

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

Technical Reference Manual for the VP B1x/msd BIOS

Manual Order Number 550 8050 Rev. 01 July 2015

Concurrent Technologies Inc
400 West Cummings Park, Suite 1300

Woburn
MA 01801
United States of America

Tel: (781) 933 5900
Fax: (781) 933 5911

E-mail: info@gocct.com

Concurrent Technologies Plc
4 Gilberd Court
Newcomen Way
Colchester, Essex, CO4 9WN

United Kingdom

Tel: (+44) 1206 752626
Fax: (+44) 1206 751116

http://www.gocct.com

NOTES

Information furnished by Concurrent Technologies is believed to be accurate and reliable. However, Concurrent Technologies assumes no responsibility for any errors contained in this document and makes no commitment to update or to keep current the information contained in this document. Concurrent Technologies reserves the right to change specifications at any time without notice.

Concurrent Technologies assumes no responsibility either for the use of this document or for any infringements of the patent or other rights of third parties which may result from its use. In particular, no license is either granted or implied under any patent or patent rights belonging to Concurrent Technologies.

No part of this document may be copied or reproduced in any form or by any means without the prior written consent of Concurrent Technologies.

All companies and product names are trademarks of their respective companies.

CONVENTIONS

Throughout this manual the following conventions will apply:

- # after a name represents an active low signal, e.g. INIT#
- 0x denotes a hexadecimal number, e.g. 0xFF45
- byte represents 8-bits
- word represents 16-bits
- dword represents 32-bits

NOTATIONAL CONVENTIONS

NOTE: Notes provide general additional information.

WARNING: Warnings provide indication of board malfunction if they are not observed.

CAUTION: Cautions provide indications of board or system damage if they are not observed

Intel® and Core™ are trademarks or registered trademarks of Intel Corporation.

Windows™ is a trademark and MS-DOS and Microsoft are registered trademarks of Microsoft Corporation.

Insyde® is a registered trademark and InsydeH2O™ is a trademark of Insyde Software.

GLOSSARY OF TERMS

ACPI	Advanced Configuration and Power Interface
ANSI	American National Standards Institute
APIC	Advanced Programmable Interrupt Controller
ASPM	Active State Power Management
ATA	AT Attachment
BIOS	Basic Input Output System
BIT	Built-In Test
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSM	Compatibility Support Module
DDR	Double Data Rate
DDR3	Double Data Rate, third generation
DRAM	Dynamic Random Access Memory
DIMM	Dual Inline Memory Module
DTS	Digital Temperature Sensor
DVI	Digital Visual Interface
DVMT	Dynamic Video Memory Technology
EFI	Extensible Firmware Interface
EHCI	Enhanced Host Controller Interface
EEPROM	Electrically Erasable Programmable Read Only Memory
ETH	Ethernet
FDD	Floppy Disk Drive
FPGA	Field Programmable Gate Array
GB	Gigabyte (1024MB)
GPIO	General Purpose I/O
HDD	Hard Disk Drive
IDE	Integrated Drive Electronics
IGD	Integrated Graphics Device
I/O	Input / Output
IPS	Intelligent Power Sharing
IRQ	Interrupt Request
KB	Kilobyte (1024 bytes)
LED	Light Emitting Diode
LPC	Low Pin Count
MB	Megabyte (1024KB)
ME	Management Engine
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect
PCIe	PCI Express
PCI-X	PCI Extended
PEG	PCI Express Graphics
PMC	PCI Mezzanine Card
PME	Power Management Event
POST	Power-On Self Test
PXE	Pre-boot Execution Environment
RAID	Redundant Array of Independent Disks

RAM	Random Access Memory
ROM	Read Only Memory
RTC	Real Time Clock
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer System Interface
SMI	System Management Interrupt
SMM	System Management Mode
SODIMM	Small Outline DIMM
SSD	Solid State Drive
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VITA	VME International Trade Association (*standards organization*)
XMC	Switched Mezzanine Card

REVISION HISTORY

Revision	Summary of Changes	Date
01	First Release	July 2015

TABLE OF CONTENTS

1 Introduction 1-1

1.1 Intended Audience 1-1

1.2 What Does This Manual Cover? 1-2

1.3 What Is Not Covered by This Manual 1-3

1.4 Additional Reference Material 1-4

1.5 BIOS Version 1-5

2 What is the BIOS 2-1

2.1 UEFI a BIOS for the 21st Century 2-1

3 VP B1x/msd Block Diagram 3-1

3.1 Hardware Block Diagram 3-1

4 Changing and Saving BIOS Settings 4-1

4.1 What are Optimal and Custom Defaults? 4-1

4.2 When Do My Settings Get Loaded? 4-2

4.3 Forcibly Loading Optimal Defaults 4-3

5 Setup Menus 5-1

5.1 Setup Menu Typographic Conventions 5-1

5.2 Entering Setup and Navigating the Setup Menus 5-2

5.3 Exiting Setup 5-3

5.3.1 Exit Saving Changes 5-3
5.3.2 Exit Discarding Changes 5-4

5.4 Loading Optimal Defaults 5-5

5.5 The Boot Manager 5-6

5.6 Main 5-7

5.6.1 Main | BIOS Version 5-7
5.6.2 Main | Processor Type 5-7
5.6.3 Main | System Bus Speed 5-8
5.6.4 Main | System Memory Speed 5-8
5.6.5 Main | CPU Microcode Revision 5-8
5.6.6 Main | Cache RAM 5-8
5.6.7 Main | Total Memory 5-9
5.6.8 Main | DIMM 0 5-9
5.6.9 Main | DIMM 1 5-9
5.6.10 Main | Intel ME Version 5-9
5.6.11 Main | Boot Features 5-10
5.6.12 Main | Board Status 5-10
5.6.13 Main | System Time 5-10
5.6.14 Main | System Date 5-10
5.6.15 Main | Default Time and Date 5-11

5.7 Main | Boot Features 5-12

5.7.1 Main | Boot Features | Primary Display 5-12
5.7.2 Main | Boot Features | Auto-retry On Boot Fail 5-13
5.7.3 Main | Boot Features | Delay Before Boot 5-13
5.7.4 Main | Boot Features | PXE Boot 5-13
5.7.5 Main | Boot Features | Front Panel ETH A 5-14
5.7.6 Main | Boot Features | Front Panel ETH B 5-14
5.7.7 Main | Boot Features | Rear Panel ETH A 5-14
5.7.8 Main | Boot Features | Rear Panel ETH B 5-15
5.7.9 Main | Boot Features | Ethernet Mode 5-15
5.7.10 Main | Boot Features | Option ROM Load 5-15
5.7.11 Main | Boot Features | CPU Operating Frequency 5-16
5.7.12 Main | Boot Features | PCI Bus Scan Delay 5-17
5.7.13 Main | Boot Features | ACPI Shutdown 5-17
5.7.14 Main | Boot Features | MP-Table Cpu Entries 5-17

5.8 Main | Boot Features | ACPI Shutdown = LED 5-18

5.8.1 Main | Boot Features | LED Action 5-18

5.9 Main | Board Status 5-19

5.9.1 Main | Board Status | VME Slot 5-19
5.9.2 Main | Board Status | VME System Controller 5-19
5.9.3 Main | Board Status | Hardware Rev 5-20

5.10 Advanced 5-21

5.10.1 Advanced | Boot Configuration 5-21
5.10.2 Advanced | Peripheral Configuration 5-22
5.10.3 Advanced | SATA Configuration 5-22
5.10.4 Advanced | Thermal Configuration 5-22
5.10.5 Advanced | Video Configuration 5-22
5.10.6 Advanced | USB Configuration 5-22
5.10.7 Advanced | Chipset Configuration 5-22
5.10.8 Advanced | ACPI Table/Features Control 5-23
5.10.9 Advanced | PCI Express Configuration 5-23
5.10.10 Advanced | Platform Configuration 5-23
5.10.11 Advanced | Console Redirection 5-23
5.10.12 Advanced | BIOS Event Log Configuration 5-23

5.11 Advanced | Boot Configuration 5-24

5.11.1 Advanced | Boot Configuration | Numlock 5-24

5.12 Advanced | Peripheral Configuration 5-25

5.12.1 Advanced | Peripheral Configuration | Serial COMx 5-26
5.12.2 Advanced | Peripheral Configuration | Base I/O Address 5-26
5.12.3 Advanced | Peripheral Configuration | Interrupt 5-26
5.12.4 Advanced | Peripheral Configuration | Configuration 5-26
5.12.5 Advanced | Peripheral Configuration | Mode 5-27
5.12.6 Advanced | Peripheral Configuration | Slew Rate 5-27
5.12.7 Advanced | Peripheral Configuration | Azalia 5-27

5.13 Advanced | SATA Configuration | AHCI and RAID mode 5-28

5.13.1 Advanced | SATA Configuration | SATA Controller 5-29
5.13.2 Advanced | SATA Configuration | HDC Configured As 5-30
5.13.3 Advanced | SATA Configuration | Software Feature Mask Configuration 5-31

5.13.4 Advanced | SATA Configuration | Aggressive LPM Support 5-31
5.13.5 Advanced | SATA Configuration | Alternate ID 5-31
5.13.6 Advanced | SATA Configuration | SATA Port x HotPlug 5-31
5.13.7 Advanced | SATA Configuration | SATA Port x - Spin-Up Device 5-31
5.13.8 Advanced | SATA Configuration | SATA Port x - SATA Device Type 5-32
5.13.9 Advanced | SATA Configuration | Serial ATA Port x 5-32
5.13.10 Advanced | SATA Configuration | SATA Port x 5-32

5.14 Advanced | SATA Configuration | Software Feature Mask Configuration 5-33

5.14.1 Advanced | SATA Configuration | Software Feature Mask Configuration | HDD Unlock 5-33
5.14.2 Advanced | SATA Configuration | Software Feature Mask Configuration | LED Locate 5-34
5.14.3 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID0 5-34
5.14.4 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID1 5-34
5.14.5 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID10 5-34
5.14.6 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID5 5-35
5.14.7 Advanced | IDE Configuration | Software Feature Mask Configuration | Intel Rapid Recovery Technology 5-35
5.14.8 Advanced | IDE Configuration | Software Feature Mask Configuration | OPROM UI and BANNER 5-35
5.14.9 Advanced | IDE Configuration | Software Feature Mask Configuration | IRRT Only on eSATA 5-35

5.15 Advanced | SATA Configuration | Serial ATA Port x 5-36

5.15.1 Advanced | SATA Configuration | SATA Port x | Security Mode 5-36

5.16 Advanced | SATA Configuration | IDE Mode 5-37

5.17 Advanced | Thermal Configuration 5-38

5.17.1 Advanced | Thermal Configuration | Platform Thermal Configuration 5-38
5.17.2 Advanced | Thermal Configuration | Cpu Thermal Configuration 5-39

5.18 Advanced | Thermal Configuration | Platform Thermal Configuration 5-40

5.18.1 Advanced | Thermal Configuration | Platform Thermal Configuration | Automatic Thermal Reporting 5-40
5.18.2 Advanced | Thermal Configuration | Platform Thermal Configuration | Thermal Device 5-41
5.18.3 Advanced | Thermal Configuration | Platform Thermal Configuration | Alert Enable Lock 5-41

5.19 Advanced | Thermal Configuration | Platform Thermal Configuration - Additional Options 5-42

5.19.1 Advanced | Thermal Configuration | Platform Thermal Configuration | Critical Thermal Trip Point 5-43
5.19.2 Advanced | Thermal Configuration | Platform Thermal Configuration | Passive Thermal Trip Point 5-44

5.20 Advanced | Thermal Configuration | CPU Thermal Configuration 5-45

5.20.1 Advanced | Thermal Configuration | CPU Thermal Configuration | DTS 5-46
5.20.2 Advanced | Thermal Configuration | Bi-Directional PROCHOT# 5-46
5.20.3 Advanced | Thermal Configuration | CPU Thermal Configuration | ACPI 3.0 T-States 5-47

5.21 Advanced | Video Configuration 5-48

5.21.1 Advanced | Video Configuration | Internal Graphic Device | Internal Graphics Device 5-48
5.21.2 Advanced | Video Configuration | Internal Graphic Device | RC6 (Render Standby) 5-49
5.21.3 Advanced | Video Configuration | Internal Graphic Device | Deep Render Standby 5-49
5.21.4 Advanced | Video Configuration | Internal Graphic Device | IGD – Gtt Size 5-49
5.21.5 Advanced | Video Configuration | Internal Graphic Device | IGD – Aperture Size 5-49
5.21.6 Advanced | Video Configuration | Internal Graphic Device | IGD – DVMT Pre Allocated 5-50
5.21.7 Advanced | Video Configuration | Internal Graphic Device | IGD – DVMT Size 5-50

5.22 Advanced | USB Configuration 5-51

5.22.1 Advanced | USB Configuration | USB BIOS Support 5-53
5.22.2 Advanced | USB Configuration | XHCI Pre-Boot Driver 5-53
5.22.3 Advanced | USB Configuration | XHCI 5-53

5.22.4 Advanced | USB Configuration | XHCI Streams 5-54
5.22.5 Advanced | USB Configuration | EHCI 1 5-54
5.22.6 Advanced | USB Configuration | EHCI 2 5-54
5.22.7 Advanced | USB Configuration | Per-Port Control 5-54
5.22.8 Advanced | USB Configuration | Usb Portx 5-55

5.23 Advanced | Chipset Configuration 5-56

5.23.1 Advanced | Chipset Configuration | CRID 5-57
5.23.2 Advanced | Chipset Configuration | Port 80h Cycles 5-57
5.23.3 Advanced | Chipset Configuration | VT-d 5-58
5.23.4 Advanced | Chipset Configuration | CHAP DEVICE (B0:D7:F0) 5-58
5.23.5 Advanced | Chipset Configuration | Thermal Device (B0:D4:F0) 5-58
5.23.6 Advanced | Chipset Configuration | Scrambler 5-58
5.23.7 Advanced | Chipset Configuration | Memory Frequency 5-59
5.23.8 Advanced | Chipset Configuration | Me Fw Image Re-Flash 5-59
5.23.9 Advanced | Chipset Configuration | After G3 On 5-59
5.23.10 Advanced | Chipset Configuration | Board Capability 5-60
5.23.11 Advanced | Chipset Configuration | DeepSx Power Policies 5-60
5.23.12 Advanced | Chipset Configuration | GPIO Lockdown 5-60
5.23.13 Advanced | Chipset Configuration | RTC Lock 5-60
5.23.14 Advanced | Chipset Configuration | DDR3 voltage mode 5-60
5.23.15 Advanced | Chipset Configuration | Max TOLUD 5-61
5.23.16 Advanced | Chipset Configuration | SATA PORT 0 Time Out(MS) 5-61

5.24 Advanced | ACPI Table Features Control 5-62

5.24.1 Advanced | ACPI Table Features Control | FACP - RTC S4 Wakeup 5-62
5.24.2 Advanced | ACPI Table Features Control | APIC – IO APIC Mode 5-62
5.24.3 Advanced | ACPI Table Features Control | ACPI Memory Debug 5-63
5.24.4 Advanced | ACPI Table Features Control | Native PCIE enable 5-63

5.25 Advanced | PCI Express Configuration 5-64

5.25.1 Advanced | PCI Express Configuration | Spread Spectrum 5-64
5.25.2 Advanced | PCI Express Configuration | PCIE Reset Delay 5-65
5.25.3 Advanced | PCI Express Configuration | XMC PCIe Link Speed 5-65
5.25.4 Advanced | PCI Express Configuration | PCI Express Clock Gating 5-65
5.25.5 Advanced | PCI Express Configuration | DMI Link ASPM Control 5-66
5.25.6 Advanced | PCI Express Configuration | DMI Extended Synch Control 5-66
5.25.7 Advanced | PCI Express Configuration | PCI Express Root Port x 5-66

5.26 Advanced | PCI Express Configuration | PCI Express Root Port x 5-67

5.26.1 Advanced | PCI Express Configuration | PCI Express Root Port x 5-67
5.26.2 Advanced | PCI Express Configuration | PCI Express Root Port x | Automatic ASPM 5-68
5.26.3 Advanced | PCI Express Configuration | PCI Express Root Port x | URR 5-68
5.26.4 Advanced | PCI Express Configuration | PCI Express Root Port x | FER 5-68
5.26.5 Advanced | PCI Express Configuration | PCI Express Root Port x | NFER 5-69
5.26.6 Advanced | PCI Express Configuration | PCI Express Root Port x | CER 5-69
5.26.7 Advanced | PCI Express Configuration | PCI Express Root Port x | CTO 5-69
5.26.8 Advanced | PCI Express Configuration | PCI Express Root Port x | SEFE 5-69
5.26.9 Advanced | PCI Express Configuration | PCI Express Root Port x | SENFE 5-70
5.26.10 Advanced | PCI Express Configuration | PCI Express Root Port x | SECE 5-70
5.26.11 Advanced | PCI Express Configuration | PCI Express Root Port x | PME Interrupt 5-70
5.26.12 Advanced | PCI Express Configuration | PCI Express Root Port x | PME SCI 5-70
5.26.13 Advanced | PCI Express Configuration | PCI Express Root Port x | Hot Plug 5-71
5.26.14 Advanced | PCI Express Configuration | PCI Express Root Port x | PCIe Speed 5-71

5.27 Advanced | Platform Configuration 5-72

5.27.1 Advanced | Platform Configuration | CPUID 5-72
5.27.2 Advanced | Platform Configuration | CPU Stepping 5-72
5.27.3 Advanced | Platform Configuration | Microcode Rev 5-73
5.27.4 Advanced | Platform Configuration | CPU Speed 5-73
5.27.5 Advanced | Platform Configuration | L1 Data Cache 5-73
5.27.6 Advanced | Platform Configuration | L1 Instruction Cache 5-73
5.27.7 Advanced | Platform Configuration | L2 Cache 5-73
5.27.8 Advanced | Platform Configuration | L3 Cache 5-73
5.27.9 Advanced | Platform Configuration | Number of Core 5-74
5.27.10 Advanced | Platform Configuration | Number of Thread 5-74
5.27.11 Advanced | Platform Configuration | SMX/TXT 5-74
5.27.12 Advanced | Platform Configuration | VT-d 5-74
5.27.13 Advanced | Platform Configuration | VMX 5-74
5.27.14 Advanced | Platform Configuration | PCH Rev / SKU 5-75
5.27.15 Advanced | Platform Configuration | VBIOS Ver 5-75
5.27.16 Advanced | Platform Configuration | Intel ME Version / SKU 5-75

5.28 Advanced | Console Redirection 5-76

5.28.1 Advanced | Console Redirection | Console Serial Redirect 5-76
5.28.2 Advanced | Console Redirection | Information Wait Time 5-77
5.28.3 Advanced | Console Redirection | C.R. After Post 5-77
5.28.4 Advanced | Console Redirection | Text Mode Resolution 5-77
5.28.5 Advanced | Console Redirection | Auto Refresh 5-77
5.28.6 Advanced | Console Redirection | FailSafeBaudRate 5-78
5.28.7 Advanced | Console Redirection | ACPI SPCR Table 5-78
5.28.8 Advanced | Console Redirection | COMx 5-78
5.28.1 Advanced | Console Redirection | [Port Settings Summary] 5-78

5.29 Advanced | Console Redirection | COMx 5-79

5.29.1 Advanced | Console Redirection | COMx | PortEnable 5-79
5.29.2 Advanced | Console Redirection | COMx | Terminal Type 5-80
5.29.3 Advanced | Console Redirection | COMx | Baud Rate 5-80
5.29.4 Advanced | Console Redirection | COMx | Data Bits 5-80
5.29.5 Advanced | Console Redirection | COMx | Parity 5-80
5.29.6 Advanced | Console Redirection | COMx | Stop Bits 5-81
5.29.7 Advanced | Console Redirection | COMx | Flow Control 5-81

5.30 Advanced | BIOS Event Log Configuration 5-82

5.30.1 Advanced | BIOS Event Log Configuration | Log Event To 5-82
5.30.2 Advanced | BIOS Event Log Configuration | Event Log Full option 5-83
5.30.3 Advanced | BIOS Event Log Configuration | Event Log Viewer 5-83

5.31 Advanced | BIOS Event Log Configuration | Event Log Viewer 5-84

5.31.1 Advanced | BIOS Event Log Configuration | Event Log Viewer 5-84
5.31.2 Advanced | BIOS Event Log Configuration | Event Log Viewer | BIOS Event Log Viewer 5-84
5.31.3 Advanced | BIOS Event Log Configuration | Event Log Viewer | Clear MEMORY Event Log 5-85
5.31.4 Advanced | BIOS Event Log Configuration | Event Log Viewer | Clear BIOS Event Log 5-86

5.32 Security 5-87

5.32.1 Security | TPM Status 5-87
5.32.2 Security | TPM Operation 5-88
5.32.3 Security | Supervisor Password 5-88
5.32.4 Security | Set Supervisor Password 5-89

5.32.5 Clearing the Supervisor Password 5-92
5.33 Security – Additional Options 5-93
5.33.1 Security | Power on Password 5-93
5.34 Power 5-94
5.34.1 Power | Advanced CPU Control 5-94
5.34.2 Power | Platform Power Management 5-94
5.34.3 Power | Wake-on-LAN 5-95
5.35 Power | Advanced CPU Control 5-96
5.35.1 Power | Advanced CPU Control | Hardware Prefetcher 5-98
5.35.2 Power | Advanced CPU Control | AES 5-98
5.35.3 Power | Advanced CPU Control | P-States(IST) 5-99
5.35.4 Power | Advanced CPU Control | Active Processor Cores 5-99
5.35.5 Power | Advanced CPU Control | HT Support 5-99
5.35.6 Power | Advanced CPU Control | BIST 5-99
5.35.7 Power | Advanced CPU Control | Execute Disable Bit 5-100
5.35.8 Power | Advanced CPU Control | Intel (VMX) Virtualization Technology 5-100
5.35.9 Power | Advanced CPU Control | Max CPUID Value Limit 5-100
5.35.10 Power | Advanced CPU Control | Boot Performance Mode 5-100
5.35.11 Power | Advanced CPU Control | C-States 5-101
5.35.12 Power | Advanced CPU Control | Enhanced C-States 5-101
5.35.13 Power | Advanced CPU Control | Enable C3 5-101
5.35.14 Power | Advanced CPU Control | Enable C6 5-101
5.35.15 Power | Advanced CPU Control | Max DeepCState 5-102
5.35.16 Power | Advanced CPU Control | C-State Auto Demotion 5-102
5.35.17 Power | Advanced CPU Control | C-State Auto Un-demotion 5-102
5.35.18 Power | Advanced CPU Control | Package C-State Demotion 5-103
5.35.19 Power | Advanced CPU Control | Package C-State Un-demotion 5-103
5.35.20 Power | Advanced CPU Control | ACPI 5.0 CPPC Support 5-103
5.35.21 Power | Advanced CPU Control | ACPI 5.0 CPPC Platform SCI 5-104
5.35.22 5-104
5.35.23 Power | Advanced CPU Control | Turbo Mode 5-104
5.35.24 Power | Advanced CPU Control | Config TDP Configurations 5-104
5.36 Power | Platform Power Management 5-105
5.36.1 Power | Platform Power Management | PCI Clock Run 5-105
5.37 Vme 5-106
5.37.1 Vme | Outbound Images 5-106
5.37.2 Vme | Inbound Images 5-106
5.37.3 Vme | Outbound Reserved Size 5-107
5.37.4 Vme | Inbound Reserved Size 5-107
5.37.5 Vme | VME SYSFAIL 5-108
5.37.6 Vme | VME System Reset 5-108
5.38 Vme | Outbound Images 5-109
5.38.1 Vme | Outbound Images | Image x | Enable Image 5-110
5.38.2 Vme | Outbound Images | Image x | PCI Address 5-111
5.38.3 Vme | Outbound Images | Image x | VME Address 5-111
5.38.4 Vme | Outbound Images | Image x | Image Size 5-111
5.38.5 Vme | Outbound Images | Image x | Posted Writes 5-112
5.38.6 Vme | Outbound Images | Image x | Transfer Mode 5-112

5.38.7 Vme | Outbound Images | Image x | Data bus width 5-112
5.38.8 Vme | Outbound Images | Image x | Supervisor Access 5-112
5.38.9 Vme | Outbound Images | Image x | Program Access 5-112
5.38.10 Vme | Outbound Images | Image x | Address Mode 5-113

5.39 Vme | Inbound Images 5-114

5.39.1 Vme | Inbound Images | Image x | Enable Image 5-115
5.39.2 Vme | Inbound Images | Image x | PCI Address 5-116
5.39.3 Vme | Inbound Images | Image x | VME Address 5-116
5.39.4 Vme | Inbound Images | Image x | Image Size 5-116
5.39.5 Vme | Outbound Images | Image x | Posted Writes 5-116
5.39.6 Vme | Outbound Images | Image x | Prefetching 5-117
5.39.7 Vme | Inbound Images | Image x | Address Space 5-117
5.39.8 Vme | Inbound Images | Image x | Supervisor Access 5-117
5.39.9 Vme | Inbound Images | Image x | Program Access 5-117

5.40 Boot 5-118

5.40.1 Boot | Boot Type 5-118
5.40.2 Boot | Quick Boot 5-119
5.40.3 Boot | Quiet Boot 5-119
5.40.4 Boot | Power Up In Standby Support 5-120
5.40.5 Boot | Add Boot Options 5-120
5.40.6 Boot | ACPI Selection 5-121
5.40.7 Boot | USB Boot 5-121
5.40.8 Boot | EFI Device First 5-121
5.40.9 Boot | Automatic Failover 5-122
5.40.10 Boot | Legacy 5-122

5.41 Boot | Legacy 5-123

5.41.1 Boot | Legacy | Normal Boot Menu 5-123
5.41.2 Boot | Legacy | Boot Type Order 5-124
5.41.3 Boot | Legacy | [device category] 5-124

5.42 Boot | Legacy | Boot Type Order 5-125

5.42.1 Boot | Legacy | Boot Type Order | Floppy Drive 5-125
5.42.2 Boot | Legacy | Boot Type Order | USB 5-126
5.42.3 Boot | Legacy | Boot Type Order | Hard Disk Drive 5-126
5.42.4 Boot | Legacy | Boot Type Order | CD/DVD-ROM Drive 5-126
5.42.5 Boot | Legacy | Boot Type Order | Others 5-126

5.43 Boot | Legacy | [device category] 5-127

5.43.1 Boot | Legacy | [device category] | [device name] 5-127

5.44 Boot | Legacy | Normal Boot Menu = Advanced 5-128

5.44.1 Boot | Legacy | [boot device] 5-128

5.45 Boot | Boot Type = UEFI Boot Type 5-129

5.45.1 Boot | Fast Boot 5-129
5.45.2 Boot | USB Hot Key Support 5-130
5.45.3 Boot | EFI 5-130

5.46 Boot | EFI 5-131

5.46.1 Boot | EFI | [device name] 5-131
5.46.2 Boot | EFI | Internal EFI Shell 5-132

5.47 Exit 5-133

5.47.1 Exit | Exit Saving Changes 5-134
5.47.2 Exit | Save Change Without Exit 5-135
5.47.3 Exit | Exit Discarding Changes 5-136
5.47.4 Exit | Load Optimal Defaults 5-137
5.47.5 Exit | Save Custom Defaults 5-138
5.47.6 Exit | Custom Defaults Status 5-139
5.47.7 5-139
5.47.8 Exit | Discard Changes 5-139
5.47.9 Exit | Load Custom Defaults 5-140

6 VGA and Serial Consoles 6-1

6.1 Enabling Serial Console Mode 6-1

6.2 COM Port Selection 6-2

6.3 Protocol Options 6-3

6.4 Terminal Type Compatibility 6-4

6.5 Corrupted Serial Console Output 6-5

6.6 VGA Display Behavior 6-6

6.7 Slow Monitor Start-up 6-7

6.8 XMC/PMC Video Controller 6-8

7 Booting and Bootable Devices 7-1

7.1 UEFI Boot 7-1

7.1.1 Enabling UEFI Boot 7-1
7.1.2 Installing UEFI Compatible Operating Systems 7-1

7.2 GPT Disk Structure 7-2

7.2.1 Booting from a GPT Disk 7-2

7.3 Boot Timings 7-3

7.4 Device Names in the Boot Menu 7-4

7.5 Bootable Device Types 7-5

7.5.1 Floppy Disk Drives 7-5
7.5.2 SATA 7-5
7.5.3 SCSI 7-5
7.5.4 Ethernet 7-5
7.5.5 USB 7-5

8 The uefi shell 8-1

8.1 Enabling the UEFI Shell 8-1

8.2 Starting the UEFI Shell 8-2

8.3 UEFI Shell Script Files 8-3

8.4 The UEFI Shell Start-up Script 8-4

8.5 UEFI Shell Commands 8-5

8.6 UEFI Shell Command Examples 8-6
8.6.1 Basic Commands 8-6
8.6.2 Selecting Drives 8-6
8.7 EFI Applications 8-8
9 BIOS Updates 9-1
9.1 How to Update a BIOS In-Circuit 9-1
9.2 Precautions During a BIOS Update 9-2
9.3 Things to Remember after Updating the BIOS 9-3
9.4 BIOS Recovery 9-4
10 Maximizing Performance or Minimizing Power 10-1
10.1 Maximizing Performance 10-1
10.2 Minimizing Power 10-2
11 Security Notes 11-1
11.1 Board Level Security Package 11-1
12 VME Image Configuration 12-1
12.1 A Note on 64-bit Operating Systems 12-1
12.2 Outbound Image Allocation 12-2
12.3 Inbound Image Allocation 12-3
12.4 VME Reserved Memory Data Structure 12-4
13 Legacy BIOS Runtime Services 13-1
13.1 Video – INT 0x10 13-1
13.2 Disk I/O – INT 0x13 13-2
13.3 USB Legacy Device Support 13-3
13.3.1 Legacy Keyboard and Mouse Emulation 13-3
13.3.2 USB Mass Storage Support 13-3
13.4 ACPI 13-4
13.5 Multi-Processor Support 13-5
13.6 PCI BIOS 13-6
Appendix A BIOS MEMORY MAP A-1
Appendix B REFERENCES B-1
B.1 UEFI Firmware B-1
B.2 General PC Industry Specifications B-1
B.3 PCI BIOS Specification B-1
B.4 PXE B-1

B.5 ACPI B-1
B.6 VME B-1

TABLE OF FIGURES

Figure 3-1	BIOS Block Diagram	3-1
Figure 5-1	General Help Window	5-2
Figure 5-2	Exiting Setup – Save Changes	5-3
Figure 5-3	Exiting Setup – Discard Changes	5-4
Figure 5-4	Load Optimal Defaults Shortcut	5-5
Figure 5-5	Boot Manager	5-6
Figure 5-6	Main Menu	5-7
Figure 5-7	Main – Boot Features Menu	5-12
Figure 5-8	ACPI Shutdown = LED Option	5-18
Figure 5-9	Main – Board Status Menu	5-19
Figure 5-10	Advanced Menu	5-21
Figure 5-11	Advanced – Boot Configuration Menu	5-24
Figure 5-12	Advanced – Peripheral Configuration Menu	5-25
Figure 5-13	Advanced – SATA Configuration Menu	5-28
Figure 5-14	Advanced – Software Feature Mask Configuration Menu	5-33
Figure 5-15	Advanced – Serial ATA Port x Menu	5-36
Figure 5-16	Advanced – IDE Mode Options	5-37
Figure 5-17	Advanced – Thermal Configuration Menu	5-38
Figure 5-18	Advanced – Platform Thermal Configuration Menu	5-40
Figure 5-19	Advanced – Platform Thermal Configuration Menu – Additional Options	5-42
Figure 5-20	Advanced – CPU Thermal Configuration Menu	5-45
Figure 5-21	Advanced – Video Configuration Menu	5-48
Figure 5-22	Advanced – USB Configuration Menu	5-51
Figure 5-23	Advanced – USB Configuration Menu	5-52
Figure 5-24	Advanced – Chipset Configuration Menu	5-56
Figure 5-25	Advanced – Chipset Configuration Menu (Continued)	5-57
Figure 5-26	Advanced – ACPI Table Features Control Menu	5-62
Figure 5-27	Advanced – PCI Express Configuration Menu	5-64
Figure 5-28	Advanced – PCI Express Root Port x Menu	5-67
Figure 5-29	Advanced – Platform Configuration Menu	5-72
Figure 5-30	Advanced – Console Redirection Menu	5-76
Figure 5-31	Advanced – Console Redirection Menu	5-79
Figure 5-32	Advanced – BIOS Event Log Configuration Menu	5-82
Figure 5-33	Advanced – BIOS Event Log Configuration Menu	5-84
Figure 5-34	Clear MEMORY Event Log - Confirmation Popup	5-85

Figure 5-35	Clear BIOS Event Log - Confirmation Popup	5-86
Figure 5-36	Security Menu	5-87
Figure 5-37	Security – Supervisor Password Popup	5-89
Figure 5-38	Security – Setup Notice Popup	5-90
Figure 5-39	Security – Setup Warning Popup	5-91
Figure 5-40	Security – Change Supervisor Password Popup	5-92
Figure 5-41	Security – Additional Options	5-93
Figure 5-42	Power Menu	5-94
Figure 5-43	Power – Advanced CPU Control Menu	5-96
Figure 5-44	Power – Advanced CPU Control Menu (continued 1)	5-97
Figure 5-45	Power – Advanced CPU Control Menu (continued 2)	5-98
Figure 5-46	Power – Platform Power Management Menu	5-105
Figure 5-47	Vme Menu	5-106
Figure 5-48	VME – Outbound Images Menu	5-109
Figure 5-49	VME – Outbound Images Menu (continued)	5-110
Figure 5-50	VME – Inbound Images Menu	5-114
Figure 5-51	VME – Inbound Images Menu (continue)	5-115
Figure 5-52	Boot Menu	5-118
Figure 5-53	Graphics Mode POST Screen	5-119
Figure 5-54	Text Mode POST Screen	5-120
Figure 5-55	Boot – Legacy Menu	5-123
Figure 5-56	Boot – Boot Type Order Menu	5-125
Figure 5-57	Boot – Device Category Menu	5-127
Figure 5-58	Boot – Advance Menu	5-128
Figure 5-59	Boot Menu (Boot Type = UEFI Boot Type)	5-129
Figure 5-60	EFI Boot Menu	5-131
Figure 5-61	Exit Menu	5-133
Figure 5-62	Exit – Exit Saving Changes Popup	5-134
Figure 5-63	Exit – Save Change Without Exit Popup	5-135
Figure 5-64	Exit – Exit Discarding Changes Popup	5-136
Figure 5-65	Exit – Load Optimal Defaults Popup	5-137
Figure 5-67	Exit – Discard Changes Popup	5-139
Figure 5-68	Exit – Load Custom Defaults Popup	5-140
Figure 6-1	Example Setup Screen seen via Serial Console Mode	6-1
Figure 8-1	The UEFI Shell Prompt	8-2
Figure 8-2	Example UEFI Startup Script	8-4

Figure 8-3 UEFI Shell Command Examples 8-6
Figure 8-4 UEFI map Command Example Output 8-6
Figure 8-5 UEFI Device Navigation Example 8-7
Figure 8-6 Executing an EFI Application 8-8
Figure A-1 BIOS Memory Map A-1

TABLE OF TABLES

Table 5-1	Setup Menu Navigation	5-2
Table 5-2	Serial Port Default Configuration	5-25
Table 5-3	SATA Port Mapping	5-28
Table 5-4	Supported RAID Modes	5-30
Table 5-5	ACPI Thermal Zone temperature readings for different DTS settings	5-46
Table 5-6	USB Pin Use on VP B1x/msd	5-52
Table 5-7	USB Legacy Device Emulation	5-53
Table 5-8	PCI Express Port Use	5-64
Table 5-9	ACPI Specification Feature Additions	5-121
Table 6-1	VT 100 Escape Sequences	6-4
Table 7-1	Typical BIOS Boot Times	7-3
Table 7-2	Embedded Device Boot Names	7-4
Table 8-1	Supported Shell Commands	8-5
Table 10-1	CPU Mark ratings for different CPU options	10-1

This page is intentionally unused.

1 INTRODUCTION

1.1 Intended Audience

This manual is aimed at system integrators and end users that wish to modify the VP B1x/msd board's BIOS settings from the factory-configured Optimal Defaults.

The majority of users do not require a detailed knowledge of BIOS operation to make these changes, however interested readers can refer to Section 6 onwards for descriptions of key functions performed by the BIOS.

1.2 What Does This Manual Cover?

This manual is a reference for the InsydeH2O® UEFI BIOS software supplied with the VP B1x/msd single board computer.

This manual covers topics such as:

- Detailed descriptions of the options that can be configured through the Setup Utility
- BIOS features of particular interest to embedded systems designers e.g. the serial console and user-selectable Setup defaults.
- In-circuit BIOS updates
- The Recovery BIOS
- A general descriptions of the BIOS operation and runtime functions

The VP B1x/msd family supports both the 4-core 4th generation Intel® Core i7™ processor and the 2-core 4th generation Intel® Core™ i5 processor, unless otherwise stated the remainder of this manual will refer generically to the Intel Core i7.

1.3 What Is Not Covered by This Manual

This manual does not attempt to describe in detail the hardware functions provided by the board. This includes details of board switch settings and functions.

This manual does not provide details of how to configure the BIOS for specific applications, however Section 5, which describes the Setup Utility and Section 10, which covers performance settings, includes some hints on selecting optimal settings for certain applications.

1.4 Additional Reference Material

In order to obtain a complete description of the options and functions provided by the board and its BIOS, the user should read this document in conjunction with the Technical Reference Manual for the VP B1x/msd board (Manual Order Code 550 0050).

Additional resources relating to the UEFI BIOS and the industry standards that it implements are detailed in Appendix B.

1.5 BIOS Version

This manual is based on BIOS 3.03.01 for the VP B1x/msd (B50501A3310).

This page is intentionally unused.

2 WHAT IS THE BIOS

The BIOS is ROM-based software that the CPU executes immediately following power-on, or after any form of board reset. The BIOS is responsible for configuring the board hardware and initiating the operating system boot process.

The BIOS also provides a built-in configuration tool called the Setup Utility. The Setup Utility allows customization of many aspects of the board's operation; for example selecting which device is used to boot-load the operating system.

In addition, the BIOS provides run-time support to the operating system. For recent operating systems, such as Microsoft® Windows® 7 and Red Hat Enterprise Linux® this might be limited to supplying details of hardware devices found on the board when the OS loads. For older operating systems the BIOS provides a number of low-level hardware support functions including disk and keyboard I/O.

Finally, the BIOS provides some System Management functions that continue to operate after the operating system loads, e.g. monitoring and reporting the CPU temperature.

Although the BIOS on Concurrent Technologies board products looks and behaves very similar to that found on laptops or desktop computers, it also includes a number of internal adaptations, which tailor it to the embedded computing environment. In particular the BIOS allows redirection of the console function to a serial terminal or emulator program rather than using a video adapter and it provides extensions to configure interfaces to the VME backplane. These features will be discussed in more detail at appropriate points throughout the remainder of this document.

2.1 UEFI a BIOS for the 21st Century

The VP B1x/msd is supplied with a UEFI BIOS implemented using InsydeH2O from Insyde Software. This is the latest generation of boot firmware for the PC compatible market and replaces the aging legacy BIOS.

IBM created the original PC BIOS in 1981 and since its birth the BIOS has evolved and grown in step with new hardware developments, but at its heart the BIOS remained an 8-bit, single-threaded, real-mode relic written exclusively in assembler.

Many new features and interfaces have been bolted on to the BIOS over the years in order to keep up with the demands of modern multi-core, multi-gigabyte PCs and their operating systems, but by the late 1990's the industry recognized that the BIOS was in need of a complete rewrite.

UEFI started life as the Intel® Boot Firmware Initiative, a modern boot framework initially developed for the Itanium processor line. Later this was renamed the Extensible Firmware Interface (EFI) and development continued until 2005 when Intel passed development over to the Unified EFI Forum, who renamed it the Unified Extensible Firmware Interface (UEFI).

In its purest form a UEFI BIOS can only boot UEFI compatible operating systems, so legacy operating systems like Windows® XP will no longer work. The InsydeH2O UEFI BIOS includes a Compatibility Support Module (CSM) that provides the necessary support functions and boot loader that allows the VP B1x/msd to continue supporting a full range of legacy operating systems.

This page is intentionally unused.

3 VP B1X/MSD BLOCK DIAGRAM

3.1 Hardware Block Diagram

The following diagram illustrates the key embedded hardware components and off-board interfaces found on the VP B1x/msd.

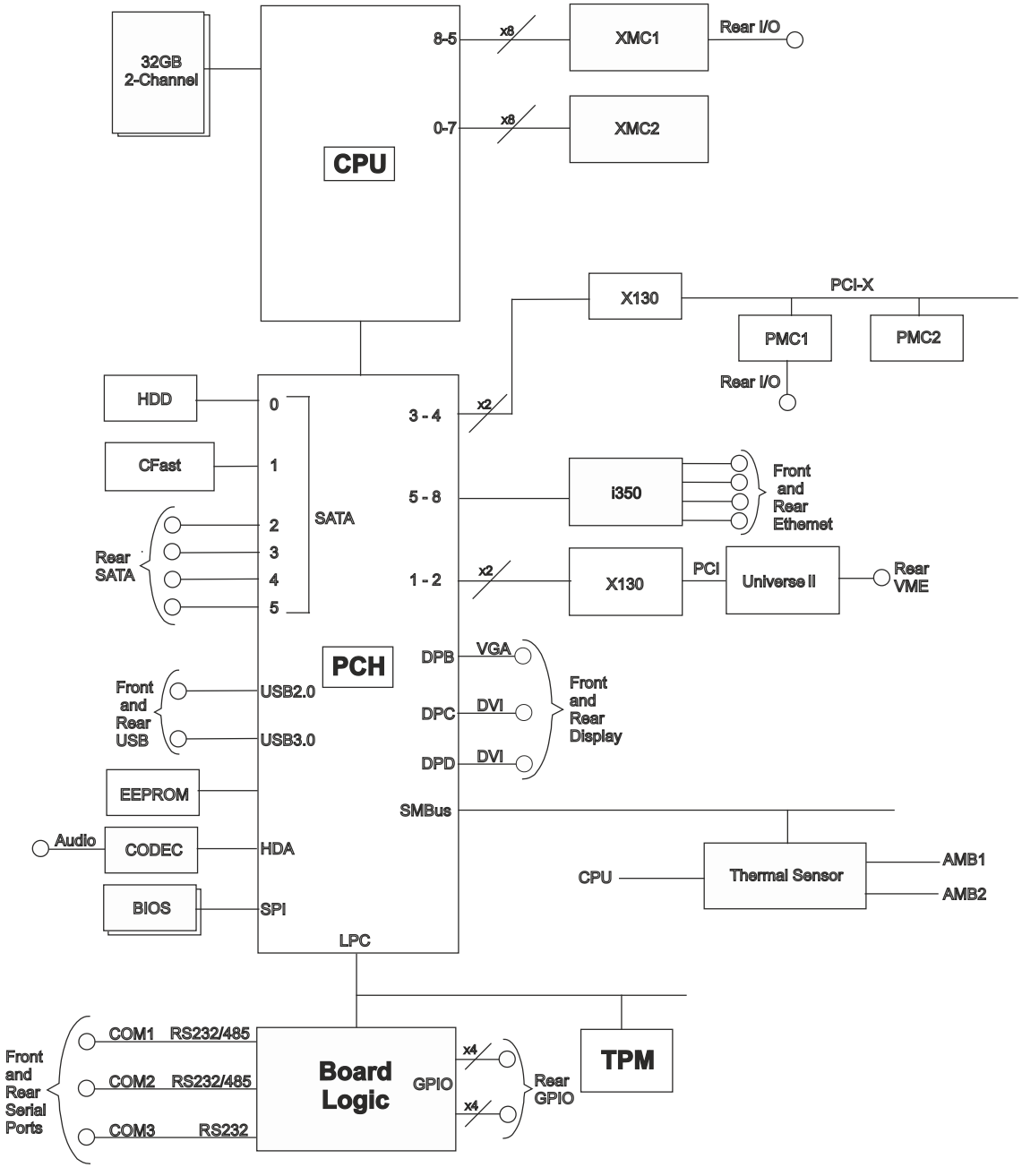


Figure 3-1 VP B1x/msd Hardware Block Diagram

VP B1X/MSD BLOCK DIAGRAM

This page is intentionally unused.

4 CHANGING AND SAVING BIOS SETTINGS

The legacy BIOS held its configuration settings in battery-backed CMOS RAM; meaning that if the board was powered-off without a battery fitted, the settings were lost. The UEFI BIOS stores its configuration settings in the BIOS ROM, so no battery is required.

> **NOTE:** The real-time clock requires a battery to maintain the correct time and date when main board power is turned off.

The BIOS shipped with the VP B1x/msd includes factory configured default values for all parameters controlled through the Setup Utility. These settings are carefully chosen to provide the best combination of features and performance. However, no set of default values can cater for all scenarios.

4.1 What are Optimal and Custom Defaults?

The board maintains three separate Setup configurations:

- The Working Set
- Optimal Defaults
- Custom Defaults

Each time the board is powered on, it reads configuration settings from the Working Set. The Working Set is stored in the BIOS ROM and will be retained without a backup supply. When changes are made via the Setup utility the Working Set will be updated when the settings are saved.

When the board is shipped from the factory, the Working Set will contain the Optimal Defaults. The board can be returned to the shipping configuration at any time by entering Setup and selecting **Load Optimal Defaults** from the **Exit** menu.

The user cannot change the Optimal Defaults, however the BIOS also provides a Custom Defaults set where the user can save a preferred configuration. If changes are subsequently made to the working set, the board can be returned to the custom configuration by entering **Setup** and selecting **Load Custom Defaults** from the **Exit** menu.

4.2 When Do My Settings Get Loaded?

Selecting **Load Optimal Defaults** or **Load Custom Defaults** from the **Exit** menu will copy the selected configuration to the Working Set.

Once the working set has been saved those settings will be retained and loaded on all subsequent boots.

4.3 Forcibly Loading Optimal Defaults

It is possible, though unlikely, that **Setup** changes could prevent the board booting. Under these circumstances, it may not be possible to enter the **Setup Utility** and make corrections. If this happens, the board can be restored to the factory shipping configurations using the Force Optimal Defaults switch. Refer to the Board's Technical Reference Manual for details.

