Intel® Server Board S2600 Family

BIOS Setup User Guide

For the Intel® Server Board S2600 family supporting the Intel® Xeon processor Scalable family and 2nd Generation Intel® Xeon processor Scalable family.

Rev 1.1

November 2019

Intel® Server Products and Solutions

Document Revision History

Date	Revision	Changes
October 2017	*1.0*	*First release based on* Intel® Server Board S2600 Family BIOS Setup Utility Specification.
November 2019	*1.1*	*Update based on* Intel Xeon Processor Scalable Family Refresh BIOS Setup Specification 1_13

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at Intel.com, or from the OEM or retailer.

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 claim 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.

Copies of documents which 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, and Intel Xeon Phi 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 document provides an overview of the features and functions of the embedded BIOS setup utility for Intel® server boards and systems supporting the Intel® Xeon® processor Scalable family. The text-based setup utility controls the platform's built-in devices, the boot manager, and error manager. Use BIOS setup to:

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

2.   BIOS Setup Operation

The BIOS setup utility is a text-based utility that allows the user to configure the system and view current settings and environment information for the platform devices. The setup utility controls the platform's built-in devices, the boot manager, and error manager.

The BIOS setup interface consists of a number of pages or screens. Each page contains information or links to other pages. The advanced tab in Setup 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:

- Localization – The Intel® server board BIOS is only available in English.
- Console Redirection – BIOS setup is functional via Console Redirection (see Intel® Server Board S2600 Family BIOS EPS, Sections 7.4) over various terminal emulation standards. When Console Redirection is enabled, the POST display out is in purely Text Mode due to Redirection data transfer in a serial port data terminal emulation mode. This may limit some functionality for compatibility, such as, usage of colors or some keys or key sequences or support of pointing devices.
    - o Setup screens are designed to be displayable in a 100-character x 31-line format to work with Console Redirection; although, that screen layout should display correctly on any format with longer lines or more lines on the screen.
- Password protection – BIOS Setup may be protected from unauthorized changes by setting an Administrative Password in the Security screen. When an Administrative Password has been set, all selection and data entry fields in setup (except System Time and Date) are grayed out and cannot be changed unless the Administrative Password has been entered.

Note: If an Administrative Password has not been set, anyone who boots the system to setup has access to all selection and data entry fields in Setup and can change any of them. For more information about BIOS password protection, see *Intel® Server Board S2600 Family BIOS EPS*, Section 9.1.

2.1   Setup Page Layout

The setup page layout is sectioned into functional areas. Each occupies a specific area of the screen and has dedicated functionality. The following table lists and describes each functional area.

The setup page is designed to a format of 80 x 24 (24 lines of 80 characters each). The typical display screen in a Legacy mode or terminal emulator mode is 80 characters by 25 lines but with "line wrap" enabled (which it usually is). The 25th line cannot be used with the setup page.

Table 1. BIOS setup page layout

Functional Area	Description
Title Bar	The Title Bar is located at the top of the screen and 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 there are more tabs than can be displayed on the Title Bar, they will scroll off to the left or right of the screen and temporarily disappear from the visible Title Bar. Using the arrow keys will scroll them back onto the visible Title Bar. When the arrow keys reach either end of the Title Bar, they will "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 currently viewing. The Page Title gives further information.
Page Title	In a multi-level hierarchy of pages beneath one of the top-level Tabs, the Page Title identifying the specific page that the user is viewing is located in the upper left corner of the page. Using the **<ESC>** key will return the user to the higher level in the hierarchy, until the top-level page is reached.

Functional Area	Description
Setup Item List	The setup item list is a set of control entries and informational items. The list is displayed in two columns. For each item in the list: 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 24 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 demarcated 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 24 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 operator navigates to the desired selection and presses **<Enter>** to go to the new screen.
Item-Specific Help Area	The item-specific help area is located 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, and so on. The help area is a 29 character by 11 line section of the 80 x 24 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 will be arbitrarily wrapped to a new line after the 29th character. Text that extends beyond the end of the 11th line will not be displayed.
Keyboard Command Area	The keyboard command area is located 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, it is important to wait until the BIOS "discovers" the keyboard and beeps – until the USB controller has been initialized and the USB keyboard activated, key pressing will not be read by the system.

When the setup utility is entered, the front page is displayed initially. However, serious errors cause the system to display the Error Manager screen instead of the front page.

It is also possible to cause a boot directly to setup using an IPMI 2.0 command Get/Set System Boot Options. For details on that capability, see the explanation in the IPMI description.

2.3 Exit BIOS Setup

There are three methods to exit BIOS setup:

- Press the hotkey <F10>
- Select Save Changes and Exit
- Select **Discard Changes and Exit**

Whether changes are made or not, the system will do a cold reset after any of the above methods are applied. For more information on the Save & Exit screen, see Section 3.9.

2.4 Setup Navigation Keyboard Commands

The bottom right portion of the setup screen provides a list of commands that are used to navigate through the Setup utility. These commands are displayed at all times.

Each setup menu page contains a number of features. Each feature is associated with a value field, except those used for informative purposes. Each value field contains configurable parameters. Depending on the security option chosen and in effect by the password, a menu feature's value may or may not be changed. If a value cannot be changed, its field is made inaccessible and appears greyed out.

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 will have 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 chapter 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 I n 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 option(s) 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 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 Menu

The setup menu 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 below, with links to each of the screens named.

Table 3. Screen map

Top-Level Categories	Second Level Screens	Third Level Screens
Main Screen	-	-
Advanced Screen	Processor Configuration	-
	Power & Performance	Uncore Power Management
		CPU P State Control
		Hardware P States
		CPU C State Control
	UPI Configuration	-
	Memory Configuration	-
		Memory RAS and Performance Configuration
	Integrated IO Configuration	-
	Mass Storage Controller Configuration	SATA Port Configuration
	PCI Configuration	PCIe* Slot Bifurcation Setting
		PCIe* Error Maintain
		NIC Configuration
		UEFI Network Stack
		UEFI Option ROM Control
		PCIe* Port Option ROM Control
		Processor PCIe* Link Speed
		Volume Management Device
	Serial Port Configuration	-
	USB Configuration	-
	System Acoustic and Performance Configuration	
	FPGA Configuration	-

FPGA Configuration

The FPGA Configuration screen allows the user to configure the available FPGA options.

To access this screen from the front page, select **Advanced > FPGA Configuration**. To move to another screen, press the **<Esc>** key to return to the Advanced screen, then select the desired screen.

Note: This configuration is only available on an FPGA-enabled platform.

FPGA Configuration

Socket 0 FPGA BBS Version	<BBS Version>
Socket 0 FPGA	**Enabled**/Disabled
Socket 0 BitStream	**Auto**/HSSI-BBS/None
Socket 1 FPGA BBS Version	<BBS Version>
Socket 1 FPGA	**Enabled**/Disabled
Socket 1 BitStream	**Auto**/HSSI-BBS/None

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

Figure 38. FPGA Configuration screen

1. **Socket 0 FPGA BBS Version**

   Value: <BBS Version>
   Help Text: None
   Comments: *Information only*. Displays current blue bit stream (BBS) Version loaded in the FPGA device. The Format of the Version: MajorVersion.MinorVersion.PatchVersion.DebugVersion.
   Back to: FPGA Configuration– Advanced Screen – Screen map

2. **Socket 0 FPGA**

   Value: **Enabled**/Disabled
   Help Text: None
   Comments: Enable/disabled the FPGA device on socket 0.
   Back to: FPGA Configuration– Advanced Screen – Screen map

3. **Socket 0 BitStream**

   Value: **Auto**/HSSI-BBS/None
   Help Text: None
   Comments: Select the BBS for the FPGA device. Use this option to not load the built-in BBS in the image and load a custom image after boot.
   Back to: FPGA Configuration– Advanced Screen – Screen map

4. **Socket 1 FPGA BBS Version**

   Value: <BBS Version>
   Help Text: None

Top-Level Categories	Second Level Screens	Third Level Screens

Comments: *Information only*. Displays current blue bit stream (BBS) Version loaded in the FPGA device. The Format of the Version: MajorVersion.MinorVersion.PatchVersion.DebugVersion.
Back to: FPGA Configuration– Advanced Screen – Screen map

5. Socket 1 FPGA

Value: **Enabled**/Disabled
Help Text: None
Comments: Enable/disabled the FPGA device on socket 1.
Back to: FPGA Configuration– Advanced Screen – Screen map

6. Socket 1 BitStream

Value: **Auto**/HSSI-BBS/None
Help Text: None
Comments: Select the BBS for the FPGA device. Use this option to not load the built-in BBS in the image and load a custom image after boot.
Back to: FPGA Configuration– Advanced Screen – Screen map

Security Screen

	Second Level Screens	Third Level Screens
	Console Redirection	-
Server Management Screen	System Information	-
	BMC LAN Configuration	User Configuration
Error Manager Screen	-	-
Boot Manager Screen	-	-
Boot Maintenance Manager Screen	Advanced Boot Options	Secure Boot Configuration
	Legacy CDROM Order	-
	Legacy Hard Disk Order	-
	Legacy Floppy Order	-
	Legacy Network Device Order	-

Top-Level Categories	Second Level Screens	Third Level Screens
	Legacy BEV Device Order	-
	Add EFI Boot Option	-
	Delete EFI Boot Option	-
	Change Boot Order	-
Save & Exit Screen	-	-
Tls Auth Configuration	Server CA Configuration	Enroll Cert
		Delete Cert
	Client Cert Configuration	-

3.2 Main Screen

The Main screen is the first screen that appears when entering the BIOS setup configuration utility, unless an error has occurred. If an error has occurred, the Error Manager Screen (see Section 3.8) appears instead.

Main	
Logged in as	**Administrator**/User
Platform ID	<Platform identification string>
System BIOS	
BIOS Boot From	Primary/Backup
Primary BIOS Version	<Platform.86B.xx.yy.zzzz>
Primary BIOS Build Date	<MM/DD/YYYY>
Backup BIOS Version	<Platform.86B.xx.yy.zzzz>
Backup BIOS Build Date	<MM/DD/YYYY>
Memory	
Total DDR4 Memory	<Total physical memory installed in system>
DCPMM	<Total capacity – Volatile capacity – Non-volatile capacity>
Quiet Boot	**Enabled**/Disabled
POST Error Pause	Enabled/**Disabled**
System Date	[MM/DD/YYYY]
System Weekday	[Day]
System Time	[HH:MM:SS]

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

Figure 1. 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 *Intel® Server Board S2600 Family BIOS EPS*, 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 *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12.

   Back to: Main Screen – Screen map

3. **BIOS Boot From**

   Value: **Primary**/Backup

   Help text: None

   Comments: *Information only*. Displays the exact BIOS portion on the board which is executing POST. Boot from backup BIOS means the BIOS is running in recovery mode and the primary BIOS may be corrupted.

   Back to: Main Screen – Screen map

4. **Primary BIOS Version**

   Value: <Platform.86B.xx.yy.zzzz>

   Help text: None

   Comments: *Information only*. The BIOS version uniquely identifies the primary BIOS that is currently 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:

   - Platform – Identifies the server platform.
   - `86B` – Identifies this BIOS as being an Intel® server BIOS.
   - xx – Major revision level of the BIOS.
   - yy – Release revision of the BIOS.
   - zzzz – Release number of the BIOS.

   For full details about interpreting the BIOS ID string, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.1.2

   Back to: Main Screen – Screen map

5. **Primary BIOS Build Date**

   Value: <MM/DD/YYYY>

   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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.1.2.

   Back to: Main Screen – Screen map

6. **Backup BIOS Version**

   Value: <Platform.86B.xx.yy.zzzz>

   Help text: None

   Comments: *Information only*. The BIOS version uniquely identifies the backup BIOS that is currently 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:

   - Platform – Identifies the server platform.
   - `86B` – Identifies this BIOS as being an Intel server BIOS.
   - xx – Major revision level of the BIOS.
   - yy – Release revision of the BIOS.
   - `zzzz` – Release number of the BIOS.

   For full details about interpreting the BIOS ID string, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.1.2

   Back to: Main Screen – Screen map

7. **Backup BIOS Build Date**

   Value: <MM/DD/YYYY>

   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 backup BIOS was created (built). For full details about the BIOS ID string, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.1.2.

   Back to: Main Screen – Screen map

8. **Total DDR4 Memory**

   Value: <Total physical DDR4 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 DDR4 DIMMs in GB. This item does not include DCPMM information.

   Back to: Main Screen – Screen map

9. **DCPMM**

   Value: <Total capacity – Volatile capacity – Non-volatile capacity>

   Help text: None

   Comments: *Information only*. Displays the current total DCPMM capacity and volatile/persistent /block partition size. If there is no DCPMM installed on the system, `Not Installed` is displayed.

   Back to: Main Screen – Screen map

10. 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 *Intel® Server Board S2600 Family BIOS EPS*, 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 – Screen map

11. 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 10.13.5.2.

Back to: Main Screen – Screen map

12. 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 2015 and 2099.`
`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 – `01/01/2015`.

Back to: Main Screen – Screen map

13. 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 01/01/2015 – `Thursday`.

Back to: Main Screen – Screen map

14. 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 – Screen map

## 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, although the options for different boards are not necessarily identical.



**Figure 2. 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 Screen – Screen map

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 Screen – Screen map

3. **UPI Configuration**

   Value: None

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

   Comments: *Selection only.* For more information on Memory Configuration settings, see Section 3.3.3.

   Back to: Advanced Screen – Screen map

4. **Memory Configuration**

   Value: None

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

   Comments: *Selection only.* For more information on Memory Configuration settings, see Section 3.3.4

   Back to: Advanced Screen – Screen map

5. **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 3.3.5.

   Back to: Advanced Screen – Screen map

6. **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 3.3.6.

   Back to: Advanced Screen – Screen map

7. **PCI Configuration**

   Value: None

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

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

   Back to: Advanced Screen – Screen map

8. **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 Section 3.3.8.

   Back to: Advanced Screen – Screen map

9. **USB Configuration**

   Value:       None

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

   Comments:  *Selection only.* For more information on USB Configuration settings, see Section 3.3.9.

   Back to:     Advanced Screen – Screen map

10. **System Acoustic and Performance Configuration**

    Value:       None

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

    Comments:  *Selection only.* For more information on System Acoustic and Performance Configuration settings, see section 3.3.10.

    All the information under System Acoustic and Performance Configuration page is grayed out if the *IPMI Security Policy information* on Server Management Screen is shown as '*IPMI Security Policy*:*Restricted*' and suppressed if shown as '*IPMI Security Policy*:*Deny All*'.

    Back to:     Advanced Screen – Screen map

11. **FPGA Configuration**

    Value:       None

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

    Comments:  *Selection only.* For more information on FPGA Configuration settings, see Section 3.3.11.

    Back to:     Advanced Screen – Screen map

### 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.

| Processor Configuration | | |
|---|---|---|
| Processor Socket | CPU 1 | CPU 2 |
| Processor ID | <CPUID> | <CPUID> |
| Processor Frequency | <Proc Freq> | <Proc Freq> |
| Microcode Revision | <Rev data> | <Rev data> |
| L1 Cache RAM | <L1 Cache Size> | <L1 Cache Size> |
| L2 Cache RAM | <L2 Cache Size> | <L2 Cache Size> |
| L3 Cache RAM | <L3 Cache Size> | <L3 Cache Size> |
| | | |
| Processor 1 Version | <ID string from Processor 1> | |
| Processor 2 Version | <ID string from Processor 2> | |
| | | |
| Intel(R) Hyper-Threading Tech | **Enabled**/Disabled | |
| Current Active Processor Cores | All/1/2/3/4/N-1 | |
| Active Processor Cores | **All**/1/2/3/4/N-1 | |
| | | |
| Intel(R) Virtualization Technology | Enabled/**Disabled** | |
| Intel(R) TXT | Enabled/**Disabled** | |
| Enhanced Error Containment Mode | Enabled/**Disabled** | |
| MLC Streamer | **Enabled**/Disabled | |
| MLC Spatial Prefetcher | **Enabled**/Disabled | |
| DCU Data Prefetcher | **Enabled**/Disabled | |
| DCU Instruction Prefetcher | **Enabled**/Disabled | |
| DBP-F | Enable/**Disable** | |
| LLC Prefetch | Enabled/**Disabled** | |
| RDT CAT Opportunistic Tuning | **Default 0x7FF**/Tuned 0x600/Tuned 0x003/Tuned 0x700 | |
| 3StrikeTimer | **Enabled**/Disabled | |

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

**Figure 3. Processor Configuration screen for dual–processor system**

1. **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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.3.2.

    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 Board S2600 family, 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 – Screen map

2. **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 – Screen map

3. **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 – Screen map

4. **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. There are two types of L1 cache, 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 – Screen map

5. **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 – Screen map

6. **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 – Screen map

7. **Processor 1 Version**
   **Processor 2 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 – Screen map

8. **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 processors installed in the system support Intel® Hyper-Threading Technology.

Back to:        Processor Configuration – Advanced Screen – Screen map

9. **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. If the Intel ME disables or enables processor cores, that overrides the BIOS setting. Any change to the Active Processor Cores setting lower than the previous setting updates this display.

Back to: Processor Configuration – Advanced Screen – Screen map

10. **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.

> **Note**: 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 – Screen map

11. **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.`
`Note: A change to this option requires the system to be powered off and then back on before the setting takes effect.`

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 in order for it to be enabled.

> **Note**: Intel VT is required to 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® Integrator Toolkit or Syscfg.

Back to: Processor Configuration – Advanced Screen – Screen map

## 12. 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 to support Intel TXT. For information about Intel TXT support, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.3.8.14.

> **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 – Screen map

## 13. Enhanced Error Containment Mode

Value:         Enabled/**Disabled**

Help text:    `Enable Enhanced Error Containment Mode (Data Poisoning) - Erroneous data coming from memory will be poisoned. If disabled (default), will be in Legacy Mode - No data poisoning support available.`

Comments:  none.

Back to:     Processor Configuration – Advanced Screen – Screen map

## 14. 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.3.4.1.

Back to:     Processor Configuration – Advanced Screen – Screen map

## 15. 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.3.4.1.

Back to:     Processor Configuration – Advanced Screen – Screen map

**16. 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.3.4.1.

Back to:        Processor Configuration – Advanced Screen – Screen map

**17. 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 Data 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 – Screen map

**18. 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 – Screen map

**19. LLC Prefetch**

Value:          Enabled/**Disabled**

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

Comments:   None

Back to:        Processor Configuration – Advanced Screen – Screen map

**20. RDT CAT Opportunistic Tuning**

Value:          **Default 0x7FF** / Tuned 0x600/ Tuned 0x003/Tuned 0x700

Help text:      `Cache Allocation Technology mask tuning options. NOTE: If IOT is enabled on any socket this option will override to 0x003`

Comments:   None

Back to:        Processor Configuration – Advanced Screen – Screen map

## 21. 3StrikeTimer

Value:  **Enabled**/Disabled

Help text:  `The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT (MSR 0x01a4).`

Comments:  This feature is recommended to be disabled for machine check debug purpose.

Back to:  Processor Configuration – Advanced Screen – 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.

There are four possible profiles from which to choose. 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 *Intel® Server Board S7200AP Family BIOS EPS*, Section 3.15.2.

**Note**: The fields on the Power & Performance screen do not support **SysCfg** changes with the `/bcs` command and do not support Intel® Integrator Tookit customization (with the exception of the Workload Configuration setting).

| Power & Performance | |
|---|---|
| CPU Power and Performance Policy | Performance / **Balanced Performance** / Balanced Power / Power |
| Workload Configuration | **Balanced**/ I/O sensitive |
| ► Uncore Power Management | |
| ► CPU P State Control | |
| ► Hardware P States | |
| ► CPU C State Control | |

| F10=Save Changes and Exit | F9=Reset to Defaults |
|---|---|
| ↕↔=Move Highlight     <Enter> = Select Entry | Esc=Exit |

