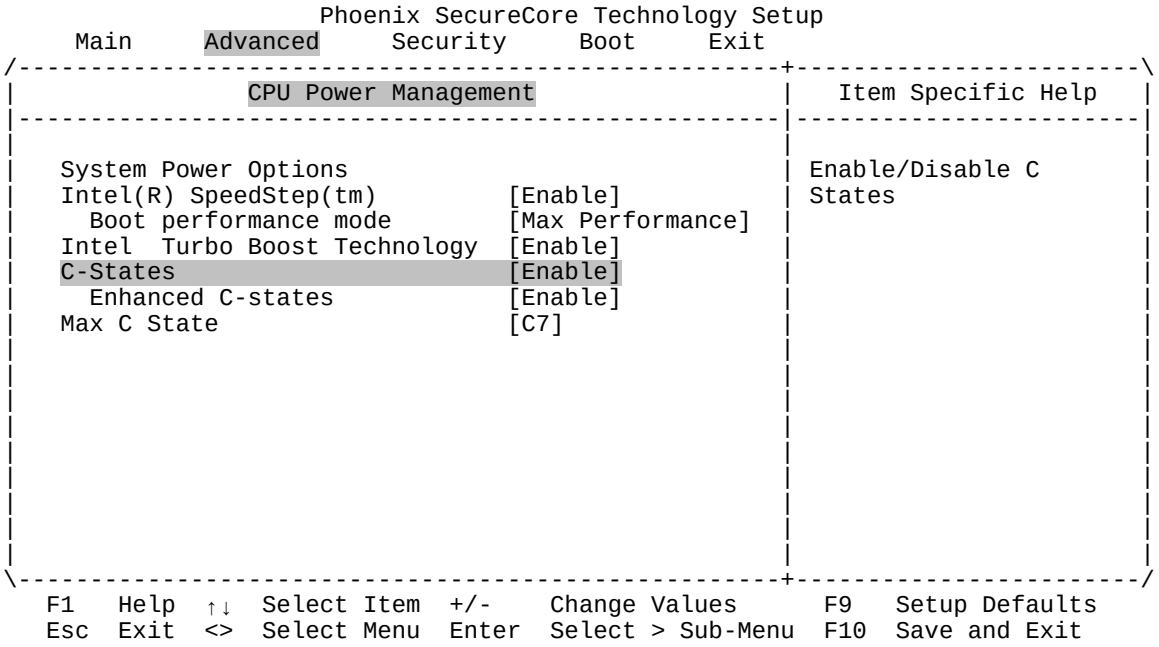
Options	**Max Performance (default)**
	Max Battery

Advanced → CPU Power Management → Intel Turbo Boost Technology



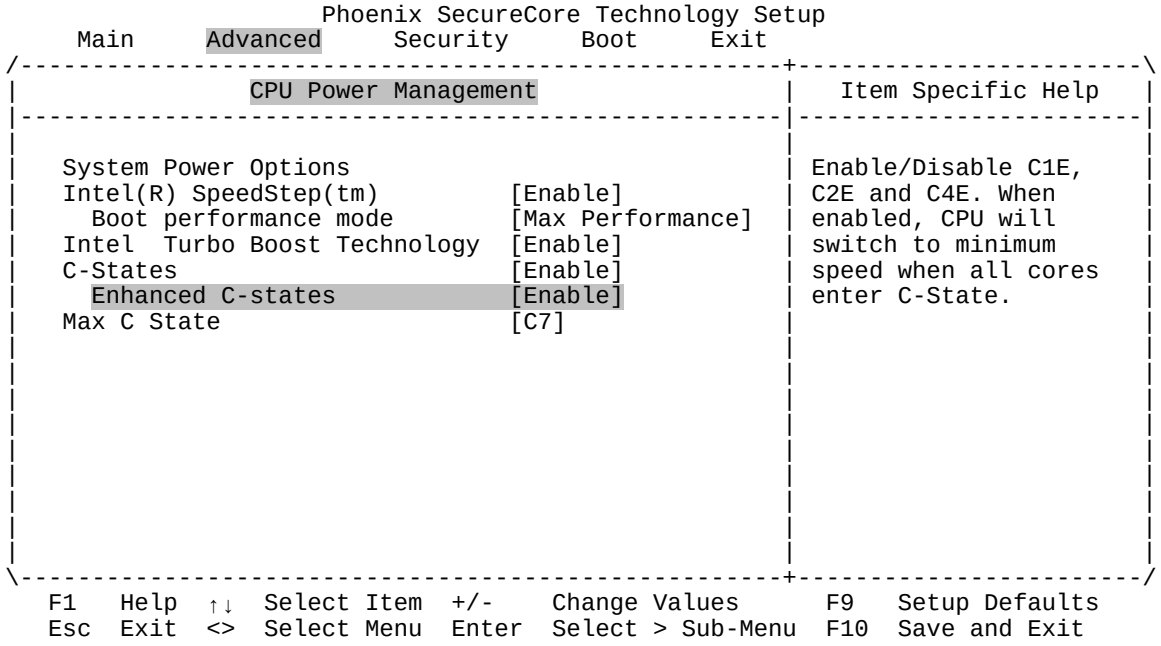
Options	Disable
	Enable (default)

Advanced → CPU Power Management → C-States



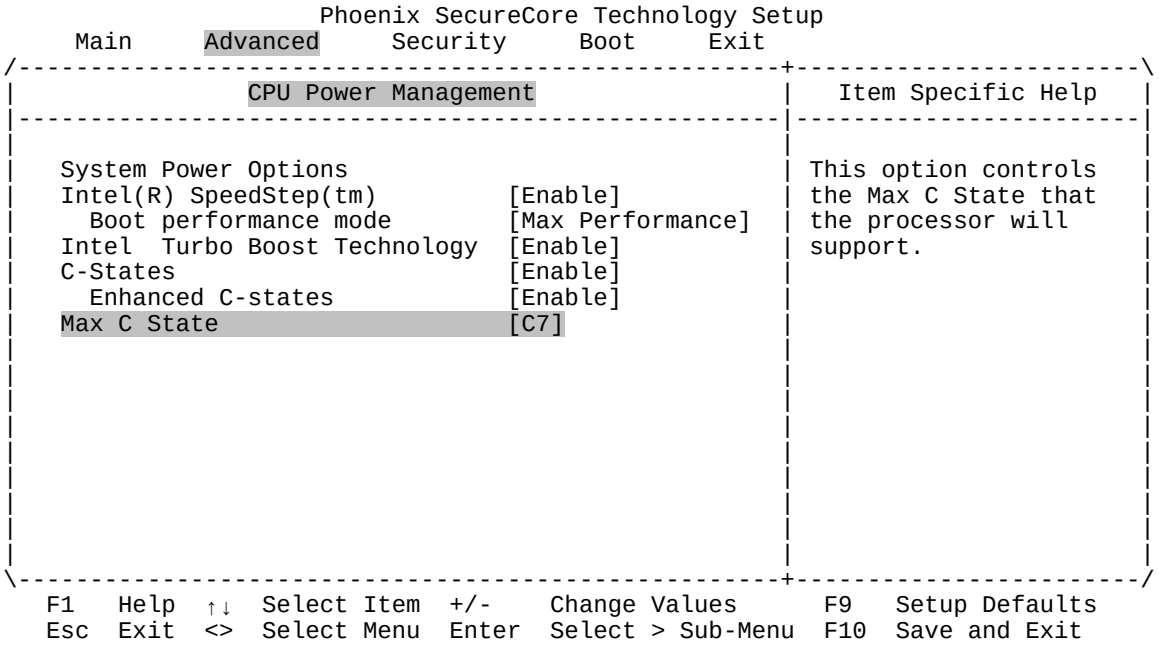
Options	Disable
	Enable (default)

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



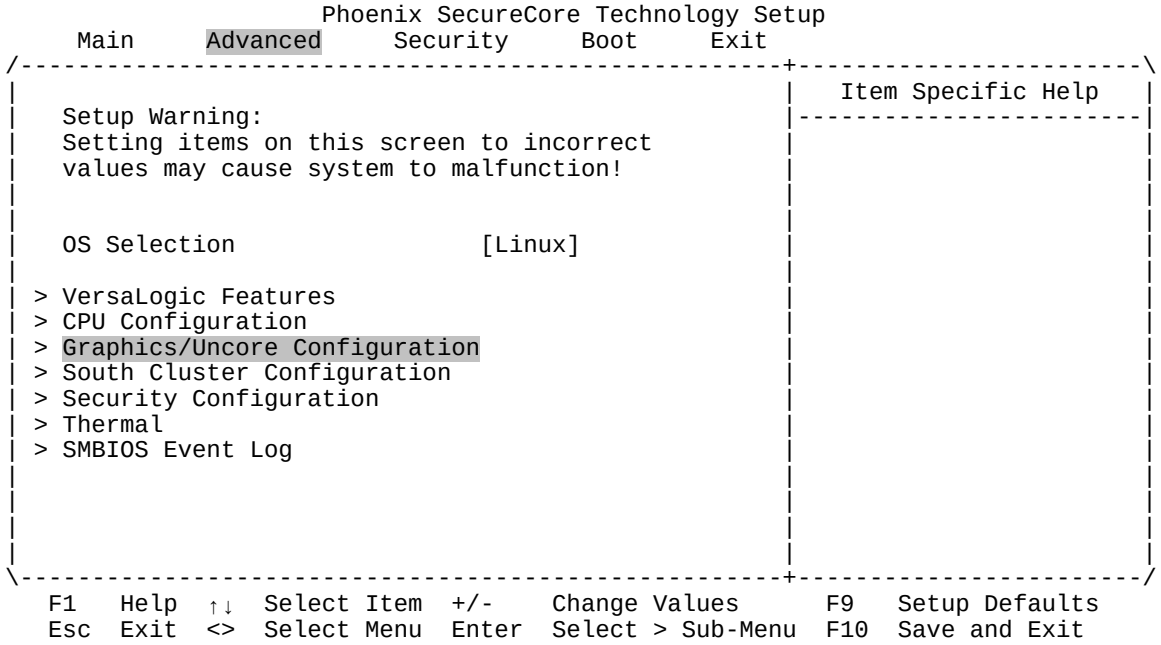
Options	Disable
	Enable (default)

Advanced → CPU Power Management → Max C State



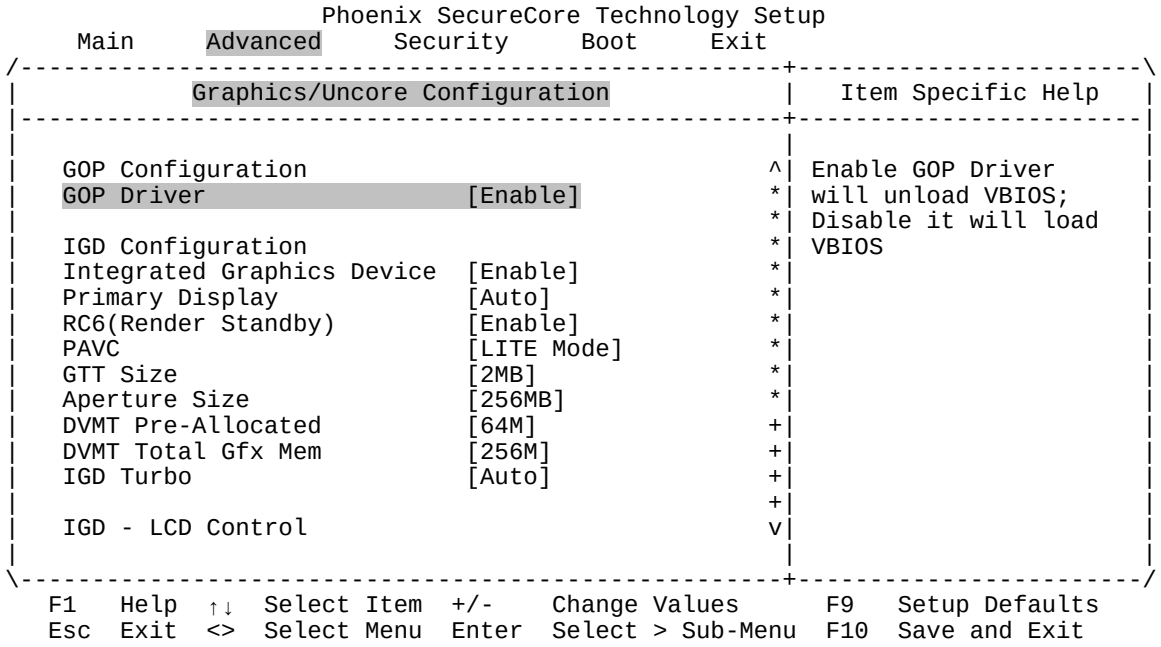
Options	**C7 (default)**
	C6
	C1

Advanced → Graphics/Uncore Configuration



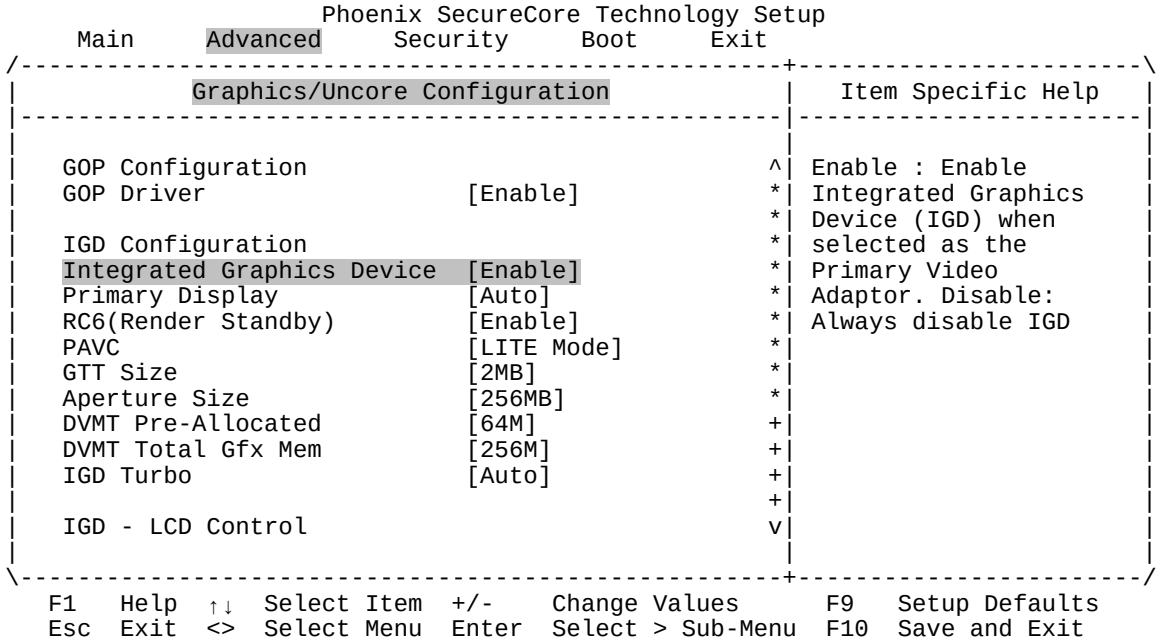
This menu enables you to configure graphics and “uncore” (that is, outside of the SoC’s core) functions.

Advanced → Graphics/Uncore Configuration → GOP Driver



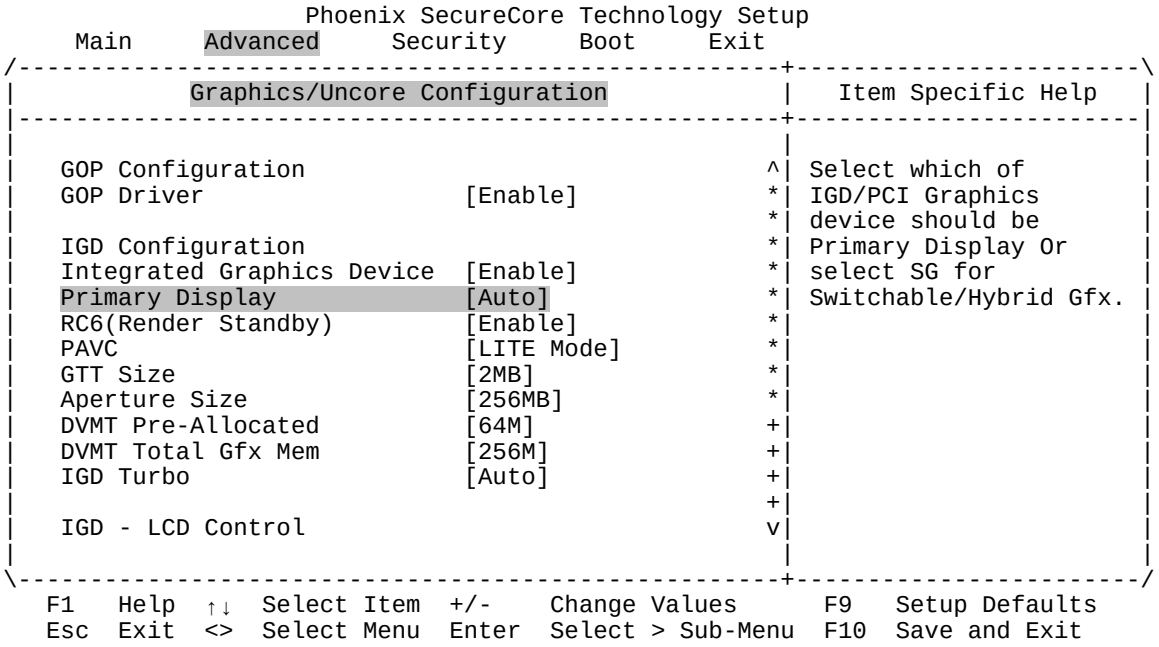
Options	**Enable (default)**	Enables the Graphics Output Protocol (GOP) driver
	Disable	Disables the Graphics Output Protocol (GOP) driver

Advanced → Graphics/Uncore Configuration → Integrated Graphics Device



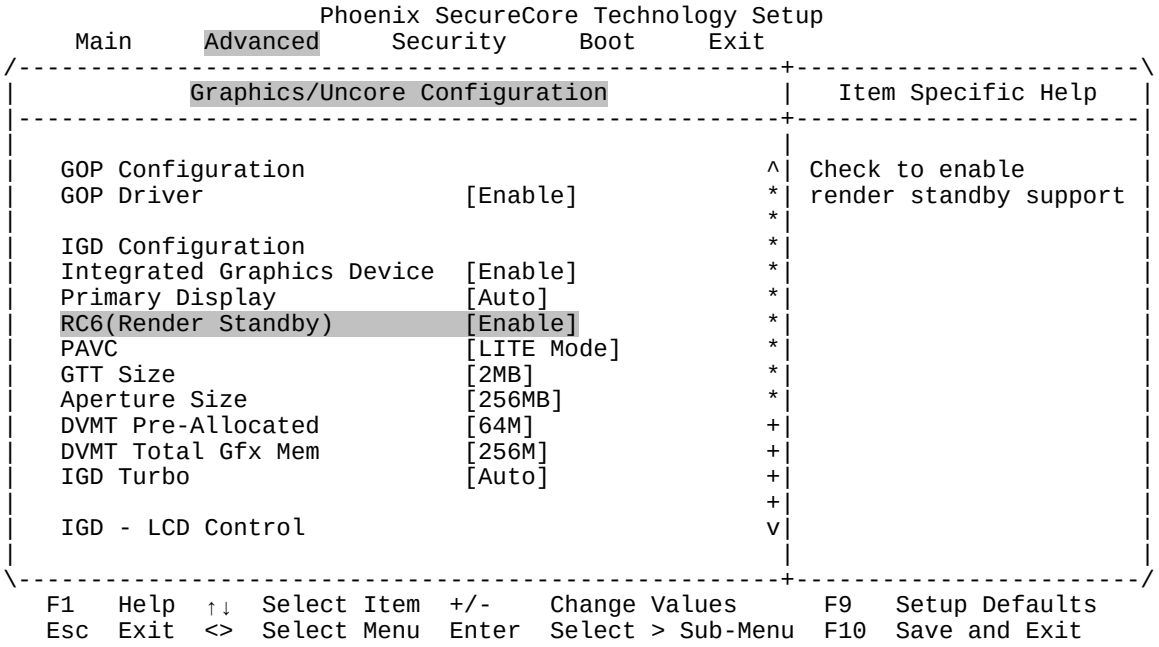
Options	Disable
	Enable (default)

Advanced → Graphics/Uncore Configuration → Primary Display



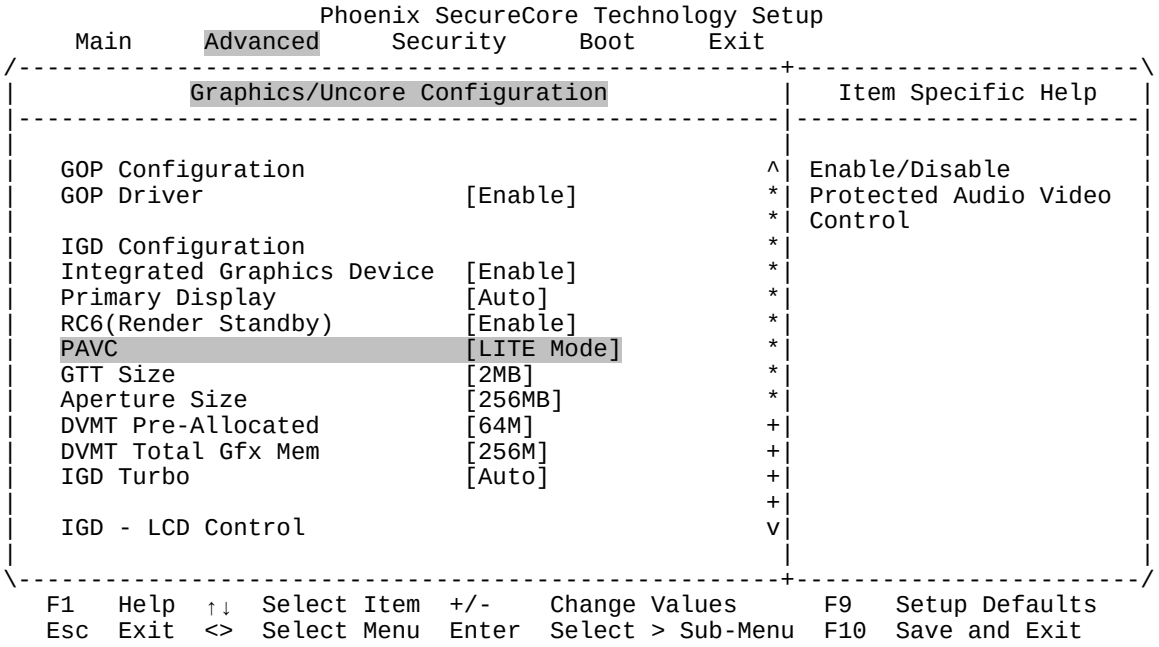
Options	**Auto (default)**
	IGD
	PCIe
	SG

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



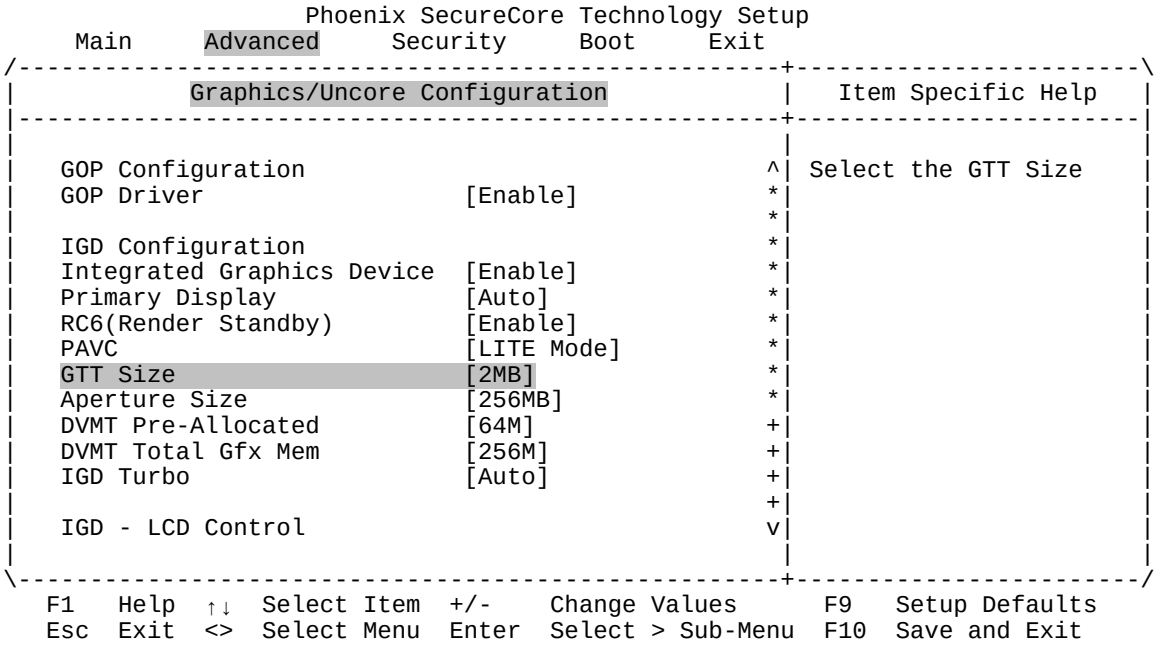
Options	**Enable (default)**
	Disable

Advanced → Graphics/Uncore Configuration → PAVC



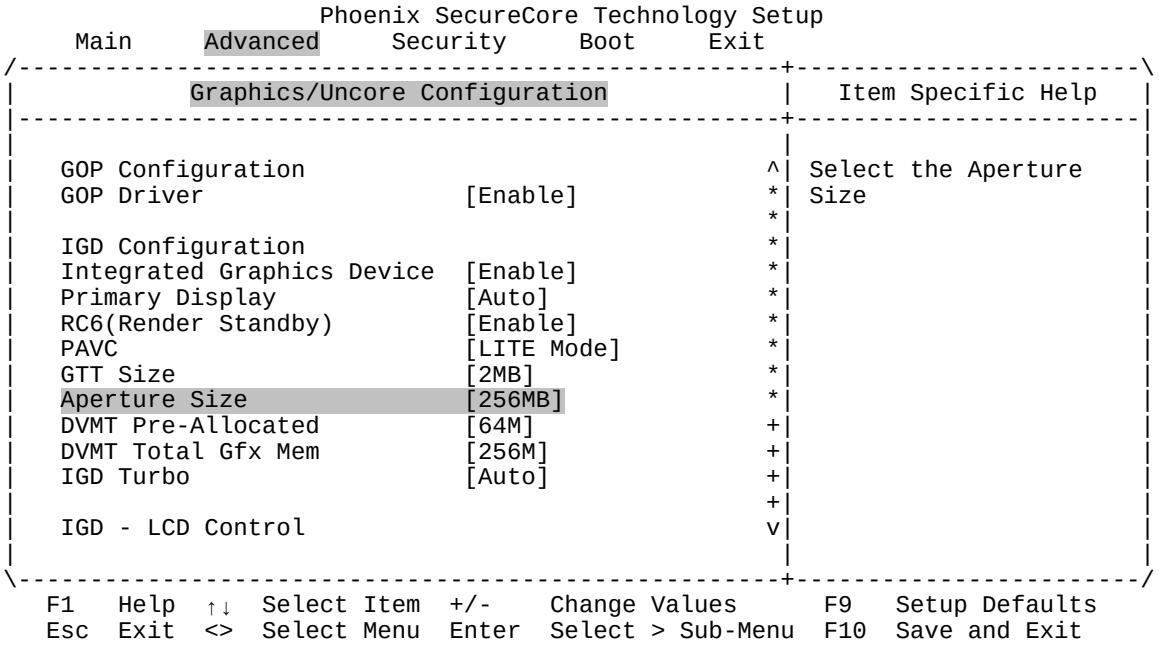
Options	Disable	Disables Protected Audio Video Control (PAVC) support
	LITE Mode (default)	Allows PAVC-protected Blu-ray disks to play.
	SERPENT Mode	Disables the Windows Aero interface and uses ~96 MB of RAM for encrypted data that the operating system cannot see.

