HEP8225

8225-xxx

No. 87-508285-001 Revision B

BIOS SETUP

TECHNICAL REFRENCE

APTIO® V UEFI BIOS FIRMWARE

For use with

Intel® Xeon® E5-2600 v3/v4 Series

14, 12, 10, 8 and 6-Core Dual Processor-Based SHB

HDEC Series®

WARRANTY

The following is an abbreviated version of Trenton Systems' warranty policy for modular blade card products. For a complete warranty statement, contact Trenton or visit our website at: www.trentonsystems.com/about-us/company-policies/.

Trenton system host board products are warranted against material and manufacturing defects for five years from date of delivery to the original purchaser. Buyer agrees that if this product proves defective Trenton Systems, Inc. is only obligated to repair, replace or refund the purchase price of this product at Trenton Systems' discretion. The warranty is void if the product has been subjected to alteration, neglect, misuse or abuse; if any repairs have been attempted by anyone other than Trenton Systems, Inc.; or if failure is caused by accident, acts of God, or other causes beyond the control of Trenton Systems, Inc. Trenton Systems, Inc. reserves the right to make changes or improvements in any product without incurring any obligation to similarly alter products previously purchased.

In no event shall Trenton Systems, Inc. be liable for any defect in hardware or software or loss or inadequacy of data of any kind, or for any direct, indirect, incidental or consequential damages arising out of or in connection with the performance or use of the product or information provided. Trenton Systems, Inc.'s liability shall in no event exceed the purchase price of the product purchased hereunder. The foregoing limitation of liability shall be equally applicable to any service provided by Trenton Systems, Inc.

RETURN POLICY

A Return Material Authorization (RMA) number, obtained from Trenton Systems prior to return, must accompany products returned for repair. The customer must prepay freight on all returned items, and the customer is responsible for any loss or damage caused by common carrier in transit. Items will be returned from Trenton via Ground, unless prior arrangements are made by the customer for an alternative shipping method

To obtain an RMA number, call us at (800) 875-6031 or (770) 287-3100. We will need the following information:

Return company address and contact

Model name and model # from the label on the back of the product

Serial number from the label on the back of the product

Description of the failure

An RMA number will be issued. Mark the RMA number clearly on the outside of each box, include a failure report for each board and return the product(s) to our Gainesville, GA facility:

Trenton Systems, Inc.

1725 MacLeod Drive

Lawrenceville, GA 30043

Attn: Repair Department

Contact Trenton Systems for our complete service and repair policy.

TRADEMARKS

HDEC is a trademark of Trenton Systems Inc.

IBM, PC/AT, VGA, EGA, OS/2 and PS/2 are trademarks or registered trademarks of International Business Machines Corp.

AMI, Aptio and AMIBIOS are trademarks of American Megatrends Inc.

Intel, Xeon, Intel Quick Path Interconnect, Intel Hyper-Threading Technology and Intel Virtualization Technology are trademarks or registered trademarks of Intel Corporation.

MS-DOS and Microsoft are registered trademarks of Microsoft Corp.

PCI Express is a trademark of the PCI-SIG.

All other brand and product names may be trademarks or registered trademarks of their respective companies.

LIABILITY DISCLAIMER

This manual is as complete and factual as possible at the time of printing; however, the information in this manual may have been updated since that time. Trenton Systems Inc. reserves the right to change the functions, features or specifications of their products at any time, without notice.

E-mail: Support@TrentonSystems.com
Web: www.TrentonSystems.com

TRENTON Systems Inc. 1725 MacLeod Drive • Lawrenceville, Georgia 30043

Sales: (800) 875-6031 • Phone: (770) 287-3100 • Fax: (770) 287-3150

Contents

Chapter 1 Starting Aptio® TSE 1

Introduction 1

Starting Aptio TSE 1

Navigation 2

Chapter 2 Main Menu 3

Aptio TSE Setup Menu 3

Chapter 3 Advanced Setup 4

Introduction 4

ACPI 5

AST 2400 SuperIO Configuration 5

Serial Port Console Redirection 5

PCI Subsystem Settings 7

Network Stack Configuration 9

CSM (Compatibility Support Module) Configuration 9

Trusted Computing 9

USB Configuration 9

iSCSI Configuration 10

Chapter 4 IntelRCSetup 11

Introduction 11

Processor Configuration 12

IIO Configuration 14

PCH Configuration 24

Server Management Engine Configuration 26

Runtime Error Logging 26

Miscellaneous Configuration 27

Chapter 5 Security 28

Two Levels of Password Protection 28

Remember the Password 28

Security Configuration 29

Chapter 6 Boot Setup 30

Introduction 30

Boot Configuration *31*

Chapter 7 Save & Exit **32**

Introduction *32*

Save Changes & Exit *33*

Discard Changes & Exit *33*

Save Changes & Reset *33*

Discard Changes & Reset *33*

Save Options *33*

Restore Defaults *33*

Save as User Defaults *34*

Restore User Defaults *34*

Boot Override *34*

Appendix A Aptio V BIOS Messages **35**

Introduction *35*

Aptio Boot Flow *35*

BIOS Beep Codes *35*

BIOS Status POST Code LEDs *35*

Table of BIOS Status and Beep Codes *37*

Checkpoint Ranges 37

Standard Checkpoints *37*

SEC Phase 37

SEC Beep Codes 38

PEI Phase 38

PEI Beep Codes 40

DXE Phase 40

DXE Beep Codes 42

ACPI/ASL Checkpoints *43*

OEM-Reserved Checkpoint Ranges *43*

SHB Handling Precautions

WARNING: This product has components that may be damaged by electrostatic discharge.

To protect your system host board (SHB) from electrostatic damage, be sure to observe the following precautions when handling or storing the board:

- Keep the SHB in its static-shielded bag until you are ready to perform your installation.
- Handle the SHB by its edges.
- Do not touch the I/O connector pins.
- Do not apply pressure or attach labels to the SHB.
- Use a grounded wrist strap at your workstation or ground yourself frequently by touching the metal chassis of the system before handling any components. The system must be plugged into an outlet that is connected to an earth ground.
- Use antistatic padding on all work surfaces.
- Avoid static-inducing carpeted areas.

Recommended Board Handling Precautions

This SHB has components on both sides of the PCB. Some of these components are extremely small and subject to damage if the board is not handled properly. It is important for you to observe the following precautions when handling or storing the board to prevent components from being damaged or broken off:

- Handle the board only by its edges.
- Store the board in padded shipping material or in an anti-static board rack.
- Do not place an unprotected board on a flat surface.

Chapter 1 Starting Aptio® TSE

Introduction

The HEP8225 features the Aptio® V BIOS from American Megatrends, Inc. (AMI) with a ROM-resident setup utility called the Aptio® Text Setup Environment, or, TSE. The TSE allows you to select from the following sections of configuration options:

- Main Menu
- Advanced Setup
- IntelRCSetup
- Security
- Boot
- Save & Exit Setup

Each of these options allow you to review and/or change various setup features of your system. Details are provided in the following chapters of this manual. Additional copies of the Trenton HEP8225 BIOS and hardware technical references are available under the **Downloads** tab on the HEP8225 web page.

Aptio Text Setup Environment (TSE) is a text-based basic input and output system intended to empower the user with complete system control at boot. This document explains the basic navigation of Aptio TSE.

Note: The contents of this document were provided as a courtesy from American Megatrends, Inc. (AMI) and describe the standard look and feel of the Aptio TSE interface. Trenton Systems, Inc. is the manufacturer of the System Host Board hardware (SHB) and during production may have made changes to the options described herein. Therefore, some of the options that are described in this document may not exist or may have been modified for use in the HEP8225 BIOS implementation. Contact Trenton technical support for any questions regarding the SHB's implementation of Aptio TSE.

Starting Aptio TSE

To enter the Aptio TSE screens, follow the steps below.

Step	Description
1	Install the SHB in a HDEC Series® backplane with the proper system power connections affixed. Attach a keyboard, mouse and monitor to the SHB.
2	Power the system on.
3	Press the <Delete> or <F2> keys on the keyboard when you see the text prompt, "**Press DEL or F2 to enter Setup.**"
4	After you press the <Delete> /<F2> key, the Aptio TSE main BIOS menu displays, you can access the other setup screens from the main BIOS setup menu, such as chipset and power control menus.

Note: In most cases, the <Delete> or <F2> keys are used to invoke the Aptio TSE screen. In some cases, other keys may be used such as <F1>, <F10> <F11> or <F12>.

Note: The user can press the <TAB> key during boot to switch from the boot splash screen to see the keystroke messages and current POST information.

There may be slight differences in the illustrations in this manual due to Trenton HEP8225 BIOS modifications. Contact Trenton Technical support for any questions regarding the SHB implementation of Aptio TSE.

