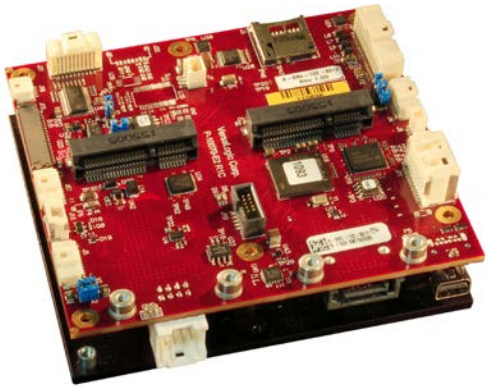

BIOS Reference Manual

REV. December 2017

Lion

(VL-EPMe-42)

VERSALOGIC CORPORATION

WWW.VERSALOGIC.COM

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

Notice:

Although every effort has been made to ensure this document is error-free, VersaLogic makes no representations or warranties with respect to this product and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

VersaLogic reserves the right to revise this product and associated documentation at any time without obligation to notify anyone of such changes.

* Other names and brands may be claimed as the property of others.

Product Release Notes

This document reflects the content of the BIOS Setup program for the EPMe-42 board.

Board Revision	BIOS Version	Comments
Rev 1.00	1.02	First release of document

Customer Support

If you are unable to solve a problem after reading this manual, visiting the product support page, or searching the KnowledgeBase, contact VersaLogic Technical Support at (503) 747-2261. VersaLogic support engineers are also available via e-mail at Support@VersaLogic.com.

Repair Service

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

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

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

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

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

Contents

Tables

1 Overview

The EPMe-42 BIOS is based on Phoenix SecureCore Technology* (SCT) Kaby Lake UEFI Firmware with VersaLogic customizations and enhancements.

The board boots and BIOS begins execution when power is applied. After a few seconds, the user may press the F2 or Del keys to enter BIOS Setup.

This manual details the editable items found in the EPMe-42 BIOS.

The table below lists the BIOS Setup program top-level menu bar features.

Table 1. Top-level Menu Bar Features

Menu	Function
Main	Displays processor and memory parameters
Advanced	Configures advanced features, including CPU, IDE, and USB
Security	Sets passwords and security features
Boot	Selects boot device options
Misc	Miscellaneous BIOS options
Save & Exit	Saves or discards changes to Setup program options

This next table lists the function keys available for menu screens.

Table 2. BIOS Setup Program Function Keys

Key	Function	Key	Function
← or →	Selects a different menu screen (Moves the cursor left or right)	↑ or ↓	Selects an item (Moves the cursor up or down)
+ or -	Changes option/field	Enter	Executes a command or selects a sub-menu
PgDn	Go to next page	PgUp	Go to previous page
Home	Go to top of screen	End	Go to bottom of screen
Tab	Select field	F1	General help
F2	Load Previous Settings	F9	Loads optimal defaults
F8	Loads failsafe default values	Esc	Exit
F10	Save and exit		

2 Main Menu

The Main menu displays BIOS, processor, memory and other system information and edits the system date and time.

System Information

This displays BIOS, processor, memory and other system information.

Example:

```
BIOS Version          EPMe42_4.0.1.359.102 KBLU X64
Build Time            11/21/2017
Processor Type        Intel(R) Core(TM) i3-7100U CPU @ 2.40GHz
Processor Speed       2.400 GHz
System Memory Speed   1600 MHz
L2 Cache RAM          512 KB
Total Memory          16384 MB
 Memory Device [0]    16384 MB (DDR3-1600) @ ChannelA-DIMM0
 Memory Device [1]    Not Installed
```

Boot Features

NumLock

Option Default: 01

01 = On

00 = Off

Option Description: Selects Power-on state for NumLock.

Timeout

Option Default: 0002

Minimum = 0000

Maximum = 0063

Step = 0001

Option Description: Number of seconds that P.O.S.T will wait for the user input before booting.

CSM Support

Option Default: 01

00 = No

01 = Yes

Option Description: Compatibility Support Module that provides backward compatibility services for legacy BIOS services like int10/int13, dependent on OS.

Quick Boot

Option Default: 00

00 = Disabled

01 = Enabled

Option Description: This enables or disables quick boot.

Diagnostic Splash Screen

Option Default: 00

00 = Disabled

01 = Enabled

Option Description: If you select 'Enabled' the diagnostic, splash screen always displays during boot. If you select 'Disabled' the diagnostic splash screen does not display unless you press HOTKEY during boot.

Diagnostic Summary Screen

Option Default: 00

00 = Disabled

01 = Enabled

Option Description: Displays the diagnostic summary screen during boot.

BIOS Level USB

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: This option enables or disables all BIOS support for USB in order to reduce boot time. Note that this will prevent using a USB keyboard in setup or a USB biometric scanner such as a finger print reader to control access to setup, but does not prevent the operating system from supporting such hardware.

USB Legacy

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: This enables or disables USB BIOS SMM support for mouse, keyboard, mass storage, etc., in legacy operating systems such as DOS.

Console Redirection

Option Default: 00000000

00000000 = Disabled

00000001 = Enabled

Option Description: Enables or disables Universal Console Redirection.

Terminal Type

Option Default: 00000000

00000000 = ANSI

00000001 = VT100

00000002 = VT100+

00000003 = UTF8

Option Description: Sets the terminal type of UCR.

Baudrate

Option Default: 0001C200

00002580 = 9600

00004B00 = 19200

00009600 = 38400

0000E100 = 57600

0001C200 = 115200

Option Description: Sets the baudrate of UCR.

Flow Control

Option Default: 00000000

00000000 = None

00000001 = RTS/CTS

00000002 = XON/XOFF

Option Description: Sets the flow control method for UCR.

[None] - No flow control.

RTS/CTS - Hardware flow control.

[XON/XOFF] - Software flow control.

Continue C.R. after POST

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: Enables Console Redirection after the OS has been loaded.

Allow Hotkey in S4 resume

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: Enable hotkey detection when the system is resuming from Hibernate state

UEFI Boot

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: Enables the UEFI boot. If bootable media support both UEFI and Legacy boot, then the BIOS will choose UEFI unless this option is disabled.

Legacy Boot

Option Default: 01

00 = Disabled

01 = Enabled

Option Description: Enables the Legacy boot.