**Figure 4. 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.
```
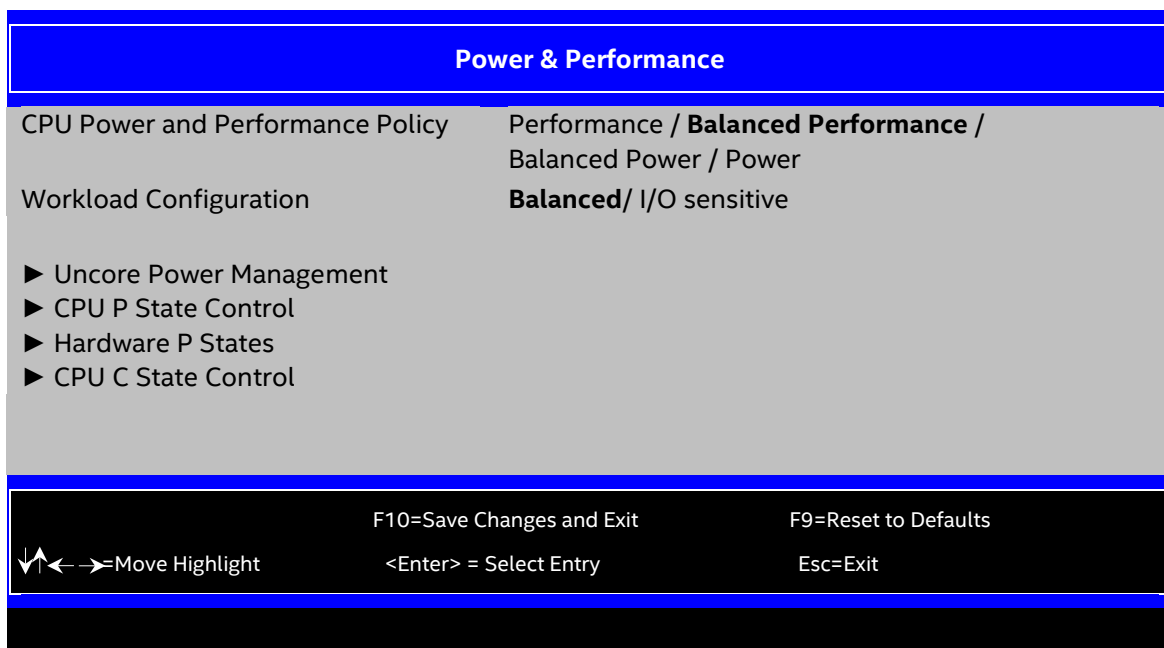
   Comments:　Choosing one of these four power and performance profiles implements a number of changes in BIOS settings, both visible settings in the setup screens and non-visible internal settings. For detailed lists of settings affected by each profile, see *Intel® Server Board S2600 Family BIOS EPS*, Section 3.16.2.

   Back to:　　Power & Performance – Advanced Screen – 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 the 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.16.2. This option is only visible when Enhanced Intel SpeedStep® Technology is enabled by the BIOS. This option is for dual-processor systems only.

   **Note**: This option can support Intel Integrator Toolkit customization, but the value may be overwritten by changing special options after entering BIOS setup.

   Back to:　　Power & Performance – Advanced Screen – Screen map

3. **Uncore Power Management**

   Value:　　　　None

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

   Comments:　*Selection only*. For more information on Uncore Power Management settings, see Section 3.3.2.1.

   Back to:　　Power & Performance – Advanced Screen – Screen map

4. **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 – Screen map

5. **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.

6. **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 – 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.

Uncore Power Management	
Uncore Frequency Scaling	**Enabled**/Disabled
Performance P-limit	**Enabled**/Disabled

F10=Save Changes and Exit   F9=Reset to Defaults

↕↔=Move Highlight   <Enter> = Select Entry   Esc=Exit
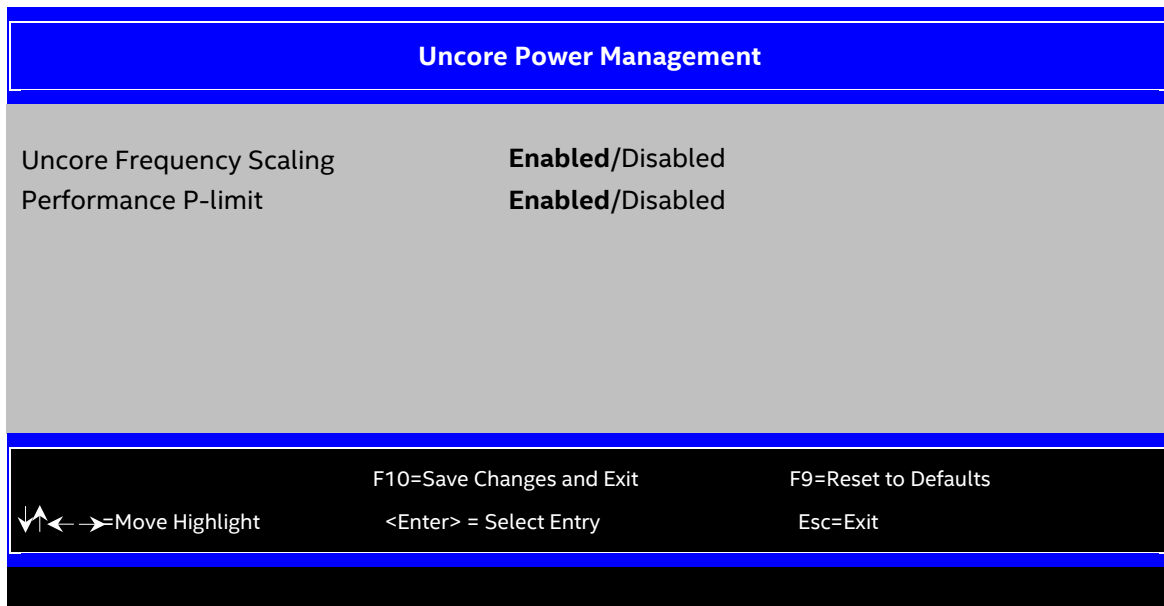
Figure 5. Uncore Power Management screen

1. **Uncore Frequency Scaling**

   Value: **Enabled**/Disabled

   Help text: `Allows the voltage and frequency of Uncore to be programmed independently. The Uncore activity is monitored to optimize the frequency in real-time.`

   Comments: 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, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.16.2. This option is only visible when Enhanced Intel SpeedStep® Technology is enabled by the BIOS.

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

2. **Performance P-limit**

   Value: **Enabled**/Disabled

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

   Comments: This option is only visible if two processors are installed in the system. 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 – Screen map

3.3.2.2 CPU P State Control

The CPU P State Control screen allows the user to specify a policy which 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.
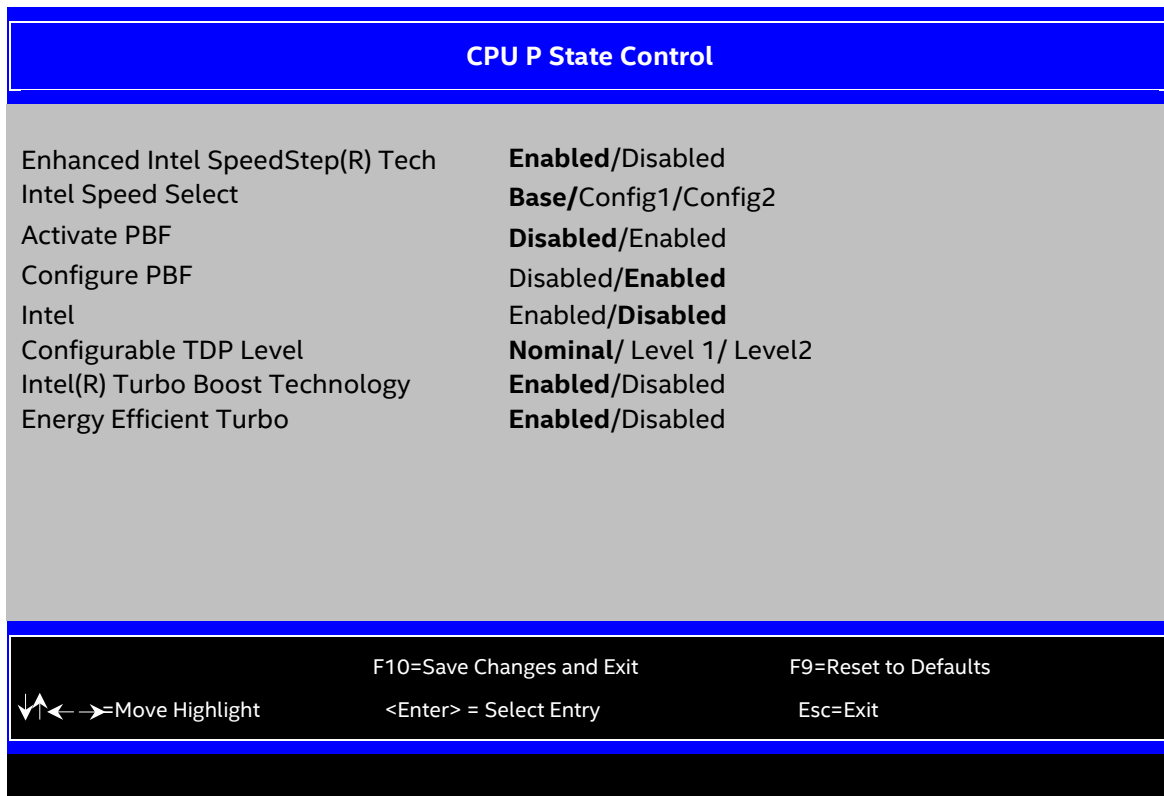
Figure 6. CPU P State Control screen

1. **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® Technology. For 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 – Screen map

2. **Intel Speed Select**

Value: **Base**/Config1/Config2

Help text: `Intel Speed Select allows user to choose from upto two additional base frequency conditions.`

Comments: This option is only visible if "Enhanced Intel SpeedStep(R) Tech" is enabled

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

3. **Activate PBF**

Value: **Disabled**/Enabled

Help text: `This Option allows PBF to be enabled.`

Comments: This option is only visible if all processors installed in the system support Prioritized Base Frequency feature and it is enabled.

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

4. **Configure PBF**

Value: Disabled/**Enabled**

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

Comments: This option is only visible if all processors installed in the system support Prioritized Base Frequency feature and it is enabled.

This option is grayed out if "Activate PBF" is set to Disabled.

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

5. **Intel Configurable TDP**

Value: Enabled/**Disabled**

Help text: `Allows the user to disable/enable Intel Config TDP.`

Comments: This option is only visible if all processors installed in the system support Configurable TDP (cTDP) technology. For this option to be available, Enhanced Intel SpeedStep Technology must be enabled.

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

6. **Configurable TDP Level**

Value: **Nominal**/Level 1/Level 2

Help text: `Allows the user to select Intel Config TDP level – Nominal is the default TDP.`

Comments: This option is only visible if all processors installed in the system support Configurable TDP (cTDP) technology. For this option to be available, Enhanced Intel SpeedStep Technology and Configurable TDP must be enabled.

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

7. **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® Turbo Boost Technology. For this option to be available, Enhanced Intel SpeedStep Technology must be enabled.

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

8. **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. For this option to be available, Intel Turbo Boost Technology must be enabled.

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

Hardware P States	
Hardware P-States	Disable/**Native Mode**/Out of Band Mode/Native mode with no legacy support
Hardware PM Interrupt	Enable/**Disable**
EPP Enable	**Enable**/Disable
APS rocketing	Enable/**Disable**
Scalability	Enable/**Disable**
RAPL Prioritization	Enable/**Disable**

F10=Save Changes and Exit   F9=Reset to Defaults

↑↓←→=Move Highlight   <Enter> = Select Entry   Esc=Exit
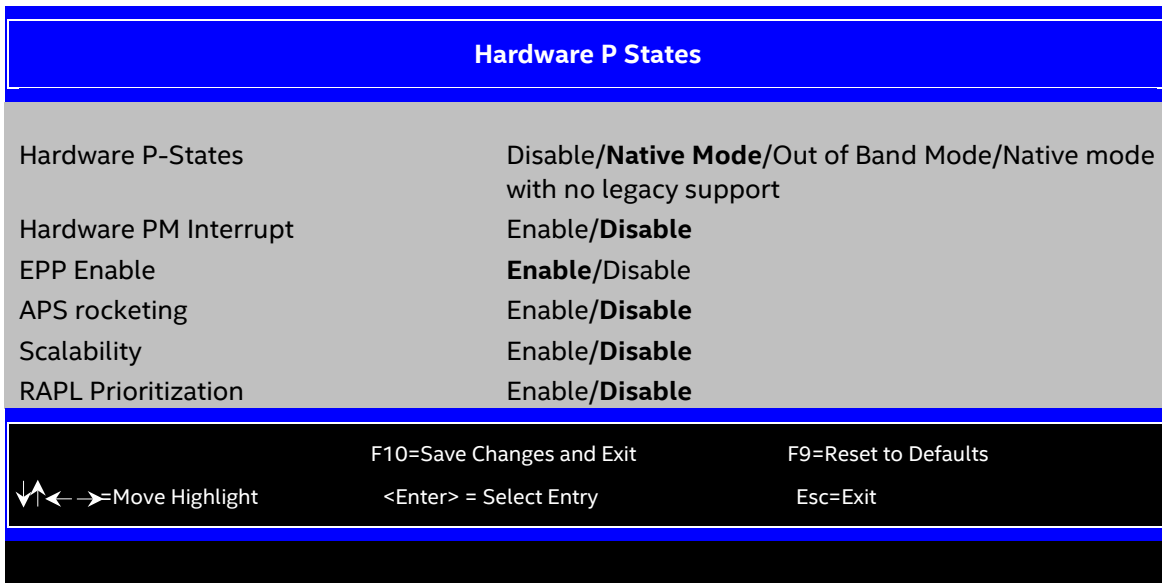
Figure 7. Hardware P States screen

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).
```

   Comments:  None

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

2. **Hardware PM Interrupt**

   Value:          Enable/**Disable**

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

   Comments:  This option is grayed out if Hardware P-States is not in Native Mode.

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

4. **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 – Screen map

5. **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 – Screen map

6. **RAPL Prioritization**

Value: Enable/**Disable**

Help text: `RAPL Prioritization allows creating core groups of different priority`

Comments: No comments.

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

3.3.2.4   CPU C State Control

The CPU C State Control screen allows the user to specify a policy which 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.

```
                              CPU C State Control


   Package C State                    C0/C1 state /C2 state/C6 (non Retention) state
                                      /C6 (Retention) state/No Limit
   C1E                                Enabled/Disabled
   Processor C6                       Enabled/Disabled




                      F10=Save Changes and Exit          F9=Reset to Defaults

    ↓↑← →=Move Highlight          <Enter> = Select Entry           Esc=Exit

```
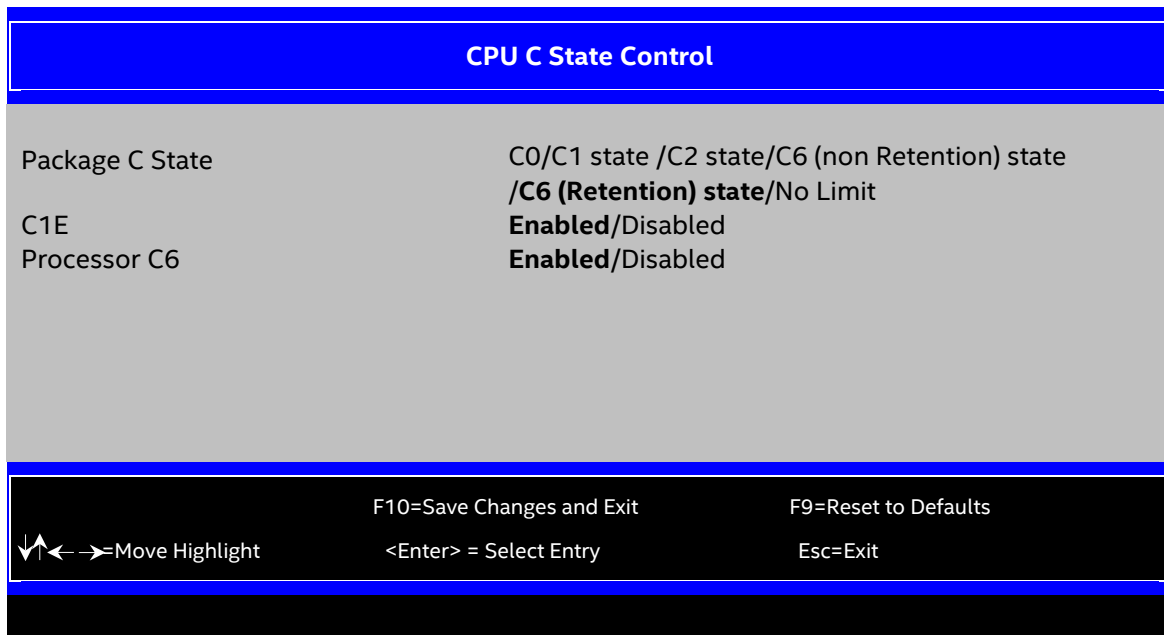
Figure 8. CPU C State Control screen

1. **Package C State**

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

   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 – 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.

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

UPI Configuration	
Current Intel(R) UPI Link Speed	Slow/Fast
Intel(R) UPI Link Frequency	N/A /PerLink/ 9.6 GT/s / 10.4GT/s /Unknown GT/s
Intel(R) UPI Frequency Select	Auto Max / 9.6 GT/s / 10.4 GT/s
XPT Prefetch	Disabled/Enabled/**Auto**
IO Directory Cache (IODC)	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
KTI Prefetch	**Enabled**/Disabled
Stale AtoS	**Disabled**/Enabled/Auto
LLC Dead LineAlloc	Disabled/**Enabled**/Auto
Direct To Core (D2C)	Disabled/Enabled/**Auto**
Direct To UPI (D2K)	Disabled/Enabled/**Auto**

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

Figure 9. UPI Configuration screen

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

   Value: Slow/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 50 MT/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 – Screen map

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

Value: N/A /PerLink/ 9.6 GT/s / 10.4GT/s /Unknown GT/s

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 – Screen map

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

Value: **Auto Max** / 9.6 GT/s / 10.4 GT/s

Help text: `Allows for selecting the Intel(R) UltraPath Interconnect Frequency. Recommended to leave in [Auto Max] 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 Max 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. Changing Intel UPI link frequency does not affect the Intel UPI link speed.

Back to: UPI Configuration – Advanced Screen – Screen map

4. **XPT Prefetch**

Value: Enabled/Disabled/**Auto**

Help text: `XPT Prefetch`

Comments: None

Back to: UPI Configuration – Advanced Screen – Screen map

5. **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 – Screen map

6. **KTI Prefetch**

    Value: **Enabled**/Disabled

    Help text: `Enable or disable KTI Prefetch.`

    Comments: None

    Back to: UPI Configuration – Advanced Screen – Screen map

7. **Stale AtoS**

    Value: Enabled/**Disabled**

    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 will not be effective in xNC configuration where BuriedM is possible.

    Back to: UPI Configuration – Advanced Screen – Screen map

8. **LLC Dead Line Alloc**

    Value: **Enabled**/Disabled

    Help text: `Enable – opportunistically fill dead lines in LLC`
                  `Disable – neverfill 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 – Screen map

9. **Direct To Core (D2C)**

    Value: **Auto**/Enabled/Disabled

    Help text: `Direct To Core (D2C)`
    Comments: No comments.

    Back to: UPI Configuration – Advanced Screen – Screen map

10. **Direct To UPI (D2K)**

    Value: **Auto**/Enabled/Disabled

    Help text: `Direct To UPI (D2K)`
    Comments: No comments.

    Back to: UPI Configuration – Advanced Screen – Screen map

3.3.4 Memory Configuration

The Memory Configuration screen allows the user to view details about the DDR4 DIMMs that are installed as system memory and alter BIOS memory configuration settings where appropriate.

For the Intel® Server Board S2600 family, 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

Figure 11. Memory Configuration screen – Page 2

Total DDR4 Memory	<Total physical DDR4 memory installed in system>
DCPMM	<Total Capacity – Volatile Capacity – Non-volatile capacity>
Effective Memory	<Total effective memory>
Current Configuration	<Independent/1LM Mirror/2LM Mirror/ Rank Sparing/ADDDC>
Current Memory Speed	<Operational memory speed in MT/s>
Memory Operating Speed Selection	**Auto**/2133/2400/2666/2933
IMC Interleaving	**Auto**/1-way Interleave/2-way Interleave
Page Policy	**Auto**/Closed/ Adaptive
Volatile Memory Mode	1LM/2LM/**Auto**
DCPMM Error Injection	**Disabled** /Enabled
Publish ARS Capability	**Auto**/Disabled/Enabled
Skip ARS on Boot	**Disabled**/Enabled
Background ARS	**Auto**/Disabled
Average Power Budget(in mW)	[15000]
SMB Clock Frequency	**Auto**/100 Khz/400 Khz/1Mhz
Snoopy mode for 2LM	Enabled/ **Disabled**
Snoopy mode for AD	Enabled/ **Disabled**
NVM Performance Setting	**BW Optimized**/ Latency Optimized
CR FastGo Configuration	**Auto**/Default (no FastGo optimization)/Option1/Option2/Option3/Option4/Option5
CR Latch System Shutdown State	Disabled/**Enabled**
CR QoS	Recipe 1 - Enables tuning recipe 1 for CR QoS knobs (recommended for 2-2-2 memory configuration in AD)/ Recipe 2 - Enables tuning recipe 2 for CR QoS knobs (recommended for other memory configuration in AD)/ Recipe 3 - Enables tuning recipe 3 for CR QoS knobs (recommended for 1 DIMM per channel config)/ **Disable - Disable CR QoS feature**
Thermal Throttling Thresolds Offset	**Auto**/Enabled
CLX A0 Starve Thresold	Disabled /Enabled
Attempt Fast Boot	**Auto**/Disabled /Enabled
Attempt Fast Cold Boot	**Auto**/Disabled /Enabled
Enable power Cycle Policy	Disabled /**Enabled**

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

Figure 10. Memory Configuration screen – Page 1

Memory Configuration

Enable ADR   Disabled/**Enabled**

MRC Promote Warnings   Disabled/**Enabled**
Promote Warnings   Disabled/**Enabled**
Halt on mem Training Error   Disabled/**Enabled**
Thermal Monitor   Disabled/**Enabled**

► Memory RAS and Performance Configuration

DIMM Information
CPU1_CPU1_DIMM_A1   <DIMM size> <DIMM status>
CPU1_CPU1_DIMM_A2   <DIMM size> <DIMM status>
CPU_DIMM_B1   <DIMM size> <DIMM status>
CPU_DIMM_B2   <DIMM size> <DIMM status>
          ~~(repeated for C1-F1, omitted)~~
CPU1_DIMM_F2   <DIMM size> <DIMM status>
          ~~(repeated for J1-T2, omitted)~~
CPU2_DIMM_A1   <DIMM size> <DIMM status>

F10=Save Changes and Exit   F9=Reset to Defaults

↕↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 11. Memory Configuration screen – Page 2

1. **Total DDR4 Memory**

    Value: <Total physical DDR4 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 DDR4 DIMMs in units of GB. This item does not include DCPMM info.

    Back to: Memory Configuration – Advanced Screen – Screen map

2. **DCPMM**

    Value: <Total capacity – Volatile capacity – Non-volatile capacity>

    Help text: None

    Comments: *Information only*. Displays the current total DCPMM capacity and volatile/persistent /block partition size. If there is no DCPMM installed on the system, `Not Installed` is displayed.

    Back to: Memory Configuration – Advanced Screen – Screen map

3. **Effective Memory**

   Value: <Total effective memory>

   Help text: None

   Comments: *Information only*. Displays the amount of memory available to the OS 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 *Intel® Server Board S2600 Family BIOS EPS*, Sections 3.4.8 and, especially, 3.4.8.2.

   Back to: Memory Configuration – Advanced Screen – Screen map

4. **Current Configuration**

   Value: Independent/1LM Mirror/2LM 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.
   - 1LM Mirror – Mirroring RAS Mode has been configured and is operational.
   - 2LM Mirror – 2LM mirror mode selected.
   - Rank Sparing – Rank Sparing RAS Mode has been configured and is operational.
   - ADDDC – ADDDC mode enabled.

   Back to: Memory Configuration – Advanced Screen – 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 currently running.

   The supported memory speeds are 2133 MT/s, 2400 MT/s, and 2666 MT/s. The actual memory speed capability depends on the memory configuration.

   Back to: Memory Configuration – Advanced Screen – Screen map

6. **Memory Operating Speed Selection**

   Value: **Auto**/2133/2400/2666/2933

   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.

   Back to: Memory Configuration – Advanced Screen – Screen map

7. **IMC Interleaving**

   Value: **Auto**/1-way Interleave/2-way Interleave

   Help text: `Select IMC Interleaving setting.`

   Comments: None

   Back to: Memory Configuration – Advanced Screen – Screen map

8. **Page Policy**

   Value: **Auto**/Closed/Adaptive

   Help text: `Select Page Policy.`

   Comments: None

   Back to: Memory Configuration – Advanced Screen – Screen map

9. **Volatile Memory Mode**

   Value: 1LM/ 2LM /**Auto**

   Help text: `Selects whether 1LM or 2LM memory mode should be enabled`

   Comments: This option is displayed only when the BIOS support DCPMM.

   On selecting the option "Auto", Internally BIOS checks for the 2LM configuration. If the configuration is matched, then the system boots with 2LM, if not matched the system boots with 1LM configuration. The Setup knob is set with value "Auto".

   On selecting the option "2LM", Internally BIOS check for the 2LM configuration. If the configuration is matched, then the system boots with 2LM, if not matched the system boots with 1LM configuration. The Setup knob is set with value "2LM".

   On selecting the option "1LM", Internally BIOS check for 1LM configuration and systems boots with the configuration. The Setup knob is set with the value "1LM".

   Back to: Memory Configuration – Advanced Screen – Screen map

10. **DCPMM Error Injection**

   Value: **Disabled**/Enabled

   Help text: `Enable / Disable DCPMM Error Injection`

   Comments: This option is displayed only when the BIOS support DCPMM.

   Back to: Memory Configuration – Advanced Screen – Screen map

11. **Publish ARS Capability**

   Value: **Auto**/Disabled/Enabled

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

   Comments: None.

   Back to: Memory Configuration – Advanced Screen – Screen map

12. Skip ARS on Boot

Value: **Disabled**/Enabled

Help text: `Enabled: prevent BIOS from starting system-wide ARS on boot`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

12. Background ARS

Value: **Auto/**Disabled

Help Text: Auto: go background on initial short ARS sequence.

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

13. Average Power Budget (in mW)

Value: **15000**

Help text: `Sets the power management policy for average power (must be an increment of 250 mW). Warning: 128GB DIMM will work on MAX 15W and 256GB/512GB cannot go below 10W. If value outside the range are set, the default will fall into the range`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

14. SMB Clock Frequency

Value: **Auto**/100 Khz/400 Khz/1Mhz

Help text: `Sets DDR4 SMBus Clock Frequencies For SPD Access. Auto - Sets it to the MRC default setting; current default is 400K.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

15. Snoopy mode for 2LM

Value: **Disabled**/Enabled

Help text: `enables new 2LM specific feature to avoid directory updates to far-memory from non-NUMA optimized workloads`

Comments: None

Back to: Memory Configuration – Advanced Screen – Screen map

16. Snoopy mode for AD

Value: **Disabled**/Enabled

Help text: `enables new AD specific feature to avoid directory updates to DDRT memory from non-NUMA optimized workloads`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

17. NVM Performace Setting

Value: **BW Optimized**/Latency Optimized

Help text: `NVM baseline performance settings depending on the workload behavior`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

18. CR FastGo Configuration

Value: **Auto**/Default (no FastGo optimization)/Option1/Option2/Option3/Option4/Option5

Help text: `Select CR QoS Configuration Profiles`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

19. CR Latch System Shutdown State

Value: Disabled/**Enabled**

Help text: `Latch System Shutdown State`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

20. CR QoS

Value: Recipe 1 - Enables tuning recipe 1 for CR QoS knobs (recommended for 2-2-2 memory configuration in AD)/ Recipe 2 - Enables tuning recipe 2 for CR QoS knobs (recommended for other memory configuration in AD)/ Recipe 3 - Enables tuning recipe 3 for CR QoS knobs (recommended for 1 DIMM per channel config)/ **Disable - Disable CR QoS feature**

Help text: `CR QoS tuning recipes`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

21. Thermal Throttling Thresolds Offset

Value: **Auto**/Enabled

Help text: `Auto = T_crit-(2/3)C Enable = T_crit-(1/2)C Threshold limits`

Comments: This option is displayed only when the BIOS support DCPMM.

Back to: Memory Configuration – Advanced Screen – Screen map

22. CLX A0 Starve Thresold

Value: **Disabled**/Enabled

Help text: `Enable / Disable DCPMM Error Injection.`

Comments: This option will be displayed in BIOS Setup only if CLX CPU with A0 stepping is installed.

Back to: Memory Configuration – Advanced Screen – Screen map

23. Attempt Fast Boot

Value: **Auto**/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. Auto - Sets it to the MRC default setting; current default is Enabled.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

24. Attempt Fast Cold Boot

Value: **Auto**/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. Auto - Sets it to the MRC default setting; current default is Enabled.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

25. Enable Power Cycle Policy

Value: Disabled/**Enabled**

Help text: `Enable/Disable power cycle policy when NVMDIMM receive surprise clock stop`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen map

26. Enable ADR

Value: **Enabled**/Disabled

Help text: `Enables the detecting and enabling of ADR.`

Comments: This option is displayed when the system installs NVDIMM.

Back to: Memory Configuration – Advanced Screen – Screen map

27. Erase-Arm NVDIMMs

Value: **Enabled**/Disabled

Help text: `Enables/Disables Erasing and Arming NVDIMMs.`

Comments: This option is displayed when the system installs NVDIMM.

Back to: Memory Configuration – Advanced Screen – Screen map

28. Restore NVDIMMs

Value: **Enabled**/Disabled

Help text: `Enables/Disables Automatic restoring of NVDIMMs.`

Comments: This option is displayed when the system installs NVDIMM.

Back to: Memory Configuration – Advanced Screen – Screen map

29. Interleave NVDIMMs

Value: Enabled/**Disabled**

Help text: `Controls if NVDIMMs are interleaved together or not.`

Comments: This option is displayed when the system installs NVDIMM.

Back to: Memory Configuration – Advanced Screen – Screen map

30. MRC Promote Warnings

Value: Disabled/**Enabled**

Help text: `Determines if MRC warnings are promoted to system level`

Comments: This option is displayed only when the BIOS support DCPMM

Back to: Memory Configuration – Advanced Screen – Screen map

31. Promote Warnings

Value: Disabled/**Enabled**

Help text: `Determines if warnings are promoted to system level`

Comments: This option is displayed only when the BIOS support DCPMM.