Navigation

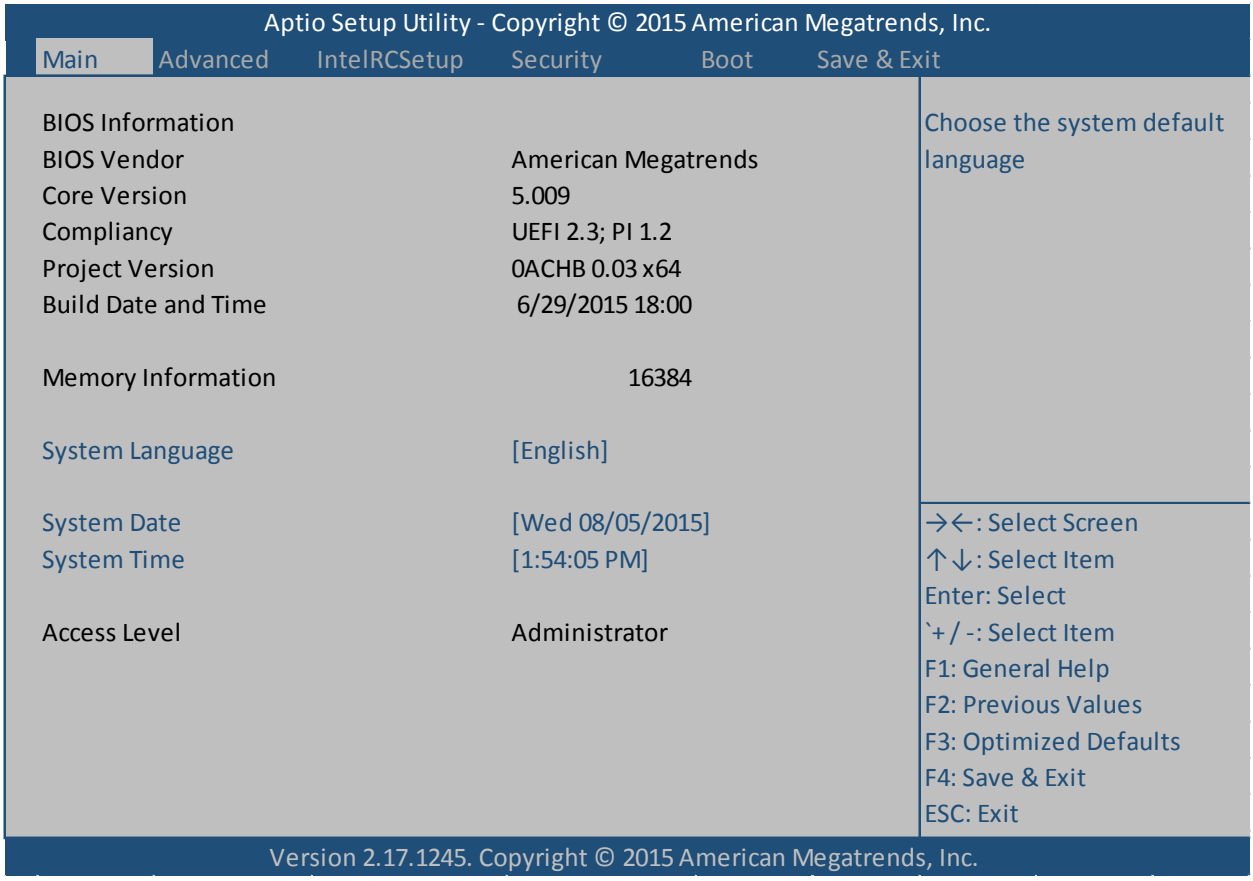
The Aptio TSE keyboard-based navigation can be accomplished using various <FUNCTION> keys as well as <ENTER>, <ESC>, <ARROW> keys, etc.

Key	Description
ENTER	The *Enter* key allows the user to select an option to edit its value or access a sub menu.
→← Left/Right	The *Left and Right* <Arrow> keys allow you to select an Aptio TSE screen. For example: Main screen, Advanced screen, Chipset screen, and so on.
↑↓ Up/Down	The *Up and Down* <Arrow> keys allow you to select an Aptio TSE item or sub-screen.
+- Plus/Minus	The *Plus and Minus* <Arrow> keys allow you to change the field value of a particular setup item. For example: Date and Time.
Tab	The <Tab> key allows you to select Aptio TSE fields.
ESC	The <Esc> key allows you to discard any changes you have made and exit the Aptio TSE. Press the <Esc> key to exit the Aptio TSE without saving your changes. The following screen will appear: Press the <Enter> key to discard changes and exit. You can also use the <Arrow> key to select *Cancel* and then press the <Enter> key to abort this function and return to the previous screen.
Function keys	When other function keys become available, they are displayed in the help screen along with their intended function.

Chapter 2 Main Menu

Aptio TSE Setup Menu

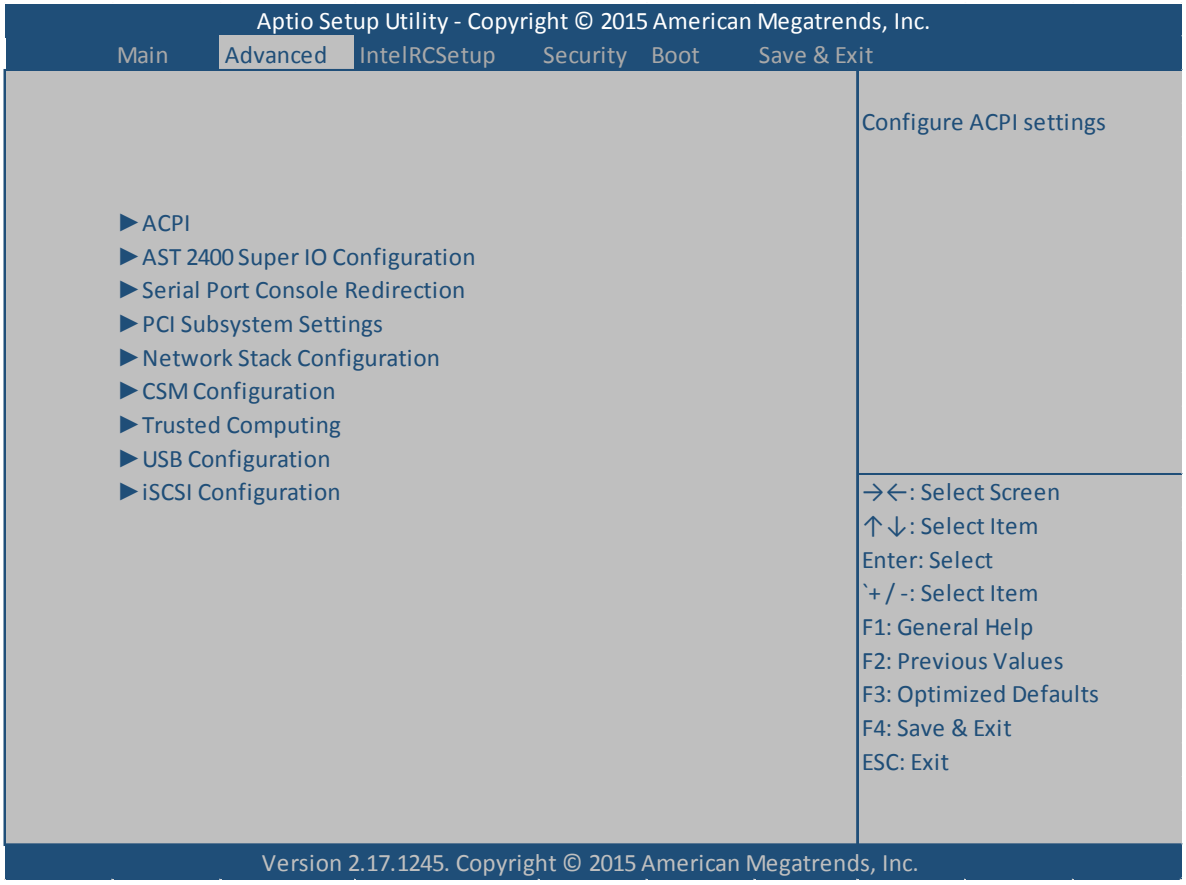
The Aptio TSE BIOS setup menu is the first screen that you can navigate. It provides basic information about current system configuration including BIOS revision, installed processor(s) and memory. In addition, it provides configuration options for System Language, current System Date and Time and current system Access Level.



Chapter 3 Advanced Setup

Introduction

Select the *Advanced* menu item from the Aptio TSE screen to enter the Advanced BIOS Setup screen. You can select any of the items in the left frame of the screen, such as ACPI, PCI Subsystem Settings or iSCSI Configuration. Selecting one of these set-up items will take you to a configuration sub menu for that item.



ACPI

Key	Description
Enable ACPI Auto Configuration	**Disabled**/Enabled -Enables or disables the Advanced Configuration and Power interface automatic configuration ability.
Enable Hibernation	**Enabled**/Disabled – Enables or disables the "hibernation" OS/4 sleep state. This function of this operation is Operating System dependent. Refer to your OS vendor for more information on hibernation.
Lock Legacy Resources	**Disabled**/Enabled – Enables or disables legacy resources.

AST 2400 SuperIO Configuration

Key	Description
►Serial Port 1 Configuration (Sub Menu)	Serial Port: **Enabled**/Disabled – Enables or disables the Serial Port.
	Device Settings: IO=3F8h; IRQ4 – This is a static, no-option display that displays the current IO and IRQ settings for Serial Port 1.
	Change Settings: **Auto** / IO=3F8h; IRQ4 / IO=3F8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=2F8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=3E8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=2E8h; IRQ=3,4,5,6,7,8,9,10,11,12
►Serial Port 2 Configuration (Sub Menu)	Serial Port: **Enabled**/Disabled – Enables or disables the Serial Port.
	Device Settings: IO=3F8h; IRQ4 – This is a static, no-option display that displays the current IO and IRQ settings for Serial Port 2.
	Change Settings: **Auto** / IO=3F8h; IRQ4 / IO=3F8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=2F8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=3E8h; IRQ=3,4,5,6,7,8,9,10,11,12 / IO=2E8h; IRQ=3,4,5,6,7,8,9,10,11,12
Boost Fans to Full Speed	**Disabled**/Enabled – When enabled, fans will always run at full speed.

Serial Port Console Redirection

Console Redirection	**Disabled**/Enabled – Enables or disables console redirection for legacy serial applications. The below options become editable when "Enabled" is selected.
►Console Redirection Settings	Terminal Type: **ANSI**/VT100/VT100+/VT-UTF8 – Selects the configuration of the terminal. Emulation: ANSI-extended character set. VT100+ extends VT100 to support color, function keys, etc. VT-UTF8 uses UTF8 encoding to map Unicode characters on to 1 or more bytes.
	Bits Per Second: **115200**/9600/19200/38400/57600 – Selects serial port transmission speed. Speed must be matched on the other side of the COM. Long or noisy lines may require lower speeds.
	Data Bits: **8**/7 – Selects the number of data bits sent with each packet.
	Parity: **None**/Even/Odd/Mark/Space – A parity bit can be sent with the data bits to

	detect some transmission errors. Even parity: a parity bit is 0 if the sum of 1s in the data bits is even. Odd parity: a parity bit is 1 if some of 1s in the data bits is odd. Mark parity: the parity bit is always 1. Space parity: the parity bit is always 0. Mark and Space parity do not allow for error detection.
	Stop Bits: **1**/2 - Stop bits indicate the end of a serial data packet. Communication with slow devices may require more than one stop bit.
	Flow Control: **None**/Hardware RTS/CTS – Flow control can prevent data loss from buffer overflow.
	VT-UTF8 Combo Key Support: **Enable**/Disable – Enables VT-UTF8 Combo Key support for ANSI/VT100 terminals.
	Recorder Mode: **Disable**/Enable – With this mode enabled, only text will be sent, this is to capture terminal data.
	Resolution 100x31: **Disable**/Enable – Enables or disables extended terminal resolution.
	Legacy OS Redirection Resolution: **80x24**/80x25 – Alters the number of rows and column supported.
	PuTTY Keypad: **VT100**/Linux/xTerm6/SCO/ESCN/VT400 – Alters the style of keypad used in transmission over SSH.
	Redirection after BIOS post: **Always Enable**/Bootloader – An option for legacy OSes that require a bootloader.
►Legacy Console Redirection Settings	Terminal Type: **VT-UTF8**/VT100/VT100+/ANSI – VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100.
	Bits Per Second: **115200**/57600/19200/9600 – Selects the serial port transmission speed. The speed must be matched on the other side of the COM. Long or noisy lines may require lower speeds.
	Flow Control: **None** / Hardware RTS/CTS / Software Xon/Xoff – Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a stop signal can be sent to stop the data flow. Once the buffers are empty, a start signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signals.