Boot in Legacy Video Mode

Option Default: 00

00 = Disabled

01 = Enabled

Option Description: Enable forces the display adapter to switch the video mode to Text Mode 3 at the end of BIOS POST for non-UEFI boot mode (Legacy Boot). Some legacy software, such as DUET, requires that the BIOS explicitly enter text video mode prior to boot.

Load OPROM

Option Default: 00

01 = All

00 = On Demand

Option Description: Loads all OPROMs or load them upon demand according to the boot device

3 Advanced Menu

Select Language

Option Default: 00

00 = English

Option Help: Select Language

SMBIOS Event Log

Manage SMBIOS Event Log and view SMBIOS events.

Platform Information Menu

Display current platform information on the processor, graphics, PCH, and memory.

Example:

```
BIOS Information
BIOS Vendor                     Phoenix Technologies Ltd.
Core Version                    4.0

Board Information
Board ID                        EPMe-42
Fab ID                          2
LAN PHY Revision                A6 (B2 Stepping)

Processor Information
Name                            Kabylake ULT
Type                            Intel(R) Core(TM) i3-7100U CPU @ 2.4GHz
Speed                           2400 MHz
ID                              0x806E9
Stepping                        H0/J0
Package                         Not Implemented Yet
Number of Processors            2Core(s) / 4Thread(s)
Microcode Revision              62
GT Info                         GT2 (0x5916)
eDRAM Size                      N/A

IGFX VBIOS Version              1049
IGFX GOP Version                N/A
```

Memory RC Version	1.9.0.0
Total Memory	16384 MB
Memory Frequency	1600 MHz
PCH Information	
Name	SKL PCH-LP
PCH SKU	(U) iHDCP 2.2 Premium
Stepping	C1
Hsio Revision	52
Package	Not Implemented Yet
TXT Capability of Platform/PCH	Unsupported
Production Type	Production
Dual Output Fast Read support	Not supported
Read ID/Status Clock Freq	17 MHz
Write and Erase Clock Freq	30 MHz
Fast Read Clock Freq	30 MHz
Fast Read support	Supported
Read Clock Freq	17 MHz
Number of Components	1 Component
SPI Component 0 Density	16 MB
EC FW Version	255.255
ME FW Version	11.6.27.3264
ME Firmware SKU	Corporate SKU
Sensor Hub FW	N/A

Intel Advanced Menu

PCI Subsystem Settings

PCI ROM Priority

Option Default: 01

00 = Legacy ROM

01 = EFI Compatible ROM

Option Help: In case of multiple Option ROMs (Legacy and EFI Compatible), specifies what PCI Option rom to launch.

Skip NVMe OpRom

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Test Option:

Enables skipping Option ROMs execution on Intel NVMe Drives

External DMA Allowed On Boot

Option Default: 00

00 = No

01 = Yes

Option Help: External DMA Allowed On Boot for devices such as 1394, PCMCIA, & CardBus

PCI Latency Timer

Option Default: 20

20 = 32 PCI Bus Clocks

40 = 64 PCI Bus Clocks

60 = 96 PCI Bus Clocks

80 = 128 PCI Bus Clocks

A0 = 160 PCI Bus Clocks

C0 = 192 PCI Bus Clocks

E0 = 224 PCI Bus Clocks

F8 = 248 PCI Bus Clocks

Option Help: Value to be programmed into PCI Latency Timer Register.

ACPI Settings

Enable Hibernation

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some OSs.

ACPI S3 Support

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable ACPI S3 support

Native PCIE Enable

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Bit - PCIe Native * control

0 - ~ Hot Plug

1 - SHPC Native Hot Plug control

2 - ~ Power Management Events

3 - PCIe Advanced Error Reporting control

4 - PCIe Capability Structure control

5 - Latency Tolerance Reporting control

Native ASPM

Option Default: 02

02 = AUTO

01 = Enabled

00 = Disabled

Option Help: Enabled - OS Controlled ASPM, Disabled - BIOS Controlled ASPM

ACPI Table Support

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enables support for the BDAT ACPI table.

Wake system from S5

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable or disable System wake on alarm event. When enabled, System will wake on the hr::min::sec specified

CPU Configuration

SW Guard Extensions (SGX)

Option Default: 02

02 = Software Controlled

01 = Enabled

00 = Disabled

Option Help: Enable/Disable Software Guard Extensions (SGX)

Select Owner EPOCH input type

Option Default: 00

00 = No Change in Owner EPOCHs

01 = Change to New Random Owner EPOCHs

02 = Manual User Defined Owner EPOCHs

Option Help: There are three Owner EPOCH modes (Each EPOCH is 64bit): no change in owner epoch, change to new random owner epoch and manually entered by user. After generating new epoch via 'Change to New Random Owner EPOCHs', the selection reverts back to 'No Change in Owner Epochs', this is to ensure Epoch stays same, across Sx states. After the user enters epoch values manually, the values will not be visible, for security reasons.

PRMRR Size

Option Default: 00000000

00000000 = INVALID PRMRR

02000000 = 32MB

04000000 = 64MB

08000000 = 128MB

Option Help: Setting the PRMRR (Processor Reserved Memory Range Register) Size

CPU Flex Ratio Override

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable CPU Flex Ratio Programming

CPU Flex Ratio Settings

Option Default: 14

Minimum = 00

Maximum = 3F

Step = 00

Option Help: This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM).

Hardware Prefetcher

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: To turn on/off the MLC streamer prefetcher.

Adjacent Cache Line Prefetch

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: To turn on/off prefetching of adjacent cache lines.

Intel (VMX) Virtualization Technology

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

Active Processor Cores

Option Default: 00

00 = All

01 = 1

02 = 2

03 = 3

Option Help: Number of cores to enable in each processor package.

Hyper-Threading

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enabled for Windows XP and Linux (OS optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology).

AES

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable AES (Advanced Encryption Standard)

Power & Performance

CPU - Power Management Control

Boot performance mode

Option Default: 01

00 = Max Battery

01 = Max Non-Turbo Performance

00 = Max Battery

02 = Turbo Performance

Option Help: Select the performance state that the BIOS will set starting from reset vector.

Intel(R) SpeedStep(tm)

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Allows more than two frequency ranges to be supported.

Intel(R) Speed Shift Technology

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.

C states

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.

Enhanced C-states

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.