Advanced → Graphics/Uncore Configuration → GTT Size



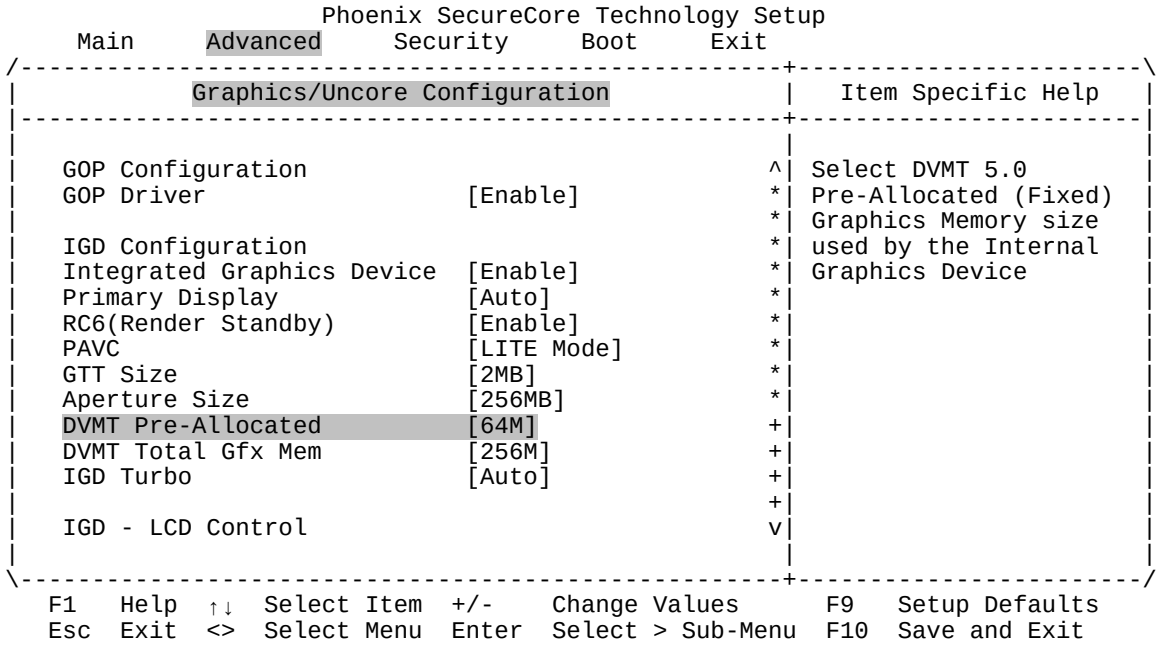
Options	1 MB	Sets the Graphics Translation Table (GTT) size to 1 MB
	2 MB (default)	Sets the Graphics Translation Table (GTT) size to 2 MB

Advanced → Graphics/Uncore Configuration → Aperture Size



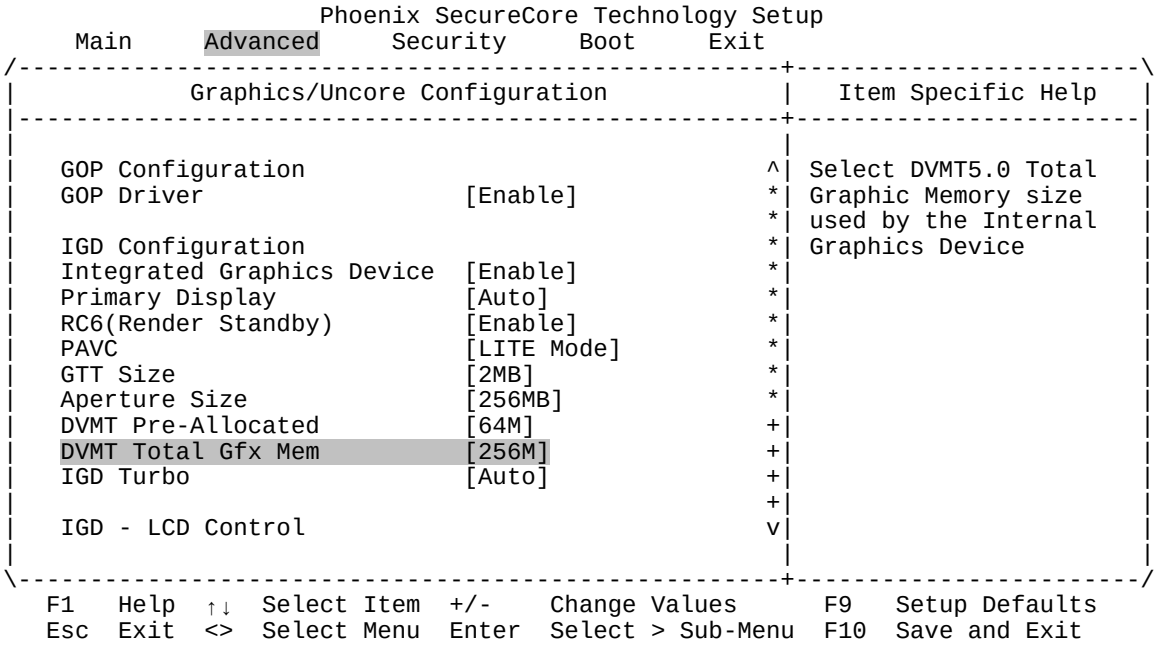
Options	128 MB
	256 MB (default)
	512 MB

Advanced → Graphics/Uncore Configuration → DVMT Pre-Allocated



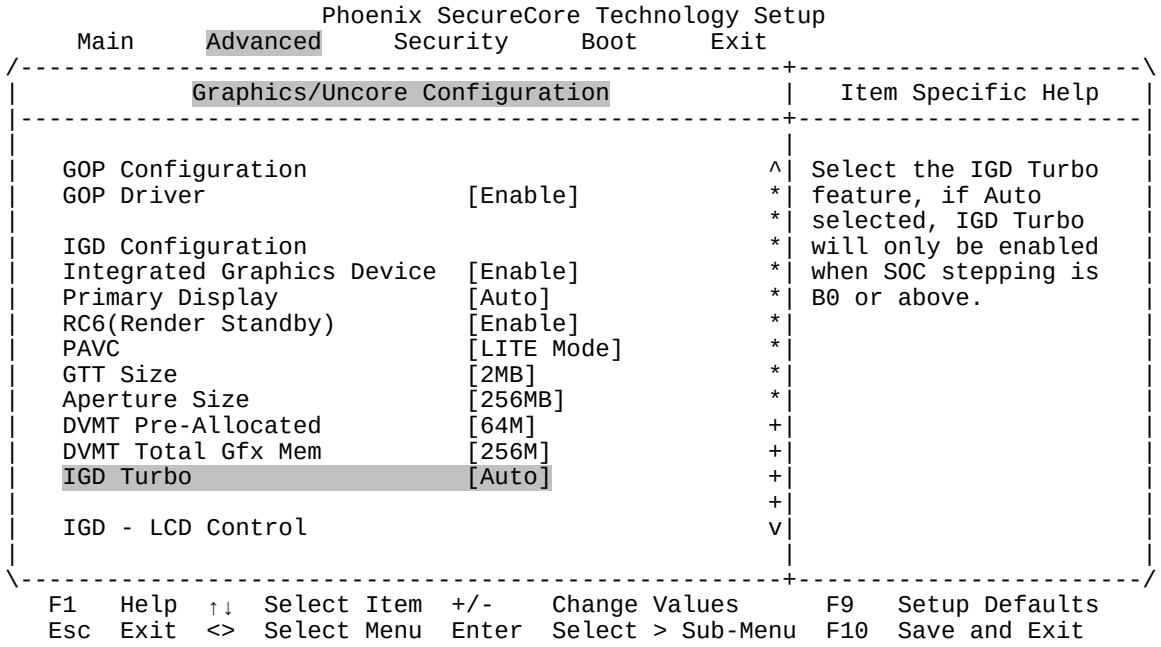
Options	**64M (default)**	Sets the Dynamic Video Memory Technology (DVMT) size to 64 MB
	96M	Sets the Dynamic Video Memory Technology (DVMT) size to 96 MB
	128M	Sets the Dynamic Video Memory Technology (DVMT) size to 128 MB
	160M	Sets the Dynamic Video Memory Technology (DVMT) size to 160 MB
	192M	Sets 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



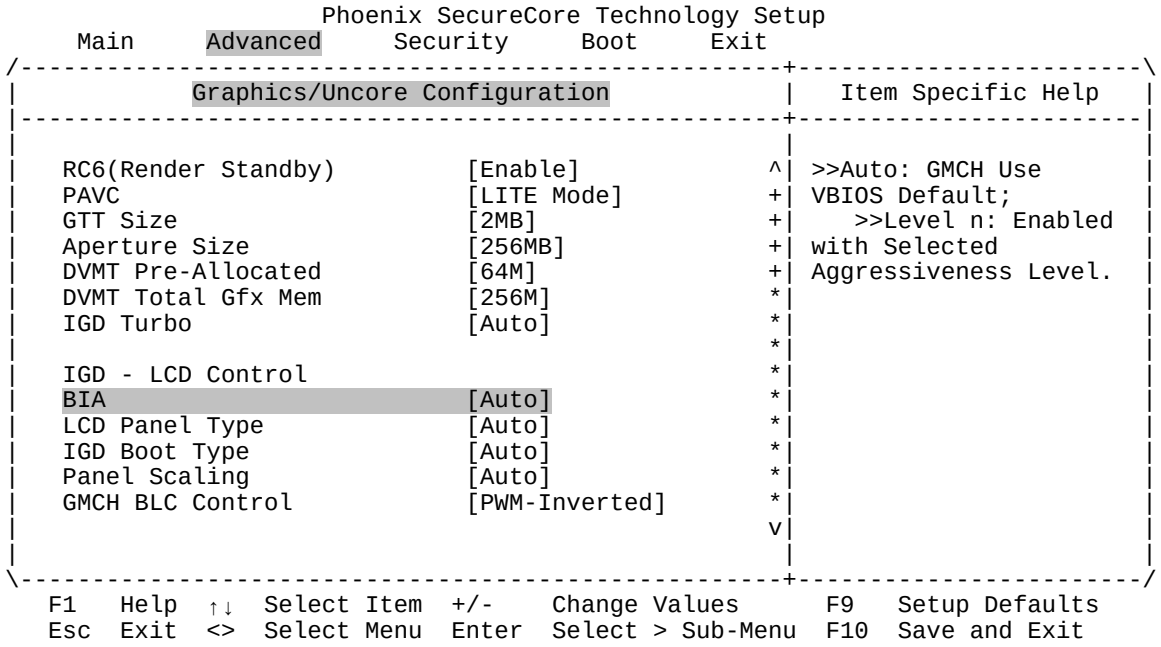
Options	128 MB
	256 MB (default)

Advanced → Graphics/Uncore Configuration → IGD Turbo



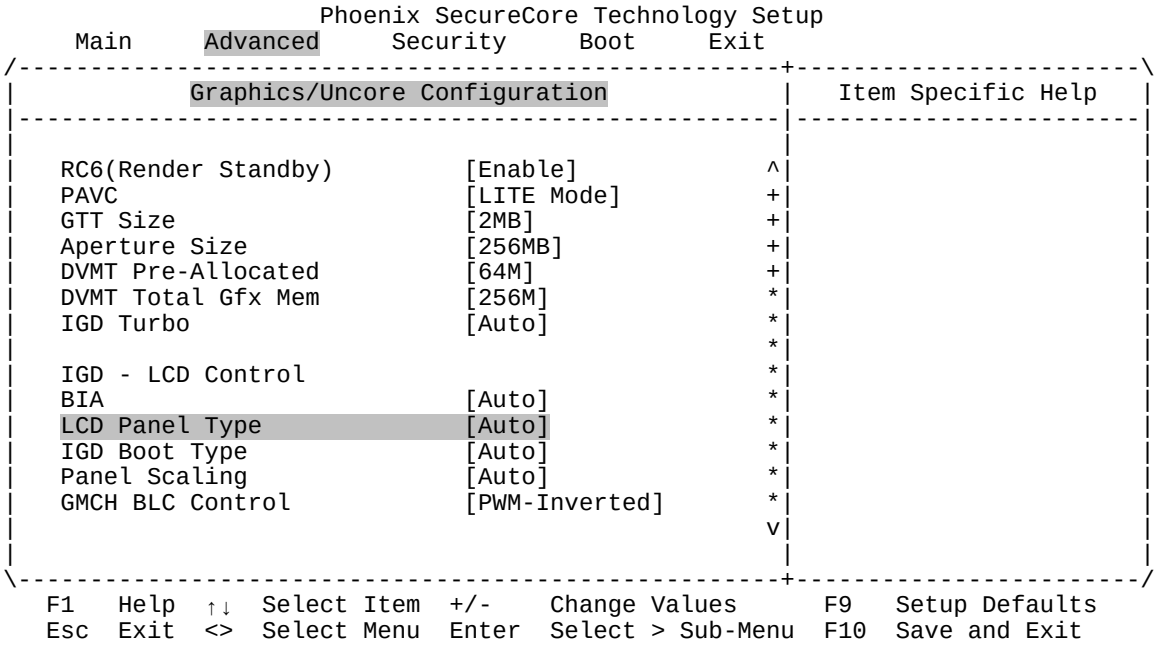
Options	**Auto (default)**
	Enable
	Disable

Advanced → Graphics/Uncore Configuration → BIA



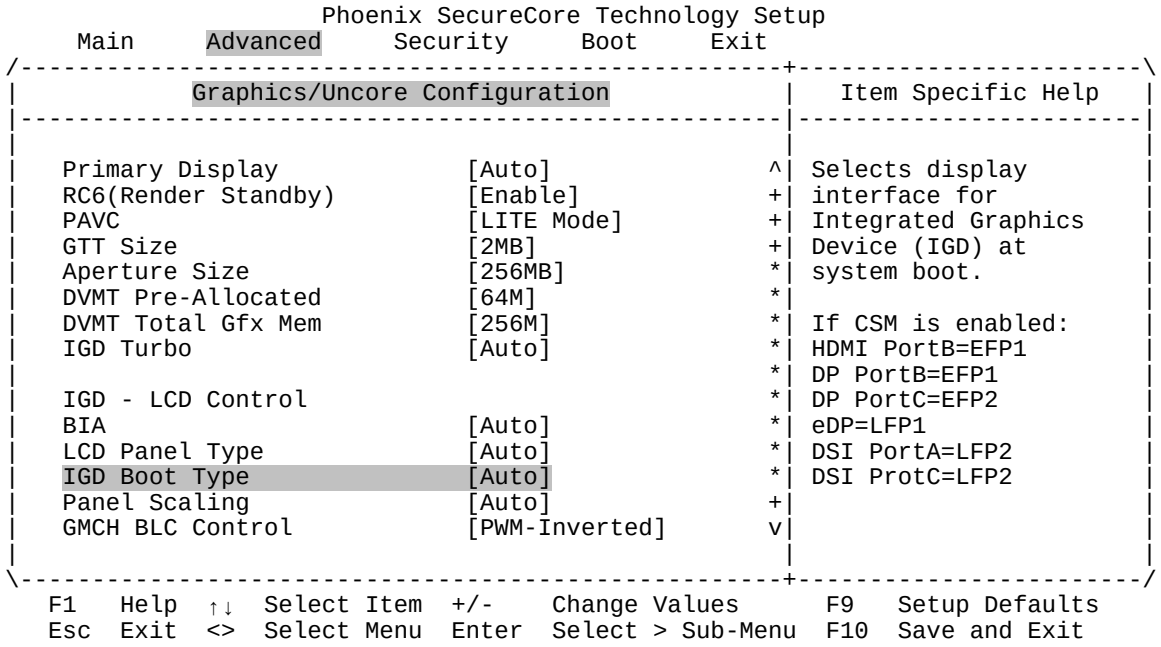
Options	**Auto (default)**	Auto-configures Backlight Image Adaptation (BIA)
	Disabled	
	Level 1	
	Level 2	
	Level 3	
	Level 4	
	Level 5	

Advanced → Graphics/Uncore Configuration → LCD Panel Type



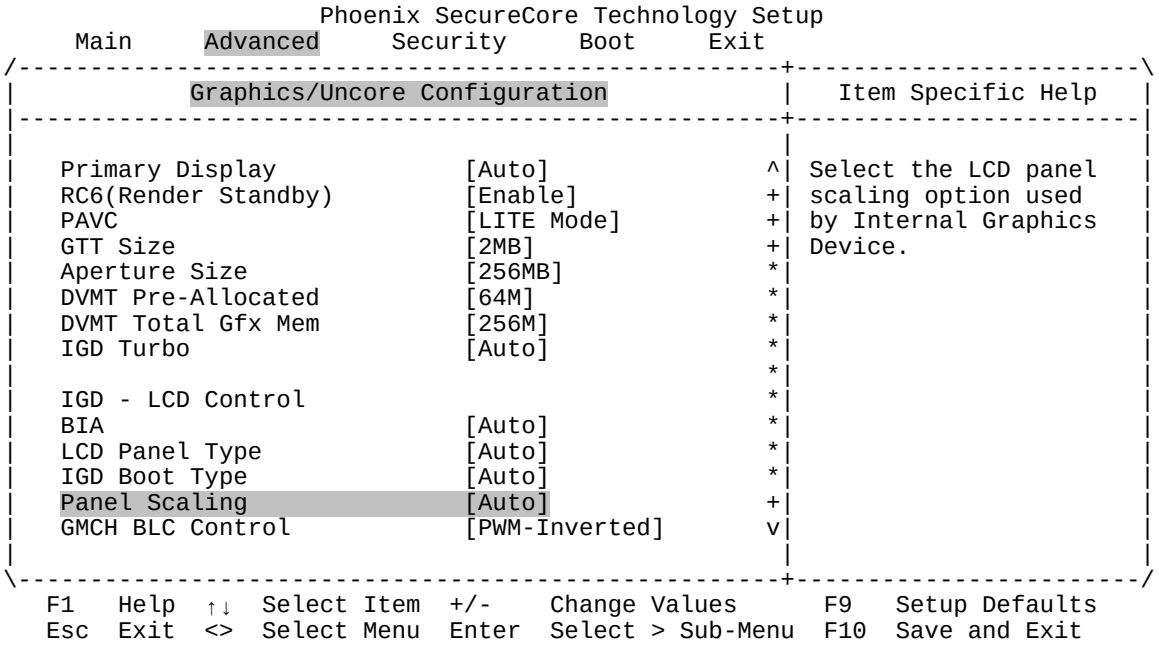
Options	**Auto (default)**
	Panel1 640 x 480
	Panel2 800 x 600
	Panel3 1024 x 768
	Panel4 1280 x 1024
	Panel5 1400 x 1050
	Panel6 1400 x 1050
	Panel7 1600 x 1200
	Panel8 1360 x 768
	Panel9 1680 x 1050
	Panel10 1820 x 1200
	Panel11 1440 x 900
	Panel12 1280 x 1024
	Panel13 1600 x 900
	Panel14 1024 x 768
	Panel15 1920 x 1080
	Panel16 2048 x 1536

Advanced → Graphics/Uncore Configuration → IGD Boot Type



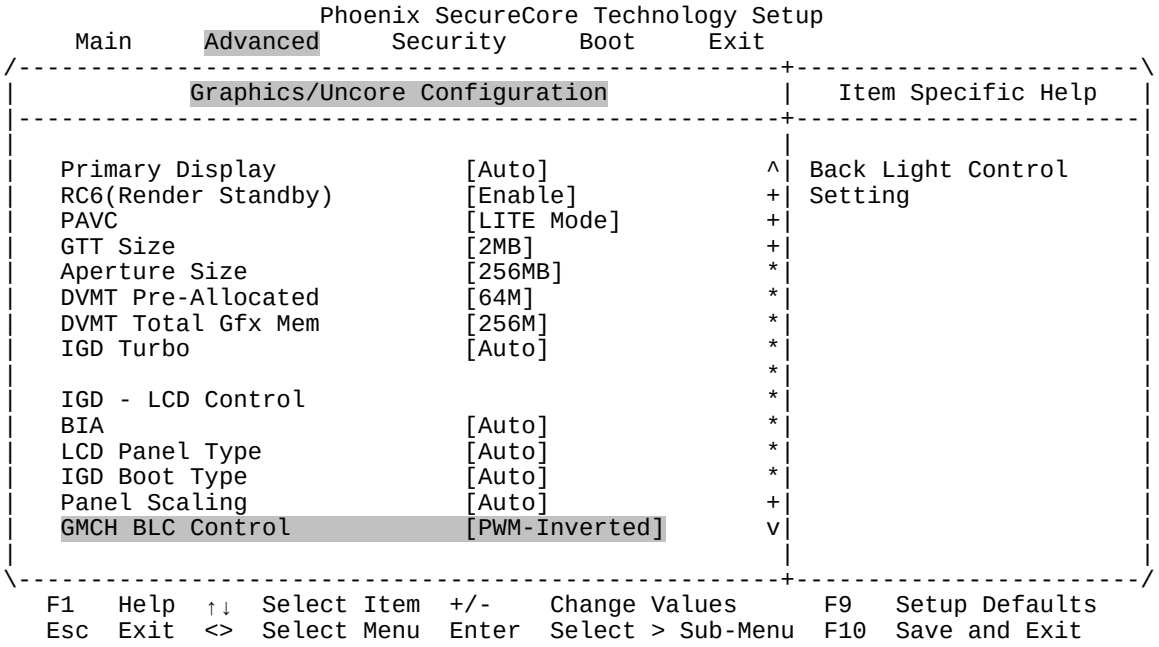
Options	**Auto (default)**
	VGA Port
	HDMI Port B
	DP Port B
	DP Port C
	DSI Port A
	DSI Port C

Advanced → Graphics/Uncore Configuration → Panel Scaling



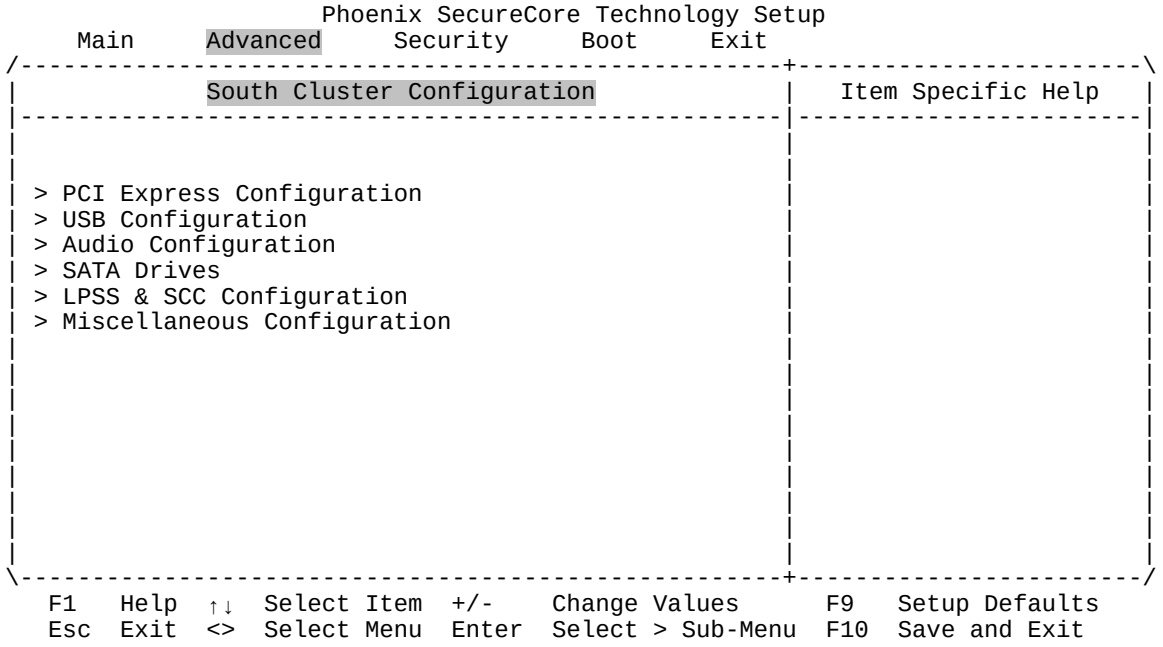
Options	**Auto (default)**
	Centering
	Stretching