Back to: Memory Configuration – Advanced Screen – Screen map

32. Halt on mem Training Error

Value: Disabled/**Enabled**

Help text: `Halt on mem Training Error Disable/Enable`

Comments: This option is displayed only when the BIOS support DCPMM.

Back to: Memory Configuration – Advanced Screen – Screen map

33. Thermal Monitor

Value: Disabled/**Enabled**

Help text: `Enable/Disable Thermal Monitor`

Comments: This option is displayed only when the BIOS support DCPMM.

Back to: Memory Configuration – Advanced Screen – Screen map

34. 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 3.3.4.1

Back to: Memory Configuration – Advanced Screen – Screen map

35. DIMM Information

CPU1_DIMM_A1, CPU1_DIMM_A2, CPU1_DIMM_B1, CPU1_DIMM_B2 … (DIMM_C1 through DIMM_F1), CPU1_DIMM_F2 … (DIMM_J1 through DIMM_T2), CPU2_DIMM_A1 … CPU2_DIMM_F2

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 three possible states:

- Installed & Operational – There is a DDR4 DIMM installed and operational in this slot.
- Not Installed – There is no DDR4 DIMM installed in this slot.
- Failed/Disabled – The DIMM installed in this slot has failed during initialization and/or was disabled during initialization.

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.

Note: For DIMM_XY, X denotes the channel identifier A-P and Y denotes the DIMM slop identifier 1-3 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.

Note: If the DIMM is a DCPMM, the DIMM size string is `xx GB–xx GB – xx GB` representing the total capacity, volatile capacity, and non-volatile capacity. No DIMM status is shown for DCPMM devices. The BIOS setup displays DIMM size - `xx GB value` by truncating decimal value. For example: 491.7 GB will be displayed in BIOS setup as 491 GB.

The Intel Server Board S2600 family can have DIMMs A1 and A2 to L1 and L2 (maximum two CPUs, six 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 *Intel® Server Board S7200AP Family BIOS EPS*, Sections 3.4.4.1 and Chapter 12.

Back to:

3.3.4.1 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.

Memory RAS and Performance Configuration	
Capabilities	
Memory Mirroring Possible	Yes/No
Memory Rank Sparing Possible	Yes/No
Memory ADDDC Possible	Yes/No
Mirror Mode	**Disabled**/1LM/2LM
ADDDC Sparing	**Enabled**/Disabled
Memory Sparing	Enabled/**Disabled**
Multi-Rank Sparing	**1 Rank**/2 Rank/Auto
NUMA Optimized	**Enabled**/Disabled
Sub_NUMA Cluster	Enabled/**Disabled**
Patrol Scrub	**Enabled**/Disabled
Correctable Error Threshold	500/100/20/**10**/5/All/None
Cloaking	Enabled/**Disabled**

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

Figure 12. 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 is capable of 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 *Intel® Server Board S2600 Family BIOS EPS*, Sections 3.4.3 and 3.4.4.

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

2. **Memory Rank Sparing Possible**

   Value: Yes/No

   Help text: None

   Comments: *Information only.* Displays whether the current DIMM configuration is capable of rank sparing. For rank sparing to be possible, there must be two or more SR DIMMs, or at least one DR DIMM installed on one channel of the system. For details about rank sparing configurations, refer to *Intel® Server Board S2600 Family BIOS EPS* sections 3.4.3 and 3.4.4.

   Note: The Correctable Error Threshold value is also the Sparing Fail Over threshold value. Threshold values of "All" or "None" are not valid for Rank Sparing. If the Correctable Error Threshold is set to either of those values, Rank Spring will not be possible. (See Section 3.3.4.)

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

3. **Memory ADDDC Possible**

   Value: Yes/No

   Help text: None

   Comments: *Information only.* Displays whether the current DIMM configuration is capable of 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 – Screen map

4. **Mirror Mode**

   Value: **Disabled**/1LM/2LM

   Help text: `Allows the user to select the Mirror Mode to be applied for the next boot. 2LM will be hidden when DCPMM is not present.`

   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.

   1LM– 1 level Mirror Mode

   2LM– 2 level Mirror Mode

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

5. **ADDDC Sparing**

    Value: **Enabled**/Disabled

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

    Comments: This setting is hidden if eight DIMMs are installed or if mirror mode or memory sparing are not disabled.

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

6. **Memory Sparing**

    Value: Enabled/**Disabled**

    Help text: `Enable/Disable Memory Rank Sparing.`

    Comments: If no channel has more than two rank, this item is hidden.

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

7. **Multi-Rank Sparing**

    Value: **1 Rank**/2 Rank/Auto

    Help text: `The Rank number used when Rank Sparing is enabled.`

    Comments: This option is only present when Memory Sparing is enabled.

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

8. **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 only hidden for boards which have only one socket installed that is SNC incapable.

                When enabled, the SRAT and SLIT ACPI tables are provided that show the locality of systems resources, especially memory, which allows a "NUMA Aware" OS 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.4.4.6.

                When NUMA Optimized is enabled and Volatile Memory Mode is 2LM, then the effective memory size is size of DCPMM.

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

9. **Sub_NUMA Cluster**

Value: Enabled/**Disabled**

Help text: `When enabled, sub NUMA cluster enabled. If any memory controller has no memory attached, this feature cannot be enabled.`

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. Sub_NUMA Cluster enables the two-cluster SNC; two-way interleave of IMC Interleaving will focus to 1-cluster. If there are DIMMs on both MCs, enable the SNC and set one-way interleave. It will enable SNC2 (two clusters).

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

10. **Patrol Scrub**

Value: **Enabled**/Disabled

Help text: `When enabled, performs periodic checks on memory cells and proactively walks through populated memory space, to seek and correct soft ECC errors.`

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 – Screen map

11. **Correctable Error Threshold**

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

Help text: `Threshold value for logging Correctable Errors (CE) – Threshold of 10 (default) logs 10th CE, "All" logs every CE, and "None"' means no CE logging. All and None are not valid with Rank Sparing.`

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 which 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 – Screen map

12. Cloaking

Value: **Disabled**/Enabled

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 – Screen map

3.3.5   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.

Integrated IO Configuration	
NTB PCIe Port 1a on CPU socket 1	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP
NTB PCIe Port 2a on CPU socket 1	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP
NTB PCIe Port 3a on CPU socket 1	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP

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

Figure 13. Integrated IO Configuration screen – page 1 for CPU socket 1

Integrated IO Configuration	
NTB PCIe Port 1a on CPU socket 2	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP
NTB PCIe Port 2a on CPU socket 2	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP
NTB PCIe Port 3a on CPU socket 2	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled** / Enabled
Enable SPLIT BARs	**Disabled** / Enabled
Primary BAR 23 Size	[0-39, **20** is Default]
Primary BAR 4 Size	[0-39, **20** is Default]
Primary BAR 5 Size	[0-39, **20** is Default]
Primary BAR 45 Size	[0-39, **20** is Default]
Secondary BAR 23 Size	[0-39, **20** is Default]
Secondary BAR 4 Size	[0-39, **20** is Default]
Secondary BAR 5 Size	[0-39, **20** is Default]
Secondary BAR 45 Size	[0-39, **20** is Default]
Crosslink control override	**DSD/USP** / USD/DSP
Intel(R) VT for Directed I/O	Enabled / **Disabled**
ACS Control	**Enabled** / Disabled
Coherency Support	Enabled / **Disabled**
Pcie Pll SSC	Disabled/Auto/0.0%/0.1%/0.1%/0.3%/0.4%/0.5%/0.6%/0.7%/0.8%/0.9%/1.0%/1.1%/1.2%/1.3%/1.4%/1.5%/1.6%/1.7%/1.8%/1.9%/**POR – Reg. Value:0x1F**

F10=Save Changes and Exit   F9=Reset to Defaults

↑↓←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 14. Integrated IO Configuration screen – page 2 for CPU socket 2

```
                            Integrated IO Configuration

Relaxed Ordering                        Disabled / Enabled
No Snoop(Sck0 IOAT Function 0)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 1)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 2)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 3)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 4)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 5)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 6)          Disabled / Enabled
No Snoop(Sck0 IOAT Function 7)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 0)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 1)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 2)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 3)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 4)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 5)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 6)          Disabled / Enabled
No Snoop(Sck1 IOAT Function 7)          Disabled / Enabled
DMI-PCIe Port MPSWorkaround             128B/256B/Auto

              F10=Save Changes and Exit            F9=Reset to Defaults

    ↕←  →=Move Highlight        <Enter> = Select Entry              Esc=Exit
```

Figure 15. Integrated IO Configuration screen – page 3

1. **NTB PCIe Port 1a on CPU socket 1**
   NTB PCIe Port 2a on CPU socket 1
   NTB PCIe Port 3a on CPU socket 1
   NTB PCIe Port 1a on CPU socket 2
   NTB PCIe Port 2a on CPU socket 2
   NTB PCIe Port 3a on CPU socket 2

   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 1A, 2A or 3A to
   support NTB configuration.

   Note: When NTB is enabled, Spread Spectrum Clocking (SSC) is required to be disabled at
   each NTB link. NTP-RP mode is not supported in the Intel Server Board S2600 family.

   Back to: Integrated IO Configuration– Advanced Screen – Screen map

2. **Enable NTB Bars**

   Value: Enabled/**Disabled**

   Help text: `If disabled, the BIOS will not 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 will 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: Integrated IO Configuration– Advanced Screen – Screen map

3. **Enable SPLIT BARs**

   Value: Enabled/**Disabled**

   Help text: `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: Integrated IO Configuration– Advanced Screen – Screen map

4. **Primary BAR 23 Size**

   Value: [0-39, **20** is default]

   Help text: `Used to set the prefetchable BAR 23 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.

   Back to: Integrated IO Configuration– Advanced Screen – Screen map

5. **Primary BAR 4 Size**

   Value: [0-39, **20** is default]

   Help text: `Used to set the prefetchable BAR 4 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: Integrated IO Configuration– Advanced Screen – Screen map

6. **Primary BAR 5 Size**

   Value: [0-39, **20** is default]

   Help text: `Used to set the prefetchable BAR 5 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: Integrated IO Configuration– Advanced Screen – Screen map

7. **Primary BAR 45 Size**

Value: [0-39, **20** is default]

Help text: `Used to set the prefetchable BAR 45 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 disabled.

Back to: Integrated IO Configuration– Advanced Screen – Screen map

8. **Secondary BAR 23 Size**

Value: [0-39, **20** is default]

Help text: `Used to set the prefetchable BAR 23 size on secondary side of NTB.`
             `Value < than 12 or > 39 disables BAR.`

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

Back to: Integrated IO Configuration– Advanced Screen – Screen map

9. **Secondary BAR 4 Size**

Value: [0-39, **20** is default]

Help text: `Used to set the prefetchable BAR 4 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: Integrated IO Configuration– Advanced Screen – Screen map

10. **Secondary BAR 5 Size**

Value: [0-39, **20** is default]

Help text: `Used to set the prefetchable BAR 5 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: Integrated IO Configuration– Advanced Screen – Screen map

11. **Secondary BAR 45 Size**

Value: [0-39, **20** is default]

Help text: `Used to set the prefetchable BAR 45 size on secondary side of NTB.`
             `Value < than 12 or > 39 disables BAR.`

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

Back to: Integrated IO Configuration– Advanced Screen – 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.7.1. This option only appears when the NTB PCIe Port is configured as NTB to NTB.

Back to: Integrated IO Configuration– Advanced Screen – Screen map

13. 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.`

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 for it to be enabled.

Back to: Integrated IO Configuration– Advanced Screen – Screen map

14. 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 – Screen map

15. Coherency Support

Value: **Enabled**/Disabled

Help text: `Enable/Disable Intel(R) VT-d Coherency support.`

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

Back to: Integrated IO Configuration– Advanced Screen – Screen map

16. Pcie Pll SSC

Value: Disabled/Auto/0.0%/0.1%/0.1%/0.3%/0.4%/0.5%/0.6%/0.7%/0.8%/0.9%/1.0%/1.1% /1.2%/1.3%/1.4%/1.5%/1.6%/1.7%/1.8%/1.9%/POR - Reg. Value:0x1F

Help text: `Pcie Pll SSC percentage or Disable SSC. Range is 0.0%-1.9%. Last one is the POR for LBG.`

Comments: None

Back to: Integrated IO Configuration– Advanced Screen – Screen map

17. **Relaxed Ordering**

    Value: **Disabled**/Enabled

    Help text: `Relaxed Ordering Enable/Disable`

    Comments: None

    Back to: Integrated IO Configuration– Advanced Screen – Screen map

18. **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 – Screen map

19. **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 – Screen map

20. **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 – Screen map

21. **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 – Screen map

22. **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 – Screen map

23. **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 – Screen map

24. **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 – Screen map

25. **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 – Screen map

26. **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 – Screen map

27. **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 – Screen map

28. **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 – Screen map

29. **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 – Screen map

30. **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 – Screen map

31. 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 – Screen map

32. 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 – Screen map

33. 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 – Screen map

34. DMI-PCIe Port MPSWorkaround

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

Help text: Configures DMI-PCIe Port Max Payload Size to 128B/256B/AUTO

Comments: None

Back to: Integrated IO Configuration– Advanced Screen – Screen map

35. PCIE Fatal Error Mask Setting

Value: None

Help text: None

Comments: *Selection only.* For more information on PCIE Fatal Error Mask Setting, see Section 3.3.1

Back to: Integrated IO Configuration– Advanced Screen – Screen map

3.3.5.1 PCIE Fatal Error Mask Setting

PCIE Fatal Error Mask Setting	
Data Link Protocol Error Mask	**Disabled** /Enabled
Surprise Down Error Mask	**Disabled** /Enabled
Poisioned TLP Mask	**Disabled** /Enabled
Flow Control Protocol Error Mask	**Disabled** /Enabled
Completion Timeout Mask	**Disabled** /Enabled
Unexpected Completion Mask	**Disabled** /Enabled
Receiver Overflow Mask	**Disabled** /Enabled
Malformed TLP Mask	**Disabled** /Enabled
ECRC Error Mask	**Disabled** /Enabled
ACS Violation Mask	**Disabled** /Enabled
Uncorrectable Internal Error Mask	**Disabled** /Enabled
MC Blocked TLP Mask	**Disabled** /Enabled
AtomicOp Egress Blocked Mask	**Disabled** /Enabled
TLP Prefix Blocked Error Mask	**Disabled** /Enabled

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

1. **Data Link Protocol Error Mask**

    Value: **Disabled**/Enabled

    Help text: None

    Comments: None

    Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

2. **Surprise Down Error Mask**

    Value: **Disabled**/Enabled

    Help text: None

    Comments: None

    Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

3. **Poisoned TLP Mask**

    Value: **Disabled**/Enabled

    Help text: None

    Comments: None

    Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

4. **Flow Control Protocol Error Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

5. **Completion Timeout Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

6. **Unexpected Completion Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

7. **Receiver Overflow Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

8. **Malformed TLP Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

9. **ECRC Error Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

10. **ACS Violation Mask**

> Value: **Disabled**/Enabled

> Help text: None

> Comments: None

> Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

11. Uncorrectable Internal Error Mask

Value: **Disabled**/Enabled

Help text: None

Comments: None

Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

12. MC Blocked TLP Mask

Value: **Disabled**/Enabled

Help text: None

Comments: None

Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

13. AtomicOp Egress Blocked Mask

Value: **Disabled**/Enabled

Help text: None

Comments: None

Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

14. TLP Prefix Blocked Error Mask

Value: **Disabled**/Enabled

Help text: None

Comments: None

Back to: PCIE Fatal Error Mask Setting - Integrated IO Configuration– Advanced Screen – Screen map

3.3.6   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.

There are two SATA port configurations in this screen, representing the SATA controller and the sSATA controller with SATA drive support and redundant array of independent disks (RAID) support. There are also informational displays of two SATA controller configurations and SATA drive information 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® Sever Board S2600 family, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 3.8. For details of the storage configurations supported by the different server boards, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 12.

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

Mass Storage Controller Configuration
► sSATA Port 0–5 ► SATA Port 0–7
Intel(R) Storage Module None/<Name of storage module detected>
F10=Save Changes and Exit   F9=Reset to Defaults Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 16. Mass Storage Controller Configuration screen

15. sSATA Port 0–5

Value:	None
Help text:	None
Comments:	*Selection only.* For more information on SATA Port configuration settings, see Section 3.3.6.1.
Back to:	Mass Storage Controller Configuration – Advanced Screen – Screen map

16. SATA Port 0–7

Value: None

Help text: None

Comments: *Selection only*. For more information on SATA Port configuration settings, see Section 3.3.6.1.

Back to: Mass Storage Controller Configuration – Advanced Screen – Screen map

17. 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® 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 3.8.7.

Back to: Mass Storage Controller Configuration – Advanced Screen – Screen map

3.3.6.1 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 are two onboard controllers – the AHCI SATA controller and the AHCI sSATA controller with SATA drive and RAID support. There are also informational displays of AHCI controller configuration and SATA drive information when applicable.