This page is intentionally unused.

5 SETUP MENUS

5.1 Setup Menu Typographic Conventions

[***text label***] Identifies an item whose label can vary, e.g. a boot device name.

<**Esc**> Indicates a key press

n Is a reference to a member of a numbered list

Sub Menu
Select a Setup Utility sub-menu or pop-up menu

A Sub menu. Selecting this option will either open a new **Setup** menu, or create a small pop-up menu.

Setup Option	
Change a BIOS Setup option.	
Disabled	The option is disabled
Enabled	The option is enabled

A Setup option; the default setting is indicated by a grey background.

Setup Option	**Caution**
Change a BIOS Setup option. Caution is advised before making the change.	
Disabled	The option is disabled
Enabled	The option is enabled

A Setup option that might adversely affect board operation if incorrectly configured for any given system; the default setting is indicated by a grey background.

Informative Field	
Reports the status of a software function or a hardware feature. This field cannot be changed though there may be other BIOS options that affect the information displayed here.	
Disabled	The hardware is disabled
Enabled	The hardware is enabled

This option displays informative text that cannot be changed directly. It usually reports the status of hardware or software features.

5.2 Entering Setup and Navigating the Setup Menus

The BIOS Setup Utility can be entered by pressing <**F2**> while the BIOS is executing POST.

Once the Setup Utility has started, the menus can be navigated using the keyboard, mouse or a combination of the two.

When using the mouse the left button selects menus and options, while the right button cancels the operation or backs up one menu level.

The keys used to navigate Setup menus are detailed in Table 5-1.

Key	Meaning
<**F1**>	Display General Help window.
<**Esc**>	Exit current menu.
← or → arrow keys	Select top-level menu.
↑ or ↓ arrow keys	Move cursor up and down.
<**F5**> or <**F6**>	Cycle up or down through settings
<**+**> or <**-**>	Increment or decrement a numeric value
<**Enter**>	Execute Command or Select a Sub-menu.
<**F3**>	Reload the Default Configuration values.
<**F4**>	Save settings and Exit Setup.

Table 5-1 Setup Menu Navigation

The General Help window can be displayed at any time by pressing the <**F1**> key.

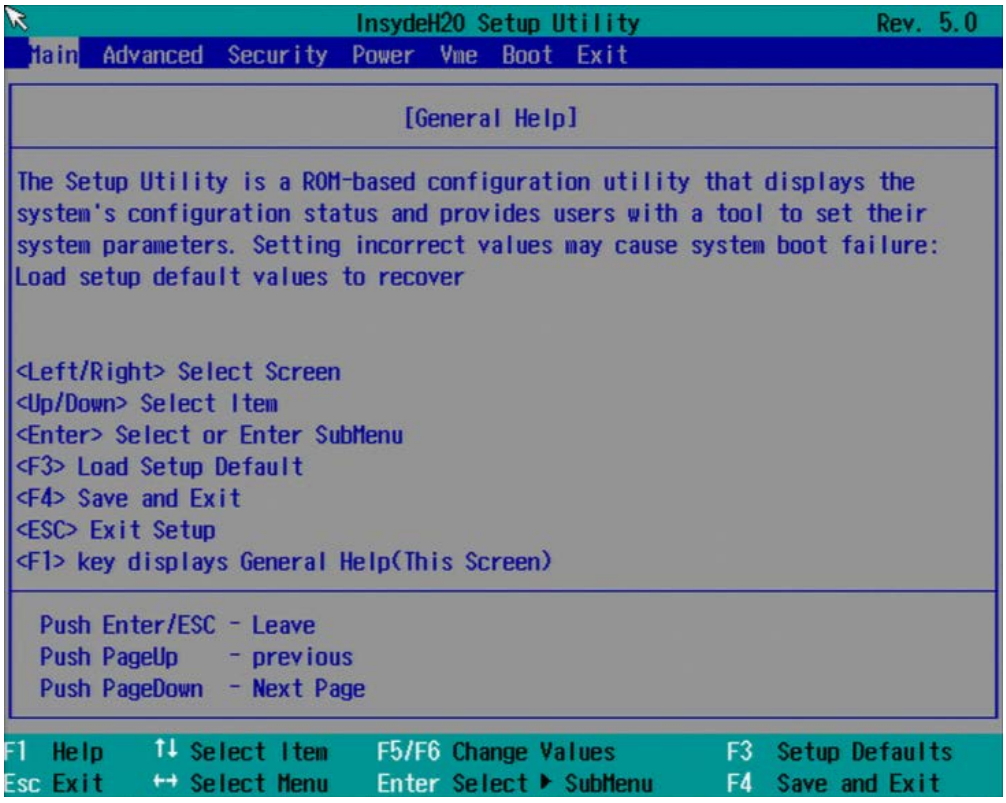


Figure 5-1 General Help Window

5.3 Exiting Setup

The **Exit** menu provides options for saving and quitting the **Setup** Utility, however two shortcut keys <**F4**> and <**Esc**> operate from within any **Setup** menu.

5.3.1 Exit Saving Changes

Pressing <**F4**> from any of the top-level menus will respond with a pop-up menu.

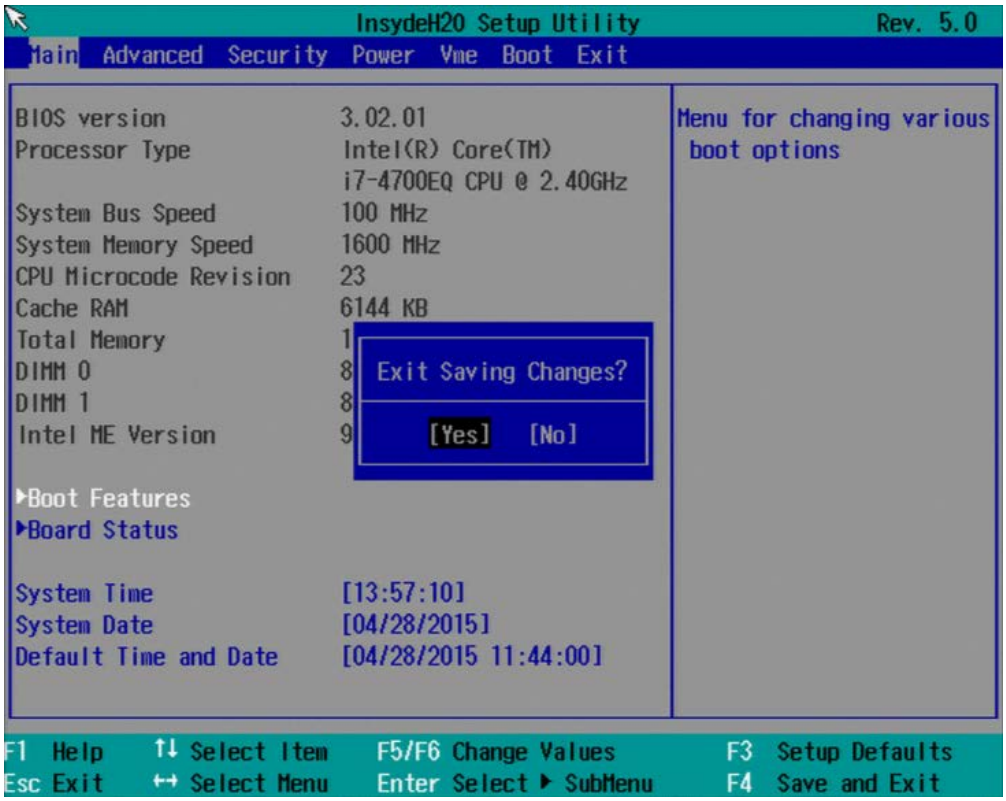


Figure 5-2 Exiting Setup – Save Changes

If the choice is confirmed, all changes made via the **Setup** utility will be saved and the board will restart.

The <**F4**> key is a shortcut for the **Exit Saving Changes** option found under the **Exit** top-level menu (see Section 5.47.1).

5.3.2 Exit Discarding Changes

Pressing <**Esc**> from any of the top-level menus will respond with a pop-up menu.

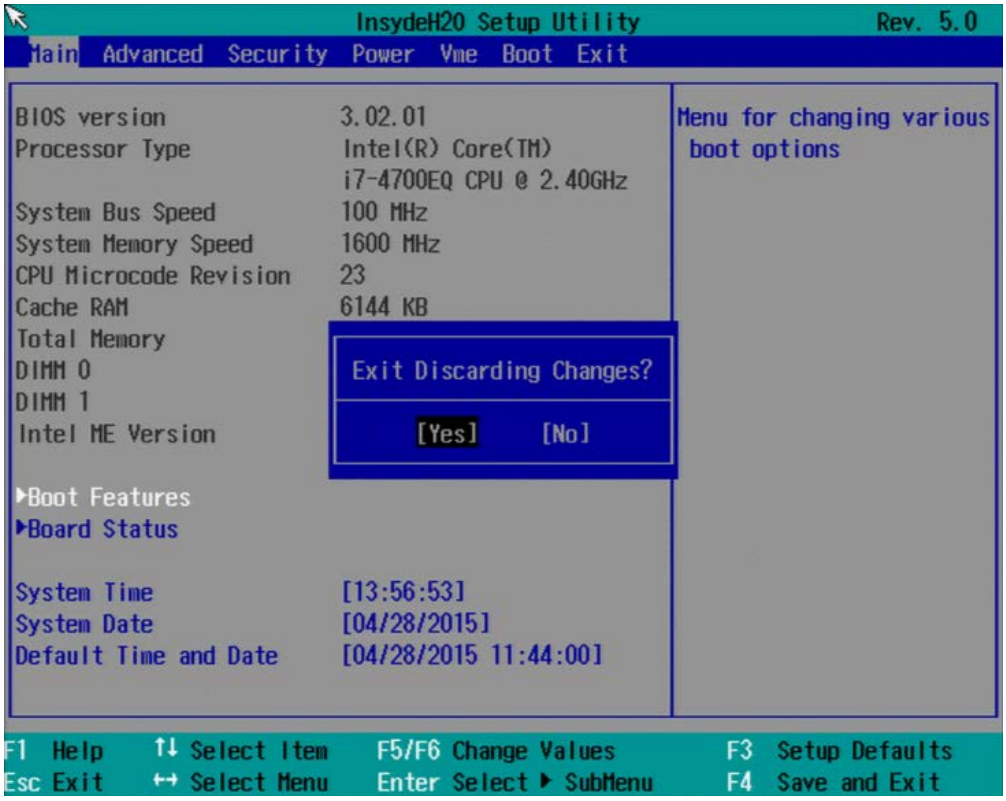


Figure 5-3 Exiting Setup – Discard Changes

If the choice is confirmed, any changes made via the **Setup** utility will be discarded and the board will restart.

The <**Esc**> key is a shortcut for the **Exit Discarding Changes** option found under the **Exit** top-level menu (see Section 5.47.3).

5.4 Loading Optimal Defaults

Pressing <**F3**> from any of the top-level menus will respond with a pop-up menu.

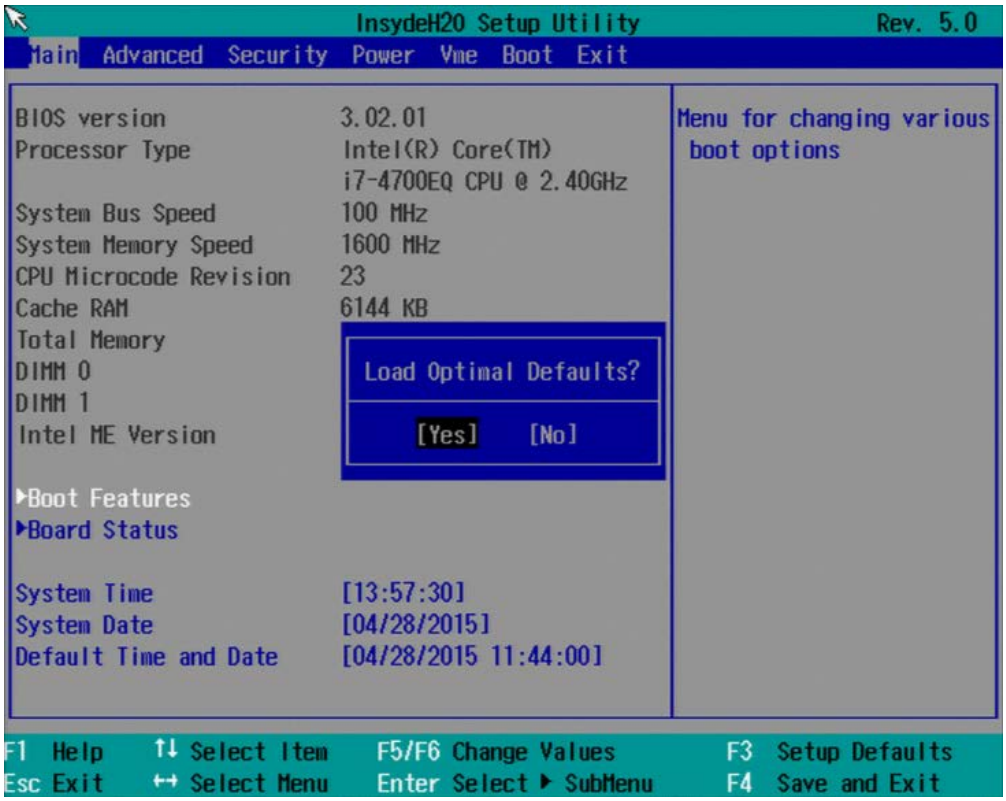


Figure 5-4 Load Optimal Defaults Shortcut

If the choice is confirmed, any changes made via the **Setup** utility will be discarded and the factory-configured Optimal Defaults will be loaded.

The <**F3**> key is a shortcut for the **Load Optimal Defaults** option found under the **Exit** top-level menu (see Section 5.47.4).

5.5 The Boot Manager

Pressing <**F12**> during BIOS POST will display the Boot Manager before entering the BIOS boot loader. From here, the user can select the boot device instead of using the boot order specified through the Setup Utility.

The list can be navigated using the <↑> and <↓> arrow keys and the selection is made with the <**Enter**> key. Once the selection has been made, the BIOS will begin booting from that device. This is a one-time selection and the Boot Manager does not change the Setup boot order.

Pressing <**Esc**> will exit the boot manager and use the Setup boot order instead.

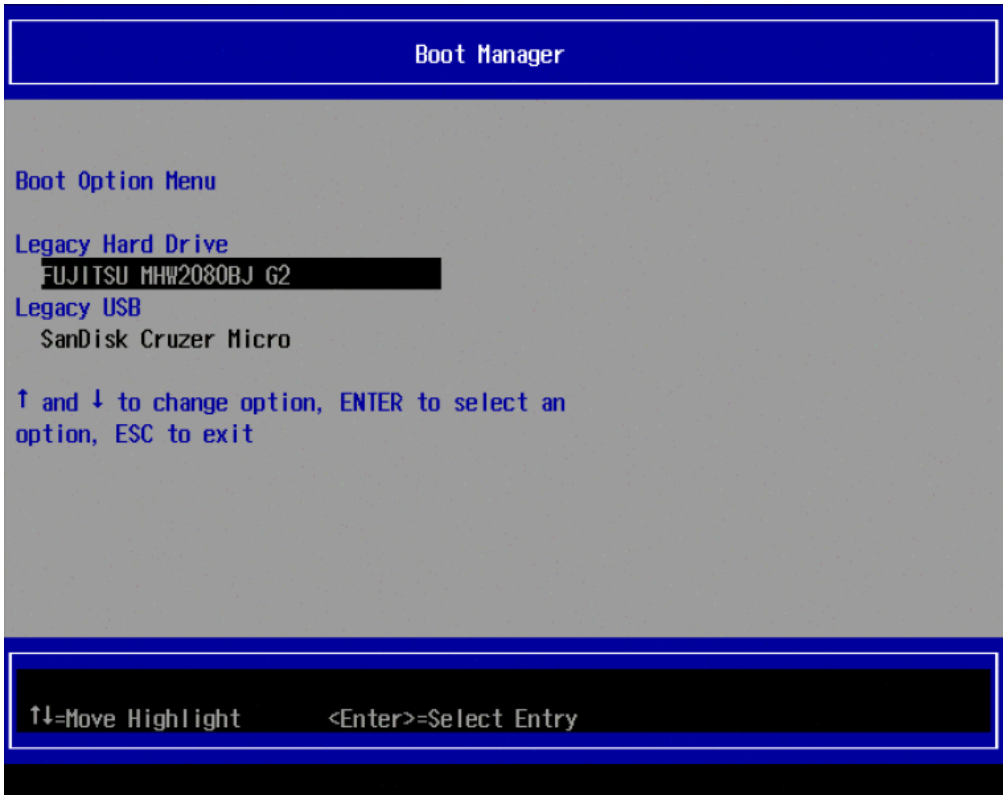


Figure 5-5 Boot Manager

5.6 Main

The main **Setup** menu displays details concerning key system configuration parameters, including fitted memory and CPU speed.

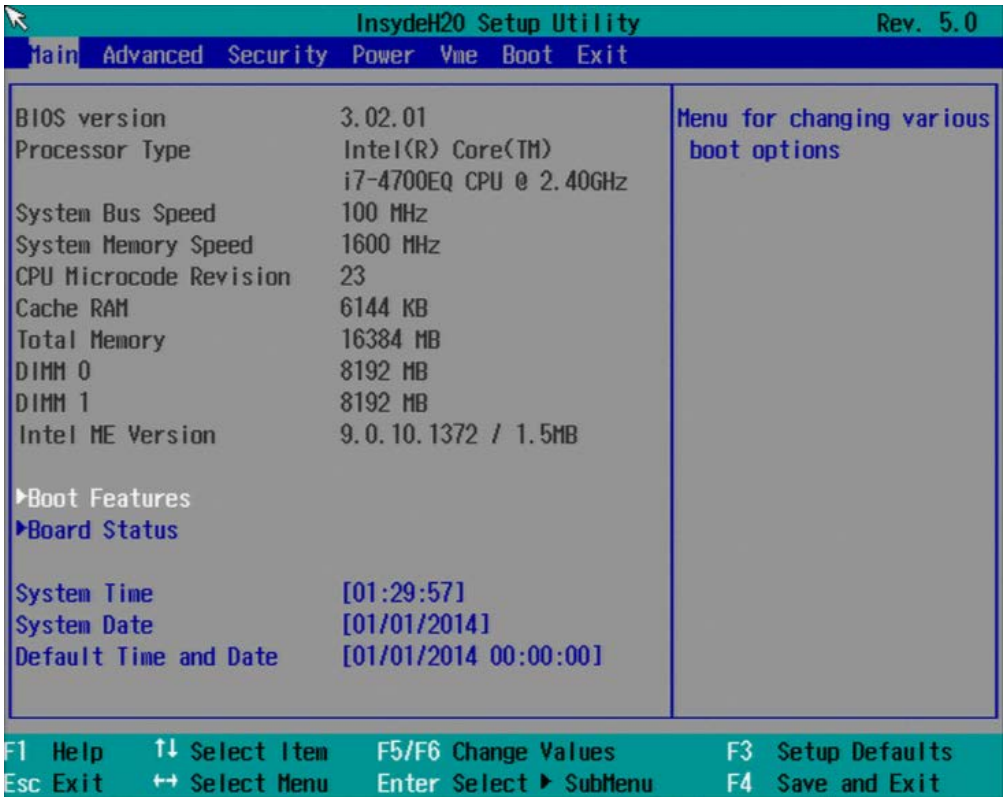


Figure 5-6 Main Menu

5.6.1 Main | BIOS Version

BIOS Version
Reports the system BIOS version installed on the board.

Pre-release or experimental BIOS versions are indicated by appending a release candidate number and the compilation date, e.g. “3.02.01-RC03 02-Jan-2013”.

5.6.2 Main | Processor Type

Processor Type
Displays the processor brand string as read from the CPU.

This is the Brand String reported by the CPU via the CPUID instruction.

5.6.3 Main | System Bus Speed

System Bus Speed
Reports the base clock speed of the bus connecting the CPU to the PCH.

This figure is equivalent to the front Side Bus (FSB) speed on traditional CPU plus North Bridge configurations.

5.6.4 Main | System Memory Speed

System Memory Speed
Reports the speed of the DRAM interface.

5.6.5 Main | CPU Microcode Revision

CPU Microcode Revision
Reports the revision number of the Intel CPU microcode.

The revision number will depend on the CPU silicon stepping and the type of CPU, so a low voltage CPU variant might have a different microcode revision to an ultra-low-voltage variant.

5.6.6 Main | Cache RAM

Cache RAM
This option reports the size of the shared Last Level Cache.

The Intel® Core™ i5 and i7 processors have three independent levels of caching:

A 32 Kbyte instruction and 32 KB data first-level cache (L1) for each core

A 256 Kbyte shared instruction/data second-level cache (L2) for each core

An instruction/data last level cache (L3), shared among all cores. Core™ i5 processors have 3 MB (2 core), while Core™ i7 processors have 6 MB (4-core) or 4 MB (2-core).

5.6.7 Main | Total Memory

Total Memory
Reports the total capacity of the memory modules fitted to the board.

NOTE: This figure indicates the maximum memory available on the board; however, the amount of memory available to the operating system will always be less, due to memory reserved for System Management Mode and the Integrated Graphics Device (IGD).

The System Management BIOS reserves 8 MB. This memory is locked and cannot be reclaimed by the operating system.

The Video Controller reserves between 32 MB and 128 MB depending on the DVMT selection. This memory is locked and cannot be reclaimed by the operating system.

If a 32-bit operating system is used then the maximum available memory will be around 3 Gbytes; the exact value depending on the address range claimed by PCI devices. The remaining memory is remapped by the chipset above the 4 Gbyte address boundary where it is inaccessible to 32-bit operating systems, unless they support Physical Address Extension (PAE).

A 64-bit operating system will be able to utilize all of the available memory.

Appendix A provides a BIOS memory map indicating the organization of the 32 and 64-bit memory address space on the VP B1x/msd.

5.6.8 Main | DIMM 0

DIMM 0
Reports the memory capacity fitted on memory controller channel A.

The VP B1x/msd does not support memory modules, the DRAM devices are soldered directly onto the baseboard, however the BIOS manages this memory as if it were two SODIMMs.

5.6.9 Main | DIMM 1

DIMM 1
Reports the memory capacity fitted on memory controller channel B.

The VP B1x/msd does not support memory modules, the DRAM devices are soldered directly onto the baseboard, however the BIOS manages this memory as if it were two SODIMMs.

5.6.10 Main | Intel ME Version

Intel ME Version
Reports the version of the Management Engine (ME) firmware fitted to the board.

The Management Engine (ME) is an embedded controller located inside the PCH. The operation of the ME is beyond the scope of this document.

5.6.11 Main | Boot Features

Boot Features
Configure options relevant to the boot environment.

The **Boot Features** options are detailed in Section 5.7.

5.6.12 Main | Board Status

Board Status
Display details of the board's hardware configuration.

The **Board Status** options are detailed in Section 5.9.

5.6.13 Main | System Time

System Time
View and set the system time maintained by the Real Time Clock in the PCH.

The time is displayed in HH:MM:SS format. Individual time fields can be changed using the **+** and **–** keys (or **F5** and **F6**) and the **Enter** key is used to move to the next time field.

When the power is switched off the time and date will be maintained if the on-board coin cell is fitted. If the coin cell is not fitted then the time will reset to the default value when the board is next powered on.

When the board is received from the factory the default time is set to 00:00:00, this can be changed using the **Default Time and Date** option (see Section 5.6.15).

5.6.14 Main | System Date

System Date
View and set the system date maintained by the Real Time Clock in the PCH.

The date is displayed in MM/DD/YYYY format. Individual date fields can be changed using the + and – keys (or **F5** and **F6**) and the **Enter** key is used to move to the next date field.

When the power is switched off the time and date will be maintained if the onboard coin cell is fitted. If the coin cell is not fitted then the date will reset to the default value when the board is next powered on.

When the board is received from the factory the default time is set to 01:01:2013, this can be changed using the **Default Time and Date** option (see Section 5.6.15).

5.6.15 Main | Default Time and Date

Default Time and Date	
Reports the BIOS defaults for date and time.	
[Date and Time]	BIOS default date and time
Yes	Set new default values

If the real time clock (RTC) looses standby power while the board is switched off the settings will be lost and as a result the BIOS will reinitialize the date and time counters when the board is next powered on. The factory configured default is midnight on 1st January 2013, however certain software may require a more recent date before it will operate.

This field allows the user to set an alternative value for the default date and time. When **Yes** is selected the current RTC date and time values are recorded as the new default value and this will be loaded instead of the factory defined value.

5.7 Main | Boot Features

The **Boot Features** menu contains many of the options commonly modified by end users.

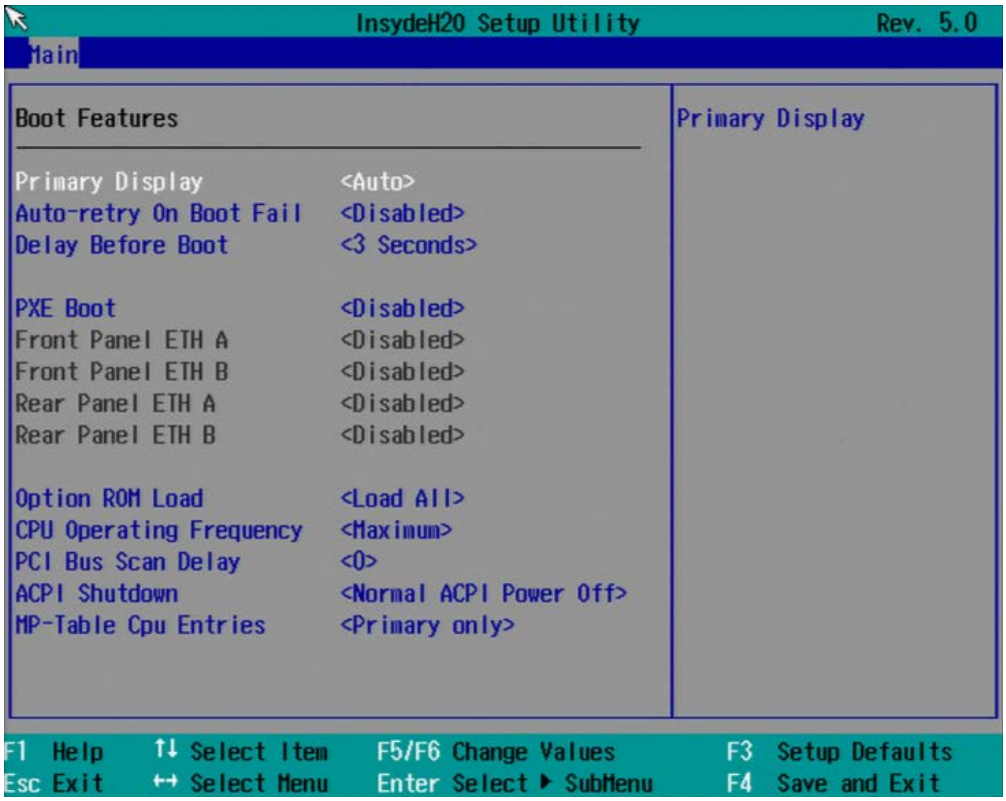


Figure 5-7 Main – Boot Features Menu

5.7.1 Main | Boot Features | Primary Display

Primary Display	
When more than one video controller is available, this option selects which will be used as the console device.	
Auto	The BIOS selects the video controller based on PCI ordering rules.
On-Board	The Intel IGD will always be used.

PCI video controller ordering rules specify that the device with the highest bus, device and function numbers will be used as the default console device in **Auto** mode, however this can cause problem for certain operating systems that require access to the IGD video BIOS. When this occurs, selecting **On-Board** as the console will resolve the issue.

5.7.2 Main | Boot Features | Auto-retry On Boot Fail

Auto-retry On Boot Fail	
Allow the BIOS to retry boot devices until successful.	
Disabled	The BIOS will try each boot device once only.
Enabled	The BIOS will retry all devices in the boot menu until successful.

This option is primarily intended for use with PXE or other network-based boot protocols where the boot server may not be available when the board attempts to boot. When set to **Enabled** the BIOS will repeatedly attempt to boot from each device specified in the **Boot** menu.

5.7.3 Main | Boot Features | Delay Before Boot

Delay Before Boot	
Introduce an optional delay before entering the BIOS boot loader.	
0	Delay interval, in seconds, before entering the boot loader.
3	
5	
10	

Modern energy-saving monitors can take a number of seconds to switch on once a video source is detected, therefore the BIOS screen may not become visible before the operating system starts to boot.

By default the BIOS will pause for three seconds before entering the boot loader, under most circumstances this will be sufficient to view any error messages or to press the **<F2>** key to enter the Setup utility.

NOTE: If boot time is critical to the system design this option should be set to zero.

5.7.4 Main | Boot Features | PXE Boot

PXE Boot	
Enable PXE boot firmware for add-in cards or one of the embedded Ethernet controller channels.	
Disabled	PXE booting is disabled for all devices
Enabled	PXE booting is enabled

This option provides a master ‘enable’ control for all devices supporting PXE boot. It covers both add-in cards and the on-board Ethernet interfaces. When this option is set to **Enabled** additional options become available for controlling PXE boot via each of the on-board interfaces.

Enabling PXE boot firmware allows the board to boot from an external PXE server via one of the embedded Ethernet channels. Further information regarding the Preboot Execution Environment can be obtained from sources detailed in Appendix B.

5.7.5 Main | Boot Features | Front Panel ETH A

NOTE: This option is only available when **PXE Boot** is set to Enabled.

Front Panel ETH A	
Enable PXE boot firmware for the front panel Ethernet controller channel A.	
Disabled	PXE boot is disabled for this controller
Enabled	PXE boot is enabled

Enabling PXE boot firmware allows the board to boot from an external PXE server connected via the front panel Ethernet controller channel A.

5.7.6 Main | Boot Features | Front Panel ETH B

NOTE: This Ethernet channel is only available on board configurations having additional front panel I/O in place of XMC1. This option is only available when **PXE Boot** is set to Enabled.

Front Panel ETH B	
Enable PXE boot firmware for the front panel Ethernet controller channel B.	
Disabled	PXE boot is disabled for this controller
Enabled	PXE boot is enabled

Enabling PXE boot firmware allows the board to boot from an external PXE server connected via the front panel Ethernet controller channel B.

5.7.7 Main | Boot Features | Rear Panel ETH A

NOTE: This option is only available when **PXE Boot** is set to Enabled.

Rear Panel ETH A	
Enable PXE boot firmware for the rear Ethernet controller channel A.	
Disabled	PXE boot is disabled for this controller
Enabled	PXE boot is enabled

Enabling PXE boot firmware allows the board to boot from an external PXE server connected via the rear Ethernet controller channel-A.

5.7.8 Main | Boot Features | Rear Panel ETH B

NOTE: This option is only available when **PXE Boot** is set to Enabled.

Rear Panel ETH B	
Enable PXE boot firmware for the rear Ethernet controller channel-B.	
Disabled	PXE boot is disabled for this controller
Enabled	PXE boot is enabled

Enabling PXE boot firmware allows the board to boot from an external PXE server connected via the rear Ethernet controller channel-B.

5.7.9 Main | Boot Features | Ethernet Mode

Ethernet Mode	
Select the interface configuration for the i350 backplane Ethernet channels.	
SerDes+SerDes	Both channels use SerDes
SerDes+Copper	One SerDes and one Copper interface

This option updates the Ethernet controller's serial EEPROM with the selected interface configuration.

After saving settings a board power cycle is required to initiate the EEPROM reprogramming operation. When the board restarts it will proceed to program the EEPROM, and then automatically restarts to load the new settings. The EEPROM is only updated when the BIOS determines that the interface configuration has changed.

5.7.10 Main | Boot Features | Option ROM Load

Option ROM Load	
Controls the loading of BIOS extension firmware to prevent resource conflicts.	
Load All	Load BIOS extension firmware for all applicable devices.
Load SCSI Once	Load only one copy of the SCSI/SAS extension firmware.

BIOS extension firmware is usually paired with a single instance of a device (e.g. PXE firmware). However, some SCSI or SAS controller firmware controls all compatible devices through a single instance of the firmware; however, the BIOS is unable to distinguish this fact and is forced to load a copy of the firmware for each controller.

The memory where BIOS extension firmware is loaded is a limited resource and loading more than one copy of SCSI or SAS controller firmware can easily exhaust this memory pool. Setting this option to **Load SCSI Once** will instruct the BIOS to load only one copy of SCSI or SAS extension firmware.

5.7.11 Main | Boot Features | CPU Operating Frequency

CPU Operating Frequency	
Limits the maximum operating frequency of all CPU cores.	
Maximum	No limit on operating frequency (if Turbo Mode enabled)
2300 MHz	Limit the maximum operating frequency to the selected value. Example operating frequencies taken from a 2.4 GHz CPU, other CPU options will have different operating frequencies.
2200 MHz	
2100 MHz	
2000 MHz	
1900 MHz	
1700 MHz	
1600 MHz	
1500 MHz	
1400 MHz	
1300 MHz	
1200 MHz	
1100 MHz	
1000 MHz	
900 MHz	
800 MHz	

Certain system configurations have tight power budgets. Under those circumstances, it may be desirable to reduce the CPU operating frequency in order to save power.

When the Maximum setting is selected Intel Turbo Boost Technology may raise an individual core's operating frequency above the rated frequency for short periods if the processing load is high and the power budget allows.

NOTE: Users should be aware that this option sets the maximum operating frequency. ACPI operating systems will not increase the CPU frequency beyond this figure; however they may reduce the frequency if the processing load is light.

NOTE: If the CPU temperature exceeds the Thermal Control Circuitry threshold the CPU frequency will be automatically reduced below this setting.

5.7.12 Main | Boot Features | PCI Bus Scan Delay

PCI Bus Scan Delay	
Introduce a delay, measured in seconds, before PCI resource allocation.	
0	No delay
1	Delay in seconds before PCI resource allocation
2	
3	
4	
5	
10	
15	
20	

Certain PMC and XMC cards, especially those containing FPGAs, require a delay (measured in seconds) while they initialize hardware interfaces. Attempting to scan for PCI devices before this initialization period is complete may result in a board hang or the add-in card being omitted from the resource allocation process.

NOTE: Devices that are omitted from the PCI resource allocation process cannot be used as a boot device and in most circumstances will not be available to the operating system.

5.7.13 Main | Boot Features | ACPI Shutdown

ACPI Shutdown	
Specifies what action the board performs when an ACPI operating system shuts down.	
Normal ACPI Power Off	Enter S5 State; on board supplies are switched off.
LED	The POST LED is driven as specified

When an ACPI operating system shuts down it transitions the board to the S5 power-off state. As an alternative, the board can be configured to change the state of an LED to indicate that the shutdown is complete.

When the LED option is selected additional Setup fields are revealed. See Section 5.8 for available options.

5.7.14 Main | Boot Features | MP-Table Cpu Entries

MP-Table Cpu Entries	
Specifies which CPU entries appear in the Multi-processor Table (MPTable)	
Primary only	Only the primary cores are listed
Both	Both primary and hyper threading cores are listed

This option is for use with non-ACPI operating systems.

By default the Multi-processor Table (MPTable) is populated with details of the primary CPU cores, in accordance with Intel design recommendations. When this option is set to **Both,** the hyper threading cores will also be included.

5.8 Main | Boot Features | ACPI Shutdown = LED

When the **ACPI Shutdown** option is set to **LED** an additional option is displayed for configuring the LED behavior at shutdown.

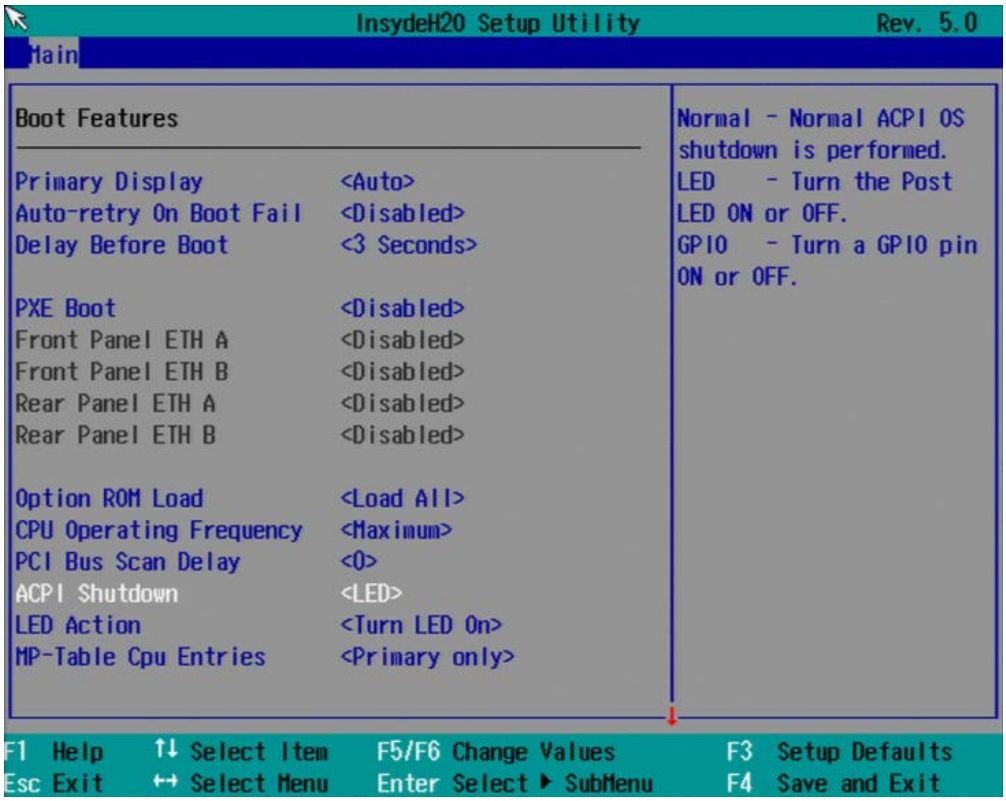


Figure 5-8 ACPI Shutdown = LED Option

5.8.1 Main | Boot Features | LED Action

LED Action	
Specify the POST LED action when an ACPI operating system shuts down.	
Turn LED Off	Turn the LED off
Turn LED On	Turn the LED on

During board initialization the BIOS will configure the POST LED to the inverse of the selected action. When the ACPI operating system shuts down the LED is driven to the selected state.

5.9 Main | Board Status

The **Board Status** menu reports the status of certain backplane signals and board options.

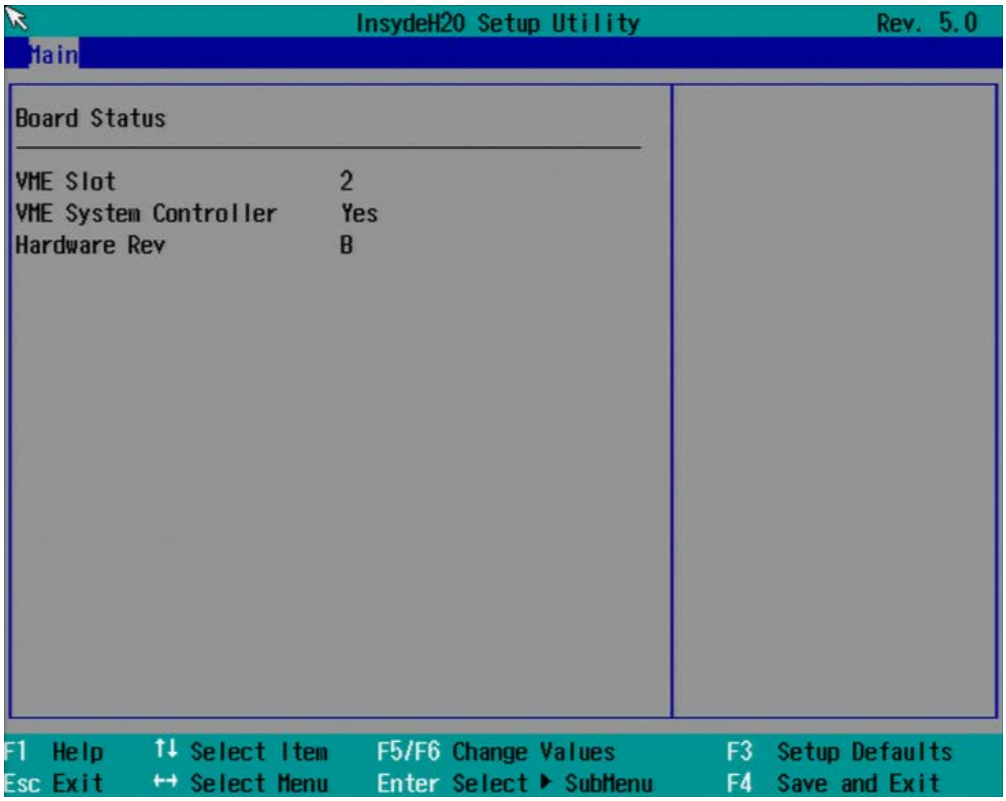


Figure 5-9 Main – Board Status Menu

5.9.1 Main | Board Status | VME Slot

VME Slot
Reports the board's VME64 slot number.

Slots in a VME64 compliant backplane are numbered starting with 1 and include a parity check which the BIOS validates before displaying this field.

If the backplane does not support VME64 slot numbering, the parity check returns an error and this field displays **Unknown**.

5.9.2 Main | Board Status | VME System Controller

VME System Controller
Indicates whether the board is the chassis System Controller.

5.9.3 Main | Board Status | Hardware Rev

Hardware Rev
Reports the revision level of the board's PCB.

Revision levels are indicated by a letter where **A** is the first revision, **B** the second revision and so on.

5.10 Advanced

The **Advanced Setup** menu contains a series of sub-menus through which key CPU, chipset, peripheral and platform options can be configured.

Some of the options in these menus can cause the board to stop booting if incorrectly configured; therefore caution should be exercised when making changes from the factory configured Optimal Default settings.

WARNING: Many of the options found under the Advanced menu can adversely affect the board operation if incorrectly configured. Users are advised against changing options unnecessarily.

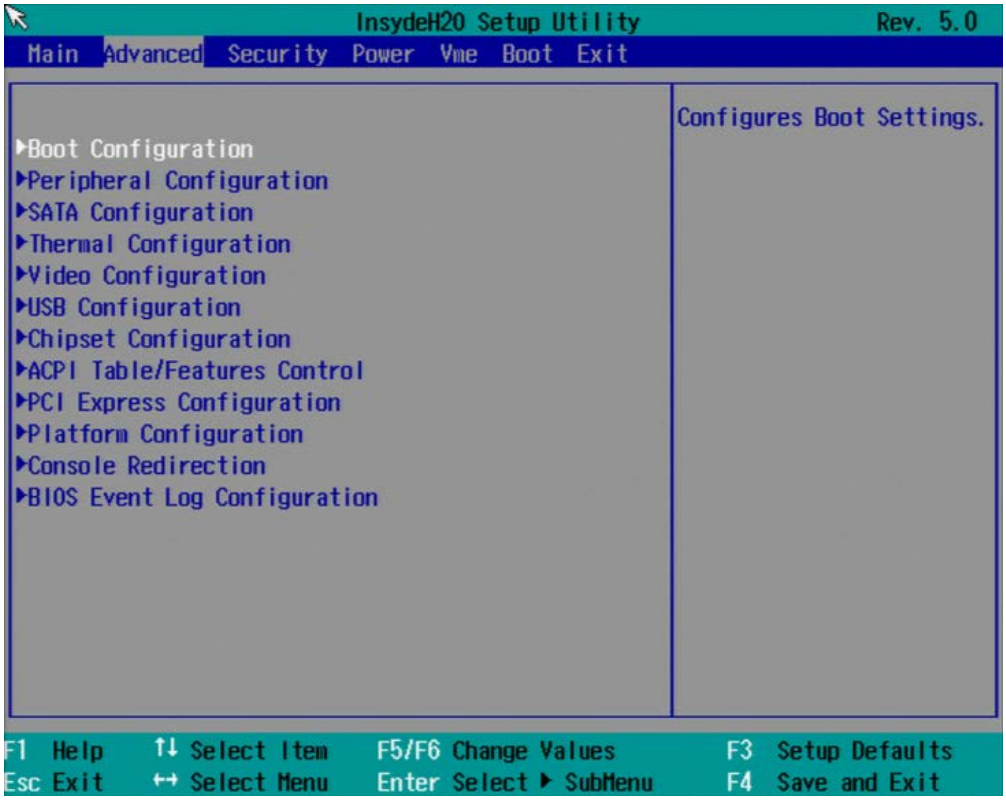


Figure 5-10 Advanced Menu

5.10.1 Advanced | Boot Configuration

Boot Configuration
Configure options relevant to the boot environment.

The **Boot Configuration** options are detailed in Section 5.11.

5.10.2 Advanced | Peripheral Configuration

Peripheral Configuration
Configure options relevant to the embedded serial ports and Intel High Definition Audio (HDA) interface.

The **Peripheral Configuration** options are detailed in Section 5.12.

5.10.3 Advanced | SATA Configuration

SATA Configuration
Configure options relevant to the embedded SATA interfaces.

The **SATA Configuration** options are detailed in Section 5.13.

5.10.4 Advanced | Thermal Configuration

Thermal Configuration
Configure options relevant to thermal management of the CPU and on board devices.

The **Thermal Configuration** options are detailed in Section 5.17.

5.10.5 Advanced | Video Configuration

Video Configuration
Configure options relevant to the Intel Embedded Graphics controller and CPU's PCI Express ports.

The **Video Configuration** options are detailed in Section 5.21.

5.10.6 Advanced | USB Configuration

USB Configuration
Configure options relevant to the embedded USB interfaces.

The **USB Configuration** options are detailed in Section 5.22.

5.10.7 Advanced | Chipset Configuration

Chipset Configuration
Configure options relevant to the PCH.

The **Chipset Configuration** options are detailed in Section 5.23.

5.10.8 Advanced | ACPI Table/Features Control

ACPI Table/Features Control
Configure options relating to the ACPI byte code and tables.

The **ACPI Table/Features Control** options are detailed in Section 5.24.

5.10.9 Advanced | PCI Express Configuration

PCI Express Configuration
Configure options relevant to the CPU and PCH PCI Express Root Ports.

The **PCI Express Configuration** options are detailed in Section 5.25.

5.10.10 Advanced | Platform Configuration

Platform Configuration
Display key details of the CPU and chipset configuration.

