

Phoenix SecureCore Tiano User Guide

Software Manual

SM-EFI.docx

Revision 0.1 / January 12

©LIPPERT Embedded Computers GmbH

Hans-Thoma-Str. 11

D-68163 Mannheim

<http://www.lippertembedded.com/>

Software Manual Phoenix SecureCore Tiano

LiPPERT Document: SM-EFI.docx Revision 0.1

Copyright ©2012 LiPPERT Embedded Computers GmbH, All rights reserved

Trademarks

MS-DOS, Windows, Windows XP, Windows 7 are trademarks of Microsoft Corporation. Intel is a trademark of Intel Corporation. Phoenix SecureCore Tiano is a trademark of Phoenix Technologies Ltd. All other trademarks appearing in this document are the property of their respective owners.

Disclaimer

Contents and specifications within this technical manual are subject of change without notice.

LiPPERT Embedded Computers GmbH provides no warranty with regard to this technical manual or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. LiPPERT Embedded Computers GmbH assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the technical manual. In no event shall LiPPERT Embedded Computers GmbH be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this user's guide or any other information contained herein or the use thereof.

Table of Contents

1	Overview	1
1.1	Introduction.....	1
1.2	General Controls.....	1
1.3	Boot up keys.....	2
2	Setup Description	3
2.1	Entering the Setup Menu.....	3
2.2	Main – Menu.....	3
2.2.1	System Date.....	3
2.2.2	System Time.....	3
2.2.3	System Information.....	4
2.2.4	Boot Features.....	5
2.2.5	Error Manager.....	6
2.3	Advanced – Menu.....	8
2.3.1	Boot Configuration.....	9
2.3.2	ACPI Configuration.....	11
2.3.3	Processor Configuration.....	12
2.3.4	Chipset Configuration.....	14
2.3.5	SMBIOS Event Log.....	16
2.3.6	Thermal Configuration.....	17
2.4	Security.....	19
2.4.1	Security Password is:.....	19
2.4.2	Set Security Password.....	19
2.4.3	Security Hint String.....	19
2.4.4	Min. password length.....	19

2.4.5	Trusted Platform Module (TPM).....	19
2.5	Boot – Menu.....	20
2.5.1	Boot Priority Order	20
2.6	Exit – Menu.....	21
2.6.1	Exit Saving Changes.....	21
2.6.2	Exit Discarding Changes.....	21
2.6.3	Load Setup Defaults.....	21
2.6.4	Discard Changes	21
2.6.5	Save Changes	22
3	Boot Menu & App Menu	23
3.1	Boot Menu	23
3.2	App Menu	24
4	UEFI Shell	25

Acronyms

ACPI	Advanced Configuration and Power Management Interface
BIOS	Basic Input Output System
CPU	Central Processing Unit
EFI	Extensible Firmware Interface
GPIO	General Purpose Input Output
LPC	Low Pin Count
LVDS	Low Voltage Differential Signaling
OS	Operation System
PCI	Peripheral Component Interconnect
SMB	System Management Bus
SVGA	Super Video Graphics Array
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VGA	Video Graphics Array

1 Overview

1.1 Introduction

This guide discusses the Phoenix SecureCore Tiano™ BIOS setup options. The BIOS setup allows users to modify the basic system configuration. This special information is stored in BIOS flash so that it retains the setup information when the power is turned off.

This operating guide was written with the intent to give a general overview of all the user-visible features in Phoenix SecureCore Tiano. However, the BIOS setup pages used in this guide were adapted for the board CoreExpress-ECO2. Therefore, some of the features discussed in this operating guide may operate differently or not apply to your system.

1.2 General Controls

In general, you use the arrow keys to highlight items and change entries by pressing **<Enter>** to select an entry and the **<Up>** and **<Down>** keys for selecting a new value. For general help press **<F1>**. To exit a menu press **<ESC>**.

The following table provides more details about how to navigate in the Setup program using the keyboard.

<Up>:	Move to the previous item
<Down>:	Move to the next item
<Left>:	Move to the previous menu
<Right>:	Move to the next menu
<Esc>:	Exit current page to the next higher level menu
<Enter>:	Enter/Select highlighted menu item
<+> key:	Increase the numeric value or make changes
<-> key:	Decrease the numeric value or make changes
<F1> key:	General help on setup navigation keys
<F9> key:	Load the optimized settings
<F10> key:	Save all the CMOS changes and exit

1.3 Boot up keys

The following keys pressed during boot up allow you to enter the Setup Menu, the Boot Menu or the UEFI Shell.

- <F2> key:** Enter the BIOS setup, see chapter 2 Setup Description
- <F5> key:** Enter the Boot Menu, see chapter 3 Boot Menu & App Menu
- <F11> key:** Enter the UEFI Shell, see chapter 4 UEFI Shell

2 Setup Description

2.1 Entering the Setup Menu

Press <F2> during boot up to enter the Setup Menu.

2.2 Main – Menu

The Main menu let you configure general settings like the system date and time.

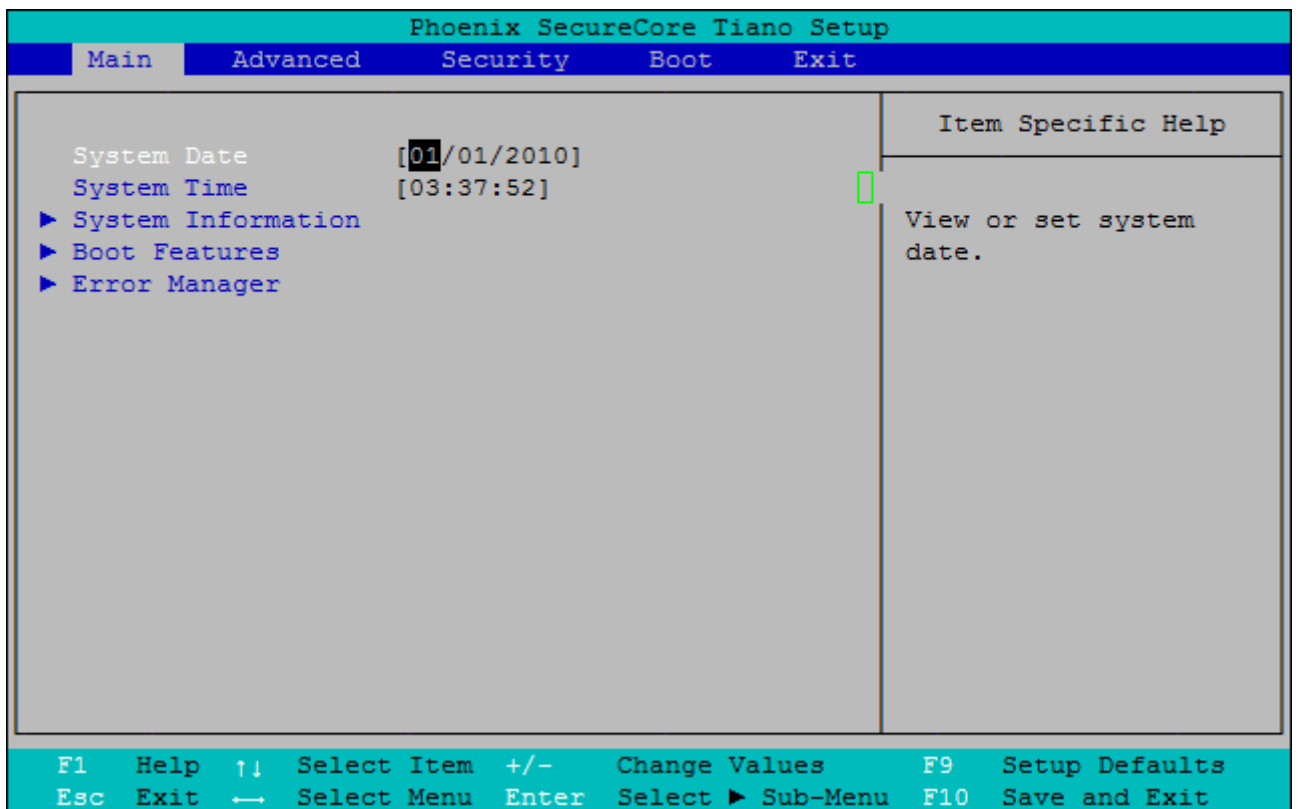


Figure 2-1: Main Menu Overview

2.2.1 System Date

System date in the format [MM/DD/YYYY]. Use <Enter> or <Tab> to switch through the fields. Adjust the values with <+> and <->.

2.2.2 System Time

System Time is in 24-Hour format [hh:mm:ss]. Use <Enter> or <Tab> to switch through the fields. Adjust the values with <+> and <->.



Caution: The System Date and Time will not be stored if the board's battery runs empty. All other changes are saved in flash.

2.2.3 System Information

Shows generic system information, like BIOS version, CPU speed or system memory, as seen in Figure 2-2.