PCI Subsystem Settings

Key	Description
PCI Bus Driver Version	A5.01.05 – This is a static display that cannot be user edited.
PCI Latency Timer	**32 PCI Bus Clocks**/64 PCI Bus Clocks/96 PCI Bus Clocks/128 PCI Bus Clocks/160 PCI Bus Clocks/192 PCI Bus Clocks/224 PCI Bus Clocks/248 PCI Bus Clocks – This is the value that is programmed into the PCI latency timer register.
PCI-X Latency Timer	**64 PCI Bus Clocks**/32 PCI Bus Clocks/96 PCI Bus Clocks/128 PCI Bus Clocks/160 PCI Bus Clocks/192 PCI Bus Clocks/224 PCI Bus Clocks/248 PCI Bus Clocks – This is the value that is programmed into the PCI latency timer register.
VGA Palette Snoop	**Disabled**/Enabled – Enables or disables VGA palette registers snooping.
PERR# Generation	**Disabled**/Enabled – Enables or disables PCI PERR# generation.
SERR# Generation	**Disabled**/Enabled – Enables or disables PCI SERR# generation.
Above 4G Decoding	**Disabled**/Enabled – Enables or disables 64 bit capable devices to be decoded in above 4g address space if system supports 64 bit PCI decoding.
SR-IOV Support	**Disabled**/Enabled – Enables or disables Single Root IO Virtualization support if system has SR-IOV-capable PCIe devices.
►PCI Express Settings	Relaxed Ordering: **Disabled**/Enabled – Enables or disables PCI express relaxed ordering.
	Extended Tag: **Disabled**/Enabled – When enabled, allows devices to use 8-bit tag field as a register.
	No Snoop: **Enabled**/Disabled – Enables or disables PCI Express device 'no snoop' option.
	Maximum Payload: **Auto**/128 Bytes/256 Bytes/512 Bytes/1024 Bytes/2048 Bytes/4096 Bytes – Selects the maximum payload for PCI Express Devices. 'Auto' allows the BIOS to select the value.
	Extended Synch: **Disabled**/Enabled – If enabled, extended synchronization patterns may be generated.
	Link Training Retry: **5**/Disabled/2/3 – Defines the number of retry attempts the BIOS will undertake to retrain the link if the previous attempt was unsuccessful.
	Link Training Timeout (uS): **1000** – Defines the number of microseconds the BIOS will wait before attempting to train the PCIe link. Values may be set from 10 to 10000uS.
	Unpopulated Links: **Keep Link ON**/Disable Link – Determines if the BIOS will power down links that are determined to be unpopulated to conserve power.
	Restore PCIe Registers: **Disabled**/Enabled – On non-PCIe-aware operating systems (i.e. pre-Windows Vista) some devices may not be correctly reinitialized after sleep sate S3. Enabling this setting restores the PCIe configurations after S3. *Enabling this setting may cause hardware stability issues. Proceed with caution.*

►PCI Express Gen2 Settings	Completion Timeout: **Default**/Shorter/Longer/Disabled – In device functions that support completion timeout programmability, this setting allows the system software to modify the value. The default value is 50uS to 50mS. If shorter is selected, the software will use shorter timeout ranges, if supported by the hardware. If longer is selected, the software will use longer timeout ranges, if supported. 'Disabled' disables this functionality.
	ARI Forwarding: **Disabled**/Enabled – If supported by hardware and enabled, the downstream port disables its traditional 'Device Number' field. This allows access to extended functions in an ARI device immediately below the port.
	AtomicOp Requester Enable: **Disabled**/Enabled – If supported by hardware and enabled, this function initiates AtomicOp requests only if the Bus Master Enable bit is in the Command Register Set.
	AtomicOp Egress Blocking: **Disabled**/Enabled – If supported by hardware and enabled, outbound AtomicOp requests via egress ports will be blocked.
	IDO Request Enable: **Disabled**/Enabled – If supported by hardware and enabled, this allows setting the number of ID-Based Ordering (IDO) bit attribute 2 requests to be initiated.
	IDO Completion Enable: **Disabled**/Enabled – If supported by hardware and enabled, this allows setting the number of ID-Based Ordering (IDO) bit attribute 2 requests to be initiated.
	LTR Mechanism Enable: **Disabled**/Enabled – If supported by hardware and enabled, this enables the Latency Tolerance Reporting (LTR) mechanism to be initiated.
	End-End TLP Prefix Blocking: **Disabled**/Enabled – If supported by hardware and set to enabled, this function will block forwarding of TLPs containing End-End TLP prefixes.
	Clock Power Management: **Disabled**/Enabled – If supported by hardware and set to enabled, the device is permitted to use 'CLKREQ#' signal for power management of Link clock in accordance to protocol defined in the appropriate form factor specification.
	Compliance SOS: **Disabled**/Enabled – If supported by hardware and set to enabled, this will force LTSSM to send SKP Ordered Sets between sequences when sending compliance pattern or modified compliance pattern.
	Hardware Autonomous Width: **Enabled**/Disabled – If supported by hardware and set to disabled, this will prevent the hardware from changing link width except in cases of unstable link operation.
	Hardware Autonomous Speed: **Enabled**/Disabled – If supported by hardware and set to disabled, this will prevent the hardware from changing link speed except in cases where transmission rate must be reduced because of unstable link operation.

Network Stack Configuration

Key	Description
►Network Stack	**Disabled**/Enabled
	IPv4 PXE Support: **Enabled**/Disabled – Enables or disables Internet Protocol version 4 Preboot eXecution Environment.
	IPv6 PXE Support: **Enabled**/Disabled – Enables or disables Internet Protocol version 4 Preboot eXecution Environment.
	PXE boot wait time: **0** – Determines the number of seconds the BIOS will wait for the <ESC> key to be pressed in order to abort a PXE boot.
	Media Detect Count: **1** – Determines the number of times interfaces will be checked viable media.

CSM (Compatibility Support Module) Configuration

Key	Description
CSM Support	**Enabled**/Disabled – Enables or disables the Compatibility Support Module.
GateA20 Active	**Upon Request**/Always – Upon Request: GA20 can be disabled using BIOS services. Always: do not allow disabling GA20; this option when any RT code is executed larger than 1MB.
Option ROM Messages	**Force BIOS**/Keep Current – Sets the display mode for the Option ROM.
Boot Option Filter	**UEFI and Legacy**/Legacy Only/UEFI Only – Selects the ROM priority.
Network	**Legacy**/Do not launch/UEFI – Controls the execution of UEFI and Legacy PXE ROMs.
Storage	**Legacy**/Do not launch/UEFI – Controls the execution of UEFI and Legacy Storage OpROMs.
Other PCI Devices	**Legacy**/UEFI – Determines OpROM execution policy for devices other than Network, Storage or Video.

Trusted Computing

Key	Description
Security Device Support	**Disabled**/Enabled – Enables or disables support for BIOS security device. Operating system will not show the security device. TCG EFI protocol and INT1A interface will not be available if enabled.

USB Configuration

Key	Description
Legacy USB Support	**Enabled**/Disabled/Auto – Enables legacy USB support. 'Auto' option disables legacy support if no applicable USB devices are connected. 'Disable' option will keep USB devices available only for EFI applications.

XHCI Hand-off	**Enabled**/Disabled – A workaround for operating systems without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI driver.
EHCI Hand-off	**Disabled**/Enabled – A workaround for operating systems without EHCI hand-off support. The EHCI ownership change should be claimed by the EHCI driver.
USB Mass Storage Driver Support	**Enabled**/Disabled – Enables support for USB mass storage devices in the boot order.
Port 60/64 Emulation	**Enabled**/Disabled – Enables I/O port 60h/64h emulation support. This should be enabled for complete legacy USB keyboard support for non-USB-aware operating systems.
USB Transfer Time-Out	**20 sec**/1 sec/ 5 sec/ 10 sec – Sets the time-out value for Control, Bulk and Interrupt transfers.
Device Reset Time-Out	**20 sec**/10 sec/30 sec/40 sec – USB mass storage device storage device 'Start Unit' command time-out.
Device Power-Up Delay	**Auto**/Manual – Sets the maximum time the device will take before it can properly report itself to the Host Controller. 'Auto' uses the default value: for a root port this is 100mS. For a hub port, the delay reported by the hub descriptor is used.

