Basic Input/Output System Setup Utility

User Guide

An overview of the BIOS Setup Utility used on **Intel® Server D50DNP** and **Intel® Server M50FCP** product families

Rev. 1.3

Jun 2024

Delivering Breakthrough Data Center System Innovation–Experience What's Inside!

<Blank Page>

Document Revision History

February 2023	1.0	• Production Release
February 2023	1.1	• Deleted content describing PMEM features
Aug 2023	1.2	• Removed Enforced Password Support knob. • Updated DIMM information. • Replaced Intel Integrator Toolkit with Intel Firmware Customization. • Updated Attempt Secure Boot notes. • Added UMA-Based Clustering knob • Updated NUMA Optimized comments • Remove Enable power Cycle Policy knob. • Remove SSC description • Added TDX Item for EMR • Add Capable information in SST-PP. • Update Memory Operating Speed Selection for EMR • Update UPI Link Frequency for EMR • Update IO Directory Cache (IODC) Default value • Updated ACS Control help info. • Updated SNC comments. • Updated C1E comments. • Update C1 Auto Demotion Default value • Update SGX PRM Size Default value • Updated the table in Appendix A. Intel Tool Support
June 2024	1.3	• Add Riser1_Slot_3 Bifurcation in “PCIe Slot Bifurcation Setting” page • Set “Correctable Error Threshold” to 500 as default • Set “Trigger SW Error Threshold” to Enable as default • Set “IIO eDPC Interrupt” to Disable as default • Add “PRS Capability for PCIe” • Add “CXL Type 3 Legacy” and “CXL Security Level” • Update the table in Appendix A. Integrated IO Configuration: NTB Configuration • Update Help text of “Correctable Error Threshold” • Remove the comment related with 4096G of Memory Mapped I/O Size.

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claims thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

Copies of documents that have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Xeon, SpeedStep, and Intel Xeon Phi, and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This user guide provides an overview of the features and functions offered by the embedded Basic Input/Output System (BIOS) setup utility included on Intel® Server D50DNP and Intel® Server M50FCP product families. These server products support the 4th Gen and 5th Gen Intel® Xeon® Scalable processor family. The BIOS setup utility manages options used to configure built-in devices, the boot manager, and the error manager.

Use the BIOS setup utility to:

- View, set, or change system configuration options.
- Set or cancel system administrator and user passwords.
- View or change baseboard management controller (BMC) access parameters.
- View system error messages.

The BIOS setup utility is a text-based utility allowing users to configure the system, view current settings, and view environmental information for platform devices.

The BIOS setup utility interface consists of several pages or screens. Each page contains information or links to other pages. The Advanced tab in the Setup screen displays a list of general categories as links. These links lead to pages containing a specific category's configuration.

The BIOS setup utility has the following features:

- **Console redirection:** The BIOS setup utility is accessible via console redirection over various terminal emulation standards (refer to the *BIOS EPS for the Intel® Server M50FCP and Intel® Server D50DNP product families.* When this feature is enabled, the POST display is purely in text mode due to the redirection data transfer in a serial port data terminal emulation mode. This mode may limit some functionality for compatibility; for example, usage of colors, some keys or key sequences, or support of pointing devices.
  - Setup screens are designed to be displayable in a 100-character per 31-line format, so they can work with console redirection. However, this screen layout should display correctly on any format with longer lines or more lines on the screen.
- **Password protection:** The BIOS Setup screen may be protected from unauthorized changes by setting an administrative password in the Security screen. When an administrative password is set, all selection and data entry fields in Setup screens (except System Time and Date) are grayed out. When grayed out, the user cannot change these fields unless the administrative password has been entered.

Note: If an administrative password has not been set, anyone who boots the system to the Setup screen has access to and can change all selection and data entry fields.

2. BIOS Setup Utility Operation

2.1 BIOS Setup Page Layout

The BIOS setup page layout is sectioned into functional areas. Each occupies a specific area of the screen and has dedicated functionality.

The setup page is designed to a format of 80 x 25 (25 lines of 80 characters each). The typical display screen in a legacy mode or in a terminal emulator mode is 80 characters by 25 lines, but with line wrapping enabled, the 25th line cannot be used with the setup page.

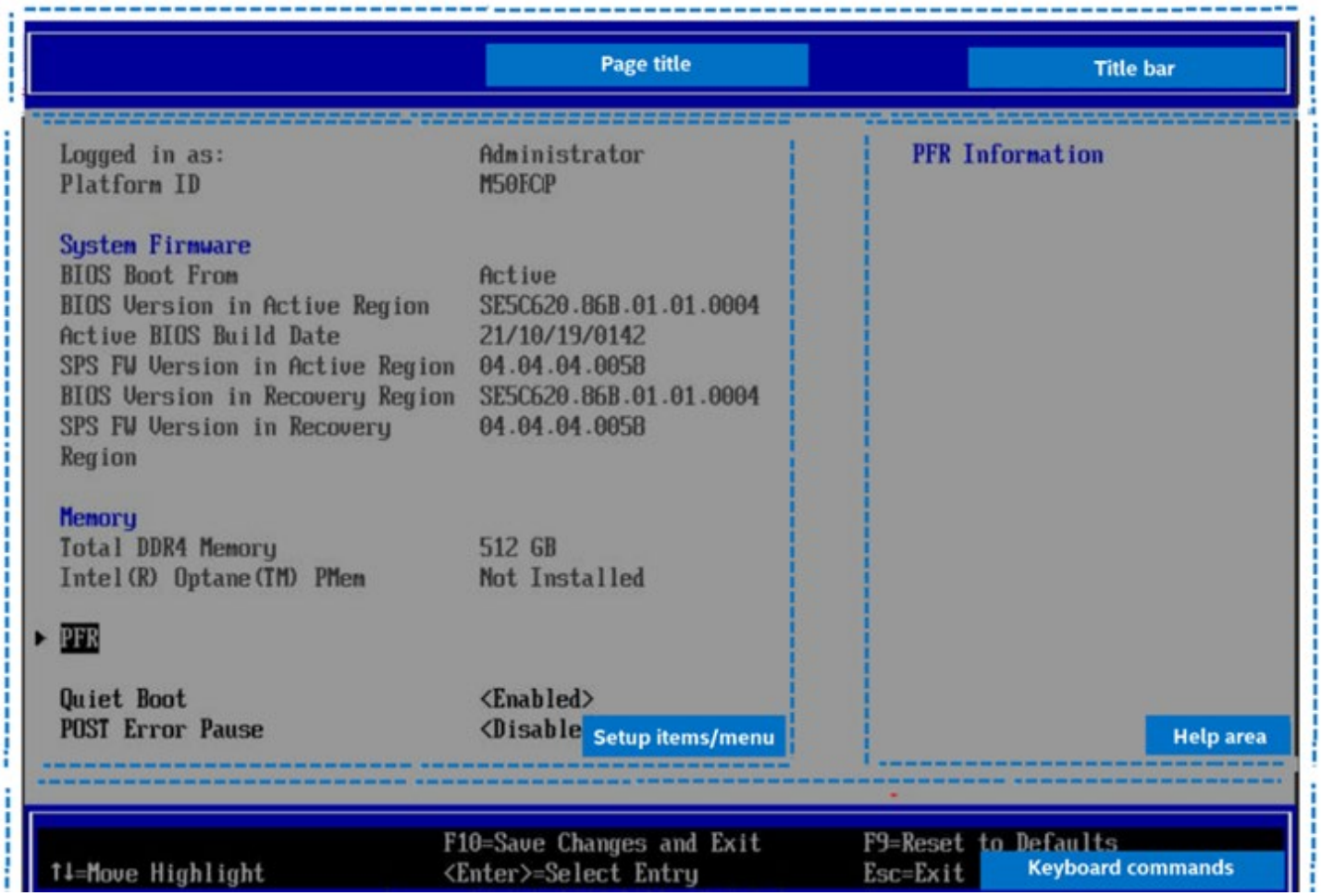

Figure 1. BIOS Setup Utility Page Layout

The following table lists and describes each functional area of a BIOS Setup page.

Table 1. BIOS Setup Page Layout

Functional Area	Description
Page Title	In a multi-level hierarchy of pages beneath one of the top-level Tabs, the Page Title identifies the specific page that the user is viewing. Using the <ESC> key returns the user to the higher level in the hierarchy, until the top-level page is reached.
Title Bar	The Title Bar displays tabs with the titles of the top-level pages or screens that can be selected. Using the left and right arrow keys moves from page to page through the tabs. When more tabs than can be displayed are open on the Title Bar, they are scrolled off to the left or right of the screen, and temporarily disappear from the visible Title Bar. Using the arrow keys scrolls them back onto the visible Title Bar. When the arrow keys reach either end of the Title Bar, they wrap around to the other end of the Title Bar. For multi-level hierarchies, this shows only the top-level page above the page that the user is viewing. The Page Title gives further information.
Setup Item List	The setup item list is a set of control entries and informational items. The list is displayed in two columns: The left column of the list contains Prompt String (or Label String), a character string that identifies the item. The Prompt String may be up to 34 characters long in the 80 x 25-page format. The right column contains a data field that may be an informational data display, a data input field, or a multiple-choice field. Data input or multiple-choice fields are identified by square brackets [....]. This field may be up to 90 characters long but only the first 22 characters can be displayed on the 80 x 25 page (24 characters for an informational display-only field). The operator navigates up and down the right-hand column through the available input or choice fields. A Setup Item may also represent a selection to open a new screen with a further group of options for specific functionality. In this case, the user navigates to the desired selection and presses <Enter> to go to the new screen.
Item-Specific Help Area	The item-specific help area is on the right side of the screen and contains help text specific to the highlighted Setup Item. Help information may include the meaning and usage of the item, allowable values, effects of the options, etc. The help area is a 29 character by 11-line section of the 80 x 25 page. The help text may have explicit line-breaks within it. When the text is longer than 29 characters, it is also broken to a new line, dividing the text at the last space (blank) character before the 29th character. An unbroken string of more than 29 characters is arbitrarily wrapped to a new line after the 29th character. Text that extends beyond the end of the 11th line is not displayed.
Keyboard Command Area	The keyboard command area is at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys.

2.2 Entering BIOS Setup

To enter the BIOS setup using a keyboard (or emulated keyboard), press the **<F2>** function key during boot time when the OEM or Intel logo screen or the POST diagnostic screen is displayed.

The following instructional message is displayed on the diagnostic screen or under the quiet boot logo screen:

```
Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot
```

Note: With a USB keyboard, wait until the BIOS discovers the keyboard and beeps. The system does not read any key press until the USB controller has been initialized and the USB keyboard activated.

If no errors are detected during POST, pressing the <F2> key will display the BIOS Setup utility's Main page. However, should a serious error occur during POST, the system will alternately display an Error Manager page instead.

It is also possible to boot directly to the BIOS Setup utility using the IPMI 2.0 command:

```
Get/Set System Boot Options
```

2.3 Exit BIOS Setup

The user exits the BIOS Setup utility using one of these three methods:

1. Pressing the hotkey **<F10>**
2. Selecting **<Save Changes and Exit>**
3. Selecting **<Discard Changes and Exit>**

The system performs a cold reset regardless of which exit option is selected.

For more information on the Save & Exit screen, see Section 3.9.

2.4 BIOS Setup Page Navigation

The bottom right portion of the BIOS setup screen displays the keyboard commands used to navigate through the BIOS Setup utility. Keyboard navigation commands are always displayed.

Table 2. BIOS Setup Keyboard Command Bar

Key	Option	Description
<Enter>	Execute Command	The **<Enter>** key is used to activate submenus when the selected feature is a submenu, or to display a pick list if a selected option has a value field, or to select a subfield for multi-valued features like time and date. If a pick list is displayed, the <Enter> key selects the currently highlighted item, undoes the pick list, and returns the focus to the parent menu.
<Esc>	Exit	The **<Esc>** key provides a mechanism for backing out of any field. When the **<Esc>** key is pressed while editing any field or selecting features of a menu, the parent menu is re-entered. When the **<Esc>** key is pressed in any submenu, the parent menu is re-entered.
<↑>	Select Item	The up arrow is used to select the previous value in a pick list, or the previous option in a menu item's option list. The selected item must then be activated by pressing the <Enter> key.
<↓>	Select Item	The down arrow is used to select the next value in a menu item's option list, or a value field's pick list. The selected item must then be activated by pressing the <Enter> key.
<Tab>	Select Field	The **<Tab>** key is used to move between fields. For example, <Tab> can be used to move from hours to minutes in the time item in the main menu.
<->	Change Value	The minus key on the keypad is used to change the value of the current item to the previous value. This key scrolls through the values in the associated pick list without displaying the full list.
<+>	Change Value	The plus key on the keypad is used to change the value of the current menu item to the next value. This key scrolls through the values in the associated pick list without displaying the full list. On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboards but has the same effect.

<F9>	Reset to Defaults	Pressing the **<F9>** key causes the following to display:
		`Load default configuration?`
		`Press 'Y' to confirm, 'N' / 'ESC' to ignore.`
		If **<Y>** is pressed, all setup fields are set to their default values. If **<N>** is pressed, or if the **<Esc>** key is pressed, the user is returned to where they were before **<F9>** was pressed without affecting any existing field values.

<F10>	Save Changes and Exit	Pressing the **<F10>** key causes the following message to display:
		`Save configuration changes and exit?`
		`Press 'Y' to confirm, 'N' / 'ESC' to ignore.`
		If **<Y>** is pressed, all changes are saved, and the setup is exited. If **<N>** is pressed, or the **<Esc>** key is pressed, the user is returned to where they were before **<F10>** was pressed without affecting any existing values.

3. BIOS Setup Screens

This section describes the screens available in the BIOS setup utility for the configuration of the server platform.

For each of these screens, there is an image of the screen with a list of field descriptions detailing the contents of each item on the screen. Each item on the screen is hyperlinked to the relevant field description.

These field description lists follow several guidelines:

- The text heading for each field description is the actual text displayed on the BIOS setup screen. The screen text in each figure is a hyperlink to its corresponding field description.
- The text shown as the value for each field description is the actual text displayed on the BIOS setup screen. The text for default value is shown in **bold**.
- The help text entry is the actual text that appears on the BIOS setup screen when the item is in focus (active on the screen).
- The comments entry provides additional information where it may be helpful. This information does not appear on the BIOS setup screen.
- Information enclosed in angular brackets (< >) in the screen figures and field descriptions identifies text that can vary, depending on the options installed. For example, <Amount of memory installed> is replaced by the actual value for the Total Memory field.
- Information enclosed in square brackets ([ ]) in the field descriptions identifies areas where the user must type in text instead of selecting from a provided option.
- When information is changed (except date and time), the system requires a save and reboot action for the changes to take effect. Alternatively, pressing **<ESC>** discards the changes and resumes power on self-test (POST) to continue to boot the system according to the boot order set from the last boot.

3.1 Setup Screen Map

The setup menu map contains the entire BIOS setup collection and organizes them into major categories. Each category has a hierarchy with a top-level screen from which lower-level screens may be selected.

Each top-level screen appears as a tab entry, arranged across the top of all top-level screens. To access a top-level screen from the front page or other top-level screen, press the up or down arrow keys to traverse the tabs until the desired screen is selected.

The categories and the screens included in each category are listed in the following table, with links to each of the screens named.

Table 3. BIOS Setup Screen Map

Top-Level Categories	Second Level Screens	Third Level Screens
Main Screen	PFR	-
Advanced Screen	Processor Configuration	-
	Power & Performance	Uncore Power Management
		CPU P State Control
		Hardware P States
		CPU C State Control
	UPI Configuration	-
	Memory Configuration	Adv MemTest Rank Selection
		Memory RAS and Performance Configuration
		-
	System Event Log	PCIE Fatal Error Mask Setting
	Integrated IO Configuration	PCIe Slot Bifurcation Setting
		Processor PCIe Link Speed
		PCIe Misc. Configuration
		Volume Management Device
		NTB Configuration
	Mass Storage Controller Configuration	SATA Port Configuration
	PCI Configuration	NIC Configuration
		UEFI Network Stack
		UEFI Option ROM Control
	Serial Port Configuration	-
	USB Configuration	-
	System Acoustic and Performance Configuration	
Security Screen	-	-
Server Management Screen	Console Redirection	-
	System Information	-
	BMC LAN Configuration	User Configuration
Error Manager Screen	-	-
Boot Manager Screen	-	-
Boot Maintenance Manager Screen	Advanced Boot Options	Secure Boot Configuration
		HTTPS Boot Configuration
	Add EFI Boot Option	-
	Delete EFI Boot Option	-
	Change Boot Order	-
Save & Exit Screen	-	-

3.2 Main Screen

If no errors are detected during POST, the BIOS Setup Main screen is the first screen when entering the BIOS setup utility.

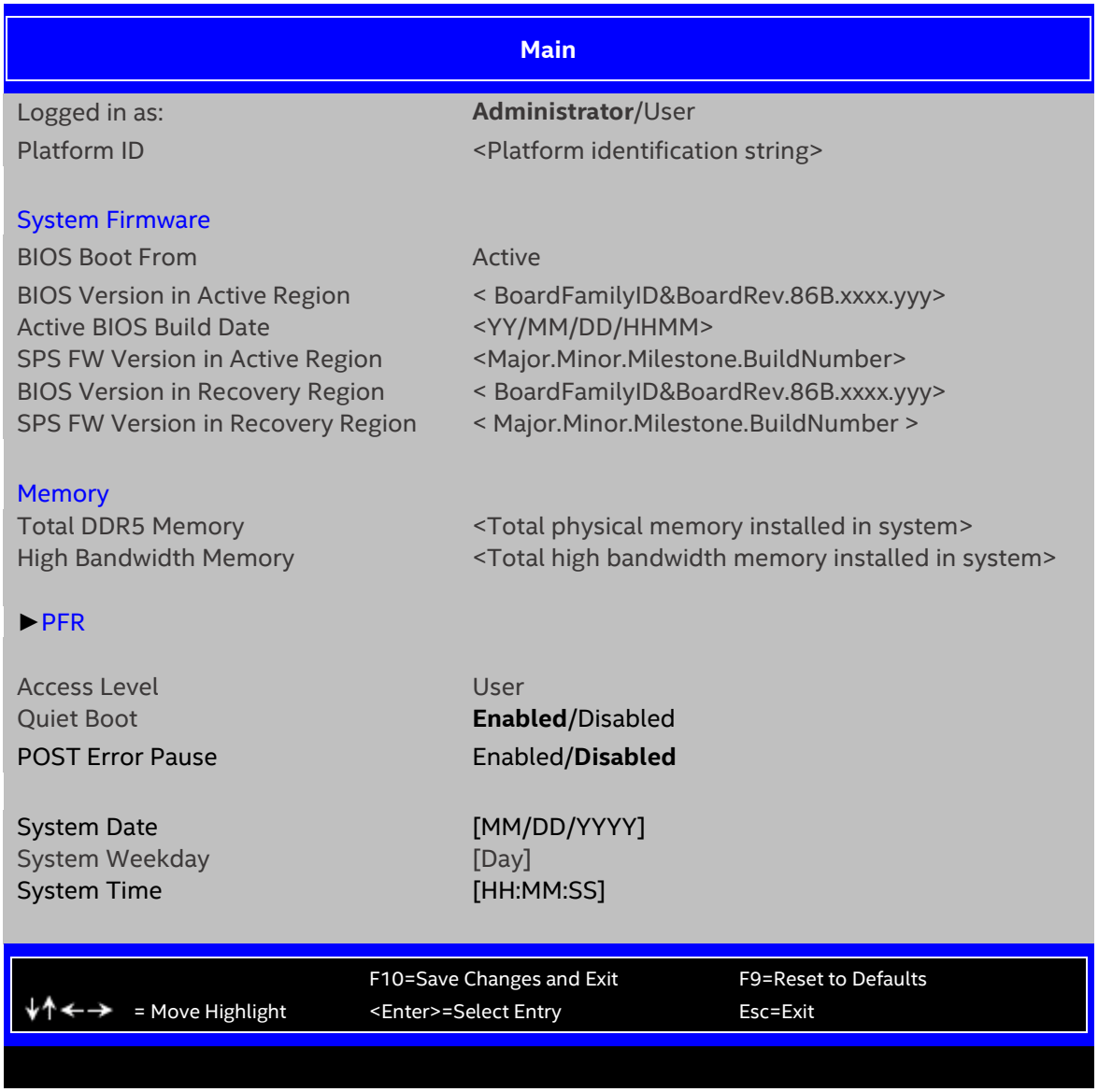

Figure 2. Main Screen

1. **Logged in as:**

   Value: **Administrator**/User

   Help text: None.

   Comments: *Information only*. Displays password level that setup is running in: Administrator or User. With no passwords set, Administrator is the default mode. For more information about BIOS password protection, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.1.

   Back to: Main Screen – Screen Map

2. **Platform ID**

   Value: <Platform identification string>

   Help text: None.

   Comments: *Information only*. Displays the platform ID (board ID) for the board on which the BIOS is executing POST.

The platform ID is limited to eight characters, a limitation of Advanced Configuration and Power Interface (ACPI) tables.

For a list of platform IDs and related product-specific information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

Back to: Main Screen – Screen Map

3. BIOS Boot From

Value: **Active**

Help text: None.

Comments: *Information only*. Per PFR feature, BIOS always boots from Active region.

Back to: Main Screen – Screen Map

4. BIOS Version in Active Region

Value: < BoardFamilyID&BoardRev.86B. xxxx.yyy>

Help text: None.

Comments: *Information only*. The BIOS version uniquely identifies the BIOS in the active region that is installed and operational on the board. The version information displayed is taken from the BIOS ID string, with the timestamp segment dropped off. The segments displayed are:

- BoardFamilyID – Identifies the server platform.
- BoardRev - define the level of debug output built into and enabled by BIOS.
- 86B – Identifies this BIOS as being a tool for Intel Server Boards.
- xxxx– Major revision level of the BIOS.
- yyy – Build type and minor revision of the BIOS.

For full details about interpreting the BIOS ID string, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.1.2.

Back to: Main Screen – Screen Map

5. Active BIOS Build Date

Value: < YY/MM/DD/HHMM >

Help text: None.

Comments: *Information only*. The date displayed is taken from the timestamp segment of the BIOS ID string and indicates the date when the currently installed primary BIOS was created (built). For full details about the BIOS ID string, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.1.2.

Back to: Main Screen – Screen Map

6. SPS FW Version in Active Region

Value: < Major.Minor.Milestone.BuildNumber >

Help text: None.

Comments: *Information only*. Detailed SPS firmware information will be available in the revision of the *Intel® Management Engine (Intel® ME)-BIOS Interface Specification* (CDI: 548530) for this generation of server boards. The segments displayed are:

- Major – a server segment code.
- Minor – a minor version number.
- MileStone – a milestone number.
- BuildNumber– a build number.

Back to: Main Screen – Screen Map

7. BIOS Version in Recovery Region

Value: < BoardFamilyID&BoardRev.86B. xxxx.yyy>

Help text: None.

Comments: *Information only*. The BIOS version uniquely identifies the BIOS in the recovery region that is installed and operational on the board. The version information displayed is taken from the BIOS ID string, with the timestamp segment dropped off. The segments displayed are:

- BoardFamilyID – Identifies the server platform.
- BoardRev - define the level of debug output built into and enabled by BIOS.
- 86B – Identifies this BIOS as being a tool for Intel Server Boards.
- xxxx– Major revision level of the BIOS.
- yyy – Build type and minor revision of the BIOS.

For full details about interpreting the BIOS ID string, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.1.2.

Back to: Main Screen – Screen Map

8. SPS FW Version in Recovery Region

Value: < Major.Minor.Milestone.BuildNumber >

Help text: None.

Comments: *Information only*. Detailed SPS firmware information will be available in the revision of the *Intel® Management Engine (Intel® ME)-BIOS Interface Specification* (CDI: 548530) for this generation of server boards. The segments displayed are:

- Major – a server segment code.
- Minor – a minor version number.
- MileStone – a milestone number.
- BuildNumber– a build number.

Back to: Main Screen – Screen Map

9. Total DDR5 Memory

Value: <Total physical DDR5 memory installed in the system>

Help text: None.

Comments: *Information only*. Displays the amount of memory available in the system in the form of installed DDR5 DIMMs in GB. This item does not include HBM information.

Back to: Main Screen – Screen Map

10. High Bandwidth Memory

Value: <Total high bandwidth memory installed in the system>

Help text: None.

Comments: *Information only*. Displays the GB amount of high bandwidth memory available in the system in the form of installed HBMs. This item does not include DDR5 information. This item gets suppressed if there is no HBM CPU installed in the system.

Back to: Main Screen – Screen Map

11. PFR

Value: None.

Help text: PFR Information

Comments: None.

Back to: Main Screen – Screen Map

12. Access Level

Value: User

Help text: None.

Comments: *Information only*. Display access level when setup is running in User. Otherwise, this item will be hidden.

Back to: Main Screen – BIOS Setup

13. Quiet Boot

Value: **Enabled**/Disabled

Help text:
```
[Enabled] – Display the logo screen during POST.

[Disabled] – Display the diagnostic screen during POST.
```

Comments: This field controls whether the full diagnostic information is displayed on the screen during POST. For more information on the POST diagnostic screen, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 4.2. When Console Redirection is enabled, the Quiet Boot setting is disregarded and the text mode diagnostic screen is displayed unconditionally.

Back to: Main Screen – BIOS Setup

14. POST Error Pause

Value: Enabled/**Disabled**

Help text:
```
[Enabled] – Go to the Error Manager for critical POST errors.
[Disabled] – Attempt to boot and do not go to the Error Manager for
critical POST errors.
```

Comments: If enabled, the POST Error Pause option takes the system to the error manager to review the errors when major errors occur. Minor and fatal error displays are not affected by this setting. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 10.4.4.3.2.

Back to: Main Screen – BIOS Setup

15. System Date

Value: [MM/DD/YYYY]

Help text:
```
System Date has configurable fields for the current Month, Day, and
Year.
The year must be between 2022 and 2121.
Use [Enter], [+] or [-] key to modify the selected field.
Use [<-] or [->] key to select the previous or next field.
```

Comments: This field initially displays the current system date. It may be edited to change the system date. When the system date is reset by the BIOS defaults jumper, BIOS recovery flash update, or other method, the date is the earliest date in the allowed range – `01/01/2022`.

Back to: Main Screen – BIOS Setup

16. System Weekday

Value: [Day]

Help text: None.

Comments: This field initially displays the current system day of the week. This field is read only. Its value is calculated from the system date. When the system time is reset by the BIOS defaults jumper, BIOS recovery flash update, or other method, the weekday is that for 01/01/2022 – Saturday.

Back to: Main Screen – BIOS Setup

17. System Time

Value: [HH:MM:SS]

Help text:
```
System Time has configurable fields for Hours, Minutes, and Seconds.
Hours are in 24-hour format.
Use [Enter], [+] or [-] key to modify the selected field.
Use [<-] or [->] key to select the previous or next field.
```

Comments: This field initially displays the current system time in 24-hour format. It may be edited to change the system time. When the system time is reset by the BIOS defaults jumper, BIOS recovery flash update, or other method, the time is the earliest time of day in the allowed range – `00:00:00` (although the time is updated beginning from when it is reset early in POST).

Back to: Main Screen – BIOS Setup

3.2.1 PFR

The PFR screen displays PFR CPLD Firmware status and shows the active and recovery region's SVN and Major/Minor information about PCH and BMC.

To access this screen from the front page, select **Main** > **PFR**. Press the **<Esc>** key to return to the Main screen.

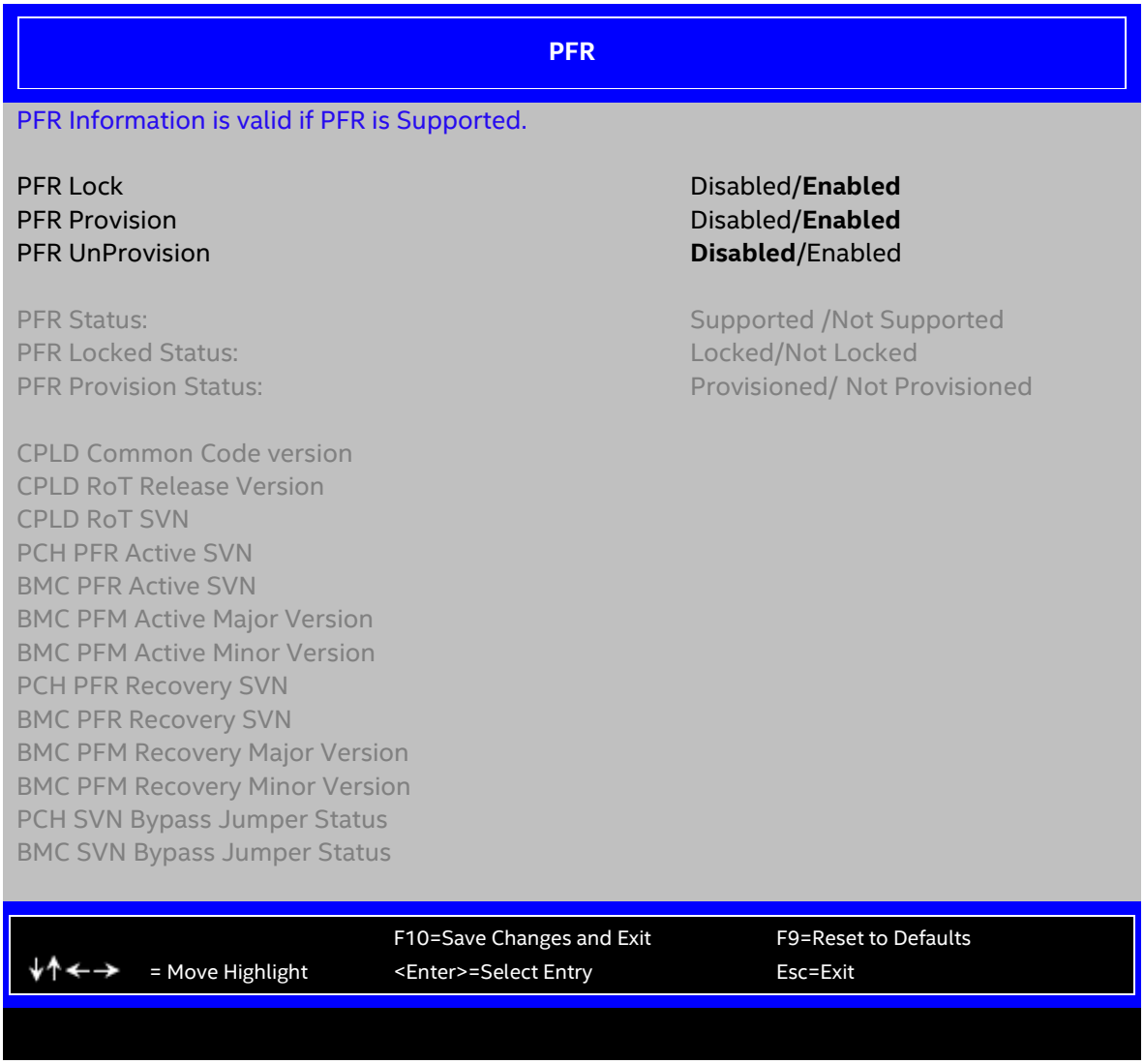

Figure 3. PFR Screen

1. PFR Lock

Value: Disabled/**Enabled**

Help text: `Disable/Enable PFR Lock. When locked, PFR cannot be unlocked unless CPLD is reprogrammed. Selectable only if PFR is (provisioned AND not locked).`

Comments: It is grayed out if it cannot be supported, and it changes to Disabled if PFR Locked Status is locked.

Back to: PFR – Main Screen – BIOS Setup

2. PFR Provision

Value: Disabled/**Enabled**

Help text: `Disable/Enable PFR Provision.Enable to perform PFR Provision. Selectable only if PFR is (not provisioned AND not locked).`

Comments: It changes to Disabled if PFR Provision status is provisioned already.

Back to: PFR – Main Screen – BIOS Setup

3. PFR UnProvision

Value: **Disabled**/Enabled

Help text: `Disable/Enable PFR UnProvision. Enable to Erase PFR Provision Information. Selectable only if PFR is (provisioned AND not locked).`

Comments: It changes to Disabled if PFR Provision status is unprovisioned already.

Back to: PFR – Main Screen – BIOS Setup

4. PFR Status

Value: Supported /Not Supported

Help text: None.

Comments: *Information only*. It gets updated during BIOS POST after getting it back from the PFR Mailbox Register.

Back to: PFR – Main Screen – BIOS Setup

5. PFR Locked Status

Value: Locked/Not Locked

Help text: None.

Comments: *Information only*. It is updated during BIOS POST after getting its value back from the PFR Mailbox Register.

Back to: PFR – Main Screen – BIOS Setup

6. PFR Provision Status

Value: Provisioned/Not Provisioned

Help text: None.

Comments: *Information only*. It is updated during BIOS POST after getting its value back from the PFR Mailbox Register.

Back to: PFR – Main Screen – BIOS Setup

7. CPLD Common Code Version
CPLD RoT Release Version
CPLD RoT SVN
PCH PFR Active SVN
BMC PFR Active SVN
BMC PFM Active Major Version
BMC PFM Active Minor Version
PCH PFR Recovery SVN
BMC PFR Recovery SVN
BMC PFM Recovery Major Version
BMC PFM Recovery Minor Version
PCH SVN Bypass Jumper Status
BMC SVN Bypass Jumper Status

Value: Information only

Help text: None.

Comments: *Information only*. It is updated during BIOS POST after getting back from the PFR Mailbox Register.

Back to: PFR – Main Screen – BIOS Setup

3.3 Advanced Screen

The Advanced screen provides an access point to configure several groups of advanced options. On this screen, select the option group to be configured. Configuration actions are performed on the selected screen and not directly on the Advanced screen.

This screen is the same for all board series, selecting between the same groups of options. However, the options for different boards are not necessarily identical.

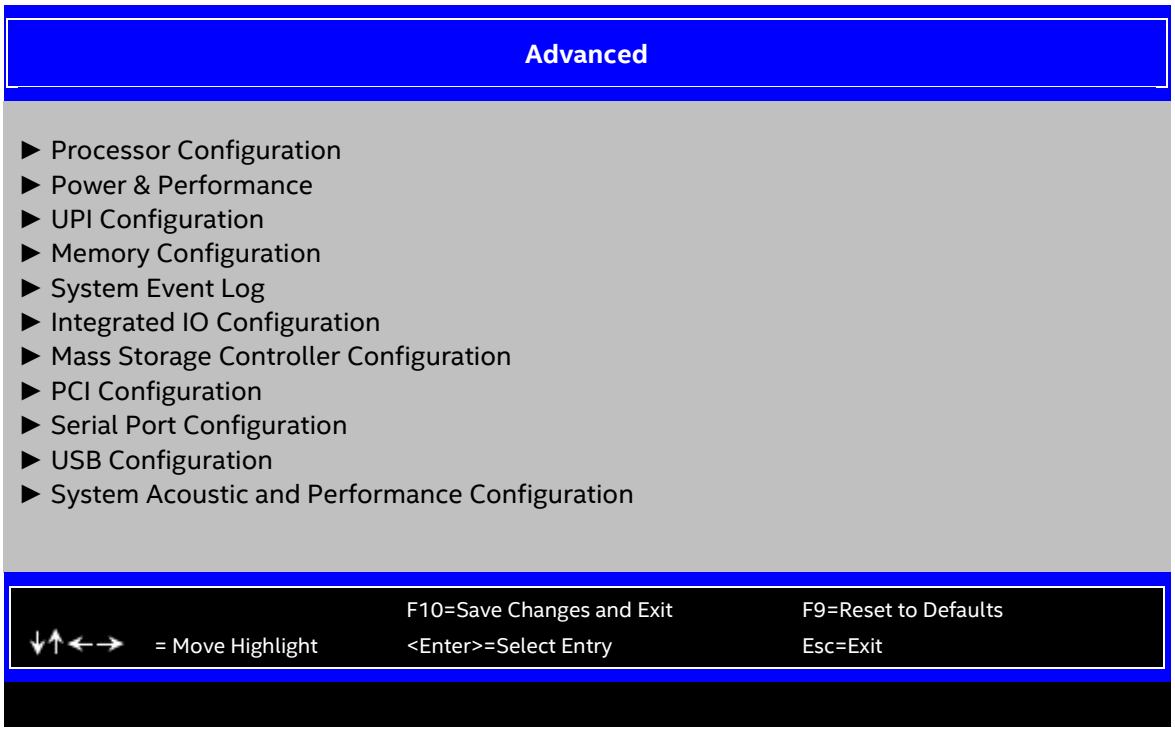

Figure 4. Advanced Screen

1. **Processor Configuration**

   Value: None.

   Help text: `View/Configure processor information and settings.`

   Comments: *Selection only*. For more information on Processor Configuration settings, see Section 3.3.1.

   Back to: Advanced – Main Screen – BIOS Setup

2. **Power & Performance**

   Value: None.

   Help text: `View/Configure power & performance information and settings.`

   Comments: *Selection only*. For more information on Power & Performance settings, see Section 3.3.2.

   Back to: Advanced – Main Screen – BIOS Setup

3. **UPI Configuration**

Value: None.

Help text: `View/Configure UPI information and settings.`

Comments: *Selection only*. For more information on Memory Configuration settings, see Section3.3.3.

Back to: Advanced – Main Screen – BIOS Setup

4. **Memory Configuration**

Value: None.

Help text: `View/Configure memory information and settings.`

Comments: *Selection only*. For more information on Memory Configuration settings, see Section3.3.4.

Back to: Advanced – Main Screen – BIOS Setup

5. **System Event Log**

Value: None.

Help text: `View/Configure system event log information and settings.`

Comments: *Selection only*. For more information on System Event Log settings, see Section3.3.5.

Back to: Advanced – Main Screen – BIOS Setup

6. **Integrated IO Configuration**

Value: None.

Help text: `View/Configure Integrated IO information and settings.`

Comments: *Selection only*. For more information on Integrated IO Configuration settings, see Section 3.3.6.

Back to: Advanced – Main Screen – BIOS Setup

7. **Mass Storage Controller Configuration**

Value: None.

Help text: View/Configure mass storage controller information and settings.

Comments: *Selection only*. For more information on Mass Storage Controller Configuration settings, see Section 3.3.7.

Back to: Advanced – Main Screen – BIOS Setup

8. **PCI Configuration**

Value: None.

Help text: `View/Configure PCI information and settings.`

Comments: *Selection only*. For more information on PCI Configuration settings, see Section 3.3.8.

Back to: Advanced – Main Screen – BIOS Setup

9. **Serial Port Configuration**

Value: None.

Help text: `View/Configure serial port information and settings.`

Comments: *Selection only*. For more information on Serial Port Configuration settings, see Section3.3.9.

Back to: Advanced – Main Screen – BIOS Setup

10. USB Configuration

Value: None.

Help text: `View/Configure USB information and settings.`

Comments: *Selection only*. For more information on USB Configuration settings, see Section 3.3.10.

Back to: Advanced – Main Screen – BIOS Setup

11. System Acoustic and Performance Configuration

Value: None.

Help text: `View/Configure system acoustic and performance information and settings.`

Comments: *Selection only*. For more information on System Acoustic and Performance Configuration settings, see Section 3.3.11.

All the information under System Acoustic and Performance Configuration page is grayed out if the IPMI Security Policy information item on the Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Advanced – Main Screen – BIOS Setup

3.3.1 Processor Configuration

The Processor Configuration screen displays the processor identification and microcode level, core frequency, cache sizes, and Intel® QuickPath Interconnect (Intel® QPI) information for all processors currently installed. It also allows the user to enable or disable a number of processor options.

To access this screen from the front page, select **Advanced** > **Processor Configuration**. Press the **<Esc>** key to return to the Advanced screen.

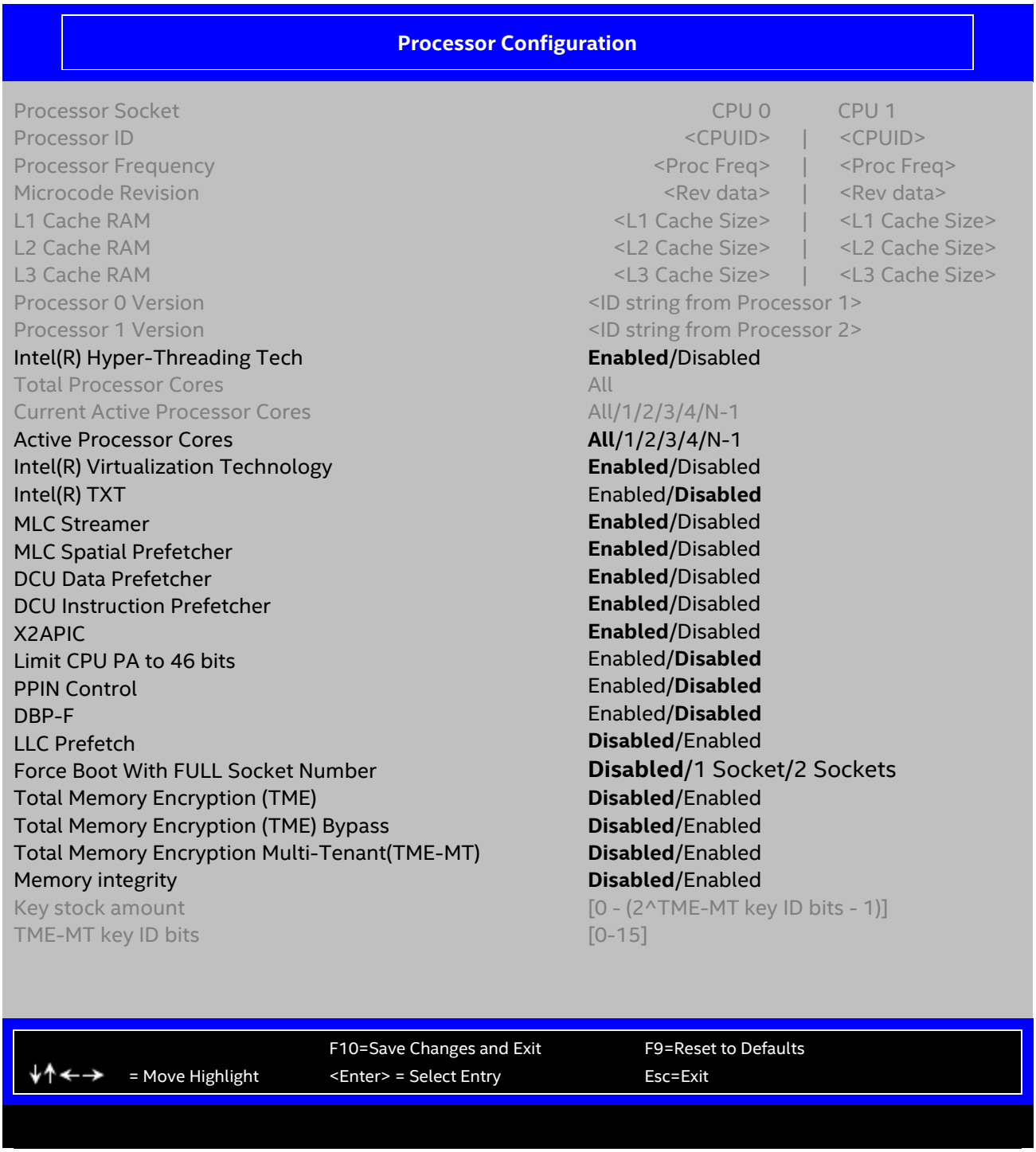

Figure 5. Processor Configuration Screen for Dual-Processor System – Page 1

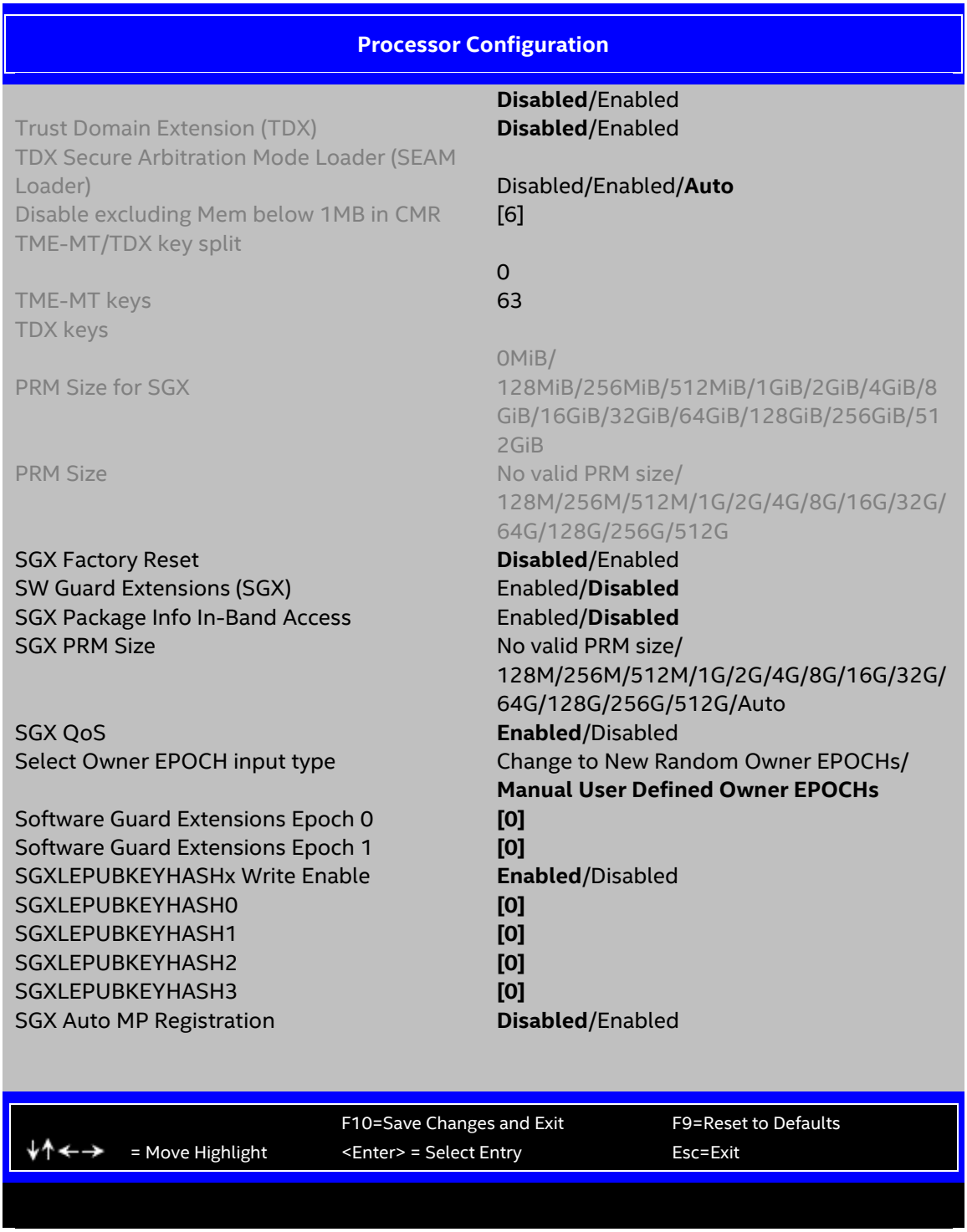

Figure 6. Processor Configuration Screen for Dual-Processor System – Page 2

1. **Processor Socket**

   Value: CPU 0 CPU 1

   Help text: None.

   Comments: *Information only.*

   Back to: Processor Configuration – Advanced– Screen Map

2. **Processor ID**

Value: <CPUID>

Help text: None.

Comments: *Information only*. Displays the processor signature value (from the CPUID instruction) identifying the type of processor and the stepping. For more information about supported processors, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.3.1.

For multi-socket boards, the processor selected as the bootstrap processor (BSP) has an asterisk (*) displayed beside the processor ID. `N/A` is displayed for a processor if not installed.

For the Intel Server Boards M50FCP and D50DNP, two processor IDs are displayed whether the second CPU socket has a processor installed or not. If the socket does not have a processor installed, `N/A` is displayed for the processor data.

Back to: Processor Configuration – Advanced– Screen Map

3. Processor Frequency

Value: <Current processor frequency>

Help text: None.

Comments: *Information only*. Displays current operating frequency of the processor.

Single-socket boards have a single processor display; two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where processors are not installed.

Back to: Processor Configuration – Advanced– Screen Map

4. Microcode Revision

Value: <Microcode revision number>

Help text: None.

Comments: *Information only*. Displays the revision level of the currently loaded processor microcode.

Single-socket boards have a single processor display; two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where processors are not installed.

Back to: Processor Configuration – Advanced– Screen Map

5. L1 Cache RAM

Value: <L1 cache size>

Help text: None.

Comments: *Information only*. Displays size in KB of the processor L1 cache. Since L1 cache is not shared between cores, this is shown as the amount of L1 cache per core. Two types of L1 cache are available, so this amount is the total of L1 Instruction Cache plus L1 Data Cache for each core.

Single-socket boards have a single processor display; two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where processors are not installed.

Back to: Processor Configuration – Advanced– Screen Map

6. **L2 Cache RAM**

   Value: <L2 cache size>

   Help text: None.

