

BIOS Reference Manual

REV. June 2018

BayCat (VL-EPM-31)

Intel® Atom™-based Single Board Computer with Dual Ethernet, Video, USB, SATA, Serial I/O, Digital I/O, Trusted Platform Module security, Counter/Timers, Mini PCIe, mSATA, PCI/104-Plus Interface, and SPX.





WWW.VERSALOGIC.COM

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

Copyright © 2016-2018 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 utility for the EPM-31 BayCat Board.

BIOS Version	BIOS ID String	Comments
1.03	BayCat_3.1.0.791.103_RC1	Updated for Rev 1.03
1.01	BayCat_3.1.0.547.r1.101	Updated ISA IRQ Options
1.01	BayCat_3.1.0.547.r1.101	First release of document

Support Page

The [BayCat 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.

Repair Service

If your product requires service, you must obtain a Returned Material Authorization (RMA) number by calling 503-747-2261. Be ready to provide the following information:

- Your name, the name of your company, your phone number, and e-mail address
- The name of a technician or engineer that can be contacted if any questions arise
- The quantity of items being returned
- The model and serial number (barcode) of each item
- A detailed description of the problem
- Steps you have taken to resolve or recreate the problem
- The return shipping address

Warranty Repair All parts and labor charges are covered, including return shipping charges for UPS Ground delivery to United States addresses.

Non-warranty Repair All approved non-warranty repairs are subject to diagnosis and labor charges, parts charges and return shipping fees. Specify the shipping method you prefer and provide a purchase order number for invoicing the repair.



Note: Mark the RMA number clearly on the outside of the box before returning.

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	40
Advanced → CPU Configuration → Execute Disable Bit.....	41
Advanced → CPU Configuration → AES-NI.....	42
Advanced → CPU Configuration → Limit CPUID Maximum.....	43
Advanced → CPU Configuration → Bi-directional PROCHOT#	44
Advanced → CPU Configuration → VTX-2.....	45
Advanced → CPU Configuration → TM1	46
Advanced → CPU Configuration → DTS.....	47
Advanced → CPU Configuration → Intel Hyper-Threading Technology	48
Advanced → CPU Power Management	49
Advanced → CPU Power Management → Intel SpeedStep	50
Advanced → CPU Power Management → Intel Turbo Boost Technology	52
Advanced → CPU Power Management → C-States	53
Advanced → CPU Power Management → Max C State	55

Advanced → Graphics/Uncore Configuration	56
Advanced → Graphics/Uncore Configuration → GOP Driver	57
Advanced → Graphics/Uncore Configuration → Integrated Graphics Device ..	58
Advanced → Graphics/Uncore Configuration → Primary Display	59
Advanced → Graphics/Uncore Configuration → RC6 (Render Standby).....	60
Advanced → Graphics/Uncore Configuration → PAVC.....	61
Advanced → Graphics/Uncore Configuration → GTT Size.....	62
Advanced → Graphics/Uncore Configuration → Aperture Size	63
Advanced → Graphics/Uncore Configuration → DVMT Pre-Allocated	64
Advanced → Graphics/Uncore Configuration → DVMT Total Gfx Mem	65
Advanced → Graphics/Uncore Configuration → IGD Turbo.....	66
Advanced → Graphics/Uncore Configuration → BIA.....	67
Advanced → Graphics/Uncore Configuration → LCD Panel Type	68
Advanced → Graphics/Uncore Configuration → IGD Boot Type	69
Advanced → Graphics/Uncore Configuration → Panel Scaling.....	70
Advanced → Graphics/Uncore Configuration → GMCH BLC Control	71
Advanced → South Cluster Configuration.....	72
Advanced → PCI Express Configuration → PCIe 0 Speed	73
Advanced → PCI Express Configuration → PCIe 1 Speed	74
Advanced → PCI Express Configuration → PCIe 2 Speed	75
Advanced → PCI Express Configuration → PCIe 3 Speed	76
Advanced → PCI Express Configuration → PCI Express Root Port 1.....	77
Advanced → PCI Express Configuration → PCI Express Root Port 2.....	78
Advanced → PCI Express Configuration → PCI Express Root Port 3.....	79
Advanced → PCI Express Configuration → PCI Express Root Port 4.....	80
Advanced → USB Configuration → XHCI Link Power Management.....	81
Advanced → USB Configuration → EHCI Controller	82
Advanced → USB Configuration → USB Per-Port Control.....	83
Advanced → USB Configuration → USB Port #0.....	84
Advanced → USB Configuration → USB Port #1.....	85
Advanced → USB Configuration → USB Port #2.....	86
Advanced → USB Configuration → USB Port #3.....	87
Advanced → Audio Configuration → Audio Controller	88
Advanced → Audio Configuration → Azalia VCi Enable.....	89
Advanced → Audio Configuration → Azalia HDMI CODEC	90
Advanced → SATA Drives → Chipset SATA.....	91
Advanced → SATA Drives → Chipset SATA Mode	92
Advanced → LPSS & SCC Configuration → LPSS Devices Mode.....	93
Advanced → LPSS & SCC Configuration → SCC SDIO Support.....	94
Advanced → LPSS & SCC Configuration → SCC SD Card Support	95
Advanced → LPSS & SCC Configuration → SD SDR 25 Support.....	96
Advanced → LPSS & SCC Configuration → SD SDR 50 Support.....	97
Advanced → LPSS & SCC Configuration → LPSS DMA #1 Support	98
Advanced → LPSS & SCC Configuration → LPSS DMA #2 Support	99
Advanced → LPSS & SCC Configuration → LPSS I2C #1 Support	100
Advanced → LPSS & SCC Configuration → LPSS PWM #1 Support.....	101
Advanced → LPSS & SCC Configuration → LPSS PWM #2 Support.....	102
Advanced → Miscellaneous Configuration → High Precision Timer.....	103