C-State Auto Demotion

Option Default: 03

00 = Disabled

01 = C1

02 = C3

03 = C1 and C3

Option Help: Configure C-State Auto Demotion

C-State Un-demotion

Option Default: 03

00 = Disabled

01 = C1

02 = C3

03 = C1 and C3

Option Help: Configure C-State Un-demotion

Package C-State Demotion

Option Default: 02

00 = Disabled

01 = Enabled

02 = AUTO

Option Help: Enable or Disable Package C-State Demotion. 0: Disable; 1: Enable; 2: Auto (Auto: Enabled for Skylake; Disabled for Kabylake)

Package C-State Un-demotion

Option Default: 02

00 = Disabled

01 = Enabled

02 = AUTO

Option Help: Enable or Disable Package C-State UnDemotion. 0: Disable; 1: Enable; 2: Auto (Auto: Enabled for Skylake; Disabled for Kabylake)

CState Pre-Wake

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake

Package C State Limit

Option Default: FF

FF = Auto

FE = Cpu Default

08 = C10

07 = C9

06 = C8

05 = C7S

04 = C7

03 = C6

02 = C3

01 = C2

00 = C0/C1

Option Help: Maximum Package C State Limit Setting. Cpu Default: Leaves to Factory default value.Auto: Initializes to deepest available Package C State Limit.

Thermal Monitor

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Thermal Monitor

GT - Power Management Control

RC6(Render Standby)

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Check to enable render standby support.

Maximum GT frequency

Option Default: FF

FF = Default Max Frequency

02 = 100Mhz

03 = 150Mhz

04 = 200Mhz

05 = 250Mhz

06 = 300Mhz

07 = 350Mhz

08 = 400Mhz

09 = 450Mhz

0A = 500Mhz

0B = 550Mhz

0C = 600Mhz

0D = 650Mhz

0E = 700Mhz

0F = 750Mhz

10 = 800Mhz

11 = 850Mhz

12 = 900Mhz

13 = 950Mhz

14 = 1000Mhz

15 = 1050Mhz

16 = 1100Mhz

17 = 1150Mhz

18 = 1200Mhz

Option Help: Maximum GT frequency limited by the user. Choose between 300 MHz (RPN) and 1000MHz (RP0). Value beyond the range will be clipped to min/max supported by the SKU

Memory Configuration

Maximum Memory Frequency

Option Default: 0000

0000 = Auto

042B = 1067

0535 = 1333

0640 = 1600

074B = 1867

0855 = 2133

0960 = 2400

0A6B = 2667

0B75 = 2933

0C80 = 3200

0D8B = 3467

0E95 = 3733

0FA0 = 4000

1025 = 4133

Option Help: Maximum Memory Frequency Selections in Mhz.

Max TOLUD

Option Default: 00

00 = Dynamic

01 = 1 GB

02 = 1.25 GB

03 = 1.5 GB

04 = 1.75 GB

05 = 2 GB

06 = 2.25 GB

07 = 2.5 GB

08 = 2.75 GB

09 = 3 GB

Option Help: Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller

Enable RH Prevention

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Actively prevent Row Hammer

Row Hammer Solution

Option Default: 00

00 = Hardware RHP

01 = 2x Refresh

Option Help: Type of method used to prevent Row Hammer

RH Activation Probability

Option Default: 0B

01 = 1/2^1

02 = 1/2^2

03 = 1/2^3

04 = 1/2^4

05 = 1/2^5

06 = 1/2^6

07 = 1/2^7

08 = 1/2^8

09 = 1/2^9

0A = 1/2^10

0B = 1/2^11

0C = 1/2^12

0D = 1/2^13

0E = 1/2^14

0F = 1/2^15

Option Help: Used to adjust MC for Hardware RHP.

Memory Scrambler

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Memory Scrambler support.

Memory Remap

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable Memory Remap above 4GB

Mrc Fast Boot

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable fast path thru the MRC

System Agent (SA) Configuration

Graphics Configuration

Skip Scanning of External Gfx Card

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: If Enable, it will not scan for External Gfx Card on PEG and PCH PCIE Ports

Primary Display

Option Default: 03

03 = Auto

00 = IGFX

02 = PCI

04 = SG

Option Help: Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select SG for Switchable Gfx.

Internal Graphics

Option Default: 02

02 = Auto

00 = Disabled

01 = Enabled

Option Help: Keep IGFX enabled based on the setup options.

GTT Size

Option Default: 03

01 = 2MB

02 = 4MB

03 = 8MB

Option Help: Select the GTT Size

Aperture Size

Option Default: 01

00 = 128MB

01 = 256MB

03 = 512MB

07 = 1024MB

0F = 2048MB

Option Help: Select the Aperture Size

Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.

DVMT Pre-Allocated

Option Default: 01

00 = 0M

01 = 32M

02 = 64M

F0 = 4M

F1 = 8M

F2 = 12M

F3 = 16M

F4 = 20M

F5 = 24M

F6 = 28M

F7 = 32M/F7

F8 = 36M

F9 = 40M

FA = 44M

FB = 48M

FC = 52M

FD = 56M

FE = 60M

Option Help: Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

DVMT Total Gfx Mem

Option Default: 02

02 = 256M

01 = 128M

03 = MAX

Option Help: Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

Gfx Low Power Mode

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: This option is applicable for SFF only.

Algorithm

Option Default: 01

01 = One-time

00 = Periodic

Option Help: HDCP Re-encryption Flow.

PM Support

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable PM Support

PAVP Enable

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable PAVP

LCD Control

Primary IGFX Boot Display

Option Default: 00

00 = VBIOS Default

04 = EFP

08 = LFP

20 = EFP3

40 = EFP2

10 = EFP4

Option Help: Select the Video Device which will be activated during POST.

This has no effect if external graphics are present.

Secondary boot display selection will appear based on your selection.

VGA modes will be supported only on the primary display.

Secondary IGFX Boot Display

Option Default: 00

00 = Disabled

04 = EFP

20 = EFP3

40 = EFP2

10 = EFP4

Option Help: Select Secondary Display Device

LCD Panel Type

Option Default: 00

00 = VBIOS Default

01 = 640x480 LVDS

02 = 800x600 LVDS

03 = 1024x768 LVDS

04 = 1280x1024 LVDS

05 = 1400x1050 LVDS1

06 = 1400x1050 LVDS2

07 = 1600x1200 LVDS

08 = 1280x768 LVDS

09 = 1680x1050 LVDS

0A = 1920x1200 LVDS

0D = 1600x900 LVDS

0E = 1280x800 LVDS

0F = 1280x600 LVDS

10 = 2048x1536 LVDS

11 = 1366x768 LVDS

Option Help: Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

Panel Scaling

Option Default: 00

00 = Auto

01 = Off

06 = Force Scaling

Option Help: Select the LCD panel scaling option used by the Internal Graphics Device.