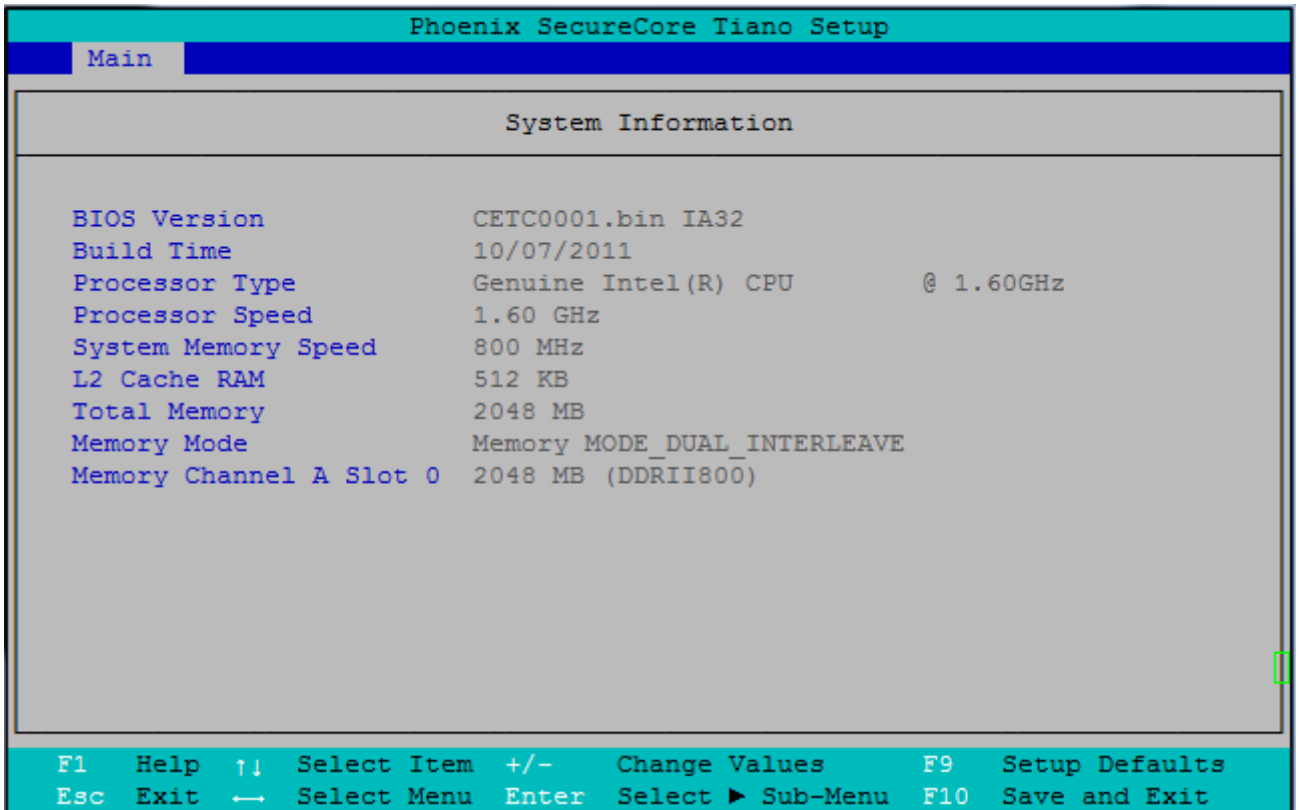


Figure 2-2: Main Menu -> System Information

2.2.4 Boot Features

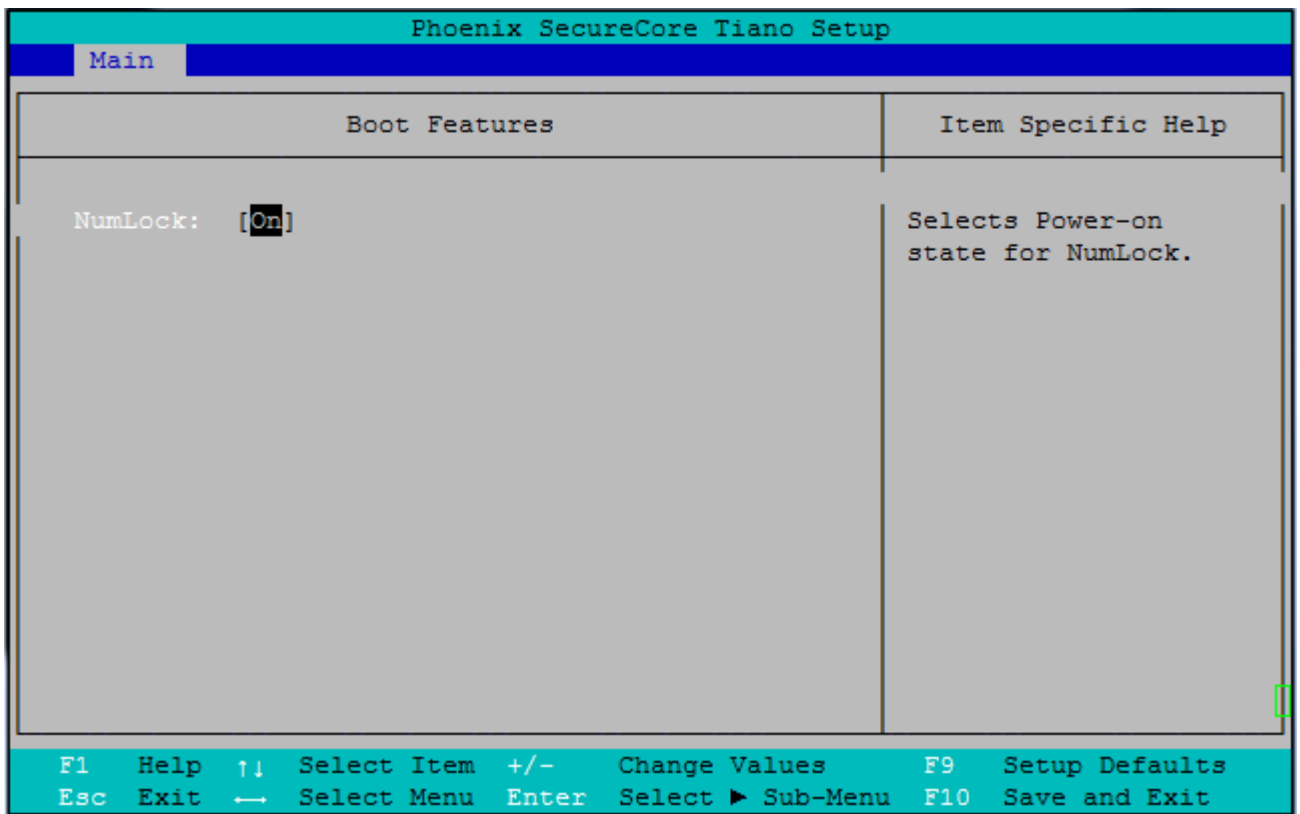


Figure 2-3: Main - Menu -> Boot Features

2.2.4.1 NumLock

This BIOS feature sets the input mode of the numeric keypad at boot up. If you turn this feature on [On], the BIOS will set the numeric keypad to function in the **numeric mode**. If you set it to off [Off], the numeric keypad will function in the **cursor control mode** instead.

Values: [On/Off]

2.2.5 Error Manager

The Error Manager let you view errors detected by the BIOS

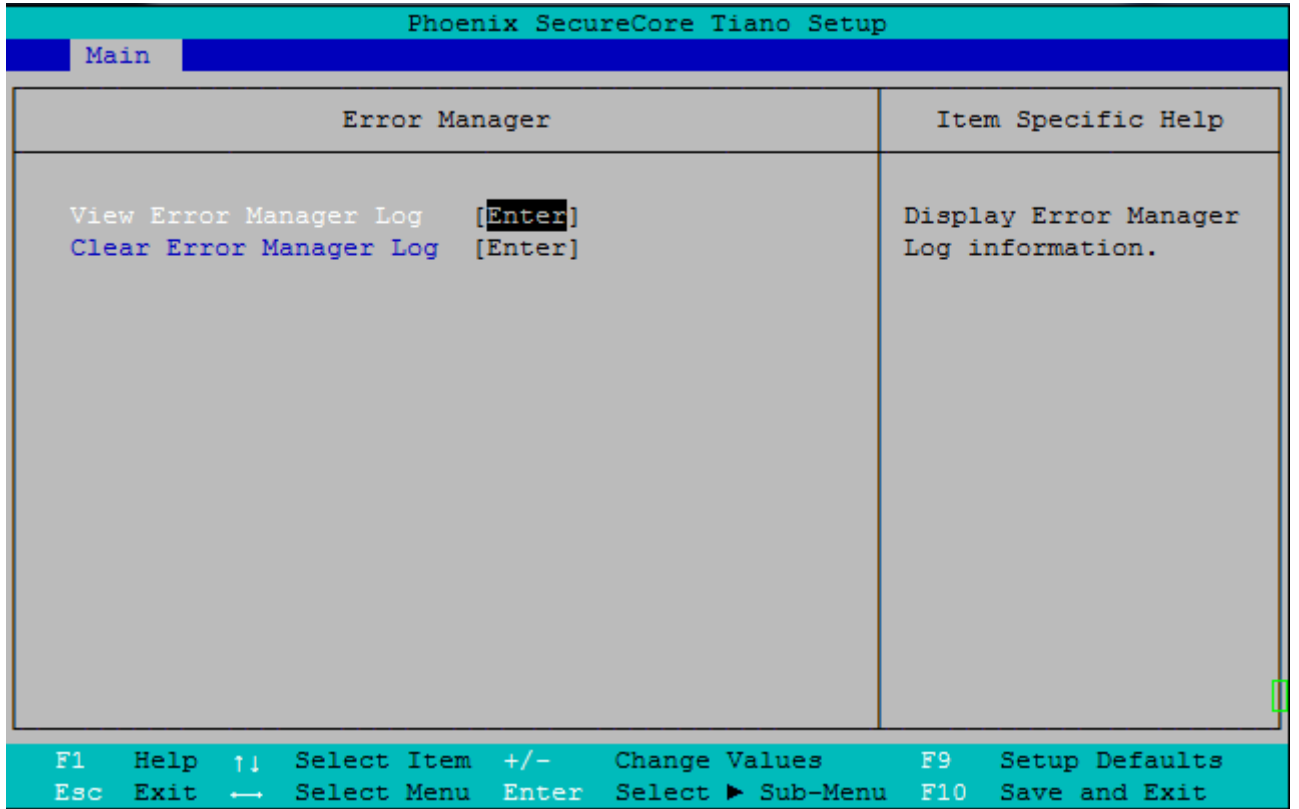


Figure 2-4: main - Menu -> Error Manager

2.2.5.1 View Error Manager Log

This item lets you view the Error Log, see Figure 2-5 as an example. Press **<Enter>** to view all detected errors.