Advanced → Miscellaneous Configuration → Boot Time with HPET Timer .	104
Advanced → Miscellaneous Configuration → State After G3	105
Advanced → Miscellaneous Configuration → SoC Debug UART	106
Advanced → Miscellaneous Configuration → SMM Lock	107
Advanced → Miscellaneous Configuration → PCI MMIO Size	108
Advanced → Security	109
Advanced → Security Configuration → TXE	110
Advanced → Security Configuration → TXE HMRFP0	111
Advanced → Security Configuration → TXE Firmware Update	112
Advanced → Security Configuration → TXE EOP Message	113
Advanced → Security Configuration → TXE Unconfiguration Perform	114
Advanced → Thermal	115
Advanced → Thermal → Critical Trip Point	116
Advanced → Thermal → Passive Trip Point	117
Advanced → Thermal → Active Trip Point	118
Advanced → Thermal → Start Fan With Cold CPU	119
Advanced → SMBIOS Event Log	120
Advanced → SMBIOS Event Log → Event Log	121
Advanced → SMBIOS Event Log → Mark SMBIOS Events As Read	122
Advanced → SMBIOS Event Log → Clear SMBIOS Events	123
Security Menu	124
Security → Set Supervisor Password	125
Security → Supervisor Hint String	126
Security → Set User Password	127
Security → User Hint String	128
Security → Min. Password Length	129
Security → TPM Support	130
Security → TPM Configuration	131
Security → TPM Configuration → Current TPM State	132
Security → TPM Configuration → TPM Action	133
Security → TPM Configuration → Omit Boot Measurements	134
Boot Menu	135
Exit Menu	137



The BIOS Setup utility is stored in the Serial Peripheral Interface (SPI) Flash device. The initial production BIOS ID string is BayCat_3.1.0.547.r1.101.

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

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

The top-level menu bar is shown below.

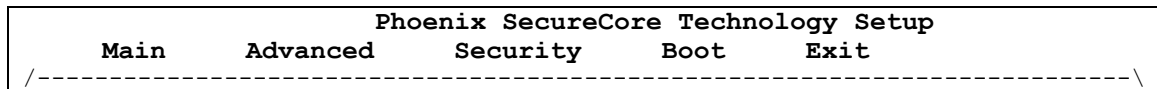











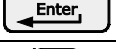

Table 1 lists the BIOS Setup utility top-level menu bar features.

Table 1: 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 2 lists the function keys available for menu screens.