Advanced → Graphics/Uncore Configuration → GMCH BLC Control



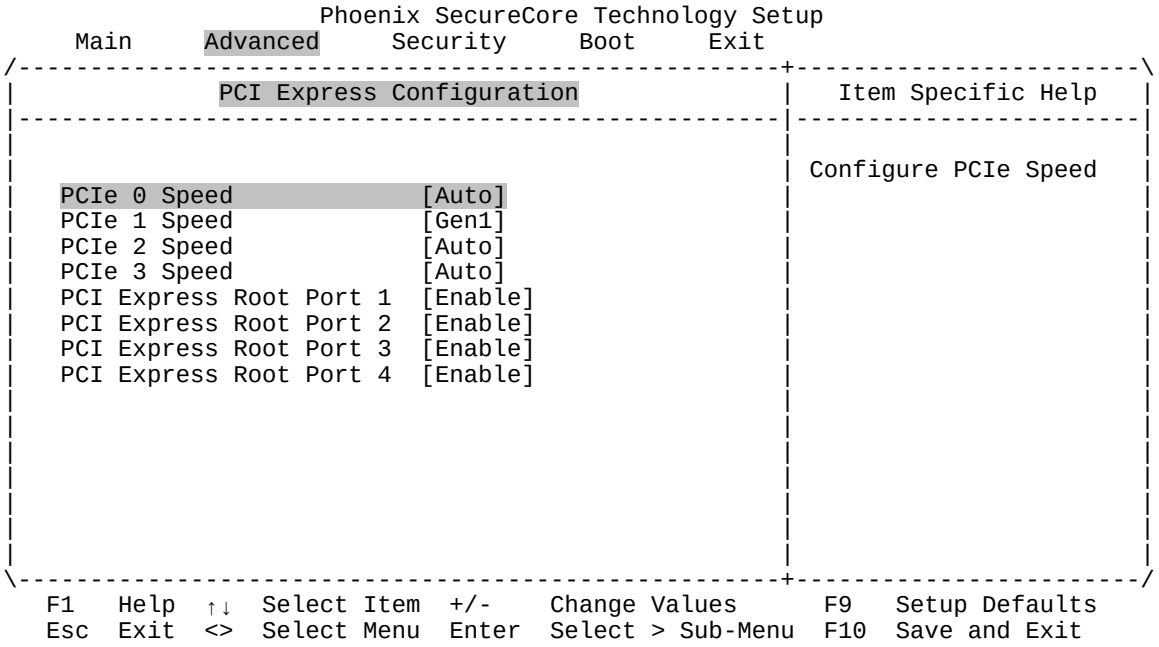
Options	**PWM-Inverted (default)**
	GMBus-Inverted
	PWM-Normal
	GMBus-Normal

Advanced → South Cluster Configuration



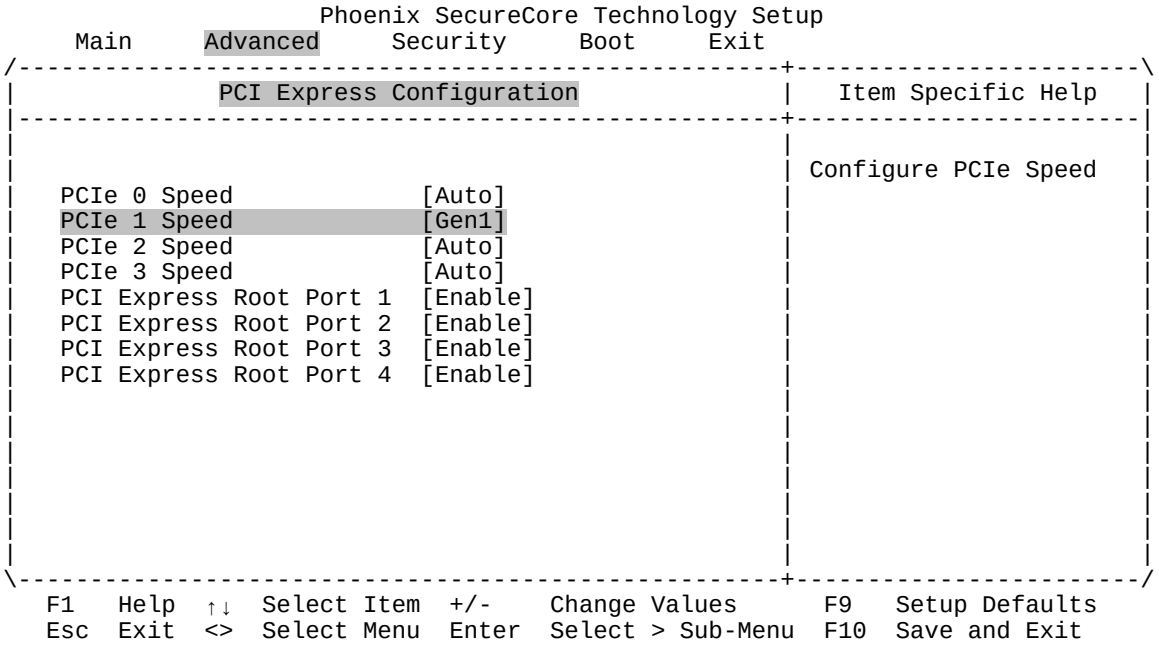
This is the top-level screen for the South Cluster Configuration sub-menu.

Advanced → PCI Express Configuration → PCIe o Speed



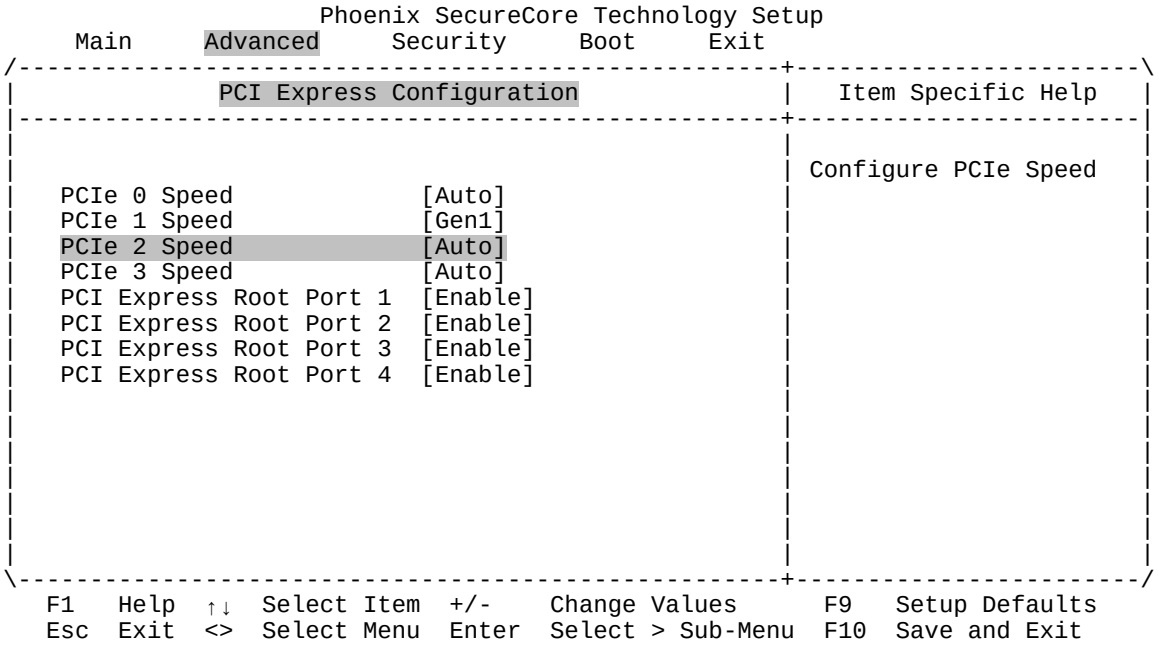
Options	**Auto (default)**
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCIe 1 Speed



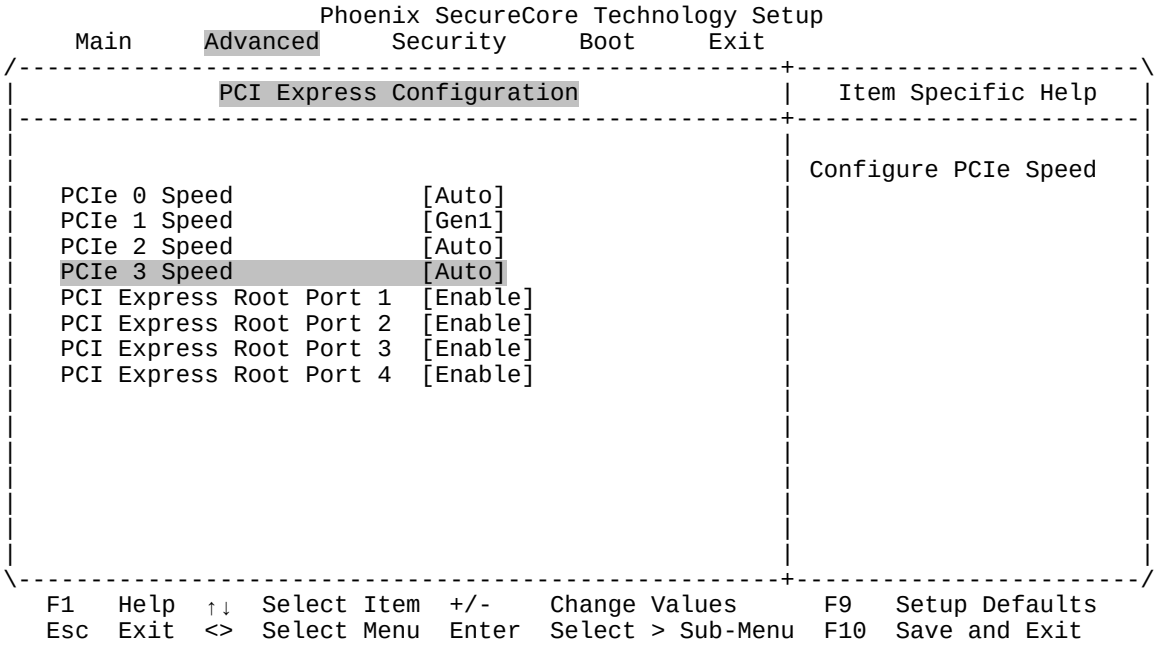
Options	Auto
	Gen 1 (default)
	Gen 2

Advanced → PCI Express Configuration → PCIe 2 Speed



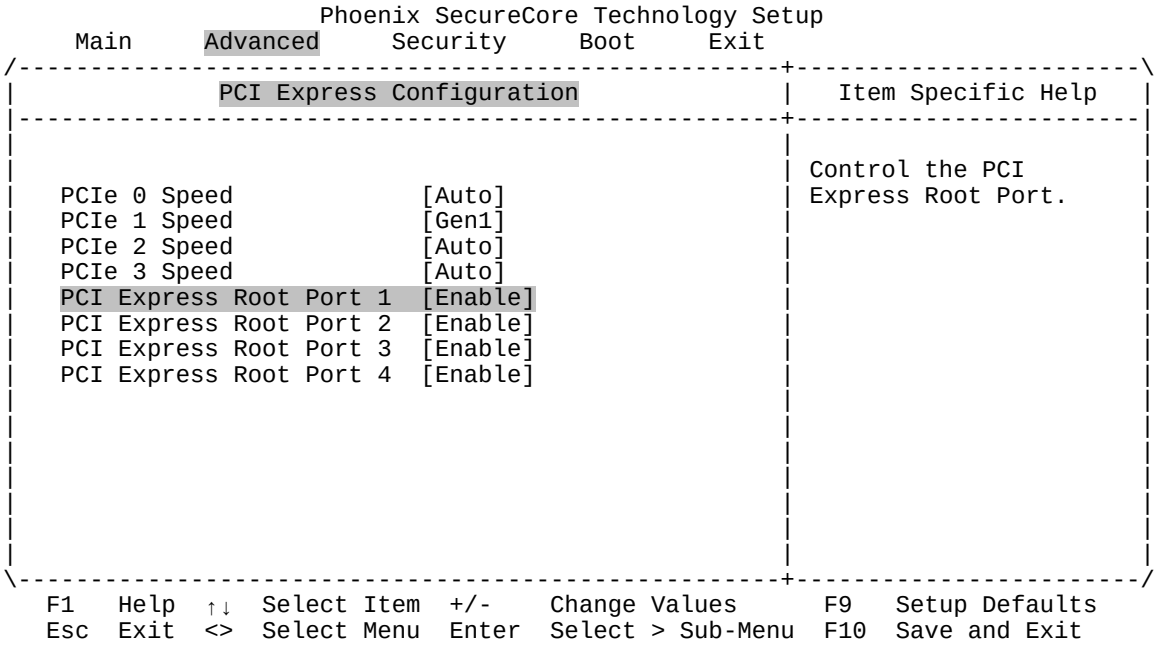
Options	**Auto (default)**
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCIe 3 Speed



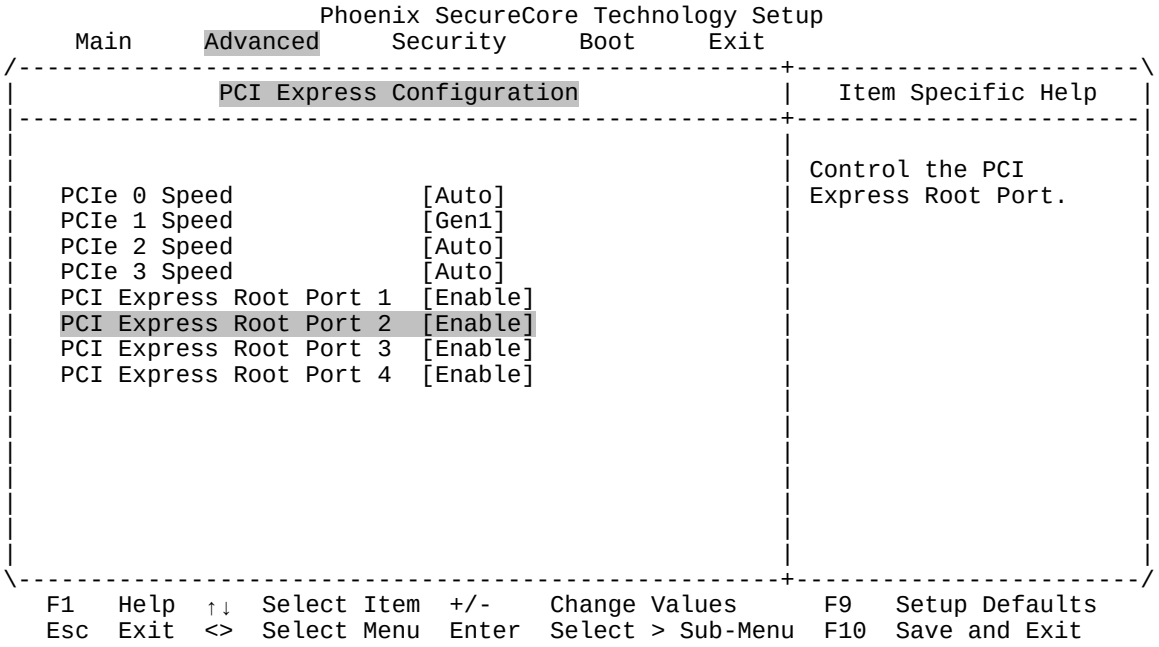
Options	**Auto (default)**
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCI Express Root Port 1



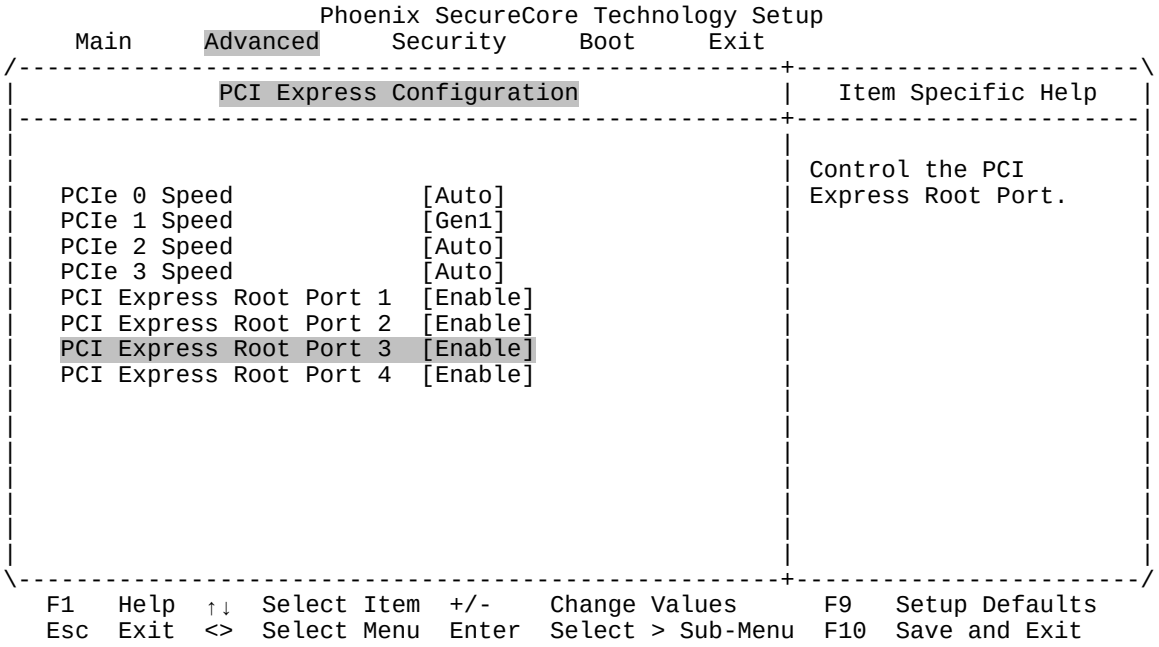
Options	**Enable (default)**
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 2



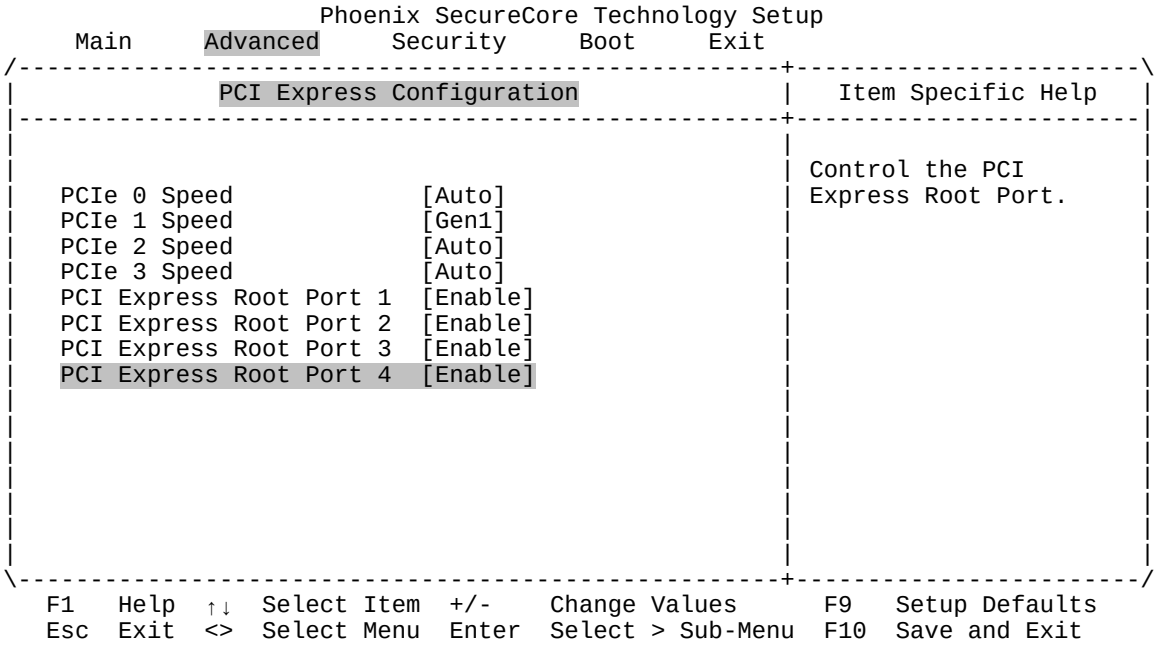
Options	**Enable (default)**
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 3



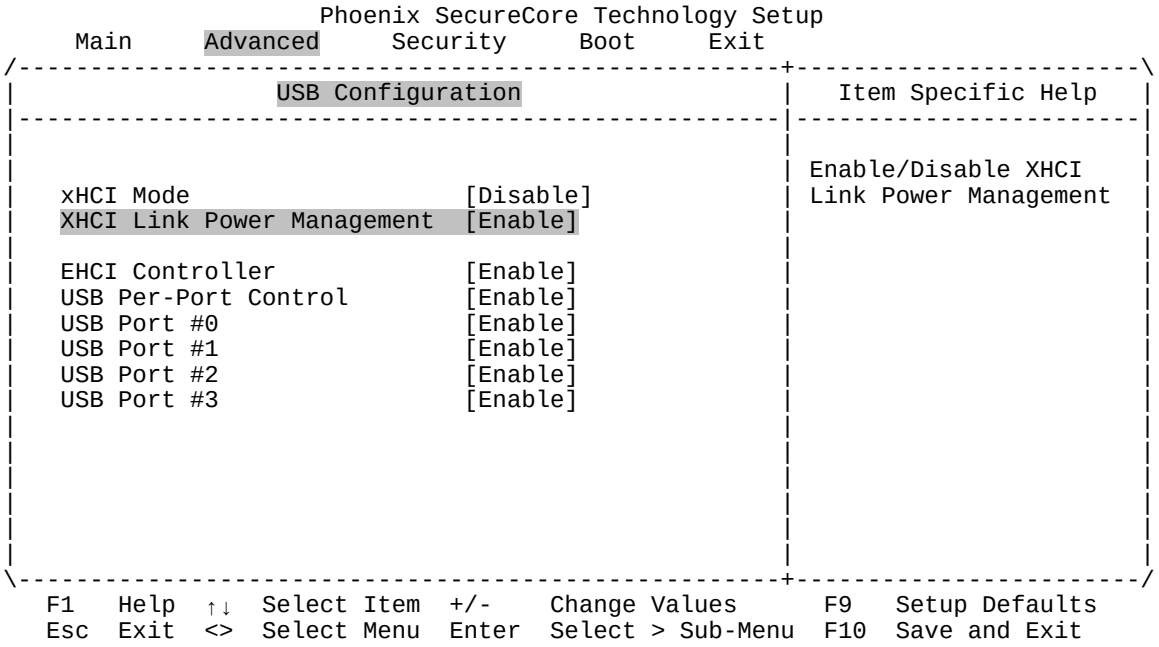
Options	**Enable (default)**
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 4



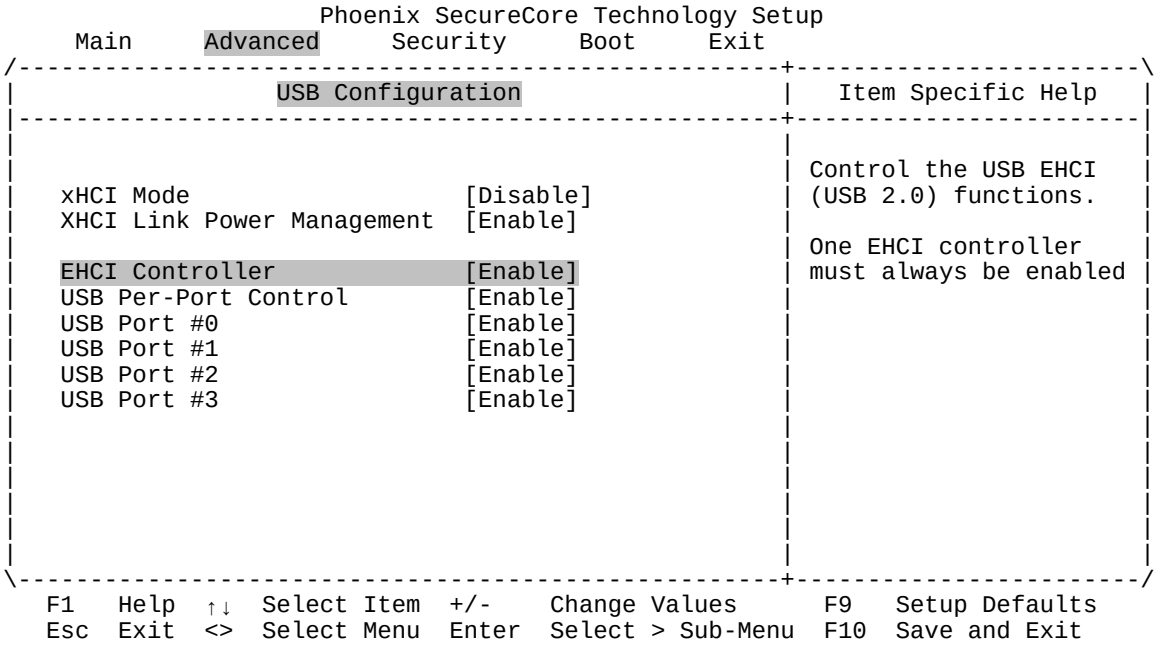
Options	**Enable (default)**
	Disable

Advanced → USB Configuration → XHCI Link Power Management



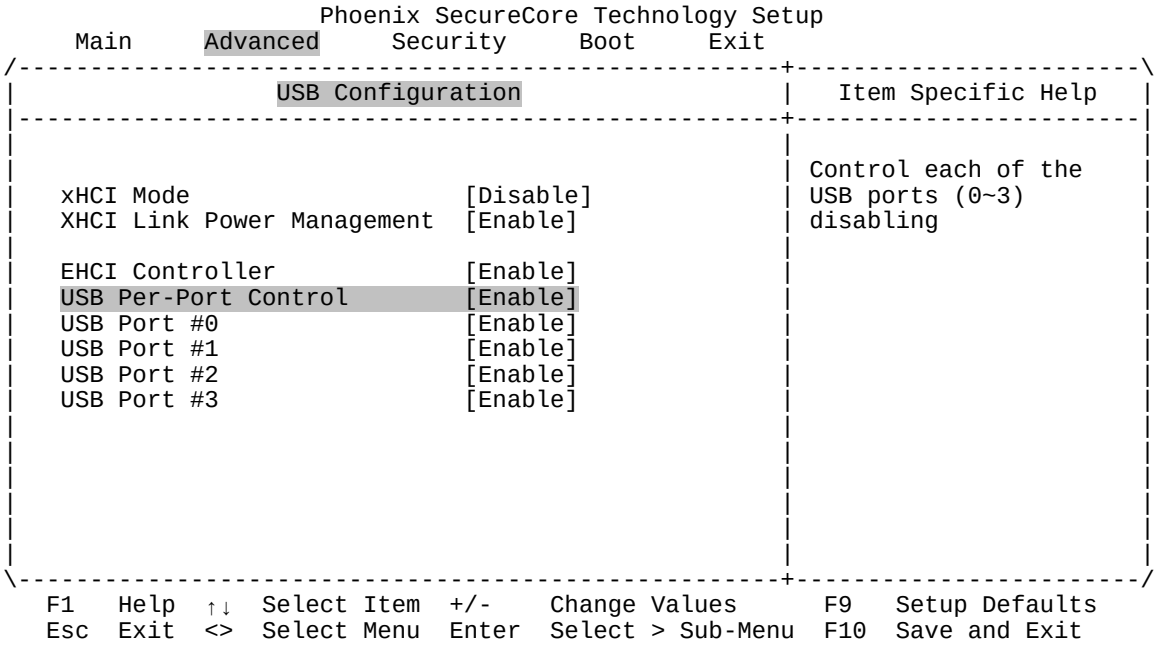
Options	Disable
	Enable (default)