Note: Due to limitations of Syscfg (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.
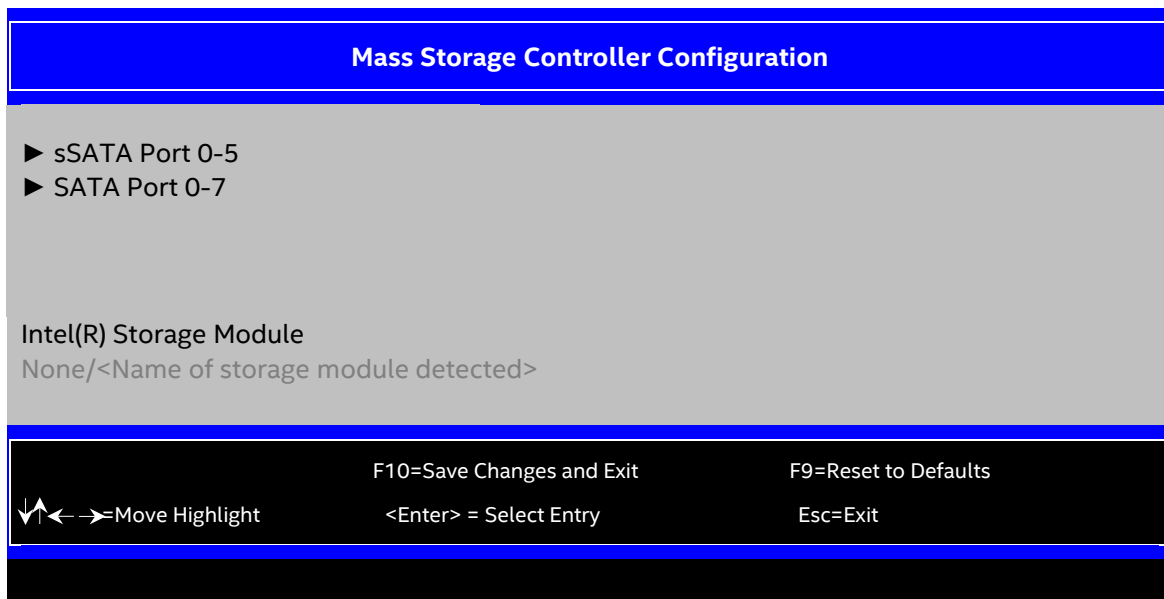
```
                         SATA Port 0-5

(s)SATA Controller Configuration      <AHCI Port Configuration>
AHCI Capable (s)SATA Controller       Disabled/AHCI /RAID Mode
(s)SATA RAID Options                  INTEL(R) ESRT2 (LSI*) / INTEL(R) RSTe
(s)SATA Controller eSATA Options      SATA/eSATA
(s)SATA HDD Staggered Spin-Up         Enabled/Disabled

SATA Port 0                           Not Installed / <Drive Information>
SATA Port 1                           Not Installed / <Drive Information>
SATA Port 2                           Not Installed / <Drive Information>
SATA Port 3                           Not Installed / <Drive Information>
SATA Port 4                           Not Installed / <Drive Information>
SATA Port 5                           Not Installed / <Drive Information>
SATA Port 6                           Not Installed / <Drive Information>
SATA Port 7                           Not Installed / <Drive Information>

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

Figure 17. SATA Port configuration screen

1. **(s)SATA Controller Configuration**

   Value: Controller is disabled/<AHCI port configuration>

   Help text: None

   Comments: *Information only.* This is a display showing which ports are available through the onboard AHCI capable SATA controller, if the controller is enabled. The port configuration is one of the following states:

   - Controller is disabled
   - 8 ports of 6 Gb/s SATA (for SATA controller)
   - 6 ports of 6 GB/s SATA (for sSATA controller)

   This information is also displayed during POST in the POST diagnostic screen. (*Intel® Server Board S2600 Family BIOS EPS*, 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. The platform ID (board ID) is displayed in the Main screen, and the corresponding SATA port configuration can be found in *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12.

   Back to: SATA Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

2. **AHCI Capable (s)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 *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12.

   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.

   Note: For Intel® Server Board S2600BT, which does not support RAID, there is no RAID Mode value in setup.

   Back to: SATA Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

3. **(s)SATA RAID Options**

Value: INTEL(R) ESRT2 (LSI*) / **INTEL(R) RSTe**

Help text: – Intel(R) ESRT2 (Powered By LSI*): Supports RAID 0/1/10 and optional RAID 5 with Inte(R) RAID5 Upgrade Keys. Uses Intel(R) ESRT2 drivers (based on LSI* MegaSR).
            – Intel(R) RSTe: Provides pass-through drive support. Also provides host based RAID 0/1/10/5 support. Uses Intel(R) RSTe 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 will be necessary to Save and Exit and reboot in order to create a RAID Volume.

            Note: This option does not appear on all boards. Intel® Embedded Server RAID Technology 2 (Intel® ESRT2) only supports SATA controllers on 1G board and BIOS should be in EUFI mode. For other configurations, the option is grayed out and the default value is Intel® Rapid Storage Technology enterprise (Intel® RSTe). The sSATA controller does not support Intel ESRT2. For Intel® Server Board S2600BT, which does not support RAID, this option is not available in setup.

Back to: SATA Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

4. **(s)SATA Controller eSATA Options**

Value: **SATA**/eSATA

Help text: – SATA mode enables the switchable internal AHCI SATA (port 1).
            – eSATA mode enables the switchable external AHCI eSATA (port 1).
            – These modes are mutually exclusive, so SATA port 1 will only be active on one connector, not both.

Comments: To use the external eSATA connection, this option must be set to eSATA. When the external eSATA connector is selected, it disables the corresponding internal SATA port 1 connector. When set to SATA, the internal connector for SATA port 1 is active, and the external eSATA connector is disabled.

            This option setting only appears when the SATA Controller is enabled, and only for platforms which support eSATA. For details on which platforms support eSATA, refer to *Intel® Server Board S2600 Family BIOS* EPS, Section 12.

Back to: SATA Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

5. **(s)SATA HDD Staggered Spin-Up**

Value: Enabled/**Disabled**

Help text: `If enabled for the AHCI Capable sSATA 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 there are enough HDDs 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 up 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 there are many HDDs 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 Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

6. **SATA Port**

SATA ports 0-7 for SATA controller and SATA ports 0-5 for sSATA 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 which 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.

Back to: SATA Port Configuration – Mass Storage Controller Configuration – Advanced Screen – Screen map

3.3.7 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.

PCI Configuration	
Memory Mapped I/O above 4	**Enabled**/Disabled
MMIO High Base	**56T/**40T/24T/16T/4T/1T
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 – Screen map	
Memory Mapped I/O Size	Auto/1G/4G/16G/64G/**256G**/1024G
Add-In Video Adapter	**Enabled** / Disabled
Onboard Video	**Enabled** / Disabled
Fast Video	**Enabled** / Disabled
Legacy VGA Socket	**CPU Socket 1**/CPU Socket 2
Onboard VGA Always On	**Disabled**/Enabled
ARI Support	**Enabled** / Disabled
SR-IOV Support	**Enabled** / Disabled
► PCIe Slot Bifurcation Setting	
► PCIe Error Maintain	
► NIC Configuration	
► UEFI Network Stack	
► UEFI Option ROM Control	
► PCIe* Port Option ROM Control	
► Processor PCIe* Link Speed	
► Volume Management Device	
F10=Save Changes and Exit F9=Reset to Defaults	
↕↔=Move Highlight <Enter> = Select Entry Esc=Exit	

Figure 18. PCI Configuration screen

1. **Memory Mapped I/O above 4 GB**

    Value: **Enabled**/Disabled

    Help text: `Enable or disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space.`

    Comments: When enabled, PCI/PCIe* Memory Mapped I/O for devices capable of 64-bit addressing is allocated to address space above 4 GB, to allow larger allocations and avoid impacting address space below 4 GB.

    Back to: PCI Configuration – Advanced Screen – Screen map

2. **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 – Screen map

3. **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 4 GB 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 will automatically calculate the required MMIO size of all add-in PCIe devices and try to assign sufficient resource for each device.

    This option is grayed out when Memory Mapped I/O above 4 GB option is disabled. In addition, the 4096G option is only valid on one- or two-socket platforms; it is hidden on a four-socket platform with all four CPUs installed.

    Note: The system will 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 – Screen map

4. **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 1 with the Legacy VGA Socket option set to CPU Socket 1, 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 2 with the Legacy VGA Socket option set to CPU Socket 2, this option is set to Disabled and grayed out and unavailable.

If the Legacy VGA Socket option is set to CPU Socket 1 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 – Screen map

5. **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 1, and the Legacy VGA Socket option is set to CPU Socket 1, 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 2, and the Legacy VGA Socket option is set to CPU Socket 2, this option is grayed out and unavailable, with a value set to Disabled. This is because the Onboard Video is connected to CPU Socket 1, and is not functional when CPU Socket 2 is the active path for video. When Legacy VGA Socket is set back to CPU Socket 1, this option becomes available again and is set to its default value of Enabled.

Note: This option does not appear on some models. Refer to *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12 for product-specific information.

Back to: PCI Configuration – Advanced Screen – Screen map

6. **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 – Screen map

7. **Legacy VGA Socket**

Value: **CPU Socket 1**/CPU Socket 2

Help text: `Determines whether Legacy VGA video output is enabled for PCIe slots`
`attached to Processor Socket 1 or 2. Socket 1 is the default.`

Comments: This option is necessary when using an add-in video card on a PCIe slot attached to CPU Socket 2, 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 2.

This option does not appear unless the BIOS is running on a board which has one processor installed on CPU Socket 2 and can potentially have a video card installed in a PCIe slot connected to CPU Socket 2.

This option is grayed out as unavailable and set to CPU Socket 1 unless there is a processor installed on CPU Socket 2 and a video card installed in a PCIe slot connected to CPU Socket 2. When this option is active and is set to CPU Socket 2, 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 1, and is unavailable when the Legacy VGA Socket is set to Socket 2.

Back to: PCI Configuration – Advanced Screen – Screen map

8. **Onboard VGA Always On**

Value: **Disabled**/Enabled

Help text: `Enable onboard video controller even if the Add-in video install in`
`CPU Socket 1, this option only visible when Legacy VGA Socket set to`
`CPU Socket 1.`

Comments: This option only visible when Legacy VGA Socket set to CPU Socket 1. If the Legacy VGA Socket set to CPU Socket 2 then this option will not be displayed.

Back to: PCI Configuration – Advanced Screen – Screen map

9. **ARI Support**

Value: **Enabled**/Disabled

Help text: `Enable or disable the ARI support.`

Comments: None

Back to: PCI Configuration – Advanced Screen – Screen map

10. SR-IOV Support

Value: **Enabled**/Disabled

Help text: `Enable or disable the SR-IOV support.`

Comments: None

Back to: PCI Configuration – Advanced Screen – Screen map

11. 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 3.3.7.1.

> **Note**: This configuration page is only visible on Intel® Server Board S2600KP.

Back to: PCI Configuration – Advanced Screen – Screen map

12. PCIe Error Maintain

Value: None

Help text: `View/Configure PCIe Error Maintain setting.`

Comments: *Selection only.* For more information on PCIe Error Maintain settings, see Section 3.3.7.2.

Back to: PCI Configuration – Advanced Screen – Screen map

13. NIC Configuration

Value: None

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

Comments: *Selection only.* For more information on NIC Configuration settings, see Section 3.3.7.3.

> **Note**: This field cannot support Syscfg changes with the `/bcs` command and cannot support Intel Integrator Tookit customization. For Intel® Server Board S2600BT, which does not have onboard ports, this page does not exist.

Back to: PCI Configuration – Advanced Screen – Screen map

14. 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 Section 3.3.7.4.

Back to: PCI Configuration – Advanced Screen – Screen map

15. 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 3.3.7.5.

Note: This field cannot support Syscfg changes with the `/bcs` command and cannot support Intel Integrator Tookit customization.

Back to: PCI Configuration – Advanced Screen – Screen map

16. PCIe Port Oprom Control

Value: None

Help text: `View/Configure PCIe Port Oprom control settings.`

Comments: *Selection only.* For more information on PCIe* Port option ROM (Oprom) Control settings, see Section 3.3.7.6.

Note: This field cannot support Syscfg changes with the `/bcs` command. For Intel Integrator Tookit customization tool, the user should change the proper item based on real configuration. For Intel® Server Board S2600BT, which only supports UEFI Mode, this page does not exist.

Back to: PCI Configuration – Advanced Screen – Screen map

17. Processor PCIe Link Speed

Value: None

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

Comments: *Selection only.* For more information on PCIe link speed settings, see Section 3.3.7.7.

Back to: PCI Configuration – Advanced Screen – Screen map

18. 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 3.3.7.8.

Back to: PCI Configuration – Advanced Screen – Screen map

3.3.7.1 PCIe* Slot Bifurcation Setting

Each board in the Intel Server Board S2600 family has different risers and different options for PCIe slot bifurcation.

PCIe Slot Bifurcation Setting

Riser_Slot_1 Bifurcation   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
Riser_Slot_2 Bifurcation   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4

F10=Save Changes and Exit   F9=Reset to Defaults

⬇⬆⬅➡=Move Highlight   <Enter> = Select Entry   Esc=Exit
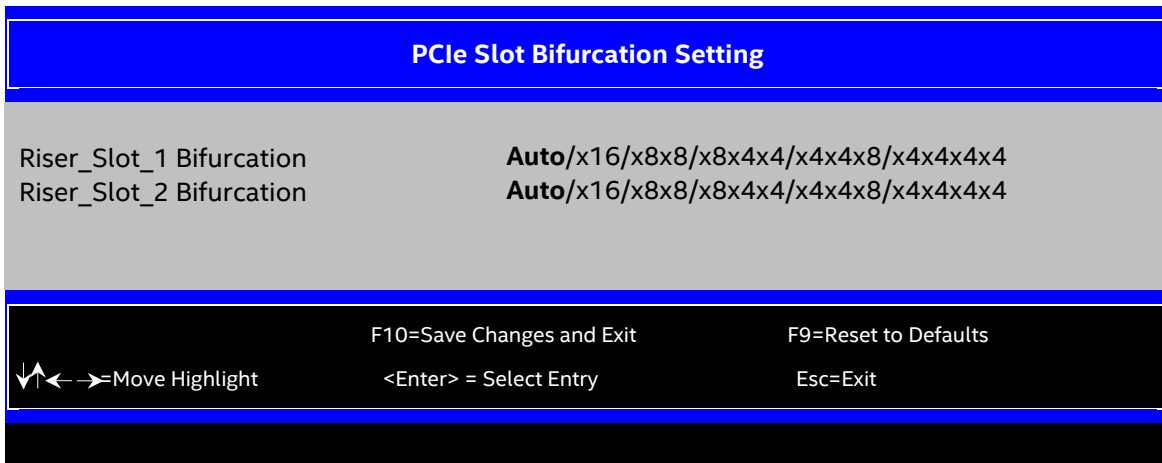
Figure 19. PCIe Slot Bifurcation Setting screen – Intel® Server Board S2600WF / S2600WFR

PCIe Slot Bifurcation Setting

Riser_Slot_1 Bifurcation
CPU1 IO2   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
Riser_Slot_2 Bifurcation
CPU1 IOU3   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
CPU1 IOU1   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
Riser_Slot_3 Bifurcation
CPU2 IOU1   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
CPU2 IOU3   **Auto**/x8
Riser_Slot_4 Bifurcation
CPU2 IOU2   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4

F10=Save Changes and Exit   F9=Reset to Defaults

⬇⬆⬅➡=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 20. PCIe Slot Bifurcation Setting screen – Intel® Server Board S2600BP / S2600BPR

PCIe Slot Bifurcation Setting

Riser_Slot_2 Bifurcation   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4
Riser_Slot_6 Bifurcation   **Auto**/x16/x8x8/x8x4x4/x4x4x8/x4x4x4x4

F10=Save Changes and Exit   F9=Reset to Defaults
↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit
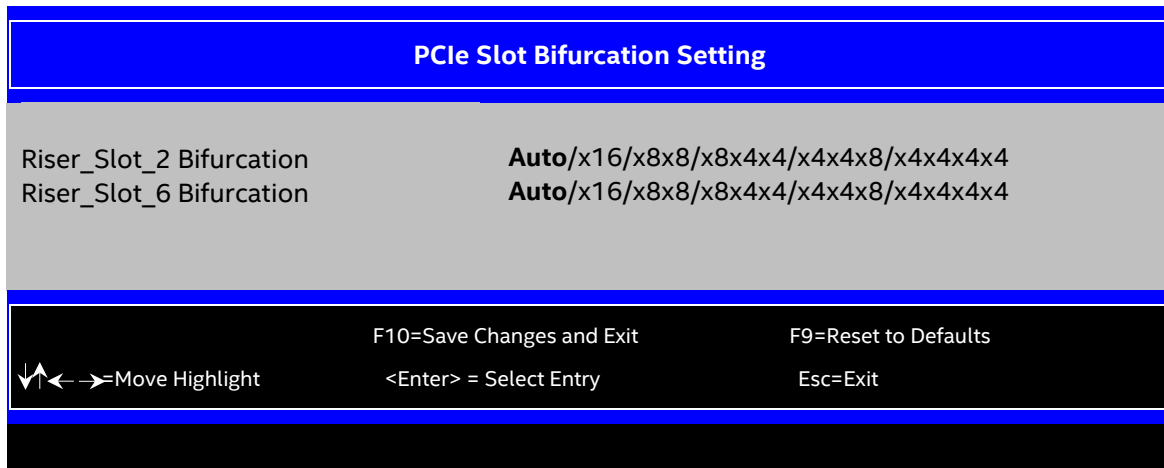
Figure 21. PCIe Slot Bifurcation Setting screen – Intel® Server Board S2600ST / S2600STR

1. **Riser_Slot_X Bifurcation**
   CPU 1/2 IOU 1/2/3 (for Intel® Server Board S2600BP / S2600BPR)

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

   Help text: None

   Comments: Select PCIe port bifurcation for the selected slot(s) of the riser.

   > **Note**: Each setup item displays if a x16 riser is plugged. Otherwise, for all SKUs except S2600ST / S2600STR, they are hidden. Intel Server Board S2600 shows the Auto bifurcation option.

   Back to:

3.3.7.2   PCIe* Error Maintain

To support the Intel® Xeon Phi™ processor error maintain feature defined in software CCB303, the BIOS provides these items for the Intel Server Board S2600 family. It is shown only if the slot bifurcation is x16; any other bifurcation will be hidden. When enabled, and an error happens on an Intel Xeon Phi card, CPLD will consume this GPIO value to skip this riser reset (whole riser include the slot card plugged). So after the reset, these errors are kept in the card for further debug.

Each item controls a GPIO pin. The default is Disabled which means the GPIO value is GPO.

PCIe Error Maintain

PCIeErrorMaintain_Riser1   Enabled/**Disabled**
PCIeErrorMaintain_Riser2   Enabled/**Disabled**

F10=Save Changes and Exit   F9=Reset to Defaults
↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit
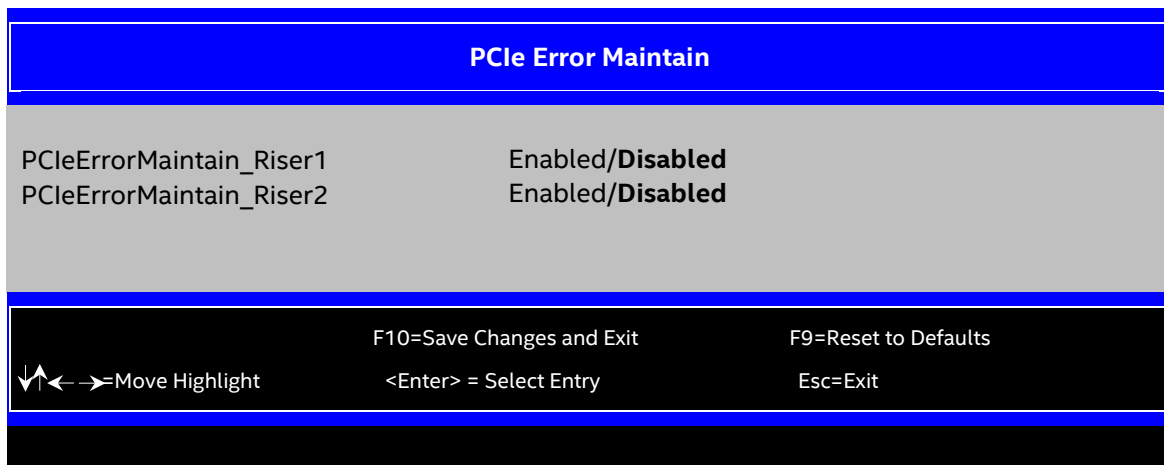
Figure 22. PCIe Error Maintain screen – Intel® Server Board S2600WF / S2600WFR

PCIe Error Maintain	
PCIeErrorMaintain_Riser1	Enabled/**Disabled**
PCIeErrorMaintain_Riser2	Enabled/**Disabled**
PCIeErrorMaintain_Riser3	Enabled/**Disabled**
PCIeErrorMaintain_Riser4	Enabled/**Disabled**

F10=Save Changes and Exit   F9=Reset to Defaults

↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit
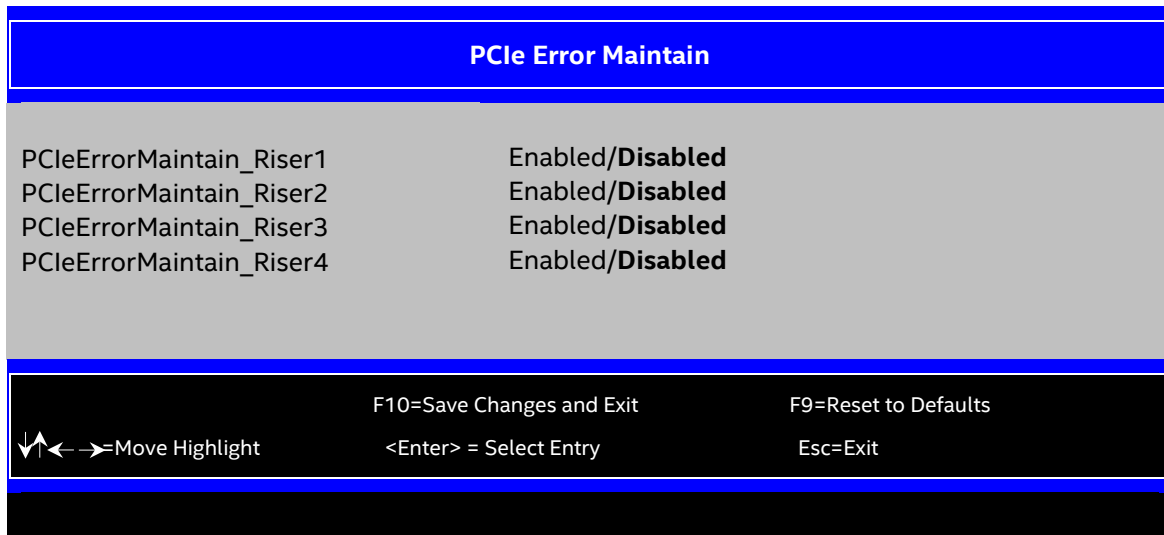
Figure 23. PCIe Error Maintain screen – Intel® Server Board S2600BP / S2600BPR

PCIe Error Maintain	
PCIeErrorMaintain_Slot2_&_Slot4	Enabled/**Disabled**
PCIeErrorMaintain_Slot6	Enabled/**Disabled**

F10=Save Changes and Exit   F9=Reset to Defaults

↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit
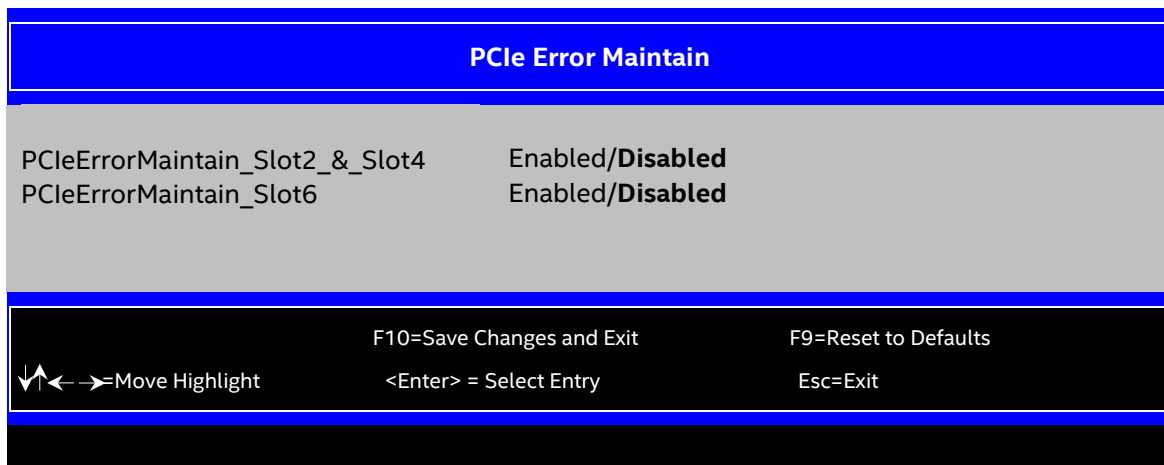
Figure 24. PCIe Error Maintain screen – Intel® Server Board S2600ST / S2600STR

1. **PCIeErrorMaintain_RiserX (Intel® Server Boards S2600WF / S2600WFR and S2600BP / S2600BPR)**
   PCIeErrorMaintain_SlotX (Intel® Server Board S2600ST / S2600STR)

   Value: Enabled/**Disabled**

   Help text: None

   Comments: Select PCIe port error maintain feature.

   Back to: PCIe* Error Maintain – PCI Configuration – Advanced Screen – Screen map

3.3.7.3 NIC Configuration

The NIC Configuration screen allows the user to configure the network interface card (NIC) controller options for BIOS POST. It also displays the NIC MAC addresses currently in use. 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 there are two onboard NICs. There are several possible types of NICs which are incorporated into different boards.

For boards with only one onboard NIC, the Onboard NIC2 entries are not present on the screen. The number of Port options displayed for each NIC will match the number of ports the onboard NIC presents.

Note: The fields on the NIC Configuration screen do not support SysCfg changes with the `/bcs` command and do not support Intel Integrator Tookit customization.

When a NIC port is disabled, its MAC address is hidden. When a NIC controller is disabled, all ports and all MAC addresses for those ports are hidden.

For the Intel Server Board S2600 family, if the onboard NIC is the Intel® C620 PCH Integrated 10 Gigabit Ethernet Controller, the NIC controller disable/enable feature will only be supported under UEFI mode. The NIC controller disable/enable will be grayed out and enabled by default under Legacy mode.

NIC Configuration

Onboard NIC1 Type	<Onboard NIC Description – Non-InfiniBand*>
NIC1 Controller	**Enabled /** Disabled
NIC1 Port1	**Enabled /** Disabled
NIC1 Port2	**Enabled /** Disabled
NIC1 Port3	**Enabled /** Disabled
NIC1 Port4	**Enabled /** Disabled
NIC1 Port1 MAC Address	<MAC Address display>
NIC1 Port2 MAC Address	<MAC Address display>
NIC1 Port3 MAC Address	<MAC Address display>
NIC1 Port4 MAC Address	<MAC Address display>
Onboard NIC2 Type	<Onboard NIC Description – Non-InfiniBand*>
NIC2 Controller	**Enabled /** Disabled
NIC2 Port1	**Enabled /** Disabled
NIC2 Port2	**Enabled /** Disabled
NIC2 Port3	**Enabled /** Disabled
NIC2 Port4	**Enabled /** Disabled
NIC 2 Port 1 MAC Address	<MAC Address display>
NIC 2 Port 2 MAC Address	<MAC Address display>
NIC 2 Port 3 MAC Address	<MAC Address display>
NIC 2 Port 4 MAC Address	<MAC Address display>

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

Figure 25. NIC Configuration screen

1. **Onboard NIC1 Type**
2. **Onboard NIC2 Type**

   Value: <Onboard NIC description>

   Help text: None

   Comments: *Information only.* This is a display showing which NICs are available as network controllers integrated into the baseboard. The possible NIC descriptions are:

   - `Intel(R) C620 PCH Integrated 10 Gigabit Ethernet Controller`
   - `Intel(R) X550 Dual-Port 10 Gigabit RJ-45 Controller`

   Each of these onboard NICs is followed by a section including a group of options that are specific to the type of NIC.

   If a board only has one onboard NIC, the second NIC type and following options section does not appear.

   For details about the NIC hardware configuration for a specific board, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 12.

Back to: NIC Configuration – PCI Configuration – Advanced Screen – Screen map

3. **NIC1 Controller**
4. **NIC2 Controller**

Value: **Enabled**/Disabled

Help text: `Enable/Disable Onboard Network Controller.`

Comments: This option completely disables the onboard network controller NIC1 or NIC2, along with all included NIC ports and their associated options. If disabled, that controller's NIC ports, port PXE options, and port MAC address displays do not appear.

Back to: NIC Configuration – PCI Configuration – Advanced Screen – Screen map

5. **NIC1 Port1**
6. **NIC1 Port2**
7. **NIC1 Port3**
8. **NIC1 Port4**
9. **NIC2 Port1**
10. **NIC2 Port2**
11. **NIC2 Port3**
12. **NIC2 Port4**

Value: **Enabled**/Disabled

Help text: `Enable/Disable Onboard NIC<n> Port<x>.`

Comments: This enables or disables port<x, x = 1-4> of onboard network controller<n, n = 1-2>, including associated port PXE options. The NIC<n> Port<x> PXE option and MAC address display do not appear when that port is disabled.

The associated port enable/disable options do not appear when NIC<n> is disabled.

Only ports that actually exist for a particular NIC appear in this section. That is, Port1-Port4 appear for a quad-port NIC, Port1-Port2 appear for a dual-port NIC, and only Port1 appears for a single-port NIC.

For details about the NIC hardware configuration for a specific board, refer to *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12 or the Technical Product Specification for that board.

Note: For the case the onboard NIC is the Intel® C620 PCH Integrated 10 Gigabit Ethernet Controller, NIC port Enable/Disable setup option will only be supported under UEFI boot mode.

Back to: NIC Configuration – PCI Configuration – Advanced Screen – Screen map

13. **NIC1 Port1 MAC Address**
14. **NIC1 Port2 MAC Address**
15. **NIC1 Port3 MAC Address**
16. **NIC1 Port4 MAC Address**
17. **NIC 2 Port 1 MAC Address**
18. **NIC 2 Port 2 MAC Address**
19. **NIC 2 Port 3 MAC Address**
20. **NIC 2 Port 4 MAC Address**

Value: <MAC address>

Help text: None

Comments: *Information only*. 12 hex digits of the MAC address of Port1-Port4 of the network controller corresponding to NIC1 or NIC2.

This display appears only for ports that actually exist on the corresponding network controller. If the network controller or port is disabled, the port MAC Address does not appear.

Back to: NIC Configuration – PCI Configuration – Advanced Screen – Screen map

3.3.7.4   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.

UEFI Network Stack	
UEFI Network Stack	**Enabled**/Disabled
IPv4 PXE Support	**Enabled**/Disabled
IPv6 PXE Support	**Enabled**/Disabled

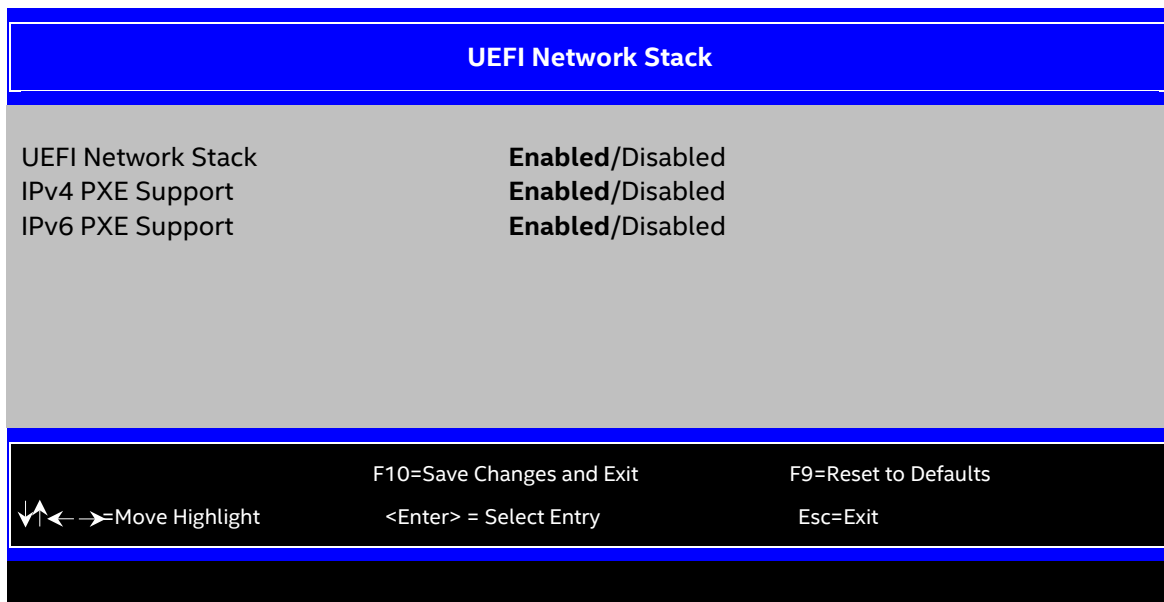| F10=Save Changes and Exit	F9=Reset to Defaults
↕←→=Move Highlight <Enter> = Select Entry	Esc=Exit

Figure 26. 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 Spec v2.3.1.

Back to: UEFI Network Stack – PCI Configuration – Advanced Screen – 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 native UEFI PXE functionality.

    Back to: UEFI Network Stack – PCI Configuration – Advanced Screen – 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 native UEFI PXE functionality.

    Back to: UEFI Network Stack – PCI Configuration – Advanced Screen – Screen map

3.3.7.5 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. There are four groups 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 SysCfg changes with the `/bcs` command and do not support Intel Integrator Tookit 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 which 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 27 is an example for the UEFI Option ROM Control screen. The exact content changes according to the system configuration.