   Comments: *Information only*. Displays size in KB of the processor L2 cache. Since L2 cache is not shared between cores, this is shown as the amount of L2 cache per core.

   Single-socket boards have a single processor display; two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where processors are not installed.

   Back to: Processor Configuration – Advanced– Screen Map

7. **L3 Cache RAM**

   Value: <L3 cache size>

   Help text: None.

   Comments: *Information only*. Displays size in KB of the processor L3 cache. Since L3 cache is not shared between cores, this is shown as the amount of L3 cache per core.

   Single-socket boards have a single processor display; two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where processors are not installed.

   Back to: Processor Configuration – Advanced– Screen Map

8. **Processor 0 Version**
   Processor 1 Version

   Value: <ID string from processor>

   Help text: None.

   Comments: *Information only*. Displays Brand ID string read from processor with CPUID instruction. Single-socket boards have a single processor display; two-socket and four-socket boards have a display line for each socket, showing `N/A` for empty sockets where processors are not installed.

   Back to: Processor Configuration – Advanced– Screen Map

9. **Intel(R) Hyper-Threading Tech**

   Value: **Enabled**/Disabled

   Help text:
   ```
   Intel(R) Hyper-Threading Technology allows multithreaded software
   applications to execute threads in parallel within each processor.

   Contact your OS vendor regarding OS support of this feature.
   ```

   Comments: This option is only visible if all the processors installed in the server system support Intel® Hyper-Threading Technology (Intel® HT Technology).

   Back to: Processor Configuration – Advanced– Screen Map

10. **Total Processor Cores**

    Value: All

Help text: `Current Total Number of cores to enable in installed processor package.`

Comments: *Information only*. The total processor cores are the number of cores in the processor package. The number of cores that is displayed depends on installed processor cores capability; this may be different from the number on different processor types.

Back to: Processor Configuration – Advanced– Screen Map

11. Current Active Processor Cores

Value: All/1/2/3/4/N-1

Help text: `Current number of cores to enable in each processor package.`

Comments: *Information only*. The current active number of cores where N is the number of cores in the processor package. The number of cores that is displayed depends on an Intel® Node Manager (Intel® NM) IPMI command to disable cores or a setup change to the number of active processor cores; this may be different from the number previously set by the user.

Note: The Intel® Management Engine (Intel® ME) can control the number of active cores independently of the Active Processor Cores BIOS setting. During POST, the BIOS calculates the Active Processor Cores disabled from BIOS setup and Intel NM IPMI command and add them together to disable the Active Process cores.

Back to: Processor Configuration – Advanced– Screen Map

12. Active Processor Cores

Value: **All**/1/2/3/4/N-1

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

Comments: The number of cores that appear as selections depends on the number of cores available in the processors installed. Boards may have as many as 28 cores in each of one, two, or four processors. The same number of cores must be active in each processor package. The “N” means the maximum cores on supported CPUs. For example, the maximum of SPR is 56.

Notes:

- According to the Total Processor Cores item, the selected value for Active Processor Cores must be smaller than the Total Processor Cores value.
- Using this setting to enable or disable processor cores updates the Current Active Processor Core display.
- Using an Intel® NM IPMI command to disable processor cores only updates the Current Active Processor Core display and does not affect this setting.

Back to: Processor Configuration – Advanced– Screen Map

13. Intel(R) Virtualization Technology

Value: **Enabled**/Disabled

Help text: Intel(R) Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions.

Comments: This option is only visible if all processors installed in the system support Intel® Virtualization Technology (Intel® VT). The software configuration installed on the system must support this feature for it to be enabled.

Note: The Intel® VT feature must be enabled to support Intel® Trusted Execution Technology (Intel® TXT). When changing Intel VT from Enabled to Disabled, first make sure Intel® TXT is set to Disabled. This also applies when changing settings using Intel® Firmware Customization or Intel® Server Configuration Utility.

Back to: Processor Configuration – Advanced– Screen Map

14. Intel(R) TXT

Value: Enabled/**Disabled**

Help text: `Enable/Disable Intel(R) Trusted Execution Technology. Takes effect after reboot.`

Comments: Intel® Trusted Execution Technology (Intel® TXT) only appears with products and processors that have Intel TXT capability. This option is only available when both Intel VT and Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) are enabled and on models equipped with a TPM. The TPM must be active in order to support Intel TXT. For information about Intel TXT support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.3.

Note: Changing the Intel® TXT setting requires the system to perform a hard reset for the setting to become effective.

Back to: Processor Configuration – Advanced– Screen Map

15. MLC Streamer

Value: **Enabled**/Disabled

Help text: `MLC Streamer is a speculative prefetch unit within the processor(s). Note: Modifying this setting may affect performance.`

Comments: MLC Streamer is normally enabled for best efficiency in L2 cache and memory channel use, but disabling it may improve performance for some processing loads and on certain benchmarks. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced– Screen Map

16. MLC Spatial Prefetcher

Value: **Enabled**/Disabled

Help text: [Enabled] – Fetches adjacent cache line (128 bytes) when required data is not currently in cache.

`[Disabled] – Only fetches cache line with data required by the processor (64 bytes).`

Comments: MLC Spatial Prefetcher is normally enabled, for best efficiency in L2 cache and memory channel use but disabling it may improve performance for some processing loads and on certain benchmarks. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced– Screen Map

17. DCU Data Prefetcher

Value: **Enabled**/Disabled

Help text: `The next cache line will be prefetched into L1 data cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data.`

`[Disabled] – Only fetches cache line with data required by the processor (64 bytes).`

Comments: DCU Data Prefetcher is normally enabled, for best efficiency in L1 data cache and memory channel use but disabling it may improve performance for some processing loads and on certain benchmarks. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced– Screen Map

18. DCU Instruction Prefetcher

Value: **Enabled**/Disabled

Help text: `The next cache line will be prefetched into L1 instruction cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data.`

Comments: DCU Instruction Prefetcher is normally enabled, for best efficiency in L1 instruction cache and memory channel use but disabling it may improve performance for some processing loads and on certain benchmarks.

Back to: Processor Configuration – Advanced– Screen Map

19. X2APIC

Value: Disabled/**Enabled**

Help text: `Enable/disable extended APIC support`

`Note: When enabled, VT-d will be automatically enabled.`

Comments: The item is for VT-D feature. With 2019 operating system to verify VT-D enabling boot, it needs to be enabled.

Back to: Processor Configuration – Advanced– Screen Map

20. Limit CPU PA to 46 bits

Value: Enabled/**Disabled**

Help text: `Limit CPU physical address to 46 bits to support older Hyper-v.`

Comments: It is a workaround for VT-D function due to operating system issue. When booting with 2019 operating system, this item needs to be enabled for VT-D enabling boot. With 2020H1OS, keep the default value for VT-D enabling boot.

Back to: Processor Configuration – Advanced– Screen Map

21. PPIN Control

Value: Enabled/**Disabled**

Help text: `Unlock and Enable/Disable PPIN Control`

Comments: When PPIN s enabled, the processor will return a 64-bit ID number via the PPIN MSR. This 64-bit ID number is unique within a product family.

Back to: Processor Configuration – Advanced– Screen Map

22. DBP-F

Value: Enabled/**Disabled**

Help text: `The DBP-F can be turned off by writing into the (MSR 792h [5]).`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

23. LLC Prefetch

Value: **Disabled**/Enabled

Help text: `Enable/Disable LLC Prefetch on all threads.`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

24. Force Boot With FULL Socket Number

Value: **Disabled**/1 Socket/2 Sockets

Help text: `Force Boot With FULL Socket Number, otherwise system will do PowerGood Reset.`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

25. Total Memory Encryption (TME)

Value: **Disabled**/Enabled

Help text: `Enable/Disable Total Memory Encryption (TME).`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

26. Total Memory Encryption (TME) Bypass

Value: **Disabled**/Enabled

Help text: `Disable/Enable Total Memory Encryption (TME).`

Comments: When Total memory Encryption knob is enabled:
• Total Memory Encryption is enabled using CPU generated ephemeral key based on hardware random number generator when this knob is disabled.
• Total Memory Encryption is bypassed (no encryption/decryption for KeyID0) when this knob is enabled. On some processors, bypassing TME encryption can provide performance benefits to accesses made with KeyID 0 by avoiding the latency of decryption or encryption and decryption.

Back to: Processor Configuration – Advanced– Screen Map

Note: Please refer to Intel® Architecture Memory Encryption Technologies Specification (DocID: 679154) for more TME details.

27. Total Memory Encryption Multi-Tenant(TME-MT)

Value: **Disabled**/Enabled

Help text: `Enable/Disable Total Memory Encryption Multi-Tenant (TME-MT). Can be enabled only if Processor Configuration -> Limit CPU PA to 46 bits = Disable.`

Comments: When TME is enabled, the item is shown in setup. When the Limit CPU PA to 46 bits is enabled, the item is grayed out.

Back to: Processor Configuration – Advanced– Screen Map

28. Memory integrity

Value: **Disabled**/Enabled

Help text: `Enable/Disable memory Integrity.`

Comments: When TME is enabled, the item is shown in setup. When the Limit CPU PA to 46 bits is enabled, the item is grayed out.

Back to: Processor Configuration – Advanced– Screen Map

29. Key stock amount

Value: [0 - (2^TME-MT key ID bits - 1)]

Help text: `Total number of keys that can be used by TME-MT.`

Comments: *Information only*. The value is 63 when MMIO High Base is 40T or 56T; the value is 127 when MMIO High Base is lower than 40T.

Back to: Processor Configuration – Advanced– Screen Map

30. TME-MT key ID bits

Value: [0 - 15]

Help text: `Total number of bits that can be used by TME-MT.`

Comments: *Information only.* The maximum value of TME-MT key ID bits equals the maximum supported physical address bits minus the current consumed address bits. The value is 6 when MMIO High Base is 40T or 56T; the value is 7 when MMIO High Base is lower than 40T.

Back to: Processor Configuration – Advanced– Screen Map

31. PRM Size for SGX

Value:

0MiB/128MiB/256MiB/512MiB/1GiB/2GiB/4GiB/8GiB/16GiB/32GiB/64GiB/128GiB/256GiB/512GiB

Help text: `Current SGX PRM size Reboot to update.`

Comments: *Information only*. When PRM SGX is edited, this item is changed. The item value is related to the CPU and memory configuration, so it may not be able to show all the options all the time. Only for EMR.

Back to: Processor Configuration – Advanced– Screen Map

32. PRM Size

Value: No valid PRM size/128M/256M/512M/1G/2G/4G/8G/16G/32G/64G/128G/256G/512G

Help text: `Current SGX PRM size Reboot to update.`

Comments: *Information only*. When PRM SGX is edited, this item is changed. The item value is related to the CPU and memory configuration, so it may not be able to show all the options all the time. Only For SPR.

Back to: Processor Configuration – Advanced– Screen Map

33. Trust Domain Extension (TDX)

Value: **Disabled** /Enabled

Help text: `Enable/Disable Trust Domain Extension (TDX).`

Comments: The knob will be grayed out in the following conditions:

- TDX is not supported from processors.
- TME-MT is disabled.
- X2APIC is diabled
- Mirror mode is not disabled.

Back to: Processor Configuration – Advanced– Screen Map

34. TDX Secure Arbitration Mode Loader (SEAM Loader)

Value: **Disabled** /Enabled

Help text: `Enable/Disable TDX Secure Arbitration Mode Loader (SEAM Loader)`

Comments: When Total Memory Encryption (TME) and Total Memory Encryption Multi-Tenant (TME-MT) are disabled, the item is grayed out.

Back to: Processor Configuration – Advanced– Screen Map

35. Disable excluding Mem below 1MB in CMR

Value: Disabled /Enabled/**Auto**

Help text: `Enable/Disable Tdx Excluding CMR below 1MB.`

Comments: When Trust Domain Extension (TDX) is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

36. TME-MT/TDX key split

Value: [1-7]

Help text: `Designate number of bits for TDX usage. The rest will be used by TME-MT.`

Comments: When Trust Domain Extension (TDX) is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

37. TME-MT keys

Value: [(2^(TME-MT key ID bits - TME-MT/TDX key split)) - 1]

Help text: `(KMK) Number of keys designated for TME-MT usage.`

Comments: *Information only*. When Trust Domain Extension (TDX) is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

38. TDX keys

Value: [(2^TME-MT key ID bits) – TME-MT keys - 1]

Help text: `(KTD) Number of keys designed for TDX usage.`

Comments: When Trust Domain Extension (TDX) is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

39. SGX Factory Reset

Value: **Disabled** /Enabled

Help text: `Perform SGX Factory Reset, on subsequent boot: delete all registration data, if SGX enabled will force Initial Platform Establishment flow.`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

40. SW Guard Extensions (SGX)

Value: Enabled/**Disabled**

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

Comments: This option is visible only if Intel® Software Guard Extensions (Intel® SGX) hardware configuration preconditions are met, and will be grayed out in the following conditions:

- Intel® SGX memory configuration is not POR.
- Mirror mode is enabled.
- NUMA is disabled.
- TME is disabled.
- X2APIC is disabled.

Note: All Intel® SGX knobs are either not visible or grayed out in the same conditions with this knob.

Back to: Processor Configuration – Advanced– Screen Map

41. SGX Package Info In-Band Access

Value: Enabled/**Disabled**

Help text: `Enable/Disable Software Guard Extensions (SGX) Package Info In-Band Access`

Comments: None.

Back to: Processor Configuration – Advanced– Screen Map

42. SGX PRM Size

Value: No valid PRM size/128M/256M/512M/1G/2G/4G/8G/16G/32G/64G/128G/256G/512G/Auto

Help text: `SGX PRM Size - just a constituent that may not be equal to the total PRM size`

Comments: When SGX is disabled, the item is grayed out. The item value is related to the CPU and memory configuration, so it may not be able to show all the options all the time. When this item is changed, PRM size gets changed accordingly. Auto is only for EMR.

Note: During POST, the Intel(R) SGX driver for BIOS verifies the system hardware configuration to decide which PRM size value settings are visible in the BIOS setup utility. Meaning that some of the settings are visible in the BIOS setup utility.

Back to: Processor Configuration – Advanced– Screen Map

43. SGX QoS

Value: **Enabled**/Disabled

Help text: `Enable/Disable SGX Quality of Service`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

44. Select Owner EPOCH input type

Value: Change to New Random Owner EPOCHs/**Manual User Defined Owner EPOCHs**

Help text: `Each EPOCH is 64bit, keys value should be different than 0. After generating new epoch via 'Change to New Random Owner EPOCHs', the selection reverts back to 'Manual User Defined Owner EPOCHs'. In next boot keys will be hidden and state will be 'SGX Owner EPOCH activated'.`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

45. Software Guard Extensions Epoch 0

Value: [0- 0xFFFFFFFFFFFFFFFF, **0** is default]

Help text: `Software Guard Extensions Epoch 0`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

46. Software Guard Extensions Epoch 1

Value: [0- 0xFFFFFFFFFFFFFFFF, **0** is default]

Help text: `Software Guard Extensions Epoch 1`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

47. SGXLEPUBKEYHASHx Write Enable

Value: Disabled/**Enabled**

Help text: `Enable writes to SGXLEPUBKEYHASH[3..0] from OS/SW`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

48. SGXLEPUBKEYHASH0

Value: [0- 0xFFFFFFFFFFFFFFFF, **0** is default]

Help text: `SGX Launch Enclave Public Key Hash byte 7-0`

Comments: When SGX is enabled and SGXLEPUBKEYHASHx Write is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

49. SGXLEPUBKEYHASH1

Value: [0- 0xFFFFFFFFFFFFFFFF, **0** is default]

Help text: `SGX Launch Enclave Public Key Hash byte 15-8`

Comments: When SGX is enabled and SGXLEPUBKEYHASHx Write is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

50. SGXLEPUBKEYHASH2

Value: [0- 0xFFFFFFFFFFFFFFFF, **0** is default]

Help text: `SGX Launch Enclave Public Key Hash byte 23-16`

Comments: When SGX is enabled and SGXLEPUBKEYHASHx Write is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

51. SGXLEPUBKEYHASH3

Value: [0- 0xFFFFFFFFFFFFFFFF, 0 is default]

Help text: SGX Launch Enclave Public Key Hash byte 31-24

Comments: When SGX is enabled and SGXLEPUBKEYHASHx Write is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

52. SGX Auto MP Registration

Value: **Disabled**/Enabled

Help text: `Enable/Disable automatic registration in OS MPA agent`

Comments: When SGX is enabled, the item is shown in setup.

Back to: Processor Configuration – Advanced– Screen Map

3.3.2 Power & Performance

The Power & Performance screen allows the user to specify a profile that is optimized in the direction of either reduced power consumption or increased performance.

To access this screen from the front page, select **Advanced** > **Power & Performance**. Press the **<Esc>** key to return to the Advanced screen.

The user can choose one of the four available profiles. When a power and performance profile is chosen, that in turn causes the system to implement a defined list of setup option settings and internal (non-visible) settings. For details on each of these power and performance profiles, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.15.2.

Note: The fields on the Power & Performance screen do not support changes through Intel® Server Configuration Utility with the `/bcs` command and do not support Intel® Firmware Customization (except for of the Workload Configuration setting).

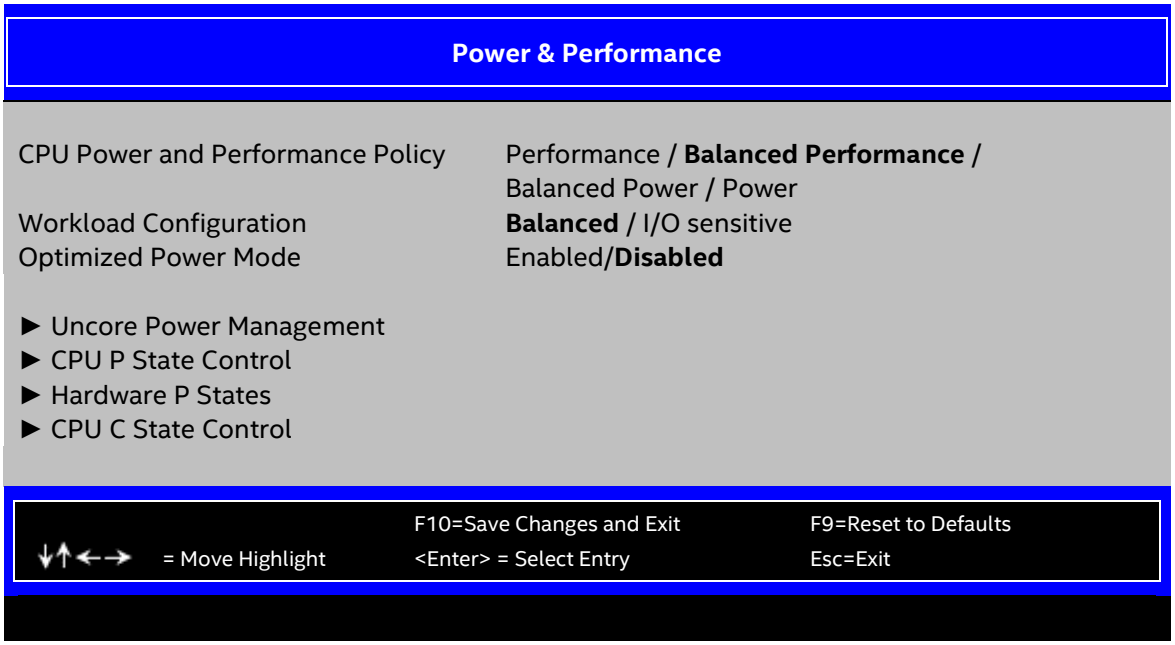

Figure 7. Power & Performance Screen

1. **CPU Power and Performance Policy**

   Value: Performance/**Balanced Performance**/Balanced Power/Power

   Help text: `Allows the user to set an overall power and performance policy for the system, and when changed will modify a selected list of options to achieve the policy. These options are still changeable outside of the policy but do reflect the changes that the policy makes when a new policy is selected.`

   `[Performance] Optimization is strongly toward performance, even at the expense of energy efficiency.`

   `[Balanced Performance] Weights optimization toward performance, while conserving energy.`

   `[Balanced Power] Weights optimization toward energy conservation, with good performance.`

   `[Power] Optimization is strongly toward energy efficiency, even at the expense of performance.`

   Comments: Choosing one of these four power and performance profiles implements a number of changes in BIOS settings, both visible settings in the setup screens and non-visible internal settings. For detailed lists of settings affected by each profile, see the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.15.2.

   Back to: Power & Performance – Advanced – Screen Map

2. **Workload Configuration**

   Value: **Balanced** / I/O Sensitive

   Help text: `Controls the aggressiveness of the energy performance BIAS settings. This bit field allows BIOS to choose a configuration that may improve performance on certain workloads.`

   Comments: Integrated Voltage Regulator (IVR) enables fine granularity voltage regulation and allows the voltage and frequency of uncore to be programmed independently. The uncore activity is monitored to optimize the frequency in real-time. For more information, see the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.15.2. This option is only visible when Enhanced Intel SpeedStep® Technology is enabled by the BIOS. This option is for dual-processor systems only.

   Back to: Power & Performance – Advanced – Screen Map

3. **Optimized Power Mode**

   Value: Enabled/**Disabled**

   Help text: Enable/Disable Optimized Power Mode

   Comments: When this option is enabled, C1E will be suppressed, power performance tuning will be bios control EPB, ENERGY_PERF_BIAS_active idle will be enabled, active idle will be enabled, active idle utilization point will be set to 6, active idle mesh frequency will be 1.4G, Uncore Maximum frequency will be 2.2G.

   Back to: Power & Performance – Advanced – Screen Map

4. **Uncore Power Management**

   Value: None.

   Help text: `View/Configure Uncore Power Management information and settings.`

   Comments: *Selection only*. This option is only visible if Enhanced Intel SpeedStep(R) Tech is enabled. For more information on Uncore Power Management settings, see Section 3.3.2.1.

   Back to: Power & Performance – Advanced – Screen Map

5. **CPU P State Control**

   Value: None.

   Help text: `View/Configure CPU P State Control information and settings.`

   Comments: *Selection only*. For more information on CPU P State Control settings, see Section 3.3.2.2.

   Back to: Power & Performance – Advanced – Screen Map

6. **Hardware P States**

   Value: None.

   Help text: `Hardware P-State setting.`

   Comments: *Selection only*. For more information on Hardware P States settings, see Section 3.3.2.3.

   Back to: Power & Performance – Advanced – Screen Map

7. **CPU C State Control**

   Value: None.

   Help text: `View/Configure CPU C State Control information and settings.`

   Comments: *Selection only*. For more information on CPU C State Control settings, see Section 3.3.2.4.

   Back to: Power & Performance – Advanced – Screen Map

3.3.2.1 Uncore Power Management

The Uncore Power Management screen allows the user to specify a policy that is optimized for the processors with the direction of either reduced power consumption or increased performance.

To access this screen from the front page, select **Advanced** > **Power & Performance** > **Uncore Power Management**. Press the **<Esc>** key to return to the Power & Performance screen.

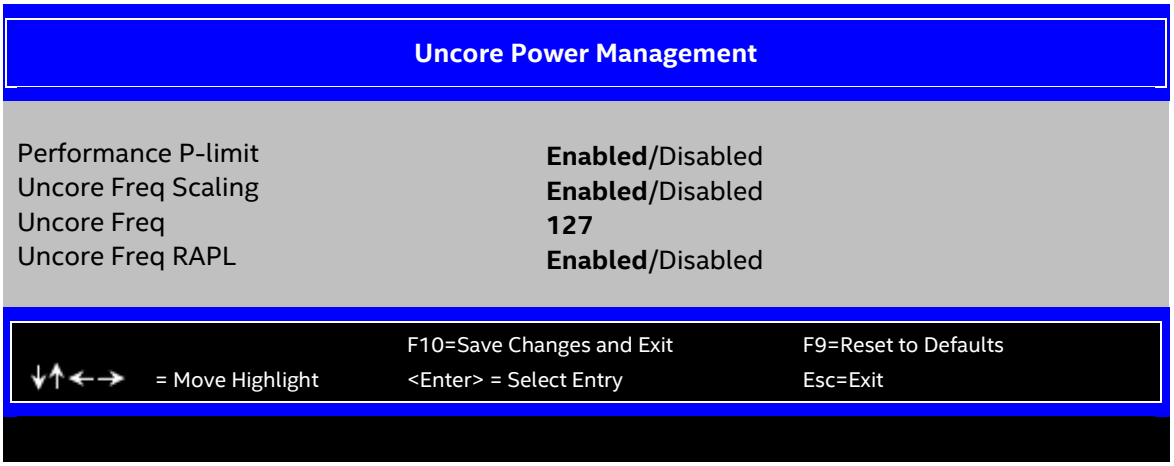

Figure 8. Uncore Power Management Screen

1. **Performance P-limit**

   Value: **Enabled**/Disabled

   Help text: `Allows the Uncore frequency coordination of two processors when enabled.`

   Comments: In a two-socket system, it may be desirable to have the two processors running at similar Uncore frequencies. The Performance P-limit feature does this by coordinating frequency between the two sockets. This avoids latency increases caused by an "idle" socket running at a low CLR frequency, slowing down accesses from a "busy" socket.

   Back to: Uncore Power Management – Power & Performance – Advanced – Screen Map

2. **Uncore Freq Scaling**

   Value: **Enabled**/Disabled

   Help text: `If disable, user can input Uncore Frequency.`

   Comments: None.

   Back to: Uncore Power Management – Power & Performance – Advanced – Screen Map

3. **Uncore Freq**

   Value: **127**

   Help text: `User input Uncore Frequency override MSR 0x620 MinClrRatio[14:8] & MaxClrRatio[6:0]`

   `If input value > MAX_CLM_RATIO, then override with MAX_CLM_RATIO`

   `If input value < MIN_CLM_RATIO, then override with MIN_CLM_RATIO`

   Comments: This option is visible only if Uncore Freq Scaling is disabled.

   Back to: Uncore Power Management – Power & Performance – Advanced – Screen Map

4. **Uncore Freq RAPL**

   Value: **Enabled**/Disabled

   Help text: `Enable: BYPASS_CLM_RAPL_LIMIT = 0`

   `Disable: BYPASS_CLM_RAPL_LIMIT = 1`

   Comments: None.

   Back to: Uncore Power Management – Power & Performance – Advanced – Screen Map

3.3.2.2 CPU P State Control

The CPU P State Control screen allows the user to specify a policy that is optimized for the processors with the direction of either reduced power consumption or increased performance.

To access this screen from the front page, select **Advanced** > **Power & Performance** > **CPU P State Control**. Press the **<Esc>** key to return to the Power & Performance screen.

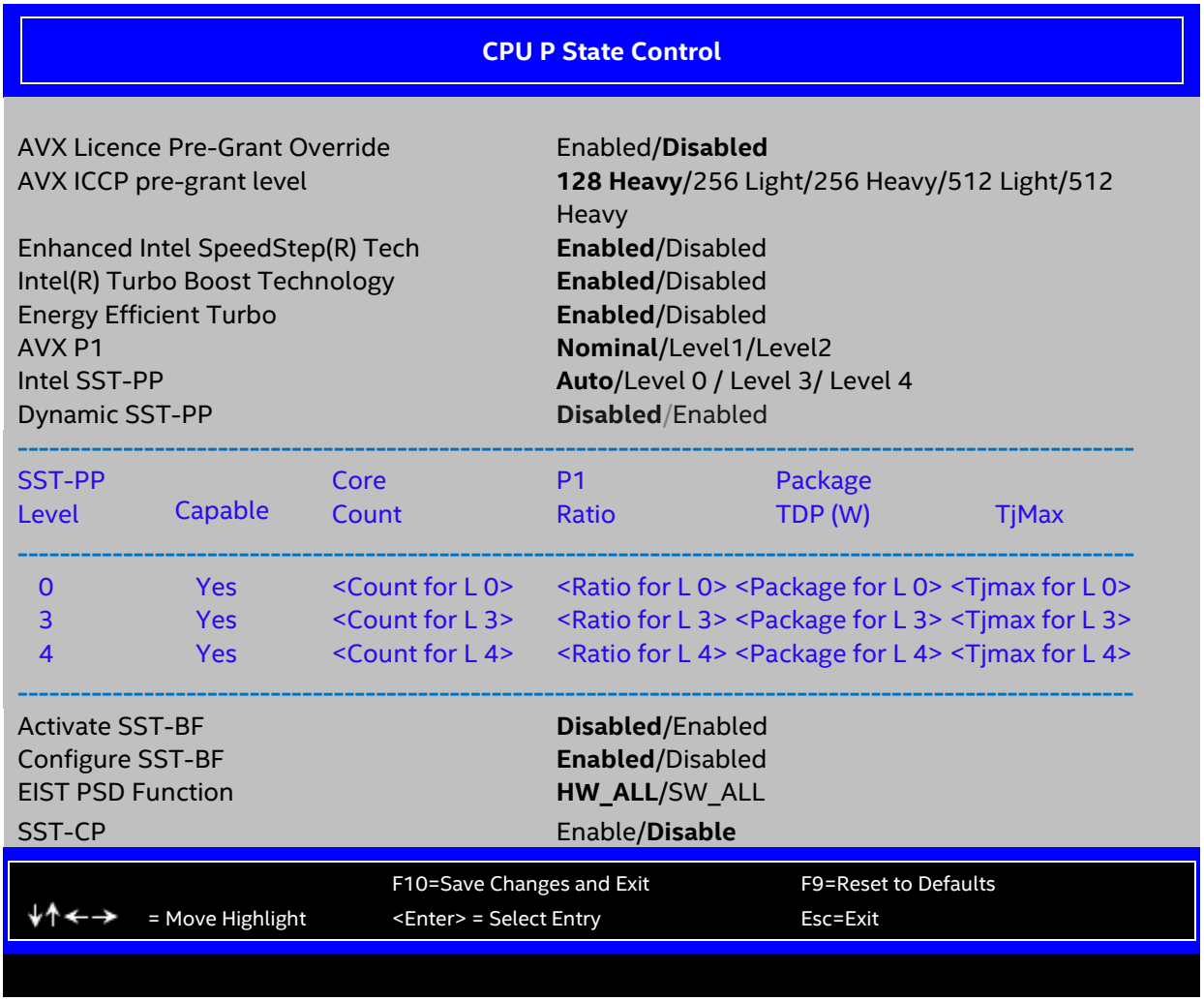

Figure 9. CPU P State Control Screen

1. **AVX Licence Pre-Grant Override**

   Value: Enabled/**Disabled**

   Help text: `Enables AVX ICCP pre-grant level override.`

   Comments: None.

   Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

2. **AVX ICCP pre-grant level**

   Value: **128 Heavy**/256 Light/256 Heavy/512 Light/512 Heavy

   Help text: `Pre-grants an AVX level to the core. Base frequency is not updated`

   Comments: This option is visible only if AVX Licence Pre-Grant Override is enabled.

   Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

3. **Enhanced Intel SpeedStep(R) Tech**

   Value: **Enabled**/Disabled

   Help text: `Enhanced Intel SpeedStep(R) Technology allows the system to dynamically adjust processor voltage and core frequency, which can`

result in decreased average power consumption and decreased average heat production.

Contact your OS vendor regarding OS support of this feature.

Comments: When disabled, the processor setting reverts to running at maximum thermal design power (TDP) core frequency (rated frequency).

This option is only visible if all processors installed in the system support Enhanced Intel SpeedStep(R) Technology. In order that the Intel® Turbo Boost option to be available, Enhanced Intel SpeedStep Technology must be enabled.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

4. **Intel(R) Turbo Boost Technology**

Value: **Enabled**/Disabled

Help text: Intel(R) Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications.

Comments: This option is only visible if all processors installed in the system support Intel(R) Turbo Boost Technology. In order that this option to be available, Enhanced Intel SpeedStep Technology must be enabled.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

5. **Energy Efficient Turbo**

Value: **Enabled**/Disabled

Help text: When Energy Efficient Turbo is enabled, the CPU cores only enter the turbo frequency when the PCU detects high utilization.

Comments: This option is only visible if all processors installed in the system support Intel Turbo Boost Technology. In order that this option to be available, Intel Turbo Boost Technology must be enabled.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

6. **AVX P1**

Value: **Nominal**/Level1/Level2

Help text: AVX P1 level selection

Comments: None.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

7. **Intel SST-PP**

Value: **Auto**/Level 0/ Level 3/ Level 4

Help text: Intel SST-PP Select allows user to choose from up to two additional base frequency conditions.

Comments: This option is visible only if Enhanced Intel SpeedStep(R) Tech is enabled and the CPU supports this feature. This item is not visible when AVX P1 is Nominal and Dynamic SST-PP is Enable.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

8. **Dynamic SST-PP**

   Value: **Disabled/**Enabled

   Help text: `Support Dynamic SST-PP selection`

   `NOTE: HWP Native Mode is a pre-requisite for enabling Dynamic SST-PP.`

   Comments: This item is visible when AVX P1 is Nominal and Hardware P-states is not disabled or Out of Band Mode.

   Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

9. **SST-PP Level**

   Value: 0/3/4

   Help text: None.

   Comments: *Information only*.

   Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

10. **Capable**

    Value: Yes/No

    Help text: None.

    Comments: *Information only*.

    Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

11. **Core Count**

    Value: Core count

    Help text: None.

    Comments: *Information only*. It shows the core count under each SST-PP mode.

    Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

12. **P1 Ratio**

    Value: Current P1 Ratio [4]

    Help text: None.

    Comments: *Information only*. It shows the Current P1 Ratio [4] value under each SST-PP mode.

    Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

13. **Package TDP(W)**

    Value: Package TDP (W)

    Help text: None.

    Comments: *Information only*. It shows the Package TDP (W) value under each SST-PP mode.

    Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

14. **Tjmax**

    Value: Tjmax

Help text: None.

Comments: *Information only*. It shows the maximum junction temperature (TjMax) value under each SST-PP mode.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

15. Activate SST-BF

Value: **Disabled**/Enabled

Help text: `This Option allows Activate SST-BF to be enabled.`

`NOTE: HWP Native Mode is a pre-requisite for enabling SST-BF; HWP Native Mode with No Legacy is a pre-requisite for configuring SST-BF.`

Comments: This option is only visible when SST-BF is capable, AVX P1 is Nominal and Hardware P-states is not disabled or Out of Band Mode.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

16. Configure SST-BF

Value: **Enabled**/Disabled

Help text: `This Option allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.`

Comments: This option is only visible when SST-BF is capable, AVX P1 is Nominal and Hardware P-states is not disabled or Out of Band Mode.

This option is grayed out if the Hardware P-states option is not in Native Mode with No Legacy Support mode or Active SST-BF option is disabled.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

17. EIST PSD Function

Value: **HW_ALL**/SW_ALL

Help text: `Choose HW_ALL/SW_ALL in _PSD return`

Comments: When Enhanced Intel SpeedStep® Technology is enabled, the item can be changed in setup.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

18. SST-CP

Value: Enable/**Disable**

Help text: `This knob controls whether SST-CP is enabled. When enabled it activates per core power budgeting.`

`NOTE: HWP Native Mode is a pre-requisite for enabling SST-CP.`

Comments: No comments.

Back to: CPU P State Control – Power & Performance – Advanced – Screen Map

3.3.2.3 Hardware P States

To access this screen from the front page, select **Advanced** > **Power & Performance** > **Hardware P States**. Press the **<Esc>** key to return to the Power & Performance screen.

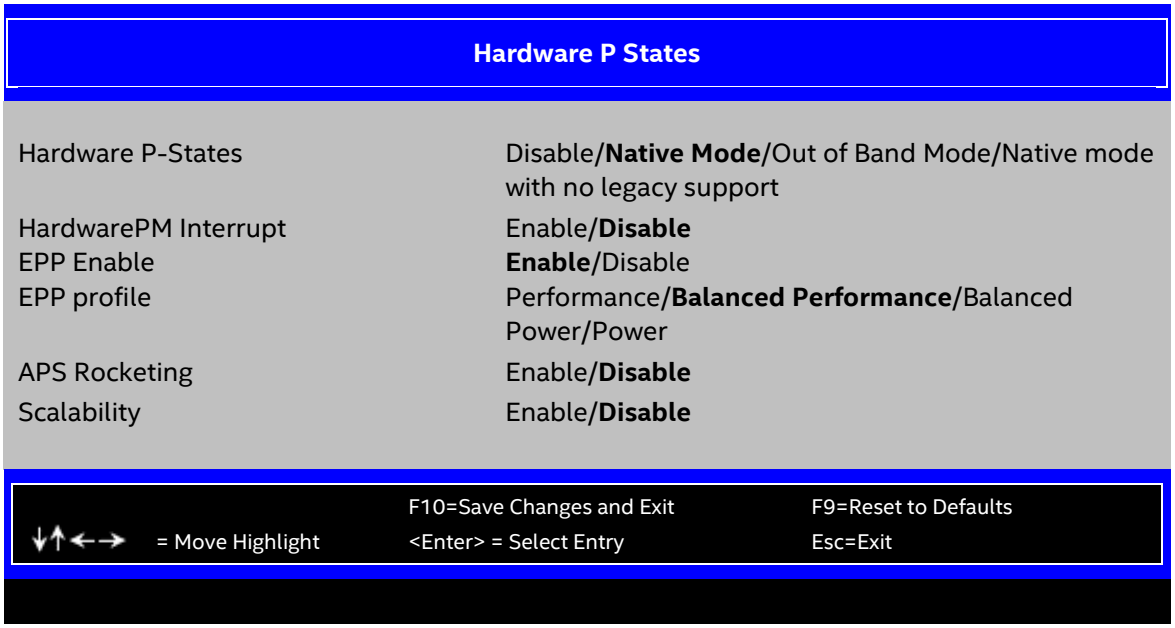

Figure 10. Hardware P States Screen

1. **Hardware P-States**

   Value: Disable/**Native Mode**/Out of Band Mode/Native Mode with No Legacy Support

   Help text:
   ```
   Disable: Hardware chooses a P-state based on OS Request (Legacy P-States)
   Native Mode:Hardware chooses a P-state based on OS guidance
   Out of Band Mode:Hardware autonomously chooses a P-state (no OS guidance)
   NOTE: When HWP mode is Disable or Out of Band Mode, Dynamic SST-PP, SST-BF and SST-CP will be disabled
   ```

   Comments: None.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

2. **HardwarePM Interrupt**

   Value: Enable/**Disable**

   Help text:
   ```
   Enable/Disable Hardware PM Interrupt.
   ```

   Comments: This option is grayed out if the Hardware P-states option is not in Native Mode or Native Mode with No Legacy Support.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

3. **EPP Enable**

   Value: **Enable**/Disable

   Help text: `When enabled, HW masks EPP in CPUID[6].10 and uses the Energy Performance Bias Register for Energy vs. Performance Preference input.`

   Comments: This option is grayed out if Hardware P-states is disabled.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

4. **EPP profile**

   Value: Performance/**Balanced Performance**/Balanced Power/Power

   Help text: `Choose an HWPM Profile (EPP)`

   Comments: This option is only visible if the Hardware P-states option is in Out of Band Mode.
   This option is grayed out if EPP Enable is disabled.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

5. **APS Rocketing**

   Value: Enable/**Disable**

   Help text: `Enable/Disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.`

   Comments: This option is grayed out if Hardware P-states is disabled.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

6. **Scalability**

   Value: Enable/**Disable**

   Help text: `Enable/Disable the use of scalability in HWP pcode power efficiency algorithms. Scalability is the measure of estimated performance improvement for a given increase in core frequency.`

   Comments: This option is grayed out if Hardware P-states is disabled.

   Back to: Hardware P States – Power & Performance – Advanced – Screen Map

3.3.2.4 CPU C State Control

The CPU C State Control screen allows the user to specify a policy that is optimized for the processor's sleep state.

To access this screen from the front page, select **Advanced** > **Power & Performance** > **CPU C State Control**. Press the **<Esc>** key to return to the Power & Performance screen.

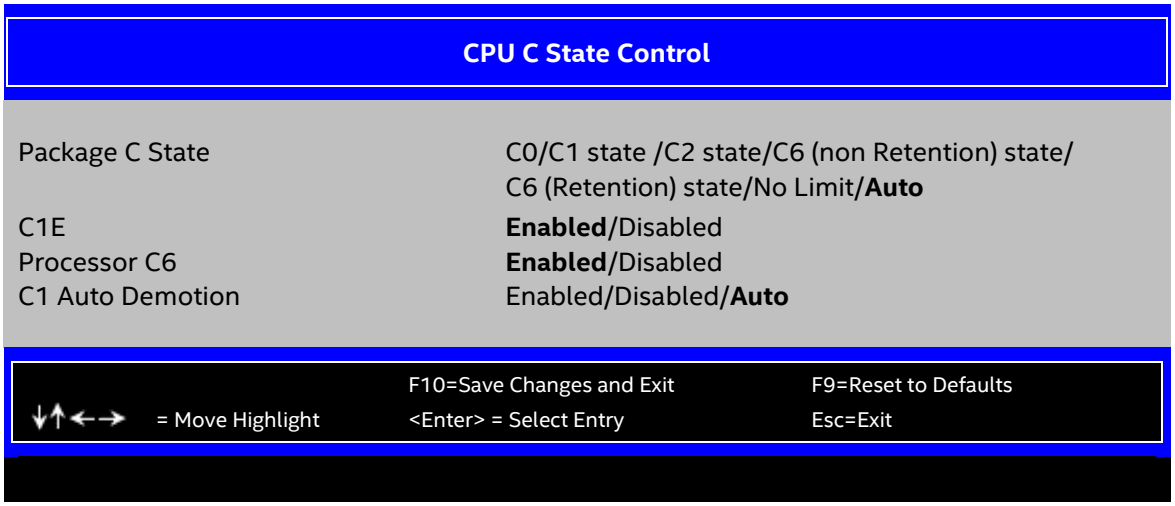

Figure 11. CPU C State Control Screen

1. **Package C State**

   Value: C0/C1 state /C2 state/C6 (non Retention) state/C6 (Retention) state/No Limit/**Auto**

   Help text: `Set and specifies the lowest C-state for Processor package. C0/C1 sate is no package C-state support. C6 retention state provides more power saving than C6 non retention state. No Limit is no package C-state limit.`

   Comments: This option specifies the lowest C state for processor packages.

   Back to: CPU C State Control – Power & Performance – Advanced – Screen Map

2. **C1E**

   Value: **Enabled**/Disabled

   Help text: `When Enabled, the CPU will switch to the Minimum Enhanced Intel SpeedStep(R) Technology operating point when all execution cores enter C1. Frequency will switch immediately, followed by gradual Voltage switching.`

   `When Disabled, the CPU will not transit to the minimum Enhanced Intel SpeedStep(R) Technology operating point when all cores enter C1.`

   Comments: This is normally disabled but can be enabled for improved performance on certain benchmarks and in certain situations. This item is suppressed when Optimized Power Mode is enabled.

   Back to: CPU C State Control – Power & Performance – Advanced – Screen Map

3. **Processor C6**

   Value: **Enabled**/Disabled

   Help text: Enable/Disable Processor C6 (ACPI C3) report to OS.

   Comments: This is normally enabled but can be disabled for improved performance on certain benchmarks and in certain situations.

   Back to: CPU C State Control – Power & Performance – Advanced – Screen Map

4. **C1 Auto Demotion**

   Value: Enabled/Disabled/**Auto**

   Help text: When set, processor will conditionally demote C3/C6/C7 requests to C1 based on uncore autodemote information.

   Comments: When this option is disabled, idle power consumption will be lower than it is enabled.

   Back to: CPU C State Control – Power & Performance – Advanced – Screen Map

3.3.3 UPI Configuration

The UPI Configuration screen allows the user to view details about the Intel® Ultra Path Interconnect (Intel® UPI) link status and alter Intel UPI link speed settings.

Note: This screen is for dual-processor systems only.

To access this screen from the front page, select **Advanced** > **UPI Configuration**. Press the **<Esc>** key to return to the **Advanced** screen.

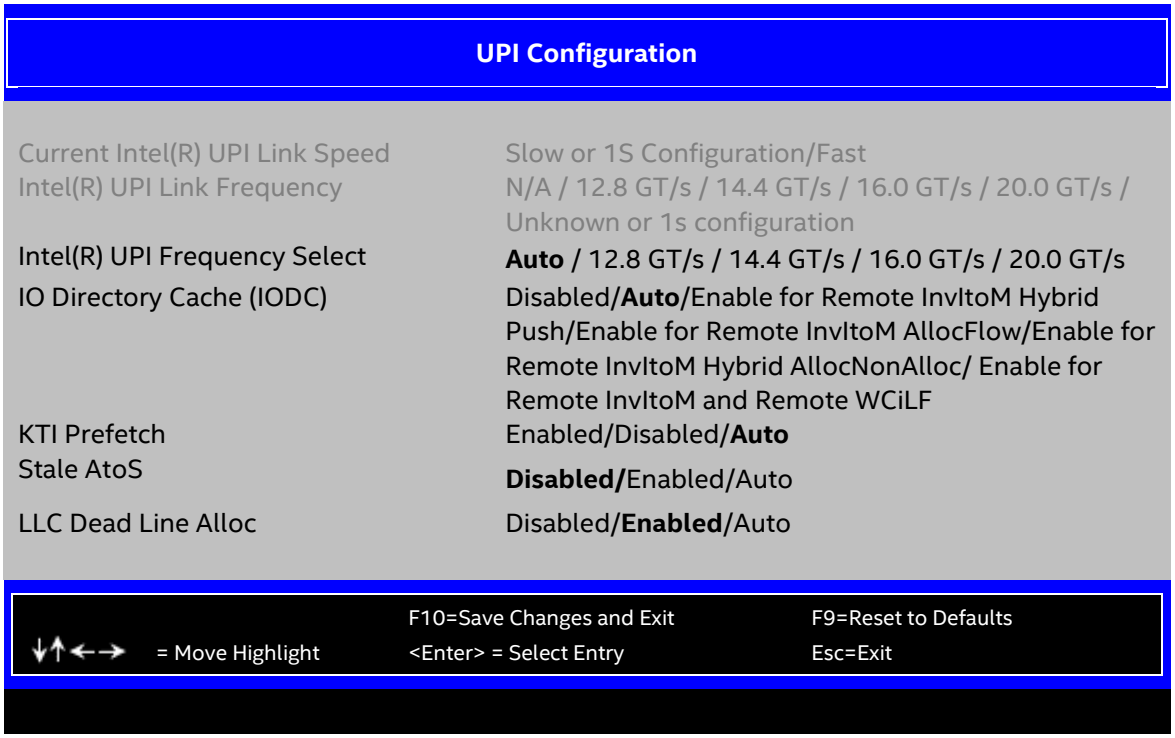

Figure 12. UPI Configuration Screen

1. **Current Intel(R) UPI Link Speed**

   Value: Slow or 1S Configuration/Fast

   Help text: None.

   Comments: *Information only*. Displays the current link speed setting for the Intel UPI links. This setting appears on multi-socket boards only.

   Intel UPI link speed should display as Slow only when running at the boot speed of 2.5 GT/s or when a multi-socket board has only one processor installed so Intel UPI is not functional. It should always display Fast when the Intel UPI link frequency is in the normal functional range of 6.4 GT/s or above.

Back to: UPI Configuration – Advanced – Screen Map

2. **Intel(R) UPI Link Frequency**

   Value: N/A / 12.8 GT/s / 14.4 GT/s / 16.0 GT/s / 20.0 GT/s / Unknown or 1s configuration

   Help text: None.

   Comments: *Information only*. Displays the current frequency at which the Intel UPI links are operating. This setting appears on multi-socket boards only.

   When a multi-socket board has only one processor installed, Intel UPI Link Frequency is shown as N/A.

   Back to: UPI Configuration – Advanced – Screen Map

3. **Intel(R) UPI Frequency Select**

   Value: **Auto** / 12.8 GT/s / 14.4 GT/s / 16.0 GT/s / 20.0 GT/s

   Help text: `Allows for selecting the Intel(R) UltraPath Interconnect Frequency. Recommended to leave in [Auto] so that the BIOS can select the highest common Intel(R) UltraPath Interconnect frequency.`

   Comments: Lowering the Intel UPI frequency may improve performance per watt for some processing loads and on certain benchmarks. Auto gives the maximum Intel UPI performance available. This setting appears on multi-socket boards only.

   When a multi-socket board has only one processor installed, this setting is grayed out with the previous value remaining displayed.

   Changes in Intel UPI link frequency do not take effect until the system reboots, so changes do not immediately affect the Intel UPI Link Frequency display.

   Back to: UPI Configuration – Advanced – Screen Map

4. **IO Directory Cache (IODC)**

   Value: Disabled/**Auto**/Enable for Remote InvItoM Hybrid Push/Enable for Remote InvItoM AllocFlow/Enable for Remote InvItoM Hybrid AllocNonAlloc/ Enable for Remote InvItoM and Remote WCiLF

   Help text: `IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores), Auto - Auto sets to WCiLF.`

   Comments: None.

   Back to: UPI Configuration – Advanced – Screen Map

5. **KTI Prefetch**

   Value: Enabled/Disabled/**Auto**

   Help text: `KTI Prefetch.`

   Comments: This item is suppressed if there is an HBM SPR CPU installed in the system.