iSCSI Configuration

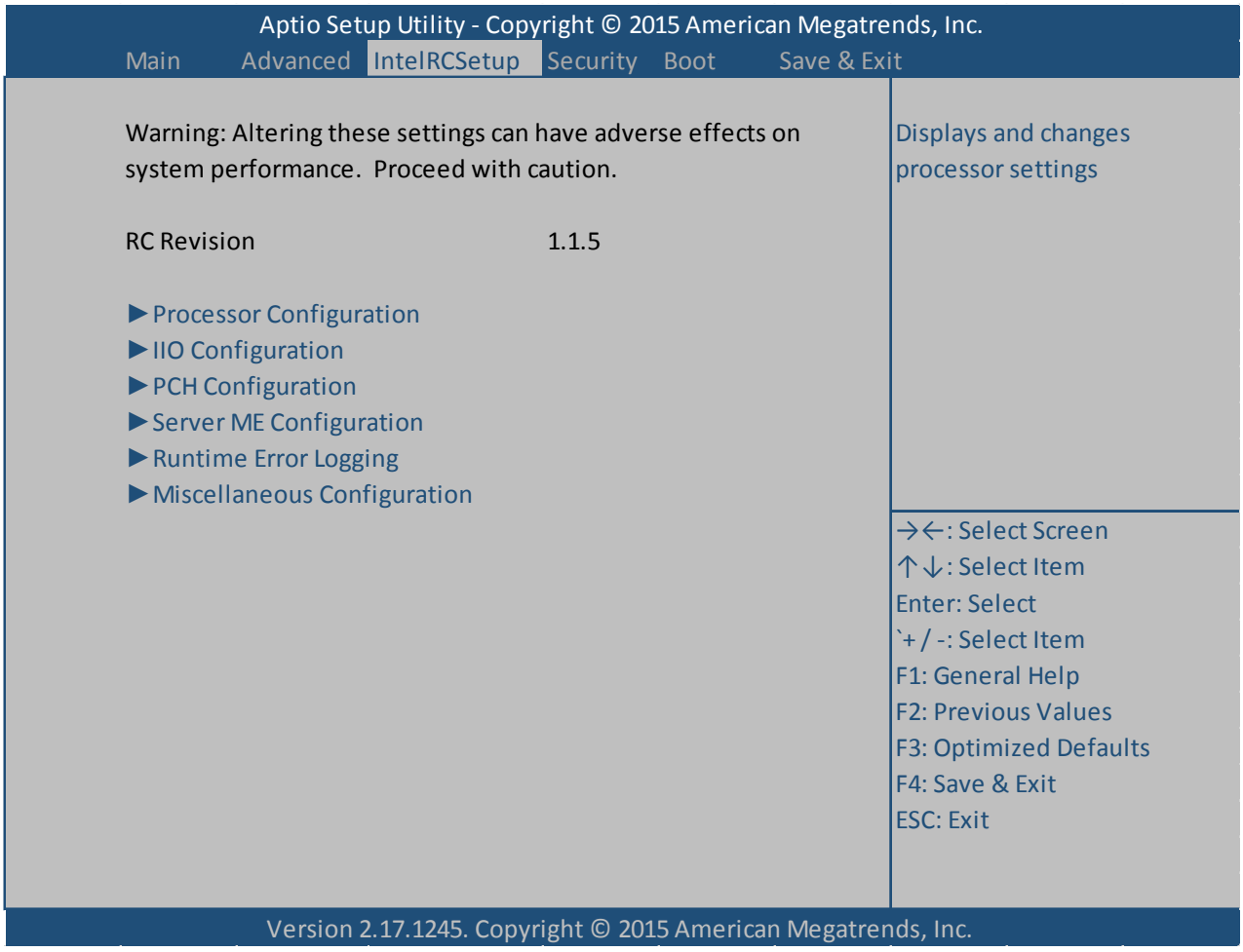
Key	**Description**
iSCSI Initiator Name	The worldwide unique name of the iSCSI Initiator. Only IQN format is accepted. Range is from 4 to 223.

Chapter 4 IntelRCSetup

Introduction

The IntelRCSetup menu contains configuration options concerning the Platform Controller Hub or PCH.

CAUTION: The options contained in the following menus can adversely affect system performance and stability. Proceed only if you are understand the ramifications of modifying a particular setting.



Processor Configuration

Key	Description
►Per-Socket Configuration	Allows Configuration of processor options on a per-socket basis.
	►CPU Socket 0 Configuration
	Cores Enabled: **0** – This is the number of cores in the processor to enable. A value of '0' enables all cores. The BIOS also provides a count of how many cores are available in the specific processor.
	IOT Configuration [bo Bitmap (hex): **0** – Each bit enables IOT/OCLA for a CBo.
	►CPU Socket 1 Configuration
	Cores Enabled: **0** – This is the number of cores in the processor to enable. A value of '0' enables all cores. The BIOS also provides a count of how many cores are available in the specific processor.
	IOT Configuration [bo Bitmap (hex): **0** – Each bit enables IOT/OCLA for a CBo.
Static Information on Installed Processors* **NOTE:** These figures for reference only. Exact system configuration information will vary.	Processor Socket | Socket 0 | Socket 1 Processor ID | 00306F2* | 00306F2 Processor Frequency | 2.400GHz | 2.400GHz Processor Max Ratio | 18H | 18H Processor Minimum Ratio | 0CH | 0CH Microcode Revision | 0000002E | 0000002E L1 Cache | 384KB | 384KB L2 Cache | 1536KB | 1536KB L3 Cache | 15360KB | 15360KB Processor 0 Version | Intel ® Xeon ® CPU E5 -2620 v3 @ 2.40GHz Processor 1 Version | Intel ® Xeon ® CPU E5 -2620 v3 @ 2.40GHz
Hyperthreading (All)	**Enabled**/Disabled – Enables or disables Intel Hyperthreading technology.
Execute Disable Bit	**Enabled**/Disabled – When disabled, forces the XD feature flag to always return '0'.
Enable Intel TXT Support	**Disabled**/Enabled – Enables or Disables Intel Trusted Execution Technology. Confirm ev dfx features are disabled if enabling this setting.
VMX	**Enabled**/Disabled – Enables or disables Vanderpool technology. Takes effect after reboot.
Enable SMX	**Disabled**/Enabled – Enables Safer Mode Extensions
MSR Lock Control	**Enabled**/Disabled – When enabled, msr3ah, msr0E2h and csr80h will lock. A power-good reset is needed to remove the lock bits.
Lock Chipset	**Enabled**/Disabled – When enabled, chipset lock is in place.
PPIn Control	**Unlocked/Enable** / Unlock/Disable – Unlocks and enables/disables the PPIn control.
Debug Interface	**Disabled**/Enabled – msr 0C80h bit 0, when set enables debug features.

Hardware Prefetcher	**Enabled**/Disabled – MLC Streamer Prefetcher enable/disable (msr 1A4h bit 0)
Adjacent Cache Prefetch	**Enabled**/Disabled – MLC Spatial Prefetch enable/disable (msr 1A4h bit 1)
DCU Streamer Prefetcher	**Enabled**/Disabled – Level 1 data cache prefetcher enable/disable. (msr 1A4h bit 2)
DCU IP Prefetcher	**Enabled**/Disabled – Level 1 data cache prefetcher enable/disable (msr 1A4h bit 3)
DCU Mode	**32kb 8-way without ECC**/16kb 4-way with ECC – msr31h bit 0 A write of '1' selects the DCU mode as 16kb 4-way with ECC.
Direct Cache Access (DCA)	**Auto**/Enable/Disable – Enables, disables or allows BIOS to select Direct Cache Access modes.
DCA Prefetch Delay	**32**/Disable/8/16/24/32/40/48/56/64/72/80/88/96//104/112 – DCA prefetch delay helper select.
X2APIC	**Disable**/Enable – Enables or disables extended APIC support.
AES-NI	**Enabled**/Disabled – Enables or disables AES-NI support.
Downstream PECI	**Disabled**/Enabled – Enables downstream PECI writes.
IIO LLSC Ways 19:0 (Hex)	**0** – msrCB0_SLICE0_CR_IIO_LLC_WAYS bitmask select.
QLRU Config 63:32 (hex)	**0** – virtual_msr_cr_QLRU_config bitmask select.
QLRU Config 31:0	**0** – virtual_msr_cr_QLRU_config bitmask select.
SMM Save State	**Disable**/Enable – System Management Mode Save State support select.
Targeted SMI	**Disable**/Enable – System Management Interrupt support select.

IIO Configuration

The following settings provide for PCIe Gen3 expansion slot link training configuration. In general, the factory default settings should be sufficient, however, if specific PCIe configuration parameters are required, these settings should be reviewed and reconfigured, as necessary.

CAUTION: The options contained in the following menus can adversely affect system performance and stability. Proceed only if you are understand the ramifications of modifying a particular setting.

Key	Description
PCIe Train by BIOS	**Yes** – Factory setting, cannot be altered
PCIe Hot Plug	**Disable**/Enable/Auto/Manual – Enables or disables PCIe hot-plug capability globally.
PCIe ACHI Hot Plug	**Disable**/Enable/Per-Port – Use in conjunction with 'PCIe Hot Plug' settings to allow or disallow hot plugging. May control which specific ports may hot-plug. When set to 'disable' msi is generated upon a HP event. When set to 'enable,' _HPGPE message is generated.
EVDfx Features	**Disable**/Enable – Set this option to allow Dfx lock bits to remain clear.
►IIO 0 Configuration	
	IOU2 (IIO PCIe Port 1): **x8**/x4x4/Auto – Selects PCIe port bifurcation for selected slots
	IOU0 (IIO PCIe Port 2): **x16**/x4x4x4x4/x4x4x8/x8x4x4/x8x8/Auto – Selects bifuction for selected slots.
	IOU1 (IIO PCIe Port 3): **x16**/x4x4x4x4/x4x4x8/x8x4x4/x8x8/Auto – Selects bifuction for selected slots.
	No PCIe Port Active ECO: **PCU Squelch Exit Ignore Option**/Reset the SQ FLOP by CSR Option – Workaround settings for when no PCIe ports are active.
	►Socket 0 PCIe D00 F0 Port 01DMI
	Link Speed: **Auto**/Gen1 (2/5GT/s)/Gen2 (5GT/s) – Link speed override.
	PCIe Port De-Emphasis: **-6.0dB**/-3.5dB – De-emphasis control (lnkcon2 [6] for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.

	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	►Socket 0 PCIe D01F0 Port 1A
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable or not.
	PCIe Port Link: **Enable/**Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event. When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.

	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.
	►Socket 0 PCIe D02F0 Port 2A
	Link Speed: **Auto**/Gen1 (2/5GT/s)/Gen2 (5GT/s) – Link speed override.
	PCIe Port De-Emphasis: **-6.0dB**/-3.5dB – De-emphasis control (lnkcon2 [6] for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	►Socket 0 PCIe D01F0 Port 1A
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable or not.
	PCIe Port Link: **Enable/**Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO

	core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event. When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.
	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.
	►Socket 0 PCIe D03F0 Port 3a
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable or not.
	PCIe Port Link: **Enable/**Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition

	from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event. When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.
	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.
►IIO 1 Configuration	
	IOU2 (IIO PCIe Port 1): **x8**/x4x4/Auto – Selects PCIe port bifurcation for selected slots
	IOU0 (IIO PCIe Port 2): **x16**/x4x4x4x4/x4x4x8/x8x4x4/x8x8/Auto – Selects bifurcation for selected slots.
	IOU1 (IIO PCIe Port 3): **x16**/x4x4x4x4/x4x4x8/x8x4x4/x8x8/Auto – Selects bifurcation for selected slots.
	No PCIe Port Active ECO: **PCU Squelch Exit Ignore Option**/Reset the SQ FLOP by CSR Option – Workaround settings for when no PCIe ports are active.
	►Socket 0 PCIe D00 F0 Port 01DMI
	Link Speed: **Auto**/Gen1 (2/5GT/s)/Gen2 (5GT/s) – Link speed override.
	PCIe Port De-Emphasis: **-6.0dB**/-3.5dB – De-emphasis control (lnkcon2 [6] for this

	port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	►Socket 0 PCIe D01F0 Port 1A
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable or not.
	PCIe Port Link: **Enable/**Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event.

	When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.
	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.
	►Socket 0 PCIe D02F0 Port 2A
	Link Speed: **Auto**/Gen1 (2/5GT/s)/Gen2 (5GT/s) – Link speed override.
	PCIe Port De-Emphasis: **-6.0dB**/-3.5dB – De-emphasis control (lnkcon2 [6] for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	►Socket 0 PCIe D01F0 Port 1A
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable

	or not.
	PCIe Port Link: **Enable**/Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event. When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.
	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.
	►Socket 0 PCIe D03F0 Port 3a
	PCIe Port: **Auto**/Enable/Disable – In 'auto' mode, the bios will remove the expansion port if there is no device and the device is not hot plug capable. 'Disable' is used to

	disable the port and hide its CFG space.
	Hot plug capable: **Disable**/Enable – This option specifies if the link is hot-plug capable or not.
	PCIe Port Link: **Enable/**Disable – This option disables the link so no training occurs but the CFG space is still active.
	Link Speed: **Auto**/Gen1 (2.5GT/s)/Gen2 (5.0GT/s)/Gen3 (8GT/s) – This option specifies the link speed for the port.
	PCIe Port Deemphasis: **-6.0dB**/-3.5dB – Deemphasis control for this port.
	PCIe Port Los Exit Latency:**4uS-8uS** - The length of time the port requires to transition from LoS to LO. (This is a factory setting and cannot be modified.)
	PCIe Port L1 Exit Latency: **8uS-16uS**/<1uS/1uS-2uS/2uS-4uS/4uS-8uS/8uS-16uS/16uS-32uS/32uS-64uS/>64uS – The length of time the port requires to transition from L1 to L0.
	Fatal Error Over: **Disabled**/Enabled – Enables forcing fatal error propagation to the IIO core error logic for this port.
	Not Fatal Error Over: **Disabled**/Enabled – Enables forcing non-fatal error propagation to the IIO core error logic for this port.
	Corr Err Over: **Disabled**/Enabled – Enables forcing correctable error propagation to the IIO core error logic for this port.
	LOs Support: **Disabled**/Enabled – When disabled, IIO never puts its transmitter in LOs state.
	PM ACPI Mode: **Disabled**/Enabled – When disabled, msi is generated upon PM event. When enabled, _HPGE message is generated.
	Gen 3 Eq Mode: **Auto**/Enable Phase 0,1,2,3/Disable Phase 0,1,2,3/Enable Phase 1 Only/Enable Phase 0,1 Only/Advanced/Enable MMM Offset West – PCIe Gen3 adaptive equalization mode.
	Gen 3 Spec Mode: **Auto**/0.70 July/0.70 September/0.71 September – PCIe Gen3 spec mode.
	Gen 3 Phase 2 Mode: **Hardware Adaptive**/Manual – PCIe gen3 phase 2 mode setting.
	Gen 3 DN Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe downstream Tx preset.
	Gen3 DN Rx Preset Hint: **Auto**/P0 (-6.0dB)/P1 (-7.0dB)/P2 (-8.0dB)/P3 (-2.5dB)/P4 (-10dB)/P5 (-11dB)/P6 (-12dB) – PCIe Gen3 downstream RX hint.
	Gen3 UP Tx Preset: **Auto**/P0 (-6.0/0.0dB)/P1 (-3.5/0.0dB)/P2 (4.5/0.0dB)/P3 (-2.5/0.0dB)/P4 (0.0/0.0dB)/P5 (0.0/2.0dB)/P6 (0.0/2.5dB)/P6 (0.0/2.5dB)/P7 (-6.0/3.5dB)/P8 (-3.5/3.5dB)/P9 (0.0/3.5dB) – PCIe Gen3 upstream Tx preset.
	Hide Port: **No**/Yes – User can force hide the root of this port from the operating system.

►IOAT Configuration	Enable IOAT: **Disable**/Enable – Enables or disables IOAT.
	No Snoop: **Disable**/Enable – No snoop enable/disable for each CB device.
	Disable TPH: **Enable**/Disable – TLP processing hint disable.
	Relaxed Ordering: **Disable**/Enable – Enable or disable relaxed ordering.
►IIO General Configuration	TXT DPR memory setting: **3m DPR**/1m DPR/64m DPR/ 128m DPR/ 255m DPR – Allows selection of the TXT DPR size in the system.
	IIO IOAPIC 0: **Enable**/Disable – Enables or disables the IIOIOAPIC.
	IIO IOAPIC 1: **Enable**/Disable – Enables or disables the IIOIOAPIC.
►Intel VT for Directed I/O (VT-d)	VTd Azalea VCp Optimizations: **Disabled**/Enabled – Enables or disables VCp optimizations.
	Intel VT for Directed I/O (VT-d): **Enable**/Disable – Enables or disables VT-d.
	Interrupt Remapping: **Enable**/Disable – Enables or disables interrupt remapping.
	Coherency Support (non-Isoch): **Enable**/Disable – Enables or disables coherency support.
	Coherency Support (Isoch): **Enable**/Disable – Enables or disables coherency support.
►TX EQ WA	**Enable**/Disable – When enabled, uses a special table for TX_EQ and vendor specific cards.
►DMI VCL Control	DMI Vcl Control: **Disable**/Enable – Enables or disables DMI Vcl Control.
	DMI Vcp Control: **Disable**/Enable – Enables or disables DMI Vcp control.
	DMI Vcm Control: **Disable**/Enable – Enables or disables DMI Vcm control.
VCO No-Snoop Configuration	**Disabled**/Enabled – Enables no-snoop on reads and writes for VcO traffic.
Gen3 Phase 3 Loop Count	**16**/1/4/16/256
Skip Halt on DMI Degradation	**Disabled**/Enabled – Enable to avoid the system halting upon DMI width/link degradation.
Power Down Unused Ports	**Disable Unused Ports (No IIO Clock Gating)**/Disable – Enables or disables unused port power down.
Rx Clock Wa	**Disable**/Enable – Enables or disables Rx Clock Wa
PCIe ASPM Support (Global)	**L1 Only**/Disable – Enables or disables ASPM support for all downstream devices.
PCIe Stop and Scream Support	**Disable**/Enable – Enables or disables PCIe Stop and Scream support.
Snoop Response Hold Off	**6** – Sets snoop response hold-off value.

PCH Configuration

Option	Description
►PCH sSATA Configuration	sSATA Controller: **Enabled**/Disabled – Enables or disables the sSATA controller.
	Configure sSATA as: **ACHI**/IDE/RAID – Selects the bus mode for sSATA.
	SATA Test Mode: **Disable**/Enable – Enables or disables SATA test mode for sSATA.
►SATA Mode Options	SATA HDD Unlock: **Enabled**/Disabled – If enabled, SATA HDD password unlock functionality is enabled in operating system.
	SATA LED Locate: **Enabled**/Disabled – If enabled, LED/SGPIO hardware is attached.
	Support Aggressive Link Power Management: **Enabled**/Disabled – Enables or disables ALPM.
►sSATA Port 0	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	sSATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►sSATA Port 1	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	sSATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►sSATA Port 2	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	sSATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►sSATA Port 3	**Information about device attached to this port appears here.**

	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	sSATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►PCH SATA Configuration	SATA Controller: **Enabled**/Disabled – Enables or disables the SATA controller.
	Configure SATA as: **ACHI**/IDE/RAID – Selects the bus mode for SATA.
	SATA Test Mode: **Disable**/Enable – Enables or disables SATA test mode for SATA.
►SATA Mode Options	SATA HDD Unlock: **Enabled**/Disabled – If enabled, SATA HDD password unlock functionality is enabled in operating system.
	SATA LED Locate: **Enabled**/Disabled – If enabled, LED/SGPIO hardware is attached.
	Support Aggressive Link Power Management: **Enabled**/Disabled – Enables or disables ALPM.
►SATA Port 0	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	SATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►SATA Port 1	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	SATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►SATA Port 2	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all

	drives spin up at boot.
	SATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►SATA Port 3	**Information about device attached to this port appears here.**
	Port 0: **Enabled**/Disabled – Enables or disables transmission for this port.
	Hot Plug: **Disabled**/Enabled – Designates hot-plug capability for this port.
	Spin Up Device: **Disabled**/Enabled – If enabled for any port, staggered spin-up will be performed and only drives with this option enabled will spin up at boot. Otherwise, all drives spin up at boot.
	SATA Device Type: **Hard Disk Drive**/Solid State Drive – Identifies what kind of device is attached to the port.
►Security Configuration	BIOS Lock: **Disabled**/Enabled – Enables or disables PCH BIOS lock feature.

Server Management Engine Configuration

Option	Description
Altitude –	**80000000** – The system location above sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide 80000000 if the altitude is unknown.
MCTP Bus Owner	**0** – The MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2,0] function. If all zeroes, sending bus owner is disabled.

Runtime Error Logging

Option	Description
System Errors	**Disable**/Enable – Enables or disables system error logging.
Mcbank error injection support	**Disabled**/Enable – When enabled, software error injection is supported by unlocking msr 0x790
Clear Mcbank errors	**Disabled**/Enable – Clears mcbank errors on warm reset
System Poison	**Disabled**/Enable – Enables or disables core, uncore and IIO poison.
IIO Error Enable	**No**/Yes – Enables or disables IIO error reporting.
PCH Error Enable	**No**/Yes – Enables or disables PCH error logging.
EMCA Logging Support	**Disable**/Enable – Enables or disables EMCA logging support.
Ignore OS EMCA Opt-In	**Disable**/Enable – Enables or disables EMCA logging requests from the operating system.