```
┌─────────────────────────────────────────────────────────────────────────┐
│                        UEFI Option ROM Control                            │
└─────────────────────────────────────────────────────────────────────────┘

 NIC Controller
 NIC Card 1 Port1 OPROM Slot:0x0331
       –   IPV4
       –   VLAN
       –   IPV6
 NIC Card 1 Port2 OPROM Slot: 0x0331
       –   IPV4
       –   VLAN
       –   IPV6
 Fiber Channel
 xxxxxx XXXxxxx xxGb FC Adaptor – xxxxxxxxxxxxxx
 Slot: 0x0332
 xxxxxx XXXxxxx xxGb FC Adaptor – xxxxxxxxxxxxxx
 Slot: 0x0332

 Storage Controller
 Storage Card 1 OPROM Slot:0x0231

 Storage Card 2 OPROM Slot:0x0232

 Others
 OPROM Name Slot: 0xxxx




┌─────────────────────────────────────────────────────────────────────────┐
│              F10=Save Changes and Exit        F9=Reset to Defaults        │
│  ↓↑←→=Move Highlight       <Enter> = Select Entry        Esc=Exit         │
└─────────────────────────────────────────────────────────────────────────┘
```

Figure 27. 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.

3.3.7.6 PCIe* Port Option ROM Control

The PCIe* Port Option ROM Control screen allows the user to configure the expansion ROM dispatching of the PCIe devices connected to the integrated IO (IIO) PCIe root port during the BIOS POST.

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

The usage for these option is to save the limited memory space for PCIe option ROM. The BIOS currently only supports controlling the PCIe devices off the IIO root ports and the design follows the IIO PCIe Lane Partitioning rules, shown in Figure 28. The IIO supports 48 PCIe lanes and four Direct Media Interface (DMI) lanes. The DMI lanes can also be strapped to operate in PCIe mode, which is displayed as PCIe Port 00. The 48 PCIe lanes are grouped as 3 x16 (Port1, Port2, and Port3). Port1, Port2, and Port3 can each be bifurcated as 2 x8 or 4 x4 or any combination thereof, which is displayed as PCIe Port 2a, 2b, 2c, or 2d and PCIe Port 3a, 3b, 3c, or 3d.
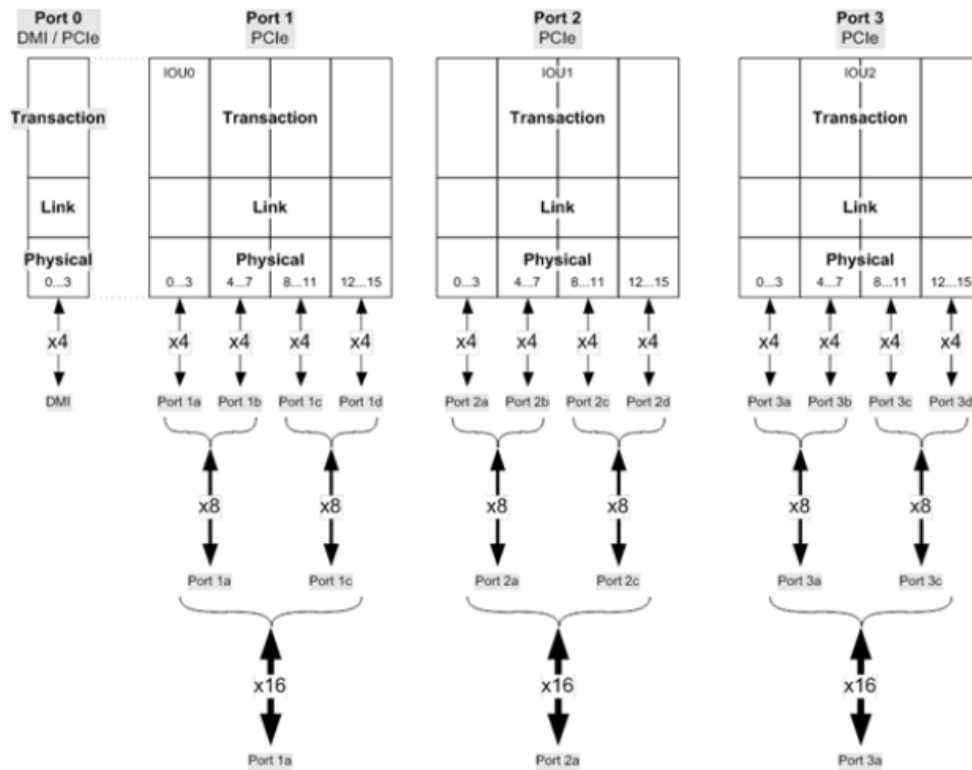

Figure 28. IIO PCIe* lane partitioning

PCIe Port Oprom Control	
CPU socket 1	
PCIe Port 1a OpROM control	**Enabled** / Disabled
PCIe Port 1b OpROM control	**Enabled** / Disabled
PCIe Port 1c OpROM control	**Enabled** / Disabled
PCIe Port 1d OpROM control	**Enabled** / Disabled
PCIe Port 2a OpROM control	**Enabled** / Disabled
PCIe Port 2b OpROM control	**Enabled** / Disabled
PCIe Port 2c OpROM control	**Enabled** / Disabled
PCIe Port 2d OpROM control	**Enabled** / Disabled
PCIe Port 3a OpROM control	**Enabled** / Disabled
PCIe Port 3b OpROM control	**Enabled** / Disabled
PCIe Port 3c OpROM control	**Enabled** / Disabled
PCIe Port 3d OpROM control	**Enabled** / Disabled
CPU socket 1	
PCIe Port 1a OpROM control	**Enabled** / Disabled
PCIe Port 1b OpROM control	**Enabled** / Disabled
PCIe Port 1c OpROM control	**Enabled** / Disabled
PCIe Port 1d OpROM control	**Enabled** / Disabled
PCIe Port 2a OpROM control	**Enabled** / Disabled
PCIe Port 2b OpROM control	**Enabled** / Disabled
PCIe Port 2c OpROM control	**Enabled** / Disabled
PCIe Port 2d OpROM control	**Enabled** / Disabled
PCIe Port 3a OpROM control	**Enabled** / Disabled
PCIe Port 3b OpROM control	**Enabled** / Disabled
PCIe Port 3c OpROM control	**Enabled** / Disabled
PCIe Port 3d OpROM control	**Enabled** / Disabled
PCIe Port 00 OpROM control	**Enabled** / Disabled

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

Figure 29. PCIe Port Oprom Control screen

1. **PCIe Port 1a/Port1b/Port1c/Port1d/Port 2a/Port 2b/Port 2c/Port 2d/ Port 3a/Port 3b/Port 3c/Port 3d/Port 00 OpROM Control**

Value: **Enabled**/Disabled

Help Text: `Enable or Disable Oprom dispatching of the PCIe Devices on this Root Port.`

Comments: Disabling option ROM dispatching of the PCIe* devices on this root port saves the limited memory space for PCIe option ROM.

Note: This field cannot support Syscfg changes with the `/bcs` command. For Intel Integrator Tookit tool, the user should change the proper item based on real configuration.

Back to:

3.3.7.7 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 option is to select the target link speed as Gen1, Gen2, or Gen3 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 Figure 28. The IIO supports 48 PCIe lanes and four DMI lanes. The DMI lanes can also be strapped to operate in PCIe mode, which is displayed as PCIe Port 00. The 48 PCIe lanes are grouped in three. Each port can be bifurcated as 2x8 or 4x4 or any combination thereof, which is displayed as PCIe Ports 1a, 1b, 1c or 1d.
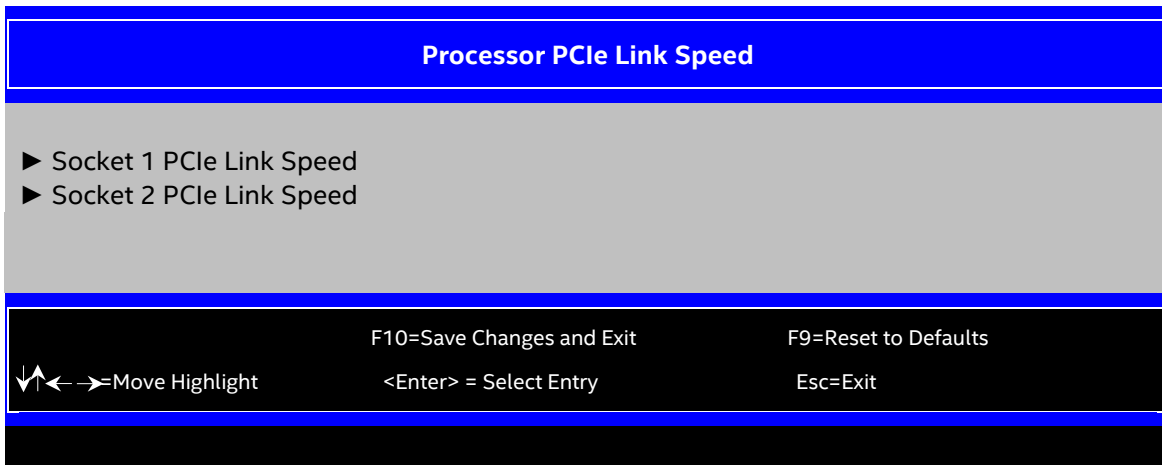

Figure 30. Processor PCIe Link Speed screen

Socket x PCIe Link Speed	
Socket x, DMI	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 1a	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 1b	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 1c	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 1d	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 2a	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 2b	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 2c	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 2d	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 3a	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 3b	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 3c	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**
Socket x, PCIe Port 3d	Gen1(2.5GT/s)/ Gen2 (5GT/s) /**Gen3(8GT/s)**

F10=Save Changes and Exit   F9=Reset to Defaults

↕↔=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 31. Processor Socket x PCIe Link Speed screen

1. **Socket x, DMI**

   Value: **Gen3(8GT/s)**/Gen2 (5GT/s)/Gen1 (2.5GT/s)

   Help Text: Allow for selecting target PCIe Link Speed as Gen1, Gen2 or Gen3.

   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.

   Back to: Processor PCIe* Link Speed – PCI Configuration – Advanced Screen – Screen map

2. **Socket x, PCIe Port 1a**
3. **Socket x, PCIe Port 1b**
4. **Socket x, PCIe Port 1c**
5. **Socket x, PCIe Port 1d**
6. **Socket x, PCIe Port 2a**
7. **Socket x, PCIe Port 2b**
8. **Socket x, PCIe Port 2c**
9. **Socket x, PCIe Port 2d**
10. **Socket x, PCIe Port 3a**
11. **Socket x, PCIe Port 3b**
12. **Socket x, PCIe Port 3c**
13. **Socket x, PCIe Port 3d**

Value: **Gen3(8GT/s)**/Gen2 (5GT/s)/Gen1 (2.5GT/s)

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

Comments: PCIe port support Gen1, Gen2 and Gen3 speed. Those options for PCIe ports are only available when there is corresponding PCIe slot implemented on the specific board.

Back to: Processor PCIe* Link Speed – PCI Configuration – Advanced Screen – Screen map

3.3.7.8 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 hotplug. It can also work with Intel RSTe to create a PCIe SSD RAID volume.

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

Volume Management Device	
Riser1, Slot1 Volume Management Device(CPU1, IOU1) (connect riser with 2 slots)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Riser1, Slot2 Volume Management Device(CPU2, IOU1) (connect riser with 2 slots)	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Riser1, Slot1 Volume Management Device(CPU1, IOU1) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
Riser1, Slot2 Volume Management Device(CPU1, IOU1) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Riser1, Slot3 Volume Management Device(CPU2, IOU1) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
CPU1 Oculink Volume Management Device (CPU1, IOU3)	Enabled / **Disabled**
VMD Port 3C (PCIe SSD0)	Enabled / **Disabled**
VMD Port 3D (PCIe SSD1)	Enabled / **Disabled**
Riser2, Slot1 Volume Management Device(CPU2, IOU2) (connect riser with 2 slots)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
Riser2, Slot2 Volume Management Device(CPU2, IOU1) (connect riser with 2 slots)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**

Riser2, Slot1 Volume Management Device(CPU2, IOU2) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
Riser2, Slot2 Volume Management Device(CPU2, IOU2) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
Riser2, Slot3 Volume Management Device(CPU2, IOU1) (connect riser with 3 slots)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
CPU2 Oculink Volume Management Device (CPU2, IOU3)	Enabled / **Disabled**
VMD Port 3A (PCIe SSD2)	Enabled / **Disabled**
VMD Port 3B (PCIe SSD3)	Enabled / **Disabled**
Riser3, Slot2 Volume Management Device(CPU2, IOU3)	Enabled / **Disabled**
VMD Port 3C	Enabled / **Disabled**
VMD Port 3D	Enabled / **Disabled**

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

Figure 32. Volume Management Device screen – Intel® Server Board S2600WF / S2600WFR

Volume Management Device	
CPU1 Oculink Volume Management Device (CPU1, IOU1)	Enabled / **Disabled**
VMD Port 1C (PCIe SSD0)	Enabled / **Disabled**
VMD Port 1D (PCIe SSD1)	Enabled / **Disabled**
Slot6 Volume Management Device(CPU1, IOU2)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
Slot5 Volume Management Device(CPU1, IOU3)	Enabled / **Disabled**
VMD Port 3C	Enabled / **Disabled**
VMD Port 3D	Enabled / **Disabled**
CPU1 Oculink Volume Management Device (CPU1, IOU3)	Enabled / **Disabled**
VMD Port 3A (PCIe SSD2)	Enabled / **Disabled**
VMD Port 3B (PCIe SSD3)	Enabled / **Disabled**
Slot1 Volume Management Device (CPU2, IOU3)	Enabled / **Disabled**
VMD Port 3A	Enabled / **Disabled**
VMD Port 3B	Enabled / **Disabled**
Slot2 Volume Management Device (CPU2, IOU1)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Slot3 Volume Management Device (CPU2, IOU3)	Enabled / **Disabled**
VMD Port 3C	Enabled / **Disabled**
VMD Port 3D	Enabled / **Disabled**
Slot4 Volume Management Device (CPU2, IOU2)	Enabled / **Disabled**
CPU2 VMD Port 2A	Enabled / **Disabled**
CPU2 VMD Port 2B	Enabled / **Disabled**
CPU2 VMD Port 2C	Enabled / **Disabled**
CPU2 VMD Port 2D	Enabled / **Disabled**

F10=Save Changes and Exit   F9=Reset to Defaults

↕←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 33. Volume Management Device screen – Intel® Server Board S2600ST / S2600STR

Volume Management Device	
Slot1 Volume Management Device(CPU1, IOU2)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
Slot2 Volume Management Device(CPU1, IOU3&IOU1)	Enabled / **Disabled**
VMD Port 3A	Enabled / **Disabled**
VMD Port 3B	Enabled / **Disabled**
VMD Port 3C	Enabled / **Disabled**
VMD Port 3D	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Slot3 Volume Management Device(CPU2, IOU1&IOU3)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
VMD Port 3A	Enabled / **Disabled**
VMD Port 3B	Enabled / **Disabled**
Slot4 Volume Management Device(CPU2, IOU2)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
CPU2 Volume Management Device(CPU2, IOU1)	Enabled / **Disabled**
VMD Port 1B (PCIe SSD0)	Enabled / **Disabled**
VMD Port 1D (PCIe SSD1)	Enabled / **Disabled**

F10=Save Changes and Exit   F9=Reset to Defaults

↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Slot1 Volume Management Device(CPU1, IOU2)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
Slot2 Volume Management Device(CPU1, IOU3&IOU1)	Enabled / **Disabled**
VMD Port 3A	Enabled / **Disabled**
VMD Port 3B	Enabled / **Disabled**
VMD Port 3C	Enabled / **Disabled**
VMD Port 3D	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Slot3 Volume Management Device(CPU2, IOU1&IOU3)	Enabled / **Disabled**
VMD Port 1A	Enabled / **Disabled**
VMD Port 1B	Enabled / **Disabled**
VMD Port 1C	Enabled / **Disabled**
VMD Port 1D	Enabled / **Disabled**
Slot4 Volume Management Device(CPU2, IOU2)	Enabled / **Disabled**
VMD Port 2A	Enabled / **Disabled**
VMD Port 2B	Enabled / **Disabled**
VMD Port 2C	Enabled / **Disabled**
VMD Port 2D	Enabled / **Disabled**
CPU2 Volume Management Device(CPU2, IOU1)	Enabled / **Disabled**
VMD Port 1B (PCIe SSD0)	Enabled / **Disabled**
VMD Port 1D (PCIe SSD1)	Enabled / **Disabled**

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

Figure 34. Volume Management Device screen – Intel® Server Board S2600BP / S2600BPR

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

   For Intel® Server Board S2600WF / S2600WFR
   Riser1, Slot1 Volume Management Device(CPU1, IOU1) (connect riser with 2 slots)
   Riser1, Slot2 Volume Management Device(CPU2, IOU1) (connect riser with 2 slots)
   Riser1, Slot1 Volume Management Device(CPU1, IOU1) (connect riser with 3 slots)
   Riser1, Slot2 Volume Management Device(CPU1, IOU1) (connect riser with 3 slots)
   Riser1, Slot3 Volume Management Device(CPU2, IOU1) (connect riser with 3 slots)
   CPU1 Oculink Volume Management Device (CPU1, IOU3)
   Riser2, Slot1 Volume Management Device(CPU2, IOU2) (connect riser with 2 slots)
   Riser2, Slot2 Volume Management Device(CPU2, IOU1) (connect riser with 2 slots)
   Riser2, Slot1 Volume Management Device(CPU2, IOU2) (connect riser with 3 slots)
   Riser2, Slot2 Volume Management Device(CPU2, IOU2) (connect riser with 3 slots)
   Riser2, Slot3 Volume Management Device(CPU2, IOU1) (connect riser with 3 slots)
   CPU2 Oculink Volume Management Device (CPU2, IOU3)
   Riser3, Slot2 Volume Management Device(CPU2, IOU3)

   For Intel® Server Board S2600BP / S2600BPR
   Slot1 Volume Management Device(CPU1, IOU2)
   Slot2 Volume Management Device(CPU1, IOU3&IOU1)
   Slot3 Volume Management Device(CPU2, IOU1&IOU3)
   Slot4 Volume Management Device(CPU2, IOU2)
   CPU2 Volume Management Device(CPU2, IOU1)

   For Intel® Server Board S2600ST / S2600STR
   CPU1 Oculink Volume Management Device (CPU1, IOU1)
   Slot6 Volume Management Device (CPU1, IOU2)
   Slot5 Volume Management Device (CPU1, IOU3)
   CPU1 Oculink Volume Management Device (CPU1, IOU3)
   Slot1 Volume Management Device (CPU2, IOU3)
   Slot2 Volume Management Device (CPU2, IOU1)
   Slot3 Volume Management Device (CPU2, IOU3)
   Slot4 Volume Management Device (CPU2, IOU2)

Value: Enabled/**Disabled**

Help Text: `[Enabled] – VMD (Volume Management Device) is enabled.`
            `[Disabled] – VMD is disabled.`

Comments: Global setup option to enable or disable VMD support for this system. And the setup maybe different based on configuration for SKUs.

            For Intel Server Board S2600WF / S2600WFR, if a riser card is inserted in Riser 1 or 2, the VMD items show under different parent items according to the type of the riser card.

Table 5. VMD items for Intel® Server Board S2600WF / S2600WFR

Card Type	Riser1	Riser2
No riser card or 2-slots riser card	Riser1, Slot1 Volume Management Device(CPU1, IOU1) VMD Port 1A VMD Port 1B VMD Port 1C VMD Port 1D Riser1, Slot2 Volume Management Device(CPU2, IOU1) VMD Port 1C VMD Port 1D	Riser2, Slot1 Volume Management Device(CPU2, IOU2) VMD Port 2A VMD Port 2B VMD Port 2C VMD Port 2D Riser2, Slot2 Volume Management Device(CPU2, IOU1) VMD Port 1A VMD Port 1B
3-slots riser card	Riser1, Slot1 Volume Management Device(CPU1, IOU1) VMD Port 1A VMD Port 1B Riser1, Slot2 Volume Management Device(CPU1, IOU1) VMD Port 1C VMD Port 1D Riser1, Slot3 Volume Management Device(CPU2, IOU1) VMD Port 1C VMD Port 1D	Riser2, Slot1 Volume Management Device(CPU2, IOU2) VMD Port 2A VMD Port 2B Riser2, Slot2 Volume Management Device(CPU2, IOU2) VMD Port 2C VMD Port 2D Riser2, Slot3 Volume Management Device(CPU2, IOU1) VMD Port 1A VMD Port 1B

For Intel Server Board S2600ST / S2600STR, which is an Intel® QuickAssist Technology (Intel® QAT) SKU, CPU1 OCuLink Volume Management Device (CPU1, IOU1) will be hidden. In addition, if an Intel QAT cable is present, then both CPU1 OCuLink Volume Management Device (CPU1, IOU1) and CPU1 OCuLink Volume Management Device (CPU1, IOU3) will be hidden.

For Intel Server Board S2600BP / S2600BPR, support depends on the SKU. For the 1G SKU, Slot 1/2 VMD ports are both supported; on L and SFP+ SKUs, only Slot 2 VMD port is supported.

Back to: Volume Management Device – PCI Configuration – Advanced Screen – Screen map

2. **VMD Port 1A**
   VMD Port 1B / VMD Port 1B (PCIe SSD0)
   VMD Port 1C / VMD Port 1C (PCIe SSD0)
   VMD Port 1D / VMD Port 1D (PCIe SSD1)
   VMD Port 2A
   VMD Port 2B
   VMD Port 2C
   VMD Port 2D
   VMD Port 3A / VMD Port 3A (PCIe SSD2)
   VMD Port 3B / VMD Port 3B (PCIe SSD3)
   VMD Port 3C / VMD Port 3C (PCIe SSD0)
   VMD Port 3D / VMD Port 3D (PCIe SSD1)

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 base on this SKU's board design, only capable root port have visible option.

Note: This area lists all setup options. For detailed setup items per SKU, see the figures in Section 3.3.7.8.

3.3.8   Serial Port Configuration

The Serial Port Configuration screen allows the user to configure the Serial A and Serial B ports. 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 Section 3.5.1.

Figure 35. Serial Port Configuration screen

3. **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 – Screen map

4. **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 – Screen map

5. **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 will not support Intel Integrator Toolkit on the Intel Server Board S2600 family.

    Back to: Serial Port Configuration– Advanced Screen – Screen map

6. **Serial B Enable**

    Value: **Enabled**/Disabled

    Help Text: `Enable or Disable Serial port B.`

    Comments: Serial port B can be used for Serial Console Redirection.

    Back to: Serial Port Configuration– Advanced Screen – Screen map

7. **Serial B Address**

    Value: 3F8h/**2F8h**/3E8h/2E8h

    Help Text: `Select Serial port B base I/O address. This field will not appear`
                    `when Serial B port enable/disable does not appear.`

    Comments: Legacy I/O port address.

    Note: The Serial A Address and Serial B Address cannot be set to the same value.

    Back to: Serial Port Configuration– Advanced Screen – Screen map

8. **Serial B IRQ**

    Value: 3/**4**

    Help Text: `Select Serial port B interrupt request (IRQ) line. This field will`
                    `not appear when Serial B port enable/disable does not appear.`

    Comments: Legacy interrupt request (IRQ). It is gray because AST2500 UART IRQ is fixed under ESPI mode, and such option will not support Intel Integrator Toolkit on the Intel Server Board S2600 family.

    Back to: Serial Port Configuration– Advanced Screen – Screen map

3.3.9   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.

This screen displays all USB mass storage devices which have been detected in the system. These include USB-attached hard disk drives (HDDs), floppy disk drives (FDDs), CDROM and DVDROM drives, and USB flash memory devices (such as s USB key or key fob).

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, there are some restrictions:

- A USB key formatted as a CDROM 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 OS environment. They are NOT displayed on this screen or enumerated as bootable devices.

USB Configuration	
Detected USB Devices	
<Number of USB devices detected in system>	
Legacy USB Support	**Enabled/**Disabled/Auto
Port 60/64 Emulation	**Enabled/**Disabled
Make USB Devices Non-Bootable	Enabled**/Disabled**
USB Mass Storage Device Configuration	
Device Reset Timeout	10 seconds/**20 seconds**/30 seconds/40 seconds
Mass Storage Devices:	
<One device per line>	**Auto/**Floppy/Forced FDD/Hard Disk/CD-ROM

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

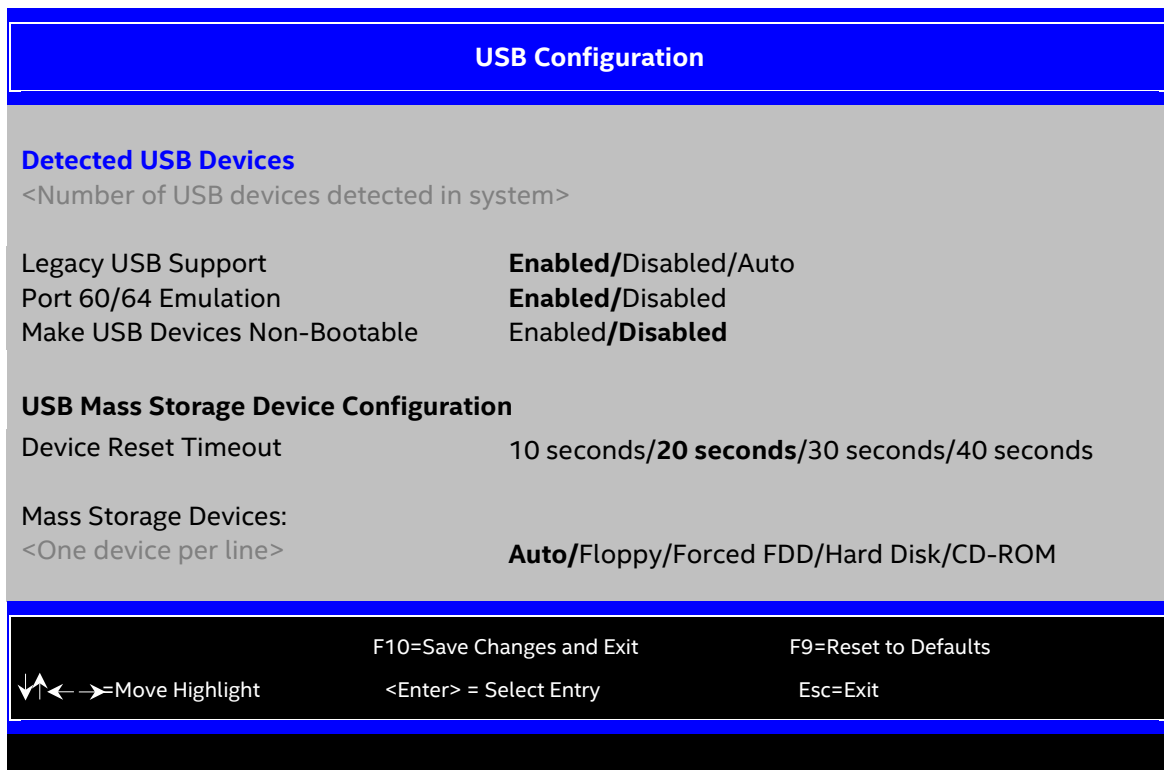**Figure 36. USB Configuration screen**

108

1. **Detected USB Devices**

   Value: <Number of USB devices detected in system>

   Help Text: None

   Comments: *Information only*. Displays the total number of USB devices of all types which have been detected in POST.

   > **Note**: There is one USB keyboard mouse and one USB mouse detected from the BMC KVM function under this item even if no USB devices are connected to the system.

   Back to: USB Configuration– Advanced Screen – Screen map

2. **Legacy USB Support**

   Value: Auto/**Enabled**/Disabled

   Help Text: `Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable option will only keep USB Keyboard devices available for EFI applications.`

   Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

   Back to: USB Configuration– Advanced Screen – Screen map

3. **Port 60/64 Emulation**

   Value: **Enabled**/Disabled

   Help Text: `Enables I/O port 60h/64h emulation support.`
   `This may be needed for legacy USB keyboard support when using an OS that is USB unaware.`

   Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

   Back to: USB Configuration– Advanced Screen – Screen map

4. **Make USB Devices Non-Bootable**

   Value: Enabled/**Disabled**

   Help Text: `Exclude USB in Boot Table.`
   `[Enabled] – This will remove all USB Mass Storage devices as Boot options.`
   `[Disabled] – This will allow all USB Mass Storage devices as Boot options.`

   Comments: This is a security option. When Disabled, the system cannot be booted directly to a USB device of any kind. USB Mass Storage devices may still be used for data storage.

   If the USB controller setting is disabled, this field is grayed out and inactive.

   Back to: USB Configuration– Advanced Screen – Screen map

5. **Device Reset Timeout**

Value: 10 seconds/**20 seconds**/30 seconds/40 seconds

Help Text: `USB Mass Storage device Start Unit command timeout.`
`Setting to a larger value provides more time for a mass storage device to be ready, if needed.`

Comments: If the USB controller setting is disabled, this field is grayed out and inactive.

Back to: USB Configuration– Advanced Screen – Screen map

6. **Mass Storage Devices**

Value: **Auto**/Floppy/Forced FDD/Hard Disk/CD-ROM

Help Text: `[Auto] – USB devices less than 530 MB are emulated as floppies.`
`[Forced FDD] – HDD formatted drive is emulated as an FDD (e.g., ZIP drive).`

Comments: This field is hidden if no USB mass storage devices are detected.

This setup screen can show a maximum of 16 USB mass storage devices on the screen. If more than 16 devices are installed in the system, the USB Devices Enabled field displays the correct count but only the first 16 devices discovered are displayed in this list.

If the USB controller setting is disabled, this field is grayed out and inactive.

These 16 options are for the USB mass storage devices from index 1 to 16, not target for specific USB device. If the USB device in index 1 is changed, the option value does not change, and it takes effect on the new USB device take this place. If the first option is set to HDD and the second option is set to FDD, and one USB device changes its order from index 1 to index 2 due to new devices added, the option value of index 2 takes effect to this device; it will emulate as FDD, not the original HDD.

Back to: USB Configuration– Advanced Screen – Screen map

3.3.10　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.