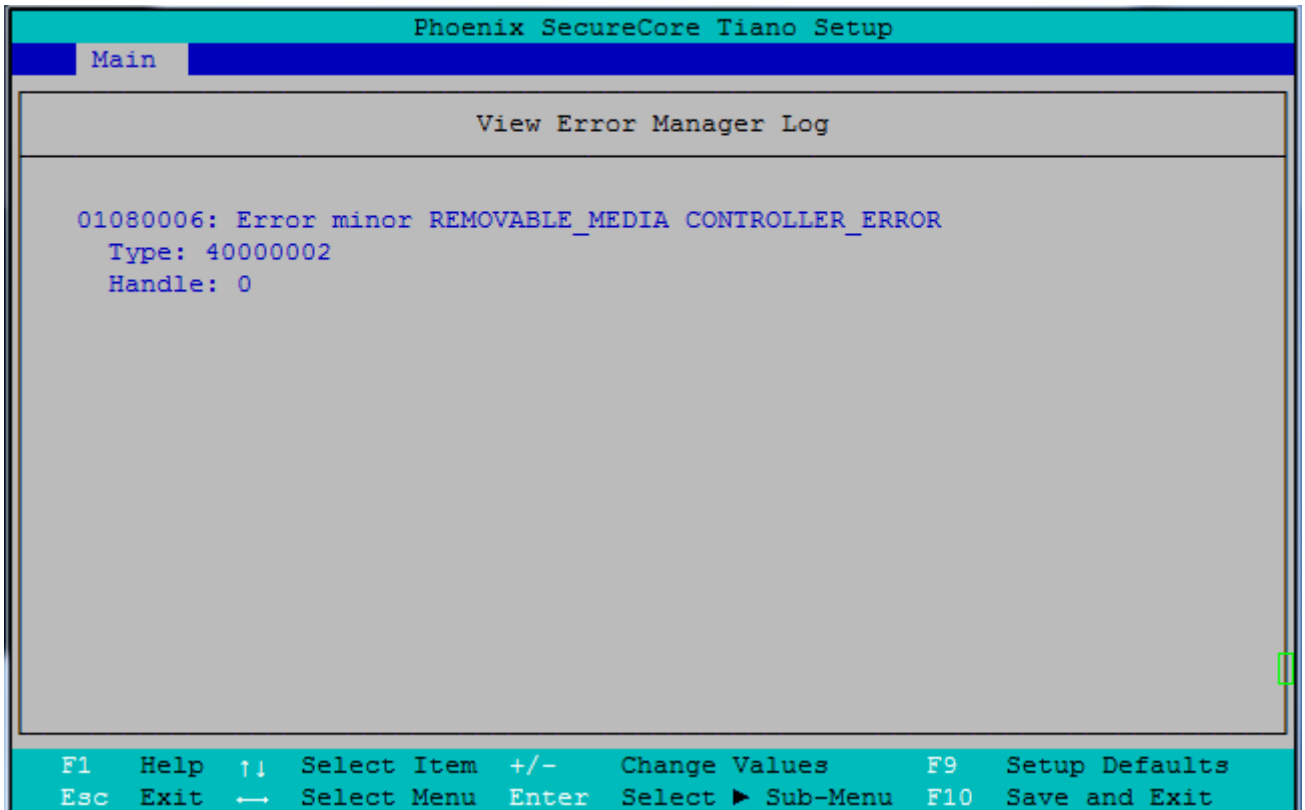


Figure 2-5: Main - Menu -> Error Manager -> View Error Manager Log

2.2.5.2 Clear Error Manager Log

This item lets you clear all entries from the Error Log Manager. Press **<Enter>** to clear the entries.

2.3 Advanced – Menu

The Advanced Menu gives you more detailed control over the system and its hardware.

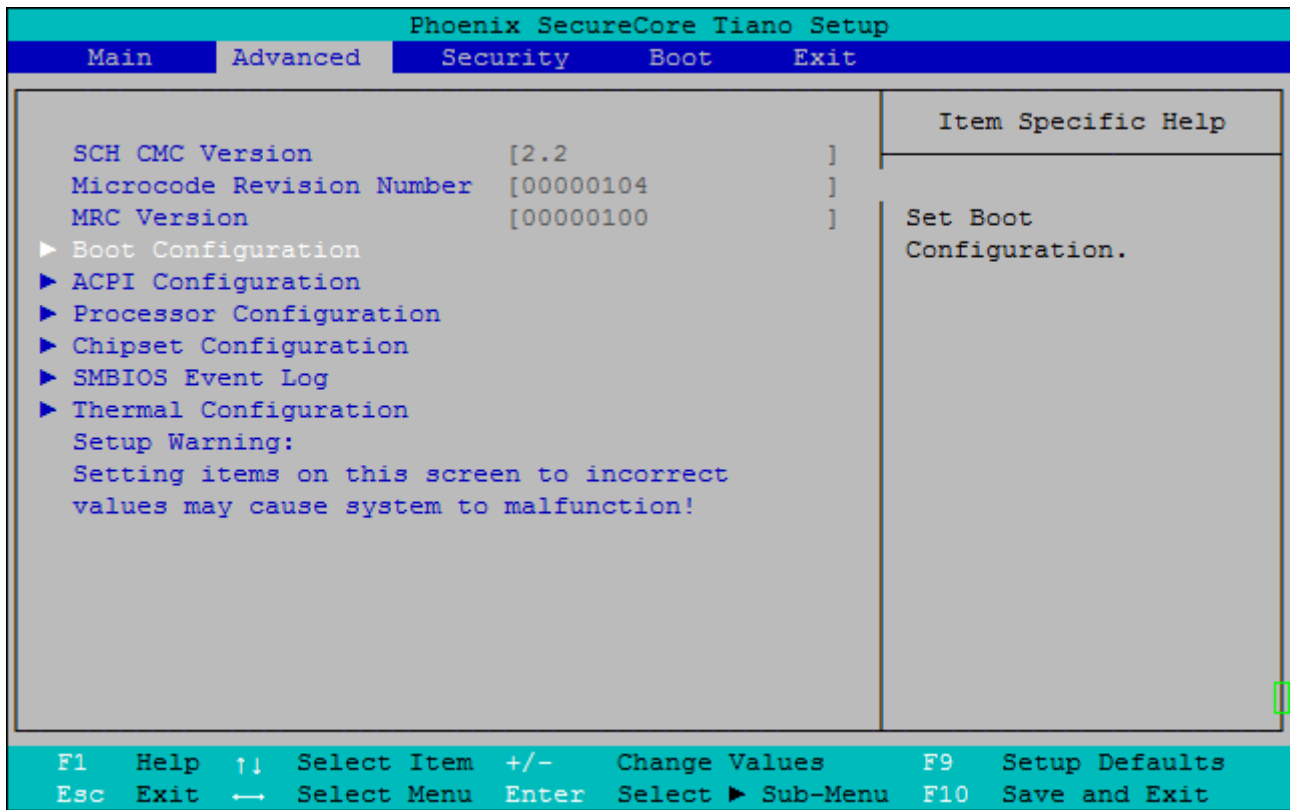


Figure 2-6: Advanced - Menu

2.3.1 Boot Configuration

The Boot Configuration Menu lets you configure boot relevant options.

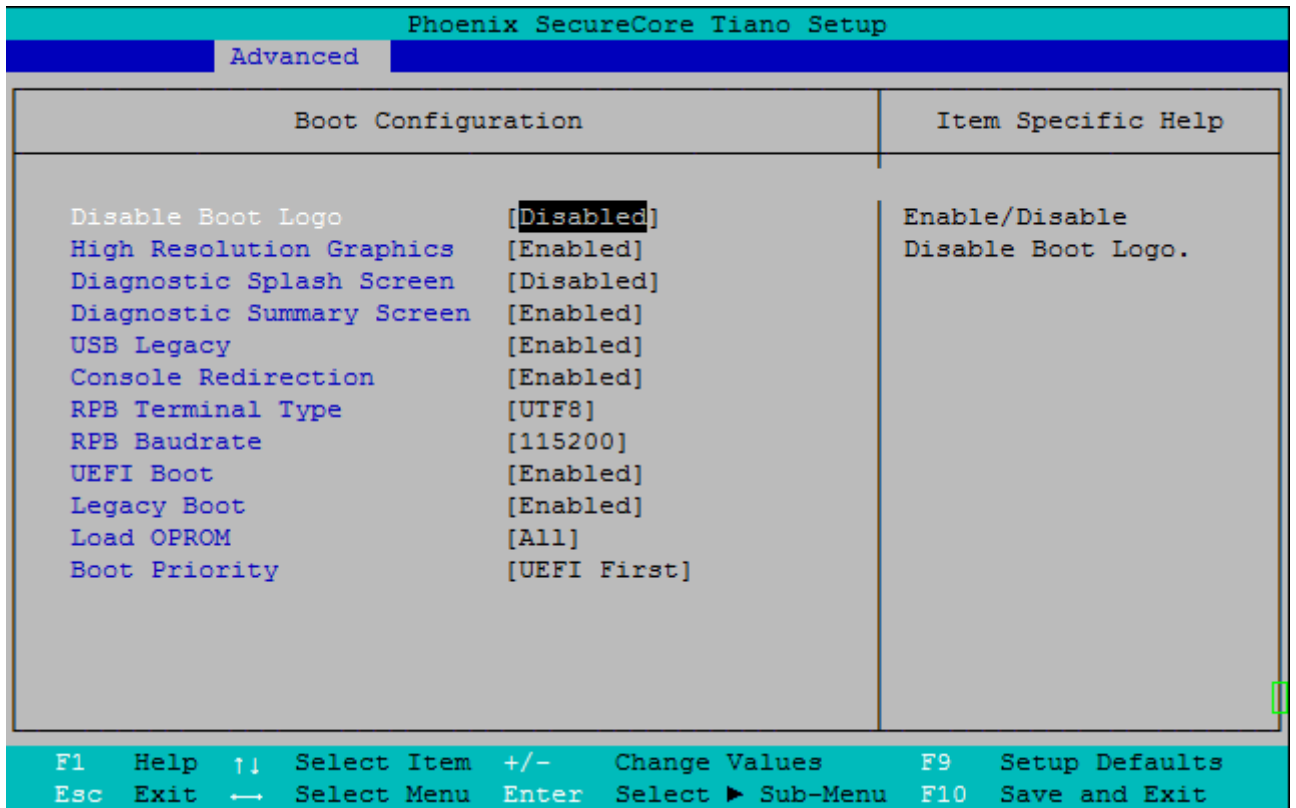


Figure 2-7: Advanced Menu -> Boot Configuration

2.3.1.1 Disable Boot Logo

This item disables the full screen boot logo during boot up. Select [Disabled] if you want to show the boot logo and select [Enabled] to disable the boot logo.

Values: [Enabled/Disabled]

2.3.1.2 High Resolution Graphics

This item enables high resolution graphics during boot. Combining display outputs (e.g. clone mode) may need high resolution graphics mode.

Values: [Enabled/Disabled]

2.3.1.3 Diagnostic Splash Screen

This item shows a Diagnostic screen during boot up. This screen is also accessible through the App Menu.