The **Platform Configuration** options are detailed in Section 5.27.

5.10.11 Advanced | Console Redirection

Console Redirection
Configure options relevant to the BIOS serial console.

The **Console Redirection Configuration** options are detailed in Section 5.28.

5.10.12 Advanced | BIOS Event Log Configuration

BIOS Event Log Configuration
Configure the BIOS Event Logging functions.

The BIOS Event Log Configuration options are detailed in Section 5.30.

5.11 Advanced | Boot Configuration

The **Boot Configuration** menu contains options for controlling the board state when entering the boot loader.

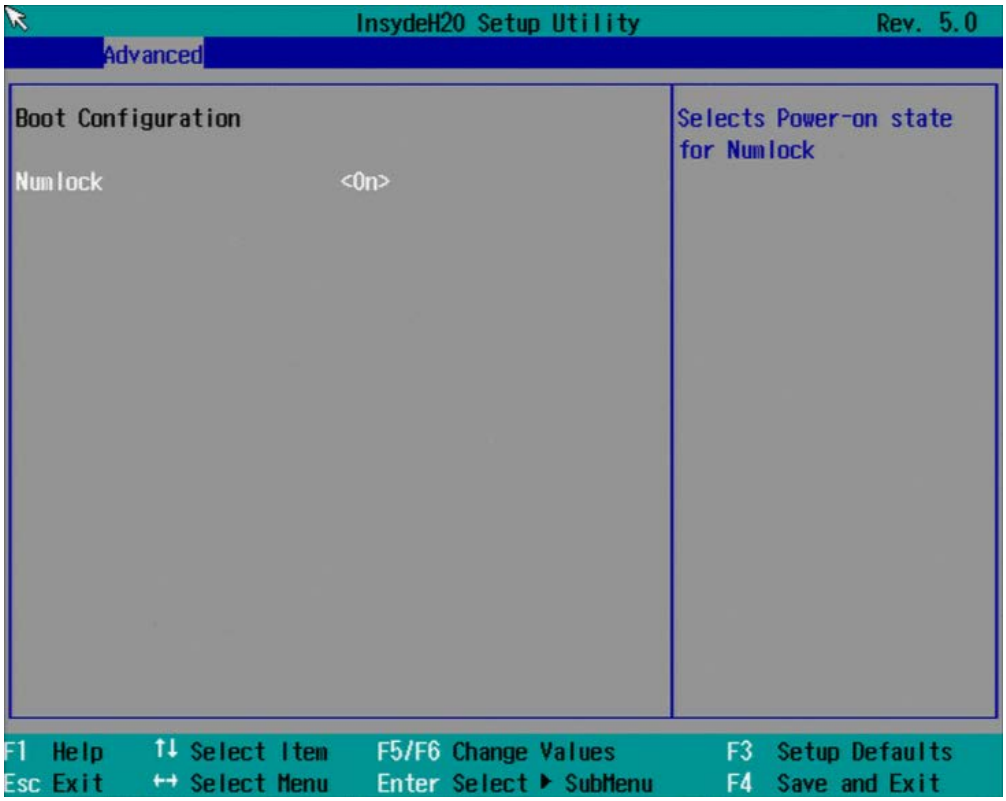


Figure 5-11 Advanced – Boot Configuration Menu

5.11.1 Advanced | Boot Configuration | Numlock

Numlock	
Specify the state of the keyboard Num Lock function at boot time.	
Off	Set Num Lock off.
On	Set Num Lock on.

5.12 Advanced | Peripheral Configuration

The Peripheral Configuration Screen controls options for the four serial ports available on the board and the Intel High Definition Audio (HDA) interface.

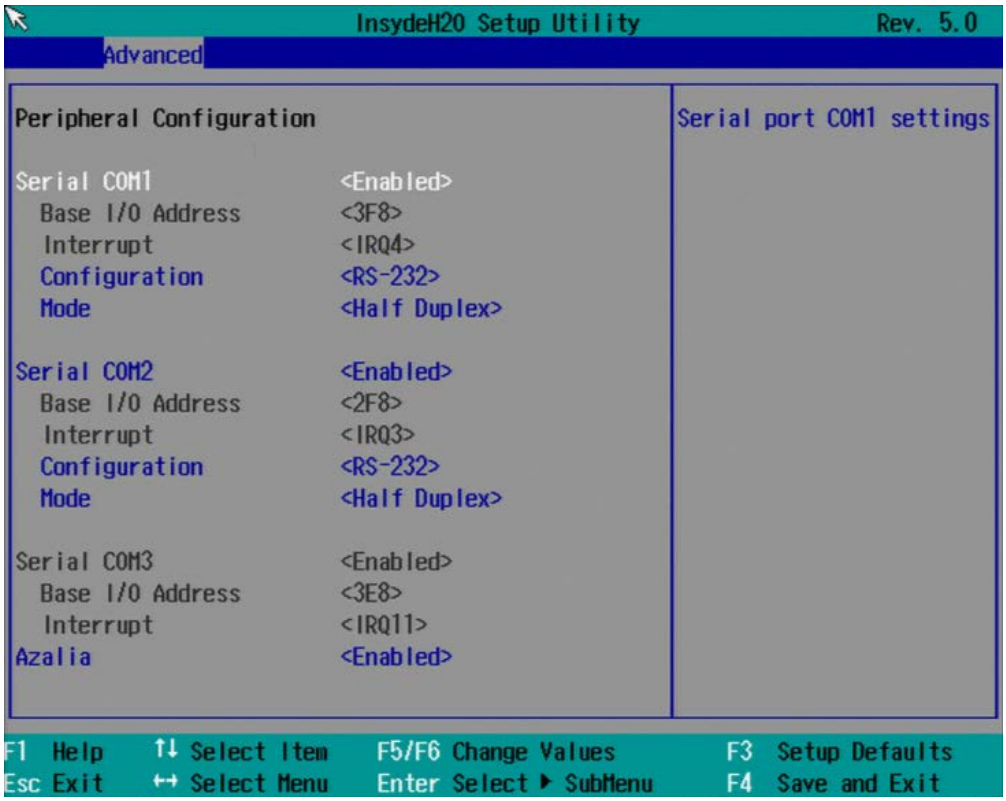


Figure 5-12 Advanced – Peripheral Configuration Menu

All serial ports support RS232 line levels. COM1 and COM2 optionally support RS-422/RS-485. The applicable options and default settings for each channel are detailed in Table 5-2.

Port Name	COM1 Serial Port	COM2 Serial Port	COM3 Serial Port
Port Status	Enabled	Enabled	Enabled
Base I/O Address	3F8	2F8	3E8
Interrupt	IRQ4	IRQ3	IRQ11
Configuration	RS-232	RS-232	
Mode	Full Duplex	Full Duplex	
Location	P2	P2	Front Panel

Table 5-2 Serial Port Default Configuration

5.12.1 Advanced | Peripheral Configuration | Serial COMx

Serial COMx	
Status of the channel.	
Disabled	Serial port is disabled
Enabled	Serial port is enabled

The COM3 serial port cannot be disabled. COM1 and COM2 serial ports are enabled by default

5.12.2 Advanced | Peripheral Configuration | Base I/O Address

Base I/O Address	
Report the base I/O port address for the channel.	
3F8	The base I/O address. See Table 5-2 for channel defaults
2F8	
3E8	

The serial port I/O addresses correspond to legacy COM1 – COM3 respectively and cannot be changed.

The serial port claims 8 bytes.

5.12.3 Advanced | Peripheral Configuration | Interrupt

Interrupt	
Set the interrupt request (IRQ) for the channel.	
IRQ3	The interrupt request. See Table 5-2 for channel defaults and options
IRQ4	
IRQ11	

COM port interrupt assignments cannot be changed.

Serial port interrupts are edge triggered.

5.12.4 Advanced | Peripheral Configuration | Configuration

Configuration	
Select the channel line drive level and I/O configuration.	
RS-232	Use RS-232 configuration
RS-485	Use RS-422/RS-485 configuration

5.12.5 Advanced | Peripheral Configuration | Mode

Mode	
Select whether a full duplex or half-duplex line is used by the channel.	
Full Duplex	Interface uses independent transmit and receive lines
Half Duplex	Transmit and receive interfaces use a shared line

5.12.6 Advanced | Peripheral Configuration | Slew Rate

NOTE: This option is only selectable when **Configuration** is set to RS-422/RS-485.

Slew Rate	
Set the slew rate for RS-422/RS-485 signal state changes.	
Slow	Slow state change
Fast	Fast state change

5.12.7 Advanced | Peripheral Configuration | Azalia

Azalia	
Enable the Intel High Definition Audio interface (HDA).	
Disabled	The HDA interface is disabled
Enabled	The HDA interface is enabled
Auto	The HDA interface will be enabled if a CODEC is detected

The HDA interface is implemented within the PCH. An audio CODEC connects the HDA interface to the optional line in, line out, microphone and headphone interfaces on P0.

5.13 Advanced | SATA Configuration | AHCI and RAID mode

This menu provides options for configuring the Serial ATA ports provided by the PCH.

The SATA controller can use either AHCI or legacy IDE programming interfaces; by default the AHCI mode is used. This section covers options provided when AHCI mode is enabled, including additional RAID extensions. Options available in IDE mode are detailed in Section 5.16.

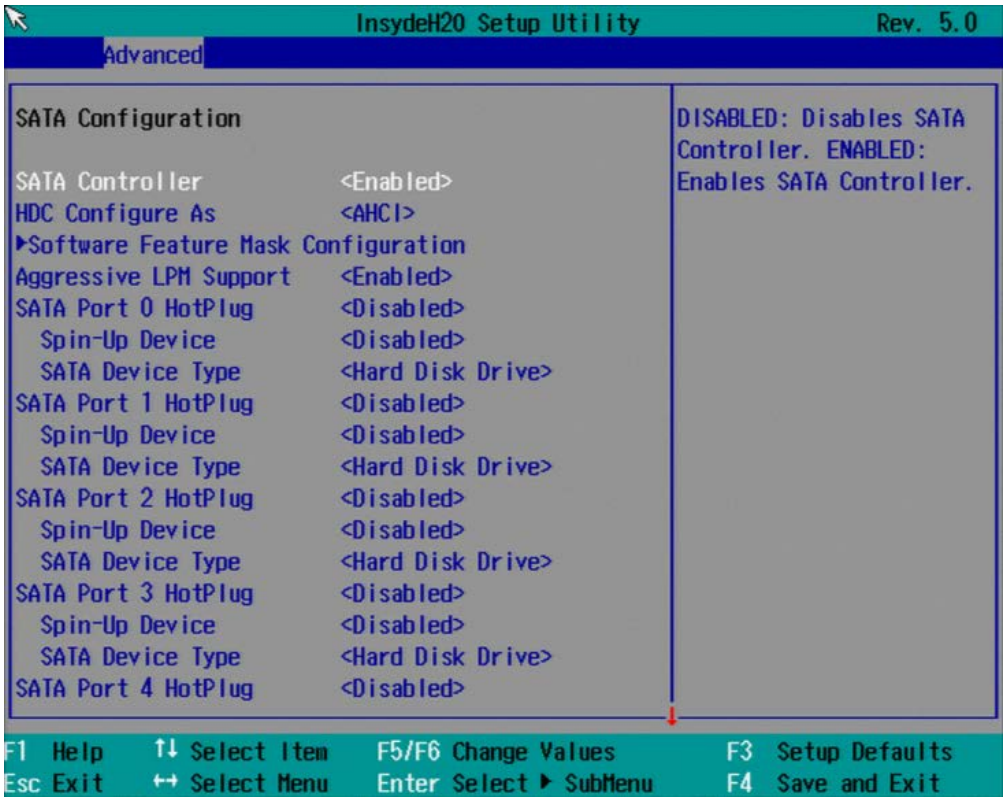


Figure 5-13 Advanced – SATA Configuration Menu

SATA port connectivity and the port's maximum operating speed are detailed in Table 5-3.

SATA Controller Port	Physical Connector	Maximum Speed
0	On-board HDD	SATA600
1	On-board CFast or NAND Flash drive	SATA600
2	Backplane P2	SATA300
3	Backplane P2	SATA300
4	Backplane P0 (optional)	SATA300
5	Backplane P0 (optional)	SATA300

Table 5-3 SATA Port Mapping

5.13.1 Advanced | SATA Configuration | SATA Controller

SATA Controller	
Disable the SATA controller.	
Disabled	The SATA controller is disabled
Enabled	The SATA controller is enabled

In systems that do not require fixed disk storage (HDD, SSD, etc.) the SATA controller can be disabled to save board power consumption.

5.13.2 Advanced | SATA Configuration | HDC Configured As

HDC Configured As	
Configure the SATA controller's programming interface.	
IDE	Legacy IDE programming interface (I/O based)
AHCI	High performance AHCI programming interface
RAID	RAID level 0, 1, 5 and 10 via the AHCI interface

The programming interface can affect both the interface performance and drive configurations supported by the board.

IDE mode is the lowest performance mode, however it is compatible with the legacy operating systems.

AHCI mode provides a high-performance programming interface. **AHCI** mode must be used with fast drives to obtain the maximum 3 Gbyte/s data throughput.

RAID mode utilizes the AHCI programming interface to provide high performance and /or data security.

Performance gains are achieved by sharing (striping) data across more than one drive, thus parallel data accesses can be performed via multiple SATA interfaces.

Security is achieved by duplicating (mirroring) data or parity information. This duplication will necessarily mean that the capacity of the RAID array will be less than the total of the constituent drives.

Table 5-4 describes the RAID modes supported by the PCH and the minimum drives required for an implementation of that configuration. Also provided is the equivalent capacity obtained when N physical drives are used.

RAID Level	Description	Minimum # Drives	Equivalent Capacity
0	High performance via data striping	N = 2	N
1	Data security via image mirroring	N = 2	N / 2
5	Performance and security via striped parity, rotated across drives	N = 3	N - 1
10	Maximum performance and security via striped RAID-1 blocks	N = 4	N / 2

Table 5-4 Supported RAID Modes

Selecting **AHCI** or **RAID** will reveal a number of additional options, these are described in Section 5.14.

When **RAID** mode is selected the PCI Device ID and Class Code of the SATA controller changes to indicate that it is a RAID controller.

NOTE: The Intel Rapid Storage Manager drivers are required to utilize RAID modes.

5.13.3 Advanced | SATA Configuration | Software Feature Mask Configuration

Software Feature Mask Configuration
Select which optional features will be supported by the AHCI or RAID BIOS

This option is available under **AHCI** or **RAID** modes.

5.13.4 Advanced | SATA Configuration | Aggressive LPM Support

Aggressive LPM Support	
Specify whether the SATA controller enables Support Aggressive Link Power Management (SALP).	
Disabled	The SATA controller does not advertised SALP.
Enabled	The SATA controller advertises SALP.

This option is available under **AHCI** or **RAID** modes.

5.13.5 Advanced | SATA Configuration | Alternate ID

Alternate ID	
Report a different PCI device ID when the SATA controller operates in RAID mode.	
Disabled	Use the same 0x8C0x PCI device ID in all modes
Enabled	Use 0x282x PCI device ID in RAID mode

This option is available under **RAID** mode only.

5.13.6 Advanced | SATA Configuration | SATA Port x HotPlug

SATA Port x Hot Plug	
Enable support for SATA hot-plug.	
Disabled	Hot-plug support disabled
Enabled	Hot-plug support enabled

This option is available under **AHCI** or **RAID** modes. Only the SATA ports routed via the backplane can support hot-plug, see Table 5-3.

5.13.7 Advanced | SATA Configuration | SATA Port x - Spin-Up Device

SATA Port x – Spin-Up Device	
Select whether SATA drives spin up in a staggered order.	
Disabled	Use staggered spin-up
Enabled	All interfaces power up immediately

This option is available under **AHCI** or **RAID** modes. Using staggered spin up reduces current surges when multiple drive motors start.

5.13.8 Advanced | SATA Configuration | SATA Port x - SATA Device Type

SATA Port x – SATA Device Type	
Specify the type of drive connected to the SATA port.	
Hard Disk Drive	Port connects to a hard disk drive (HDD)
Solid State Drive	Port connects to a solid state drive (SSD)

This option is available under **AHCI** or **RAID** modes.

5.13.9 Advanced | SATA Configuration | Serial ATA Port x

Serial ATA Port x	
Select drive-specific options for each of the SATA ports 0 – 7	
Not Installed	No drive attached to the SATA port
[drive name]	Identity of attached drive

When a drive is attached to the port, the drive model string (as reported by the drive) is displayed alongside the sub-menu option to assist with identification. SATA port connectivity is detailed in Table 5-3.

Pressing <**Enter**> will display a sub-menu containing port-specific options. See Section 5.15 for details of the port-specific options.

5.13.10 Advanced | SATA Configuration | SATA Port x

SATA Port x	
Specify the maximum interface speed for the SATA port.	
150	Limit the port to SATA150 (1.5 Gbits/s)
300	Limit the port to SATA300 (3 Gbits/s)
Auto	Use the maximum speed supported by the drive

5.14 Advanced | SATA Configuration | Software Feature Mask Configuration

This menu primarily provides options for configuring features implemented by the built-in AHCI and RAID BIOS extensions.

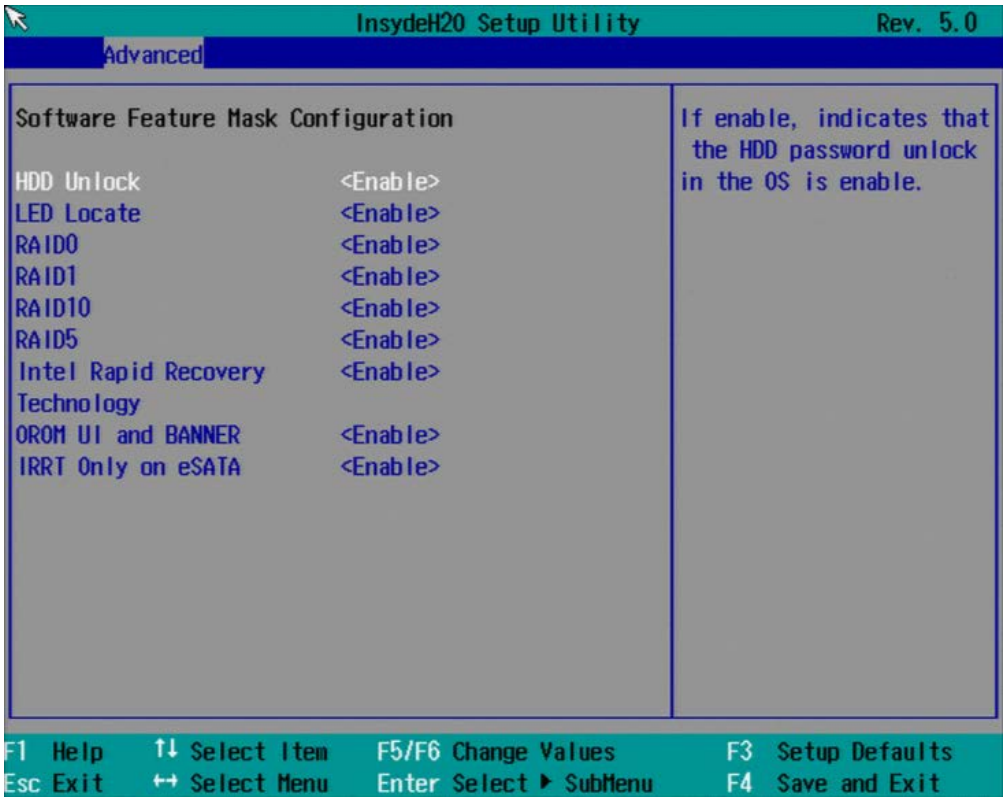


Figure 5-14 Advanced – Software Feature Mask Configuration Menu

5.14.1 Advanced | SATA Configuration | Software Feature Mask Configuration | HDD Unlock

HDD Unlock	
Indicate to the OS the requested status of HDD Password Unlock	
Disabled	HDD Password Unlock is enabled
Enable	HDD Password Unlock is disabled

This option is available under **AHCI** or **RAID** modes. When set to **Enabled** this option indicates to the OS driver that HDD Password Unlock should be left enabled.

NOTE: The VP B1x/msd does not implement the SGPIO interface.

5.14.2 Advanced | SATA Configuration | Software Feature Mask Configuration | LED Locate

LED Locate	
Enable support for LED Locate in AHCI or RAID modes.	
Disabled	LED Locate support is disabled.
Enable	LED Locate is enabled.

This option is available under **AHCI** or **RAID** modes. The chipset Serial GPIO (SGPIO) signals can provide per-port drive status indicators. When **Enabled** this option allows the OS driver to identify physical disk drives by flashing their status LED.

NOTE: The VP B1x/msd does not implement the SGPIO interface.

5.14.3 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID0

RAID0	
Enable support for RAID mode 0.	
Disabled	RAID mode 0 support disabled
Enabled	RAID mode 0 support enabled

RAID mode 0 provides high performance via data striping across two or more drives.

5.14.4 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID1

RAID1	
Enable support for RAID mode 1.	
Disabled	RAID mode 1 support disabled
Enabled	RAID mode 1 support enabled

RAID mode 1 provides data security by mirroring data across two or more drives.

5.14.5 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID10

RAID10	
Enable support for RAID mode 10.	
Disabled	RAID mode 10 support disabled
Enabled	RAID mode 10 support enabled

RAID mode 10 provides maximum performance and maximum data security by mirroring striped data blocks using four or more drives.

5.14.6 Advanced | IDE Configuration | Software Feature Mask Configuration | RAID5

RAID5	
Enable support for RAID mode 5.	
Disabled	RAID mode 5 support disabled
Enabled	RAID mode 5 support enabled

RAID mode 5 provides performance and data security using striped parity information that is rotated across three or more drives.

5.14.7 Advanced | IDE Configuration | Software Feature Mask Configuration | Intel Rapid Recovery Technology

Intel Rapid Recovery Technology	
Enable support for Intel Rapid Recovery Technology in the RAID BIOS.	
Disabled	Rapid Recovery Technology support disabled
Enabled	Rapid Recovery Technology support enabled

5.14.8 Advanced | IDE Configuration | Software Feature Mask Configuration | OPROM UI and BANNER

OPROM UI and BANNER	
Control when the RAID BIOS sign-on message is displayed.	
Disabled	The sign-on message is not displayed if all drives report a normal status
Enabled	The sign-on message is displayed for all boots

The sign-on message also gives access to the RAID BIOS Setup utility.

5.14.9 Advanced | IDE Configuration | Software Feature Mask Configuration | IRRT Only on eSATA

IRRT Only on eSATA	
Specify whether Intel Rapid Recovery Technology is limited to external SATA drives (eSATA).	
Disabled	RAID volumes can span internal and external SATA drives
Enabled	RAID volumes are restricted to external SATA drives

5.15 Advanced | SATA Configuration | Serial ATA Port x

When a drive is connected to one of the SATA ports additional Setup options become available.

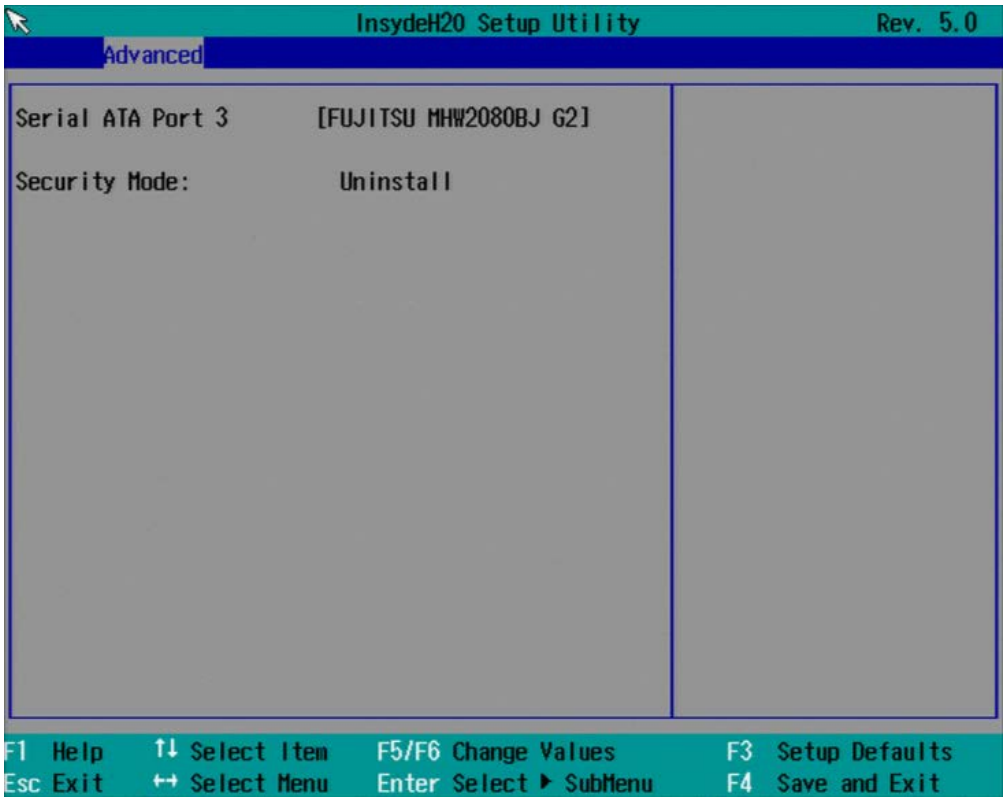


Figure 5-15 Advanced – Serial ATA Port x Menu

5.15.1 Advanced | SATA Configuration | SATA Port x | Security Mode

Security Mode	
Reports the status of drive security.	
Uninstall	Drive security not installed
Not Accessed	A HDD password has not been specified
Disable	Drive security is not supported
Lock	Drive password is locked
Unlock	Drive password is unlocked
Change	Drive password change is in progress

NOTE: The VP B1x/msd does not currently support drive security features.

5.16 Advanced | SATA Configuration | IDE Mode

When the SATA controller is configured for **IDE** mode, a reduced set of options are available. These options are described in Sections 5.13 and 5.15.

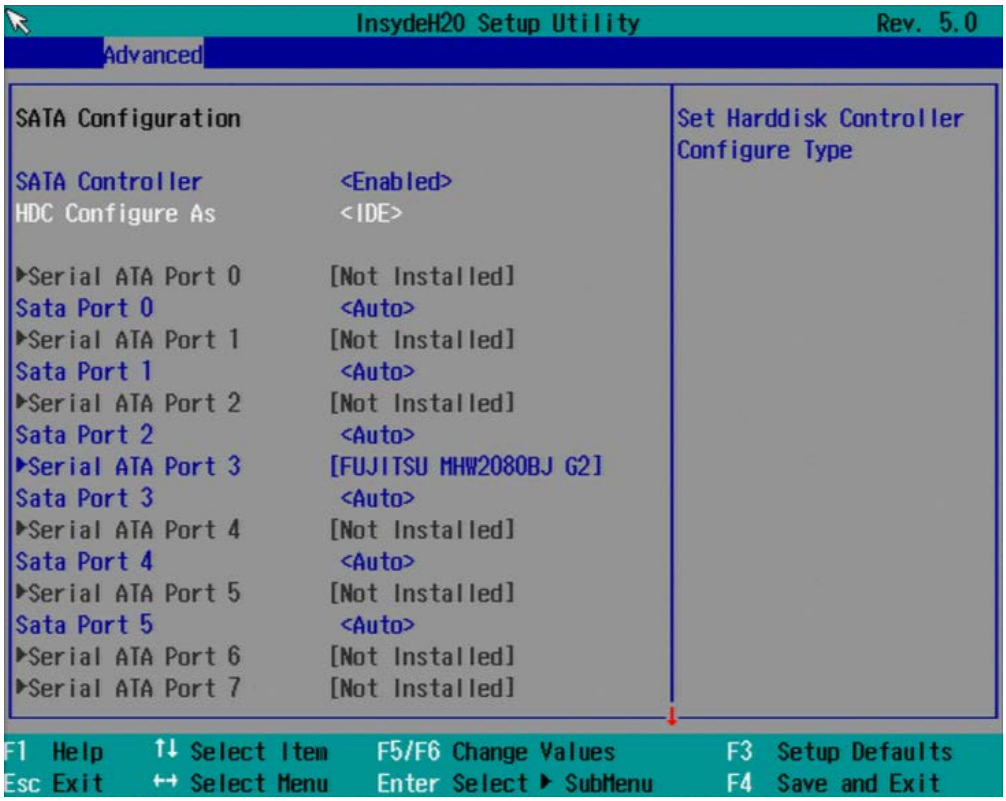


Figure 5-16 Advanced – IDE Mode Options

5.17 Advanced | Thermal Configuration

This menu provides options for configuring thermal and power related parameters. There are no user configurable options on this screen, only sub-menus.

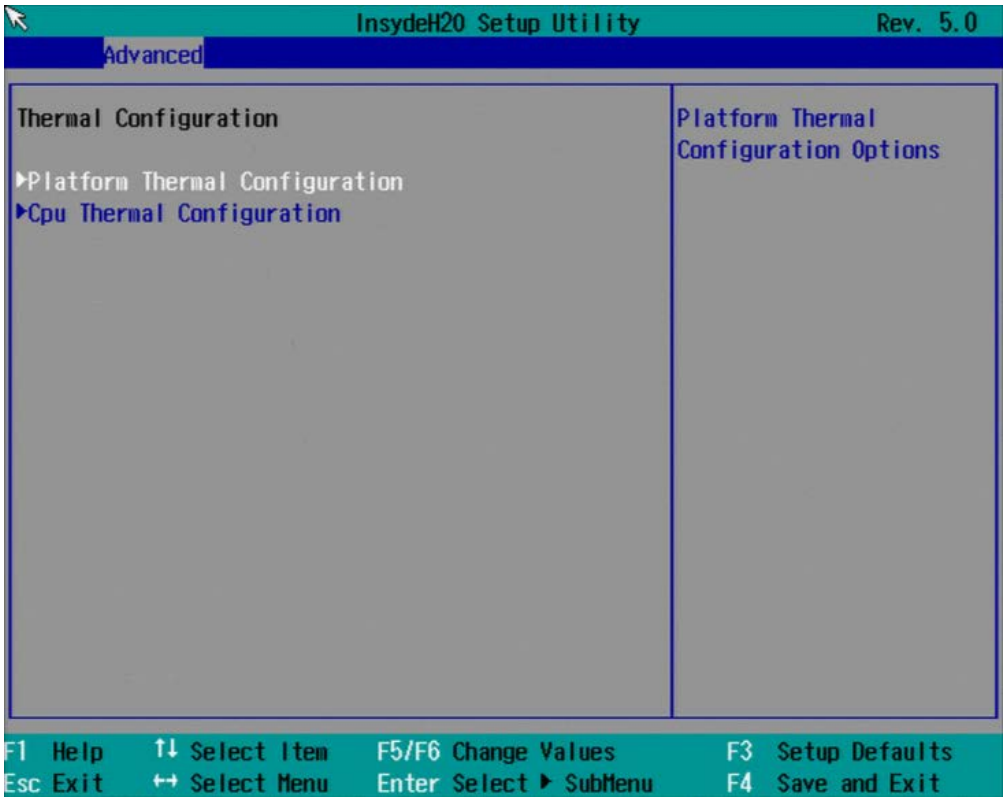


Figure 5-17 Advanced – Thermal Configuration Menu

5.17.1 Advanced | Thermal Configuration | Platform Thermal Configuration

Platform Thermal Configuration
Configure thermal options for the platform.

The options available through this sub-menu control how an operating system will interact with the thermal monitoring hardware using ACPI.

The Platform Thermal Configuration options are detailed in Section 5.18.

5.17.2 Advanced | Thermal Configuration | Cpu Thermal Configuration

Cpu Thermal Configuration
Configure thermal options specific to the CPU.

The options available through this sub-menu control the reporting of the CPU temperature and the operation of thermal control circuits.

The CPU Thermal Configuration options are detailed in Section 5.20.

5.18 Advanced | Thermal Configuration | Platform Thermal Configuration

This menu provides options for configuring the thermal properties of the platform such as shutdown temperatures and various alerts.

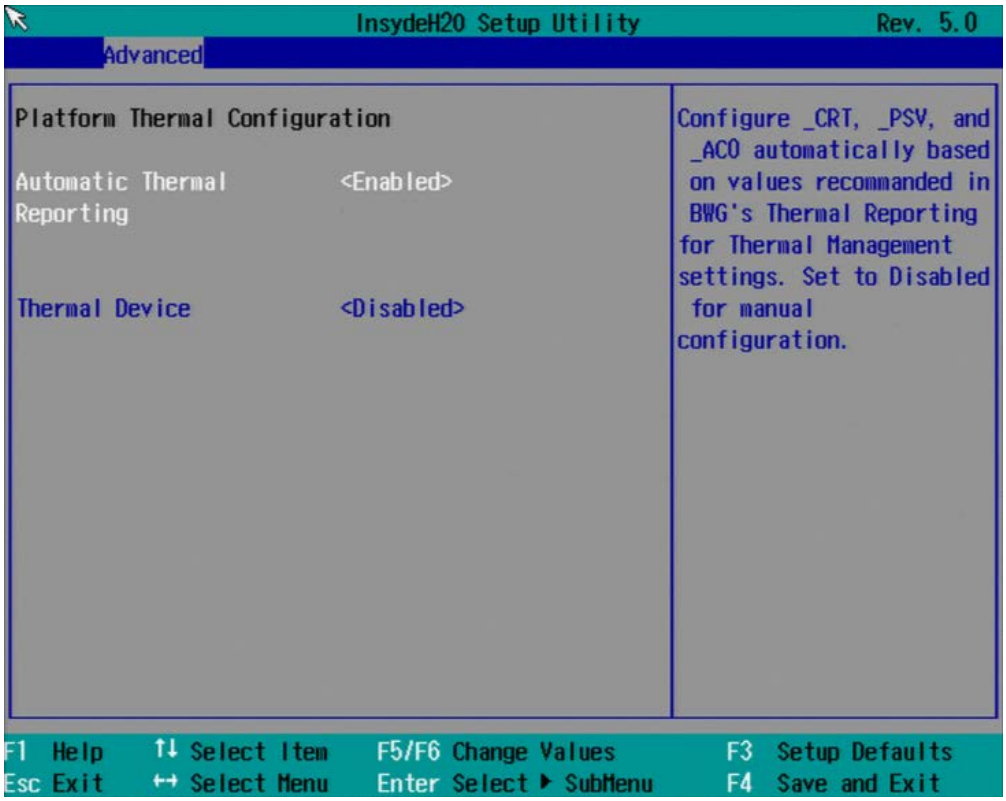


Figure 5-18 Advanced – Platform Thermal Configuration Menu

5.18.1 Advanced | Thermal Configuration | Platform Thermal Configuration | Automatic Thermal Reporting

Automatic Thermal Reporting	
Use BIOS selected thermal thresholds, or allow manual selection.	
Disabled	Thermal thresholds can be manually adjusted
Enabled	Use BIOS selected thermal thresholds

When set to Enabled the BIOS will set the ACPI Critical Thermal Trip Point and Passive Thermal Trip Point temperatures using optimal values defined by Intel.

If this option is set to Disabled, two additional fields are displayed allowing manual selection of the Trip Point temperatures. Section 5.19 describes these options in detail.

5.18.2 Advanced | Thermal Configuration | Platform Thermal Configuration | Thermal Device

Thermal Device	
Control access to the PCH Thermal Sensor registers.	
Disabled	Disable access to the registers
Enabled	Enable access to the registers

The Thermal sensor registers are implemented by the PCH as PCI device 31, function 6.

5.18.3 Advanced | Thermal Configuration | Platform Thermal Configuration | Alert Enable Lock

NOTE: This option is only available when **Thermal Device** is set to Enabled.

Alert Enable Lock	
Lock the BIOS assigned PCH and DIMM thermal alert settings.	
Disabled	Thermal alert settings can be changed by the OS or application
Enabled	Thermal alert settings are locked until reset

When this option is set to **Enabled** the BIOS assigned thermal alert (enable/disable) setting for the DIMM and PCH sensors is locked.

5.19 Advanced | Thermal Configuration | Platform Thermal Configuration - Additional Options

When the **Automatic Thermal Reporting** option is set to Disabled, two additional options are displayed allowing the user to manually configure the ACPI thermal trip points.

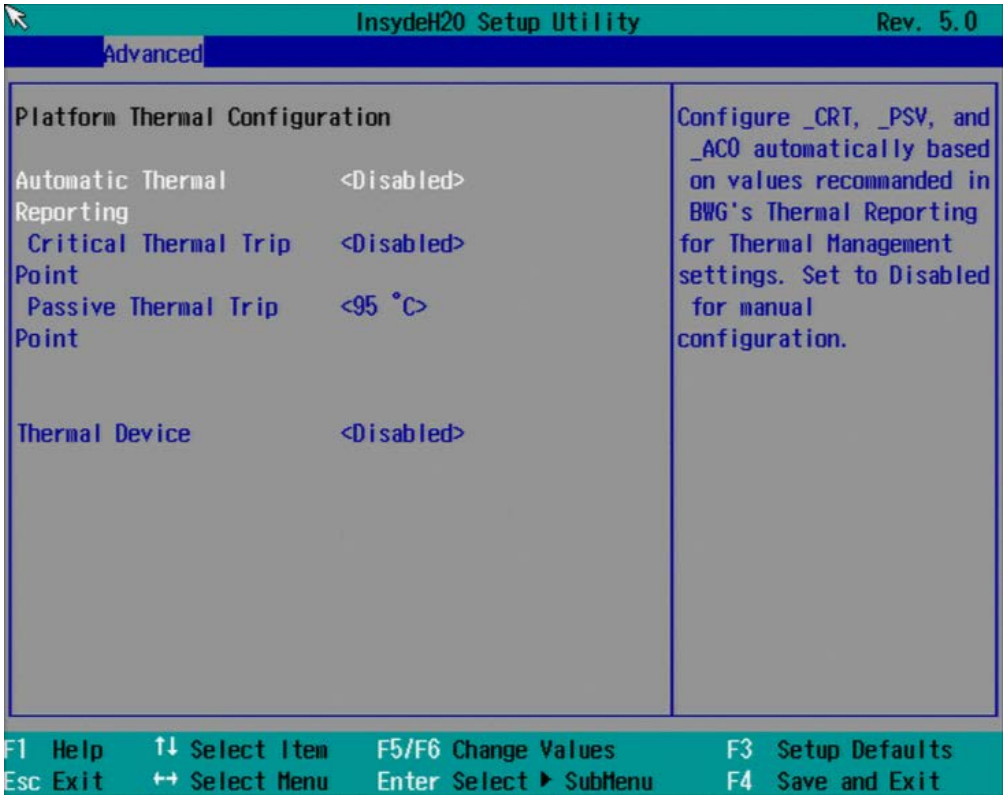


Figure 5-19 Advanced – Platform Thermal Configuration Menu – Additional Options

5.19.1 Advanced | Thermal Configuration | Platform Thermal Configuration | Critical Thermal Trip Point

Critical Thermal Trip Point	Caution
Set the temperature at which an ACPI operating system will shutdown	
Disabled	ACPI critical reporting disabled
15 °C	ACPI Critical Trip Point
23 °C	
31 °C	
39 °C	
47 °C	
55 °C	
63 °C	
71 °C	
79 °C	
87 °C	
95 °C	
103 °C	
111 °C	
119 °C	
127 °C	

The CPU includes a catastrophic shutdown detector that will halt the CPU if the temperature reaches a level that could result in damage. Using ACPI an operating system can be instructed to perform an orderly shutdown if the CPU is in danger of reaching the catastrophic threshold.

This option sets the temperature at which the request to shut down will be sent to the operating system. If the system has poor cooling, a lower threshold may be required in order to give sufficient time for shutdown.

WARNING: Adjusting this option without a full understanding of the thermal characteristics of the system can result in less reliable operation.

5.19.2 Advanced | Thermal Configuration | Platform Thermal Configuration | Passive Thermal Trip Point

Passive Thermal Trip Point	Caution
Set the temperature at which the CPU will begin throttling.	
Disabled	ACPI throttling disabled
15 °C	CPU throttle-on temperature
23 °C	
31 °C	
39 °C	
47 °C	
55 °C	
63 °C	
71 °C	
79 °C	
87 °C	
95 °C	
103 °C	
111 °C	
119 °C	

In order to prevent the CPU reaching the Shutdown Temperature (see Section 5.19.1) software-driven performance throttling can be used to reduce the CPU temperature to within acceptable levels.

This option sets the temperature at which an ACPI operating system will engage throttling mechanisms. Throttling will remain enabled until the CPU temperature drops below this threshold.

WARNING: Throttling should not activate under normal use with the default settings and adequate cooling.

WARNING: Adjusting this option without a full understanding of the thermal characteristics of the system can result in less reliable operation.

5.20 Advanced | Thermal Configuration | CPU Thermal Configuration

This menu provides options for configuring settings relating to the CPU thermal sensor and temperature event reporting.

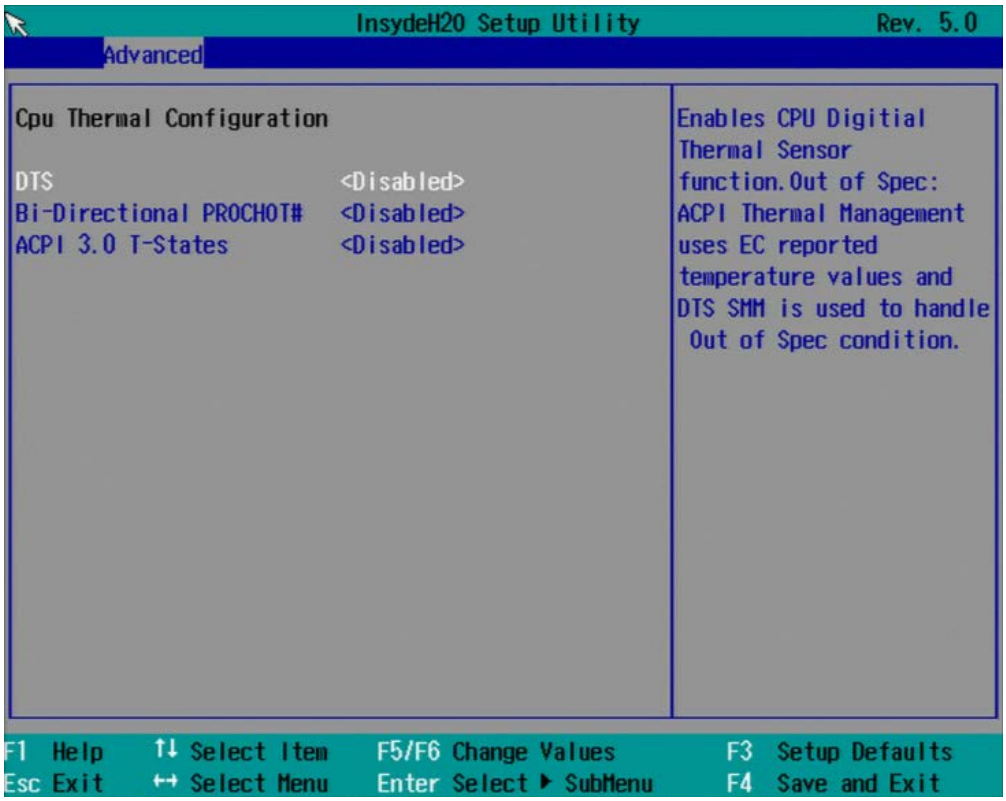


Figure 5-20 Advanced – CPU Thermal Configuration Menu

5.20.1 Advanced | Thermal Configuration | CPU Thermal Configuration | DTS

DTS	
Controls how the CPU Digital Thermal Sensor (DTS) is reported via ACPI.	
Disabled	The DTS is disabled
Enabled	The DTS is enabled and temperature readings are reported
Critical Reporting	Only activation of the Critical Temperature Status are reported

In addition to the per-core DTS, the CPU has a package thermal sensor that reports the maximum value of the individual core sensors. This value is used by the ACPI code.

This option controls the values that are reported via the **`ACPI Thermal Zone _TMP`** method. The VP B1x/msd implements two thermal zones TZ00 (package) and TZ01 (CPU). Table 5-5 describes the temperature readings that will be reported for each setting of the DTS option.

DTS Setting	TZ00 _TMP Reports	TZ01 _TMP Reports
Disabled	Constant 26.8 ^{0}C	Constant 28.8 ^{0}C
Enabled	DTS reading in ^{0}C	DTS reading in ^{0}C
Critical Reporting	27.8^{o}C until out-of-spec, then 105^{o}C	29.8^{o}C until out-of-spec, then 105^{o}C

Table 5-5 ACPI Thermal Zone temperature readings for different DTS settings

When set to **Critical Reporting**, a constant value is returned via ACPI until the package temperature reaches the Critical Temperature, and then a value of 105^{o}C is reported.

5.20.2 Advanced | Thermal Configuration | Bi-Directional PROCHOT#

Bi-Directional PROCHOT#	
Enable PROCHOT# to be driven by an external device.	
Disabled	PROCHOT# is an output
Enabled	PROCHOT# is bi-directional

The **PROCHOT#** signal indicates when the thermal control circuits are active. By default **PROCHOT#** is an output and indicates that the CPU has reached the critical threshold. If enabled as a bi-directional signal, external devices can enable the thermal control circuit by driving **PROCHOT#**.

When **PROCHOT#** is configured for bidirectional operation, the CPU will immediately throttle to its lowest operating frequency if the thermal control circuit activates.

NOTE: This VP B1x/msd does not use bidirectional **PROCHOT#**.

5.20.3 Advanced | Thermal Configuration | CPU Thermal Configuration | ACPI 3.0 T-States

ACPI 3.0 T-States	
Enable CPU throttling states to be reported via ACPI.	
Disabled	T-states are not reported
Enabled	T-states are reported via ACPI

The ACPI 3.0 specification introduced new Control Methods allowing operating systems to move the processor to a defined throttling state. When this option is enabled, details of the supported throttling states (T-states) will be included in the ACPI 3.0 tables.

5.21 Advanced | Video Configuration

This menu provides options for configuring the Internal Graphics Device (IGD).