6. Back to: UPI Configuration – Advanced – Screen Map**Stale AtoS**

   Value: **Disabled**/Enabled/Auto

   Help text: `Stale A to S Dir optimization.`

Comments: A to S directory optimization. When RdData finds DIR=A and all snoop responses received are RspI, then directory is moved to S, and data is returned in S-state. This optimization is not effective in an xNC configuration where BuriedM is possible.

Back to: UPI Configuration – Advanced – Screen Map

7. **LLC Dead Line Alloc**

Value: Disabled/**Enabled**/Auto

Help text:
```
Enable – opportunistically fill dead lines in LLC.
Disable – never fill dead lines in LLC.
```

Comments: If Downgrade is set on follower, do not fill in LLC regardless of available LLC I-state ways.

Back to: UPI Configuration – Advanced – Screen Map

3.3.4 Memory Configuration

The Memory Configuration screen allows the user to view details about the DDR5 DIMMs that are installed as system memory and alter BIOS memory configuration settings where appropriate.

For the Intel Server Boards M50FCP and D50DNP, this screen shows memory system information, has options to select, and allows the user to select the Configure Memory RAS and Performance screen for further system memory information and configuration.

This screen differs somewhat between different boards that have different memory configurations. Some boards have one processor socket and fewer DIMMs, while other boards have two sockets or four sockets, more DIMMs, and the boards may have RAS and performance options if configured for them.

To access this screen from the front page, select **Advanced** > **Memory Configuration**. Press the **<Esc>** key to return to the **Advanced** screen.

Memory Configuration	
Total DDR5 Memory	<Total physical DDR5 memory installed in system>
High Bandwidth Memory	<Total high bandwidth memory installed in system>
Effective Memory	<Total effective memory>
Current Configuration	<Independent/Full Mirror /Partial Mirror Rank Sparing/ADDDC>
Current Memory Speed	<Operational memory speed in MT/s>
Current HBM Speed	<Operational HBM speed in MT/s>
Memory Operating Speed Selection	**Auto**/3200/3600/4000/4400/4800/5200/5600
Page Policy	**Closed**/ Adaptive
Enforce Population POR	**Disabled** /Enabled
Volatile Memory Mode	**1LM**
HBM Mode	1LM/ **2LM**
Allow Memory Test Correctable Error	**Enabled**/Disabled
HBM Memory Test	Disable HBM Memory Test/**Enable HBM Memory Test**
HBM Adv MemTest PPR	
HBM Adv MemTest Retry After Repair	Disabled /**Enabled**
HBM Adv MemTest Reset Failure Tracking List	Disabled /**Enabled**
HBM PPR Type	**Disabled** Enabled/
MemTest	Hard PPR / **Soft PPR** / PPR Disabled

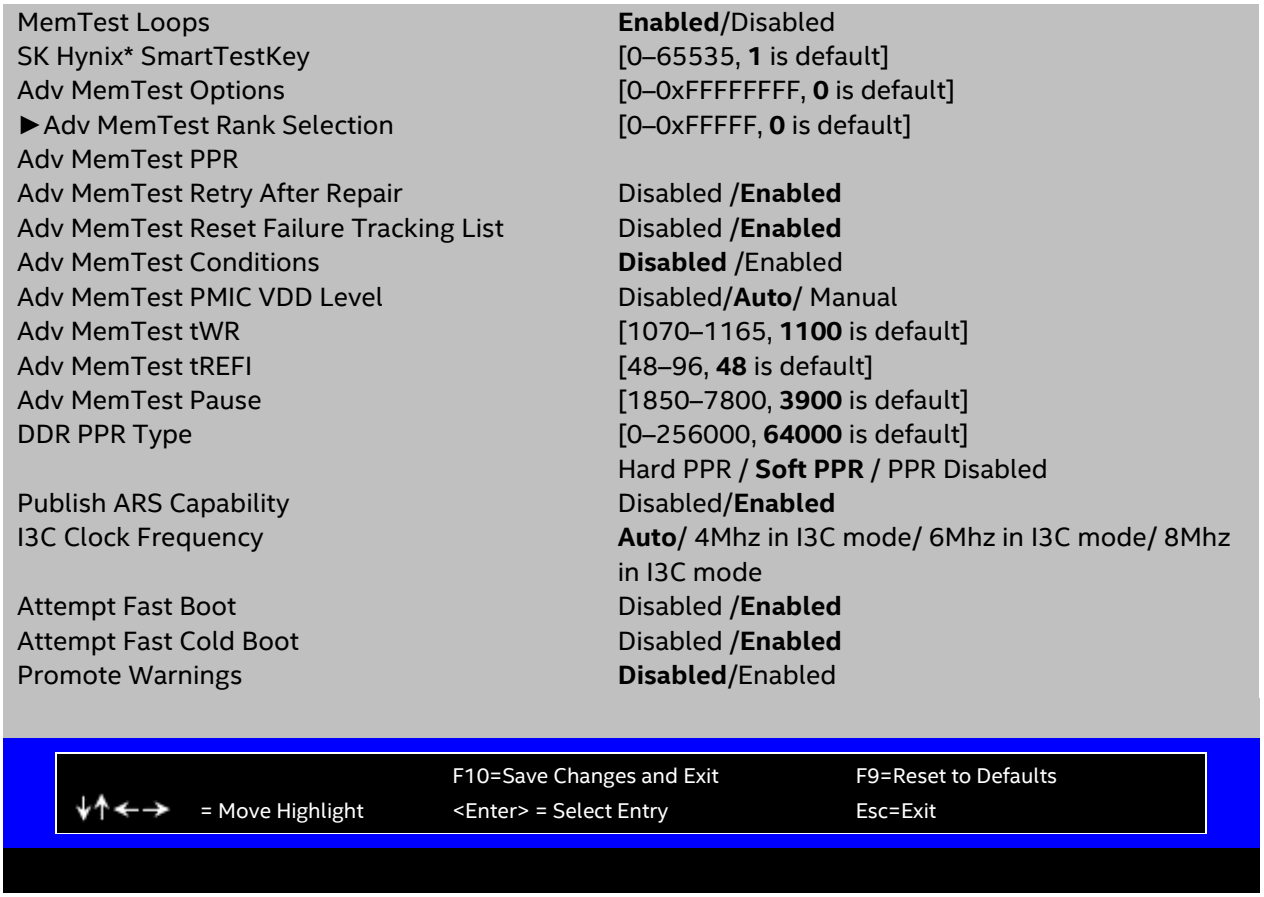

Figure 13. Memory Configuration Screen – Page 1

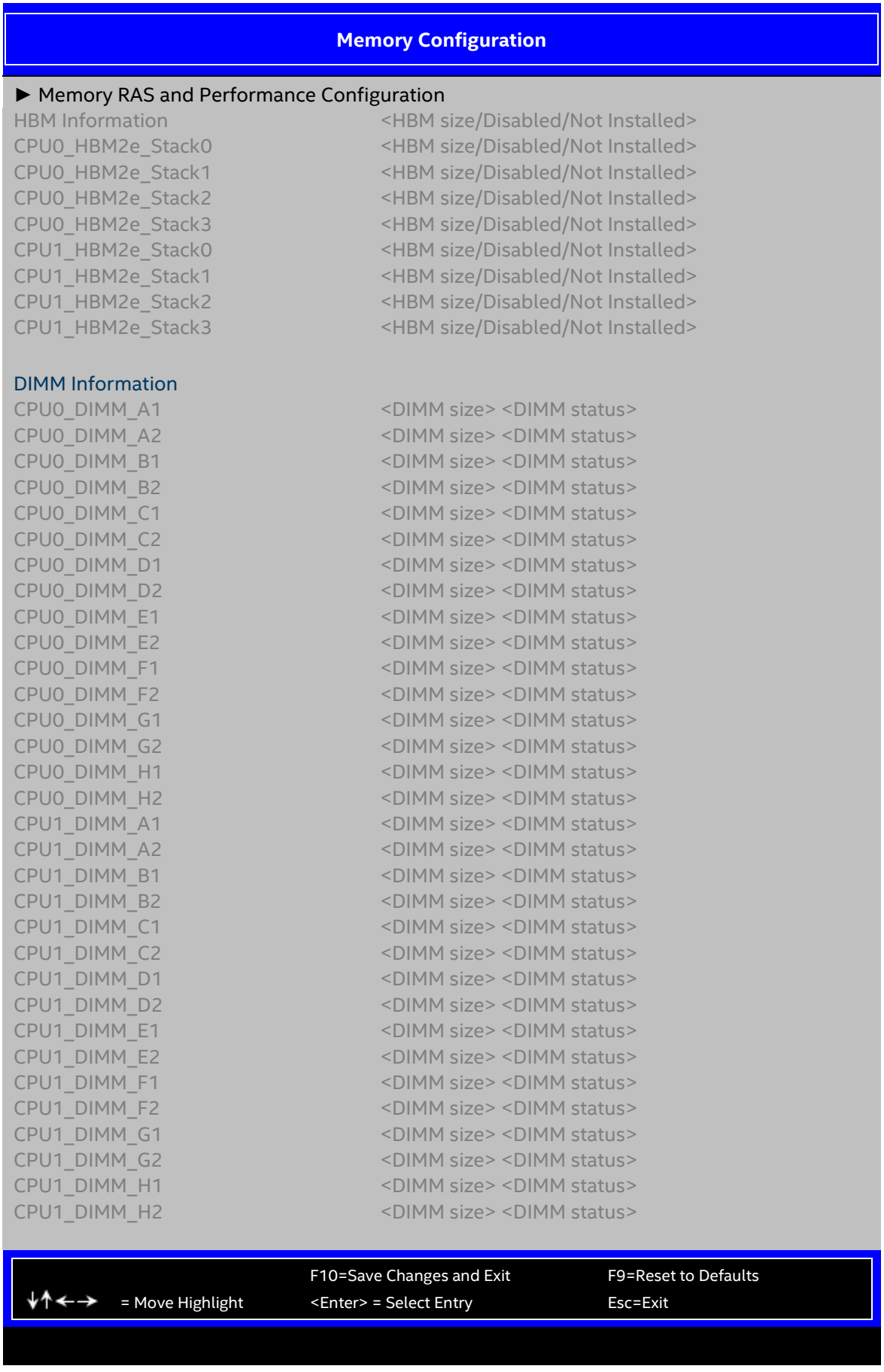

Figure 14. Memory Configuration Screen – Page 2

1. **Total DDR5 Memory**

   Value: <Total physical DDR5 memory installed in the system>

   Help text: None.

   Comments: *Information only*. Displays the amount of memory available in the system in the form of installed DDR5 DIMMs in units of GB. This item does not include and HBM information.

   Back to: Memory Configuration – Advanced – Screen Map

2. **High Bandwidth Memory**

   Value: <Total high bandwidth memory installed in the system>

   Help text: None.

   Comments: *Information only*. Displays the GB amount of high bandwidth memory available in the system in the form of installed HBMs. This item does not include DDR5 information. This item is suppressed if there is no HBM CPU installed in the system.

   Back to: Memory Configuration – Advanced – Screen Map

3. **Effective Memory**

   Value: <Total effective memory>

   Help text: None.

   Comments: *Information only*. Displays the amount of memory available to the operating system in MB or GB. The effective memory is the total physical memory minus the sum of all memory reserved for internal usage, RAS redundancy, and system management RAM (SMRAM).

   Note: Some server operating systems do not display the total physical memory installed.

   For more information on memory sizing, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.4.7 and especially 3.4.7.1.

   Back to: Memory Configuration – Advanced – Screen Map

4. **Current Configuration**

   Value: <**Independent**/Full Mirror/Partial Mirror/Rank Sparing/ADDDC>

   Help text: None.

   Comments: *Information only*. Displays one of the following:

   - Independent – DIMMs are operating in Independent Channel mode, the default configuration when there is no RAS mode configured.
   - Full Mirror – Full Mirroring RAS mode has been configured and is operational.
   - Partial Mirror – Partial Mirroring RAS mode has been configured and is operational.
   - Rank Sparing – Rank Sparing RAS mode has been configured and is operational.
   - ADDDC–ADDDC mode enabled.

   Back to: Memory Configuration – Advanced – Screen Map

5. **Current Memory Speed**

   Value: <Operational memory speed in MT/s>

   Help text: None.

Comments: *Information only*. Displays the speed in MT/s at which the memory is running.

The supported memory speeds are 3200 MT/s, 3600 MT/s, 4000 MT/s, 4400 MT/s, 4800 MT/s, 5200 MT/s, and 5600 MT/s. The actual memory speed capability depends on the memory configuration.

Back to: Memory Configuration – Advanced – Screen Map

6. **Current HBM Speed**

Value: <Operational HBM speed in MT/s>

Help text: None.

Comments: *Information only*. Displays the speed in MT/s at which the HBM is running. The HBM speed should be 3200 MT/s on server platforms based on the 4th Gen Intel Xeon Scalable processors family. This item is suppressed if there is no HBM CPU installed in the system.

Back to: Memory Configuration – Advanced – Screen Map

7. **Memory Operating Speed Selection**

Value: **Auto**/3200/3600/4000/4400/4800/5200/5600

Help text: Force specific Memory Operating Speed or use Auto setting.

Comments: Allows the user to select a specific speed at which memory operates. Only speeds that are legitimate are available; that is, the user can only specify speeds less than or equal to the auto-selected memory operating speed. The default Auto setting selects the highest achievable memory operating speed consistent with the installed DIMMs and processors. The knob cannot change the HBM speed.

Back to: Memory Configuration – Advanced – Screen Map

8. **Page Policy**

Value: **Closed**/Adaptive

Help text: `Select Page Policy.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

9. **Enforce Population POR**

Value: **Disabled**/Enabled

Help text: Enable Memory Population POR Enforcement.

Comments: When Disabled is selected, UEFI firmware shall completely bypass this feature and proceed to memory decode without any additional population restrictions. When Enabled is selected, UEFI firmware shall compare the current DIMM population against all configurations in the provided POR worksheet. Also error code record as memory population error shows in setup error manager and logs to system event log (BMC SEL).

When memory population enforcement selected, it needs to follow POR worksheet to install DIMMs. Otherwise, memory reference code degrades the memory population to align with an established POR that must occur before the memory decode flow. This is needed to ensure non-POR DIMMs are never identified by the current flow for addition to the memory map.

Back to: Memory Configuration – Advanced – Screen Map

10. Volatile Memory Mode

Value: **1LM**

Help text: `Selects 1LM mode for volatile memory.`

Comments: The Volatile Memory Mode knob has only one options, 1LM.

This item is not visible when it's HBM CPU.

Back to: Memory Configuration – Advanced – Screen Map

11. HBM Mode

Value: 1LM/**2LM**

Help text: `Selects 1LM or 2LM mode for HBM. For 2LM memory mode, BIOS will try to configure 2LM but if BIOS is unable to configure 2LM, HBM mode will fall back to 1LM.`

Comments: The HBM Mode knob has two options, 1LM and 2LM. For HBM CPU, MRC uses this knob to decide whether configuring the HBM as the cache of DDR5 DIMM. The HBM is configured as the cache of DDR5 DIMM when this knob is set to 2LM. The HBM and DDR5 DIMM are configured as the system memory when this knob is set to 1LM.

Aligning with RP BIOS, PC BIOS keeps the default value of this knob as 2LM.

This item is not visible when the CPU is not HBM CPU or NUMA Optimized is disabled.

Back to: Memory Configuration – Advanced – Screen Map

12. Allow Memory Test Correctable Error

Value: **Enabled**/Disabled

Help text: `Enable - Logs error and allows correctable errors during memory test(DIMM Rank not removed). Disable - Logs error and removes DIMM Rank.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

13. HBM Memory Test

Value: Disable HBM Memory Test/**Enable HBM Memory Test**

Help text: `Enable / Disable Hbm Memory Test`

Comments: Only HBM CPU supports HBM Memory Test; otherwise, this item is hidden.

Back to: Memory Configuration – Advanced – Screen Map

14. HBM Adv MemTest PPR

Value: **Enabled**/Disabled

Help text: `This option enable/disable ppr flow for HBM MemTest`

Comments: Only HBM CPU supports HBM Memory Test; otherwise, this item is hidden.

Back to: Memory Configuration – Advanced – Screen Map

15. HBM Adv MemTest Retry After Repair

Value: **Enabled**/Disabled

Help text: `Enable/disable Retry of the current Adv MemTest step after a PPR repair is done.`

Comments: Only HBM CPU supports HBM Memory Test; otherwise, this item is hidden.

Back to: Memory Configuration – Advanced – Screen Map

16. HBM Adv MemTest Reset Failure Tracking List

Value: Enabled/**Disabled**

Help text: `Enable/disable Reset of the Row Failure Tracking List after each Adv MemTest option. Useful for testing performance of multiple options.`

Comments: Only HBM CPU supports HBM Memory Test; otherwise, this item is hidden.

Back to: Memory Configuration – Advanced – Screen Map

17. HBM PPR Type

Value: Hard PPR / **Soft PPR** / PPR Disabled

Help text: `Selects HBM Post Package Repair Type - Hard / Soft / Disabled. Current default is Disabled.`

Comments: Only HBM CPU supports HBM Memory Test; otherwise, this item is hidden.

Back to: Memory Configuration – Advanced – Screen Map

18. MemTest

Value: Disabled/**Enabled**

Help text: `Enable - Enables memory test during normal boot. Disable - Disables this feature.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

19. MemTest Loops

Value: [Entry Field 0–65535, **1** is default]

Help text: `Number of memory test loops during normal boot, set to 0 to run memtest infinitely.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

20. SK Hynix* SmartTestKey

Value: [Entry Field 0-0xFFFFFFFF, **0** is default]

Help text: `SmartTest Key Value`

Comments: This item only works for SK Hynix* DIMM. A SmartTest* that refers to SK Hynix DDR5 AMT algorithms is executed with vendor mode if the confidential key value is valid. Otherwise, it is executed with normal mode. PPR resources are different under vendor mode and normal mode.

Back to: Memory Configuration – Advanced – Screen Map

21. Adv MemTest Options

Value: [Entry Field 0-0xFFFFF, **0** is default]

Help text: `This option is a bit mask[19:0]: All 0 = disabled: bit-0=XMATS8, bit-1=XMATS16, bit-2=Reserved, bit-3=Reserved, bit-4=WCMATS8, bit-5=WCMCH8, bit-6=Reserved, bit-7=MARCHCM64, bit-8=Reserved, bit-9=Reserved, bit-10=Reserved, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3, bit-16=SK-HYNIX, bit-17=SAMSUNG, bit-18=MICRON-RMW, bit-19=SCRAM_X2.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

22. Adv MemTest Rank Selection

Value: None.

Help text: `Indicate which Ranks will be tested by AdvMemTest.`

Comments: *Selection only*. For more information on Adv MemTest Rank Selection settings, see Section 3.3.4.2.

Back to: Memory Configuration – Advanced – Screen Map

23. Adv MemTest PPR

Value: Disabled/**Enabled**

Help text: `This option enable/disable PPR flow for MemTest.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

24. Adv MemTest Retry After Repair

Value: Disabled/**Enabled**

Help text: `Enable/Disable retry of the current Adv MemTest step after a PPR repair is done.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

25. Adv MemTest Reset Failure Tracking List

Value: **Disabled**/Enabled

Help text: `Enable/Disable reset of the Row Failure Tracking List after each Adv MemTest option. Useful for testing performance of multiple options.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

26. Adv MemTest Conditions

Value: Disabled/**Auto**/ Manual

Help text: `Auto = set test conditions based on test type; Manual = specify global test conditions; Disable = Do not apply test conditions.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

27. Adv MemTest PMIC VDD Level

Value: [Entry Field 1070–1165, **1100** is default]

Help text: `Specify PMIC VDD and VDDQ level in units of mV.`

Comments: The option is shown when the Adv MemTest Conditions item is set to manual.

Back to: Memory Configuration – Advanced – Screen Map

28. Adv MemTest tWR

Value: [Entry Field 48–96, **48** is default]

Help text: `Specify tWR timing between 48 to 96 in units of tCK.`

Comments: The option is shown when the Adv MemTest Conditions item is set to manual.

Back to: Memory Configuration – Advanced – Screen Map

29. Adv MemTest tREFI

Value: [Entry Field 1850–7800, **3900** is default]

Help text: `Specify tREFI (refresh rate) timing between 1850 to 7800 in nsec.`

Comments: The option is shown when the Adv MemTest Conditions item is set to manual.

Back to: Memory Configuration – Advanced – Screen Map

30. Adv MemTest Pause

Value: [Entry Field 0–256000, **64000** is default]

Help text: `Specify a pause delay between 0 to 256000 in units of usec. This is a time period where refresh is disabled between write and read sequences.`

Comments: The option is shown when the Adv MemTest Conditions item is set to manual.

Back to: Memory Configuration – Advanced – Screen Map

31. DDR PPR Type

Value: Hard PPR / **Soft PPR** / PPR Disabled

Help text: `Selects DDR Post Package Repair Type - Hard / Soft / Disabled. Current default is Soft PPR.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

32. Publish ARS Capability

Value: Disabled/**Enabled**

Help text: `Enable\Disable publishing of the Address Range Scrub capability to the OS`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

33. I3C Clock Frequency

Value: **Auto**/ 4Mhz in I3C mode/ 6Mhz in I3C mode/ 8Mhz in I3C mode

Help text: `Sets DDR5 I3C Clock Frequencies For SPD Access.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

34. Attempt Fast Boot

Value: Disabled/**Enabled**

Help text: `Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

35. Attempt Fast Cold Boot

Value: Disabled/**Enabled**

Help text: `Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature.`

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

36. Promote Warnings

Value: **Disabled**/Enabled

Help text: Determines if warnings are promoted to system level

Comments: None.

Back to: Memory Configuration – Advanced – Screen Map

37. Memory RAS and Performance Configuration

Value: None.

Help text: `Configure memory RAS (Reliability, Availability, and Serviceability) and view current memory performance information and settings.`

Comments: *Selection only*. For more information on Memory RAS and Performance Configuration settings, see Section 3.3.4.2.

Back to: Memory Configuration – Advanced – Screen Map

38. HBM Information

CPU0_HBM2e_Stack0, CPU0_HBM2e_Stack1, CPU0_HBM2e_Stack2, CPU0_HBM2e_Stack3, CPU1_HBM2e_Stack0, CPU1_HBM2e_Stack1, CPU1_HBM2e_Stack2, CPU1_HBM2e_Stack3

Value: <HBM size/Disabled/Not Installed>

Help text: None.

Comments: *Information only*. Displays the status of each HBM controller present on the board. There is one line for each HBM controller.

One HBM CPU has 4 HBM controllers and the HBM size of each HBM controller is 16GB. If HBM training failed, the MRC downgrades 4 controllers to 0 controller. For example, if any controller training fails, MRC disables all HBM controllers and the system attempts to boot on DDR5 only mode. Then, if no DDR5 DIMM is present, the system boot fails.

- **16 GB** – This memory controller can work well and its size is 16 GB.
- **Disabled** – This memory controller is disabled due to training failed.
- **Not Installed** – For a two-sockets platform, if the user only installs one HBM CPU on the platform, the `CPU1_HBM2e_Stackx` is shown as Not Installed.

This information is suppressed if there is no HBM CPU installed in the system.

Back to: Memory Configuration – Advanced – Screen Map

39. DIMM Information

CPU0_DIMM_A1, CPU0_DIMM_A2, CPU0_DIMM_B1, CPU0_DIMM_B2 ... (DIMM_C1 through DIMM_H1), CPU1_DIMM_H2 ... (DIMM_J1 through DIMM_T2), CPU1_DIMM_A1 ... CPU1_DIMM_H2

Value: <DIMM size><DIMM status>

Help text: None.

Comments: *Information only*. Displays the status of each DIMM socket present on the board. There is one line for each DIMM socket.

For each DIMM socket, the DIMM status reflects one of the following five possible states:

- **Installed & Mapped out** – A DDR5 DIMM is installed and mapped out in this slot.
- **Installed & Operational** – A DDR5 DIMM is installed and operational in this slot.
- **Not Installed** – No DDR5 DIMM is installed in this slot.
- **Installed & Failed** – The DIMM installed in this slot has failed during initialization and/or was disabled during initialization.
- **Installed & Disabled** – A DDR5 DIMM is installed and disabled in this slot.

For each DIMM that is in the Installed & Operational state, the DIMM size in GB of that DIMM is displayed. This is the physical size of the DIMM, regardless of how it is counted in the effective memory size.

Notes:

- For DIMM_XY, X denotes the channel identifier A-H; and Y denotes the DIMM slop identifier 1–2 within the channel. For example, DIMM_A2 is the DIMM socket on channel A, slot 2. Not all boards have the same number of channels and slots; this is dependent on the board features.

The Intel Server Boards M50FCP and D50DNP can have DIMMs A1 and A2 to H1 and H2 (maximum two CPUs, eight channels, two DPC). Each project may have a different DIMM slot topology; this document just gives a general design. Adjust per the DIMM schematic to tune.

For details about different board configurations, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.4.3.4 and 11.

Back to: Memory Configuration – Advanced – Screen Map

3.3.4.1 Adv MemTest Rank Selection

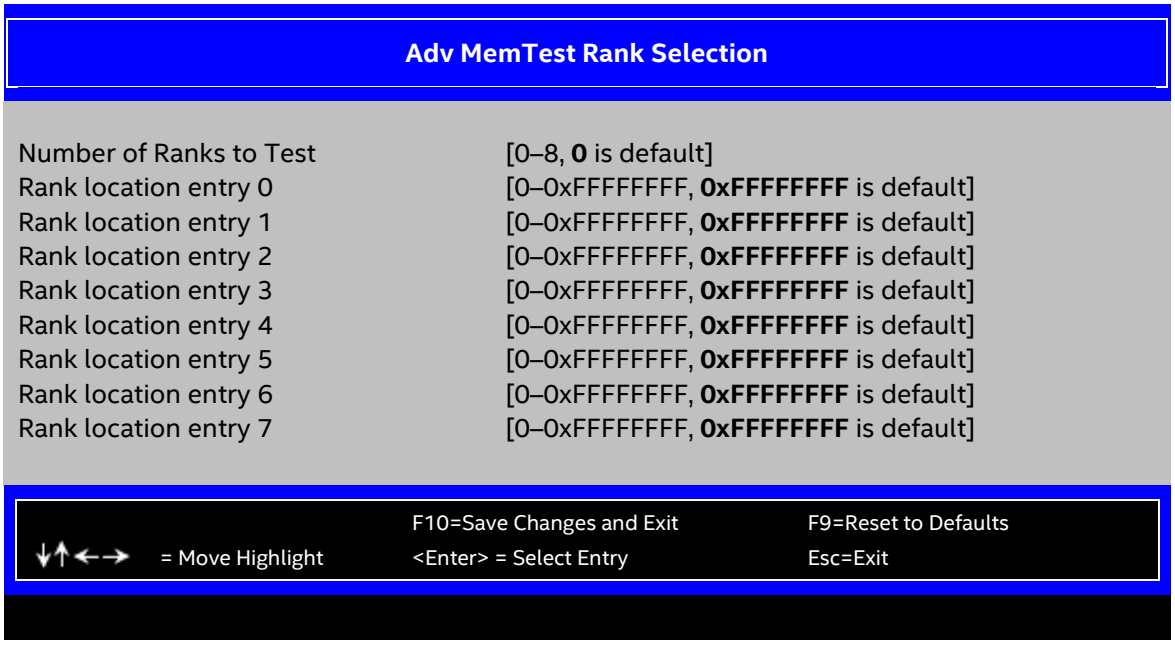

Figure 15. Adv MemTest Rank Selection Screen

1. **Number of Ranks to Test**

   Value: [Entry Field 0–8, **0** is default]

   Help text: `Select how many Ranks will be tested by AdvMemTest. Maximum of 8 Ranks are allowed. Default value of 0 will test all present Ranks in the system.`

   Comments: None.

   Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

2. **Rank location entry 0**

   Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

   Help text: `Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.`

   Comments: The option is shown when Number of Ranks to Test item is set to greater than 0.

   Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

3. **Rank location entry 1**

   Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

   Help text: `Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16]`

and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

Comments: The option is shown when Number of Ranks to Test item is set to greater than 1.

Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

4. **Rank location entry 2**

Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

Comments: The option is shown when Number of Ranks to Test item is set to greater than 2.

Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

5. **Rank location entry 3**

Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

Comments: The option is shown when Number of Ranks to Test item is set to greater than 3.

Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

6. **Rank location entry 4**

Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

Comments: The option is shown when Number of Ranks to Test item is set to greater than 4.

Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

7. **Rank location entry 5**

   Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

   Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in `bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.`

   Comments: The option is shown when Number of Ranks to Test item is set to greater than 5.

   Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

8. **Rank location entry 6**

   Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

   Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

   Comments: The option is shown when Number of Ranks to Test item is set to greater than 6.

   Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

9. **Rank location entry 7**

   Value: [Entry Field 0–0xFFFFFFFF, **0xFFFFFFFF** is default]

   Help text: Specify the Rank location using this format: Rank number in bits[3:0]; DIMM number in bits[7:4]; Channel number in the MC in bits[11:8]; MC number in bits[15:12]; Socket number in bits [19:16] and bits [31:20] are reserved. For example to test MC 0, CH 1, DIMM 0, RANK 0 on Socket 0, you need to enter a value of 0x100.

   Comments: The option is shown when the Number of Ranks to Test item is set to greater than 7.

   Back to: Adv MemTest Rank Selection – Memory Configuration – Advanced – Screen Map

3.3.4.2 Memory RAS and Performance Configuration

The Memory RAS and Performance Configuration screen allows the user to customize several memory configuration options.

To access this screen from the front page, select **Advanced** > **Memory Configuration** > **Memory RAS and Performance Configuration**. Press the **<Esc>** key to return to the Memory Configuration screen.

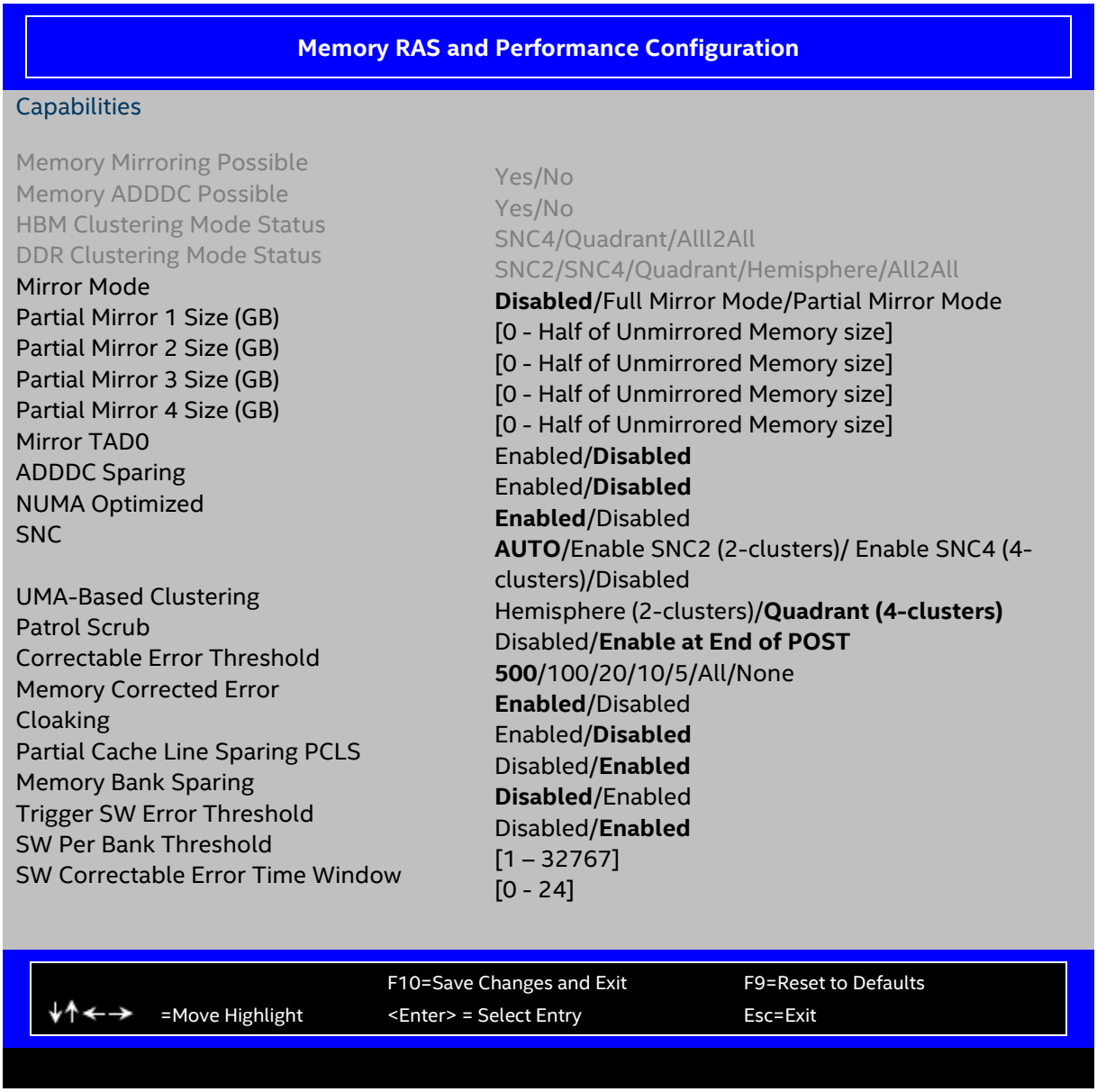

Figure 16. Memory RAS and Performance Configuration Screen

1. **Memory Mirroring Possible**

   Value: Yes/No

   Help text: None.

   Comments: *Information only.* Displays whether the current DIMM configuration supports memory mirroring. For memory mirroring to be possible, DIMM configurations on all paired channels must be identical between the channel pair (Mirroring Domain). For details about mirroring configurations, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.4.3 and 3.4.4.

   Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

2. **Memory ADDDC Possible**

   Value: Yes/No

   Help text: None.

Comments: *Information only.* Displays whether the current DIMM configuration supports Adaptive Double Device Data Correction (ADDDC).

Note: There might be some silicon workarounds that block enabling ADDDC function when this setting displays Yes.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

3. **HBM Clustering Mode Status**

   Value: SNC4/Quadrant/All2All

   Help text: `HBM Clustering Mode Status.`

   Comments: *Information only*. It displays the current HBM clustering mode only when HBM CPU is installed; otherwise, this item is hidden.

   Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

4. **DDR Clustering Mode Status**

   Value: SNC2/SNC4/Quadrant/Hemisphere/All2All

   Help text: `DDR Clustering Mode Status.`

   Comments: *Information only*. It displays the current DDR clustering mode if there is DDR memory available; otherwise, this item is hidden.

   Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

5. **Mirror Mode**

   Value: **Disabled**/Full Mirror Mode/Partial Mirror Mode

   Help text: `Full Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect.`

   Comments: This setting is shown when the current CPU supports mirror mode, the DIMM population meets mirror requirements, and no spare or lockstep is enabled. This knob is suppressed when the ADDDC is enabled. The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

   The error message “Error: Disable Mirror TAD0 to enable Full Mirror Mode 1LM/2LM. Press ENTER to continue” pops up if the user attempts to configure this knob to Full Mirror Mode meanwhile the Mirror TAD0 is enabled.

   Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

6. **Partial Mirror 1 Size (GB)**

   Value: 0 - Half of Unmirrored Memory size

   Help text: `Select multiplier of 1 GB for the size of the SAD to be created.`

Comments: This setting is shown when the user configures the Mirror Mode as Partial Mirror Mode.

This knob is suppressed when the ADDDC is enabled.

This setting is suppressed when the user enables the MirrorMemoryBelow4GB item or MirrorPercentageAbove4GB item with the `efibootmgr` command in Linux* operating system.

The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

7. **Partial Mirror 2 Size (GB)**

Value: 0 - Half of Unmirrored Memory size

Help text: `Select multiplier of 1 GB for the size of the SAD to be created.`

Comments: This setting is shown when the user configures the Mirror Mode as Partial Mirror Mode.

This knob is suppressed when the ADDDC is enabled.

This setting is suppressed when user enables the MirrorMemoryBelow4GB item or MirrorPercentageAbove4GB item with the `efibootmgr` command in Linux operating system.

This setting is suppressed when the value of Partial Mirror 1 Size (GB) item is 0.

The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

8. **Partial Mirror 3 Size (GB)**

Value: 0 - Half of Unmirrored Memory size

Help text: `Select multiplier of 1 GB for the size of the SAD to be created.`

Comments: This setting is shown when the user configures the Mirror Mode as Partial Mirror Mode.

This knob is suppressed when the ADDDC is enabled.

This setting is suppressed when the user enables the MirrorMemoryBelow4GB item or MirrorPercentageAbove4GB item with the `efibootmgr` command in Linux operating system.

This setting is suppressed when the value of Partial Mirror 2 Size (GB) item is 0.

The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

9. Partial Mirror 4 Size (GB)

Value: 0 - Half of Unmirrored Memory size

Help text: `Select multiplier of 1 GB for the size of the SAD to be created.`

Comments: This setting is shown when the user configures the Mirror Mode as Partial Mirror Mode.

This knob is suppressed when the ADDDC is enabled.

This setting is suppressed when user enables the MirrorMemoryBelow4GB item or MirrorPercentageAbove4GB item with the `efibootmgr` command in Linux operating system.

This setting is suppressed when the value of Partial Mirror 3 Size (GB) item is 0.

The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

10. Mirror TAD0

Value: Enabled/**Disabled**

Help text: `Enable Mirror on entire memory for TAD0.`

Comments: This setting is grayed out if the user configures the Mirror Mode as Full Mirror Mode.

This knob is suppressed when the ADDDC is enabled.

This setting is suppressed when the user enables the MirrorMemoryBelow4GB item or MirrorPercentageAbove4GB item with the `efibootmgr` command in Linux operating system.

The knob is suppressed when the user only installs HBM CPU on the system and does not install DDR5 on the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

11. ADDDC Sparing

Value: Enabled/**Disabled**

Help text: `Enable/Disable Adaptive Double Device Data Correction Sparing.`

Comments: This setting is hidden if x8 data width DIMMs are installed or if mirror mode or memory sparing are not disabled. This setting is gray out when Intel SGX enabled.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

12. NUMA Optimized

Value: **Enabled**/Disabled

Help text: `If enabled, BIOS includes ACPI tables that are required for NUMA-aware Operating Systems.`

Comments: This option is hidden for boards that have only one socket installed or HBM CPU installed.

When enabled, the SRAT and SLIT ACPI tables are provided that show the locality of systems resources, especially memory, which allows a NUMA-aware operating system to optimize which processor threads are used by processes that can benefit by having the best access to those resources. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.4.3.6.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

13. SNC

Value: **AUTO**/Enable SNC2 (2-clusters)/Enable SNC4 (4-clusters)/Disabled

Help text: `Disable supports 1-cluster and 4-IMC way interleave. Enable SNC2 supports 2-clusters SNC and 2-way IMC interleave. Enable SNC4 supports 4-cluster and 1-IMC way interleave.`

Comments: This feature is similar to COD on previous generations. It produces more NUMA objects under ACPI. The major difference is that SNC LLC is unified and COD LLC is separated. SNC (Sub NUMA) enables the two-cluster SNC; two-way interleave of IMC interleaving focuses to 1-cluster.

If DIMMs are installed on both MCs, enable the SNC and set one-way interleave. It enables SNC2 (two clusters). The option Enable SNC2 (2-clusters) is suppressed if the user installs HBM CPU. The option Enable SNC4 (4-clusters) is only available on SPR XCC.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

14. UMA-Based Clustering

Value: Hemisphere (2-clusters)/**Quadrant (4-clusters)**

Help text: `UMA Based Clustering options include Hemisphere (2-clusters) and Quadrant (4-clusters). These options are only available on XCC and only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS.`

Comments: The knob is only available on SPR XCC.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

15. Patrol Scrub

Value: Disabled/**Enable at End of POST**

Help text: `Enable/Disable Patrol Scrub`

Comments: When enabled, Patrol Scrub is initialized to read through all of memory in a 24-hour period, correcting any correctable error correction code (ECC) errors it encounters by writing back the corrected data to memory.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

16. Correctable Error Threshold

Value: **500**/100/20/10/5/All/None

Help text: `Threshold value for logging Correctable Errors(CE) - Threshold of 500(default) logs 500th CE,"All" logs every CE, and "None" means no CE logging. All and None are not valid with Rank Sparing. Only support DDR5.`

Comments: Specifies how many correctable errors (CEs) must occur before triggering the logging of a system event log (SEL) CE event. Only the first threshold crossing is logged, unless the All or None options are selected. The All option causes every CE that occurs to be logged. The None option suppresses CE logging completely.

The All and None options only apply to the independent mode.

This threshold is applied on a per-rank basis. CE occurrences are counted for each memory rank. If ADDDC mode is enabled, every threshold crossing is logged until this rank ECC becomes +1 mode (ADDDC exhausted). This is also the CE threshold used when Rank Sparing RAS mode is configured. When a CE threshold crossing occurs in Rank Sparing mode on a channel that is in the redundant state, it causes a Sparing Fail Over (SFO) event to occur. That threshold crossing is also logged as a CE event if it is the first to occur in the system.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

17. Memory Corrected Error

Value: **Enabled**/Disabled

Help text: `Enable/Disable Memory Corrected Error.`

Comments: None.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

18. Cloaking

Value: Enabled/**Disabled**

Help text: `If disabled, CMCI event appears when CE happens. If enabled, CMCI event is blocked when CE happens.`

Comments: None.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

19. Partial Cache Line Sparing PCLS

Value: Disabled/**Enabled**

Help text: `Enable/Disable PCLS Sparing`

Comments: Only HBM CPU supports PCLS; otherwise, this item is hidden.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

20. Memory Bank Sparing

Value: **Disabled**/Enabled

Help text: `Enable/Disable Memory Bank Sparing. This feature is only available for HBM. The correctable errors threshold is 0x7FFF.`

Comments: Only HBM CPU supports Memory Bank Sparing; otherwise, this item is hidden.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

21. Trigger SW Error Threshold

Value: Disabled/**Enabled**

Help text: `Enable or Disable Sparing trigger SW Error Match Threshold. Only support DDR5.`

Comments: None.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

22. SW Per Bank Threshold

Value: [1 – 32767, **3 is default**]

Help text: `SW Per Bank Correctable Error Threshold (1 - 32767) used for bank level error. Only support DDR5.`

Comments: None.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

23. SW Correctable Error Time Window

Value: [0 – 24, **24 is default**]

Help text: `Sw Correctable Error time window based interface in Hour (0 - 24). Only support DDR5.`

Comments: None.

Back to: Memory RAS and Performance Configuration – Memory Configuration – Advanced – Screen Map

3.3.5 System Event Log

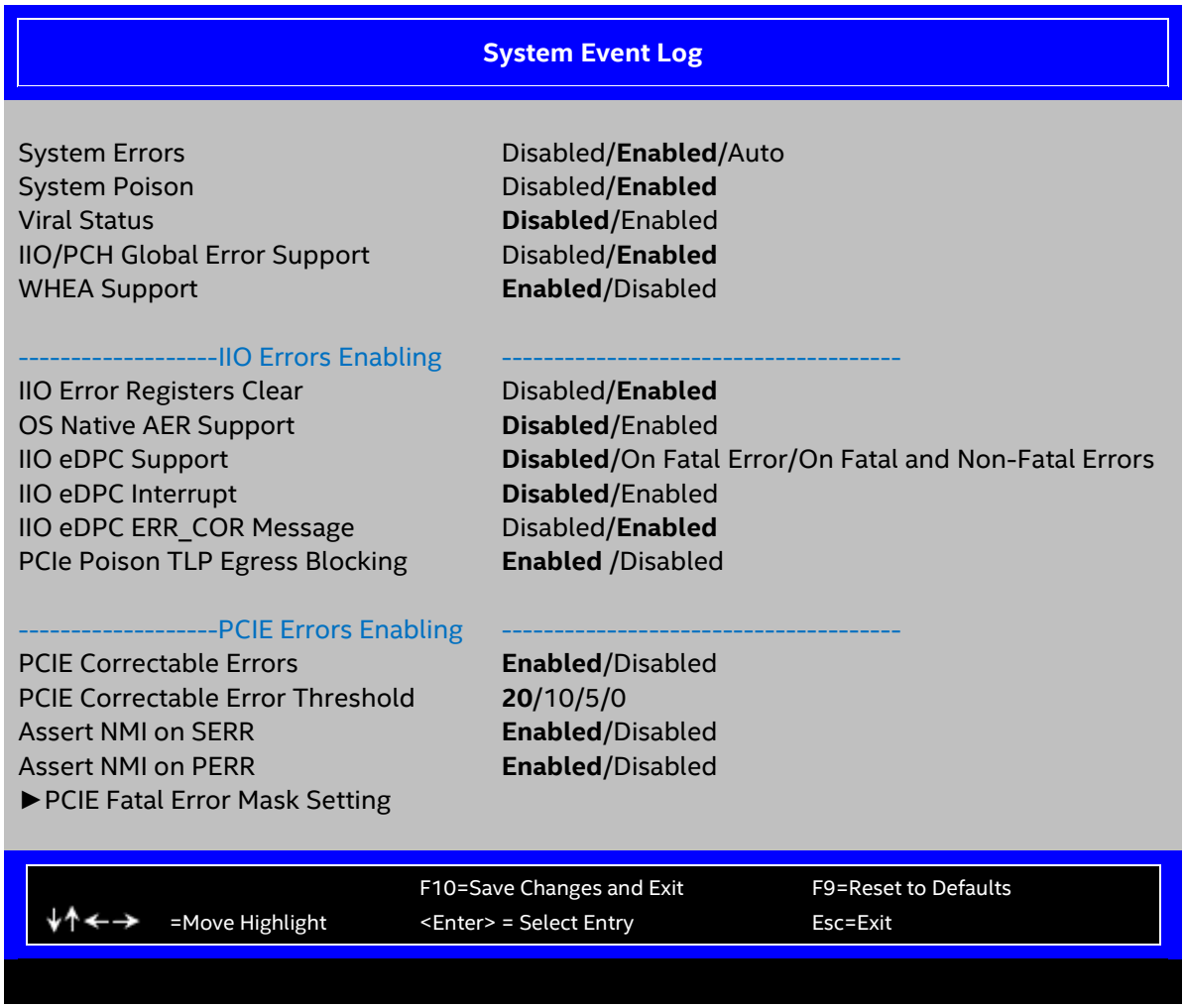

Figure 17. System Event Log Screen

1. **System Errors**

   Value: Disabled/**Enabled**/Auto

   Help text: `System Error Enable/Disable setup options.`

   Comments: If system errors are disabled or auto, no other error items are shown in setup.

   Back to: System Event Log – Advanced – Screen Map

2. **System Poison**

   Value: Disabled/**Enabled**

   Help text: `Enable/Disable System Poison.`

   Comments: If Intel SGX is enabled, the item is grayed out.

   Back to: System Event Log – Advanced – Screen Map

3. **Viral Status**

   Value: **Disabled**/Enabled

   Help text: Enable/Disable Viral.

Comments: It is grayed out when system errors disabled or Auto.

Back to: System Event Log – Advanced – Screen Map

4. **IIO/PCH Global Error Support**

   Value: Disabled/**Enabled**

   Help text: `Enable/Disable IIO/PCH Error Support.`

   Comments: None.

   Back to: System Event Log – Advanced – Screen Map

5. **WHEA Support**

   Value: **Enabled**/Disabled

   Help text: `[Enabled] - WHEA (Windows Hardware Error Architecture) is enabled.`
   `[Disabled] - WHEA is disabled.`

   Comments: None.

   Back to: System Event Log – Advanced – Screen Map

6. **IIO Error Registers Clear**

   Value: Disabled/**Enabled**

   Help text: `Enable/Disable Clear IIO Error Registers`

   Comments: This item is hidden if IIO/PCH Global Error Support is disabled.

   Back to: System Event Log – Advanced – Screen Map

7. **OS Native AER Support**

   Value: **Disabled**/Enabled

   Help text: `Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.`

   Comments: This item is hidden if IIO/PCH Global Error Support is disabled.

   Back to: System Event Log – Advanced – Screen Map

8. **IIO eDPC Support**

   Value: **Disabled** /On Fatal Error/ On Fatal and Non-Fatal Errors

   Help text: `Enable/Disable IIO eDPC Support`

   Comments: This item is hidden if IIO/PCH Global Error Support is disabled. It is grayed out when the system errors are set as Disabled or Auto.

   Back to: System Event Log – Advanced – Screen Map

9. **IIO eDPC Interrupt**

   Value: **Disabled**/Enabled

   Help text: `Enable/Disable IIO eDPC Interrupt`

   Comments: This item is hidden if IIO/PCH Global Error Support or IIO eDPC Support is disabled.

   Back to: System Event Log – Advanced – Screen Map

10. **IIO eDPC ERR_COR Message**

    Value: Disabled/**Enabled**

    Help text: `Enable/Disable IIO eDPC ERR_COR Message`

    Comments: This item is hidden if IIO/PCH Global Error Support or IIO eDPC Support is disabled.

    Back to: System Event Log – Advanced – Screen Map

11. **PCIe Poison TLP Egress Blocking**

    Value: **Enabled**/Disabled

    Help text: `Enable/Disable PCIe Poison TLP Egress Blocking`

    Comments: This item is hidden if IIO eDPC Support is disabled.