Values: [Enabled/Disabled]

2.3.1.4 Diagnostic Summary Screen

This item shows a Diagnostic Summary Screen during boot up. The boot process will stop by displaying this screen until a key is pressed.

Values: [Enabled/Disabled]

2.3.1.5 USB Legacy

Enables support for USB Legacy emulation for keyboard, mouse and mass storage devices. If Legacy mode is disabled legacy operation systems without USB support (e.g. DOS) cannot use USB devices like keyboard, mouse or mass storage.

Values: [Enabled/Disabled]

2.3.1.6 Console Redirection

Enables console redirection over a serial port. [Enabled] causes the BIOS to always use the serial port as the console. [Disabled] causes the BIOS to never invoke console redirection but instead always use the main keyboard and video display.

Values: [Enabled/Disabled]

2.3.1.7 RPB Terminal Type

This item selects the console type for the console Redirection function mentioned above. Select a value according to your terminal program.

Values: [ANSI/VT100/VT100+/UTF8]

2.3.1.8 RPB Terminal Baudrate

This item selects the Baudrate for the serial port used for the console redirection.

Values: [9600/19200/38400/57600/115200]

2.3.1.9 UEFI Boot

This item enables the UEFI Boot. Enable this function if you want to boot UEFI aware operation systems like Windows 7 64Bit or Linux.

Values: [Enabled/Disabled]

2.3.1.10 Legacy Boot

This item enables the legacy boot portion of the BIOS, if you want to boot non-EFI capable operation systems, like Windows XP or DOS this item must be enabled. Disabling this function may speed up boot time by approximately 1-2 seconds.

Values: [Enabled/Disabled]

2.3.1.11 Load OPROM

This item determinates if all available Option ROMs are loaded [All] or only these needed for booting [On Demand]. Additional Option ROMs may be provided from additional hardware such as SCSI or network cards.

Values: [All/On Demand]

2.3.1.12 Boot Priority

This item selects the order of the boot method the BIOS tries first.

Values: [UEFI First/Legacy First]

2.3.2 ACPI Configuration

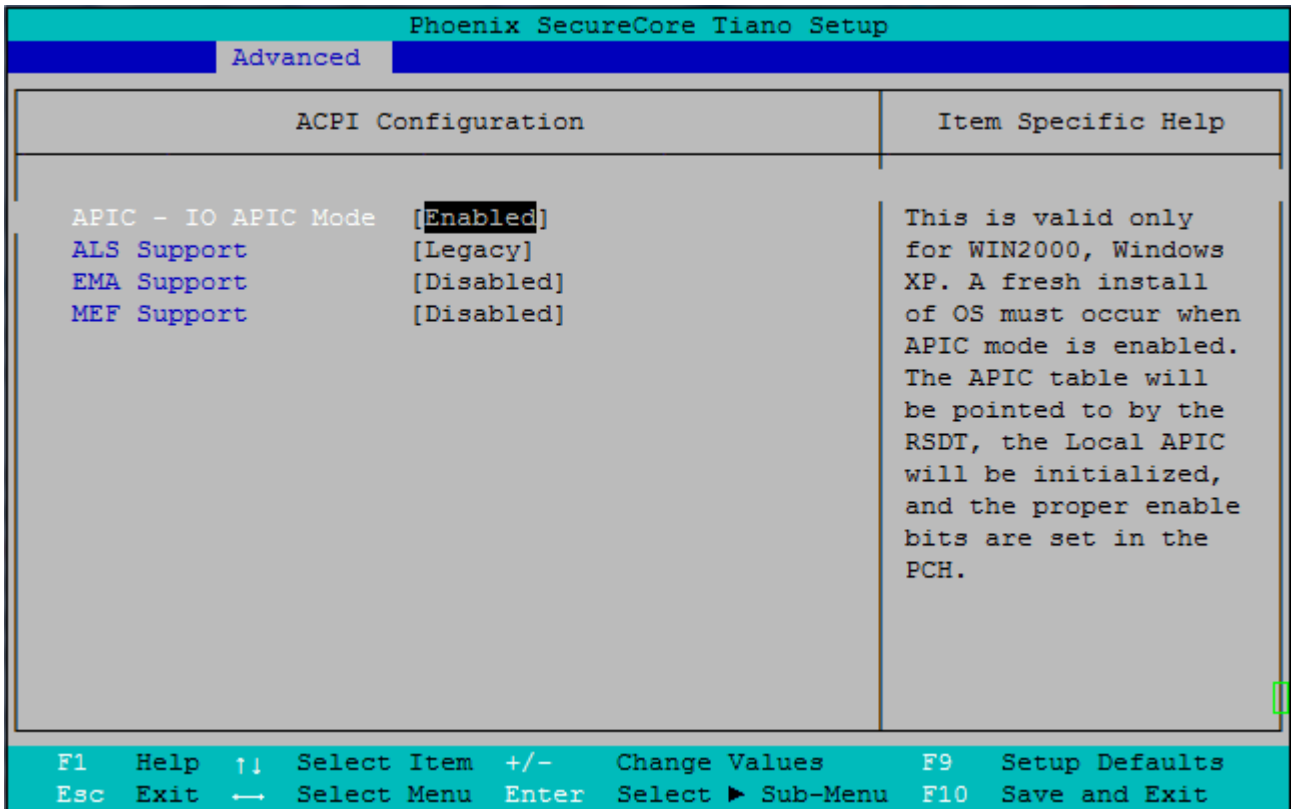


Figure 2-8: Advanced - Menu -> ACPI Menu

2.3.2.1 APIC – IO APIC Mode

Enables or disables the IO APIC. Changes to this setting may require a new installation of your operating system.

Values: [Enable/Disable]

2.3.2.2 ALS/EMA/MEF Support

These options let you enable or disable ACPI specific devices.

Values: [Enable/Disable or Legacy/ACPI]

2.3.3 Processor Configuration

This Menu shows setup options for all hardware integrated into the systems main processor.

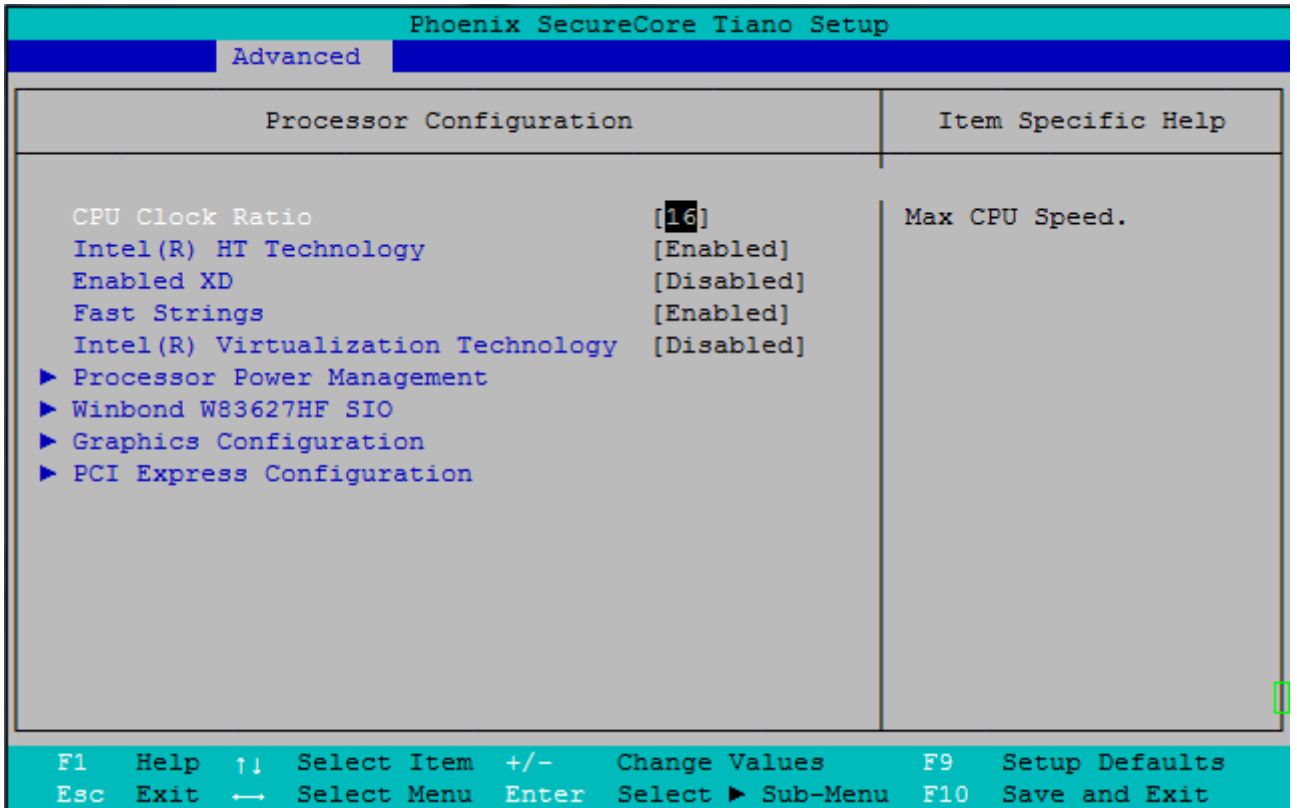


Figure 2-9: Processor Options for CoreExpress-ECO2

2.3.3.1 CPU Clock Ratio

This item let you select the maximum CPU clock. The value is the CPU multiplier. Use <+/->- keys to select the Value.

Values: [CPU dependant]

2.3.3.2 Intel® HT Technology

This item enables the Intel Hyper-Threading Technology function for certain CPUs, virtually creating a second CPU core.

Values: [Enabled/Disabled]

2.3.3.3 Enabled XD

This item enables the Execute Disabled bit, increasing the security by preventing the execution of code in marked memory regions.

Values: [Enabled/Disabled]

2.3.3.4 Fast Strings

Enables the Fast Strings feature of the processor.

Values: [Enabled/Disabled]

2.3.3.5 Intel® Virtualization Technology

This item enables the VT-x Virtualization technique. If you want to use a virtual machine enabling this feature is recommended for better performance.

Values: [Enabled/Disabled]

2.3.3.6 Processor Power Management

The Processor Power Management sub menu let you configure the CPUs power management facilities.