Backlight Control

Option Default: 02

00 = PWM Inverted

02 = PWM Normal

Option Help: Back Light Control Setting

Active LFP

Option Default: 03

00 = No eDP

03 = eDP Port-A

Option Help: Select the Active LFP Configuration.

No LVDS:VBIOS does not enable LVDS.

Int-LVDS:VBIOS enables LVDS driver by Integrated encoder.

SDVO LVDS:VBIOS enables LVDS driver by SDVO encoder.

eDP Port-A:LFP Driven by Int-DisplayPort encoder from Port-A.

eDP Port-D:LFP Driven by Int-DisplayPort encoder from Port-D(through PCH).

Panel Color Depth

Option Default: 00

00 = 18 Bit

01 = 24 Bit

Option Help: Select the LFP Panel Color Depth

Backlight Brightness

Option Default: FF

Minimum = 00

Maximum = FF

Step = 00

Option Help: Set VBIOS Brightness.

Range : 0-255.

VT-d

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: VT-d capability

Above 4GB MMIO BIOS assignment

Option Default: 00

01 = Enabled

00 = Disabled

Option Help: Enable/Disable above 4GB MemoryMappedIO BIOS assignment

PCH-IO Configuration

PCI Express Configuration

Option Name: PCI Express Clock Gating

Option Default: 01

01 = Disabled

00 = Enabled

Option Help: PCI Express Clock Gating Enable/Disable for each root port.

Legacy IO Low Latency

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.

DMI Link ASPM Control

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: The control of Active State Power Management of the DMI Link.

Auto is equal to POR setting.

Port8xh Decode

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Port8xh Decode Enable/Disable.

Port8xh Decode Port#

Option Default: 00

Minimum = 00

Maximum = 14

Step = 01

Option Help: Select PCI Express Port8xh Decode Root Port. User to ensure port availability

Peer Memory Write Enable

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Peer Memory Write Enable/Disable

PCIe-USB Glitch W/A

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCIe-USB Glitch W/A for bad USB device(s) connected behind PCIE/PEG Port.

PCIe function swap

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When Disabled, prevents PCIE rootport function swap. If any function other than 0th is enabled, 0th will become visible.

PCI Express Root Port 1-12

Port Mappings:

1 – XIO2001 PCIe-to-PCI Bridge

2 – I210 Ethernet (J4.2)

5 – PC104/Express OneBlade.

6 – PC104/Express OneBlade.

11 – PCIe Minicard.

12 – (HSIO16 used for SATA2 to Minicard)

PCI Express Root Port x

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Control the PCI Express Root Port.

ASPM

Option Default: 00

04 = Auto

03 = L0sL1

02 = L1

01 = L0s

00 = Disabled

Option Help: Automatically enable ASPM based on reported capabilities and known issues.

L1 Substates

Option Default: 03

00 = Disabled

01 = L1.1

02 = L1.2

03 = L1.1 & L1.2

Option Help: PCI Express L1 Substates settings.

Gen3 Eq Phase3 Method

Option Default: 02

01 = Hardware

04 = Static Coeff.

02 = Software Search

Option Help: PCIe Gen3 Equalization Phase 3 Method

ACS

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Access Control Services Extended Capability

URR

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Unsupported Request Reporting Enable/Disable.

FER

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Device Fatal Error Reporting Enable/Disable.

NFER

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Device Non-Fatal Error Reporting Enable/Disable.

CER

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Device Correctable Error Reporting Enable/Disable.

CTO

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Completion Timer TO Enable/Disable.

SEFE

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Root PCI Express System Error on Fatal Error Enable/Disable.

SENFE

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Root PCI Express System Error on Non-Fatal Error Enable/Disable.

SECE

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Root PCI Express System Error on Correctable Error Enable/Disable.

PME SCI

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: PCI Express PME SCI Enable/Disable.

Hot Plug

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCI Express Hot Plug Enable/Disable.

Advanced Error Reporting

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Advanced Error Reporting Enable/Disable.

PCIe Speed

Option Default: 00

00 = AUTO

01 = Gen1

02 = Gen2

03 = Gen3

Option Help: Configure PCIe Speed

Detect Timeout

Option Default: 0000

Minimum = 0000

Maximum = FFFF

Step = 0001

Option Help: The number of milliseconds reference code will wait for link to exit. Detect state for enabled ports before assuming there is no device and potentially disabling the port.

Extra Bus Reserved

Option Default: 00

Minimum = 00

Maximum = 07

Step = 01

Option Help: Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

Reserved Memory

Option Default: 000A

Minimum = 0001

Maximum = 0014

Step = 0001

Option Help: Reserved Memory for this Root Bridge (1-20) MB

Reserved I/O

Option Default: 04

Minimum = 04

Maximum = 14

Step = 04

Option Help: Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.

PCIEx CLKREQ Mapping Override

Option Default: 00

00 = Default

01 = No CLKREQ

02 = Custom number

Option Help: PCIE CLKREQ Override for default platform mapping.

SATA and RST Configuration

SATA Controller(s)

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable SATA Device.

SATA Mode Selection

Option Default: 00

00 = AHCI

01 = Intel RST Premium

Option Help: Determines how SATA controller(s) operate.

RAID Device ID

Option Default: 00

00 = Client

01 = Alternate

Option Help: Choose RAID Device ID

Port [0/1]

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable or Disable SATA Port

Hot Plug

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Designates this port as Hot Pluggable.

Spin Up Device

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

SATA Device Type

Option Default: 00

00 = Hard Disk Drive

01 = Solid State Drive

Option Help: Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

USB Configuration

Port Disable Override

Option Default: 00

00 = Disable

01 = Select Per-Pin

Option Help: Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

USB SS Physical Connector #0-5

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.

USB HS Physical Connector #0-9

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.

Serial IO Configuration

Option Name: I2C[0-5], SPI[0-1], UART[0-2] Controller

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enables/Disables Serial IO Controller

The following devices depend on each other:

I2C0 and I2C1,2,3

UART0 and UART1,SPI0,1

UART2 and I2C4,5

EPMe-42 Usage:

I2C0 = User interface (3.3V). CBR-4005B J2[1,3].

I2C1 = Interface to LPC header / A-EPM43S.

Port 2,3,4,5 Not used.