Table 2. BIOS Setup Utility Function Keys



Menu	Function
	Help
 or 	Selects an item (Moves the cursor up or down)
 or 	Changes values
	Loads setup default values
	Exits the menu
 or 	Selects a different menu screen (Moves the cursor left or right)
	Executes a command or selects a sub-menu
	Saves the current values and exits the BIOS Setup utility



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           BayCat 3.1.0.547.rl.101 X64
| Build Time             01/14/2016
| Processor Type         Intel(R) Atom(TM) CPU E3826 @ 1.46GHz
| Processor Speed        1.474 GHz
| System Memory Speed    1066 MHz
| L2 Cache RAM           1024 KB
| Total Memory           4096 MB
| [1]                    4096 MB (DDR3- 1066) @ 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
Timeout		[2]	*	state for NumLock.
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
Esc Exit	<>	Select Menu	Enter	Select > Sub-Menu
			F9	Setup Defaults
			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
Timeout		[2]	*	that P.O.S.T will
CSM Support		[Yes]	*	wait for the user
Quick Boot		[Disabled]	*	input before booting.
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
Timeout		[2]	*	Support Module
CSM Support		[Yes]	*	supports legacy
Quick Boot		[Disabled]	*	(non-UEFI) OSes and
Diagnostic Splash Screen		[Disabled]	*	provides legacy BIOS
Diagnostic Summary Screen		[Disabled]	*	services, such as
BIOS Level USB		[Enabled]	*	software interrupt
Console Redirection		[Disabled]	*	Int10/Int13.
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
Timeout		[2]	*	boot.
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
Timeout		[2]	*	Diagnostic summary
CSM Support		[Yes]	*	screen during 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)	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	9600	Sets baudrate to 9600
	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
Timeout		[2]	*	Redirection after OS
CSM Support		[Yes]	*	has loaded.
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
Quick Boot		[Disabled]	+	display adapter to
Diagnostic Splash Screen		[Enabled]	+	switch the video mode
Diagnostic Summary Screen		[Disabled]	*	to Text Mode 3 at the
BIOS Level USB		[Enabled]	*	end of BIOS POST for
Console Redirection		[Disabled]	*	non-UEFI boot mode
Allow Hotkey in S4 resume		[Enabled]	+	(Legacy Boot). Some
UEFI Boot		[Enabled]	+	legacy software, such
Legacy Boot		[Enabled]	v	as DUET, requires
Boot in Legacy Video Mode		[Disabled]	*	that the BIOS
Load OPROM		[On Demand]	v	explicitly enter text
				video mode prior to
				boot.
F1	Help	↑↓	Select Item	+/-
Esc	Exit	<>	Select Menu	Enter
			Change Values	F9
			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	Disabled	Do not load option ROMs.
	On Demand (default)	Load all Option ROMs (OPROMs) directly – or on demand – according to the requirements of the boot device.