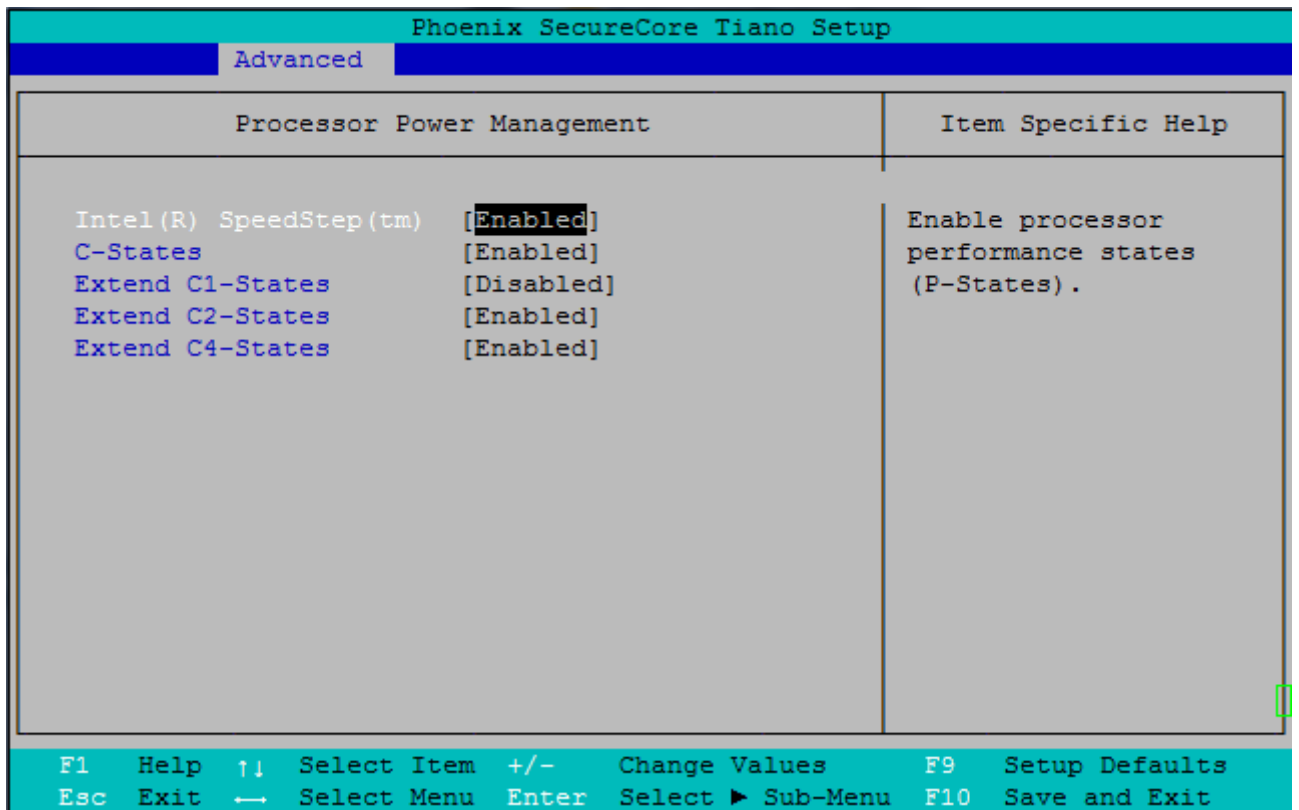


Figure 2-10: Advanced Menu -> Processor Configuration -> Processor Power Management

2.3.3.6.1 Intel® SpeedStep™

This item enables the Intel SpeedStep™ function of the CPU. This feature lets the OS dynamical throttle the CPU speed.

Values: [Enabled/Disabled]

2.3.3.6.2 C-States – Extend C[1,2,4,x]-States

These items let you configure the use of C-States. Higher C[1,2,4,x]-States will save more power if the CPU is idle.

Values: [Enabled/Disabled]

2.3.3.7 Winbond W83627HF SIO (Name depends on the installed SuperIO)

This sub menu configures the features of the installed SuperIO. The functions in this menu configure the devices provided by the SuperIO, such as serial / parallel ports or floppy controllers.

2.3.3.8 Graphics Configuration

This item configures the internal graphics device

2.3.3.8.1 Internal Graphics

This item let you enable or disable the internal graphics adapter.

Values: [Enabled/Disabled/Auto]

2.3.3.8.2 Primary Display Selection

This item let you select which graphics adapter is your primary adapter. Possible values are [IGD], which is the internal graphics device, [PEG] which is an external graphic card inserted into a PCI Express Slot and finally [PCI] which is for a PCI card.

Values: [IGD/PEG/PCI/Auto]

2.3.3.8.3 IGD Configuration

This menu let you change the settings for the internal graphics device, such as LVDS resolution or Panel scaling modes.

2.3.3.9 PCI Express Configuration

This sub menu controls the PCI Express root ports integrated into the processor.

2.3.4 Chipset Configuration

The Chipset Configuration – Menu allows you to configure the devices provided by the chipset

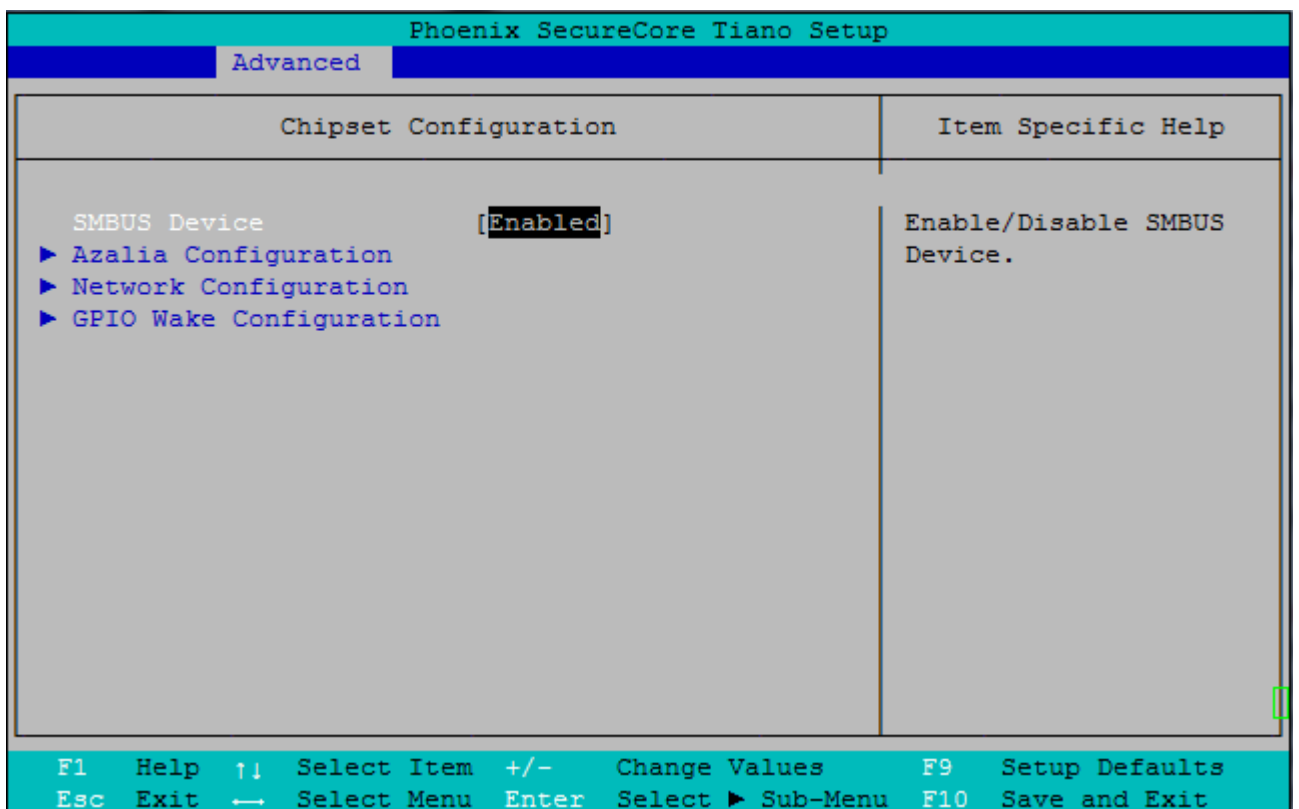


Figure 2-11: Advanced - Menu -> Chipset Configuration

2.3.4.1 SMBUS Device

This item let you disable the SMBus device.

Values: [Enabled/Disabled]

2.3.4.2 Azalia Configuration

The Azalia sub menu let you configure the HD-Audio device included in the chipset.

2.3.4.2.1 Azalia

This item enables or disables the onboard HDA – Audio device.

Values: [Enabled/Disabled/Auto]

2.3.4.2.2 Azalia PME Enable

This item enables or disables the Power Management Events for the HDA audio controller.

Values: [Enabled/Disabled]

2.3.4.2.3 Azalia Vci Enable

This function enables the enhanced Virtual Channel.

Values: [Enabled/Disabled]

2.3.4.3 Network Configuration

This sub menu includes configuration options for the network device.

2.3.4.3.1 PxeOProm Configuration

This item let you enable the PXE Boot Rom for the Ethernet port. If the system should be booted over the network this function must be enabled.

Values: [Enabled/Disabled]

2.3.4.3.2 Wake On Lan

This item enables Wake On Lan.

Values: [Enabled/Disabled]

2.3.4.3.3 WOL Mode

This item let you select the wake packet for Wake On Lan. Magic Packet or Wake up Frame.

Values: [Magic Packet/Wake Up Frame]

2.3.4.3.4 WOL Speed

This item selects the network speed used when the device waits for the wake packet.

Values: [10 Mbps/100 Mbps/1000 Mbps]

2.3.4.4 GPIO Wake Configuration

This sub menu let you configure wake facilities by using GPIOs. To wake up the system by using a GPIO you must enable the wake function for the used GPIO.

2.3.5 SMBIOS Event Log

This menu let you show and configure the SMBios log facilities.