Advanced → USB Configuration → EHCI Controller



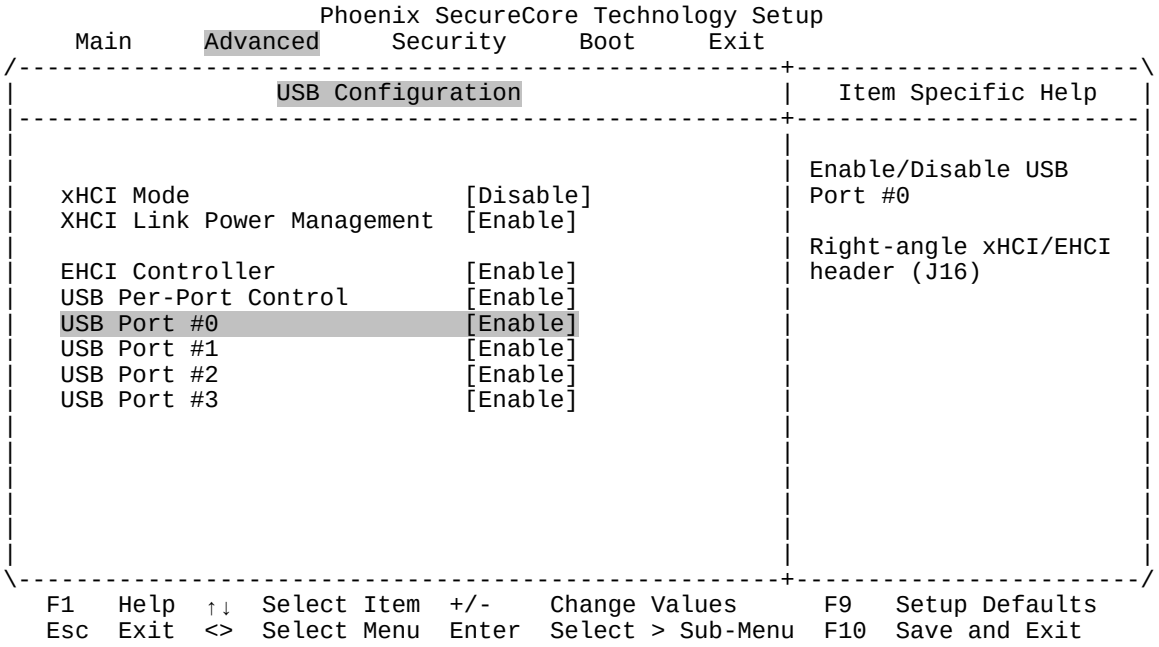
Options	**Enable (default)**
	Disable

Advanced → USB Configuration → USB Per-Port Control



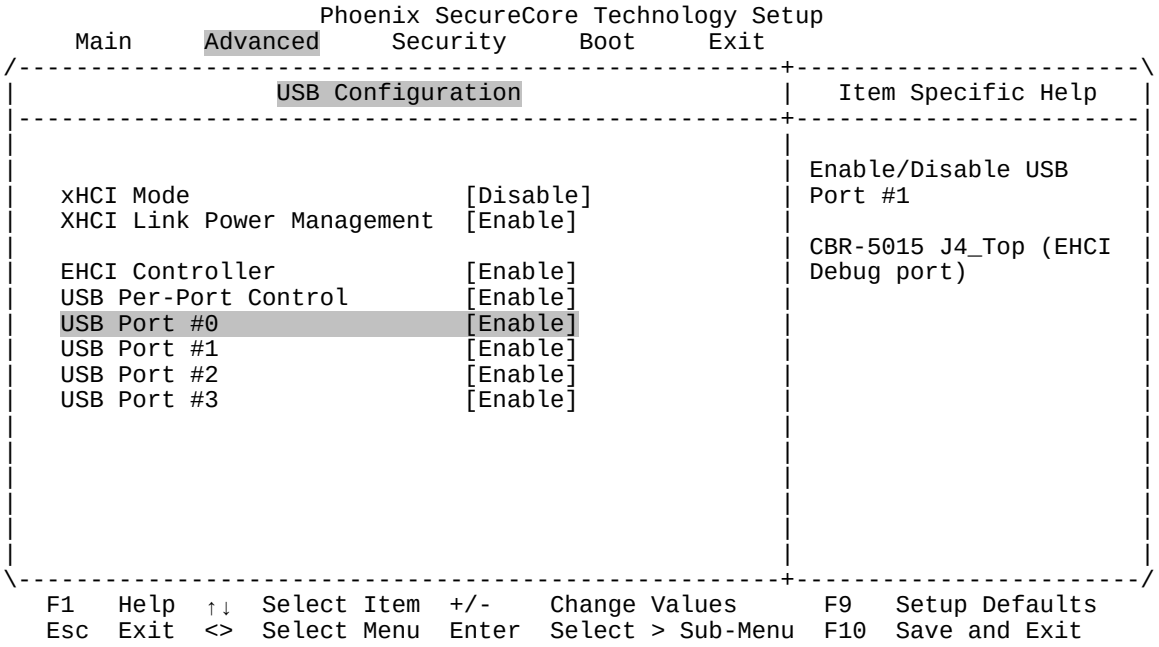
Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #0



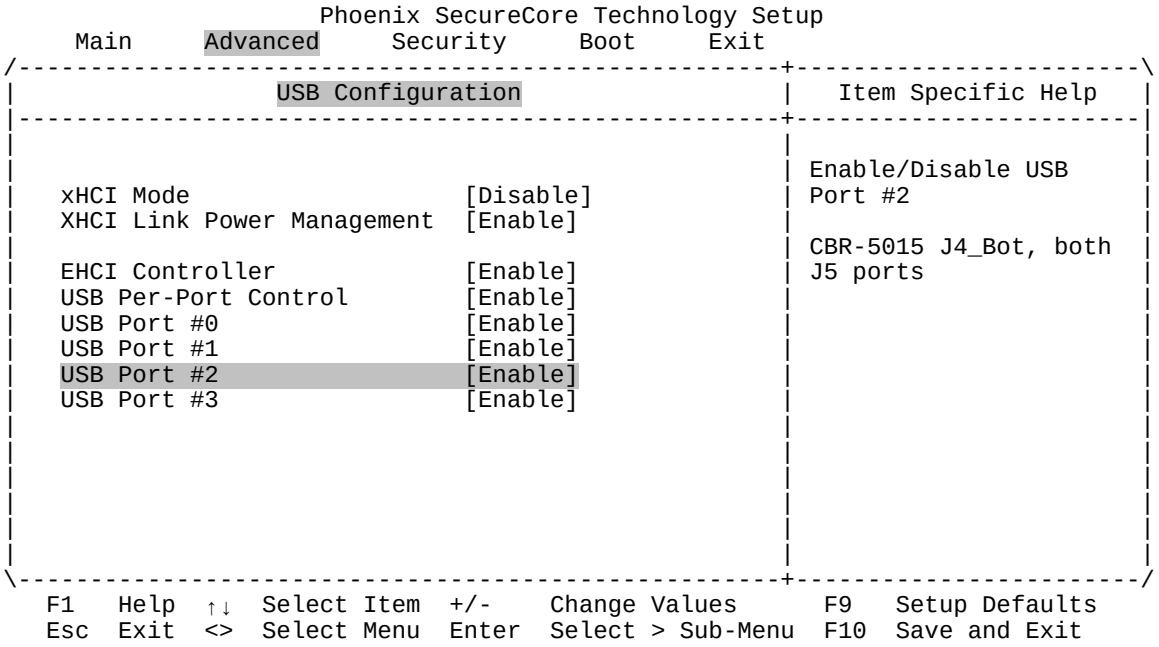
Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #1



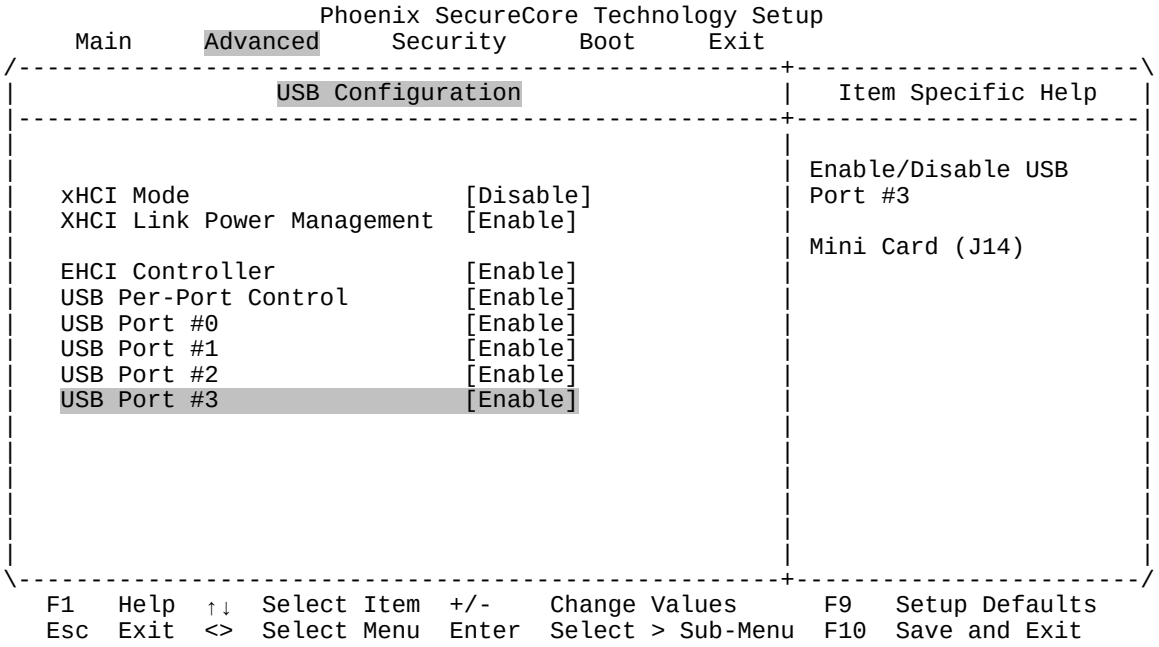
Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #2



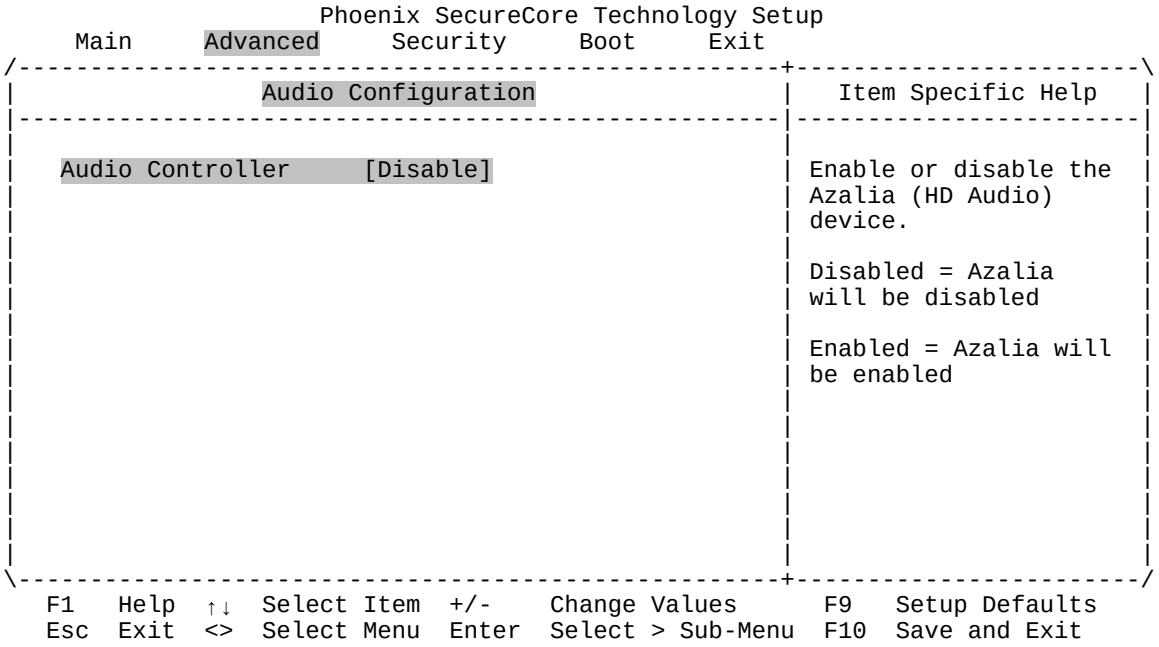
Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #3



Options	Disable
	Enable (default)

Advanced → Audio Configuration → Audio Controller

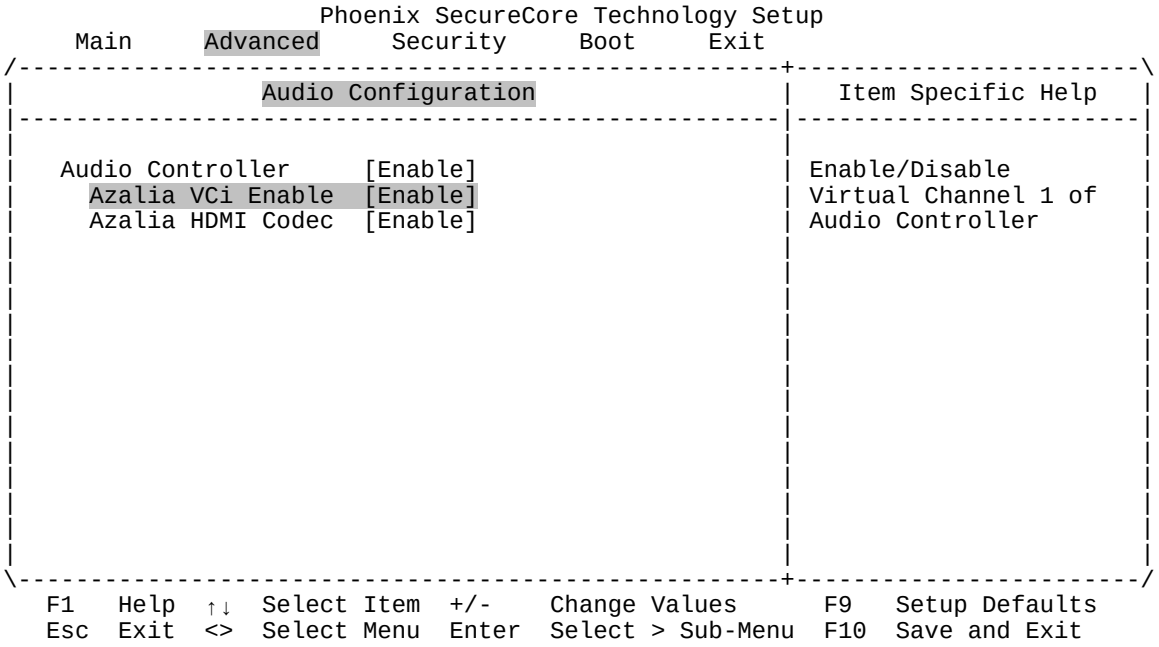


Options	**Disable (default)**	Disable “Azalia” (high-definition) audio
	Enable	Enable “Azalia” (high-definition) audio

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

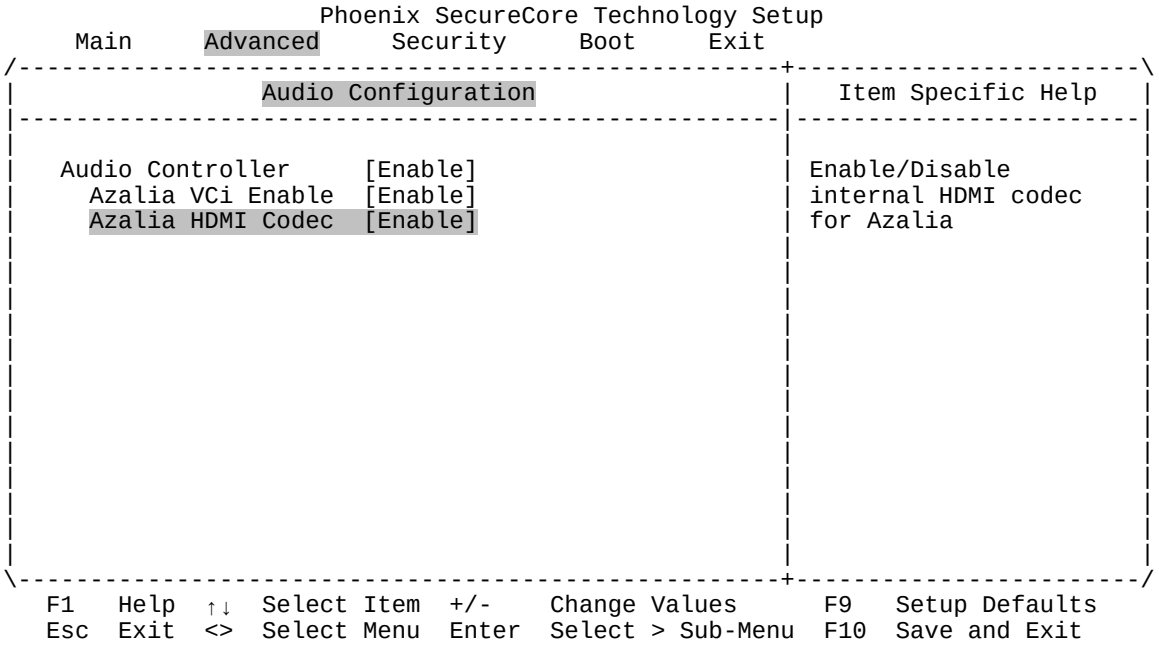
- Azalia VCi Enable (see page 88)
- Azalia HDMI Codec (see page 89)

Advanced → Audio Configuration → Azalia VCi Enable



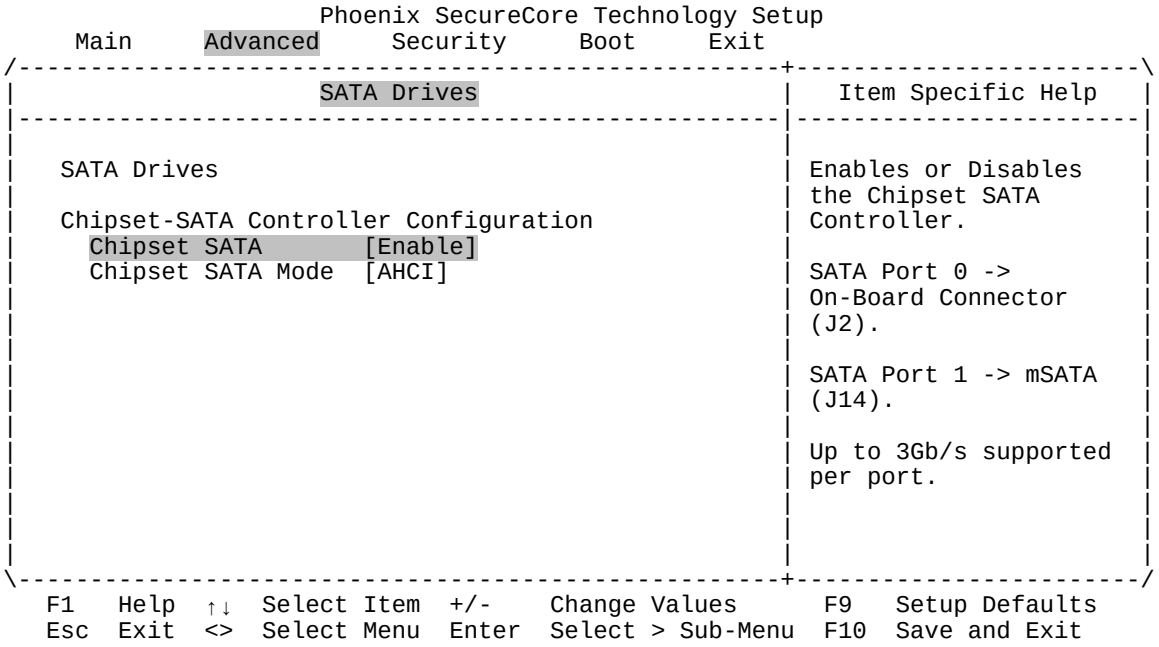
Options	Disable
	Enable (default)

Advanced → Audio Configuration → Azalia HDMI CODEC



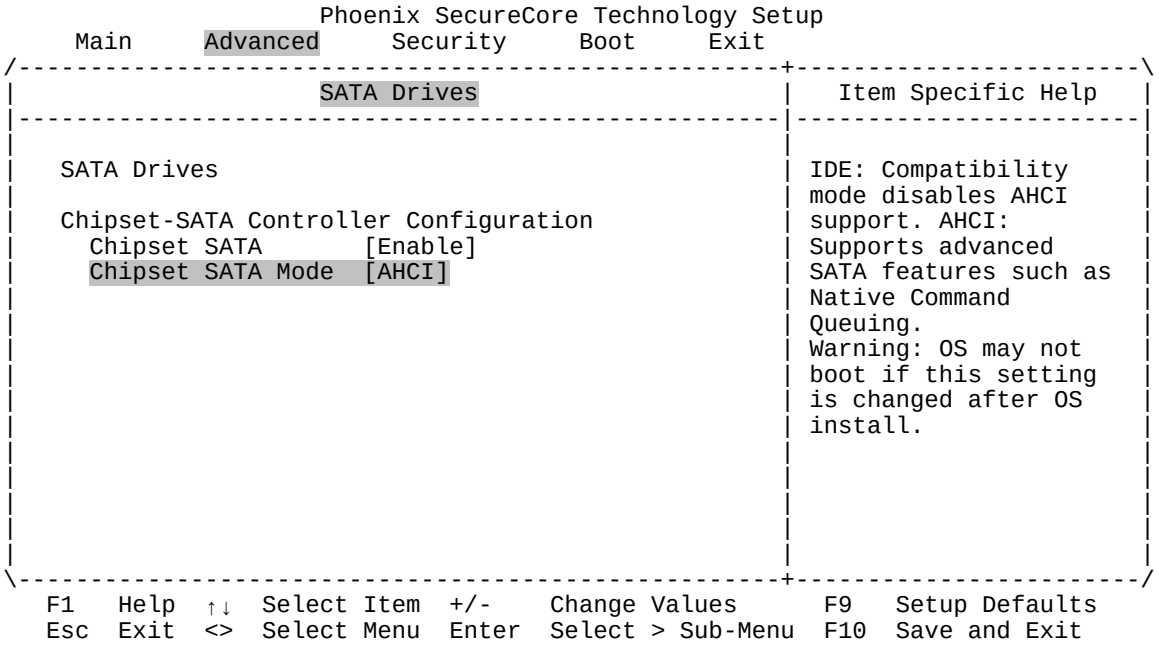
Options	Disable
	Enable (default)

Advanced → SATA Drives → Chipset SATA



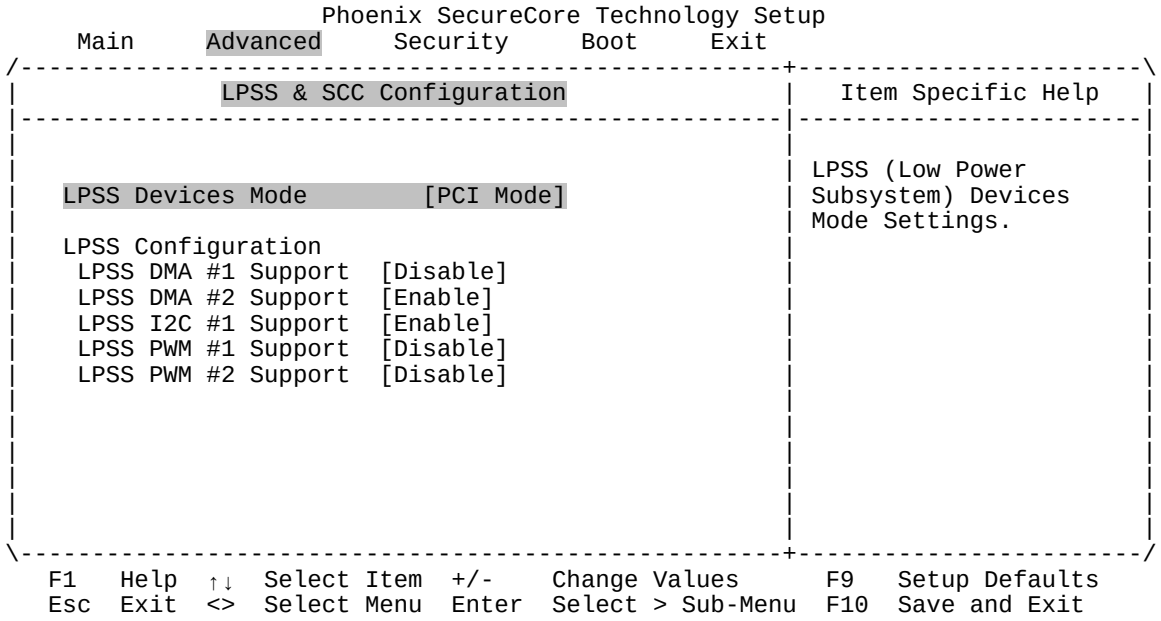
Options	**Enable (default)**	Enables onboard SATA ports
	Disable	Disables onboard SATA ports