    Back to: System Event Log – Advanced – Screen Map

12. **PCIE Correctable Errors**

    Value: **Enabled/**Disabled

    Help text: `[Enabled] - Processor & PCH PCIe correctable error logging is enabled.`
    `[Disabled] - Processor & PCH PCIe correctable error logging is disabled.`

    Comments: None.

    Back to: System Event Log – Advanced – Screen Map

13. PCIE Correctable Error Threshold

Value: **20**/10/5/0

Help text: `Threshold value for logging Correctable Errors(CE) - Threshold of 20/10/5 logs 20th/10th/5th CE, "0" logs every CE.`

Comments: None.

Back to: System Event Log – Advanced – Screen Map

14. Assert NMI on SERR

Value: **Enabled**/Disabled

Help text: `On SERR, generate an NMI and log an error.`
`Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be active.`

Comments: None.

Back to: System Event Log – Advanced – Screen Map

15. Assert NMI on PERR

Value: **Enabled**/Disabled

Help text: `On PERR, generate an NMI and log an error.`
`Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.`

Comments: None.

Back to: System Event Log – Advanced – Screen Map

16. PCIE Fatal Error Mask Setting

Value: None.

Help text: None.

Comments: *Selection only*. For more information on PCIE Fatal Error Mask Setting, see Section 3.3.5.1.

Back to: System Event Log – Advanced – Screen Map

3.3.5.1 PCIE Fatal Error Mask Setting

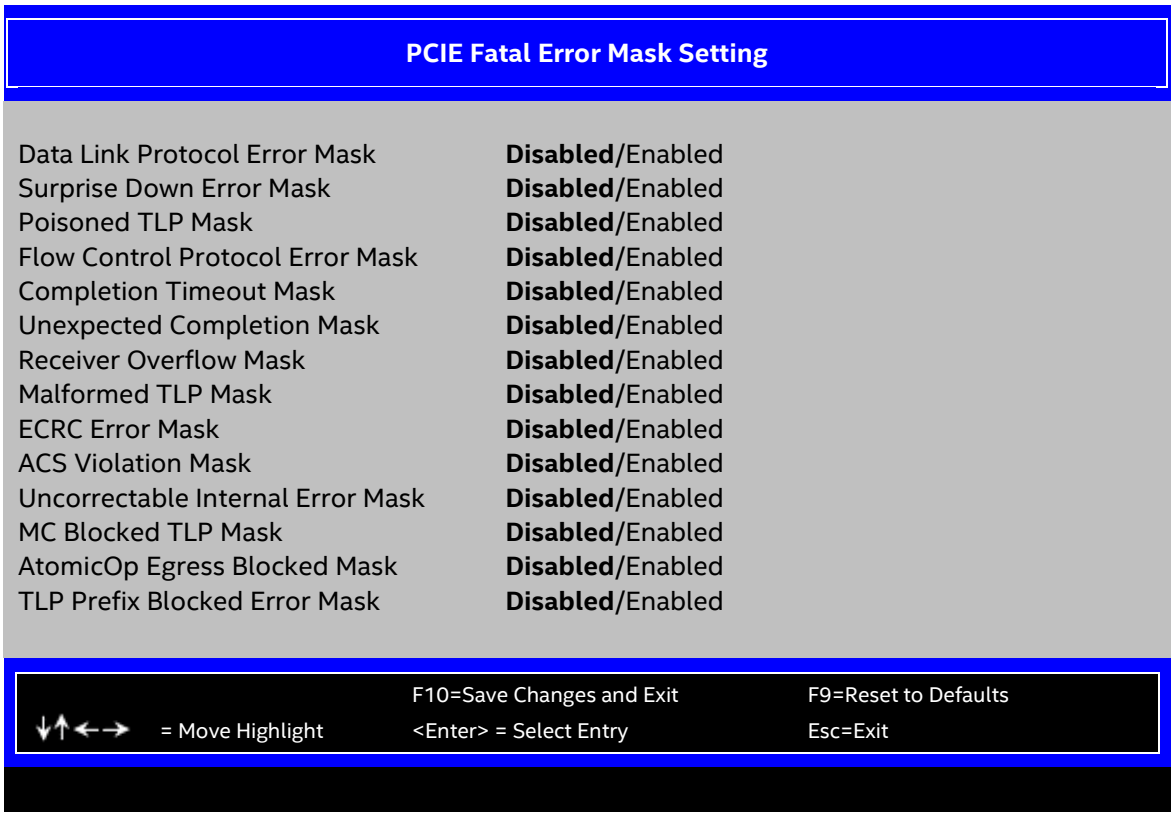

Figure 18. PCIe* Fatal Error Mask Setting Screen

1. **Data Link Protocol Error Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

2. **Surprise Down Error Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

3. **Poisoned TLP Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

4. **Flow Control Protocol Error Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

5. **Completion Timeout Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

6. **Unexpected Completion Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

7. **Receiver Overflow Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

8. **Malformed TLP Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

9. **ECRC Error Mask**

   Value: **Disabled**/ Enabled

   Help text: None.

   Comments: None.

   Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

10. **ACS Violation Mask**

    Value: **Disabled**/ Enabled

    Help text: None.

    Comments: None.

Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

11. Uncorrectable Internal Error Mask

Value: **Disabled**/ Enabled

Help text: None.

Comments: None.

Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

12. MC Blocked TLP Mask

Value: **Disabled**/ Enabled

Help text: None.

Comments: None.

Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

13. AtomicOp Egress Blocked Mask

Value: **Disabled**/ Enabled

Help text: None.

Comments: None.

Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

14. TLP Prefix Blocked Error Mask

Value: **Disabled**/ Enabled

Help text: None.

Comments: None.

Back to: PCIE Fatal Error Mask Setting – System Event Log – Advanced – Screen Map

3.3.6 Integrated IO Configuration

The Integrated IO Configuration screen allows the user to configure the integrated IO used for onboard devices inside the processors.

To access this screen from the front page, select **Advanced** > **PCI Configuration**. Press the **<Esc>** key to return to the Advanced screen.

Note: NTB features are only supported on a dual-processor system.

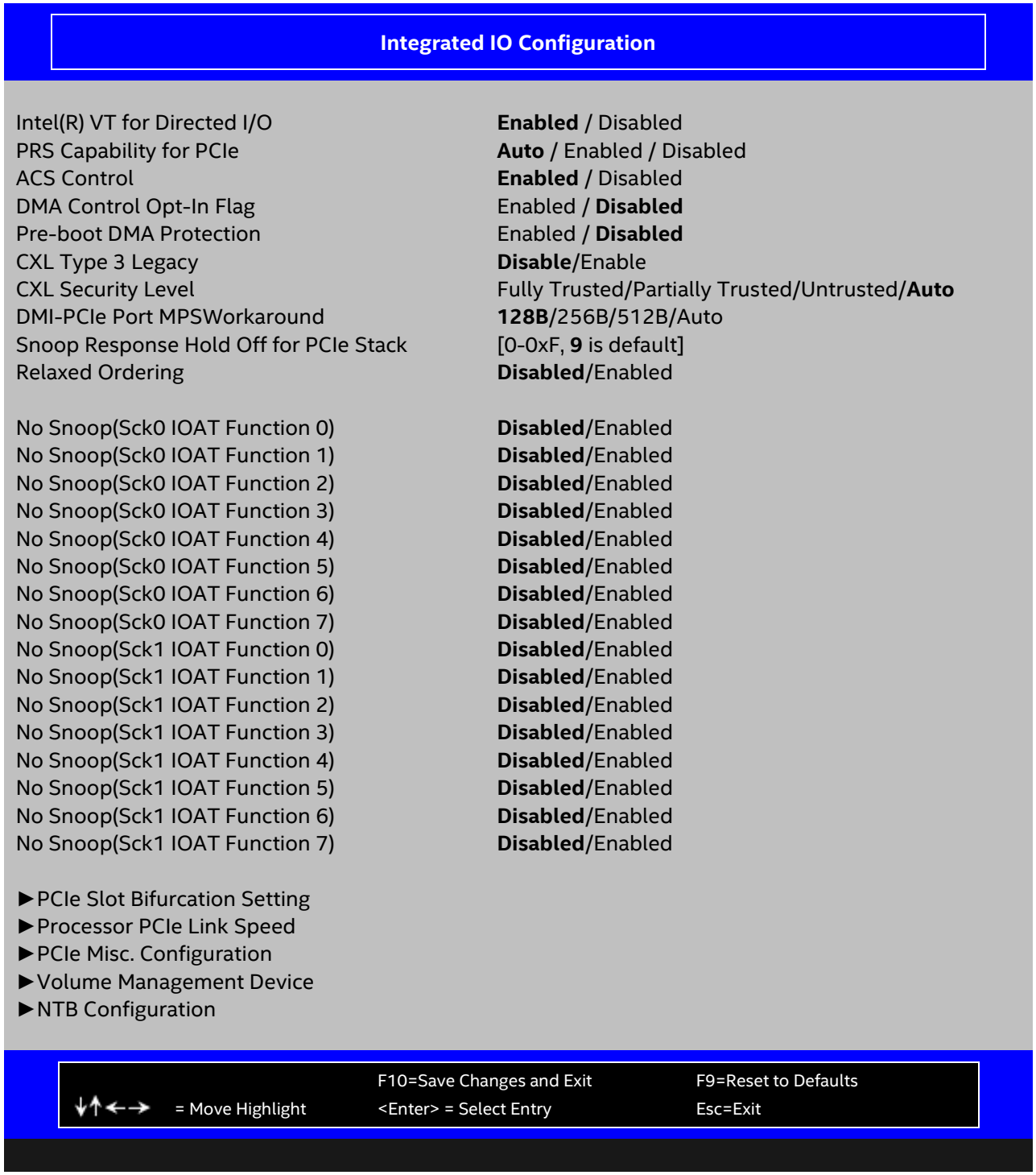

Figure 19. Integrated IO Configuration Screen

1. **Intel(R) VT for Directed I/O**

   Value: **Enabled**/Disabled

   Help text: Enable/Disable Intel(R) Virtualization Technology for Directed I/O (Intel(R) VT-d).

   Report the I/O device assignment to VMM through DMAR ACPI Tables. To disable VT-d, X2APIC must also be disabled.

   Comments: This option is only visible if all processors installed in the system support Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d). The software configuration installed on the system must support this feature in order to be enabled.

Note: When enabling this function to boot to 2019 Windows* operating system, Limit CPU PA to 64-bits setup knob need to be enabled firstly. When booting to 2020H1 operating system, no need to enable Limit CPU PA to 64-bits setup knob.

Back to: Integrated IO Configuration – Advanced – Screen Map

2. **PRS Capability for PCIe**

   Value: **Auto**/Enabled/Disabled

   Help text: `Enable/Disable support for page request services capability on discrete PCIe devices. Enabling should only be to test vehicle for PCIe cards supporting PRS, and it might lead to platform hang.`

   Comments: The knob is only for EMR.

Back to: Integrated IO Configuration – Advanced – Screen Map

3. **ACS Control**

   Value: **Enabled**/Disabled

   Help text: `Enable: Programs ACS only to Chipset Pcie Root Ports Bridges; Disable: Programs ACS to all Pcie bridges.`

   Comments: This option only appears when Intel VT for Directed I/O is enabled.

Back to: Integrated IO Configuration – Advanced – Screen Map

4. **DMA Control Opt-In Flag**

   Value: Enabled/**Disabled**

   Help text: `Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).`

   Comments: This option only appears when Intel VT for Directed I/O is enabled.

Back to: Integrated IO Configuration – Advanced – Screen Map

5. **Pre-boot DMA Protection**

   Value: Enabled/**Disabled**

   Help text: `Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)`

   Comments: This option only appears when Intel VT for Directed I/O is enabled.

Back to: Integrated IO Configuration – Advanced – Screen Map

6. **CXL Type 3 Legacy**

   Value: Enable/**Disable**

   Help text: `Enable or disable CXL type 3 device using CXL type 2 flow`

   Comments: This option is hidden if CXL type 3 device supports native mode.

Back to: Integrated IO Configuration – Advanced – Screen Map

7. **CXL Security Level**

   Value: Fully Trusted/Partially Trusted/Untrusted/**Auto**

Help text: `Fully Trusted: CXL Device can get access on CXL.$ for host-attached and device attached memory ranges in the WB address space; Partially Trusted: CXL Device can get access on CXL.$ for device attached memory ranges only; Untrusted: All requests on CXL.$ will be aborted by the Host. Auto - Auto decides based on Si Compatibility.`

Comments: None

Back to: Integrated IO Configuration – Advanced – Screen Map

8. **DMI-PCIe Port MPSWorkaround**

Value: **128B**/256B/512B/Auto

Help text: Set Maxpayload size to 256B if possible

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

9. **Snoop Response Hold Off for PCIe Stack**

Value: [0-0xF, **9** is default]

Help text: Sets Snoop Response Hold Off value, 256 cycles as Default

Comments: The value is displayed as a hexadecimal value in the range of 0x0–0xF. This should be set based on guidance received from component vendors. If no guidance is received, the default value should be maintained.

Back to: Integrated IO Configuration – Advanced – Screen Map

10. **Relaxed Ordering**

Value: **Disabled**/Enabled

Help text: `Relaxed Ordering Enable/Disable`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

11. **No Snoop(Sck0 IOAT Function 0)**

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

12. **No Snoop(Sck0 IOAT Function 1)**

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

13. No Snoop(Sck0 IOAT Function 2)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

14. No Snoop(Sck0 IOAT Function 3)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

15. No Snoop(Sck0 IOAT Function 4)

Value: **Disabled**/Enabled

Help text: No Snoop Enable/Disable for each CB device

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

16. No Snoop(Sck0 IOAT Function 5)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

17. No Snoop(Sck0 IOAT Function 6)

Value: **Disabled**/Enabled

Help text: No Snoop Enable/Disable for each CB device

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

18. No Snoop(Sck0 IOAT Function 7)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

19. No Snoop(Sck1 IOAT Function 0)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

20. No Snoop(Sck1 IOAT Function 1)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

21. No Snoop(Sck1 IOAT Function 2)

Value: **Disabled**/Enabled

Help text: No Snoop Enable/Disable for each CB device

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

22. No Snoop(Sck1 IOAT Function 3)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

23. No Snoop(Sck1 IOAT Function 4)

Value: **Disabled**/Enabled

Help text: No Snoop Enable/Disable for each CB device

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

24. No Snoop(Sck1 IOAT Function 5)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

25. No Snoop(Sck1 IOAT Function 6)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

26. No Snoop(Sck1 IOAT Function 7)

Value: **Disabled**/Enabled

Help text: `No Snoop Enable/Disable for each CB device`

Comments: None.

Back to: Integrated IO Configuration – Advanced – Screen Map

27. PCIe Slot Bifurcation Setting

Value: None.

Help text: View/Configure PCIe Slot Bifurcation setting.

Comments: *Selection only*. For more information on PCIe Slot Bifurcation settings, see Section 3.3.6.1.

Note: This configuration page is only visible on Intel® Server Boards M50FCP and D50DNP.

Back to: Integrated IO Configuration – Advanced – Screen Map

28. Processor PCIe Link Speed

Value: None.

Help text: `Allow for selecting target PCIe Link Speed as Gen1, Gen2, Gen3, Gen4 or Gen5.`

Comments: *Selection only*. For more information on PCIe link speed settings, see Section 3.3.6.2.

Back to: Integrated IO Configuration – Advanced – Screen Map

29. Volume Management Device

Value: None.

Help text: `Allow Volume Management Device to manage down stream NVMe SSD.`

Comments: *Selection only*. For more information on Volume Management Device settings, see Section 3.3.6.4.

Back to: Integrated IO Configuration – Advanced – Screen Map

30. PCIe Misc. Configuration

Value: None.

Help text: `Displays and provides option to change the IIO PCIE Misc Settings.`

Comments: *Selection only*. For more information on PCIe Misc. Configuration item, see Section 3.3.6.4.

Back to: Integrated IO Configuration – Advanced – Screen Map

31. NTB Configuration

Value: None.

Help text: `View/Configure NTB information and settings.`

Comments: *Selection only*. For more information on NTB Configuration settings, see Section 3.3.6.5.

Back to: Integrated IO Configuration – Advanced – Screen Map

3.3.6.1 PCIe Slot Bifurcation Setting

Each board in the Intel Server Boards M50FCP and D50DNP has different risers and different options for PCIe slot bifurcation.

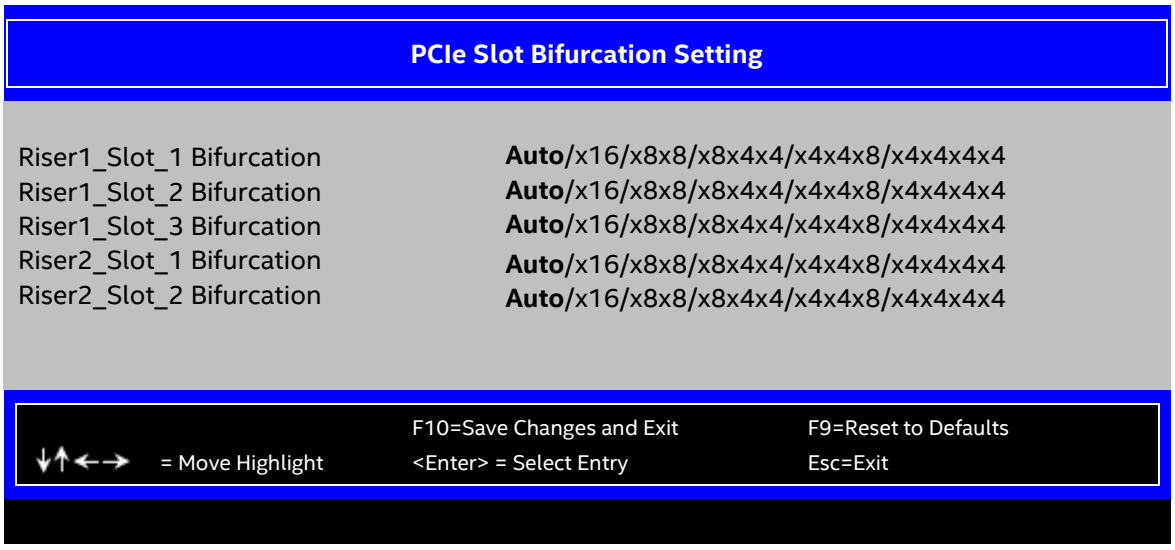

Figure 20. PCIe* Slot Bifurcation Setting Screen – Intel® Server Board M50FCP

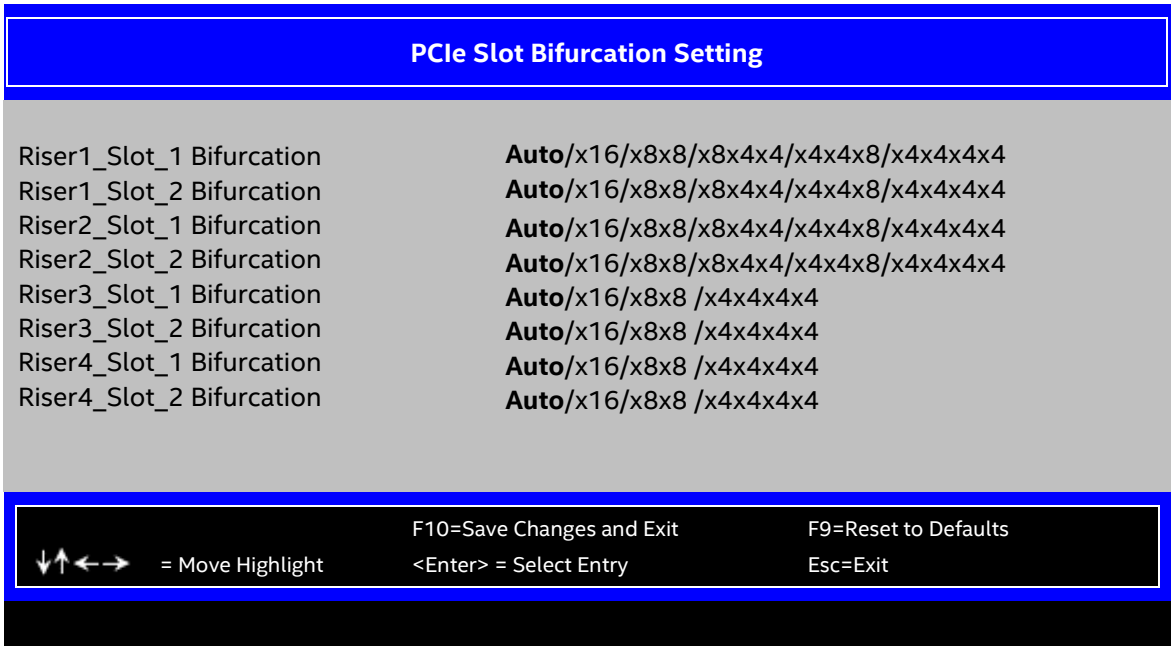

Figure 21. PCIe* Slot Bifurcation Setting Screen – Intel® Server Board D50DNP

1. **RiserX_Slot_X Bifurcation**

   Value: **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4

   Help text: `Select PCIe port Bifurcation for selected slot(s) of Riser.`

   Comments: None.

   Note: Each setup item displays if a x16 riser or add-in card interposer is plugged. For the Intel® Server Board M50FCP, when an add-in card interposer is plugged, the Riser2_Slot_2 Bifurcation option value is Auto/x8x8/x8x4x4.

   Back to: PCIe Slot Bifurcation Setting – Integrated IO Configuration – Advanced – Screen Map

3.3.6.2 Processor PCIe Link Speed

The Processor PCIe Link Speed configuration screen allows user to configure the PCIe link speed of the processor IIO PCIe root port and the PCIe devices connected to this port.

To access this screen from the front page, select **Advanced** > **PCI Configuration** > **Processor PCIe Link Speed**. Press the **<Esc>** key to return to the PCI Configuration screen.

The usage for these options is to select the target link speed as Gen1, Gen2, Gen3, Gen4, or Gen5 speed. The BIOS currently only supports controlling the PCIe link off the IIO root ports and the design follows the IIO PCIe Lane Partitioning rules, shown in the following figure. The IIO supports 80 PCIe lanes and 8 DMI lanes. The DMI lanes can also be strapped to operate in PCIe mode, which is displayed as PCIe Port 00. The 80 PCIe lanes are grouped in four. Each port can be bifurcated as 2x8 or 4x4 or any combination thereof, which is displayed as PCIe Ports 1a, 1b, 1c, or 1d.

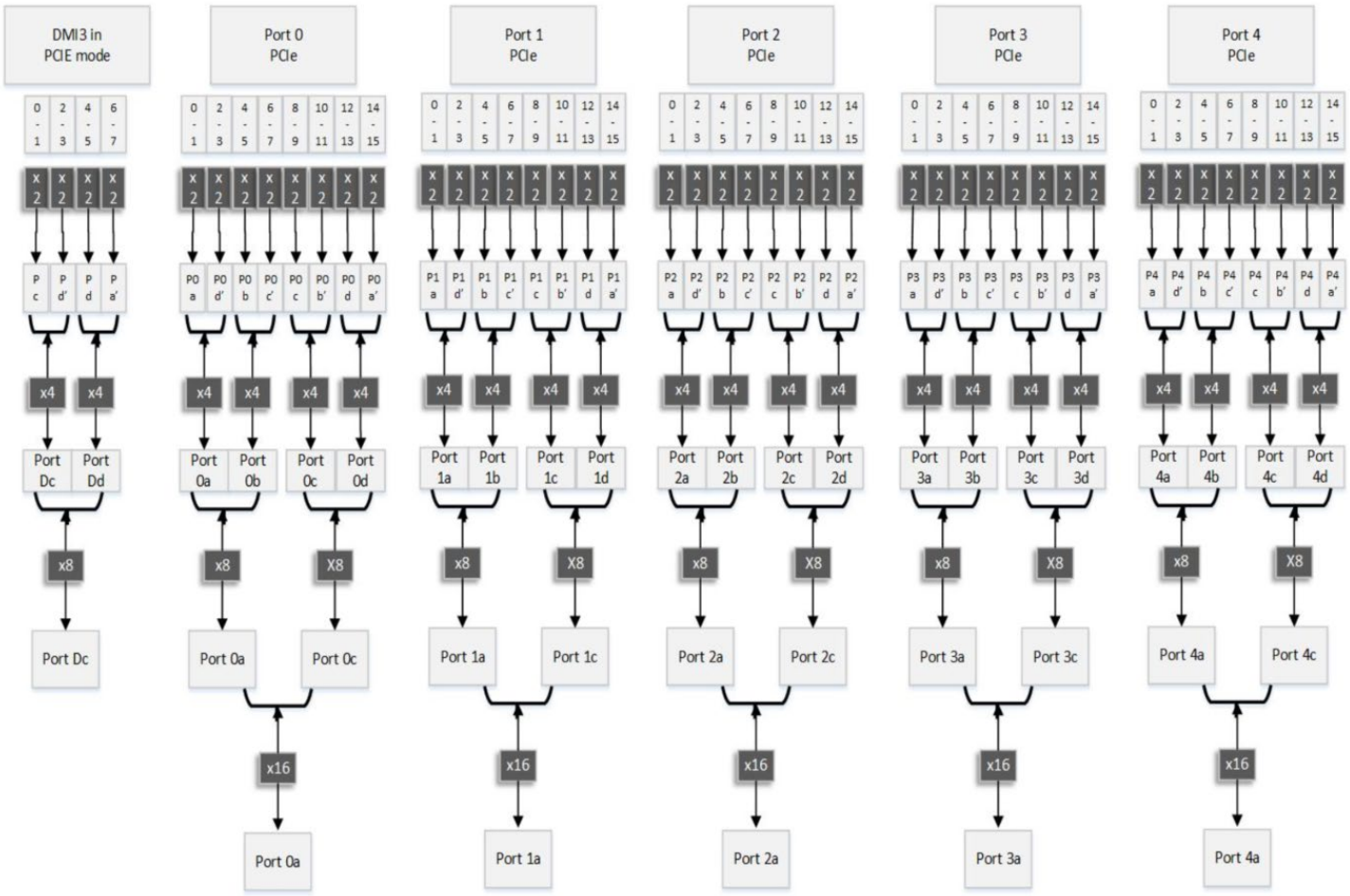

Figure 22. IIO PCIe* Lane Partitioning

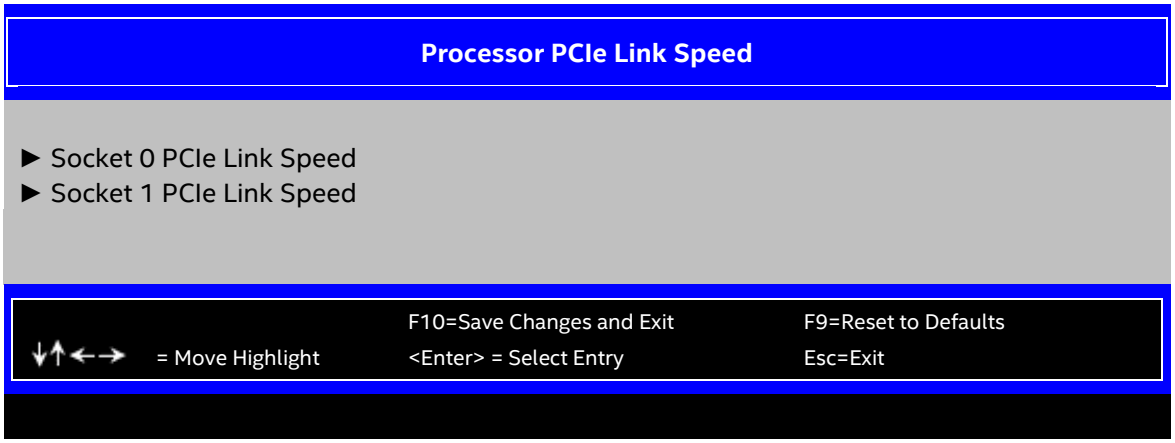

Figure 23. Processor PCIe* Link Speed Screen

Socket x PCIe Link Speed

Socket x, DMI	Gen1 / Gen2 / **Gen3**
Socket x, PCIe Port 0a	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 0b	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 0c	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 0d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 1a	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 1b	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 1c	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 1d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2a	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2b	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2c	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**
Socket x, PCIe Port 2d	Gen1 / Gen2 / Gen3 / Gen4 / **Gen5**

	F10=Save Changes and Exit	F9=Reset to Defaults
↓↑←→ = Move Highlight	<Enter> = Select Entry	Esc=Exit

Figure 24. Processor Socket x PCIe* Link Speed Screen

1. **Socket x, DMI**

Value: Gen3/ Gen2 /Gen1

Help text: Allow for selecting target PCIe Link Speed as Gen1(2.5GT/s), Gen2(5GT/s), Gen3(8GT/s).

Comments: DMI port supports Gen1, Gen 2, and Gen3 speed. This option is only available when there is corresponding PCIe slot implemented on the specific board.

Note: For Intel® Server Boards M50FCP and D50DNP, Socket 0, DMI is already connected to the PCH. So, it should not be visible.

Back to: Processor PCIe Link Speed – Integrated IO Configuration – Advanced – Screen Map

2. **Socket x, PCIe Port 0a**
Socket x, PCIe Port 0b
Socket x, PCIe Port 0c
Socket x, PCIe Port 0d
Socket x, PCIe Port 1a
Socket x, PCIe Port 1b
Socket x, PCIe Port 1c

Socket x, PCIe Port 1d
Socket x, PCIe Port 2a
Socket x, PCIe Port 2b
Socket x, PCIe Port 2c
Socket x, PCIe Port 2d
Socket x, PCIe Port 3a
Socket x, PCIe Port 3b
Socket x, PCIe Port 3c
Socket x, PCIe Port 3d
Socket x, PCIe Port 4a
Socket x, PCIe Port 4b
Socket x, PCIe Port 4c
Socket x, PCIe Port 4d

Value: **Gen5**/Gen4/Gen3/Gen2 /Gen1

Help text: `Allow for selecting target PCIe Link Speed as Gen1(2.5GT/s), Gen2(5GT/s), Gen3(8GT/s), Gen4(16GT/s) or Gen5(32GT/s).`

Comments: PCIe ports support the speeds for generations 1.0 (2.5 GT/s), 2.0 (5 GT/s), and 3.0 (8 GT/s). SPR SP supports the speed for 5.0 (32 GT/s). Those options for PCIe ports are only available when the corresponding PCIe slot is implemented on the specific board.

Back to: Processor PCIe Link Speed – Integrated IO Configuration – Advanced – Screen Map

3.3.6.3 PCIe Misc. Configuration

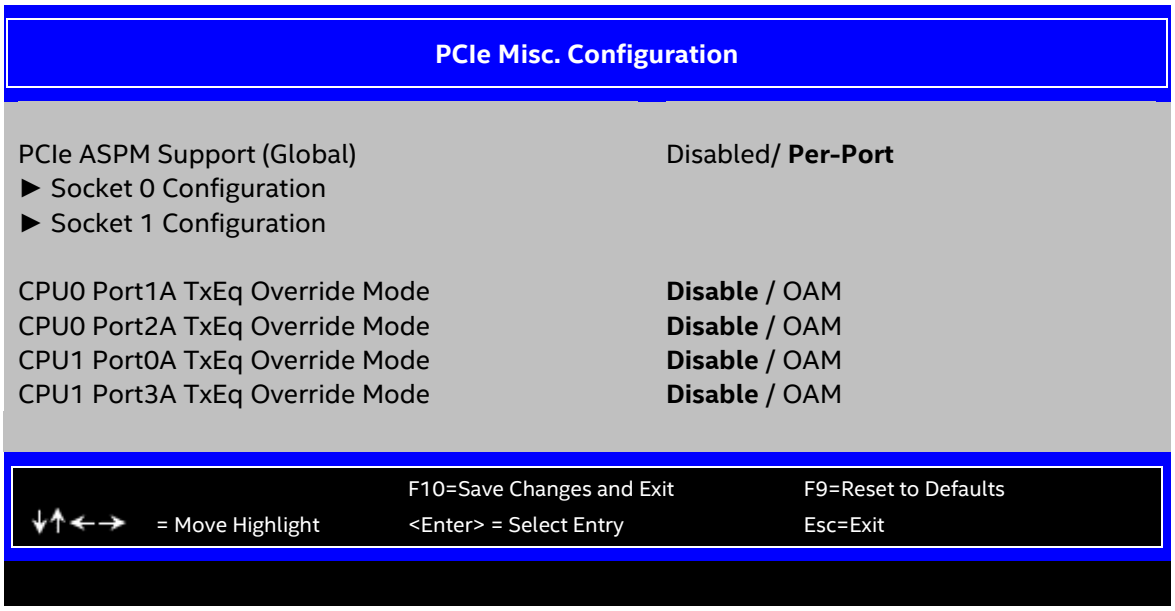

Figure 25. PCIe* Misc. Configuration Screen

1. **PCIe ASPM Support (Global)**

Value: Disabled/**Per-Port**

Help text: `This option allows setting ASPM support for all downstream devices.`

Comments: None.

Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

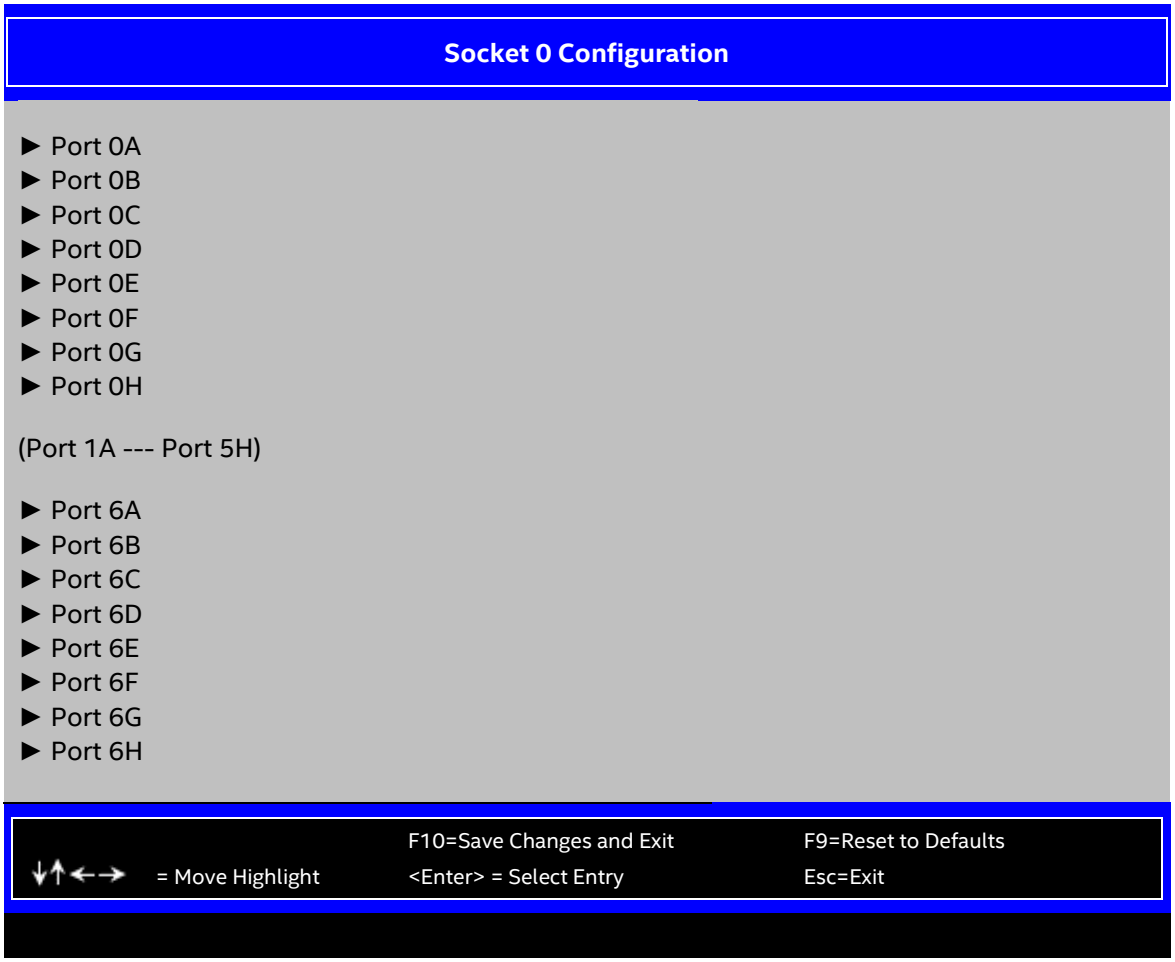

Figure 26. PCIe* Misc. Socket 0 Configuration Screen

2. **Port 0A/0B/0C/0D/0E/0F/0G/0H ----6A/6B/6C/6D/6E/6F/6G/6H**

   Value: None.

   Help text: `Settings related to PCI Express Ports (0A/0B/0C/0D/0E/0F/0G/0H/1A/1B/1C/1D/1E/1F/1G/1H/2A/2B/2C/2D/2E/2F/2G/2H/3A/3B/3C/3D/3E/3F/3G/3H/4A/4B/4C/4D/4E/4F/4G/4H/5A/5B/5C/5D/5E/5F/5G/5H/6A/6B/6C/6D/6E/6F/6G/6H)`

   Comments: *Selection only*. This option is only available when a corresponding PCIe slot is implemented on the specific board.

   Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

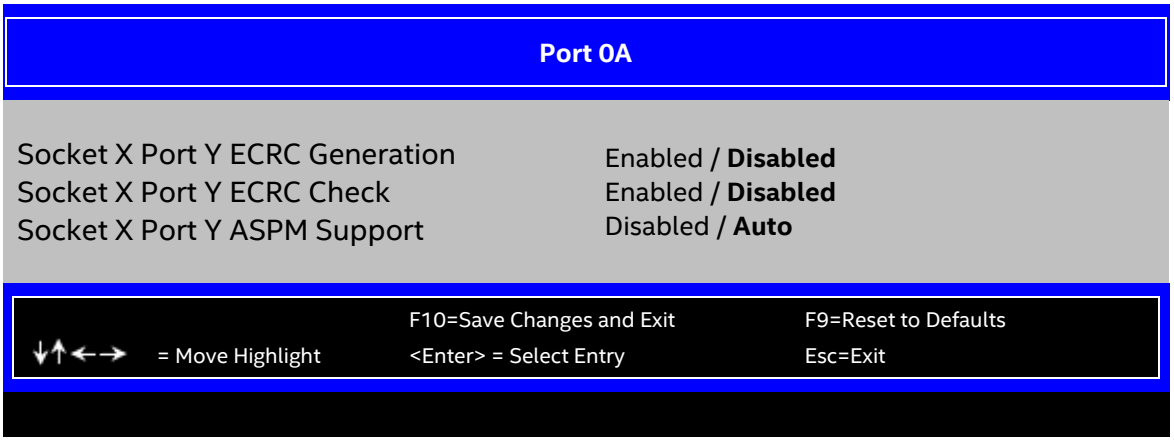

Figure 27. PCIe* Misc. Port 0A Screen

3. **Socket X Port Y ECRC Generation**

   Value: Enabled/**Disabled**

   Help text: `Enable or Disable ECRC Generation (Error Capabilities and Control Register)`

   Comments: None.

   Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

4. **Socket X Port Y ECRC Check**

   Value: Enabled/**Disabled**

   Help text: `Enable or Disable ECRC Check (Error Capabilities and Control Register)`

   Comments: None.

   Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

5. **Socket X Port Y ASPM Support**

   Value: Disabled/**Auto**

   Help text: `This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.`

   Comments: It is grayed out when Global ASPM per port is not supported.

   Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

6. CPU0 Port1A TxEq Override Mode

   Value: **Disabled**/OAM

   Help text: CPU0 Port1A TxEq override for PVC OAM/AIC setting.

   Comments: This knob is only visiable for D50DNP.

   Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

7. CPU0 Port2A TxEq Override Mode

   Value: **Disabled**/OAM

   Help text: CPU0 Port2A TxEq override for PVC OAM/AIC setting.

Comments: This knob is only visiable for D50DNP.

Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

8. CPU1 Port0A TxEq Override Mode

Value: **Disabled**/OAM

Help text: CPU1 Port0A TxEq override for PVC OAM/AIC setting.

Comments: This knob is only visiable for D50DNP.

Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

9. CPU1 Port3A TxEq Override Mode

Value: **Disabled**/OAM

Help text: CPU1 Port3A TxEq override for PVC OAM/AIC setting.

Comments: This knob is only visiable for D50DNP.

Back to: PCIe Misc. Configuration – Integrated IO Configuration – Advanced – Screen Map

3.3.6.4 Volume Management Device

Volume Management Device is enhanced feature to support NVMe* storage devices, it is responsible for managing attached PCIe SSD device access and hot plugging. It can also work with Intel RSTe to create a PCIe SSD RAID volume.

To access this screen from the front page, select **Advanced** > **Integrated IO Configuration** > **Volume Management Device**. Press the **<Esc>** key to return to the Integrated IO Configuration screen.

Figure 28. Volume Management Device Screen – Intel® Server Board M50FCP

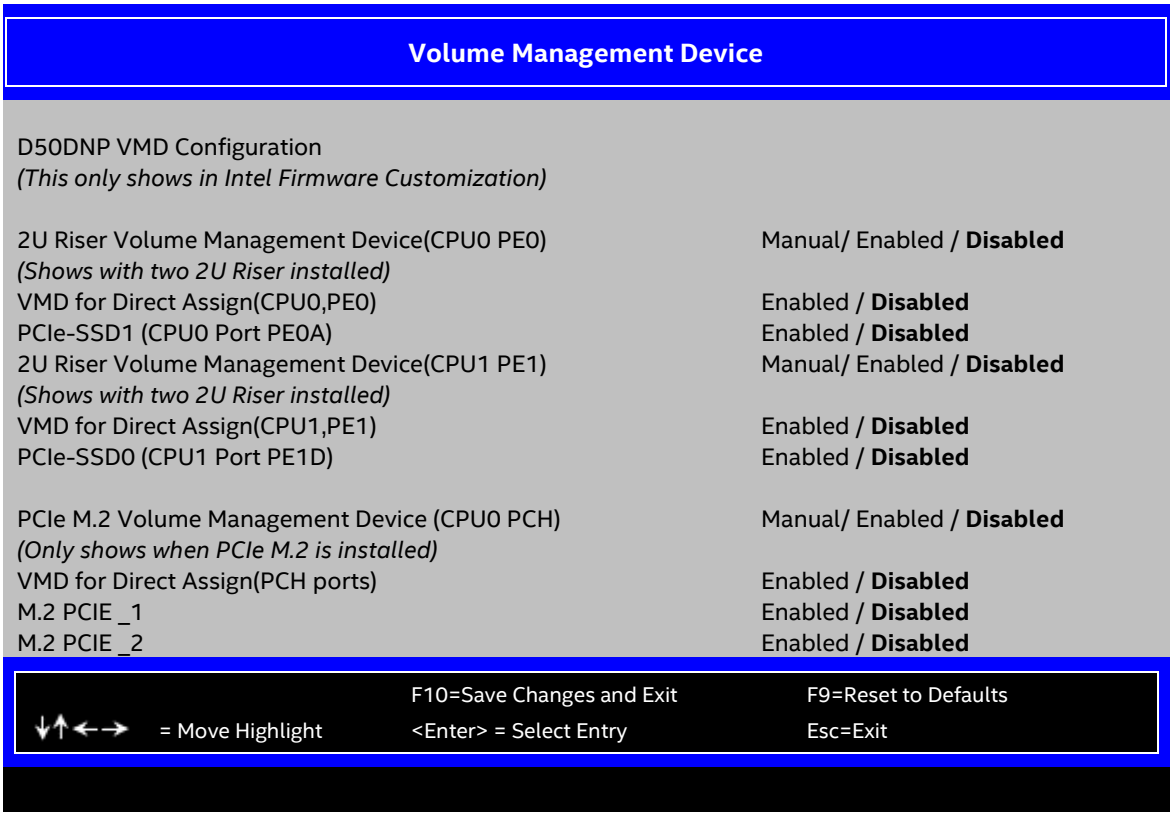

Figure 29. Volume Management Device Screen – Intel® Server Board D50DNP

1. **List of VMD Switches Based on SKU**

For Intel® Server Board D50DNP

- 2U Riser Volume Management Device(CPU0 PE0)
- 2U Riser Volume Management Device(CPU1 PE1)

For Intel® Server Board M50FCP

- Riser1 Volume Management Device(CPU0,PE2) – Shows with riser 1 with retimer
- Riser3, NVMe Volume Management Device(CPU1,PE0) – Shows with the riser 3 NVMe card
- Direct HSBP Volume Management Device(CPU0,PE3) – Shows with HSBP Direct connection
- Direct HSBP Volume Management Device(CPU0,PE4) – Shows with HSBP Direct connection
- Direct HSBP Volume Management Device(CPU1,PE3) – Shows with HSBP Direct connection
- Direct HSBP Volume Management Device(CPU1,PE4) – Shows with HSBP Direct connection

Value: Manual/Enabled/**Disabled**

Help text: `[Manual] – All specified VMD ports can be selected to enable or disable alone.`
`[Enabled] – All specified VMD ports are forced to enable.`
`[Disabled] – All specified VMD ports are forced to disable.`

Comments: Global setup option to enable or disable VMD support for this system. The setup could be different, based on system configurations for SKUs.

For the Intel® Server Board M50FCP2SBSTD, the display of VMD setup options relies on ID detection of riser or direct HSBP ID. Refer to the server boards design and configurations table.

Back to: Volume Management Device – Integrated IO Configuration – Advanced – Screen Map

2. **PCIe M.2 Volume Management Device (CPU0 PCH)**

   Value: Manual/Enabled/**Disabled**

   Help text: `[Manual] – All specified VMD ports can be selected to enable or disable alone.`
   `[Enabled] – All specified VMD ports are forced to enable.`
   `[Disabled] – All specified VMD ports are forced to disable.`

   Comments: None.

   Back to: Volume Management Device – Integrated IO Configuration – Advanced – Screen Map

3. **VMD for Direct Assign**

   Value: Enabled/**Disabled**

   Help text: `Enable/Disable VMD for Direct Assign`

   Comments: Enable or disable VMD for Direct Assign for the corresponding PCIe root port. This option is shown or hidden based on the board design SKU. Only capable root ports have visible option.

   Back to: Volume Management Device – Integrated IO Configuration – Advanced – Screen Map

4. **PCIe-SSD0 (CPU0 Port PE2A)**
   PCIe-SSD1 (CPU0 Port PE2B)
   PCIe-SSD2 (CPU0 Port PE2C)
   PCIe-SSD3 (CPU0 Port PE2D)
   …

   Value: Enabled/**Disabled**

   Help text: `Enable/Disable VMD on this port.`

   Comments: Enable or disable VMD support for corresponding PCIe root port, this option is show or hide based on this SKU's board design, only capable root port have visible option.

   The VMD function selection of M.2 PCIE only works on SPR CPU installed.

   Back to: Volume Management Device – Integrated IO Configuration – Advanced – Screen Map

5. **M.2 PCIE _1**
   M.2 PCIE _2

   Value: Enabled/**Disabled**

   Help text: `Configuration PCH root port: Enable - VMD ownership root port. M50FCP M.2 is x2 width. D50DNP M.2 is x4 width.`

   Comments: The VMD function selection of M.2 PCIE only works on SPR CPU installed.

   Note: This area lists all setup options. For detailed setup items per SKU, see the figures in Section 3.3.6.4.

