

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





WWW.VERSALOGIC.COM

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

Copyright © 2016-2017 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.

† 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	
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
<u>Added option to configure action on boot failure.</u>	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
Main Menu.....	2
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 OPROM	23
Main → Error Manager	24
Main → Error Manager → View Error Manager Log.....	25
Main → Error Manager → Clear Error Manager Log.....	26
Advanced Menu	27
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 HMRFP0	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
Security Menu.....	119
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
Boot Menu.....	130
Exit Menu	132



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

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.

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
System Date      [01/14/2016]
System Time      [11:31:50]
> System Information
> Boot Features
> Error Manager

Item Specific Help
-----
View or set system
date.

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```


Main → System Date

```



Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
System Date      [01/14/2016]
System Time      [11:31:50]



> System Information
> Boot Features
> Error Manager



Item Specific Help
-----
View or set system
date.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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

```



Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
System Date      [01/14/2016]
System Time      [11:32:50]



> System Information
> Boot Features
> Error Manager



Item Specific Help
-----
View or set system
time.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
System Date      [01/14/2016]
System Time      [11:38:50]
> System Information
> Boot Features
> Error Manager

Item Specific Help
-----
Display System
Information.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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

Example view of System Information screen:

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
System Information
-----
BIOS Version      Bengal_3.1.0.547.r1.104 X64
Build Time        02/04/2016
Processor Type    Intel(R) Atom(TM) CPU E3845 @ 1.91GHz
Processor Speed   1.924 GHz
System Memory Speed 1333 MHz
L2 Cache RAM     2048 KB
Total Memory      4096 MB
[1]              4096 MB (DDR3- 1333) @ DIMMO
[2]              0 MB

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

Main → Boot Features

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				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	+/- Change Values	F9 Setup Defaults	
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit	

Main → Boot Features → NumLock

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features			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 +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Main → Boot Features → Timeout

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
Boot Features			Item Specific Help				
NumLock:		[On]	^	Number of seconds that P.O.S.T will wait for the user input before booting.			
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	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

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

Main → Boot Features → CSM Support

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
Boot Features			Item Specific Help				
NumLock:		[On]	^	The Compatibility Support Module supports legacy (non-UEFI) OSes and provides legacy BIOS services, such as software interrupt Int10/Int13.			
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	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

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

Main → Boot Features → Quick Boot

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
Boot Features				Item Specific Help			
NumLock:		[On]	^	Enable/Disable quick boot.			
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	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

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

Main → Boot Features → Diagnostic Splash Screen

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
NumLock:		[On]	^	If you select
Timeout		[2]	*	'Enabled' the
CSM Support		[Yes]	*	diagnostic splash
Quick Boot		[Disabled]	*	screen always
Diagnostic Splash Screen		[Enabled]	*	displays during boot.
Diagnostic Summary Screen		[Disabled]	*	If you select
BIOS Level USB		[Enabled]	*	'Disabled' the
Console Redirection		[Disabled]	*	diagnostic splash
Allow Hotkey in S4 resume		[Enabled]	+	screen does not
UEFI Boot		[Enabled]	+	display unless you
Legacy Boot		[Enabled]	v	press HOTKEY during
Boot in Legacy Video Mode		[Disabled]	*	boot.
Load OPROM		[On Demand]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
Boot Features				Item Specific Help			
NumLock:		[On]	^	Display the Diagnostic summary screen during boot.			
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]	+				
UEFI Boot		[Enabled]	+				
Legacy Boot		[Enabled]	v				
Boot in Legacy Video Mode		[Disabled]	*				
Load OPROM		[On Demand]	v				
F1	Help	↑↓	Select Item	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

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

Main → Boot Features → BIOS Level USB

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features			Item Specific Help	
NumLock:		[On]	^	Enable/Disable all
Timeout		[2]	*	BIOS support for USB
CSM Support		[Yes]	*	in order to reduce
Quick Boot		[Disabled]	*	boot time. Note that
Diagnostic Splash Screen		[Enabled]	*	this will prevent
Diagnostic Summary Screen		[Disabled]	*	using a USB keyboard
BIOS Level USB		[Enabled]	*	in setup or a USB
Console Redirection		[Disabled]	*	biometric scanner
Allow Hotkey in S4 resume		[Enabled]	+	such as a finger
UEFI Boot		[Enabled]	+	print reader to
Legacy Boot		[Enabled]	v	control access to
Boot in Legacy Video Mode		[Disabled]	*	setup, but does not
Load OPROM		[On Demand]	v	prevent the operating
			+	system from
			v	supporting such
				hardware.
F1	Help	↑↓	Select Item	+/- Change Values
F9	Setup Defaults			
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
F10	Save and Exit			

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

Main → Boot Features → Console Redirection

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
NumLock:		[On]	^	Enable/Disable
Timeout		[2]	*	Universal Console
CSM Support		[Yes]	*	Redirection.
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]	*	
Load OPROM		[On Demand]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features			Item Specific Help	
NumLock:	[On]	^	Set terminal type of	
Timeout	[2]	*	UCR.	
CSM Support	[Yes]	*		
Quick Boot	[Disabled]	*	In VT100+ mode, send	
Diagnostic Splash Screen	[Enabled]	*	Fx keys as Esc,x	
Diagnostic Summary Screen	[Disabled]	*	sequence	
BIOS Level USB	[Enabled]	*		
Console Redirection	[Enabled]	*	F1 = Esc,1	
Terminal Type	[VT100+]	*	F2 = Esc,2	
Baudrate	[115200]	*		
Flow Control	[None]	*		
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	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

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
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				
F1	Help	↑↓	Select Item	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				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]	*	
Flow Control		[None]	*	
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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
NumLock:		[On]	^	Enables Console Redirection after OS has loaded.
Timeout		[2]	*	
CSM Support		[Yes]	*	
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]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
NumLock:		[On]	^	Enable hotkey
Timeout		[2]	*	detection when system
CSM Support		[Yes]	*	resuming from
Quick Boot		[Disabled]	*	Hibernate state
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]	*	
Load OPROM		[On Demand]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
NumLock:		[On]	^	Enable the UEFI boot.
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]	+	
UEFI Boot		[Enabled]	+	
Legacy Boot		[Enabled]	v	
Boot in Legacy Video Mode		[Disabled]	*	
Load OPROM		[On Demand]	v	
F1 Help ↑↓ 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
	Enabled (default)	Enables Unified Extensible Firmware Interface (UEFI) boot

Main → Boot Features → Legacy Boot

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features				Item Specific Help
CSM Support		[Yes]	^	Enable the Legacy boot.
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]	*	
Load OPROM		[On Demand]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Main → Boot Features → Boot In Legacy Video Mode

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features			Item Specific Help	
CSM Support		[Yes]	^	Enable to force the display adapter to switch the video mode to Text Mode 3 at the end of BIOS POST for non-UEFI boot mode (Legacy Boot). Some legacy software, such as DUET, requires that the BIOS explicitly enter text video mode prior to boot.
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]	*	
Load OPROM		[On Demand]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Boot Features			Item Specific Help	
CSM Support	[Yes]	^	Load all OPROMs or on demand according to the boot device.	
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]	*		
Load OPROM	[On Demand]	v		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

```
Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
System Date      [12/31/2017]
System Time     [12:34:25]

> System Information
> Boot Features
> Error Manager

Item Specific Help
-----
Display Error Manager
Log information.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
```

Main → Error Manager → View Error Manager Log

```


Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
Error Manager
-----
View Error Manager Log [Enter]
Clear Error Manager Log [Enter]
-----
Item Specific Help
-----
Display Error Manager
Log information.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

Press  to view the Error Manager Log information.

Main → Error Manager → Clear Error Manager Log

```
Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
Error Manager
-----
View Error Manager Log  [Enter]
Clear Error Manager Log [Enter]
-----
Item Specific Help
Clear Error Manager
Log.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit
```

Press  to clear the Error Manager Log information.

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
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Graphics/Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help
-----
Select which OS will
be loaded.

Warning: Linux boot
may fail if Windows
is selected.

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit
    
```

Advanced → OS Selection

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Graphics/Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help
-----
Select which OS will
be loaded.