Advanced → SATA Drives → Chipset SATA Mode



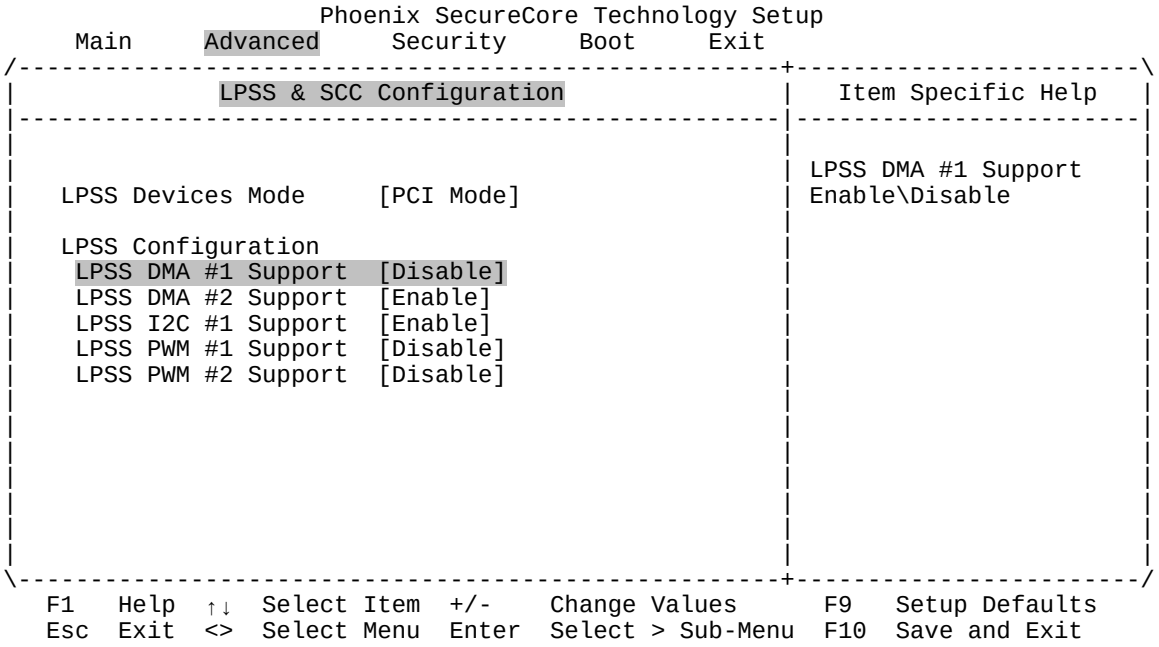
Options	IDE
	ACHI (default)

Advanced → LPSS & SCC Configuration → LPSS Devices Mode



Options	ACPI Mode
	PCI Mode (default)

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

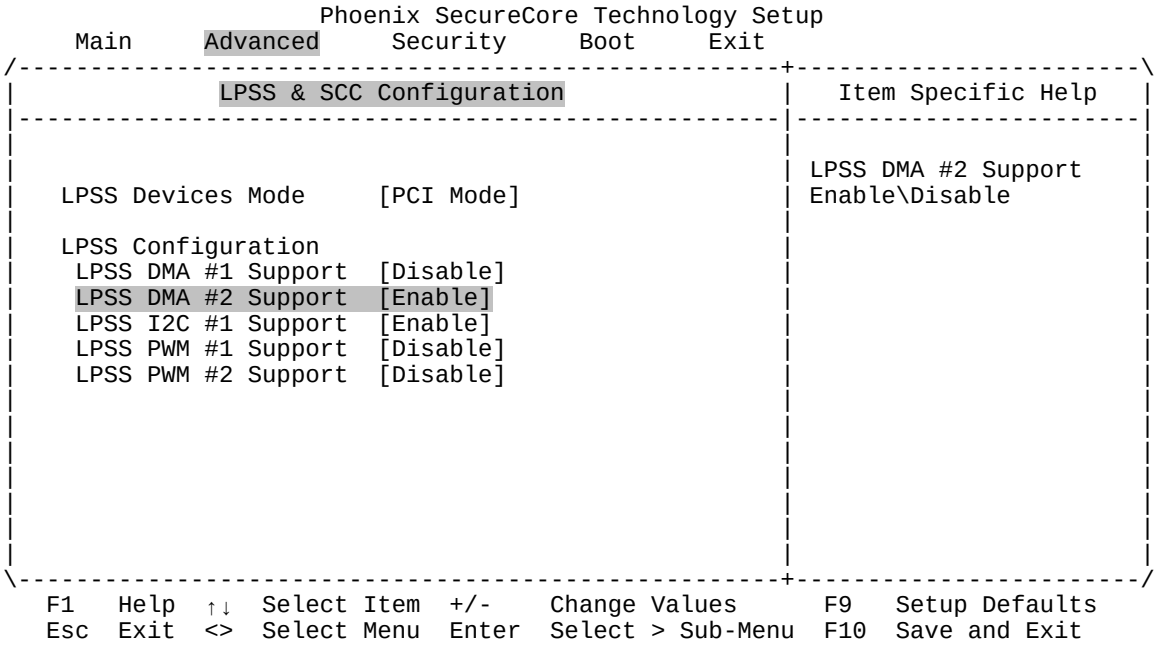


Options	**Disable (default)**
	Enable

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

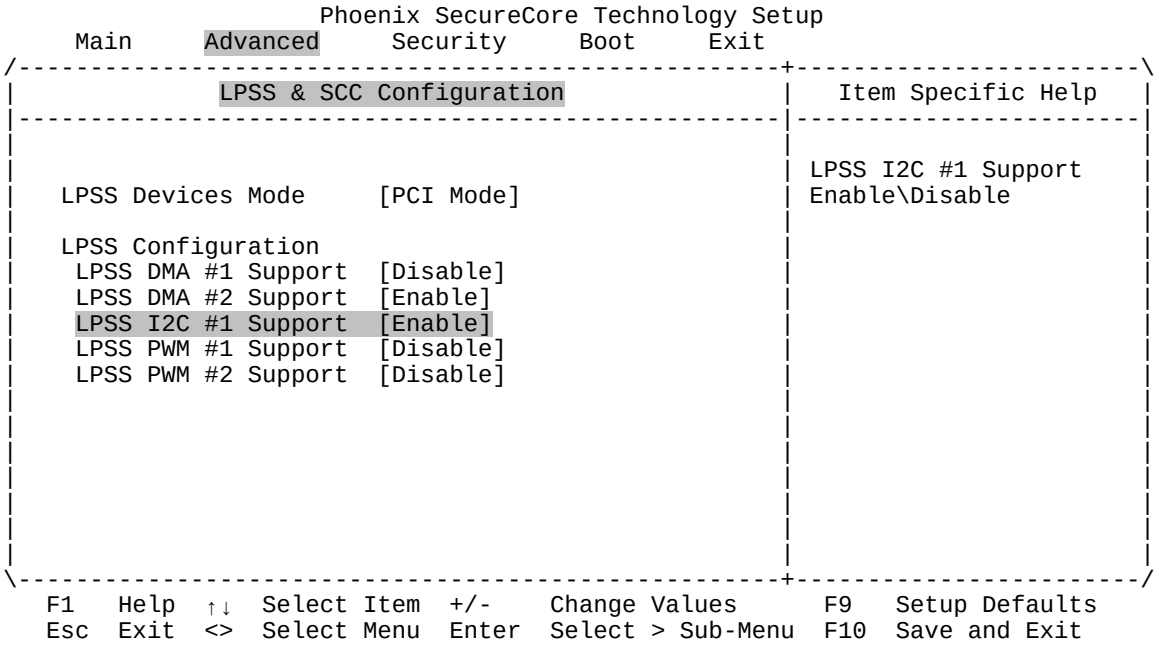
- LPSS PWM #1 Support
- LPSS PWM #2 Support

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



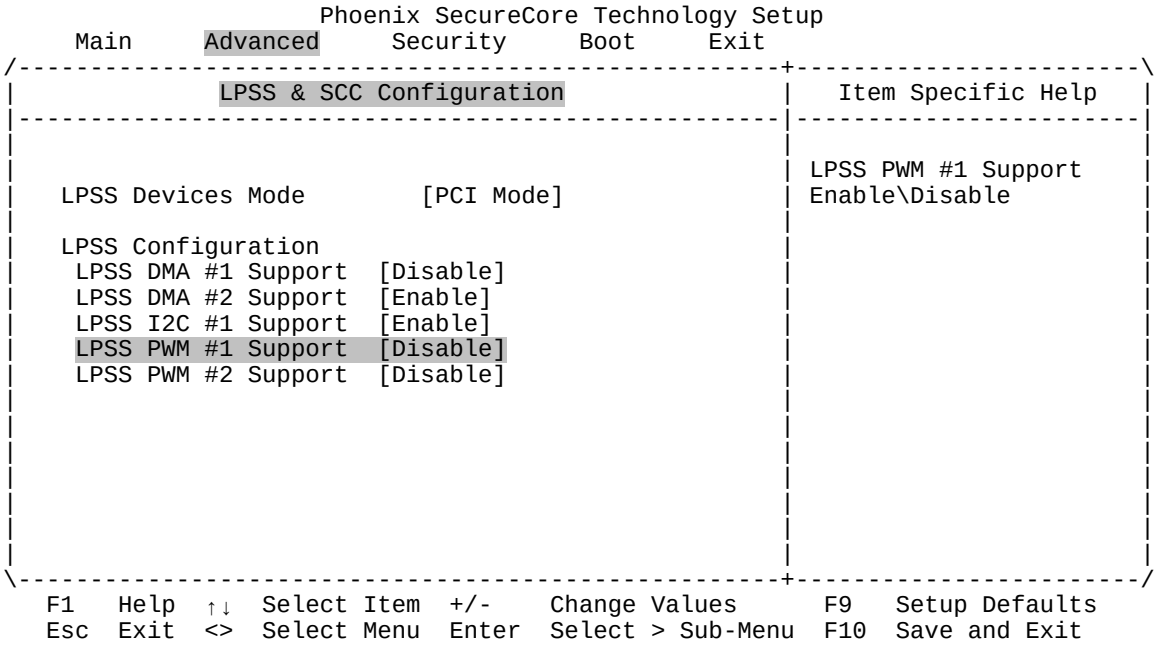
Options	Disable
	Enable (default)

Advanced → LPSS & SCC Configuration → LPSS I2C #1 Support



Options	Disable	Disables the I^2C ports and the LPSS I2C #1 support option.
	Enable (default)	Enables I^2C ports and the LPSS I2C #1 support option.

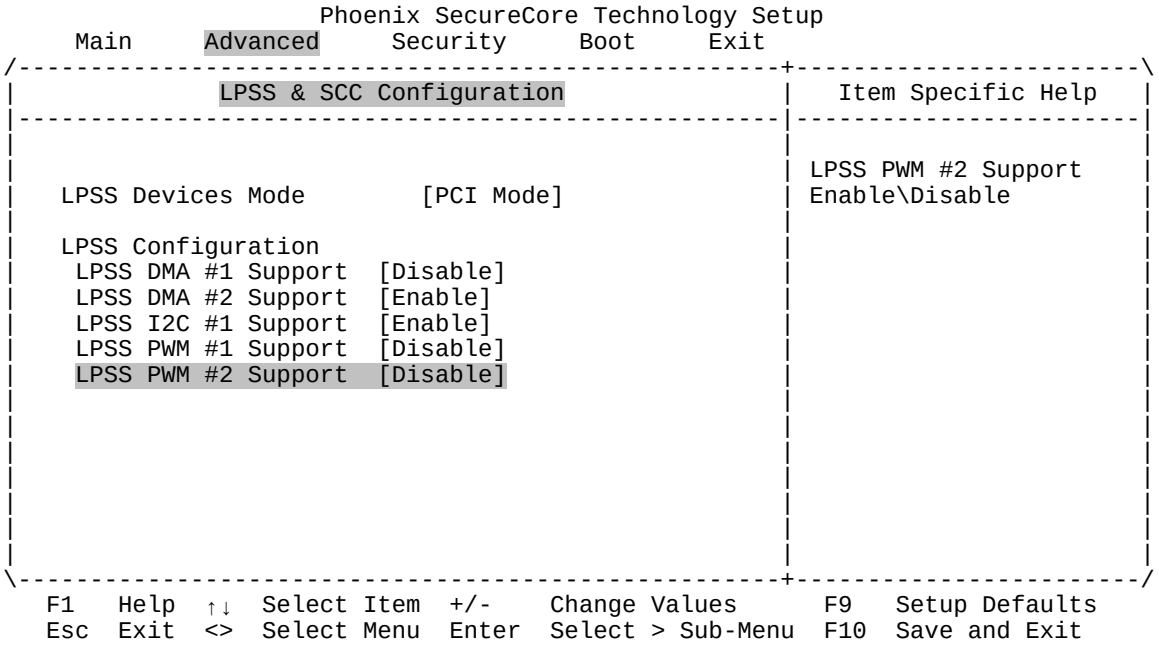
Advanced → LPSS & SCC Configuration → LPSS PWM #1 Support



Options	**Disable (default)**
	Enable

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

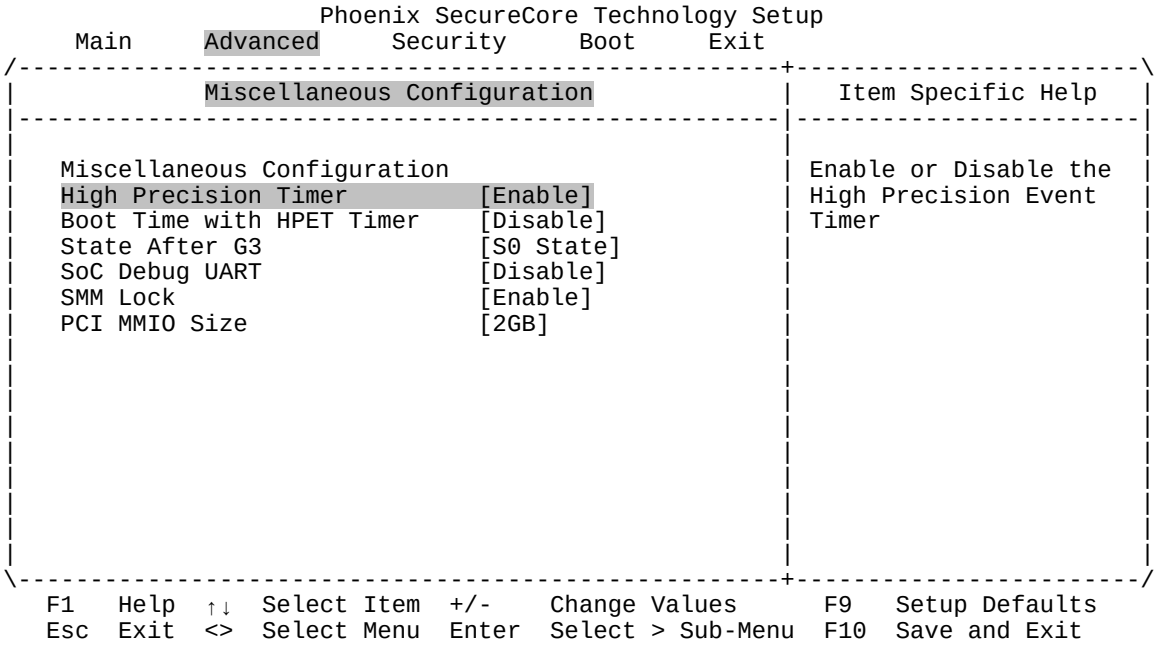
Advanced → LPSS & SCC Configuration → LPSS PWM #2 Support



Options	**Disable (default)**
	Enable

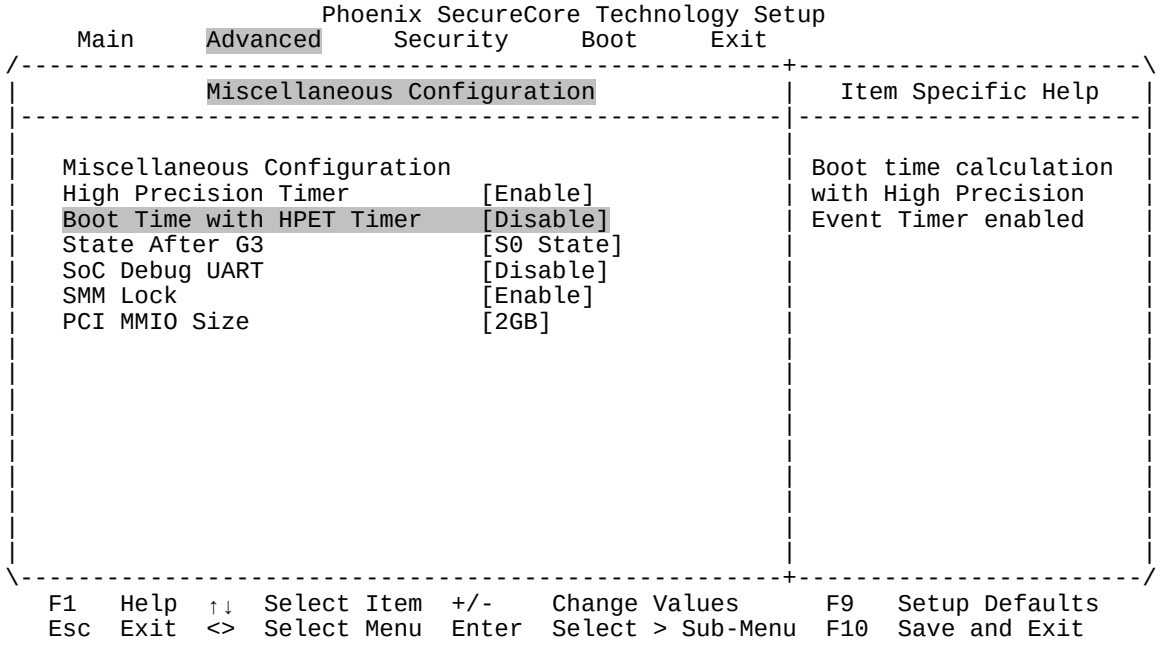
Note: This option is accessible only when LPSS DMA #1 is enabled. (See page 93.)

Advanced → Miscellaneous Configuration → High Precision Timer



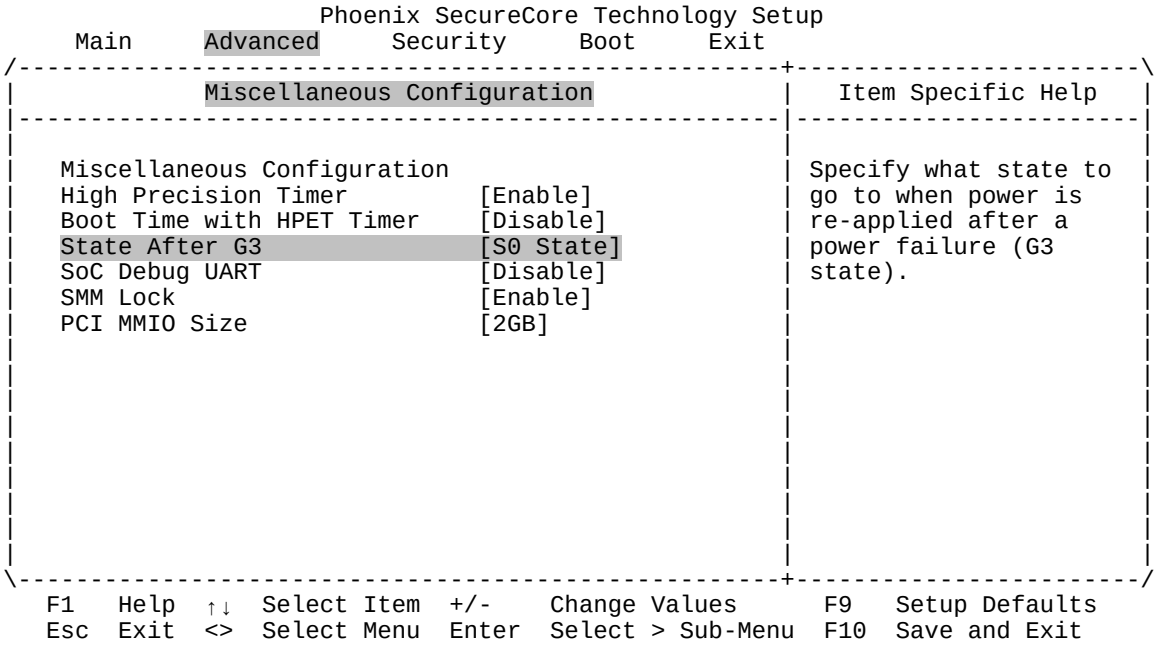
Options	Disable
	Enable (default)

Advanced → Miscellaneous Configuration → Boot Time with HPET Timer



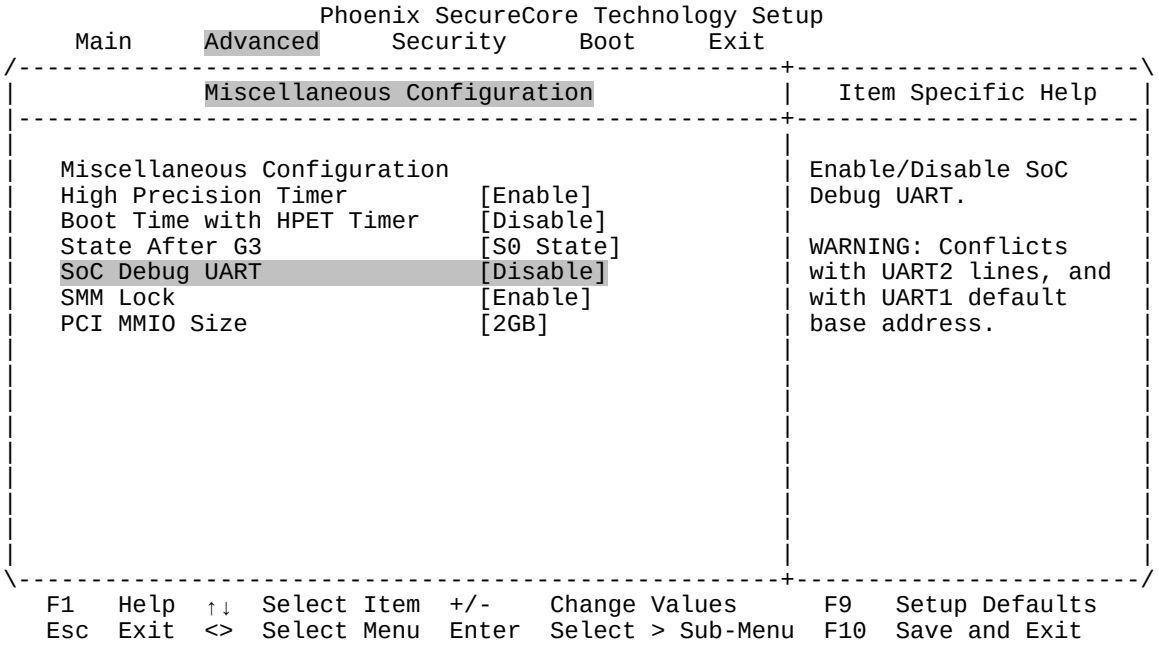
Options	**Disable (default)**
	Enable

Advanced → Miscellaneous Configuration → State After G3



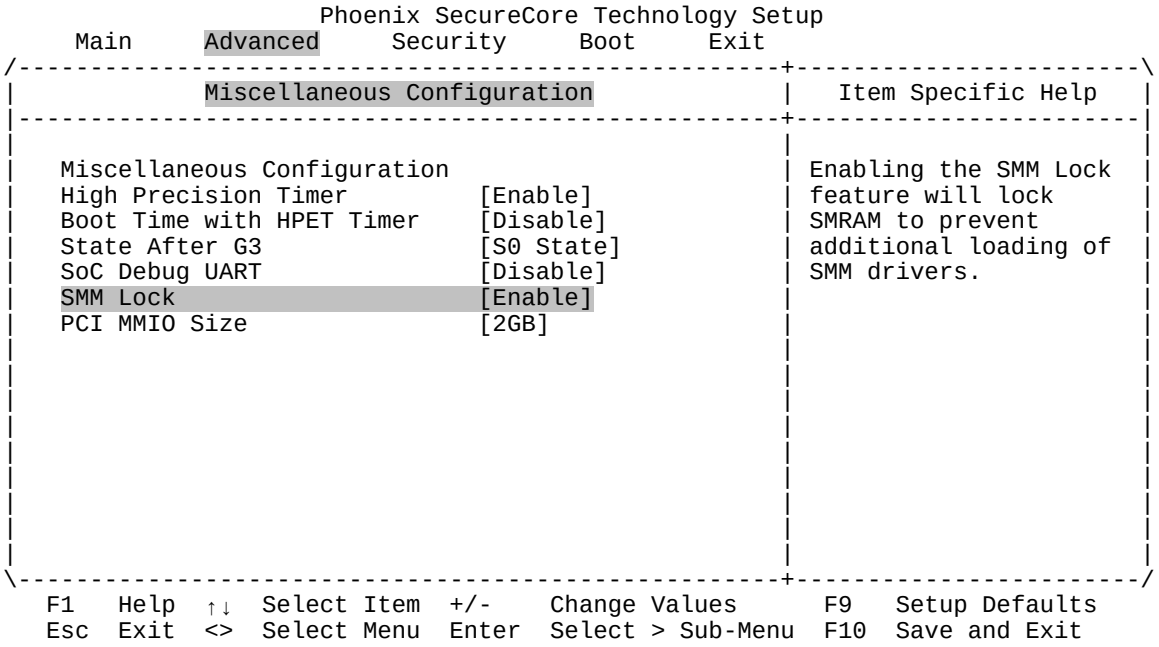
Options	**S0 State (default)**
	S5 State