   Back to: Volume Management Device – Integrated IO Configuration – Advanced – Screen Map

3.3.6.5 NTB Configuration

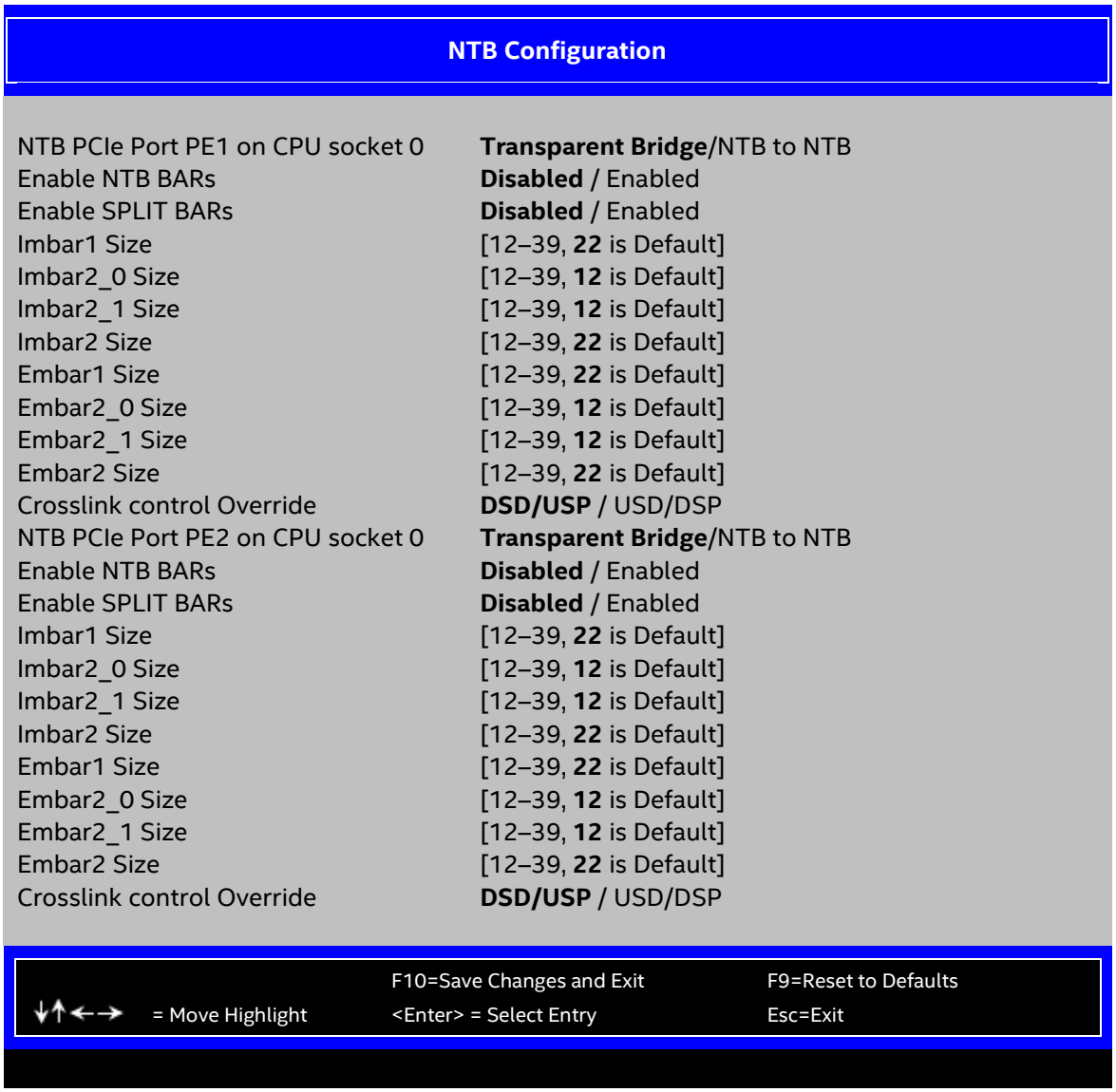

Figure 30. NTB Configuration Screen – Page 1

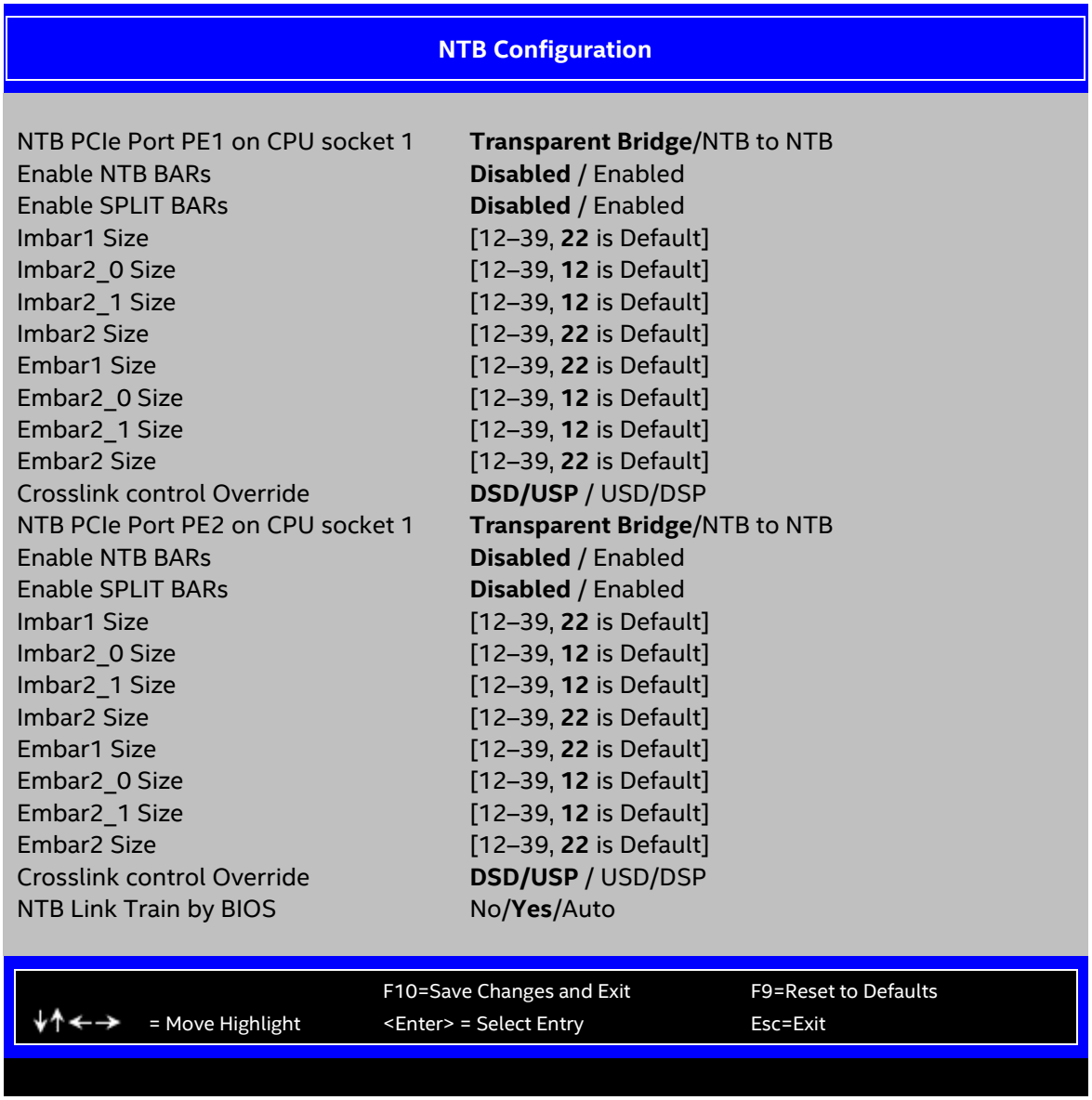

Figure 31. NTB Configuration Screen – Page 2

1. **Intel® Server Board M50FCP:**

   NTB PCIe Port PE1 on CPU socket 0
   NTB PCIe Port PE2 on CPU socket 0
   NTB PCIe Port PE1 on CPU socket 1
   NTB PCIe Port PE2 on CPU socket 1

   Intel® Server Board D50DNP:

   NTB PCIe Port PE3 on CPU socket 0
   NTB PCIe Port PE4 on CPU socket 0
   NTB PCIe Port PE2 on CPU socket 1
   NTB PCIe Port PE4 on CPU socket 1

   Value: **Transparent Bridge**/NTB to NTB

   Help text: `Configures port as TB, NTB-NTB.`

   Comments: This option selects the configuration mode of PCI Express (PCIe) port PE1, PE2, PE3, PE4 to support NTB configuration.

Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

2. **Enable NTB BARs**

   Value: Enabled/**Disabled**

   Help text: `[IMBAR1] If Enabled, BIOS will program NTB BAR size registers.`

   Comments: This option allows the BIOS to program NTB BAR registers with default values when enabled. If disabled, the BIOS does not program NTB BARs registers, and the task is left to drivers. This option only appears when NTB PCIe port is not configured as Transparent Bridge.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

3. **Enable SPLIT BARs**

   Value: Enabled/**Disabled**

   Help text: `[IMBAR2, EMBAR2] If Enabled, will use two 32 bit BARs instead of 64 bit BAR.`

   Comments: When this option enabled, BIOS can split Primary BAR 45 Size and Secondary BAR 45 Size into Primary BAR 4/5 Size and Secondary BAR 4/5 Size. This option only appears when Enable NTB BARs is enabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

4. **Imbar1 Size**

   Value: [12–39, **22** is Default]

   Help text: `[IMBAR1SZ] Used to set the prefetchable Imbar1 size on primary side of NTB. Value range <12...39> representing BAR sizes <4KB ... 512GB>.`

   Comments: This option only appears when Enable NTB BARs is enabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

5. **Imbar2_0 Size**

   Value: [12–39, **12** is Default]

   Help text: `Used to set the prefetchable Imbar2_0 size on primary side of NTB. Value < than 12 or > 29 (39 for BIOS supporting > 4G PCI) disables BAR.`

   Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is enabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

6. **Imbar2_1 Size**

   Value: [12–39, **12** is Default]

   Help text: `Used to set the prefetchable Imbar2_1 size on primary side of NTB. Value < than 12 or > 29 (39 for BIOS supporting > 4G PCI) disables BAR.`

   Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is enabled.

Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

7. **Imbar2 Size**

   Value: [12–39, **22** is Default]

   Help text: `[IMBAR2SZ] Used to set the prefetchable Imbar2 size on primary side of NTB. Value range <12...39> representing BAR sizes <4KB ... 512GB>.`

   Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is disabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

8. **Embar1 Size**

   Value: [12–39, **22** is Default]

   Help text: `[EMBAR1SZ] Used to set the prefetchable Embar1 size on secondary side of NTB. Value range <12...39> representing BAR sizes <4KB ... 512GB>.`

   Comments: This option only appears when Enable NTB BARs is enabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

9. **Embar2_0 Size**

   Value: [12–39, **12** is Default]

   Help text: `Used to set the prefetchable Embar2_0 size on Secondary side of NTB. Value < than 12 or > 29 (39 for BIOS supporting > 4G PCI) disables BAR.`

   Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is enabled.

   Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

10. **Embar2_1 Size**

    Value: [12–39, **12** is Default]

    Help text: `Used to set the prefetchable Embar2_1 size on Secondary side of NTB. Value < than 12 or > 29 (39 for BIOS supporting > 4G PCI) disables BAR.`

    Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is enabled.

    Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

11. Embar2 Size

Value: [12–39, **22** is Default]

Help text: `[EMBAR2SZ] Used to set the prefetchable Embar2 size on secondary side of NTB. Value range <12...39> representing BAR sizes <4KB ... 512GB>.`

Comments: This option only appears when Enable NTB BARs is enabled and Enable SPLIT BARs is disabled.

Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

12. Crosslink control Override

Value: **DSD/USP** / USD/DSP

Help text: `Configure NTB port as DSD/USP, USD/DSP, or use external pins.`

Comments: This option configures the crosslink configuration of the NTB port. For more details about the crosslink configuration, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.6.1. This option only appears when the NTB PCIe Port is configured as NTB to NTB.

Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

13. NTB Link Train by BIOS

Value: No/**Yes**/Auto

Help text: `This knob enables or disables the BIOS to train the NTB link`

Comments: None.

Back to: NTB Configuration – Integrated IO Configuration – Advanced – Screen Map

3.3.7 Mass Storage Controller Configuration

The Mass Storage Configuration screen allows the user to configure the mass storage controllers that are integrated into the server board on which the BIOS is executing. This includes only onboard mass storage controllers. Mass storage controllers on add-in cards are not included in this screen, nor are other storage mechanisms such as USB-attached storage devices or network attached storage.

SATA port configuration options are available in this screen, representing the SATA controller. Informational displays of SATA controller configuration are also available when applicable. If the presence of an Intel® Storage Module is detected, the type of storage module is displayed as information only.

For more detailed information about mass storage in the Intel Server Boards M50FCP and D50DNP, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.7. For details of the storage configurations supported by the different server boards, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

To access this screen from the front page, select **Advanced** > **Mass Storage Controller Configuration**. Press the **<Esc>** key to return to the Advanced screen.

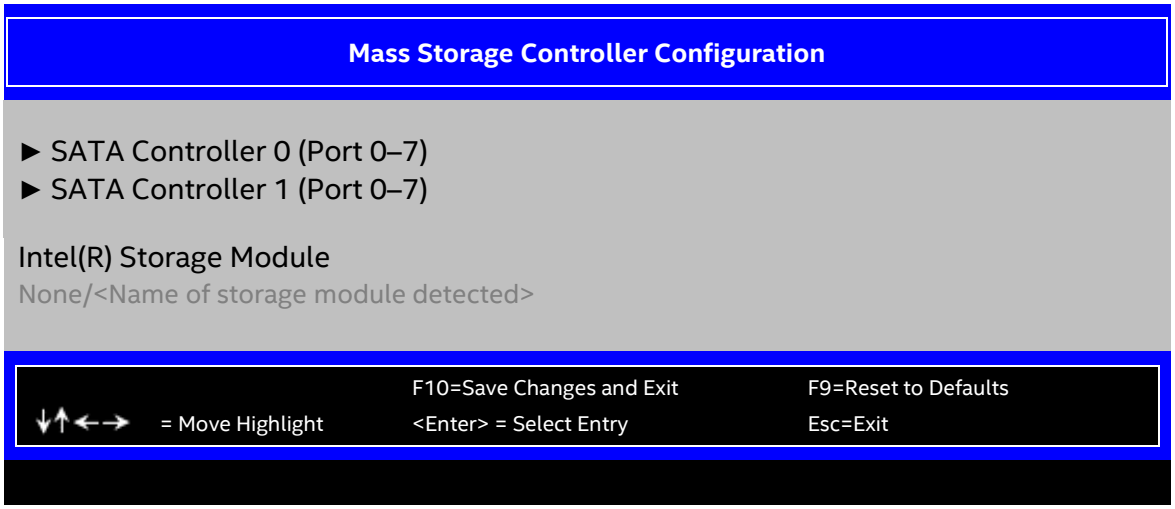

Figure 32. Mass Storage Controller Configuration Screen

1. **SATA Controller 0 (Port 0–7)**

   Value: None.

   Help text: `Configure the SATA Port 0-7 and view current disk drive information.`

   Comments: *Selection only*. For more information on SATA Port configuration settings, see Section 3.3.7.1.

   Back to: Mass Storage Controller Configuration – Advanced – Screen Map

2. **SATA Controller 1 (Port 0–7)**

   Value: None.

   Help text: `Configure the SATA Port 0-7 and view current disk drive information.`

   Comments: *Selection only*. For more information on SATA Port configuration settings, see Section 3.3.7.1.

   Back to: Mass Storage Controller Configuration – Advanced – Screen Map

3. **Intel(R) Storage Module**

   Value: None/<Name of storage module detected>

   Help text: None.

   Comments: *Information only*. This displays the product name of the Intel(R) Storage Module installed, which helps in identifying drivers, support, documentation, and so on. If no module is detected, then None is displayed.

   For details about Intel Storage Modules support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 3.7.6.

   Back to: Mass Storage Controller Configuration – Advanced – Screen Map

3.3.7.1 SATA Port Configuration

The SATA Port Configuration screen allows the user to configure the AHCI-capable controllers that are integrated into the server board on which the BIOS is executing. There is an onboard controller – the AHCI SATA controller with SATA drive and RAID support. Informational displays of AHCI controller configuration and SATA drive information are also available when applicable.

Note: Due to limitations of Intel® Server Configuration Utility (cannot change two options with the same name), change all SATA options to different names.

To access this screen from the front page, select **Advanced** > **Mass Storage Controller Configuration**. Press the **<Esc>** key to return to the Advanced screen.

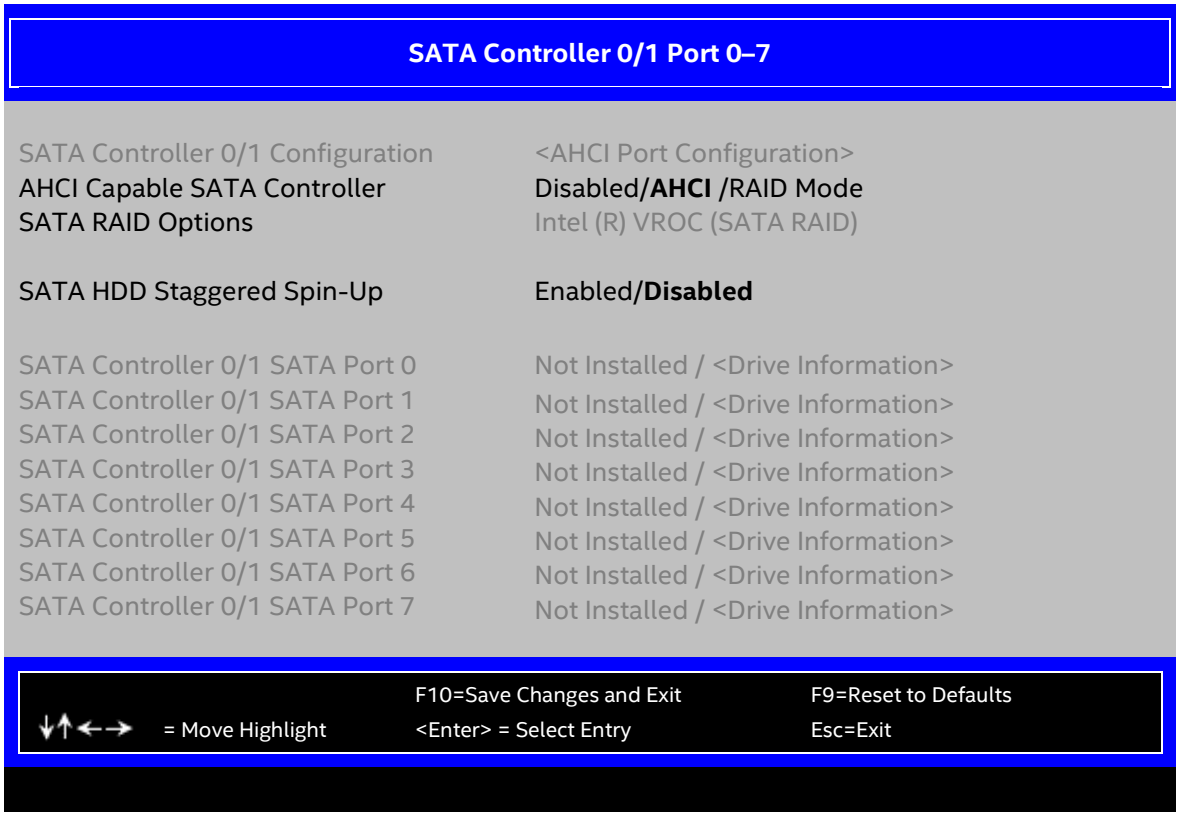

Figure 33. SATA Port Configuration Screen

1. **SATA Controller 0/1 Configuration**

   Value: Controller is disabled/<AHCI port configuration>

   Help text: None.

   Comments: *Information only*. This is a display showing the capability of onboard AHCI capable SATA controller, if the controller is enabled. The controller configuration is one of the following states:

   - Controller is disabled
   - 8 ports of 6 Gb/s SATA (for SATA controller)

   This information is also displayed during POST in the POST diagnostic screen. Refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 4.2.

   The number of SATA ports available from the integrated AHCI-capable SATA controller is dependent on the specific server board installed in the system. Different server board designs expose different SATA port configurations. If no M.2 is attached, it shows that the Controller option is disabled in the Intel Server Boards M50FCP and D50DNP.

   The platform ID (board ID) is displayed in the Main screen, and the corresponding SATA port configuration can be found in the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

Back to: SATA Controller 0/1 Configuration – Mass Storage Controller Configuration – Advanced – Screen Map

2. **AHCI Capable SATA Controller**

   Value: Disabled/**AHCI**/RAID Mode

   Help text: `- AHCI enables the Advanced Host Controller Interface, which provides Enhanced SATA functionality.`
   `- RAID Mode provides host based RAID support on the onboard SATA ports.`

   Comments: This option configures the onboard AHCI-capable SATA controller, which is distinct from the storage control unit (SCU). The number and type of ports it controls differ between board series. For capabilities of specific boards, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

   If the SATA controller is disabled, the SATA ports do not operate, and any installed SATA devices are unavailable. RAID Mode provides host based RAID support on the onboard SATA ports. RAID levels supported and required drivers depend on the RAID stack selected.

   Back to: SATA Controller 0/1 Configuration – Mass Storage Controller Configuration – Advanced – Screen Map

3. **SATA RAID Options**

   Value: **Intel (R) VROC (SATA RAID)**

   Help text: `- Intel(R) VROC (SATA RAID): Provides pass-through drive support. Also provides host based RAID 0/1/10/5 support. Uses Intel(R) VROC (SATA RAID) iastor drivers.`

   Comments: This option only appears when the SATA Controller is enabled, and RAID Mode has been selected as the operational SATA mode. This setting selects the RAID stack to be used for SATA RAID with the onboard AHCI SATA controller.

   If a RAID Volume has not previously been created that is compatible with the RAID stack selected, it is necessary to Save and Exit and reboot in order to create a RAID Volume.

   Back to: SATA Controller 0/1 Configuration – Mass Storage Controller Configuration – Advanced – Screen Map

4. **SATA HDD Staggered Spin-Up**

   Value: Enabled/**Disabled**

   Help text: `If enabled for the AHCI Capable SATA controller, Staggered Spin-Up will be performed on drives attached to it. Otherwise these drives will all spin up at boot.`

   Comments: This option enables or disables staggered spin-up only for disk drives attached to ports on the AHCI-capable SATA controller. Disk drives attached to SATA/SAS ports on the SCU are controlled by a different method for staggered spin-pp and this option does not affect them.

   This option is only visible when the SATA controller is enabled and AHCI or RAID has been selected as the operational SATA mode.

   Staggered spin-up is needed when enough HDDs are attached to the system to cause a marked startup power demand surge when all drives start spin-up together. Since the power demand is greatest just as the drive spinning is started, the overall startup power demand

can be leveled off by starting each drive at a slightly different time, so the power demand surges for multiple drives do not coincide and cause too great a power draw.

When staggered spin-up is enabled, it does have a possibility of increasing boot time if many HDDs are attached, because of the interval between starting drives spinning. However, that is exactly the scenario in which staggered spin-up is most needed, because the more disk drives attached, the greater the startup demand surge.

Setting the external eSATA connector to Enabled (when available) does not invalidate the staggered spin-Up option, although there may be less need for staggered spin-up in a system configured for eSATA use.

Back to: SATA Controller 0/1 Configuration – Mass Storage Controller Configuration – Advanced – Screen Map

5. **SATA Port**

   SATA Controller 0/1 ports 0–7 for SATA controller

   Value: Not installed/<Drive information>

   Help text: None.

   Comments: *Information only.* The drive information, when present, typically consists of the drive model identification and size for the disk drive installed on a particular port.

   This drive information line is repeated for the SATA ports for the two onboard AHCI-capable SATA controllers. However, for any given board, only the ports that are physically populated on the board are shown. That is, a board that only implements the two 6 GB/s ports 0 and 1, only shows those two ports in this drive information list.

   This section for drive information does not appear when the SATA operational mode is RAID Mode.

   Note: For the Intel® Server Board M50FCP, SATA controller 0 port 4/5/6/7 and SATA controller 1 port 5/7 are not supported; these options are not shown on the page. For the Intel® Server Board D50DNP, only SATA controller 0 port 0 and SATA controller 1 port 4 are shown.

Back to: SATA Controller 0/1 Configuration – Mass Storage Controller Configuration – Advanced – Screen Map

3.3.8 PCI Configuration

The PCI Configuration screen allows the user to configure the PCI memory space used for onboard and add-in adapters, configure video options, and configure onboard adapter options. It also includes a selection option to go to the NIC Configuration screen.

To access this screen from the front page, select **Advanced** > **PCI Configuration**. Press the **<Esc>** key to return to the Advanced screen.

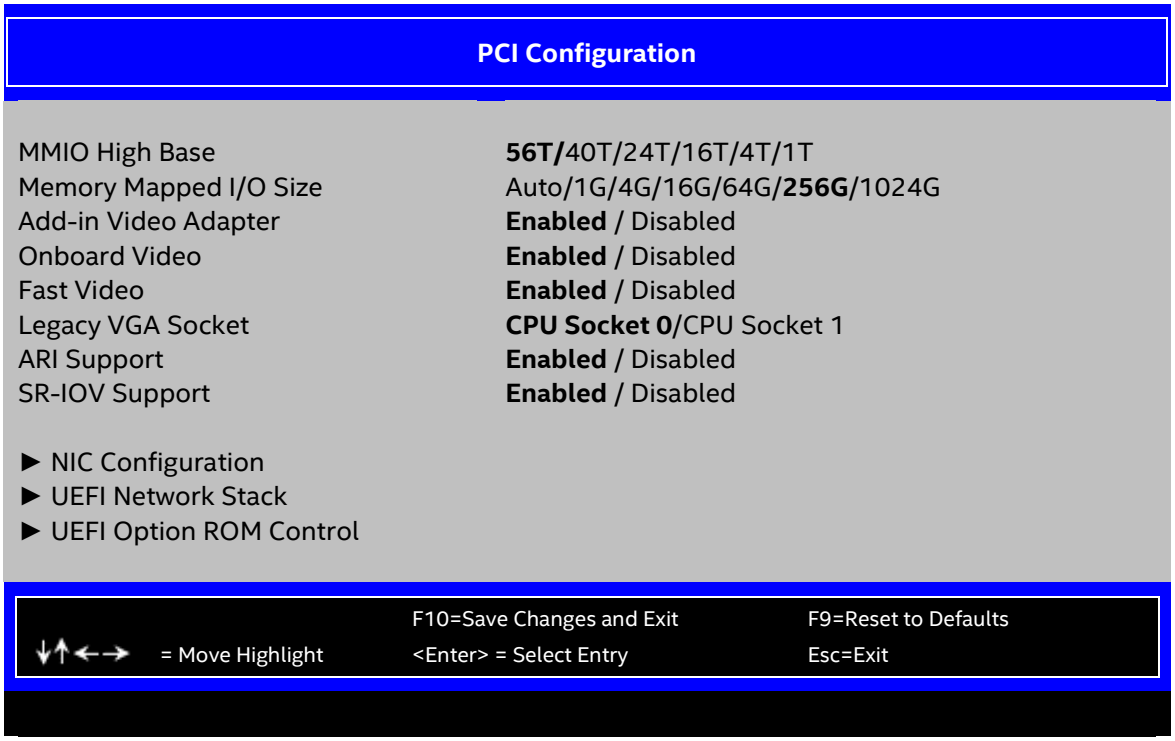

Figure 34. PCI Configuration Screen

6. **MMIO High Base**

   Value: **56T**/40T/24T/16T/4T/1T

   Help text: `Select MMIO High Base`

   Comments: This option selects the MMIO high base address. Default value is 56T.

   Back to: PCI Configuration – Advanced – Screen Map

7. **Memory Mapped I/O Size**

   Value: Auto/1G/4G/16G/64G/**256G**/1024G

   Help text: `Sets the Size of MMIO space above 4GB.`

   Comments: When Memory Mapped I/O above 4GB option enabled, this option sets the preserved MMIO size as PCI/PCIe Memory Mapped I/O for devices capable of 64-bit addressing. The Auto setting automatically calculates the required MMIO size of all add-in PCIe devices and attempts to assign sufficient resources for each device.

   This option is grayed out when Memory Mapped I/O above 4GB option is disabled.

   Note: The system does not work normally if the system requested memory mapped I/O size is greater than the chosen value (1G/4G/16G/64G). This is an expected behavior due to MMIO resource shortage. Change the value to Auto or a larger size.

   Back to: PCI Configuration – Advanced – Screen Map

8. Add-in Video Adapter

Value: **Enabled**/Disabled

Help text: `When Onboard Video is Enabled, and Add-in Video Adapter is also Enabled, both can be active. The onboard video is still the primary console and active during BIOS POST; the add-in video adapter would be active under an OS environment with the video driver support.`

`When Onboard Video is Enabled, and Add-in Video Adapter is Disabled, then only the onboard video would be active.`

`When Onboard Video is Disabled, and Add-in Video Adapter is Enabled, then only the add-in video adapter would be active.`

Comments: This option must be enabled to use an add-in card as a primary POST legacy video device.

If there is no add-in video card in any PCIe slot connected to CPU Socket 0 with the Legacy VGA Socket option set to CPU Socket 0, this option is set to Disabled and grayed out and unavailable.

If there is no add-in video card in any PCIe slot connected to CPU Socket 1 with the Legacy VGA Socket option set to CPU Socket 1, this option is set to Disabled and grayed out and unavailable.

If the Legacy VGA Socket option is set to CPU Socket 0 with both Add-in Video Adapter and Onboard Video enabled, the onboard video device works as primary video device while add-in video adapter as secondary.

Back to: PCI Configuration – Advanced – Screen Map

9. Onboard Video

Value: **Enabled**/Disabled

Help text: `Enable or disable onboard video controller.`

`Warning: System video is completely disabled if this option is disabled and an add-in video adapter is not installed.`

Comments: When disabled, the system requires an add-in video card for the video to be seen. When there is no add-in video card installed, Onboard Video is set to Enabled and grayed out so it cannot be changed.

If there is an add-in video card installed in a PCIe slot connected to CPU Socket 0, and the Legacy VGA Socket option is set to CPU Socket 0, then this Onboard Video option is available to be set and default as Disabled.

If there is an add-in video card installed on a PCIe slot connected to CPU Socket 1, and the Legacy VGA Socket option is set to CPU Socket 1, this option is grayed out and unavailable, with a value set to Disabled. This is because the Onboard Video is connected to CPU Socket 0, and is not functional when CPU Socket 1 is the active path for video. When Legacy VGA Socket is set back to CPU Socket 0, this option becomes available again and is set to its default value of Enabled.

Note: This option does not appear on some models. For product-specific information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

Back to: PCI Configuration – Advanced – Screen Map

10. Fast Video

Value: **Enabled**/Disabled

Help text: `Enable/disable fast video. Fast video allows the screen light up in early phase.`

`Note: Fast Video only appears when Onboard Video is Enabled.`

Comments: None.

Back to: PCI Configuration – Advanced – Screen Map

11. Legacy VGA Socket

Value: **CPU Socket 0**/CPU Socket 1

Help text: `Determines whether Legacy VGA video output is enabled for PCIe slots attached to Processor Socket 0 or 1. Socket 0 is the default.`

Comments: This option is necessary when using an add-in video card on a PCIe slot attached to CPU Socket 1, due to a limitation of the processor IIO. The Legacy video device can be connected through either socket but there is a setting that must be set on only one of the two. This option allows the switch to using a video card in a slot connected to CPU Socket 1.

This option does not appear unless the BIOS is running on a board that has one processor installed on CPU Socket 1 and can potentially have a video card installed in a PCIe slot connected to CPU Socket 1.

This option is grayed out as unavailable and set to CPU Socket 0 unless there is a processor installed on CPU Socket 1 and a video card installed in a PCIe slot connected to CPU Socket 1.When this option is active and is set to CPU Socket 1, then both Onboard Video and Dual Monitor Video are set to Disabled and grayed out as unavailable. This is because the Onboard Video is a PCIe device connected to CPU Socket 0, and is unavailable when the Legacy VGA Socket is set to Socket 1.

Back to: PCI Configuration – Advanced – Screen Map

12. ARI Support

Value: **Enabled**/Disabled

Help text: `Enable or disable the ARI support.`

Comments: None.

Back to: PCI Configuration – Advanced – Screen Map

13. SR-IOV Support

Value: **Enabled**/Disabled

Help text: `Enable or disable the SR-IOV support.`

Comments: None.

Back to: PCI Configuration – Advanced – Screen Map

14. NIC Configuration

Value: None.

Help text: `View/Configure NIC information and settings.`

Comments: *Selection only*. For more information on NIC Configuration settings, see Section3.3.8.1.

Note: This field cannot support changes through Intel® Server Configuration Utility with the `/bcs` command and cannot support Intel® Firmware Customization.

Back to: PCI Configuration – Advanced – Screen Map

15. UEFI Network Stack

Value: None.

Help text: `View/Configure UEFI Network Stack control settings.`

Comments: *Selection only*. For more information on UEFI Network Stack settings, see Section3.3.8.2.

Back to: PCI Configuration – Advanced – Screen Map

16. UEFI Option ROM Control

Value: None.

Help text: `View/Configure UEFI Oprom control settings.`

Comments: *Selection only*. For more information on UEFI Option ROM Control settings, see Section 3.3.8.3.

Note: This field cannot support changes through Intel® Server Configuration Utility with the `/bcs` command and cannot support Intel® Firmware Customization.

Back to: PCI Configuration – Advanced – Screen Map

3.3.8.1 NIC Configuration

The NIC Configuration screen allows the user to configure the network interface card (NIC) controller options for BIOS POST. This NIC Configuration screen handles network controllers built in on the baseboard (onboard). It does not configure or report anything related to add-in network adapter cards.

To access this screen from the front page, select **Advanced** > **PCI Configuration** > **NIC Configuration**. Press the **<Esc>** key to return to the PCI Configuration screen.

There is usually one onboard NIC built into the baseboard, although in some cases two onboard NICs are available. Several possible types of NICs can be incorporated into different boards.

Note: The fields on the NIC Configuration screen do not support changes through Intel® Server Configuration Utility with the `/bcs` command and do not support Intel® Firmware Customization.

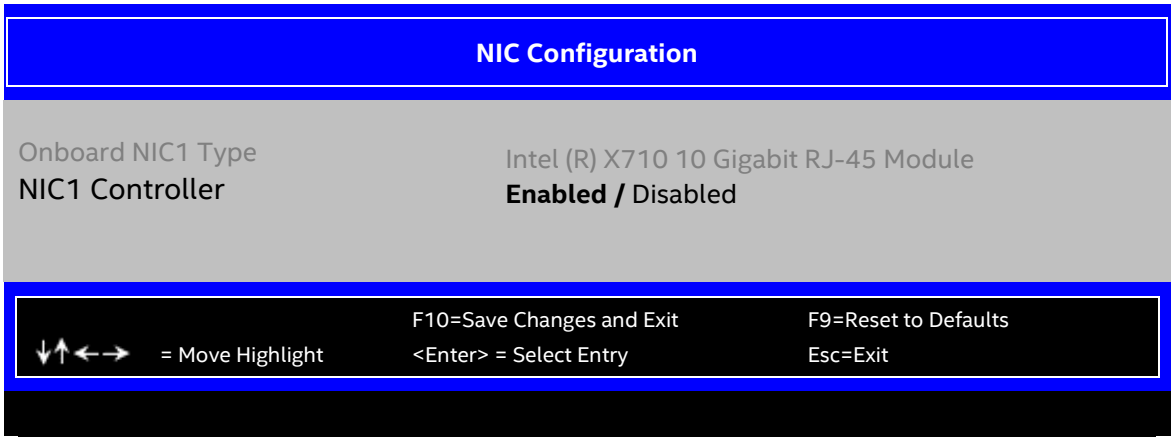

Figure 35. NIC Configuration Screen

1. **Onboard NIC1 Type**

   Value: Intel (R) X710 10 Gigabit RJ-45 Module

   Help text: None.

   Comments: *Information only*. This is a display showing which NICs are available as network controllers integrated into the baseboard. The NIC description is:

   ```
   Intel(R) X710 10 Gigabit RJ-45 Module
   ```

   For details about the NIC hardware configuration for a specific board, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 11.

   The Intel® Server Board D50DNP1SB board only supports an onboard X710 10 Giga controller and one NIC port. So the NIC1 controller option designates this NIC port enabling/disabling.

   The Intel® Server Board M50FCP2SBSTD board does not support an onboard NIC controller by default.

   Back to: NIC Configuration – PCI Configuration – Advanced – Screen Map

2. **NIC1 Controller**

   Value: **Enabled**/Disabled

   Help text: `Enable/Disable Onboard Network Controller.`

   Comments: This option completely disables the onboard network controller NIC1, along with all included NIC ports and their associated options.

   Back to: NIC Configuration – PCI Configuration – Advanced – Screen Map

3.3.8.2 UEFI Network Stack

The UEFI Network Stack screen provides access to network devices while executing in the Unified Extensible Firmware Interface (UEFI) boot services environment. This stack follows the UEFI Specification Version 2.3.1.

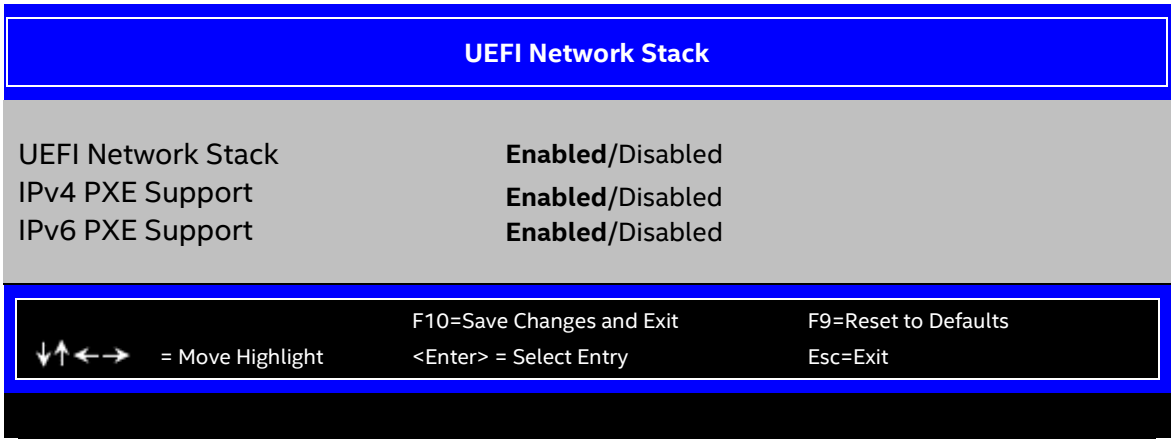

Figure 36. UEFI Network Stack Screen

1. **UEFI Network Stack**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable the whole UEFI Network Stack.`

   Comments: Disabling the UEFI Network Stack disables the network protocols defined in UEFI specifications v2.3.1.

   Back to: UEFI Network Stack – PCI Configuration – Advanced – Screen Map

2. **IPv4 PXE Support**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable IPv4 PXE Support in the UEFI Network Stack.`

   Comments: This option is not accessible if UEFI Network Stack is disabled. Enabling IPv4 PXE support is required to perform built-in UEFI PXE functionality.

   Back to: UEFI Network Stack – PCI Configuration – Advanced – Screen Map

3. **IPv6 PXE Support**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable IPv6 PXE Support in the UEFI Network Stack.`

   Comments: This option is not accessible if UEFI Network Stack is disabled. Enabling IPv6 PXE Support is required to perform built-in UEFI PXE functionality.

   Back to: UEFI Network Stack – PCI Configuration – Advanced – Screen Map

3.3.8.3 UEFI Option ROM Control

The UEFI Option ROM Control configuration screen is brought by the EFI PCI option ROM compliant with the Human Interface Infrastructure (HII) Specification 2.3.1. Those configuration settings are provided by third-party PCI device provider and not controlled directly by the BIOS. The BIOS parses the HII package provided by the EFI PCI Option ROM and groups them with their ClassID into this screen. Four groups are designed for network controller, storage controller, fiber channel, and other controller types. The BIOS also puts the Driver Health configuration pages behind the option ROM.

Note: The fields on the UEFI Option ROM Control screen do not support changes through Intel® Server Configuration Utility with the `/bcs` command and do not support Intel® Firmware Customization.

To identify each option ROM with the physical device's location, the BIOS attaches the SlotID to them. The SlotID is designed based on various products' configuration that covers onboard devices, I/O modules, storage modules, and riser slots. Table 4 defines how to translate the SlotID into the physical address.

Table 4. Slot ID and Physical Address

HII Name	Expansion	Type	Subtype	Slot
Bit location	12:10	9:8	7:4	3:0
No slots	00 – Reserved	0	0	0
Internal slot	00 – Reserved	1	0 = Internal slots	0:F = Slot number
External box slots	00 – Reserved	1	1:F = External box number	0:F = Possible slots per box
IO Module	00 – Reserved	2	0 = IO Module	0:F = IOM Number
Storage module	00 – Reserved	2	1 = Storage module	0:F = Storage module number
Riser slot	00 – Reserved	3	0:F = 16 possible risers	0:F = Possible slots per riser

Figure 38 is an example for the UEFI Option ROM Control screen. The exact content changes according to the system configuration.

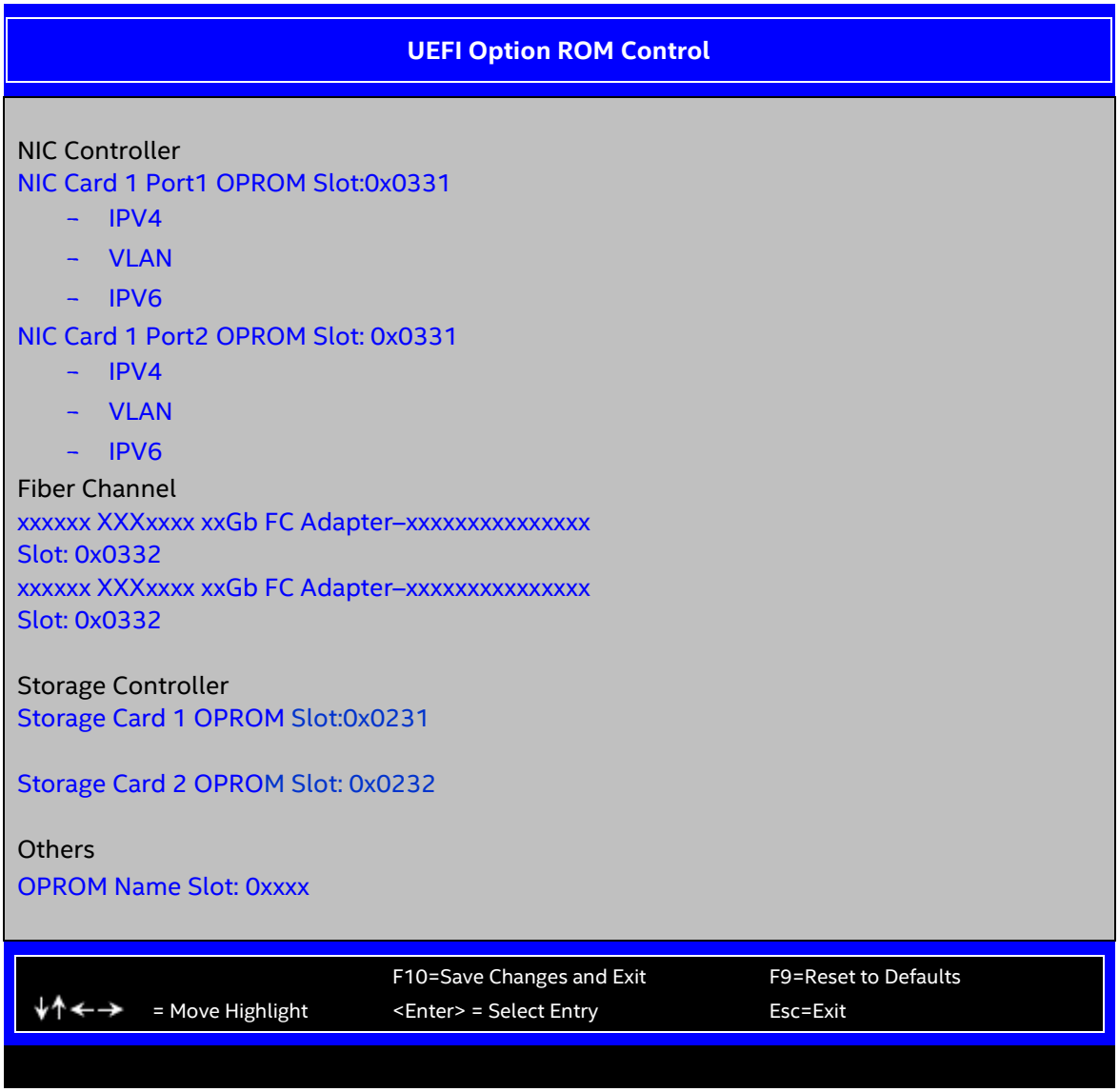

Figure 37. UEFI Option ROM Control Screen

Note: This document does not describe configuration items brought by EFI PCI option ROMs as their appearance depends on the PCI device vendor, which is out of the baseboard BIOS scope.

3.3.9 Serial Port Configuration

The Serial Port Configuration screen allows the user to configure the Serial A port. In legacy Industry Standard Architecture (ISA) nomenclature, these are ports COM1 and COM2, respectively.

To access this screen from the front page, select **Advanced** > **Serial Port Configuration**. Press the **<Esc>** key to return to the advanced screen.

The primary usage for these serial ports is to enable serial console redirection and serial-over-LAN (SOL) capabilities. Either port can be used for Serial Console Redirection, but SOL is only supported on Serial A. For more information on console redirection, see Section3.5.1.

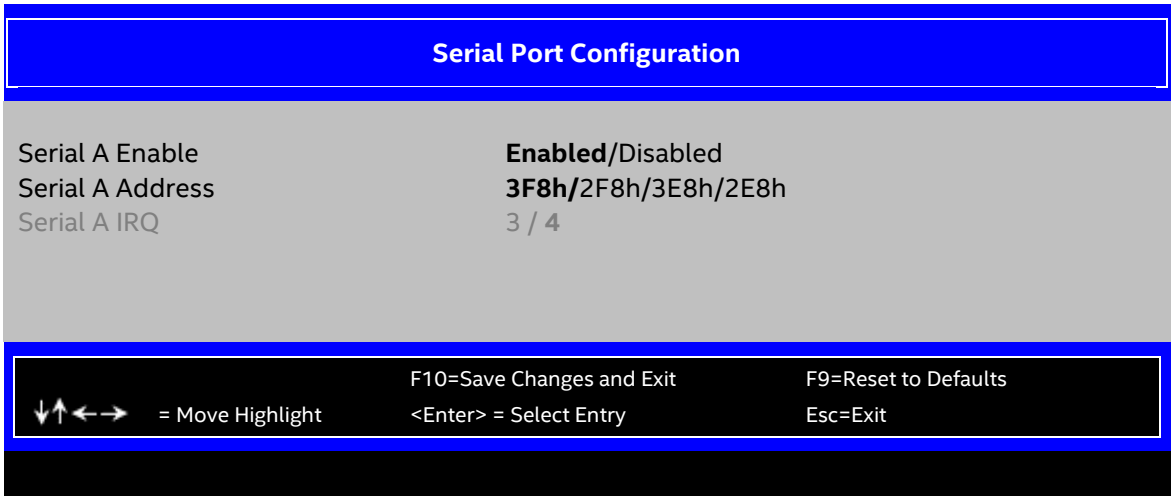

Figure 38. Serial Port Configuration Screen

1. **Serial A Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable Serial port A.`

   Comments: Serial port A can be used for either serial-over-LAN or serial console redirection.

   Back to: Serial Port Configuration – Advanced – Screen Map

2. **Serial A Address**

   Value: **3F8h**/2F8h/3E8h/2E8h

   Help text: `Select Serial port A base I/O address.`

   Comments: Legacy I/O port address. This field does not appear when Serial A port enable/disable does not appear.

   Note: The Serial A Address and Serial B Address cannot be set to the same value.

   Back to: Serial Port Configuration – Advanced – Screen Map

3. **Serial A IRQ**

Value: 3/**4**

Help text: `Select Serial port A interrupt request (IRQ) line.`

Comments: Legacy interrupt request (IRQ). This field does not appear when Serial A port enable/disable does not appear. It is gray because AST2500 UART IRQ is fixed under ESPI mode, and such option does not support Intel Firmware Customization on the Intel Server Boards M50FCP and D50DNP.

Back to: Serial Port Configuration – Advanced – Screen Map

3.3.10 USB Configuration

The USB Configuration screen allows the user to configure the available USB controller options.

To access this screen from the front page, select **Advanced** > **USB Configuration**. Press the **<Esc>** key to return to the Advanced screen.

Each USB mass storage device may be set to allow the media emulation for which it is formatted, or an emulation may be specified. For USB flash memory devices in particular, these restrictions apply:

- A USB key formatted as a CD-ROM drive is recognized as an HDD.
- A USB key formatted without a partition table is forced to FDD emulation.
- A USB key formatted with one partition table and less than 528 MB in size is forced to FDD emulation; otherwise, if it is 528 MB or greater in size, it is forced to HDD emulation.

Note: USB devices can be hot plugged during POST, and are detected, enumerated, and work under operating system environment. They are not displayed on this screen or enumerated as bootable devices.

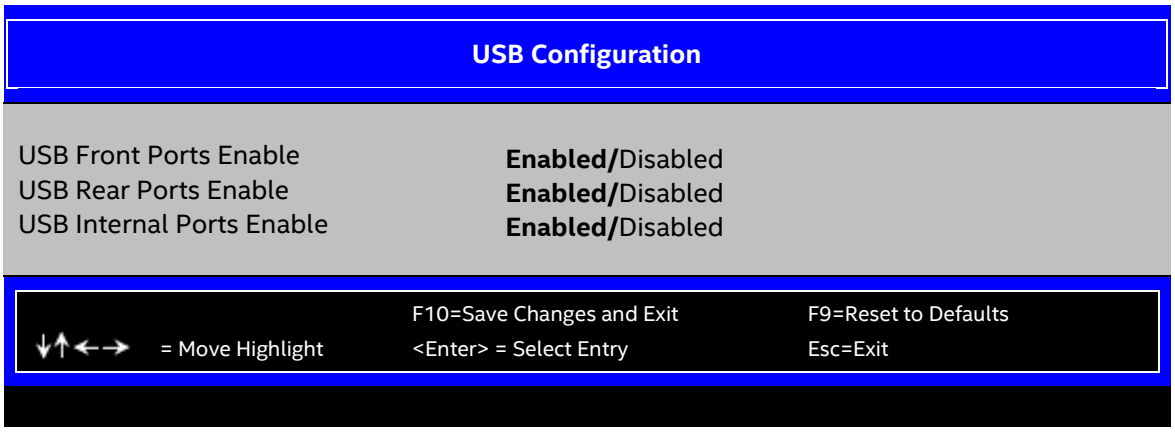

Figure 39. USB Configuration Screen

1. **USB Front Ports Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or disable the USB Front Ports`

   Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

   Back to: USB Configuration – Advanced – Screen Map

2. **USB Rear Ports Enable**

   Value: **Enabled**/Disabled

Help text: `Enable or disable the USB Rear Ports`

Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

Back to: USB Configuration – Advanced – Screen Map

3. **USB Internal Ports Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or disable the USB Internal and BMC Ports`

   Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

   Back to: USB Configuration – Advanced – Screen Map

3.3.11 System Acoustic and Performance Configuration

The System Acoustic and Performance Configuration screen allows the user to configure the thermal control behavior of the system with respect to the parameters used in the system's fan speed control algorithms.