Warning: Linux boot
may fail if Windows
is selected.

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
VersaLogic Features		Item Specific Help	
FPGA Revision	[6]	^	The Mini Card slot can support either a PCIe Mini Card or an mSATA module. The mSATA specifications states that Pin 51 on the connector can be used to automatically detect an mSATA module. But some modules also use Pin 43 due to conflicts on Pin 51. Almost all modules will be 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.
FPGA Flags	[EXTEMP]	*	
Battery Status	[OK]	*	
Fan Speed (RPM)	[5430]	*	
Mini Card Mode	[Pin 43 or 51 mSATA Detect]	*	
UART1	[Enabled]	*	
Base Address	[3F8]	*	
IRQ	[IRQ4]	*	
Mode	[RS-232]	+	
UART2	[Enabled]	v	
Base Address	[2F8]	*	
IRQ	[IRQ3]	*	
Mode	[RS-232]	+	
F1 Help	↑↓ Select Item	+/- Change Values	
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

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

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

Advanced → VersaLogic Features → UART1

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

Options	Disabled	Disables UART1
	Enabled (default)	Enables UART1

Advanced → VersaLogic Features → UART1 → Base Address

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

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

Advanced → VersaLogic Features → UART1 → IRQ

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

VersaLogic Features		Item Specific Help
FPGA Revision	[6]	^
FPGA Flags	[EXTEMP]	*
Battery Status	[OK]	*
Fan Speed (RPM)	[5400]	*
Mini Card Mode	[Pin 43 or 51 mSATA Detect]	*
UART1	[Enabled]	*
Base Address	[3F8]	*
IRQ	[IRQ4]	*
Mode	[RS-232]	+
		+
UART2	[Enabled]	v
Base Address	[2F8]	
IRQ	[IRQ3]	*
Mode	[RS-232]	+

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

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

Advanced → VersaLogic Features → UART1 → Mode

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

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

Advanced → VersaLogic Features → UART2

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
VersaLogic Features				Item Specific Help
FPGA Revision	[6]			^
FPGA Flags	[EXTEMP]			*
Battery Status	[OK]			^
Fan Speed (RPM)	[5370]			+
Mini Card Mode	[Pin 43 or 51 mSATA Detect]			+
UART1	[Enabled]			*
Base Address	[3F8]			*
IRQ	[IRQ4]			*
Mode	[RS-232]			*
UART2	[Enabled]			*
Base Address	[2F8]			*
IRQ	[IRQ3]			*
Mode	[RS-232]			v
F1	Help	↑↓	Select Item	+/-
Esc	Exit	<>	Select Menu	Enter
			Change Values	F9
			Select > Sub-Menu	F10
			Setup Defaults	
			Save and Exit	

Options	Disabled	Disables UART2
	Enabled (default)	Enables UART2

Advanced → VersaLogic Features → UART2 → Base Address

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

VersaLogic Features		Item Specific Help
FPGA Revision	[6]	^
FPGA Flags	[EXTEMP]	*
Battery Status	[OK]	^
Fan Speed (RPM)	[5370]	+
Mini Card Mode	[Pin 43 or 51 mSATA Detect]	*
UART1	[Enabled]	*
Base Address	[3F8]	*
IRQ	[IRQ4]	*
Mode	[RS-232]	*
UART2	[Enabled]	*
Base Address	[2F8]	*
IRQ	[IRQ3]	*
Mode	[RS-232]	v

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

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

Options

Advanced → VersaLogic Features → UART2 → IRQ

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

VersaLogic Features		Item Specific Help
FPGA Revision [6]	^	Select the IRQ for UART2, or disable it.
FPGA Flags [EXTEMP]	*	
Battery Status [OK]	^	
Fan Speed (RPM) [5370]	+	
Mini Card Mode [Pin 43 or 51 mSATA Detect]	*	
UART1 [Enabled]	*	
Base Address [3F8]	*	
IRQ [IRQ4]	*	
Mode [RS-232]	*	
UART2 [Enabled]	*	
Base Address [2F8]	*	
IRQ [IRQ3]	*	
Mode [RS-232]	v	

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

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

Advanced → VersaLogic Features → UART2 → Mode

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
VersaLogic Features		Item Specific Help	
FPGA Revision	[6]	^	Selects the mode for UART2.
FPGA Flags	[EXTEMP]	*	
Battery Status	[OK]	^	
Fan Speed (RPM)	[5370]	+	
Mini Card Mode	[Pin 43 or 51 mSATA Detect]	*	
UART1	[Enabled]	*	
Base Address	[3F8]	*	
IRQ	[IRQ4]	*	
Mode	[RS-232]	*	
UART2	[Enabled]	*	
Base Address	[2F8]	*	
IRQ	[IRQ3]	*	
Mode	[RS-232]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Advanced → CPU Configuration

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Graphics/Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

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

Advanced → CPU Configuration → Execute Disable Bit

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
CPU Configuration		Item Specific Help		
CPU Configuration		Execute Disable Bit		
Execute Disable Bit		prevent certain		
AES-NI		classes of malicious		
Limit CPUID Maximum		buffer overflow		
Bi-directional PROCHOT#		attacks when combined		
VTX-2		with a supporting OS		
TMI				
DTS				
Intel Hyper-Threading Technology		Not Supported		
> CPU Power Management				
F1	Help	↑↓	Select Item	+/- Change Values
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
F9	Setup Defaults			F10 Save and Exit

Options	Disable
	Enable (default)

Advanced → CPU Configuration → AES-NI

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Configuration		Item Specific Help	
CPU Configuration		AES-NI	
Execute Disable Bit	[Enable]		
AES-NI	[Enable]		
Limit CPUID Maximum	[Disable]		
Bi-directional PROCHOT#	[Enable]		
VTX-2	[Enable]		
TMI	[Enable]		
DTS	[Enable]		
Intel Hyper-Threading Technology	Not Supported		
> CPU Power Management			
F1	Help	↑↓	Select Item +/- Change Values
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9	Setup Defaults		F10 Save and Exit

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Configuration		Item Specific Help	
CPU Configuration		When enabled, code cannot execute CPUID function > 3.	
Execute Disable Bit		[Enable]	
AES-NI		[Enable]	
Limit CPUID Maximum		[Disable]	
Bi-directional PROCHOT#		[Enable]	
VTX-2		[Enable]	
TMI		[Enable]	
DTS		[Enable]	
Intel Hyper-Threading Technology		Not Supported	
> CPU Power Management			
F1	Help	↑↓	Select Item +/- Change Values
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9	Setup Defaults		F10 Save and Exit