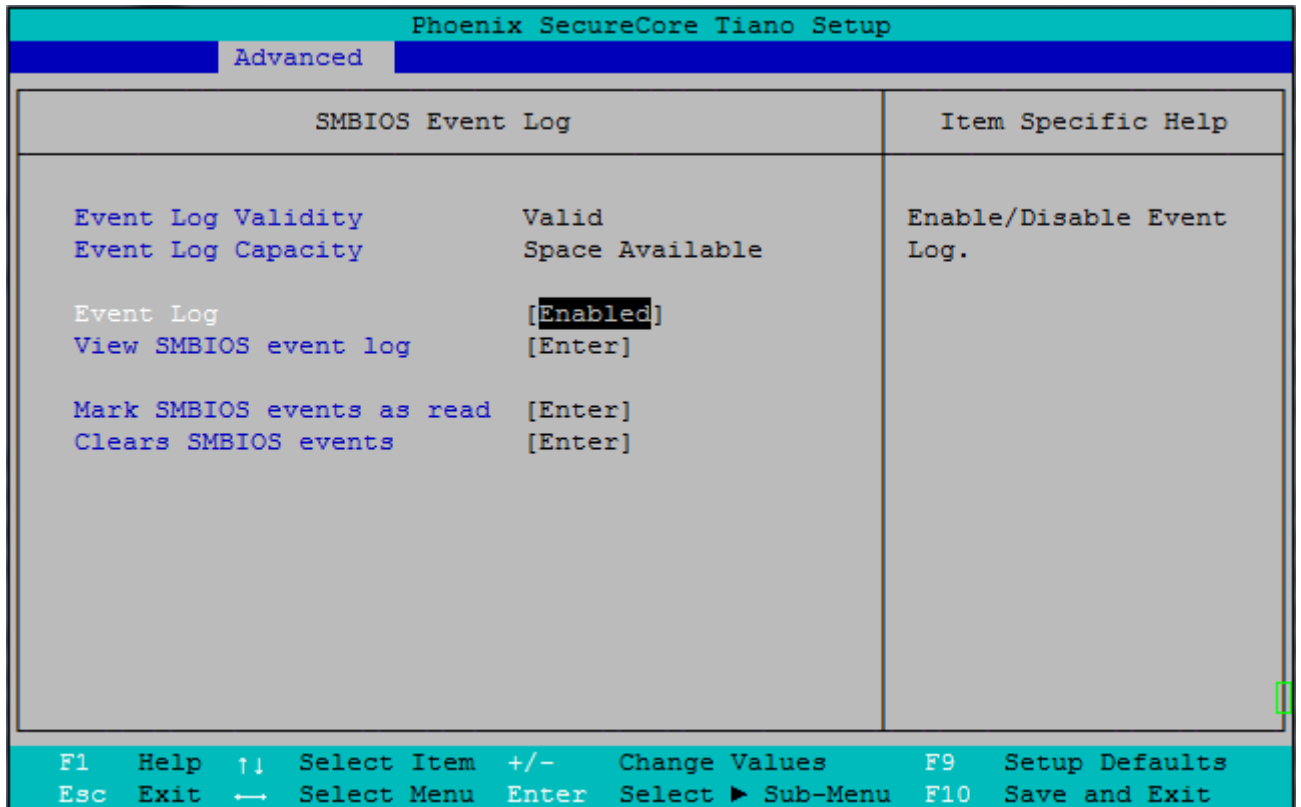


Figure 2-12: advanced Menu -> SMBIOS Event Log

2.3.5.1 Event Log

This item let you disable or enable the event log.

Values: [Enabled/Disabled]

2.3.5.2 View SMBIOS event log

Press <Enter> to show the event log.

2.3.5.3 Mark SMBIOS events as read

This item will mark the event log as read. Events marked as read won't show up in the event log.

2.3.5.4 Clears SMBIOS events

This item clears the entire event log.

2.3.6 Thermal Configuration

The Thermal sub menu let you configure the system thermal monitor facilities.

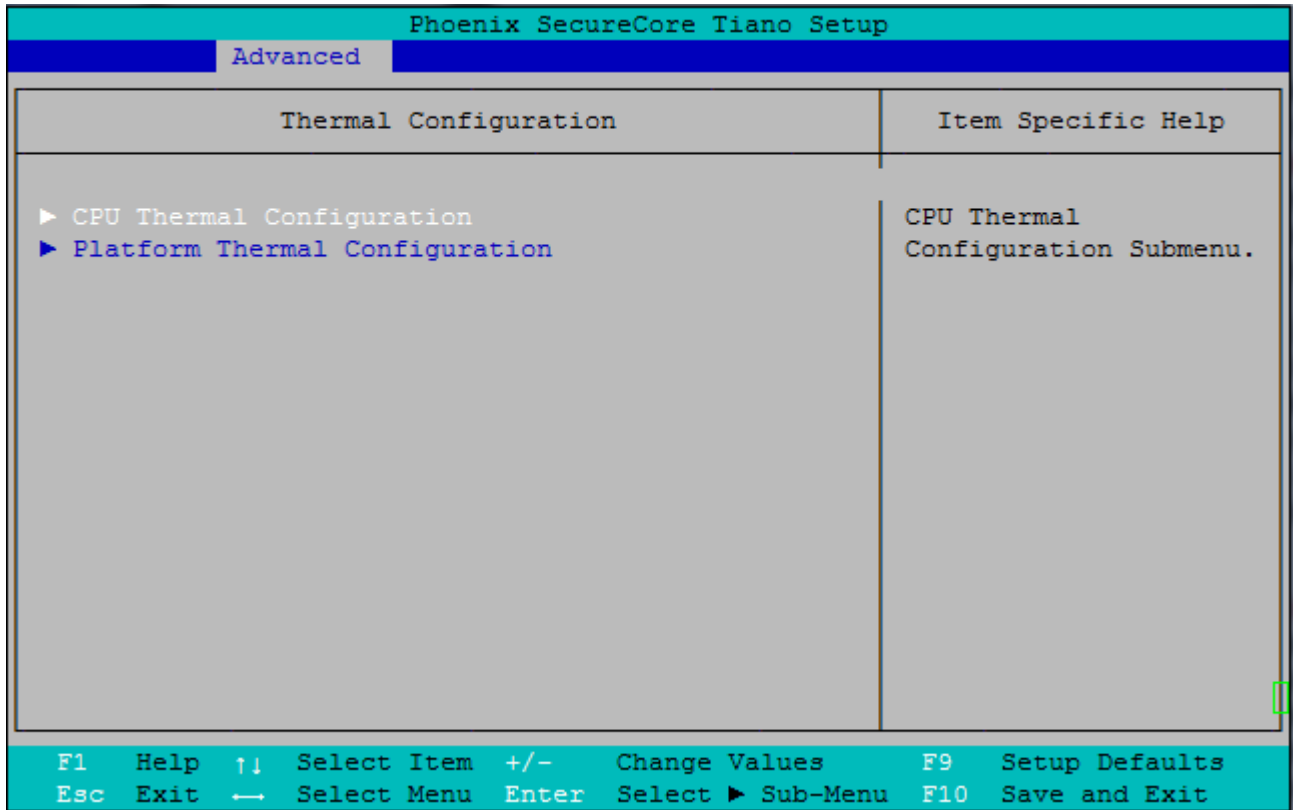


Figure 2-13: Advanced Menu -> Thermal Configuration

2.3.6.1 CPU Thermal Configuration

This sub menu let you configure the CPU specific thermal options. The options in this sub menu are CPU dependent.

2.3.6.1.1 Thermal Monitor TM2

This item enables the processor Thermal Monitor 2. If the CPU core temperature exceeds a certain threshold TM2 will reduce the operating frequency and voltage of the processor.

Values: [Enabled/Disabled]

2.3.6.1.2 Thermal Monitor TM1

This item enables the processor Thermal Monitor 1. If the CPU core temperature exceeds a certain threshold TM1 will reduce the duty cycle of the processor clock to reduce the CPU temperature.

Values: [Enabled/Disabled]

2.3.6.1.3 ACPI 3.0 T-States

Enables the ACPI CPU Throttling states. This feature requires a recent operation system.

Values: [Enabled/Disabled]

2.3.6.2 Platform Thermal Configuration

This sub menu let you configure the Platform/Chipset specific thermal options. The options in this sub menu are system dependent.

2.3.6.2.1 Critical Trip Point

This item let you set up the critical temperature where the OS should shutdown the system.

2.3.6.2.2 Passive TC1 / TC2 / TSP Values

These items configure the constants for the ACPI Passive Cooling. Use the <+> or <-> Keys to adjust the values to your needs. For specific info please see the ACPI Specification.

2.3.6.2.3 Thermal Data Report Enable

This item enables the reporting of thermal data for the OS.

Values: [Enabled/Disabled]

2.3.6.2.4 SCH/CPU Temp/Energy Read Enable

These items are read only.

2.4 Security

The Security Menu let you restrict the access to the Setup Menu by protecting it with a password.