UART 0 = HSUART COM3 RS-232 / J3[1..5]

UART 1 = HSUART COM4 RS-232 / J3[6..10]

UART 2 = Optional Debug

Serial IO I2C0 Settings

I2C IO Voltage Select

Option Default: 00

00 = 3.3V

01 = 1.8V

Option Help: Selects 1.8v or 3.3v for the controller.

Connected device

Option Default: 00

00 = Disabled

01 = Synaptics Precision Touchpad

02 = Synaptics Forcepad

05 = Custom device

Option Help: Indicates what type of device is connected to this Serial IO controller

Interrupt mode

Option Default: 01

00 = GPIO Interrupt

01 = APIC Interrupt

Option Help: Selects different routing for interrupts from external device

Device's bus address

Option Default: 00

Minimum = 00

Maximum = 7F

Step = 01

Option Help: Specify parameters of custom I2C device

Device's HID address

Option Default: 0000

Minimum = 0000

Maximum = FFFF

Step = 0001

Option Help: Specify parameters of custom I2C device

Device's bus speed

Option Default: 00

00 = 100kHz

01 = 400kHz

02 = 1MHz

Option Help: Specify parameters of custom I2C device

Serial IO I2C1 Settings

I2C IO Voltage Select

Option Default: 00

00 = 3.3V

01 = 1.8V

Option Help: Selects 1.8v or 3.3v for the controller.

Connected device

Option Default: 00

00 = Disabled

01 = Atmel3432 TouchPanel

02 = Atmel2952 TouchPanel

03 = Elan2097 TouchPanel

04 = N-Trig/Samsung 13.3"

05 = N-Trig/Sharp 12.5"

06 = WACOM9015 TouchPanel"

07 = Custom device

Option Help: Indicates what type of device is connected to this Serial IO controller

Interrupt mode

Option Default: 01

00 = GPIO Interrupt

01 = APIC Interrupt

Option Help: Selects different routing for interrupts from external device

Device's bus address

Option Default: 00

Minimum = 00

Maximum = 7F

Step = 01

Option Help: Specify parameters of custom I2C device

Device's HID address

Option Default: 0000

Minimum = 0000

Maximum = FFFF

Step = 0001

Option Help: Specify parameters of custom I2C device

Device's bus speed

Option Default: 00

00 = 100kHz

01 = 400kHz

02 = 1MHz

Option Help: Specify parameters of custom I2C device

Serial IO I2C[2-3] Settings

I2C IO Voltage Select

Option Default: 01

00 = 3.3V

01 = 1.8V

Option Help: Selects 1.8v or 3.3v for the controller.

Serial IO I2C5 Settings

I2C IO Voltage Select

Option Default: 00

00 = 3.3V

01 = 1.8V

Option Help: Selects 1.8v or 3.3v for the controller.

Serial IO UART0 Settings

Bluetooth Device

Option Default: 00

00 = Disabled

01 = Intel Snowfield Peak

02 = Broadcom BRCM 43241

Option Help: Enables/Disables the Vendor Sensor

BT Interrupt Mode

Option Default: 00

00 = GPIO Interrupt

01 = APIC Interrupt

Option Help: Selects different routing for interrupts from external device

Wireless Charging Mode

Option Default: 00

00 = WC Disabled

01 = WC Enabled

Option Help: Set the Wireless Charging Mode

Hardware Flow Control

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When enabled configures additional 2 GPIO pads for use as RTS/CTS signals for UART

Serial IO UART1 Settings

Hardware Flow Control

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When enabled configures additional 2 GPIO pads for use as RTS/CTS signals for UART

Serial IO GPIO Settings

GPIO IRQ Route

Option Default: 0E

0E = IRQ14

0F = IRQ15

Option Help: Route all GPIOs to one of the IRQ.

Serial IO timing parameters

Serial IO timing parameters

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: Serial IO timing parameters (test only)

SCS Configuration

eMMC 5.0 Controller

Option Default: 00

01 = Enabled

00 = Disabled

Option Help: Enable or Disable SCS eMMC 5.0 Controller

eMMC 5.0 HS400 Mode

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable or Disable SCS eMMC 5.0 HS400 Mode

Driver Strength

Option Default: 01

00 = 33 Ohm

01 = 40 Ohm

02 = 50 Ohm

Option Help: Sets I/O driver strength

SDCard 3.0 Controller

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable or Disable SCS SDHC 3.0 Controller

PCH LAN Controller

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable onboard NIC.

Wake on LAN Enable

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable integrated LAN to wake the system.

EFI Network

Option Default: 00

01 = Enabled

00 = Disabled

Option Help: Enable/Disable EFI Network support for onboard LAN.

PXE ROM

Option Default: 01

01 = Enabled

00 = Disabled

Option Help: Enable/Disable PXE Option ROM execution.

CLKRUN# logic

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable the CLKRUN# logic to stop the PCI clocks.

Serial IRQ Mode

Option Default: 01

00 = Quiet

01 = Continuous

Option Help: Configure Serial IRQ Mode.

State After G3

Option Default: 00

00 = S0 State

01 = S5 State

Option Help: Specify what state to go to when power is re-applied after a power failure (G3 state).

Port 80h Redirection

Option Default: 00

00 = LPC Bus

01 = PCIE Bus

Option Help: Control where the Port 80h cycles are sent.

Enhance Port 80h LPC Decoding

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Support the word/dword decoding of port 80h behind LPC

Compatible Revision ID

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable the PCH Compatible Revision ID feature

Enable TCO Timer

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, and stops TCO timer.

Pcie Pll SSC

Option Default: FF

FF = Auto

00 = 0.0%

01 = 0.1%

02 = 0.2%

03 = 0.3%

04 = 0.4%

05 = 0.5%

06 = 0.6%

07 = 0.7%

08 = 0.8%

09 = 0.9%

0A = 1.0%

0B = 1.1%

0C = 1.2%

0D = 1.3%

0E = 1.4%

0F = 1.5%

10 = 1.6%

11 = 1.7%

12 = 1.8%

13 = 1.9%

14 = 2.0%

Option Help: Pcie Pll SSC percentage.AUTO - Keep hw default, no BIOS override. Range is 0.0%-2.0%.

PCH-FW Configuration

Configure Management Engine Technology Parameters

ME State

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When Disabled ME will be put into ME Temporarily Disabled Mode.

Manageability Features State

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Intel(R) Manageability features.

Note: This option disables/enables Manageability Features support in FW.