Advanced → Miscellaneous Configuration → SoC Debug UART



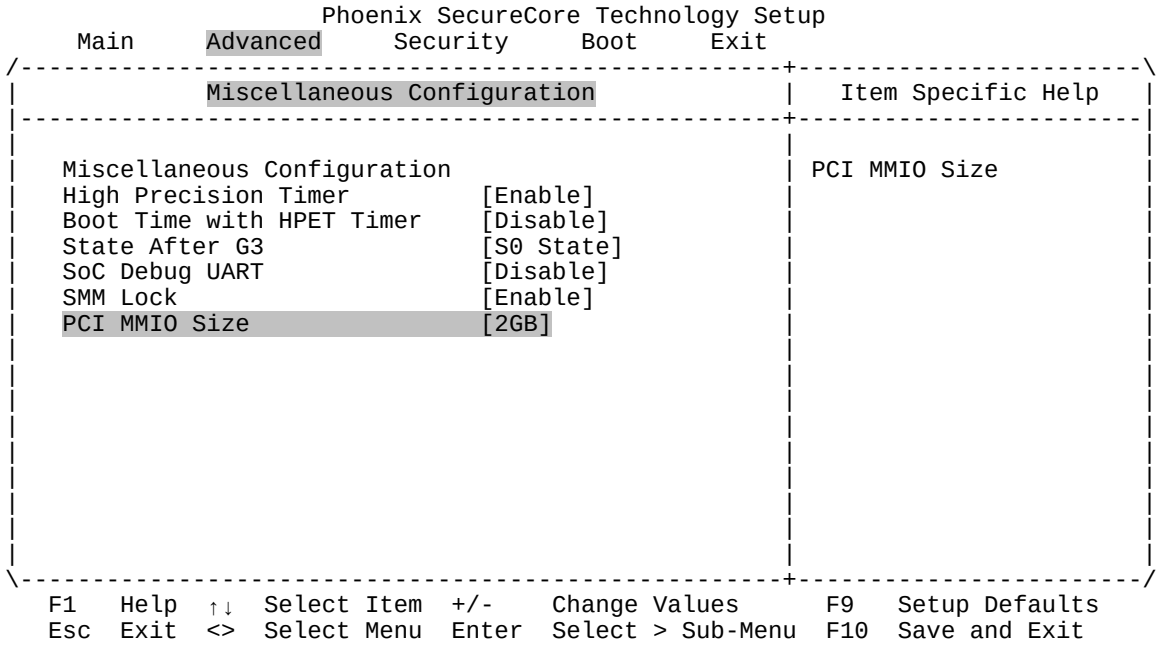
Options	**Disable (default)**
	Enable

Advanced → Miscellaneous Configuration → SMM Lock



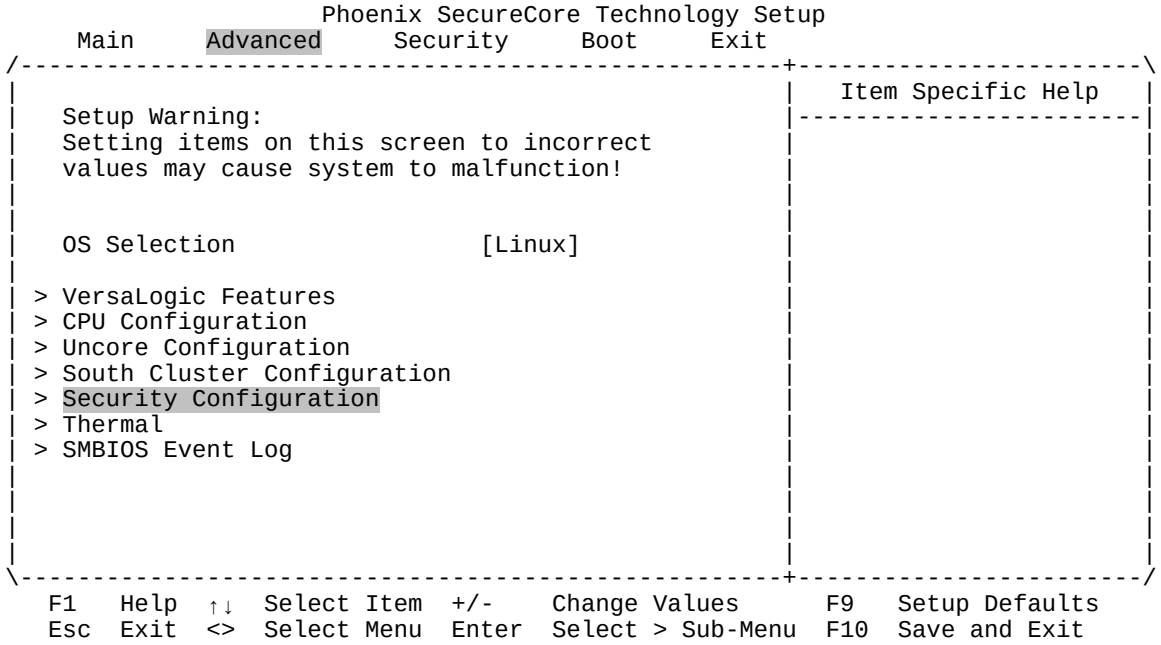
Options	Disable	Allows additional SMM (System Management Mode) drivers to be loaded
	Enable (default)	Prevents additional SMM (System Management Mode) drivers from being loaded

Advanced → Miscellaneous Configuration → PCI MMIO Size



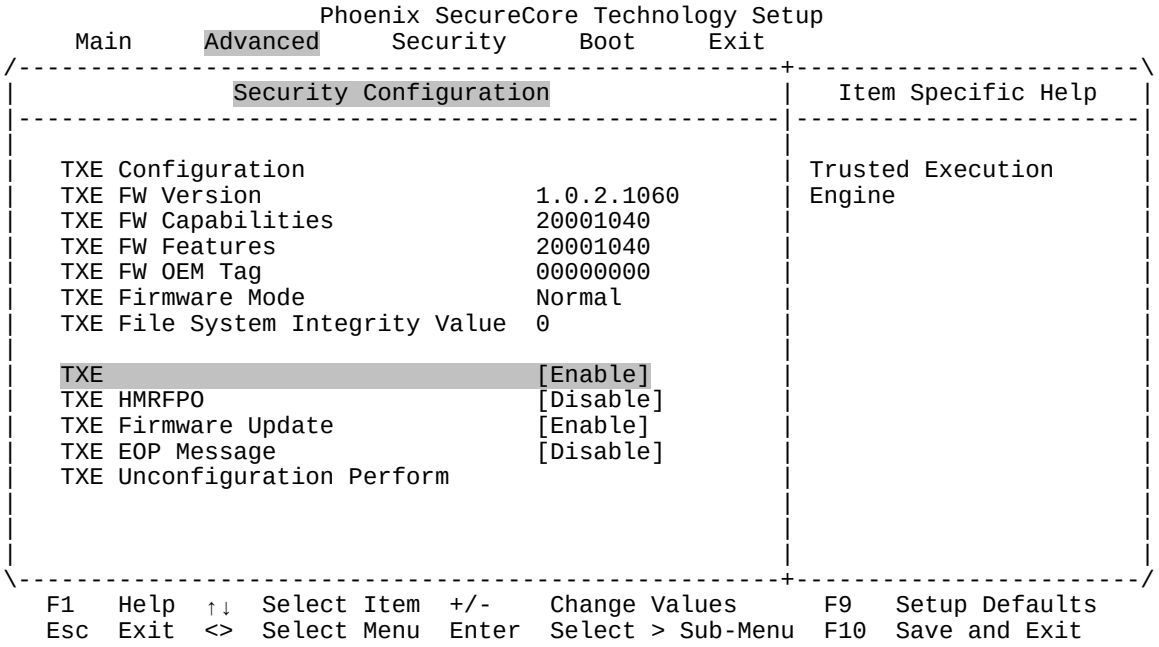
Options	**2GB (default)**
	1.5GB
	1.25GB
	1GB

Advanced → Security



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

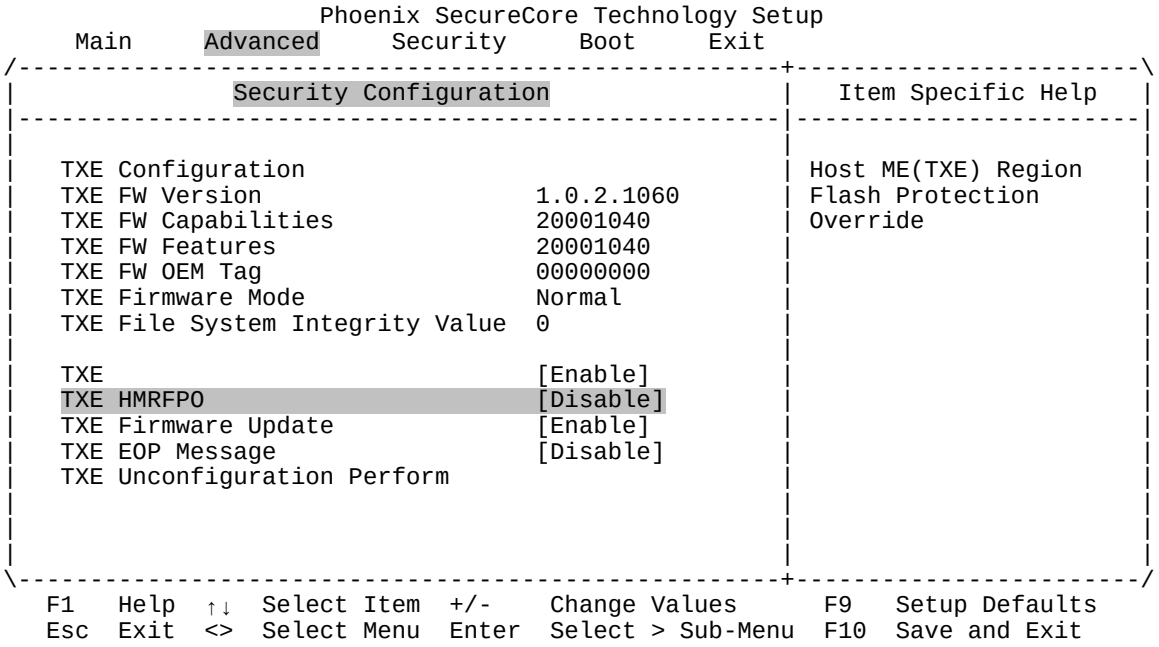
Advanced → Security Configuration → TXE



Options	Disable
	Enable (default)

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

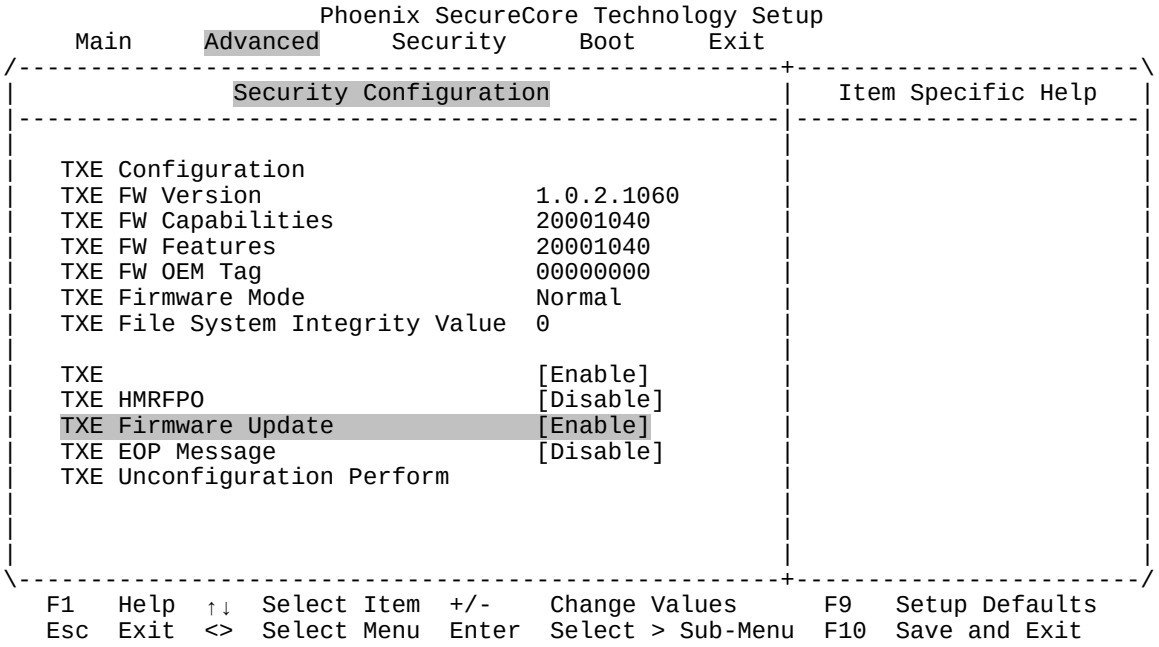
Advanced → Security Configuration → TXE HMRFPO



Options	**Disable (default)**
	Enable

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

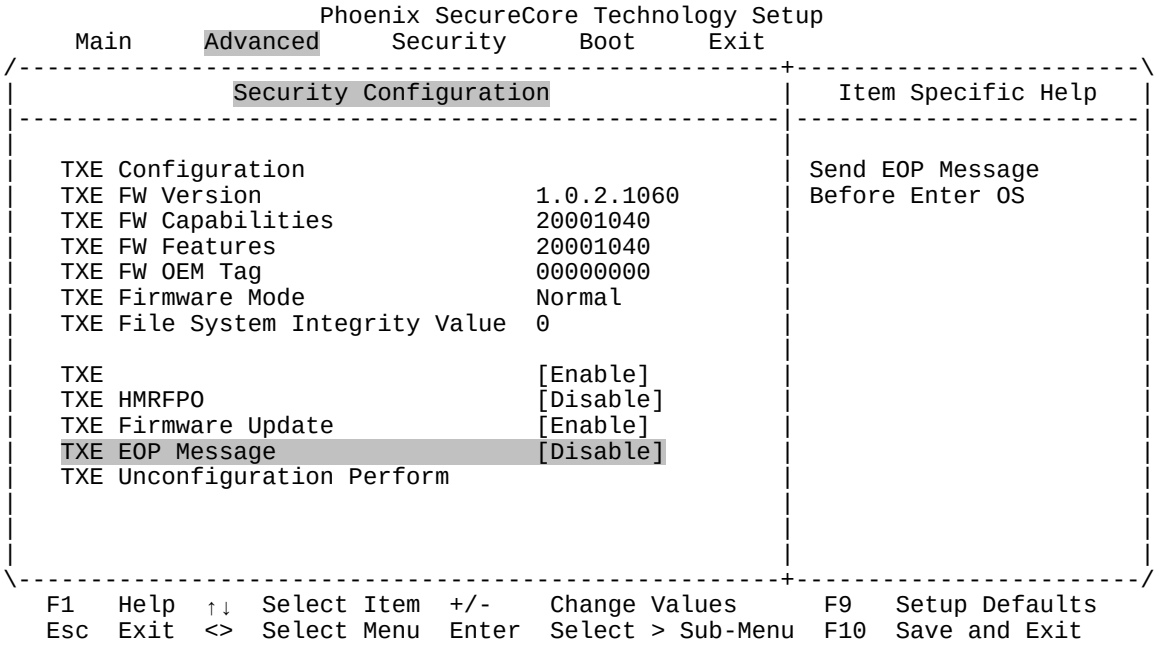
Advanced → Security Configuration → TXE Firmware Update



Options	Disable
	Enable (default)

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

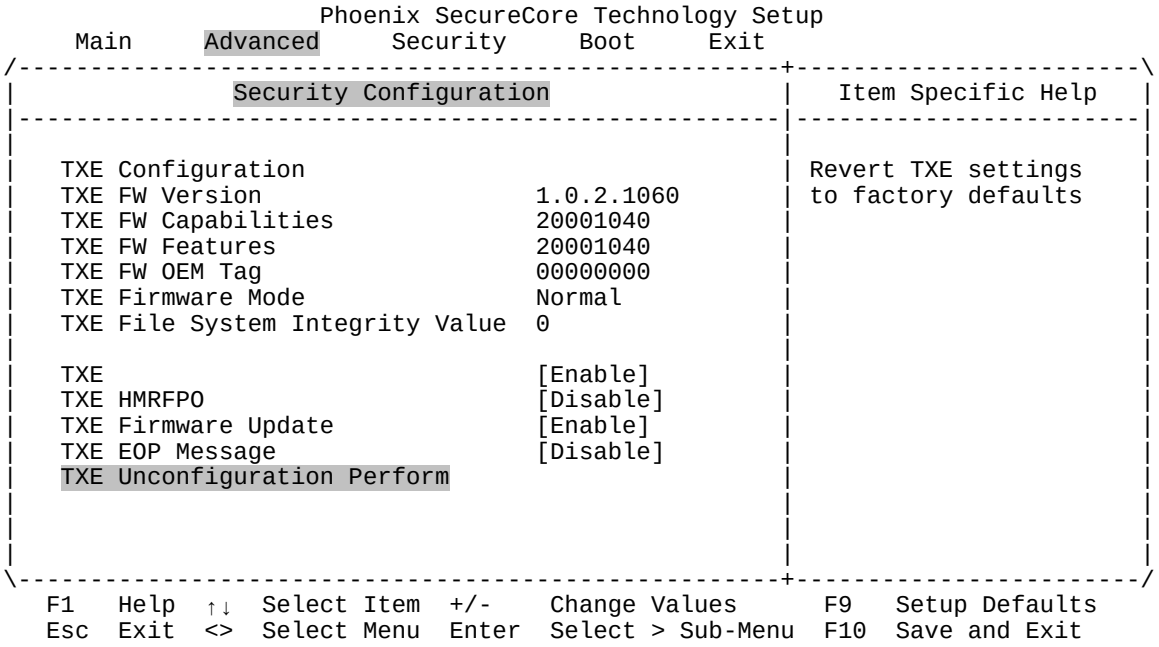
Advanced → Security Configuration → TXE EOP Message



Options	**Disable (default)**	Do not send an End-of-POST (EOP) message before entering the operating system
	Enable	Send an End-of-POST (EOP) message before entering the operating system

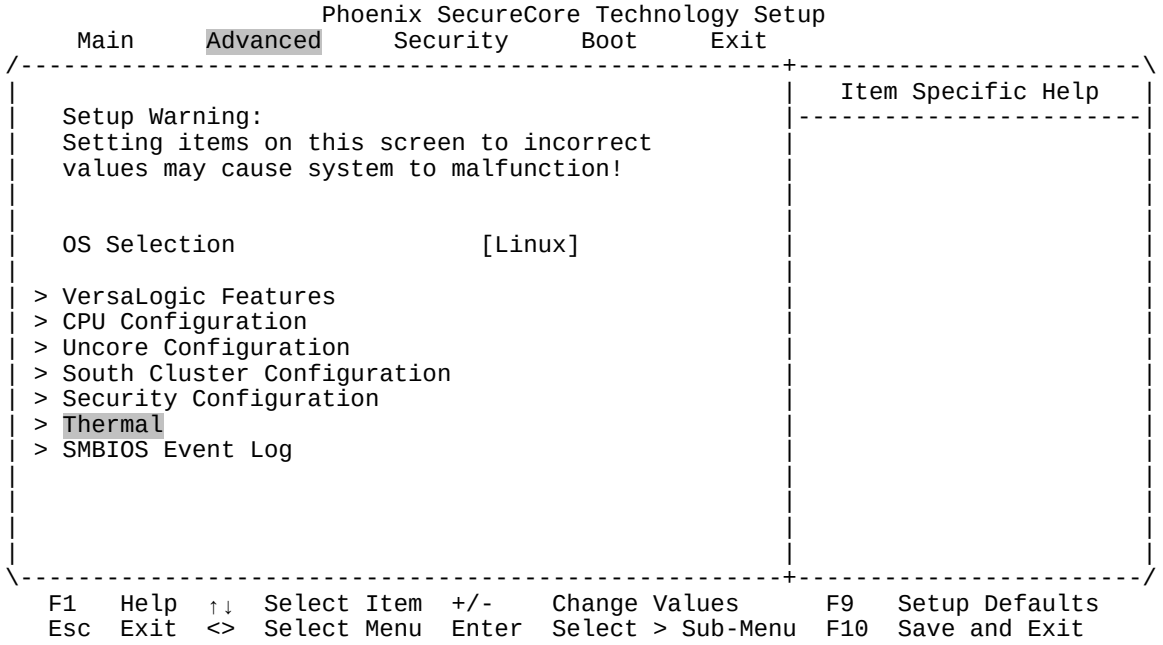
This screen also provides status on the Trusted Execution Engine (TXE).

Advanced → Security Configuration → TXE Unconfiguration Perform



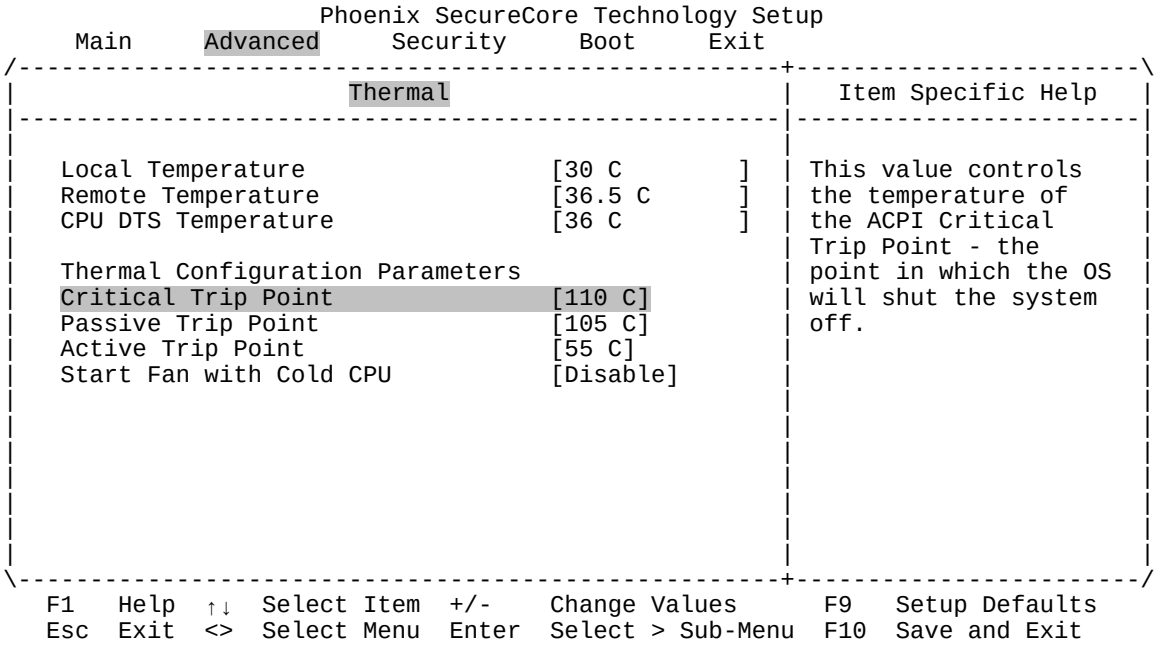
Options	**No (default)**	Do not perform a TXE unconfiguration
	Yes	Perform a TXE unconfiguration

Advanced → Thermal



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

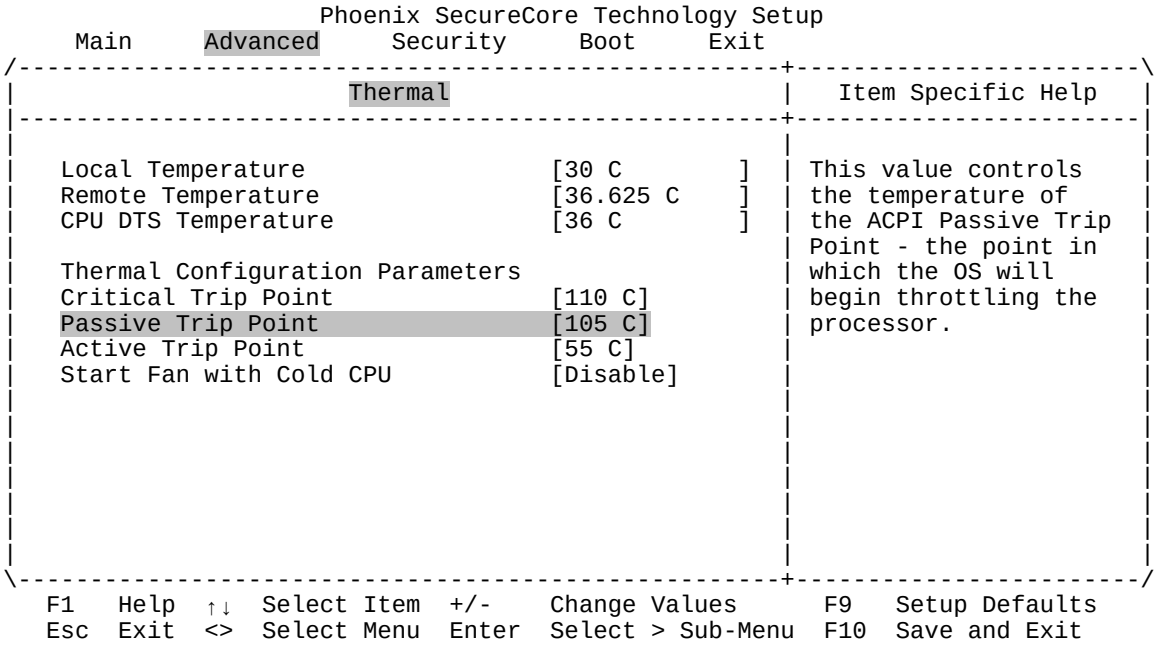
Advanced → Thermal → Critical Trip Point