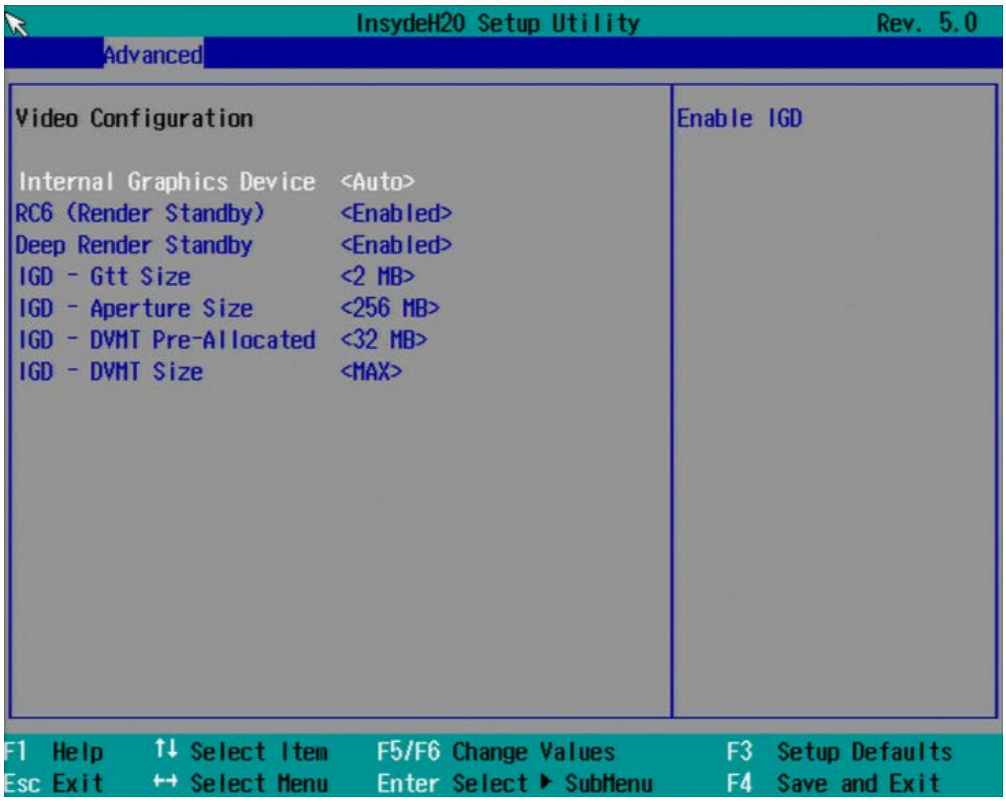


Figure 5-21 Advanced – Video Configuration Menu

5.21.1 Advanced | Video Configuration | Internal Graphic Device | Internal Graphics Device

Internal Graphics Device	
Enable or disable the Internal Graphics Device (IGD).	
Auto	Enable IGD only if it is the default graphics controller
Enabled	Always enable the IGD
Disabled	Always disable the IGD

If an external graphics controller is fitted and the IGD is required as a secondary display device then this option should be set to **Enabled**.

5.21.2 Advanced | Video Configuration | Internal Graphic Device | RC6 (Render Standby)

RC6 (Render Standby)	
Allow the IGD render engine to enter a low power state when idle.	
Disabled	RC6 low power transitions disabled
Enabled	RC6 low power transitions enabled

The IGD can reduce power consumption (and temperature) by entering a low power state when idle. The disadvantage of this setting is increased latency when exiting the low power state.

5.21.3 Advanced | Video Configuration | Internal Graphic Device | Deep Render Standby

Deep Render Standby	
Allow the IGD render engine to enter a deeper low power state when idle (RC6+).	
Disabled	RC6+ low power transitions disabled
Enabled	RC6+ low power transitions enabled

The IGD can reduce power consumption (and temperature) by entering a low power state when idle. The disadvantage of this setting is increased latency when exiting the low power state.

5.21.4 Advanced | Video Configuration | Internal Graphic Device | IGD – Gtt Size

IGD – Gtt Size	
Set the size of system memory reserved for the Graphics Translation Table (GTT).	
1 MB	Graphics Translation Table size
2 MB	

The Graphics Translation Table (GTT) is used by the graphics engine when mapping memory accesses between video memory addresses and physical system memory.

5.21.5 Advanced | Video Configuration | Internal Graphic Device | IGD – Aperture Size

IGD – Aperture Size	
Set the size of the PCI address space decoded by the Internal Graphics Device.	
128 MB	PCI address aperture size
256 MB	
512 MB	

Accesses to the IGD aperture are mapped via the GTT onto physical system memory. Increasing the aperture size reduces the amount of physical memory available to 32-bit operating systems.

5.21.6 Advanced | Video Configuration | Internal Graphic Device | IGD – DVMT Pre Allocated

IGD – DVMT Pre Allocated	
Select the size of pre-allocated Graphics Memory for the Internal Graphics Device (IGD).	
0 MB	Pre-allocated graphics memory size
32 MB	
64 MB	
96 MB	
128 MB	
160 MB	
192 MB	
224 MB	
256 MB	
288 MB	
320 MB	
352 MB	
384 MB	
416 MB	
448 MB	
480 MB	
512 MB	
1024 MB	

The Integrated Graphics Device (IGD) supports Dynamic Video Memory Technology (DVMT). This mechanism allows the IGD to dynamically allocate memory from the operating system based on active requirements, rather than pre-allocating a larger block during PCI resource allocation.

The small, pre-allocated memory block is accessed through the IGD PCI base address registers and hidden from operating systems using the chipset memory configuration registers. Dynamically allocated memory is managed by the video driver and is allocated directly from the operating system's memory pool.

5.21.7 Advanced | Video Configuration | Internal Graphic Device | IGD – DVMT Size

IGD – DVMT Size	
Set maximum memory size that can be allocated by a DVMT driver.	
128 MB	Maximum graphics memory size allocated through DVTM.
256 MB	
MAX	Allocated memory size is determined by the operating system and driver

This option sets the maximum memory size that can be allocated from an operating system by a Dynamic Video Memory Technology (DVMT) video driver.

5.22 Advanced | USB Configuration

This menu provides options for configuring the board's USB interfaces. The VP B1x/msd supports both EHCI (USB 2.0 and USB 1.1) and XHCI (USB 3.0).

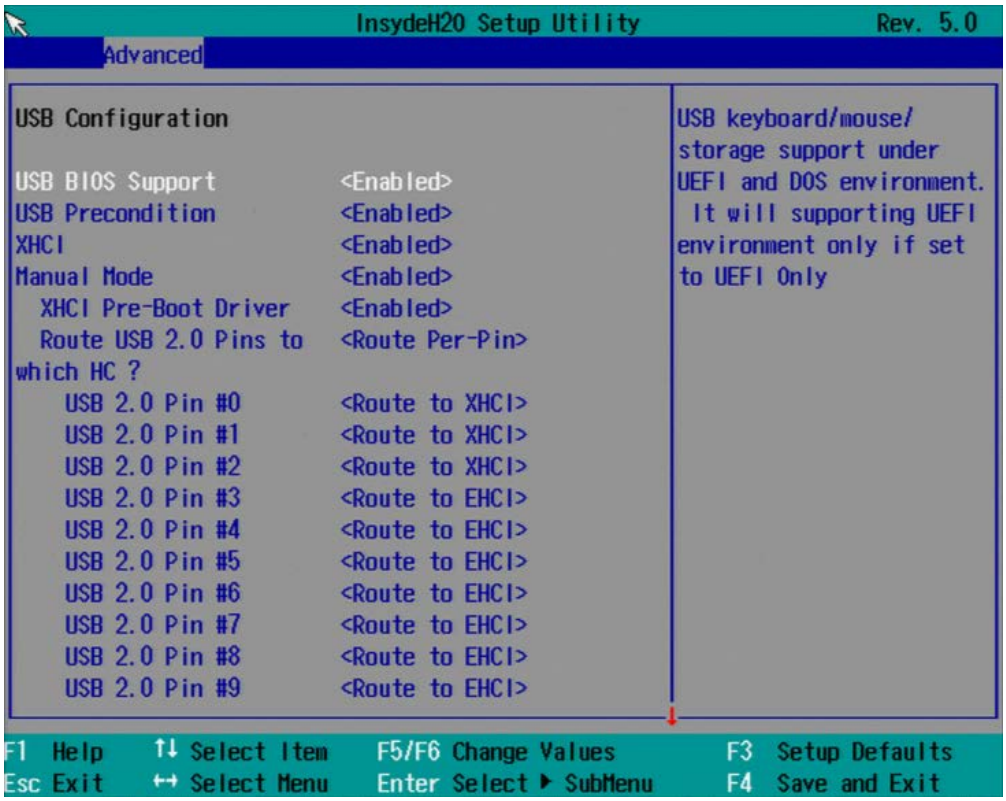


Figure 5-22 Advanced – USB Configuration Menu

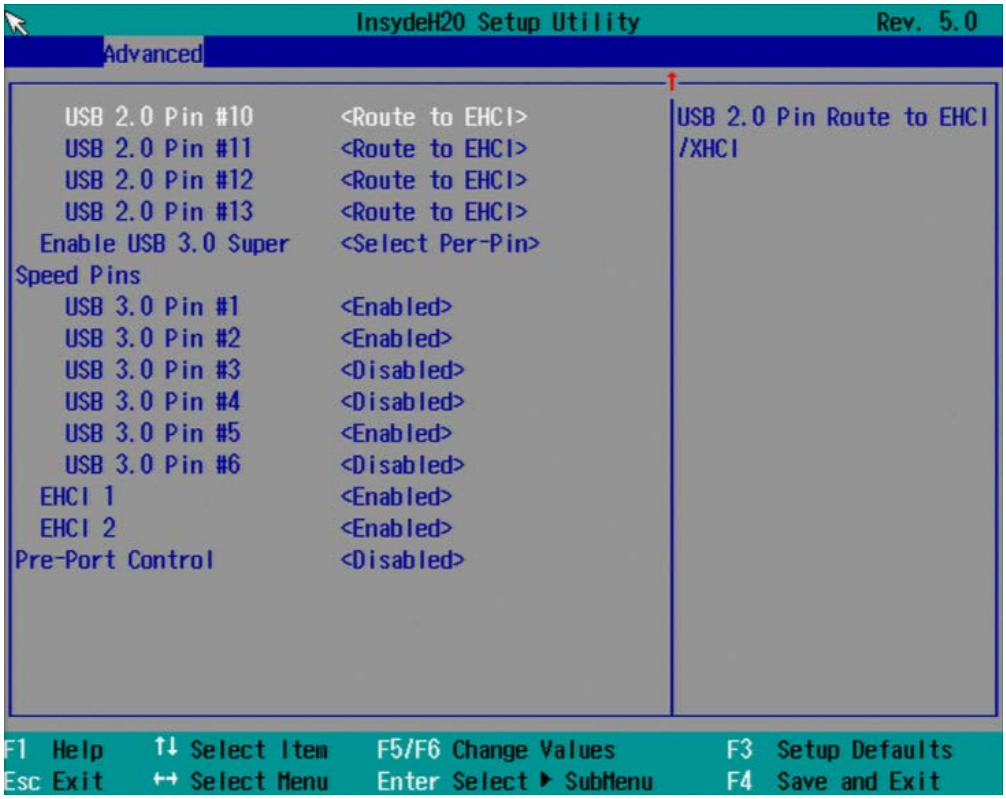


Figure 5-23 Advanced – USB Configuration Menu

USB 3.0 connectors contain both a USB3.0 and USB2.0 interfaces, but only one interface can be used by the attached device.

EHCI Pin	XHCI Pin	Board Location
0	1	Front Panel P4 (optional)
1	2	Front Panel P5 (optional)
2	5	Backplane P0
4		Backplane P0 (optional)
5		Backplane P0 (optional)
8		Backplane P2
9		Front Panel J1
10		Backplane P0
11		Front Panel J1
12		Front Panel J1 (optional)

Table 5-6 USB Pin Use on VP B1x/msd

5.22.1 Advanced | USB Configuration | USB BIOS Support

USB BIOS Support	
Enable legacy support for USB peripherals.	
Disabled	Legacy support disabled
Enabled	Legacy support enabled
UEFI Only	Legacy support only available when booting in UEFI mode

USB legacy support is required by operating systems that do not include native USB drivers.

When USB legacy support is enabled the BIOS will provide translation between USB device protocols and legacy I/O ports and BIOS interrupt services. USB legacy support operates transparently under System Management Mode (SMM) and therefore will represent a small CPU load.

Emulated Device	BIOS Interrupt service	I/O Ports	Interrupt Request
PS/2 Keyboard	INT 0x16	0x60 / 0x64	IRQ 1
PS/2 Mouse (aux device)	N/A	0x60 / 0x64	IRQ 12
Floppy Disk Drive	INT 0x13	0x3F0 – 0x3F7	IRQ 6
Hard Disk Drive	INT 0x13	0x1F0 – 0x1F7	IRQ 14

Table 5-7 USB Legacy Device Emulation

5.22.2 Advanced | USB Configuration | XHCI Pre-Boot Driver

XHCI Pre-Boot Driver	
Enable the XHCI (USB 3.0) pre-boot driver	
Disabled	XHCI pre-boot support disabled
Enabled	XHCI pre-boot support enabled

When set to **Enabled** the BIOS supports booting at USB 3.0 speeds from compatible devices attached to a USB 3.0 capable port (see **XHCI** and **HS Port Switch x** below).

NOTE: The XHCI pre-boot driver is only applicable to UEFI boot.

5.22.3 Advanced | USB Configuration | XHCI

XHCI	
Configure the level of XHCI (USB 3.0) support provided by the BIOS.	
Disabled	USB 3.0 support disabled, all ports use USB 2.0
Enabled	USB 3.0 support enabled on all supported ports
Auto	USB 3.0 enabled, port rerouting by OS supported
Smart Auto	USB 3.0 enabled, port rerouting by pre-boot firmware and OS supported

If the **XHCI Pre-Boot Driver** option is set to **Enabled** this option defaults to **Smart Auto**, otherwise it defaults to **Auto** and the Smart Auto option is not available.

When port rerouting is enabled the operating system or pre-boot firmware (**Smart Auto** only) can switch ports to the XHCI (USB 3.0) controller.

5.22.4 Advanced | USB Configuration | XHCI Streams

NOTE: This option is only displayed when XHCI support is enabled.

XHCI Streams	
Disable XHCI controller support for streams.	
Disabled	Set primary stream array size to zero
Enabled	Primary stream array size is unchanged (chipset default)

5.22.5 Advanced | USB Configuration | EHCI 1

EHCI 1	
Enable the first USB EHCI device, which implements USB ports 0 – 7.	
Disabled	EHCI1 is disabled
Enabled	EHCI1 is enabled

When set to **Disabled**, the USB Enhanced Host Controller Interface ports 0 to 7 will be disabled.

CAUTION: The VP B1x/msd requires USB for keyboard operation. Disabling both **EHCI 1** and **EHCI 2** will disable the keyboard and prevent further access to the Setup utility. If this occurs, the Load Optimal Defaults switch can be used to restore the board to factory settings. Refer to the board's Technical Reference Manual for further details.

5.22.6 Advanced | USB Configuration | EHCI 2

EHCI 2	
Enable the second USB EHCI device, which implements USB ports 8 – 13.	
Disabled	EHCI 2 is disabled
Enabled	EHCI 2 is enabled

When set to **Disabled**, the USB Enhanced Host Controller Interface ports 8 to 13 will be disabled.

5.22.7 Advanced | USB Configuration | Per-Port Control

Per-Port Control	
Allow control of USB ports on a per-port basis.	
Disabled	Per-port control is disabled
Enabled	Per-port control is enabled

When this option is set to **Enabled** a further 14 Setup options are displayed, one for each USB port. See Section 5.22.8 for further details.

5.22.8 Advanced | USB Configuration | Usb Portx

NOTE: These options are only displayed when Per-Port Control is set to **Enabled**.

Usb Portx	
Disable USB ports on a per-port basis.	
Disabled	Port is disabled
Enabled	Port is enabled

There are 14 USB ports implemented through two EHCI devices. The USB port use on the VP B1x/msd is detailed in Table 5-6.

5.23 Advanced | Chipset Configuration

This menu provides options for configuring various features of the PCH.

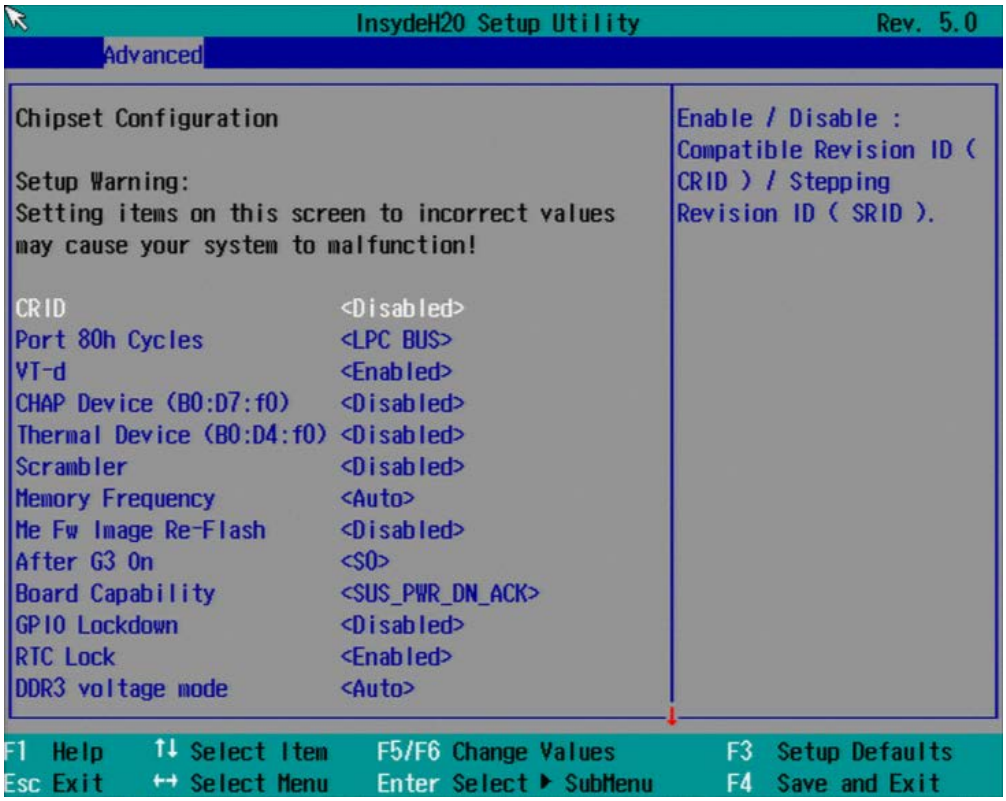


Figure 5-24 Advanced – Chipset Configuration Menu

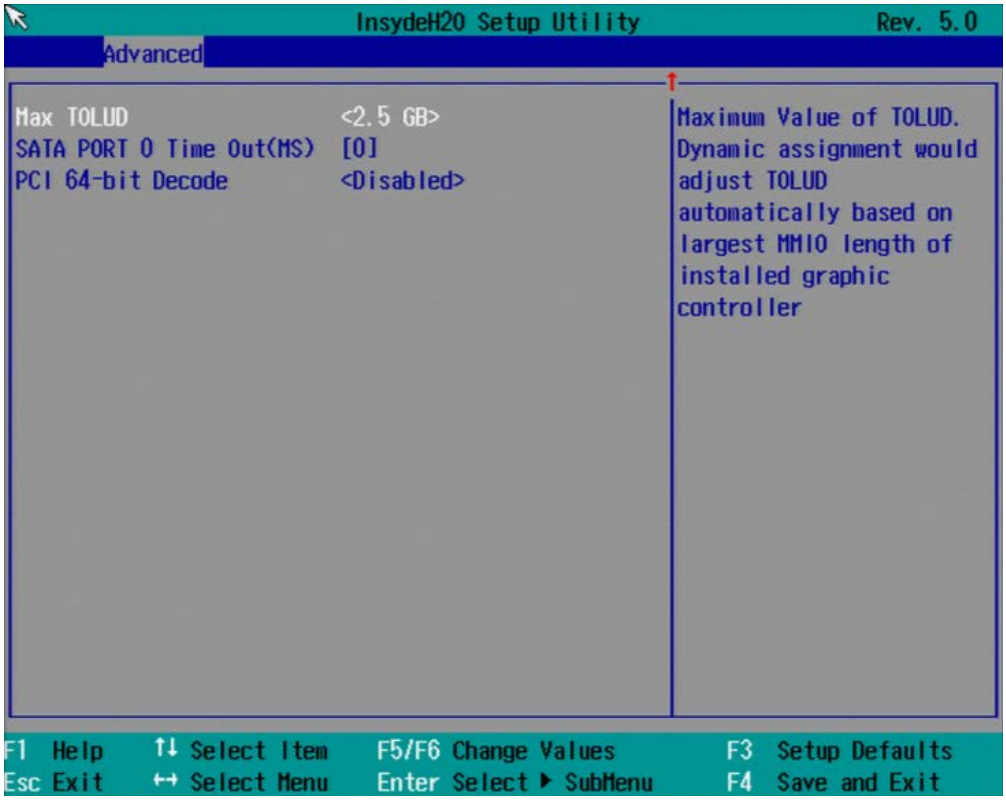


Figure 5-25 Advanced – Chipset Configuration Menu (Continued)

5.23.1 Advanced | Chipset Configuration | CRID

CRID	
Enable Compatible Revision and stepping Ids (CRID).	
Disabled	Compatible IDs are disabled
Enabled	Compatible IDs are enabled

For compatibility with older operating system drivers, the PCH can be configured to report Compatible Revision ID (CRID) and Compatible Stepping ID (CSID).

5.23.2 Advanced | Chipset Configuration | Port 80h Cycles

Port 80h Cycles	
Specify where accesses to I/O Port 0x80 are routed.	
LPC BUS	Port 0x80 accesses go to the LPC bus
PCI BUS	Port 0x80 accesses go to the PCI bus

The BIOS and certain operating systems report their progress via Port 0x80 accesses.

5.23.3 Advanced | Chipset Configuration | VT-d

VT-d	
Enable Virtualization Technology for Directed I/O	
Disabled	VT-d disabled
Enabled	VT-d enabled

Intel Virtualization Technology for Directed I/O (**VT-d**) provides a mechanism for virtual machines to gain direct access to the PCH hardware.

5.23.4 Advanced | Chipset Configuration | CHAP DEVICE (B0:D7:F0)

CHAP DEVICE (B0:D7:F0)	Caution
This option is provided for factory debug purposes and must not be changed.	
Disabled	PCI bus 0, device 7 (CHAP) disabled
Enabled	PCI bus 0, device 7 (CHAP) enabled

5.23.5 Advanced | Chipset Configuration | Thermal Device (B0:D4:F0)

Thermal Device (B0:D4:F0)	Caution
This option is provided for factory debug purposes and must not be changed.	
Disabled	PCI bus 0, device 4 disabled
Enabled	PCI bus 0, device 4 enabled

5.23.6 Advanced | Chipset Configuration | Scrambler

Scrambler	
Enable scrambling and descrambling of data sent over the link between the CPU cores and the memory controller.	
Disabled	Scrambler disabled
Enabled	Scrambler enabled

5.23.7 Advanced | Chipset Configuration | Memory Frequency

Memory Frequency	Caution
Set the memory bus frequency.	
Auto	BIOS sets optimal memory bus frequency
1067	Select fixed memory bus frequency
1200	
1333	
1400	
1600	
1800	
1867	
2000	
2133	
2200	
2400	
2600	
2667	

The memory bus frequency selected by the **Auto** setting depends on the fitted CPU type and DRAM speed. The value will be chosen by the BIOS as the maximum supported by the CPU + DRAM combination. The memory bus frequency can be reduced to save power.

WARNING: Increasing the memory bus frequency above the DRAM rated speed will result in unreliable operation.

5.23.8 Advanced | Chipset Configuration | Me Fw Image Re-Flash

Me Fw Image Re-Flash	
Enable downgrading of the Management Engine (ME) firmware	
Disabled	ME firmware downgrade disabled
Enabled	ME firmware downgrade enabled

Normally downgrading of the Management Engine firmware is not allowed.

5.23.9 Advanced | Chipset Configuration | After G3 On

After G3 On	
Specify the board behavior when power is re-applied after a power failure.	
Power On (S0)	Power-on the system when power is restored
Power Off (S5)	Keep the system powered off when power is restored
Return to last power state	Go to the power state before power failure

If main power is disconnected from the board, rather than going through an orderly shutdown (to ACPI power-state S5), this option specifies the board behavior when power is re-applied.

This option is intended for use with equipment operating unattended and specifies how the board should respond after a blackout or brownout event.

5.23.10 Advanced | Chipset Configuration | Board Capability

Board Capability	
Specify how the board manages the Suspend power well (SUS) in system low power states	
SUS_PWR_DN_ACK	The PCH (and ME) manage SUS power
DeepSx	SUS power is controlled automatically by Deep S4/S5 transitions

When **DeepSx** is selected an additional option is displayed for selecting the Deep S4/S5 policy.

5.23.11 Advanced | Chipset Configuration | DeepSx Power Policies

DeepSx Power Policies	
Select which system power states will support automatic SUS power control	
Disable	Don't allow automatic SUS power control
Enable In S5	Power states supporting automatic SUS control
Enable In S4-S5	
Enable In S3-S4-S5	

5.23.12 Advanced | Chipset Configuration | GPIO Lockdown

GPIO Lockdown	
Configure the PCH GPIO registers as read-only	
Disabled	GPIO registers are R/W.
Enabled	GPIO registers are RO

5.23.13 Advanced | Chipset Configuration | RTC Lock

RTC Lock	
Prevent access to bytes 0x38 – 0x3F in the upper and lower 128 byte bank of the CMOS NVRAM.	
Disabled	Access to the range is allowed
Enabled	Read and Write access to the 0x38 – 0x3F range is ignored

5.23.14 Advanced | Chipset Configuration | DDR3 voltage mode

DDR3 voltage mode	Caution
Select the DDR3 DRAM operating voltage.	
Auto	Select the setting based on Serial Presence data

5.23.15 Advanced | Chipset Configuration | Max TOLUD

Max TOLUD	Caution
Specify the amount of DRAM available below 4GB.	
Dynamic	TOLUD is adjusted automatically
1.00 GB	Configure fixed value for TOLUD
1.25 GB	
1.50 GB	
1.75 GB	
2.00 GB	
2.25 GB	
2.50 GB	
2.75 GB	
3.00 GB	
3.25 GB	

TOLUD (Top Of Low User DRAM) is a chipset parameter that specifies the amount of DRAM available below the 4 Gbyte threshold. Addresses between TOLUD and 4GB are required for chipset resources and PCI devices.

When set to **Dynamic** the value of TOLUD will be set based on the available free memory after PCI resources have been allocated. Selecting a fixed size will use that value for TOLUD.

WARNING: If a fixed-value TOLUD setting does not account for all of the address space required by PCI devices there may be an overlap and affected devices will be inaccessible.

5.23.16 Advanced | Chipset Configuration | SATA PORT 0 Time Out(MS)

SATA PORT 0 Time Out(MS)	
Add a delay (measured in milliseconds) before enabling SATA port 0.	
0	No delay
1 ≤ n ≤ 65535	Delay in milliseconds

5.24 Advanced | ACPI Table Features Control

This menu provides options for configuring features that can be included in the ACPI tables.

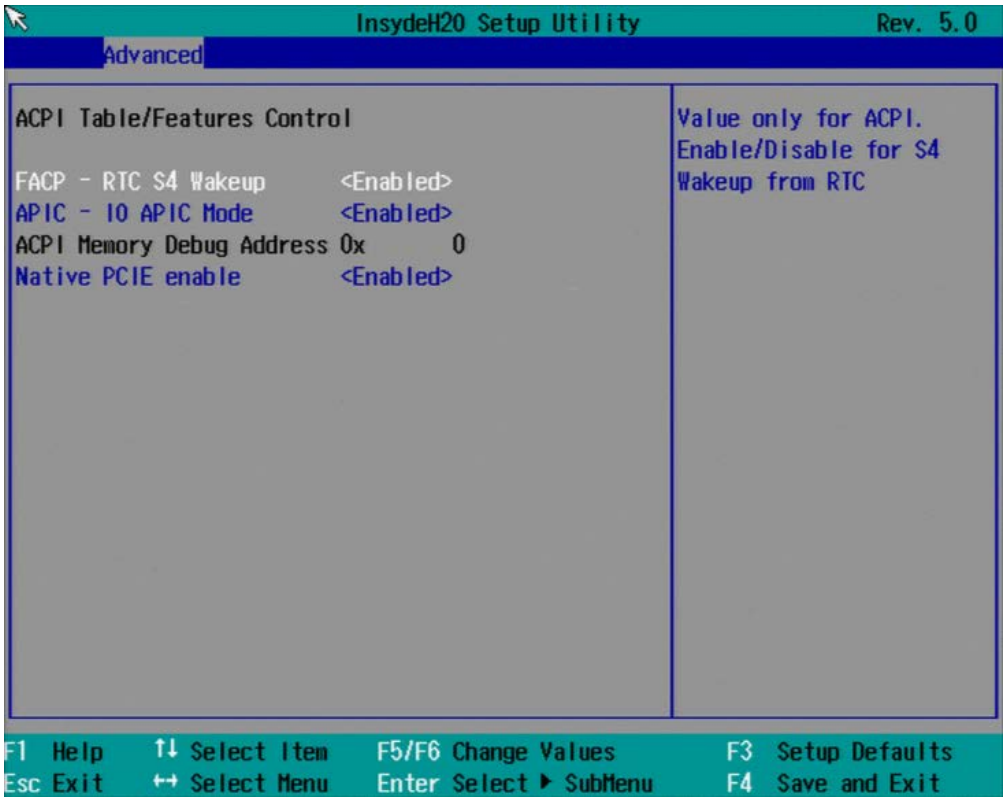


Figure 5-26 Advanced – ACPI Table Features Control Menu

5.24.1 Advanced | ACPI Table Features Control | FACP - RTC S4 Wakeup

FACP – RTC S4 Wakeup	
Enable the RTC as a wake event from S4.	
Disabled	RTC wake from S4 disabled
Enabled	RTC wake from S4 enabled

When set to **Enabled**, a wake event from the RTC Alarm can wake the board from ACPI S4.

5.24.2 Advanced | ACPI Table Features Control | APIC – IO APIC Mode

APIC – IO APIC Mode	
Disable the CPU APICs and PCH IOAPIC.	
Disabled	APIC mode disabled
Enabled	APIC mode enabled

This option should be set to **Disabled** for operating systems that are not SMP capable.

5.24.3 Advanced | ACPI Table Features Control | ACPI Memory Debug

ACPI Memory Debug
Reports the state of ACPI debug.

This option is provided for factory debug only.

5.24.4 Advanced | ACPI Table Features Control | Native PCIE enable

Native PCIE enable	
Specify whether an APCI OS has control of certain PCI Express functions	
Disabled	PCI Express Native Control disabled
Enabled	PCI Express Native Control enabled

When the PCI Express Native Control function is **Enabled** this allows an ACPI operating system to manage certain PCI Express functions such as hot plug, power management events and error reporting.

5.25 Advanced | PCI Express Configuration

This menu provides options for configuring the PCI Express interfaces implemented by the CPU and PCH.

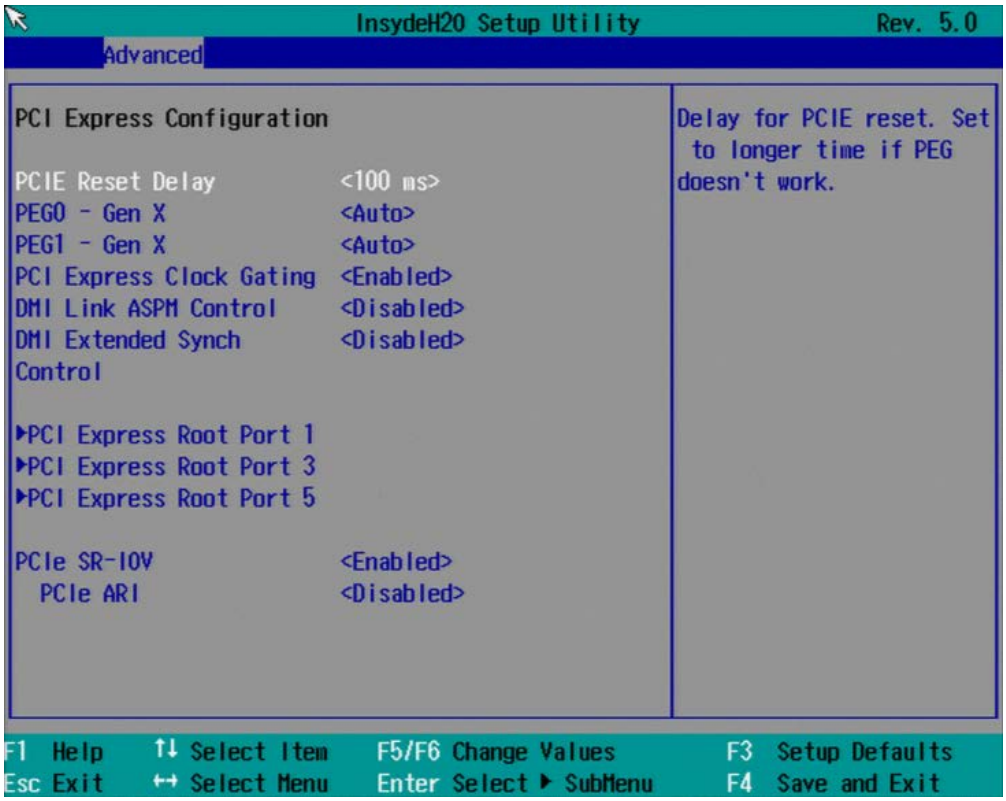


Figure 5-27 Advanced – PCI Express Configuration Menu

The VP B1x/msd uses two PCH PCI Express ports, which are detailed in Table 5-8.

PCIe Port	Width	Device/Function
2	x2	Intel i350 dual-channel GbE controller
7	x1	Intel i210 GbE controller

Table 5-8 PCI Express Port Use

5.25.1 Advanced | PCI Express Configuration | Spread Spectrum

Spread Spectrum	
Enable spread spectrum clocking for PCH clock sources.	
Disabled	Spread spectrum clocking disabled
Enabled	Spread spectrum clocking enabled

Enabling spread-spectrum clocking affects the PCH PCIe root ports, the DMI link to the CPU, DisplayPort interface and LPC bus.

5.25.2 Advanced | PCI Express Configuration | PCIE Reset Delay

PCIE Reset Delay	
Set an additional interval to wait while PCIe devices associated with the PEG port establish link.	
Disabled	Don't wait for devices
50 ms	Delay interval
100 ms	
200 ms	
300 ms	

The PCI Express Graphics (PEG) port on the VP B1x/msd connects to the XMC sites. Some add-in cards, particularly those containing FPGAs require additional time after reset to initialize hardware and establish a link.

If the BIOS fails to detect an add-in card, it may be necessary to increase this setting.

5.25.3 Advanced | PCI Express Configuration | XMC PCIe Link Speed

XMC PCIe Link Speed	
Set the PCI Express Link Speed for XMC1.	
Auto	Link Speed is set according to the endpoint capabilities
Gen1	Force link to Gen1 (250 MB/s per lane)
Gen2	Force link to Gen2 (500 MB/s per lane)
Gen3	Force link to Gen3 (1 Gbytes/s per lane)

Some XMCs, particularly those based on FPGA technology, can experience problems establishing a link when **Auto** is selected. If this happens, **Gen1**, **Gen2** or **Gen3** should be selected according to the capabilities of the XMC card.

5.25.4 Advanced | PCI Express Configuration | PCI Express Clock Gating

PCI Express Clock Gating	
Control PCI Express Clock Gating for all ports on the PCH.	
Disabled	Clock gating disabled
Enabled	Clock gating enabled

Enabling Clock Gating allows a power reduction by switching of parts of the clock circuitry associated with the PCI express ports when the links are idle.

The disadvantaged is increased latency required when the clocks are restarted.

5.25.5 Advanced | PCI Express Configuration | DMI Link ASPM Control

DMI Link ASPM Control	
Configure Active State Power Management (ASPM) for the DMI link.	
Disabled	DMI link ASPM disabled
Enabled	DMI link ASPM enabled

Enabling Active State Power Management (ASPM) allows the DMI link between the CPU and PCH to enter low power states when the link is inactive. Enabling this option will introduce a latency period while the link returns to full power.

5.25.6 Advanced | PCI Express Configuration | DMI Extended Synch Control

DMI Extended Synch Control	
Enable extended transmission of FTS data when exiting L0s.	
Disabled	Use default length FTS
Enabled	Use extended FTS

Fast Training Sequence (FTS) data sets are transmitted in order to re-establish the link on exit from L0s to L0.

5.25.7 Advanced | PCI Express Configuration | PCI Express Root Port x

PCI Express Root Port x
Setup options specific to individual PCH PCI Express Ports.

The port-specific Setup options are identical for all ports; these are detailed in Section 5.26.

5.26 Advanced | PCI Express Configuration | PCI Express Root Port x

This menu provides options for configuring PCH PCI Express ports. The options available to each of these ports are identical and port 1 is used in the examples below.

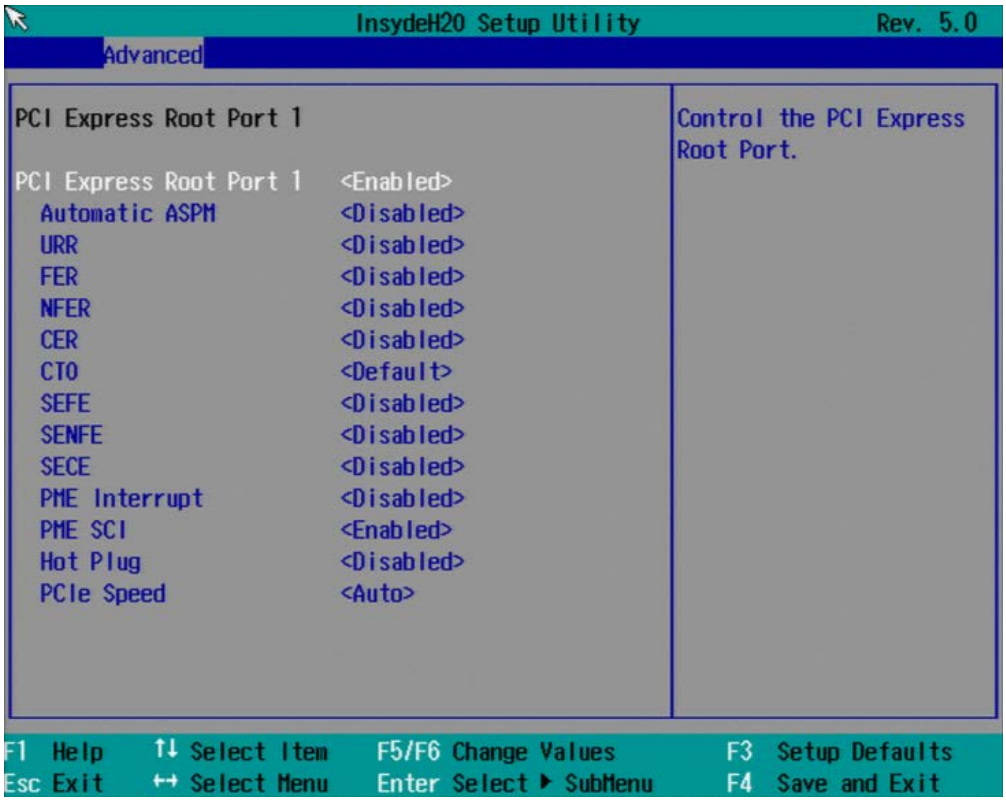


Figure 5-28 Advanced – PCI Express Root Port x Menu

NOTE: If the Root Port (Port 1) is set to **Disabled** the remaining port options are hidden.

5.26.1 Advanced | PCI Express Configuration | PCI Express Root Port x

PCI Express Root Port x	Caution
Control the PCI Express Root Port.	
Disabled	Port disabled
Enabled	Port enabled

When a Root Port is **Disabled** all downstream devices will be inaccessible.

WARNING: Disabling root Port 1 will disable all PCH PCI Express ports.

5.26.2 Advanced | PCI Express Configuration | PCI Express Root Port x | Automatic ASPM

Automatic ASPM	
Configure Active State Power Management (ASPM) for the PCI Express port.	
Disabled	ASPM disabled.
L0s	L0s enabled
L1	L1 enabled
L0sL1	L0s and L1 enabled
Auto	The BIOS chooses the appropriate setting for the attached device

Enabling Active State Power Management (ASPM) allows the PCI Express port to enter low power states when the link is inactive.

L0 is the active link-state. L0s is a low power state with the advantage of low latency when returning to L0. L1 is a lower power state than L0s, but the latency when returning to L0 is higher than that for L0s.

If '**Auto**' is selected, the BIOS uses details provided by the Root Port and attached device to select the best operating mode.

5.26.3 Advanced | PCI Express Configuration | PCI Express Root Port x | URR

URR	
PCI Express Unsupported Request Reporting (URR) control.	
Disabled	URR disabled
Enabled	URR enabled

When Enabled Unsupported Request errors received from an upstream device will be reported inside the PCH. Errors will be reported as Fatal, Non-Fatal or Correctable (see FER, NFER and CER below).

5.26.4 Advanced | PCI Express Configuration | PCI Express Root Port x | FER

FER	
PCI Express Fatal Error Reporting (FER) control.	
Disabled	FER disabled
Enabled	FER enabled

When Enabled a PCI Express Fatal Error received from an upstream device will be reported inside the PCH.

5.26.5 Advanced | PCI Express Configuration | PCI Express Root Port x | NFER

NFER	
PCI Express Non-Fatal Error Reporting (NFER) control.	
Disabled	NFER disabled
Enabled	NFER enabled

When Enabled a PCI Express Non-Fatal Error will be reported inside the PCH.

5.26.6 Advanced | PCI Express Configuration | PCI Express Root Port x | CER

CER	
PCI Express Correctable Error Reporting (CER) control.	
Disabled	CER disabled
Enabled	CER enabled

When Enabled a PCI Express Correctable Error received from an upstream device will be reported inside the PCH.

5.26.7 Advanced | PCI Express Configuration | PCI Express Root Port x | CTO

CTO	
Set PCI Express Completion Timer Timeout (CTO).	
Default	Specification default 50µs-50ms
16-55ms	Timeout interval
65-210ms	
260-900ms	
1-3.5ms	
Disabled	Timeout disabled

Set the interval before uncompleted PCI Express transactions are timed-out.

5.26.8 Advanced | PCI Express Configuration | PCI Express Root Port x | SEFE

SEFE	
PCI Express System Error on Fatal Error (SEFE) control.	
Disabled	SEFE disabled
Enabled	SEFE enabled

When Enabled PCI Express Fatal Errors reported via FER (above) or by the Root Port will generate System Error (SERR).

5.26.9 Advanced | PCI Express Configuration | PCI Express Root Port x | SENFE

SENFE	
PCI Express System Error on Non-Fatal Error (SENFE) control.	
Disabled	SENFE disabled
Enabled	SENFE enabled

When Enabled PCI Express Non-Fatal Errors reported via NFER (above) or by the Root Port will generate System Error (SERR).

5.26.10 Advanced | PCI Express Configuration | PCI Express Root Port x | SECE

SECE	
PCI Express System Error on Correctable Error (SECE) control.	
Disabled	SECE disabled
Enabled	SECE enabled

When Enabled PCI Express Correctable Errors reported via CER (above) or by the Root Port will generate System Error (SERR).

5.26.11 Advanced | PCI Express Configuration | PCI Express Root Port x | PME Interrupt

PME Interrupt	
PCI Express Power Management Event (PME) Interrupt control.	
Disabled	PME Interrupt disabled
Enabled	PME Interrupt enabled

When Enabled PCI Express Power Management Events will generate a PCI interrupt.

5.26.12 Advanced | PCI Express Configuration | PCI Express Root Port x | PME SCI

PME SCI	
PCI Express Power Management Event (PME) System Control Interrupt (SCI) control.	
Disabled	PME SCI disabled
Enabled	PME SCI enabled

When Enabled PCI Express Power Management Events will generate a System Control Interrupt (SCI).

5.26.13 Advanced | PCI Express Configuration | PCI Express Root Port x | Hot Plug

Hot Plug	
PCI Express Hot Plug control.	
Disabled	Hot Plug disabled
Enabled	Hot Plug enabled

NOTE: The PCH PCI Express ports on the VP B1x/msd do not implement, or require Hot Plug support.

5.26.14 Advanced | PCI Express Configuration | PCI Express Root Port x | PCIe Speed

PCIe Speed	
Set the PCI Express Link Speed for the associated PCH port.	
Auto	Link Speed is set according to the endpoint capabilities
Gen1	Force link to Gen1 (250 MB/s per lane)
Gen2	Force link to Gen2 (500 MB/s per lane)

The PCH PCIe ports are all connected to embedded devices on the VP B1x/msd so this setting should not need to be changed.

5.27 Advanced | Platform Configuration

This menu provides a summary of device features and add-on firmware revisions for the CPU and PCH devices.

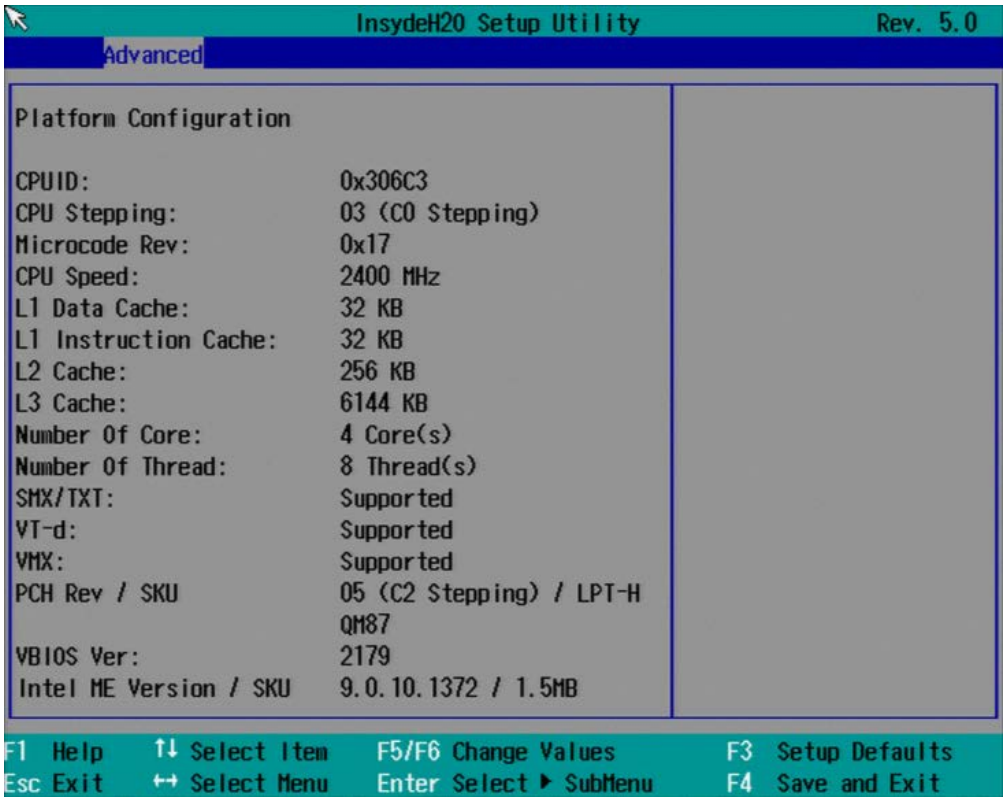


Figure 5-29 Advanced – Platform Configuration Menu

NOTE: The configuration shown in Figure 5-29 is an example and individual boards may have different values.