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

Advanced → OS Selection

```

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 F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			

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

Advanced → VersaLogic Features → Mini Card Mode

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

	Pin 43 or 51 mSATA Detect (default)
	Pin 43 mSATA Detect
Options	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]			^ Enable or disable
FPGA Flags	[EXTEMP]			* UART1.
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
Esc	Exit	<>	Select Menu	Enter Select > Sub-Menu
				F9 Setup Defaults
				F10 Save and Exit

Options	Disabled	Disables UART1
	Enabled (default)	Enables UART1

Advanced → VersaLogic Features → UART1 → Base Address

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]	^	Select the IRQ for UART1, or disable it.
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
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9	Setup Defaults		
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]		^	Enable or disable
FPGA Flags	[EXTEMP]		*	UART2.
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	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
Options	200
	208
	220
	228
	238
	338

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 → VersaLogic Features → ISA (PC/104) Bus IRQ Control

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
VersaLogic Features		Item Specific Help	
IRQ Mode	[IRQ3]	^	Enable this IRQ on the ISA (PC/104) bus.
	[RS-232]	+	
		+	
ISA (PC/104) bus IRQ control			
IRQ IRQ 3	[Disabled]	+	
IRQ IRQ 4	[Disabled]	+	
IRQ IRQ 5	[Disabled]	+	
IRQ IRQ 6	[Disabled]	+	
IRQ IRQ 7	[Disabled]	*	
IRQ IRQ 9	[Disabled]	*	
IRQ IRQ 10	[Disabled]	*	
IRQ IRQ 11	[Disabled]	*	
IRQ IRQ 12	[Disabled]	*	
IRQ IRQ 14	[Disabled]	*	
IRQ IRQ 15	[Disabled]	v	
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu F10 Save and Exit			



Note: This screen is replicated for IRQ IRQs 4, 5, 6, 7, 9, 10, 11, 12, 14, and 15.

Options	Disabled (default)	Disables ISA IRQ
	Enabled	Enables ISA IRQ

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      |      |      |      |      |
|      |      |      |      |      |      |
|-----|-----
| 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 [Enable]		prevent certain	
AES-NI [Enable]		classes of malicious	
Limit CPUID Maximum [Disable]		buffer overflow	
Bi-directional PROCHOT# [Enable]		attacks when combined	
VTX-2 [Enable]		with a supporting OS	
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
	Enable (default)

Advanced → CPU Configuration → AES-NI

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
CPU Configuration	
CPU Configuration	Item Specific Help
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 F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu 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]	
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 (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	
Execute Disable Bit		[Enable]	thermal sensor trips
AES-NI		[Enable]	(either core), the
Limit CPUID Maximum		[Disable]	PROCHOT# will be
Bi-directional PROCHOT#		[Enable]	driven.
VTX-2		[Enable]	If bi-direction is
TM1		[Enable]	enabled, external
DTS		[Enable]	agents can drive
Intel Hyper-Threading Technology		Not Supported	PROCHOT# to throttle
the processor.			
> CPU Power Management			
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 Configuration → VTX-2

Phoenix SecureCore Technology Setup				
Main	Advanced	Security	Boot	Exit
CPU Configuration				Item Specific Help
CPU Configuration				To enable or disable
Execute Disable Bit				[Enable] the VTX-2 Mode support
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 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]	
Tm1		[Enable]	
DTS		[Enable]	
Intel Hyper-Threading Technology		Not Supported	
> CPU Power Management			
F1 Help ↑↓ Select Item +/- Change Values F9 Setup Defaults Esc Exit <> Select Menu Enter Select > Sub-Menu 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]
TM1                                             [Enable]
DTS                                             [Enable]
Intel Hyper-Threading Technology Not Supported
-----
> CPU Power Management
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  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  Item Specific Help
-----
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]
-----
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			
Intel(R) SpeedStep(tm)	[Enable]	Select the	
Boot performance mode	[Max Performance]	performance state	
Intel Turbo Boost Technology	[Enable]	that the BIOS will	
C-States	[Enable]	set before OS handoff.	
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	
Boot performance mode	[Max Performance]	processor cores to	
Intel Turbo Boost Technology	[Enable]	run faster than the	
C-States	[Enable]	base operating	
Enhanced C-states	[Enable]	frequency if it's	
Max C State	[C7]	operating below	
		power, current, and	
		temperature	
		specification limits.	
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			
Intel(R) SpeedStep(tm)	[Enable]	Enable/Disable C 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 → 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		Item Specific Help	
System Power Options		This option controls	
Intel(R) SpeedStep(tm)	[Enable]	the Max C State that	
Boot performance mode	[Max Performance]	the processor will	
Intel Turbo Boost Technology	[Enable]	support.	
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	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                            |      |      |      |      |      |
|      |      |      |      |      |      |      |
|-----|-----
| 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	Disable	Disables the Graphics Output Protocol (GOP) driver
	Enable (default)	Enables 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
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9	Setup Defaults		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]	*	Select which of			
				IGD/PCI Graphics			
				device should be			
IGD Configuration			*	Primary Display Or			
Integrated Graphics Device		[Enable]	*	select SG for			
Primary Display		[Auto]	*	Switchable/Hybrid Gfx.			
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
GOP Driver	[Enable]	*	render standby support
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
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9			Setup Defaults
F10			Save and Exit

Options	Disable
	Enable (default)

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	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)
IGD Configuration				* Graphics Memory size
Integrated Graphics Device		[Enable]		* used by the Internal
Primary Display		[Auto]		* 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				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
			* 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		

Options	128 MB
	256 MB (default)

Advanced → Graphics/Uncore Configuration → IGD Turbo

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Graphics/Uncore Configuration		Item Specific Help	
GOP Configuration			^ Select the IGD Turbo
GOP Driver	[Enable]		* feature, if Auto
IGD Configuration			* selected, IGD Turbo
Integrated Graphics Device	[Enable]		* will only be enabled
Primary Display	[Auto]		* when SOC stepping is
RC6(Render Standby)	[Enable]		* B0 or above.
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
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9			Setup Defaults
F10			Save and Exit

Options	Auto (default)
	Enable
	Disable

Advanced → Graphics/Uncore Configuration → BIA