Options
15 C
23 C
31 C
39 C
47 C
55 C
63 C
71 C
79 C
85 C
87 C
90 C
100 C
105 C
110 C (default)

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

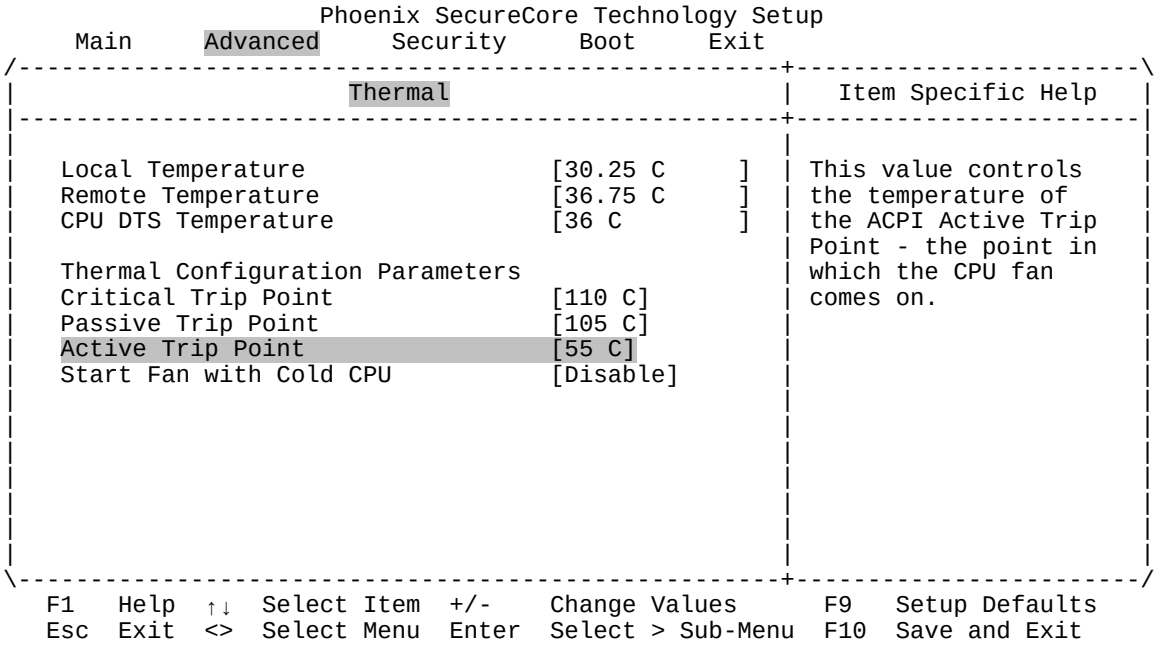
Advanced → Thermal → Passive Trip Point



Options
15 C
23 C
31 C
39 C
47 C
55 C
63 C
71 C
79 C
85 C
87 C
90 C
95 C
100 C
105 C (default)
110 C

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

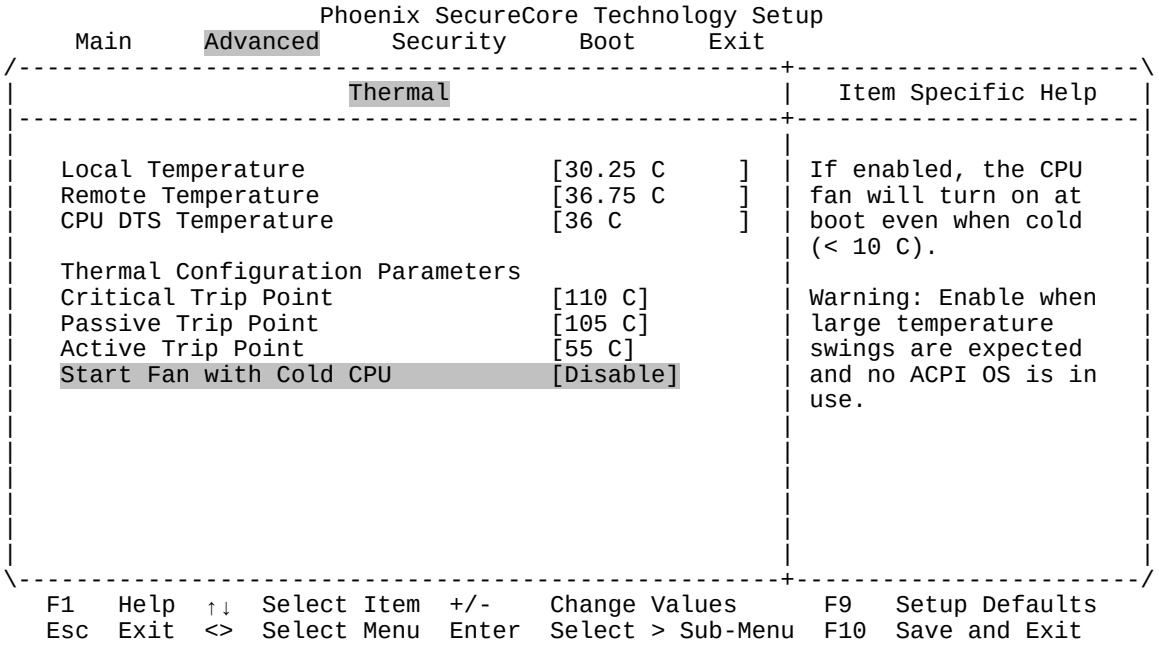
Advanced → Thermal → Active Trip Point



Options	Fan always on
	Fan always off
	15 C
	39 C
	47 C
	55 C (default)
	63 C
	71 C
	79 C
	85 C
	87 C
	90 C
	95 C
	100 C
	105 C
	110 C

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

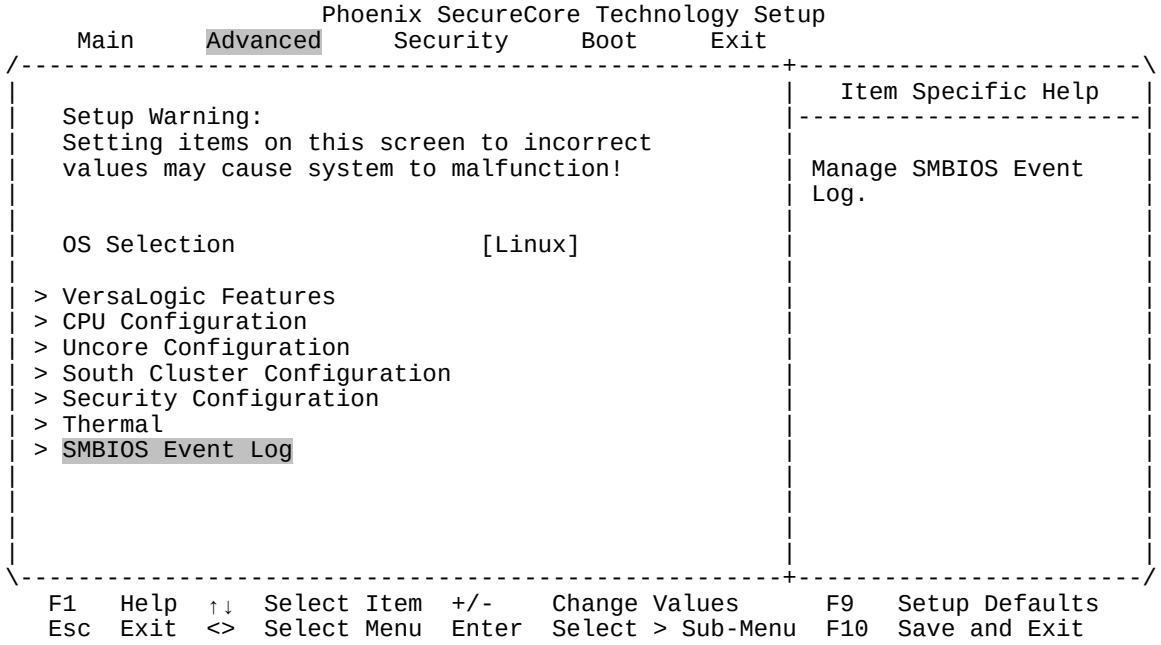
Advanced → Thermal → Start Fan With Cold CPU



Options	**Disable (default)**
	Enable

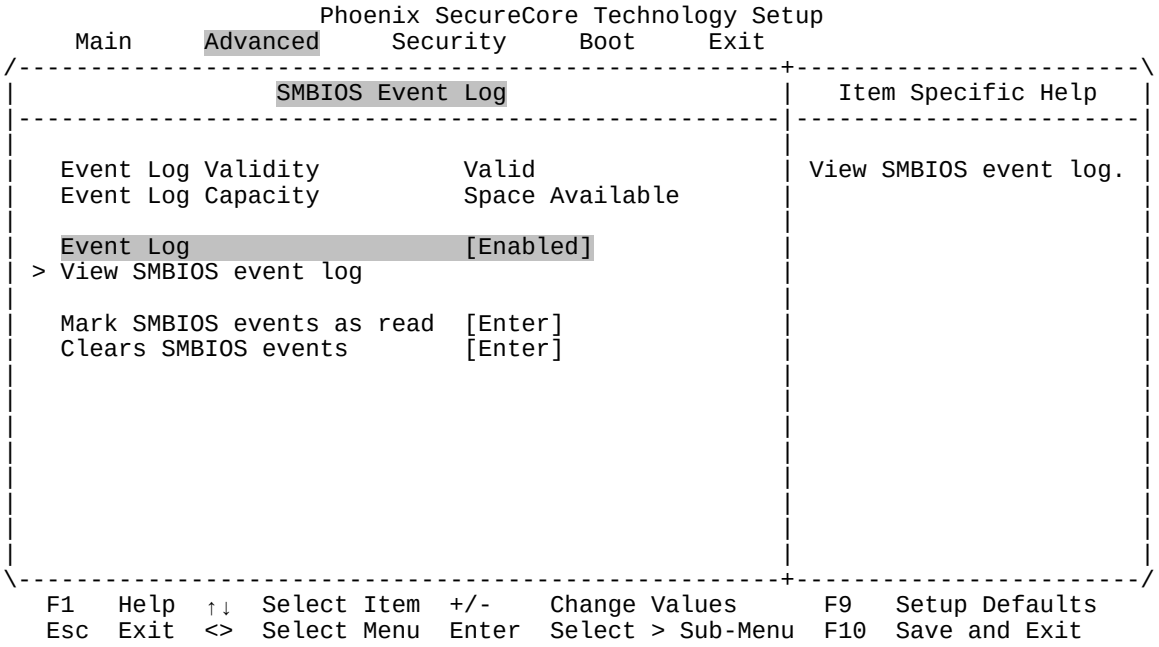
This screen also provides temperature information (local, remote, and CPU digital thermal sensor).

Advanced → SMBIOS Event Log



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

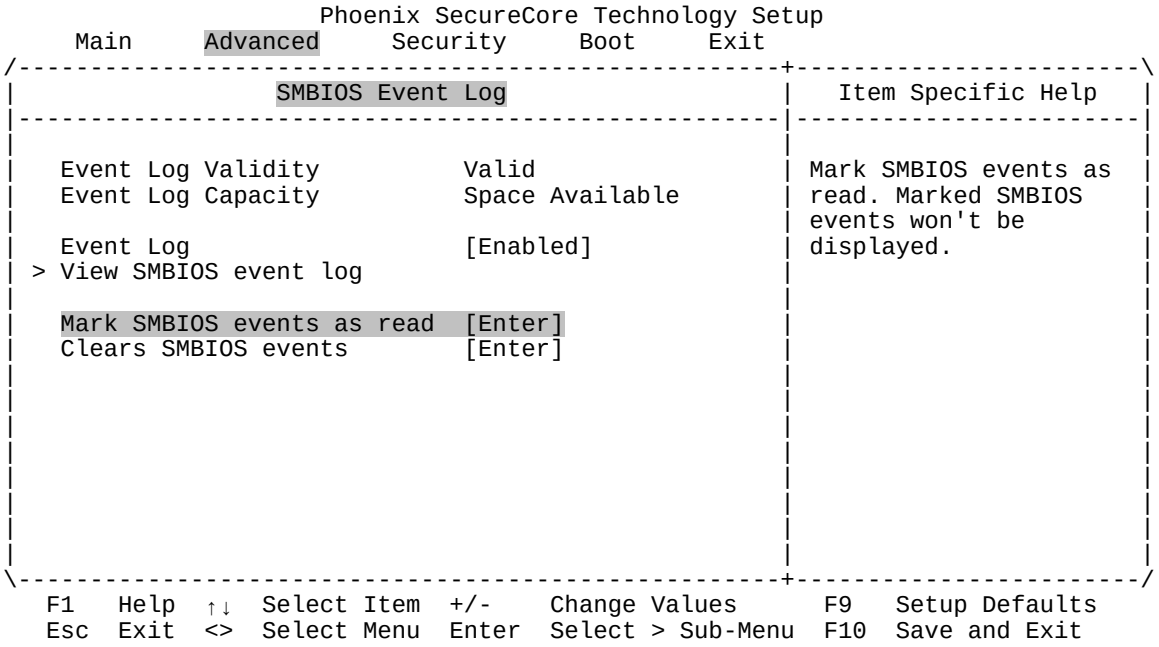
Advanced → SMBIOS Event Log → Event Log



Options	Disable
	Enable (default)

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

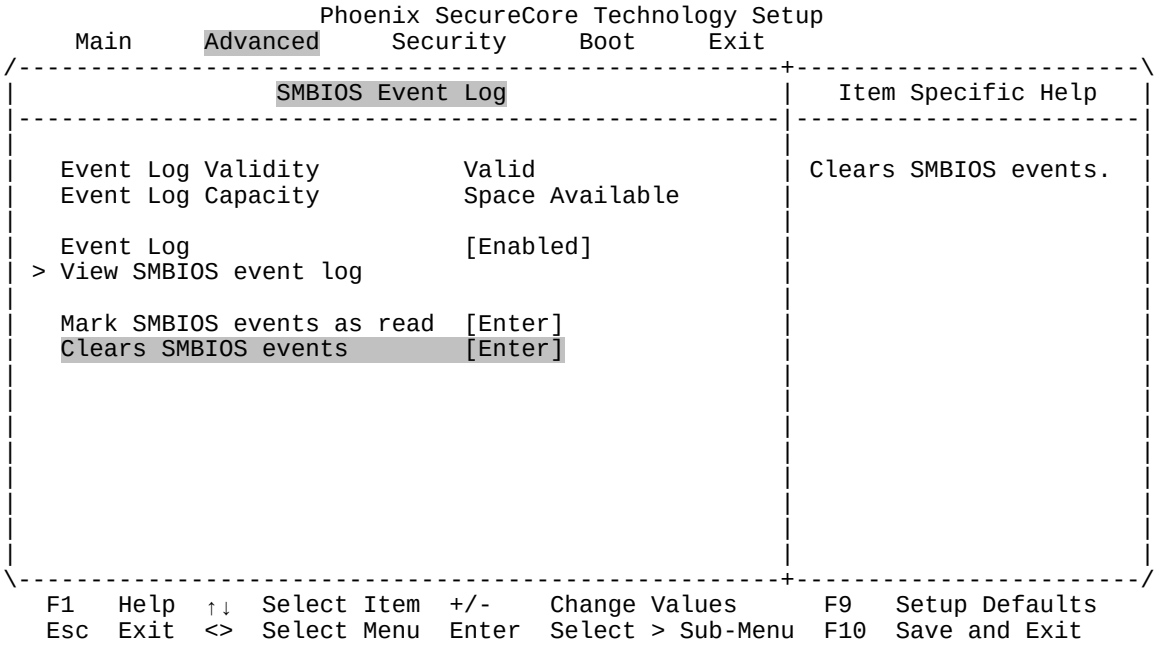
Advanced → SMBIOS Event Log → Mark SMBIOS Events As Read



Press Enter 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 Enter to clear SMBIOS events.

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

Security Menu

4

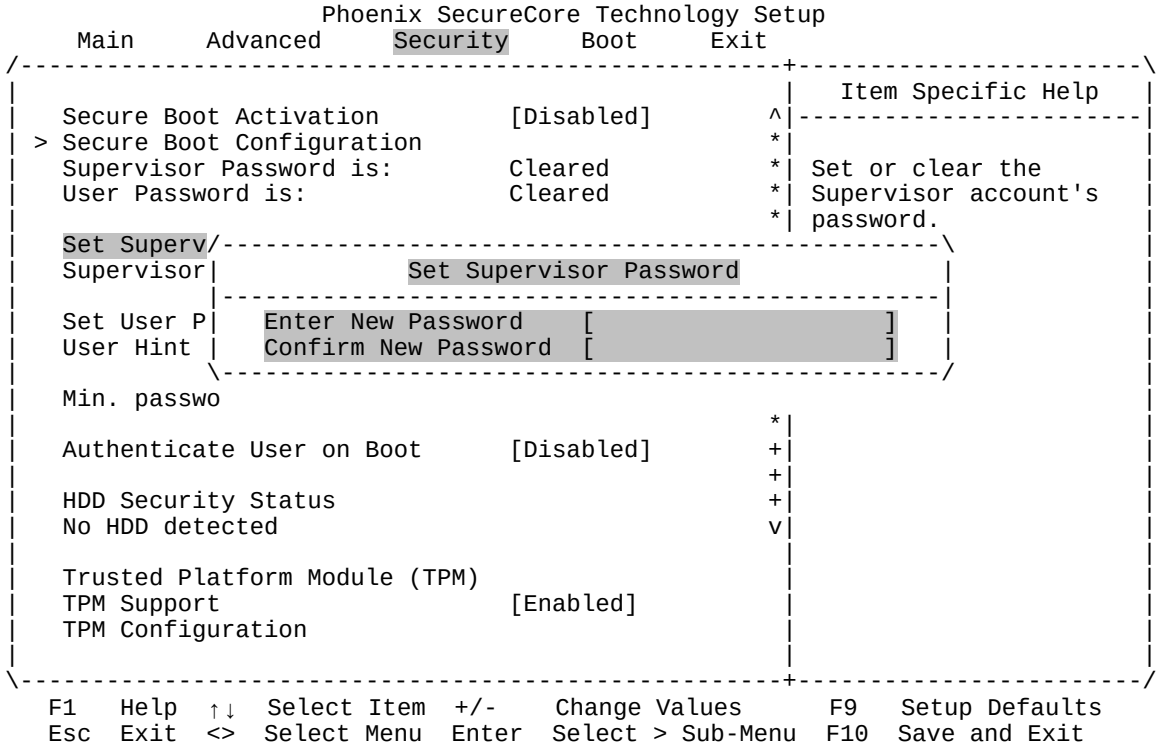
The Security menu enables you to:

- 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:

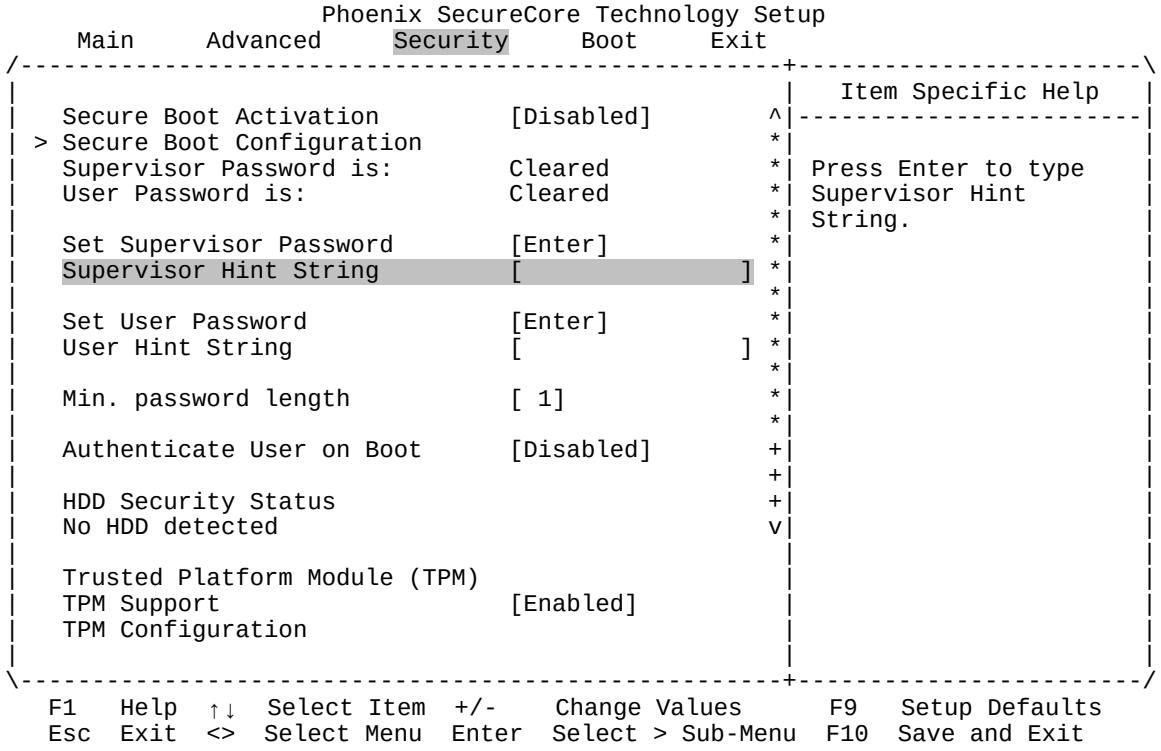
```
                    Phoenix SecureCore Technology Setup
     Main     Advanced     Security     Boot     Exit
/-------------------------------------------------------+-------------------------\
|                                                       |   Item Specific Help    |
|   Secure Boot Activation          [Disabled]        ^ |-------------------------|
| > Secure Boot Configuration                         * |                         |
|   Supervisor Password is:         Cleared           * | Set or clear the        |
|   User Password is:               Cleared           * | Supervisor account's    |
|                                                     * | password.               |
|   Set Supervisor Password         [Enter]           * |                         |
|   Supervisor Hint String          [               ] * |                         |
|                                                     * |                         |
|   Set User Password               [Enter]           * |                         |
|   User Hint String                [               ] * |                         |
|                                                     * |                         |
|   Min. password length            [ 1]              * |                         |
|                                                     * |                         |
|   Authenticate User on Boot       [Disabled]        + |                         |
|                                                     + |                         |
|   HDD Security Status                               + |                         |
|   No HDD detected                                   v |                         |
|                                                       |                         |
|   Trusted Platform Module (TPM)                       |                         |
|   TPM Support                     [Enabled]           |                         |
|   TPM Configuration                                   |                         |
|                                                       |                         |
\-------------------------------------------------------+-------------------------/
   F1   Help  ↑↓  Select Item  +/-    Change Values      F9   Setup Defaults
   Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit
```

Security → Set Supervisor Password



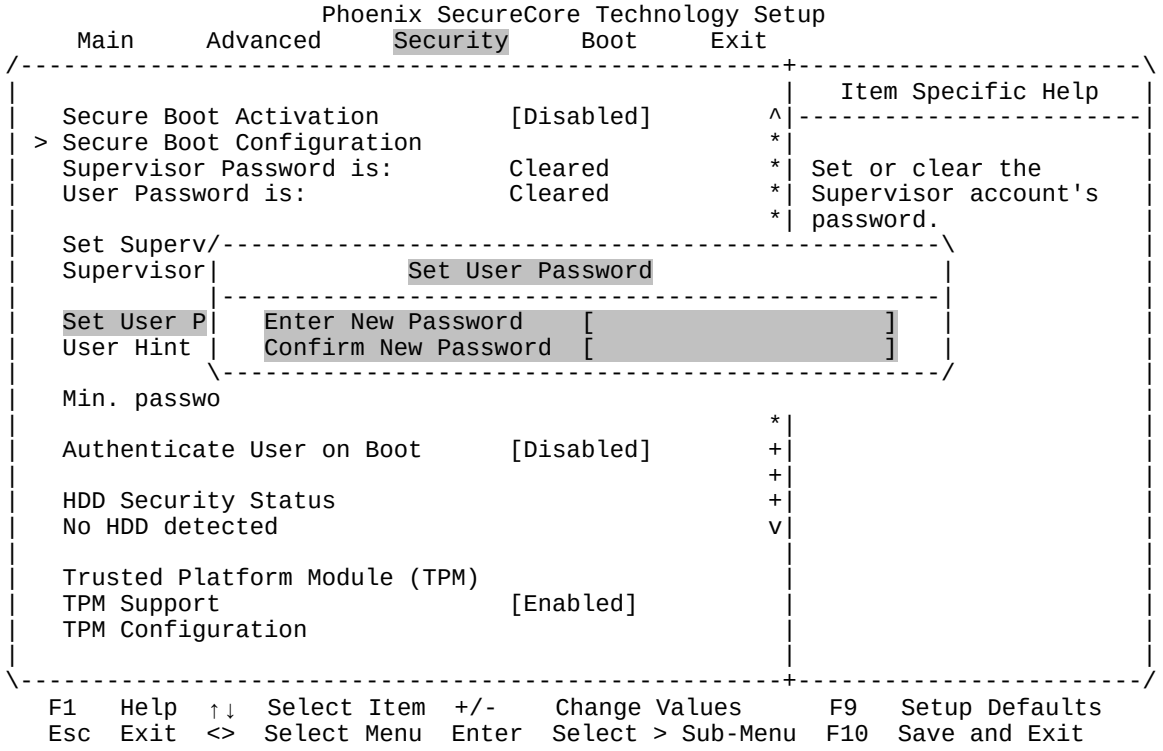
1. Type the supervisor password
2. Confirm the supervisor password

Security → Supervisor Hint String



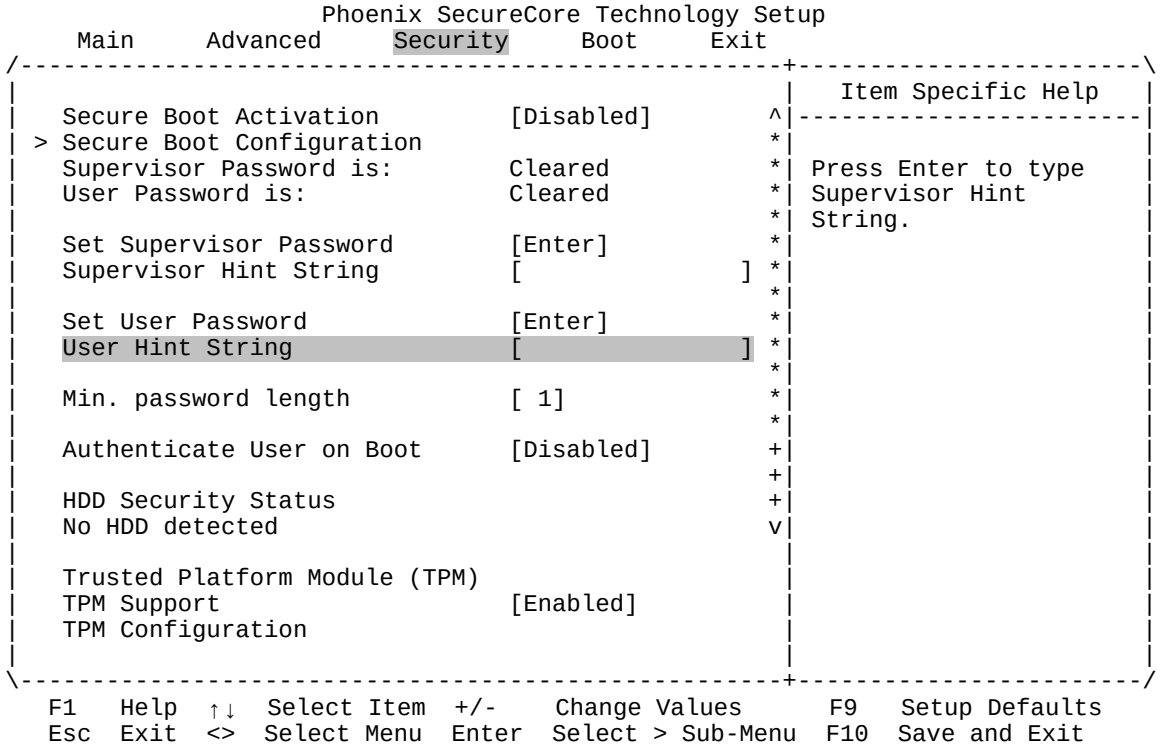
Press Enter to type the supervisor password hint string.