EMCA CMCI-SMI Morphing	**Disable**/Enable – Enables or disables EMCA CMCI-SMI support
►WHEA Settings	WHEA Support: **Disable**/Enable – Enables or disables WHEA support.
►QPI Error Enabling	SMI API Lane Failover: **Disable**/Enable – Enables or disables SMI when clock/data failover is set.
►Memory Error Enabling	►Memory Corrected Error Enabling: **Disabled**/Enabled – Enables or disables memory corrected errors.
	Spare Interrupt: **CMCI**/SMI/Error Pin – Select spare interrupt type.
	Mirror Failover SMI: **CMCI**/SMI – Enables or disables mirror failover generation.
►PCI/PCI Error Enabling	PCI-EX Error Enable: **No**/Yes – Enables or disables PCI-EX error reporting.
	Enable SERR Propagation: **No**/Yes – Enables or disables SERR.
	Enable PERR Propagation: **No/**Yes – Enables or disables PERR.

Miscellaneous Configuration

Option	**Description**
Target VGA	Static Information Screen. Displays information about the current display configuration.
Active Video	**Offboard**/Onboard – Selects which graphics adapter will be default. Offboard selects an external PCIe option card, onboard selects the onboard Intel HD Graphics.

Chapter 5 Security

Two Levels of Password Protection

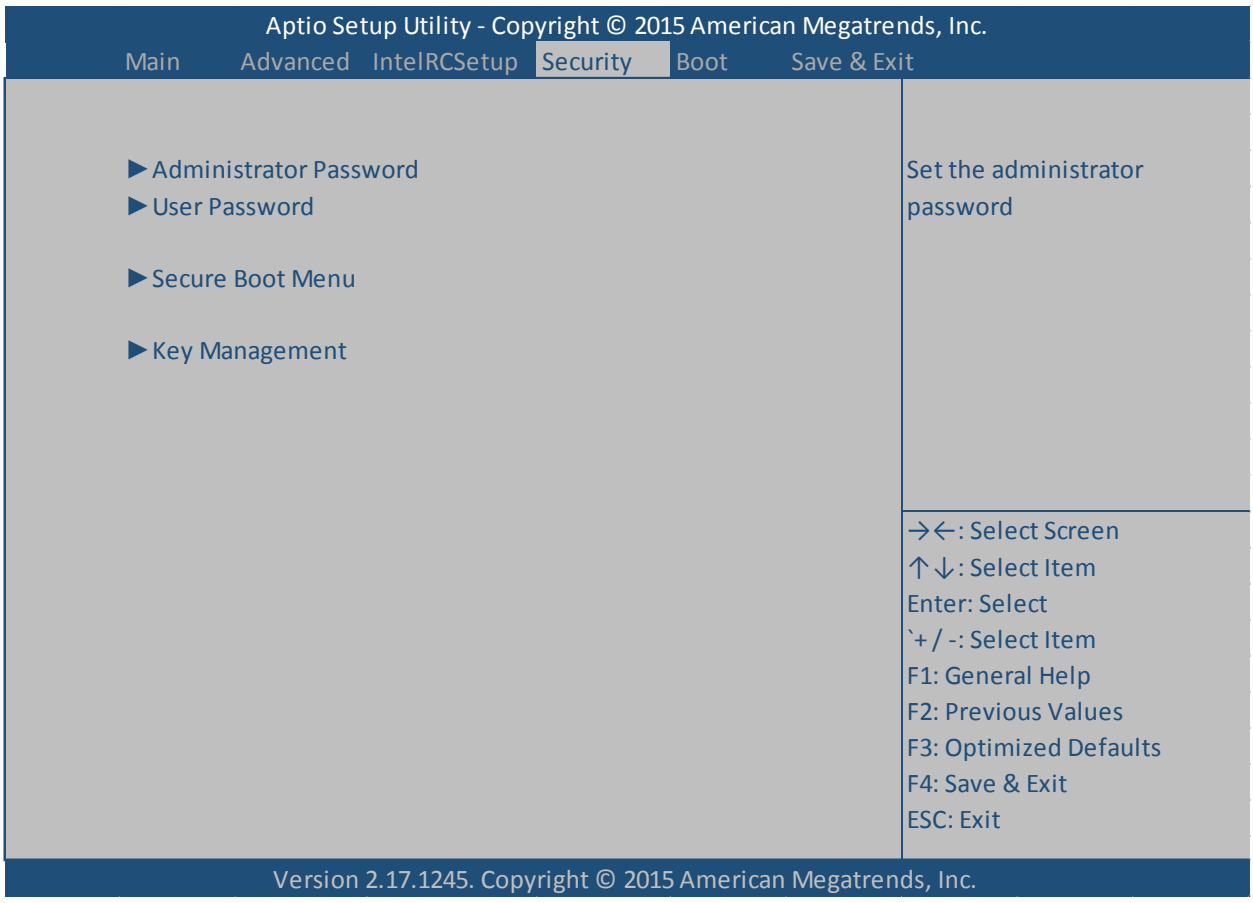
Security Setup provides both an Administrator and User password. If you use both passwords, the Administrator password must be set first.

The system can be configured so that all users must enter a password every time the system boots or when Setup is executed, using either or either the Supervisor password or User password.

The Administrator and User passwords activate two different levels of password security. If you select password support, you are prompted for a one to six character password. Type the password on the keyboard. The password does not appear on the screen when typed. Make sure you write it down. If you forget it, you must drain NVRAM and reconfigure.

Remember the Password

Keep a record of the new password when the password is changed. If you forget the password, you must erase the system configuration information in NVRAM.



Security Configuration

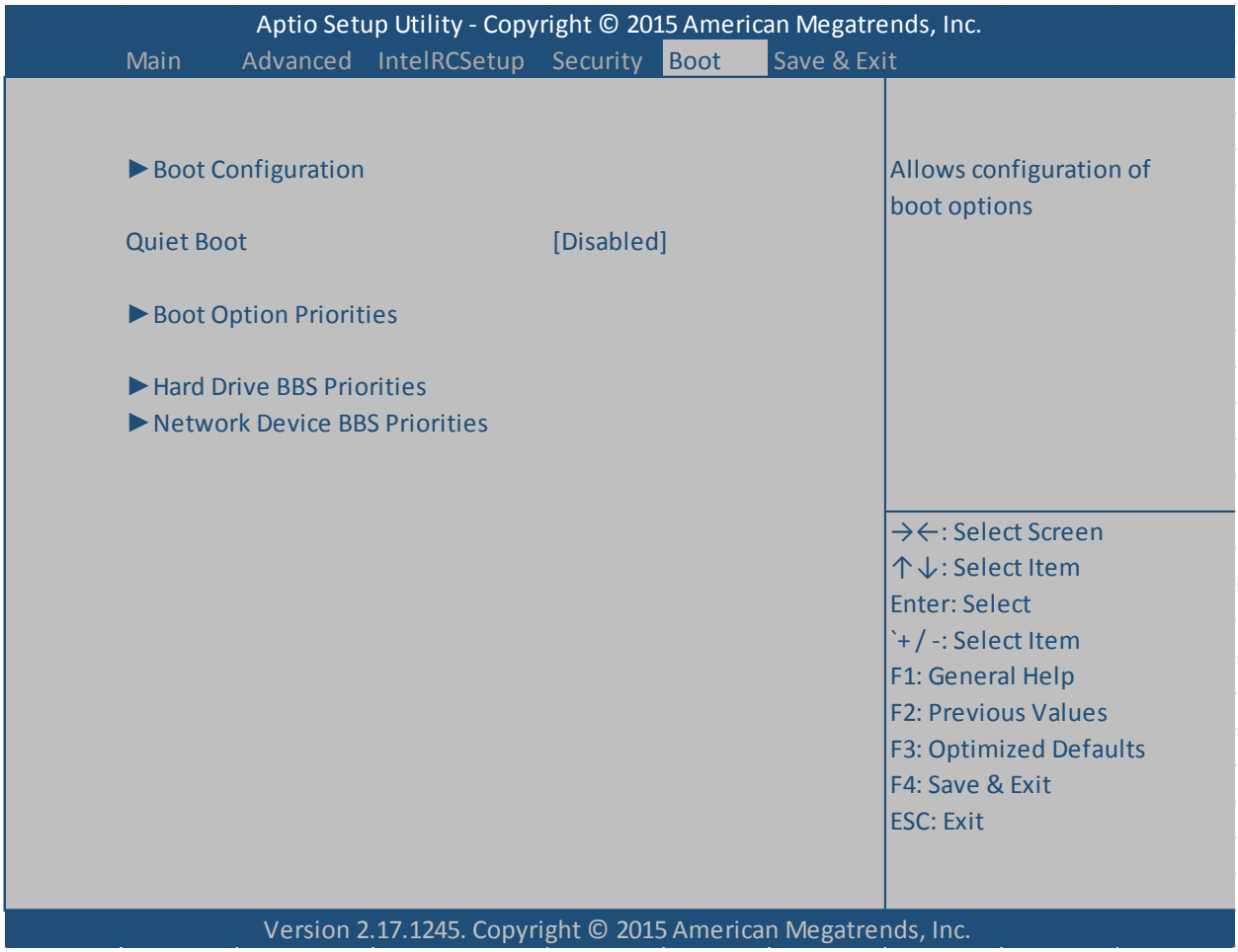
The *Security* setup menu item allows the user to do the following:

Option	Description
Administrator Password	This option allows the user to set an administrative level password for the BIOS. BIOS access passwords must be between 3 and 20 characters in length.
User Password	This option allows the user to set a user level password for the BIOS.
►Secure Boot Menu	Inside the Secure Boot Menu is the Secure Boot setting. By default it is **Disabled. -** Secure Boot may be enabled if: 1: the system is running in user mode with enrolled platform key (PK). 2: CSM function is disabled.
	Secure Boot Mode: **Custom**/Standard – Secure boot mode selector. 'Custom' enables users to change the image execution policy and manage secure boot keys.
►Key Management	Enables experienced users to modify secure boot variables.
	Default Key Provision: **Disabled**/Enabled – Allows users to install factory default secure boot keys when system is in setup mode.
	Enroll All Factory Default Keys: **No**/Yes – Forces system into user mode and installs all factory default keys. (PK, KEK, DB, DBT, DBX) Changes take effect after reboot.
	Save All Secure Boot Variables: **No**/Yes – Saves all settings for the above menus.
Platform Key	**Not Installed**/Installed – This is a static information line and cannot be directly altered.
	Delete PK: **No**/Yes – Allows the user to delete installed platform keys. Requires the personal portion of the key.
	Set New PK – Opens a new window. Press 'Yes' to load PK from factory defaults or 'No' to load from a file. If you choose neither of these options and press <ESC> the system will return a message of 'No valid file system available.' Valid file nomenclatures for loading from a file are a) efi_signature_list b) efi_cert_x509 (der encoded) c) efi_cert_rsa2048 (bin) d) efi_cert_sha256 (bin) e) efi time-based authenticated table

Chapter 6 Boot Setup

Introduction

Select the *Boot* menu item from the Aptio TSE screen to enter the setup screen. The Boot menu option allows you to access the following the following boot setup features.



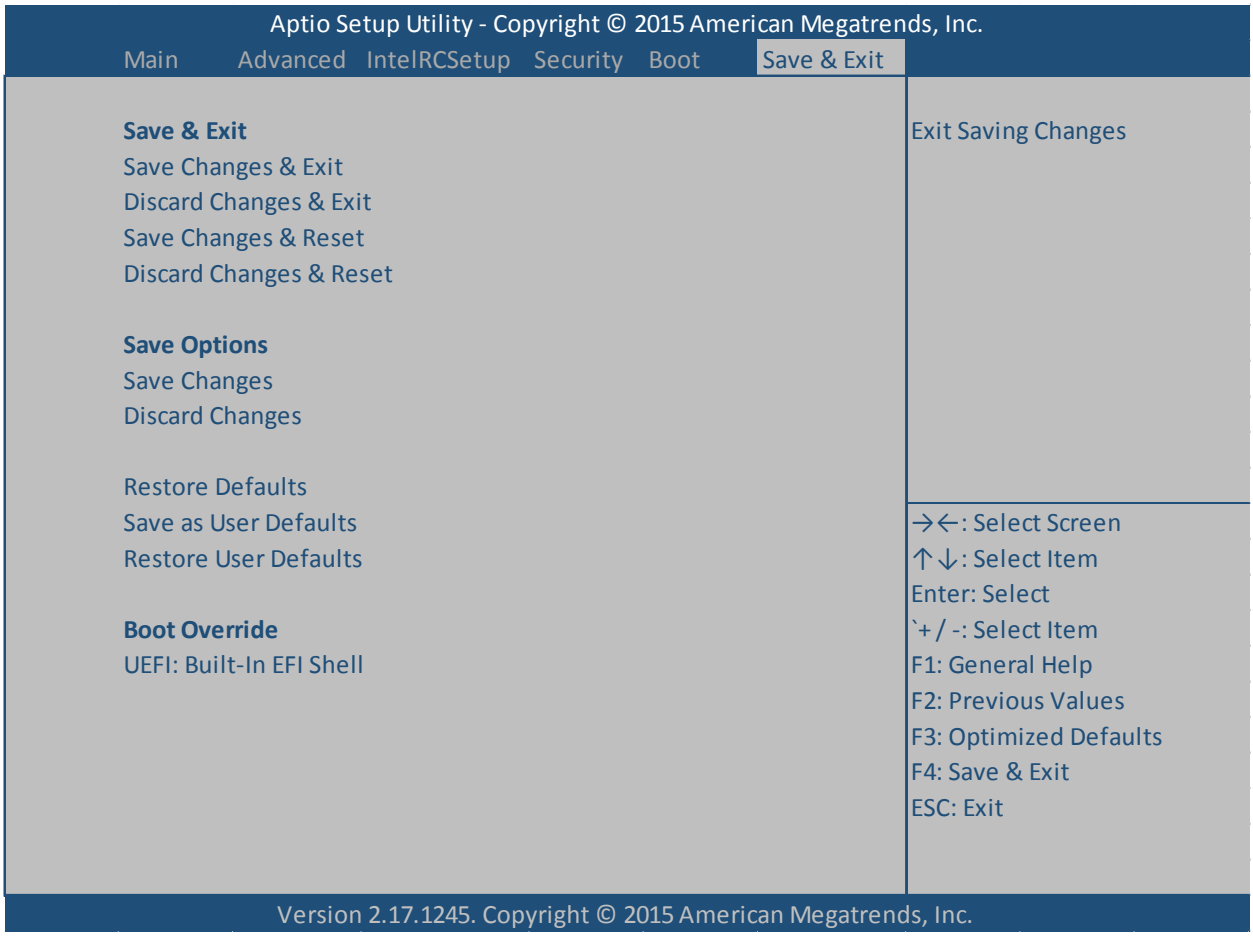
Boot Configuration

Option	Description
Setup Prompt Timeout	1 **(bold** = default setting) A numeric value of 1 is the default setting with a range of 1 to 65355 entered is in seconds being valid inputs. A value of 65355 or FFFFh means an indefinite wait period
Bootup NumLock State	The default setting is ***On*** with an option to turn the setting *Off*. The *On* setting enables the numpad to automatically enable at system boot and allows the immediate use of the 10-key numeric keypad located on the right side of the keyboard. In the Off setting, the NumLock keyboard key will need to be pressed to use the 10-key numeric pad.
Quiet Boot	**Disabled**/Enabled
Boot Option Priorities	Boot Option #1: **P4:ST3160316AS** (UEFI: Built-In EFI Shell, **P4:ST3160316AS**, Disabled) Boot Option #2: **UEFI: Built-In EFI Shell** (**UEFI: Built-In EFI Shell**, P4:ST3160316AS, Disabled) Boot Option #3: **Disabled** (UEFI: Built-In EFI Shell, P4:ST3160316AS, **Disabled**) Boot Option #4: **Disabled** (UEFI: Built-In EFI Shell, P4:ST3160316AS, **Disabled**) Note: ST3160316AS is the boot drive identifier in this particular test lab set-up. Your particular boot drive identifier will be different.
►Hard Drive BBS Priorities	Sets the boot priority of the physical drives attached to the system, either SATA or USB. Boot Option #1 P4:ST3160316AS Note: The boot options listed here are particular to this test lab setup. Your particular identifiers will be different. Note: Additional boot options will propagate in this menu if additional SATA or USB devices are attached to the SHB.
►Network Device BBS Priorities	Sets the boot priority of the PXEs of the different network interfaces. Boot Option #1 IBA GE Slot 00C8 v1562 Boot Option #2 IBA GE Slot 0400 v1561 Boot Option #3 IBA XE Slot 0700 v2330 Boot Option #4 IBA XE Slot 0700 v2330 Note: The boot options listed here are particular to this test lab setup. Your particular identifiers will be different.

Chapter 7 Save & Exit

Introduction

There are four methods of saving BIOS changes and leaving Aptio TSE: Save & Exit, Discard & Exit, Save & Reset and Discard and Reset.



Save Changes & Exit

When you have completed the system configuration changes, select this option to save your BIOS changes and leave Aptio TSE. You will need to reboot the computer for the new system configuration parameters to take effect.

Select Save Changes & Exit from the Exit menu and press <Enter>.

Save Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to save changes and exit.

Discard Changes & Exit

Select this option to quit Aptio TSE without making any permanent changes to the system configuration.

Select Discard Changes & Exit from the Exit menu and press <Enter>.

Discard Changes and Exit Setup Now?

[YES] [NO] Select *YES* to discard changes and exit.

Save Changes & Reset

When you have completed the system configuration changes, select this option to save the BIOS changes, leave Aptio TSE and reset the computer so the new system configuration parameters can take effect.

Select Save Changes & Reset from the Exit menu and press <Enter>.

Save Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to save changes and reset.

Discard Changes & Reset

Choose this option if you decide to discard your BIOS changes, but what to reset the system upon leaving Aptio TSE.

Select Discard Changes & Reset from the Exit menu and press <Enter>.

Discard Configuration Changes and Exit Now?

[YES] [NO] appears in the window. Select *YES* to discard changes and reset.

Save Options

The following two screen options allow save or discard BIOS changes without leaving Aptio TSE:

Save Changes [YES] [NO]

Discard Changes [YES] [NO]

The following menu options for BIOS defaults are available:

Restore Defaults

Aptio TSE automatically sets all Aptio TSE options to a complete set of factory default settings when you select this option.

Select restore defaults from the Exit menu and press <Enter>.

Restore Defaults?

[YES] [NO] appears in the window. Select *YES* to load restore defaults.

Save as User Defaults

With this option the BIOS changes done so far by the user are saved as User Defaults.

Select save as user defaults from the Exit menu and press <Enter>.

Save as User Defaults?

[YES] [NO] appears in the window. Select *YES* to save user defaults.

Restore User Defaults

Aptio TSE automatically sets all Aptio TSE options to a complete set of user default settings when you select this option.

Select restore user defaults from the Exit menu and press <Enter>.

Restore User Defaults?

[YES] [NO] appears in the window. Select *YES* to load restore user defaults.

Boot Override

Select this option to allow a system boot override from either a specific device connected to the SHB or from the BIOS' EFI Shell. A sample board configuration yields the following boot override selections:

UEFI: Built-In EFI Shell

P4: ST3160316AS (system configuration dependent)

Appendix A Aptio V BIOS Messages

Introduction

A status code is a data value used to indicate progress during the boot phase. These codes are output to I/O port 80h on the SHB. Aptio 5.x core outputs checkpoints throughout the boot process to indicate the task the system is currently executing. Status codes are very useful in aiding software developers or technicians in debugging problems that occur during the pre-boot process.

Aptio Boot Flow

While performing the functions of the traditional BIOS, Aptio 5.x core follows the firmware model described by the Intel Platform Innovation Framework for EFI ("the Framework"). The Framework refers the following "boot phases", which may apply to various status code descriptions:

- Security (SEC) – initial low-level initialization
- Pre-EFI Initialization (PEI) – memory initialization
- Driver Execution Environment (DXE) – main hardware initialization
- Boot Device Selection (BDS) – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, HDD, USB, Network, Shell, …)

1 Analogous to "bootblock" functionality of legacy BIOS
2 Analogous to "POST" functionality in legacy BIOS

BIOS Beep Codes

The Pre-EFI Initialization (PEI) and Driver Execution Environment (DXE) phases of the Aptio BIOS use audible beeps to indicate error codes. The number of beeps indicates specific error conditions.