```

Phoenix SecureCore Technology Setup
Main    Advanced Security Boot Exit
-----
Graphics/Uncore Configuration | Item Specific Help
-----
RC6(Render Standby)          [Enable]      ^ | >>Auto: GMCH Use
PAVC                          [LITE Mode]   + | VBIOS Default;
GTT Size                      [2MB]         + | >>Level n: Enabled
Aperture Size                 [256MB]       + | with Selected
DVMT Pre-Allocated           [64M]         + | Aggressiveness Level.
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
    
```

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

Advanced → Graphics/Uncore Configuration → LCD Panel Type

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	F9 Setup Defaults
Esc Exit	<> Select Menu	Enter Select > Sub-Menu	F10 Save and Exit

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

Advanced → Graphics/Uncore Configuration → IGD Boot Type

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	
		*	DP PortB=EFP1	
IGD - LCD Control		*	DP PortC=EFP2	
BIA	[Auto]	*	eDP=LFP1	
LCD Panel Type	[Auto]	*	DSI PortA=LFP2	
IGD Boot Type	[Auto]	*	DSI ProtC=LFP2	
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				

	Auto (default)
Options	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
RC6 (Render Standby)	[Enable]		+	scaling option used
PAVC	[LITE Mode]		+	by Internal Graphics
GTT Size	[2MB]		+	Device.
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	
	Item Specific Help
	Configure PCIe Speed
PCIe 0 Speed	[Auto]
PCIe 1 Speed	[Auto]
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	

	Auto (default)
Options	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] | Configure PCIe Speed
PCIe 1 Speed [Auto] |
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	Auto (default)
	Gen 1
	Gen 2

Advanced → PCI Express Configuration → PCIe 2 Speed

```

Phoenix SecureCore Technology Setup
Main    Advanced Security Boot Exit
-----
PCI Express Configuration | Item Specific Help
-----
PCIe 0 Speed [Auto] | Configure PCIe Speed
PCIe 1 Speed [Auto] |
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	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 | Item Specific Help
-----
PCIe 0 Speed              [Auto]
PCIe 1 Speed              [Auto]
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	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]
PCIe 1 Speed              [Auto]
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	[Auto]		
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 |
| PCIe 1 Speed [Auto] | Express Root Port. |
| 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 |
| PCIe 1 Speed [Auto] | Express Root Port. |
| 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
USB Configuration	
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]
Item Specific Help	
Enable/Disable XHCI Link Power Management	
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 → 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]	One EHCI controller must always be enabled	
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	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-4005 J3_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-4005 J3_Bot, both J4 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]	Mini Card (J14)	
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
Esc	Exit	<>	Select Menu Enter Select > Sub-Menu
F9			Setup Defaults
F10			Save and Exit

Options	Disable
	Enable (default)

Advanced → Audio Configuration → Audio Controller

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
Audio Configuration	
Audio Controller	[Disable]
Item Specific Help	
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 89)
- Azalia HDMI Codec (see page 90)

Advanced → Audio Configuration → Azalia VCI Enable

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
Audio Configuration	
Audio Controller [Enable]	Item Specific Help
Azalia VCI Enable [Enable]	Enable/Disable
Azalia HDMI Codec [Enable]	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]	Item Specific Help
Azalia VCi Enable [Enable]	Enable/Disable
Azalia HDMI Codec [Enable]	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	Item Specific Help
Chipset-SATA Controller Configuration	Enables or Disables the Chipset SATA Controller.
Chipset SATA [Enable]	SATA Port 0 -> On-Board Connector (J2).
Chipset SATA Mode [AHCI]	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]
-----
SCC SDIO Support [Enable]
SCC SD Card Support [Enable]
SD SDR 25 Support [Enable]
SD SDR 50 Support [Enable]
-----
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 → SCC SDIO Support