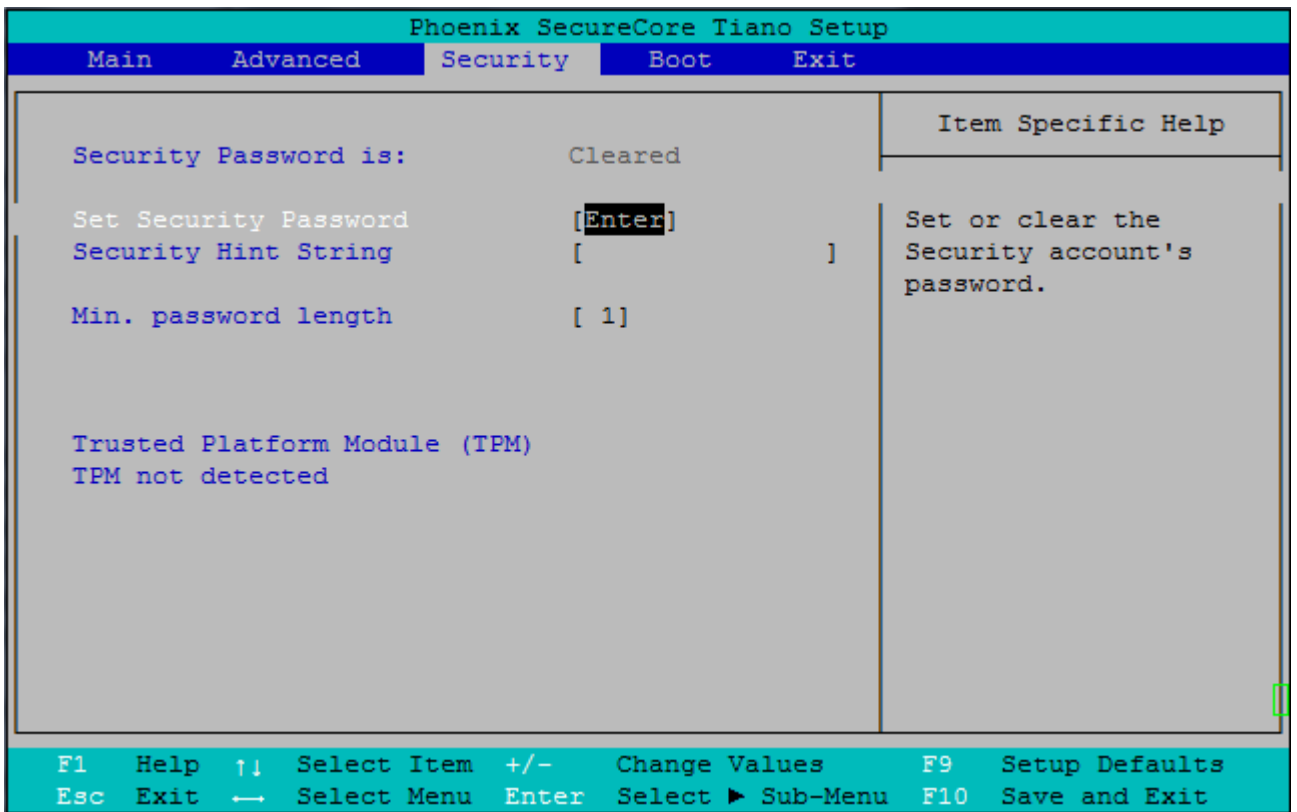


Figure 2-14: Security Menu

2.4.1 Security Password is:

Show whether the Security Password is set or cleared.

2.4.2 Set Security Password

Select to specify a security password. The security password protects the BIOS setup with a password.

2.4.3 Security Hint String

Select to specify a hint string for the security password.

2.4.4 Min. password length

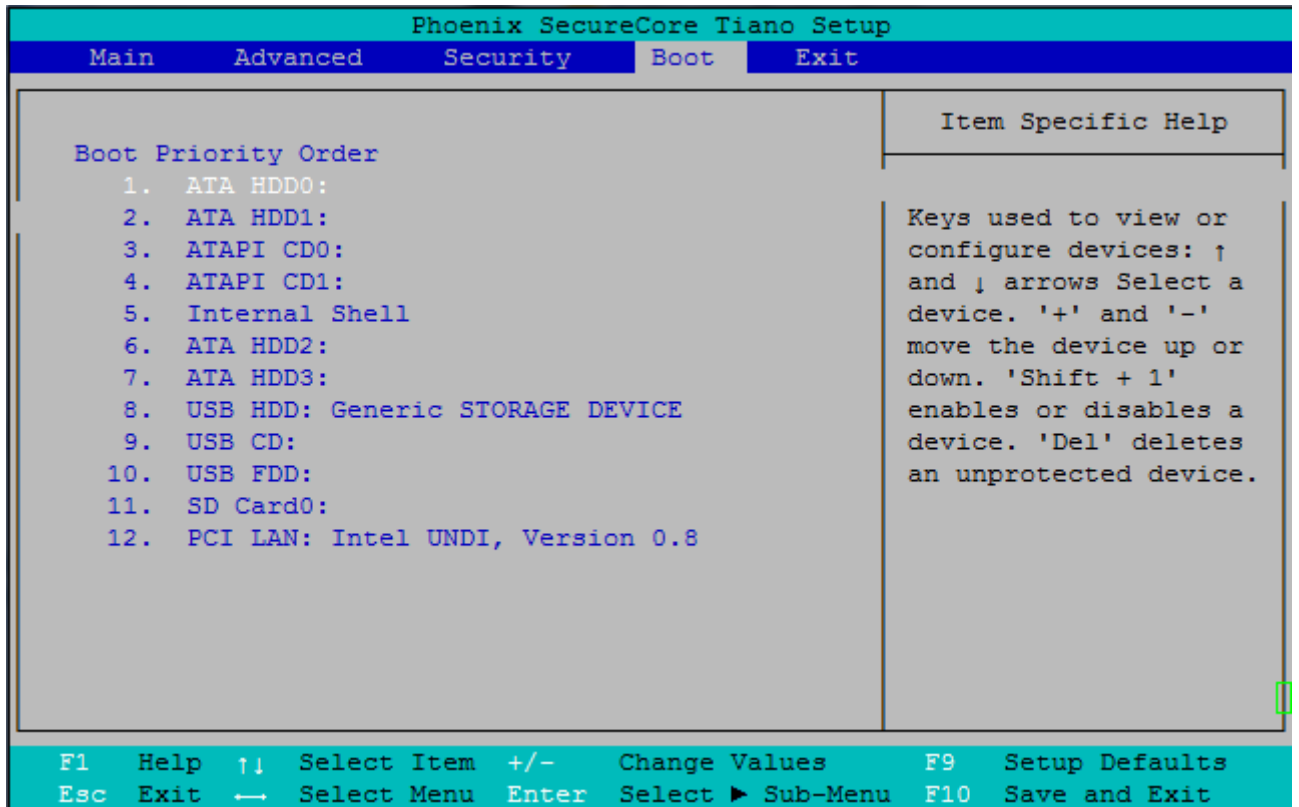
Specify the minimum password length.

2.4.5 Trusted Platform Module (TPM)

Read-only field that shows whether a TPM device is connected to the board or not.

2.5 Boot – Menu

In the Boot Menu the boot priority for connected storage devices can be set up.



2-15: Boot Menu: -> Boot Priority Order

2.5.1 Boot Priority Order

This menu let you change the boot device order. To move a device up or down in the list use <+> or <-> to change the position. A special entry is the Internal Shell item. This item will boot to the integrated UEFI-Shell.

2.6 Exit – Menu

In the Exit Menu you can save or discard all changes and exit the setup tool.

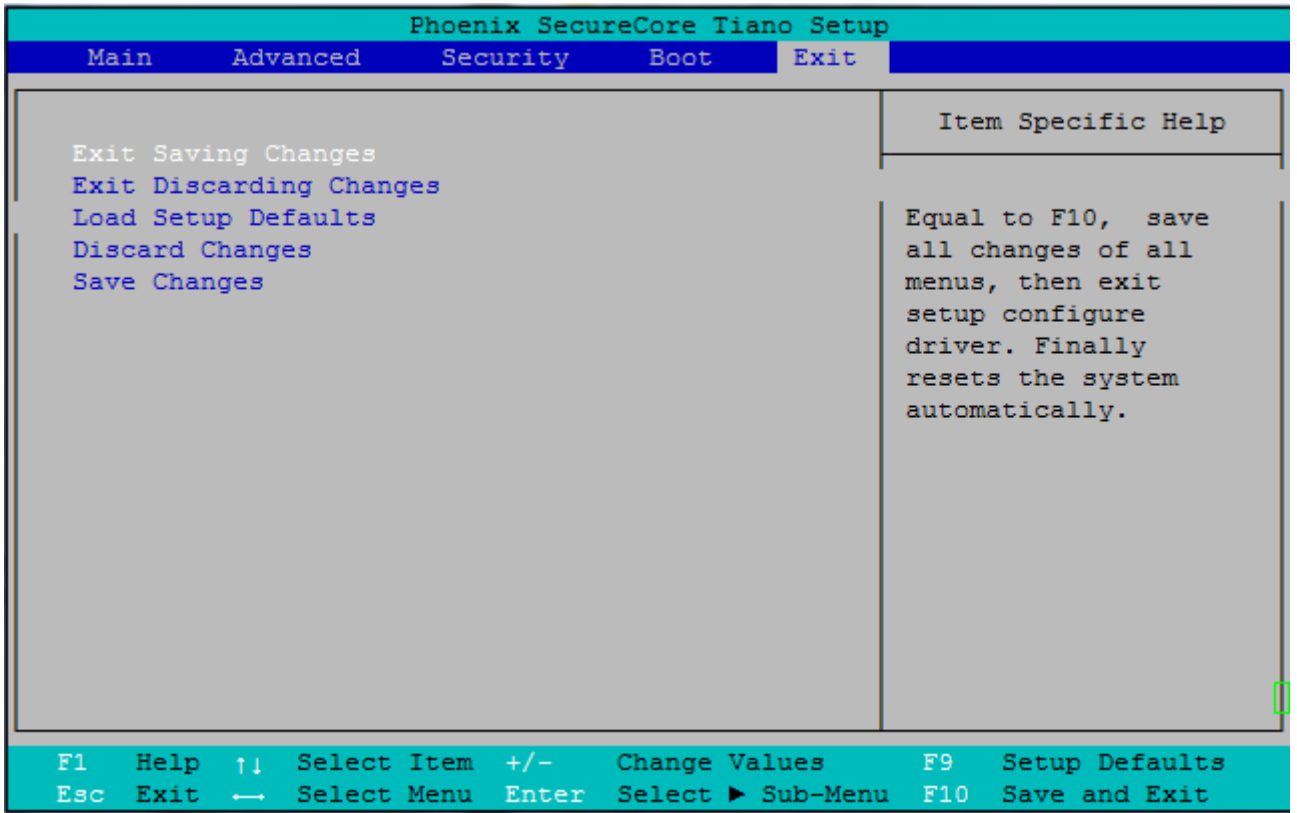


Figure 2-16: Exit - Menu

2.6.1 Exit Saving Changes

Selecting this is equivalent to pressing <F10>. All changes on all menus will be saved, and the system will exit the setup menu and will reset automatically.

2.6.2 Exit Discarding Changes

No changes will be saved, and the system will exit the setup menu and will reset automatically.

2.6.3 Load Setup Defaults

Selecting this is equivalent to pressing <F9>. The system will reset to the default configuration.

2.6.4 Discard Changes

Selecting this causes the system to load the original options at this current boot time. The system will not exit the setup menu after discarding changes.