To disable support platform must be in an unprovisioned state first.

AMT BIOS Features

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When disabled AMT BIOS Features are no longer supported and user is no longer able to access MEBx Setup.

Note: This option does not disable Manageability Features in FW.

AMT Configuration

ASF support

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Alert Standard Format support.

USB Provisioning of AMT

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable of AMT USB Provisioning.

CIRA Configuration

Activate Remote Assistance Process

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: Trigger CIRA (Client Initiated Remote Access) boot

Note: Network Access must be activated first from MEBx Setup.

CIRA Timeout

Option Default: 00

Minimum = 00

Maximum = FF

Step = 01

Option Help: OEM defined timeout for MPS connection to be established.

0 - use the default timeout value of 60 seconds.

255 - MEBx waits until the connection succeeds

ASF Configuration

PET Progress

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PET Events Progress to receive PET Events.

WatchDog

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable WatchDog Timer.

OS Timer

Option Default: 0000

Minimum = 0000

Maximum = FFFF

Step = 0001

Option Help: Set OS watchdog timer.

BIOS Timer

Option Default: 0000

Minimum = 0000

Maximum = FFFF

Step = 0001

Option Help: Set BIOS watchdog timer.

Secure Erase Configuration

Secure Erase mode

Option Default: 00

00 = Simulated

01 = Real

Option Help: Change Secure Erase module behavior:

Simulated: Performs SE flow without erasing SSD

Real: Erase SSD.

Force Secure Erase

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Force Secure Erase on next boot

OEM Flags Configuration

MEBx hotkey Pressed

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: OEMFLag Bit 1:

Enable automatic MEBx hotkey press.

MEBx Selection Screen

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: OEMFLag Bit 2:

Enable MEBx selection screen with 2 options:

Press 1 to enter ME Configuration Screens

Press 2 to initiate a remote connection

Note: Network Access must be activated from MEBx Setup for this screen to be displayed.

Hide Unconfigure ME Confirmation Prompt

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: OEMFlag Bit 6:

Hide Unconfigure ME confirmation prompt when attempting ME unconfiguration.

MEBx OEM Debug Menu Enable

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: OEMFlag Bit 14:

Enable OEM debug menu in MEBx.

Unconfigure ME

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: OEMFlag Bit 15:

Unconfigure ME with resetting MEBx password to default.

MEBx Resolution Settings

Non-UI Mode Resolution

Option Default: 00

00 = Auto

01 = 80x25

02 = 100x31

Option Help: Resolution for non-UI text mode.

UI Mode Resolution

Option Default: 00

00 = Auto

01 = 80x25

02 = 100x31

Option Help: Resolution for UI text mode.

Graphics Mode Resolution

Option Default: 00

00 = Auto

01 = 640x480

02 = 800x600

03 = 1024x768

Option Help: Resolution for graphics mode.

ME Unconfig on RTC Clear

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: When Disabled ME will not be unconfigured on RTC Clear

Comms Hub Support

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enables/Disables support for Comms Hub.

JHI Support

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Intel(R) DAL Host Interface Service (JHI)

Core Bios Done Message

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Core Bios Done message sent to ME

Firmware Update Configuration

Me FW Image Re-Flash

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable Me FW Image Re-Flash function. Enable needed only for FW downgrades.

Thermal Configuration

CPU Thermal Configuration

DTS SMM

Option Default: 01

00 = Disabled

01 = Enabled

02 = Critical Temp Reporting (Out Of spec)

Option Help: Disabled: ACPI thermal management uses EC reported temperature values.

Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values.

Out of Spec: ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of Spec condition.

Tcc Activation Offset

Option Default: 00

Minimum = 00

Maximum = 3F

Step = 00

Option Help: Offset from factory set Tcc activation temprature at which the Thermal Control Circuit must be activated. Tcc will be activated at: Tcc Activation Temp - Tcc Activation Offset. Tcc Activation Offset range is 0 to 63.

Tcc Offset Time Window

Option Default: 00000000

00000000 = Disabled

00000005 = 5 ms

0000000A = 10 ms

00000037 = 55 ms

…

0004E200 = 320 sec

0005DC00 = 384 sec

0006D600 = 448 sec

Option Help: Tcc Offset Time Window for Running Average Temperature Limit(RATL) feature. The Tcc offset time window can range from 5ms to 448s. For SKL Y SKU the recommended default is 5 Sec, and all other SKUs the recommended default are disabled.

Tcc Offset Clamp Enable

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Tcc Offset Clamp bit Enable for Running Average Temperature Limit(RATL) feature to allow CPU to throttle below P1.

Tcc Offset Lock Enable

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Lock Enable for Running Average Temperature Limit(RATL) feature to lock Temperature Target MSR.

Bi-directional PROCHOT#

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: When a processor thermal sensor trips (either core), the PROCHOT# will be driven.

If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.

Disable PROCHOT# Output

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PROCHOT# Output

Disable VR Thermal Alert

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable VR Thermal Alert

PROCHOT Response

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PROCHOT Response

PROCHOT Lock

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PROCHOT Lock

ACPI T-States

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: Enable/Disable ACPI T-States.

PECI Reset

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PECI Reset during Sx. Enabling will trigger a PECI Reset during boot to resolve rare Sx PECI issue. Via pcode mailbox command 0x36. Default is disabled.

PECI C10 Reset

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable PECI C10 Reset command. Enables a mailbox command to resolve rare PECI related C10 issues. Via pcode mailbox command 0x24. Default is disabled/ no command sent.

Platform Thermal Configuration

Automatic Thermal Reporting

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Configure _CRT, _PSV and _AC0 automatically based on values recommended in BWG's Thermal Reporting for Thermal Management settings. Set to Disabled for manual configuration.

Critical Trip Point

Option Default: 77

7F = 127 C

77 = 119 C (POR)

6F = 111 C

67 = 103 C

64 = 100 C

5F = 95 C

57 = 87 C

4F = 79 C

47 = 71 C

3F = 63 C

37 = 55 C

2F = 47 C

27 = 39 C

1F = 31 C

17 = 23 C

0F = 15 C

Option Help: This value controls the temperature of the ACPI Critical Trip Point - the point in which the OS will shut the system off.

Note: 119C is the Plan of Record (POR) for all Intel mobile processors.