Options	Disable (default)
	Enable

Advanced → CPU Configuration → Bi-directional PROCHOT#

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
CPU Configuration			Item Specific Help	
CPU Configuration			When a processor thermal sensor trips (either core), the PROCHOT# will be driven.	
Execute Disable Bit			[Enable]	
AES-NI			[Enable]	
Limit CPUID Maximum			[Disable]	
Bi-directional PROCHOT#			[Enable]	
VTX-2			[Enable]	
TMI			[Enable]	
DTS			[Enable]	
Intel Hyper-Threading Technology			Not Supported	
> CPU Power Management				
F1	Help	↑↓	Select Item	+/- Change Values
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
F9	Setup Defaults			F10 Save and Exit

Options	Disable
	Enable (default)

Advanced → CPU Configuration → VTX-2

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
CPU Configuration			Item Specific Help	
CPU Configuration			To enable or disable the VTX-2 Mode support	
Execute Disable Bit			[Enable]	
AES-NI			[Enable]	
Limit CPUID Maximum			[Disable]	
Bi-directional PROCHOT#			[Enable]	
VTX-2			[Enable]	
TMI			[Enable]	
DTS			[Enable]	
Intel Hyper-Threading Technology			Not Supported	
> CPU Power Management				
F1	Help	↑↓	Select Item	+/- Change Values
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
F9	Setup Defaults			F10 Save and Exit

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

Advanced → CPU Configuration → TM1

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
CPU Configuration			Item Specific Help	
CPU Configuration			Enable/Disable TM1	
Execute Disable Bit		[Enable]		
AES-NI		[Enable]		
Limit CPUID Maximum		[Disable]		
Bi-directional PROCHOT#		[Enable]		
VTX-2		[Enable]		
TM1		[Enable]		
DTS		[Enable]		
Intel Hyper-Threading Technology		Not Supported		
> CPU Power Management				
F1	Help	↑↓	Select Item	+/- Change Values
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
F9	Setup Defaults			F10 Save and Exit

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

Advanced → CPU Configuration → DTS

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Configuration		Item Specific Help	
CPU Configuration		Enabled/Disable	
Execute Disable Bit	[Enable]	Digital Thermal Sensor	
AES-NI	[Enable]		
Limit CPUID Maximum	[Disable]		
Bi-directional PROCHOT#	[Enable]		
VTX-2	[Enable]		
TMI	[Enable]		
DTS	[Enable]		
Intel Hyper-Threading Technology	Not Supported		
> CPU Power Management			
F1	Help	↑↓	Select Item +/- Change Values
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9			Setup Defaults
F10			Save and Exit

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

Advanced → CPU Configuration → Intel Hyper-Threading Technology

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Configuration		Item Specific Help	
CPU Configuration			
Execute Disable Bit		[Enable]	
AES-NI		[Enable]	
Limit CPUID Maximum		[Disable]	
Bi-directional PROCHOT#		[Enable]	
VTX-2		[Enable]	
TMI		[Enable]	
DTS		[Enable]	
Intel Hyper-Threading Technology		Not Supported	
> CPU Power Management			
F1	Help	↑↓	Select Item +/- Change Values
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9	Setup Defaults		F10 Save and Exit



Note: This feature is not supported at this time.

Advanced → CPU Power Management

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
CPU Power Management
-----
System Power Options
Intel(R) SpeedStep(tm)      [Enable]
  Boot performance mode    [Max Performance]
Intel Turbo Boost Technology [Enable]
C-States                    [Enable]
  Enhanced C-states        [Enable]
Max C State                  [C7]
-----
Item Specific Help
-----

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

Advanced → CPU Power Management → Intel SpeedStep

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Power Management		Item Specific Help	
System Power Options			
Intel(R) SpeedStep(tm)	[Enable]	Enable processor performance states (P-States).	
Boot performance mode	[Max Performance]		
Intel Turbo Boost Technology	[Enable]		
C-States	[Enable]		
Enhanced C-states	[Enable]		
Max C State	[C7]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Disable
	Enable (default)

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Power Management		Item Specific Help	
System Power Options		Select the	
Intel(R) SpeedStep(tm)	[Enable]	performance state	
Boot performance mode	[Max Performance]	that the BIOS will	
Intel Turbo Boost Technology	[Enable]	set before OS handoff.	
C-States	[Enable]		
Enhanced C-states	[Enable]		
Max C State	[C7]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Max Performance (default)
	Max Battery

Advanced → CPU Power Management → Intel Turbo Boost Technology

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Power Management		Item Specific Help	
System Power Options			
Intel(R) SpeedStep(tm)	[Enable]	Enable to automatically allow processor cores to run faster than the base operating frequency if it's operating below power, current, and temperature specification limits.	
Boot performance mode	[Max Performance]		
Intel Turbo Boost Technology	[Enable]		
C-States	[Enable]		
Enhanced C-states	[Enable]		
Max C State	[C7]		
F1 Help ↑↓ Select Item +/- Change Values		F9 Setup Defaults	
Esc Exit <> Select Menu Enter Select > Sub-Menu		F10 Save and Exit	

Options	Disable
	Enable (default)

Advanced → CPU Power Management → C-States

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
CPU Power Management	Item Specific Help
System Power Options	Enable/Disable C States
Intel(R) SpeedStep(tm) [Enable]	
Boot performance mode [Max Performance]	
Intel Turbo Boost Technology [Enable]	
C-States [Enable]	
Enhanced C-states [Enable]	
Max C State [C7]	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Options	Disable
	Enable (default)

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
CPU Power Management		Item Specific Help	
System Power Options			
Intel(R) SpeedStep(tm)	[Enable]	Enable/Disable C1E, C2E and C4E. When enabled, CPU will switch to minimum speed when all cores enter C-State.	
Boot performance mode	[Max Performance]		
Intel Turbo Boost Technology	[Enable]		
C-States	[Enable]		
Enhanced C-states	[Enable]		
Max C State	[C7]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable
	Enable (default)

Advanced → CPU Power Management → Max C State

Phoenix SecureCore Technology Setup	
Main	Advanced
Security	Boot
Exit	
CPU Power Management	
System Power Options	
Intel(R) SpeedStep(tm)	[Enable]
Boot performance mode	[Max Performance]
Intel Turbo Boost Technology	[Enable]
C-States	[Enable]
Enhanced C-states	[Enable]
Max C State	[C7]
Item Specific Help	
This option controls the Max C State that the processor will support.	
F1 Help	↑↓ Select Item +/- Change Values
Esc Exit	<> Select Menu Enter Select > Sub-Menu F9 Setup Defaults
	F10 Save and Exit

Options	C7 (default)
	C6
	C1

Advanced → Graphics/Uncore Configuration

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection           [Linux]