To access this screen from the front page, select **Advanced** > **System Acoustic and Performance Configuration**. Press the **<Esc>** key to return to the Advanced screen.

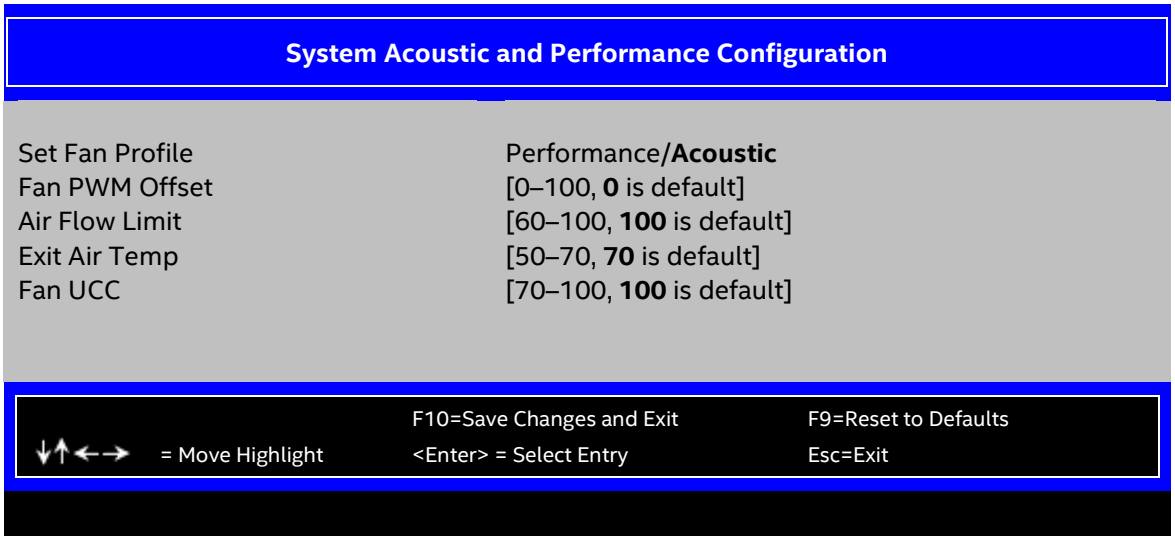

Figure 40. System Acoustic and Performance Configuration Screen

1. **Set Fan Profile**

   Value: Performance/**Acoustic**

   Help text: `[Performance] – Fan control provides primary system cooling before attempting to throttle memory.`

   `[Acoustic] – The system will favor using throttling of memory over boosting fans to cool the system if thermal thresholds are met.`

   Comments: This option allows the user to choose a fan profile that is optimized for maximizing performance or for minimizing acoustic noise.

   When Performance is selected, the system thermal conditions are controlled by raising fan speeds when necessary. This provides cooling without impacting system performance but may impact system acoustic performance as fans running faster are typically louder.

When Acoustic is selected, the system attempts first to control thermal conditions by throttling memory to reduce heat production. This regulates the system's thermal condition without changing the acoustic performance, but throttling memory may impact system performance.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, Set Fan Profile should get from BMC via IPMI but not from BIOS variable via `/bcs`. This option is required to support Intel Firmware Customization.

Back to: System Acoustic and Performance Configuration – Advanced – Screen Map

2. Fan PWM Offset

Value: [Entry Field 0–100]

Help text: `Valid Offset 0-100. This number is added to the calculated PWM value to increase Fan Speed.`

Comments: This is a percentage by which the calculated fan speed is increased. The user can apply a positive offset that results in increasing the minimum fan speeds.

At each system boot, BIOS queries the BMC for the current PWM offset setting and displays this in the BIOS setup utility.

This PWM offset setting is specified through the BIOS setup utility and is applicable to both Intel® Server Chassis and third-party chassis, however the BMC firmware is the owner of the PWM offset setting. Only if a user changes the BIOS setting for the PWM offset does the BIOS send the new setting to the BMC.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, Set Fan Profile should get from BMC via IPMI but not from BIOS variable via `/bcs`. This option does not support Intel® Firmware Customization.

Back to: System Acoustic and Performance Configuration – Advanced – Screen Map

3. Air Flow Limit

Value: [Entry Field 60–100, **100** is default]

Help text: `System CFM Limit. BIOS valid range 60-100. This set the maximum allowable system CFM under normal operating conditions. This value will be ignored during error conditions such as a fan failure or a critical temperature event. The value in this item is percentage of max CFM. The resolution is 1%.`

Comments: On each boot, the BIOS sends a `Get FSC Parameter` IPMI command to the BMC to read, and then shows it at setup. The BMC owns the policy. If the user changes this value at setup, the BIOS sends a `Set FSC Parameter` command to BMC immediately.

Get FSC parameter gets the max system CFM. So this option value's scope is 60% to 100%. The user selection cannot be out of scope.

Table 5. Set FSC Parameter and Get FSC Parameter Commands for Air Flow Limit Option

NetFn 0x30	Request	Response	Notes
Set FSC Parameter – 0x90	Byte 1 – Parameter number Byte 2:n – Varies based on parameter number Parameter 4 – System CFM Limit Byte 2:3 – CFM in cf/min	Byte 1 – Completion code	Byte 1 is 4 in request.
Get FSC Parameter – 0x91	Request: Byte 1 – Parameter number Byte 2:n – Varies based on parameter number	Byte 1 – Completion code Byte 2:n – Varies based on parameter number Parameter 4 – System CFM Limit Byte 2:3 – CFM limit in cf/min Bytes 4:5 – Maximum system CFM in cf/min	Byte 1 is 4 in request.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, Set Fan Profile should get from BMC via IPMI but not from BIOS variable via `/bcs`. This option does not support Intel® Firmware Customization.

Back to: System Acoustic and Performance Configuration – Advanced – Screen Map

4. Exit Air Temp

Value: [Entry Field 50–70]

Help text: `Exit Air temperature. BIOS valid range 50-70. This is to give MAX exit air temperature to BMC.`

Comments: On each boot, BIOS reads the value from the BMC as the BMC owns the policy. So default setting is got from BMC through IPMI command. If the user changes the value at setup, BIOS sends the value to BMC immediately. If the BMC has no response when reading, BIOS hides this item. This option is suppressed on M50FCP 2U and D50DNP 1U/2U systems. For details, please refer to BMC EPS "Exit Air Temperature Sensor".

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Table 6. Set FSC Parameter and Get FSC Parameter Commands for Exit Air Temp Option

NetFn 0x30	Request	Response	Notes
Set FSC Parameter – 0x90	Byte 1 – Parameter number Byte 2:n – Varies based on parameter number Parameter 1 – Tcontrol Byte 2 – Sensor number (0x2e) Byte 3 – Tcontrol value	Byte 1 – Completion code	Byte1 is 1 in request.
Get FSC Parameter – 0x91	Request: Byte 1 – Parameter number Byte 2:n – Varies based on parameter number	Byte 1 – Completion code Byte 2:n – Varies based on parameter number	Byte1 is 1 in request.

	Parameter 1 Byte 2 – Sensor number(0x2e)	Parameter 1 – Tcontrol Byte 2 – Tcontrol modifier value Byte 3 – Tcontrol SDR value	

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, Set Fan Profile should get from BMC via IPMI but not from BIOS variable via `/bcs`. This option does not support Intel® Firmware Customization.

Back to: System Acoustic and Performance Configuration – Advanced – Screen Map

5. Fan UCC

Value: [Entry Field 70–100, **100** is default]

Help text: `Max domain PWM. BIOS valid range 70-100. This set the absolute maximum fan PWM for the domain.`

Comments: On each boot, the BIOS reads the value from the BMC as the BMC owns the policy. At one system, several fan domains are available. This item is not for a specific domain or individual domain. It is for total domain. If the user changes the value at Setup, BIOS sends the value to the BMC immediately. If the BMC has no response when reading, BIOS hides this item.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Table 7. Set FSC Parameter and Get FSC Parameter Commands for Fan UCC Option

NetFn 0x30	Request	Response	Notes
Set FSC Parameter – 0x90	Byte 1 – Parameter number Byte 2:n – Varies based on parameter number Parameter 3 – Max domain PWM Byte 2 – Domain mask Byte 3 – Max PWM	Byte 1 – Completion code	Byte1 is 3 in request. Byte2 is 0xff for all domains.
Get FSC Parameter – 0x91	Request: Byte 1 – Parameter number Byte 2:n – Varies based on parameter number	Byte 1 – Completion code Byte 2:n – Varies based on parameter number Parameter 3 – Max domain PWM Byte 2:9 – Max PWM for each domain 0–7	Byte1 is 3 in request. BIOS uses domain 0 value for setup item.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, Set Fan Profile should get from BMC via IPMI but not from BIOS variable via `/bcs`. This option does not support Intel® Firmware Customization.

Back to: System Acoustic and Performance Configuration – Advanced – Screen Map

3.4 Security Screen

The Security screen allows the user to enable and set the administrator and user passwords and to lock out the front panel buttons so they cannot be used. This screen also allows the user to enable and activate the Trusted Platform Module (TPM) security settings on those boards that support TPM.

Note that it is necessary to activate the TPM to enable Intel® Trusted Execution Technology (Intel® TXT) on server boards that support it. Changing the TPM state in setup requires a hard reset for the new state to become effective. For enabling Intel TXT, see the Processor Configuration screen in Section 0.

This BIOS supports (but does not require) strong passwords for security. The strong password criteria for both administrator and user passwords require that passwords be from 8 through 32 characters in length, and a password must contain at least one case-sensitive alphabetical character, one numeric character, and one special character. A warning is given when a password is set which does not meet the strong password criteria, but the password is accepted.

For further security, the BIOS optionally may require a power on password to be entered in early POST to boot the system. When the Power-on Password option is enabled, POST is halted soon after power-on while the BIOS queries for a power on password. Either the administrator or the user password may be entered for a power on password.

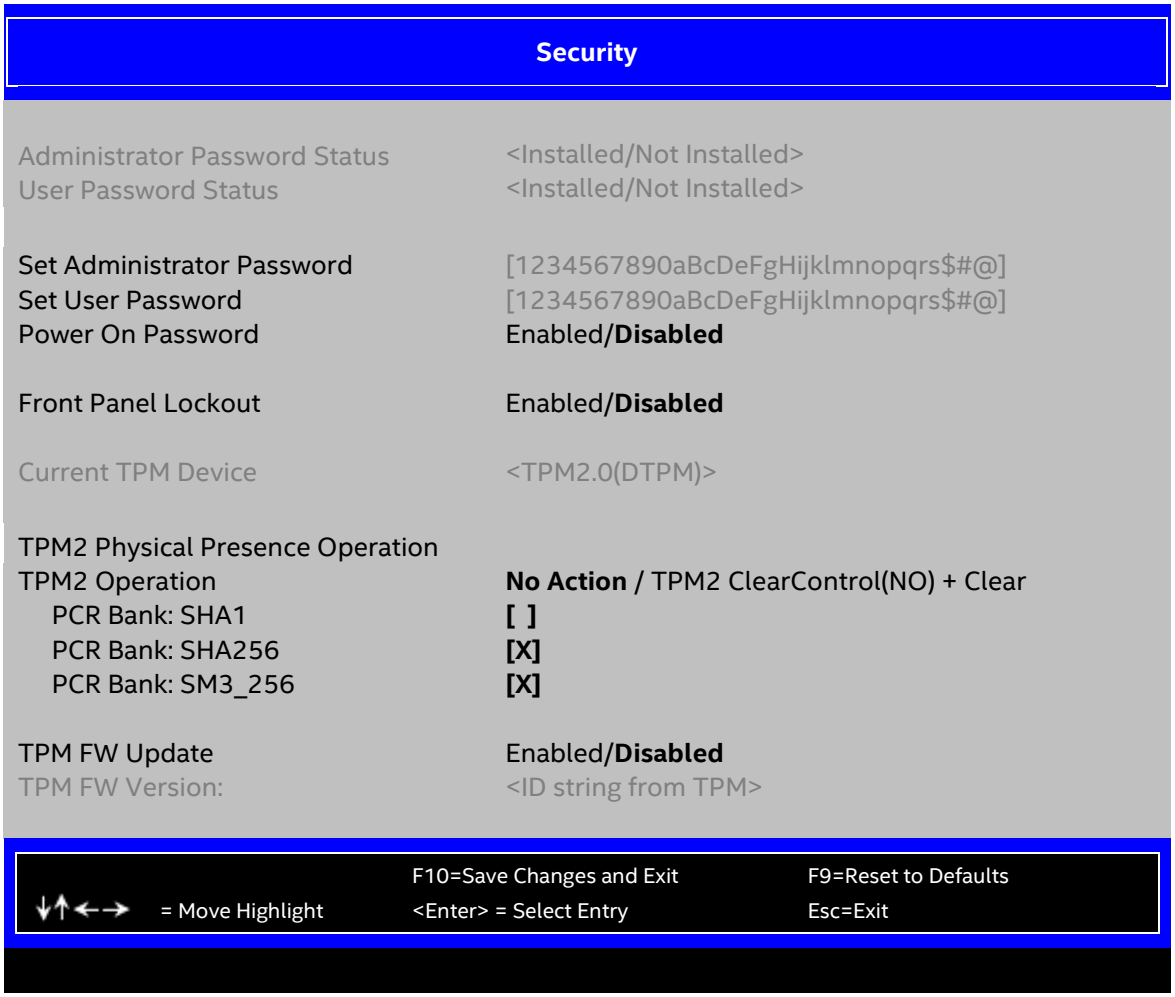

Figure 41. Security Screen

1. **Administrator Password Status**

   Value: <Installed/Not Installed>

   Help text: None.

   Comments: *Information only*. Indicates the status of the administrator password.

Note: This field does not support Intel® Server Configuration Utility display with the `/bcs` command.

Back to: Security – Screen Map

2. **User Password Status**

   Value: <Installed/Not Installed>

   Help text: None.

   Comments: *Information only*. Indicates the status of the user password.

   Note: This field does not support Intel® Server Configuration Utility display with the `/bcs` command.

   Back to: Security – Screen Map

3. **Set Administrator Password**

   Value: [Entry Field – 8–32 characters]

   Help text: `Administrator password is used if Power On Password is enabled and to control change access in BIOS Setup. Length is 8-32 characters. Case sensitive alphabetic, numeric and special characters !@#$%^&*()-_+=? are allowed. The change of this option will take effect immediately.`

   `Note: Administrator password must be set in order to use the User account.`

   Comments: This password controls change access to setup. The administrator has full access to change settings for any setup options, including setting the administrator and user passwords.

   When Power On Password protection is enabled, the administrator password may be used to allow the BIOS to complete POST and boot the system.

   This password is a null string when the password is not set or the password entry field is cleared. Clearing the administrator password also clears the user password.

   If invalid characters are present in the entered password, it is not accepted and there is a dialog with an error message:

   ```
   Password entered is not valid. Only case sensitive alphabetical, numeric, and special characters !@#$%^&*()-_+=? are allowed. Length should be at least 8 characters.
   ```

   The administrator and user passwords must be different. If the password entered is the same as the user password, it is not accepted and there is a dialog with an error message:

   ```
   Password entered is not valid. New password must be different from previous 5 Administrator and User passwords.
   ```

   Strong passwords are encouraged, although not mandatory. If a password is entered which does not meet the strong password criteria, there is a popup warning message:

   ```
   Warning – a Strong Password should include at least one each case sensitive alphabetical, numeric, and special character. Length should be 8 to 32 characters.
   ```

   For full details on BIOS password protection, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.1.

Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bap` command can be used to set the administrator password.

Back to: Security – Screen Map

4. **Set User Password**

   Value: [Entry Field – 8–32 characters]

   Help text: `User password is used if Power On Password is enabled and to allow restricted access to BIOS Setup. Length is 8-32 characters. Case sensitive alphabetic, numeric and special characters !@#$%^&*()-_+=? are allowed. The change of this option will take effect immediately.`

   `Note: Removing the administrator password also removes the user password.`

   Comments: The user password is available only if the administrator password has been installed. This option protects setup settings and boot choices. The user password only allows limited access to the setup options, and no choice of boot devices.

   When Power On Password protection is enabled, the user password may be used to allow the BIOS to complete POST and boot the system.

   The password format and entry rules and popup error and warning message are the same for the user password as for the administrator password (see previous field description number 3).

   For full details of BIOS password protection, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.1.

   Note: This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bup` command can be used to set the user password.

   Back to: Security – Screen Map

5. **Power On Password**

   Value: Enabled/**Disabled**

   Help text: `Enable Power On Password support. If enabled, password entry is required in order to boot the system.`

   Comments: When Power-on Password security is enabled, the system halts soon after power-on, and the BIOS asks for a password before continuing POST and booting. Either the administrator or user password may be used.

   If an administrator password has not been set, this option is grayed out and unavailable. Removing the administrator password also disables this option.

   Back to: Security – Screen Map

6. **Front Panel Lockout**

   Value: Enabled/**Disabled**

Help text: `If enabled, locks the power button OFF function and the reset and NMI Diagnostic Interrupt buttons on the system's front panel. If [Enabled] is selected, power-off and reset must be controlled via a system management interface, and the NMI Diagnostic Interrupt is not available.`

Comments: None.

Back to: Security – Screen Map

7. Current TPM Device

Value: TPM2.0(DTPM)

Help text: None.

Comments: *Information only*. Shows the current TPM device. If the current TPM device is DTPM, TPM2.0(DTPM) is shown. If there is no TPM device, this information is not shown.

Back to: Security – Screen Map

8. TPM2 Operation

Value: **No Action**/TPM2 ClearControl(NO) + Clear

Help text: `Select one of the supported operation to change TPM2 state.`

Comments: Any TPM2 operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.2.

If an administrator password has not been set, this option is grayed out and unavailable.

Back to: Security – Screen Map

9. PCR Bank: SHA1

Value: [Check box]

Help text: `TCG2 Request PCR Bank: SHA1`

Comments: Use check box to select the TPM active PRC bank. Any TPM2 operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.2.

If an administrator password has not been set, this option is grayed out and unavailable.

Back to: Security – Screen Map

10. PCR Bank: SHA256

Value: [Checkbox]

Help text: `TCG2 Request PCR Bank: SHA256`

Comments: Use check box to select the TPM active PRC bank. Any TPM2 operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.2.

If an administrator password has not been set, this option is grayed out and unavailable.

Back to: Security – Screen Map

11. PCR Bank: SM3_256

Value: [Checkbox]

Help text: `TCG2 Request PCR Bank: SM3_256`

Comments: Use check box to select the TPM active PRC bank. Any TPM2 operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 9.2.

If an administrator password has not been set, this option is grayed out and unavailable.

Back to: Security – Screen Map

Notes:

TPM2 Operation, PCR Bank: SHA1 and PCR Bank : SHA256 appear only on boards equipped with a TPM. SM3_256 only works on a TPM module with SM3 capability (Like TPM module - China).

User should keep one PCR Bank checked when do PCR bank modification, otherwise the warning message shows up like “Warning – Need one PCR Bank active. Press ENTER to continue...”. See the BIOS EPS for the Intel® Server Boards M50FCP and D50DNP, Section 11 for Product-Specific Information about TPM availability.

TPM2 Operation, PCR Bank : SHA1 and PCR Bank : SHA256 options do not support BIOS customization utilities (Intel® Server Configuration Utility or Intel® Firmware Customization). This can only be changed within the setup menus of the target system.

12. TPM FW Update

Value: Enabled/**Disabled**

Help text: `Enable/disable Update TPM firmware.`

Comments: If an administrator password has not been set, this option is grayed out and unavailable.

Back to: Security – Screen Map

13. TPM FW Version:

Value: ID String for TPM

Help text: `Show current TPM FW Version.`

Comments: *Information only*. Displays TPM firmware version string read from TPM. This is displayed only if the TPM FW Update option is enabled.

Back to: Security – Screen Map

3.5 Server Management Screen

The Server Management screen allows the user to configure several server management features. This screen also provides an access point to the screens for configuring console redirection, displaying system information, and controlling the BMC LAN configuration.

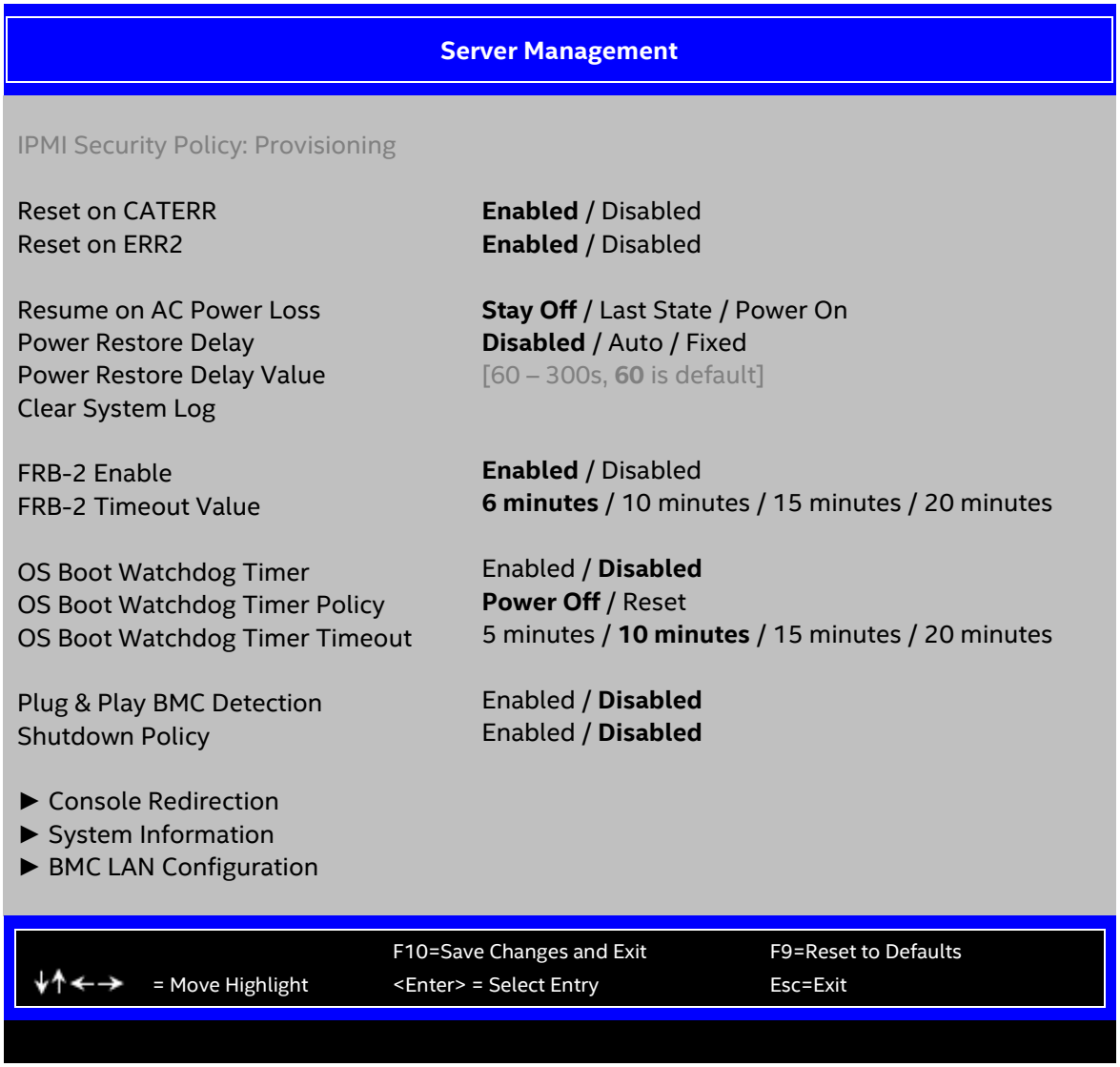

Figure 42. Server Management Screen

1. **IPMI Security Policy**

   Value: **Provisioning**/Provisioned Host Allowlist/Provisioned Host Disabled

   Help text: `Shows current IPMI Security Policy information.`

   Comments: This option shows the IPMI Security Policy information that the BMC is set to be functioning and if it is functioning in any mode out of Provisioning, Provisioned Host Allowlist and Provisioned Host Disabled. This information is suppressed if the BMC is functioning on any Unknown state.

   Back to: Server Management – Screen Map

2. **Reset on CATERR**

   Value: **Enabled**/Disabled

   Help text: `When enabled system gets reset upon encountering Catastrophic Error (CATERR); when disabled system does not get reset on CATERR.`

   Comments: This option controls whether the system is reset when the catastrophic error `CATERR#` signal is held asserted, rather than just pulsed to generate a system management interrupt (SMI). This indicates that the processor has encountered a fatal hardware error.

Note: If this option is disabled, this can result in a system hang for certain error conditions, possibly with the system unable to update the system status LED or log an error to the SEL before hanging.

Back to: Server Management – Screen Map

3. **Reset on ERR2**

   Value: **Enabled**/Disabled

   Help text: `When enabled system gets reset upon encountering ERR2 (Fatal error); when disabled system does not get reset on ERR2.`

   Comments: This option controls whether the system is reset if the BMC's ERR2 monitor times out meaning that the ERR2 signal has been continuously asserted long enough to indicate that the SMI handler is not able to service the condition.

   Note: If this option is disabled, this can result in a system hang for certain error conditions, possibly with the system unable to update the system status LED or log an error to the SEL before hanging.

   Back to: Server Management – Screen Map

4. **Resume on AC Power Loss**

   Value: **Stay Off**/Last State/Power On

   Help text:
   ```
   System action to take on AC power loss recovery.
   [Stay Off] – System stays off.
   [Last State] – System returns to the same state before the AC power loss.
   [Power On] – System powers on.
   ```

   Comments: This option controls the policy that the BMC follows when AC power is restored after an unexpected power outage. The BMC either holds DC power-off or always turns it on to boot the system, depending on this setting. If this option is set to Last State, the behavior depends on whether the power was on, and the system was running before the AC power went off.

   When this setting is changed in setup, the new setting is sent to the BMC. However, the BMC maintains (owns) this power restore policy setting, and it can be changed independently with an IPMI command to the BMC. The BIOS gets this setting from the BMC early in POST, and also for the Setup Server Management screen.

   This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Notes:
   - The system automatically powers on after doing a CMOS clear when AC is applied because this option does not take effect in this situation.
   - For Intel® Server Configuration Utility, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

   Back to: Server Management – Screen Map

5. **Power Restore Delay**

Value: **Disabled**/Auto/Fixed

Help text: `Allows a delay in powering up after a power failure, to reduce peak power requirements. The delay can be fixed or automatic between 60-300 seconds.`

Comments: When the AC power resume policy (see previous field description number 5) is either Power On or Last State, this option allows a delay to be taken after AC power is restored before the system actually begins to power up. This delay can be either a fixed time or an automatic time meaning that the BIOS selects a randomized delay time of 55-300 seconds when it sends the Power Restore Delay setting to the BMC.

The purpose of this delay is to avoid having all systems draw startup surge power at the same time. Different systems or racks of systems can be set to different delay times to spread out the startup power draws. Alternatively, all systems can be set to Automatic and then each system waits for a random period before powering up.

This option is grayed out and unavailable when the AC power resume policy is Stay Off.

The Power Restore Delay setting is maintained by the BIOS. This setting does not take effect until a reboot is done. Early in POST, the Power Restore Policy is read from the BMC, and if the policy is Power On or Last State, the delay settings are sent to the BMC.

Note that even if the Power Restore Delay setting is disabled, it does not mean it starts to power on the host immediately after AC is applied; it means that the BMC starts to power on the host with no delay after it finishes BMC's IPMI stack initialization. Still, a delay occurs; this delay time depends on how long BMC needs to boot after AC power is restored.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Notes:

- This option applies only to powering on when AC is applied. It has no effect on powering the system up using the power button on the front panel. A DC power-on using the power button is not delayed.
- If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

For additional information about BIOS/BMC power control, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 7.1.3.

Back to: Server Management – Screen Map

6. **Power Restore Delay Value**

Value: [Entry Field 60–300, **60** is default]

Help text: `Fixed time period 60-300 seconds for Power Restore Delay.`

Comments: When the power restore policy is Power On or Last State, and the Power Restore Delay option is set to Fixed, this field specifies the length of the fixed delay in seconds.

When the Power Restore Delay option is set to Disabled or Auto, this field is grayed out and unavailable.

The Power Restore Delay Value setting is maintained by the BIOS. This setting does not take effect until a reboot is done. Early in POST, the power restore policy is read from the BMC

and, if the policy is Power On or Last State, the delay settings are sent to the BMC. When the Power Restore Delay setting is Fixed, this delay value is used to provide the length of the delay.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

Back to: Server Management – Screen Map

7. Clear System Log

Value: None.

Help text: `Clears the System Event Log and Redfish Log if selected. All current entries in SEL will be lost.`
`Note: This option will take effect immediately without reboot.`

Comments: *Selection only*. This option sends a message to the BMC to request it to clear the system event log (SEL) and Redfish log. The log is cleared, and then the clear action itself is logged as an event. This gives the user a time/date when the log was cleared.

After selected, a confirmation pop-up appears. If the Clear System Event Log action is positively confirmed, the BIOS sends a message to the BMC to request it to clear the SEL.

If the Clear System Log action is not confirmed, the BIOS resumes executing setup.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

8. FRB-2 Enable

Value: **Enabled**/Disabled

Help text: `Fault Resilient Boot (FRB).`
`The BIOS programs the BMC watchdog timer for approximately 6 minutes. If the BIOS does not complete POST before the timer expires, the BMC will reset the system.`

Comments: This option controls whether the system is reset if the BMC watchdog timer detects what appears to be a hang during POST. When the BMC watchdog timer is set as a fault resistant booting level 2 (FRB-2) timer, it is initially set to allow six minutes for POST to complete.

However, the FRB-2 timer is suspended during times when some lengthy operations are in progress, like executing option ROMS, during setup, and when the BIOS is waiting for a password or for an input to the BBS Boot Menu. The FRB-2 timer is also suspended while POST is paused with the **<Pause>** key.

For more information on FRB-2 timer operation, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.16.4, 6.1.1.1, and 10.6.3.2.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

9. FRB-2 Timeout Value

Value: **6 minutes**/10 minutes/15 minutes/20 minutes

Help text: If FRB-2 enabled, this is the timeout value that BIOS will use to configure the FRB-2 timer.

Comments: This option controls FRB-2 timer threshold if the BMC watchdog timer detects what appears to be a hang during POST. it is optionally set to 6/10/15/20 minutes for POST to complete.

For more information on FRB-2 timer operation, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.16.4, 6.1.1.1, and 10.6.3.2.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

10. OS Boot Watchdog Timer

Value: Enabled/**Disabled**

Help text: `The BIOS programs the watchdog timer with the timeout value selected. If the OS does not complete booting before the timer expires, the BMC will reset the system and an error will be logged.`
`Requires OS support or Intel Management Software Support.`

Comments: This option controls whether the system sets the BMC watchdog to detect an apparent hang during operating system boot. The BIOS sets the timer before starting the operating system bootstrap load procedure. If the operating system boot watchdog timer times out, then presumably the operating system failed to boot properly.

If the operating system does boot successfully, it must be aware of the operating system boot watchdog timer, and immediately turns it off before it expires. The operating system may turn off the timer or, more often, the timer may be repurposed as an operating system watchdog timer to protect against runtime operating system hangs.

Unless the operating system does have timer-aware software to support the operating system boot watchdog timer, the system is unable to boot successfully with the operating system boot watchdog timer enabled. When the timer expires without having been reset or turned off, the system either resets or powers off repeatedly.

For more information about the FRB-2 timer operation, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Sections 3.16.4, 6.1.1.2, and 10.6.3.3.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

11. OS Boot Watchdog Timer Policy

Value: **Power** Off/Reset

Help text: If the OS watchdog timer is enabled, this is the system action taken if the watchdog timer expires.

[Reset] – System performs a reset.
[Power Off] – System powers off.

Comments: This option is grayed out and unavailable when the OS Boot Watchdog Timer option is disabled.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

12. OS Boot Watchdog Timer Timeout

Value: 5 minutes/**10 minutes**/15 minutes/20 minutes

Help text: `If the OS watchdog timer is enabled, this is the timeout value the BIOS will use to configure the watchdog timer.`

Comments: This option is grayed out and unavailable when the OS Boot Watchdog Timer option is disabled.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

13. Plug & Play BMC Detection

Value: Enabled/**Disabled**

Help text: `If enabled, the BMC will be detectable by OSes which support plug and play loading of an IPMI driver. Do not enable this option if your OS does not support this driver.`

Comments: This option controls whether the operating system server management software is able to find the BMC and automatically load the correct IPMI support software for it. If the operating system does not support plug and play for the BMC, the correct IPMI driver software is not loaded.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

14. Shutdown Policy

Value: Enabled/**Disabled**

Help text: `Enable/Disable Shutdown Policy.`

Comments: This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: Server Management – Screen Map

15. Console Redirection

Value: None.

Help text: `View/Configure Console Redirection information and settings.`

Comments: *Selection only*. For more information on Console Redirection settings, see Section 3.5.1.

Back to: Server Management – Screen Map

16. System Information

Value: None.

Help text: `View System Information.`

Comments: *Selection only*. For more information on System Information settings, see Section 3.5.2.

Back to: Server Management – Screen Map

17. BMC LAN Configuration

Value: None.

Help text: `View/Configure BMC LAN and user settings.`

Comments: Selection only. For more information on BMC LAN Configuration settings, see Section 3.5.3.

Back to: Server Management – Screen Map

3.5.1 Console Redirection

The Console Redirection screen allows the user to enable or disable console redirection for remote system management, and to configure the connection options for this feature.

To access this screen from the front page, select **Server Management** > **Console Redirection**. Press the **<Esc>** key to return to the Server Management screen.

When console redirection is active, all POST and setup displays are in text mode. The text mode POST diagnostic screen is displayed regardless of the Quiet Boot setting. This is due to the limitations of console redirection, which is based on data terminal emulation using a serial data interface to transfer character data.

Console redirection can use either of the two serial ports provided by the SuperIO in the BMC. However, if console redirection is to be coordinated with serial-over-LAN (SOL), the user should be aware that SOL is only supported through serial port A.

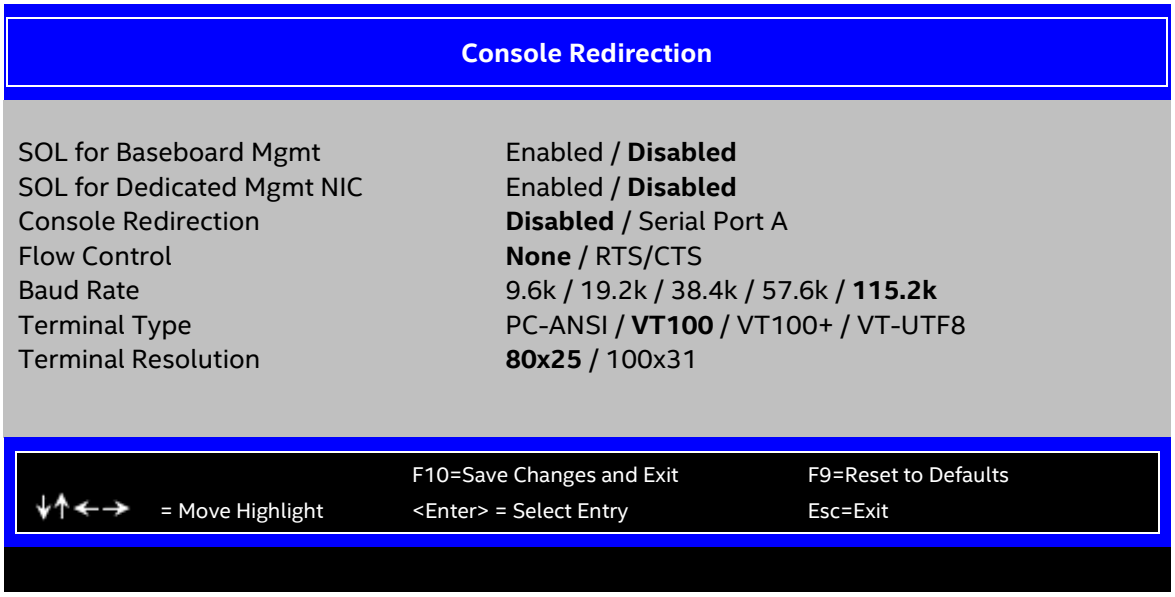

Figure 43. Console Redirection Screen

1. **SOL for Baseboard Mgmt**

   Value: Enabled/**Disabled**

   Help text: `Enable/disable Serial Over LAN feature for Baseboard Management Lan. [Advanced > Serial Port Configuration > Serial A Enable] needs be enabled before enabling this option.`

   Comments: This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   For the Intel® Server Board M50FCP, this item is suppressed if there is no OCP card installed in the system.

   Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`. This field does not support Intel® Firmware Customization.

   Back to: Console Redirection – Server Management – Screen Map

2. **SOL for Dedicated Mgmt NIC**

   Value: Enabled/**Disabled**

   Help text: `Enable/disable Serial Over LAN feature for Dedicated Mgmt NIC. [Advanced > Serial Port Configuration > Serial A Enable] needs be enabled before enabling this option.`

   Comments: This option controls whether the BMC enables or disables the SOL feature on each LAN channel of the system following the IPMI 2.0 Specification. This feature could be re-enabled using the specific IPMI command. For more information, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 7.4. When SOL is enabled and saved, the BIOS automatically updates the console redirection settings to use Serial Port A with 115.2k baud rate, VT100+ terminal type, and RTS/CTS flow control; on the setup screen, console redirection related options are grayed out and keep their previous values.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`. This field does not support Intel® Firmware Customization.

Back to: Console Redirection – Server Management – Screen Map

3. **Console Redirection**

   Value: **Disabled**/Serial Port A

   Help text:
   ```
   Console redirection allows a serial port to be used for server management tasks.
   [Disabled] – No console redirection.
   [Serial Port A] – Configure serial port A for console redirection.
   Enabling this option will disable display of the Quiet Boot logo screen during POST. [Advanced > Serial Port Configuration > Serial A Enable] needs be enabled before enabling this option.
   ```

   Comments: Serial console redirection can use either Serial Port A. Note that SOL is only supported through Serial Port A.

   Only serial ports that are enabled are available to choose for console redirection. If Serial A is not set to Enabled, then the Console Redirection setting is disabled and grayed out as inactive. In that case, all other options on this screen are also grayed out.

Back to: Console Redirection – Server Management – Screen Map

4. **Flow Control**

   Value: **None** / RTS/CTS

   Help text:
   ```
   Flow control is the handshake protocol.
   This setting must match the remote terminal application.
   [None] – Configure for no flow control.
   [RTS/CTS] – Configure for hardware flow control.
   ```

   Comments: Flow control is necessary only when there is a possibility of data overrun. In that case, the Request to Send/Clear to Send (RTS/CTS) hardware handshake is a relatively conservative protocol that can usually be configured at both ends.

Back to: Console Redirection – Server Management – Screen Map

5. **Baud Rate**

   Value: 9.6k/19.2k/38.4k/57.6k/**115.2k**

   Help text:
   ```
   Serial port transmission speed. This setting must match the remote terminal application.
   ```

   Comments: In most modern server management applications, serial data transfer is consolidated over an alternative faster medium like LAN, and 115.2k is the speed of choice.

Back to: Console Redirection – Server Management – Screen Map

6. **Terminal Type**

Value: PC-ANSI/**VT100**/VT100+/VT-UTF8

Help text: `Character formatting used for console redirection. This setting must match the remote terminal application.`

Comments: The VT100 and VT100+ terminal emulations are essentially the same. VT-UTF8 is a UTF8 encoding of VT100+. PC-ANSI is the built-in character encoding used by PC-compatible applications and emulators. For more information about character encoding, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 7.4.

Back to: Console Redirection – Server Management – Screen Map

7. **Terminal Resolution**

Value: **80x25**/100x31

Help text: `Remote Terminal Resolution.`

Comments: This option allows the use of a larger terminal screen area, although it does not change setup displays to match.

Back to: Console Redirection – Server Management – Screen Map

3.5.2 System Information

The System Information screen allows the user to view part numbers, serial numbers, and firmware revisions. This is an information-only screen.

To access this screen from the front page, select **Server Management** > **System Information**. Press the **<Esc>** key to return to the Server Management screen.

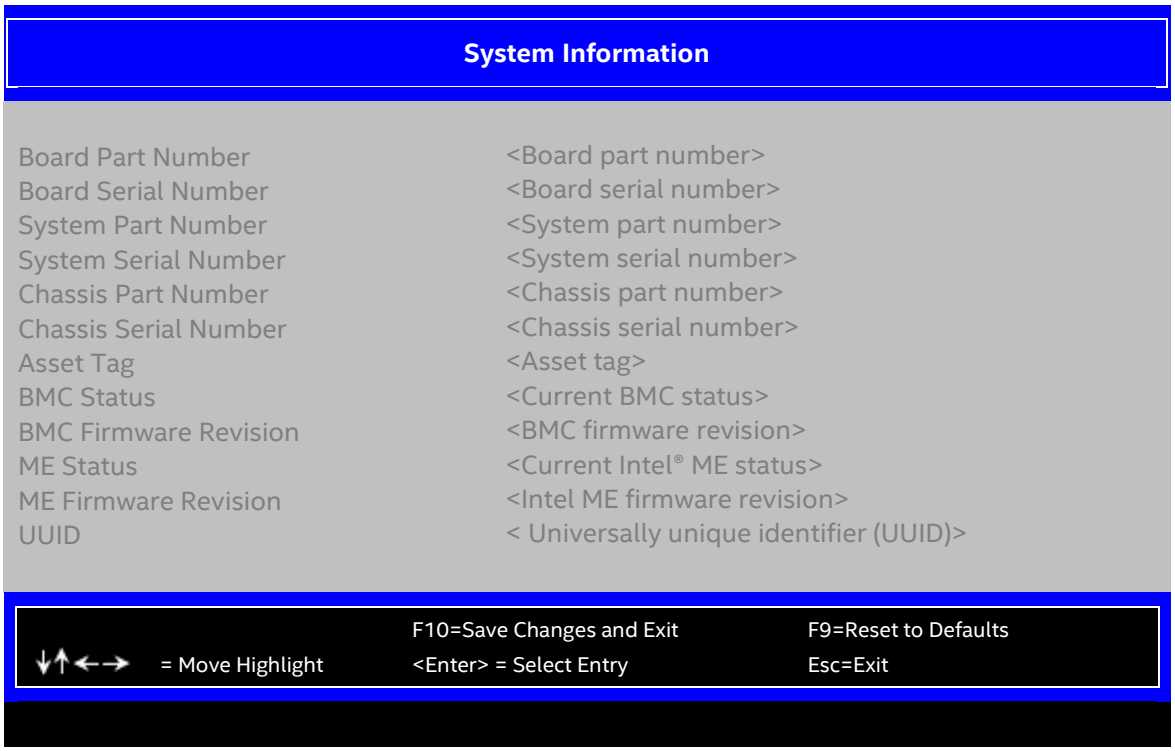

Figure 44. System Information Screen

1. **Board Part Number**

Value: <Board part number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

2. **Board Serial Number**

Value: <Board serial number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

3. **System Part Number**

Value: <System part number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

4. **System Serial Number**

Value: <System serial number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

5. **Chassis Part Number**

Value: <Chassis part number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

6. **Chassis Serial Number**

Value: <Chassis serial number>

Help text: None.

Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

Back to: System Information – Server Management – Screen Map

7. **Asset Tag**

   Value: <Asset tag>

   Help text: None.

   Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

   Back to: System Information – Server Management – Screen Map

8. **BMC Status**

   Value: <Current BMC status>

   Help text: None.

   Comments: *Information only*. This option indicates the BMC status – functional or failed. This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

   Back to: System Information – Server Management – Screen Map

9. **BMC Firmware Revision**

   Value: <BMC firmware revision>

   Help text: None.

   Comments: This information gets suppressed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Disabled.

   Back to: System Information – Server Management – Screen Map

10. **ME Status**

    Value: <Current Intel® Management Engine (Intel® ME) status>

    Help text: None.

    Comments: *Information only*. This option indicates the Intel ME status – functional or failed.

    Back to: System Information – Server Management – Screen Map

11. **ME Firmware Revision**

    Value: <Intel ME firmware revision>

    Help text: None.

    Comments: *Information only*.

    Back to: System Information – Server Management – Screen Map

12. **UUID**

    Value: <Universally unique identifier (UUID)>

    Help text: None.

    Comments: *Information only*.

    Back to: System Information – Server Management – Screen Map

3.5.3 BMC LAN Configuration

The BMC configuration screen allows the user to configure the BMC baseboard LAN channel and a dedicated management LAN channel, and to manage BMC user settings for up to five BMC users.

To access this screen from the front page, select **Server Management** > **BMC LAN Configuration**. Press the **<Esc>** key to return to the Server Management screen.

A Dedicated Management NIC Module (DMN) may be installed in the server system. In that case, the LAN settings for the DMN NIC may be configured.

This screen has a choice of IPv4 or IPv6 addressing. When IPv6 is disabled, only the IPv4 addressing options appear. When IPv6 is enabled, the IPv4 options are grayed out and unavailable, and there is an additional section active for IPv6-addressing. This is true for both the Baseboard LAN configuration and the Dedicated Server Management NIC Module.

IP addresses for either IPv4 or IPv6 addressing can be assigned by static IP addresses manually typed in, or by dynamic IP addresses supplied by a Dynamic Host Configuration Protocol (DHCP) server. IPv6 addressing can also be provided by stateless autoconfiguration that does not require a DHCP server.

The BMC LAN Configuration screen is unusual in that the LAN configuration parameters are maintained by the BMC itself, so this screen is just a user interface to the BMC configuration. As such, the initial values of the LAN options shown on the screen are acquired from the BMC when this screen is initially accessed by a user.

For the default values of the LAN options, to refer to the *BMC EPS for the Intel® Server Boards M50FCP and D50DNP*. Any values changed by the user are communicated back to the BMC when changes are saved. If changes are discarded, any accumulated changes from this screen are disregarded and lost.

This page displays two different messages on the top of the body of the page and options are controlled accordingly depending on the IPMI Security Policy information on Server Management screen. Unable to display some management LAN configuration settings due to IPMI Security Policy message are shown if IPMI Security Policy information being displayed as IPMI Security Policy: Provisioned Host Allowlist; and unable to display management LAN configuration settings due to IPMI Security Policy message if IPMI Security Policy information being displayed as IPMI Security Policy: Provisioned Host Disabled on Server Management screen.

Currently, only NCSI supported LAN that embedded in baseboard can act as BMC LAN, the setup options of IPv4 and IPv6 exposed accordingly.

Note: If Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility support is needed, this all settings under BMC LAN Configuration should get from BMC via IPMI but not from BIOS variable via `/bcs`. These fields on this screen do not support Intel® Firmware Customization.