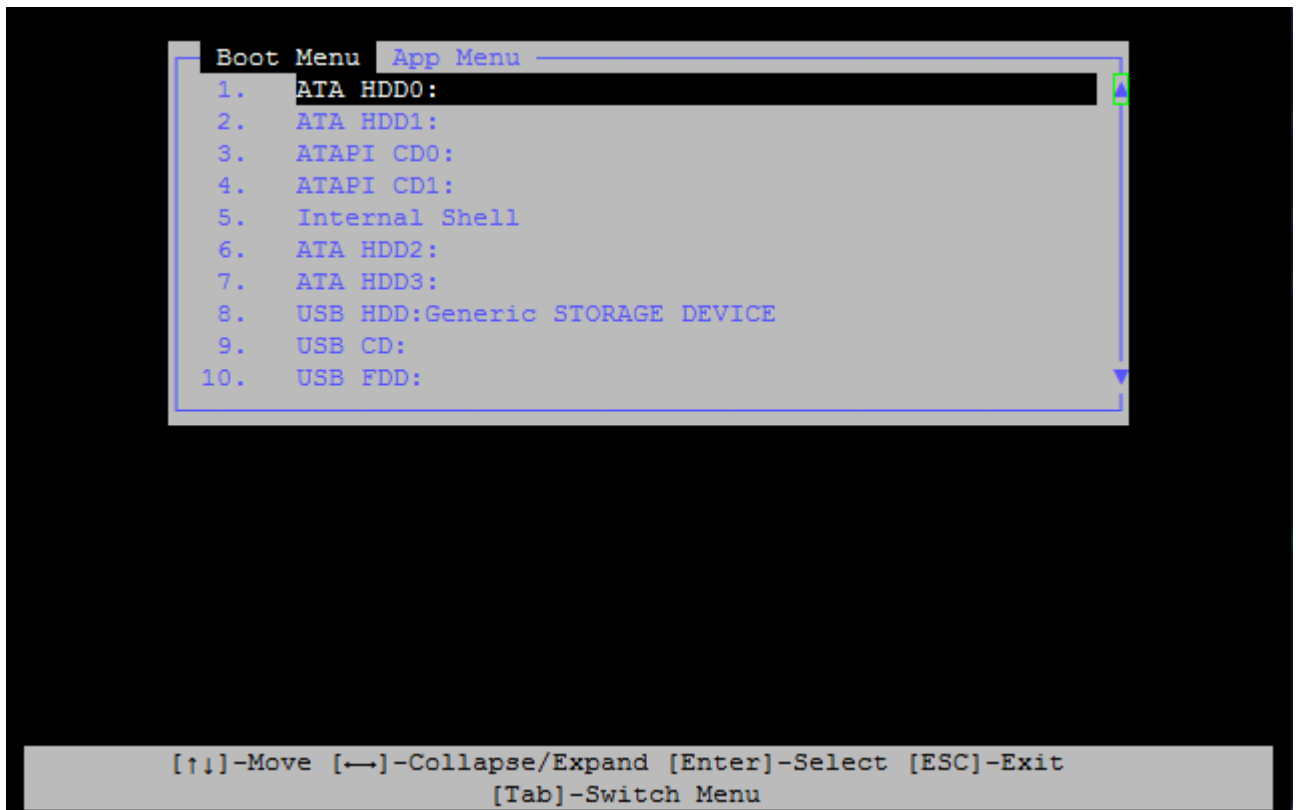
2.6.5 Save Changes

Selecting this causes the system to save all changes on all menus. The system will not exit the setup menu after saving.

3 Boot Menu & App Menu

3.1 Boot Menu

The Boot Menu let you choose an alternate boot device during startup. For a permanent change of the boot device use the Boot Priority Order item in the BIOS setup. To bring up the Boot Menu, press <F5> during boot up. Use <Up> and <Down> to select the boot medium. Press <Enter> to continue booting from this device.



3-1: Boot Menu

3.2 App Menu

With the App Menu you can enter the BIOS setup screen or view the Diagnostic Splash screen. The App Menu is accessed through the Boot Menu, press <F5> during boot to bring up the Boot Menu, then press <Tab> to switch to the App Menu.

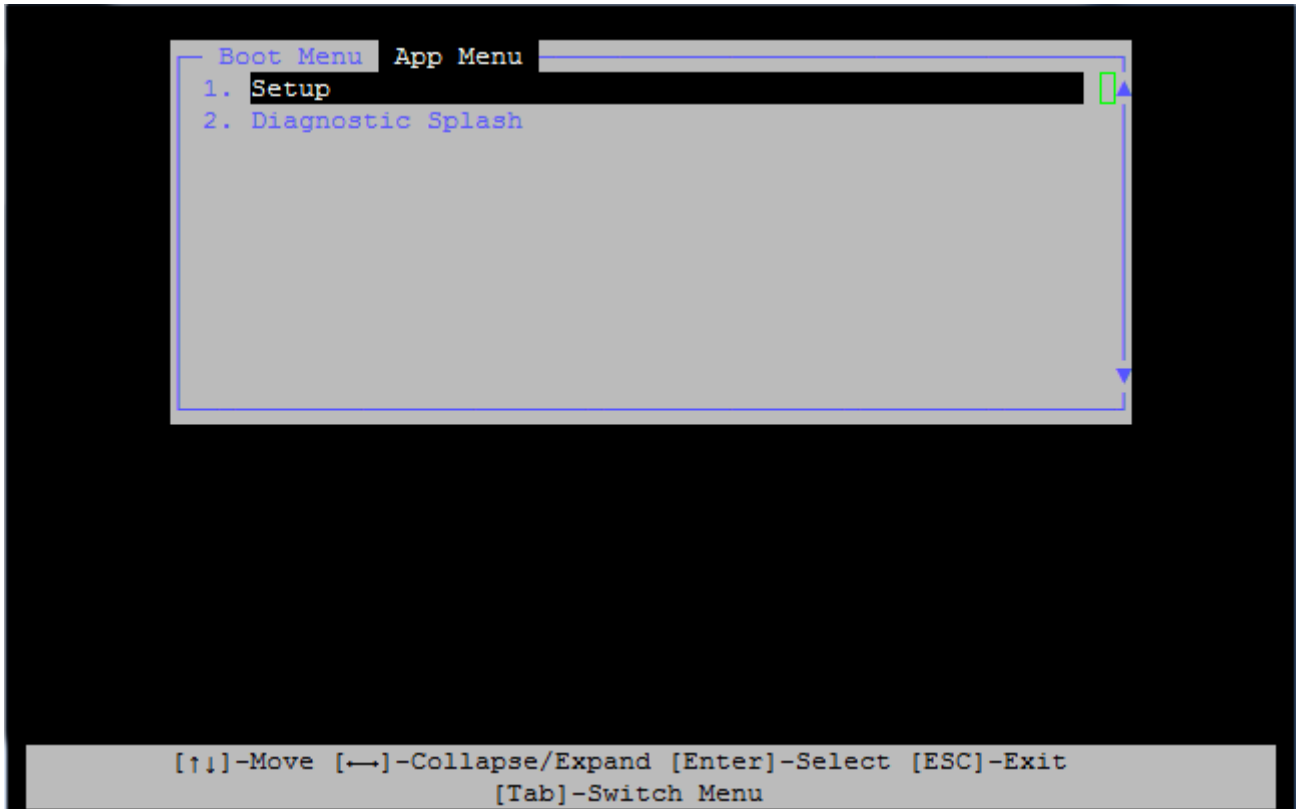


Figure 3-2: App Menu

4 UEFI Shell

The UEFI shell let you run EFI programs directly. The UEFI-Shell is similar to a DOS or Unix Shell. For a general command overview type *help* in the shell and press **<Enter>**. To exit the UEFI shell and continue booting use the *exit* command.

```
Acpi (PNP0A03,0)/Pci (17|0)/Pci (0|0)/Pci (2|2)/Usb (0,0)/HD (Part1,SigD1DC
F877)
  blk0      :Removable HardDisk - Alias hd29a0b fs0
            Acpi (PNP0A03,0)/Pci (17|0)/Pci (0|0)/Pci (2|2)/Usb (0,0)/HD (Part1,SigD1DC
F877)
  blk1      :Removable BlockDevice - Alias (null)
            Acpi (PNP0A03,0)/Pci (17|0)/Pci (0|0)/Pci (2|2)/Usb (0,0)

Press ESC in 5 seconds to skip startup.nsh, any other key to continue.
Shell> fs0:

fs0:\> cd IA32

fs0:\IA32> ls HelloWorld.efi
Directory of: fs0:\IA32

    12/08/11  03:07p                7,008  HelloWorld.efi
            1 File(s)                7,008 bytes
            0 Dir(s)

fs0:\IA32> HelloWorld.efi
UEFI Hello World!

fs0:\IA32> █
```

Figure 4-1: EFI - Shell

Appendix A, Contact Information

Headquarters

LiPPERT Embedded Computers GmbH

Hans-Thoma-Straße 11

68163 Mannheim

Germany

Phone	+49 621 43214-0
Fax	+49 621 4321430
E-mail	sales@lippertembedded.com
	support@lippertembedded.com
Website	www.lippertembedded.com

US Office

LiPPERT Embedded Computers, Inc.

2220 Northmont Parkway, Suite 250

Duluth, GA 30096

USA

Phone	+1 (770) 295 0031
Fax	+1 (678) 417 6273
E-mail	ussales@lippertembedded.com
	support@lippertembedded.com
Website	www.lippertembedded.com

Appendix B, Getting Help

Should you have technical questions that are not covered by the respective manuals, please contact our support department at support@lippertembedded.com .

Please allow one working day for an answer!

Technical manuals as well as other literature for all LiPPERT products can be found in the *Products* section of LiPPERT's website www.lippertembedded.com. Simply locate the product in question and follow the link to its manual.

Returning Products for Repair

To return a product to LiPPERT for repair, you need to get a Return Material Authorization (RMA) number first. Please print the RMA Request Form from <http://www.lippertembedded.com/service/repairs.html> fill in the blanks and fax it to +49 621 4321430. We'll return it to you with the RMA number.

Deliveries without a valid RMA number are returned to sender at his own cost!

LiPPERT has a written Warranty and Repair Policy, which can be retrieved from <http://www.lippertembedded.com/service/warranty.html>

It describes how defective products are handled and what the related costs are. Please read this document carefully before returning a product.

Appendix C, Revision History

Revision	Date	Edited by	Change
0.0	2011-12-23	SLB	Draft
0.1	2012-01-23	MG	Release