```
System Acoustic and Performance Configuration


Set Fan Profile                     Performance/Acoustic
Fan PWM Offset                      [0 – 100, 0 is default]
Air Flow Limit                      [60 – 100, 100 is default]
Exit Air Temp                       [50 – 70, 70 is default]
Fan UCC                             [70 – 100, 100 is default]



            F10=Save Changes and Exit           F9=Reset to Defaults

↕↔=Move Highlight          <Enter> = Select Entry           Esc=Exit
```

Figure 37. 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

   　　　　　　Note: If Syscfg/Sysinfo 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 Integrator Toolkit.

   Back to:

2. **Fan PWM Offset**

Value: [Entry Field 0-100, **0 is default**]

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.

This PWM offset setting is specified through the BIOS setup utility and is applicable to both Intel® server chassis and third-party chassi. However, the BMC firmware is the owner of the PWM offset setting. At each system boot, BIOS queries the BMC for the current PWM offset setting and displays this in the BIOS setup utility. 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 :Restricted*' and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Note: If Syscfg/Sysinfo 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 Integrator Toolkit.

Back to: System Acoustic and Performance Configuration– Advanced Screen – 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 6. Set FSC Parameter and Get FSC Parameter commands for Air Flow Limit option

NetFn 0x30	Request	Response	Note
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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

> **Note**: If Syscfg/Sysinfo 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 Integrator Toolkit.

Back to: System Acoustic and Performance Configuration– Advanced Screen – Screen map

4. **Exit Air Temp**

Value: [Entry Field 50-70, **70 is default**]

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. 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 gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Table 7. Set FSC Parameter and Get FSC Parameter commands for Exit Air Temp option

NetFn 0x30	Request	Response	Note
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 Parameter 1 Byte 2 – Sensor number(0x2e)	Byte 1 – Completion code Byte 2:n – Varies based on parameter number Parameter 1 – Tcontrol Byte 2 – TControl modifier value Byte 3 – Tcontrol SDR value	Byte1 is 1 in request.

> **Note**: If Syscfg/Sysinfo 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 Integrator Toolkit.

Back to: System Acoustic and Performance Configuration– Advanced Screen – 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, there are several fan domains. 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Table 8. Set FSC Parameter and Get FSC Parameter commands for Fan UCC option

NetFn 0x30	Request	Response	Note
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 Syscfg/Sysinfo 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 Integrator Toolkit.

Back to: System Acoustic and Performance Configuration– Advanced Screen – Screen map

3.3.11   FPGA Configuration

The FPGA Configuration screen allows the user to configure the available FPGA options.

To access this screen from the front page, select **Advanced > FPGA Configuration**. To move to another screen, press the **<Esc>** key to return to the Advanced screen, then select the desired screen.

Note: This configuration is only available on an FPGA-enabled platform.

FPGA Configuration

Socket 0 FPGA BBS Version	<BBS Version>
Socket 0 FPGA	**Enabled**/Disabled
Socket 0 BitStream	**Auto**/HSSI-BBS/None
Socket 1 FPGA BBS Version	<BBS Version>
Socket 1 FPGA	**Enabled**/Disabled
Socket 1 BitStream	**Auto**/HSSI-BBS/None

F10=Save Changes and Exit   F9=Reset to Defaults

↕←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 38. FPGA Configuration screen

1. **Socket 0 FPGA BBS Version**

   Value: <BBS Version>

   Help Text: None

   Comments: *Information only*. Displays current blue bit stream (BBS) Version loaded in the FPGA device. The Format of the Version: MajorVersion.MinorVersion.PatchVersion.DebugVersion.

   Back to: FPGA Configuration– Advanced Screen – Screen map

2. **Socket 0 FPGA**

   Value: **Enabled**/Disabled

   Help Text: None

   Comments: Enable/disabled the FPGA device on socket 0.

   Back to: FPGA Configuration– Advanced Screen – Screen map

3. **Socket 0 BitStream**

   Value: **Auto**/HSSI-BBS/None

   Help Text: None

   Comments: Select the BBS for the FPGA device. Use this option to not load the built-in BBS in the image and load a custom image after boot.

   Back to: FPGA Configuration– Advanced Screen – Screen map

4. **Socket 1 FPGA BBS Version**

    Value: \<BBS Version\>

    Help Text: None

    Comments: *Information only*. Displays current blue bit stream (BBS) Version loaded in the FPGA device. The Format of the Version: MajorVersion.MinorVersion.PatchVersion.DebugVersion.

    Back to: FPGA Configuration– Advanced Screen – Screen map

5. **Socket 1 FPGA**

    Value: **Enabled**/Disabled

    Help Text: None

    Comments: Enable/disabled the FPGA device on socket 1.

    Back to: FPGA Configuration– Advanced Screen – Screen map

6. **Socket 1 BitStream**

    Value: **Auto**/HSSI-BBS/None

    Help Text: None

    Comments: Select the BBS for the FPGA device. Use this option to not load the built-in BBS in the image and load a custom image after boot.

    Back to: FPGA Configuration– Advanced Screen – 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 the boards that support TPM.

It is necessary to activate the TPM to enable Intel® Trusted Execution Technology (Intel® TXT) on 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 3.3.1.

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 between 8 and 14 characters in length, and a password must contain at least one case-sensitive alphabetic 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.

Security	
Administrator Password Status	<Installed/Not Installed>
User Password Status	<Installed/Not Installed>
Set Administrator Password	[123aBcDeFgH$#@]
Set User Password	[123aBcDeFgH$#@]
Power On Password	Enabled/**Disabled**
Front Panel Lockout	Enabled/**Disabled**
Current TPM Device	<TPM2.0(FTPM)>
TPM2 Physical Presence Operation	
TPM2 Operation	**No Action** / TPM2 ClearControl(NO) + Clear
PCR Bank : SHA1	**[X]**
PCR Bank : SHA256	**[X]**
TPM FW Update	Enabled/**Disabled**
TPM FW Version :	<ID string from TPM>

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

Figure 39. 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 Syscfg display with the `/bcs` command.

    Back to:

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 Syscfg display with the `/bcs` command.

    Back to:

3. **Set Administrator Password**

    Value: [Entry Field – 0-14 characters]

    Help Text:
    ```
    Administrator password is used if Power On Password is enabled and to
    control change access in BIOS Setup. Length is 1-14 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.

    Deleting all characters in the password entry field removes a password previously set. 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 popup error message:

    ```
    Password entered is not valid. Only case sensitive alphabetic,
    numeric and special characters !@#$%^&*()-_+=? are allowed.
    ```

    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 popup error message:

    ```
    Password entered is not valid. Administrator and User passwords
    must be different.
    ```

    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 alphabetic, numeric, and special character. Length
    should be 8 to 14 characters.
    ```

For full details on BIOS password protection, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 9.1.

Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bap` command can be used to set the administrator password.

Back to: Security – Screen map

4. **Set User Password**

Value: [Entry Field – 0-14 characters]

Help Text: `User password is used if Power On Password is enabled and to allow restricted access to BIOS Setup. Length is 1-14 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 as well as 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 9.1.

Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bap` 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(FTPM)

   Help Text: None

   Comments: *Information only*. Shows the current TPM device. If the current TPM device is FTPM, TPM2.0(FTPM) is shown. 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 9.2.

   Back to: Security – Screen map

9. **PCR Bank : SHA1**

   Value: [Checkbox]

   Help Text: `TCG2 Request PCR Bank: SHA1`

   Comments: Use checkbox to select the TPM active PRC bank. Its default value relies on the TPM capability. Any TPM2 Operation selected will require the system to perform a hard reset to become effective. For information about TPM support, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 9.2.

   Back to: Security – Screen map

10. **PCR Bank : SHA256**

   Value: [Checkbox]

   Help Text: `TCG2 Request PCR Bank: SHA256`

   Comments: Use checkbox to select the TPM active PRC bank. Its default value relies on the TPM capability. Any TPM2 Operation selected will require the system to perform a hard reset to become effective. For information about TPM support, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 9.2.

   Back to: Security – Screen map

11. TPM FW Update

Value: Enabled**/Disabled**

Help Text: `Enable/disable Update TPM frimware.`

Comments: None

Back to: Security – Screen map

12. TPM FW Version

Value: ID String for TPM

Help Text: `Show current TPM FW Version.`

Comments: *Information only.* Displays TPM FW Version string read from TPM. This will be displayed only if TPM FW Update option is enabled.

Back to: Security – Screen map

Note: TPM2 Operation, PCR Bank: SHA1 and PCR Bank: SHA256 options do not support BIOS customization utilities (Syscfg or Intel Integrator Toolkit). This can only be changed within the setup menus of the target system.

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.
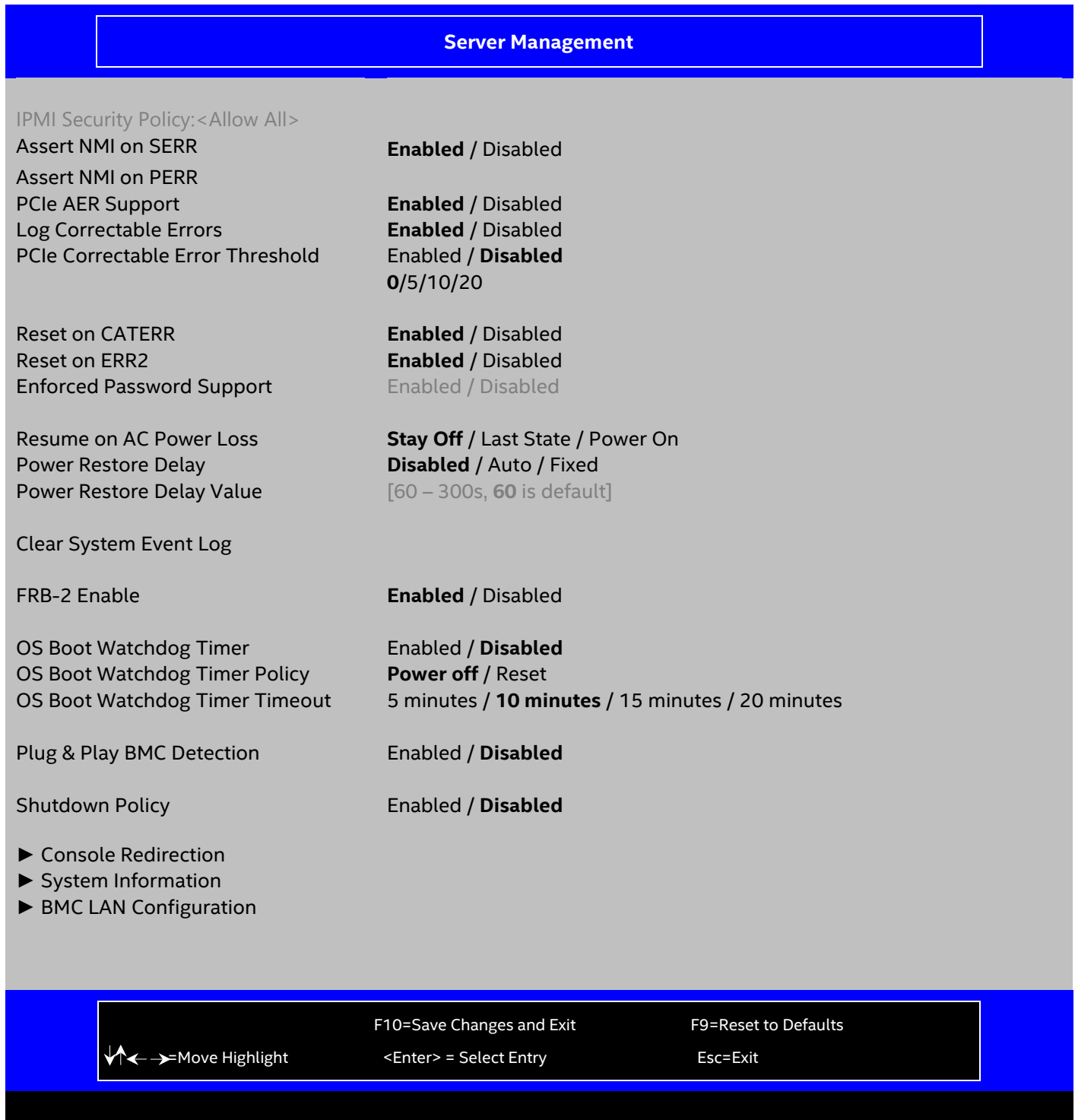
Server Management	
IPMI Security Policy:<Allow All>	
Assert NMI on SERR	**Enabled** / Disabled
Assert NMI on PERR	
PCIe AER Support	**Enabled** / Disabled
Log Correctable Errors	**Enabled** / Disabled
PCIe Correctable Error Threshold	Enabled / **Disabled**
	0/5/10/20
Reset on CATERR	**Enabled** / Disabled
Reset on ERR2	**Enabled** / Disabled
Enforced Password Support	Enabled / Disabled
Resume on AC Power Loss	**Stay Off** / Last State / Power On
Power Restore Delay	**Disabled** / Auto / Fixed
Power Restore Delay Value	[60 – 300s, **60** is default]
Clear System Event Log	
FRB-2 Enable	**Enabled** / Disabled
OS Boot Watchdog Timer	Enabled / **Disabled**
OS Boot Watchdog Timer Policy	**Power off** / Reset
OS Boot Watchdog Timer Timeout	5 minutes / **10 minutes** / 15 minutes / 20 minutes
Plug & Play BMC Detection	Enabled / **Disabled**
Shutdown Policy	Enabled / **Disabled**
► Console Redirection	
► System Information	
► BMC LAN Configuration	

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

Figure 40. Server Management screen

1. **IPMI Security Policy Information**

   Value: **Allow All**/Restricted/Deny All

   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 at if it is functioning in any mode out of *'Allow All'*, *'Restricted'* and *'Deny All'*. This information will be suppressed if the BMC is functioning on any Unknown state.

   Back to: Server Management Screen– Screen map

2. **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 visible.`

   Comments: This option allows the system to generate a non-maskable interrupt (NMI) when a system error (SERR) occurs, which is a method legacy operating system error handlers may use instead of processing a machine check.

   Back to: Server Management Screen– Screen map

3. **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: This option allows the system to generate an NMI when a parity error (PERR) occurs, which is a method legacy operating system error handlers may use instead of processing a machine check.

   Back to: Server Management Screen– Screen map

4. **PCIe AER Support**

   Value: **Enabled**/Disabled

   Help Text: `[Enabled] – PCIe AER (Advanced Error Reporting) is enabled.`
   `[Disabled] – PCIe AER is disabled. All PCIe AER errors will be masked once PCIe AER is disabled.`

   Comments: This option allows the system to monitor and handle PCIe* advanced error reporting (AER) errors on PCIe devices with PCIe AER support. As described in the PCI Express Base Specification, any third-party software or OS could override this BIOS policy and take ownership of PCIe AER handling after BIOS POST.

   Back to: Server Management Screen– Screen map

5. **Log 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: This option allows the system to monitor and handle PCIe correctable errors on PCIe
              devices behind processor and platform controller hub (PCH). This option is only available
              when the PCIe AER Support option is enabled.

Back to: Server Management Screen– Screen map

6. **PCIe Correctable Error Threshold**

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

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

Comments: Specifies how many Correctable Errors must occur before triggering the logging of a SEL
              Correctable Error Event. Only the first threshold crossing is logged, unless 0 is selected
              which causes every CE that occurs to be logged.

Back to: Server Management Screen– Screen map

7. **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– Screen map

8. **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– Screen map

9. **Enforced Password Support**

Value: Enabled/**Disabled**

Help Text: `Enables or Disables the Enforced Password support. Enabling it will`
`allow the BIOS to send the Seed, Algorithm and password information`
`to BMC.`

Comments: No Comments

Back to: Server Management Screen– Screen map

10. **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 intelligent platform management interface (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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Note: The system automatically powers on after doing a CMOS clear when AC is applied because this option does not take effect in this situation.

Note: For Syscfg, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

Back to: Server Management Screen– Screen map

11. **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 10) 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.

     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 BMC will start to power on the host with no delay after it finishes BMC's IPMI stack initialization. There will still be a delay. The delay time depends on how long BMC needs to boot up 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 :Restricted*' and suppressed if shown as '*IPMI Security Policy:Deny All*'.

Note: 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.

Note: If Syscfg/Sysinfo 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 *Intel® Server Board S2600 Family BIOS EPS*, Section 7.1.3.

Back to: Server Management Screen– Screen map

12. 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Note: If Syscfg/Sysinfo support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

Back to: Server Management Screen– Screen map

13. Clear System Event Log

Value: None

Help Text: `Clears the System Event 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). 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 Event 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Back to: Server Management Screen– Screen map

14. 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 purposed 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 *Intel® Server Board S2600 Family BIOS EPS*, Sections 3.17.4, 6.1.1.1, and 10.5.1.

This option gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Back to: Server Management Screen– Screen map

15. 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 OS boot. The BIOS sets the timer before starting the OS bootstrap load procedure. If the OS boot watchdog timer times out, then presumably the OS failed to boot properly.

If the OS does boot up successfully, it must be aware of the OS boot watchdog timer and immediately turn it off before it expires. The OS may turn off the timer or, more often, the timer may be repurposed as an OS watchdog timer to protect against runtime OS hangs.

Unless the OS does have timer-aware software to support the OS boot watchdog timer, the system is unable to boot successfully with the OS 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 *Intel® Server Board S2600 Family BIOS EPS*, Sections 3.17.4, 6.1.1.2, and 10.5.1.2.

This option gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Back to: Server Management Screen– Screen map

16. 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 is disabled.

This option gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy :Restricted*' and suppressed if shown as '*IPMI Security Policy:Deny All*'.

Back to: Server Management Screen– Screen map

17. 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 is disabled.

This option gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy :Restricted*' and suppressed if shown as '*IPMI Security Policy:Deny All*'.

Back to: Server Management Screen– Screen map

18. Shutdown Policy

Value: Enabled/**Disabled**

Help Text: `Enable/Disable Shutdown Policy.`

Comments: This option is designed for multiple-node systems and to control the policy that the BMC should shut down one node if it detects over-current or over-temperature condition. The BIOS and the BMC synchronize the policy during the BIOS POST and the current value of the BMC is displayed in BIOS setup.

This option is only displayed when the BMC supports this feature on the node. For details on which platforms support it, refer to *Intel® Server Board S2600 Family BIOS EPS*, Chapter 12 and the BMC firmware EPS.

This option gets grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as '*IPMI Security Policy:Restricted*' and suppressed if shown as '*IPMI Security Policy:Deny All*'.

Note: If Syscfg/Sysinfo support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`.

Back to: Server Management Screen– Screen map

19. 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 OS server management software is able to find the BMC and automatically load the correct IPMI support software for it. If the OS 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Back to: Server Management Screen– Screen map

20. 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– Screen map

21. 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– Screen map

22. 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– 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.