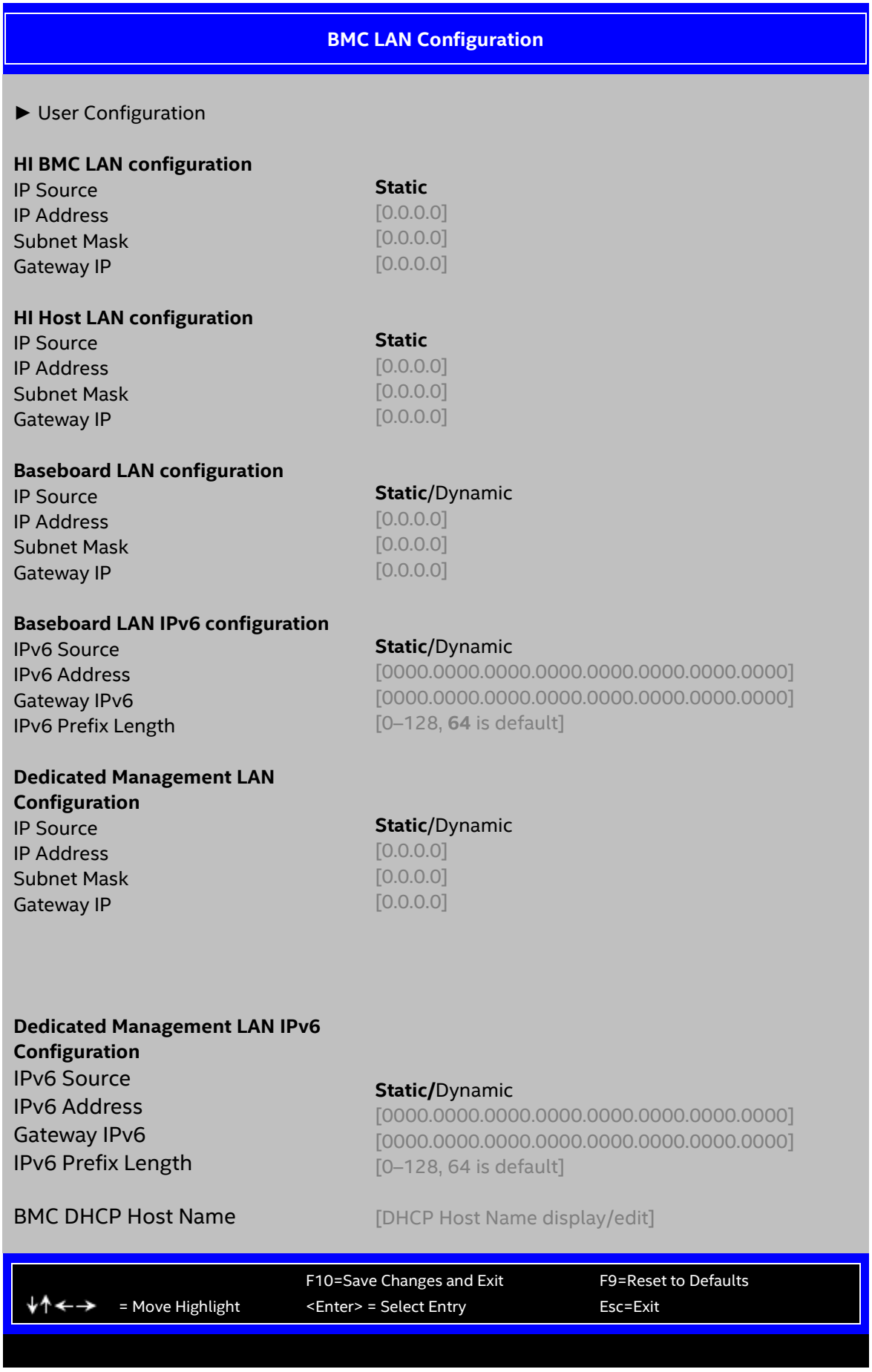

Figure 45. BMC LAN Configuration Screen

1. **User Configuration**

   Value: None.

   Help text: View/Configure User information and settings of the BMC.

   Comments: *Selection only*. For more information on User Configuration settings, see Section 3.5.3.1.

   This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

2. **IP Source**

   Value: **Static**

   Help text: `Select BMC IP Source. If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).`

   Comments: This specifies the IP source for IPv4 addressing for the Redfish* BMC LAN connection. There is a separate IP Source field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

3. **IP Address**

   Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

   Help text: `View/Edit IP Address. Press <Enter> to edit.`

   Comments: This specifies the IPv4 address for the Redfish BMC LAN. There is a separate IPv4 address field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

4. **Subnet Mask**

   Value: [Entry Field 0.0.0.0, 0.0.0.0 is default]

   Help text: View/Edit Subnet Mask. Press <Enter> to edit.

   Comments: This specifies the IPv4 addressing subnet mask for the Redfish BMC LAN. There is a separate IPv4 Subnet Mask field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

5. **Gateway IP**

   Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

   Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

   Comments: This specifies the IPv4 addressing gateway IP for the Redfish BMC LAN. There is a separate IPv4 addressing gateway IP field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

6. **IP Source**

   Value: **Static**

   Help text: `Select BMC IP Source. If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).`

   Comments: This specifies the IP source for IPv4 addressing for the Redfish Host LAN connection. There is a separate IP Source field for the HI Host LAN configuration.

   When IPv4 addressing is used, the initial value for this field is configured by user.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

7. **IP Address**

   Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

   Help text: View/Edit IP Address. Press <Enter> to edit.

   Comments: This specifies the IPv4 address for the Redfish Host LAN. There is a separate IPv4 address field for the HI Host LAN configuration.

   When IPv4 addressing is used, the initial value for this field is configured by the user.

   This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

   Back to: BMC LAN Configuration – Server Management – Screen Map

8. **Subnet Mask**

   Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

   Help text: `View/Edit Subnet Mask. Press <Enter> to edit.`

   Comments: This specifies the IPv4 addressing subnet mask for the Redfish Host LAN. There is a separate IPv4 Subnet Mask field for the HI Host LAN configuration.

When IPv4 addressing is used, the initial value for this field is configured by user.

This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

9. Gateway IP

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing gateway IP for the Redfish Host LAN. There is a separate IPv4 addressing gateway IP field for the HI Host LAN configuration.

When IPv4 addressing is used, the initial value for this field is configured by the user.

This option gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

10. IP Source

Value: **Static**/Dynamic

Help text: `Select BMC IP Source. If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).`

Comments: This specifies the IP source for IPv4 addressing for the baseboard LAN. There is a separate IP Source field for the dedicated management LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC, and its setting determines whether the other baseboard LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

11. IP Address

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit IP Address. Press <Enter> to edit.`

Comments: This specifies the IPv4 address for the baseboard LAN. There is a separate IPv4 Address field for the dedicated management LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

---

Note: The IP address will be set to 0.0.0.0 when no network cable is connected to system, and this will impact both dynamic and static IP address settings.

---

12. Subnet Mask

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit Subnet Mask. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing subnet mask for the baseboard LAN. There is a separate IPv4 Subnet Mask field for the dedicated management LAN configuration.

If IP Source is Static, the default value of Subnet Mask is 0.0.0.0. If cable is connected, and IP Source has been set to be Dynamic, the default value of Subnet Mask that comes from BMC should be 255.255.255.0.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

13. Gateway IP

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing gateway IP for the baseboard LAN. There is a separate IPv4 Gateway IP field for the dedicated management LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

14. IPv6 Source

Value: **Static**/Dynamic

Help text: `Select BMC IPv6 Source. If [Static], IPv6 parameters may be edited. If [Dynamic], these fields are display-only and IPv6 address is acquired automatically (DHCP).`

Comments: This specifies the IP source for IPv6 addressing for the baseboard LAN configuration. There is a separate IPv6 Source field for the dedicated management LAN configuration.

When IPv6 addressing is enabled, the initial value for this field is acquired from the BMC, and its setting determines whether the other baseboard LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

15. IPv6 Address

Value: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000, **0000:0000:0000:0000:0000:0000:0000:0000** is default]

Help text: `View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4-digit numbers separated by colons.`

Comments: This specifies the IPv6 address for the baseboard LAN. There is a separate IPv6 Address field for the dedicated management LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The IPv6 Source setting determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

---

Note: The IP address will be set to 0000:0000:0000:0000:0000:0000:0000:0000 when no network cable is connected to system, and this will impact both dynamic and static IP address settings.

---

16. Gateway IPv6

Value: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000, **0000:0000:0000:0000:0000:0000:0000:0000** is default]

Help text: `View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4-digit numbers separated by colons.`

Comments: This specifies the gateway IPv6 address for the baseboard LAN. There is a separate Gateway IPv6 address field for the dedicated management LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The IPv6 Source setting determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

17. IPv6 Prefix Length

Value: [Entry Field 0–128, **64** is default]

Help text: `View/Edit IPv6 Prefix Length from 0 to 128 (default 64). Press <Enter> to edit.`

Comments: This specifies the IPv6 prefix length for the baseboard LAN. There is a separate IPv6 Prefix Length field for the dedicated management LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The IPv6 Source setting determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

18. IP Source

Value: **Static**/Dynamic

Help text: `Select Dedicated Management LAN IP source. If [Static], IP parameters may be edited. If [Dynamic], these fields are display-only and IP address is acquired automatically (DHCP).`

Comments: This specifies the IP source for IPv4 addressing for the DMN LAN connection. There is a separate IP Source field for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC, and its setting determines whether the other DMN LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

19. IP Address

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit IP Address. Press <Enter> to edit.`

Comments: This specifies the IPv4 address for the DMN LAN. There is a separate IPv4 Address field for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

---

Note: The IP address will be set to 0.0.0.0 when no network cable is connected to system, and this will impact both dynamic and static IP address settings.

---

20. Subnet Mask

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit Subnet Mask. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing subnet mask for the DMN LAN. There is a separate IPv4 Subnet Mask field for the baseboard LAN configuration.

If IP Source is Static, the default value of Subnet Mask is 0.0.0.0. If cable is connected, and IP Source has been set to be Dynamic, the default value of Subnet Mask that comes from BMC should be 255.255.255.0 .

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

21. Gateway IP

Value: [Entry Field 0.0.0.0, **0.0.0.0** is default]

Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing gateway IP for the DMN LAN. There is a separate IPv4 Gateway IP field for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

22. IPv6 Source

Value: **Static**/Dynamic

Help text: `Select DMN LAN IPv6 source. If [Static], IPv6 parameters may be edited. If [Dynamic], these fields are display-only and IPv6 address is acquired automatically (DHCP).`

Comments: This specifies the IP source for IPv6 addressing for the DMN LAN configuration. There is a separate IPv6 Source field for the baseboard LAN configuration.

When IPv6 addressing is enabled, the initial value for this field is acquired from the BMC, and its setting determines whether the other DMN LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

23. IPv6 Address

Value: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000, **0000:0000:0000:0000:0000:0000:0000:0000** is default]

Help text: `View/Edit IPv6 address. Press <Enter> to edit. IPv6 addresses consist of 8 hexadecimal 4-digit numbers separated by colons.`

Comments: This specifies the IPv6 address for the DMN LAN. There is a separate IPv6 Address field for the baseboard LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The setting of IPv6 Source determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

---

Note: The IP address will be set to 0000:0000:0000:0000:0000:0000:0000:0000 when no network cable is connected to system, and this will impact both dynamic and static IP address settings.

---

24. Gateway IPv6

Value: [Entry Field 0000:0000:0000:0000:0000:0000:0000:0000, **0000:0000:0000:0000:0000:0000:0000:0000** is default]

Help text: `View/Edit Gateway IPv6 address. Press <Enter> to edit. Gateway IPv6 addresses consist of 8 hexadecimal 4-digit numbers separated by colons.`

Comments: This specifies the gateway IPv6 address for the DMN LAN. There is a separate Gateway IPv6 Address field for the baseboard LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The IPv6 Source setting determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

25. IPv6 Prefix Length

Value: [Entry Field 0–128, **64** is default]

Help text: View/Edit IPv6 Prefix Length from 0 to 128 (default 64). Press <Enter> to edit.

Comments: This specifies the IPv6 prefix length for the DMN LAN. There is a separate IPv6 Prefix Length field for the baseboard LAN configuration.

When IPv6 addressing is used, the initial value for this field is acquired from the BMC. The IPv6 Source setting determines whether this field is display-only (when Dynamic or Auto) or can be edited (when Static).

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

26. BMC DHCP Host Name

Value: [Entry Field, 2–63 characters]

Help text: `View/Edit BMC DHCP host name. Press <Enter> to edit. Host name should start with an alphabetic, remaining can be alphanumeric characters. Host name length may be from 2 to 63 characters.`

Comments: This field is active and may be edited whenever at least one of the IP Source or IPv6 Source options is set to Dynamic. This is the name of the DHCP host from which dynamically assigned IPv4 or IPv6 addressing parameters are acquired.

The initial value for this field is supplied from the BMC, if there is a DHCP host available. The user can edit the existing host or enter a different DHCP host name.

If none of the IP/IPv6 Source fields are set to Dynamic, then this BMC DHCP Host Name field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Back to: BMC LAN Configuration – Server Management – Screen Map

3.5.3.1 User Configuration

The User Configuration screen allows the user to manage BMC user settings for up to five BMC users.

To access this screen from the front page, select **Server Management** > **BMC LAN Configuration** > **User Configuration**. Press the **<Esc>** key to return to the BMC LAN Configuration screen.

This form option is not configurable and gets grayed out if the IPMI Security Policy item on the Server Management Screen is shown as IPMI Security Policy: Provisioned Host Allowlist; if shown as IPMI Security Policy: Provisioned Host Disabled, this option is suppressed.

Figure 46. User Configuration Screen

1. **Password Complexity**

   Value: **Low**/Medium/High

   Help text: `Set user password Low/Medium/High complexity level.`

   Comments: Note that the default status setting is Low. When password complexity is changed, there is a popup warning message if passwords are entered which do not meet current password complexity.

   Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

2. **User ID**

   Value: User1/User2/User3/User4/User5

   Help text: None.

   Comments: *Information only*. These five user IDs are fixed and cannot be changed. The BMC supports 15 user IDs natively but only the first five are supported through this interface.

Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

3. **Privilege**

   Value: User/Operator/Administrator/**No Access**

   Help text: `View/Select user privilege. All users must be set to a privilege other than No Access and enabled for IPMI messaging before they can be used on any channel.`

   Comments: The level of privilege that is assigned for a user ID affects which functions that user may perform.

   Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

4. **User Status**

   Value: Enabled/**Disabled**

   Help text: `Enable/Disable LAN access for selected user. Also enables/disables SOL, KVM, and media redirection.`

   Comments: Note that the default status setting is Disabled.

   Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

5. **User Name**

   Value: [Entry Field, 1–16 characters]

   Help text: `Press <Enter> to edit User Name. User Name is a string of 1 to16 alpha-numeric characters or'.', '_' or '-', and must begin with alpha-numeric character or '_'. User Name cannot be named 'root'.`

   Comments: With the condition that user names are unique, no other users can be named null or any other existing user name.

   Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

6. **User Password**

   Value: [Popup Entry Field, 8–20 characters]

   Help text: `Press <Enter> key to enter password. Any ASCII printable characters can be used. The password must be between 8-20 characters. Please see user guide for password low, medium and high complexity rules on number of characters, case of characters and other rules regarding numbers and symbols.`

   `Note: Password entered will override any previously set password.`

   Comments: This field does not indicate whether there is a password set already. There is no display; press **<Enter>** to open a popup with an entry field to enter a new password. Any new password overrides the previous password, if there was one.

   Back to: User Configuration – BMC LAN Configuration – Server Management – Screen Map

Note: Privilege and User Status items are grayed out if the User Name field is empty or not configured.

3.6 Error Manager Screen

The Error Manager screen displays any POST error codes encountered during BIOS POST, along with an explanation of the meaning of the error code in the form of help text. This is an information-only screen.

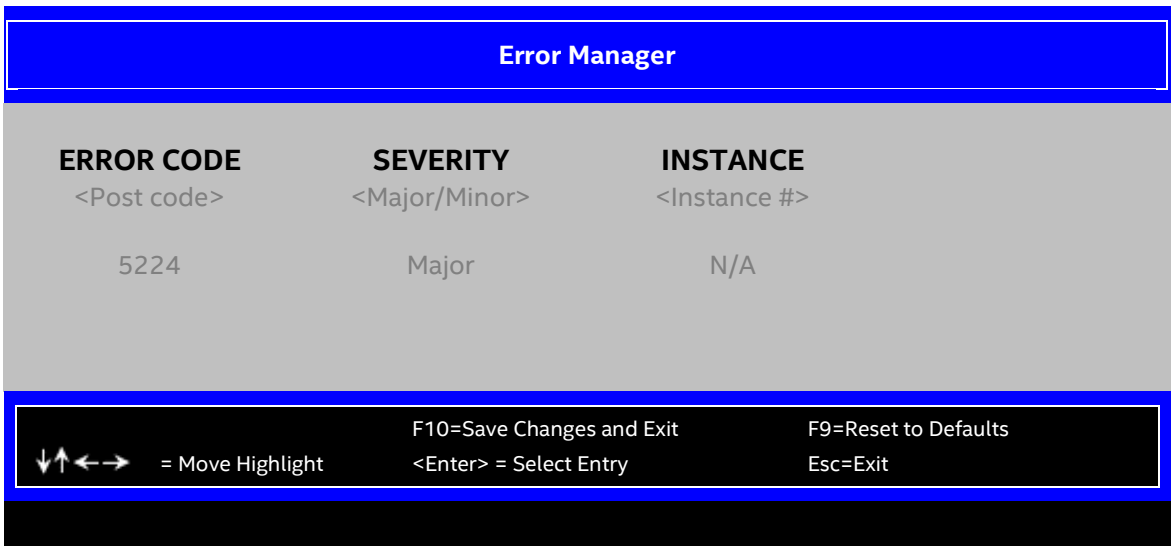

Figure 47. Error Manager Screen

1. **ERROR CODE**

   Value: <POST error code>

   Help text: N/A

   Comments: The POST error code is a BIOS-originated error that occurred during POST initialization. For more information on POST error codes, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 10.4.4.3.

   Back to: Error Manager – Screen Map

2. **SEVERITY**

   Value: Minor/Major/Fatal

   Help text: N/A

   Comments: Each POST error code has a severity associated to it. For more information on POST error codes, refer to the *BIOS EPS for the Intel® Server Boards M50FCP and D50DNP*, Section 10.4.4.3.

   Back to: Error Manager – Screen Map

3. **INSTANCE**

   Value: <Depends on error code>

   Help text: N/A

   Comments: Where applicable, this field shows a value indicating which one of a group of components was responsible for generating the POST error code that is being reported.

   Back to: Error Manager – Screen Map

3.7 Boot Manager Screen

The Boot Manager screen allows the user to view a list of devices available for booting and to select a boot device for immediately booting the system. There is no predetermined order for listing bootable devices, they are simply listed in order of discovery.

Regardless of whether any other bootable devices are available, the Internal EFI Shell option is always available.

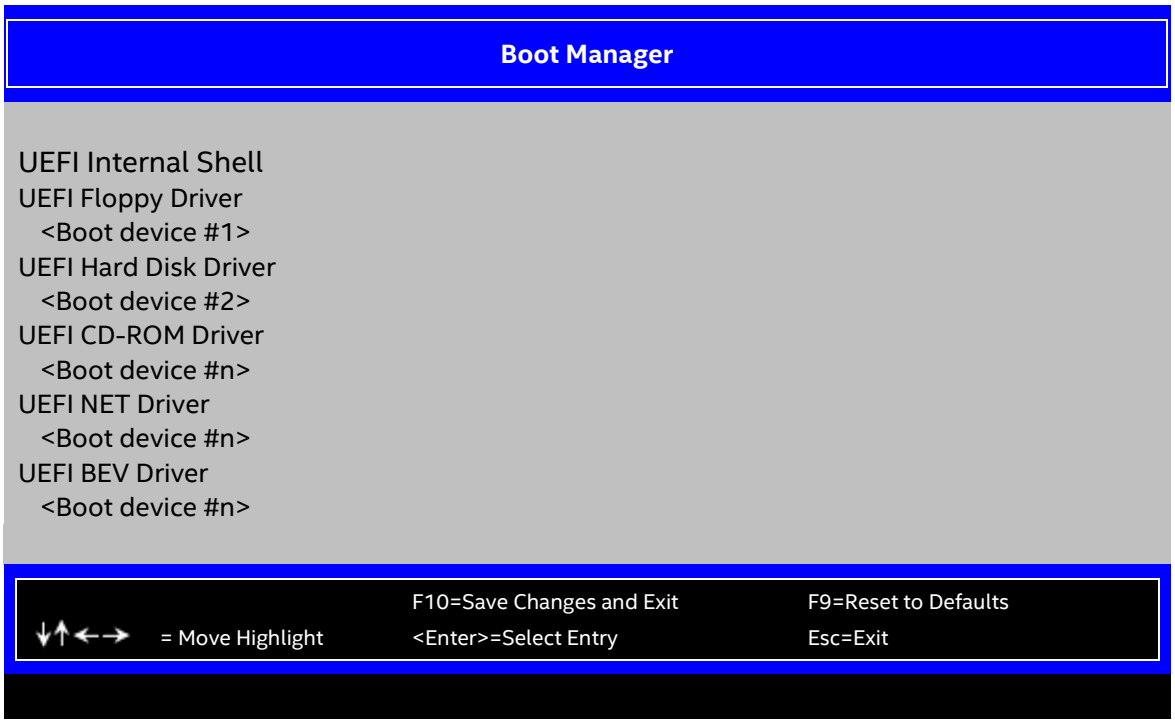

Figure 48. Boot Manager Screen

1. **UEFI Internal Shell**

   Value: None.

   Help text: `Select this option to boot now.`
   `Note: This list is not the system boot option order. Use the Boot Maintenance Manager menu to view and configure the system boot option order.`

   Comments: The EFI shell is always present in the list of bootable devices.

   Note: This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order.

   Back to: Boot Manager – Screen Map

2. **<Boot device #1>**
3. **<Boot device #2>**
4. **<Boot device #n>**

Value: None.

Help text: `Select this option to boot now.`

`Note: This list is not the system boot option order. Use the Boot Maintenance Manager menu to view and configure the system boot option order.`

Comments: These are names of bootable devices discovered in the system. The system user can choose any of them to initiate a one-time boot from it. Booting from any device in this list does not permanently affect the defined system boot order.

These bootable devices are not displayed in any specified order, particularly not in the system boot order established by the Boot Maintenance Manager screen. This is just a list of bootable devices in the order in which they were enumerated.

Note: This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order.

Back to: Boot Manager – Screen Map

3.8 Boot Maintenance Manager Screen

The Boot Maintenance Manager screen contains all bootable media encountered during POST and allows the user to configure the desired order in which boot devices are to be tried.

The first boot device in the specified boot order that is present and bootable during POST is used to boot the system. The same device continues to be used to reboot the system until the boot device configuration has changed (that is, a change in which boot devices are present), or until the system has been powered down and booted in a cold power-on boot.

Notes:

- USB devices can be hot-plugged during POST, they are detected and beeped. They are enumerated and displayed on the USB Configuration Setup screen. However, they may not be enumerated as bootable devices, depending on when in POST they were hot plugged. If they were recognized before the enumeration of bootable devices, they appear as boot devices, if appropriate. If they were recognized after the enumeration, they do not appear as a bootable device on the Boot Maintenance Manager screen, the Boot Manager screen, or the Boot Menu.
- A USB key (USB flash drive) can be formatted to emulate either a floppy drive or a hard drive and appears in that boot device class. Although it can be formatted as a CD-ROM drive, it is not detected as such and is treated as a hard disk drive appearing in the list of available hard drives.

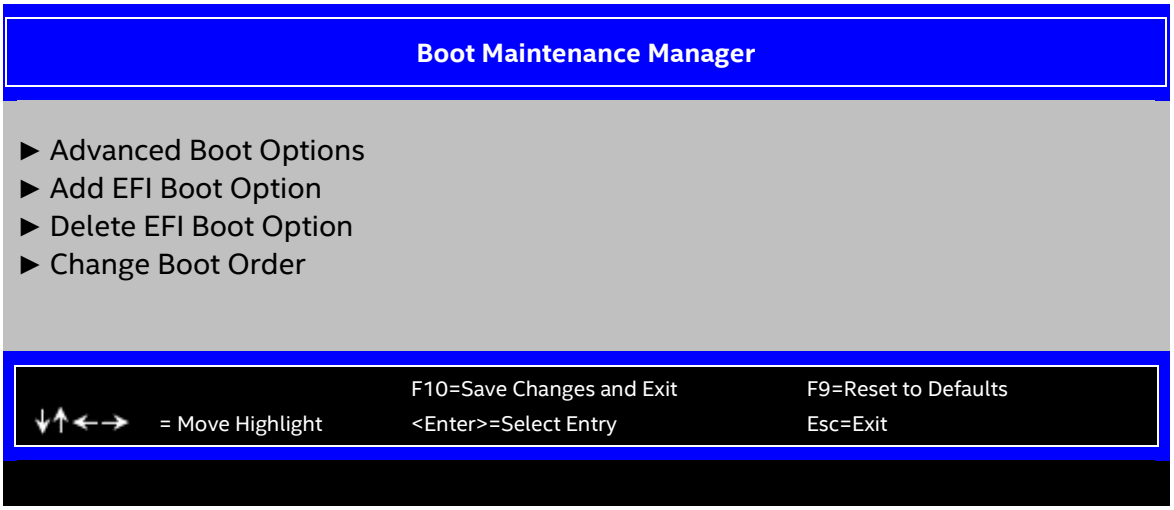

Figure 49. Boot Maintenance Manager Screen

1. **Advanced Boot Options**

   Value: None.

   Help text: `Set the Advanced Boot Options in this group.`

   Comments: *Selection only*. For more information on Advanced Boot Options, see Section 3.8.1.

   Back to: Boot Maintenance Manager – Screen Map

2. **Add EFI Boot Option**

   Value: None.

   Help text: `Add a new EFI boot option to the boot order.`

   Comments: *Selection only*. For more information on Add EFI Boot Option, see Section 3.8.2.

   This option is only displayed if an EFI bootable device is available to the system.

   Note: This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel® Firmware Customization.

   Back to: Boot Maintenance Manager – Screen Map

3. **Delete EFI Boot Option**

   Value: None.

   Help text: `Remove an EFI boot option from the boot order.`

   Comments: *Selection only*. For more information on Delete EFI Boot Option settings, see Section 3.8.3.

   This option is only displayed if an EFI boot path is included in the boot order.

   Notes:
   - This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel® Firmware Customization.

- For the boot option added by BIOS BDS, it can be deleted in this menu, and it can be added into end of boot order again in next BIOS POST.

Back to: Boot Maintenance Manager – Screen Map

4. **Change Boot Order**

Value: None.

Help text: `Set the Boot Order in this group.`

Comments: *Selection only*. For more information on Change Boot Order settings, see Section 3.8.4.

Note: This field does not support changes through Intel® Server Configuration Utility with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel® Firmware Customization.

Back to: Boot Maintenance Manager – Screen Map

3.8.1 Advanced Boot Options

The Advanced Boot Options screen allows the user to control the advanced boot options features like boot mode.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

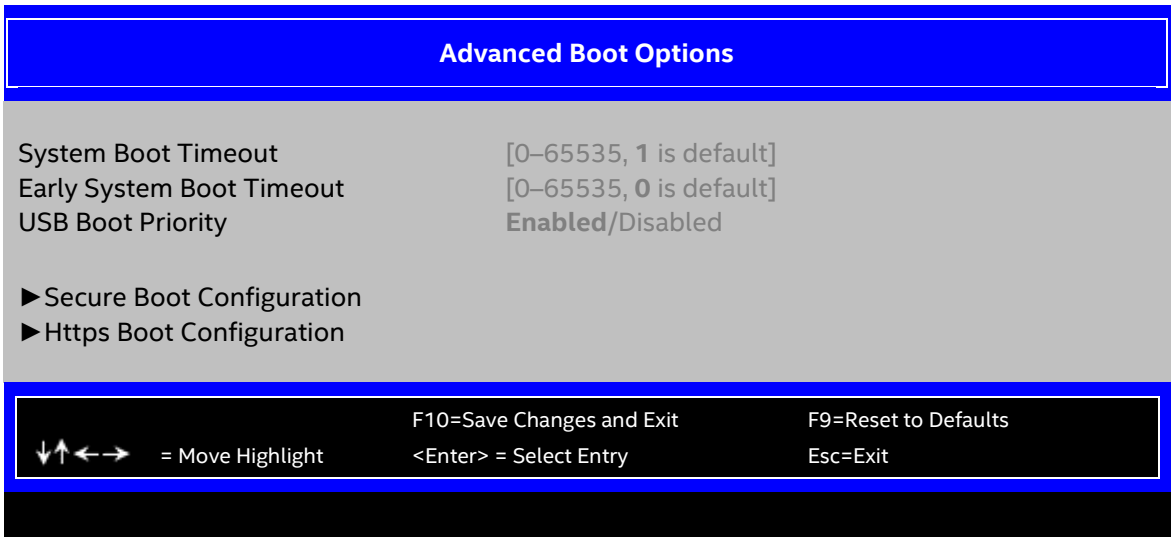

Figure 50. Advanced Boot Options Screen

1. **System Boot Timeout**

Value: [Entry Field 0–65535, **1** is default]

Help text: `The number of seconds BIOS will pause at the end of POST to allow the user to press the [F2] key for entering the BIOS Setup utility. Valid values are 0-65535. 1 is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.`

Comments: After entering the desired timeout in seconds, press the **<Enter>** key to register that timeout value to the system. The timeout value entered takes effect on the next boot.

This timeout value is independent of the FRB-2 setting for BIOS boot failure protection. The FBR-2 countdown is suspended during the time that the boot timeout countdown is active.

If the **<Pause>** key is pressed while the boot timeout is active, the boot timeout countdown is suspended until the pause state is dismissed and normal POST processing is resumed.

Back to: Advanced Boot Options – Boot Maintenance Manager – Screen Map

2. Early System Boot Timeout

Value: [Entry Field 0–65535, **0** is default]

Help text: The number of seconds the BIOS will pause before Option ROMs are dispatched. Valid values are 0–65535. Zero is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.

Comments: After entering the desired timeout in seconds, press the **<Enter>** key to register that timeout value to the system. The timeout value takes effect on the next boot.

This timeout value is independent of the FRB-2 setting for BIOS boot failure protection. The FBR2 countdown is suspended during the time that the boot timeout countdown is active.

Also, the BIOS cannot support any key that is pressed during the time that the Early Boot Timeout is active because the keyboard service is still not active.

Back to: Advanced Boot Options – Boot Maintenance Manager – Screen Map

3. USB Boot Priority

Value: **Enabled**/Disabled

Help text: `If enabled, newly discovered USB devices are moved to the top of their boot device category.`

`If disabled, newly discovered USB devices are moved to the bottom of their boot device category.`

Comments: None.

Back to: Advanced Boot Options – Boot Maintenance Manager – Screen Map

4. Secure Boot Configuration

Value: None.

Help text: `Set the Secure Boot Configuration Options in this group.`

Comments: None.

Back to: Advanced Boot Options – Boot Maintenance Manager – Screen Map

5. Https Boot Configuration

Value: None.

Help text: `Set the Https Boot Configuration Options in this group.`

Comments: None.

Back to: Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.1.1 Secure Boot Configuration

The Secure Boot Configuration screen allows the user to configure UEFI secure boot.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Secure Boot Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

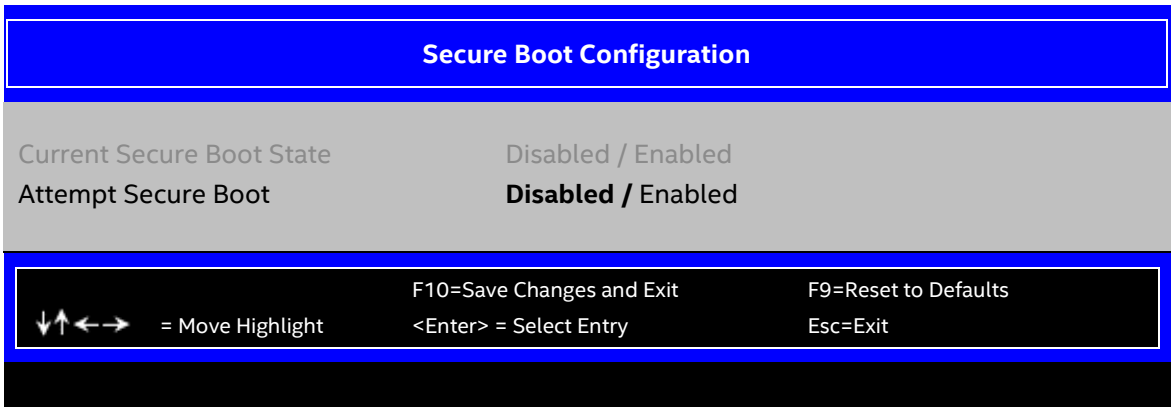

Figure 51. Secure Boot Configuration Screen

1. **Current Secure Boot State**

   Value: Disabled/Enabled

   Help text: `Current Secure Boot state: enabled or disabled.`

   Comments: *Information only*. Displays current secure boot state. Platform reset is required after enabling or disabling BIOS UEFI secure boot feature in the following Attempt Secure Boot option.

   Note: This field does not support Intel® Server Configuration Utility display with the `/bcs` command. However, the Intel® Server Configuration Utility `/d sboot` commands can be used to show current secure boot status.

   Back to: Secure Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

2. **Attempt Secure Boot**

   Value: **Disabled**/Enabled

   Help text:
   ```
   [Enabled] - Enable the Secure Boot feature after platform reset.
   [Disabled] - Disable the Secure Boot feature after platform reset.
   ```

   Comments: Secure Boot related keys (PK, KEK, db, and dbx) are required in order to enable UEFI secure boot feature. During platform reset after this option is turned to Enabled. The BIOS provisions the default keys automatically if the corresponding key is not present.

   Notes:
   - Product BIOS ships a default set of PK, KEK, db, and dbx in BIOS release images. The BIOS provisions the keys for the first time a user successfully enables this option.
   - This option is protected by BIOS administrator password as basic security level. More advanced security level requires that platform physical presence policy needs to be applied in order to change secure boot feature control option. Therefore, Current Secure

Boot State option is not always changed successfully after a platform reset if the advanced security check fails.

- For support related to Intel® Server Configuration Utility, Secure Boot just supports proprietary solution defined in the *Intel® Server Configuration Utility User Guide*. The user can use Intel® Server Configuration Utility `/sboot` to attempt to change current secure boot enable or disable status; the BIOS does not support other commands for general setup options, such as `/s` or `/bcs` command.

Back to: Secure Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.1.2 HTTPS Boot Configuration

The HTTPS Boot Configuration allows the user to configure HTTPS Boot Configuration Options.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **HTTPS Boot Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

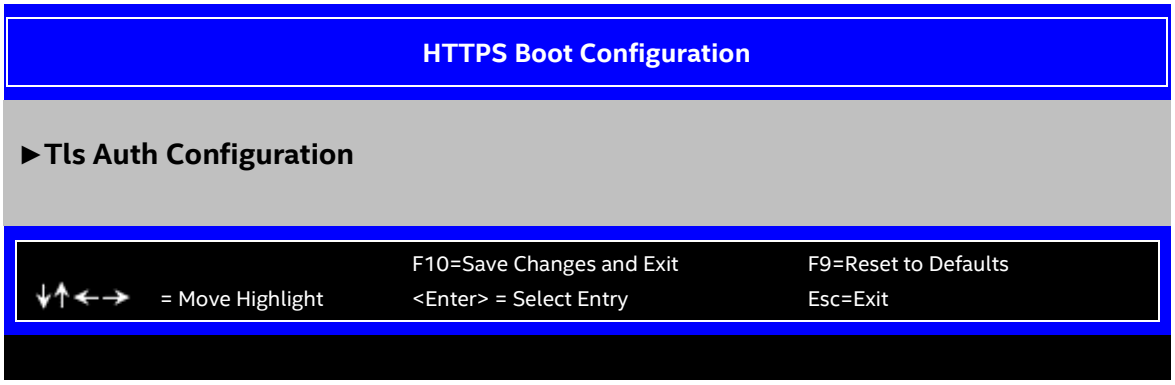

Figure 52. HTTPS Boot Configuration Screen

1. Tls Auth Configuration

Value: None.

Help text: `Press <Enter> to select Tls Auth Configuration.`

Comments: None.

Back to: HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.1.2.1 Tls Auth Configuration

The HTTPS Boot Configuration allows the user to configure Tls Auth Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **HTTPS Boot Configuration** > **Tls Auth Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

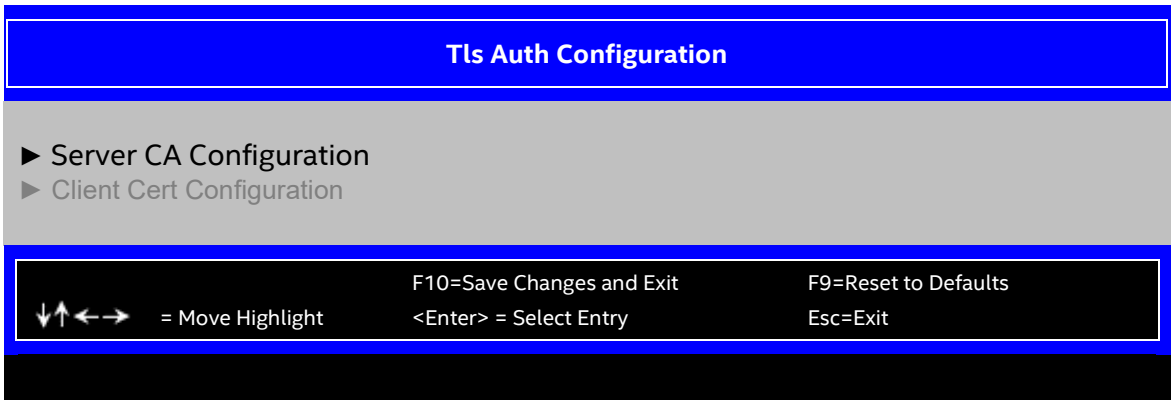

Figure 53. Tls Auth Configuration Screen

1. Server CA Configuration

Value: None.

Help text: `Press <Enter> to configure Server CA.`

Comments: None.

Back to: Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

2. Client Cert Configuration

Value: None.

Help text: `Client Cert Configuration`

Comments: Current unsupported.

Back to: Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.1.2.1.1 Server CA Configuration

The HTTPS Boot Configuration allows the user to configure Server CA Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **HTTPS Boot Configuration** > **Tls Auth Configuration** > **Server CA Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

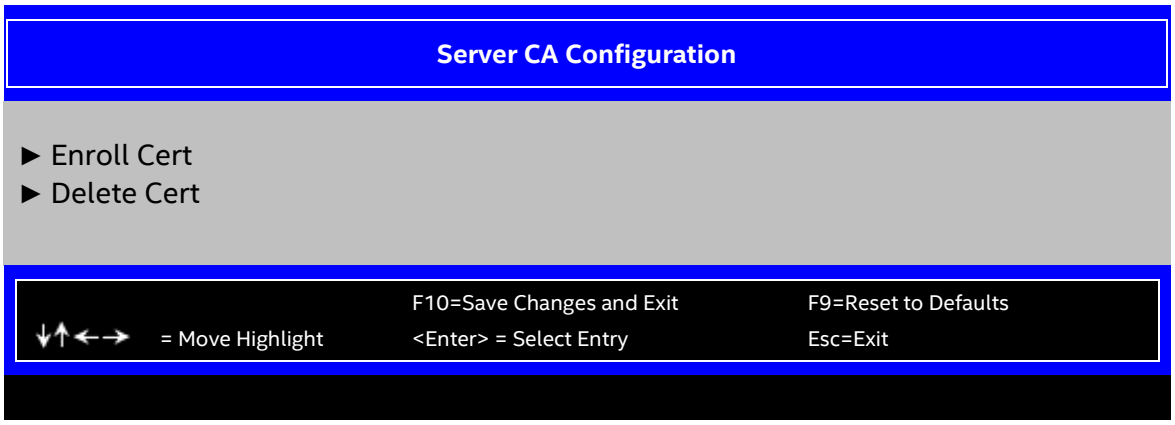

Figure 54. Server CA Configuration Screen

1. **Enroll Cert**

Value: None.

Help text: `Press <Enter> to enroll cert.`

Comments: None.

Back to: Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

2. **Delete Cert**

Value: None.

Help text: `Press <Enter> to delete cert.`

Comments: None.

Back to: Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.1.2.1.1.1 Enroll Cert

The HTTPS Boot Configuration allows the user to configure Server CA Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **HTTPS Boot Configuration** > **Tls Auth Configuration** > **Server CA Configuration** > **Enroll Cert**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

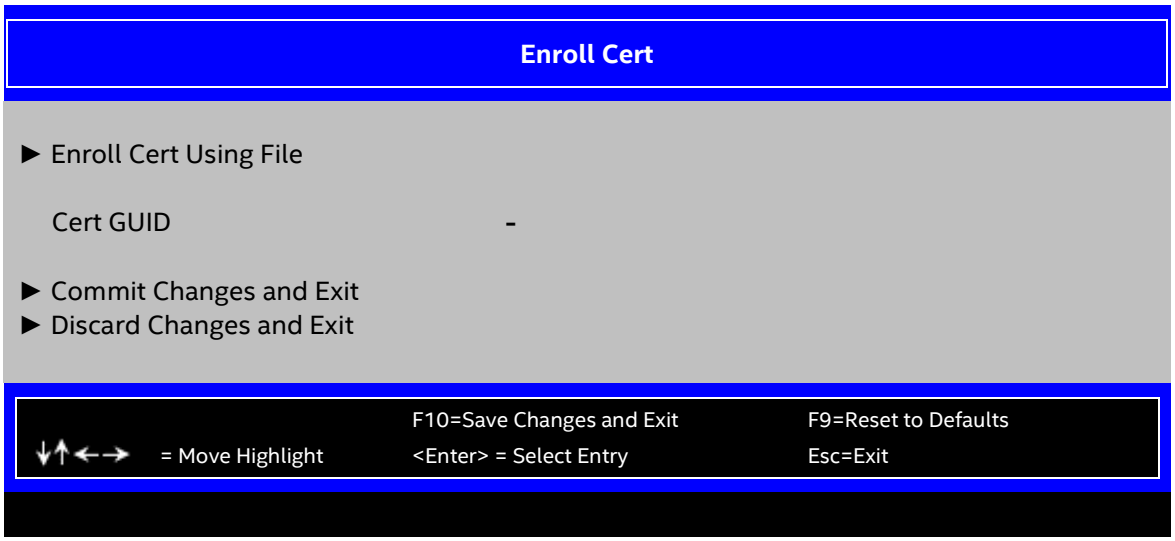

Figure 55. Enroll Cert Screen

1. **Enroll Cert Using File**

Value: None.

Help text: `Enroll Cert Using File`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

2. **Cert GUID**

Value: -

Help text: `Input digit character in 11111111-2222-3333-4444-1234567890ab format.`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3. **Commit Changes and Exit**

Value: None.

Help text: `Commit Changes and Exit`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

4. **Discard Changes and Exit**

Value: None.

Help text: `Discard Changes and Exit`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – HTTPS Boot Configuration – Advanced Boot Options – Boot Maintenance Manager – Screen Map

3.8.2 Add EFI Boot Option

The Add EFI Boot Option screen allows the user to add an EFI boot option to the boot order. The Internal EFI Shell boot option is permanent and cannot be added or deleted.

To access this screen from the front page, select **Boot Maintenance Manager** > **Add EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

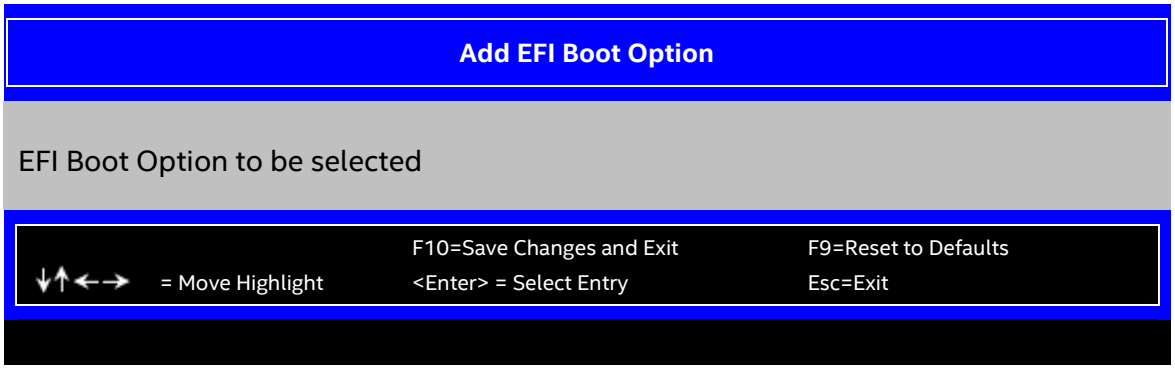

Figure 56. Add EFI Boot Option Screen

1. **EFI Boot Option to be selected**

Value: None.

Help text: None.

Comments: *Selection only*. This lists current EFI devices paths enumerated by the BIOS during the POST to select the EFI Boot Option.

Back to: Add EFI Boot Option – Boot Maintenance Manager – Screen Map

3.8.3 Delete EFI Boot Option

The Delete EFI Boot Option screen allows the user to remove an EFI boot option from the boot order. The Internal EFI Shell boot option is not listed, since it is permanent and cannot be added or deleted.

To access this screen from the front page, select **Boot Maintenance Manager** > **Delete EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

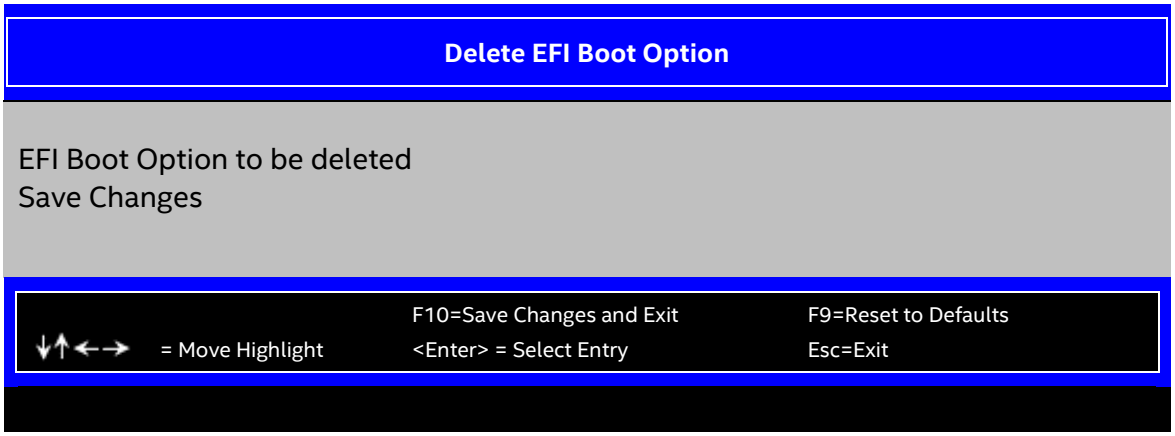

Figure 57. Delete EFI Boot Option Screen

1. **EFI Boot Option to be deleted**

   Value: [Checkbox]

   Help text: `Select one to delete.`

   Comments: Use the check box to select the EFI boot option to be deleted. This does not allow a user to delete the EFI shell.

   Back to: Delete EFI Boot Option – Boot Maintenance Manager – Screen Map

3.8.4 Change Boot Order

The Change Boot Order screen allows the user to configure the desired order of UEFI boot devices in which the boot device is to be tried sequentially.

To access this screen from the front page, select **Boot Maintenance Manager** > **Delete EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

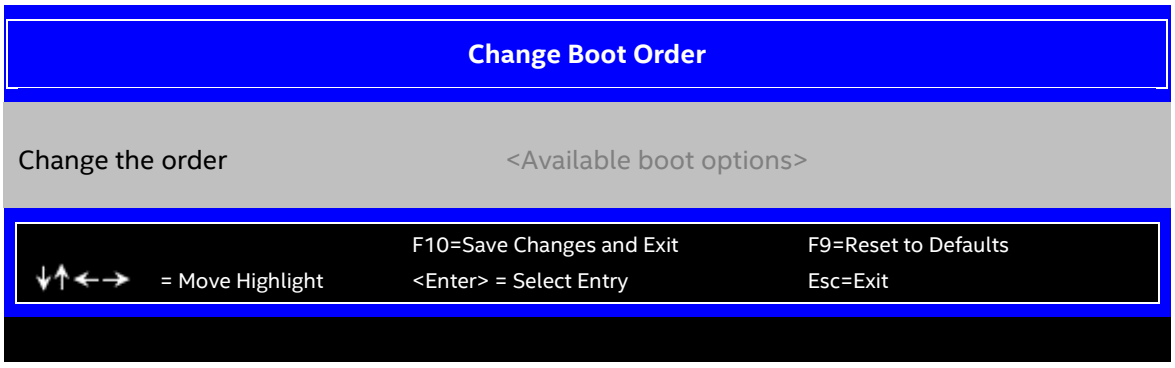

Figure 58. Change Boot Order Screen

1. **Change the order**

   Value: <Available boot options>

   Help text: `Use [Enter] key and [Up Arrow] or [Down Arrow] to select the booting device. Use [+] or [-] key to move up/down the selected field.`

   Comments: None.

   Back to: Change Boot Order – Boot Maintenance Manager – Screen Map

3.9 Save & Exit Screen

The Save & Exit screen allows the user to choose whether to save or discard the configuration changes made on other setup screens. It also allows the user to restore the BIOS settings to the factory defaults or to save or restore them to a set of user-defined default values. If **Load Default Values** is selected, the factory default settings (noted in bold in the setup screen images) are applied. If **Load User Default Values** is selected, the system is restored to previously saved user default values.

Note: There is a legal disclaimer footnote at the bottom of the Save & Exit screen:

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

This is reference to any instance in the setup screens where names belonging to other companies may appear. For example, `LSI*` appears in setup in the context of mass storage RAID options.