Security → Set User Password



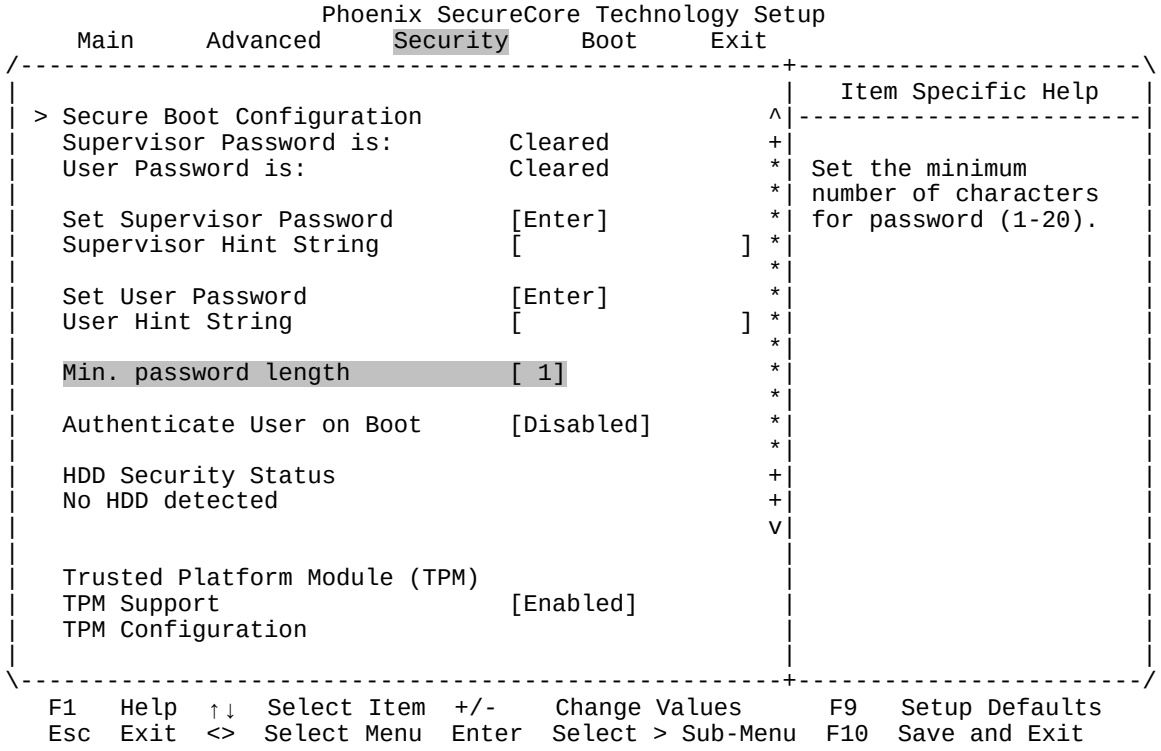
1. Type the user password
2. Confirm the user password

Security → User Hint String



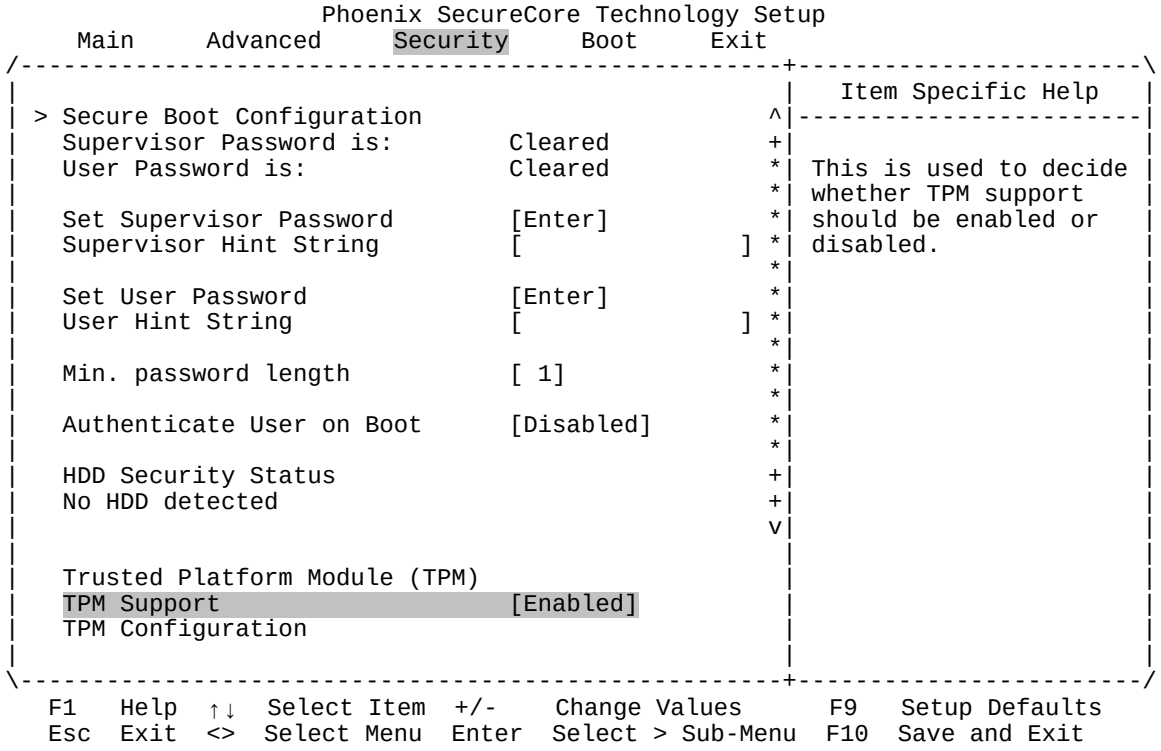
Press Enter to type the user password hint string.

Security → Min. Password Length



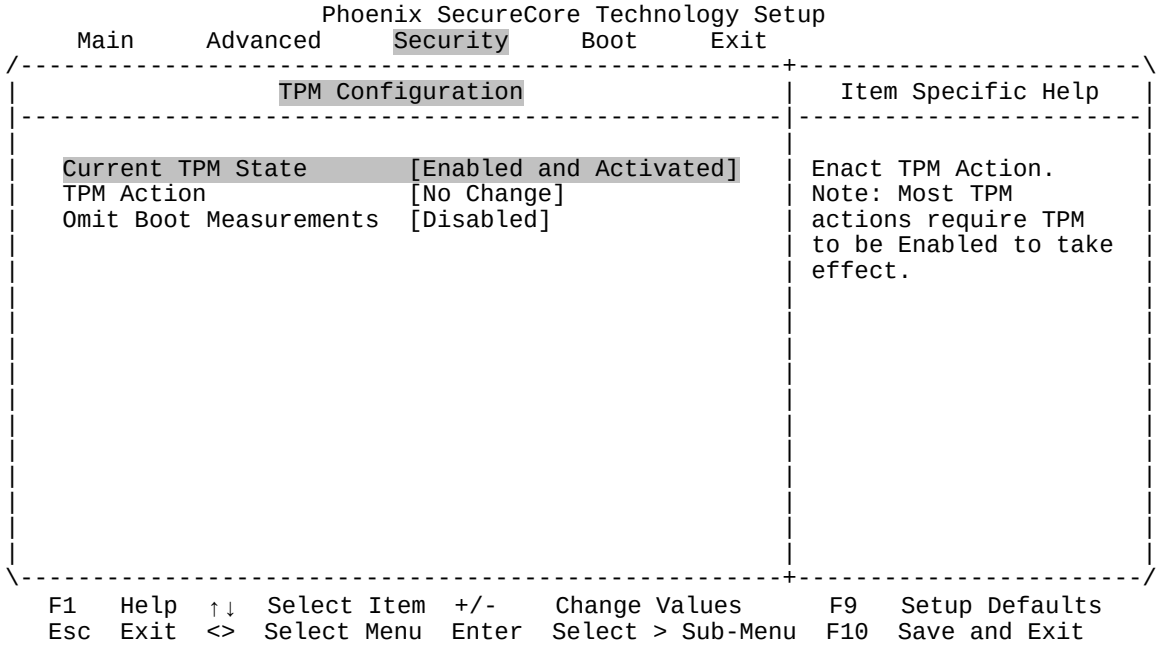
Enter the minimum number of characters for passwords. Range is 1 to 20.

Security → TPM Support

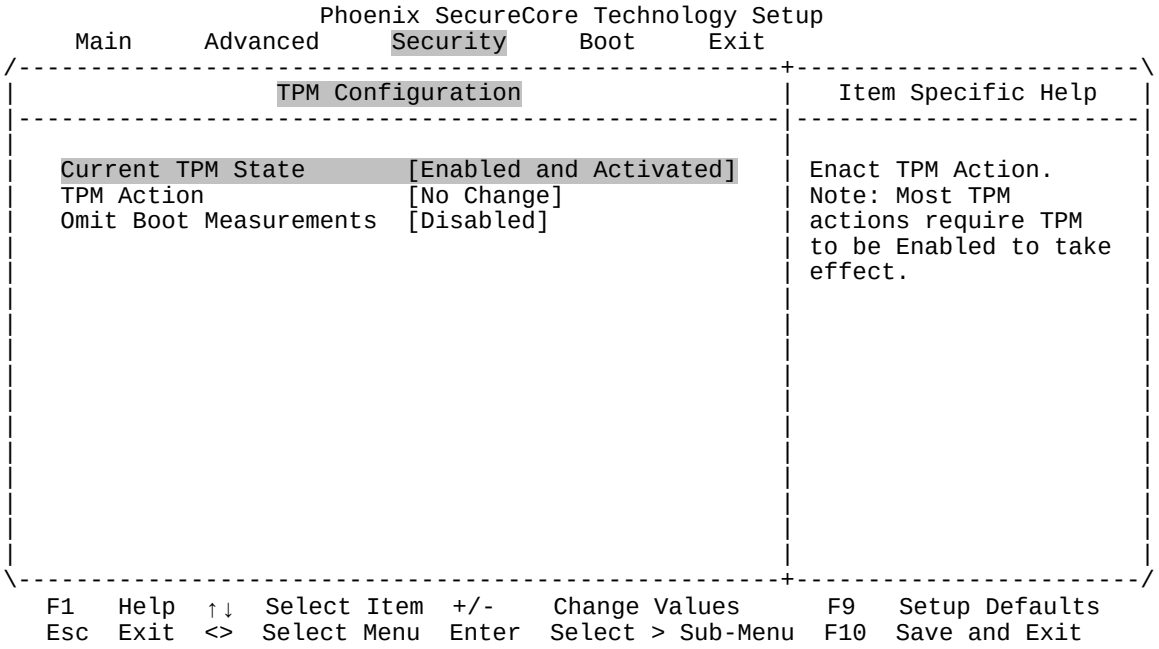


Options	Disabled	Disables TPM configuration options
	Enabled (default)	Enables TPM configuration options

Security → TPM Configuration

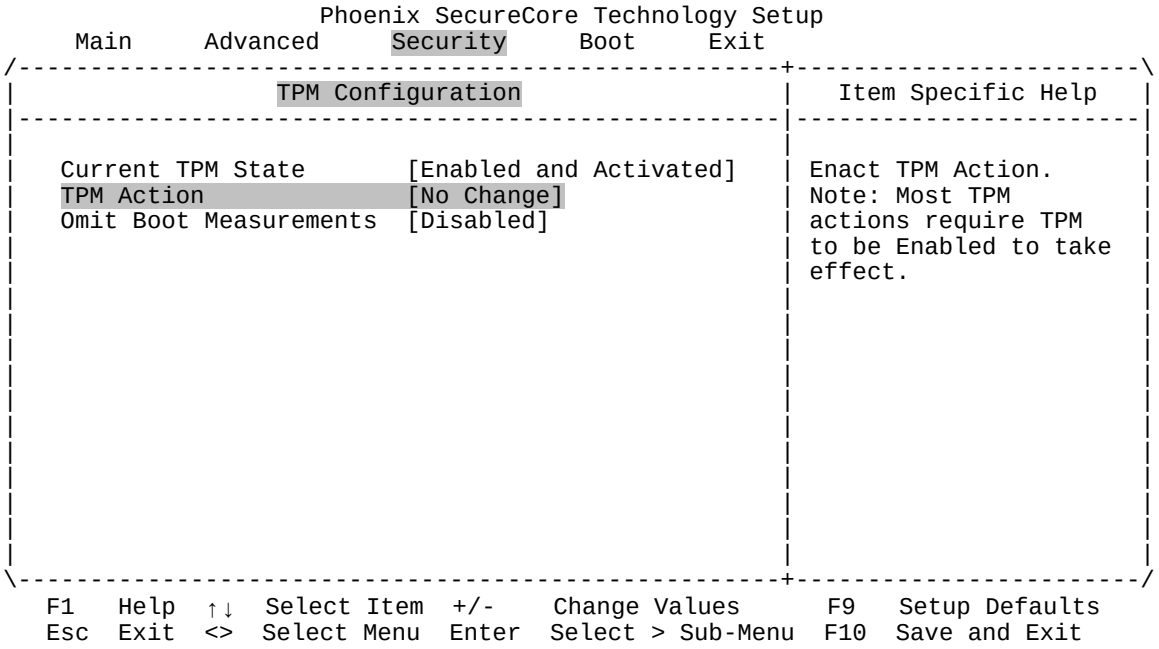


Security → TPM Configuration → Current TPM State



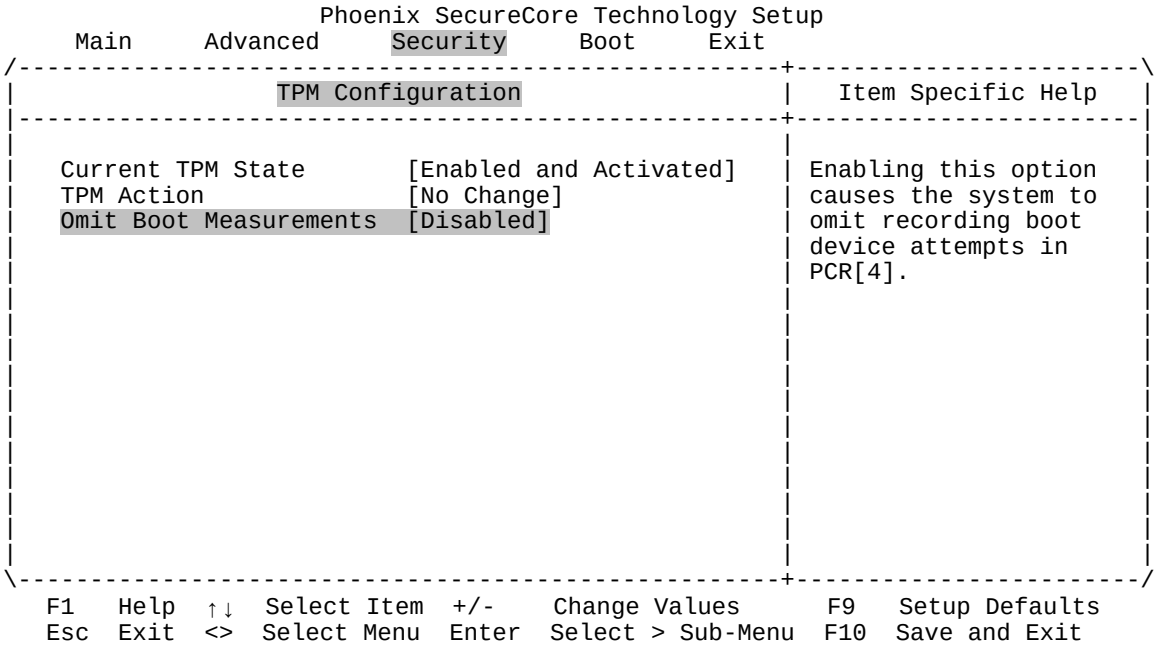
This screen displays the current state of the TPM.

Security → TPM Configuration → TPM Action



Options	**No change (default)**
	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

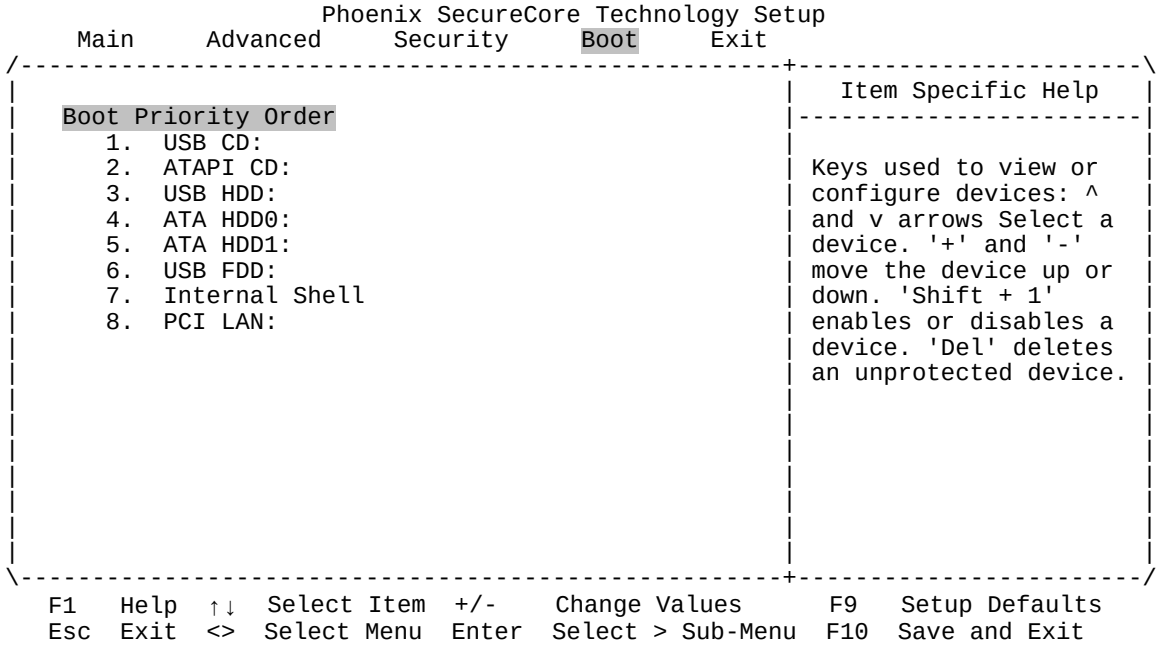
Security → TPM Configuration → Omit Boot Measurements



Options	**Disabled (default)**	Boot device attempts are recorded in PCR[4]
	Enabled	Causes the system to omit recording boot device attempts in PCR[4]

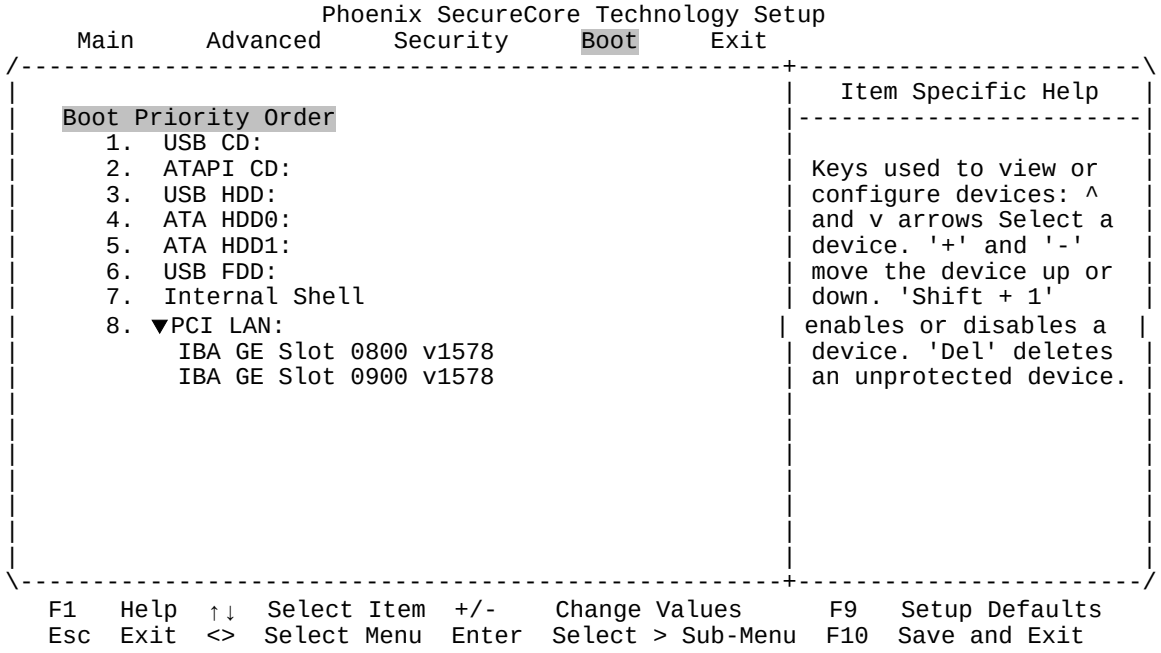
Boot Menu 5

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



Options	↑ or ↓	Selects a device from the list
	+ or -	Moves a selected device up or down the list
	Shift ⇧ + ! 1	Enables or disables a device
	Del	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.

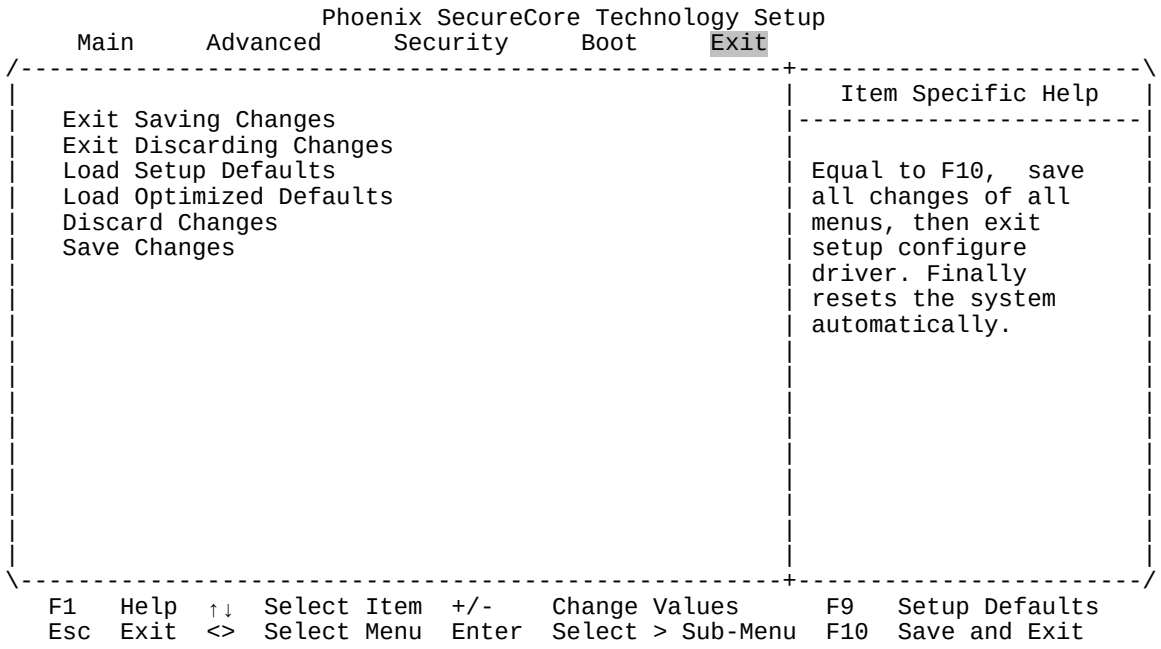


.

Exit Menu 6

The Exit menu provides options for the following:

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



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

**** End of document ****