```
                              Console Redirection


    SOL for Baseboard Mgmt            Enabled / Disabled
    SOL for Baseboard Mgmt2           Enabled / Disabled
    SOL for Dedicated Mgmt NIC        Enabled / Disabled
    Console Redirection               Disabled / Serial Port A/Serial Port B
    Flow Control                      None / RTS/CTS
    Baud Rate                         9.6k / 19.2k / 38.4k / 57.6k / 115.2k
    Terminal Type                     PC-ANSI / VT100 / VT100+ / VT-UTF8
    Legacy OS Redirection             Enabled / Disabled
    Terminal Resolution               80x25 / 100x31


              F10=Save Changes and Exit        F9=Reset to Defaults

    ↕←→=Move Highlight     <Enter> = Select Entry        Esc=Exit
```

Figure 41. 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

   Note: If Syscfg/Sysinfo support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`. This field does not support Intel Integrator Toolkit customization.

   Back to: Console Redirection – Server Management Screen– Screen map

2. **SOL for Baseboard Mgmt2**

Value: Enabled/**Disabled**

Help Text: `Enable/disable Serial Over LAN feature for Baseboard Management Lan 2. [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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Note: If Syscfg/Sysinfo support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`. This field does not support Intel Integrator Toolkit customization.

Back to: Console Redirection – Server Management Screen– Screen map

3. **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 *Intel® Server Board S2600 Family BIOS EPS*, 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 :Restricted'* and suppressed if shown as '*IPMI Security Policy:Deny All'*.

Note: If Syscfg/Sysinfo support is needed, this setting should get from BMC via IPMI but not from BIOS variable via `/bcs`. This field does not support Intel Integrator Toolkit customization.

Back to: Console Redirection – Server Management Screen– Screen map

4. **Console Redirection**

Value: **Disabled**/Serial Port A/Serial Port B

Help Text:
```
Console redirection allows a serial port to be used for server
management tasks.
```
```
[Disabled] – No console redirection.
[Serial Port A/B] – Configure serial port A/B for console
redirection.
```
```
Enabling this option will disable display of the Quiet Boot logo
screen during POST. [Advanced > Serial Port Configuration > Serial
A/B Enable] needs be enabled before enabling this option.
```

Comments: Serial console redirection can use either Serial Port A or Serial Port B. 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– Screen map

5. **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– Screen map

6. **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– Screen map

7. **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 native character encoding used by PC-compatible applications and emulators. For more information about character encoding, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 7.4.

   Back to: Console Redirection – Server Management Screen– Screen map

8. **Legacy OS Redirection**

   Value: Enabled/**Disabled**

   Help Text: `This option enables legacy OS redirection (i.e., DOS) on serial port. If it is enabled, the associated serial port is hidden from the legacy OS.`

   Comments: Operating systems that are redirection-aware implement their own console redirection mechanisms. For a legacy OS that is not aware, this option allows the BIOS to handle redirection.

   Back to: Console Redirection – Server Management Screen– Screen map

9. **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– 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.

System Information	
Board Part Number	<Board part number>
Board Serial Number	<Board serial number>
System Part Number	<System part number>
System Serial Number	<System serial number>
Chassis Part Number	<Chassis part number>
Chassis Serial Number	<Chassis serial number>
Asset Tag	<Asset tag>
BMC Status	<Current BMC status>
BMC Firmware Revision	<BMC firmware revision>
ME Status	<Current Intel® ME status>
ME Firmware Revision	<Intel ME firmware revision>
SDR Revision	<Sensor data record (SDR) revision>
UUID	< Universally unique identifier (UUID)>

F10=Save Changes and Exit   F9=Reset to Defaults

↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 42. 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:Deny All'*.

   Back to: System Information – Server Management Screen– 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:Deny All'*.

   Back to: System Information – Server Management Screen– 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:Deny All'*.

    Back to: System Information – Server Management Screen– 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:Deny All'*.

    Back to: System Information – Server Management Screen– 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:Deny All'*.

    Back to: System Information – Server Management Screen– 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:Deny All'*.

    Back to: System Information – Server Management Screen– 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:Deny All'*.

    Back to: System Information – Server Management Screen– Screen map

8. **BMC Status**

    Value: \<Current BMC status\>

    Help Text: None

    Comments: 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:Deny All'*.

Back to: System Information – Server Management Screen– 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:Deny All'*.

Back to: System Information – Server Management Screen– 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– Screen map

11. ME Firmware Revision

Value: <Intel ME firmware revision>

Help Text: None

Comments: *Information only.*

Back to: System Information – Server Management Screen– Screen map

12. SDR Revision

Value: <Sensor data record (SDR) revision>

Help Text: None

Comments: *Information only.* This information gets suppressed out if the *IPMI Security Policy information* on Server Management Screen is shown as '*IPMI Security Policy:Deny All'*.

Back to: System Information – Server Management Screen– Screen map

13. UUID

Value: <Universally unique identifier (UUID)>

Help Text: None

Comments: *Information only.*

Back to: System Information – Server Management Screen– 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", which 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. Any values changed by the user are communicated back to the BMC when a 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 will be shown if *IPMI Security Policy information* being displayed as "IPMI Security Policy:Restricted" 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:Deny All" on Server Management Screen.

Note: If Syscfg/Sysinfo support is needed, this all settings under BMC LAN Configuration should get from BMC via IPMI but not from BIOS variable via `/bcs`. This fields on this screen do not support Intel Integrator Toolkit customization.

BMC LAN Configuration

► User Configuration

Baseboard LAN configuration
IP Source	**Static**/Dynamic
IP Address	[0.0.0.0]
Subnet Mask	[0.0.0.0]
Gateway IP	[0.0.0.0]

Baseboard LAN IPv6 configuration
IPv6	Enabled/**Disabled**
IPv6 Source	**Static**/Dynamic
IPv6 Address	[0000.0000.0000.0000.0000.0000.0000.0000]
Gateway IPv6	[0000.0000.0000.0000.0000.0000.0000.0000]
IPv6 Prefix Length	[0 – 128, **64** is default]

Dedicated Management LAN Configuration
Remote Management Module	<Not Present/ Present >
IP Source	**Static**/Dynamic
IP Address	[0.0.0.0]
Subnet Mask	[0.0.0.0]
Gateway IP	[0.0.0.0]

Dedicated Management LAN IPv6 Configuration
Dedicated IPv6	Enabled**/Disabled**
IPv6 Source	**Static/**Dynamic
IPv6 Address	[0000.0000.0000.0000.0000.0000.0000.0000]
Gateway IPv6	[0000.0000.0000.0000.0000.0000.0000.0000]
IPv6 Prefix Length	[0 – 128, 64 is default]
BMC DHCP Host Name	[DHCP Host Name display/edit]

F10=Save Changes and Exit   F9=Reset to Defaults

↕←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 43. 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 :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

   Back to: BMC LAN Configuration – Server Management Screen– Screen map

2. **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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

   Back to: BMC LAN Configuration – Server Management Screen– 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 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

   Back to: BMC LAN Configuration – Server Management Screen– 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 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 the cable is connected, and IP Source has been set to be Dynamic, the default value of Subnet Mask, which 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– 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 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

6. **IPv6**

Value: Enabled/**Disabled**

Help Text: `Option to Enable/Disable IPv6 addressing and any IPv6 network traffic on these channels.`

Comments: The initial value for this field is acquired from the BMC. It may be changed to switch between IPv4 and IPv6 addressing technologies.

If this option is set to Disabled, all other IPv6 fields are not visible for the baseboard LAN. When IPv6 addressing is enabled, all IPv6 fields for the baseboard LAN become visible and all IPv4 fields are grayed out and inactive.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

7. **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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

8. **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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

9. **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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

10. **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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

11. Remote Management Module

Value: <Not Present/Present>

Help Text: None

Comments: *Information only.* Displays whether a dedicated management LAN component is currently installed. This information may come from querying the BMC.

When a Remote Management Module is installed, the Remote Management Module field only "Present". When no Remote Management Module is installed, this option is set to the value "Not Present".

When the Management Module is Not Present at all, the fields for Dedicated Management LAN Configuration will not be visible.

When IPv6 is disabled, the IPv4 configuration fields will be visible and the IPv6 configuration fields will not be visible. When IPv6 is enabled, the IPv4 fields will be grayed out and inactive, while the IPv6 Configuration fields will be visible.

In either case, the Dedicated Management Lan section IP Source or IPv6 Source will determine whether the IPv4 or IPv6 address fields are display-only or can be edited.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Note: The Intel® Remote Management Module 4 Lite (Intel® RMM4 Lite) NIC (dedicated NIC) should always available. The Remote Management Module field should display the Intel RMM4 Lite module status.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

12. 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:    BMC LAN Configuration – Server Management Screen– Screen map

**13. 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

**14. Subnet Mask**

Value: [Entry Field 255.255.255.0, **255.255.255.0 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 which comes from BMC and 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

**15. 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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– Screen map

### 16. Dedicated IPv6

Value:          Enabled/**Disabled**

Help Text:     `Enable/Disable Dedicated IPv6.`

Comments:    The initial value for this field is acquired from the BMC. It may be changed in order to switch between IPv4 and IPv6 addressing technologies for Dedicated LAN.

When this option is set to Disabled, all other IPv6 fields will not be visible for Dedicated Management DMN (if installed). When IPv6 addressing is enabled, all IPv6 fields for the Dedicated Management DMN will become visible, and all IPv4 fields for Dedicated LAN will be grayed out and inactive.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:       BMC LAN Configuration – Server Management Screen– Screen map

### 17. 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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:       BMC LAN Configuration – Server Management Screen– Screen map

### 18. 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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:       BMC LAN Configuration – Server Management Screen– Screen map

**19. 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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:        BMC LAN Configuration – Server Management Screen– Screen map

**20. 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.

This option is only visible when the IPv6 option is set to Enabled.

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 option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to:        BMC LAN Configuration – Server Management Screen– Screen map

## 21. 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 is set to Dynamic, then this BMC DHCP Host Name field is grayed out and inactive.

This option gets grayed out if the IPMI Security Policy information on Server Management Screen is shown as IPMI Security Policy :Restricted and suppressed if shown as IPMI Security Policy:Deny All.

Back to: BMC LAN Configuration – Server Management Screen– 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 will not be configurable and grayed out if the *IPMI Security Policy* information on Server Management Screen is shown as *'IPMI Security Policy:Restricted'* and suppressed if shown as *'IPMI Security Policy:Deny All'*.

```
                               User Configuration

Enable Complex Password              Enabled/Disabled
Error! Reference source not found.   anonymous
Privilege                            Callback/User/Operator/Administrator/No Access
User Status                          Enabled/Disabled
User Password

Error! Reference source not found.   User2
Privilege                            Callback/User/Operator/Administrator/No Access
User Status                          Enabled/Disabled
User Name                            [User Name display/edit]
User Password

Error! Reference source not found.   User3
Privilege                            Callback/User/Operator/Administrator/No Access
User Status                          Enabled/Disabled
User Name                            [User Name display/edit]
User Password

Error! Reference source not found.   User4
Privilege                            Callback/User/Operator/Administrator/No Access
User Status                          Enabled/Disabled
User Name                            [User Name display/edit]
User Password

Error! Reference source not found.   User5
Privilege                            Callback/User/Operator/Administrator/No Access
User Status                          Enabled/Disabled
User Name                            [User Name display/edit]
User Password

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

Figure 44. User Configuration screen

1. **Enable Complex Password**

   Value: **Disabled**/Enabled

   Help Text: Password should contain 8 to 20 characters which should include Uppercase letters A to Z, Lowercase letters a to z, Digits 0 to 9, at least a space or one of the following special characters:`~!@#$%^&*()-_=+\|[{}];:'",<.>/?

   Comments: This option is provided for customers to be able to go for any of two types of password strategy. If this option is disabled (default value), then the user does not have to follow any password strategy and can use any combination of 8-20 characters. Enabling this option leads users to use the complex password strategy for any password to be set and it is that the password must contain 8-20 characters, must have at least a space or one of the '~!@#$%^&*()-_ =+\|[{}];:'",<.>/?' special characters, must contain 'n Uppercase letters A to Z' and 'n Lowercase letters A to Z' and 'n Digits 0 to 9', cannot be the same as the user name or the user name in reverse order, and must have at least two new characters when compared to the previous password. BMC is requested to do complex password check when "Enable Complex Password" is set to "Enabled".

   Back to: User Configuration – BMC LAN Configuration – Server Management Screen– Screen map

2. **User ID**

   Value: anonymous/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– Screen map

3. **Privilege**

   Value: Callback/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– 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– 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 to 16 alpha-numeric characters or'.', '_' or '-', and must begin with alpha-numeric character or '_'. User Name cannot be changed for User1 (anonymous).`

Comments: The User Name field can only be edited for user IDs other than anonymous. The user names for user ID 1 cannot be changed and is always null/blank. 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– Screen map

6. **User Password**

Value: [Popup Entry Field, 0-20 characters]

Help Text: `Press <Enter> key to enter password. Minimum is 6 characters. Maximum length is 20 characters. Any ASCII printable characters can be used: case-sensitive alphabetic, numeric, and special characters.`

              `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– Screen map

3.6   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.

Note: USB devices can be "hotplugged" during POST and 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 hotplugged. 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.

There are two main types of boot order control – legacy boot and UEFI boot. These are mutually exclusive; when UEFI boot is enabled, legacy boot (the default) is disabled. Within legacy boot operation, there are two further methods of ordering boot devices – dynamic boot order and static boot order. For more information on these different boot option methods, refer to *Intel® Server Board S7200AP Family BIOS EPS*, Section 6.1.

The default for boot order control is legacy boot with dynamic boot order. If all types of bootable devices are installed in the system, then the default boot order is as follows:

- Legacy CD/DVD-ROM
- Legacy Floppy Disk Drive
- Legacy Hard Disk Drive
- Legacy PXE Network Device
- Legacy Boot Entry Vector (BEV) Device
- EFI Shell and EFI Boot paths

In this default boot order, a USB device may appear in any of several device classes, due to the flexibility of USB connections and USB emulation of various types of devices.

Note: A USB key (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 CDROM drive, it is not detected as such and is treated as a hard disk appearing in the list of available hard drives.

Figure 45. 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 3.6.1.

   Back to: Boot Maintenance Manager Screen – Screen map

2. **Legacy CDROM Order**

   Value: None

   Help Text: `Set the order of the legacy devices in this group.`

   Comments: *Selection only.* For more information on Legacy CDROM Order settings, see Section 3.6.2.

       This option appears when one or more bootable CDROM drives are available in the system and the Boot Mode options is set as Legacy. This includes USB CDROM devices but not USB keys formatted for CDROM emulation, which are seen as hard disk drives.

       Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

   Back to: Boot Maintenance Manager Screen – Screen map

3. **Legacy Hard Disk Order**

    Value: None

    Help Text: `Set the order of the legacy devices in this group.`

    Comments: *Selection only.* For more information on Legacy Hard Disk Order settings, see Section 3.6.3.

            This option appears when one or more bootable hard disk drives are available in the system and the Boot Mode options is set as Legacy. This includes USB hard disk devices and USB keys formatted for hard disk or CDROM emulation.

            Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

    Back to: Boot Maintenance Manager Screen – Screen map

4. **Legacy Floppy Order**

    Value: None

    Help Text: `Set the order of the legacy devices in this group.`

    Comments: *Selection only.* For more information on Legacy Floppy Order, see Section 3.6.4.

            This option appears when one or more bootable floppy disk drives are available in the system and the Boot Mode options is set as Legacy. This includes USB floppy disk devices and USB keys formatted for floppy disk emulation.

            Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

    Back to: Boot Maintenance Manager Screen – Screen map

5. **Legacy Network Device Order**

    Value: None

    Help Text: `Set the order of the legacy devices in this group.`

    Comments: *Selection only.* For more information on Legacy Network Device Order, see Section 3.6.5.

            This option appears when one or more bootable network devices are available in the system and the Boot Mode options is set as Legacy.

            Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

    Back to: Boot Maintenance Manager Screen – Screen map

6. **Legacy BEV Device Order**

    Value: None

    Help Text: `Set the order of the legacy devices in this group.`

    Comments: *Selection only.* For more information on Legacy DEV Device Order, see Section 3.6.6.

              This option appears when one or more bootable BEV devices are available in the system and the Boot Mode options is set as Legacy.

> **Note**: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

    Back to: Boot Maintenance Manager Screen – Screen map

7. **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 3.6.7.

              This option is only displayed if an EFI bootable device is available to the system.

> **Note**: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

    Back to: Boot Maintenance Manager Screen – Screen map

8. **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 3.6.8.

              This option is only displayed if an EFI boot path is included in the boot order.

> **Note**: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.
>
> **Note**: 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 – Screen map

9. **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 3.6.9.

Note: This field does not support Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Intel Integrator Toolkit customization.

Back to: Boot Maintenance Manager Screen – Screen map

3.6.1 Advanced Boot Options

The Advanced Boot Options screen allows the user to control the advanced boot options features like Boot Mode and Static Boot Order.

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.

```
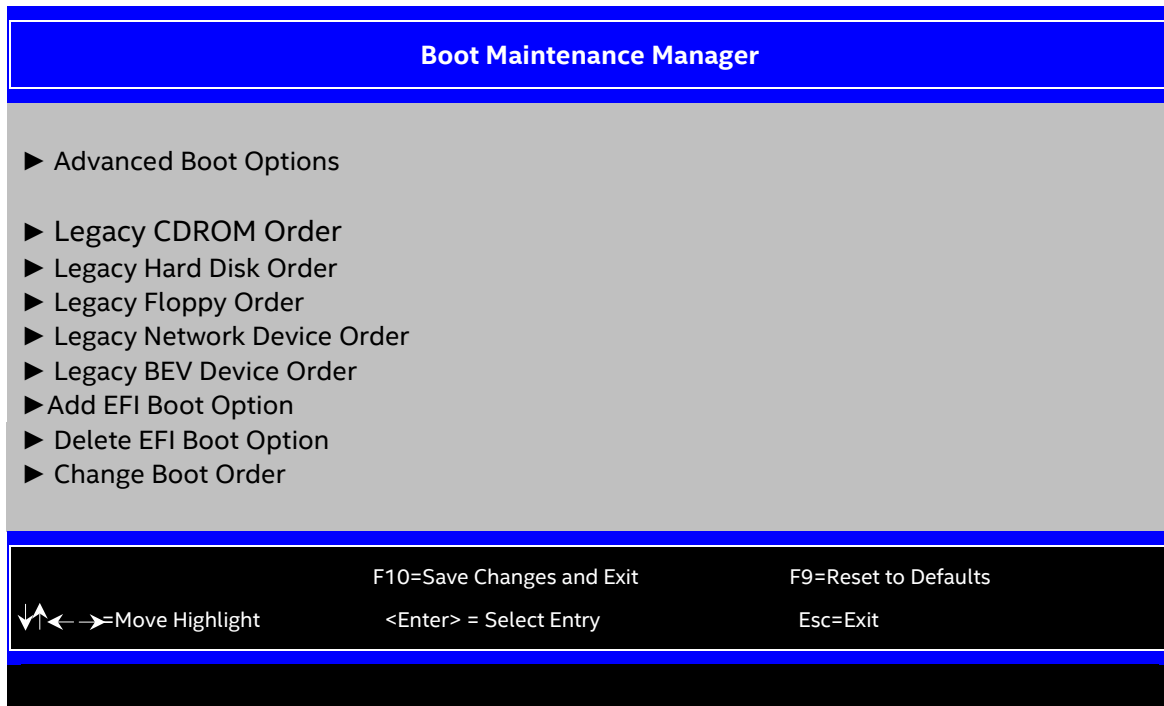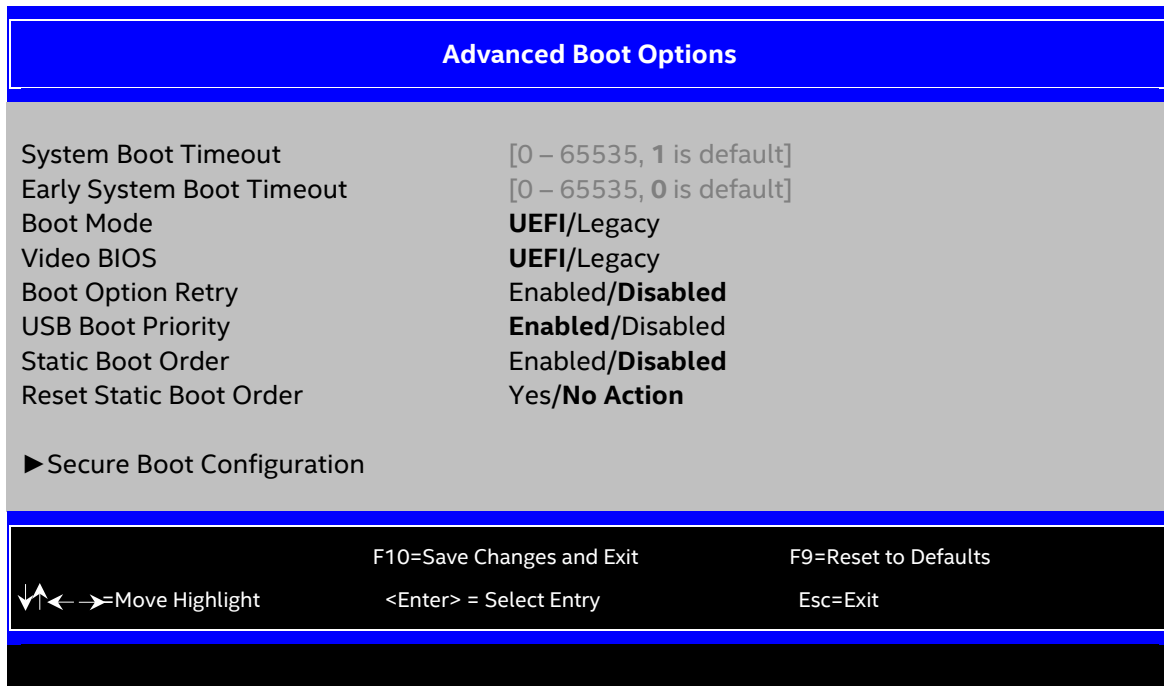                        Advanced Boot Options


System Boot Timeout                 [0 – 65535, 1 is default]
Early System Boot Timeout           [0 – 65535, 0 is default]
Boot Mode                           UEFI/Legacy
Video BIOS                          UEFI/Legacy
Boot Option Retry                   Enabled/Disabled
USB Boot Priority                   Enabled/Disabled
Static Boot Order                   Enabled/Disabled
Reset Static Boot Order             Yes/No Action

►Secure Boot Configuration


                  F10=Save Changes and Exit        F9=Reset to Defaults

 ↕←  →=Move Highlight        <Enter> = Select Entry            Esc=Exit
```

Figure 46. Advanced Boot Options screen

1. **System Boot Timeout**

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

   Help Text: The number of seconds the 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 – 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 – Screen map

3. **Boot Mode**

Value: **UEFI**/Legacy

Help Text: When Boot Mode is Legacy, the BIOS only loads modules required for booting Legacy Operating Systems.

When Boot Mode is UEFI, the BIOS only loads modules required for booting UEFI-aware Operating Systems.

Comments: When Boot Mode is Legacy, only Legacy Option ROMs and Legacy OS Boot are supported; UEFI option ROMs and UEFI OS Boot are not supported.

When Boot Mode is UEFI, Only UEFI option ROMs and UEFI OS boot are supported; Legacy option ROMs and Legacy OS Boot are not supported.

Note: For Intel® Server Board S2600BT, UEFI is the only available boot mode. Legacy mode is greyed out and not an option.

Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

4. **Video BIOS**

Value: **UEFI**/Legacy

Help Text: If Video BIOS is Legacy, the BIOS uses the legacy video ROM instead of the EFI video ROM when Boot Mode is UEFI.

Comments: This option appears only when Boot Mode option is set as UEFI. The default – UEFI – is to use UEFI Graphic Output Protocol (GOP); if it is Legacy, legacy video ROM is used.

If Boot Mode changes to Legacy, Video BIOS changes to Legacy and is hidden automatically.

Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

5. **Boot Option Retry**

    Value: Enabled/**Disabled**

    Help Text: `If enabled, this continually retries non-EFI-based boot options without waiting for user input.`

    Comments: This option is intended to keep retrying in cases where the boot devices are initially slow to respond, such as if the devices are asleep and do not wake quickly enough. However, if none of the devices in the boot order ever responds, the BIOS continues to reboot indefinitely.

    Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

6. **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: This option enables or disables the USB reorder functionality. Enabling USB Boot Priority allows a user to plug in a USB device and immediately boot to it, for example, in case of a maintenance or system administration operation. If a user password is installed, USB Boot Priority action is suspended. For more information, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 6.1.2.3.

    Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

7. **Static Boot Order**

    Value: Enabled/**Disabled**

    Help Text: `[Disabled] – Devices removed from the system are deleted from Boot Order Tables.`

                   `[Enabled] – Devices removed have positions in Boot Order Tables retained for later reinsertion.`

    Comments: This option appears only when the Boot Mode option is set as Legacy. If the Static Boot Order option is set to Enabled, it enables Static Boot Order (SBO) from the next boot onward and the current boot order is stored as the SBO template.

               If the option is set to Disabled, the SBO is disabled and the SBO template is cleared.

               For information about static boot options, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 6.1.2.2.

    Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

8. **Reset Static Boot Order**

Value: Yes/**No Action**

Help Text: `[Yes] Take snapshot of current boot order to save as Static Boot`
`Order Template.`

Comments: This option appears only when the Boot Mode option is set as Legacy. This option allows the user to save the boot order list as the SBO template without disabling and re-enabling the Static Boot Order option.

Select Yes to snapshot the current boot options list into the SBO list on the next boot. After saving the SBO list, this option changes back to No Action automatically.

This option is available only when the Static Boot Order option is enabled. Otherwise, it is grayed out and unavailable.

Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

9. **Secure Boot Configuration**

Value: None

Help Text: `Set the Secure Boot Configuration Options in this group.`

Comments: *Selection only.* This option appears only when Boot Mode option is chosen as UEFI as legacy boot mode does not support UEFI Secure Boot.

Back to: Advanced Boot Options – Boot Maintenance Manager Screen – Screen map

3.6.1.1   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 47. 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 below Attempt Secure Boot option.

    Note: This field does not support Syscfg display with the `/bcs` command. However, the Syscfg `/d sboot` commands can be used to show current secure boot status.

    Back to: Advanced Boot Options – Boot Maintenance Manager Screen – 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 to enable the UEFI secure boot feature. Once this feature is enabled, BIOS will provision the keys automatically during platform reset. BIOS will provision the default keys if the corresponding key is not present.

Notes:

Product BIOS will ship a default set of PK, KEK, db, and dbx in BIOS release images. BIOS will provision the keys for the first time user, enabling this option. After PK, KEK, db, and dbx provision, the user needs to use SysCfg to update these keys using digitally signed payloads (according to UEFI spec 2.3.1). When new BIOS capsule release contain new keys (in case of private key compromise or known security vulnerability):

- If user has already done the provision, the new keys will NOT be provisioned and old keys still take effect. Using SysCfg to update keys with signed payload is mandatory.

- If user has not yet done the provision (never enabled UEFI secure boot before), the new keys will be provisioned and take effect.

This option is protected by BIOS administrator password as the basic security level. More advanced security level requires that platform physical presence policy needs to be applied in order to change the secure boot feature control option. Therefore, Current Secure Boot State will not be always changed successfully after platform reset if the advanced security check fails.

For Syscfg related support, Secure Boot just supports proprietary solution defined in utility SysConfig EPS. The user can use SysCfg `/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:

3.6.2   Legacy CDROM Order

The Legacy CDROM Order screen allows the user to control the order in which the BIOS attempts to boot from the Legacy CDROM drives installed in the system. This screen is only available when there is at least one CDROM device available in the system configuration and the Boot Mode options is chosen as Legacy.

Note: A USB attached CDROM device appears in this section. However, a USB key formatted as a CRDOM device does not appear. It is detected as a hard disk device and included in the Hard Disk Order screen.

To access this screen from the front page, select **Boot Maintenance Manager** > **Legacy CDROM Order**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

Legacy CDROM Order	
CDROM #1	<Available CDROM devices>
CDROM #2	<Available CDROM devices>
F10=Save Changes and Exit	F9=Reset to Defaults
↓↑←→=Move Highlight <Enter> = Select Entry	Esc=Exit

Figure 48. Legacy CDROM Order screen

1. **CDROM #1**
2. **CDROM #2**

    Value: <Available CDROM devices>

    Help Text: `Set system boot order by selecting the boot option for this position.`

    Comments: Choose the order of booting among CDROM devices by choosing which available CDROM device should be in each position in the order.

    Back to: Legacy CDROM Order – Boot Maintenance Manager Screen – Screen map

3.6.3   Legacy Hard Disk Order

The Legacy Hard Disk Order screen allows the user to control the order in which the BIOS attempts to boot from the hard disk drives installed in the system. This screen is only available when there is at least one hard disk device available in the system configuration and the Boot Mode option is set as Legacy. A USB attached hard disk drive or a USB key device formatted as a hard disk appear in this section.

To access this screen from the front page, select **Boot Maintenance Manager** > **Legacy Hard Disk Order**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

Note: The BCV devices that are storage devices are also grouped in the Legacy Hard Disk Order screen.

Figure 49. Legacy Hard Disk Order screen

1. **Hard Disk #1**
2. **Hard Disk #2**

    Value: <Available hard disk devices>

    Help Text: `Set system boot order by selecting the boot option for this position.`

    Comments: Choose the order of booting among hard disk devices by choosing which available hard disk device should be in each position in the order.

    Back to: Legacy Hard Disk Order – Boot Maintenance Manager Screen – Screen map

3.6.4   Legacy Floppy Order

The Legacy Floppy Order screen allows the user to control the order in which the BIOS attempts to boot from the legacy floppy disk drives installed in the system. This screen is only available when there is at least one floppy disk (diskette) device available in the system configuration and the Boot Mode option is set as Legacy. A USB attached diskette drive or a USB key device formatted as a diskette drive appear in this section.

To access this screen from the front page, select **Boot Maintenance Manager** > **Legacy Floppy Order**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

Figure 50. Legacy Floppy Order screen

1. **Floppy Disk #1**
2. **Floppy Disk #2**

    Value: <Available floppy disk devices>

    Help Text: `Set system boot order by selecting the boot option for this position.`

    Comments: Choose the order of booting among floppy disk devices by choosing which available floppy disk device should be in each position in the order.

    Back to: Legacy Floppy Order – Boot Maintenance Manager Screen – Screen map

3.6.5   Legacy Network Device Order

The Legacy Network Device Order screen allows the user to control the order in which the BIOS attempts to boot from the network bootable devices installed in the system. This screen is only available when there is at least one network bootable device available in the system configuration and the Boot Mode options is set as Legacy.

To access this screen from the front page, select **Boot Maintenance Manager** > **Legacy Network Device Order**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

Legacy Network Device Order

Network Device #1   <Available bootable network devices>
Network Device #2   <Available bootable network devices>

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

Figure 51. Legacy Network Device Order screen

1. **Network Device #1**
2. **Network Device #2**

Value: <Available bootable network devices>

Help Text: `Set system boot order by selecting the boot option for this position.`

Comments: Choose the order of booting among network devices by choosing which available network device should be in each position in the order.

Back to: Legacy Network Device Order – Boot Maintenance Manager Screen – Screen map

3.6.6   Legacy BEV Device Order

The Legacy BEV Device Order screen allows the user to control the order in which the BIOS attempts to boot from the BEV devices installed in the system. This screen is only available when there is at least one BEV device available in the system configuration and the Boot Mode options is set as Legacy.

To access this screen from the front page, select **Boot Maintenance Manager** > **Legacy BEV Device Order**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

Legacy BEV Device Order
BEV Device #1   <Available BEV devices>
BEV Device #2   <Available BEV devices>
F10=Save Changes and Exit   F9=Reset to Defaults
⤒⤓←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 52. Legacy BEV Device Order screen

1. **BEV Device #1**
2. **BEV Device #2**

   Value: <Available BEV devices>

   Help Text: `Set system boot order by selecting the boot option for this position.`

   Comments: Choose the order of booting among BEV devices by choosing which available BEV device should be in each position in the order.

   Back to: Legacy BEV Device Order– Boot Maintenance Manager Screen – Screen map

3.6.7   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.

Add EFI Boot Option

EFI Boot Option to be selected

F10=Save Changes and Exit   F9=Reset to Defaults

↓↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 53. 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 – Screen map

3.6.8   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.

<div style="border:1px solid #000;">

Delete EFI Boot Option

EFI Boot Option to be deleted

Save Changes

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

</div>

Figure 54. Delete EFI Boot Option screen

1. **EFI Boot Option to be deleted**

    Value: [Checkbox]

    Help Text: `Select one to delete.`

    Comments: Use the checkbox 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 – Screen map

3.6.9   Change Boot Order

The Change Boot Order screen allows the user to configure the desired order of legacy or 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.

Change Boot Order

Change the order   <Available boot options>

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

Figure 55. Change Boot Order screen

1. **Change the order**

   Value: <Available boot options>

   Help Text: Choose the boot order of booting Devices. Use [+] or [-] key to move up/down the selected field.

   Comments: None

   Back to: Change Boot Order– Boot Maintenance Manager Screen – 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.

```
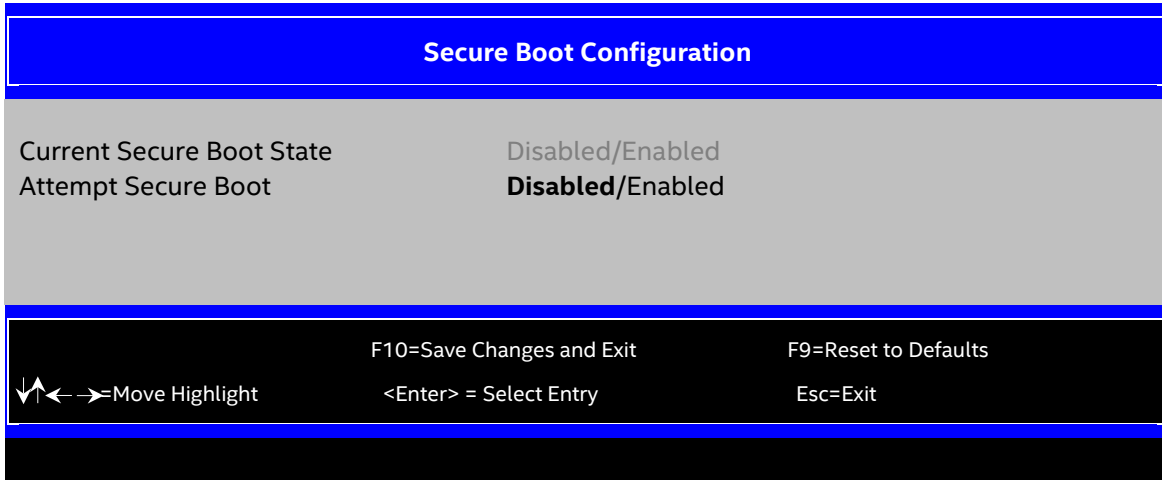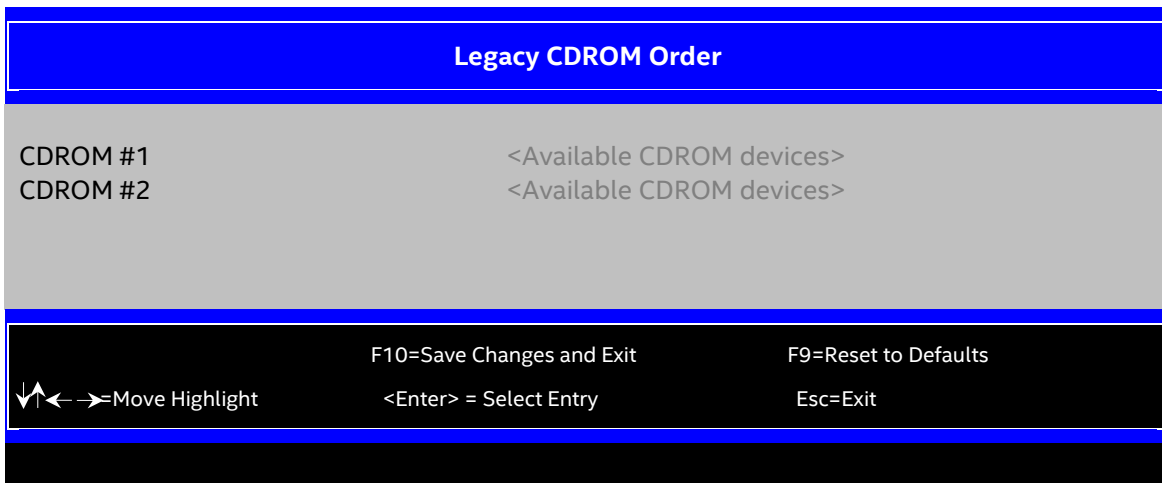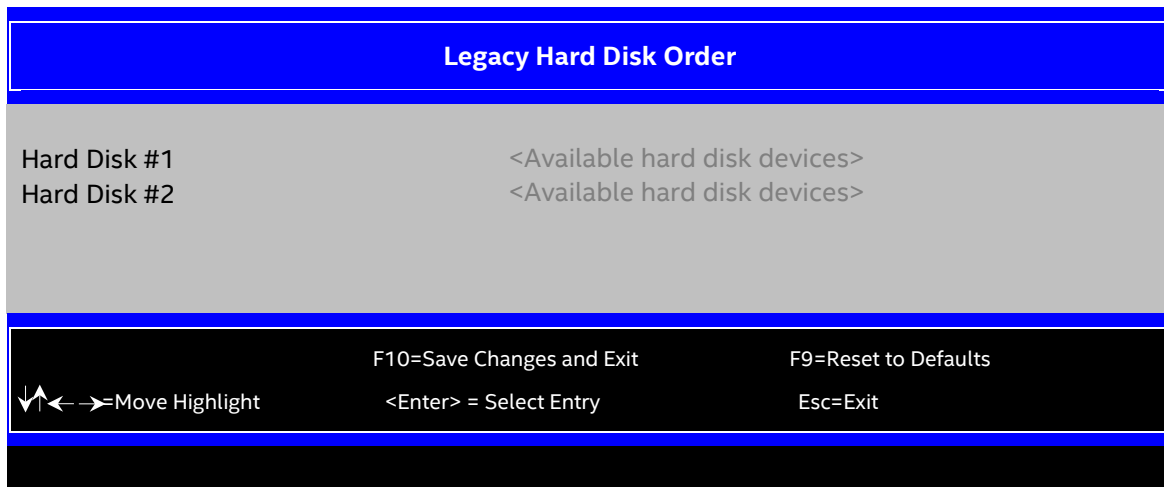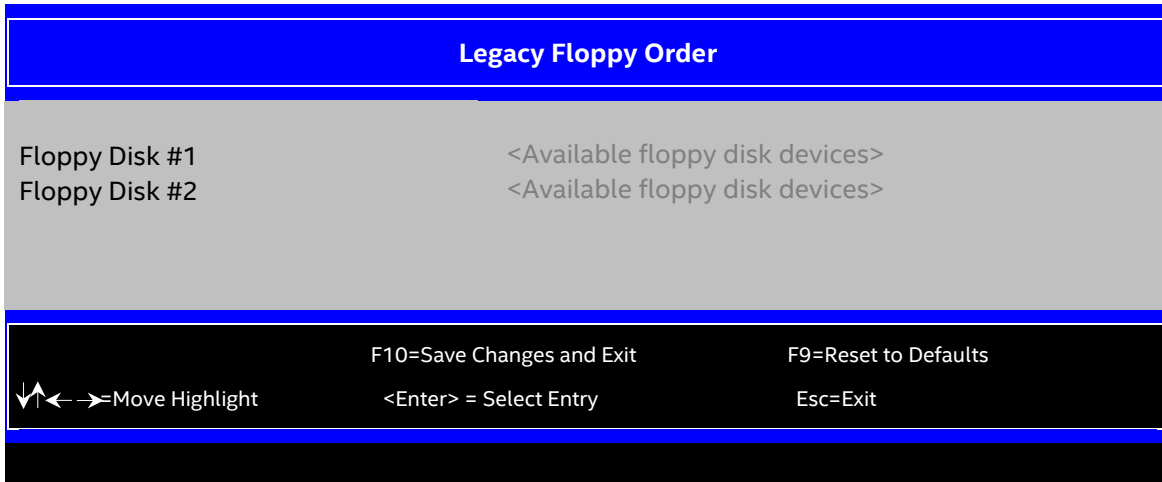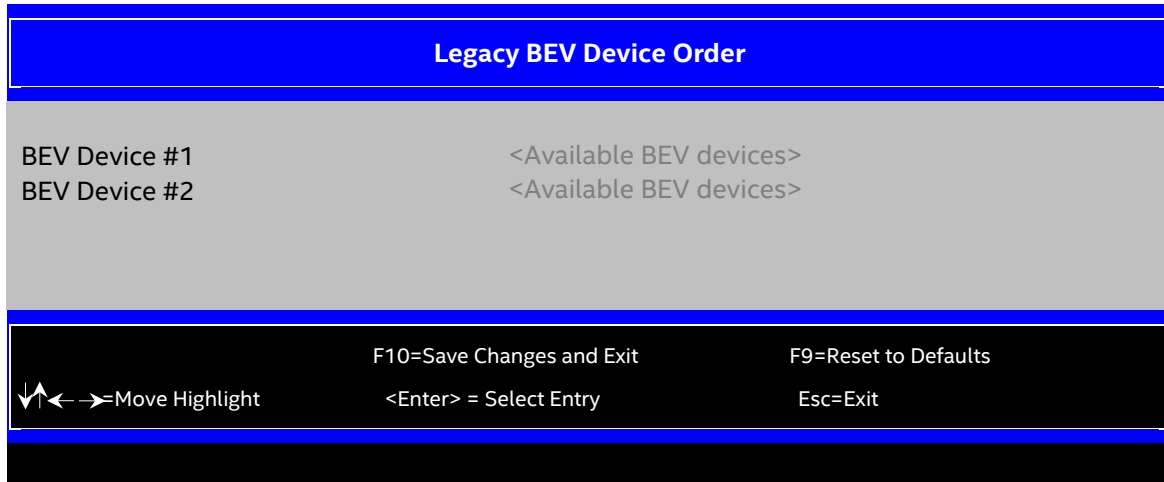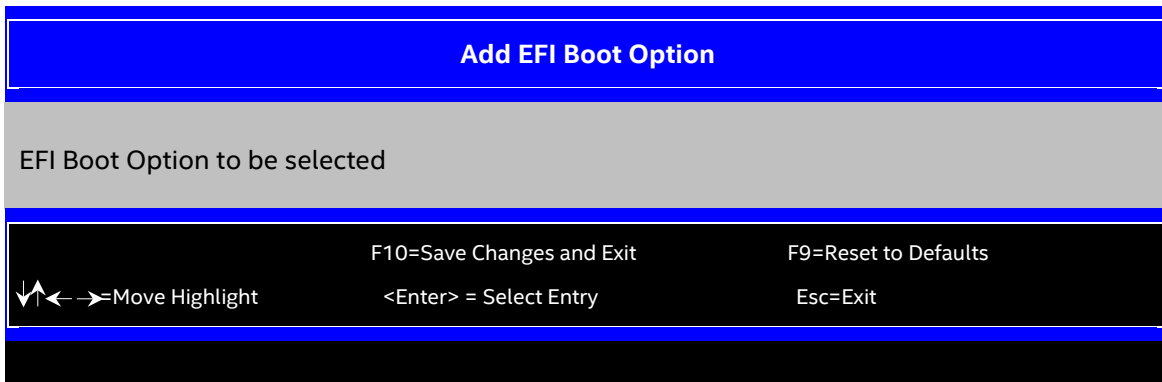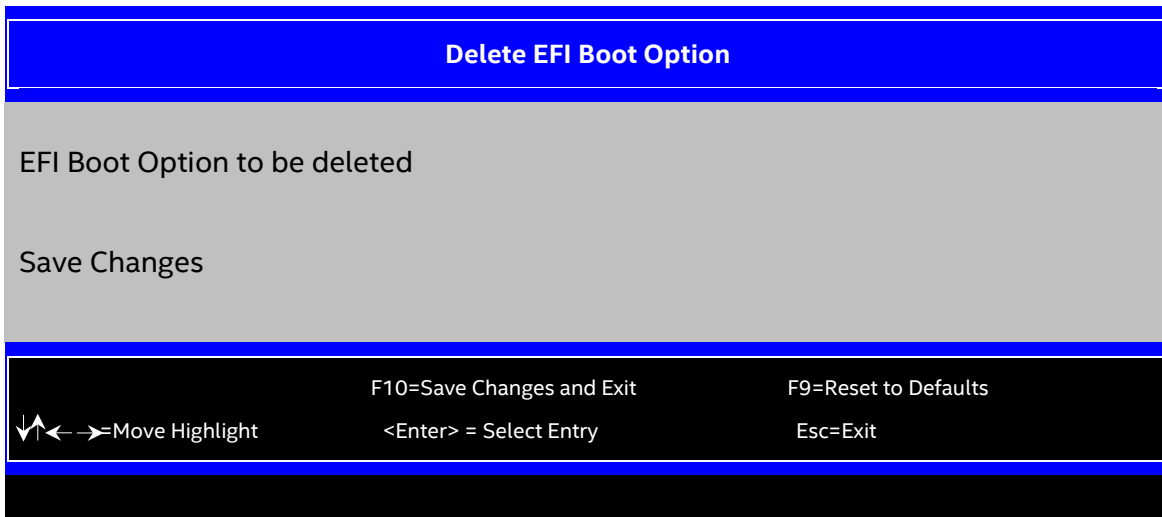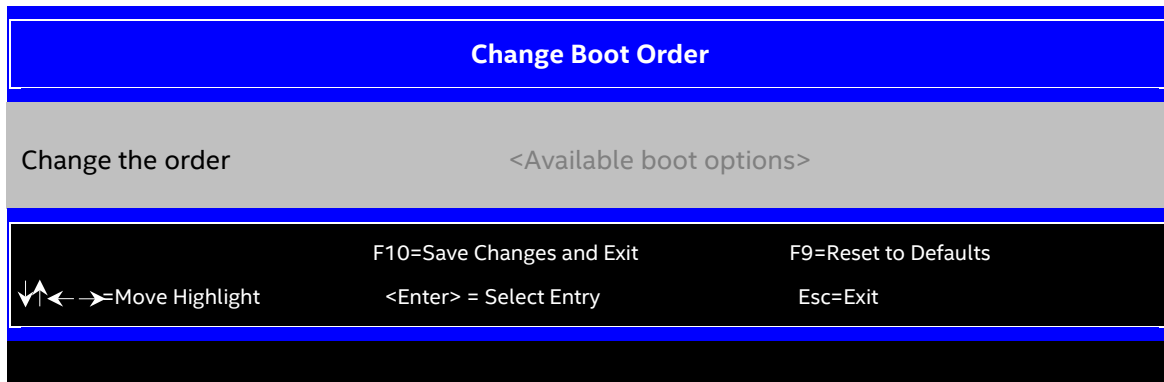                                    Boot Manager


      Launch EFI Shell
      Legacy Floppy Driver
       <Boot device #1>
      Legacy Hard Disk Driver
       <Boot device #2>
      Legacy CD-ROM Driver
       <Boot device #n>
      Legacy NET Driver
       <Boot device #n>
      Legacy BEV Driver
       <Boot device #n>




                  F10=Save Changes and Exit          F9=Reset to Defaults

     ↕↔=Move Highlight           <Enter> = Select Entry              Esc=Exit
```

Figure 56. Boot Manager screen

1. **Launch EFI 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 Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order.

     Back to: Boot Manager Screen – 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 from which to initiate a one-time boot. 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 Syscfg changes with the `/bcs` command. However, the Syscfg `/bbo` or `/bbosys` commands can be used to set boot order.

Back to: Boot Manager Screen – Screen map

3.8   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 57. 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 *Intel® Server Board S7200AP Family BIOS EPS*, Section 10.11.5.

   Back to: Error Manager Screen – Screen map

2. **SEVERITY**

   Value: Minor/Major/Fatal

   Help Text: N/A

   Comments: Each POST error code has a severity associated with it. For more information on POST error codes, refer to *Intel® Server Board S2600 Family BIOS EPS*, Section 10.13.5.

   Back to: Error Manager Screen – 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 – 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 58. 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 – 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 – 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 – 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 – Screen map

5. **Load Default Values**

Value: None

Help Text: `Load Defaults 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 – 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 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.

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 options are in this scope, such as Power Restore Policy, thermal related options, and all settings under BMC LAN Configuration.

3.10 Tls Auth Configuration

TLS Auth configuration allows the user to set the authentication mode. It supports three authentication modes that are listed below:

1. **Two-way authentication:** Authentication of both parties. In this mode, both server and client will be authenticated.

2. **One-way authentication:** Server authentication with an unauthenticated client.That means only the server is authenticated by the client, and the client will not be authenticated by the server.

3. **Total anonymity:** The server and client will not authenticate each other.

Tls Auth Configuration
► Server CA configuration
► Client Cert Configuration
F10=Save Changes and Exit   F9=Reset to Defaults
↕←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

Figure 60. Tls Auth Configuration.

1. **Server CA Configuration**

Value: None

Help text: Press <Enter> to configure Server CA.

Comments: *Selection only.* This option allows the user to configure Server CA. Once this option is selected, the user can input the CA certificate from the file system.

Back to: Tls Auth Configuration – Screen map

2. Client Cert Configuration

Value: None

Help text: Client cert configuration is unsupported currently.

Comments: *Selection only.* This option provides user to configure Client certificate configuration which is not supported on sever BIOS as of now.

Back to: Tls Auth Configuration – Screen map

3.10.1   Server CA Configuration

This is the main form which allows the user to configure Server CA. This allows to both enroll the required certificate files and also to delete the certificates which are not required.

<div style="border:1px solid #000;">

Server CA Configuration

► Enroll Cert

► Delete Cert

F10=Save Changes and Exit   F9=Reset to Defaults

↕↑←→=Move Highlight   <Enter> = Select Entry   Esc=Exit

</div>

Figure 61. Server CA Configuration.

1. **Enroll Cert**

Value: None

Help text: Press <Enter> to enroll cert.

Comments: *Selection only.* Select this line and press the **<Enter>** key to enroll the cert.

Back to: Server CA Configuration – Screen map

2. Delete Cert

Value: None

Help text: Press <Enter> to delete cert.

Comments: *Selection only.* Select this line and press the **<Enter>** key to delete the cert.

Back to: Server CA Configuration – Screen map

3.10.1.1   Enroll Cert

Figure 62. Enroll Cert.

1. Enroll Cert Using File

Value: None

Help text: Enroll Cert Using File.

Comments: *Selection only.* This helps to choose the Cert files from the file systems. User can input certificate file using this option. Certifcate file can be copied to UEFI file system using USB keys or any other supported media.

Back to: Enroll Cert – Screen map

2. Cert GUID

Value: GUID

Help text: Input digit character in 11111111-2222-3333-4444-1234567890ab format.

Comments: *The Cert GUID is provided as input in the format mentioned in the Help Text.*

Back to: Enroll Cert – Screen map

3. Commit Changes and Exit

Value: None

Help text: Commit Changes and Exit.

Comments: *Selection only.* Select this line and press the **<Enter>** key to commit the changes.

Back to: Enroll Cert – Screen map

4. Discard Changes and Exit

Value: None

Help text: Discard Changes and Exit.

Comments: *Selection only.* Select this line and press the **<Enter>** key to discard the changes.

Back to: Enroll Cert – Screen map

Appendix A. 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 OS 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 OS.
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	Boot strap 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
DCPMM	Data Centre 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

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 OS. 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
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
MBR	Master Boot Record
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.
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
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
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 malicious software to execute code. |