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
LPSS & SCC Configuration		Item Specific Help	
LPSS Devices Mode	[PCI Mode]	SCC SDIO Support Enable\Disable	
SCC SDIO Support	[Enable]		
SCC SD Card Support	[Enable]		
SD SDR 25 Support	[Enable]		
SD SDR 50 Support	[Enable]		
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


Note:

- SCC = Storage Control Cluster
- SDIO = Secure Digital Input Output

Options	Disable (default)
	Enable

Advanced → LPSS & SCC Configuration → SCC SD Card Support

Phoenix SecureCore Technology Setup		
Main	Advanced	Security Boot Exit
LPSS & SCC Configuration		Item Specific Help
LPSS Devices Mode	[PCI Mode]	SCC SD Card Support Enable\Disable
SCC SDIO Support	[Enable]	
SCC SD Card Support	[Enable]	
SD SDR 25 Support	[Enable]	
SD SDR 50 Support	[Enable]	
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)	Disable support for Storage Control Cluster (SCC) SD memory cards.
	Enable	Enable support for Storage Control Cluster (SCC) SD memory cards.

Advanced → LPSS & SCC Configuration → SD SDR 25 Support

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
LPSS & SCC Configuration
-----
LPSS Devices Mode      [PCI Mode]
SCC SDIO Support       [Enable]
SCC SD Card Support    [Enable]
SD SDR 25 Support     [Enable]
SD SDR 50 Support     [Enable]
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

```


Note:

- SDR = Single Data Rate
- SDR 25 memory cards support a maximum frequency of 50 MHz with a bus maximum performance of 25 MB/s

Options	Disable (default)	Disable support for SDR 25 memory cards.
	Enable	Enable support for SDR 25 memory cards.

Advanced → LPSS & SCC Configuration → SD SDR 50 Support

```

Phoenix SecureCore Technology Setup
Main   Advanced Security Boot Exit
-----
LPSS & SCC Configuration
-----
LPSS Devices Mode      [PCI Mode]

SCC SDIO Support       [Enable]
SCC SD Card Support    [Enable]
SD SDR 25 Support      [Enable]
SD SDR 50 Support      [Enable]