5.27.1 Advanced | Platform Configuration | CPUID

CPUID
Reports the value returned by the basic CPUID instruction (EAX = 0).

The CPUID value may differ between silicon steppings.

5.27.2 Advanced | Platform Configuration | CPU Stepping

CPU Stepping
Reports the hardware revision (stepping) of the CPU.

The CPU stepping may change over the lifetime of the board in response to Intel updates.

5.27.3 Advanced | Platform Configuration | Microcode Rev

Microcode Rev
Reports the version of CPU microcode currently installed.

The CPU microcode version may change over the lifetime of the board, but only as part of a BIOS version change.

5.27.4 Advanced | Platform Configuration | CPU Speed

CPU Speed
Reports the rated speed of the CPU.

The speed reported by this field is the rated speed of the CPU, not the current speed.

5.27.5 Advanced | Platform Configuration | L1 Data Cache

L1 Data Cache
Reports the size of the Level 1 data cache.

Each CPU core has a dedicated Level 1 cache.

5.27.6 Advanced | Platform Configuration | L1 Instruction Cache

L1 Instruction Cache
Reports the size of the Level 1 instruction cache.

Each CPU core has a dedicated Level 1 cache.

5.27.7 Advanced | Platform Configuration | L2 Cache

L2 Instruction Cache
Reports the size of the Level 2 cache.

Each CPU core has a dedicated Level 2 cache.

5.27.8 Advanced | Platform Configuration | L3 Cache

L3 Instruction Cache
Reports the size of the Level 3 (last level) cache.

The Last Level cache is shared by all of the CPU cores.

5.27.9 Advanced | Platform Configuration | Number of Core

Number of Core
Reports the number of physical CPU cores on the board.

5.27.10 Advanced | Platform Configuration | Number of Thread

Number of Thread
Reports the number of logical CPU cores available on the board.

Logical cores are enabled when Hyper Threading is enabled.

In the screen shot example above there are two physical cores with two threads per core, giving a total of four logical CPU cores available for use by SMP-capable operating systems.

5.27.11 Advanced | Platform Configuration | SMX/TXT

SMX/TXT
Indicates whether the CPU supports Intel trusted computing extensions

Intel Safer Mode Extensions (SMX) and Trusted Execution Technology (TXT) are additions to the IA32 and Intel 64 CPU architecture and instruction set specifically aimed at secure computing.

5.27.12 Advanced | Platform Configuration | VT-d

VT-d
Indicates whether the CPU supports Intel Virtualization Technology for Directed I/O (VT-d)

Intel Virtualization Technology for Directed I/O (VT-d) gives virtual machines direct access to certain peripheral devices by implementing DMA and interrupt remapping, thereby improving performance.

5.27.13 Advanced | Platform Configuration | VMX

VMX
Indicates whether the CPU supports Intel Virtual Machine Extensions (VXM).

Intel Virtual Machine Extensions (VXM) are additions to the IA32 and Intel 64 CPU instruction set specifically aimed at virtualization support.

5.27.14 Advanced | Platform Configuration | PCH Rev / SKU

PCH Rev / SKU
Reports the revision ID and SKU for the PCH silicon (PCI bus 0, device 31, function 0).

5.27.15 Advanced | Platform Configuration | VBIOS Ver

VBIOS Ver
Reports the internal version number of the Intel video BIOS.

5.27.16 Advanced | Platform Configuration | Intel ME Version / SKU

Intel ME Version / SKU
Reports the version number and SKU of the ME firmware.

5.28 Advanced | Console Redirection

This menu provides options for configuring the BIOS Serial Console. The VP B1x/msd supports serial console operation via COM1, COM2 and COM3.

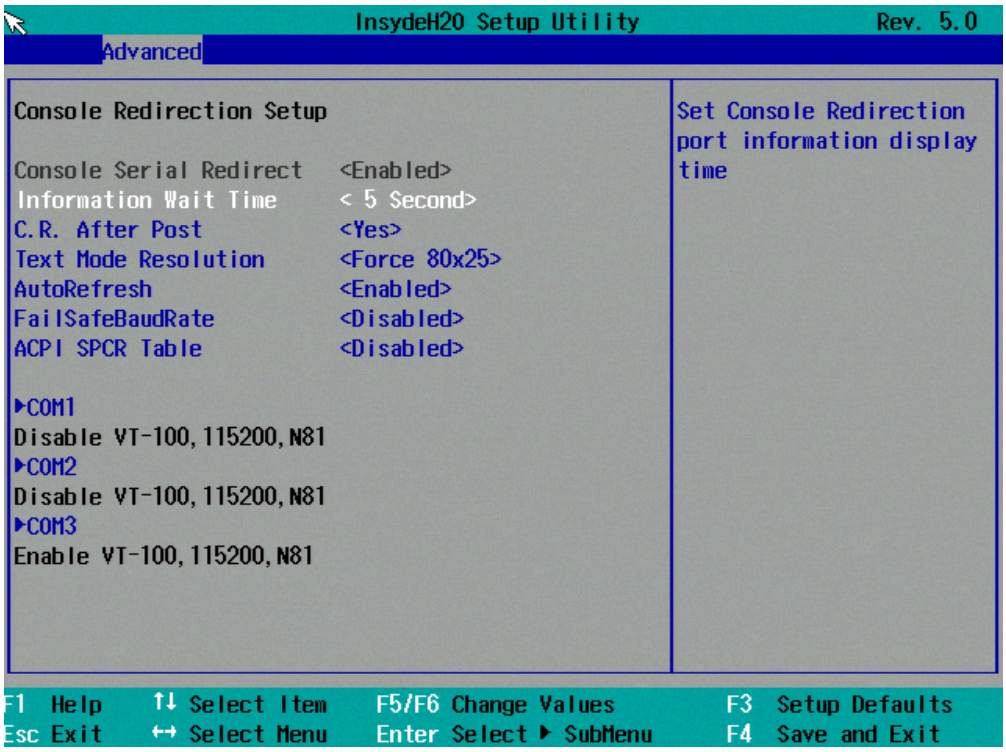


Figure 5-30 Advanced – Console Redirection Menu

See Section 6 for details relating to the BIOS Serial Console and considerations when booting operating systems.

5.28.1 Advanced | Console Redirection | Console Serial Redirect

Console Serial Redirect	
Status of the board's Serial Console DIP switch.	
Enabled	Serial Console enabled
Disabled	Serial Console disabled

Serial Console mode is enabled using a DIP switch (refer to the board's technical reference manual for details).

With some operating systems, or in some applications, it is preferable to use a serial terminal as an operator console device for the board.

5.28.2 Advanced | Console Redirection | Information Wait Time

Information Wait Time	
Specify how long the BIOS will pause displaying the serial console sign-on (information) screen.	
0 Second	Delay period
2 Second	
5 Second	
10 Second	
30 Second	

5.28.3 Advanced | Console Redirection | C.R. After Post

C.R. After Post	
Enable a carriage return (CR) after completion of the BIOS power-on self test (POST).	
Yes	Output a carriage return after completion of POST
No	Don't output a carriage return

5.28.4 Advanced | Console Redirection | Text Mode Resolution

Text Mode Resolution	
Set the size of the serial console screen.	
AUTO	Text resolution follows the VGA text mode resolution
Force 80x25	Ignore VGA mode and force 80x25 resolution
Force 80x24 (DEL FIRST ROW)	Ignore VGA mode and force 80x24 resolution, the first screen line will be omitted
Force 80x25 (DEL LAST ROW)	Ignore VGA mode and force 80x24 resolution, the last screen line will be omitted

If the terminal (or terminal emulation software) fails to display the Setup screen correctly, this option can be used to match the serial console output to the capabilities of the terminal device.

5.28.5 Advanced | Console Redirection | Auto Refresh

Auto Refresh	
Automatically refresh the screen when a remote serial terminal is connected.	
Disabled	Only new output is sent to the terminal
Enabled	Refresh and resend the entire screen when a terminal is connected

5.28.6 Advanced | Console Redirection | FailSafeBaudRate

FailSafeBaudRate	
Auto detects the remote terminal baud rate and connects at that speed.	
Disabled	Use the Setup configured baud rate
Enabled	Auto detect the remote terminal baud rate

5.28.7 Advanced | Console Redirection | ACPI SPCR Table

ACPI SPCR Table	
Add a Serial Port Console Redirection (SPCR) table to the board's ACPI tables.	
Disabled	No SPCR
Enabled	Include SPCR

The ACPI Serial Port Console Redirection (SPCR) table provides details of the Serial Console implementation to operating systems.

NOTE: For use with Microsoft Windows operating systems the Terminal Type must be set to VT100+.

5.28.8 Advanced | Console Redirection | COMx

NOTE: This option is only visible when Console Serial Redirect is set to **Enabled**.

COMx
Configure port settings for a specific COM port.

The port-specific Setup options are identical for all ports; these are detailed in Section 5.29.

5.28.1 Advanced | Console Redirection | [Port Settings Summary]

NOTE: This option is only visible when Console Serial Redirect is set to **Enabled**.

[Port Settings Summary]
Displays a summary of the settings configured via the associated COMx menu.

5.29 Advanced | Console Redirection | COMx

This menu provides options for configuring COM port parameters for use with the BIOS Serial Console. The VP B1x/msd supports serial console operation via COM1, COM2 and COM3; the Setup options are identical for all ports.

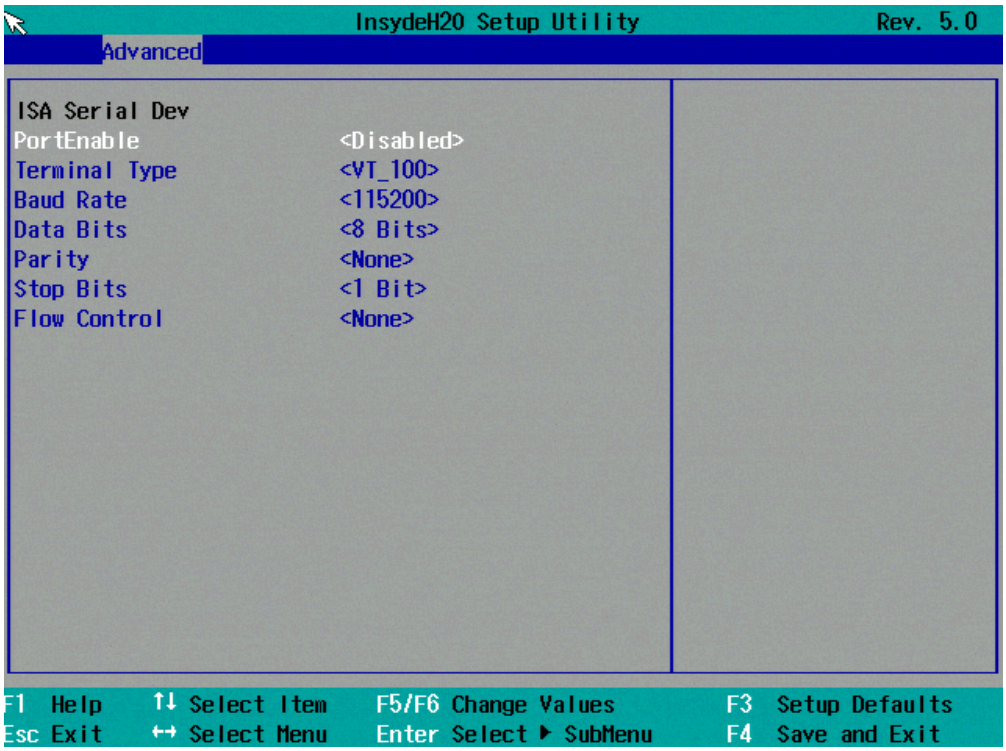


Figure 5-31 Advanced – Console Redirection Menu

5.29.1 Advanced | Console Redirection | COMx | PortEnable

PortEnable	
Software enable for COMx port	
Disabled	COMx port is disabled
Enabled	COMx port is enabled

The default Serial Console COM port is enabled using DIP switches (refer to the board's technical reference manual for details). This option can be used to enable additional COMx ports as serial consoles; the BIOS Serial Console will operate over all enabled ports simultaneously.

5.29.2 Advanced | Console Redirection | COMx | Terminal Type

Terminal Type	
Select the command protocol used to communicate with the serial terminal.	
VT_100	Terminal command mode
VT_100+	
VT_UTF8	
PC_ANSI	

The **PC_ANSI** setting provides an environment very similar to a conventional CRT (see Figure 6-1).

The VT100 setting offers maximum compatibility with older terminals, however the appearance of the POST and Setup Utility screens will differ from the CRT display.

5.29.3 Advanced | Console Redirection | COMx | Baud Rate

Baud Rate	
Select the console port baud rate.	
115200	Baud rate
57600	
38400	
19200	
9600	

The higher the speed, the more responsive the BIOS Setup Utility will appear.

When the serial console is used at high speeds, particularly with an asynchronous link, there is a small possibility of data corruption. If this occurs the serial terminal should be power cycled, or the terminal emulation utility should be restarted.

5.29.4 Advanced | Console Redirection | COMx | Data Bits

Data Bits	
Select the number of data bits sent in each packet.	
7 Bits	Number of data bits
8 Bits	

5.29.5 Advanced | Console Redirection | COMx | Parity

Parity	
Select whether a parity bit is sent with the packet and the encoded parity type.	
None	The parity bit is not sent
Even	Even parity used
Odd	Odd parity used

5.29.6 Advanced | Console Redirection | COMx | Stop Bits

Stop Bits	
Select the number of stop bits terminating each packet.	
1 Bit	Number of stop bits
2 Bits	

5.29.7 Advanced | Console Redirection | COMx | Flow Control

Flow Control	
Select whether flow control is used when packets are sent and the type.	
None	No flow control is used
RTS/CTS	Use the RTS and CTS hardware signals
XON/XOFF	Use XON/XOFF packets

Many implementations do not use Flow Control to regulate the Serial Console output and it is not a requirement; however when flow control is used, terminal corruption is less likely

5.30 Advanced | BIOS Event Log Configuration

This menu provides options for configuring the BIOS event logging feature.

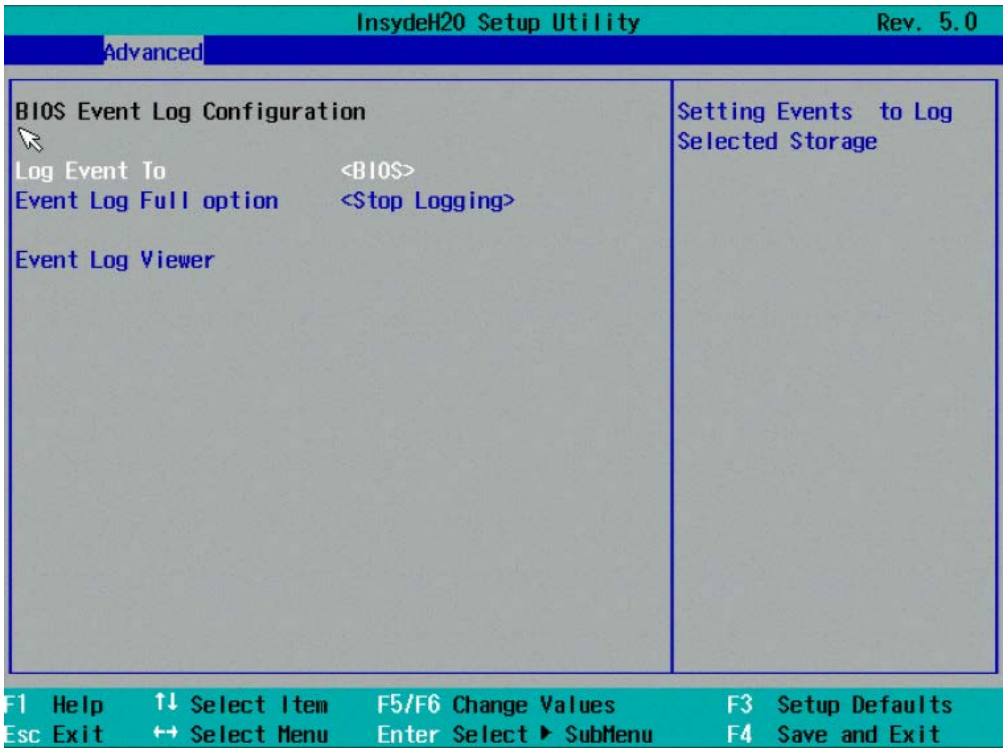


Figure 5-32 Advanced – BIOS Event Log Configuration Menu

5.30.1 Advanced | BIOS Event Log Configuration | Log Event To

Log Event To	
Select device where BIOS events are recorded.	
ALL	Log event s in Flash, Memory and via the BMC
BIOS	Log events in BIOS Flash storage
BMC SEL	Log events via the BMC (where present)
MEMORY	Log events in memory

NOTE: The VP B1x/msd does not have a BMC, so selecting this option will disable logging of events.

5.30.2 Advanced | BIOS Event Log Configuration | Event Log Full option

Event Log Full option	
Select how to respond to new events when the Event Log becomes full.	
Overwrite	New events overwrite the oldest events
Clear All	Clear the entire event log before recording the new event
Stop Logging	Stop logging when the log becomes full

With some operating systems, or in some applications, it is preferable to use a serial terminal as an operator console device for the board.

5.30.3 Advanced | BIOS Event Log Configuration | Event Log Viewer

Event Log Viewer
Select the Event Viewer sub menu.

Details of the Event Log Viewer sub-menu can be found in Section 5.31.

5.31 Advanced | BIOS Event Log Configuration | Event Log Viewer

This menu provides options for viewing and clearing the different BIOS Event Logs.

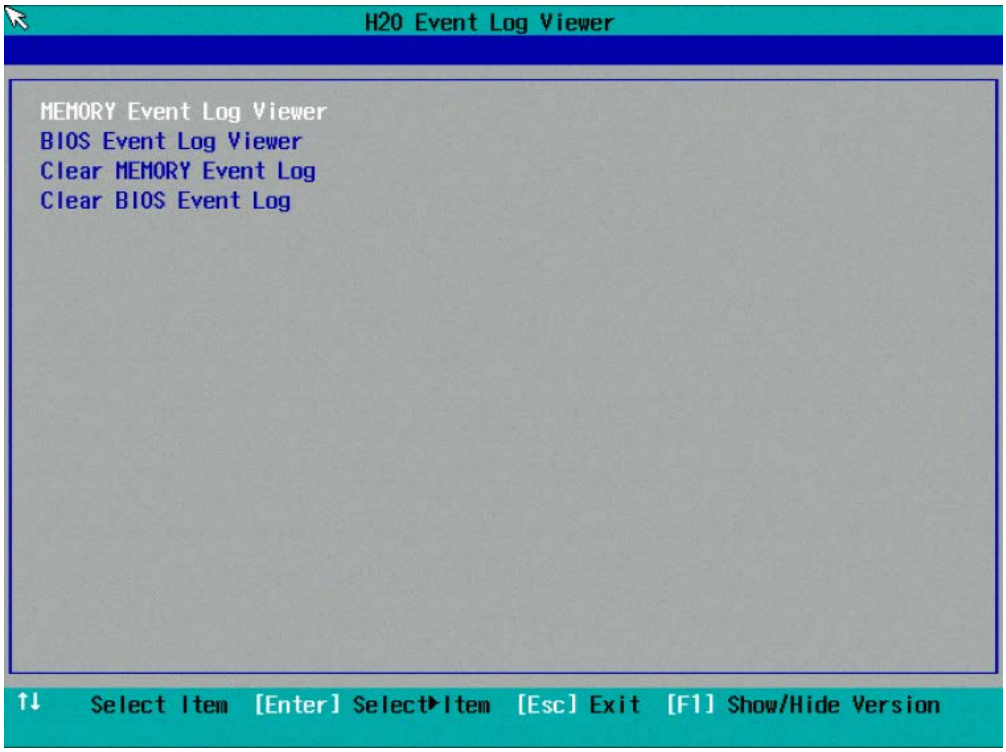


Figure 5-33 Advanced – BIOS Event Log Configuration Menu

5.31.1 Advanced | BIOS Event Log Configuration | Event Log Viewer

MEMORY Event Log Viewer
Select the MEMORY Event Log viewer.

5.31.2 Advanced | BIOS Event Log Configuration | Event Log Viewer | BIOS Event Log Viewer

BIOS Event Log Viewer
Select the BIOS Flash Event Log viewer.

5.31.3 Advanced | BIOS Event Log Configuration | Event Log Viewer | Clear MEMORY Event Log

Clear MEMORY Event Log
Clears the contents of the memory-resident Event Log.

This option responds with a popup menu requesting confirmation before completing the operation.

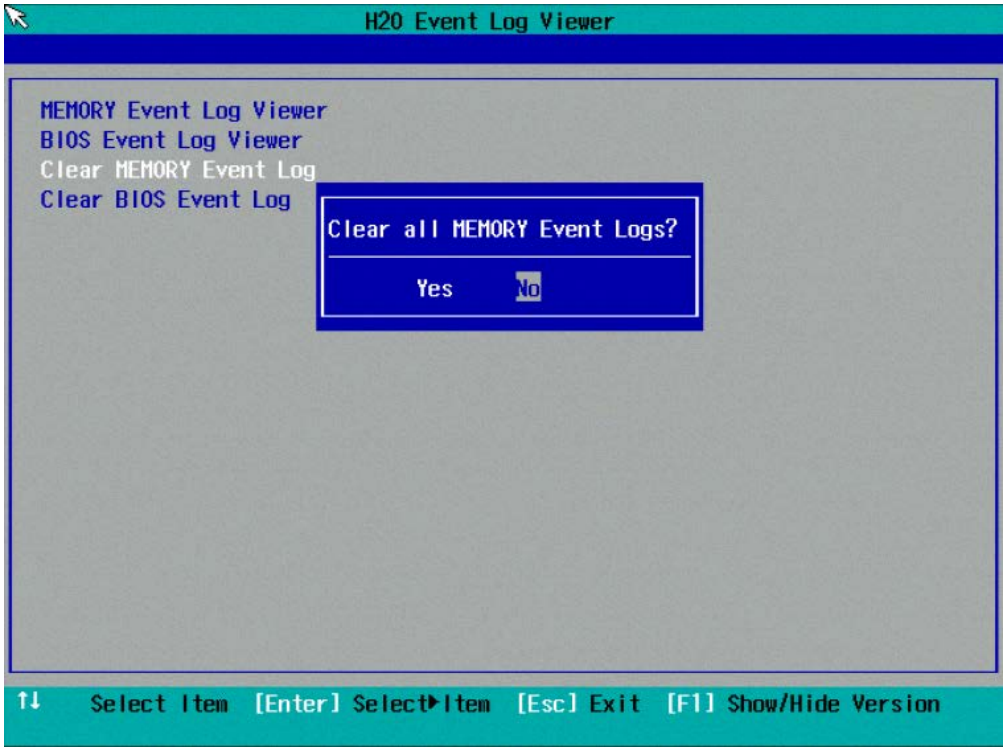


Figure 5-34 Clear MEMORY Event Log - Confirmation Popup

5.31.4 Advanced | BIOS Event Log Configuration | Event Log Viewer | Clear BIOS Event Log

Clear BIOS Event Log
Clears the contents of the BIOS flash Event Log.

This option responds with a popup menu requesting confirmation before completing the operation.

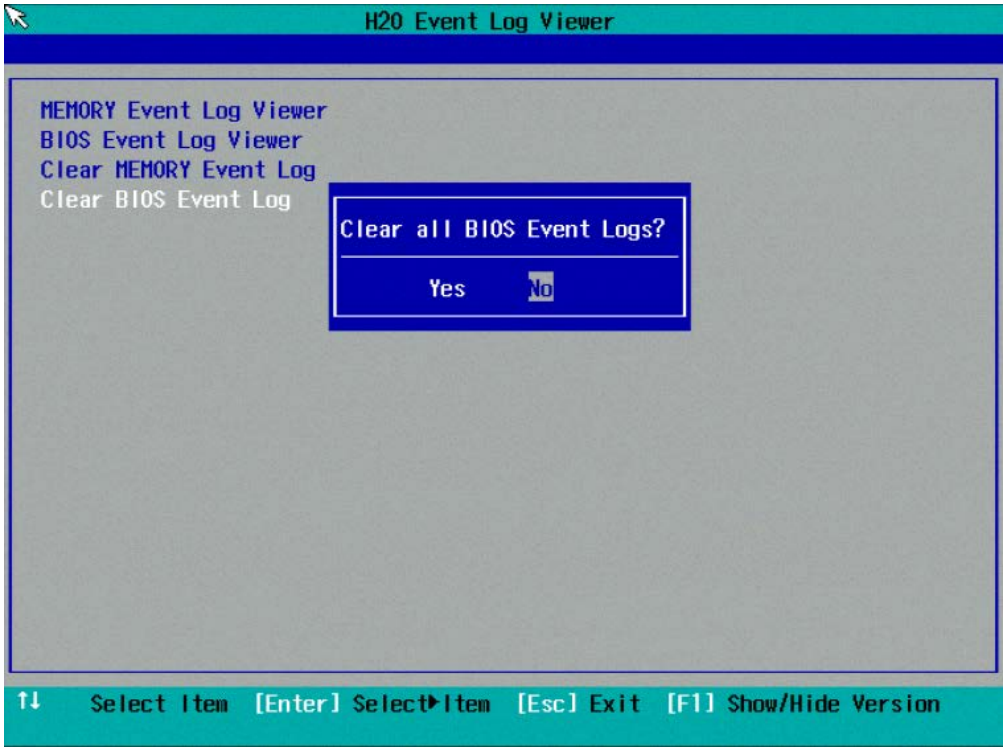


Figure 5-35 Clear BIOS Event Log - Confirmation Popup

5.32 Security

The **Security** Setup menu provides option for managing the BIOS security features. See Section 11 for a description of the BIOS security model.

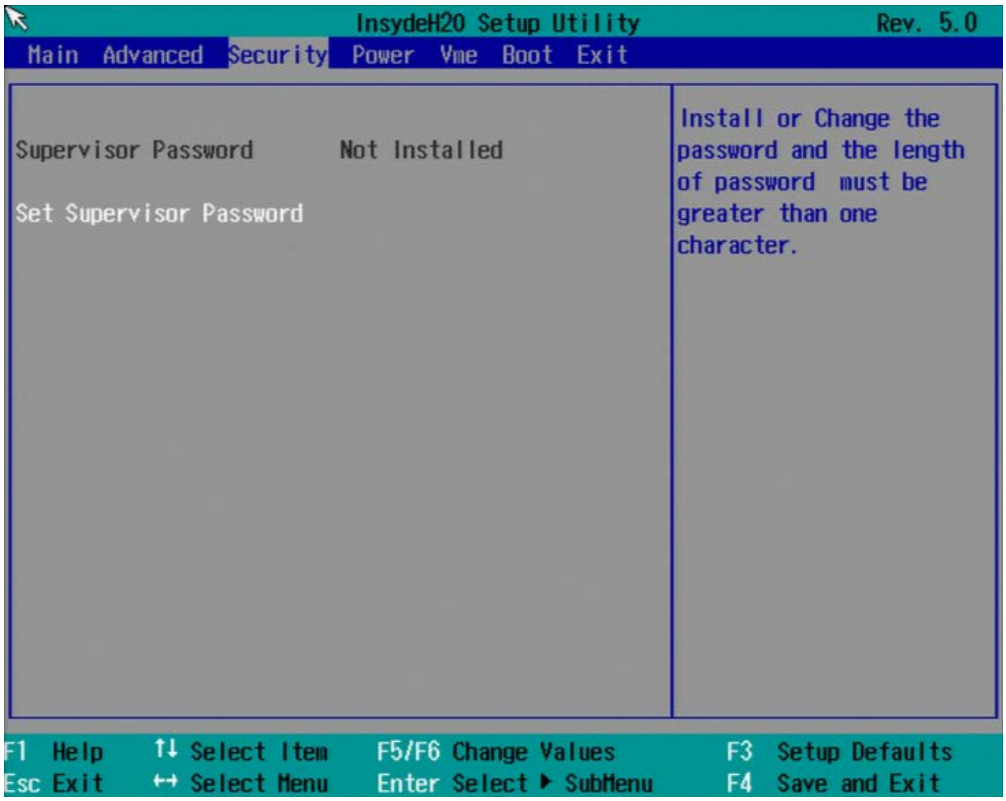


Figure 5-36 Security Menu

5.32.1 Security | TPM Status

NOTE: this option is only available on boards where a TPM is fitted.

TPM Status	
Indicates the status of the board's TPM hardware.	
Not Installed	TPM device is not fitted to the board.
Enabled and Active	Status reported by the TPM device
Enabled and Inactive	
Disabled and Active	
Disabled and Inactive	

The TPM status can be changed using the **TPM Operation** option, see Section 5.32.2.

5.32.2 Security | TPM Operation

NOTE: this option is only available on boards where a TPM is fitted.

TPM Operation	
Change the status of the TPM hardware	
No Operation	No change
Disable and Deactivate	Disable the TPM hardware
Enable and Activate	Enable the TPM hardware

The TPM hardware is enabled and active by default, it may be disabled by selecting **Disable and Deactivate**. Changes to the TPM configuration are applied when the board restarts.

Once the TPM status change has been applied this option will revert to **No Operation**.

5.32.3 Security | Supervisor Password

Supervisor Password	
Indicates the status of the Supervisor Password.	
Not Installed	No password has been configured
Installed	Password configured

5.32.4 Security | Set Supervisor Password

Set Supervisor Password
Install a Supervisor Password or change the existing password.

This option responds with a pop-up dialog when selected.

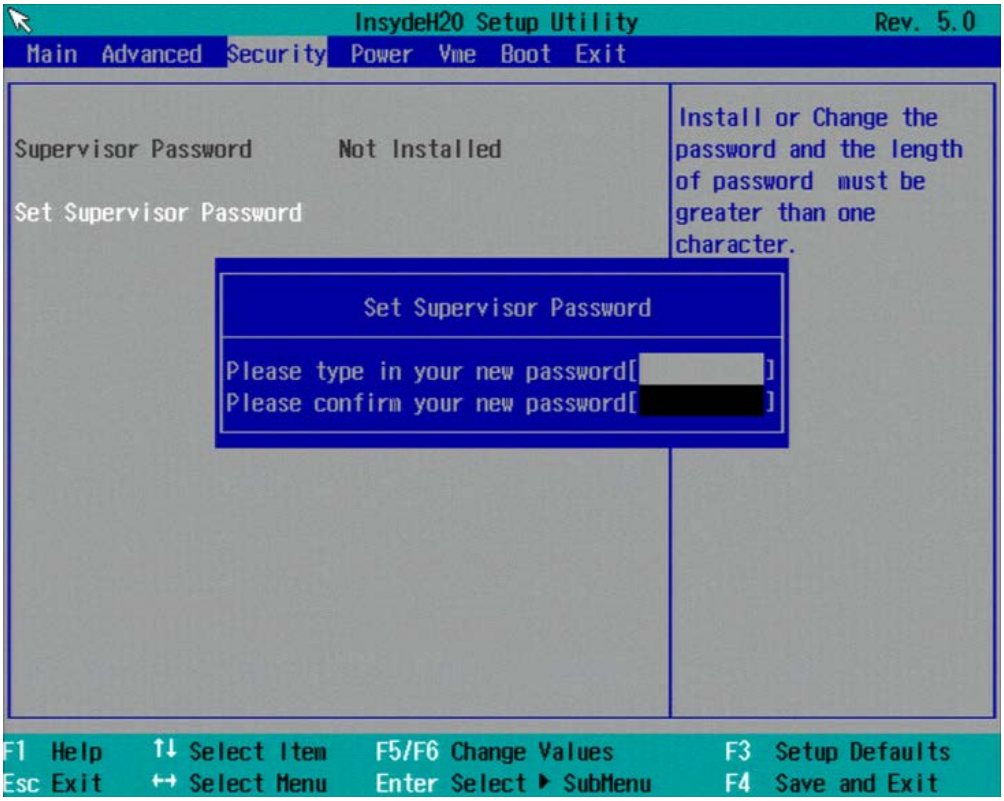


Figure 5-37 Security – Supervisor Password Popup

Enter the chosen password, which can contain up to 10 characters. The password must be entered twice as the characters are hidden from view. If the two passwords match the password status changes to **Installed** and Setup responds with a confirmation pop-up (see Figure 5-38).

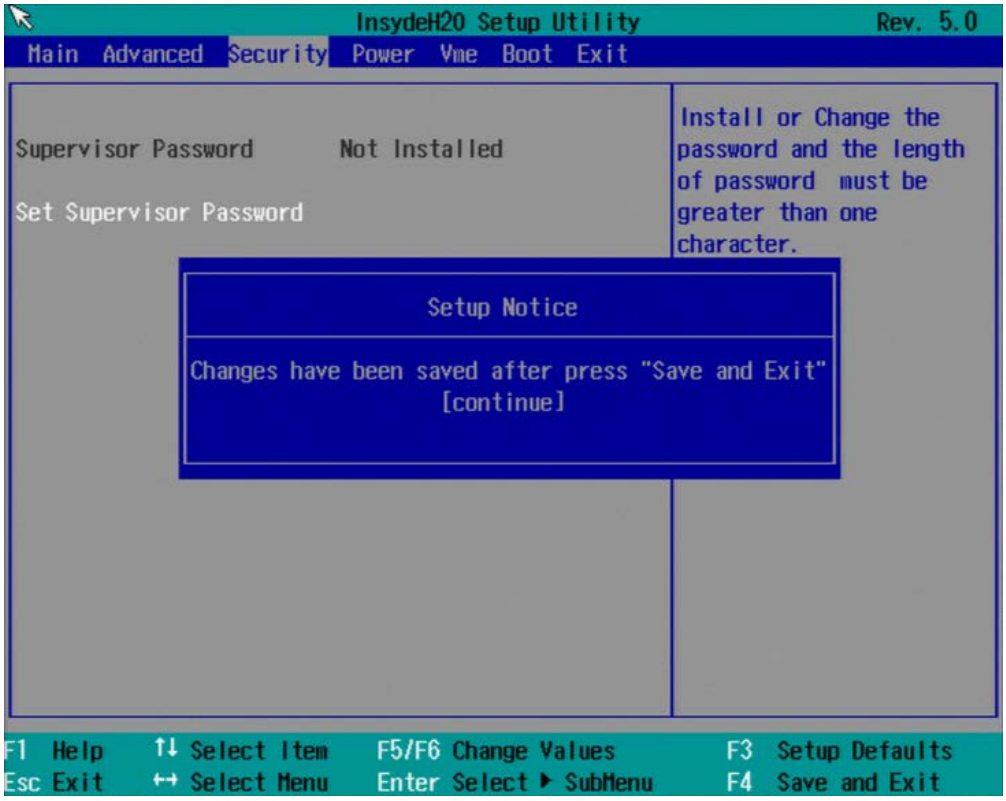


Figure 5-38 Security – Setup Notice Popup

If the entered passwords do not match a warning pop-up will be displayed (see Figure 5-39).

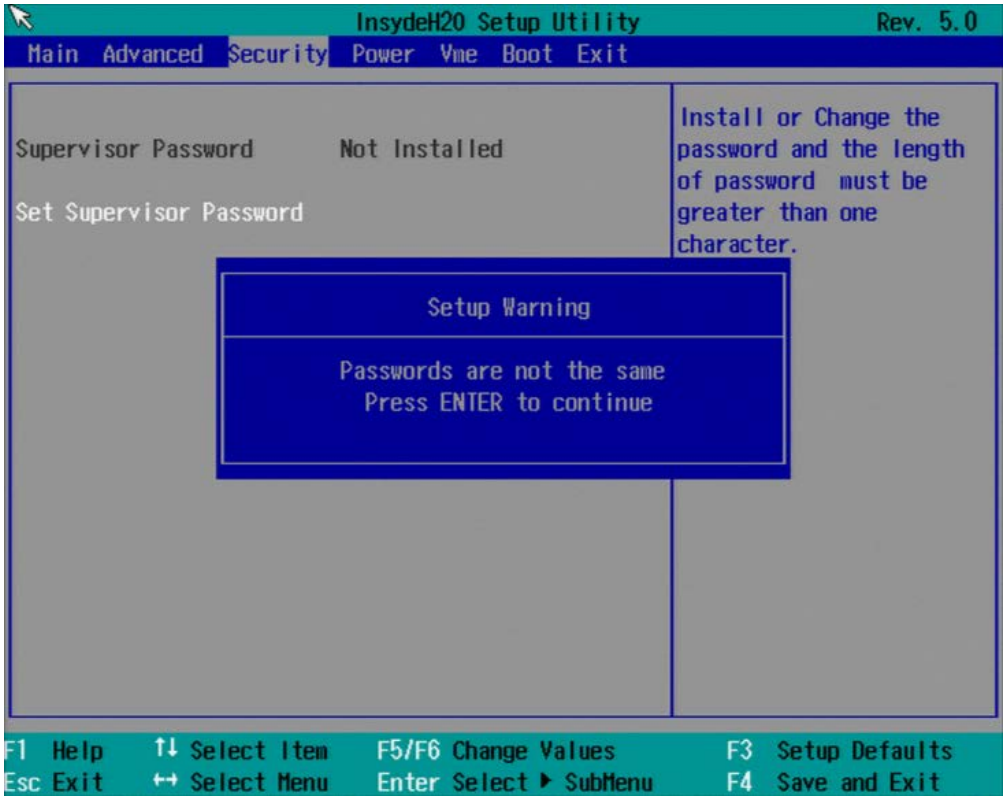


Figure 5-39 Security – Setup Warning Popup

When changing a password the user must first supply the old password, then enter the new password twice, Figure 5-40 illustrates the password change dialog.

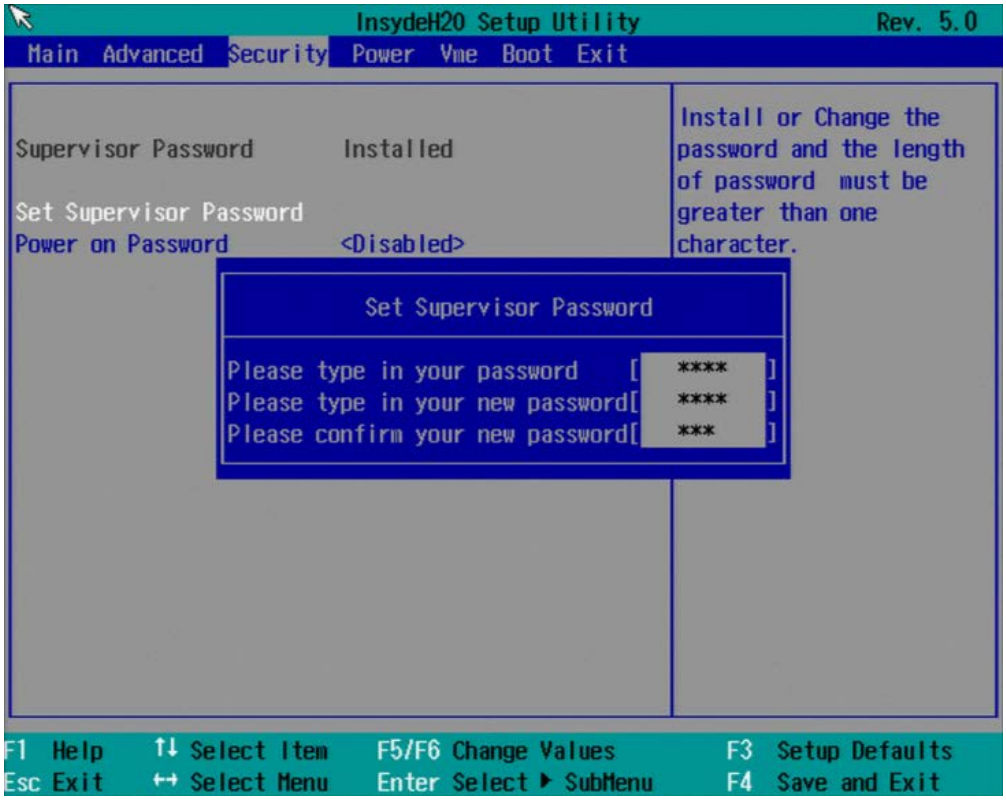


Figure 5-40 Security – Change Supervisor Password Popup

When the Supervisor password has been installed, further Setup options are displayed, see Section 5.33 for further details.

5.32.5 Clearing the Supervisor Password

The Supervisor Password can be cleared by making a blank entry in both new password fields of the **Set Supervisor Password option**, but the current password string must be known to do this.

WARNING: If the Supervisor Password has been forgotten a BIOS update will be required to return the board to the shipping configuration. However if the **Power on Password** option has been **Enabled** this will not be possible and the board must be returned to the factory.

5.33 Security – Additional Options

The following options are only displayed once a supervisor password has been installed.

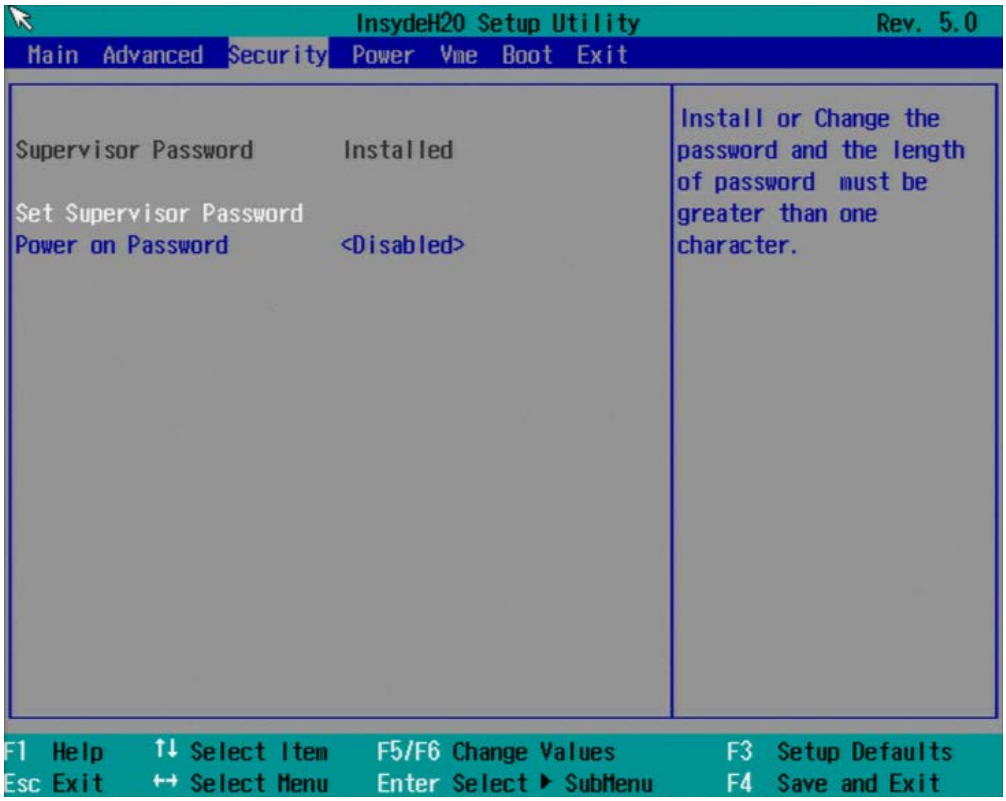


Figure 5-41 Security – Additional Options

5.33.1 Security | Power on Password

Power on Password	
Specify whether a password must be provided during POST.	
Enabled	Ask for password during POST
Disabled	Don't ask for password during POST

If set to **Enabled** the user will be prompted for a password during POST and the board will not proceed (into Setup or the Boot Loader) until a correct password is supplied. If set to **Disabled**, the user will be prompted for a password before entering Setup.

5.34 Power

The **Power** Setup menu configures options related to CPU and chipset low-power states.

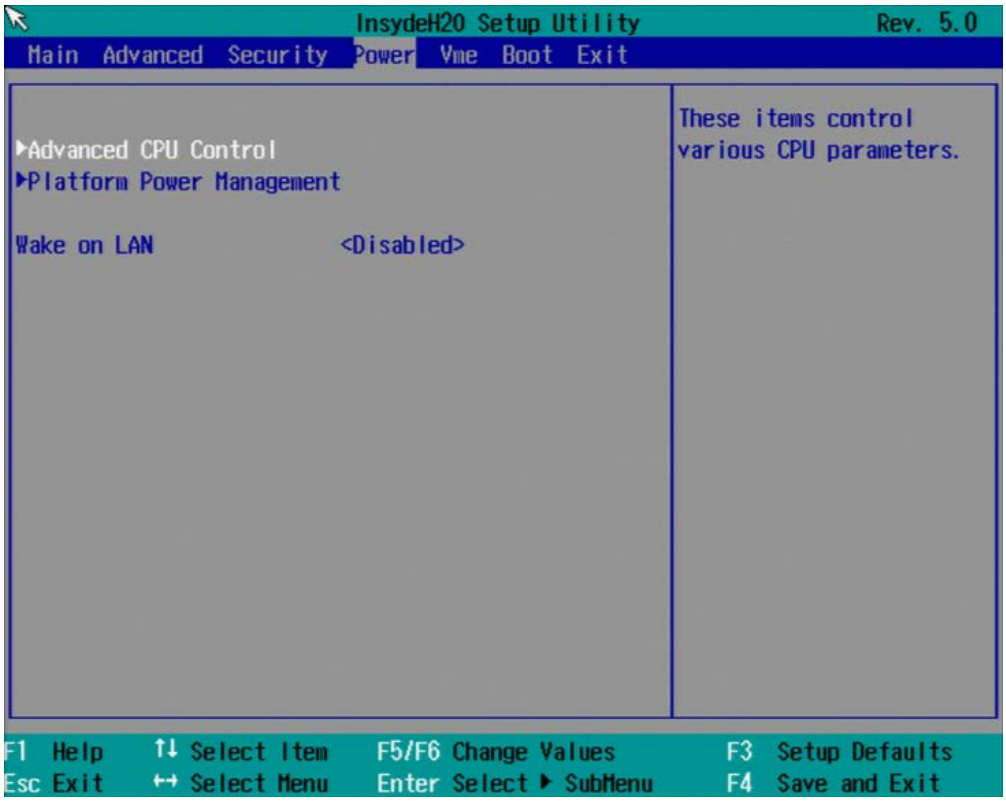


Figure 5-42 Power Menu

5.34.1 Power | Advanced CPU Control

Advanced CPU Control
Configure CPU related power management options.