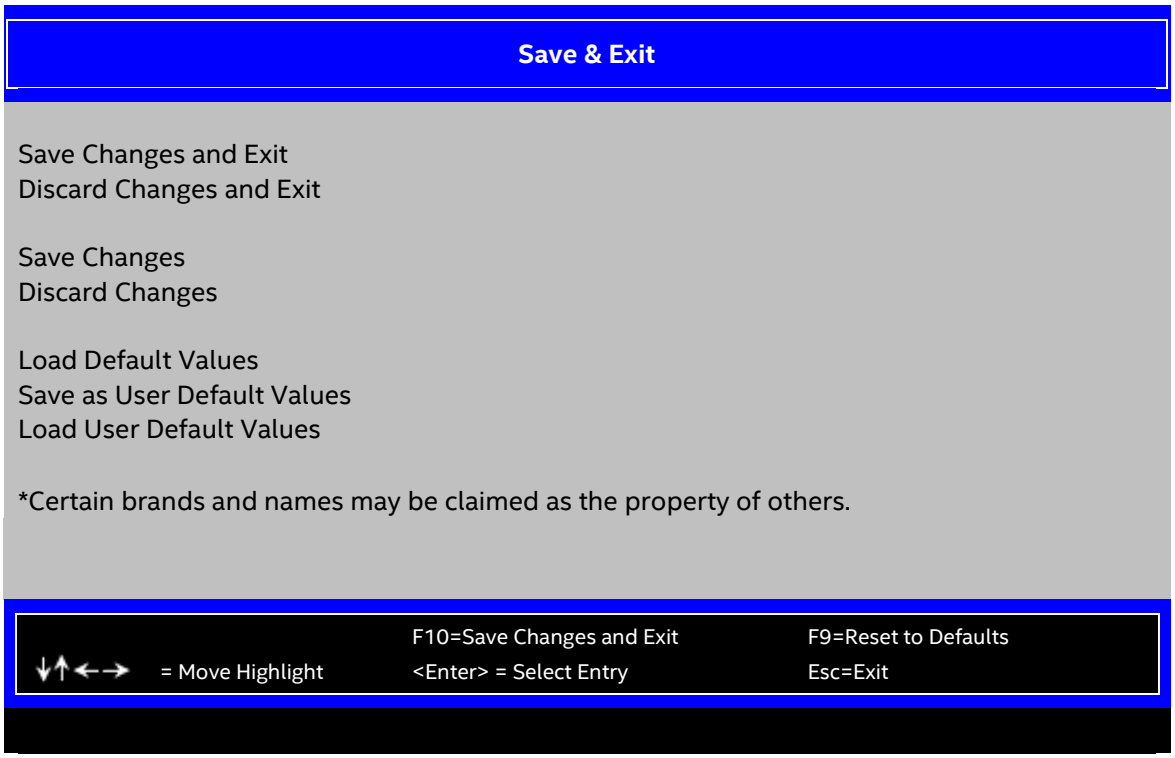

Figure 59. Save & Exit Screen

1. **Save Changes and Exit**

   Value: None.

   Help text: `Exit BIOS Setup Utility after saving changes. The system will reboot if required.`

   Comments: *Selection only*. Select this line and press the **<Enter>** key to exit setup with any changes in BIOS settings saved. If there have been no changes made in the settings, the BIOS resumes executing POST.

   If changes have been made in BIOS settings, a confirmation pop-up appears. If the Save Changes and Exit action is positively confirmed, any persistent changes are applied and saved to the BIOS settings in non-volatile RAM (NVRAM) storage and the system reboots, if necessary (which is normally the case). If the Save Changes and Exit action is not confirmed, the BIOS resumes executing setup.

The **<F10>** function key may also be used from any screen in setup to initiate a Save Changes and Exit action.

Back to: Save & Exit – Screen Map

2. **Discard Changes and Exit**

   Value: None.

   Help text: `Exit BIOS Setup Utility without saving changes.`

   Comments: *Selection only*. Select this line and press the **<Enter>** key to exit setup without saving any changes in BIOS settings. If there have been no changes made in the settings, the BIOS resumes executing POST.

   If changes have been made in BIOS settings, a confirmation pop-up appears. If the Discard Changes and Exit action is positively confirmed, all pending changes are discarded and the BIOS resumes executing POST. If the Discard Changes and Exit action is not confirmed, the BIOS resumes executing setup without discarding any changes.

   Back to: Save & Exit – Screen Map

3. **Save Changes**

   Value: None.

   Help text: `Save Changes made so far to any of the setup options.`

   Comments: *Selection only*. Select this line and press the **<Enter>** key to save any pending changes in BIOS settings. If there have been no changes made in the settings, the BIOS resumes executing POST.

   Also, the user should be aware that most changes require a reboot to become active. If changes have been made and saved without exiting setup, the system should be rebooted later even if no additional changes are made.

   Back to: Save & Exit – Screen Map

4. **Discard Changes**

   Value: None.

   Help text: `Discard Changes made so far to any of the setup options.`

   Comments: *Selection only*. Select this line and press the **<Enter>** key to discard any pending unsaved changes in BIOS settings. If there have been no changes made in the settings, the BIOS resumes executing POST.

   If changes have been made in BIOS settings and not yet saved, a confirmation pop-up appears. If the Discard Changes action is positively confirmed, all pending changes are discarded and the BIOS resumes executing POST. If the Discard Changes action is not confirmed, the BIOS resumes executing setup without discarding pending changes.

   Back to: Save & Exit – Screen Map

5. **Load Default Values**

   Value: None.

   Help text: Load Default Values for all the setup options.

Comments: *Selection only*. Select this line and press the <Enter> key to load default values for all BIOS settings. These are the initial factory settings (failsafe settings) for all BIOS parameters.

There is a confirmation popup to verify that the user really meant to take this action.

After initializing all BIOS settings to default values, the BIOS resumes executing setup, so the user may make additional changes in the BIOS settings if necessary (for example, boot order) before doing a Save Changes and Exit action with a reboot to make the default settings take effect, including any changes made after loading the defaults.

The **<F9>** function key may also be used from any screen in setup to initiate a Load Default Values action.

Back to: Save & Exit – Screen Map

6. Save as User Default Values

Value: None.

Help text: `Save the changes made so far as User Default Values.`

Comments: *Selection only*. Select this line and press the **<Enter>** key to save the current state of the settings for all BIOS parameters as a customized set of user default values.

These are a user-determined set of BIOS default settings that can be used as an alternative instead of the initial factory settings (failsafe settings) for all BIOS parameters.

By changing the BIOS settings to user-preferred values and then using this operation to save them as user default values, that version of BIOS settings can be restored at any time by using the following Load User Default Values operation.

There is a confirmation popup to verify that the user really intended to take this action.

Loading the factory default values does not affect the user default values. They remain set to whatever values that they were last saved as.

Note: Due to a setup limitation, BIOS variables in type VARSTORE do not need to support Save As/Load User Default. For example, BMC owned option are in this scope such as Power Restore Policy, thermal related options, and all settings under BMC LAN Configuration.

Back to: Save & Exit – Screen Map

7. Load User Default Values

Value: None.

Help text: `Load the User Default Values to all the setup options.`

Comments: *Selection only*. Select this line and press the **<Enter>** key to load user default values for all BIOS settings. These are user-customized BIOS default settings for all BIOS parameters previously established by doing a Save User Defaults action.

There is a confirmation popup to verify that the user really intended to take this action.

Note: Due to a setup limitation, BIOS variables in type VARSTORE do not need to support Save As/Load User Default. For example, BMC owned option are in this scope such as Power Restore Policy, thermal related options, and all settings under BMC LAN Configuration.

Back to: Save & Exit – Screen Map

Appendix A. Intel Tool Support

Intel has developed tools that allow the user to customize BIOS settings, meaning that these tools support actions like saving and setting selected configurations for the system firmware and the BIOS. Such tools include Intel® Firmware Customization, Intel® Server Configuration Utility, and OOB Configuration. The following table summarizes these tools' support status for the BIOS setup utility options.

The table includes these symbols:

- × – Means that the corresponding tool is not supported.
- √ – Means that the corresponding tool is supported.

Note: Some options are supported by the BIOS, while some may need Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility to get values from the BMC via IPMI. Said values cannot be obtained from the BIOS variable via `/bcs`, especially for the BMC-controlled setup options.

For BMC-controlled options, the BIOS does not support neither Intel® Server Configuration Utility nor Intel® Server Information Retrieval Utility via `/bcs` command. For information-only items, if Intel Server Configuration Utility is marked as √, the items are read-only for this tool.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Main				
Logged in as:	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Platform ID	×	×	×	
BIOS Boot From	×	×	×	
BIOS Version in Active Region	×	×	×	
Active BIOS Build Date	×	×	×	
SPS FW Version in Active Region	×	×	×	
BIOS Version in Recovery Region	×	×	×	
SPS FW Version in Recovery Region	×	×	×	
Total DDR5 Memory	×	×	×	
High Bandwidth Memory	×	×	×	
Access Level	×	×	×	Information only.
Quiet Boot	√	√	√	
POST Error Pause	√	√	√	
System Date	×	√	×	For Intel Server Configuration Utility, supports `/dt`, but not `/bcs`.
System Weekday	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
System Time	×	√	×	For Intel Server Configuration Utility, support `/dt`, but not `/bcs`.
PFR				
PFR Lock	√	√	√	
PFR Provision	√	×	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
PFR UnProvision	√	√	√	
PFR Status	x	x	x	Information only.
PFR Locked Status	x	x	x	Information only.
PFR Provision Status	x	x	x	Information only.
CPLD Common Code version	x	x	x	Information only.
CPLD RoT Release Version	x	x	x	Information only.
CPLD RoT SVN	x	x	x	Information only.
PCH PFR Active SVN	x	x	x	Information only.
BMC PFR Active SVN	x	x	x	Information only.
BMC PFM Active Major Version	x	x	x	Information only.
BMC PFM Active Minor Version	x	x	x	Information only.
PCH PFR Recovery SVN	x	x	x	Information only.
BMC PFR Recovery SVN	x	x	x	Information only.
BMC PFM Recovery Major Version	x	x	x	Information only.
BMC PFM Recovery Minor Version	x	x	x	Information only.
PCH SVN Bypass Jumper Status	x	x	x	Information only.
BMC SVN Bypass Jumper Status	x	x	x	Information only.
Advanced: Processor Configuration				
Processor Socket	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Processor ID	×	×	×	
Processor Frequency	×	×	×	
Microcode Revision	×	×	×	
L1 Cache RAM	×	×	×	
L2 Cache RAM	×	×	×	
L3 Cache RAM	×	×	×	
Processor 0 Version	×	√	×	
Processor 1 Version	×	√	×	
Intel(R) Hyper-Threading Tech	√	√	√	
Total Processor Cores	×	×	×	Information only.
Current Active Processor Cores	×	×	×	Information only.
Active Processor Cores	√	√	√	
Intel® Virtualization Technology	√	√	√	
Intel® TXT	√	√	√	
MLC Streamer	√	√	√	
MLC Spatial Prefetcher	√	√	√	
DCU Data Prefetcher	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
DCU Instruction Prefetcher	√	√	√	
X2APIC	√	×	√	
Limit CPU PA to 46 bits	√	√	√	
PPIN Control	√	√	√	
DBP-F	√	√	√	
LLC Prefetch	√	√	√	
Force Boot With FULL Socket Number	√	√	√	
Total Memory Encryption (TME)	√	√	√	
Total Memory Encryption (TME) Bypass	√	√	√	
Total Memory Encryption Multi-Tenant(TME-MT)	√	√	√	
Memory integrity	√	√	√	
Key stock amount	×	×	×	Information only.
TME-MT key ID bits	×	×	×	Information only.
Trust Domain Extension (TDX)	√	√	√	
TDX Secure Arbitration Mode Loader (SEAM Loader)	√	√	√	
Disable excluding Mem below 1MB in CMR	√	√	√	
TME-MT/TDX key split	√	√	√	
TME-MT keys	×	×	×	Information only
TDX keys	×	×	×	Information only
PRM Size	×	×	×	Information only.
SGX Factory Reset	√	×	×	Callback function to complete the function, Does not support `/bcs` command for Intel® Server Configuration Utility.
SW Guard Extensions (SGX)	√	√	√	
SGX Package Info In-Band Access	√	√	√	
SGX PRM size	√	√	√	
SGX QoS	√	√	√	
Select Owner EPOCH input type	√	√	√	
Software Guard Extensions Epoch 0	√	√	√	
Software Guard Extensions Epoch 1	√	√	√	
SGXLEPUBKEYHASHx Write Enable	√	√	√	
SGXLEPUBKEYHASH0	√	√	√	
SGXLEPUBKEYHASH1	√	√	√	
SGXLEPUBKEYHASH2	√	√	√	
SGXLEPUBKEYHASH3	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
SGX Auto MP Registration	√	√	√	
Advanced: Power & Performance				
CPU Power and Performance Policy	√	√	√	
Workload Configuration	√	√	√	
Optimized Power Mode	√	√	√	
Advanced: Power & Performance: Uncore Power Management				
Performance P-limit	√	√	√	This option can support Intel Firmware Customization, but the value may be overwritten by changing special options after enter bios setup.
Uncore Freq Scaling	√	√	√	
Uncore Freq	√	√	√	
Uncore Freq RAPL	√	√	√	
Advanced: Power & Performance: CPU P State Control				
AVX Licence Pre-Grant Override	√	√	√	
AVX ICCP pre-grant level	√	√	√	
Enhanced Intel SpeedStep(R) Tech	√	√	√	
Intel® Turbo Boost Technology	√	√	√	
Energy Efficient Turbo	√	√	√	
AVX P1	√	√	√	
Dynamic SST-PP	√	√	√	
Intel SST-PP	×	√	√	
SST-PP Level 0/3/4	x	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Core Count	x	x	x	
P1 Ratio	x	x	x	
Package TDP (W)	x	x	x	
Tjmax	x	x	x	
Activate SST-BF	√	√	√	
Configure SST-BF	√	√	√	
EIST PSD Function	√	√	√	
SST-CP	√	√	√	
Advanced: Power & Performance: Hardware P States				
Hardware P-states	√	√	√	
HardwarePM Interrupt	√	√	√	
EPP Enable	√	√	√	
EPP profile	√	√	√	
APS Rocketing	√	√	√	
Scalability	√	√	√	
Advanced: Power & Performance: CPU C State Control				
Package C state	√	√	√	
C1E	√	√	√	This option can support Intel Firmware Customization, but the value may be overwritten by changing special options after enter bios setup.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Processor C6	√	√	√	
C1 Auto Demotion	√	√	√	
Advanced: UPI Configuration				
Current Intel(R) UPI Link Speed	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Intel(R) UPI Link Frequency	×	×	×	
Intel(R) UPI Frequency Select	√	√	√	
IO Directory Cache (IODC)	√	√	√	
KTI Prefetch	√	√	√	
Stale AtoS	√	√	√	
LLC Dead Line Alloc	√	√	√	
Advanced: Memory Configuration				
Total DDR5 Memory	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
High Bandwidth Memory	×	×	×	
Effective Memory	×	×	×	
Current Configuration	×	×	×	
Current Memory Speed	×	×	×	
Current HBM Speed	×	×	×	
Memory Operating Speed Selection	√	√	√	
Page Policy	√	√	√	
Enforce Population POR	√	√	√	
Volatile Memory Mode	×	√	√	
HBM Mode	√	√	√	
Allow Memory Test Correctable Error	√	√	√	
HBM Memory Test	√	√	√	
HBM Adv MemTest PPR	√	√	√	
HBM Adv MemTest Retry After Repair	√	√	√	
HBM Adv MemTest Reset Failure Tracking List	√	√	√	
HBM PPR Type	√	√	√	
MemTest	√	√	√	
MemTest Loops	√	√	√	
SK Hynix SmartTestKey	√	√	√	
Adv MemTest Options	√	√	√	
Adv MemTest PPR	√	√	√	
Adv MemTest Retry After Repair	√	√	√	
Adv MemTest Reset Failure Tracking List	√	√	√	
Adv MemTest Conditions	√	√	√	
Adv MemTest PMIC VDD Level	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Adv MemTest tWR	√	√	√	
Adv MemTest tREFI	√	√	√	
Adv MemTest Pause	√	√	√	
DDR PPR Type	√	√	√	
Publish ARS Capability	√	√	√	
Average Power Budget (in mW)	x	x	x	
I3C Clock Frequency	√	√	√	
Attempt Fast Boot	√	√	√	
Attempt Fast Cold Boot	√	√	√	
Promote Warnings	√	√	√	
NVDIMM Mailbox in NFIT (not POR for Intel® Server Systems based on the 4th Gen Intel® Xeon® Scalable processors family)	√	√	√	
CPU0_HBM2e_Stack0	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
...	×	×	×	
CPU1_HBM2e_Stack3	×	×	×	
CPU0_DIMM_A1	×	×	×	
...	×	×	×	
CPU1_DIMM_H2	×	×	×	
Advanced: Memory Configuration: Memory RAS and Performance Configuration				
Memory Mirroring Possible	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Memory ADDDC Possible	×	×	×	
HBM Clustering Mode Status	×	×	×	
DDR Clustering Mode Status	×	×	×	
Mirror Mode	√	√	√	Need disable ADDDC Sparing first in Setup UI for x4 DIMM. For Intel Firmware Customization support, its GUI shows two options for Mirror Mode, the user should choose which option to change based on their real configuration.
Partial Mirror 1 Size (GB)	√	√	√	
Partial Mirror 2 Size (GB)	√	√	√	
Partial Mirror 3 Size (GB)	√	√	√	
Partial Mirror 4 Size (GB)	√	√	√	
Mirror TAD0	√	√	√	
ADDDC Sparing	√	√	√	
NUMA Optimized	√	√	√	
SNC	√	√	√	
UMA-Based Clustering	√	√	√	
Patrol Scrub	√	√	√	
Correctable Error Threshold	√	√	√	For Intel Firmware Customization support, user should know the configuration and choose proper value to update, or it may cause potential issue for RAS Error handling.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Memory Corrected Error	√	√	√	
Cloaking	√	√	√	
Partial Cache Line Sparing PCLS	√	√	√	
Memory Bank Sparing	√	√	√	
Trigger SW Error Threshold	√	√	√	
SW Per Bank Threshold	√	√	√	
SW Correctable Error Time Window	√	√	√	
Advanced: Memory Configuration: Adv MemTest Rank Selection				
Number of Ranks to Test	√	√	√	
Rank location entry 0	√	√	√	
Rank location entry 1	√	√	√	
Rank location entry 2	√	√	√	
Rank location entry 3	√	√	√	
Rank location entry 4	√	√	√	
Rank location entry 5	√	√	√	
Rank location entry 6	√	√	√	
Rank location entry 7	√	√	√	
Advanced: System Event Log				
System Errors	√	√	√	
System Poison	√	√	√	
Viral Status	√	√	√	
IIO/PCH Global Error Support	√	√	√	
WHEA Support	√	√	√	
IIO Error Registers Clear	√	√	√	
OS Native AER Support	√	√	√	
IIO eDPC Support	√	√	√	
IIO eDPC Interrupt	√	√	√	
IIO eDPC ERR_COR Message	√	√	√	
PCIe Poison TLP Egress Blocking	√	√	√	
PCIE Correctable Errors	√	√	√	
PCIE Correctable Error Threshold	√	√	√	
Assert NMI on SERR	√	√	√	
Assert NMI on PERR	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Advanced: System Event Log: PCIE Fatal Error Mask Setting				
Data Link Protocol Error Mask	√	√	√	
Surprise Down Error Mask	√	√	√	
Poisoned TLP Mask	√	√	√	
Flow Control Protocol Error Mask	√	√	√	
Completion Timeout Mask	√	√	√	
Unexpected Completion Mask	√	√	√	
Receiver Overflow Mask	√	√	√	
Malformed TLP Mask	√	√	√	
ECRC Error Mask	√	√	√	
ACS Violation Mask	√	√	√	
Uncorrectable Internal Error Mask	√	√	√	
MC Blocked TLP Mask	√	√	√	
AtomicOp Egress Blocked Mask	√	√	√	
TLP Prefix Blocked Error Mask	√	√	√	
Advanced: Integrated IO Configuration				
Intel(R) VT for Directed I/O	√	√	√	
PRS Capability for PCIe	√	√	√	
ACS Control	√	√	√	Need enable Intel(R) VT for Directed I/O first
DMA Control Opt-In Flag	√	√	√	
Pre-boot DMA Protection	√	√	√	
CXL Type 3 Legacy	√	√	√	
CXL Security Level	√	√	√	
DMI-PCIe Port MPSWorkaround	√	√	√	
Snoop Response Hold Off for PCIe Stack	√	√	√	
Relaxed Ordering	√	√	√	
No Snoop(Sck0 IOAT Function 0)	√	√	√	
No Snoop(Sck0 IOAT Function 1)	√	√	√	
No Snoop(Sck0 IOAT Function 2)	√	√	√	
No Snoop(Sck0 IOAT Function 3)	√	√	√	
No Snoop(Sck0 IOAT Function 4)	√	√	√	
No Snoop(Sck0 IOAT Function 5)	√	√	√	
No Snoop(Sck0 IOAT Function 6)	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
No Snoop(Sck0 IOAT Function 7)	√	√	√	
No Snoop(Sck1 IOAT Function 0)	√	√	√	
No Snoop(Sck1 IOAT Function 1)	√	√	√	
No Snoop(Sck1 IOAT Function 2)	√	√	√	
No Snoop(Sck1 IOAT Function 3)	√	√	√	
No Snoop(Sck1 IOAT Function 4)	√	√	√	
No Snoop(Sck1 IOAT Function 5)	√	√	√	
No Snoop(Sck1 IOAT Function 6)	√	√	√	
No Snoop(Sck1 IOAT Function 7)	√	√	√	
Integrated IO Configuration: PCIe Slot Bifurcation Setting				
Riserx_Slot_x Bifurcation	√	√	√	
Integrated IO Configuration: Processor PCIe Link Speed				
Integrated IO Configuration: Processor PCIe Link Speed: Socket x PCIe Link Speed				
Socket x, DMI	√	√	×	
Socket x, PCIe Port 0a	√	√	√	
Socket x, PCIe Port 0b	√	√	√	
Socket x, PCIe Port 0c	√	√	√	
Socket x, PCIe Port 0d	√	√	√	
Socket x, PCIe Port 1a	√	√	√	
Socket x, PCIe Port 1b	√	√	√	
Socket x, PCIe Port 1c	√	√	√	
Socket x, PCIe Port 1d	√	√	√	
Socket x, PCIe Port 2a	√	√	√	
Socket x, PCIe Port 2b	√	√	√	
Socket x, PCIe Port 2c	√	√	√	
Socket x, PCIe Port 2d	√	√	√	
Socket x, PCIe Port 3a	√	√	√	
Socket x, PCIe Port 3b	√	√	√	
Socket x, PCIe Port 3c	√	√	√	
Socket x, PCIe Port 3d	√	√	√	
Socket x, PCIe Port 4a	√	√	√	
Socket x, PCIe Port 4b	√	√	√	
Socket x, PCIe Port 4c	√	√	√	
Socket x, PCIe Port 4d	√	√	√	
Integrated IO Configuration: Volume Management Device				
Riser1 Volume Management Device(CPU0,PE2)	√	√	√	Intel® Server Board M50FCP2SBSTD, riser 1 with retimer.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
VMD for Direct Assign(CPU0,PE2)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU0 Port PE2A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU0 Port PE2B)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD2 (CPU0 Port PE2C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU0 Port PE2D)	√	√	√	Intel® Server Board M50FCP2SBSTD
Riser3, NVMe Volume Management Device(CPU1,PE0)	√	√	√	Intel® Server Board M50FCP2SBSTD, riser 3 with NVMe card.
VMD for Direct Assign(CPU1,PE0)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU1 Port PE0A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU1 Port PE0B)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD2 (CPU1 Port PE0C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU1 Port PE0D)	√	√	√	Intel® Server Board M50FCP2SBSTD
Direct HSBP Volume Management Device(CPU0,PE3)	√	√	√	Intel® Server Board M50FCP2SBSTD, HSBP direct connection.
VMD for Direct Assign(CPU0,PE3)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU0 Port PE3A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU0 Port PE3B)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD2 (CPU0 Port PE3C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU0 Port PE3D)	√	√	√	Intel® Server Board M50FCP2SBSTD
Direct HSBP Volume Management Device(CPU0,PE4)	√	√	√	Intel® Server Board M50FCP2SBSTD, HSBP direct connection.
VMD for Direct Assign(CPU0,PE4)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU0 Port PE4A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU0 Port PE4B)	√	√	√	
PCIe-SSD2 (CPU0 Port PE4C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU0 Port PE4D)	√	√	√	Intel® Server Board M50FCP2SBSTD

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Direct HSBP Volume Management Device(CPU1,PE3)	√	√	√	Intel® Server Board M50FCP2SBSTD, HSBP direct connection.
VMD for Direct Assign(CPU1,PE3)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU1 Port PE3A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU1 Port PE3B)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD2 (CPU1 Port PE3C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU1 Port PE3D)	√	√	√	Intel® Server Board M50FCP2SBSTD
Direct HSBP Volume Management Device(CPU1,PE4)	√	√	√	Intel® Server Board M50FCP2SBSTD, HSBP direct connection.
VMD for Direct Assign(CPU1,PE4)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD0 (CPU1 Port PE4A)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD1 (CPU1 Port PE4B)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD2 (CPU1 Port PE4C)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe-SSD3 (CPU1 Port PE4D)	√	√	√	Intel® Server Board M50FCP2SBSTD
PCIe M.2 Volume Management Device (CPU0 PCH)	√	√	√	Intel® Server Board M50FCP2SBSTD
VMD for Direct Assign(PCH ports)	√	√	√	Intel® Server Board M50FCP2SBSTD
M.2 PCIE_1	√	√	√	Intel® Server Board M50FCP2SBSTD
M.2 PCIE_2	√	√	√	Intel® Server Board M50FCP2SBSTD
2U Riser Volume Management Device(CPU0 PE0)	√	√	√	Intel® Server Board D50DNP1SB, 2U riser.
VMD for Direct Assign(CPU0,PE0)	√	√	√	Intel® Server Board D50DNP1SB
PCIe-SSD1 (CPU0 Port PE0A)	√	√	√	Intel® Server Board D50DNP1SB
2U Riser Volume Management Device(CPU1 PE1)	√	√	√	Intel® Server Board D50DNP1SB, 2U riser.
VMD for Direct Assign(CPU1,PE1)	√	√	√	Intel® Server Board D50DNP1SB
PCIe-SSD0 (CPU1 Port PE1D)	√	√	√	Intel® Server Board D50DNP1SB
PCIe M.2 Volume Management Device (CPU0 PCH)	√	√	√	Intel® Server Board D50DNP1SB

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
VMD for Direct Assign(PCH ports)	√	√	√	Intel® Server Board D50DNP1SB
M.2 PCIE_1	√	√	√	Intel® Server Board D50DNP1SB
M.2 PCIE_2	√	√	√	Intel® Server Board D50DNP1SB
Integrated IO Configuration: PCIe Misc. Configuration				
PCIe ASPM Support (Global)	√	√	√	
Socket X Port Y ECRC Generation	√	√	√	
Socket X Port Y ECRC Check	√	√	√	
Socket X Port Y ASPM Support	√	√	√	
CPU0 Port1A TxEq Override Mode	√	√	√	
CPU0 Port2A TxEq Override Mode	√	√	√	
CPU1 Port0A TxEq Override Mode	√	√	√	
CPU1 Port3A TxEq Override Mode	√	√	√	
Integrated IO Configuration: NTB Configuration				
NTB PCIe Port PE1 on CPU socket 0/1	√	√	√	Intel® Server Board M50FCP2SBSTD
Enable NTB BARs	×	×	√	
Enable SPLIT BARs	×	×	√	
Imbar1 Size	×	×	√	
Imbar2_0 Size	×	×	√	
Imbar2_1 Size	×	×	√	
Imbar2 Size	×	×	√	
Embar1 Size	×	×	√	
Embar2_0 Size	×	×	√	
Embar2_1 Size	×	×	√	
Embar2 Size	×	×	√	
Crosslink control Override	×	×	√	
NTB PCIe Port PE2 on CPU socket 0/1	√	√	√	Intel® Server Board M50FCP2SBSTD
Enable NTB BARs	×	×	√	
Enable SPLIT BARs	×	×	√	
Imbar1 Size	×	×	√	
Imbar2_0 Size	×	×	√	
Imbar2_1 Size	×	×	√	
Imbar2 Size	×	×	√	
Embar1 Size	×	×	√	
Embar2_0 Size	×	×	√	
Embar2_1 Size	×	×	√	
Embar2 Size	×	×	√	
Crosslink control Override	×	×	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
NTB PCIe Port PE3 on CPU socket 0	√	√	√	Intel® Server Board D50DNP1SB
Enable NTB BARs	×	×	√	
Enable SPLIT BARs	×	×	√	
Imbar1 Size	×	×	√	
Imbar2_0 Size	×	×	√	
Imbar2_1 Size	×	×	√	
Imbar2 Size	×	×	√	
Embar1 Size	×	×	√	
Embar2_0 Size	×	×	√	
Embar2_1 Size	×	×	√	
Embar2 Size	×	×	√	
Crosslink control Override	×	×	√	
NTB PCIe Port PE4 on CPU socket 0/1	√	√	√	Intel® Server Board D50DNP1SB
Enable NTB BARs	×	×	√	
Enable SPLIT BARs	×	×	√	
Imbar1 Size	×	×	√	
Imbar2_0 Size	×	×	√	
Imbar2_1 Size	×	×	√	
Embar1 Size	×	×	√	
Embar2_0 Size	×	×	√	
Embar2_1 Size	×	×	√	
Embar2 Size	×	×	√	
Crosslink control Override	×	×	√	
NTB Link Train by BIOS	√	√	√	
NTB PCIe Port PE2 on CPU socket 1	√	√	√	Intel® Server Board D50DNP1SB
Enable NTB BARs	×	×	√	
Enable SPLIT BARs	×	×	√	
Imbar1 Size	×	×	√	
Imbar2_0 Size	×	×	√	
Imbar2_1 Size	×	×	√	
Imbar2 Size	×	×	√	
Embar1 Size	×	×	√	
Embar2_0 Size	×	×	√	
Embar2_1 Size	×	×	√	
Embar2 Size	×	×	√	
Crosslink control Override	×	×	√	
Advanced: Mass Storage Controller Configuration				
Intel(R) Storage Module	×	×	x	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Advanced: Mass Storage Controller Configuration: SATA Controller 0/1 (Port 0–7)				
SATA Controller 0/1 Configuration	×	×	x	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
AHCI Capable SATA Controller	√	√	√	
SATA RAID Options	x	√	x	Information only.
SATA HDD Staggered Spin-Up	√	√	√	
SATA Controller 0/1 Port 0…7	×	√	x	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Advanced: PCI Configuration				
MMIO High Base	√	√	√	
Memory Mapped I/O Size	√	√	√	
Add-in Video Adapter	√	√	√	
Onboard Video	√	√	√	
Fast Video	√	√	√	
Legacy VGA Socket	√	√	√	
ARI Support	√	√	√	
SR-IOV Support	√	√	√	
Advanced: PCI Configuration: NIC Configuration				
Onboard NIC1 Type	×	×	×	Information only.
NIC1 Controller	×	√	×	Intel® Server Board D50DNP1SB
Advanced: PCI Configuration: UEFI Network Stack				
UEFI Network Stack	√	√	√	
IPv4 PXE Support	√	√	√	
IPv6 PXE Support	√	√	√	
Advanced: PCI Configuration: UEFI Option ROM Control				
NIC Controller	×	×	×	Information only.
NIC Card 1 Port1 OPROM Slot:	×	×	×	Information only.
NIC Card 1 Port2 OPROM Slot:	×	×	×	Information only.
Fiber Channel	×	×	×	Information only.
FC Adapter Slot	×	×	×	Information only.
FC Adapter Slot	×	×	×	Information only.
Storage Controller	×	×	×	Information only.
Storage Card 1 OPROM Slot:	×	×	×	Information only.
Storage Card 2 OPROM Slot:	×	×	×	Information only.
Others	×	×	×	Information only.
OPROM Name Slot:	×	×	×	Information only.
Advanced: Serial Port Configuration				
Serial A Enable	√	√	√	
Serial A Address	√	√	√	
Serial A IRQ	×	√	×	
Advanced: USB Configuration				
USB Front Ports Enable	√	√	√	
USB Rear Ports Enable	√	√	√	
USB Internal Ports Enable	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Advanced: System Acoustic and Performance Configuration				
Set Fan Profile	√	√	√	BMC-controlled option. BIOS does not support Intel Server Configuration Utility/Intel Server Information Retrieval Utility via `/bcs` command.
Fan PWM Offset	×	×	×	
Air Flow Limit	×	×	×	
Exit Air Temp	×	×	×	
Fan UCC	×	×	×	
Security				
Administrator Password Status	×	√	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
User Password Status	×	√	×	
Set Administrator Password	×	√	×	Intel Server Configuration Utility does not support `/bcs` command, but supports `/bap`.
Set User Password	×	√	×	Intel Server Configuration Utility does not support `/bcs` command, but supports `/bup`.
Power On Password	√	√	√	
Front Panel Lockout	√	√	√	
Current TPM Device	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
TPM2 Operation	×	×	×	
PCR Bank: SHA1	×	×	×	
PCR Bank: SHA256	×	×	×	
TPM FW Update	×	×	×	
TPM FW Version	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Server Management				
IPMI Security Policy	x	x	x	
Reset on CATERR	√	√	√	
Reset on ERR2	√	√	√	
Resume on AC Power Loss	×	√	x	BMC-controlled option. For Intel Server Configuration Utility/Intel Server Information Retrieval Utility, this setting should be got from the BMC via IPMI but not from the BIOS variable via `/bcs`.
Power Restore Delay	√	×	x	BMC-controlled option. The BIOS does not support Intel Server Configuration Utility/Intel Server Information Retrieval Utility via `/bcs` command.
Power Restore Delay Value	√	×	x	
Clear System Log	×	√	×	Intel Server Configuration Utility does not support `/bcs` command, but support `/csel`.
FRB-2 Enable	√	√	√	
FRB-2 Timeout Value	√	√	√	
OS Boot Watchdog Timer	√	√	√	
OS Boot Watchdog Timer Policy	√	√	√	
OS Boot Watchdog Timer Timeout	√	√	√	
Plug & Play BMC Detection	√	√	√	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Shutdown Policy	×	√	x	BMC-controlled option. For Intel Server Configuration Utility/Intel Server Information Retrieval Utility, this setting should be got from the BMC via IPMI but not from the BIOS variable via `/bcs`.
Server Management: Console Redirection				
SOL for Baseboard Mgmt	×	x	×	BMC-controlled option. BIOS does not support Intel Server Configuration Utility/Intel Server Information Retrieval Utility via `/bcs` command.
SOL for Dedicated Mgmt NIC	×	x	×	
Console Redirection	√	√	√	
Flow Control	√	√	√	
Baud Rate	√	√	√	
Terminal Type	√	√	√	
Terminal Resolution	√	√	√	
Server Management: System Information				
Board Part Number	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
Board Serial Number	×	×	×	
System Part Number	×	×	×	
System Serial Number	×	×	×	
Chassis Part Number	×	×	×	
Chassis Serial Number	×	×	×	
Asset Tag	×	×	×	
BMC Status	×	×	×	
BMC Firmware Revision	×	×	×	
ME Status	×	×	×	
ME Firmware Revision	×	×	×	
UUID	×	×	×	
Server Management: BMC LAN Configuration **Note:** For Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility, if need support, all settings under BMC LAN Configuration should get from BMC via IPMI but not from BIOS variable via `/bcs`. This screen field does not support Intel® Firmware Customization.				
Baseboard LAN configuration	×	×	×	*Information only*. Does not support `/bcs` command for the Intel Server Configuration Utility.
IP Source	×	×	×	Does not support `/bcs` command for the Intel Server Configuration Utility.
IP address	×	×	×	
Subnet Mask	×	×	×	
Gateway IP	×	×	×	
Baseboard LAN IPv6 configuration	×	×	×	*Information only*. Does not support `/bcs` command for the Intel Server Configuration Utility.
IPv6 Source	×	×	×	Does not support `/bcs` command for the Intel Server Configuration Utility.
IPv6 Address	×	×	×	
Gateway IPv6	×	×	×	
IPv6 Prefix Length	×	×	×	
Dedicated Management LAN Configuration	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
IP Source	×	×	×	Does not support `/bcs` command for the Intel Server Configuration Utility.
IP address	×	×	×	
Subnet Mask	×	×	×	

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Gateway IP	×	×	×	
Dedicated Management LAN IPv6 Configuration	×	×	×	Information only. Does not support `/bcs` command for the Intel Server Configuration Utility.
IPv6 Source	×	×	×	Does not support `/bcs` command for the Intel Server Configuration Utility.
IPv6 Address	×	×	×	
Gateway IPv6	×	×	×	
IPv6 Prefix Length	×	×	×	
BMC DHCP Host Name	×	×	×	
Server Management: BMC LAN Configuration: User Configuration				
Password Complexity	×	×	×	Does not support `/bcs` command for the Intel Server Configuration Utility.
User ID	×	×	×	
Privilege	×	×	×	
User Status	×	×	×	
User Name	×	×	×	
User Password	×	×	×	
Boot Maintenance Manager				
Boot Maintenance Manager: Advanced Boot Options				
System Boot Timeout	√	√	√	
Early System Boot Timeout	√	√	√	
USB Boot Priority	√	√	√	
Boot Maintenance Manager: Advanced Boot Options: Secure Boot Configuration				
Current Secure Boot State	×	√	×	Intel Firmware Customization support by option Secure Boot Enable, to enable Secure boot feature by Intel Firmware Customization, need follow EPS to set Secure Boot Enable=enable and Boot Mode=UEFI. For support related to Intel Server Configuration Utility, Secure Boot just supports proprietary solution defined in the *Intel® Server Configuration Utility User Guide*, but does not support other general commands for general setup options, such as `/s` or `/bcs` command.
Attempt Secure Boot	√	√	×	
Boot Maintenance Manager: Add EFI Boot Option				
EFI Boot Option to be selected	×	×	×	For Intel Server Configuration Utility, this screen field does NOT support changes through Intel Server Configuration Utility with `/bcs` command. However, user can use Intel Server Configuration Utility `/bbo` or `/bbosys` command to set boot order.
Boot Maintenance Manager: Delete EFI Boot Option				
EFI Boot Option to be deleted	×	×	×	For Intel Server Configuration Utility, this screen field does NOT support changes through Intel Server Configuration Utility with `/bcs` command. However, user can use Intel Server Configuration Utility `/bbo` or `/bbosys` command to set boot order.

Setup Option	Intel® Firmware Customization	Intel® Server Configuration Utility	OOB Configuration	Comments
Boot Maintenance Manager: Change Boot Order				
Change the order	×	×	×	1. For Intel Server Configuration Utility, this screen field does NOT support changes through Intel Server Configuration Utility with `/bcs` command. However, user can use Intel Server Configuration Utility `/bbo` or `/bbosys` command to set boot order. 2. Intel Firmware Customization can only support Add boot order option by customized Intel Firmware Customization GUI
Boot Manager Screen				
UEFI Internal Shell	×	×	×	
UEFI Floppy Driver	×	×	×	
UEFI Hard Disk Driver	×	×	×	
UEFI CD-ROM Driver	×	×	×	
UEFI NET Driver	×	×	×	
UEFI HTTPs boot	×	×	×	
Error Manager				
Save & Exit				
Save Changes and Exit	×	×	×	
Discard Changes and Exit	×	×	×	
Save Changes	×	×	×	
Discard Changes	×	×	×	
Load Default Values	×	×	×	
Save as User Default Values	×	×	×	
Load User Default Values	×	×	×	

Appendix B. Glossary

Term	Definition
16-bit legacy	The traditional personal computer environment. Includes legacy Option ROMs and legacy 16-bit code.
ACM	Authenticated Code Mode.
ACPI	Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft, and Toshiba. ACPI enables and supports reliable power management through improved hardware and operating system coordination.
AES	Advanced Encryption Standard – encryption algorithm.
Intel® AES-NI	Intel® AES New Instructions.
AER	Advanced Error Reporting.
AHCI	Advanced Host Controller Interface, a USB controller standard.
AMB	Advanced Memory Buffer.
AML	ACPI Machine Language.
ANSI	American National Standards Institute.
API	Application Programming Interface. A software abstraction provided by the BIOS to applications and/or the operating system.
AP	Application Processor.
ASCII	American Standard Code for Information Interchange. An 8-level code (7 bits plus parity check) widely used in data processing and data communications systems.
ASR	Asynchronous System Reset.
ATA	Advanced Technology Attachment, a disk interface standard.
BAR	Base Address Register. Device configuration registers that define the start address, length, and type of memory space required by a device.
BERT	Boot Error Record Table.
BIOS	Basic Input/Output System.
BIST	Built-in Self-Test.
BMC	Baseboard Management Controller.
BOT	Boot Order Table.
BSP	Bootstrap processor. The processor selected at boot time to be the primary processor in a multi-processor system.
CATERR#	Catastrophic Error Signal.
CD	Compact Disk.
CE	Correctable Error.
CLTT	Closed Loop Thermal Throttling.
CMCI	Corrected Machine Check Interrupt.
CMOS	Complementary Metal-oxide-semiconductor.
COM1	Communication Port 1, serial port 1.
COM2	Communication Port 2, serial port 2.
CPEI	Corrected Platform Error Interrupt.
CRTM	Core Root of Trust Measurement.
CSM	Compatibility Support Module.
PMem	Data Center Persistent Memory Module (Refers to Intel® Optane™ DC Persistent Memory Module).
DDR3	Double Data Rate 3 is a high bandwidth memory technology.
DIMM	Dual In-line Memory Module, a plug-in memory module with signal and power pins on both sides of the internal printed circuit board (front and back).
DMA	Direct Memory Access.
DMAR	DMA Resource.
DRAM	Dynamic Random Access Memory, memory chips from which DIMMs are constructed.

Term	Definition
DR	Dual Rank – memory DIMM organization, DRAMs organized in two ranks.
DRHD	DMA Remapping Hardware Unit Definition.
DSDT	Differentiated System Description Table. An OEM must supply a DSDT to an ACPI-compatible operating system. The DSDT contains the Differentiating Definition Block, which supplies the implementation and configuration information about the base system.
DWORD	Double Word, a 32-bit quantity.
DXE	Driver Execution Environment. Component of Intel® Platform Innovation Framework for EFI architecture.
ECC	Error Correction Code. Refers to a memory system that has extra bit(s) to support limited detection/correction of memory errors.
EEPROM	Electrically Erasable Programmable Read Only Memory – called flash memory.
EFI	Extensible Firmware Interface *(see also UEFI).*
EHCI	Enhanced Host Controller Interface, a USB controller standard.
EINJ	Error Injection.
EMP	Emergency Management Port.
EPS	External Product Specification.
EPSD	Enterprise Platforms and Services Division – parent Division for Server development.
ERST	Error Record Serialization Table.
FIPS	Federal Information Processing Standard.
Formset	Framework term for display pages, which includes Setup pages.
FRB	Fault Resilient Booting.
FRU	Field Replaceable Unit.
FSB	Front Side Bus.
FV	Firmware Volume.
Gb	Gigabit, 1,073,741,824 bits – lowercase “b” distinguishes “bits” from uppercase “B” for “bytes”.
GbE	Gigabit Ethernet, an Ethernet connection operating at gigabit/second speed.
GB	Gigabyte. 1024 Megabytes, 1,073,741,824 bytes.
GPA	Guest Physical Address.
GUID	Globally Unique Identifier.
HEST	Hardware Error Source Table.
HLT	Halt.
KB	Kilobyte; 1024 bytes .
Intel® HT Technology	Intel® Hyper-Threading Technology.
IBMC	Integrated Baseboard Management Controller.
ICH	I/O Control Hub, a chipset component.
IDE	Integrated Drive Electronics, a disk interface standard.
IMC	Integrated Memory Controller.
INTR	Interrupt Request.
I/O	Input/Output.
IOH	Input/output hub, a chipset component.
IPMI	Intelligent Platform Management Interface – an industry standard that defines standardized, abstracted interfaces to platform management hardware.
IRQ	Interrupt Request.
JEDEC	Joint Electron Device Engineering Council, industry organization for memory standards
KB	Kilobyte; 1024 bytes.
KCS	Keyboard Controller Style.
KVM	Keyboard, Video, and Mouse – an attachment that mimics those devices and connects them to a remote I/O user.

Term	Definition
LAN	Local Area Network.
LED	Light Emitting Diode.
LHEH	Low Level Hardware Error Handler.
Mb	Megabit, 1,048,576 bits – lowercase “b” distinguishes “bits” from uppercase “B” for “bytes”.
MB	Megabyte. 1024 Kilobytes, 1,048,576 bytes.
MC	Multi-core.
MCA	Machine Check Architecture.
MCE	Machine Check Exception.
Intel® ME	Intel® Management Engine.
MHz	Megahertz, a frequency measurement, a million cycles/second.
MMIO	Memory Mapped I/O.
MRC	Memory Reference Code.
MSR	Model Specific Register.
MTRR	Memory Type Range Register.
MT/s	Megatransfers per second.
MWAIT	Monitor Wait.
NIC	Network Interface Card.
Intel® NM	Intel® Node Manager – now Intel® Intelligent Power Node Manager.
NMI	Non-Maskable Interrupt.
NPTM	Node Power Thermal Management – now Intel® Intelligent Power Node Manager.
NUMA	Non-Uniform Memory Access (secondary usage as Non-Uniform Memory Architecture).
OEM	Original Equipment Manufacturer.
OLTT	Open Loop Thermal Throttling.
OS	Operating System.
PAE	Physical Address Extension.
PCI	Peripheral Component Interconnect, or PCI Standard.
PCIe*	PCI Express*.
PCR	Platform Configuration Register.
PECI	Platform Environmental Control Interface.
PEI	Pre EFI Initialization. Component of Intel® Platform Innovation Framework for EFI architecture.
PERR	Program Error.
PIC	Programmable Interrupt Controller.
PMI	Platform Management Interrupt.
PnP	Plug and Play. Used as “PnP BIOS” and “PnP ISA”.
POR	Process of Record.
POST	Power On Self-Test.
PSHED	Platform specific Hardware Error Driver.
PTS	Platform Trust Services.
PXE	Pre-execution Environment.
Intel® QPI	Intel® QuickPath Interconnect.
QR	Quad Rank – memory DIMM organization, DRAMs organized in four ranks.
RAID	Redundant Array of Inexpensive Disks – provides data security by spreading data over multiple disk drives. RAID 0, RAID 1, RAID 10, and RAID 5 are different patterns of data on varying numbers of disks to provide varying degrees of security and performance.
RAS	Reliability, Availability, Serviceability.
RDIMM	Registered DIMM (also called buffered) memory modules have a register between the SDRAM modules and the system's memory controller.

Term	Definition
RMRR	Reserved Memory Region Reporting.
RTC	Real Time Clock.
ROM	Read-only memory.
RS-232	Recommended Standard 232 for serial binary data transmission.
RT	Runtime. Component of Intel® Platform Innovation Framework for EFI architecture.
RTM	Root of Trust Measurement.
RTR	Root of Trust Reporting.
RTS	Root of Trust Storage.
SAS	Serial Attached SCSI, a high speed serial data version of SCSI.
SATA	Serial ATA, a high speed serial data version of the disk ATA interface.
SCI	System Control Interrupt.
SCSI	Small Computer System Interface, a connection usually used for disks of various types.
SDR	Sensor Data Record.
SEC	Security. Component of Intel® Platform Innovation Framework for EFI architecture.
SEEPROM	Serial Electrically Erasable Programmable Read Only Memory.
SEL	System Event Log.
SERR	System Error.
SFO	Spare Fail-Over (event).
SIMD	Single Instruction Multiple Data – instruction type.
SMBIOS	System Management BIOS.
SMI	System Management Interrupt.
SMM	System Management mode.
SOL	Serial-over-LAN.
SPD	Serial Presence Detect.
SPI	Serial Peripheral Interface, a serial data interface used for Flash memory.
SR	Single Rank – memory DIMM organization, DRAMs organized in a single rank.
SRK	Storage Root Key.
SRTM	Static Root of Trust Measurement.
SSE	Streaming SIMD Extensions.
TCG	Trusted Computing Group.
TjMax	Maximum junction temperature.
TM1	Thermal Monitor 1.
TPM	Trusted Platform Module.
TSE	Text Setup Engine – the Setup screen display and options choosing utility.
TSS	TCG Software Stack.
Intel® TXT	Intel® Trusted Execution Technology.
UDIMM	Unregistered DIMM (also called unbuffered) memory modules do not have a register between the SDRAM modules and the system's memory controller.
UE or UCE	Uncorrectable Error.
UEFI	Unified Extensible Firmware Interface – replacement for Legacy BIOS and Legacy DOS interface.
UGA	Ultra-Graphics Array.
USB	Universal Serial Bus, a standard serial expansion bus meant for connecting peripherals.
UUID	Universally Unique Identifier. See also GUID.
Intel® VT	Intel® Virtualization Technology.
Intel® VT-d	Intel® Virtualization Technology (Intel® VT) for Directed I/O.
WFM	Wired For Management.
WHEA	Windows* Hardware Error Architecture.

Term	Definition
WHQL	Windows* Hardware Quality Labs.
XD bit	Execute Disable bit. An IA-32 processor that supports the Execute Disable Bit feature can prevent data pages from being used by malware to execute code.