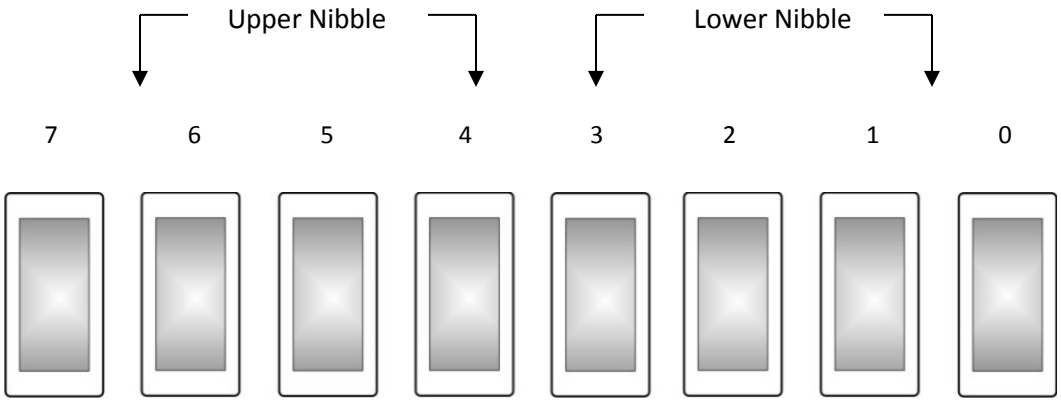
BIOS Status Codes

As the POST (Power On Self Test) routines are performed during boot-up, test codes are displayed on Port 80 POST code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LED are located on the top of the SHB, just above the board's battery socket. The POST Code LEDs and are numbered from right (position 1 = LED0) to left (position 8 – LED7). The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following chart is a key to interpreting the POST codes displayed on LEDs 0 through 7 on the HEP8225 SHBs. Refer to the board layout in the *Specifications* chapter for the exact location of the POST code LEDs.

The HEX to LED chart in the POST Code LEDs section will serve as a guide to interpreting specific BIOS status codes.

BIOS Status POST Code LEDs

As the POST (Power On Self Test) routines are performed during boot-up, test codes are displayed on Port 80 POST code LEDs 0, 1, 2, 3, 4, 5, 6 and 7. These LED are located on the top of the SHB, just above the board's battery socket. The POST Code LEDs and are numbered from right (position 1 = LED0) to left (position 8 – LED7). The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following chart is a key to interpreting the POST codes displayed on LEDs 0 through 7 on the HEP8225.



Upper Nibble (UN)				
Hex. Value	LED7	LED6	LED5	LED4
0	Off	Off	Off	Off
1	Off	Off	Off	On
2	Off	Off	On	Off
3	Off	Off	On	On
4	Off	On	Off	Off
5	Off	On	Off	On
6	Off	On	On	Off
7	Off	On	On	On
8	On	Off	Off	Off
9	On	Off	Off	On
A	On	Off	On	Off
B	On	Off	On	On
C	On	On	Off	Off
D	On	On	Off	On
E	On	On	On	Off
F	On	On	On	On

Lower Nibble (LN)				
Hex. Value	LED3	LED2	LED1	LED0
0	Off	Off	Off	Off
1	Off	Off	Off	On
2	Off	Off	On	Off
3	Off	Off	On	On
4	Off	On	Off	Off
5	Off	On	Off	On
6	Off	On	On	Off
7	Off	On	On	On
8	On	Off	Off	Off
9	On	Off	Off	On
A	On	Off	On	Off
B	On	Off	On	On
C	On	On	Off	Off
D	On	On	Off	On
E	On	On	On	Off
F	On	On	On	On

Table of BIOS Status and Beep Codes

Checkpoint Ranges

Status Code Range	Description
0x01 - 0x0B	SEC execution
0x0C - 0x0F	SEC errors
0x10 - 0x2F	PEI execution up to and including memory detection
0x30 - 0x4F	PEI execution after memory detection
0x50 - 0x5F	PEI errors
0x60 - 0x8F	DXE execution up to BDS
0x90 - 0xCF	BDS execution
0xD0 - 0xDF	DXE errors
0xE0 - 0xE8	S3 Resume (PEI)
0xE9 - 0xEF	S3 Resume Errors (PEI)
0xF0 - 0xF8	Recovery (PEI)
0xF9 - 0XFF	Recovery Errors (PEI)

Standard Checkpoints

SEC Phase

Status Code	Description
0x00	Not Used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading.
0x03	North Bridge initialization before microcode loading.
0x04	South Bridge initialization before microcode loading.
0x05	OEM initialization before microcode loading.
0x06	Microcode loading.
0x07	AP initialization after microcode loading.
0x08	North Bridge initialization after microcode loading.
0x09	South Bridge initialization after microcode loading.
0x0A	OEM initialization after microcode loading.
0x0B	Cache initialization.
SEC Error Codes	
0x0C - 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found.
0x0F	Microcode not loaded.

SEC Beep Codes

None

PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started.
0x11	Pre-memory CPU initialization is started.
0x12	Pre-memory CPU initialization (CPU module specific).
0x13	Pre-memory CPU initialization (CPU module specific).
0x14	Pre-memory CPU initialization (CPU module specific).
0x15	Pre-memory North Bridge initialization is started.
0x16	Pre-memory North Bridge initialization (North Bridge module specific.)
0x17	Pre-memory North Bridge initialization (North Bridge module specific.)
0x18	Pre-memory North Bridge initialization (North Bridge module specific.)
0x19	Pre-memory South Bridge initialization is started.
0x1A	Pre-memory South Bridge initialization (South Bridge module specific.)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific.)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific.)
0x1D - 0x2A	OEM pre-memory initialization codes.
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading.
0x2C	Memory initialization. Memory presence detection.
0x2D	Memory initialization. Programming memory timing information.
0x2E	Memory initialization. Configuring memory.
0x2F	Memory initialization. (other)
0x30	Reserved for ASL (see ASL status Codes section below)
0x31	Memory installed.
0x32	CPU post-memory initialization is started.
0x33	CPU post-memory initialization. Cache initialization.
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization.
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection.
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization.
0x37	Post-Memory North Bridge initialization is started.
0x38	Post-Memory North Bridge initialization (North Bridge Module Specific).
0x39	Post-Memory North Bridge initialization (North Bridge Module Specific).
0x3A	Post-Memory North Bridge initialization (North Bridge Module Specific).
0x3B	Post-Memory South Bridge initialization is started.
0x3C	Post-Memory South Bridge initialization (South Bridge Module Specific).
0x3D	Post-Memory South Bridge initialization (South Bridge Module Specific).
0x3E	Post-Memory South Bridge initialization (South Bridge Module Specific).

0x3F - 0x4E	OEM post memory initialization codes.
0x4F	DXE IPL is started.
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed.
0x51	Memory initialization error. SPD reading has failed.
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected.
0x54	Unspecified memory initialization error.
0x55	Memory not installed.
0x56	Invalid CPU type or speed.
0x57	CPU mismatch.
0x58	CPU self test failed or possible CPU cache error.
0x59	CPU micro-code is not found or micro-code update is failed.
0x5A	Internal CPU error.
0x5B	Reset PPI is not available
0x5C - 0x5F	Reserved for Future AMI error codes.
S3 Resume Progress Codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)>
0xE1	S3 Boot Script execution.
0xE2	Video repost.
0xE3	OS S3 wake vector call
0xE4 - 0xE7	Reserved for Future AMI error codes.
S3 Resume Error Codes	
0xE8	S3 Resume failed.
0xE9	S3 Resume PPI not found.
0x3A	S3 Resume Boot script error.
0xEB	S3 OS wake error.
0xEC - 0xEF	Reserved for Future AMI error codes.
Recovery Progress Codes	
0xF0	Recovery condition trigged by firmware (Auto recovery).
0xF1	Recovery condition triggered by user (Forced recovery).
0xF2	Recovery process started.
0xF3	Recovery firmware image is found.
0xF4	Recovery firmware image is loaded.
0xF5 - 0xF7	Reserved for Future AMI progress codes.

Recovery Error Codes	
0xF8	Recovery PPI is not available.
0xF9	Recovery capsule is not found.
0xFA	Invalid recovery capsule.
0xFB - 0xFF	Reserved for Future AMI error codes.

PEI Beep Codes

# of Beeps	Description
1	Memory not installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice).
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume Failed
7	Reset PPI is not available

DXE Phase

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started.
0x64	CPU DXE initialization is started. (CPU module specific).
0x65	CPU DXE initialization is started. (CPU module specific).
0x66	CPU DXE initialization is started. (CPU module specific).
0x67	CPU DXE initialization is started. (CPU module specific).
0x68	PCI host bridge initialization.
0x69	North Bridge DXE initialization is started.
0x6A	North Bridge DXE SMM initialization is started.
0x6B	North Bridge DXE initialization (North Bridge module specific.)
0x6C	North Bridge DXE initialization (North Bridge module specific.)
0x6D	North Bridge DXE initialization (North Bridge module specific.)
0x6E	North Bridge DXE initialization (North Bridge module specific.)
0x6F	North Bridge DXE initialization (North Bridge module specific.)
0x70	South Bridge DXE initialization is started.
0x71	South Bridge DXE SMM initialization is started.
0x72	South Bridge devices initialization.
0x73	South Bridge DXE initialization (South Bridge module specific.)
0x74	South Bridge DXE initialization (South Bridge module specific.)

0x75	South Bridge DXE initialization (South Bridge module specific.)
0x76	South Bridge DXE initialization (South Bridge module specific.)
0x77	South Bridge DXE initialization (South Bridge module specific.)
0x78	ACPI module initialization.
0x79	CSM initialization.
0x7A - 0x7F	Reserved for future AMI DXE codes
0x80 - 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started.
0x91	Driver connecting is started.
0x92	PCI Bus initialization is started.
0x93	PCI Bus Hot Plug Controller Initialization.
0x94	PCI Bus Enumeration.
0x95	PCI Bus Request Resources.
0x96	PCI Bus Assign Resources.
0x97	Console Output devices connect.
0x98	Console input devices connect.
0x99	Super IO initialization.
0x9A	USB initialization is started.
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E - 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready to Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP begin
0xB1	Runtime Set Virtual Address MAP end
0xB2	Legacy Option Rom Initialization

0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM setting)
0xB8 - 0xBF	Reserved for future AMI codes
0xC0 - 0xCF	OEM BDS initialization codes

DXE Error Codes

0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources.
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset Protocol is not available

DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

ACPI/ASL Checkpoints

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

OEM-Reserved Checkpoint Ranges

Status Code	Description
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D - 0x2A	OEM pre-memory initialization codes
0x3F - 0x4E	OEM PEI post memory initialization codes
0x80 - 0x8F	OEM DXE initialization codes
0xC0 - 0xCF	OEM BDS initialization codes