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

```


Note:

- SDR = Single Data Rate
- SDR 50 memory cards support a maximum frequency of 100 MHz with a bus maximum performance of 50 MB/s.

Options	Disable (default)	Disable support for SDR 50 memory cards.
	Enable	Enable support for SDR 50 memory cards.

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

Phoenix SecureCore Technology Setup	
Main	Advanced
Security	Boot
Exit	
LPSS & SCC Configuration	
LPSS Devices Mode	[PCI Mode]
SCC SDIO Support	[Enable]
SCC SD Card Support	[Enable]
SD SDR 25 Support	[Enable]
SD SDR 50 Support	[Enable]
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 DMA #1 Support Enable\Disable	
F1	Help
Esc	Exit
↑↓	Select Item
<>	Select Menu
+/-	Change Values
Enter	Select > Sub-Menu
F9	Setup Defaults
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	
SCC SDIO Support	[Enable]		
SCC SD Card Support	[Enable]		
SD SDR 25 Support	[Enable]		
SD SDR 50 Support	[Enable]		
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		Item Specific Help
Main	Advanced	Security
		Boot
		Exit
LPSS & SCC Configuration		LPSS I2C #1 Support Enable\Disable
LPSS Devices Mode	[PCI Mode]	
SCC SDIO Support	[Enable]	
SCC SD Card Support	[Enable]	
SD SDR 25 Support	[Enable]	
SD SDR 50 Support	[Enable]	
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
Esc Exit	<> Select Menu	Enter Select > Sub-Menu
		F9 Setup Defaults
		F10 Save and Exit

Options	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]
SCC SDIO Support	[Enable]
SCC SD Card Support	[Enable]
SD SDR 25 Support	[Enable]
SD SDR 50 Support	[Enable]
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 98.)

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

Phoenix SecureCore Technology Setup	
Main	Advanced Security Boot Exit
LPSS & SCC Configuration	
Item Specific Help	
LPSS Devices Mode	[PCI Mode]
LPSS PWM #2 Support	Enable\Disable
SCC SDIO Support	[Enable]
SCC SD Card Support	[Enable]
SD SDR 25 Support	[Enable]
SD SDR 50 Support	[Enable]
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 98.)

Advanced → Miscellaneous Configuration → High Precision Timer

Phoenix SecureCore Technology Setup	
Main	Advanced
Miscellaneous Configuration	
Miscellaneous Configuration	Item Specific Help
High Precision Timer [Enable]	Enable or Disable the High Precision Event Timer
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	
High Precision Timer [Enable]		with High Precision	
Boot Time with HPET Timer [Disable]		Event Timer enabled	
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	Specify what state to
High Precision Timer [Enable]	go to when power is
Boot Time with HPET Timer [Disable]	re-applied after a
State After G3 [S0 State]	power failure (G3
SoC Debug UART [Disable]	state).
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	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
High Precision Timer [Enable]	feature will lock
Boot Time with HPET Timer [Disable]	SMRAM to prevent
State After G3 [S0 State]	additional loading of
SoC Debug UART [Disable]	SMM drivers.
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
Esc Exit	<> Select Menu
+/-	Change Values
Enter	Select > Sub-Menu
F9	Setup Defaults
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
|
|-----|-----
|
| 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		Item Specific Help	
TXE Configuration			Trusted Execution Engine
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 HMRFPO

Phoenix SecureCore Technology Setup			
Main	Advanced	Security	Boot Exit
Security Configuration		Item Specific Help	
TXE Configuration			Host ME (TXE) Region
TXE FW Version	1.0.2.1060		Flash Protection
TXE FW Capabilities	20001040		Override
TXE FW Features	20001040		
TXE FW OEM Tag	00000000		
TXE Firmware Mode	Normal		
TXE File System Integrity Value	0		
TXE	[Enable]		
TXE HMRFPO	[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 (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		Item Specific Help	
TXE Configuration			
TXE FW Version		1.0.2.1060	
TXE FW Capabilites		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		Item Specific Help	
TXE Configuration			Send EOP Message
TXE FW Version		1.0.2.1060	Before Enter OS
TXE FW Capabilites		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 (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		Item Specific Help	
TXE Configuration			Revert TXE settings to factory defaults
TXE FW Version		1.0.2.1060	
TXE FW Capabilites		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	No (default)	Do not perform a TXE unconfiguration
	Yes	Perform a TXE unconfiguration

Advanced → Thermal

```

Phoenix SecureCore Technology Setup
Main  Advanced  Security  Boot  Exit
-----|-----
|                                         | Item Specific Help
| Setup Warning:                         |-----|
| Setting items on this screen to incorr |
| ect values may cause system to malfunc |
| tion!                                   |
|                                         |
| OS Selection                           | [Linux]
| > VersaLogic Features
| > CPU Configuration
| > Uncore Configuration
| > South Cluster Configuration
| > Security Configuration
| > Thermal
| > SMBIOS Event Log
|                                         |
|-----|-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit

```

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                          |      |      |      |
|      |      |      |      |      |
|-----|-----
| 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]
-----
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          | Item Specific Help |
|-----|-----|
| Event Log Validity                 Valid | Mark SMBIOS events as |
| Event Log Capacity                 Space Available | read. Marked SMBIOS |
|                                     | events won't be |
| Event Log                           [Enabled] | displayed. |
| > View SMBIOS event log            | |
| Mark SMBIOS events as read [Enter] | |
| Clears SMBIOS events               [Enter] | |
|                                     | |
|-----|-----|
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          | Item Specific Help |
|-----|-----|
| Event Log Validity                 Valid | Clears SMBIOS events. |
| Event Log Capacity                 Space Available |
|
| Event Log                           [Enabled] |
| > View SMBIOS event log             |
|
| Mark SMBIOS events as read [Enter] |
| Clear SMBIOS events [Enter] |
|
|-----|-----|
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                  v
|
| Trusted Platform Module (TPM)
| TPM Support                      [Enabled]
| TPM Configuration
|
|-----
F1  Help  ↑↓  Select Item  +/-  Change Values      F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10 Save and Exit
    
```