> VersaLogic Features
> CPU Configuration
> Graphics/Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu F10 Save and Exit

```

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

Advanced → Graphics/Uncore Configuration → GOP Driver

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Graphics/Uncore Configuration		Item Specific Help	
GOP Configuration		^	Enable GOP Driver
GOP Driver	[Enable]	*	will unload VBIOS;
		*	Disable it will load
		*	VBIOS
IGD Configuration		*	
Integrated Graphics Device	[Enable]	*	
Primary Display	[Auto]	*	
RC6(Render Standby)	[Enable]	*	
PAVC	[LITE Mode]	*	
GTT Size	[2MB]	*	
Aperture Size	[256MB]	*	
DVMT Pre-Allocated	[64M]	+	
DVMT Total Gfx Mem	[256M]	+	
IGD Turbo	[Auto]	+	
IGD - LCD Control		v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Graphics/Uncore Configuration		Item Specific Help	
GOP Configuration		^	Enable : Enable
GOP Driver	[Enable]	*	Integrated Graphics
IGD Configuration		*	Device (IGD) when
Integrated Graphics Device	[Enable]	*	selected as the
Primary Display	[Auto]	*	Primary Video
RC6(Render Standby)	[Enable]	*	Adaptor. Disable:
PAVC	[LITE Mode]	*	Always disable IGD
GTT Size	[2MB]	*	
Aperture Size	[256MB]	*	
DVMT Pre-Allocated	[64M]	+	
DVMT Total Gfx Mem	[256M]	+	
IGD Turbo	[Auto]	+	
IGD - LCD Control		v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable
	Enable (default)

Advanced → Graphics/Uncore Configuration → Primary Display

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

Graphics/Uncore Configuration		Item Specific Help
GOP Configuration		^
GOP Driver	[Enable]	*
IGD Configuration		*
Integrated Graphics Device	[Enable]	*
Primary Display	[Auto]	*
RC6(Render Standby)	[Enable]	*
PAVC	[LITE Mode]	*
GTT Size	[2MB]	*
Aperture Size	[256MB]	*
DVMT Pre-Allocated	[64M]	+
DVMT Total Gfx Mem	[256M]	+
IGD Turbo	[Auto]	+
IGD - LCD Control		v

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

Options	Auto (default)
	IGD
	PCIe
	SG

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration		Item Specific Help		
GOP Configuration			^	Check to enable render standby support
GOP Driver	[Enable]		*	
IGD Configuration			*	
Integrated Graphics Device	[Enable]		*	
Primary Display	[Auto]		*	
RC6(Render Standby)	[Enable]		*	
PAVC	[LITE Mode]		*	
GTT Size	[2MB]		*	
Aperture Size	[256MB]		*	
DVMT Pre-Allocated	[64M]		+	
DVMT Total Gfx Mem	[256M]		+	
IGD Turbo	[Auto]		+	
IGD - LCD Control			v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	Enable (default)
	Disable

Advanced → Graphics/Uncore Configuration → PAVC

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration			Item Specific Help	
GOP Configuration			^	Enable/Disable
GOP Driver	[Enable]		*	Protected Audio Video Control
IGD Configuration			*	
Integrated Graphics Device	[Enable]		*	
Primary Display	[Auto]		*	
RC6(Render Standby)	[Enable]		*	
PAVC	[LITE Mode]		*	
GTT Size	[2MB]		*	
Aperture Size	[256MB]		*	
DVMT Pre-Allocated	[64M]		+	
DVMT Total Gfx Mem	[256M]		+	
IGD Turbo	[Auto]		+	
IGD - LCD Control			v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	Options	Description
	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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration			Item Specific Help	
GOP Configuration			^	Select the GTT Size
GOP Driver		[Enable]	*	
IGD Configuration			*	
Integrated Graphics Device		[Enable]	*	
Primary Display		[Auto]	*	
RC6(Render Standby)		[Enable]	*	
PAVC		[LITE Mode]	*	
GTT Size		[2MB]	*	
Aperture Size		[256MB]	*	
DVMT Pre-Allocated		[64M]	+	
DVMT Total Gfx Mem		[256M]	+	
IGD Turbo		[Auto]	+	
IGD - LCD Control			v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	Value	Description
	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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration			Item Specific Help	
GOP Configuration			^	Select the Aperture
GOP Driver	[Enable]		*	Size
			*	
IGD Configuration			*	
Integrated Graphics Device	[Enable]		*	
Primary Display	[Auto]		*	
RC6(Render Standby)	[Enable]		*	
PAVC	[LITE Mode]		*	
GTT Size	[2MB]		*	
Aperture Size	[256MB]		*	
DVMT Pre-Allocated	[64M]		+	
DVMT Total Gfx Mem	[256M]		+	
IGD Turbo	[Auto]		+	
			+	
IGD - LCD Control			v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	128 MB
	256 MB (default)
	512 MB

Advanced → Graphics/Uncore Configuration → DVMT Pre-Allocated

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration		Item Specific Help		
GOP Configuration			^	Select DVMT 5.0
GOP Driver	[Enable]		*	Pre-Allocated (Fixed)
			*	Graphics Memory size
			*	used by the Internal
			*	Graphics Device
IGD Configuration			*	
Integrated Graphics Device	[Enable]		*	
Primary Display	[Auto]		*	
RC6(Render Standby)	[Enable]		*	
PAVC	[LITE Mode]		*	
GTT Size	[2MB]		*	
Aperture Size	[256MB]		*	
DVMT Pre-Allocated	[64M]		+	
DVMT Total Gfx Mem	[256M]		+	
IGD Turbo	[Auto]		+	
			+	
IGD - LCD Control			v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

	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
Options	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

Phoenix SecureCore Technology Setup							
Main	Advanced	Security	Boot	Exit			
Graphics/Uncore Configuration			Item Specific Help				
GOP Configuration			^	Select DVMT5.0 Total			
GOP Driver [Enable]			*	Graphic Memory size			
			*	used by the Internal			
IGD Configuration			*	Graphics Device			
Integrated Graphics Device [Enable]			*				
Primary Display [Auto]			*				
RC6(Render Standby) [Enable]			*				
PAVC [LITE Mode]			*				
GTT Size [2MB]			*				
Aperture Size [256MB]			*				
DVMT Pre-Allocated [64M]			+				
DVMT Total Gfx Mem [256M]			+				
IGD Turbo [Auto]			+				
IGD - LCD Control			v				
F1	Help	↑↓	Select Item	+/-	Change Values	F9	Setup Defaults
Esc	Exit	<>	Select Menu	Enter	Select > Sub-Menu	F10	Save and Exit

Options	128 MB
	256 MB (default)

Advanced → Graphics/Uncore Configuration → BIA

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Graphics/Uncore Configuration
-----
RC6(Render Standby)      [Enable]      ^
PAVC                     [LITE Mode]   +
GTT Size                 [2MB]         +
Aperture Size            [256MB]       +
DVMT Pre-Allocated      [64M]         +
DVMT Total Gfx Mem      [256M]       *
IGD Turbo                [Auto]        *
                         *
IGD - LCD Control        *
BIA                      [Auto]          *
LCD Panel Type           [Auto]        *
IGD Boot Type           [Auto]        *
Panel Scaling            [Auto]        *
GMCH BLC Control        [PWM-Inverted] *
                         v
-----
F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
    
```

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Graphics/Uncore Configuration		Item Specific Help	
RC6(Render Standby)	[Enable]	^	
PAVC	[LITE Mode]	+	
GTT Size	[2MB]	+	
Aperture Size	[256MB]	+	
DVMT Pre-Allocated	[64M]	+	
DVMT Total Gfx Mem	[256M]	*	
IGD Turbo	[Auto]	*	
IGD - LCD Control		*	
BIA	[Auto]	*	
LCD Panel Type	[Auto]	*	
IGD Boot Type	[Auto]	*	
Panel Scaling	[Auto]	*	
GMCH BLC Control	[PWM-Inverted]	*	
		v	
F1	Help	↑↓	Select Item +/- Change Values
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu F9 Setup Defaults F10 Save and Exit

Auto (default)	
Options	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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration		Item Specific Help		
Primary Display	[Auto]	^	Selects display	
RC6(Render Standby)	[Enable]	+	interface for	
PAVC	[LITE Mode]	+	Integrated Graphics	
GTT Size	[2MB]	+	Device (IGD) at	
Aperture Size	[256MB]	*	system boot.	
DVMT Pre-Allocated	[64M]	*		
DVMT Total Gfx Mem	[256M]	*	If CSM is enabled:	
IGD Turbo	[Auto]	*	HDMI PortB=EFP1	
IGD - LCD Control		*	DP PortB=EFP1	
BIA	[Auto]	*	DP PortC=EFP2	
LCD Panel Type	[Auto]	*	eDP=LFP1	
IGD Boot Type	[Auto]	*	DSI PortA=LFP2	
Panel Scaling	[Auto]	+	DSI ProtC=LFP2	
GMCH BLC Control	[PWM-Inverted]	v		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration			Item Specific Help	
Primary Display	[Auto]	^	Select the LCD panel scaling option used by Internal Graphics Device.	
RC6(Render Standby)	[Enable]	+		
PAVC	[LITE Mode]	+		
GTT Size	[2MB]	+		
Aperture Size	[256MB]	*		
DVMT Pre-Allocated	[64M]	*		
DVMT Total Gfx Mem	[256M]	*		
IGD Turbo	[Auto]	*		
IGD - LCD Control		*		
BIA	[Auto]	*		
LCD Panel Type	[Auto]	*		
IGD Boot Type	[Auto]	*		
Panel Scaling	[Auto]	+		
GMCH BLC Control	[PWM-Inverted]	v		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	Auto (default)
	Centering
	Stretching

Advanced → Graphics/Uncore Configuration → GMCH BLC Control

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Graphics/Uncore Configuration			Item Specific Help	
Primary Display	[Auto]	^	Back Light Control	
RC6(Render Standby)	[Enable]	+	Setting	
PAVC	[LITE Mode]	+		
GTT Size	[2MB]	+		
Aperture Size	[256MB]	*		
DVMT Pre-Allocated	[64M]	*		
DVMT Total Gfx Mem	[256M]	*		
IGD Turbo	[Auto]	*		
IGD - LCD Control		*		
BIA	[Auto]	*		
LCD Panel Type	[Auto]	*		
IGD Boot Type	[Auto]	*		
Panel Scaling	[Auto]	+		
GMCH BLC Control	[PWM-Inverted]	v		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Advanced → South Cluster Configuration

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
South Cluster Configuration  Item Specific Help
-----
> PCI Express Configuration
> USB Configuration
> Audio Configuration
> SATA Drives
> LPSS & SCC Configuration
> Miscellaneous Configuration
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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

Advanced → PCI Express Configuration → PCIe 0 Speed

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
PCI Express Configuration
-----
PCIe 0 Speed [Auto]
PCIe 1 Speed [Gen1]
PCIe 2 Speed [Auto]
PCIe 3 Speed [Auto]
PCI Express Root Port 1 [Enable]
PCI Express Root Port 2 [Enable]
PCI Express Root Port 3 [Enable]
PCI Express Root Port 4 [Enable]
-----
Item Specific Help
Configure PCIe Speed
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

Options	Auto (default)
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCIe 1 Speed

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
PCI Express Configuration	Item Specific Help
PCIe 0 Speed [Auto] PCIe 1 Speed [Gen1] PCIe 2 Speed [Auto] PCIe 3 Speed [Auto] PCI Express Root Port 1 [Enable] PCI Express Root Port 2 [Enable] PCI Express Root Port 3 [Enable] PCI Express Root Port 4 [Enable]	Configure PCIe Speed
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Options	Auto
	Gen 1 (default)
	Gen 2

Advanced → PCI Express Configuration → PCIe 2 Speed

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
PCI Express Configuration
-----
PCIe 0 Speed      [Auto]
PCIe 1 Speed      [Gen1]
PCIe 2 Speed      [Auto]
PCIe 3 Speed      [Auto]
PCI Express Root Port 1 [Enable]
PCI Express Root Port 2 [Enable]
PCI Express Root Port 3 [Enable]
PCI Express Root Port 4 [Enable]
-----
Item Specific Help
Configure PCIe Speed
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

Options	Auto (default)
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCIe 3 Speed

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
PCI Express Configuration
-----
PCIe 0 Speed      [Auto]
PCIe 1 Speed      [Gen1]
PCIe 2 Speed      [Auto]
PCIe 3 Speed      [Auto]
PCI Express Root Port 1 [Enable]
PCI Express Root Port 2 [Enable]
PCI Express Root Port 3 [Enable]
PCI Express Root Port 4 [Enable]
-----
Item Specific Help
Configure PCIe Speed
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

Options	Auto (default)
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCI Express Root Port 1

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
PCI Express Configuration		Item Specific Help	
PCIe 0 Speed	[Auto]	Control the PCI Express Root Port.	
PCIe 1 Speed	[Gen1]		
PCIe 2 Speed	[Auto]		
PCIe 3 Speed	[Auto]		
PCI Express Root Port 1	[Enable]		
PCI Express Root Port 2	[Enable]		
PCI Express Root Port 3	[Enable]		
PCI Express Root Port 4	[Enable]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Enable (default)
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 2

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
PCI Express Configuration		Item Specific Help	
PCIe 0 Speed	[Auto]	Control the PCI Express Root Port.	
PCIe 1 Speed	[Gen1]		
PCIe 2 Speed	[Auto]		
PCIe 3 Speed	[Auto]		
PCI Express Root Port 1	[Enable]		
PCI Express Root Port 2	[Enable]		
PCI Express Root Port 3	[Enable]		
PCI Express Root Port 4	[Enable]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Enable (default)
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 3

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
PCI Express Configuration		Item Specific Help	
PCIe 0 Speed	[Auto]	Control the PCI Express Root Port.	
PCIe 1 Speed	[Gen1]		
PCIe 2 Speed	[Auto]		
PCIe 3 Speed	[Auto]		
PCI Express Root Port 1	[Enable]		
PCI Express Root Port 2	[Enable]		
PCI Express Root Port 3	[Enable]		
PCI Express Root Port 4	[Enable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Enable (default)
	Disable

Advanced → PCI Express Configuration → PCI Express Root Port 4

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
PCI Express Configuration		Item Specific Help	
PCIe 0 Speed	[Auto]	Control the PCI Express Root Port.	
PCIe 1 Speed	[Gen1]		
PCIe 2 Speed	[Auto]		
PCIe 3 Speed	[Auto]		
PCI Express Root Port 1	[Enable]		
PCI Express Root Port 2	[Enable]		
PCI Express Root Port 3	[Enable]		
PCI Express Root Port 4	[Enable]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Enable (default)
	Disable

Advanced → USB Configuration → XHCI Link Power Management

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
USB Configuration	
Item Specific Help	
xHCI Mode	[Disable]
XHCI Link Power Management	[Enable]
EHCI Controller	[Enable]
USB Per-Port Control	[Enable]
USB Port #0	[Enable]
USB Port #1	[Enable]
USB Port #2	[Enable]
USB Port #3	[Enable]
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Options	Disable
	Enable (default)

Advanced → USB Configuration → EHCI Controller

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
USB Configuration		Item Specific Help	
xHCI Mode	[Disable]	Control the USB EHCI (USB 2.0) functions.	
XHCI Link Power Management	[Enable]		
EHCI Controller	[Enable]	One EHCI controller must always be enabled	
USB Per-Port Control	[Enable]		
USB Port #0	[Enable]		
USB Port #1	[Enable]		
USB Port #2	[Enable]		
USB Port #3	[Enable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Enable (default)
	Disable

Advanced → USB Configuration → USB Per-Port Control

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
USB Configuration		Item Specific Help	
xHCI Mode	[Disable]	Control each of the USB ports (0~3) disabling	
XHCI Link Power Management	[Enable]		
EHCI Controller	[Enable]		
USB Per-Port Control	[Enable]		
USB Port #0	[Enable]		
USB Port #1	[Enable]		
USB Port #2	[Enable]		
USB Port #3	[Enable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #0

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
USB Configuration		Item Specific Help	
xHCI Mode	[Disable]	Enable/Disable USB Port #0	
XHCI Link Power Management	[Enable]	Right-angle xHCI/EHCI header (J16)	
EHCI Controller	[Enable]		
USB Per-Port Control	[Enable]		
USB Port #0	[Enable]		
USB Port #1	[Enable]		
USB Port #2	[Enable]		
USB Port #3	[Enable]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #1

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
USB Configuration		Item Specific Help	
xHCI Mode	[Disable]	Enable/Disable USB Port #1	
XHCI Link Power Management	[Enable]	CBR-5015 J4_Top (EHCI Debug port)	
EHCI Controller	[Enable]		
USB Per-Port Control	[Enable]		
USB Port #0	[Enable]		
USB Port #1	[Enable]		
USB Port #2	[Enable]		
USB Port #3	[Enable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #2

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
USB Configuration		Item Specific Help	
xHCI Mode	[Disable]	Enable/Disable USB Port #2	
XHCI Link Power Management	[Enable]	CBR-5015 J4_Bot, both J5 ports	
EHCI Controller	[Enable]		
USB Per-Port Control	[Enable]		
USB Port #0	[Enable]		
USB Port #1	[Enable]		
USB Port #2	[Enable]		
USB Port #3	[Enable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable
	Enable (default)

Advanced → USB Configuration → USB Port #3

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

USB Configuration	Item Specific Help
xHCI Mode [Disable]	Enable/Disable USB Port #3
XHCI Link Power Management [Enable]	
EHCI Controller [Enable]	Mini Card (J14)
USB Per-Port Control [Enable]	
USB Port #0 [Enable]	
USB Port #1 [Enable]	
USB Port #2 [Enable]	
USB Port #3 [Enable]	

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

Options		Disable
		Enable (default)

Advanced → Audio Configuration → Audio Controller

Phoenix SecureCore Technology Setup

Main **Advanced** Security Boot Exit

Audio Configuration	Item Specific Help
<div style="border: 1px solid gray; padding: 2px; display: inline-block;"> Audio Controller [Disable] </div>	Enable or disable the Azalia (HD Audio) device. Disabled = Azalia will be disabled Enabled = Azalia will be enabled

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

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

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Audio Configuration
-----
Audio Controller [Enable]
Azalia VCI Enable [Enable]
Azalia HDMI Codec [Enable]
-----
Item Specific Help
-----
Enable/Disable
Virtual Channel 1 of
Audio Controller
-----
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

Options	Disable
	Enable (default)

Advanced → Audio Configuration → Azalia HDMI CODEC

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
Audio Configuration
-----
Audio Controller      [Enable]
Azalia VCi Enable    [Enable]
Azalia HDMI Codec    [Enable]
-----
Item Specific Help
-----
Enable/Disable
internal HDMI codec
for Azalia
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit
    
```

Options	Disable
	Enable (default)

Advanced → SATA Drives → Chipset SATA

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
SATA Drives
-----
SATA Drives
Chipset-SATA Controller Configuration
Chipset SATA [Enable]
Chipset SATA Mode [AHCI]
-----
Item Specific Help
-----
Enables or Disables
the Chipset SATA
Controller.

SATA Port 0 ->
On-Board Connector
(J2).

SATA Port 1 -> mSATA
(J14).

Up to 3Gb/s supported
per port.
-----
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit
    
```

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

Advanced → SATA Drives → Chipset SATA Mode

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
SATA Drives
-----
SATA Drives
Chipset-SATA Controller Configuration
Chipset SATA [Enable]
Chipset SATA Mode [AHCI]
-----
Item Specific Help
-----
IDE: Compatibility
mode disables AHCI
support. AHCI:
Supports advanced
SATA features such as
Native Command
Queuing.
Warning: OS may not
boot if this setting
is changed after OS
install.
-----
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

Options	IDE
	AHCI (default)

Advanced → LPSS & SCC Configuration → LPSS Devices Mode

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
LPSS & SCC Configuration
-----
LPSS Devices Mode  [PCI Mode]
-----
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]
-----
Item Specific Help
-----
LPSS (Low Power
Subsystem) Devices
Mode Settings.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

Options	ACPI Mode
	PCI Mode (default)

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

Phoenix SecureCore Technology Setup				
Main	Advanced	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 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
LPSS & SCC Configuration		Item Specific Help	
LPSS Devices Mode	[PCI Mode]	LPSS DMA #2 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
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Disable
	Enable (default)

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

Phoenix SecureCore Technology Setup	
Main	Advanced
Security	Boot
Exit	
LPSS & SCC Configuration	
LPSS Devices Mode	[PCI Mode]
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]
Item Specific Help	
LPSS I2C #1 Support Enable\Disable	
F1 Help	↑↓ Select Item +/- Change Values
Esc Exit	<> Select Menu Enter Select > Sub-Menu
F9	Setup Defaults
F10	Save and Exit

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

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
LPSS & SCC Configuration		Item Specific Help	
LPSS Devices Mode [PCI Mode]		LPSS PWM #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 Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Phoenix SecureCore Technology Setup	
Main	Advanced
Security	Boot
Exit	
LPSS & SCC Configuration	
LPSS Devices Mode	[PCI Mode]
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]
Item Specific Help	
LPSS PWM #2 Support Enable\Disable	
F1 Help	↑↓ Select Item +/- Change Values
Esc Exit	<> Select Menu Enter Select > Sub-Menu F9 Setup Defaults
	F10 Save and Exit

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Miscellaneous Configuration		Item Specific Help	
Miscellaneous Configuration		Enable or Disable the High Precision Event Timer	
High Precision Timer	[Enable]		
Boot Time with HPET Timer	[Disable]		
State After G3	[S0 State]		
SoC Debug UART	[Disable]		
SMM Lock	[Enable]		
PCI MMIO Size	[2GB]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Options	Disable
	Enable (default)

Advanced → Miscellaneous Configuration → Boot Time with HPET Timer

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Miscellaneous Configuration		Item Specific Help	
Miscellaneous Configuration		Boot time calculation with High Precision Event Timer enabled	
High Precision Timer	[Enable]		
Boot Time with HPET Timer	[Disable]		
State After G3	[S0 State]		
SoC Debug UART	[Disable]		
SMM Lock	[Enable]		
PCI MMIO Size	[2GB]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

Options	Disable (default)
	Enable

Advanced → Miscellaneous Configuration → State After G3

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
Miscellaneous Configuration	Item Specific Help
Miscellaneous Configuration High Precision Timer [Enable] Boot Time with HPET Timer [Disable] State After G3 [S0 State] SoC Debug UART [Disable] SMM Lock [Enable] PCI MMIO Size [2GB]	Specify what state to go to when power is re-applied after a power failure (G3 state).
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

Options	S0 State (default)
	S5 State

Advanced → Miscellaneous Configuration → SoC Debug UART

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
Miscellaneous Configuration	Item Specific Help
Miscellaneous Configuration	Enable/Disable SoC Debug UART.
High Precision Timer [Enable]	
Boot Time with HPET Timer [Disable]	
State After G3 [S0 State]	
SoC Debug UART [Disable]	WARNING: Conflicts with UART2 lines, and with UART1 default base address.
SMM Lock [Enable]	
PCI MMIO Size [2GB]	
F1 Help ↑↓ Select Item +/- Change Values	F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu	F10 Save and Exit

Options	Disable (default)
	Enable

Advanced → Miscellaneous Configuration → SMM Lock

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Miscellaneous Configuration		Item Specific Help	
Miscellaneous Configuration		Enabling the SMM Lock feature will lock SMRAM to prevent additional loading of SMM drivers.	
High Precision Timer	[Enable]		
Boot Time with HPET Timer	[Disable]		
State After G3	[S0 State]		
SoC Debug UART	[Disable]		
SMM Lock	[Enable]		
PCI MMIO Size	[2GB]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
Miscellaneous Configuration | Item Specific Help
-----
Miscellaneous Configuration | PCI MMIO Size
High Precision Timer       | [Enable]
Boot Time with HPET Timer  | [Disable]
State After G3             | [S0 State]
SoC Debug UART            | [Disable]
SMM Lock                  | [Enable]
PCI MMIO Size             | [2GB]
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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

Advanced → Security

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

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

Advanced → Security Configuration → TXE

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Security Configuration
-----
TXE Configuration
TXE FW Version           1.0.2.1060
TXE FW Capabilities      20001040
TXE FW Features          20001040
TXE FW OEM Tag           00000000
TXE Firmware Mode        Normal
TXE File System Integrity Value 0

TXE [Enable]
TXE HMRFP0 [Disable]
TXE Firmware Update [Enable]
TXE EOP Message [Disable]
TXE Unconfiguration Perform

Item Specific Help
-----
Trusted Execution Engine
-----

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

Options	Disable
	Enable (default)

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

Advanced → Security Configuration → TXE HMRFP0

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Security Configuration
-----
TXE Configuration
TXE FW Version           1.0.2.1060
TXE FW Capabilities      20001040
TXE FW Features          20001040
TXE FW OEM Tag           00000000
TXE Firmware Mode        Normal
TXE File System Integrity Value 0

TXE                       [Enable]
TXE HMRFP0                 [Disable]
TXE Firmware Update        [Enable]
TXE EOP Message            [Disable]
TXE Unconfiguration Perform

Item Specific Help
Host ME(TXE) Region
Flash Protection
Override

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu F10 Save and Exit

```

Options | **Disable (default)**
 | Enable

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

Advanced → Security Configuration → TXE Firmware Update

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Security Configuration
-----
TXE Configuration
TXE FW Version           1.0.2.1060
TXE FW Capabilities      20001040
TXE FW Features          20001040
TXE FW OEM Tag           00000000
TXE Firmware Mode        Normal
TXE File System Integrity Value 0

TXE                       [Enable]
TXE HMRFP0                 [Disable]
TXE Firmware Update        [Enable]
TXE EOP Message            [Disable]
TXE Unconfiguration Perform

-----
F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu F10 Save and Exit

```

Options	Disable
	Enable (default)

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

Advanced → Security Configuration → TXE EOP Message

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Security Configuration
-----
TXE Configuration
TXE FW Version           1.0.2.1060
TXE FW Capabilities      20001040
TXE FW Features          20001040
TXE FW OEM Tag           00000000
TXE Firmware Mode        Normal
TXE File System Integrity Value 0

TXE                       [Enable]
TXE HMRFP0                 [Disable]
TXE Firmware Update        [Enable]
TXE EOP Message            [Disable]
TXE Unconfiguration Perform

Item Specific Help
-----
Send EOP Message
Before Enter OS
-----

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu F10 Save and Exit

```

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

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Security Configuration
-----
TXE Configuration
TXE FW Version           1.0.2.1060
TXE FW Capabilities      20001040
TXE FW Features          20001040
TXE FW OEM Tag           00000000
TXE Firmware Mode        Normal
TXE File System Integrity Value 0
TXE                       [Enable]
TXE HMRFP0                [Disable]
TXE Firmware Update       [Enable]
TXE EOP Message           [Disable]
TXE Unconfiguration Perform
-----
Item Specific Help
-----
Revert TXE settings
to factory defaults
-----
F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu F10 Save and Exit

```

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

Advanced → Thermal

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

Advanced → Thermal → Critical Trip Point

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Thermal		Item Specific Help	
Local Temperature	[30 C]	This value controls the temperature of the ACPI Critical Trip Point - the point in which the OS will shut the system off.	
Remote Temperature	[36.5 C]		
CPU DTS Temperature	[36 C]		
Thermal Configuration Parameters			
Critical Trip Point	[110 C]		
Passive Trip Point	[105 C]		
Active Trip Point	[55 C]		
Start Fan with Cold CPU	[Disable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Thermal			Item Specific Help	
Local Temperature		[30 C]	This value controls the temperature of the ACPI Passive Trip Point - the point in which the OS will begin throttling the processor.
Remote Temperature		[36.625 C]	
CPU DTS Temperature		[36 C]	
Thermal Configuration Parameters				
Critical Trip Point		[110 C]		
Passive Trip Point		[105 C]		
Active Trip Point		[55 C]		
Start Fan with Cold CPU		[Disable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

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

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Thermal		Item Specific Help	
Local Temperature	[30.25 C]	This value controls the temperature of the ACPI Active Trip Point - the point in which the CPU fan comes on.
Remote Temperature	[36.75 C]	
CPU DTS Temperature	[36 C]	
Thermal Configuration Parameters			
Critical Trip Point	[110 C]		
Passive Trip Point	[105 C]		
Active Trip Point	[55 C]		
Start Fan with Cold CPU	[Disable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
Thermal				Item Specific Help
Local Temperature		[30.25 C]	If enabled, the CPU fan will turn on at boot even when cold (< 10 C).
Remote Temperature		[36.75 C]	
CPU DTS Temperature		[36 C]	
Thermal Configuration Parameters				
Critical Trip Point		[110 C]		Warning: Enable when large temperature swings are expected and no ACPI OS is in use.
Passive Trip Point		[105 C]		
Active Trip Point		[55 C]		
Start Fan with Cold CPU		[Disable]		
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit				

Options	Disable (default)
	Enable

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

Advanced → SMBIOS Event Log

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
Setup Warning:
Setting items on this screen to incorrect
values may cause system to malfunction!

OS Selection [Linux]

> VersaLogic Features
> CPU Configuration
> Uncore Configuration
> South Cluster Configuration
> Security Configuration
> Thermal
> SMBIOS Event Log

Item Specific Help
-----
Manage SMBIOS Event
Log.

F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults
Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit

```

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

Advanced → SMBIOS Event Log → Event Log

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
SMBIOS Event Log
-----
Event Log Validity          Valid
Event Log Capacity         Space Available

Event Log [Enabled]
> View SMBIOS event log

Mark SMBIOS events as read [Enter]
Clears SMBIOS events      [Enter]
-----
Item Specific Help
-----
View SMBIOS event log.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
SMBIOS Event Log
-----
Event Log Validity          Valid
Event Log Capacity         Space Available

Event Log                  [Enabled]
> View SMBIOS event log

Mark SMBIOS events as read [Enter]
Clears SMBIOS events      [Enter]
-----
Item Specific Help
-----
Mark SMBIOS events as
read. Marked SMBIOS
events won't be
displayed.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

```


Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----
SMBIOS Event Log
-----
Event Log Validity          Valid
Event Log Capacity         Space Available

Event Log                  [Enabled]
> View SMBIOS event log

Mark SMBIOS events as read [Enter]
Clears SMBIOS events      [Enter]
-----
Item Specific Help
-----
Clears SMBIOS events.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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:

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Secure Boot Activation      [Disabled]      ^
> Secure Boot Configuration *
Supervisor Password is:    Cleared          *
User Password is:         Cleared          *
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 +
Trusted Platform Module (TPM)
TPM Support                 [Enabled]       v
TPM Configuration

Item Specific Help
-----
Set or clear the
Supervisor account's
password.

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

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Secure Boot Activation      [Disabled]      ^
> Secure Boot Configuration *
Supervisor Password is:    Cleared          *
User Password is:         Cleared          *
                          *
Set Superv/-----\
Supervisor |                Set Supervisor Password
          |-----|
Set User P | Enter New Password  [          ]
User Hint  | Confirm New Password [          ]
          |-----|
Min. passwo
          |
Authenticate User on Boot  [Disabled]      +
          |
HDD Security Status      +
No HDD detected          +
          |
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

```

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

Security → Supervisor Hint String


```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Secure Boot Activation      [Disabled]      ^
> Secure Boot Configuration
Supervisor Password is:    Cleared      *
User Password is:         Cleared      *
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 +
Trusted Platform Module (TPM)
TPM Support                 [Enabled]   v
TPM Configuration

Item Specific Help
-----
Press Enter to type
Supervisor Hint
String.

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

Press  to type the supervisor password hint string.

Security → Set User Password

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Secure Boot Activation      [Disabled]      ^
> Secure Boot Configuration  *
Supervisor Password is:    Cleared          *
User Password is:          Cleared          *
                          *
Set Superv/-----\
Supervisor|              Set User Password
          |-----|
Set User P| Enter New Password [          ]
User Hint | Confirm New Password [          ]
          |-----|
Min. passwo
          *
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

```

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

Security → User Hint String


```

Phoenix SecureCore Technology Setup
Main      Advanced  Security  Boot      Exit
-----
Secure Boot Activation      [Disabled]      ^
> Secure Boot Configuration *
Supervisor Password is:    Cleared         *
User Password is:         Cleared         *
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 +
Trusted Platform Module (TPM)
TPM Support                 [Enabled]      v
TPM Configuration

Item Specific Help
-----
Press Enter to type
Supervisor Hint
String.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

Press  to type the user password hint string.

Security → Min. Password Length

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
> Secure Boot Configuration
Supervisor Password is:      Cleared
User Password is:           Cleared

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

Trusted Platform Module (TPM)
TPM Support                  [Enabled]
TPM Configuration

Item Specific Help
-----
+
* Set the minimum
* number of characters
* for password (1-20).
*
+
+
v

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

Security → TPM Support

```

Phoenix SecureCore Technology Setup
Main      Advanced  Security  Boot      Exit
-----
> Secure Boot Configuration
Supervisor Password is:      Cleared
User Password is:           Cleared

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

Trusted Platform Module (TPM)
TPM Support                  [Enabled]
TPM Configuration

Item Specific Help
-----
* This is used to decide
* whether TPM support
* should be enabled or
* disabled.

F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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

Security → TPM Configuration

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
TPM Configuration		Item Specific Help	
Current TPM State	[Enabled and Activated]	Enact TPM Action. Note: Most TPM actions require TPM to be Enabled to take effect.	
TPM Action	[No Change]		
Omit Boot Measurements	[Disabled]		
F1 Help	↑↓ Select Item	+/- Change Values	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

Security → TPM Configuration → Current TPM State

```

Phoenix SecureCore Technology Setup
Main   Advanced   Security   Boot   Exit
-----
TPM Configuration
-----
Current TPM State [Enabled and Activated]
TPM Action        [No Change]
Omit Boot Measurements [Disabled]
-----
Item Specific Help
-----
Enact TPM Action.
Note: Most TPM
actions require TPM
to be Enabled to take
effect.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

This screen displays the current state of the TPM.

Security → TPM Configuration → TPM Action

```

Phoenix SecureCore Technology Setup
Main    Advanced    Security    Boot    Exit
-----
TPM Configuration
-----
Current TPM State      [Enabled and Activated]
TPM Action             [No Change]
Omit Boot Measurements [Disabled]
-----
Item Specific Help
-----
Enact TPM Action.
Note: Most TPM
actions require TPM
to be Enabled to take
effect.
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
    
```

	No change (default)
	Enable
	Disable
	Activate
	Deactivate
	Clear
	Enable and Activate
	Disable and Deactivate
	Set Owner Install, with state=True
Options	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

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
TPM Configuration	
Current TPM State	[Enabled and Activated]
TPM Action	[No Change]
Omit Boot Measurements	[Disabled]
Item Specific Help	
Enabling this option causes the system to omit recording boot device attempts in PCR[4].	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit	

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








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

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Boot Priority Order
1.  USB CD:
2.  ATAPI CD:
3.  USB HDD:
4.  ATA HDD0:
5.  ATA HDD1:
6.  USB FDD:
7.  Internal Shell
8.  PCI LAN:

Item Specific Help
-----
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  ↑↓  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
	 or 	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.

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Boot Priority Order
1.  USB CD:
2.  ATAPI CD:
3.  USB HDD:
4.  ATA HDD0:
5.  ATA HDD1:
6.  USB FDD:
7.  Internal Shell
8.  ▼PCI LAN:
    IBA GE Slot 0800 v1578
    IBA GE Slot 0900 v1578

Item Specific Help
-----
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  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
    
```

The Exit menu provides options for the following:




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

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
Exit Saving Changes
Exit Discarding Changes
Load Setup Defaults
Load Optimized Defaults
Discard Changes
Save Changes

Item Specific Help
-----
Equal to F10, save
all changes of all
menus, then exit
setup configure
driver. Finally
resets the system
automatically.

F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
    
```

Exit Saving Changes	Save all changes in all menus, exit setup, and perform a reset; same as 
Exit Discarding Changes	Exit Setup without saving changes; same as 
Load Setup Defaults	Load standard default values; same as 
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 ***