The **Advanced CPU Control** options are detailed in Section 5.35.

5.34.2 Power | Platform Power Management

Platform Power Management
Configure power management options for chipset devices.

The **Platform Power Management** options are detailed in Section 5.36.

5.34.3 Power | Wake-on-LAN

Wake-on-LAN	
Allow the board to be woken from the ACPI S4/S5 states by an Ethernet ‘magic packet’.	
Disabled	Ignore LAN controller wake
Enabled	Wake board if LAN magic packet is received

The board is placed into the ACPI S4 power-state by an operating system ‘**Hibernate**’ and the S5 power-state by going through an operating system shutdown.

5.35 Power | Advanced CPU Control

This menu provides options for configuring CPU low-power states.

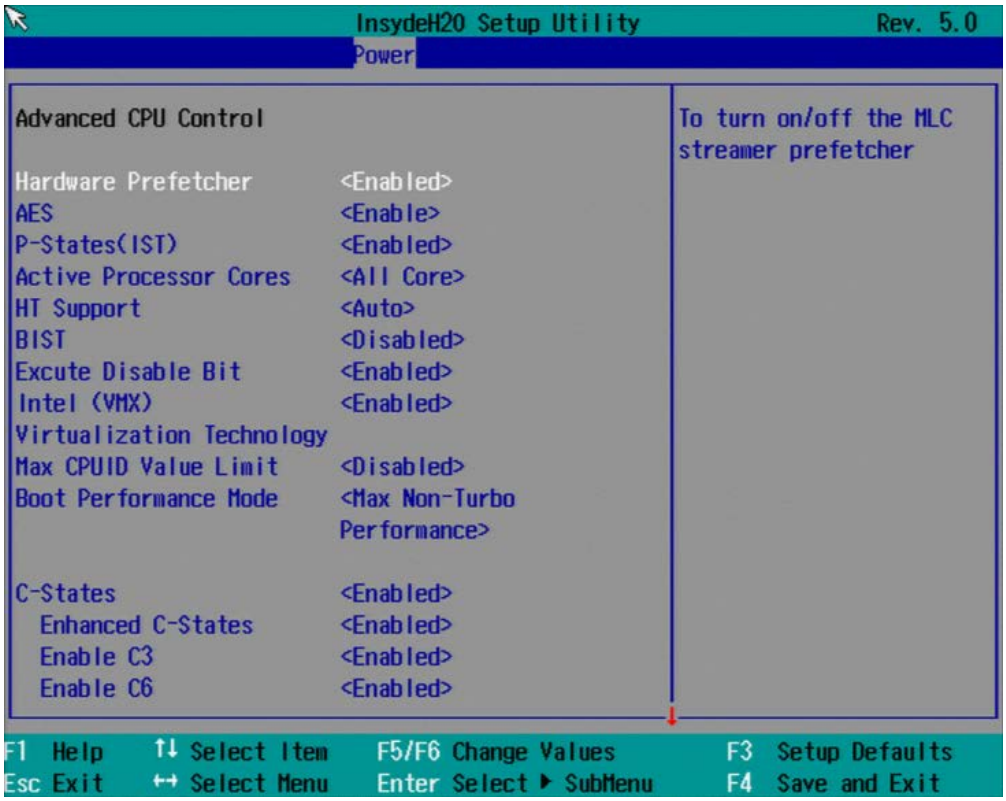


Figure 5-43 Power – Advanced CPU Control Menu

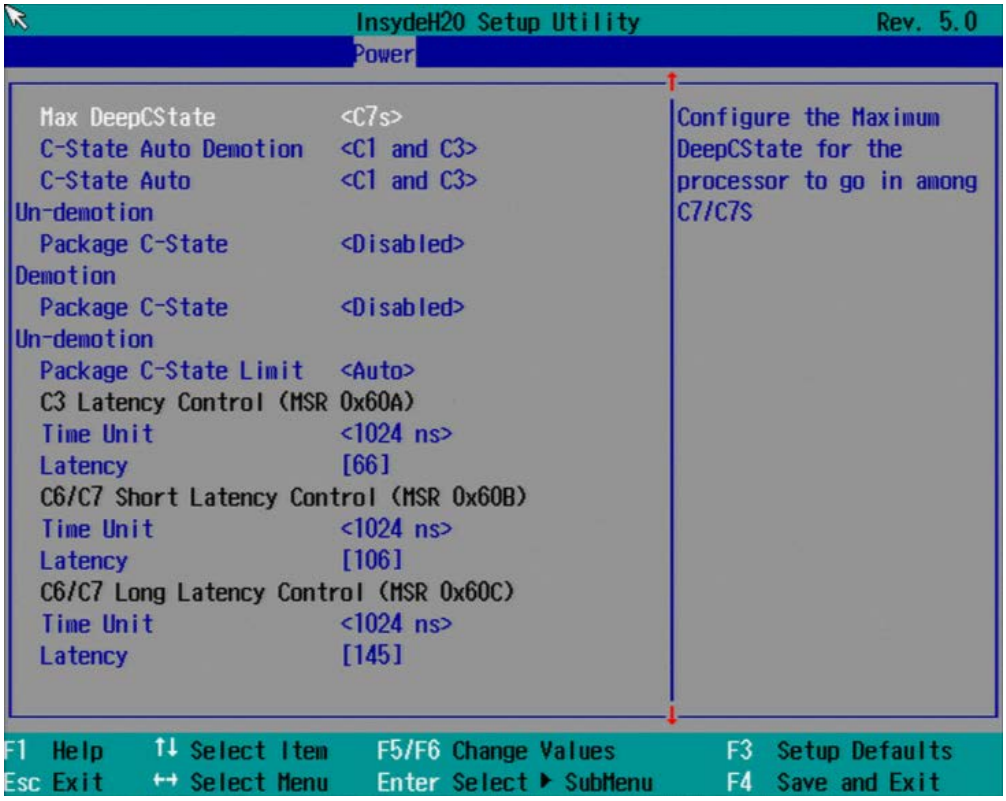


Figure 5-44 Power – Advanced CPU Control Menu (continued 1)

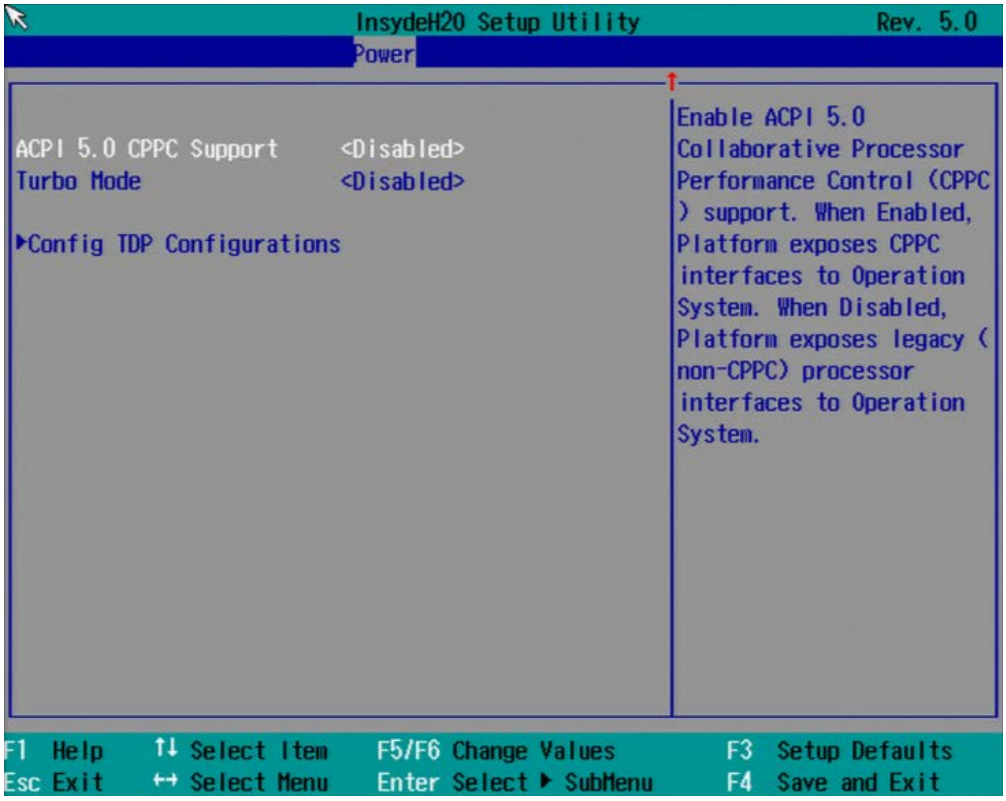


Figure 5-45 Power – Advanced CPU Control Menu (continued 2)

5.35.1 Power | Advanced CPU Control | Hardware Prefetcher

Hardware Prefetcher	
Disable the CPU 2nd level cache predictive hardware prefetch.	
Disabled	CPU hardware prefetcher disabled
Enabled	CPU hardware prefetcher enabled

Disabling the hardware prefetcher will reduce the CPU performance.

5.35.2 Power | Advanced CPU Control | AES

AES	
Enable CPU support for Advanced Encryption Standard (AES) instructions.	
Enable	AES support is enabled
Disable	AES support is disabled

With the Core i7 processor, Intel introduced a number of new instructions to speed up encryption and decryption of data using the Advanced Encryption Standard (AES).

5.35.3 Power | Advanced CPU Control | P-States(IST)

P-States(IST)	
Enable processor Performance States (P-States) in ACPI.	
Disabled	P-States disabled
Enabled	P-States enabled

While the processor is operating in the C0 (active) power-state an ACPI operating system can select different processor Performance States (P-States) by activating the CPU throttling mechanism thereby reducing power consumption and ultimately, the CPU temperature.

5.35.4 Power | Advanced CPU Control | Active Processor Cores

Active Processor Cores	Caution
Select the number of physical CPU cores enabled and reported to operating systems.	
All Core	Enable all CPU cores
1 Core	Limit the number of enabled CPU cores (settings are for a 4-Core CPU)
2 Core	
3 Core	

If application software does not require all four CPU cores, the power consumption of the board can be reduced by disabling unused cores.

This option can be set to **1-Core** for operating systems that are not SMP capable.

WARNING: All Cores should be enabled for maximum performance.

5.35.5 Power | Advanced CPU Control | HT Support

HT Support	Caution
Disable Hyper-Threading (HT).	
Auto	Enable HT if the CPU supports the feature
Disabled	HT disabled

When set to **Enabled** Intel Hyper-Threading Technology (HT) implements two logical CPUs for each physical CPU core. The '**Auto**' setting enables HT provided the CPU supports the feature.

WARNING: HT Support should be enabled for maximum performance.

5.35.6 Power | Advanced CPU Control | BIST

BIST	
Enable the CPU Built-In Self Test (BIST)	
Disabled	CPU BIST disabled
Enabled	CPU BIST will run following reset

When CPU BIST is enabled the boot time will be slightly increased.

5.35.7 Power | Advanced CPU Control | Execute Disable Bit

Execute Disable Bit	
Enable the processor's Execute Disable (XD) capability.	
Disabled	XD is disabled
Enabled	XD is enabled

The **Execute Disable** (**XD**) feature of the CPU allows operating systems that support XD to mark areas of memory as non-executable, thus provide greater security against malicious software.

5.35.8 Power | Advanced CPU Control | Intel (VMX) Virtualization Technology

Intel (VMX) Virtualization Technology	
Disable Intel Virtualization Technology (VT).	
Enabled	Enable VT
Disabled	Disable VT

I**ntel Virtualization Technology** (**VT**) provides support for hardware virtualization in multi-OS environments.

5.35.9 Power | Advanced CPU Control | Max CPUID Value Limit

Max CPUID Value Limit	
Limit the maximum supported CPUID function to EAX = 3.	
Disabled	All CPUID functions are enabled
Enabled	Only CPUID functions EAX = 0 – 3 are available

This option should only be set to **Enabled** when using Legacy operating systems that have problems operating on modern CPUs.

5.35.10 Power | Advanced CPU Control | Boot Performance Mode

Boot Performance Mode	
Select which CPU performance state the BIOS will select before booting an operating system.	
Max Non-Turbo Performance	Select the maximum performance state without enabling Turbo mode
Max Battery	Select the minimum performance state (lowest CPU frequency)
Turbo Performance	Select the maximum performance state (maximum CPU frequency)

Once the operating system boots then its performance management drivers and settings will take over.

5.35.11 Power | Advanced CPU Control | C-States

C-States	
Disable processor Power States (C-States) in ACPI.	
Disabled	C-States disabled
Enabled	C-States enabled

The C0 power-state indicates that CPU is active and executing instructions. C-States C1, C2, C3, etc. represent increasingly low-power sleep states.

When the CPU enters a sleep state, it halts instruction execution. The latency involved in returning to C0 increases as the C-State number increases.

5.35.12 Power | Advanced CPU Control | Enhanced C-States

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

Enhanced C-States	
Disable support for combination C-State and P-State transitions.	
Disabled	Enhanced C-State support disabled
Enabled	Enhanced C-State support enabled

When **Enhanced C-State** support is enabled the CPU can enter a low-power sleep state and at the same time throttling can be enabled to reduce clock frequencies and lower the core voltage, resulting in greater power savings.

5.35.13 Power | Advanced CPU Control | Enable C3

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

Enable C3	
Enable support for CPU low power state C3.	
Disabled	C3 disabled
Enabled	C3 enabled

Processor power-state **C3** is a lower power sleep state than C0-C2. When in C3 the per-core cache contents is flushed and PLLS are turned off

5.35.14 Power | Advanced CPU Control | Enable C6

Enable C6	
Disable the C6 Power State.	
Disabled	C6 disabled
Enabled	C6 enabled

Processor power-state **C6** is the second lowest power sleep state. When in C6 the CPU state is saved to internal SRAM and the core voltage reduced to almost zero.

5.35.15 Power | Advanced CPU Control | Max DeepCState

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

Max DeepCState	
Select the deepest sleep state that the CPU will support.	
Disabled	C7 and C7s are not supported
C7	Limit C-state transitions to C7
C7s	C7s is the deepest supported sleep state

Processor power-state **C7** is the lowest-power sleep state that was introduced with the Intel Core i7 CPU. On entering C7 the last level cache is also flushed. If the C7s sub-state is selected, the last level cache will be flushed as one block instead of using multiple steps.

5.35.16 Power | Advanced CPU Control | C-State Auto Demotion

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

C-State Auto Demotion	Caution
Temporarily limit the depth of C-state transitions to C1 or C3 in order to keep power consumption low.	
Disabled	Don't limit the depth of C-state transitions
C1 only	Limit transitions to C1
C 3 only	Limit transitions to C3
C1 and C3	Limit transitions to C1 and C3

If the processor switches to the lowest power states (C6/C7) too frequently then the current required to transition back to C0 will actually result in an overall increase in power consumption.

When this option is selected the CPU monitors the frequency of C6/C7 transitions and temporarily restricts the depth of C-state transition to C1 and/or C3 to keep the overall power consumption low.

WARNING: Disabling this option may increase the overall CPU power consumption when cores are lightly loaded.

5.35.17 Power | Advanced CPU Control | C-State Auto Un-demotion

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

C-State Auto Un-demotion	Caution
Allow demoted C-state transitions to be un-demoted and reach their original target.	
Disabled	Don't un-demote C-state transitions
C1 only	Allow un-demotion of demoted C1 transitions
C 3 only	Allow un-demotion of demoted C3 transitions
C1 and C3	Allow un-demotion of demoted C1 and C3 transitions

When this option is enabled the CPU can allow demoted C-state transitions that were initially targeted for C6 or C7 to transition to their original target state after initially entering the demoted state.

5.35.18 Power | Advanced CPU Control | Package C-State Demotion

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

Package C-State Demotion	Caution
Temporarily limit the depth of package-level C-state transitions in order to keep power consumption low.	
Disabled	Don't limit the depth of C-state transitions
Enabled	Limit transitions to C1 and C3

If the processor switches to the lowest power states (C6/C7) too frequently then the current required to transition back to C0 will actually result in an overall increase in power consumption.

When this option is selected the CPU monitors the frequency of C6/C7 transitions and temporarily restricts the depth of C-state transition to C1 and/or C3 to keep the overall power consumption low.

5.35.19 Power | Advanced CPU Control | Package C-State Un-demotion

NOTE: This option is only available when C-States are Enabled (Section 5.35.11).

Package C-State Un-demotion	Caution
Allow demoted C-state transitions to be un-demoted and reach their original target.	
Disabled	Don't un-demote C-state transitions
Enabled	Allow un-demotion of demoted C1 and C3 transitions

When this option is enabled the CPU can allow demoted C-state transitions that were initially targeted for C6 or C7 to transition to their original target state after initially entering the demoted state.

5.35.20 Power | Advanced CPU Control | ACPI 5.0 CPPC Support

ACPI 5.0 CPPC Support	
Enable ACPI 5.0 Collaborative Processor Performance Control.	
Disabled	CPPC support disabled
Enabled	CPPC support enabled

When this option is enabled ACPI tables exposed by the board will include Collaborative Processor Performance Control. This feature was introduced as part of the ACPI 5.0 specification and provides a new way for the operating system to control the hardware performance.

When disabled the legacy processor interfaces will be used.

5.35.21 Power | Advanced CPU Control | ACPI 5.0 CPPC Platform SCI

NOTE: This option is only available when ACPI 5.0 CPPC Support is Enabled (Section 5.35.20).

ACPI 5.0 CPPC Platform SCI	
Use SCI to signal completion of CPPC commands	
Disabled	The operating system must poll for command completion
Enabled	SCI is used to signal command completion

5.35.22

5.35.23 Power | Advanced CPU Control | Turbo Mode

NOTE: Certain board variants intended for harsh environments require greater control over CPU power dissipation and in those cases Turbo Mode is not available.

Turbo Mode	Caution
Enable the CPU Turbo Mode.	
Disabled	Turbo Mode disabled
Enabled	Turbo Mode enabled

When Turbo Mode is **Enabled**, the frequency of individual CPU cores can be increased above the rated CPU frequency to provide a short burst of additional processing capacity. Turbo Mode is only engaged when the package temperature, power and current consumption allow.

Turbo Mode offers maximum processing performance at the expense of variable latency due to fluctuations in the core frequencies.

WARNING: The CPU does not report the actual clock frequency when Turbo Mode is engaged; instead it indicates 1 MHz above the rated frequency.

5.35.24 Power | Advanced CPU Control | Config TDP Configurations

Config TDP Configurations
Configure options related to the CPU Thermal Design Power (TDP).

The options available through this sub-menu are beyond the scope of this document.

WARNING: Making changes to settings found within these sub-menus can reduce the performance of the CPU.

5.36 Power | Platform Power Management

This menu provides options for configuring platform low-power states.

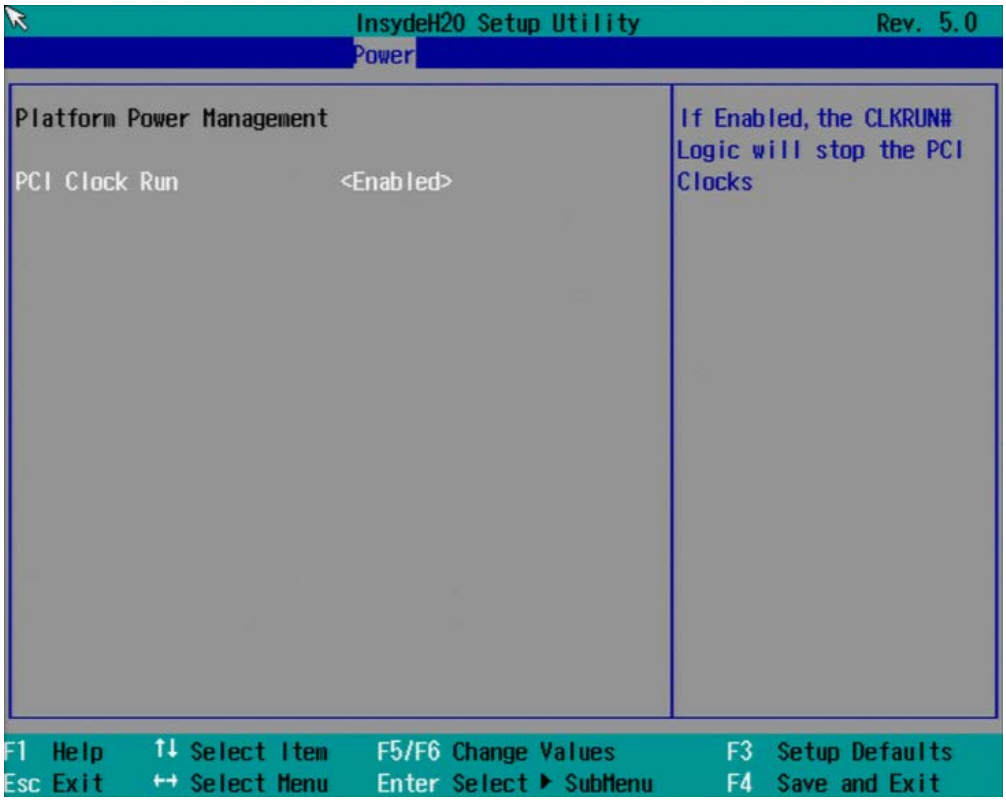


Figure 5-46 Power – Platform Power Management Menu

5.36.1 Power | Platform Power Management | PCI Clock Run

PCI Clock Run:	
Disable PCI Clock Run (CLKRUN#) logic.	
Disabled	CLKRUN# disabled
Enabled	CLKRUN# enabled

When set to **Enabled** the PCI Clock Run (**CLKRUN#**) logic can save power by stopping PCI clocks if the bus is inactive. The disadvantage of this setting is increased latency when restarting the clocks.

5.37 Vme

The **Vme** Setup menu configures options for the VMEbus inbound and outbound images. See Section 12 for more details of how VMEbus setup information is passed to the operating system driver.

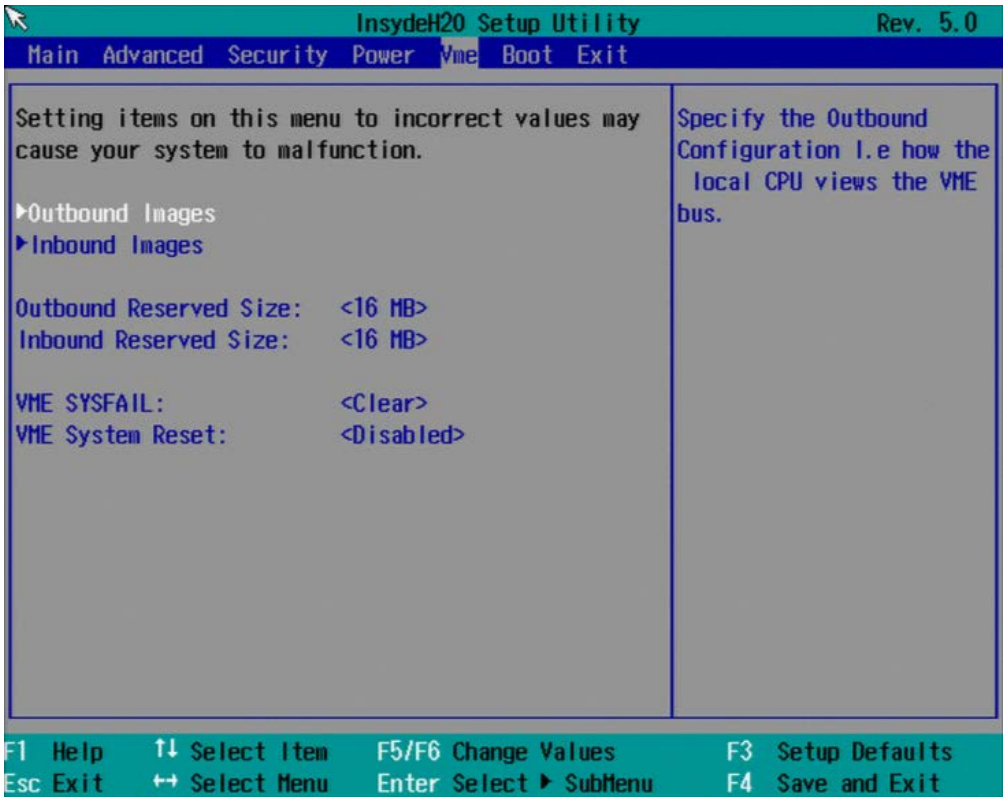


Figure 5-47 Vme Menu

5.37.1 Vme | Outbound Images

Outbound Images
Configure options for VME Outbound Images.

Outbound Images give the local CPU access to the VME bus address space. Setup options for the Outbound Images are detailed in Section 5.38.

5.37.2 Vme | Inbound Images

Inbound Images
Configure options for VME Inbound Images.

Inbound Images map VME bus accesses onto the boards DRAM. Setup options for the Inbound Images are detailed in Section 5.39.

5.37.3 Vme | Outbound Reserved Size

Outbound Reserved Size	
Configure the address space size reserved for Outbound Images.	
16 Mbyte	Reserved address-space size
32 Mbyte	
64 Mbyte	
128 Mbyte	
256 Mbyte	
512 Mbyte	
1 Gbyte	

VME drivers require a fixed block of address space below 4 GB for mapping Outbound Images and DMA transfers. Therefore the BIOS must reserve a block of address space before the top-of-DRAM is locked down.

This option specifies the reserved block size. The reserved address space can then be used by the BIOS to map Outbound Images configured through the Setup Utility and/or by an operating system driver. The address of the reserved address range is communicated to operating systems via a memory structure that is constructed by the BIOS. Further details of this structure are given in Section 12.

5.37.4 Vme | Inbound Reserved Size

Inbound Reserved Size	
Configure the size of memory reserved for Inbound Images.	
16 Mbyte	Reserved memory size
32 Mbyte	
64 Mbyte	
128 Mbyte	
256 Mbyte	
512 Mbyte	
1 Gbyte	

VME drivers require a fixed block of direct mapped DRAM for mapping Inbound Images and DMA transfers. Therefore the BIOS must reserve a block of DRAM separate from any memory used by the operating system.

This option specifies the reserved block size. The reserved memory can then be used by the BIOS to map Inbound Images configured through the Setup Utility and/or by an operating system driver. The address of the reserved address range is communicated to operating systems via a memory structure that is constructed by the BIOS. Further details of this structure are given in Section 12.

5.37.5 Vme | VME SYSFAIL

VME SYSFAIL	
Specify the state that SYSFAIL# is driven to prior to entering the boot loader.	
Don't Clear	Leave SYSFAIL# low
Clear	Drive SYSFAIL# high

SYSFAIL# is an active-low, bi-directional VME backplane signal.

If the board is installed in a 5-row VM64 backplane implementing the Geographic Address signals then **SYSFAIL#** will be automatically driven high (cleared) following application of board power.

5.37.6 Vme | VME System Reset

VME System Reset	
Select whether VME SYSRESET# can reset the board	
Disabled	SYSRESET# does not reset the board
Enabled	SYSRESET# resets the board

SYSRESET# is an active-low, input VME backplane signal.

5.38 Vme | Outbound Images

This menu provides options for configuring the VME Outbound Images. The BIOS Setup Utility supports configuring Image 0 and Image 1.

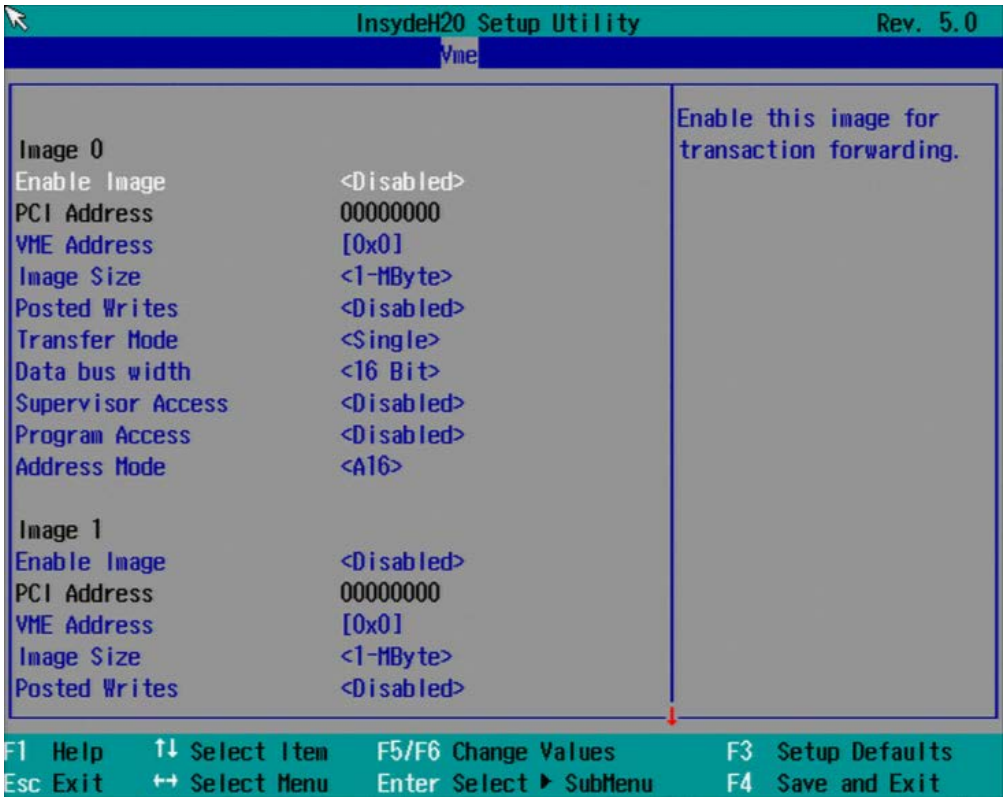


Figure 5-48 VME – Outbound Images Menu

NOTE: Menu items below 'Image 1' are initially off-screen and can be reached using the 'down arrow' cursor key.

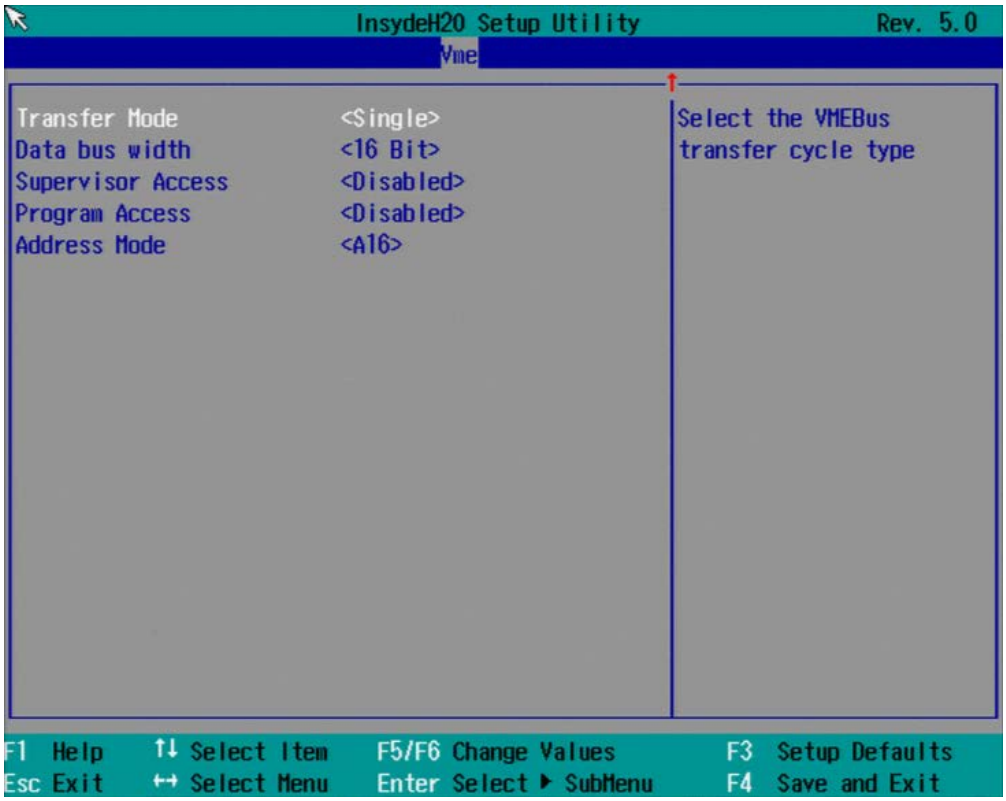


Figure 5-49 VME – Outbound Images Menu (continued)

NOTE: The following descriptions apply equally to Image 0 and Image 1.

5.38.1 Vme | Outbound Images | Image x | Enable Image

Enable Image	
Enable the image.	
Disabled	Image disabled
Enabled	Image enabled

When the image is **Enabled,** PCI transactions falling within the image window is decoded and forwarded to the VME bus.

5.38.2 Vme | Outbound Images | Image x | PCI Address

PCI Address	
Reports the PCI address assigned to the image.	
00000000	The image has not been configured
Non-zero value	The image has been configured by the BIOS

This option reports the PCI base address assigned to an enabled image by the BIOS. Once the image has been specified it is necessary to restart the board and re-enter Setup in order to see the BIOS assigned base address.

The PCI base address assigned to images configured via the Setup Utility is communicated to operating systems via a memory structure that is constructed by the BIOS. Further details of this structure are given in Section 12.

NOTE: Software and drivers should always read the Outbound Image PCI Address from the BIOS memory structure, since assigned addresses may change.

5.38.3 Vme | Outbound Images | Image x | VME Address

VME Address	
Set bits[31:16] of the base address for VME transfers	
[16-bit value]	VME base address

This option sets the VME base address corresponding to the PCI Address above. There is no special alignment requirement when using this option.

Enter the address by typing the hexadecimal value.

5.38.4 Vme | Outbound Images | Image x | Image Size

Image Size	
Set the size of the decoded PCI image	
1 Mbyte	Image size
2 Mbytes	
4 Mbytes	
8 Mbytes	
16 Mbytes	
32 Mbytes	
64 Mbytes	
128 Mbytes	
256 Mbytes	
512 Mbytes	
1024 Mbytes	

5.38.5 Vme | Outbound Images | Image x | Posted Writes

Posted Writes	
Configure the image to support posted writes.	
Disabled	Posted writes disabled
Enabled	Posted writes enabled

5.38.6 Vme | Outbound Images | Image x | Transfer Mode

Transfer Mode	
Set the VME bus cycle type for accesses to this image	
Single	VME bus cycle type
Block	

5.38.7 Vme | Outbound Images | Image x | Data bus width

Data bus width	
Set the maximum VME data bus width for SCT and BLT modes.	
8 Bit	Data bus width
16 Bit	
32 Bit	
64 Bit	

5.38.8 Vme | Outbound Images | Image x | Supervisor Access

Supervisor Access	
Enable supervisory access for VME transfers performed via this image.	
Disabled	Non-privileged access
Enabled	Supervisory access

When **Enabled**, supervisor access is enabled in the transaction's Address Modifier (AM).

5.38.9 Vme | Outbound Images | Image x | Program Access

Program Access	
Select Program Access in the Address Modifier (AM) code for VME transfers performed via this image.	
Disabled	Data access
Enabled	Program access

When **Enabled**, program access is enabled in the transaction's Address Modifier (AM).

5.38.10 Vme | Outbound Images | Image x | Address Mode

Address Mode	
Select the address mode Address Modifier (AM) used for VME transfers performed via this image.	
A16	Address Mode
A24	
A32	
CSR	
User 1	
User 2	

The settings for **Supervisor Access** and **Program Access** (above) are combined with this setting to determine the address modifier (AM) for the image.

5.39 Vme | Inbound Images

This menu provides options for configuring the VME Inbound Images. The BIOS Setup Utility supports configuring Image 0 and Image 1.

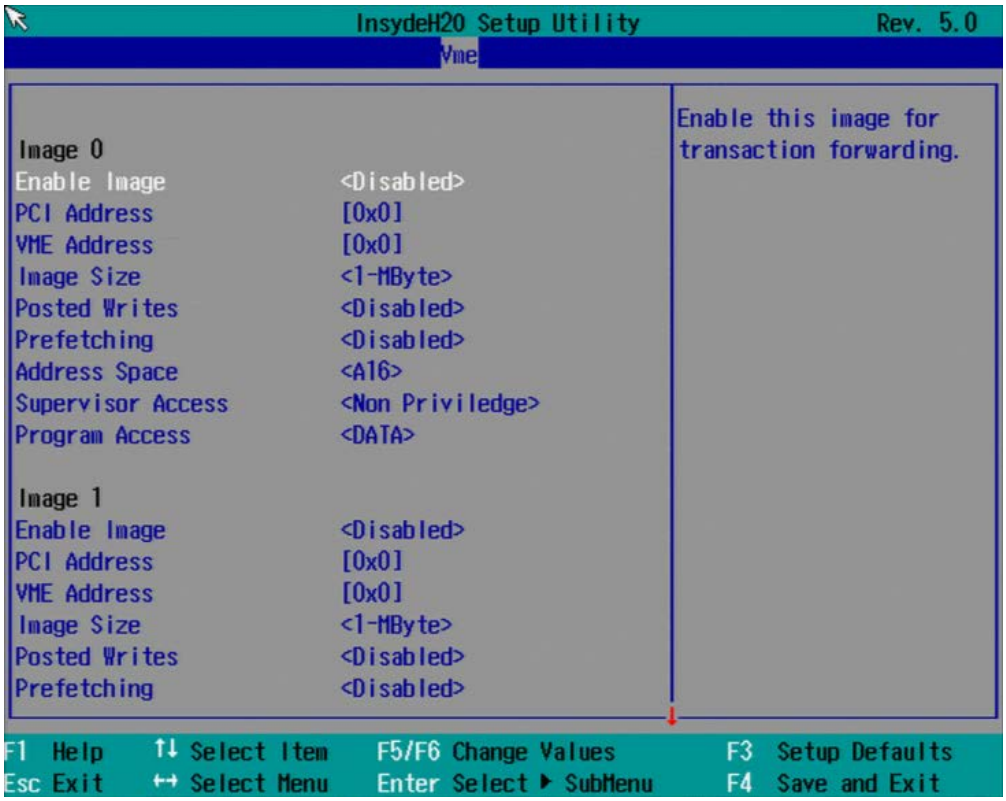


Figure 5-50 VME – Inbound Images Menu

NOTE: Menu items below 'Image 1' are initially off-screen and can be reached using the 'down arrow' cursor key.

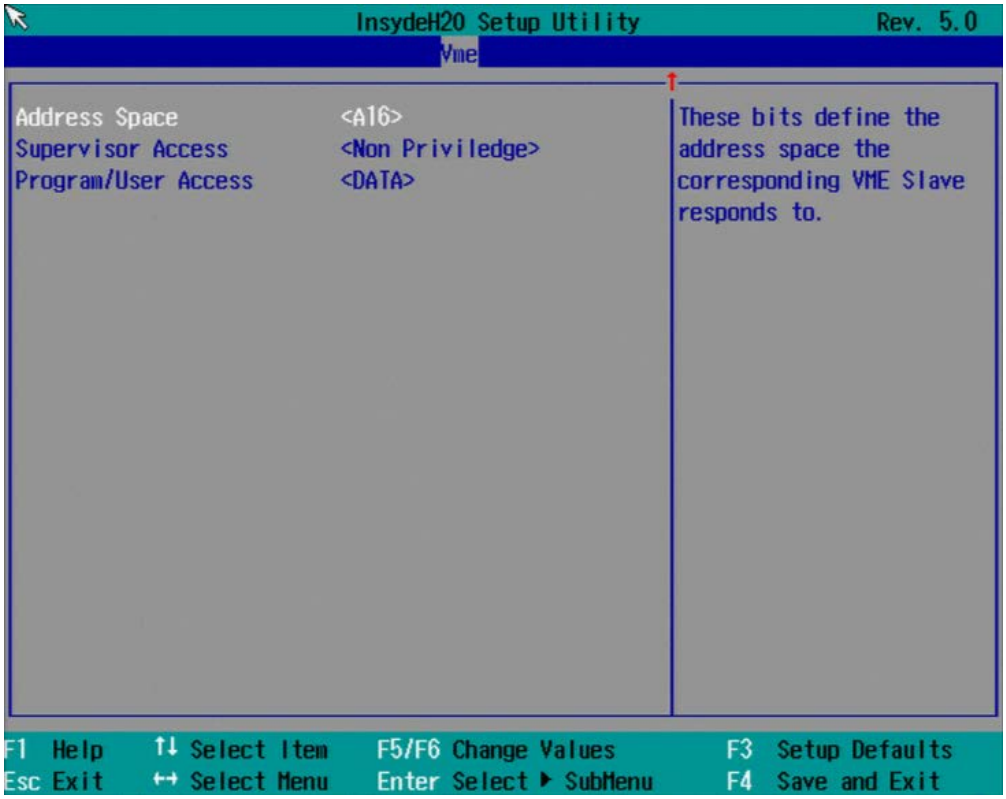


Figure 5-51 VME – Inbound Images Menu (continue)

NOTE: The following descriptions apply equally to Image 0 and Image 1.

5.39.1 Vme | Inbound Images | Image x | Enable Image

Enable Image	
Enable the image.	
Disabled	Image disabled
Enabled	Image enabled

When the image is enabled, VME transactions falling within the image window is decoded and forwarded to the PCI bus.

5.39.2 Vme | Inbound Images | Image x | PCI Address

PCI Address	Caution
Set bits[31:16] of the base address for PCI transfers	
[16-bit value]	PCI base address

This option sets the base address for PCI transfers driven by accesses from the VME bus.

Enter the address by typing the hexadecimal value.

WARNING: This option allows users to direct VME transactions to any region of the local 32-bit address space. Users have to ensure that the selected address range does not conflict with the memory used by the operating system. There is no special alignment required when using this option.

5.39.3 Vme | Inbound Images | Image x | VME Address

VME Address	
Set bits[31:16] of the base address for VME transfers	
[16-bit value]	VME base address

This option sets the VME base address corresponding to the PCI Address above. There is no special alignment required when using this option.

Enter the address by typing the hexadecimal value.

5.39.4 Vme | Inbound Images | Image x | Image Size

Image Size	
Set the size of the decoded PCI image	
1-Mbyte	Image size
2 Mbytes	
4 Mbytes	
8 Mbytes	
16 Mbytes	
32 Mbytes	
64 Mbytes	
128 Mbytes	
256 Mbytes	
512 Mbytes	
1024 Mbytes	

5.39.5 Vme | Outbound Images | Image x | Posted Writes

Posted Writes	
Configure the image to support posted writes.	
Disabled	Posted writes disabled
Enabled	Posted writes enabled

5.39.6 Vme | Outbound Images | Image x | Prefetching

Prefetching	
Configure the image to support prefetching.	
Disabled	Prefetching disabled
Enabled	Prefetching enabled

5.39.7 Vme | Inbound Images | Image x | Address Space

Address Space	
Specify which Address Modifier (AM) this image responds to.	
A16	Address Space
A24	
A32	
User 1	
User 2	

The settings for **Supervisor Access** and **Program Access** (below) are combined with this setting to determine the Address Modifier (AM) for the image.

5.39.8 Vme | Inbound Images | Image x | Supervisor Access

Supervisor Access	
Specify which privilege-level Address Modifier (AM) this VME image responds to.	
Non Privilege	Non-privileged access only
Supervisor	Supervisory access only
Both	Allow access from either privilege level

5.39.9 Vme | Inbound Images | Image x | Program Access

Program Access	
Specify which data-access Address Modifier (AM) this VME image responds to.	
Data	Data access only
Program	Program access only
Both	Allow access from either data type

5.40 Boot

The **Boot** Setup menu provides options for managing the order of bootable devices and miscellaneous options relating to the boot process.

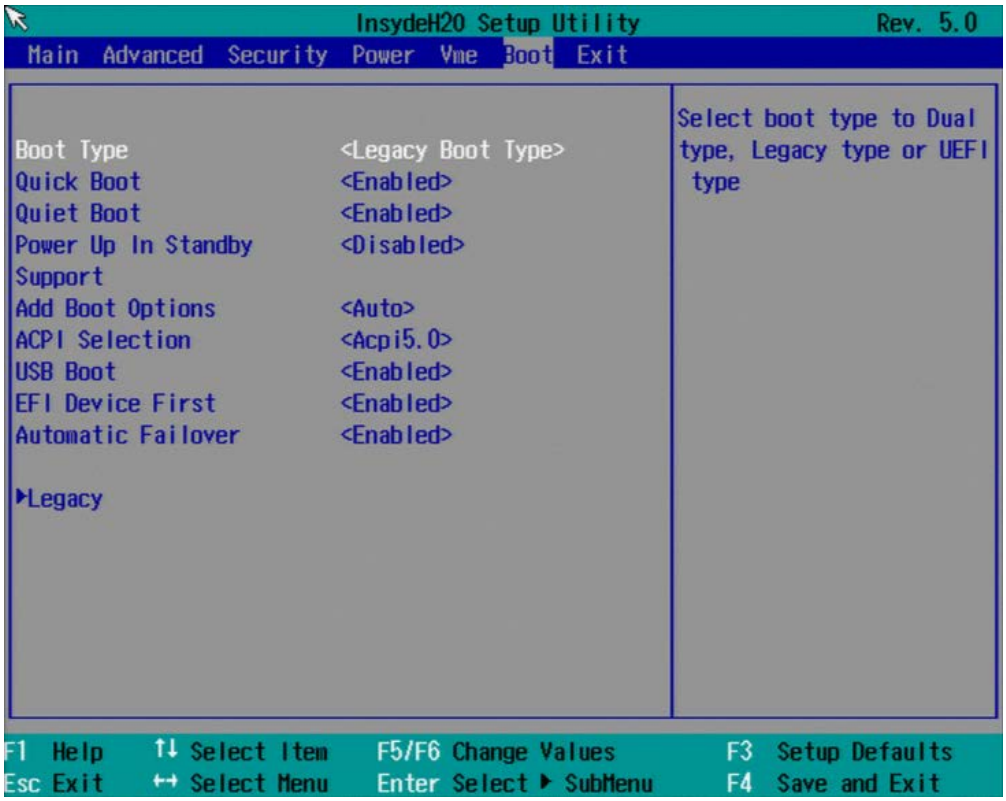


Figure 5-52 Boot Menu

5.40.1 Boot | Boot Type

Boot Type	
Select whether to support legacy boot, UEFI boot or both.	
Dual Boot Type	Boot from legacy or UEFI media
Legacy Boot Type	Boot from legacy media only
UEFI Boot Type	Boot from UEFI media only

When UEFI Boot Type or Dual Boot Type is selected then additional menu items will become available, see Section 5.44 for details.