Active Trip Point 0

Option Default: 47

7F = Disabled

0F = 15 C

17 = 23 C

1F = 31 C

27 = 39 C

2F = 47 C

37 = 55 C

3F = 63 C

47 = 71 C

4F = 79 C

57 = 87 C

5F = 95 C

67 = 103 C

6F = 111 C

77 = 119 C (POR)

Option Help: This value controls the temperature of the ACPI Active Trip Point 0 - the point in which the OS will turn the processor fan on Active Trip Point 0 Fan Speed.

Active Trip Point 0 Fan Speed

Option Default: 64

Minimum = 00

Maximum = 64

Step = 01

Option Help: Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (Fan off) - 100 (Max fan speed). This is the speed at which fan will run when Active Trip Point 0 is crossed.

Active Trip Point 1

Option Default: 37

7F = Disabled

0F = 15 C

17 = 23 C

1F = 31 C

27 = 39 C

2F = 47 C

37 = 55 C

3F = 63 C

47 = 71 C

4F = 79 C

57 = 87 C

5F = 95 C

67 = 103 C

6F = 111 C

77 = 119 C (POR)

Option Help: This value controls the temperature of the ACPI Active Trip Point 1 - the point in which the OS will turn the processor fan on Active Trip Point 1 Fan Speed.

Active Trip Point 1 Fan Speed

Option Default: 4B

Minimum = 00

Maximum = 64

Step = 01

Option Help: Active Trip Point 1 Fan Speed in percentage. Value must be between 0 (Fan off) - 100 (Max fan speed). This value must be less than Active Trip Point 0 Fan speed. This is the speed at which fan will run when Active Trip 1 is crossed.

Passive Trip Point

Option Default: 5F

77 = 119 C (POR)

6F = 111 C

67 = 103 C

5F = 95 C

57 = 87 C

4F = 79 C

47 = 71 C

3F = 63 C

37 = 55 C

2F = 47 C

27 = 39 C

1F = 31 C

17 = 23 C

0F = 15 C

7F = Disabled

Option Help: This value controls the temperature of the ACPI Passive Trip Point - the point in which the OS will begin throttling the processor.

Passive TC1 Value

Option Default: 01

Minimum = 01

Maximum = 10

Step = 01

Option Help: This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 - 16

Passive TC2 Value

Option Default: 05

Minimum = 01

Maximum = 10

Step = 01

Option Help: This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 - 16

Passive TSP Value

Option Default: 0A

Minimum = 02

Maximum = 20

Step = 02

Option Help: This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 - 32

Active Trip Points

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Disable Active Trip Points

Passive Trip Points

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Disable Passive Trip Points

Critical Trip Points

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Disable Critical Trip Points

PCH Thermal Device

Option Default: 01

00 = Disabled

01 = Enabled in PCI mode

02 = Enabled in ACPI mode

Option Help: Enable/Disable PCH Thermal Device(D20:F2)

PCH Temp Read

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: PCH Temperature Read Enable

CPU Energy Read

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: CPU Energy Read Enable

CPU Temp Read

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: CPU Temperature Read Enable

Alert Enable Lock

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Lock all Alert Enable settings

PCH Alert

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: PCH Alert pin enable

DIMM Alert

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: DIMM Alert pin enable

CPU Temp

Option Default: 48

Minimum = 01

Maximum = 6E

Step = 01

Option Help: Help on CPU Temperature

CPU Fan Speed

Option Default: 41

Minimum = 01

Maximum = 64

Step = 01

Option Help: Fan speed that EC will use if OS is hung

VersaLogic Features

Mini Card Mode

Option Default: 02

00 = Pin 43 mSATA Detect

01 = Pin 51 mSATA Detect

02 = Pin 43 or 51 mSATA Detect

03 = Force PCIe Mini Card Mode

04 = Force mSATA SSD Mode

Option Help: The Mini Card slot can support either a PCIe Mini Card or an mSATA module. The mSATA specifications states that Pin 51 on the connector can be used to automatically detect an mSATA module. But some modules also use Pin 43 due to conflicts on Pin 51. Almost all modules will be correctly detected by using the setting of Pin 43 or Pin 51 mSATA Detect, but there may be cases on older or non-standard modules where more specific settings are required (including forcing the slot to always be a PCIe Mini Card or an mSATA module).

FPGA UARTs

UART[1/2]

Option Default: 01

00 = Disabled

01 = Enabled

Option Help: Enable or disable UART[1/2]. Note: These settings apply to COM1 and COM2 which are RS232/422/485 ports based in the FPGA. COM3 and COM4 are also RS232 ports but use Kaby Lake HSUARTs and require special OS drivers.

Base Address

Option Default: 00

00 = 3F8

01 = 2F8

02 = 220

03 = 228

04 = 238

05 = 2E8

06 = 338

07 = 3E8

Option Help: Select the base address for UART1.

IRQ

Option Default: 09

00 = Disabled

08 = IRQ3

09 = IRQ4

0A = IRQ5

0B = IRQ10

0C = IRQ6

0D = IRQ7

0F = IRQ11

Option Help: Select the IRQ for UART1, or disable it.

Mode

Option Default: 00

00 = RS-232

01 = RS-422

02 = RS-485 (Manual Direction Control)

03 = RS-485 (Automatic Direction Control)

Option Help: Select the mode for UART1.

Subtitle: EPM-43 ISA (PC/104) Bus Options

Option Name: 16-bit Access Mode

Option Default: 00

00 = Standard

01 = Legacy

Option Help: Standard: 16-bit cards support both 8-bit (using SBHE) and 16-bit accesses.

Legacy: 16-bit cards support only 16-bit or paired 8-bit accesses. SBHE signal not supported.

ISA Bus I/O Space

I/O decoder [1-3] base address (hex)

Option Default: 0000

Minimum = 0000

Maximum = FFFC

Step = 0004

Option Help: Specify base address of ISA I/O space decoder.

Valid range is 0x100 to 0xFFFC. Base address must be size-aligned. E.g. 0x40 byte window can be based at 0x100, 0x140,…

Warning: Setting this to areas conflicting with other devices may cause boot failure. A value below 0xFFC is recommended.

I/O decoder [1-3] size

Option Default: 0004

0004 = 4 bytes

0008 = 8 bytes

0010 = 16 bytes

0020 = 32 bytes

0040 = 64 bytes

0080 = 128 bytes

0100 = 256 bytes

Option Help: Specify size of ISA I/O space decoder. Valid range is 4 to 256 bytes, and it must be a power of 2.

Regions must not overlap.