Security → Set Supervisor Password

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----+-----+-----+-----+-----+
| Secure Boot Activation          [Disabled]      ^ | Item Specific Help |
| > Secure Boot Configuration      * | -----+-----+ |
| Supervisor Password is:          Cleared              * | Set or clear the   |
| User Password is:                Cleared              * | Supervisor account's |
|                                     * | password.          |
| 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                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 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  +
|                            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

```

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                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

```

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 the minimum
| Set Supervisor Password             [Enter] * | number of characters
| Supervisor Hint String              [          ] * | for password (1-20).
|                                     * |
| Set User Password                   [Enter] * |
| User Hint String                    [          ] * |
|                                     * |
| Min. password length [ 1 ] * |
|                                     * |
| Authenticate User on Boot           [Disabled] * |
|                                     * |
| HDD Security Status                 + |
| No HDD detected                     + |
|                                     v |
|
| Trusted Platform Module (TPM)
| TPM Support                         [Enabled]
| TPM Configuration
|-----|-----|-----|-----|
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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  * |
|                                     * | This is used to decide
| Set Supervisor Password              [Enter]  * | whether TPM support
| Supervisor Hint String               [        ] * | should be enabled or
|                                     * | disabled.
|                                     * |
| Set User Password                    [Enter]  * |
| User Hint String                     [        ] * |
|                                     * |
| Min. password length                 [ 1]    * |
|                                     * |
| Authenticate User on Boot            [Disabled] * |
|                                     * |
| HDD Security Status                  + |
| No HDD detected                      + |
|                                     v |
|
| Trusted Platform Module (TPM)
| TPM Support                          [Enabled]
| TPM Configuration
|
-----
F1  Help  ↑↓  Select Item  +/-  Change Values  F9  Setup Defaults
Esc  Exit  <>  Select Menu  Enter  Select > Sub-Menu  F10  Save and Exit

```

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. |
| TPM Action [No Change] | Note: Most TPM |
| Omit Boot Measurements [Disabled] | 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

```

Security → TPM Configuration → Current TPM State

```

Phoenix SecureCore Technology Setup
Main      Advanced      Security      Boot      Exit
-----
|          TPM Configuration          |          Item Specific Help          |
|-----|-----|
| Current TPM State [Enabled and Activated] | Enact TPM Action.                   |
| TPM Action [No Change]                   | Note: Most TPM                      |
| Omit Boot Measurements [Disabled]        | 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          | Item Specific Help |
|-----|-----|
| Current TPM State      [Enabled and Activated] | Enact TPM Action. |
| TPM Action             [No Change]             | Note: Most TPM   |
| Omit Boot Measurements [Disabled]             | 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		Item Specific Help			
Current TPM State	[Enabled and Activated]		Enabling this option causes the system to omit recording boot device attempts in PCR[4].		
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

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.  ATAPI CD:
2.  ATA HDD0:
3.  ATA HDD1:
4.  USB HDD:
5.  USB CD:
6.  USB FDD:
7.  eMMC Card0:
8.  SD Card1:
9.  Internal Shell
10. 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 |          | Item Specific Help |
|-----+-----+-----+-----+-----+
| 1.  USB CD:          |          | Keys used to view or |
| 2.  ATAPI CD:       |          | configure devices: ^ |
| 3.  USB HDD:        |          | and v arrows Select a |
| 4.  ATA HDD0:       |          | device. '+' and '-' |
| 5.  ATA HDD1:       |          | move the device up or |
| 6.  USB FDD:        |          | down. 'Shift + 1'   |
| 7.  Internal Shell  |          |                       |
| 8.  ▼PCI LAN:       |          | enables or disables a |
|      IBA GE Slot 0800 v1578 |          | device. 'Del' deletes |
|      IBA GE Slot 0900 v1578 |          | 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 F10
Exit Discarding Changes	Exit Setup without saving changes; same as Esc
Load Setup Defaults	Load standard default values; same as F9
Load Optimized Defaults	Load settings for optimized boot time and system performance
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 ***