Booting in UEFI mode is covered in more detail in Section 7.1.

5.40.2 Boot | Quick Boot

Quick Boot	
Disable the BIOS Quick Boot path.	
Enabled	Quick Boot enabled
Disabled	Quick Boot disabled

When **Quick Boot** is set to **Enabled** the BIOS will bypass non-essential POST tasks and hardware tests to decrease the BIOS boot time.

5.40.3 Boot | Quiet Boot

Quiet Boot	
Select between graphics mode and text mode POST screens	
Enabled	Graphics mode
Disabled	Text mode

When **Quiet Boot** is set to **Enabled** the BIOS POST screen uses graphics mode and reports minimal details regarding boot progress.



Figure 5-53 Graphics Mode POST Screen

When **Quiet Boot** is set to **Disabled** the BIOS POST screen switches to text mode and provides more on-screen detail regarding the boot process.

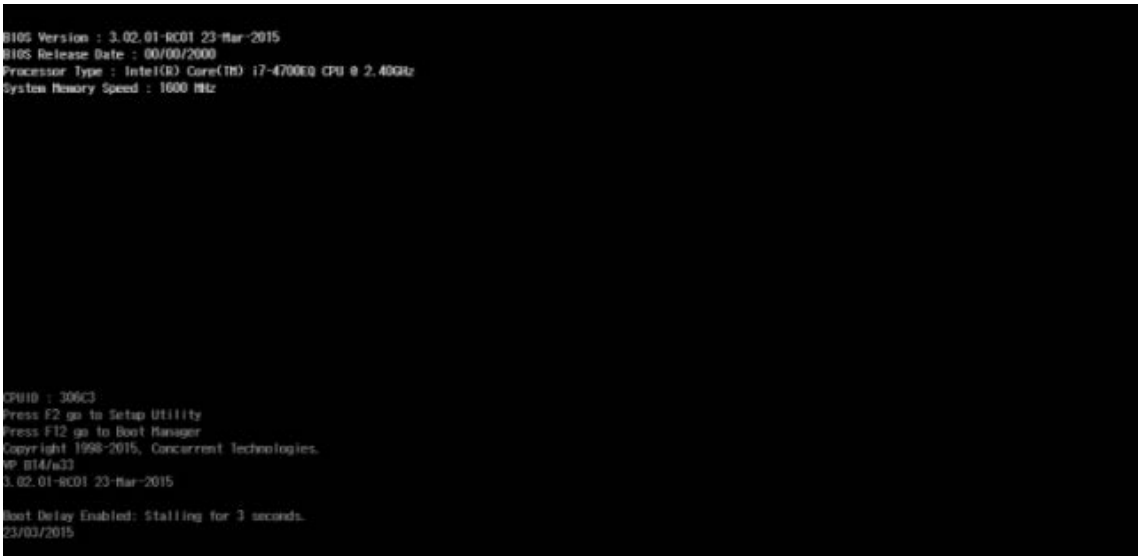


Figure 5-54 Text Mode POST Screen

5.40.4 Boot | Power Up In Standby Support

Power Up In Standby Support	
Enable delayed Hard Disk Drive spin-up.	
Enabled	Delay drive spin-up until commanded
Disabled	Drives spin up when power is applied

When set to **Enabled**, Hard Disk Drives will power on in standby mode and platter spin-up will be delayed until the spin-up command is issued. Enabling this option will conserve power and reduce the power-on current surge.

5.40.5 Boot | Add Boot Options

Add Boot Options	
Specify how newly discovered boot devices are added to the boot order.	
First	Add new devices at top of list
Last	Add new devices at end of list
Auto	Use normal BIOS ordering rules

When bootable removable drives are used (e.g. USB flash drives) then **First** should be selected to ensure that the BIOS will automatically boot from the new device. When removable data drives are used **Last** should be selected to maintain the existing boot order.

5.40.6 Boot | ACPI Selection

ACPI Selection	
Select ACPI specification version supported in the ACPI tables.	
Acpi1.0B	ACPI specification support level
Acpi3.0	
Acpi4.0	
Acpi5.0	

The ACPI specification support level determines which features of the CPU and chipset are exposed through ACPI; Table 5-9 summarizes the changes between versions.

ACPI Specification	Added Features
1.0b	N/A
3.0	SATA, PCI Express, Extended thermal model
4.0	Logical processor idling, USB3.0
5.0	Improve and extend hardware platform description

Table 5-9 ACPI Specification Feature Additions

Most modern operating systems support ACPI 4.0 to gain maximum control over performance and power management; however older operating systems like Microsoft Windows XP are limited to ACPI 1.0b.

5.40.7 Boot | USB Boot

USB Boot	Caution
Disable support for booting from USB devices.	
Enabled	USB device boot enabled
Disabled	USB device boot disabled

Removable USB devices can represent a security threat and it may be desirable to prevent users booting from USB connected media. Maximum platform security can be achieved by setting this option to **Disabled** and then configuring password authentication through the Security options (see Section 5.30).

5.40.8 Boot | EFI Device First

EFI Device First	
Select whether the BIOS attempts boot from EFI devices before Legacy devices.	
Disabled	Give preference to Legacy boot devices
Enabled	Give preference to EFI boot devices

If no bootable device is found within the preferred boot category, the BIOS will attempt to boot from devices in the second category.

5.40.9 Boot | Automatic Failover

Automatic Failover	
Select whether the BIOS attempts boot from each device in turn, or halts if the first boot device fails.	
Disabled	Halt with warning if booting from the first device fails
Enabled	Attempt to boot from each device in turn

5.40.10 Boot | Legacy

NOTE: This option is only available when the Boot Type is set to **Legacy** or **Dual Boot Type**.

Legacy
Configure device boot order in Legacy boot mode.

The Legacy options are detailed in Section 5.41.

5.41 Boot | Legacy

This menu provides options for configuring boot device priorities for the legacy boot manager.

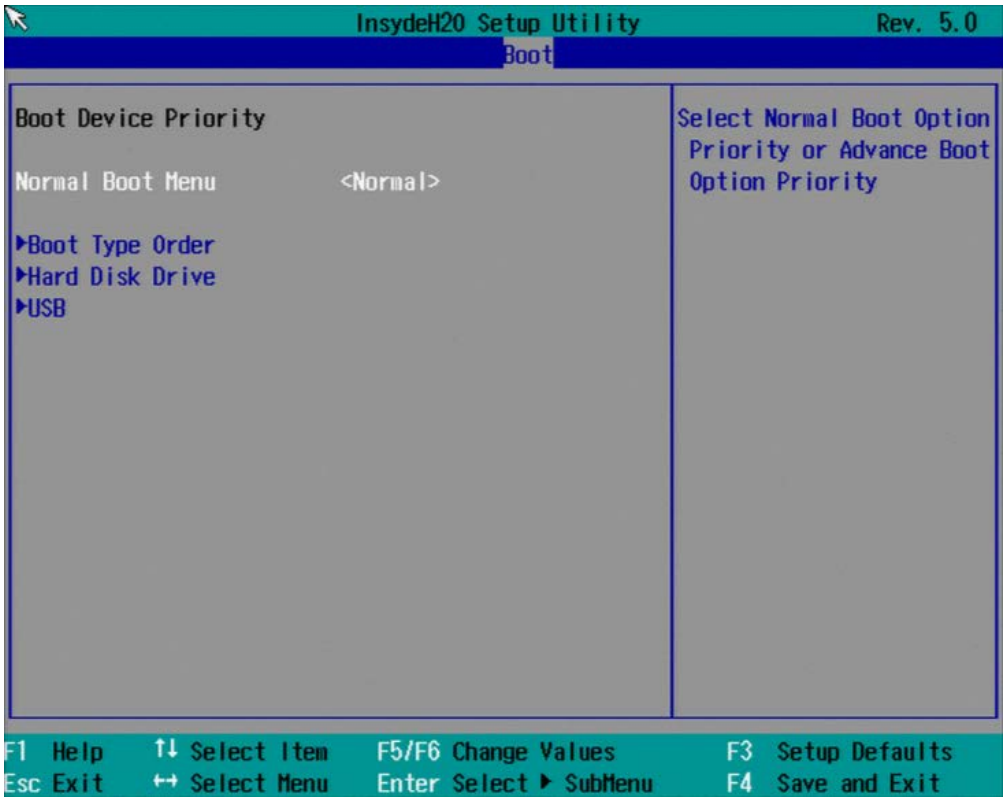


Figure 5-55 Boot – Legacy Menu

5.41.1 Boot | Legacy | Normal Boot Menu

Normal Boot Menu	
Selects how the boot device priority is specified.	
Normal	Boot order specified by device categories
Advance	Boot order specified by individual devices

When this option is set to **Normal** the boot manager determines the boot order using generic device categories; when set to **Advanced** the boot manager determines the boot order on an individual device basis.

The **Advanced** mode provides the greatest flexibility when specifying the boot order, however it also requires a more detailed knowledge of attached device types, serial numbers and PCI function addresses. The **Advanced** mode options are described in Section 5.44.

5.41.2 Boot | Legacy | Boot Type Order

Boot Type Order
Specify the boot order based on device categories.

The Boot Type Order options are detailed in Section 5.42.

5.41.3 Boot | Legacy | [device category]

[device category]
Specify the boot order for devices in a particular category.

A sub-menu is created for each device category where there is an installed device. For the example configuration shown in Figure 5-55 sub-menus have been created for the **Hard Disk Drive** and **USB** device categories. All device categories have the same options and these are detailed in Section 5.43.

5.42 Boot | Legacy | Boot Type Order

This menu provides options for configuring boot devices based on their device category.

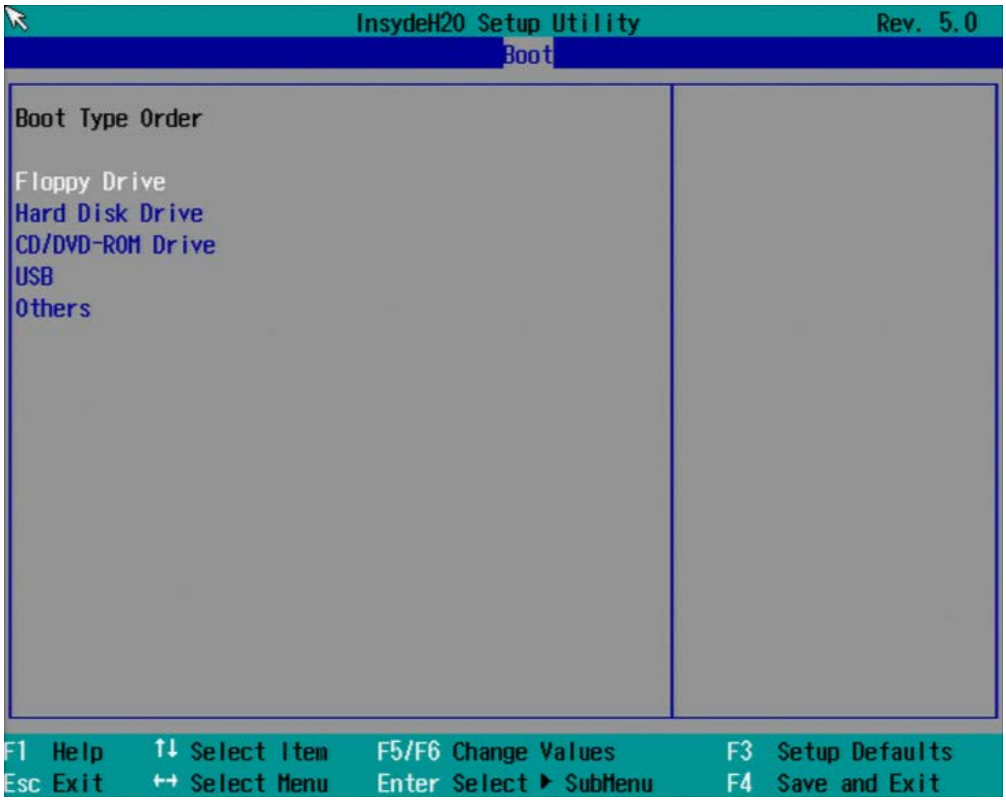


Figure 5-56 Boot – Boot Type Order Menu

Selecting a device category from the list and using the <**+** > and <**-**> keys will move it up or down the boot order. Once the changes made via the Setup Utility have been saved, the boot order will be preserved provided no devices are added or removed.

NOTE: The screen shot (Figure 5-56) and the sub-sections below are based on the default category ordering.

5.42.1 Boot | Legacy | Boot Type Order | Floppy Drive

Floppy Drive
Specifies the relative position within the boot order of the Floppy Drive device class.

When <**Enter**> is pressed, this option responds with a further Setup menu where the boot order of all Floppy Drives can be specified. See Section 5.43 for an example device-boot-order configuration menu.

5.42.2 Boot | Legacy | Boot Type Order | USB

USB
Specifies the relative position within the boot order of the USB category.

When <**Enter**> is pressed, this option responds with a further Setup menu where the boot order of all USB devices can be specified. See Section 5.43 for an example device-boot-order configuration menu.

5.42.3 Boot | Legacy | Boot Type Order | Hard Disk Drive

Hard Disk Drive
Specifies the relative position within the boot order of the Hard Disk Drive category.

When <**Enter**> is pressed, this option responds with a further Setup menu where the boot order of all Hard Disk Drives can be specified. See Section 5.43 for an example device-boot-order configuration menu.

5.42.4 Boot | Legacy | Boot Type Order | CD/DVD-ROM Drive

CD/DVD-ROM Drive
Specifies the relative position within the boot order of the CD-ROM and DVD-ROM Drive category.

When <**Enter**> is pressed, this option responds with a further Setup menu where the boot order of all CD-ROM and DVD-ROM Drives can be specified. See Section 5.43 for an example device-boot-order configuration menu.

5.42.5 Boot | Legacy | Boot Type Order | Others

Others
Specifies the relative position within the boot order of any devices that do not fit into one of the named categories.

When <**Enter**> is pressed, this option responds with a further Setup menu where the boot order of devices falling into the ‘Other’ category can be specified. See Section 5.43 for an example device-boot-order configuration menu.

5.43 Boot | Legacy | [device category]

This menu allows the boot order of devices within a specific category to be configured.

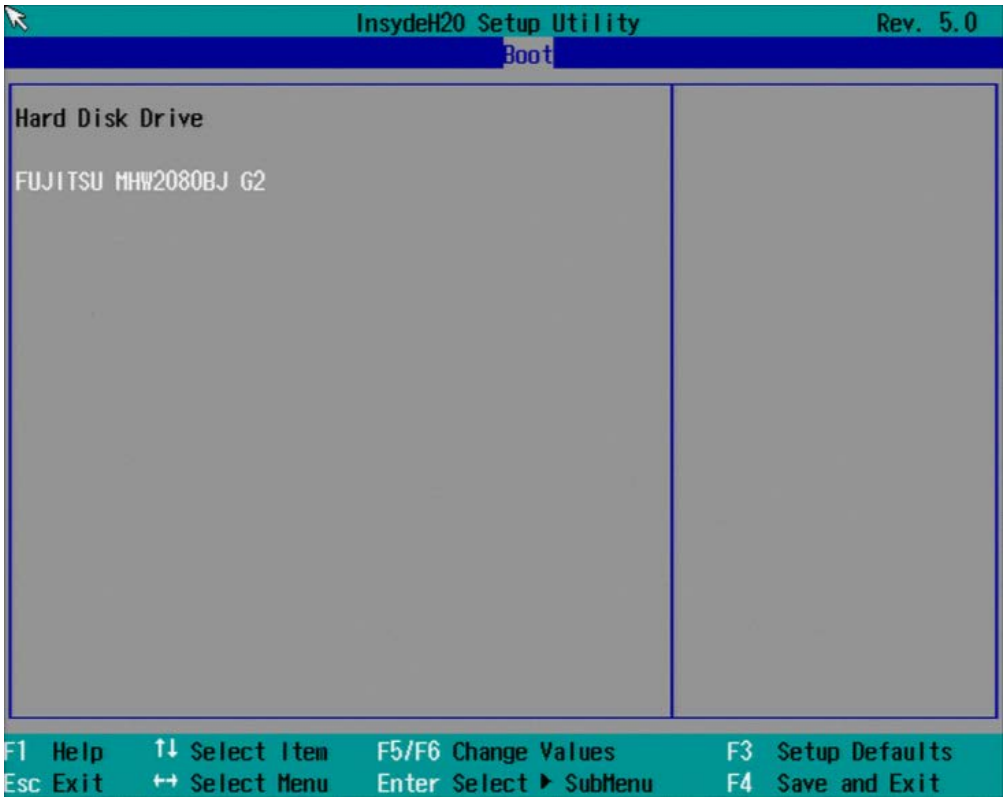


Figure 5-57 Boot – Device Category Menu

5.43.1 Boot | Legacy | [device category] | [device name]

[device name]	
The full device name held by the BIOS legacy boot manager.	
[device name]	The device name

Selecting a device from the list and using the <+ > and <-> keys will move it up or down the boot order. Once the changes made via the Setup Utility have been saved, the boot order will be preserved, provided no devices are added or removed.

5.44 Boot | Legacy | Normal Boot Menu = Advanced

When the **Normal Boot** Menu option is set to '**Advanced**' the boot order is managed on an individual device basis and a list of available boot devices is displayed by the BIOS.

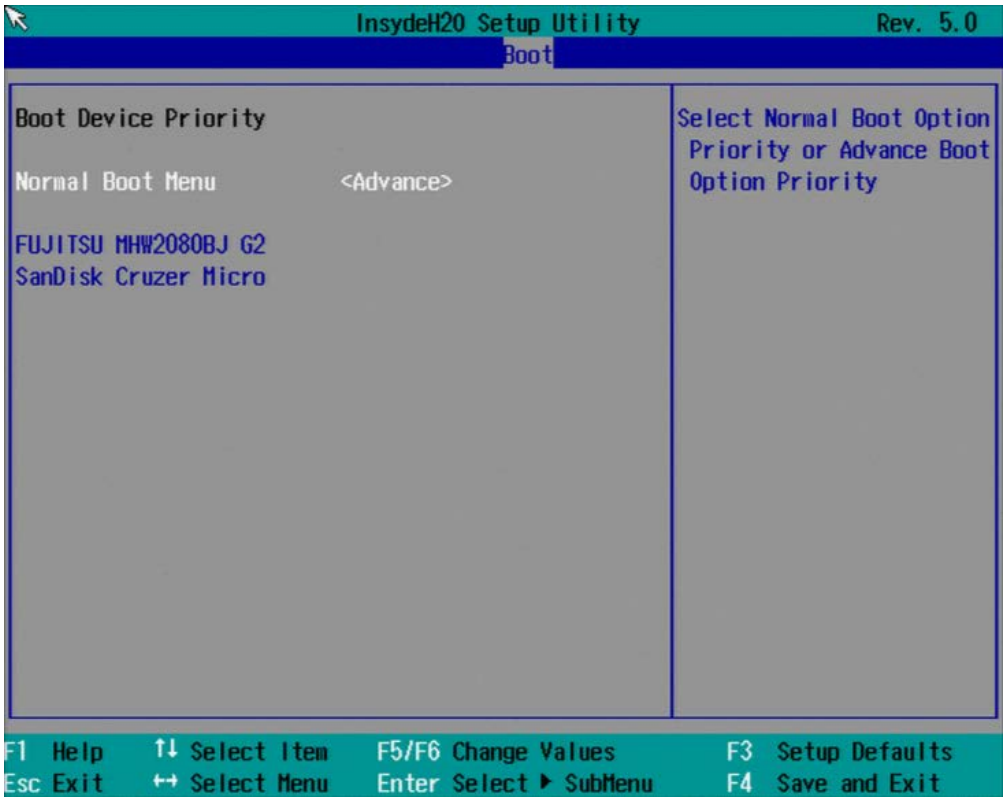


Figure 5-58 Boot – Advance Menu

5.44.1 Boot | Legacy | [boot device]

[boot device]	
The full device name held by the BIOS legacy boot manager.	
[device name]	The device name

NOTE: If there are no attached boot devices, or the BIOS fails to detect the boot device, this field will be absent from this Setup menu.

In the screenshot example the BIOS has detected two boot devices: a Hard Disk Drive and a USB memory drive:

FUJITSU MHW2080BJ G2
SanDisk Cruzer Micro

Selecting a device from the list and using the <**+** > and <**-**> keys will move it up or down the boot order. Once the changes made via the Setup Utility have been saved the boot order will be preserved providing no devices are added or removed.

5.45 Boot | Boot Type = UEFI Boot Type

When the **Boot Type** option is set to UEFI Boot Type, or Dual Boot Type, then additional options are displayed for configuring EFI boot devices.

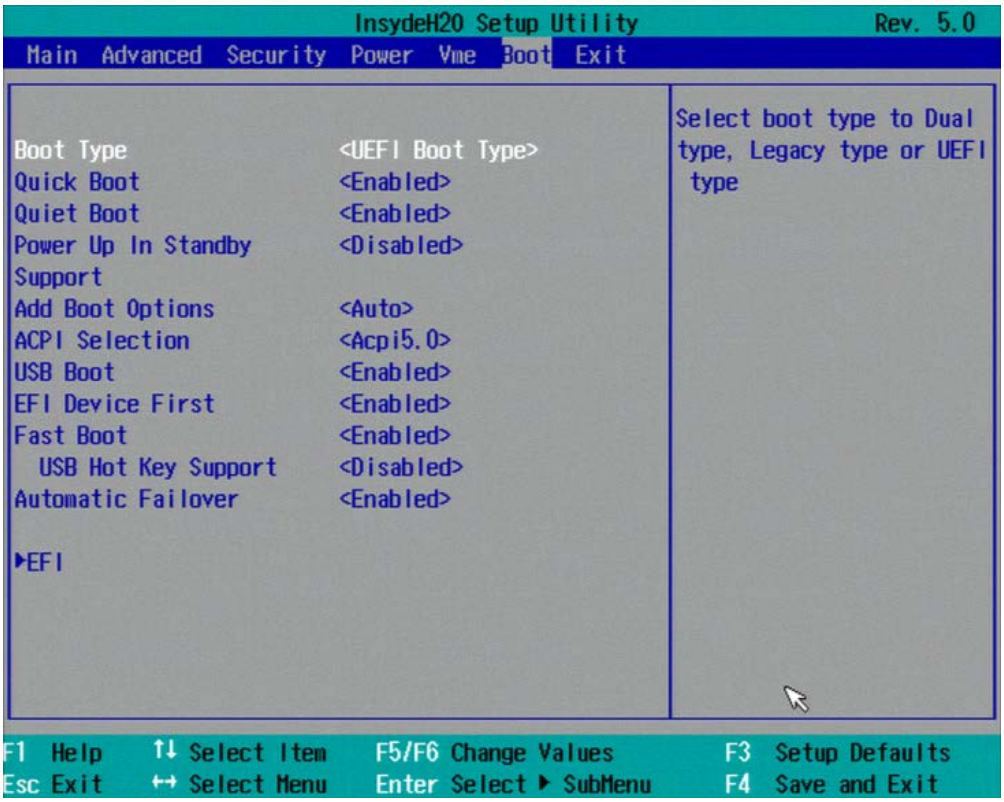


Figure 5-59 Boot Menu (Boot Type = UEFI Boot Type)

5.45.1 Boot | Fast Boot

Fast Boot	
Skip certain POST tasks to minimize boot time.	
Enabled	Enable Fast Boot features
Disabled	Don't skip startup tasks

When **Fast Boot** is enabled an additional option is displayed allowing finer-grained control over the Fast Boot process.

5.45.2 Boot | USB Hot Key Support

NOTE: This option is only available when **Fast Boot** is set to Enabled.

USB Hot Key Support	
Disable support for USB keyboard Hot Keys while booting.	
Enabled	Enable the UEFI shell
Disabled	Disable the UEFI shell

5.45.3 Boot | EFI

EFI
Configure device boot order in EFI boot mode.

The EFI boot order options are detailed in Section 5.46.

5.46 Boot | EFI

This menu provides options for configuring boot device priorities for the EFI boot manager.

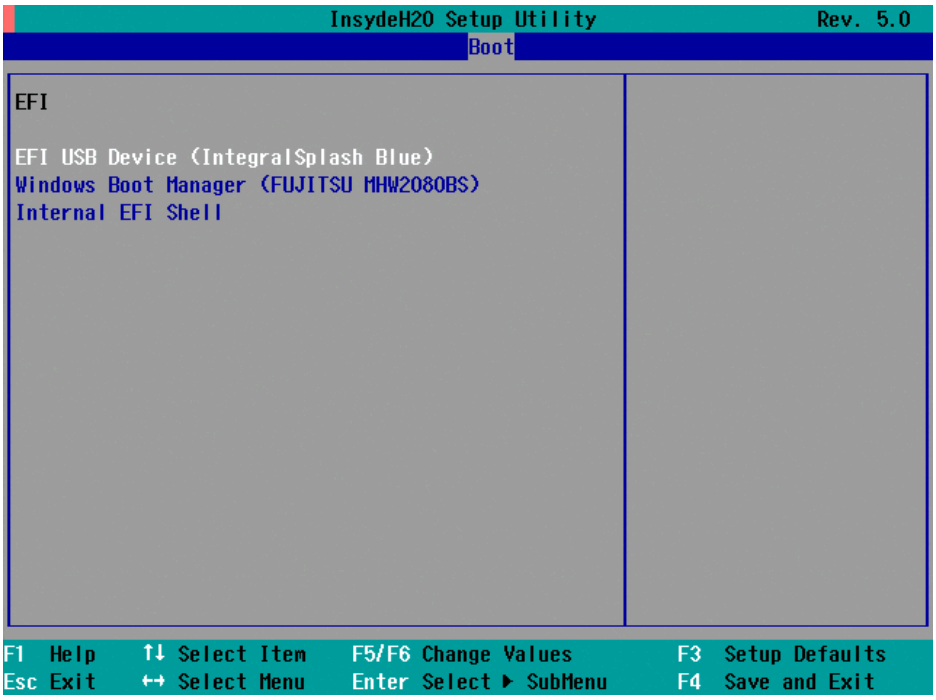


Figure 5-60 EFI Boot Menu

5.46.1 Boot | EFI | [device name]

[device name]	
The full device name held by the BIOS EFI boot manager	
[device name]	The device name

Selecting a device from the list and using the <+ > and <-> keys moves it up or down the boot order. Once the changes made via the Setup Utility have been saved, the boot order is preserved, provided no devices are added or removed.

5.46.2 Boot | EFI | Internal EFI Shell

Internal EFI Shell	
Boot placeholder for the UEFI Shell.	
Internal EFI Shell	Boot entry for the UEFI Shell

The UEFI Shell is managed as if it were a boot device. Selecting **Internal EFI Shell** from the list and using the <**+** > and <**-**> keys moves it up or down the boot order. Once the changes made via the Setup Utility have been saved, the boot order is preserved, provided no devices are added or removed.

When booting from the EFI shell, a number of maintenance and diagnostic functions become available to the user including: disk maintenance, executing shell scripts and pre-OS diagnostic applications, and automatic execution of a custom boot script.

For a more detailed description of the UEFI Shell refer to Section 8.

5.47 Exit

The **Exit** menu provides options for saving changes made via the Setup Utility.

From this screen, a user-defined Setup configuration can be saved or loaded and the board configuration can be restored to the factory specified defaults. See Section 4 for a detailed explanation of the different Setup configurations supported by the board.

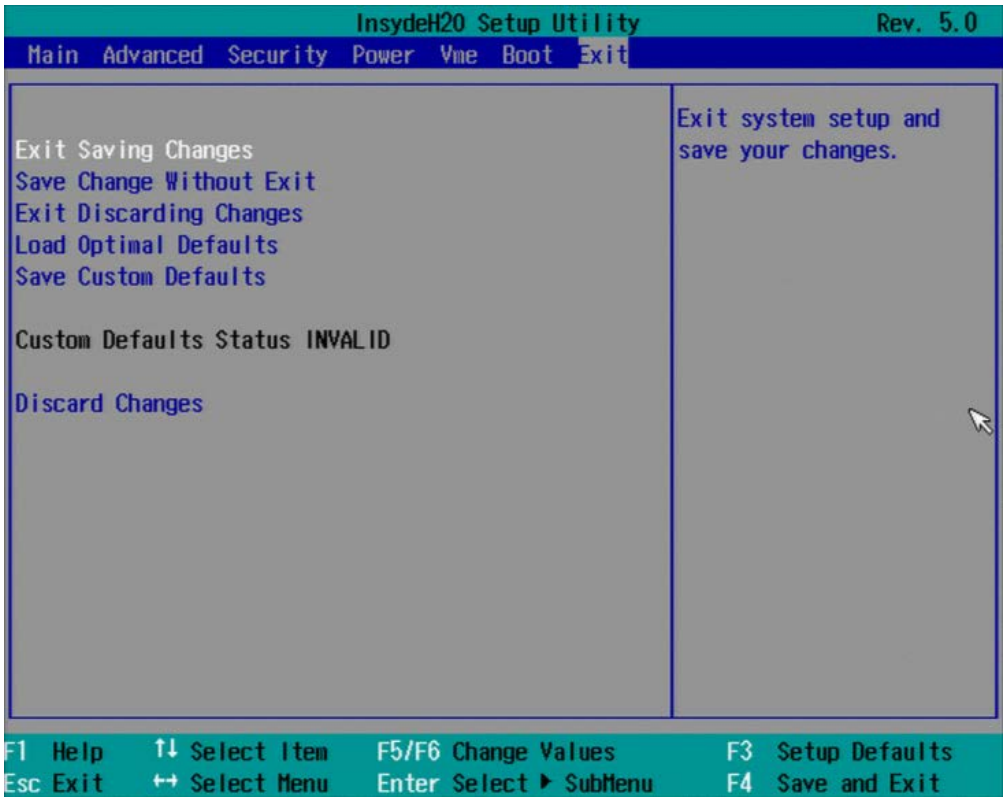


Figure 5-61 Exit Menu

NOTE: Most of the options provided by the **Exit** menu create pop-up menus with a **Yes**/**No** choice to confirm or abort the operation.

5.47.1 Exit | Exit Saving Changes

Exit Saving Changes
Save any changes made and restart the board.

This option responds with a confirmation dialog when selected (Figure 5-62).

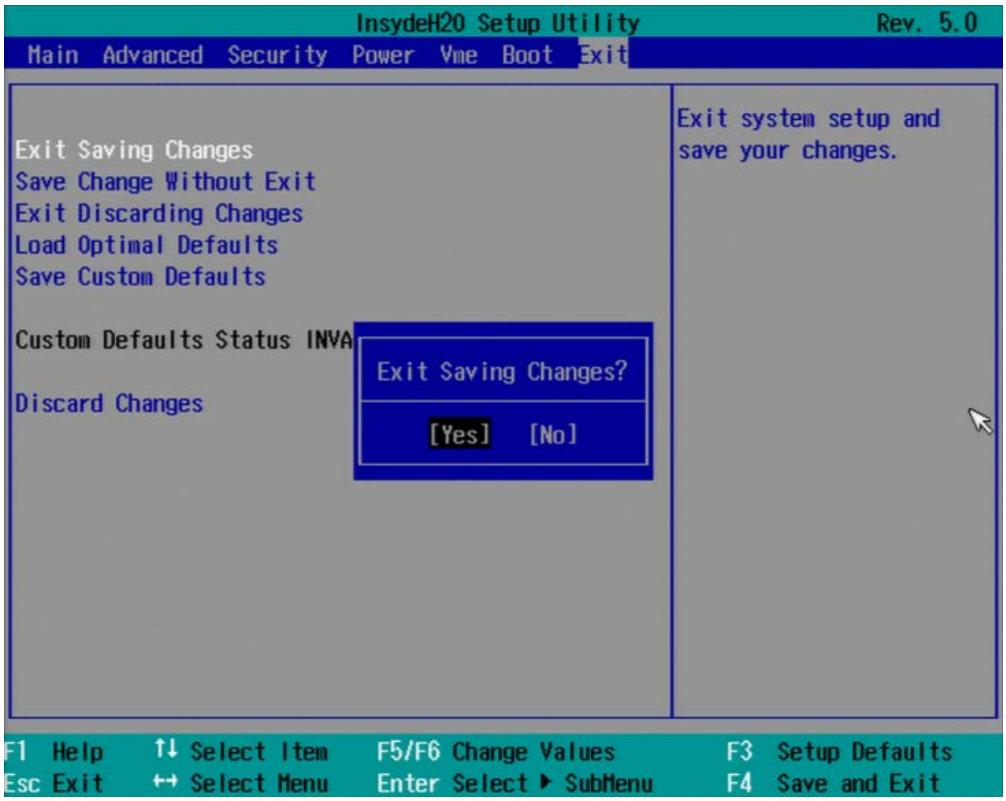


Figure 5-62 Exit – Exit Saving Changes Popup

If the choice is confirmed, all changes made via the Setup utility will be written to the Working Configuration. When the save completes the board will restart in order to load the new settings.

5.47.2 Exit | Save Change Without Exit

Save Change Without Exit
Save changes made so far, but remain in the Setup utility.

This option responds with a confirmation dialog when selected (Figure 5-63).

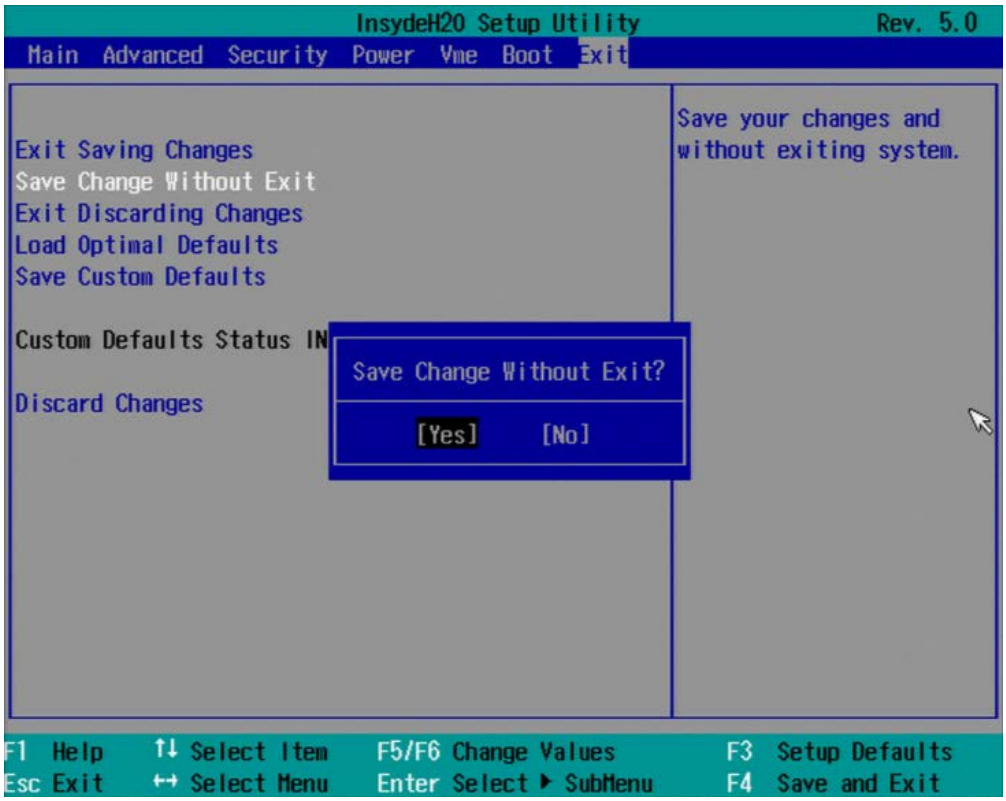


Figure 5-63 Exit – Save Change Without Exit Popup

If the choice is confirmed, all changes made via the Setup utility will be written to the Working Configuration. When the save completes the user will remain in the Setup Utility.

5.47.3 Exit | Exit Discarding Changes

Exit Discarding Changes
Discard any changes made since entering Setup and restart the board.

This option responds with a confirmation dialog when selected (Figure 5-64)

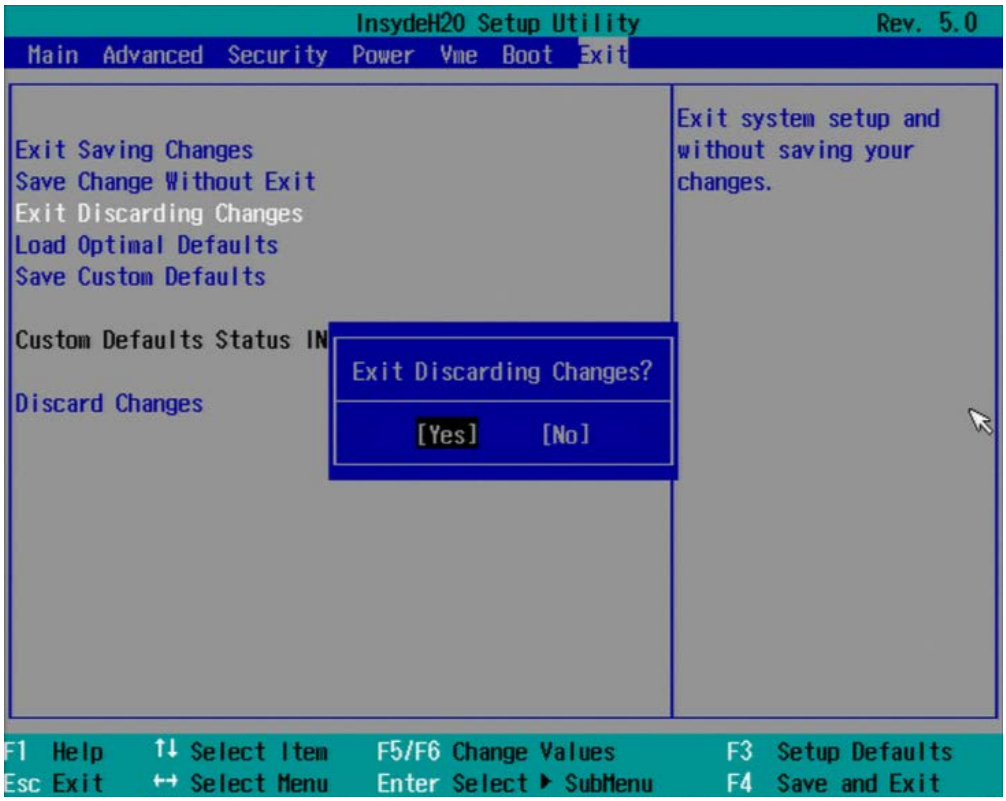


Figure 5-64 Exit – Exit Discarding Changes Popup

If the choice is confirmed any changes made via the Setup utility will be discarded and the board will continue operating with its existing configuration.

5.47.4 Exit | Load Optimal Defaults

Load Optimal Defaults
Load the factory-configured optimal defaults.

This option responds with a confirmation dialog when selected (Figure 5-65).

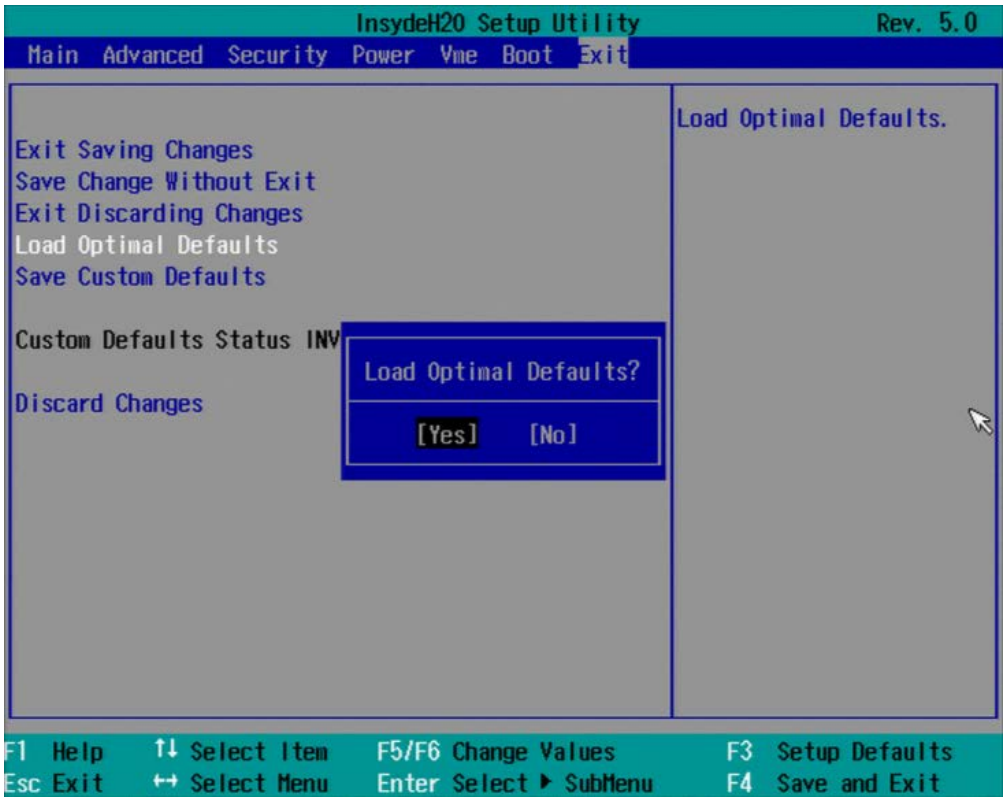


Figure 5-65 Exit – Load Optimal Defaults Popup

If the choice is confirmed any changes made via the Setup utility will be discarded and the board configuration will be loaded with the factory-specified Optimal Defaults.

5.47.5 Exit | Save Custom Defaults

Save Custom Defaults
Save current Setup configuration as custom defaults.

This option responds with a confirmation dialog when selected (Figure 5-66).

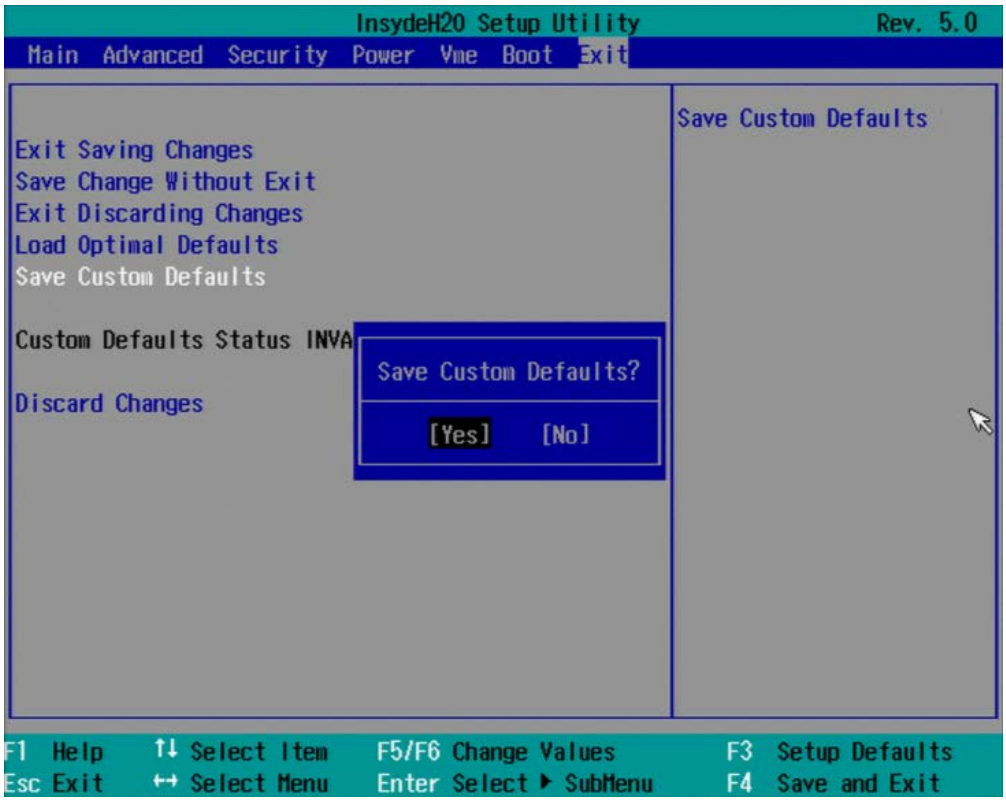


Figure 5-66 Exit – Save Custom Defaults Popup

If the choice is confirmed the Working Configuration and any changes made via the Setup utility will be written to the Custom Defaults.

Once the custom default settings have been saved, the **Custom Defaults Status** option changes to VALID and a further option for **Load Custom Defaults** becomes available, see Section 5.47.9 for details.

5.47.6 Exit | Custom Defaults Status

Custom Defaults Status	
Reports whether user-specified Custom Defaults are present in the BIOS ROM.	
INVALID	No Custom Defaults have been saved
VALID	Custom Defaults have been saved

5.47.7

5.47.8 Exit | Discard Changes

Discard Changes
Discard changes made so far, but remain in the Setup utility.

This option responds with a confirmation dialog when selected (Figure 5-67).