ISA Bus Memory Space

64KB Memory Space at 0xD0000

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Memory cycles from 0xD0000 to 0xDFFFF are routed to the ISA / PC/104 bus.

ISA bus IRQ control

ISA IRQ [3-15]

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable this IRQ on the ISA bus.

Warnings:

3: UART2 uses IRQ3 by default.

4: UART1 uses IRQ4 by default.

7, 10, 11: PCI devices may this use this IRQ.

PIRQ[A-H] Routing

Option Default: 0B

03 = IRQ3

04 = IRQ4

05 = IRQ5

06 = IRQ6

07 = IRQ7

0A = IRQ10

0B = IRQ11

0E = IRQ14

0F = IRQ15

Option Help: Configure PCI IRQ

IRQ9 is reserved for SCI. IRQ14/15 can be used for interrupt of Serial IO GPIO controller

Security Menu 4

Secure Boot Configuration

Secure Boot Option

Option Default: 01

00 = Disabled

01 = Enabled

Delete Platform Key

Option Help: PK will be deleted but keep other signatures such as KEK/db/dbx, which allow platform owner to modify the secure boot variables without authentication. The platform will be changed to setup mode, and secure boot is disabled automatically.

Delete All Signatures

Option Help: Delete all the secure boot signatures including PK/KEK/db/dbx.

The platform will be changed to setup mode, and secure boot is disabled automatically.

Reset to Default

Option Help: Reset secure boot variables to manufacturing default including PK/KEK/db/dbx.

Delete Signatures

Signatures Information

Enroll Signatures

Option Help: It helps the physical present user to enroll signatures from files into signature database (db).

When the user clicks this menu item, the system displays file explorer. If the user selects one file of the extension EFI, CER or DER, it will be enrolled as a signature into signature database.

Set Supervisor Password

Option Help: Set or clear the Supervisor account's password.

Set User Password

Option Help: Set to clear the User account's password.

Min. password length

Option Default: 01

Minimum = 01

Maximum = 14

Option Help: Set the minimum number of characters for password (1-20).

Authenticate User on Boot

Option Default: 00

00 = Disabled

01 = Enabled

Option Help: Enable/Disable User Authentication Prompt on boot.

Option Name: HDD Password Select

Option Default: 01

00 = User+Master

01 = User Only

Option Help: Supports user only or both user and master password.

HDD Security Status

HDDxx Password State

Option Default: N/A

Unsupported

Cleared

User

User+Master

Master

Frozen

Count Expired

Option Help: States whether the HDD user and master password is set or cleared.

Subtitle: Trusted Platform Module (TPM)

Option Name: Current Selected TPM Device

Option Default: 02

00 = Disabled

03 = fTPM

02 = TPM 2

01 = TPM 1.2

Option Help: Choose current on board TPM device.

Submenu: TPM Configuration

Option Name: Current TPM State

Option Default: N/A

00 = Unknown

01 = Enabled and Activated

02 = Enabled and Deactivated

03 = Disabled and Activated

04 = Disabled and Deactivated

05 = TPM 2

Option Name: TPM Action

Option Default: 00

00 = No Change

01 = TPM2 HierarchyControl (TPM_RH_OWNER YES, TPM_RH_ENDORSEMENT YES)

02 = TPM2 HierarchyControl (TPM_RH_OWNER NO, TPM_RH_ENDORSEMENT NO)

05 = TPM2 ClearControl(NO) + Clear

17 = TPM2 PCR_Allocate(Algorithm IDs)

18 = TPM2 Change EPS

21 = TCG2 LogAllDigests

22 = TPM2 HierarchyControl (TPM_RH_OWNER NO, TPM_RH_ENDORSEMENT YES)

60 = TCG2 Storage Enable Block SID

61 = TCG2 Storage Disable Block SID

Option Help: Enact TPM Action. Note: Most TPM actions require TPM to be Enabled to take effect.

TCG2 Protocol Configuration

Information fields at default values:

```
Supported Event Log Format   TCG_1_2, TCG_2
Hash Algorithm Bitmap        SHA1, SHA256
Number of PCR Banks          2
Active PCR Banks             SHA1, SHA256
  PCR Bank: SHA1             [X]
  PCR Bank: SHA256           [X]
  PCR Bank: SHA384           [ ]
  PCR Bank: SHA512           [ ]
  PCR Bank: SM3_256          [ ]
```

Option Name: PCR Bank: SHA1

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: TCG2 Request PCR Bank: SHA1

Option Name: PCR Bank: SHA256

Option Default: 01

0 = Unchecked

1 = Checked

Option Help: TCG2 Request PCR Bank: SHA256

Option Name: PCR Bank: SHA384

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: TCG2 Request PCR Bank: SHA384

Option Name: PCR Bank: SHA512

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: TCG2 Request PCR Bank: SHA512

Option Name: PCR Bank: SM3_256

Option Default: 00

0 = Unchecked

1 = Checked

Option Help: TCG2 Request PCR Bank: SM3_256

5 Boot Menu

View or configure boot device order

Keys used to view or configure devices: ↑ and ↓ arrows Select a device. '+' and '-' move the device up or down. 'Shift + 1' enables or disables a device. 'Del' deletes an unprotected device.

Example menu:

```
Boot Priority Order
   1. USB HDD: Flash Drive
   2. USB CD:
   3. USB FDD:
   4. ATAPI CD:
   5. ATA HDD0:
   6. ATA HDD1: WDC WD3200AAJS-56M0A0
   7. ATA HDD2:
   8. ATA HDD3:
   9. ATA HDD4:
  10. ATA HDD5:
  11. Other HDD:
  12. SD Card:
  13. PCI LAN: IBA CL Slot 00FE v0104
```

6 Misc Menu

File Explorer

Browse local FAT-formatted media for Secure Boot certificate files for key enrollment into DB, DBX, DBT, PK, and KEK databases.

Intel(R) Ethernet Connection I219-LM – xx:xx:xx:xx:xx:xx

Configure the PCH LAN Controller.

iSCSI Configuration

Configure iSCSI boot attempts.

Opal

Configure Opal compliant data storage devices.

Driver Health Manager

Manage UEFI Driver Health

Exit Menu 7

Exit Saving Changes

This item saves changes to the system, exits the setup menu and reboots.

Exit Discarding Changes

This option exits the setup menu without saving any changes.

Load Setup Defaults

Equal to F9. Load standard default values.

Discard Changes

This option will reset the system without any changes being saved.

Save Changes

This option saves changes and resets the system.