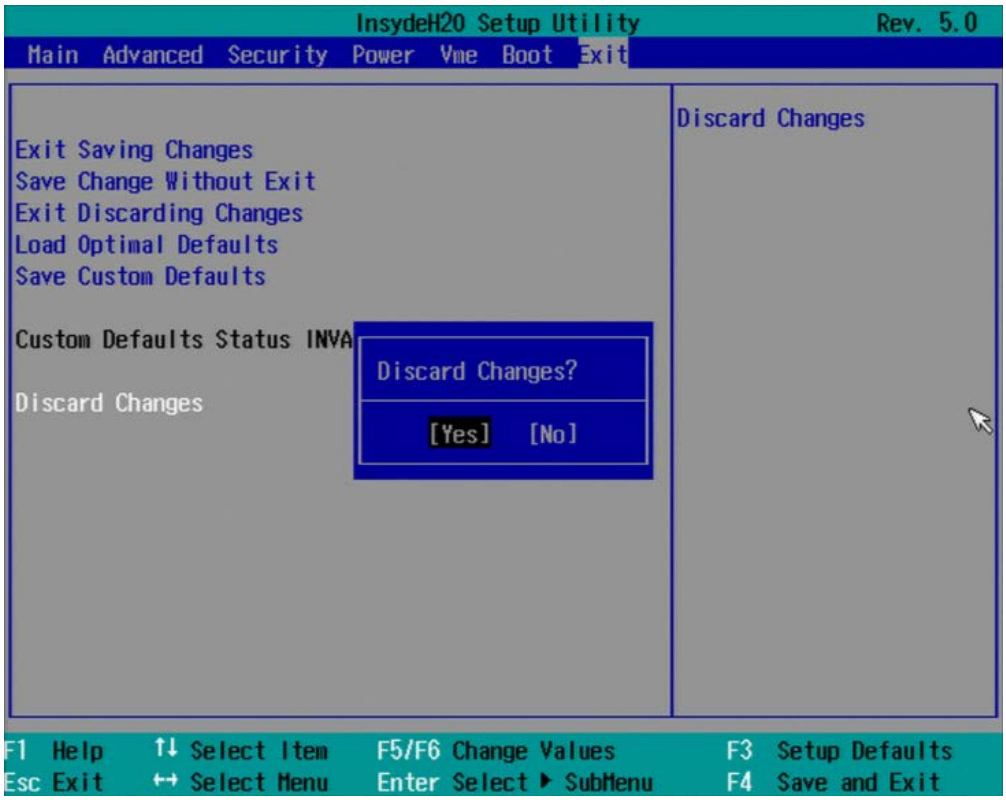


Figure 5-67 Exit – Discard Changes Popup

If the choice is confirmed any changes made via the Setup utility will be discarded and the Working Configuration will be reloaded.

5.47.9 Exit | Load Custom Defaults

NOTE: This option is only available after Save Custom Defaults has been used to save settings.

Load Custom Defaults
Load user defined custom defaults.

This option responds with a confirmation dialog when selected. If the user has not yet saved a custom configuration, an error message will be displayed. If a custom configuration has been created, a confirmation dialog will be displayed ().

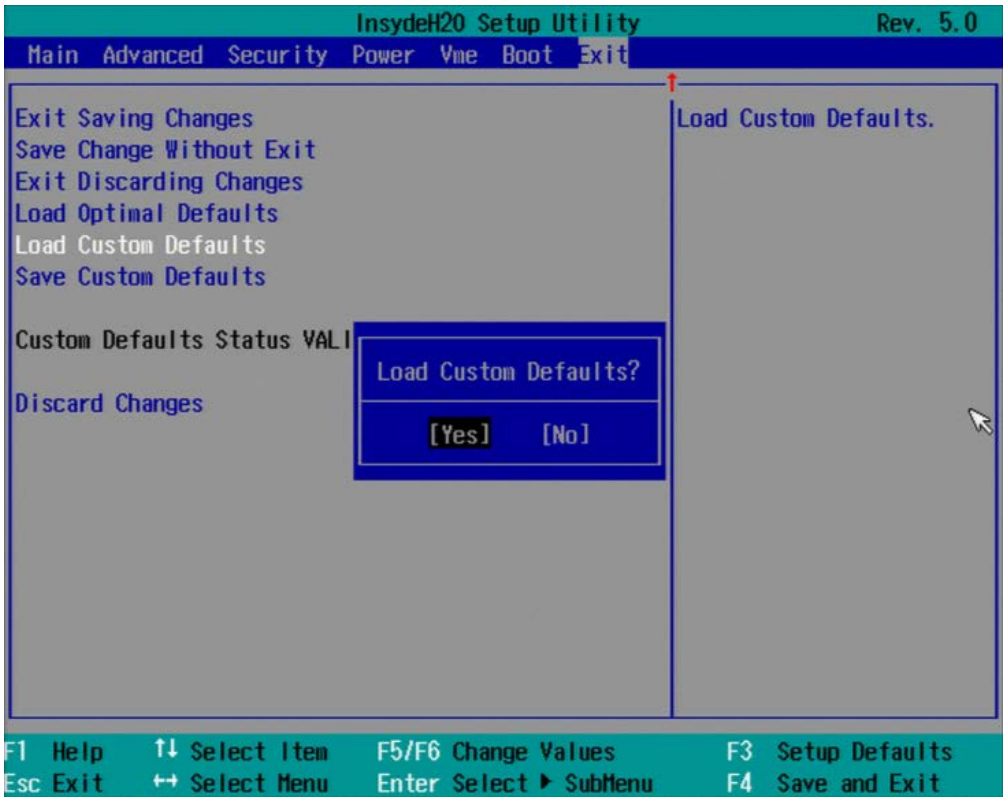


Figure 5-68 Exit – Load Custom Defaults Popup

If the choice is confirmed any changes made via the Setup utility will be discarded and the board configuration will be loaded with the user-specified Custom Defaults.

6 VGA AND SERIAL CONSOLES

6.1 Enabling Serial Console Mode

Concurrent Technologies boards can be used in systems where a VGA screen and keyboard are impractical, or are an unnecessary cost. However the user may still require access to the Setup Utility in order to configure the board; or may require visibility of POST output during boot.

The BIOS can optionally redirect all text-mode screen output and keyboard input to a serial terminal or suitably configured terminal emulation program. When used in the optimal PC-ANSI setting, the output very closely resembles that seen with a VGA display.

Figure 6-1 shows an example PC-ANSI Serial Console screen using the Tera Term terminal emulator.

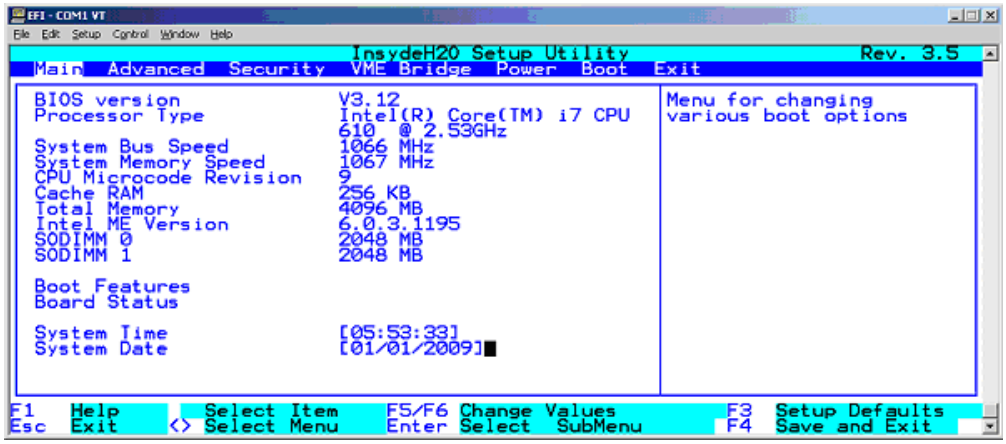


Figure 6-1 Example Setup Screen seen via Serial Console Mode

Serial Console mode is enabled via a switch. Refer to the board's Technical Reference manual for details of the switch location and settings.

6.2 COM Port Selection

The VP B1x/msd can use either COM1 (via the front panel) or COM2 (via the backplane J5 connector) for the BIOS serial console. Port selection is made via a switch - see the board's technical reference manual for details of the switch settings.

6.3 Protocol Options

The Serial Console operates by default at 115,200 Baud, 8 data bits, 1 stop bit and no parity. There is no flow control.

The serial console can be configured via Setup to use data rates between 9600 Baud and 115,200 Baud. Rates below 9600 Baud are not supported as boot time and board operation becomes severely limited by the link speed. Additional options are provided for specifying data-bit, stop-bit and parity settings and enabling flow control.

See Section 5.28 for details of the Serial Console configuration options.

6.4 Terminal Type Compatibility

The Serial Console can be configured to support a selection of industry-standard terminal types:

- VT 100
- VT 100+
- VT UTF8
- PC ANSI

When using Microsoft Windows operating systems the VT 100+ setting must be used.

The VT 100 setting offers maximum compatibility across the range of terminal emulation software, however, in this mode, the character set is limited and therefore the appearance of the Setup Utility may differ from the illustrations in this manual.

When using terminal emulation software it may be necessary to configure appropriate command sequences for the cursor and function keys. Table 6-1 defines the escape sequences expected by the BIOS.

Terminal Key	VT100 Escape Sequence
Cursor Up	<Esc>[A
Cursor Down	<Esc>[B
Cursor Left	<Esc>[C
Cursor Right	<Esc>[D
PF1	<Esc>OP
PF2	<Esc>OQ
PF3	<Esc>OR
PF4	<Esc>OS

Table 6-1 VT 100 Escape Sequences

6.5 Corrupted Serial Console Output

If the Serial Console uses an asynchronous serial connection, then on rare occasions the console display can become confused or corrupted. If this situation occurs, the serial terminal or terminal emulation software should be restarted.

6.6 VGA Display Behavior

When the board is configured for serial console mode all display output continues to be sent to the VGA controller (if it is enabled, including XMC or PMC display controllers). This happens because the BIOS still initializes the video controller and runs its BIOS extension firmware.

6.7 Slow Monitor Start-up

Modern energy-saving monitors can take a number of seconds to switch on once a video source is detected, as a consequence the POST screen may not become visible before the operating system starts to boot.

The BIOS includes a Setup option that introduces a five-second delay before entering the BIOS boot loader (see Section 5.7.3). This will be sufficient in the majority of cases to view the POST screen.

6.8 XMC/PMC Video Controller

When a PMC or XMC video controller is used, the BIOS will automatically switch to use the add-in card as the default video console. This may not always suit the desired configuration, therefore the BIOS provides a Setup option that will force the video console to use the embedded controller when an add-in card is fitted, see Section 5.7.1 for details.

7 BOOTING AND BOOTABLE DEVICES

7.1 UEFI Boot

The UEFI BIOS firmware previously fitted to the VP B1x/msd supported booting in legacy mode only and therefore the board would only boot from a MBR (Master Boot Record) format disk.

Starting with BIOS version 3.13.01, UEFI boot support has been included in the standard factory fitted firmware. This allows the board to boot UEFI compatible operating systems from GPT (GUID Partition Table) format disks.

7.1.1 Enabling UEFI Boot

The VP B1x/msd is configured to operate in legacy boot mode by default, to maintain backwards compatibility with previous BIOS releases, however UEFI boot mode can be enabled via the Boot Setup menu, by setting **Boot Type** to **UEFI Boot Type** or **Dual Boot Type** (see Section 5.40.1).

7.1.2 Installing UEFI Compatible Operating Systems

UEFI compatible operating systems usually install to GPT formatted disks, though MBR formatted disks can be used if dual-boot capability is required. Installing operating systems in UEFI mode is no more complicated than installing in legacy mode. Simply enable UEFI boot mode and boot from the installation media.

NOTE: The VP B1x/msd has 64-bit UEFI firmware and therefore it is unable to boot 32-bit UEFI operating systems. (With a suitable intermediary boot loader it may be possible to boot a 32-bit operating system, but the UEFI runtime services will not be accessible).

7.2 GPT Disk Structure

GUID Partition Table (GPT) is a new disk structure that replaces the ageing Master Boot Record (MBR) format that has been in use since the early days of the IBM PC.

MBR was limited to 4 primary partitions and 32-bit logical block addresses, resulting in a maximum disk (and partition) size of 2TB (with 512 byte sectors).

GPT supports 2^32 partitions and uses 64-bit logical block addresses. This increases the maximum disk (and partition) size to 9.4 ZB with 512 byte sectors (1 zetta byte = 10^21 bytes). Individual GPT partitions are identified using Globally Unique Identifiers (GUIDs).

The GPT structure starts with the second logical block on the disk because GPT format disks retain a 'protective MBR' in the first logical block. This MBR defines a single partition covering the entire disk (up to the 2TB MBR limit) and helps to prevent accidental overwriting of the disk by operating systems and utilities that do not support the GPT standard.

7.2.1 Booting from a GPT Disk

The MBR contains initial boot code that is loaded and executed when first booting from the disk in legacy mode. It is then the responsibility of this boot code to manage partition selection and loading of the operating system.

The GPT contains no code; instead the UEFI firmware boot manager controls the boot procedure using a combination of Boot Configurations (selected via the **Boot** Setup Menu, see Section 5.46) and standardized boot loader file paths.

All OS loaders must be held within a FAT formatted EFI System Partition (ESP). The ESP is identified via a known GUID.

7.3 Boot Timings

The BIOS boot time can vary considerably depending on the selection of peripheral devices attached to the board and the options configured through the Setup Utility.

Rotating media, particularly CD and DVD drives can increase the boot time by many seconds while the drive spins up. Therefore if boot time is important, these devices should be disabled when not required.

Table 7-1 illustrates the base-line boot times for an 16 Gbyte VP B1x/msd board with a 2.4 GHz CPU and a single USB Flash drive. Boot time is defined as the interval between application of power (or reset) and the first access to the boot media.

Boot Time (seconds)	
Graphics Console	24
Serial Console	31

Table 7-1 Typical BIOS Boot Times

The boot times above can be reduced by 3 seconds if **Delay Before Boot** is set to 0 (see Section 5.7.3), however the board may start to boot before energy-saving monitors have enabled the display.

7.4 Device Names in the Boot Menu

When peripheral devices are added to the Boot menu the name that appears in the list of bootable devices is either supplied by the device's internal firmware or constructed by the BIOS based on the characteristics of the device.

Hard disk drives, optical drives and USB devices can be readily identified by their manufacture and model names. However, the names used for PXE boot channels may not be familiar to users. Table 7-2 details the names that are used for the on-board Ethernet channels.

Device	BIOS Boot Name
Front Panel ETH A	IBA GE Slot 0700 v1504
Front Panel ETH B	IBA GE Slot 0701 v1504
Rear Panel ETH A	IBA GE Slot 0702 v1504
Rear Panel ETH B	IBA GE Slot 0703 v1504

Table 7-2 Embedded Device Boot Names

NOTE: The "00xx" and "07xx" in the Ethernet channel identifiers above is determined by the PCI bus number where the device resides. If a PMC, XMC or PMC carrier is installed then this number may change.

7.5 Bootable Device Types

The VP B1x/msd UEFI BIOS supports most common peripheral types as bootable devices. The following sections provide some additional information relating to some of these device types.

7.5.1 Floppy Disk Drives

The VP B1x/msd BIOS supports booting from USB floppy disk drives - these will be represented as removable devices (DOS drive A:). Legacy floppy disk drives are not supported.

7.5.2 SATA

The VP B1x/msd BIOS supports booting from all six of the board's SATA channels. The board provides two SATA600 ports for the on-board mass storage options, two SATA300 ports via P2 and two optional SATA300 ports via P0.

7.5.3 SCSI

The VP B1x/msd BIOS supports add-in SCSI controllers. If the add-in PMC or XMC includes BIOS extension firmware then the attached SCSI drives will be automatically included in the boot menu.

7.5.4 Ethernet

The VP B1x/msd includes PXE BIOS extension firmware that allows booting over a network connection via any of the four on-board Ethernet channels.

If an add-in Ethernet PMC or XMC includes PXE firmware then those controller channels will be automatically included to the boot menu.

7.5.5 USB

The VP B1x/msd board can boot from a wide range of USB mass-storage devices, including CD or DVD-ROM drives, Flash memory drives, floppy drives and hard drives.

Some USB peripherals require a connection to two USB ports in order to satisfy their current demand. If this requirement is not followed the board may fail to detect the device.

This page is intentionally unused.

8 THE UEFI SHELL

The UEFI Shell provides a pre-OS interactive environment where users can inspect boot media, manipulate files and execute pre-OS EFI applications. For many users there is no need to enable the UEFI Shell, or understand its features and it will be sufficient to enable UEFI boot and install the chosen operating system.

The UEFI Shell is a powerful tool and a full description of its features and capabilities is beyond the scope of this document. For readers wishing to gain a greater understanding of the features provided by the UEFI Shell there are various online resources available, including those provided by the UEFI Forum (see Appendix B).

Intel Press publish a book devoted to the UEFI Shell:

Harnessing the UEFI Shell: Moving the Platform Beyond DOS

Michael Rothman, Tim Lewis, Vincent Zimmer and Robert Hale

ISBN-13: 978-1934053140

8.1 Enabling the UEFI Shell

The UEFI Shell is enabled when **Boot Type** is set to UEFI Boot Type or Dual Boot Type, see Section 5.40.1.

The UEFI Shell is accessed as if it were another boot device. An **Internal EFI Shell** entry will be added to the bootable device list under the **Boot | EFI** sub-menu and the F5/F6 keys can be used to change the placement of the Internal EFI Shell entry in the boot order. The Internal UEFI Shell option also appears in the Boot Manager menu when F12 is pressed.

NOTE: Selecting **Internal EFI Shell** from the Boot Manager might result in the board restarting to enter the UEFI shell.

8.2 Starting the UEFI Shell

When the UEFI shell starts it displays the shell version and a list of available device handles (the device mapping table). After a pause the Shell searches for and executes an optional start-up script (see Section 8.4).



Figure 8-1 The UEFI Shell Prompt

The shell prompt will default to **`Shell>`** unless the start-up script explicitly selects a device.

8.3 UEFI Shell Script Files

UEFI Shell Script Files provide a way to package a series of shell commands and automate repeated operations.

> **NOTE:** For users familiar with the Windows command shell, UEFI scripts are analogous to batch files and many of the UEFI shell commands, and the overall command syntax will be familiar.

UEFI scripts can contain any valid shell command (certain shell commands can only be used inside a script) and they can execute EFI pre-Operating System applications and boot loaders

8.4 The UEFI Shell Start-up Script

When the UEFI Shell starts up it will enumerate the attached disk devices. The shell also looks in the root directory of FAT and FAT32 formatted partitions for the special script file, **`startup.nsh`**, and if this file is found it will be executed by the shell before the command prompt is displayed.

If **`startup.nsh`** is present on more than one drive, only the first copy will be executed; in addition **`startup.nsh`** does not need to be held on the first boot device.

> **NOTE:** When booting directly from a device, instead of booting to the UEFI Shell, **`startup.nsh`** does not get executed.

Figure 8.2 shows an example startup.nsh file running when the UEFI Shell starts.

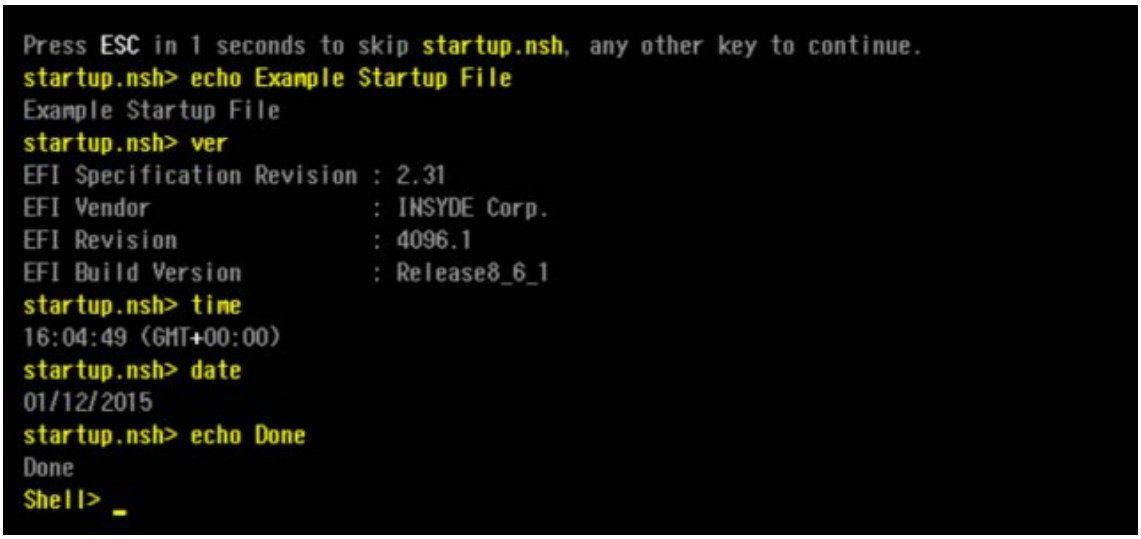


Figure 8-2 Example UEFI Startup Script

The startup.nsh file contained the following statements:

```
echo Example Startup File
ver
time
date
echo Done
```

8.5 UEFI Shell Commands

The UEFI Shell provides a number of commands for use in script files or direct execution from the command prompt. Table 8-1 provides a summary of the available commands.

Command	Description
?	Display Help
alias	Display, create and delete EFI shell aliases
attrib	Display or change attributes for files and directories
cd	Display or change the current directory
cls	Clear the screen (and optionally set the color)
connect	Connect an EFI driver to a device
cp	Copy files and directories
date	Display the system date
dh	Display EFI handle information
disconnect	Disconnect an EFI driver from a device
drivers	Display a list of installed drivers
drvcfg	Invoke a driver's configuration protocol
drvdiag	Invoke a driver's diagnostic protocol
echo	Display text (or turn command echoing on and off)
exit	Exit the shell
for	Execute command for each item in a set
goto	Jump to a script label
help	Display Help
if	Conditional command execution
load	Load (and connect to) an EFI driver
ls	List files and sub-directories
map	Display or define device mappings
mkdir	Create a directory
mv	Move files and directories
pause	Wait for keyboard response
reconnect	Reconnect an EFI driver to a device
reset	Reset the board
rm	Delete files and directories
set	Display or modify shell variables
shift	Shift batch-processing parameters
time	Display the system time
touch	Update a file timestamp
type	Display a (text) file
unload	Unload an EFI driver
ver	Display the EFI firmware version
vol	Display or change a system volume name

Table 8-1 Supported Shell Commands

For more details on individual commands refer to the UEFI Shell built in help. To obtain a list of supported commands type **`help -b`** at the command prompt.

> **NOTE:** Whenever a UEFI Shell command generates more than one screen of output, the **-b** flag can be used to pause after each screen and wait for the <**Enter**> key to continue, or <**q**> to exit.

To obtain detailed help on a specific command enter **`help`** followed by the command, e.g. for help on the file copy command enter **`help cp –b`**

8.6 UEFI Shell Command Examples

The following sections present some simple examples to illustrate how UEFI Shell commands may be utilized.

8.6.1 Basic Commands

Commands are entered at the prompt followed by <**Enter**>. When the shell starts the prompt will default to **`Shell>`** unless the start-up script explicitly selects a device.

The example Figure 8-3 uses the **`date`** and **`time`** commands to display the current clock settings.

```
Shell> date
01/12/2015

Shell> time
15:49:13 (GMT+00:00)

Shell> _
```

Figure 8-3 UEFI Shell Command Examples

8.6.2 Selecting Drives

The UEFI Shell lists available mass storage devices when it starts up, however if a large number of devices are discovered the details may have scrolled off the screen. Use the **`map -b`** command to re-list the devices a page at a time.

Figure 8-4 shows example output from the map command. Device partitions may appear more than once in this list, using different identifiers, since the shell assigns helpful aliases that can be used to refer to devices. In the example the first partition of the removable drive can be referenced as **fs0** and **blk0**, in addition to the default name **hd31a0d0b**.

```
Shell> map
Device mapping table
  fs0  :Removable HardDisk - Alias hd31a0d0b blk0
        PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x3,0x0)/HD(1,MBR,0x00000000
,0x3F,0xF327F)
  blk0 :Removable HardDisk - Alias hd31a0d0b fs0
        PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x3,0x0)/HD(1,MBR,0x00000000
,0x3F,0xF327F)
  blk1 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x3,0x0)
  hd31a0d0b :Removable HardDisk - Alias fs0 blk0
            PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x3,0x0)/HD(1,MBR,0x000
00000,0x3F,0xF327F)

Shell> _
```

Figure 8-4 UEFI map Command Example Output

To select a device enter the name (or one of its aliases) followed by a colon. Once the device is selected, the prompt will change to match the selected device name.

Once a drive has been selected the **ls** command can be used to list files and directories.

NOTE: The shell uses Unix-like names for the file manipulation commands (**ls**, **cp**, **rm** and **mkdir**), however the shell automatically creates aliases mapping familiar Windows shell commands (**dir**, **copy**, **del**, **md** and **rd**) onto their shell equivalent.

Directories are navigated using the **cd** command and the prompt will be updated to identify the path to the current working directory.

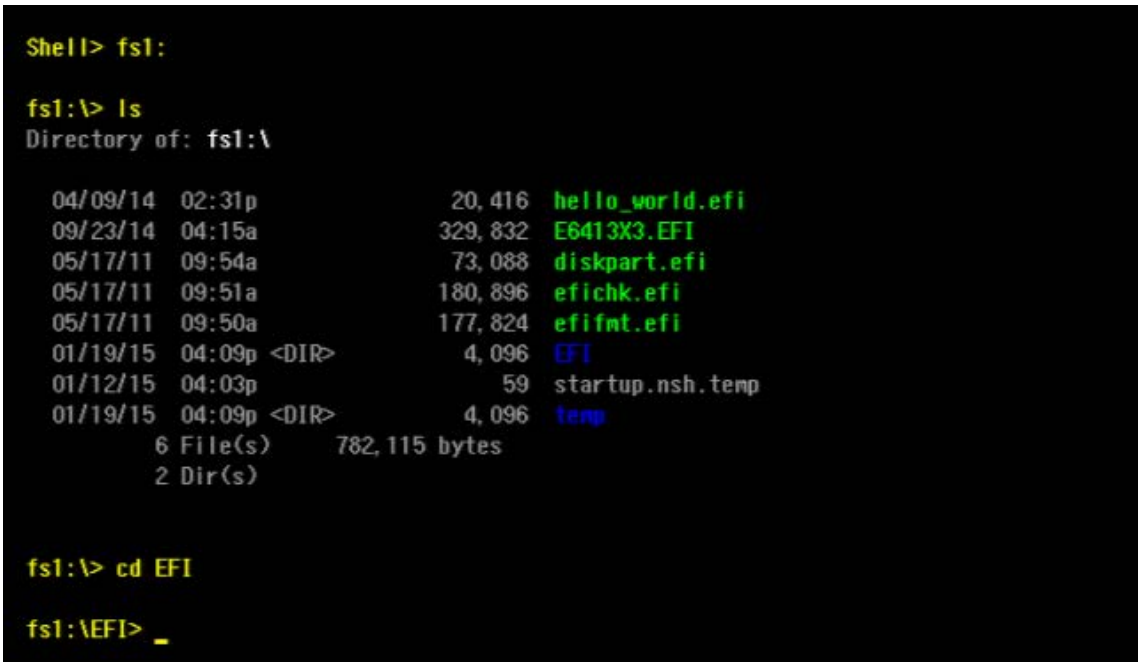


Figure 8-5 UEFI Device Navigation Example

NOTE: The shell (and hence the map command) can only operate on FAT formatted partitions (FAT12, FAT16 and FAT32). For this reason the EFI System Partition (ESP) where the boot loader resides, is always formatted as FAT.

8.7 EFI Applications

The UEFI shell (and script files) can be used to execute EFI applications. EFI applications have an **`.efi`** file extension. EFI applications are specially constructed executable files and they must be correctly compiled using UEFI libraries and data structures. Details of how to create a custom EFI application are beyond the scope of this document. Examples of EFI applications are: configuration tools, diagnostic utilities and operating system boot loaders.

Figure 8-6 shows an example EFI application being executed from the command prompt (this could also have been done as part of a shell script).

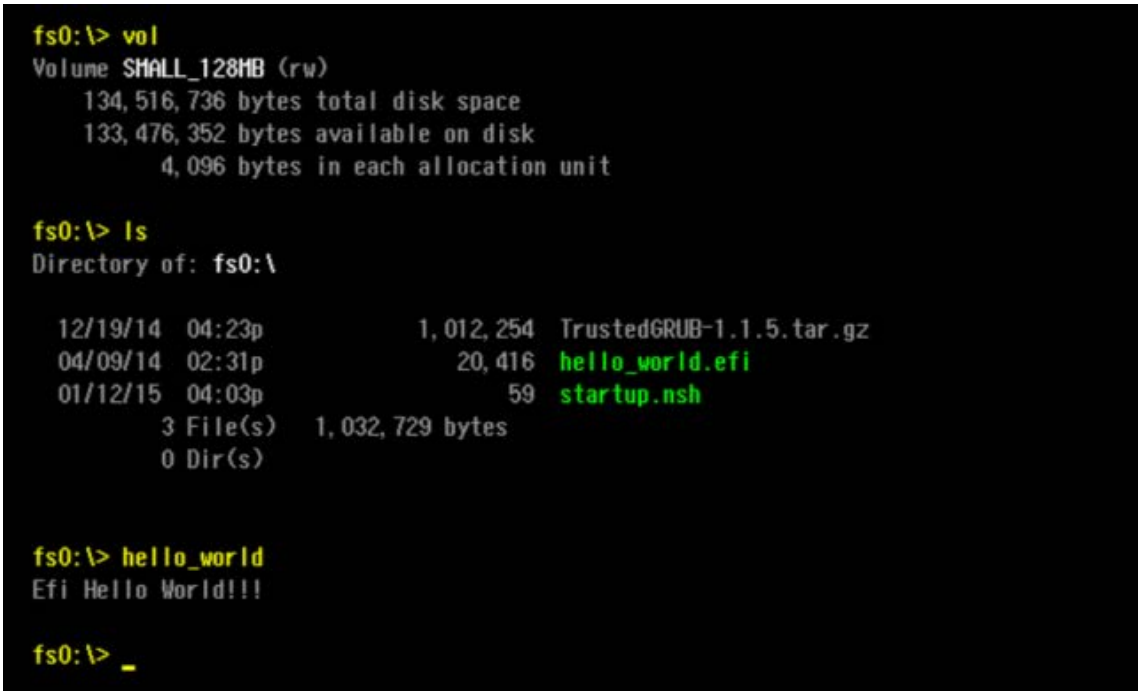


Figure 8-6 Executing an EFI Application

9 BIOS UPDATES

The VP B1x/msd board supports in-circuit programming of the BIOS firmware using a proprietary utility. Performing a BIOS update is a simple matter and also safe, provided that basic rules are followed.

Updates can be performed using a VGA screen and keyboard, or from a serial terminal (with the board configured for Serial Console mode).

9.1 How to Update a BIOS In-Circuit

The BIOS update is typically supplied as an ISO that can be used to create a bootable CD-ROM. The ISO image contains a copy of FreeDOS, the Concurrent Technologies BIOS update utility (UNIPROG) and the new BIOS firmware.

The FreeDOS installation is configured to automatically perform the BIOS update once the board boots from the CD-ROM. There is no need to connect a keyboard when performing a BIOS update.

NOTE: It is advisable, though not essential that a VGA screen or serial terminal is connected during the update in order to observe the progress. If it is not possible to do this, the board should be left for 3 minutes to ensure that the update has been completed before switching off the power.

9.2 Precautions During a BIOS Update

CAUTION: It is essential that board power is not switched off until the update has completed. Turning off the power part way through an update will corrupt the BIOS ROM contents and render the board inoperable.

If power is lost during an update it may be possible to perform a BIOS recovery; however if this does not work the board must be returned to the factory.

Some BIOS updates are only compatible with particular hardware revisions, or board Modification states. Always ensure that an update is compatible with all boards to which the update will be applied.

9.3 Things to Remember after Updating the BIOS

The new BIOS will clear any saved Setup Configurations and the board will be restored to the Optimal Default configuration, so any custom settings must be reconfigured.

9.4 BIOS Recovery

If the BIOS gets corrupted and the board is no longer able to boot, it may be possible to perform a BIOS recovery using a special BIOS image.

If a BIOS recovery is required, contact your local distributor or sales representative for further details.

10 MAXIMIZING PERFORMANCE OR MINIMIZING POWER

10.1 Maximizing Performance

The 4th generation Intel® Core™ processor used on the VP B1x/msd has a complex architecture. The different internal modules, CPU cores, Graphics core and memory controller hub (MCH) all draw power and generate heat in proportion to their utilization; however the package's ability to consume current and dissipate heat has physical limitations that cannot support a simultaneous maximum demand from all modules.

The VP B1x/msd UEFI BIOS offers a number of options for balancing performance, power consumption and heat generation between the competing modules, therefore the optimum configuration will depend on the specific application.

The BIOS Optimal Default settings configured by the factory aim to provide maximum CPU performance. Two Setup options contribute most to the CPU performance level:

- Hyper-threading, see Section 5.35.5.
- Turbo Mode, see Section 5.35.22.

When Turbo Mode is enabled the maximum CPU performance is obtained, at the expense of variable latency due to Turbo Mode transitions. Table 10-1 illustrates the PassMark® CPU Mark rating for different CPU options using version 8.0 of the PassMark Performance Test running on Windows 7 Ultimate 64-bit. For further details on the range of 4th generation Intel Core processors supported please refer to the board's Technical Reference Manual or Datasheet.

CPU	Turbo Mode = Enabled	Turbo Mode = Disabled
2-Core 1.8 GHz	TBD	TBD
2-Core 2.9 GHz	TBD	TBD
4-Core 2.4 GHz	8113	6852

Table 10-1 CPU Mark ratings for different CPU options

Maximum performance is usually obtained when all CPU cores are enabled and a SMP operating system is used, therefore the following settings should also be left in their default Enabled configuration:

- APIC, see Section 5.24.2.
- Active Processor Cores, see Section 5.35.4.
- Hyper-Treading (HT) Support, see Section 5.35.5.

10.2 Minimizing Power

Although gaining maximum performance is the usual goal of system integrators, there are a number of designs where managing power consumption is a primary goal, either because the system operates from batteries or because of thermal considerations.

The VP B1x/msd UEFI BIOS provides many different Setup options that can be used to reduce power consumption by allowing different interfaces and hardware components to enter low power states when they are idle. The major disadvantage with using low-power options is the associated latency while the interface or component switches back to the operational mode.

Possibly the best option for reducing power consumption, while minimizing system latency, is to reduce the operating frequency of the CPU and memory interfaces using the following options:

- CPU operating frequency, see Section 5.7.11.
- Memory frequency, see Section 5.23.7.

In addition, there are a number of options available through the **Power** Setup menus that can affect the power consumption and users should ensure that these are set to their factory-configured defaults.

11 SECURITY NOTES

The BIOS implements a simple, single-tier security model where one password is used to manage access to the Setup utility and boot media.

Specifying a supervisor password enables password control of the Setup Utility. Once this has been specified the BIOS can additionally be configured to require a password before booting. Hashed versions of the passwords are stored in the BIOS flash ROM.

BIOS passwords are not a substitute for physical security of the SBC. Anyone with physical access to the board could reprogram the BIOS and erase any stored passwords.

NOTE: BIOS passwords are not reset when the Load Optimal Defaults jumper is fitted.

11.1 Board Level Security Package

The Concurrent Technologies Board Level Security Package provides a means to enhance the security of equipment and thus prevent access to sensitive data and key Intellectual Property. The security is implemented on our single board computers using a combination of deeply embedded proprietary hardware, firmware and software countermeasures.

The Board Level Security Package must be purchased with the board and cannot be supplied as an after-sales add-on. Contact your local distributor or sales representative for further details.

This page is intentionally unused.

12 VME IMAGE CONFIGURATION

12.1 A Note on 64-bit Operating Systems

The Universe-IIe is a 32-bit PCI device and therefore it is unable to generate addresses above the 4Gbyte address boundary. All Outbound and Inbound image local addresses must be located within the 32-bit address space, below 4 Gbytes. For details on the BIOS set up options for the VME interface, Outbound and Inbound images refer to Section 5.37, Section 5.38 and Section 5.39 respectively.

12.2 Outbound Image Allocation

Boards fitted with 4 Gbytes or more of DRAM do not have a convenient ‘hole’ in the address map where Local Outbound Slave Images can be mapped. Therefore the BIOS must reserve a block of address space for this purpose.

The BIOS reserves memory by increasing the size of the block used by PCI devices, i.e. the top of DRAM is lowered. The BIOS creates a data-structure in DRAM that defines details of the reserved memory, this is described in Section 12.4.

The reserved memory can be used by the BIOS Setup options, the driver or both.

12.3 Inbound Image Allocation

Operating systems wishing to map VME Slave (Inbound) Images into DRAM usually encounter problems allocating the required fixed-address buffers. To overcome this, the BIOS reserves a block of DRAM (below 4 Gbytes) that is hidden from the operating system memory-manager, but is available to the VME driver.

The BIOS allocates this memory by marking the specified block as reserved, thus preventing the operating system memory-manager from utilizing it. The Inbound Reserved Size option controls the size of reserved memory, (see Section 5.37.4).

The reserved memory can be used by the BIOS Setup options, the driver or both.

Details of the data structure are described in Section 12.4.

12.4 VME Reserved Memory Data Structure

Details of the Outbound and Inbound memory reservations are provided by the VME Reserved Memory data structure, which the BIOS constructs in DRAM.

Legacy-boot software requiring details of the VME reserved memory can locate this structure by searching for the signature bytes between addresses 0xE0000 and 0xFFFFF.

UEFI-boot software requiring details of the VME reserved memory should read the UEFI variable "VME_INFO", which contains a copy of this structure.

```
/* Header part */

UINT32 vmeLsi_header       = 'EMV$';     /* signature, '$' in LSB */
UINT8  vmeLsi_version      = 0x02;       /* version of structure */
UINT8  vmeLsi_length;                    /* total length of structure */
UINT16 vmeLsi_reserved     = 0;

/* Version 1 payload */

UINT32 vmeLsi_mem_base;           /* physical address of reserved block */
UINT32 vmeLsi_mem_size;           /* size (in bytes) of reserved block */
UINT32 vmeLsi_image_0_base;       /* base address of enabled LSI images /
UINT32 vmeLsi_image_1_base;
UINT32 vmeLsi_image_2_base;
UINT32 vmeLsi_image_3_base;
UINT32 vmeLsi_image_4_base;
UINT32 vmeLsi_image_5_base;
UINT32 vmeLsi_image_6_base;
UINT32 vmeLsi_image_7_base;

/* Version 2 payload */

UINT32 vmeVsi_mem_base;           /* physical address of reserved block */
UINT32 vmeVsi_mem_size;           /* size (in bytes) of reserved block */
UINT32 vmeVsi_image_0_base;       /* base address of enabled VSI images */
UINT32 vmeVsi_image_1_base;
UINT32 vmeVsi_image_2_base;
UINT32 vmeVsi_image_3_base;
UINT32 vmeVsi_image_4_base;
UINT32 vmeVsi_image_5_base;
UINT32 vmeVsi_image_6_base;
UINT32 vmeVsi_image_7_base;
```

13 LEGACY BIOS RUNTIME SERVICES

The InsydeH20 UEFI BIOS includes a Compatibility Support Module (CSM) that provides legacy BIOS services that allow operating systems without UEFI support to boot on the board.

13.1 Video – INT 0x10

In VGA mode, the BIOS extension firmware for the video controller handles the INT 0x10 BIOS services.

In Serial Console mode the BIOS supports text-mode INT 0x10 calls. Text output and cursor movements are translated to the appropriate terminal command codes and sent over the serial link.

13.2 Disk I/O – INT 0x13

The BIOS supports INT 0x13 calls SATA drives. The BIOS also provides an INT 0x13 interface to bootable USB storage devices. Other bootable devices (e.g. SCSI disks) are supported by their associated BIOS extension firmware.

13.3 USB Legacy Device Support

13.3.1 Legacy Keyboard and Mouse Emulation

The BIOS includes functions that will allow a USB keyboard and mouse to emulate their legacy PS/2 equivalents. This allows the use of USB input devices with operating systems that do not include native USB support.

Device emulation is provided by intercepting accesses to the keyboard and mouse I/O ports (ports 0x0060 and 0x0064) and by driving the legacy interrupts (IRQ1 and 12 respectively).

USB Legacy Emulation must be enabled in the BIOS Setup utility, see Section 5.22.1 for details.

13.3.2 USB Mass Storage Support

The BIOS includes code to support USB floppy disks, Flash memory sticks, hard disk drives and CD-ROMs via INT 0x13. This allows USB mass storage devices to be used as boot devices and makes them useable from MS-DOS.

13.4 ACPI

The BIOS is compatible with all major releases of the ACPI specification up to version 4.0. A Setup option (see Section 5.40.6) is provided for configuring the level of ACPI support implemented by the BIOS.

Additional Setup options are provided for configuring ACPI options relating to CPU throttling and power management.

13.5 Multi-Processor Support

The BIOS will detect, initialize and idle all application processor (AP) cores, including those implemented via hyper-threading.

The BIOS will also construct in memory a Multi-Processor Configuration Table (MP-Table) for use by SMP enabled operating systems that do not support ACPI (e.g. VxWorks).

13.6 PCI BIOS

The BIOS includes support for V3.0 of the PCI BIOS Specification.

APPENDIX A BIOS MEMORY MAP

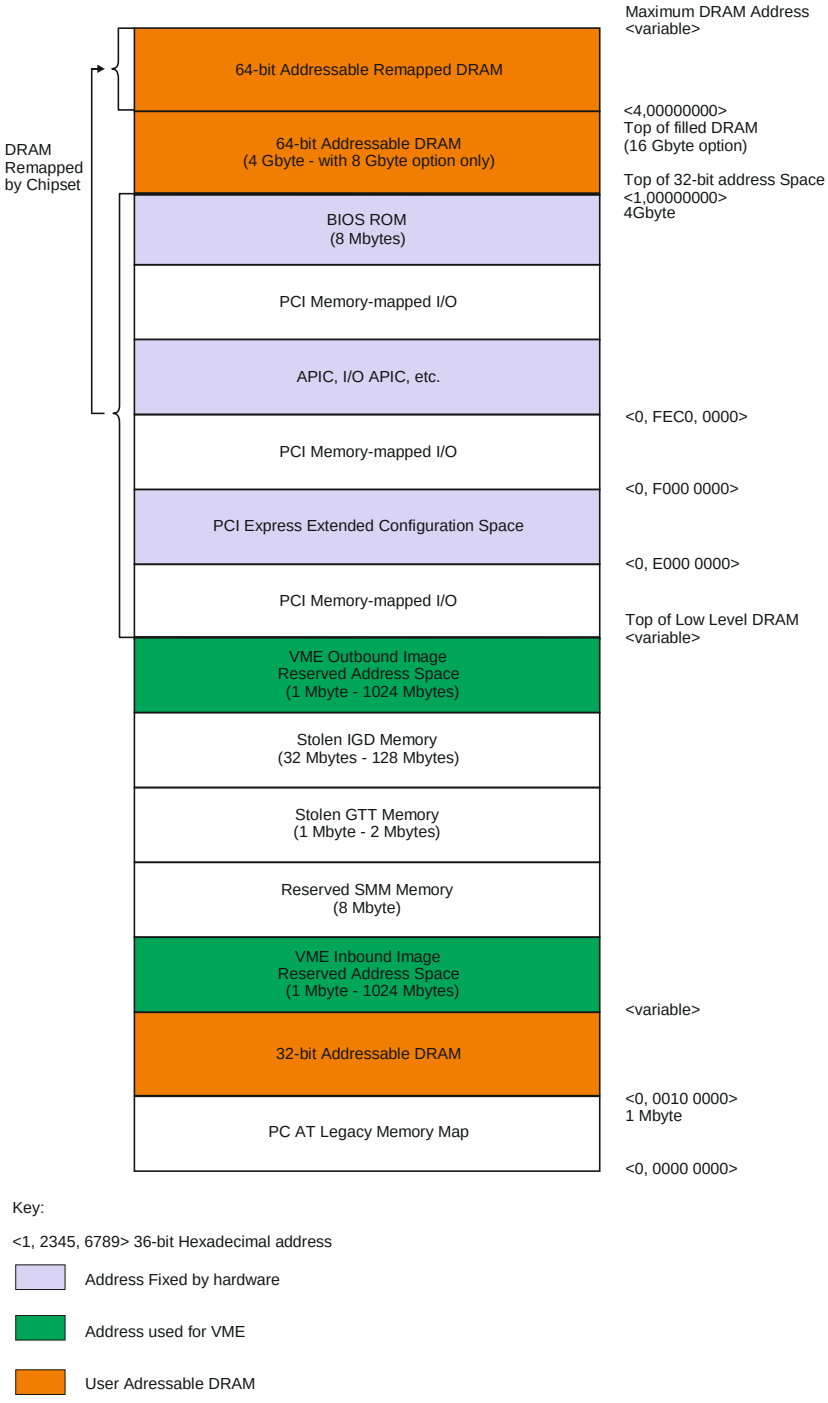


Figure A-1 BIOS Memory Map

This page is intentionally unused.

APPENDIX B REFERENCES

For further details on the specifications mentioned in the preceding text please consult the following sources.

B.1 UEFI Firmware

Interested readers are referred to the website of the Unified EFI Forum where various documents and specifications are available for download by non-menders:

- http://www.uefi.org

B.2 General PC Industry Specifications

Details of the various BIOS related specifications referenced by this manual, e.g. Plug-and-Play, System Management BIOS are available from:

- http://www.phoenix.com
- http://microsoft.com

B.3 PCI BIOS Specification

For details of the PCI BIOS Specification and PCI in general, contact the PCI Special Interest Group (PCISIG):

- http://www.pcisig.com

B.4 PXE

Documentation relating to the Preboot Execution Environment (PXE) standard is available from Intel:

- http://www.intel.com

B.5 ACPI

Presentations, specifications and tools relating to the Advanced Configuration and Power Interface (ACPI) are available from:

- http://www.acpi.info

B.6 VME

The VME International Trade Association standard VITA 1 defines VME64. Further details, including presentations and specifications are available from:

- http://www.vita.com

This page is intentionally unused.

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP